SEIKO

導入・運用の手引
Installation and Operation Manual

ロードバランサー

NetwiSer

SX-3990
SX-3950
SX-3945
SX-3940
SX-3920

第９版
2023 年 3 月 28 日
U00141574409

セイコーソリューションズ株式会社

はじめに

このたびは、＜セイコーソリューションズ製品＞をお買い上げいただきまして、誠にありがとうございます。

安全にお使いいただくために必ずお守りください

本書には、あなたや他の人への危害や財産への損害を防ぐために、守っていただきたい事項について表示と図記号が記述されています。
内容をよく理解してから本文をお読みいただくようお願いいたします。

表示と図記号の意味

本体および説明書に使われる表示

⚠ 警告	この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容を示しています。
⚠ 注意	この表示を無視して誤った取り扱いをすると、人が障害を負う可能性が想定される内容、および物的損害だけの発生が想定される内容を示しています。

本書（導入運用の手引）に使われることがある表示と図記号

⚠ 注意	この表示を無視して誤った取り扱いをすると、本商品の本来の性能を発揮できず、機能停止をまねく内容を示しています。
ポイント	この表示は本商品を取り扱う上で知っておくと便利な内容、もしくは間違いを防ぐ内容、機器の仕様などを示しています。

本書に記載された製品（ソフトウェアを含む）の使用に起因する損失、逸失利益などの請求につきましては、いかなる責任も負いかねます。

上記の各表示と図記号は、機器および説明書によって使用しない場合があります。たとえば、「危険」表示がない機器および説明書や、「お願い」表示のない説明書があります。

⚠ 警告	
	＜本機＞の分解（ネジをとる、ふたを外すなど）、および改造を行わないでください。火災・感電の原因となります。
	異常音がしたり、＜本機＞が熱くなっている状態のまま使用すると、火災・感電の原因となります。すぐに本体の電源を切り、差し込みプラグをコンセントから抜いて弊社サービス窓口に点検をご依頼ください。
	万一、煙が出ている、異臭がするなどの異常状態のまま使用すると、火災・感電の原因となります。すぐに本体の電源を切り、その後、必ず差し込みプラグをコンセントから抜き、煙が出なくなるのを確認して弊社サービス窓口に修理をご依頼ください。お客様による修理は危険ですから絶対におやめください。
	＜電源コード＞を傷つけたり、破損したり、加工したり、無理に曲げたり、引っ張ったり、ねじったり、たばねたりしないでください。また重いものを乗せたり、加熱したりすると＜電源コード＞が破損し、火災・感電の原因となります。＜電源コード＞が傷んだら弊社サービス窓口に修理をご依頼ください。
	万一、内部に異物（金属片、水、液体など）が入った場合は、まず本体の電源を切り、差し込みプラグをコンセントから抜いて、弊社サービス窓口にご連絡ください。そのまま使用すると、火災・感電の原因となります。
	ぬれた手で差し込みプラグを抜き差ししないでください。感電の原因となります。

⚠ 注意	
	ぐらついた台の上や傾いた所など不安定な場所に置かないでください。落ちたり、倒れたりして、けがの原因となることがあります。
	＜本機＞の上に花びん、植木鉢、コップ、化粧品、薬品や水および飲み物の入った容器、または小さな金属類を置かないでください。こぼれたり、中に入った場合、火災・感電の原因となります。
	風呂場や加湿器のそばなど、湿度の高いところでは使用しないでください。火災・感電の原因となります。
	プラグを抜くときは電源コードを引っ張らないでください。（必ずプラグを持って抜いてください。）コードが傷つき、火災、感電の原因となることがあります。
	＜本機＞を移動させる場合は、必ず電源プラグをコンセントから抜いて行ってください。コードが傷つき、火災、感電の原因となることがあります。
	電源プラグは奥まで確実に挿入してください。火災、感電の原因となることがあります。
	万一、＜本機＞を落としたり、破損した場合、本体の電源を切り、差し込みプラグをコンセントから抜いて、弊社サービス窓口にご連絡ください。そのまま使用すると、火災・感電の原因となります。

本　書　の　使　い　方

本書は、SX-3990,SX-3950,SX-3945,SX-3940,SX-3920 ロードバランサーの導入・運用の手引です。

関連文書には「SX-3990_3950_3945_3940_3920 コマンドリファレンス」、[SX-3990 インストールガイド]「SX-3950 取扱説明書」、「SX-3945,40 取扱説明書」、「SX-3920 取扱説明書」があります。

目次

［　空　白　］

第1章　概要

本製品は、接続された機器への負荷分散をおこない、ネットワーク環境の効率、可用性を高める負荷分散装置/ソフトウェアです。本章では、本製品のおもな特長と機能の概要を説明します。

1.1 主な特長

■IPv6 対応
アドレス枯渇の心配のないIPv6に対応しています。

■SSL 対応
SSL 処理機能を全機種、標準搭載しています。

■日本語 GUI（Graphical User Interface）
わかりやすい洗練されたデザインを採用し、運用・管理の負担を減らせます。
各設定項目にはヘルプボタンが用意され、更に数値入力欄にマウスカーソルを重ねると制限値が表示されるため、設定入力時の作業負担が軽減されます。
また、利用者の設定ポリシーに合わせた設定項目のみを表示させておく事ができるため、シンプルでわかり易い設定画面にカスタマイズできます。

■かんたん設定【SX-3920 のみ】
GUI により手軽に設定ができる、「かんたん設定」機能を搭載しています。わずか 5 項目の入力で基本設定が完了します。

■機能が向上した CLI（Command Line Interface）
コマンド補完機能が強化され、すべてのパラメーターが補完可能です。この機能により入力時に入力コマンドの候補が表示出来るためコマンドをすべて覚える必要がなく設定作業が楽になります。また従来通りのコマンド省略もサポートしています。

■使いやすい設定保存機能
冗長構成時の機器故障などの場合に必要となる設定のコピーが簡単に行えるコマンドを用意しています。

1.2 機能概要

1.2.1 負荷分散機能

本製品は、以下の負荷分散機能をサポートしています。

■負荷分散
負荷分散アルゴリズムとして、ラウンドロビン、重み付きラウンドロビン、最小コネクション、重み付き最小コネクションの4通りの負荷分散方法を選択できます。

■セッション維持
クライアントIPアドレス、SSLセッションID、HTTP Cookie、HTTP Cookie挿入、X-Forwarded-For セッションの 5 通りのセッション維持方式を選択できます。

■DSR（Direct Sever Return）
DSR 機能は、クライアントへの下りのパケットを本製品を経由せずにサーバー機器より直接返送する方式です。この機能により、動画再生などの下りのデータ量が多いアプリケーションでも本製品がボトルネックとなることを防ぎます。

■URL スイッチング
URL に含まれるコンピューター名やプロトコル、ファイル名などを識別し処理を特定のサーバーへ振り分ける機能です。

■IPv4⇔IPv6 SLB（Server Load Balance）機能
IPv4⇔IPv6 SLB機能は、IPv6 または IPv4 クライアントからのリクエストを IPv4 または IPv6 サーバーへ振り分ける機能です。

1.2.2 故障監視機能

■ヘルスチェック機能

本製品にはサーバーの稼働状態をチェックするヘルスチェック機能があります。ICMP、TCP コネクション、SSL コネクション、UDP のほか、アプリケーションレベルの HTTP、FTP、SMTP、POP3、IMAP4、NTP、DNS、HTTPS のチェックが可能です。

1.2.3 冗長機能

■冗長構成

本製品を2台で使用し、マスター、バックアップの冗長構成で使用することが可能です。また、設定情報やセッション情報のリアルタイム同期や一括同期など、豊富な同期機能をサポートしています。

■フェイルスルー機能【SX-3940,SX-3920 のみ】

フェイルスルー機能とは、本製品に何らかの障害が発生し処理が継続出来ない場合、ポート1とポート2をハードウェアにより直結することができる機能です。このため万が一本製品に障害が発生しても、提供中のサービスを止めることなくサービスを継続することが可能です。主に小規模向けのサービスに有効な機能です。

1.2.4 SSL アクセラレーション機能

本製品が SSL 処理を肩代わりすることで、レイヤー7での SSL 負荷分散が可能です。

■ソフトウェア SSL アクセラレーション機能

本製品はソフトウェアによる SSL 処理機能を標準で搭載しています。

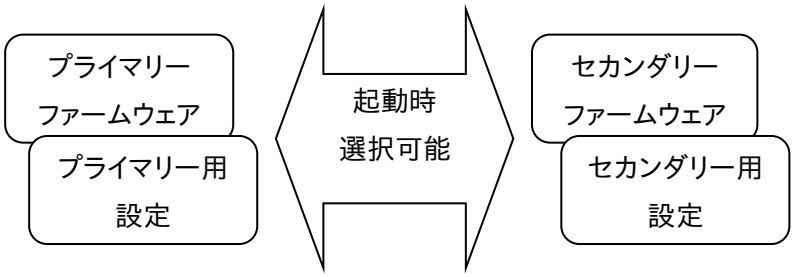
■ハードウェア SSL アクセラレーション機能

SX-3950,SX-3945,SX-3940 は、ハードウェア SSL アクセラレーション機能（以下 SSL オプション）を出荷時オプションとしてご用意しています。SSL オプションを搭載するとソフトウェアによる SSL 処理と比較し、より高速な SSL 処理が可能です。

1.2.5 運用・管理機能

■ファームウェア2重化

本製品は、ファームウェアのバージョンをプライマリー、セカンダリーとして2種類保持することが可能です。バージョンアップ時に何らかの原因により失敗した場合でも、切り戻し作業を迅速に行うことが可能です。



■SNMP機能

本製品には、SNMP エージェント機能がありますので、負荷分散の状況、トラフィック量などを、SNMP マネージャーより取得することが可能です。また SX-3950,SX-3945,SX-3940,SX-3920 は、ハードウェアの障害を SNMP トラップで通知する機能もあります。

■統計・管理機能

本製品の WEB 管理画面では、各種設定や動作状況の確認が行えます。またリアルタイムの通信状況表示や過去の統計情報などの確認が簡単に行えます。

■メール通知機能

本製品は、SYSLOG をメールで送信する機能があります。使用する場合は、メールサーバーのIPアドレス、送信元メールアドレス、宛先メールアドレスの設定を行います。

1.3 機種間の相違点

SX-3950,SX-3945,SX-3940,SX-3920 は、専用のハードウェアで動作します。これらの製品は、処理性能やポート数などの以下の違いがあります。

	SX-3950	SX-3945	SX-3940	SX-3920
1Gb RJ45 ポート数	10	10	6	3
10Gb SFP+ポート数※1	2	―	―	―
フェイルスルー機能	―	―	○	○
SSL ソフトウェア	○	○	○	○
SSL オプション※2	○	○	○	―
冗長電源	○	―	―	―

※1　10Gb SFP+光トランシーバモジュールはオプションです。
※2　ハードウェアにより SSL を高速処理する出荷時オプションです。

SX-3990 は、ハイパーバイザ上に定義された仮想マシンに対して、弊社の提供する仮想イメージファイルをインストールすることで、ソフトウェアロードバランサとして動作します。

第2章　コンフィグレーションガイド（CLI 編）

2.1 概要

本章では、本製品の設定作業について、コマンドラインインターフェイス（以下、CLI）上での設定方法を例とともに記します。
SX-3990 は、設定作業を開始するまえに、本ソフトウェアをハイパーバイザー上にインストールする必要があります。詳しくは**「SX-3990 インストールガイド」**（別紙）を参照してください。
各入力値の範囲や制限等の情報は、**「SX-3990_3950_3945_3940_3920 コマンドリファレンス」**（別紙）を参照してください。
また、WEB 管理画面を使用した設定方法は「第3章コンフィグレーションガイド（WEB 管理画面編）」を参照してください。

ポイント

本章で CLI とは、コマンドプロンプト画面を指す場合があります。
たとえば、「CLI にログインする」とは、「端末を使用してコマンドプロンプト画面にログインする」ことを指します。

2.1.1 はじめに

シリアルコンソールから設定する場合は、VT100 エミュレーションを使用してください。動作確認済みの VT100 エミュレータとして「Tera Term(Pro)」があります。VT100 エミュレータの接続プロパティを以下のように設定してください。

ボー・レート:　9600bps
データ長:　8bit
パリティ:　none
ストップ・ビット:　1bit
フロー制御:　none

本製品へはシリアルコンソール以外にも、telnet、ssh で CLI へログインできます。また、WEB ブラウザを使用して WEB 管理画面へログインできます。

本製品のユーザーアカウント情報は全てのログイン方法において共通化されています。CLI へアクセスする場合も、WEB 管理画面へアクセスする場合も、共通のユーザー名、パスワードを使用してログインします。

システムの初期状態から設定を始める際は、項目「2.5初期設定」を参考にしてください。

2.2 コマンドラインインターフェイスについて

本章では、本製品のコマンドラインインターフェイス（以下、CLI）について説明します。

2.2.1 コマンドの使用方法

コマンドの文法や入力値の範囲、またはコマンド文法の見方の説明は**「SX-3990_3950_3945_3940_3920 コマンドリファレンス」**（別紙）を参照してください。

2.2.2 設定モード

本製品は、複数の設定モードを持ちます。階層化された各種設定モード上でコマンドを実行します。

階層①	グローバルモード		
階層②	特権モード		
	仮想サーバー設定モード	VLAN 設定モード	Firewall ルール設定モード
	リバース NAT 設定モード	NAT プール設定モード	MAC アクセスリスト設定モード
	VRRP 設定モード	ヘルスチェック設定モード	IP アクセスリスト設定モード
階層③	SSL 設定モード	イーサネット設定モード	チャネル設定モード

2.2.2.1 グローバルモード

シリアルコンソールや、telnet、ssh で本製品へログインすると、グローバルモードに移行します。グローバルモードでは特権モードへの移行、機器情報の参照、設定情報のエクスポート等が行えます。また、パスワード変更など、限られた範囲で設定の変更が行えます。

```
Netwiser (Netwiser) (pts/0)
```

```
login: adm
Password:
Netwiser>
```

グローバルモード上で *config* コマンドを実行すると、特権モードに移行します。ただし、readonly 権限のユーザーアカウントは *config* コマンドの実行権限を持ちません。
グローバルモードで使用可能なコマンドは、*config* コマンドを除き、特権モードでも使用することができます。

また、以下の様に、admin 権限(または sub-admin 権限)と readonly 権限とではプロンプト上に表示される記号が異なります。

```
netwiser>
```

admin 権限(または sub-admin 権限)

```
netwiser$
```

readonly 権限

2.2.2.2 特権モード

グローバルモードから *config* コマンドで移行します。本製品の基本設定や、各種設定モードへの移行が可能です。
複数ユーザーが同時に CLI へログインすることは可能ですが、特権モードに遷移できるのは 1 ユーザーだけです。

```
netwiser> config
netwiser(config)#
```

2.2.2.3 VLAN 設定モード

特権モードから *interface vlan* コマンドで移行します。VLAN の設定を登録・変更できます。

```
netwiser> config
netwiser(config)# interface vlan 1
```

```
netwiser(config-vlan)#
```

2.2.2.4 イーサネット設定モード

特権モードから *interface ethernet* コマンドで移行します。イーサネットポートの設定を登録・変更できます。

下記のようにハイフン(-)やカンマ(,)を使用して範囲を指定することで、複数ポートの設定を変更することができます。

```
netwiser> config
netwiser(config)# interface ethernet 1-4,6
netwiser(config-if)#
```

2.2.2.5 チャネル設定モード

特権モードから *interface channel* コマンドで移行します。チャネルインターフェイスの設定を登録・変更できます。

イーサネット設定モードとは違い、複数のチャネル番号を指定することはできません。

```
netwiser> config
netwiser(config)# interface channel 1
netwiser(config-channel)#
```

2.2.2.6 IP アクセスリスト設定モード

特権モードから *access-list {ipv4 | ipv6}*コマンドで移行します。VLAN インターフェイスに対してパケットの許可・拒否を行うための、IP アクセスリストを登録・変更できます。

IPv4 アクセスリストを登録する場合 *ipv4* を、IPv6 アクセスリストを登録する場合 *ipv6* を指定します。

```
netwiser> config
netwiser(config)# access-list ipv4 ipv4_acl
netwiser(config-acl)#
```

2.2.2.7 MAC アクセスリスト設定モード

特権モードから *access-list mac* コマンドで移行します。イーサネットポートに対してパケットの許可・拒否を行うための、MAC アクセスリストを登録・変更できます。

```
netwiser> config
netwiser(config)# access-list mac mac_acl
netwiser(config-mac-acl)#
```

2.2.2.8 VRRP 設定モード

特権モードから *vrrp instance 0* コマンドで移行します。VRRP プライオリティーなどの設定値を登録・変更できます。第二引数は省略可能ですが、指定する場合必ず 0 を指定します。

```
netwiser> config
netwiser(config)# vrrp instance 0
netwiser(config-vrrp)#
```

2.2.2.9 NAT プール設定モード

特権モードから *nat-pool* コマンドで移行します。本製品の NAT 処理で使用するためのアドレスプールを登録・変更できます。

```
netwiser> config
netwiser(config)# nat-pool np_1
netwiser(config-natpool)#
```

2.2.2.10 リバース NAT 設定モード

特権モードから *reverse-nat* コマンドで移行します。サーバーから発信されるパケットに対する NAT 処理の設定を登録・変更できます。

```
netwiser> config
netwiser(config)# reverse-nat np_1.0.tcp
netwiser(config-reverse-nat)#
```

2.2.2.11 SSL 設定モード

特権モードから *ssl* コマンドで移行します。SSLアクセラレーションで使用するための SSL 証明書ポリシーを登録します。

```
netwiser> config
netwiser(config)# ssl cert_1-2048
netwiser(config-ssl)#
```

2.2.2.12 仮想サーバー設定モード

特権モードから *virtual* コマンドで移行します。仮想サーバー設定を登録・変更できます。

```
netwiser> config
netwiser(config)# virtual 192.168.1.100.80.tcp
netwiser(config-virtual)#
```

2.2.2.13 ヘルスチェック設定モード

特権モードから *probe* コマンドで移行します。サーバーに対するヘルスチェック設定を登録・変更できます。

```
netwiser> config
netwiser(config)# probe server_A 192.168.1.10.80.tcp
netwiser(config-probe)#
```

2.2.2.14 Firewall ルール設定モード

特権モードから *ipfw-list {ethport | vlan}* コマンドで移行します。VLAN インターフェイスに対してパケットの許可・拒否を行うための、ファイアウォールルールリストを登録・変更できます。

VLAN にファイアウォールルールリストを登録する場合 *vlan* を指定します。イーサネットポート、または論理チャネルにファイアウォールルールリストを登録する場合 *ethport* を指定します。

```
netwiser> config
```

```
netwiser(config)# ipfw-list ethport <list-name>
netwiser(config-eth-ipfw)#
  または
netwiser(config)# ipfw-list vlan <list-name>
netwiser(config-vlan-ipfw)#
```

2.2.3 機能

本製品のコマンドラインインターフェイスには以下の機能があります。

2.2.3.1 コマンドヘルプ

コマンドプロンプト上で*?*を入力すると、現在遷移している設定モードで実行可能なコマンドのヘルプメッセージが表示されます。

```
netwiser> ?
clear           Clear the machine data.
config          Entering to configuration mode.
exit            Exit from current mode.
export          Get a file from a machine.
help            Command usage.
no              Delete settings or set its defaults.
passwd          Change the password.
ping            Send ICMP echo messages.
ping6           Send ICMPv6 echo messages.
show            Show information.
terminal        Set terminal settings.
traceroute      Survey the path of network.
traceroute6     Survey the path of network.
```

コマンドのパラメーターとして「*?*」を入力する事で、パラメーター毎のヘルプメッセージを出力する事も可能です。
また、それらのパラメーターが省略可能で、その時点でコマンドが実行可能である場合、以下のようにヘルプメッセージの最後の行に<cr>と表示されます。

```
netwiser(config)# write erase ?
all             All configuration. (mean 'clear config all' command)
current         Current boot area.
Primary         Primary boot area.
Secondary       Secondary boot area.
<cr>
```

固定文字列以外のパラメーターは、カギ括弧<>で囲まれて表示されます。
括弧内の内容に沿ったパラメーターを入力してください。

```
netwiser(config)# arp ?
<ipv4-addr>        IP address or ip-name.
aging-time         Set arp entry timeout.
```

該当コマンドの実行を許可する全ての設定モードの中で、最も低い階層のモードでのみ、ヘルプメッセージが出力されます。その他のモードでは TAB 補完等は行えますがヘルプメッセージの表示は行いません。
たとえば、*ping* コマンドは全ての設定モードで実行可能ですが、ヘルプメッセージの出力はグローバルモードでしか行われません。

また、任意の入力値を指定するパラメーターの場合、ヘルプメッセージで入力値の範囲や制限を表示します。設定の際の参考にしてください。
以下に表示の例を挙げます。

■文字列パラメーター

パラメーターに文字列を取る場合、設定可能な文字列の最大長を明示します。

```
netwiser(config)# probe ?
<probe-name>        <STRING> [max-length:64]
```

■数値パラメーター

パラメーターに数値を取る場合、設定可能な数値の範囲を明示します。

```
netwiser(config)# terminal history-size ?
<size>        <NUM> [range:0-500]
```

■時間パラメーター

パラメーターに時間の文字列を取る場合、設定できる時間の範囲を明示します。

```
netwiser(config-virtual)# timeout ?
<time-expression>        <TIME> [range:0s-365d]
```

本製品の時間に関する入力は、<日>d<時>h<分>m<秒>s のように入力します。たとえば、「2 日と 12 時間 30 分 50 秒」を入力したい場合、「*2d12h30m50s*」のように入力します。
上の例で挙げた[range:0s-365d]では、0 秒～365 日の範囲で時間指定が可能であることを意味します。

更に、*help*コマンドを使用することでコマンドの文法を表示させることが可能です。ただし、遷移している設定モード上で実行可能なコマンドのみ *help*コマンドは実施可能です。たとえば、*arp*コマンドは特権モードでのみ *help*コマンドのパラメーターとして指定可能です。また、ヘルプコマンドのパラメーターは TAB 補完機能を使用できず、省略形でのコマンド実行もできません。

```
netwiser(config)# help arp
Commands available:
    arp <ipv4-addr> <mac-addr>
no arp <ipv4-addr>
    arp aging-time <time-expression(hm)>
no arp aging-time
```

2.2.3.2 TAB 補完

「TAB キー」を押下する事で、コマンド文字列やパラメーターの固定文字列の補完が可能です。
入力した文字列に前方一致するコマンドが複数存在する場合は、補完可能な文字数分だけが補完されます。

また、コマンドが一意に特定できるだけの十分な入力がされていれば、省略形でのコマンド実行も可能です。

```
netwiser> show running-config virtual
↓  省略
netwiser> sh ru vi
```

入力パラメーターが「任意の文字列」と「特定の文字列」の両方をとり得る場合、TAB 補完機能を使用することはできず、省略形での実行も認められません。たとえば以下の場合、固定文字列"*restrict*"は「TAB キー」での補完や省略形での実行はできません。

```
netwiser(config)# ntp ?
<ip-addr>        IP address or ip-name.
restrict         Does not make the exchange of ntp packet with
                 the NTP server other than the config.
Netwiser(config)# ntp r  ← 補完も省略もできない
```

2.2.3.3 自動ログアウト

CLI 上で、最後に「Enter キー」が入力されてから任意の時間が経過すると、該当のユーザーアカウントは自動的にログアウトします。自動ログアウト時間のデフォルトは 10 分です。

自動ログアウト時間の変更や、自動ログアウト機能を無効化することも可能です。詳細は「2.6.1.1自動ログアウト」を参照してください。

2.2.3.4 コマンド履歴

CLI 上で入力した入力履歴を上下キーで辿ることが可能です。保持しておく履歴件数はデフォルトで 20 件です。

これは、ログインセッション毎（ユーザーがログインしてから、ログアウトするまで）の履歴であり、ログアウトすると履歴はクリアされます。

履歴件数の変更や、履歴機能を無効化することも可能です。詳細は「2.6.1.2コマンド履歴保存件数」を参照してください。

2.2.3.5 ページ単位出力

showコマンドの出力をページ単位に表示します。

ページ単位出力機能を設定で無効化する事は可能ですが、無効化されるのはログアウトするまでの間です。

設定変更の詳細は「2.6.1.3ページ単位出力」を参照してください。

2.2.3.6 grep 機能

コマンドラインの末尾にパイプ(|)を指定する事で、「show」コマンドの出力に対して、grep オプションを使用する事が可能です。
grep オプションを使用する事で、任意の文字列が含まれる行のみを出力します。

```
netwiser> show running-config | grep “interface ethernet 1”
interface ethernet 1
interface ethernet 10
netwiser>
```

grep には以下のオプションを指定することができます。

オプション	説明	使用例
-v	任意の文字列が含まれる行以外を出力	*show running-config | grep -v interface*
-c	任意の文字列が含まれる行をカウント	*show running-config | grep -c interface*

2.2.3.7 ショートカットキー

本製品では、以下のショートカットキーが使用可能です。

キー	実行内容
Ctrl + A	カーソル位置を行頭まで移動する
Ctrl + E	カーソル位置を行末まで移動する
Ctrl + F	カーソル位置から右に一文字移動する
Ctrl + B	カーソル位置から左に一文字移動する
Ctrl + U	一行削除する
Ctrl + K	カーソル位置より右側を全て削除する
Ctrl + W	カーソル位置より左側を全て削除する
Ctrl + H	カーソル位置の直前の一文字を削除する
Ctrl + D	カーソル位置の直後の一文字を削除する
Ctrl + J	改行する
Ctrl + P	コマンドの履歴を戻る
Ctrl + N	コマンドの履歴を進む
[Home]	カーソル位置を行頭まで移動する
[End]	カーソル位置を行末まで移動する

2.2.4 CLI 制限

CLI には、以下の制限が設けられています。

■入力文字数の制限

一行に入力可能な文字は最大 1056 文字です。

■引用符を使用する際の制限

文字列内に単一引用符(')や二重引用符(")を使用する場合は、バックスラッシュ(¥)でエスケープし、更に二重引用符で囲んで使用してください。

例)command　“aaa¥”bbb"

■行末に入力できない文字

入力行の末尾にバックスラッシュ(¥)を使用することはできません。

■入力文字列に「?」を含ませる場合

「?」はヘルプメッセージ出力のための特別なキーとして定義されており、そのままでは入力文字列内に「?」を含ませることはできません。

「?」を文字列に含ませたい場合は、「Ctrl+v」を押下した後に「?」を入力してください。

■文字列パラメーター末尾の入力制限

文字列パラメーターの末尾にバックスラッシュを使用することはできません。

例)command　"abc¥"　　←失敗します

■複数ユーザーのログイン

複数ユーザーが同時に CLI へログインすることは可能ですが、特権モードに遷移できるユーザーは 1 人だけです。複数ユーザーが同時に特権モードに遷移することはできません。また、冗長構成時のコマンド同期機能が有効である場合、自機器か冗長相手機器のどちらか一方のみが特権モードに遷移できます。

2.3 設定数制限

本項では、各種設定の登録件数制限をまとめて記します。

特権モード		
access-list ipv4	IPv4 アクセスリスト	128 件 ＊ IPv4,IPv6 合計
access-list ipv6	IPv6 アクセスリスト	
access-list mac	MAC アクセスリスト	128 件
arp	静的 ARP テーブル	128 件
import content	sorry コンテンツインポート	32 件
interface vlan	VLAN ID 設定数	128 件
ipfw-list	ファイアウォールルールリスト	128 件
logging host	SYSLOG サーバー	4 件
logging to	SYSLOG 配信の宛先メールアドレス	16 件
mac address	静的 MAC アドレステーブル	128 件
name	IP 名	512 件
nat-pool	NAT プールエントリー	256 件
ndp	静的 NDP テーブル	128 件
ntp	NTP サーバー	4 件
probe	ヘルスチェックポリシー	1024 件
real	実サーバーID	512 件 ＊ IPv4 256 件 IPv6 256 件
reverse-nat	リバース NAT	256 件
route	静的ルート	128 件
rule	HTTP 負荷分散ルール	1024 件
snmp host	SNMP マネージャーアドレス	4 件
snmp trap trigger	トラップ送信のトリガーにするログ文字列	16 件
ssh	SSH リモートアクセス許可	32 件
ssl	SSL ポリシー	256 件
telnet	TELNET リモートアクセス許可	32 件
user-mgmt	ユーザーアカウント	4 件
virtual	仮想サーバーID	512 件 ＊ IPv4 256 件 IPv6 256 件
web-mgmt	HTTP リモートアクセス許可(WEB 管理画面へのアクセス許可)	32 件

VLAN 設定モード		
ip virtual-address	仮想 IP アドレス	512 件 ＊ IPv4 256 件 IPv6 256 件
NAT プール設定モード		
ip address	プールアドレス	16 件 *1
仮想サーバー設定モード		
bind	実サーバーバインド	256 件 ＊ 仮想サーバー毎
match <net-addr>	IP スイッチングルール	256 件 ＊ 仮想サーバー毎
match <rule-name>	URL スイッチングルール	32 件 ＊ 仮想サーバー毎
match redirect	リダイレクト設定	
match forbid	403 応答設定	
ssl	SSL アクセラレーション（SNI 登録数）	32 件 ＊ 仮想サーバー毎
permit-nat-filter	ソース NAT フィルター設定	256 件 ＊ 仮想サーバー毎
リバース NAT 設定モード		
bind	バインド登録	256 件 ＊リバース NAT ポリシー毎
IPv4 アクセスリスト設定モード		
line	IPv4 ACL ルール	128 件 ＊アクセスリストポリシー毎
IPv6 アクセスリスト設定モード		
line	IPv6 ACL ルール	128 件 ＊アクセスリストポリシー毎
MAC アクセスリスト設定モード		
line	MAC ACL ルール	128 件 ＊アクセスリストポリシー毎
ファイアウォールルールリスト設定モード		
line	ファイアウォールルール	127 件 ＊ルールリストポリシー毎

*1 システム全体で登録可能な件数（ただし、仮想サーバーIP アドレスとして登録されているアドレスは登録制限に含まれない）

2.4 設定の保存

本製品の CLI にログインし設定の変更を行った場合、必ず *write memory* コマンドで設定内容を保存してください。

write memory コマンドは特権モードより高い階層なら、いずれの設定モードでも実行可能です。

2.5 初期設定

本章では、システムの初期状態から設定を始める場合について、本製品に対してネットワーク経由でアクセス可能にするまでの流れを説明します。

2.5.1 デフォルトユーザーアカウント / デフォルトアドレス

本製品には、初期ユーザーアカウントとして"adm"が登録されています。
パスワードも同様に"adm"です。
また、初期状態では全てのイーサネットポートに対してアドレス
'192.168.0.1/24'（VLAN 1）が割り当てられています。

```
login: adm
Password: adm
netwiser>
```

2.5.2 パスワードの変更・ユーザーアカウントの管理

admin 権限のユーザーアカウントを新規に作成します。

```
netwiser> config
netwiser(config)# user-mgmt <ユーザー名> password <パスワード> permissio
n admin
```

readonly 権限のユーザーアカウントを作成したい場合は、*permission* のパラメーターに *readonly* を指定します。

更に、WEB 管理画面へログインした際に、画面カスタマイズ操作を実施できないユーザーアカウント権限を作成するには *sub-admin* を指定します。
画面カスタマイズ機能に関しての詳細は「3.6画面カスタマイズ機能」を参照し

てください。

また、*no user-mgmt* コマンドで、ユーザーアカウントの削除を行えます。
以下、デフォルトのユーザーアカウント'adm'を削除します。

```
netwiser> config
netwiser(config)# no user-mgmt adm
```

ポイント

自ユーザーアカウント（現在、ログインしているアカウント）は削除できません。別アカウントでログインし直してから削除してください。

ポイント

登録済みのユーザーアカウントの権限を変更することはできません。
一度削除してから再度登録し直してください。

また、パスワードを変更したい場合は *passwd* コマンドを使用します。

```
netwiser> passwd

New Password:
Retype New Password:
password changed successfully
netwiser>
```

2.5.3 機器 IP アドレスの変更

システムの初期状態では全てのポートが VLAN 1 に定義されています。

デフォルト VLAN（VLAN 1）の初期アドレスである'192.168.0.1/24'は削除または変更することが可能です。

以下、例として VLAN 10 に管理用の IP アドレスを割り当て、さらにイーサネットポート10を VLAN 10 に割り当てます。また、最後に VLAN 1 の IP アドレスを削除します。

```
  ① VLAN 10 に任意の IP アドレスを割り当てる
netwiser> config
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.10/24
netwiser(config-vlan)# exit
  ② イーサネットポート 10 に VLAN 10 を割り当てる
netwiser(config)# interface ethernet 10
netwiser(config-if)# vlan 10
  ③ システムの初期アドレスを削除
netwiser(config)# interface vlan 1
netwiser(config-vlan)# no ip address 192.168.0.1/24
netwiser(config-vlan)# exit
```

VLAN インターフェイスとイーサネットポートや論理チャネルとの関連は、*show vlan* コマンドで確認できます。詳細は**「SX-3990_3950_3945_3940_3920 コマンドリファレンス」**（別紙）を参照してください。

⚠ 注意

IP アドレスにリンクローカルアドレス（IPv4： 169.254.0.0/16, IPv6: fe80::/10）を指定しないでください。
これは、機器 IP アドレスだけではなく、IP アドレスを指定する必要のある全ての設定において共通の制限です。

2.5.4 管理専用ポートの定義

任意の単一ポートを管理専用ポートとして設定できます。管理専用ポートは、管理 IP アドレスやそのポートを経由するアクセスを制限します。

以下、例としてイーサネットポート10を管理専用ポートとして定義します。

```
netwiser> config
netwiser(config)# interface ethernet 10
netwiser(config-if)# slb mgmt secure
netwiser(config-if)# exit
```

以下、管理専用ポートの動作を説明します。

■管理 IP アドレスへのアクセスを制限する

管理専用ポートに設定されたポートが所属する VLAN の管理 IP アドレス、または冗長アドレスへは、管理専用ポートからのみアクセス可能であり、その他のポートからアクセスすることはできません。

また、管理専用ポートでないポートが所属する VLAN の管理 IP アドレスへは、管理専用ポートからアクセスできません。

■管理専用ポートを経由するアクセスを制限する

管理専用ポート以外のポートで受信したパケットを、管理専用ポートへ転送しません。

また、管理専用ポートで受信したパケットを、管理専用ポート以外のポートへ転送しません。

■負荷分散パケットの遮断

管理専用ポートでは、負荷分散パケットを送受信しません。

管理専用ポートを設定するうえで、以下のような制限があります。

- ✓ 管理専用ポートは任意の 1 ポートにのみ設定可能です
- ✓ 管理専用ポートが所属する VLAN に対して、その他のポートを割り当てることはできません
- ✓ 管理専用ポートが所属する VLAN には、必ず管理 IP アドレスが設定されている必要があります
- ✓ 管理専用ポートが所属するVLANには、仮想サーバーIPを設定することはできません

- ✓ 管理専用ポートはアクセスポートである必要があります
- ✓ 管理専用ポートは論理チャネルに所属することはできません
- ✓ 管理専用ポートに対して spanning-tree 設定をすることはできません

⚠ 注意

管理専用ポートの設定が存在し、かつ特定のポートをトランクポートに設定する場合は、*allowed-vlan* コマンドにより、許可する VLAN タグの ID を明示的に設定し、その際に、管理専用ポートの所属する VLAN の ID を除外してください。*allowed-vlan* の設定は「2.7.3 タグ VLAN の設定」を参照してください。

2.5.5 デフォルトルーターと経路情報の設定

デフォルトルーターの IPv4 アドレスを設定します。

```
netwiser(config)# route 0.0.0.0/0 <IPv4 ｱﾄﾞﾚｽ>
```

IPv6 アドレスであれば、以下のように設定します。

```
netwiser(config)# route ::/0 <IPv6 ｱﾄﾞﾚｽ>
```

デフォルト以外の経路情報を設定する必要がある場合は以下のコマンドを使用します。

```
netwiser(config)# route <ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ/ﾈｯﾄﾏｽｸ> <ﾙｰﾀｰ IP ｱﾄﾞﾚｽ>
```

設定を削除するには以下のコマンドを使用します。

```
netwiser(config)# no route <ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ/ﾈｯﾄﾏｽｸ> <ﾙｰﾀｰ IP ｱﾄﾞﾚｽ>
```

IPv4 ネットワークの経路情報であれば、<ネットマスク>をアドレス表記で指定することも可能です。

```
netwiser(config)# route <IPv4 ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ> <ﾏｽｸｱﾄﾞﾚｽ> <ﾙｰﾀｰ IP ｱﾄﾞﾚｽ>
```

本製品ではルーティングテーブルをルート ID 単位に複数持つことができます。テーブルの ID(ルート ID)を設定するには以下のように *id*オプションを使用します。

```
netwiser(config)# route 0.0.0.0/0 <IPv4 ｱﾄﾞﾚｽ> id <num>
netwiser(config)# route ::/0 <IPv6 ｱﾄﾞﾚｽ> id <num>
netwiser(config)# route <ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ/ﾈｯﾄﾏｽｸ> <ﾙｰﾀｰ IP ｱﾄﾞﾚｽ> id <num>
```

設定できるルート ID の範囲は 0 から 15 です。*id*オプションを指定しない場合はルート ID 0 が設定されます。

ポイント

ルート ID は VLAN 設定モード、仮想サーバー設定モード、リバース NAT 設定モードで使用することができます。
各モードでは使用するルーティングテーブルのルート ID を指定できます。

ポイント

traceroute コマンドを除き、自機発のパケット(*ping* コマンド, ヘルスチェック等)にはルート ID を指定することができません。ルート ID 0 が使用されます。

ポイント

Netwiser に設定されているどの VLAN のネットワークアドレスにも合致しない IP アドレスを、ゲートウェイアドレスに指定することはできません。
また、ルーティングエントリーを登録後に、ゲートウェイアドレスが合致するネットワークを持つ VLAN に対して以下の変更を行う場合、該当のルーティングエントリーを削除してから設定を変更する必要があります。

- ✓ 該当の VLAN を削除したい場合
- ✓ 該当の VLAN に設定された IP アドレスを削除したい場合
- ✓ 該当の VLAN に設定された IP アドレスを、別のネットワークアドレスへ変更したい場合

ポイント

本製品の管理 IP アドレスへの接続は VLAN に設定されているルート ID が使用されません。ルート ID 0 が使用されます。
PING への応答は VLAN に設定されているルート ID が使用されます。

2.5.6 リモートアクセスの許可

デフォルト設定では、telnetを使用した本製品へのリモートアクセスは許可されていません。更に、WEB 管理画面への HTTP アクセスは HTTPS へリダイレクトされます。

本製品への telnet でのアクセスや、WEB 管理画面への HTTP アクセスを許可するには、以下のように設定します。

```
  ①  全ての端末から、 telnet アクセスを許可する
netwiser> config
netwiser(config)# telnet 0.0.0.0/0
netwiser(config)# telnet ::/0
  ②  HTTP アクセスを HTTPS にリダイレクトしない
netwiser(config)# no web-mgmt auto-redirect
```

リモートアクセスに関するフィルタリング設定の詳細は「2.6.2リモートアクセスフィルターの設定」を参照してください。

2.5.7 設定ファイルをインポートする場合

あらかじめ本製品からエクスポートしておいた設定情報を取り込むことが可能です。

本製品への設定情報のインポートは「5.3.1設定情報のインポートとファームウェアアップグレード」を参照してください。

2.6 基本設定

2.6.1 リモート端末設定

2.6.1.1 自動ログアウト

本製品へのログイン後、リモート端末に対して一定時間入力がなければ自動的にログアウトします。
自動ログアウト時間の変更や無効化を行うには、*terminal auto-logout* コマンドを使用します。
デフォルトは 10 分です。セキュリティポリシーに合う間隔を設定してください。

```
netwiser(config)# terminal auto-logout 30m
```

自動ログアウト機能を無効化するには、時間に 0 を指定するか、*no terminal auto-logout* で設定を削除します。

```
netwiser(config)# terminal auto-logout 0m
```

設定した自動ログアウトタイマーは WEB 管理画面にも適用されます。
WEB 管理画面では、自動ログアウト時間が経過した場合再度パスワードの入力が求められます。

2.6.1.2 コマンド履歴保存件数

端末上に保持するコマンド履歴の件数はデフォルトで 20 件です。
変更するには *terminal history* コマンドを使用します。

```
netwiser(config)# terminal history-size 500
```

これは、ログインセッション毎（ユーザーがログインしてから、ログアウトするまで）の履歴であり、ログアウトすると履歴はクリアされます。
また、コマンド履歴機能を無効化することで、上下キーでコマンド履歴を辿ることができなくなります。無効化するには、履歴件数に 0 を指定するか、*no terminal history-size* で設定を削除します。

現在の設定情報を確認するには、*show terminal* コマンドを使用します。

```
netwiser> show terminal
Max History-Size: 500
Auto Logout Time: 30m
```

2.6.1.3 ページ単位出力

ログインすると、ページ単位表示機能は必ず有効になっています。本機能が有効である場合、*show*コマンドの出力は端末サイズに合わせてページ単位で出力されます。

本機能を無効にするには *no terminal pager* コマンドを実行します。

再び有効にするには *terminal pager* コマンドを実行します。

```
netwiser(config)# no terminal pager
netwiser(config)# terminal pager
```

ただし、本設定はログインセッション毎（ユーザーがログインしてから、ログアウトするまで）に影響を受ける設定であり、ログインの度に初期化（ページ単位表示が有効化）されます。

2.6.2 リモートアクセスフィルターの設定

デフォルト設定では、ssh でのリモートアクセスは許可されていますが、telnet での接続は拒否されます。セキュリティポリシーに応じて、本製品へのリモートアクセスに関するフィルター設定を行います。

任意のネットワークセグメントからのみ、telnet/ ssh/ web でのアクセスを許可する場合、以下のように設定します。

```
netwiser(config)# telnet <ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ>/<ﾏｽｸ長>
netwiser(config)# ssh <ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ>/<ﾏｽｸ長>
netwiser(config)# web-mgmt <ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ>/<ﾏｽｸ長>
```

また、WEB 管理画面への HTTP アクセスを HTTPS にリダイレクトさせることが可能です。HTTPS へのリダイレクト機能を有効にするには以下の設定を行います。

```
netwiser(config)# web-mgmt auto-redirect
```

デフォルト設定では HTTPS にリダイレクトされる設定になっています。

設定を解除するには、*no web-mgmt auto-redirect* コマンドを実施します。

例として、以下のセキュリティポリシーを基に設定例を示します。

■telnetでの接続は192.168.1.110と2001:db8::c0:a8:1:6eからのみ許可する

■sshとHTTPでの接続は192.168.1.0/24と2001:db8::/32のネットワークからのみ許可する

■WEB管理画面へのアクセスに対する自動リダイレクト機能を無効にする

```
netwiser(config)# telnet 192.168.1.110/32
netwiser(config)# telnet 2001:db8::c0:a8:1:6e/128
netwiser(config)# ssh 192.168.1.0/24
netwiser(config)# ssh 2001:db8::/32
netwiser(config)# no ssh 0.0.0.0/0
netwiser(config)# no ssh ::/0
netwiser(config)# web-mgmt 192.168.1.0/24
netwiser(config)# web-mgmt 2001:db8::/32
netwiser(config)# no web-mgmt 0.0.0.0/0
netwiser(config)# no web-mgmt ::/0
netwiser(config)# no web-mgmt auto-redirect
```

ポイント

リモートアクセスフィルターの設定をしても、アクセスリストを使用したフィルタリング設定と相反するルールとなる場合（かつ該当のアクセスリストのフィルタリング設定が有効である場合）、アクセスリストのフィルタリングルールが優先されます。

show access-list mgmtコマンドで、リモートアクセスフィルターの統計情報を参照できます。詳しくは**「SX-3990_3950_3945_3940_3920 コマンドリファレンス」**（別紙）を参照してください。

2.6.3 日時の設定

現在の日時を参照する場合は *show date* コマンドを使用します。

変更する場合は date *[[[[[cc]yy]mm]dd]HH]MM[.ss]*([年]月日時分[.秒])と入力してください。

```
netwiser(config)# show date
Fri Oct  1 10:44:07 JST 2014
netwiser(config)# date 201409151520.30
Wed Sep 15 15:20:30 JST 2014
```

2.6.4 サーバーの名前付け

IP アドレスに名前付けすることで、以降の入力を簡略化することが可能です。

名前付けを行うと、設定ファイルにもその文字列で表示されます。

```
  ① 名前付けする
netwiser(config)# name real4_1 192.168.1.100
netwiser(config)# name real6_1 2001:db8::c0:a8:1:64
  ② 名前を使用する
netwiser(config)# real real4_1.80.tcp
netwiser(config)# real real6_1.80.tcp
```

ポイント

機器 IP アドレスやゲートウェイ登録などのように、ネットワークアドレスやサブネットマスク、IPv6 プレフィクスを指定するコマンドでは、名前を使用した設定ができません。それらのコマンドはアドレス形式で入力してください。

2.6.5 DNS の設定

SSL アクセラレーション機能をお使いの際、クライアント証明書の失効リストを取得するため、取得先サーバーの URL を入力を必要とする場合があります。この際に、本製品が FQDN を使用してサーバーへアクセスするためには、DNS サーバーの IP アドレスを本製品に設定する必要があります。
（失効リストの取得を行わない場合、DNS の設定は不要です）
DNS サーバーの設定を行うには *dns* コマンドを実行し、プライマリーDNS サーバー、セカンダリーDNS サーバーを登録します。

```
netwiser(config)# dns primary <IP ｱﾄﾞﾚｽ>
netwiser(config)# dns secondary <IP ｱﾄﾞﾚｽ>
```

設定を削除するには以下のコマンドを使用します。

```
netwiser(config)# no dns primary <IP ｱﾄﾞﾚｽ>
netwiser(config)# no dns secondary <IP ｱﾄﾞﾚｽ>
```

ポイント

セカンダリーDNS サーバーの設定は必須ではありませんが、プライマリーDNS サーバーの設定がなく、セカンダリーDNS サーバーのみが設定されている状態では動作しません。

2.6.6 NTP サーバーの設定

NTP サーバーの IP アドレスを設定します。

```
netwiser(config)# ntp <IP ｱﾄﾞﾚｽ>
```

設定を削除するには以下のコマンドを使用します。

```
netwiser(config)# no ntp <IP ｱﾄﾞﾚｽ>
```

本製品は、デフォルト設定では自身が NTP サーバーとしても動作しています。ただし、*restrict* オプションを有効にすると、設定した NTP サーバー以外との時刻情報の交換を行いません。*restrict* オプションは、本製品を NTP サーバーとして利用しない場合において、NTP のセキュリティを確保するために有効です。

```
netwiser(config)# ntp restrict
```

2.6.7 ホスト名の設定

本製品のホスト名はデフォルトで"netwiser"が設定されています。

変更する場合は *hostname* コマンドを使用します。

```
netwiser(config)#  hostname LB-Master
LB-Master(config)#
```

2.6.8 LAN ポートの速度固定設定

SX-3950,SX-3945,SX-3940,SX-3920 の場合、LAN ポートのリンク速度はデフォルトでオートネゴシエーションに設定されています。速度を固定する場合はイーサネット設定モードで変更してください。

(SX-3990 では、LAN ポートの速度固定設定は動作しません)

```
netwiser(config-if)# speed {10half | 10full | 100half | 100full | 1000full | auto}
```

以下の例では、ポート 1,2 に対して、リンク速度 100full 設定を設定します。

```
netwiser(config)# interface ethernet 1,2
netwiser(config-if)# speed 100full
```

ポイント

speed auto/1000full 設定時には auto MDI/MDI-X で動作しますが、それ以外の設定時は MDI-X で動作します。この場合、他のスイッチと接続する際はクロスケーブルで接続してください。

SX-3950 のポート 11 および 12 の回線速度はオートネゴシエーションに設定されており変更できません。

2.6.9 SYSLOG の設定

リモートの syslog サーバーに常時メッセージを送信するには *logging host* コマンドを使用します。

```
netwiser(config)# logging host <IP ｱﾄﾞﾚｽ>
```

syslog サーバーに送信されるメッセージのファシリティーはデフォルトで LOCAL4 (20)、下限レベルはデフォルトで notice(5)です。変更するには *logging output* コマンドを使用します。

```
netwiser(config)# logging output <ﾌｧｼﾘﾃｨｰ,ﾚﾍﾞﾙ>
```

ファシリティー、ログレベルを表す数値の対応を以下に明記します。

ファシリティー		レベル	
LOCAL0	16	emerg	0
LOCAL1	17	alert	1
LOCAL2	18	crit	2
LOCAL3	19	err	3
LOCAL4	20	warn	4
LOCAL5	21	notice	5
LOCAL6	22	info	6
LOCAL7	23	debug	7

syslog サーバー設定とは別に、syslog メッセージをメールで配信することも可能です。この場合、以下のコマンドを使用してメールサーバーの IP アドレス、送信元メールアドレス、宛先メールアドレスの設定を行います。

```
netwiser(config)# logging mail-host <ﾒｰﾙｻｰﾊﾞｰ IP ｱﾄﾞﾚｽ> <ﾚﾍﾞﾙ>
netwiser(config)# logging from <送信元ﾒｰﾙｱﾄﾞﾚｽ>
netwiser(config)# logging to <宛先ﾒｰﾙｱﾄﾞﾚｽ>
netwiser(config)# logging reply-to <返信先ﾒｰﾙｱﾄﾞﾚｽ> (ｵﾌﾟｼｮﾝ)
```

logging mail-host コマンドでメールサーバーIP アドレスに加え、メール配信の対象となるメッセージの下限レベルを指定します。この値は *logging output* の下限レベルと異なっていても構いません。

本製品にはメール受信の機能はありませんので、送信元メールアドレスには netwiser@sx3950 のような架空のアドレスを設定してください。

メールを返信する必要がある場合は *logging reply-to* コマンドで実在するメールアドレスを設定してください。

syslog サーバーと宛先メールアドレスは複数設定することが可能です。その他の項目は 1 件のみ設定します。

2.6.10 SNMP の設定

SNMP トラップの送信先ホストを設定します。

```
netwiser(config)# snmp host <IP ｱﾄﾞﾚｽ>
```

SNMP のシステム情報を設定します

```
netwiser(config)# snmp community "<文字列>"
netwiser(config)# snmp contact "<文字列>"
netwiser(config)# snmp location "<文字列>"
```

プライベート MIB の定義ファイルを取り出すには *export mib* コマンドを使用します。詳細は「5.3.2.5MIB 定義ファイルのエクスポート」を参照してください。

ポイント

コマンドプロンプトを起動し
> tftp -i <本製品の IP ｱﾄﾞﾚｽ> get mib.zip
を実行してください。
" Transfer is completed."と出力されたら、転送が成功です。

ファイルの取り出しには zmodem を使用することも可能です。

```
netwiser(config)# export mib zmodem
Ready to ZMODEM send 'mib.zip'.
**B00000000000000l time to cancel: rz
Transfer is completed.
netwiser(config)#
```

また、syslog に任意の文字列が出力された際に SNMP トラップを送信することが可能です。設定を行うには、*snmp trap trigger* コマンドを実行します。
once オプションを指定すると、当該コマンドが実行された後、任意の文字列が最初に検出された際にのみ、SNMP トラップを送信します。

```
netwiser(config)# snmp trap trigger "<任意の文字列>" [once]
```

SNMPv1 トラップ発行時のエージェントアドレスの設定を行うには、*snmp trap agent-address vlan* コマンドを実行します。指定した VLAN に設定されている IPv4 管理アドレスがエージェントアドレスとして使用されます。
snmp trap agent-address vlan の設定がない場合は SNMPv1 トラップの agent-addr に 0.0.0.0 が設定されます。

```
netwiser(config)# snmp trap agent-address vlan <VLAN ID>
```

ポイント

- 作成されていない VLAN を指定することはできません。
- IPv4 管理 IP アドレスの設定がない VLAN を指定することはできません。
- *snmp trap agent-address vlan* 設定後、該当 VLAN の IPv4 管理 IP アドレスを変更した場合、SNMPv1 トラップ発行時のエージェントアドレスも自動的に変更されます。

また、lacp 論理チャネルなど、リンク状態の変化に伴い状態の収束に一定の時間が生じるポートからトラップが送信される可能性がある場合、リンクアップまたはリンクダウンのトラップ送信が失敗する場合があります。
snmp trap link-updown-delay コマンドを実行する事で、リンクアップまたはリンクダウントラップの送信を、指定した秒数だけ遅らせることが可能です。
これにより該当トラップの送信失敗を防ぎます。

```
netwiser(config)# snmp trap link-updown-delay <time-expression>
```

no を指定することで、デフォルトの状態（遅延なし）に設定できます。

```
netwiser(config)# no snmp trap link-updown-delay
```

2.7 VLAN の設定

2.7.1 ポート VLAN の設定

全てのイーサネットポートはデフォルトで VLAN 1 に割り当てられています。

変更するにはイーサネット設定モードで *vlan* コマンドを実行します。

```
netwiser(config-if)# vlan <VLAN ID>
```

以下の例では、ポート1～4 を VLAN 2 に割り当てます。

```
netwiser(config)# interface ethernet 1-4
netwiser(config-if)# vlan 2
```

2.7.2 プライベート VLAN の設定

プライベート VLAN を有効にするには *protected* コマンドを使用します。

プライベート VLAN に設定することで同一 VLAN に属する全てのポート間の通信を禁止します。1 つの VLAN 内でブロードキャストドメインを分割できるので、同一サブネット上でのセキュリティが確保されます。

プライベート VLAN はデフォルトで無効になっています。

以下は、イーサネット設定モードで実施してください。

```
netwiser(config-if)# protected
```

2.7.3 タグ VLAN の設定

任意のポートをトランクポートに設定します。
デフォルトでは送受信パケットに 802.1q タグを付けません(アクセスポート)。
802.1q タグを有効(トランクポート)にするには *tagged* コマンドを使用します。
以下は、イーサネット設定モードで実施してください。

```
netwiser(config)# interface ethernet 1
netwiser(config-if)# tagged
```

タグ付パケットは、タグ内の VLAN ID を使用し、タグなしパケットは、ネイティブ VLAN に設定された VLAN ID を使用します。
ネイティブ VLAN はデフォルトで 1 ですが、変更することもできます。
ネイティブ VLAN を変更するには *native-vlan* コマンドを使用します。

```
netwiser(config-if)# native-vlan 2
```

また、特定の VLAN ID のパケットのみ通過させる場合は、*allowed-vlan* で指定する必要があります。

```
netwiser(config-if)# allowed-vlan 4000,4010-4020
```

指定のない場合は、全てのパケットが通過します。
トランクポートをプライベート VLAN に設定することはできません。

トランクポートから *no tagged* コマンドでアクセスポートに設定変更すると、ポートは VLAN1 に割り当てられます。

ポイント

イーサネットポートまたは論理チャネルにタグ VLAN の設定がされている場合（SX-3990 ではイーサネットポートにタグ VLAN の設定がされている場合）、MTU サイズは全ての VLAN で統一されている必要があります。
本製品では、タグ VLAN を設定した際、設定されている MTU サイズの中で最小の値が全 VLAN に対して自動で設定されます。
ただし、VLAN に IPv6 アドレスが設定されている場合、該当の VLAN に設定可能な MTU 値の範囲を下回って設定されることがあります。手動で適切な値に変更してください。
MTU 設定の詳細は「2.10MTU 値の変更」を参照してください。

2.7.4 VLAN MAC アドレスの設定（SX-3990 のみ）

すべての VLAN インターフェースはデフォルトでポート1の MAC アドレスが割り振られます。そのため、VLAN に割り当てた IP アドレスあるいは仮想 IP アドレスが使用する MAC アドレスは、ポート1の MAC アドレスに設定されます。仮想 NIC のプロミスキャスモード(promiscuous mode）を無効にしたとき、仮想 NIC はその NIC 向けのフレームのみを受信するため、バランシング動作可能な構成は One-Arm 構成のみとなります。複数のポートを使用した構成の場合は、仮想 IP アドレスの MAC アドレスと仮想 NIC の MAC アドレスとが異なるため、仮想 IP 向けのフレームを受信できません。このとき、仮想 NIC をプロミスキャスモードで動作させる必要があります。

1つの VLAN に1つのポートを割り当てたルーター構成の場合は、プロミスキャスモードを無効にしたまま、*vlan-mac* コマンドで MAC アドレスを変更することでバランシング動作が可能になります。

以下は、VLAN 設定モードで実施してください。

```
netwiser(config-vlan)# vlan-mac <PORT NUM>
```

以下の例では、VLAN 2 が使用する MAC アドレスにポート 2 の MAC アドレスを割り当てます。

```
netwiser(config)# interface vlan 2
netwiser(config-vlan)# vlan-mac 2
```

ポイント

以下の場合は、仮想 NIC のプロミスキャスモードを有効化してください。

- 1 つの VLAN に複数のポートを割り当てる
- 冗長構成

2.8 リンク集約

本章では、SX-3950,SX-3945,SX-3940,SX-3920 のリンク集約機能の設定方法を例とともに記します（SX-3990 ではリンク集約機能は動作しません）。

リンク集約設定を行うと、複数のイーサネットポートを集約し 1 つの論理チャネルとして扱うことが可能になり、帯域幅が増幅します。
論理チャネルの設定を行うには、*interface channel* コマンドで論理チャネル設定モードに遷移します。ただし、事前にイーサネット設定モードで論理チャネルの生成を行う必要があります。

論理チャネル設定モードで使用可能なコマンドは、*mode* コマンドを除き、全てがイーサネット設定モードでも使用できるコマンドです。各コマンドのデフォルト値や使用方法も同じです。

以下に、論理チャネル設定モードで使用可能なコマンドについて記載します。

WEB 管理画面上の表記	CLI コマンド
VLAN ID	vlan
タグ VLAN	tagged
ネイティブ VLAN	native-vlan
VLAN フィルター	allowed-vlan
プライベート VLAN	protected
スパニングツリー	spanning-tree
動作モード	mode
バランシングポート定義	slb

2.8.1 論理チャネルの生成

リンク集約を設定するには、事前に *channel* コマンドで新規に論理チャネルを生成するか、または既存のチャネルにポートを割り当てます。

```
netwiser(config-if)# channel <論理チャネル番号>
```

以下では、ポート1～3 を集約し、論理チャネル 1 を生成します。

```
netwiser(config)# interface ethernet 1-3
netwiser(config-if)# channel 1
channel 1 created
```

設定可能なチャネル数は SX-3950/3945 が最大4（チャネル番号 1-4）、SX-3940 が最大2（チャネル番号 1-2）、SX-3920 が1（チャネル番号 1）となります。
※1G I/F と 10G I/F でリンク集約の設定をすることはできません。

以下に挙げる設定をチャネルモードで設定変更した場合、所属する全てのイーサネットポートに設定変更が反映されます。

VLAN ID	(vlan)
タグ VLAN	(tagged)
ネイティブ VLAN	(native-vlan)
VLAN フィルター	(allowed-vlan)
プライベート VLAN	(protected)
スパニングツリー	(spanning-tree)
バランシングポート定義	(slb)

これらの設定、またはリンク速度が異なるポート同士で論理チャネルを形成しないでください。また、ミラーポートを論理チャネルに含めることはできません。

ポイント

論理チャネル生成前にイーサネット設定モードでこれらの設定を実施した場合、論理チャネル生成時に、論理チャネルの設定内容にこれらの設定が反映されます。ただし、論理チャネル生成後、イーサネット設定モードでこれらのコマンドを実行することはできませんので注意してください。

該当の設定を変更するには、論理チャネル設定モードで行います。

```
  ① イーサネット 1～3 の設定を行う
netwiser(config)# interface ethernet 1-3
netwiser(config-if)# tagged
netwiser(config-if)# allowed-vlan 4000
  ② イーサネット 1～3 をリンク集約する
netwiser(config-if)# channel 1
channel 1 created
  ③ 生成した論理チャネルの設定を確認する(イーサネットポートの設定
     が反映されている)
netwiser(config-if)# show running-config interface channel 1
!
interface channel 1
 slb both
 tagged
 allowed-vlan 4000
 mode lacp
!
  ④ 論理チャネル設定モードで変更する
netwiser(config-if)# exit
netwiser(config)# interface channel 1
netwiser(config-channel)# no tagged
```

ポイント

リンク集約で使用するポートを速度固定で使用する場合、100MbpsFulll、または 1GbpsFull で使用してください。
half 設定では動作しません。

⚠ 注意

リンク集約設定からリンク集約をしない設定にする際、ネットワークがループします。
ケーブルを外してから設定を変更してください。

2.8.2 リンク集約モード

デフォルト設定で、論理チャネルは、IEEE802.3ad 準拠の Link Aggregation Control Protocol（LACP）で動作します。

動作モードを変更するには *mode* コマンドを使用します。

```
netwiser(config-if)# mode {lacp | static}
```

■ *lacp*

論理チャネルの動作モードを LACP(IEEE802.3ad 準拠)モードに変更します。LACP では、本装置と論理チャネルを形成するスイッチとネゴシエーションを取ることでダイナミックに動作します。

ポイント

本装置と論理チャネルを形成するスイッチ側の設定を active モード（LACP ネゴシエーション要求を自ら送るモード）に設定してください。

■ *static*

論理チャネルの動作モードをスタティックモードに変更します。スタティックモードではリンク集約動作を手動で切り替えます。

2.9 スパニングツリーの設定

デフォルトで Spanning-Tree Protocol （STP）は停止状態になっています。
STP を開始するには *spanning-tree* コマンドを使用します。
以下は、イーサネット設定モード、またはチャネル設定モードで実施してください。

```
netwiser(config-if)# spanning-tree
```

STP を有効にすると、STP オプション設定が実施できるようになります。

```
netwiser(config-if)# spanning-tree [edge | priority <ﾎﾟｰﾄﾌﾟﾗｲｵﾘﾃｨｰ> | cost <ﾎﾟｰﾄｺｽﾄ> | restart]
```

■*edge*

Rapid Spanning-Tree Protocol（RSTP）はスイッチ以外の装置が接続されたエッジポートを自動的に検出し 3 秒後に forwarding(転送)状態へ移行します。3 秒の遅延なく直ちに forwarding 状態に移行させるには *spanning-tree edge* コマンドを使用します。

```
netwiser(config-if)# spanning-tree edge
```

⚠ 注意 リンク集約ポート(channel)でも STP を有効にすることができます。ただし、集約されたポートがすべて半二重状態になってしまった場合、正しくスパニングツリーを形成できませんので注意してください。

■*priority*

ポートプライオリティーを設定します。範囲は 0 から 240 で、16 の倍数で登録する必要があります。

```
netwiser(config-if)# spanning-tree priority <ﾌﾟﾗｲｵﾘﾃｨｰ値>
```

no を指定するとデフォルト値（128）にセットします。

```
netwiser(config-if)# no spanning-tree priority
```

■*cost*

ポートコストを設定します。範囲は 1 から 200000000 です。

```
netwiser(config-if)# spanning-tree cost <ｺｽﾄ値>
```

no を指定するとデフォルト値（auto）にセットします。

```
netwiser(config-if)# no spanning-tree cost
```

■*restart*

リンク集約設定時のデフォルトの動作モードは RSTP であり変更できません。
しかし、以下の場合は 802.1D 互換モードで動作します。

・ RSTP 未対応のスイッチを検出
・ バス接続されている(半二重リンク)

802.1D 互換モードで動作中のポートを強制的に RSTP に戻すにはイーサネット設定モード、またはチャネル設定モードで *spanning-tree restart* コマンドを使用します。

```
netwiser(config-if)# spanning-tree restart
```

2.10 MTU 値の変更

本製品の MTU サイズのデフォルトは 1500 です。MTU サイズを変更するには VLAN 設定モードで *mtu* コマンドを実行します。

```
netwiser(config-vlan)# mtu <MTU ｻｲｽﾞ>
```

設定できるMTUサイズの範囲は576から1500ですが、該当のVLANにIPv6アドレスが設定されている場合、1280 が最小になります。

ポイント

イーサネットポート、または論理チャネルにタグ VLAN の設定がされている場合、MTU サイズは全ての VLAN で統一されている必要があります。
タグVLANの設定がある状態でMTUサイズの変更を行うと、全VLANのMTUサイズが、*mtu*コマンドで指定した値に変更されます。ただし、タグVLAN設定がされていても、新規にVLANを作成した場合、MTUサイズはデフォルトの1500に設定されます。手動で他の VLAN の MTU サイズに合わせてください。

⚠ 注意

MTU を小さい値から大きい値に変更する場合、再起動する必要があります。

2.11 VLAN へのルーティングテーブルの設定

VLANで使用するルーティングテーブルのルートIDを設定することができます。

VLANで使用するルートIDを設定するにはVLAN設定モードで *route-id*コマンドを実行します。ルート ID が設定されている場合は、VLAN で受信したパケットは VLAN に設定されたルート ID と同一の ID を持つルーティングテーブルに従います。

ルート ID を設定しない場合はルート ID 0 が使用されます。
削除するには *no* を使用するか、ルート ID 0 を指定します。

```
netwiser(config-vlan)# route-id <ﾙｰﾄ ID>
netwiser(config-vlan)# no route-id
```

設定できるルート ID の範囲は 0 から 15 です。

ポイント

1. パケットを受信したポートがトランクポートの場合は、タグ情報の VLAN ID を読み取り、該当する VLAN に設定されているルート ID のルーティングテーブルに従います。
2. タグ情報の VLAN ID が本製品に設定されていない VLAN ID の場合は、ルート ID 0 が使用されます。
3. パケットにタグ情報がない場合はネイティブ VLAN に設定されている VLAN のルート ID が使用されます。

ポイント

負荷分散対象、またはリバース NAT の対象となるパケットは各設定モードに設定されているルート ID に従います。

⚠ 注意

本製品の管理 IP アドレスへの接続は VLAN に設定されているルート ID が使用されません。ルート ID 0 が使用されます。
PING への応答は VLAN に設定されているルート ID が使用されます。

2.12 ルーター広告の設定

Router Advertisement（RA）機能を有効にするには、*rtadv* コマンドを実行します。

```
netwiser(config-vlan)# rtadv [flag {managed | other | both}] [dns primary <IPv6 ｱﾄﾞﾚｽ> [secondary <IPv6 ｱﾄﾞﾚｽ>]]
```

■*flag {managed | other | both}*

RA パケット中の M フラグ(*managed*)、O フラグ(*other*)、またはその両方(*both*)をセットします。

managed が指定されている場合、DHCPv6 サーバーから IPv6 アドレスを取得します。また、*other* が指定されている場合、アドレス以外の情報も DHCP サーバーから取得します。

flag パラメーターが省略された場合、そのどちらもセットされません。

■*dns primary <ipv6-addr> [secondary <ipv6-addr>]*

RA の DNS オプションを有効にし、プライマリーDNS サーバーとセカンダリーDNS サーバーを設定します。

セカンダリーDNS サーバーの設定は省略可能です。また、*dns* パラメーター自体を省略した場合、RA の DNS オプションは無効になります。

2.13 フィルタリングの設定

本章では、本製品のフィルタリングに関する設定を例とともに説明します。

2.13.1 リモートアクセスフィルタリング

telnet、ssh を使用したアクセスや、WEB 管理画面へのアクセスといった、本製品へのリモートアクセスに関して、アクセスフィルターを設定することが可能です。

詳細は「2.6.2リモートアクセスフィルターの設定」を参照してください。

2.13.2 VLAN ID フィルタリング

トランクポートはデフォルトで全 VLAN のパケットを通過させます。特定の VLAN ID のみ許可するには ***allowed-vlan*** コマンドを使用します。

VLAN ID はカンマで区切るか、ハイフンによる範囲指定が可能です。以下は、イーサネット設定モード、またはチャネル設定モードで実施してください。

```
netwiser(config-if)# allowed-vlan <VLAN ID>
```

以下の例では、VLAN 10、VLAN 20、VLAN 30～40 のパケットを通過させ、その他の VLAN ID は拒否します。

```
netwiser(config-if)# allowed-vlan 10,20,30-40
```

全ての VLAN のパケットを通過させる設定に戻すには no を指定します。

```
netwiser(config-if)# no allowed-vlan
```

2.13.3 L2 パケットフィルタリング

L2 パケットに対するアクセス制御リスト(Access Control List、以下 ACL)を作成するには、*access-list mac* コマンドを使用します。

```
netwiser(config)# access-list mac <ACL 名>
netwiser(config-mac-acl)#
```

MAC アクセスリスト設定モードで、*deny* または *permit* コマンドを使用してフィルタリングルールを定義します。
デフォルトルールとして行番号 65535 に全ての受信拒否(*line 65535 deny any any*)が設定されています。

```
netwiser(config-mac-acl)# [line <行番号>] permit <送信元> <宛先> [type <ﾌﾟﾛﾄｺﾙ>]
netwiser(config-mac-acl)# [line <行番号>] deny <送信元> <宛先> [type <ﾌﾟﾛﾄｺﾙ>] [log]
```

■*<行番号>*

ACL 内の位置を指定する。指定可能な行番号の範囲は 1-65534 で、省略した場合は最後のルールに 10 を加えた番号が割り当てられます。

■*<送信元>, <宛先>*

登録するルールの送信元 MAC アドレスと、宛先 MAC アドレスを入力します。
MAC アドレスに *any* を入力すると、全ての MAC アドレスをフィルタリングの対象とします。

■*<ﾌﾟﾛﾄｺﾙ>*

プロトコル文字列またはプロトコル番号を入力し、ルールにマッチさせるプロトコルを指定します。省略した場合、全てのプロトコルが対象となります。
使用できるプロトコル文字列を以下に示します。

プロトコル文字列	プロトコル番号
ip	0x800
arp	0x806
bpdu	0x4242
rarp	0x8035
appletalk	0x809b
ibmsna	0x80d5

aarp	0x80f3
ipv6	0x86dd
ipx	0xe0e0
netbios	0xf0f0

その他のプロトコルを指定する場合、プロトコル番号を入力します。
プロトコル番号は 5dd から ffff までの 16 進数で入力してください。

■ *log*

*log*オプションを指定すると、ルールに一致した場合に syslog メッセージを生成します。

フィルタリングを開始する場合は、イーサネット設定モードで *filter* コマンドを使用します。受信パケットに対して適用するには *in*、送信パケットに対して適用するには *out*、送受信ともに適用するにはその両方を指定します。
送信フィルターと受信フィルターに、異なるフィルタリングルールを設定することも可能です。

```
netwiser(config-if)# filter mac-acl-01 in
netwiser(config-if)# filter mac-acl-02 out
```

フィルタリングを停止させるには *no* を指定します。

```
netwiser(config-if)# no filter mac-acl-01 in
netwiser(config-if)# no filter mac-acl-02 out
```

たとえば、ポート1, 2に対しての ARP リクエストに応答しない設定にするには、以下のようにします。

```
  ① ARP リクエストの拒否と、その他のパケットの許可
netwiser(config)# access-list mac mac-acl-1_2
netwiser(config-mac-acl)# deny any any type arp
netwiser(config-mac-acl)# permit any any
netwiser(config-mac-acl)# exit
  ② ポート 1,2 への適用
netwiser(config)# interface ethernet 1,2
netwiser(config-if)# filter mac-acl-1_2 in
```

ポイント

イーサネット設定モードで *filter* コマンドを使用した後、*access-list mac* を変更しても設定は反映されません。
access-list mac 変更後は再度 *filter* コマンドを実施してください。

2.13.4 L3/L4 パケットフィルタリング

L3/L4 パケットに対するアクセス制御リスト(Access Control List、以下 ACL)を作成するには、*access-list* コマンドを使用します。
IPv4 のアクセスリストを設定したい場合は *ipv4*、IPv6 のアクセスリストを設定したい場合は *ipv6* を指定してください。

```
netwiser(config)# access-list ipv4 <ACL 名>
netwiser(config-acl)#
```

IP アクセスリスト設定モードで、*deny* または *permit* コマンドを使用してフィルタリングルールを定義します。
デフォルトルールとして行番号 65535 に全ての受信拒否(*line 65535 deny ip any any*)が設定されています。

基本的な文法は以下です。

```
netwiser(config-acl)# [line <行番号>] permit <ﾌﾟﾛﾄｺﾙ> <送信元> <宛先>
netwiser(config-acl)# [line <行番号>] deny <ﾌﾟﾛﾄｺﾙ> <送信元> <宛先> [log]
```

■*<行番号>*

ACL 内の位置を指定する。指定可能な行番号の範囲は 1-65534 で、省略した場合は最後のルールに 10 を加えた番号が割り当てられます。

■*<送信元>, <宛先>*

登録するルールの送信元 IP アドレスと、宛先 IP アドレスを入力します。
IP アドレスに *any* を入力すると、全ての IP アドレスをフィルタリングの対象とします。

■*<ﾌﾟﾛﾄｺﾙ>*

プロトコル文字列またはプロトコル番号を入力し、ルールにマッチさせるプロトコルを指定します。省略した場合、全てのプロトコルが対象となります。
使用できるプロトコル文字列を以下に示します。

プロトコル文字列	プロトコル番号
ip	0
icmp	1

igmp	2
ipip	4
tcp	6
udp	17
gre	47
esp	50
ospf	89
pim	103

その他のプロトコルを指定する場合、プロトコル番号を入力します。
プロトコル番号は 0 から 255 までの 10 進数を入力します。
0 または文字列"ip"は全ての IP パケットを表します。

プロトコル名に"tcp"または"udp"を指定する場合は、「2.13.4.1TCP/UDP パケットのフィルタリング」を参照してください。
"icmp"または"icmpv6"を指定する場合は、「2.13.4.2ICMP パケットのフィルタリング」を参照してください。

■ *log*

*log*オプションを指定すると、ルールに一致した場合に syslog メッセージを生成する。

フィルタリングを開始する場合は、VLAN 設定モードで *filter* コマンドを使用します。IPv4 のアクセスリストを適用したい場合は *ipv4*、IPv6 のアクセスリストを適用したい場合は *ipv6* を指定してください。

```
netwiser(config-vlan)# filter {ipv4 | ipv6} <ACL 名>
```

フィルタリングを停止する場合は *no* を指定してください。

```
netwiser(config-vlan)# no filter {ipv4 | ipv6}
```

ポイント

VLAN 設定モードの *filter* コマンドでフィルタリングを開始した後、アクセスリスト設定モードで、フィルタリングルールを変更しても、起動中のフィルタリング処理には反映されません。
フィルタリングルール変更後は、再度 VLAN 設定モードの *filter* コマンドを実施してください。

ポイント

VLAN 設定モードの *filter* コマンドで設定するフィルタリング設定は、受信パケットにのみ適用されます。送信パケットには適用されません。

2.13.4.1 TCP/UDP パケットのフィルタリング

*〈ﾌﾟﾛﾄｺﾙ〉*に *tcp* または *udp* を指定する場合、演算子とともにポート番号の指定が可能です。

```
netwiser(config-acl)# [line 〈行番号〉] permit { tcp | udp } 〈送信元 IP〉 [ 〈演算子〉 〈送信元ﾎﾟｰﾄ〉 [〈ﾎﾟｰﾄ〉] ]
    〈宛先 IP〉 [ 〈演算子〉 〈宛先ポート〉 [〈ﾎﾟｰﾄ〉] ]
netwiser(config-acl)# [line 〈行番号〉] deny { tcp | udp } 〈送信元 IP〉 [ 〈演算子〉 〈送信元ﾎﾟｰﾄ〉 [〈ﾎﾟｰﾄ〉] ]
    〈宛先 IP〉 [ 〈演算子〉 〈宛先ポート〉 [〈ﾎﾟｰﾄ〉] ] [log]
```

■*〈送信元ﾎﾟｰﾄ〉, 〈宛先ﾎﾟｰﾄ〉*

ポート指定無しの場合は、全てのポート番号が対象になります。

ポートを指定する場合、以下の演算子を使用します。

eq(=), ne(!=), gt(>), lt(<), range

range の場合は 2 個のポート番号を指定します。

例) eq 23 ,　range 8000 9000 ,　etc…

たとえば、VLAN 10 に設定されている仮想サーバーIP アドレス 192.168.1.100 に対する、192.168.0.0/16 からの HTTP リクエストの拒否を設定にするには、以下のようにします。

```
  ① HTTP リクエストの拒否と、その他のパケットの許可
netwiser(config)# access-list ipv4 acl-vl-10
netwiser(config-acl)# deny tcp 192.168.0.0/16 192.168.1.100 eq 80
netwiser(config-acl)# permit ip any any
netwiser(config-mac-acl)# exit
  ② VLAN 10 への適用
netwiser(config)# interface vlan 10
netwiser(config-vlan)# filter ipv4 acl-vl-10
```

2.13.4.2 ICMP パケットのフィルタリング

*<プロトコル>*に *icmp* または *icmpv6* を指定する場合、icmp タイプの指定が可能です。

```
netwiser(config-acl)# [line <行番号>] permit {icmp | icmpv6} <送信元 IP> <宛先 IP> [ type <ICMP ﾀｲﾌﾟ>]
netwiser(config-acl)# [line <行番号>] deny {icmp | icmpv6} <送信元 IP> <宛先 IP> [ type <ICMP ﾀｲﾌﾟ>] [log]
```

■*<ICMP ﾀｲﾌﾟ>*

icmp タイプ文字列または icmp タイプ番号を入力し、ルールにマッチさせる icmp タイプを指定します。省略した場合、全ての icmp タイプが対象となります。

*<プロトコル>*に *icmp* が指定された際に使用できる icmp タイプ文字列を以下に示します。

icmp タイプ文字列	タイプ番号
echo-reply	0
unreachable	3
source-quench	4
redirect	5
echo	8
router-advertisement	9
router-solicitation	10
time-exceeded	11
parameter-problem	12
timestamp-request	13
timestamp-reply	14
information-request	15
information-reply	16
mask-request	17
mask-reply	18
traceroute	30
conversion-error	31
mobile-redirect	32

*<プロトコル>*に *icmpv6*が指定された際に使用できる icmp タイプ文字列を以下に示します。

icmpv6 タイプ文字列	タイプ番号
unreachable	1
too-big	2
time-exceeded	3
parameter-problem	4
echo-request	128
echo-reply	129
router-solicitation	133
router-advertisement	134
neighbor-solicitation	135
neighbor-advertisment	136
redirect	137

その他の icmp/icmpv6 タイプを指定する場合、タイプ番号を入力します。
タイプ番号は 0 から 255 までの 10 進数を入力します。

たとえば、VLAN 10 に設定されている機器 IP アドレス 192.168.1.10 に対する、icmp リクエストの拒否を設定にするには、以下のようにします。

```
  ① ICMP リクエストの拒否と、その他のパケットの許可
netwiser(config)# access-list ipv4 icmp_fil
netwiser(config-acl)# deny icmp any 192.168.1.10 type echo
netwiser(config-acl)# permit ip any any
netwiser(config-acl)# exit
  ② VLAN 10 への適用
netwiser(config)# interface vlan 10
netwiser(config-vlan)# filter ipv4 icmp_fil
```

2.14 ファイアウォールの設定

本章では、本製品のファイアウォール機能に関する設定を例とともに説明します。

2.14.1 ファイアウォール機能

ファイアウォール機能を使用すると、本製品を流れる着信トラフィックと発信トラフィックをフィルタリングできます。

ファイアウォール機能は、1 つ以上の「ルール」のセットを使用して、ネットワークパケットを送受信するときにネットワークパケットを検査し、トラフィックの通過を許可またはブロックします。

ファイアウォール機能のルールは、プロトコルタイプ、送信元または宛先のホストアドレス、送信元または宛先のポートなど、パケットの 1 つ以上の特性を検査できます。

2.14.2 ファイアウォールルール設定モード

ファイアウォールルール制御リストを作成するには、*ipfw-list*コマンドを使用します。

```
netwiser(config)# ipfw-list ethport <list-name>
netwiser(config-eth-ipfw)#
  または
netwiser(config)# ipfw-list vlan <list-name>
netwiser(config-vlan-ipfw)#
```

イーサネットポート、または論理チャネルにファイアウォールルールを設定したい場合は *ethport*（イーサネットポート ipfw 設定モード）、特定の vlan にファイアウォールルールを設定したい場合は *vlan*（VLAN ipfw 設定モード）を指定してください。

list-name にはリスト名を指定します。リスト名が存在しない場合、新規のルールリストが生成されます。

リスト名は、1 から 64 文字まで文字列を付けることができます。半角英数、ハイフン(-)、アンダーバー(_)、シャープ(#)、スラッシュ(/)、コマーシャルアット(@)が使用可能です。先頭文字に数字、記号を使用することはできません。

ルールリストの最大設定数は 128 件、各リストのルール最大設定数は 127 件です。

2.14.3 ファイアウォールルール定義

ファイアウォールルールリスト設定モードで、*deny*または *permit* コマンドを使用してファイアウォールルールを定義します。
デフォルトルールとして行番号 65535 に全ての受信許可(*line 65535 permit in ip any any*)が設定されています。

ファイアウォールルールを作成する場合、キーワードは次の順序で記述する必要があります。一部のキーワードは必須ですが、他のキーワードはオプションです。

基本的な構文は以下です。

```
netwiser(config-eth-ipfw)# [line <行番号>] permit <方向> <ﾌﾟﾛﾄｺﾙ> <送信元> <宛先>  {[setup] [keep-state] | [established]}
netwiser(config-eth-ipfw)# [line <行番号>] deny <方向> <ﾌﾟﾛﾄｺﾙ> <送信元> <宛先> [log]
```

ICMP/ICMPv6 の構文は以下です。

```
netwiser(config-eth-ipfw)# [line <行番号>] permit <方向> <ﾌﾟﾛﾄｺﾙ> <送信元> <宛先> [type <icmp-type>] [keep-state]
netwiser(config-eth-ipfw)# [line <line-num>] deny <方向> <ﾌﾟﾛﾄｺﾙ> <送信元> <宛先> [type <icmp-type>] [log]
```

ルールを削除するには以下のように先頭に *no* を付けて*<行番号>*を指定します。

```
netwiser(config-eth-ipfw)# no line <行番号>
```

■*<行番号>*

行番号は1から65534まで使用することが出来ます。この番号は、ルール処理の順序を示すために使用されます。省略した場合、10 番おきに番号が割り当てられます。同じファイアウォールルール制御リスト内では同じ番号を付けることは出来ません。

■*permit*, *deny*

ルールは次のいずれかのアクションに関連付けることができます。指定されたアクションは、パケットがルールに一致したときに実行されます。

アクション	実行処理
permit	ルールに一致するパケットを許可
deny	ルールに一致するパケットをサイレントに破棄

■*〈方向〉*

トラフィックは、着信または発信方向で一致させることができます。

方向	内容	適用可能設定モード
in	着信パケットに対してルールを適用	vlan ipfw 設定モード イーサネットポート ipfw 設定モード
out	発信パケットに対してルールを適用	vlan ipfw 設定モード

■*〈ﾌﾟﾛﾄｺﾙ〉*

対象となるプロトコル名を指定します。

プロトコル名	対象となるトラフィック
ip	IPv4 トラフィック
ip6	IPv6 トラフィック
tcp	TCP/IPv4 トラフィック
tcp6	TCP/IPv6 トラフィック
udp	UDP/IPv4 トラフィック
udp6	UDP/IPv6 トラフィック
icmp	ICMP/IPv4 トラフィック
icmp6	ICMP/IPv6 トラフィック

その他のプロトコルを指定する場合、プロトコル番号を入力します。
プロトコル名 *ip* または *ip6* に続いてオプション *proto* を使用して、以下の表にある任意のプロトコル名を指定できます。その他のプロトコルを指定する場合、プロトコル番号を入力します。

プロトコル文字列	プロトコル番号
ip	0
icmp	1
igmp	2
ipip	4
tcp	6
tcp6	6
udp	17
udp6	17
ip6	41
gre	47
esp	50
ah	51
icmp6	58
eigrp	88
ospf	89
pim	103
carp	112

プロトコル番号は 0 から 255 までの 10 進数を入力します。
0 または文字列"ip"は全ての IP パケットを表します。

■*〈送信元〉、〈宛先〉*
送信元および宛先 IP アドレス、ポート番号を指定します。IP アドレスを指定する場合、オプションで 1.2.3.4/25 のように CIDR マスクを続けることができます。キーワード *any* を指定した場合はすべての IP アドレスに一致します。キーワード *me* を指定した場合は自局 IP アドレスに一致します。

ポート番号は、以下の演算子の後ポート番号を使用して指定できます。

演算子	一致する値	例
eq	指定したポート番号	eq 443
ne	指定したポート番号以外	ne 23
range	指定したポート番号範囲内	range 1 1024

ポート番号を省略した場合は、全てのポート番号が対象になります。

■*<icmp-type>*

*<プロトコル>*に *icmp* または *icmp6* を指定する場合、icmp タイプの指定が可能です。

icmp タイプ文字列または icmp タイプ番号を入力し、ルールにマッチさせる icmp タイプを指定します。省略した場合、全ての icmp タイプが対象となります。

*<プロトコル>*に *icmp* が指定された際に使用できる icmp タイプ文字列を以下に示します。

icmp タイプ文字列	タイプ番号
echo-reply	0
unreachable	3
source-quench	4
redirect	5
echo	8
router-advertisement	9
router-solicitation	10
time-exceeded	11
parameter-problem	12
timestamp-request	13
timestamp-reply	14
information-request	15
information-reply	16
mask-request	17
mask-reply	18
traceroute	30
conversion-error	31

mobile-redirect	32

*<プロトコル>*に *icmp6* が指定された際に使用できる icmp タイプ文字列を以下に示します。

icmpv6 タイプ文字列	タイプ番号
unreachable	1
too-big	2
time-exceeded	3
parameter-problem	4
echo-request	128
echo-reply	129
router-solicitation	133
router-advertisement	134
neighbor-solicitation	135
neighbor-advertisment	136
redirect	137

その他の icmp/icmp6 タイプを指定する場合、タイプ番号を入力します。
タイプ番号は 0 から 255 までの 10 進数を入力します。

■*setup*

*<プロトコル>*に *tcp* または *tcp6* が指定されたときコネクション確立要求(SYN=1)の TCP パケットにマッチします。*keep-state* と合わせて指定することでコネクション確立要求に合わせて動的ルールを作成します。

■*keep-state*

アクション *permit* を設定したとき指定可能です。
ルールに一致するとファイアウォールは、一致したルールと同じプロトコルを使用して送信元アドレスと宛先アドレスおよびポート間の双方向トラフィックを一致させる動的ルールを作成します。

■*established*

*<プロトコル>*に *tcp* または *tcp6* が指定されたときパケットがすでに確立されている TCP コネクションの一部であれば(RST または ACK ビットがセットされていれば)マッチします。

■ *log*

アクション ***deny***を設定したとき指定可能です。

ルールに一致した場合に syslog メッセージを生成します。

2.14.4 ファイアウォールルールの適用

2.14.4.1 イーサネットポート ipfw 設定の適用

イーサネットポート ipfw 設定モードで作成したファイアウォールルールリストを適用する場合はイーサネット設定モードで、*firewall*コマンドを使用します。

```
netwiser(config-if)# firewall <list-name>
```

ファイアウォールルールの適用を停止する場合は *no* を指定してください。

```
netwiser(config-if)# no firewall <list-name>
```

ポイント

イーサネット設定モードの *firewall*コマンドでルールの適用を開始した後、イーサネットポート ipfw 設定モードで、ファイアウォールルールを変更しても、起動中のファイアウォール処理には反映されません。
ファイアウォールルール変更後は、再度イーサネット設定モードの *firewall*コマンドを実施してください。

ポイント

イーサネット設定モードの *firewall*コマンドで設定するフィルタリング設定は、受信パケットにのみ適用されます。送信パケットには適用されません。

ポイント

carp(vrrp)はイーサネットポートのフィルタリング設定ではマッチしません。
VLAN のフィルタリングにて設定してください。

2.14.4.2 VLAN ipfw 設定の適用

vlan ipfw 設定モードで作成したファイアウォールルールリストを適用する場合は VLAN 設定モードで、*firewall*コマンドを使用します。

```
netwiser(config-vlan)# firewall  <list-name>
```

ファイアウォールルールの適用を停止する場合は *no* を指定してください。

```
netwiser(config-vlan)# no firewall <list-name>
```

ポイント

VLAN 設定モードの *firewall* コマンドでルールの適用を開始した後、VLAN ipfw 設定モードで、ファイアウォールルールを変更しても、起動中のファイアウォール処理には反映されません。
ファイアウォールルール変更後は、再度 VLAN 設定モードの *firewall* コマンドを実施してください。

2.14.5 ファイアウォールルールの例

2.14.5.1 TCP/UDP パケットのフィルタリング

VLAN 10 に設定されている仮想サーバーIP アドレス 192.168.1.100 に対する、192.168.0.0/16 からの HTTP(S)リクエストの許可を設定にするには、以下のようにします。

```
 ① HTTP（S）リクエストの許可と、その他のパケットの拒否
netwiser(config)# ipfw-list vlan fw-vl-10
netwiser(config-vlan-ipfw)# permit in tcp 192.168.0.0/16 192.168.1.100 eq 80 setup keep-state
netwiser(config-vlan-ipfw)# permit in tcp 192.168.0.0/16 192.168.1.100 eq 443 setup keep-state
netwiser(config-vlan-ipfw)# deny in ip any any
netwiser(config-vlan-ipfw)# exit

 ② VLAN 10 への適用
netwiser(config)# interface vlan 10
netwiser(config-vlan)# firewall fw-vl-10
```

2.14.5.2 ICMP パケットのフィルタリング

ファイアウォールの観点からは、一部の ICMP 制御メッセージは既知の攻撃に対して脆弱です。
また、診断用のトラフィックをすべて無条件に通過させると、デバッグが容易になりますが、他者からネットワークに関する情報を抽出されやすくなります。
これらの理由から、以下のルールをすべてのイーサネットポートに適用することは最適とは言えないかもしれません。

```
netwiser(config-eth-ipfw)# permit in icmp any any keep-state
```

たとえば、VLAN 10 に設定されている機器 IP アドレス 192.168.1.10 に対する Echo リクエストの拒否、その他アドレスへは Echo リクエスト・リプライのみ許可を設定にするには、以下のようにします。

```
 ① ICMP リクエストの拒否と、その他のパケットの許可
netwiser(config)# ipfw-list vlan fw-vl-icmp
netwiser(config-vlan-ipfw)# deny in icmp any 192.168.1.10 type echo log
```

```
netwiser(config-vlan-ipfw)# permit in icmp any any type echo
netwiser(config-vlan-ipfw)# permit out icmp any any type echo-reply
netwiser(config-vlan-ipfw)# deny in icmp any any log
netwiser(config-vlan-ipfw)# deny out icmp any any log
netwiser(config-vlan-ipfw)# exit

  ② VLAN 10 への適用
netwiser(config)# interface vlan 10
netwiser(config-vlan)# firewall fw-vl-icmp
```

2.15 接続先ネットワーク種別

イーサネットポートまたは論理チャネルの接続先ネットワーク種別を定義することが可能です。

```
netwiser(config-if)# slb {both | mgmt [secure] | network | server}
```

■*both*

クライアント側ネットワークとサーバー側ネットワークのどちらも接続可能な設定となります。

■*network*

クライアント側ネットワークが接続されていることを意味します。
フェイルスルー設定がされている場合、ポート１を本設定にする必要があります。
非フェイルスルーモードで動作中に本設定を行っても動作に影響はないため、デフォルト設定のままで問題ありません。

■*server*

サーバー側ネットワークが接続されていることを意味します。
フェイルスルー設定がされている場合、ポート２を本設定にする必要があります。
非フェイルスルーモードで動作中に本設定を行っても動作に影響はないため、デフォルト設定のままで問題ありません。

■*mgmt [secure]*

管理ポートとして動作させるポートに指定します。このポートから受信した仮想サーバーへの ARP/NDP 問い合わせには答えません。
また、*secure* オプションが指定された場合、指定ポートへのアクセスや指定ポートを経由するアクセスを制限します。ただし、*secure* オプションは論理チャネルに対して設定することはできません。
secure オプションが指定された場合の詳しい動作は「2.5.4 管理専用ポートの定義」を参照してください。

ポイント

フェイルスルー設定がされた場合、システムが自動的にポート1を *network*、ポート２を *server* に設定します。
ただし、フェイルスルー設定が解除されても本設定はそのままですので注意し

てください。

ポイント

デフォルト設定は *both* です。非フェイルスルー設定でも設定変更は可能ですが、必須ではありません。

2.16 ポートミラーリングの設定

ミラーリング設定を行うことで、本製品の送受信するネットワークパケットを任意のイーサネットポートにミラーリングすることができます。
ミラーリングを設定するにはイーサネット設定モードで *mirror-port* コマンドを使用します。この設定は単一ポートにのみ設定できます。

```
netwiser(config-if)# mirror-port
```

監視対象のポートでは *monitor* コマンドを実行します。
監視対象は複数設定することができますが、複数ポートを監視する対象とした場合にミラーポートはデータをロストする場合があります。また、ミラーポートを論理チャネルに含めることはできません。

```
netwiser(config-if)# monitor {tx | rx | both}
```

監視するパケットの種別は、送信パケット(*tx*)、受信パケット(*rx*)、送受信パケット(*both*)から選択できます。

以下、例としてポート 1～5 の送受信パケットをポート 6 にミラーリングします。

```
netwiser(config)# interface ethernet 6
netwiser(config-if)# mirror-port
netwiser(config-if)# exit
netwiser(config)# interface ethernet 1-5
netwiser(config-if)# monitor both
```

2.17 MAC アドレスの追加・削除

MAC アドレステーブルに静的エントリーを追加するには特権モードで *mac address* コマンドをポート番号またはチャネル番号、そしてVLAN ID を指定して実行します。VLAN ID は対象となるイーサネットポート、または論理チャネルがトランクポートである場合指定します。トランクポートでない場合、省略可能です。

削除するには *no mac address* を実行します。

```
netwiser(config)# mac address <MAC ｱﾄﾞﾚｽ> { ethernet <ｲﾝﾀｰﾌｪｲｽ番号> |
 channel <ﾁｬﾈﾙ番号> } [vlan <VLAN ID>]
netwiser(config)# no mac address <MAC ｱﾄﾞﾚｽ>
```

2.18 ARP、NDP

2.18.1 ARP テーブルエントリーの追加・削除

ARP テーブルに静的エントリーを追加するには設定モードで *arp* コマンドを使用します。

削除するには *no arp* を実行します。

既存 VLAN のネットワークセグメントに属する IP アドレスでないと arp テーブルに登録できません。

```
netwiser(config)# arp <IPv4 ｱﾄﾞﾚｽ> <MAC ｱﾄﾞﾚｽ>
```

動的 ARP エントリーの生存時間はデフォルトで 20 分です。

変更するには *arp aging-time* コマンドを実行します。

デフォルトに戻す場合 *no* を指定します。

```
netwiser(config)# arp aging-time <生存時間(dhm)>
```

2.18.2 NDP テーブルエントリーの追加・削除

NDP テーブルに静的エントリーを追加するには設定モードで *ndp* コマンドを使用します。

削除するには *no ndp* を実行します。

既存 VLAN のネットワークセグメントに属する IP アドレスでないと ndp テーブルに登録できません。

```
netwiser(config)# ndp <IPv6 ｱﾄﾞﾚｽ> <MAC ｱﾄﾞﾚｽ>
netwiser(config)# no ndp <IPv6 ｱﾄﾞﾚｽ> <MAC ｱﾄﾞﾚｽ>
```

2.19 サーバー負荷分散の設定

本章ではサーバー負荷分散に関する設定方法を例とともに記します。
更に具体的な設定例については「第4章設定例」を参照してください。

2.19.1 同時に設定できない機能

以下に挙げる機能は、同一の仮想サーバーに対して同時に設定することができません。ご注意ください。

機能	同時に設定できない機能
Cookie によるセッション維持 ［２．１９．１７．５］ ［２．１９．１７．６］	･複数のサーバーにまたがるセッション維持（仮想サーバーグループの設定） ・DSR モード
SSL セッション ID によるセッション維持 ［２．１９．１７．４］	･複数のサーバーにまたがるセッション維持（仮想サーバーグループの設定） ・DTLS プロトコル ・DSR モード ・URL スイッチング ・HTTP リダイレクトの送信 ・アクセスログの生成 ・403 レスポンスの送信 ・URL スイッチング設定 ・Fallback-url の設定 ・Location ヘッダー書き換え設定 ・発信元 IP アドレス、プロトコル情報の挿入 ・sorry コンテンツの設定 ･X-Forwarded-For セッション維持設定 ･X-Forwarded-For スイッチング設定
複数のサーバーにまたがるセッション維持（仮想サーバーグループの設定） ［２．１９．１７．１］	・Cookie によるセッション維持 ・SSL セッション ID によるセッション維持
X-Forwarded-For ヘッダーに明示された IP アドレス情報によるセッション維持 ［２．１９．１７．２］	・DSR モード ・SSL セッション ID によるセッション維持
DSR モード（dsr オプション）	・Cookie によるセッション維持

［２．１９．１８．９］	・SSL セッション ID によるセッション維持 ・URL スイッチング ・HTTP リダイレクトの送信 ・403 レスポンスの送信 ・Location ヘッダーの書き換え ・ソース NAT ・発信元 IP アドレス、プロトコル情報の挿入 ・アクセスログの生成 ・SSL アクセラレーション ・フェイルスルー ・IPv4/IPv6 変換 ・sorry コンテンツの設定 ・Fallback-url の設定 ・X-Forwarded-For スイッチング設定 ・X-Forwarded-For セッション維持設定
発信元 IP アドレスに基づく負荷分散 ［２．１９．１８．２］	・URL スイッチング ・HTTP リダイレクトの送信 ・403 レスポンスの送信 ・Location ヘッダーの書き換え
URL スイッチング ［２．１９．１８．４］ HTTP リダイレクトの送信 ［２．１９．１８．５］ 403 レスポンスの送信 ［２．１９．１８．５］	・発信元 IP アドレスに基づく負荷分散 ・DSR モード ・SSL セッション ID によるセッション維持
Location ヘッダーの書き換え ［２．１９．１８．６］	・発信元 IP アドレスに基づく負荷分散 ・DSR モード ・SSL セッション ID によるセッション維
発信元 IP アドレス、プロトコル情報の挿入 ［２．１９．１４］	・DSR モード
アクセスログ ［２．１９．１５］	・DSR モード ・SSL セッション ID によるセッション維
SSL アクセラレーション ［２．２０］	・DSR モード
sorry コンテンツの設定 ［２．１９．１８．７］	・DSR モード ・SSL セッション ID によるセッション維

Fallback-url の設定 ［２．１９．１８．８］	・DSR モード ・SSL セッション ID によるセッション維

※ 表中の「Cookie によるセッション維持」は、cookie セッション維持と cookie 挿入機能の両方を指します。
※ 表中の「発信元 IP アドレスに基づく負荷分散」は、送信元 IP アドレスによる負荷分散と X-Forwarded-For ヘッダー情報の内容による負荷分散の両方を指します。

2.19.2 実サーバーの設定

負荷分散対象となるサーバーの設定を行います。
実サーバーは<実サーバーIP アドレス>.<ポート>.<プロトコル>の形式で設定します。この形式を実サーバーID と呼称します。
削除するには *no* を使用します。

```
netwiser(config)# real <IP アドレス>.<ポート>.{tcp | udp}
netwiser(config)# no real <IP アドレス>.<ポート>.{tcp | udp}
```

ポイント

仮想サーバーにバインドされている実サーバーID を削除することはできません。*no bind* コマンドで仮想サーバーとの対応を解除してから削除してください。

ポイント

no real コマンドで実サーバーID を削除すると、そのサーバーとの間で確立中のコネクションに関する情報は失われます。

show real コマンドで実サーバー情報を参照することができます。
詳しくは「SX-3990_3950_3945_3940_3920 コマンドリファレンス」（別紙）を参照してください。

2.19.3 実サーバー状態の設定

設定直後のデフォルトでは実サーバーは稼動状態です。停止状態にするには *no enable real* コマンドを使用します。停止状態の実サーバーには新規のコネクション要求が割り振られません。ただし稼動中に確立したコネクションはそのまま維持されます。
再び稼働状態に戻す場合、*enable real* コマンドを実施します。

```
netwiser(config)# no enable real <実サーバーIP>.<ﾎﾟｰﾄ>.<ﾌﾟﾛﾄｺﾙ>
netwiser(config)# enable real <実サーバーIP>.<ﾎﾟｰﾄ>.<ﾌﾟﾛﾄｺﾙ>
```

ポート番号とプロトコルを省略すると、任意の IP アドレスに関する全てのアプリケーションが停止状態になります。以下の例では 192.168.1.10 に定義された全てのアプリケーションを停止します。

```
netwiser(config)# no enable real 192.168.1.10
```

2.19.4 最大コネクション数の設定

システム全体で実サーバーの受け付ける最大コネクション数を設定するには *maxconns* コマンドを使用します。
サーバーの最大コネクション数は、デフォルトで無制限です。
デフォルトに戻すには *no maxconns* コマンドを使用します。
以下の例では、HTTP サーバー192.168.1.10 の最大コネクションを 2 万に設定します。

```
netwiser(config)# maxconns 192.168.1.10.80.tcp 20000
```

最大コネクション数を無制限に戻すには no を指定します。

```
netwiser(config)# no maxconns 192.168.1.10.80.tcp
```

maxconns コマンドは UDP サーバーに対して適用できません。

ポイント 接続中のコネクションがある状態で最大コネクション数を変更した場合、現在接続中のコネクションが切れてから設定が反映されますので注意してください。

ポイント コネクション接続とコネクション切断のタイミングによっては、設定より小さい値で最大コネクション数に達することがあります。

ポイント 最大コネクション数に達した実サーバーへは、新規コネクションを確立することができません。ただし、セッション維持機能により生成されたセッション情報に合致する新規コネクションに関しては、最大コネクション制限の対象になりません。

ポイント 仮想サーバー毎に実サーバーの最大コネクションを指定することも可能です。詳しくは「2.19.18仮想サーバーと実サーバーの関連付け」を参照してください。

2.19.5 MSL タイマーの設定

本製品の負荷分散処理におけるTCPコネクションのMSLタイマー（Maximum Segment Lifetime） はデフォルトで 2 秒です。
MSL タイマーを変更することで、本製品が管理する TCP コネクションの TIME_WAIT 状態における待ち時間（=MSL タイマーの 2 倍）が変化します。
変更するには *system msl-timer* コマンドを実施します。
以下では、MSL タイマーを 5 秒に設定することで、TIME_WAIT 状態の待ち時間（=MSL タイマーの 2 倍）を 10 秒に設定します。

```
netwiser(config)# system msl-timer 5s
```

デフォルトの MSL タイマーに戻す場合は、*no system msl-timer* コマンドを実施します。

```
netwiser(config)# no system msl-timer
```

⚠ 注意 MSLタイマー値の変更は負荷分散動作だけでなく、TCP ヘルスチェック時の動作など、システム全体に影響します。

2.19.6 仮想サーバーの設定

仮想サーバーを設定するにはあらかじめ仮想サーバーIP アドレスの設定を行わなければなりません。
仮想サーバーIP アドレスの設定は VLAN 設定モードで *ip virtual-address* コマンドを使用します。

```
netwiser(config)# interface vlan <VLAN ID>
netwiser(config-vlan)# ip virtual-address <仮想サーバーIP>
```

仮想サーバーIP アドレスの設定が完了した後、仮想サーバーの設定を行います。
仮想サーバーは<仮想サーバーIP アドレス>.<ポート>.<プロトコル>の形式で設定します。この形式を仮想サーバーID と呼称します。

仮想サーバーを設定するには特権モードで *virtual* コマンドを実行します。
virtual コマンドを実行すると仮想サーバー設定モードに遷移します。

```
netwiser(config)# virtual <IP ｱﾄﾞﾚｽ>.<ﾎﾟｰﾄ番号>.{tcp|udp|ftp}
netwiser(config-virtual)#
```

FTP パケットはデータ部分に IP アドレス情報を含むため、負荷分散するには特殊な処理が必要になります。FTP サーバーの制御ポートとしてデフォルトの 21 以外を使用する場合はプロトコルに ftp と設定してください。
tftp の負荷分散をするには、ポート番号に 69、プロトコルに udp と設定してください。

仮想サーバーの設定を削除するには、特権モードで *no virtual* コマンドを使用します。

```
netwiser(config)# no virtual <IP ｱﾄﾞﾚｽ>.<ﾎﾟｰﾄ番号>.{tcp|udp|ftp}
```

show virtual コマンドで仮想サーバー情報を参照することができます。
詳しくは「**SX-3990_3950_3945_3940_3920 コマンドリファレンス**」（別紙）を参照してください。

仮想サーバーに名前付けして管理することが可能です。名前付けするには仮想サーバー設定モードで *name* コマンドを使用します。
名前付けをすると、仮想サーバーID の代わりに仮想サーバー名を使用すること

が可能です。

```
netwiser(config)# virtual 192.168.1.100.80.tcp
netwiser(config-virtual)# name http-app
netwiser(config-virtual)# exit
netwiser(config)# virtual http-app
netwiser(config-virtual)#
```

ポイント

仮想サーバー名を指定して仮想サーバー設定モードに遷移し、かつその状態で仮想サーバー名を変更した場合、それ以降仮想サーバー設定モードで実行するコマンドは失敗します。
一旦仮想サーバー設定モードから *exit* し、新しい仮想サーバー名を指定して仮想サーバー設定モードに入り直してください。

⚠ 注意

ポート番号 0 を指定した仮想サーバーに対して、以下の設定はできません。

- アクセスログ設定
- SSL アクセラレーション設定
- SSL セッション維持設定
- cookie セッション維持設定
- URL スイッチング設定
- URL リダイレクト設定、または 403 応答の設定
- Fallback-url の設定
- Location ヘッダー書き換え設定
- ヘッダー挿入設定
- sorry コンテンツの設定
- IPv4/IPv6 変換設定
- X-Forwarded-For セッション維持設定
- X-Forwarded-For スイッチング設定

2.19.7 仮想サーバー状態の設定

仮想サーバーはデフォルトで停止状態です。稼働状態にするには *enable* コマンドを使用します。また、停止状態に戻すには *no enable* コマンドを使用します。

```
netwiser(config)# enable virtual {<IP ｱﾄﾞﾚｽ>.<ﾎﾟｰﾄ番号>.{tcp|udp|ftp} | <IP ｱﾄﾞﾚｽ>}
netwiser(config)# no enable virtual {<IP ｱﾄﾞﾚｽ>.<ﾎﾟｰﾄ番号>.{tcp|udp|ftp} | <IP ｱﾄﾞﾚｽ>}
```

仮想サーバー状態の変更は、仮想サーバー設定モードで *enable* コマンドを実行することでも実現できます。

```
netwiser(config-virtual)# enable
netwiser(config-virtual)# no enable
```

特権モードで *enable* コマンドを実行する場合、ポート番号とプロトコルを省略すると、全てのアプリケーションが稼動状態になります。以下の例では 192.168.1.100 に定義された全てのアプリケーションを停止します。

```
netwiser(config)# no enable virtual 192.168.1.100
```

停止状態の仮想サーバーは新規のコネクション要求を受け付けません。ただし稼動中に確立したコネクションはそのまま維持されます。

2.19.8 仮想サーバーへの ping 許可設定

デフォルトでは、仮想サーバーIP アドレスへの ping には応答しません。
仮想サーバーIP アドレスへの ping に応答するには、特権モードで ***allow-ping*** コマンドを実行します。
仮想サーバーIP アドレスへの ping に応答しない設定に戻すには ***no*** を指定します。

```
netwiser(config)# allow-ping
netwiser(config)# no allow-ping
```

⚠ 注意 同一 IP アドレスの仮想サーバーが複数登録されており、ルート ID がそれぞれの仮想サーバーで異なる場合は、応答パケットは最初に登録されている仮想サーバーのルート ID のルーティングテーブルに従います。

2.19.9 負荷分散方式の変更

任意の仮想サーバーにおいて、負荷分散方式を設定するには ***predictor*** コマンドを使用します。
ラウンドロビン方式の場合 ***robin***、最小コネクション方式の場合 ***load*** を指定します。

```
netwiser(config-virtual)# predictor {robin | load}
```

プロトコルが tcp、または ftp の仮想サーバーは、デフォルトで最小コネクションが設定されます。
プロトコルが udp の仮想サーバーは、ラウンドロビンのみ設定可能です。

2.19.10 アイドルタイマー値の変更

アイドル状態（無通信状態）の L4 コネクションを破棄する時間はデフォルトで、tcp が 30 分、udp が 5 分です。このタイマー値を変更するには、仮想サーバー設定モードで *timeout* コマンドを使用します。

```
adm(config-virtual)# timeout <日時分秒(dhms)>
```

範囲は 0 秒（無期限）から 365 日です。ただし、udp 仮想サーバーには、0（または 0s）を指定しないでください。

タイマー値をデフォルト設定に戻すには *no* を指定します。

```
adm(config-virtual)# no timeout
```

ポイント

この設定は L7 コネクションには適用されません。

L7 コネクションとは、以下のいずれかの設定がされた仮想サーバーが処理するコネクションのことを指します。

- SSL アクセラレーション設定
- SSL セッション維持設定
- cookie セッション維持設定
- URL スイッチング設定
- HTTP リダイレクト設定
- Location ヘッダー書き換え設定
- Fallback-url の設定
- sorry コンテンツの設定
- アクセスログ設定
- ヘッダー挿入設定
- IPv4/IPv6 変換設定
- X-Forwarded-For スイッチング設定
- X-Forwarded-For セッション維持設定

2.19.11 送信元アドレスの変換(ソース NAT)

実サーバーへの送信元アドレスの変換を仮想サーバーで行うには、NAT プールを定義し、定義した NAT プールを仮想サーバーへ割り当てます。

NAT プールを定義するには NAT プール設定モードに遷移し、プールアドレスを登録します。

```
adm(config)# nat-pool <ﾎﾟﾘｼｰ名>
adm(config-natpool)# ip address { <ﾌﾟｰﾙｱﾄﾞﾚｽ> | range <開始ﾌﾟｰﾙｱﾄﾞﾚｽ> <終了ﾌﾟｰﾙｱﾄﾞﾚｽ>}
```

プールアドレスの削除や NAT プールポリシーの削除には *no* を指定します。

```
adm(config-natpool)# no ip address { <ﾌﾟｰﾙｱﾄﾞﾚｽ> | range <開始ﾌﾟｰﾙｱﾄﾞﾚｽ> <終了ﾌﾟｰﾙｱﾄﾞﾚｽ>}
adm(config)# no nat-pool <ﾎﾟﾘｼｰ名>
```

ポイント

範囲指定(*range* オプション指定)でアドレスを登録する場合、範囲内に仮想サーバーIP アドレスを含めることはできません。仮想サーバーIP アドレスは *range* オプションを付けずに1件ずつ登録してください。

ポイント

NAT プールのポリシーは 256 件まで登録可能です。
プールアドレスの最大登録数はシステム全体で 16 件です。ただし、仮想サーバーIP アドレスは登録制限に含まれません。
また、NAT プールアドレスにはリンクローカルアドレスを設定しないでください。

定義した NAT プールを仮想サーバーに割り当てるには、仮想サーバー設定モードで *source-nat* コマンドを実行します。また、NAT プールの割り当てを解除するには *no* を指定します。

```
adm(config-virtual)# source-nat <ﾎﾟﾘｼｰ名>
adm(config-virtual)# no source-nat
```

仮想サーバー設定に割り当てられている状態の NAT プールポリシーを削除することはできません。仮想サーバーでの割り当てを解除してから削除してください。

以下の例では、仮想サーバー192.168.1.100.80.tcp の送信元アドレス変換ルールとして 192.168.1.100～103 を定義します。

```
adm(config)# nat-pool pool_addr
adm(config-natpool)# ip address 192.168.1.100
adm(config-natpool)# ip address range 192.168.1.101 192.168.1.103
adm(config-natpool)# exit
adm(config)# virtual 192.168.1.100.80.tcp
adm(config-virtual)# source-nat pool_addr
```

ポイント

NAT プール設定モードでプールアドレスの追加・削除を行うだけで、該当の NAT プールポリシーを割り当てている仮想サーバーにも設定が反映されます。

show nat-pool コマンドで NAT プールアドレスの使用状況を統計情報として表示させることができます。
詳しくは**「SX-3990_3950_3945_3940_3920 コマンドリファレンス」**（別紙）を参照してください。

ポイント

source-nat コマンドを実施した場合、該当の仮想サーバーに対する全てのアクセスの送信元アドレスが、プールアドレスに変換されます。特定のネットワークからのアクセスにのみ送信元アドレスの変換機能を適用したい場合は NAT フィルター設定を実施します。NAT フィルター設定は「2.19.13ソース NAT フィルタリングの設定」を参照してください。

2.19.12 ワンアームゲートウェイモードの設定

ワンアーム構成でソース NAT 設定を使用せずに負荷分散するにはワンアームゲートウェイモード設定を使用します。

ワンアームゲートウェイモードを使用するには、仮想サーバー設定モードで、*onearm-gateway-mode* コマンドを実行します。

```
adm(config-virtual)# onearm-gateway-mode
```

設定を削除するには *no* を指定します。

```
adm(config-virtual)# no onearm-gateway-mode
```

ポイント

ワンアームゲートウェイモードで使用する場合、実サーバーのデフォルトゲートウェイを本製品の管理 IP アドレス、または冗長 IP アドレス(冗長構成の場合)に設定する必要があります。

ポイント

この設定はソース NAT 設定、ソース NAT フィルタリング設定と併用することで、指定した任意のクライアントアドレスのみソース NAT させることが可能です。
仮想サーバーと同じ VLAN に存在するクライアントからアクセスする場合は、ソース NAT 設定、ソース NAT フィルタリング設定が必須となります。
詳しくはワンアーム構成の構成例「4.7.3構成例 3(ソース NAT+ワンアームゲートウェイモード)」を参照してください。

2.19.13 ソース NAT フィルタリングの設定

仮想サーバーに対して、特定のネットワークアドレスからのアクセスにのみ、送信元アドレスの変換機能を適用するには *permit-nat-filter* コマンドでソース NAT フィルタールールを登録します。
ソース NAT フィルタールールを登録するには、事前に *source-nat* コマンドで送信元アドレス変換機能を有効にする必要があります。送信元アドレス変換機能の設定は「2.19.11送信元アドレスの変換」を参照してください。

source-nat コマンド実施後、*permit-nat-filter* コマンドで任意のネットワークアドレスを指定します。指定されたネットワークアドレスからのアクセスの送信元アドレスが、*source-nat* コマンドで指定した NAT プールアドレスに変換されます。

```
adm(config-virtual)# permit-nat-filter {<ipv4ｱﾄﾞﾚｽ> <ﾏｽｸｱﾄﾞﾚｽ> | <ipv4ｱﾄﾞﾚｽ/ﾏｽｸ長> | <ipv6ｱﾄﾞﾚｽ/ﾌﾟﾚﾌｨｸｽ長>}
```

以下では、仮想サーバー192.168.1.100.80.tcp に対する、192.168.1.0/24 からのアクセスにのみ、送信元アドレス変換機能が適用され、その他のネットワークからのアクセスには、送信元アドレス変換機能が適用されません。

```
adm(config)# virtual 192.168.1.100.80.tcp
adm(config-virtual)# permit-nat-filter 192.168.1.0/24
```

削除する場合は *no* を指定します。

```
adm(config-virtual)# no permit-nat-filter 192.168.1.0/24
```

アドレスの変換には、*source-nat* コマンドで指定した NAT プールのプールアドレスが使用されます。
no source-nat コマンドにより、仮想サーバーの送信元アドレス変換機能が無効に設定された場合は、該当の仮想サーバーに設定された全てのソース NAT フィルター設定が自動で削除されます。

ポイント

permit-nat-filter コマンドは、新規コネクションから適用されるものであり、既存コネクションには影響しません。

2.19.14 発信元 IP アドレス、プロトコル情報のヘッダーおよび Cokkie 属性挿入

仮想サーバーが HTTP サーバーの場合、変換前の発信元 IP アドレス、プロトコルを HTTP リクエストに挿入することが可能です。

```
adm(config-virtual)# header insert {x-forwarded-for | x-forwarded-proto | both}
```

header insert x-forwarded-for コマンドを実施することで、該当の仮想サーバーに対する全てのリクエストに以下のヘッダーを挿入して実サーバーに送信します。

```
X-Forwarded-For: 変換前の発信元 IP ｱﾄﾞﾚｽ
```

header insert x-forwarded-proto コマンドを実施することで、該当の仮想サーバーに対する全てのリクエストに以下のヘッダーを挿入して実サーバーに送信します。

```
X-Forwarded-Proto: 変換前の宛先ﾌﾟﾛﾄｺﾙ
```

実サーバーが発行した Set-Cookie ヘッダーに任意の Cookie 属性を挿入することが可能です。

```
adm(config-virtual)# server-cookie-attribute insert "cookie属性"
```

以下のように、HttpOnly 属性が設定された cookie は JavaScript からアクセスできなくなり、Secure 属性が設定された cookie は HTTPS 通信時だけその cookie を送信します。

```
adm(config-virtual)# server-cookie-attribute insert "Secure; HttpOnly"
```

⚠ 注意

*cookie 属性*で指定した文字列についてはチェックせずにそのまま付加します。指定文字列が属性として正しいことをご確認ください。

ポイント

ヘッダー挿入機能は L7 負荷分散機能の一部です。ヘッダー挿入機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

2.19.15 アクセスログ

仮想サーバーが HTTP サーバーの場合、アクセスログを生成し外部の syslog サーバーへ送信することが可能です。

```
adm(config-virtual)# access-log <IP アドレス> <ファシリティー、レベル>
```

本設定は *logging* コマンドの設定状態と関連していません。また、生成されたログは本製品内部の syslog バッファには残りません。

本製品は以下の例のような NCSA 共通形式のメッセージを生成します。形式を変更することはできません。

<送信元アドレス> --[<日時分>] "<アクセス先 URL パス>" <ステータスコード> <応答メッセージのボディサイズ>

以下に実際に送出されるメッセージの例を示します。

```
127.0.0.1 - - [15/Aug/2012:18:15:05 +0900] "/cgi-bin/index.cgi" 200 1050
```

ポイント

アクセスログ機能は L7 負荷分散機能の一部です。アクセスログ機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

ファシリティー、ログレベルを表す数値の対応を以下に明記します。

ファシリティー		レベル	
LOCAL0	16	emerg	0
LOCAL1	17	alert	1
LOCAL2	18	crit	2
LOCAL3	19	err	3
LOCAL4	20	warn	4
LOCAL5	21	notice	5
LOCAL6	22	info	6
LOCAL7	23	debug	7

2.19.16 仮想サーバーへのルーティングテーブルの設定

仮想サーバーで使用するルーティングテーブルのルート ID を設定できます。

仮想サーバーで使用するルート ID を設定するには *route-id* コマンドを実行します。ルート ID が設定されている場合は、負荷分散対象となるパケットが仮想サーバーに設定されたルート ID と同一の ID を持つルーティングテーブルに従います。

ルート ID を設定しない場合はルート ID 0 が使用されます。
削除するには *no* を使用するか、ルート ID 0 を指定します。

```
netwiser(config-virtual)# route-id <ルート ID>
netwiser(config-virtual)# no route-id
```

設定できるルート ID の範囲は 0 から 15 です。

2.19.17 セッション維持機能の設定

仮想サーバー設定モードで *sticky* コマンドを使用すると、同一クライアントからの通信が、一定時間同一のサーバーに割り振られるようになります。たとえば、クライアントがオンラインで何かのフォームを記入するような場合、一定の時間通信を同一のサーバーに割り振ることにより、トランザクションを完結させることができます。

セッションの維持として利用可能な情報は IP アドレス、X-Forwarded-For ヘッダー、cookie、SSL セッション ID の 4 種類です。

```
adm(config-virtual)# sticky {{generic | x-forwarded-for} [mask <マスク長>] | cookie <クッキー名> [insert {always | once} [attribute <attribute-string>]] | ssl} [timeout <日時分(dhm)>]
```

timeout <分>で指定する時間は、あるクライアントからのコネクションが全て終了したアイドル状態で、セッション維持機能が有効である時間を指します。

たとえば *sticky* コマンドで *timeout 5m* と設定すると、次のコネクション要求が 5 分以内に発生すれば前と同じサーバーに送信されますが、5 分を経過すると別のサーバーに割り振られる可能性があります。

timeout の範囲は 1 分から 365 日です。ただし、*insert* オプション付き cookie セッション維持の場合 0 分を指定することが可能です。

2.19.17.1 IP アドレスセッション維持

クライアントの IP アドレスに基づいたセッション維持を設定するには *generic* オプションを指定します。

```
adm(config-virtual)# sticky generic [mask <マスク長>] [timeout <日時分(dhm)>]
```

セッション維持のタイムアウト間隔は日時分(dhm)で指定します。省略した場合 15 分に設定されます。

IP アドレス単位ではなくサブネット単位でセッションを維持したい場合、*mask* オプションを指定し、任意のマスク/プレフィックス長を入力します。
以下の例では、送信元 IP アドレスを 24bit でマスクし、同じサブネットとなるクライアントからのアクセスに関して、振り分け先サーバーを統一します。

```
adm(config-virtual)# sticky generic mask 24
```

IP アドレスセッション維持を無効にするには *no sticky generic* コマンドを実施します。

```
adm(config-virtual)# no sticky generic
```

show sticky generic コマンドで IP アドレスセッション維持情報を参照することができます。詳しくは**「SX-3990_3950_3945_3940_3920 コマンドリファレンス」**（別紙）を参照してください。

更に、仮想サーバーグループを作成することで、複数の仮想サーバー間で IP セッション維持情報を共有することが可能です。
仮想サーバーグループ設定の詳細は「2.19.17.3 仮想サーバーグループの形成」を参照してください。

2.19.17.2 X-Forwarded-For セッション維持

X-Forwarded-For ヘッダー情報に明示されている IP アドレス情報に基づいてセッション維持を行うことが可能です。これにより、X-Forwarded-For ヘッダーにクライアントの IP アドレス情報が埋め込まれてさえいれば、プロキシサーバーを経由するなどして IP アドレスが隠蔽されている場合においても、クライアント IP アドレスに基づくセッション維持が可能です。

X-Forwarded-For セッション維持を設定するには ***x-forwarded-for*** オプションを指定します。

```
adm(config-virtual)# sticky x-forwarded-for [mask <マスク長>] [timeout <日時分(dhm)>]
```

HTTP リクエスト内に X-Forwarded-For ヘッダーが存在しない場合、IP ヘッダーの送信元アドレス情報を基にセッション維持情報が生成されます。また、X-Forwarded-For ヘッダーに複数の IP アドレス情報が明示されている場合は、先頭の IP アドレス情報を参照します。

ポイント

X-Forwarded-For ヘッダー情報に基づいて生成されたセッション維持情報は、IP アドレスセッション維持情報と同等に扱われます。IP アドレスセッション維持設定と同様にタイムアウト間隔やサブネット単位でのセッション維持が可能です。

ただし、X-Forwarded-For セッション維持設定は L7 負荷分散機能の一部であるため、設定された仮想サーバーに対する全てのリクエストは L7 レベルで処理されます。その点で、IP アドレスセッション維持設定とは異なります。

なお、X-Forwarded-For セッション維持設定がされている状態から、IP アドレスセッション維持設定に切り替えた場合、その時点における該当仮想サーバーの IP セッション情報は全て削除されるのでご注意ください。

セッション維持のタイムアウト間隔は日時分(dhm)で指定します。省略した場合 15 分に設定されます。

IP アドレス単位ではなくサブネット単位でセッションを維持したい場合、***mask*** オプションを指定し、任意のマスク/プレフィックス長を入力します。

以下の例では、X-Forwarded-For ヘッダーに明示された IP アドレス情報を

24bit でマスクし、同じサブネットとなるクライアントからのアクセスに関して、振り分け先サーバーを統一します。

```
adm(config-virtual)# sticky x-forwarded-for mask 24
```

X-Forwarded-For ヘッダー情報に基づくセッション維持を無効にするには *no sticky x-forwarded-for* コマンドを実施します。

```
adm(config-virtual)# no sticky x-forwarded-for
```

show sticky generic コマンドで X-Forwarded-For セッション維持情報を参照することができます。詳しくは**「SX-3990_3950_3945_3940_3920 コマンドリファレンス」**（別紙）を参照してください。

更に、仮想サーバーグループを作成することで、複数の仮想サーバー間で X-Forwarded-For セッション維持情報を共有することが可能です。
仮想サーバーグループ設定の詳細は「2.19.17.3 仮想サーバーグループの形成」を参照してください。

⚠ 注意

仮想サーバーIP のアドレスファミリーと、X-Forwarded-For ヘッダーにセットされた IP アドレスのアドレスファミリーが一致しない場合、セッション維持情報が正常に生成されません。

2.19.17.3 仮想サーバーグループの形成

IP セッション維持設定、または X-Forwarded-For セッション維持設定で動作する仮想サーバー同士をグループ化することで、異なる仮想サーバー同士でセッション維持情報を共有することが可能です。

複数の仮想サーバーにわたって IP アドレスに基づいたセッション維持を設定するには、*buddy* コマンドを使用して複数の仮想サーバーをグループ化します。これにより、グループに属する複数の仮想サーバー間で、セッション情報を共有することが可能です。
以下は特権モードで実施してください。

```
adm(config)# buddy <グループ名> <仮想サーバー ID 1> [<仮想サーバー ID 2> ...]
```

ひとつのグループには最大で 5 つの仮想サーバーを追加することができます。ただし、一つの仮想サーバーが複数のグループに所属することはできません。

以下の例では my_app という名前のグループを作り、HTTP 仮想サーバー（192.168.1.100.80.tcp）と HTTPS 仮想サーバー（192.168.1.100.443.tcp）を所属させます。これにより、2 台の仮想サーバー間でセッション情報を共有して動作します。

```
adm(config)# virtual 192.168.1.100.80.tcp
adm(config-virtual)# sticky generic timeout 30m
adm(config-virtual)# exit
adm(config)# virtual 192.168.1.100.443.tcp
adm(config-virtual)# sticky generic timeout 30m
adm(config-virtual)# ssl my-app-cert
adm(config-virtual)# exit
adm(config)# buddy my_app 192.168.1.100.443.tcp 192.168.1.100.80.tcp
```

sticky コマンドは buddy グループ全体に対して有効となるので、クライアントが仮想サーバー192.168.1.100.443.tcp へアクセス後 192.168.1.100.80.tcp へアクセスすると、そのリクエストは 192.168.1.100.443.tcp と同一の実サーバーに割り振られます。これは、逆の順番でも同じです。
セッション維持のポリシーが X-Forwarded-For セッション維持であっても同様の設定が可能です。

*buddy*コマンドで指定する仮想サーバーIDには、仮想サーバーに付けた名前を指定することも可能です。

```
adm(config)# virtual 192.168.1.100.80.tcp
adm(config-virtual)# sticky generic timeout 30m
adm(config-virtual)# name my-app-http
adm(config-virtual)# exit
adm(config)# virtual 192.168.1.100.443.tcp
adm(config-virtual)# sticky generic timeout 30m
adm(config-virtual)# name my-app-https
adm(config-virtual)# ssl my-app-cert
adm(config-virtual)# exit
adm(config)# buddy my_app my-app-https my-app-http
```

任意の仮想サーバーを buddy グループメンバーから解除する、もしくは buddy グループを削除するには、*no buddy*コマンドを使用します。

```
① 仮想サーバーmy-aap-http のみグループから解除する
adm(config)# no buddy my_app my-app-http
② グループ my_app を削除する
adm(config)# no buddy my_app
```

ポイント

timeout 設定、*mask* 設定に関して、buddy グループ内の各仮想サーバーは共通の設定値を使用して動作します。このとき、IP セッション維持（あるいは X-Forwarded-For セッション維持）が設定されている仮想サーバーの中で、buddy グループの最初に指定されている仮想サーバーの設定情報が buddy グループ内で共有されます。

上の設定例では、my-app-http は my-app-https に設定されたセッション維持設定情報を基に動作します。

これは、my-app-http の *timeout* や *mask* の設定値が my-app-https と異なる場合や、my-app-http にセッション維持が設定されていない場合においても同様です。 ただし、my-app-https にセッション維持が設定されていない場合は、my-app-http の設定情報が buddy グループ内で共有されます。

更には、IP セッション維持が設定されている仮想サーバーと X-Forwarded-For セッション維持が設定されている仮想サーバー間で仮想サーバーグループを形成した場合も、同様に buddy グループの最初に指定されている仮想サーバーのセッション維持設定が有効になります。

buddy グループ内のどの仮想サーバーにもセッション維持設定がされていない場合、buddy グループの各仮想サーバー間でセッション情報を共有することはできません。

2.19.17.4 SSL セッション維持

SSL セッション ID に基づいたセッション維持を設定するには ***ssl*** オプションを指定します。

※ DTLS(Datagram Transport Layer Security)プロトコルでは機能しません。

セッション維持のタイムアウト間隔は日時分(dhm)で指定します。省略した場合 15 分に設定されます。

```
adm(config-virtual)# sticky ssl [timeout <日時分(dhm)>]
```

SSL セッション維持を無効にするには ***no sticky ssl*** コマンドを実施します。

```
adm(config-virtual)# no sticky ssl
```

show sticky ssl コマンドで SSL セッション維持情報を参照することができます。

詳しくは**「SX-3990_3950_3945_3940_3920 コマンドリファレンス」**（別紙）を参照してください。

2.19.17.5 cookie セッション維持

cookieに基づいたセッション維持を設定するには ***cookie***オプションを指定します。
セッション維持のタイムアウト間隔は日時分(dhm)で指定します。省略した場合30 分に設定されます。

```
adm(config-virtual)# sticky cookie <クッキー名> [timeout <日時分(dhm)>]
```

クッキー名は実サーバーによって生成され、Set-Cookie ヘッダーで通知されるcookie の名前です。
クッキー名は 255 文字以内に設定してください。

ポイント

cookie 情報は、cookie セッション維持が設定されている全ての仮想サーバー間で共有されます。

URL によるセッション維持は cookie によるセッション維持設定を行うことによって同時に使用可能になります。この場合も web サーバーからのレスポンスにSet-Cookie ヘッダーが含まれていなければなりません。URL によるセッション維持は、cookie セッション維持が設定してあり、クライアントからのリクエストにcookie ヘッダーがなかった場合に行われます。URL とパラメーターの区切り文字には";"(セミコロン),"?"(疑問符)が使用できます。パラメーター同士の区切り文字には"&"(アンパサンド), "?"(疑問符)が使用できます。

ポイント

クッキー名を sessionid と設定した場合、HTTP リクエストに下記のような URLが含まれると下線部を HTTP cookie と同等のものとして解釈します。
例)
/page.html?sessionid=abcdefg
/page.html;sessionid=abcdefg
/page.html;sessionid=abcdefg?dummy=xxxx
/page.html?dummy=xxxx?sessionid=abcdefg
/page.html?dummy=xxxx&sessionid=abcdefg
/page.html?dummy=xxxx&dummy2=yyyy&sessionid=abcdefg

show sticky cookie コマンドでcookieセッション維持情報を参照することができます。

詳しくは「SX-3990_3950_3945_3940_3920 コマンドリファレンス」（別紙）を参照してください。

2.19.17.6 cookie 挿入機能

本製品が実サーバーの代わりに生成した cookie をセッション維持に利用するには、*insert* オプションを指定します。
セッション維持のタイムアウト間隔は日時分(dhm)で指定します。省略した場合 0 分に設定されます。

```
adm(config-virtual)# sticky cookie <クッキー名> insert {always | once }
  [attribute <attribute-string>] [timeout <日時分(dhm)>]
```

timeout で指定する時間はクライアント側に記憶される cookie の有効期間を指します。
0(または 0m)を指定した場合、cookie の保持期間はクライアントがブラウザを閉じるまでとなります。

また、*insert* オプション付き cookie セッション維持機能では *always*、*once* のいずれかを選択します。
always を指定した場合、サーバーからの全ての HTTP 応答に Cookie を挿入します。*always* を指定することにより、アクセスのたびに cookie の有効期限が更新されます。

once を指定した場合、HTTP リクエストに該当の Cookie が含まれていない場合にのみ Cookie を挿入します。*once* を指定することにより、cookie の有効期限は最初のアクセスからの経過時間になります。

attribute オプションでは、Secure 属性や HttpOnly 属性など指定した属性を Set-cookie ヘッダに付加します。

```
adm(config-virtual)# sticky cookie SESSIONID insert once attribute
"Secure; HttpOnly"
```

⚠ 注意

attribute で指定した文字列についてはチェックせずにそのまま付加します。指定文字列が属性として正しいことをご確認ください。

2.19.18 仮想サーバーと実サーバーの関連付け

仮想サーバーに実サーバーを関連付けるには、*bind*コマンドを使用します。
また、*bind*コマンドに *weight* オプションを指定することで、負荷分散の重みを指定することが可能です。
更に、*bind*コマンドに *backup* オプションを指定することで、任意の実サーバーをバックアップサーバーとして仮想サーバーに関連付けることが可能です。
また、*overflow*オプションを指定することで、任意の実サーバーをオーバーフローサーバーとして仮想サーバーに関連付けることが可能です。

ポイント

バックアップサーバーとはプライマリーサーバーが DOWN 状態に変化したときに、プライマリーサーバーに代わって負荷分散対象となるサーバーです。
オーバーフローサーバーとはプライマリーサーバーが最大コネクションに達したときに、プライマリーサーバーに代わって負荷分散対象となるサーバーです。

以下の例では、実サーバー192.168.1.11.80.tcpと実サーバー192.168.1.12.80.tcp に対して 3 対 1 で負荷分散し、かつ実サーバー192.168.1.13.80.tcp をバックアップサーバーとして待機させます。

```
adm(config-virtual)# bind 192.168.1.11.80 weight 3
adm(config-virtual)# bind 192.168.1.12.80 weight 1
adm(config-virtual)# bind 192.168.1.13.80 weight 1 backup
```

以下の例では、実サーバー192.168.1.11.80.tcpと実サーバー192.168.1.12.80.tcp に対して最大コネクション数を指定して負荷分散し、かつ実サーバー192.168.1.13.80.tcp をオーバーフローサーバーとして待機させます。
最大コネクション数を設定するには *maxconns* オプションを使用します。

```
adm(config-virtual)# bind 192.168.1.11.80 weight 1 maxconns 1000
adm(config-virtual)# bind 192.168.1.12.80 weight 1 maxconns 2000
adm(config-virtual)# bind 192.168.1.13.80 weight 1 overflow
```

仮想サーバーとの関連付けを解除するには *no* を指定します。

```
adm(config-virtual)# no bind <実サーバーIP> ,<ﾎﾟｰﾄ>
```

重みに 0 を指定すると、*no bind*と同等の動作になります。重みに 0 指定した場合は、*no bind*で関連付けを解除した場合と違い、設定ファイル上に *bind*設定情報が残ります。そのため、サーバーメンテナンスなどで一時的に仮想サーバーとの関連付けから解除する場合などで使用します。

ポイント

同一の実サーバーを複数のバインドグループに所属させる場合、*maxconns* の値は同じである必要があります。そのため *maxconns* の値を設定した場合は、同一の実サーバーの *maxconns* の値が全て最新の値で上書きされます。
以下の設定例では、実サーバー192.168.1.11.80 の *maxconns* の値は全て 3000 に設定されます。

```
adm(config-virtual)# bind 192.168.1.11.80 group 1 maxconns 1000
adm(config-virtual)# bind 192.168.1.11.80 group 2 maxconns 2000
adm(config-virtual)# bind 192.168.1.11.80 group 3 maxconns 3000
```

weight の値も同様に、同一の実サーバーの *weight* の値が全て最新の値で上書きされます。
また、以下のように、実サーバー192.168.1.11.80 の *maxconns* の値を省略した場合は、同一の実サーバーの *maxconns* の値が適用されます。

```
adm(config-virtual)# bind 192.168.1.11.80 group 1 maxconns 1000
adm(config-virtual)# bind 192.168.1.11.80 group 2 maxconns 1000
adm(config-virtual)# bind 192.168.1.11.80 group 3
```

ポイント

システム全体で実サーバーの受け付ける最大コネクション数を設定することも可能です。このシステム全体の最大コネクション数に達している場合、bind コマンドで指定した最大コネクション数に達していなくても、コネクション数が制限されます。詳しくは「2.19.4最大コネクション数の設定」を参照してください。

IP アドレスを基に負荷分散を行う場合「2.19.18.2IP スイッチングの設定」を参照してください。
HTTP ヘッダー情報を基に負荷分散を行う場合「2.19.18.4URL スイッチングの設定」を参照してください。

show bind コマンドで仮想サーバーと実サーバーの関連付けと、それら統計情報が表示できます。
詳しくは**「SX-3990_3950_3945_3940_3920 コマンドリファレンス」**（別紙）を参照してください。

2.19.18.1 バックアップサーバー・オーバーフローサーバーの動作

待機系サーバーの挙動に関して設定を変更するには、*backup-policy* コマンドを実行します。待機系のサーバーとはバックアップサーバー、またはオーバーフローサーバーに設定された実サーバーを指します。

adm(config-virtual)# *backup-policy {single | multi} [failback {forced | orderly}]*

待機系サーバーが active 状態になるタイミングとして、以下のいずれかを選択できます。デフォルトでは、*single* が設定されています。

■*single*

バックアップサーバー	全てのプライマリーサーバーが DOWN すると、バックアップサーバーが起動（プライマリーへ昇格）します。
オーバーフローサーバー	全てのプライマリーサーバーが最大コネクション数に達すると、オーバーフローサーバーが稼働（プライマリーへ昇格）します。

■*multi*

バックアップサーバー	プライマリーサーバーのうち 1 台が DOWN すると、バックサップサーバーが起動（プライマリーへ昇格）します。
オーバーフローサーバー	プライマリーサーバーのうち 1 台が最大コネクション数に達すると、オーバーフローサーバーが稼働（プライマリーへ昇格）します。

ポイント

single、*multi* のどちらを指定した場合においても、待機系サーバーを複数台登録する事が可能です。
待機系サーバーは登録した順に起動（プライマリーへ昇格）します。

また、プライマリーに昇格したサーバーが再び待機系に降格した場合の動作として、以下のいずれかを選択できます。デフォルトでは、*orderly* が設定されています。

■*forced*

プライマリーサーバーが起動しフェイルバックした際に、待機系サーバーへのセッション維持情報（sticky 情報）を使用しなくなります。これにより、以降の全ての新規接続要求を強制的にプライマリーサーバーに戻します。

■*orderly*

プライマリーサーバーが復帰して、フェイルバック動作が発生しても、現在生成されている待機系サーバーへのセッション維持情報（sticky 情報）をタイムアウトするまで使用し、ゆるやかに全体の接続をプライマリーサーバーに戻します。

更に、ヘルスチェック設定モードの *manual-failback* コマンドを使用することで、ヘルスチェックで DOWN 状態になったサーバーが ALIVE 状態に復帰した際も、負荷分散対象から外したままにしておくことが可能です。
詳細は「2.22.1サーバー復旧時動作」を参照してください。

⚠ 注意

複数のサーバーをバックアップサーバー、かつオーバーフローサーバーとして登録した場合に、*backup-policy multi* を設定した場合の待機系サーバーの昇格動作を説明します。以下の例では、

- 実サーバー1(Server1.80)が DOWN 状態になり、
  実サーバー2(Server2.80)が最大コネクションに達した場合、
  実サーバー3(Server3.80)がプライマリーサーバーに昇格しバックアップサーバーおよびオーバーフローサーバーとして動作します。
- 実サーバー1 および実サーバー2 が DOWN 状態になった場合、実サーバー3 および実サーバー4(Server4.80)がプライマリーサーバーに昇格しバックアップサーバーとして動作します。
- 実サーバー1 およびサーバー2 が最大コネクションに達した場合、実サーバー3 および実サーバー4 がプライマリーサーバーに昇格しオーバーフローサーバーとして動作します。

```
adm(config-virtual)# bind Server1.80 weight 1 maxconns 2000
adm(config-virtual)# bind Server2.80 weight 1 maxconns 2000
adm(config-virtual)# bind Server3.80 weight 1 backup overflow
adm(config-virtual)# bind Server4.80 weight 1 backup overflow
adm(config-virtual)# backup-policy multi failback orderly
```

2.19.18.2 IP スイッチングの設定

クライアントの IP アドレスを基に負荷分散先を決定するには、*match* コマンドで任意のネットワークセグメントに対してグループ ID を割り当てます。

```
adm(config-virtual)# match {<IP アドレス> <サブネットマスク> | < IP アドレス/マスク長>} group <グループ ID>
```

ID の割り当てが完了したら、*bind* コマンドで IP スイッチングのグループ ID を指定します。

```
adm(config-virtual)# bind <実サーバー IP アドレス.ポート番号> group <グループ ID> [ weight <重み> ] [ dsr ] [ backup ]
```

デフォルトグループの設定を行うことで、任意のスイッチングルール以外のアクセスに対する振り分け先グループを設定することが可能です。
デフォルトグループを設定するには以下の通りです。

```
adm(config-virtual)# 0.0.0.0/0 group <グループ ID>
```

以下の例では、クライアントの IP が 192.168.0.0/16 からのアクセスを、サーバー10.168.1.11 とサーバー10.168.1.12 に、その他のアクセスをサーバー10.168.1.10 に振り分けます。

```
adm(config-virtual)# match 0.0.0.0/0 group 1
adm(config-virtual)# match 192.168.0.0/16 group 2
adm(config-virtual)# bind 10.168.1.10.80 group 1
adm(config-virtual)# bind 10.168.1.11.80 group 2
adm(config-virtual)# bind 10.168.1.12.80 group 2
```

ポイント 一つの仮想サーバーID に対して IP スイッチングと URL スイッチングを同時に設定することはできません。

ポイント *match* コマンドを使用してスイッチング設定をした場合、グループ ID がない実サーバーは負荷分散対象になりません。

ポイント 範囲が重複するネットワークアドレスが複数登録された場合、ネットワーク範囲の一番狭い設定行から優先して評価されます。

⚠ 注意 仮想サーバーIP のアドレスファミリーと異なるアドレスファミリーのスイッチングルールを設定すると、IP アドレス負荷分散は正しく動作しません。

2.19.18.3 X-Forwarded-For スイッチングの設定

X-Forwarded-For ヘッダー情報に明示された IP アドレスを基に IP アドレススイッチングを行うことが可能です。これにより、X-Forwarded-For ヘッダーにクライアントの IP アドレス情報が埋め込まれてさえいれば、プロキシサーバーを経由するなどして IP アドレスが隠蔽されている場合においても、クライアント IP アドレスに基づく負荷分散先の決定が可能です。

X-Forwarded-For スイッチングを設定するには、IP スイッチングの設定をした後に、***xff-balancing***コマンドを実施します。(IP スイッチングの設定は「2.19.18.2 IP スイッチングの設定」を参照してください)

```
adm(config-virtual)# xff-balancing
```

HTTP リクエスト内に X-Forwarded-For ヘッダーが存在しない場合、IP ヘッダーの送信元アドレス情報を基に負荷分散先が決定されます。また、
X-Forwarded-For ヘッダーに複数の IP アドレス情報が明示されている場合は、先頭の IP アドレス情報を参照します。

ポイント

X-Forwarded-For スイッチング設定は L7 負荷分散機能の一部であるため、設定された仮想サーバーに対する全てのリクエストは L7 レベルで処理されます。その点で IP スイッチング設定とは異なります。

ポイント

一つの仮想サーバーID に対して X-Forwarded-For スイッチングと URL スイッチングを同時に設定することはできません。

⚠ 注意

仮想サーバーIP のアドレスファミリーと、X-Forwarded-For ヘッダーにセットされた IP アドレスのアドレスファミリーが一致しない場合、X-Forwarded-For スイッチングは正しく動作しません。

2.19.18.4 URL スイッチングの設定

URL や HTTP ヘッダーに含まれる文字列によって負荷分散を行う場合、初めに特権モードの *rule* コマンドでスイッチングルールを定義します。

```
adm(config)# rule <ルール名> { host | method | path | user-agent }
"<文字列>"
```

■*host*

HTTP リクエストヘッダーの Host ヘッダー値によるルールを定義します。

設定例

```
adm(config)# rule host_r1 host " www.seiko-sol.co.jp"
```

■*method*

HTTP リクエストヘッダーのメソッド種別によるルールを定義します。

設定例

```
adm(config)# rule method_r1 method "GET"
adm(config)# rule method_r2 method "!POST"
```

■*path*

HTTP リクエストヘッダーのリクエストパスによるルールを定義します。

設定例

```
adm(config)# rule path_r_1 path "/home.html"
adm(config)# rule path_r_2 path "/test_dir/*"
adm(config)# rule path_r_3 path "*.gif"
adm(config)# rule path_r_4 path "*cgi-bin*"
```

■*user-agent*

HTTP リクエストヘッダーの User-Agent ヘッダー値によるルールを定義します。

```
adm(config)# rule ua_r1 user-agent "!mozilla/4.*"
```

ポイント

指定する文字列は"(ダブルクオーテーション)で挟む必要があります。

文字列が HTTP メソッドの場合、大文字と小文字を区別します。また、文字列が HTTP メソッドの場合、ワイルドカード(*)を含んではなりません。

ワイルドカード(*)は以下のように使用します。

例） "string*"(前方一致)、"*string(後方一致) "、"*string*" (部分一致)

また、先頭に NOT (!) を付けるとその文字列以外を表します。

スイッチングルールを定義した後、仮想サーバー設定モードの *match* コマンドで任意のスイッチングルールに対してグループ ID を割り当てます

```
adm(config-virtual)# match { <ルール名> | default } group <グループ ID>
```

デフォルトグループの設定を行うことで、任意のスイッチングルール以外のアクセスに対する振り分け先グループを設定することが可能です。デフォルトグループを設定するには *default* を設定します。
ひとつの仮想サーバーに最大 31 個のルールを登録することができます。

グループ ID を定義したら、*bind* コマンドで URL スイッチングのグループ ID を指定します。

```
adm(config-virtual)# bind <実サーバー IP アドレス.ポート番号> group <グループ ID> weight <重み> ] [ backup ]
```

ポイント

リクエストがどのルールにも一致せず、かつデフォルトルールが割り当てられたサーバーがない場合、そのリクエストは破棄されます。

以下の例では、www.seiko-sol.co.jp へのリクエストを、サーバー 10.168.1.11 とサーバー10.168.1.12 に、その他のリクエストをサーバー 10.168.1.10 に振り分けます。

```
adm(config)# rule rule_seiko_sol host "www.seiko-sol.co.jp"
adm(config)# virtual 192.168.1.10.80.tcp
adm(config-virtual)# match default group 1
adm(config-virtual)# match rule_seiko_sol group 2
adm(config-virtual)# bind 10.168.1.10.80 group 1
adm(config-virtual)# bind 10.168.1.11.80 group 2
adm(config-virtual)# bind 10.168.1.12.80 group 2
```

複数のルールを組み合わせて別のルールを定義することも可能です。
最大 4 個までのルールを以下のように AND (&&) または OR (||) 演算子で組み合わせることで設定します。
OR で結ばれたルールはどれかひとつでもマッチすると真と判断されます。
AND で結ばれたルールは、全てがマッチした際に真と判断されます。

```
adm(config)# rule nested_rule "r1 && (r2 || r3 || r4)"
```

ポイント

ルールを AND (&&) や OR (||) 演算子で組み合わせる場合、演算子の前後はブランクが必要です。

ポイント

リクエスト受信時に、振り分け先候補として複数グループが該当する場合は、*match*コマンド実行順序（グループ ID を割り当てた順序）で、負荷分散対象のバインドグループが選定されます。

2.19.18.5 HTTP リダイレクションとエラーレスポンスの設定

特定のルールに合致した HTTP リクエストを本製品が別の URL にリダイレクトさせることができます。

設定するには、*rule*コマンドでルールを定義し、*match*コマンド(redirect)でリダイレクト先の URL を設定します。

```
adm(config-virtual)# match {<ルール名> | default} redirect {http|https}
 <ﾄﾞﾒｲﾝ> <URL ﾊﾟｽ> [<ﾎﾟｰﾄ番号>]
```

■*<ﾄﾞﾒｲﾝ>*

リダイレクト先のドメインを指定します。

ドメインにワイルドカード（＊）を指定すると、リダイレクト先のドメインは元のリクエストと同じになります。

ドメインは二重引用符(")で挟んで標記する必要があります。

また、ドメインに IPv6 アドレスを使用する場合は大括弧（[]）で囲う必要があります。

■*<URL ﾊﾟｽ>*

リダイレクト先のパスを指定します。

URL にワイルドカード（＊）を指定すると、リダイレクト先の URL パスは元のリクエストと同じになります。

パスは二重引用符(")で挟んで標記する必要があります。

■*<ﾎﾟｰﾄ番号>*

リダイレクト先スキームが http で 80 以外のポート、または https で 443 以外のポートにリダイレクトしたい場合に任意のポート番号を指定します。

以下では、仮想サーバーへのリクエストがルール r1 に合致する場合、リクエストを http://newdomain.com:8080/newlocation/index.html へリダイレクトします。

```
adm(config-virtual)# match r1 redirect http newdomain.com “newlocati
on/index.html” 8080
```

ドメインと URL パラメーターにワイルドカード(*)を指定すると、リダイレクト先のドメインと URL は元のリクエストと同じになります。
以下の設定例では、ルール r1 に合致した仮想サーバー宛ての HTTP リクエストを全て HTTPS へリダイレクトします。

```
adm(config-virtual)# match r1 redirect https * *
```

特定のルールに合致したHTTPリクエストに対し本製品が403エラーレスポンスを返すことができます。*rule*コマンドでルールを定義し、*match*コマンド(*forbid*)で 403 エラーレスポンスを返答する設定を行います。

```
adm(config-virtual)# match {<ルール名> | default} forbid
```

以下では、仮想サーバーへのリクエストがルール r2 に合致する場合、そのリクエストに対し 403 エラーレスポンスを返します。

```
adm(config-virtual)# match r2 forbid
```

以下の例のように、ある仮想サーバーに対し、ルールに応じて HTTP リダイレクション、403 エラーを同時に設定することができます。

```
adm(config)# virtual 192.168.1.10.80.tcp
adm(config-virtual)# bind 192.168.1.1.80 group 1
adm(config-virtual)# bind 192.168.2.100.80 group 1
adm(config-virtual)# match r2 redirect http "newdomain.com" "newurl.
html"
adm(config-virtual)# match r3 redirect https * *
adm(config-virtual)# match r4 forbid
```

*rule*コマンドの詳細は「2.19.18.4 URL スイッチングの設定」を参照してください。

ポイント

*match*コマンドを使用する場合、バインド設定には必ずグループ番号を割り当てる必要があります。上の設定例では、URL スイッチングルールによる負荷分散設定はありませんが、各バインド設定時にグループ番号 1 を割り当てています。

2.19.18.6 Location ヘッダーの書き換え

本製品の SSL アクセラレーション機能を使用すると、実サーバーが返す 300 番台のレスポンスのリダイレクト先が https ではなく http になってしまうことがあります。
この問題を回避するには *rule* コマンドで location ルールを定義し、*match* コマンド(redirect)で正しい URL を設定します。

初めに、*rule* コマンドでサーバーのリダイレクト応答に含まれる Location ヘッダーを置換するためのルールを定義します。

```
adm(config)# rule <ルール名> location {http | https} <ドメイン> <URL パス>
```

■*http | https*
ルールにマッチさせたいリダイレクト先のスキームを選択します。

■*ドメイン*
ルールにマッチさせたいリダイレクト先のドメインを指定します。
ドメインは二重引用符(")で挟んで標記する必要があります。

■*URL パス*
ルールにマッチさせたいリダイレクト先のパスを指定します。
URL パスは二重引用符(")で挟んで標記する必要があります。

ポイント

location ルールのドメインと URL は大文字と小文字を区別しません。文字列の前後にワイルドカード(*)を付けて、先頭、末尾または任意の部分を指定することができます。また、先頭に NOT (!) を付けるとその文字列以外を表します。ワイルドカード(*)だけの場合は任意の文字列を表します。

次に、仮想サーバー設定モードで、変換するドメイン、パスを設定します。
redirect オプションを指定して *match* コマンドを実施します。

```
adm(config-virtual)# match <ルール名> redirect {http|https} <ドメイン> <URL パス> [ポート番号]
```

■*ドメイン*
リダイレクト先を変更させたい場合は、任意のドメインを指定します。

ワイルドカード(*)を指定すると、リダイレクト先を書き換えません。
ドメインは二重引用符(")で挟んで標記する必要があります。

■*URL ﾊﾟｽ*

リダイレクト先のパスを変更させたい場合は、任意の URL パスを指定します。
ワイルドカード(*)を指定すると、リダイレクト先のパスを書き換えません。
パスは二重引用符(")で挟んで標記する必要があります。

■*ﾎﾟｰﾄ番号*

リダイレクト先スキームが http で 80 以外のポート、または https で 443 以外のポートにリダイレクトしたい場合に任意のポート番号を指定します。
省略するとポート番号の書き換えは行いません。

以下では、Location ヘッダーの値が http://www.seiko-sol.co.jp/bar/で始まる場合、https に書き換えます。

```
adm(config)# rule r1 location http "www.seiko-sol.co.jp" "/bar/*"
adm(config)# virtual 192.168.1.10.80.tcp
adm(config-virtual)# match r1 redirect https * *
adm(config-virtual)# bind 192.168.1.1.80 group 1
```

*rule*コマンドの詳細は「2.19.18.4 URL スイッチングの設定」、*redirect*オプションの詳細は「2.19.18.5 HTTP リダイレクションとエラーレスポンスの設定」を参照してください。

ポイント

*match*コマンドを使用する場合、バインド設定には必ずグループ番号を割り当てる必要があります。上の設定例では、URL スイッチングルールによる負荷分散設定はありませんが、バインド設定時にグループ番号 1 を割り当てています。

2.19.18.7 sorry コンテンツの設定

実サーバーの障害時や過負荷状況、またはメンテナンスなど、なんらかの理由で HTTP リクエストの振り分けが出来ない場合、サービスが提供できない旨の代替コンテンツを本製品から返信することが可能です。
本製品は、以下のいずれかの状況になると sorry コンテンツでの応答を行います。

- 仮想サーバーに実サーバーが1台もバインドされていない
- バインドされている全ての実サーバーが DOWN 状態になっている
- バインドされている全ての実サーバーが無効になっている
- バインドされている全ての実サーバーのコネクション数が最大コネクション数に達してしまっている

この機能を有効にするには、*import content* コマンドで代替コンテンツを本製品にインストールします。sorry コンテンツのインポートは「5.3.1.5sorry コンテンツのインポート」を参照してください。
インポートが完了したら、*bind* コマンドで仮想サーバーにコンテンツを割り当てます。

```
adm(config)# virtual <仮想ｻｰﾊﾞｰ ID>.<ﾎﾟｰﾄ>.<ﾌﾟﾛﾄｺﾙ>
adm(config-virtual)# bind content <ｺﾝﾃﾝﾂ名>
```

ポイント

代替コンテンツは HTML 形式のみサポートします。また、以下の制約があります。

■コンテンツ名
コンテンツ名は 16 文字以内の半角英数字または半角記号で、先頭は数字であってはいけません。また、使用可能な記号はハイフン(-)、アンダーバー(_)のみです。

■コンテンツサイズ
インポートするコンテンツサイズは 4500 バイト以内でなければなりません。

■コンテンツ内容
コンテンツ内に、画像ファイルなどへのリンクを含んではなりません。

コンテンツは、以下の例のようにコンテンツの文字コードを表す META タグと、ブラウザにキャッシュされるのを防ぐための META タグを HEAD 部に含めてください。

```
<HTML>
    <HEAD>
        <TITLE>OUT OF SERVICE</TITLE>
        <META http-equiv="Content-Type" content="text/html; charset=
shift_jis">
        <META http-equiv="Pragma" content="no-cache">
        <META http-equiv="Cache-Control" content="no-cache">
        <META http-equiv="Expires" content="0">
    </HEAD>
    <BODY>
        <H2>ただいまサーバーが混雑しています。しばらく経ってから再度
接続してください。</H2>
    </BODY>
</HTML>
```

インポートしたファイルはそのままで使用可能な状態ですが、フラッシュメモリーには保存されていません。保存するには ***write memory*** コマンドを実行してください。

```
adm(config)# write memory
```

ポイント

sorry コンテンツ機能は L7 負荷分散機能の一部です。sorry コンテンツをバインドすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

ポイント

バインド中の sorry コンテンツと同じ名前のコンテンツ名を指定して新規にファイルをインポートした場合、仮想サーバーから当該コンテンツを解除し、仮想サーバーへ割り当て直してください。

2.19.18.8 Fallback-url の設定

実サーバーの障害時や過負荷状況、またはメンテナンスなど、なんらかの理由で HTTP リクエストの振り分けが出来ない場合に 302 レスポンスを返し、任意の URL にリダイレクトさせることが可能です。

以下のいずれかの状況になると 302 応答を行います。

- ✓ 仮想サーバーに実サーバーが1台もバインドされていない
- ✓ バインドされている全ての実サーバーが無効になっている
- ✓ バインドされている全ての実サーバーが DOWN 状態、またはコネクション数が最大数に達した状態のいずれかの状態になっている

この機能を有効にするには、*fallback-url* コマンドでリダイレクト先の URL を設定します。

```
adm(config)# virtual <仮想ｻｰﾊﾞｰ ID>.<ﾎﾟｰﾄ>.<ﾌﾟﾛﾄｺﾙ>
adm(config-virtual)# fallback-url <URL>
```

ポイント

sorry コンテンツ機能と fallback-url 機能が同時に設定されている場合は、fallback-url の設定が優先されます。

ポイント

fallback-url 機能は L7 負荷分散機能の一部です。fallback-url の設定をすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

2.19.18.9 DSR（Direct Server Return）

仮想サーバーに関連付ける実サーバーを DSR モードで動作させた場合、実サーバーからの送信パケットはロードバランサーを経由せず直接クライアントコンピューターへ返送されます。このため、ロードバランサーの処理を軽減させることが可能となります。

実サーバーを DSR モードで動作させる場合、*bind* コマンドで *dsr* オプションを指定します。

```
adm(config-virtual)# bind <IP ｱﾄﾞﾚｽ.ﾎﾟｰﾄ> [group <ｸﾞﾙｰﾌﾟ ID>] [weight
<重み>] [dsr] [backup]
```

ポイント

DSR モードで使用する場合、実サーバーのループバックアドレスに仮想サーバーIP アドレスを登録する必要があります。
また、ループバックインターフェイスは ARP リクエストの送信、ARP リクエストへの応答を行わないよう設定する必要があります。
詳しくは「4.9.1DSR 実サーバーの設定例」を参照してください。

ポイント

DSR モードで使用する場合バインドする実サーバーに対して、ヘルスチェックを必ず設定してください。

2.19.18.10 FTP-DATA ポートの設定

FTP のアクティブモード接続時、FTP サーバーから接続される FTP データコネクトの発ポートを指定します。通常は指定不要です。

```
adm(config-virtual)# [no] ftp-data-port <port>
```

・指定がないとき（初期値）は、制御ポートから1を引いたポート番号を使用します。
・仮想サーバが FTP 設定ではないとき(ポートが 21 以外かつプロトコルが ftp 以外)、入力された値は意味を持ちません。

ftp-data-port を使用した設定例:

```
virtual 10.100.13.60.1021.ftp is
 predictor load
 timeout 30m
 sticky generic timeout 10m
 ftp-data-port 1234
 backup-policy multi failback orderly
 bind 10.101.1.60.1221 weight 1
 bind 10.101.1.61.1221 weight 1 backup
```

2.19.19 実サーバーIP アドレスの変換

実サーバーから開始されるコネクションの送信元 IP アドレスを任意の NAT プールアドレスに変換するには、リバース NAT の設定を行います。

変換に使用するアドレスは *nat-pool* コマンドで定義します。*nat-pool* コマンドの詳細は「2.19.11送信元アドレスの変換」を参照してください。

NAT プールアドレスとして定義したアドレスプールを変換に使用します。また、変換に使用するポート、プロトコルも同時に指定します。
ポート番号に 0 を指定すると、任意の未使用ポート番号を使用します。

```
adm(config)# reverse-nat <nat-pool 名>.<ﾎﾟｰﾄ>.{tcp|udp|ftp}
```

リバース NAT 設定モードで、変換対象のサーバーIP、送信元ポート、宛先ポートを登録します。ただし、指定した NAT プールアドレスと異なるアドレスファミリーのサーバ IP を登録しても動作しません。

```
adm(config-reverse-nat)# bind <IP ｱﾄﾞﾚｽ>.<送信元ﾎﾟｰﾄ> [dstport <宛先ﾎﾟｰﾄ>]
```

ポイント

宛先ポート番号を設定すると、そのポート宛のトラフィックのみアドレス変換します。

リバース NAT 設定では、送信元ポート番号を以下のルールで変換します。

reverse-nat コマンドで指定するポート番号（VP）	*bind* コマンドで指定するポート番号（RP）	変換ルール
任意の数値	任意の数値	送信元ポート番号が RP なら VP に変換
任意の数値	0	送信元ポート番号が 1024 未満ならそのままで、1024 以上なら VP に変換
0	任意の数値	送信元ポート番号が RP なら 1024 以上の未使用ポート番号に変換

0	0	送信元ポート番号が1024 未満ならそのままで、1024 以上なら1024 以上の未使用ポート番号に変換

以下の例ではサーバー192.168.1.10 から送信される TCP パケットの送信元 IP アドレスを 192.168.1.101 に、そして送信元ポート番号を任意の未使用ポート番号に変換します。ただし、上表の通り、サーバー発パケットの送信元ポート番号が 1024 未満である場合、ポート番号は変換せず IP アドレスのみを変換します。

```
  ① NAT プールの登録
adm(config)# nat-pool pool_addr
adm(config-natpool)# ip address 192.168.1.101
adm(config-natpool)# exit
  ② 変換に使用するアドレス、ポート、プロトコルの登録
adm(config)# reverse-nat pool_addr.0.tcp
  ③ 変換対象のサーバーアドレス、ポートの登録
adm(config-reverse-nat)# bind 192.168.1.10.0
```

ポイント

リバース NAT 設定モードの *bind* コマンドで設定したサーバーのポート番号が 0 ではなく、かつそのサーバーが実サーバーとして定義されているサーバーに対して、ポート番号、プロトコル含めて合致する場合、サーバーから発信されるコネクションもそのサーバーのコネクション数にカウントされるため、負荷分散や最大コネクション数に影響します。

リバース NAT セッションのアイドルタイムアウトを設定するには *timeout* コマンドを使用します。

```
adm(config-reverse-nat)# timeout <日時分秒(dhms)>
```

enable コマンドを使用することで、リバース NAT 設定の有効/無効状態を変更することができます。

```
adm(config-reverse-nat)#{enable | no enable}
```

特権モードの *enable* コマンドでも同様にリバース NAT 設定の有効/無効状態を変更することができます。

```
adm(config)# enable <nat-pool 名>.<ﾎﾟｰﾄ>.{tcp|udp|ftp}
```

```
adm(config)# no enable <nat-pool 名>.<ﾎﾟｰﾄ>.{tcp|udp|ftp}
```

show nat-pool コマンドで NAT プールアドレスの使用状況を統計情報として表示させることができます。
詳しくは「SX-3990_3950_3945_3940_3920 コマンドリファレンス」（別紙）を参照してください。

2.19.20 リバース NAT へのルーティングテーブルの設定

リバース NAT で使用するルーティングテーブルのルート ID を設定できます。

リバース NAT で使用するルート ID を設定するには *route-id* コマンドを実行します。ルート ID が設定されている場合は、リバース NAT の対象となるパケットがリバース NAT に設定されたルート ID と同一の ID を持つルーティングテーブルに従います。

ルート ID を設定しない場合はルート ID 0 が使用されます。
削除するには no を使用するか、ルート ID 0 を指定します。

```
adm(config-reverse-nat)# route-id <num>
adm(config-reverse-nat)# no route-id
```

設定できるルート ID の範囲は 0 から 15 です。

ポイント

仮想サーバー登録を行っていない仮想 IP（VLAN 内の *ip virtual-address* コマンドで設定されただけの IP アドレス）を NAT プールアドレスとして登録しても、正しく動作しません。
使用する仮想 IP を用いて仮想サーバーを登録し、*enable* コマンドで有効にする必要があります。この仮想サーバーは疑似的なサーバーとして登録するため、ID で使用するポート番号、プロトコルはどんな値でも問題ありません。

ポイント

ワンアーム構成の場合には実サーバーIP アドレスの変換は動作しません。
インライン構成の場合にのみ利用可能です。

2.19.21 NAT ログ情報の送信

本製品の負荷分散機能によって NAT 変換された IP アドレスのログを外部の syslog サーバーへ送信することが可能です。

```
netwiser(config)# nat-log <IP ｱﾄﾞﾚｽ> <ﾌｧｼﾘﾃｨｰ.ﾚﾍﾞﾙ>
```

以下の形式でメッセージを生成します。形式を変更することはできません。

<日時分> <ﾎｽﾄ名> PCB CREATED: <ﾌﾟﾛﾄｺﾙ> <送信元 IP>.<ﾎﾟｰﾄ> -> <仮想サーバーIP>.< ﾎﾟｰﾄ> -> <仮想サーバーIP>.< 送信元ﾎﾟｰﾄ> -> <実サーバーIP>.<ﾎﾟｰﾄ>

以下に実際に送出されるメッセージの例を示します。

```
Sep  2 16:56:24 netwiser PCB CREATED: tcp 10.208.11.146.49278 ->
10.208.10.95.80 -> 10.208.10.95.1025 -> 10.208.11.145.80
```

ポイント

本設定は *logging* コマンドの設定状態と関連していません。また、生成されたログは本製品内部の syslog ファイルには残りません。

2.20 SSL アクセラレーション設定

SSL による暗号通信を復号化し各サーバーに負荷分散することで、サーバーの SSL 通信による処理負荷を軽減させます。
本章では SSL アクセラレーションに関する設定方法を例とともに記します。

2.20.1 SSL アクセラレーション機能の仕様

本製品で対応する公開鍵方式、SSL バージョン、暗号スイート、証明書形式について、以下に明記します。

■対応する暗号スイート

暗号スイート	SSL 3.0	TLS 1.0	TLS 1.2	DTLS 1.0	DTLS 1.2
DES-CBC-SHA	○	○	×	○	×
DES-CBC3-SHA	○	○	○	○	○
AES128-SHA	○	○	○	○	○
AES256-SHA	○	○	○	○	○
DHE-RSA-AES128-SHA	×	×	○	×	○
DHE-RSA-AES256-SHA	×	×	○	×	○
AES128-SHA256	×	×	○	×	○
AES256-SHA256	×	×	○	×	○
DHE-RSA-AES128-SHA256	×	×	○	×	○
DHE-RSA-AES256-SHA256	×	×	○	×	○
AES128-GCM-SHA256	×	×	○	×	×
AES256-GCM-SHA384	×	×	○	×	×
DHE-RSA-AES128-GCM-SHA256	×	×	○	×	×
DHE-RSA-AES256-GCM-SHA384	×	×	○	×	×
ECDHE-RSA-AES256-GCM-SHA384	×	×	○	×	×
ECDHE-ECDSA-AES256-GCM-SHA384	×	×	○	×	×
ECDHE-RSA-AES256-SHA384	×	×	○	×	○
ECDHE-ECDSA-AES256-SHA384	×	×	○	×	○
ECDHE-RSA-AES256-SHA	×	×	○	×	○
ECDHE-ECDSA-AES256-SHA	×	×	○	×	○
ECDHE-RSA-AES128-GCM-SHA256	×	×	○	×	×

ECDHE-ECDSA-AES128-GCM-SHA256	×	×	○	×	×
ECDHE-RSA-AES128-SHA	×	×	○	×	○
ECDHE-RSA-AES128-SHA256	×	×	○	×	○
ECDHE-ECDSA-AES128-SHA	×	×	○	×	○
ECDHE-ECDSA-AES128-SHA256	×	×	○	×	○

※ SX-3920 では ECDHE 系の暗号スイートに対応していません

※ DTLS1.2 では、クライアント認証が有効の時だけ "DHE-RSA-AES128-SHA"、"DHE-RSA-AES256-SHA"をサポートします。クライアント認証が無効の時は、これらの暗号スイートは SSL ネゴシエーション時に選択されません。

■対応する証明書形式

本製品への鍵・証明書のインポート/エクスポートでは以下の形式をサポートします。

- DER Encoded Binary X.509（鍵・証明書）
- Base64 Encoded X.509（鍵・証明書）
- PKCS#12（鍵＋証明書）
- Base64 Encoded PKCS#10（署名要求のエクスポート）

2.20.2 SSL ポリシーの作成

SSL アクセラレーションの設定を行うにはまず SSL 関連ファイルを管理するための SSL ポリシーを作成する必要があります。

SSL ポリシーは特権モードの *ssl* コマンドで作成します。

```
netwiser(config)# ssl <ﾎﾟﾘｼｰ名> [test]
netwiser(config-ssl)#
```

test オプションを指定して SSL ポリシーを作成すると、テスト用の証明書、秘密鍵、中間証明書がインポートされた状態の SSL ポリシーを作成することができます。

```
netwiser(config)# ssl test_cert test
```

ポイント テスト用証明書は正規の認証局が発行した証明書ではありません。SSL アクセラレーション機能の動作テスト以外の目的には使用しないでください。

⚠ 注意 テスト証明書では ECDHE-ECDSA 系の暗号スイートを利用することは出来ません。

⚠ 注意 SSL 証明書自動更新のプレフィックスにマッチする SSL ポリシーの追加、変更、削除は、証明書自動更新に影響が出る可能性があるため警告が出ます。

2.20.3 電子証明書と鍵のインポート

Web サーバーが OpenSSL を用いた Apache, Apache-SSL, stronghold の場合は既存のサーバーの鍵と電子証明書を取得する方法が公開されていますので、サーバー情報を取得し本製品にインポートして使用します。
鍵ファイル、電子証明書ファイル、中間証明書ファイルの取得は各サーバー用のソフトウェアマニュアルを参照してください。
ファイルの転送をするためにはネットワークを使用して本製品に tftp で put するか、zmodem で送信する必要があります。
署名アルゴリズム SHA-1,MD5,SHA-2 ファミリー(SHA224, SHA256, SHA384, SHA512)で署名されたサーバー電子証明書のインポートが可能です。

Web サーバーから鍵ファイル、電子証明書ファイル、中間証明書を取得しメンテナンス用パソコンに保存します。

本製品への電子証明書と秘密鍵のインポートは *import ssl* コマンドを使用します。また、インポートが完了したら *write memory* コマンドで情報を保存してください。

```
netwiser(config)# import ssl <ポリシー名> {cert | chain | client | key |pkcs12} [tftp | zmodem ]
```

証明書や鍵のインポート時には、SSL ポリシーが作成されている必要があります。SSL ポリシーの作成は「2.20.2SSL ポリシーの作成」を参照してください。

■*cert*
サーバー証明書をインポートします。

■*chain*
中間証明書をインポートします。
2枚までインポートすることが可能です。

■*client*

クライアント認証で使用する CA 局の証明書をインポートします。
2枚までインポートすることが可能です。

■*key*

サーバー証明書に対応する秘密鍵をインポートします。
RSA 秘密鍵は 1024bit、2048bit、4096bit に対応します。
ECC 秘密鍵は EC 名前付き曲線 secp256r1、secp384r1 に対応します。

■*pkcs12*

サーバー証明書、中間 CA 局証明書、秘密鍵をまとめて PKCS#12 形式で投入します。

■*tftp*

tftp によってファイルを投入します。
省略した場合は tftp 動作となります

■*zmodem*

zmodem によってファイルを投入します。

中間証明書や、クライアント認証で使用する CA 証明書は多段インポートが可能です。
多段インポートをするには、証明書が既にインポートされている任意の SSL ポリシーに対して再度 *import* コマンドを実施します。この時、インポート時に表示される対話形式の設問に'y'を入力すると、新規ファイルがインポート済みファイルにチェーンされます。

```
Do you want to add another component for the chain? Are you sure ?
[y/n]: y
```

ポイント

証明書を多段インポートする場合、必ず以下の順序で証明書のインポートを行ってください。

- 一段目の証明書: サーバー証明書（あるいはクライアント証明書）を署名する証明書
- 二段目の証明書: 一段目の証明書を署名する証明書

既にインポートされている証明書ファイルに対してデータ内容の上書きを行いたい場合、インポート時に表示される対話形式の設問に'n'を入力するとインポ

ート済みファイルが新規ファイルで上書きされます。

```
Do you want to add another component for the chain? Are you sure ?
[y/n]: n
```

ポイント

二段にチェーンされた中間証明書（あるいはクライアント CA 証明書）を 1 ファイルにまとめてインポートすることも可能です
ただし、以下の例に示す通り、PEM 形式の証明書であり、かつ一段目の証明書の終端ラベル（"----- END <label> -----"）と二段目の証明書の開始ラベル（"----- BEGIN <label> -----"）が改行コードで繋がれている必要があります。

```
-----BEGIN CERTIFICATE-----

<証明書データ>

-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

<証明書データ>

-----END CERTIFICATE-----
```

show ssl コマンドで、証明書や秘密鍵のインポート状態と SSL アクセラレーションの統計情報を参照することができます。詳しくは
「SX-3990_3950_3945_3940_3920 コマンドリファレンス」（別紙）を参照してください。

ポイント

冗長構成で、かつ冗長相手とコマンドの同期が可能な状態であれば、自機器にインポートした証明書や鍵はピア側の機器にコピーされます。

```
①秘密鍵のインポート
netwiser(config)# import ssl netwiser_ssl key
Ready to TFTP receive.
Press 'q[ENTER]' to cancel: .

Transfer is complete.
Enter Import Password:
②サーバー証明書のインポート
netwiser(config)# import ssl netwiser_ssl cert
Ready to TFTP receive.
Press 'q[ENTER]' to cancel: .
```

```
Transfer is complete.
③中間証明書のインポート
netwiser(config)# import ssl netwiser_ssl chain zmodem
Ready to ZMODEM receive.
Press '^X' several time to cancel: **B0100000063f694

Transfer is complete.
④中間証明書のインポート（2段目）
netwiser(config)# import ssl netwiser_ssl chain zmodem
There's already a certificate chain.
Do you want to add another component for the chain? Are you sure ?
[y/n]: y
Ready to ZMODEM receive.
Press '^X' several time to cancel: **B0100000063f694

Transfer is complete.
⑤CA証明書のインポート
netwiser(config)# import ssl netwiser_ssl client zmodem
Ready to ZMODEM receive.
Press '^X' several time to cancel: **B0100000063f694

Transfer is complete.
⑥CA証明書のインポート（上書き）
netwiser(config)# import ssl netwiser_ssl client zmodem
There's already a certificate chain.
Do you want to add another component for the chain? Are you sure ?
[y/n]: n
Ready to ZMODEM receive.
Press '^X' several time to cancel: **B0100000063f694

Transfer is complete.
netwiser(config)# write memory
```

インポートした鍵や証明書ファイルを取り出すには *export ssl* コマンドを使用します。詳細は「5.3.2.4SSL 関連ファイルのエクスポート」を参照してください。

ポイント

import config によって設定ファイルのインポートを行った後で SSL 関連ファイルのインポートを行った場合、以下のメッセージが出力されることがあります。

```
ERROR: <0307E> Invalid ssl directory structure. Please reconstruct t
he setting of ssl.
```

これは、インポートしたファイルと自機器の SSL 設定の間で食い違いが発生しているためです。*no ssl* コマンドで全ての SSL 設定を削除し、SSL ポリシーの登

録からやり直すか、*import all*コマンドで全ての設定情報をインポートしてください。

2.20.4 電子署名要求の作成と取り出し

本製品で電子証明書署名要求（CSR）を作成し、認証局で認証をしてもらい、その電子証明書を利用します。
このオペレーションでは証明書要求と秘密鍵が作成されます。

下記の例では SSL ポリシー"TEST1"に csr と秘密鍵の作成を行います。
入力項目は適切な情報を入力してください。
また、作成後は *write memory*コマンドで情報を保存してください。

*csr*コマンドを実行し、RSA 証明書用の CSR を作成するか、EC 証明書用の CSR を作成するかを選択した後に、表示に従い署名要求内容を入力していきます。

```
netwiser(config)# ssl TEST1
netwiser(config-ssl)# csr
use the EC parameter? (y/n) [n]:
```

RSA 証明書を利用する場合

```
use the EC parameter? (y/n) [n]: n
key length (1024/2048/4096) [2048]: 2048  # 任意の鍵長を選択
2048 semi-random bytes loaded
Generating RSA private key, 2048 bit long modulus
.............+++
.............+++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorpor
ated
into your certificate request.
What you are about to enter is what is called a Distinguished Name o
r a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:jp
State or Province Name (full name) [Some-State]:chiba
```

```
Locality Name (eg, city) []:makuhari
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SEIKO SOL
UTIONS INC
Organizational Unit Name (eg, section) []:development
Common Name (e.g. server FQDN or YOUR name) []:www.seiko-sol.co.jp
Email Address []:test@seiko-sol.co.jp

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:seiko
An optional company name []:seiko-sol

CSR successfully created.
You can retrieve it by typing 'export ssl TEST1 csr'.
netwiser(config-ssl)# write memory
netwiser(config-ssl)# show ssl
policy            cert    chain   client  key
TEST1                                     2048


total handshake                 = 0
total RSA decrypt               = 0
total SSL connections           = 0
current SSL connections         = 0
current session                 = 0
max SSL connections             = 0
max SSL sessions                = 0
--More--(byte 454)
```

ECC 証明書を利用する場合

```
use the EC parameter? (y/n) [n]: y
Please select either secp256r1(=256) or secp384r1(=384).
elliptic curve (256/384) [256]: 256  # 任意の曲線を選択
using curve name prime256v1 instead of secp256r1
～ 以下、RSA 証明書用 CSR 作成時と同様 ～
```

ポイント

作成した秘密鍵、署名要求書は必ず保管しておいてください。

本製品から署名要求を取りだすためには、*export* コマンドを使用します。
エクスポートには tftp または zmodem を使用します。ただし、省略された場合 tftp でのエクスポート動作なります。

```
netwiser> export ssl <ﾎﾟﾘｼｰ名> csr [tftp | zmodem]
```

```
①tftp で export
netwiser> export ssl TEST1 csr
Ready to TFTP send 'TEST1.csr'.
Press 'q[ENTER]' to cancel: .
Transfer is completed.
②zmodem で export
netwiser> export ssl TEST1 csr zmodem
Ready to ZMODEM send 'TEST1.csr'.
**B00000000000000l time to cancel: rz
Transfer is completed.
```

ポイント

認証局から発行された証明書は、事前に作成しておいた SSL ポリシーに対してインポートしてください。
また、必要に応じて中間証明書をインポートしてください。

⚠ 注意

Netwiser で CSR を行った場合、秘密鍵は Netwiser 以外の機器にインポートすることは出来ません。

2.20.5 仮想サーバーへの割り当て

必要な証明書や鍵ファイルをインポートしたら、任意の仮想サーバーに対して SSL ポリシーを割り当てます。
仮想サーバーに SSL ポリシーを割り当てるには、仮想サーバー設定モードに遷移して *ssl* コマンドを実施します。
ただし、仮想サーバーに SSL ポリシーを割り当てるためには、該当の SSL ポリシーに秘密鍵、サーバー証明書の両方がインポートされている必要があります。

```
netwiser(config-virtual)# ssl <ポリシー名> [default]
```

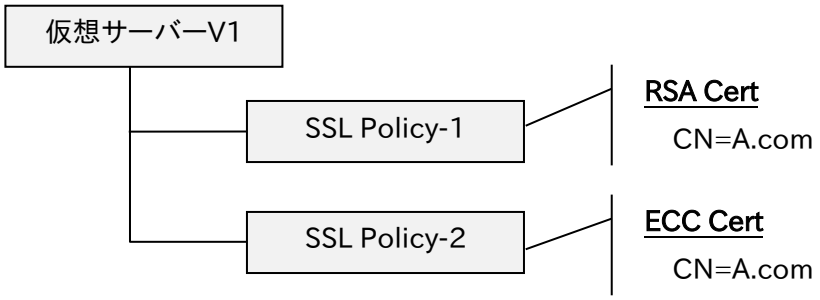
SSL ポリシーの作成は「2.20.2SSL ポリシーの作成」を参照してください。
また、証明書、秘密鍵のインポートは「2.20.3電子証明書と鍵のインポート」を参照してください。

■SNI（Server Name Indication）
本製品は SSL/TLS の拡張仕様の一つである SNI に対応しています。
仮想サーバーに対して複数の証明書を割り当てた場合や、複数の CN（Common Name）がセットされている証明書（拡張領域"Subject Alternative Names"を利用した証明書）を割り当てた場合、SNI ヘッダの内容によって証明書を使い分けることが可能になります。
最初に割り当てられた証明書が SNI デフォルト証明書として動作します。
デフォルト証明書を変更するには *default* オプションが指定します。
default オプションが指定された証明書がデフォルト証明書として動作します。

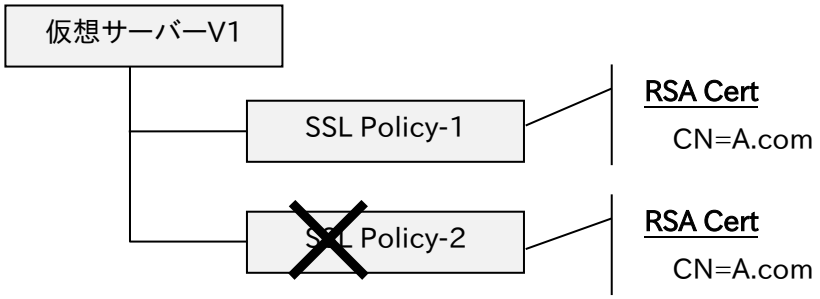
```
netwiser(config-virtual)# ssl <ポリシー名> default
```

ポイント

単一の仮想サーバーにおいて RSA/ECDSA 両方の署名方式に対応させたい場合、同じ CN（Common Name）の RSA 証明書と ECC 証明書を別々の SSL ポリシーにインポートし、それぞれを同一の仮想サーバーにバインドする必要があります。



ただし、同じ署名方式（RSA 証明書同士、あるいは ECC 証明書同士）で、かつ同じ CN（Common Name）であるサーバー証明書を同一仮想サーバーに対して複数バインドすると、正常に動作しなくなることがあるため、このような操作はしないでください。



もし、このような操作を行ってしまった場合は、該当の仮想サーバーにバインドされている SSL ポリシーを全てアンバインドしてからバインドし直してください。

ポイント

SNI に対応しないアクセスがあった場合は、SNI デフォルト証明書がサーバー証明書として使用されます。

ポイント

仮想サーバーに割り当てられた SSL ポリシーは、特権モード上で *no ssl* コマンドを実施しても削除することはできません。
仮想サーバー設定モードの *no ssl* コマンドで仮想サーバーからの割り当てを解除してから、特権モード上で SSL ポリシーの削除を行ってください。

ポイント

クライアント証明書がインポートされている SSL ポリシーは、仮想サーバー毎に 1 件のみ割り当て可能です。

ポイント

仮想サーバーに割り当てられた状態のままでも、SSL ポリシーに秘密鍵や証明

書をインポートし更新することが可能です。ただし、秘密鍵とサーバー証明書を更新する場合、「秘密鍵」→「サーバー証明書」の順で更新してください。
正しい順序で更新しなかった場合は、仮想サーバー設定モードの *no ssl* コマンドで、SSL ポリシーの割り当てを一旦解除してから、再度 *ssl* コマンドで割り当てを行ってください。

ポイント

SSL サーバー証明書の拡張領域"Subject Alternative Names"で指定する CN（Common Name）にはワイルドカード（＊）を使用することが可能です。
ただし、ワイルドカードは先頭のサブドメインのみが対象となります。

⚠ 注意

仮想サーバーに割り当てられている状態の SSL ポリシーに対して秘密鍵や証明書の更新を行う場合、証明書と秘密鍵の更新の間（1～数秒程度）その仮想サーバーに割り当てられた全ての SSL ポリシーに対して新規に SSL セッションが作れない状態になりますので注意してください。

show ssl コマンドで、証明書や秘密鍵のインポート状態と SSL アクセラレーション処理の統計情報を参照することができます。詳しくは
「SX-3990_3950_3945_3940_3920 コマンドリファレンス」（別紙）を参照してください。

2.20.6 SSL セッションタイムアウト

SSL セッション情報の保持時間はデフォルトで 5 分です。
値を変更するには *ssl session-timeout* コマンドを実行します。

```
netwiser(config)# ssl session-timeout <タイムアウト値>
```

2.20.7 クライアント認証

クライアント認証を有効にするには、クライアント証明書を発行した CA 局の自己署名証明書（self-signed certificate）を本製品にインストールする必要があります。更に、自己署名証明書がインストールされたSSLポリシーを仮想サーバーに割り当てます。
クライアント認証のためにインポートする自己署名証明書に、ECC 証明書を利用することはできません。

本製品に証明書をインストールするには *import ssl* コマンドを実施します。
import ssl コマンドの詳細は「2.20.3電子証明書と鍵のインポート」を参照してください。

SSL ポリシーを仮想サーバーへ割り当てるには仮想サーバー設定モードで *ssl* コマンドを実施します。詳細は「2.20.5仮想サーバーへの割り当て」を参照してください。

ポイント

SNI 利用時にクライアント認証を行う SSL ポリシーを割り当てた場合、その他すべての SSL ポリシーでクライアント認証が行われます。
また、仮想サーバーID に対して、クライアント証明書がインポートされている SSL ポリシーを複数件割り当てることはできません。

2.20.7.1 証明書失効時リスト(CRL)の更新

有効期限前に失効したクライアント証明書のチェックは CA 局が発行する証明書失効リスト(CRL)を用いて行います。本製品が CRL を使用してクライアント証明書の期限前失効をチェックする必要がある場合は、CRL の配布元 URL を設定します。CRL は PEM 形式、DER 形式の何れでもかまいません。

以下の例では 192.168.1.251:8009 から MyCRL.der ファイルを 10 分毎にダウンロードします。

```
netwiser(config)# ssl ssl_2048_app1
netwiser(config-ssl)# crl http://192.168.1.251:8009/MyCRL.der interv
al 10m
```

ポイント

URL に IPv6 アドレスを使用する場合は、以下のように[ ]で囲んでください。
"http://[2001:db8::c0:a8:1:fb]:8009/MyCRL.der"

プロキシサーバー経由で CRL の配布元 URL へアクセスする場合、本製品にプロキシサーバーの登録をする必要があります。
プロキシサーバーを登録するには特権モードで *proxy* コマンドを実行します。

```
netwiser(config)# proxy <IP ｱﾄﾞﾚｽ> <ﾎﾟｰﾄ番号>
```

2.20.7.2 クライアント証明書の挿入

クライアント認証を使用すると、本製品で認証を行った後 HTTP リクエスト（GET、POST）に以下のデータを追加してサーバーへ送ることができます。

- base64 形式、または pem 形式に変換されたクライアント証明書
- base64 形式に変換された SSL セッション ID

ポイント

SSL セッション ID はクライアント認証なしであっても、設定することが可能です。

クライアント証明書は SSL ハンドシェーク終了後、最初の HTTP リクエストにセットされます。SSL セッション ID は同一の TCP コネクションで複数の GET、POST メソッドが発生する場合にもセットされます。

クライアント証明書と SSL セッション ID はデフォルトでは送信されません。クライアント証明書と SSL セッション ID をサーバーへ送る必要がある場合は、HTTP ヘッダーに追加されるタグ名を設定します。設定を行うには、仮想サーバー設定モードで *certheader* コマンドを実施します。

```
netwiser(config-virtual)# certheader <ﾍｯﾀﾞｰ名> [base64 | pem]
```

変換形式を省略した場合、base64 形式が選択されます。

以下の例では"client-cert"をタグ名として使用します。

```
netwiser(config-virtual)# certheader client-cert
```

sidheader コマンドを使用して SSL セッション ID のタグ名を設定します。以下の例では"ssl-session-id"をタグ名として使用します。

```
netwiser(config-virtual)# sidheader ssl-session-id
```

2.20.7.3 クライアント認証失敗時の動作

クライアント証明書が提示されない、または証明書の期限切れ、失効などの理由により認証に失敗した場合の動作を設定することが出来ます。
本製品のデフォルト設定では、SSL alert メッセージを送信しコネクションを終了します。
デフォルト以外の処理を選択するには *authfail* コマンドを使用します。

```
nentwiser(config-virtual)# authfail {alert | forbid | redirect <URL>}
```

■*alert*
alert を送信し SSL ハンドシェークを強制終了します。

■*forbid*
403 Forbidden レスポンスを返します。

■*redirect*
302 レスポンスを返し*<URL>*で指定されたページへリダイレクトします。

ポイント

CRL の取得が成功するまで、証明書の期限切れ、失効に関してはチェックされません。

クライアント認証が失敗したときでも通常の SSL アクセラレーションを行うには *no* を指定します。

```
nentwiser(config-virtual)# no authfail
```

2.20.8 使用する暗号スイートの選択

SSL アクセラレーションで使用する暗号スイートを指定できます。

デフォルト設定は、以下の暗号スイートの許可/拒否をしています。

許可する暗号スイート
DES-CBC3-SHA
AES128-SHA
AES128-SHA256
AES256-SHA
AES256-SHA256
AES128-GCM-SHA256
AES256-GCM-SHA384
DHE-AES128-SHA
DHE-AES128-SHA256
DHE-AES128-GCM-SHA256
DHE-AES256-SHA
DHE-AES256-SHA256
DHE-AES256-GCM-SHA384
拒否する暗号スイート
DES-CBC-SHA
ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES128-SHA256
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-SHA
ECDHE-RSA-AES256-SHA384
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES128-SHA
ECDHE-ECDSA-AES128-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-SHA
ECDHE-ECDSA-AES256-SHA384
ECDHE-ECDSA-AES256-GCM-SHA384

使用する暗号スイートの選択を行うには、仮想サーバー設定モードで

cipher-suite コマンドを実施します。

ただし、SX-3920 では、ECDHE 系の暗号スイートをサポートしていないため、

許可する暗号スイートに含めることはできません。

```
netwiser(config-virtual)# cipher-suite <暗号ｽｲｰﾄ文字列>
```

暗号スイート文字列は以下のようにカンマ(,)で区切ります。区切り文字に空白

は使用しないでください。

```
netwiser(config-virtual)# cipher-suite DES-CBC3-SHA,AES128-SHA
```

該当の仮想サーバーは指定された暗号スイート内のいずれかを SSL アクセラレーション時に使用します。

暗号スイート文字列には、抽象表記を使用することが可能です。
以下に、使用可能な抽象表現と対応する暗号スイート文字列を示します。

抽象表記	対応する暗号スイート
DES	DES-CBC-SHA DES-CBC3-SHA
DES3	DES-CBC3-SHA
AES	AES128-SHA AES128-SHA256 AES256-SHA AES256-SHA256 AES128-GCM-SHA256 AES256-GCM-SHA384 DHE-AES128-SHA DHE-AES128-SHA256 DHE-AES128-GCM-SHA256 DHE-AES256-SHA DHE-AES256-SHA256 DHE-AES256-GCM-SHA384 ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES256-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384

AES128	AES128-SHA AES128-SHA256 AES128-GCM-SHA256 DHE-AES128-SHA DHE-AES128-SHA256 DHE-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256
AES256	AES256-SHA AES256-SHA256 AES256-GCM-SHA384 DHE-AES256-SHA DHE-AES256-SHA256 DHE-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES256-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384
SHA	DES-CBC-SHA DES-CBC3-SHA AES128-SHA AES128-SHA256 AES256-SHA AES256-SHA256 AES128-GCM-SHA256 AES256-GCM-SHA384 DHE-AES128-SHA DHE-AES256-SHA DHE-AES128-SHA256 DHE-AES256-SHA256

	DHE-AES128-GCM-SHA256 DHE-AES256-GCM-SHA384 ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES256-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384
SHA256	AES128-SHA256 AES256-SHA256 AES128-GCM-SHA256 DHE-AES128-SHA256 DHE-AES256-SHA256 DHE-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256
SHA384	AES256-GCM-SHA384 DHE-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384
DHE	DHE-AES128-SHA DHE-AES256-SHA DHE-AES128-SHA256 DHE-AES256-SHA256 DHE-AES128-GCM-SHA256 DHE-AES256-GCM-SHA384

GCM	AES128-GCM-SHA256 AES256-GCM-SHA384 DHE-AES128-GCM-SHA256 DHE-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384
CBC	DES-CBC-SHA DES-CBC3-SHA AES128-SHA AES128-SHA256 AES256-SHA AES256-SHA256 DHE-AES128-SHA DHE-AES256-SHA DHE-AES128-SHA256 DHE-AES256-SHA256 ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES256-SHA384
ECDHE	ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-SHA

	ECDHE-ECDSA-AES256-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384
ECDSA	ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES256-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384
ALL	全ての暗号スイート

抽象表記をカンマ(,)でつなげることが可能です。

```
netwiser(config-virtual)# cipher-suite SHA384,DHE,DES-CBC-SHA
```

デフォルト設定に戻すには *no* を指定します。

```
netwiser(config-virtual)# no cipher-suite
```

2.20.9 SSL3.0 の有効化

SSL 3.0 はデフォルトで無効化されています。SSL 3.0 での SSL アクセラレーションを有効化するためには *sslv3-enable* コマンドを使用します。

```
netwiser(config)# sslv3-enable
```

⚠ 注意

SSL 3.0 を有効化すると脆弱性 CVE-2014-3566 に該当しますので、設定変更の際は注意してください。

2.20.10 SSL 証明書自動更新

SSL 証明書自動更新を有効化するためには ***cert-update*** コマンドを使用します。

cert-update は既に使用中の ssl ポリシーにある証明書に対して更新していきます。例として ssl1 という名称の ssl ポリシーがあるものとします。

```
netwiser(config)# cert-update ssl1
```

ここで、 ssl1 の部分は証明書自動更新ではプレフィックス(prefix)と表現されます。

自動更新の対象は *prefix* または *prefix*_XXX にマッチする SSL ポリシーです。

※XXX は任意の数値 ※*prefix* のみは 0 扱い

以降この XXX の値をインデックス値と称します。

インデックス値が一番大きいものが最新の SSL ポリシーと判断されます。

cert-update は有効期限により CSR を作成する CSR ありモードと

ダウンロード完了後直ちに次のダウンロードの準備を始める CSR なしモードがあります。

csr-update コマンドが 0 以外のとき CSR ありモードとなります。

```
netwiser(config-cert-update)# csr-update 7
```

⚠ 注意

cert-update はプレフィックスにマッチする SSL ポリシーのすべてが自動更新の対象となります。※今回の例では、ssl1_1 や ssl1_199 などが該当します。

対象となる SSL ポリシーは 3 世代以前の(インデックス値が小さい)物は自動的に削除されますので注意してください。

Prefix にマッチしてしまう SSL ポリシーが既にあり、自動更新の対象外にしたい場合は、違う名前の SSL ポリシーを作成して、各証明書をインポートし直したうえで仮想サーバーの SSL 登録も切り替える必要があります。

ポイント

プレフィックスにマッチする SSL ポリシーがない状態から証明書自動更新を開始することもできます。この場合、仮想サーバーへの割り当てがないままとなりますので、証明書のダウンロードが完了した時点で仮想サーバーへ割り当てる必要があります。

2.20.10.1 CSR ありモード時の動作

証明書の期限切れまで、csr-update で指定した日数を切るとインデックス値+1 の新しい SSL ポリシーを作成し、そこに CSR コマンドで設定した CSR と秘密鍵が作成されます。country と fqdn は設定が必須です。
keylen は通常現在と同じものを設定します。
※現在の keylen(鍵長)は show ssl で見ることができます。
※fqdn はドメイン名を指定します。

```
netwiser(config-cert-update)# csr country JP
netwiser(config-cert-update)# csr fqdn "xxxx.zzzz.jp"
netwiser(config-cert-update)# csr keylen 2048
```

ポイント 作成した秘密鍵は適宜 export して保管しておいてください。

⚠ 注意 Netwiser で CSR を行った場合、秘密鍵は Netwiser 以外の機器にインポートすることは出来ません。
全ての SSL 証明書自動更新の設定が終わって **enable コマンドを発行するまで、自動更新は開始されません**。

2.20.10.2 CSR アップロード

CSR が作成されると put-url コマンドで指定したサーバーにアップロードされます。
put した CSR ファイルをサーバーのローカルストレージに保存するためのスクリプトを指定してください。

```
netwiser(config-cert-update)# put-url https://xxxx.yyyy.jp/upload_csr.php
```

複数の証明書自動更新を使用する場合は、それぞれ別のフォルダとスクリプトが必要になります。

・アップロードのスクリプトについて
http[s]でアップロードしたファイルはサーバー側のスクリプト等で適切な場所へ保存する必要があります。下記は PHP での実装例です。

```
upload_csr.php の例。csr.pem は/var/www/upload/ へ保存されます。
※php がインストールされ、動作している必要があります。

<?php
```

```
$uploaddir = '/var/www/upload/';
$csrfile = $uploaddir . basename($_FILES['userfile']['name']);
if (move_uploaded_file($_FILES['userfile']['tmp_name'], $csrfile)) {
        echo "<b>CSR Upload success.</b>";
} else {
        echo "<b>Save failed.</b>";
}
?>
```

サーバー内での保存の失敗は http[s]のレスポンスコードでは検出できないため、保存が成功したときは、" Upload success"の文字列を含む HTML 文書またはテキストを返送してください。

アップロードが成功すると Netwisr にログが出力されます。

```
lbcud: CSR uploaded. Certificate update time has come. ssl [ssl ポリシー名]
```

ポイント

アップロードされた csr.pem がどこの物かわからくなった時は、show cert-update で表示される 'CSR: ' 以降の文字列と、アップロード先の csr.pem ファイルの MD5 ハッシュ値を比較することで区別できます。

注意

再起動時およびフェイルオーバー時、正しい証明書のダウンロード完了前は同じ CSR が再度アップロードされる場合があります。

2.20.10.3 証明書ダウンロード

証明書をダウンロードするためには、http サーバー上の任意のフォルダを使用します。また、複数の証明書自動更新を使用する場合は、それぞれ別のフォルダが必要になります。

CSR 提出により CA 局から証明書が提供されたら、証明書をダウンロード元の http サーバーにセットします。

get-url コマンドでセットしたフォルダの url を指定します。

中間証明書がある場合はその数を intermidiate-cert-num コマンドで指定します。(1～2 まで。サーバー証明書のみのときは 0)

```
netwiser(config-cert-update)# get-url https://xxxx.yyyy.jp/cert_tmp/
netwiser(config-cert-update)# intermidiate-cert-num 1
```

各ファイルは以下のファイル名である必要があります。また、PEM フォーマットである必要があります。

サーバー証明書 ：cert.pem

中間証明書　：chain.pem　※intermidiate-cert-num が 1 か 2 のとき

中間証明書 2 段目 ：chain2.pem　※intermidiate-cert-num が 2 のとき

秘密鍵 ：key.pem ※CSR なしモード時のみ

⚠ 注意 intermidiate-cert-num に 1,2 を指定した場合、ダウンロード元から chain.pem, (chain2.pem)が取得できるまで、証明書自動更新は進みません。

2.20.10.4 ダウンロード／アップロード時のユーザー認証

ダウンロード／アップロード時にユーザー認証が必要な http サーバーにアクセスするときは、アカウントとそのパスワードを設定できます。
使用できる認証方式は、Basic 認証または Digest 認証です。

```
netwiser(config-cert-update)# get-account user1
netwiser(config-cert-update)# get-password pass1
```

※パスワードは show running-config cert-update 等で見ることはできません。

⚠ 注意 ユーザー認証のパスワードや秘密鍵のパスフレーズには、“ (ダブルクォーテーション)は使用できません。
ユーザー認証のパスワードや秘密鍵のパスフレーズの文字列の最後には、¥ (バックスラッシュ)は使用できません。

2.20.10.5 ダウンロードした SSL 証明書の有効化

ダウンロードした証明書が正常(有効期限内かつ公開鍵が一致)なとき、Netwiser 内に保存され、以下のログがでます。

```
New certificate［SSL ポリシー名］was ready.
```

SSL 証明書の有効化後、毎日 15:00～16:59 の間に全仮想サーバーを検索します。
仮想サーバーでプレフィックスにマッチする SSL ポリシーが使用されている場合は、作成された新しい SSL ポリシーへ切り替え、以下のログがでます。

```
New SSL［SSL ポリシー名］was effect to virtual.〈仮想サーバーへ適用した数〉
```

この段階で SSL アクセラレートは新しい証明書に切り替わります。

2.20.10.6 CSR なしモード

csr-update コマンドが 0 とき CSR なしモードとなります。

```
netwiser(config-cert-update)# csr-update 0
```

CSR なしモードでは、秘密鍵と証明書を同時にダウンロードし、正常であれば直ちに最大のインデックス値+1 の新しい SSL ポリシーを作成し、新しいダウンロードに備えます。
ダウンロードのための設定は CSR ありモードと同じです。
ダウンロードされた証明書が前回 (インデックス値が 1 つ前) のものと同一なときは、ダウンロードされた秘密鍵と証明書は破棄されます。

2.20.10.7 SSL 証明書自動更新設定上の注意

証明書自動更新では、SSL ポリシーの追加、証明書や秘密鍵の保存のため、一時的に特権モード権限が必要です。
また、冗長構成の時は BACKUP 機(スタンバイ機)に設定や証明書・秘密鍵等を同期するため、vrrp 設定モードの peer-address を設定し同期できる状態にする必要があります。

```
netwiser(config)# vrrp instance 0
netwiser(config-vrrp)# peer-address
<ip-addr>        IP address or IP name.
```

以下のログが出る場合は、他の端末で特権モードになっていないか、冗長構成の時は peer-address で指定したネットワークが BACKUP 機に到達可能か確認してください。

```
Can't entering config mode. check other terminal.
```

設定情報のインポートおよび全ての設定情報のインポートでは、エクスポート時と現在の証明書自動更新の進捗が異なる場合があります。
アップロード／ダウンロード先のサーバーとミスマッチが起こったり、冗長構成の相手と状態の不整合が起こる可能性があるため、証明書自動更新はインポート後強制的に無効(no enable)になります。
アップロード先の csr.pem が証明書自動更新で処理中の物と違う場合は init コマンドで初期化してから有効(enable)にしてください。
冗長構成の場合は冗長構成の相手と仮想サーバーおよび SSL ポリシーを比較し、異なる場合は合わせてから有効(enable)にしてください。
※init コマンド使用後 csr.pem と秘密鍵は新しく作り直されます。

⚠ 注意

証明書自動更新では更新状況により適宜設定の保存が行われるため、ユーザが一時的に設定しておいたものが、タイミングにより保存されてしまう可能性があります。

⚠ 注意

プレフィックスにマッチする SSL ポリシーの変更、削除や証明書等のインポートは、証明書自動更新に影響が出る可能性があります。

2.21 クラウド WAF

本章では、本製品のクラウド WAF 連携機能について説明します。

2.21.1 クラウド WAF 連携

クラウド WAF 連携機能を使用すると、本製品を流れる着信トラフィックと発信トラフィックをフィルタリングできます。

クラウド WAF 連携機能は、L7 負荷分散のアクセスログ機能(2.19.15)を使用して、WAF センタールールとシグネチャマッチングをおこないます。攻撃検知対象の場合は、センターから本製品へ遮断命令を送信し、遮断対象 IP アドレスをブロックします。

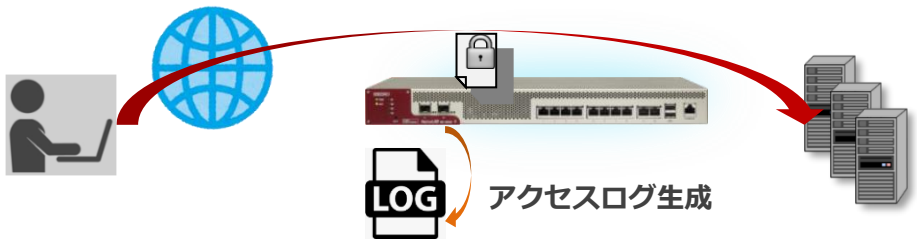
⚠ 注意 遮断対象 IP アドレスは IPv4 アドレスとなります。

2.21.2 クラウド WAF 連携動作イメージ

攻撃検知後の遮断動作イメージを以下に示します。

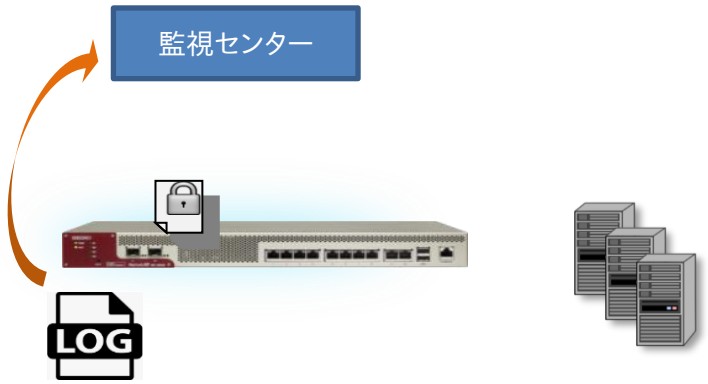
2.21.2.1 アクセスログの生成

① クライアントから Web サーバーへ HTTP リクエストを送信
② Web アプリケーションが HTTP レスポンスを送信
③ 本製品がアクセスログを生成



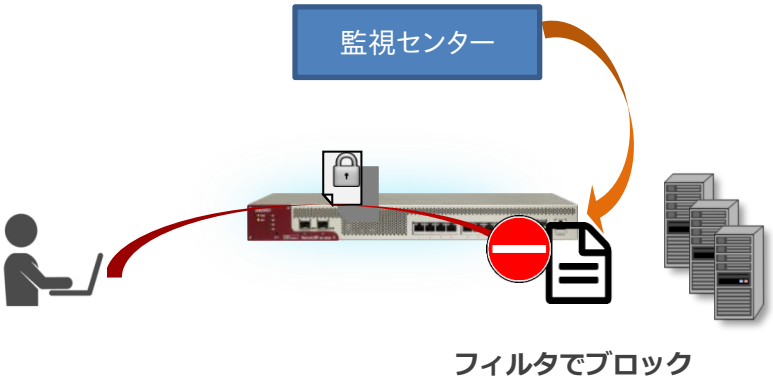
2.21.2.2 監視センターへログ送信

① アクセスログを収集
② 監視センターへログを送信（UDP）



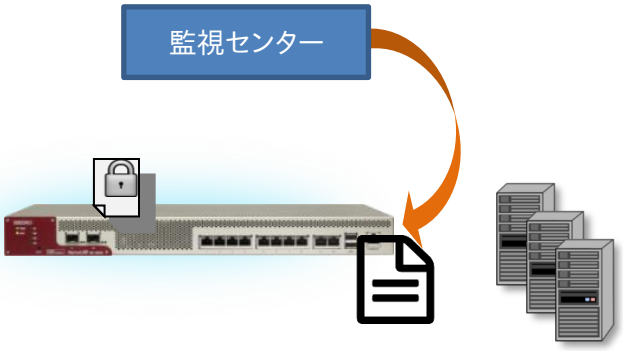
2.21.2.3 遮断命令の送信

① 監視センターで、ログを WAF センタールールとシグネチャマッチング
② 攻撃検知対象の場合は、監視センターから本製品へ遮断命令を送信
③ 遮断対象 IP アドレスを引数に遮断ルールを追加（接続元 IP アドレスの拒否）



2.21.2.4 ブロック解除命令の送信

① 遮断時間（初期値：10 分間）を経過した場合は、本製品へ遮断解除命令を送信
② 対象 IP アドレスを引数に遮断ルールを削除（接続元 IP アドレスのブロック解除）



2.21.3 クラウド WAF の有効

クラウド WAF を利用する場合は、以下を設定します。

クラウド WAF マネージャーの IP アドレスとポートを指定します。

```
netwiser(config)# cloud-waf manager-address <IP ｱﾄﾞﾚｽ> port <ﾎﾟｰﾄ>
netwiser(config)# no cloud-waf manager-address
```

クラウド WAF エージェントキーを指定します。

```
netwiser(config)# cloud-waf key <key>
netwiser(config)# no cloud-waf key
```

クラウド WAF 有効・無効を指定します。

```
netwiser(config)# enable cloud-waf
netwiser(config)# no enable cloud-waf
```

ポイント

有効時は manager-address, key の変更はできません。

2.21.4 アクセスログ設定

クラウド WAF を使用する場合は、クラウド WAF を適用する仮想サーバーの設定に以下のようにアクセスログを設定します。

```
adm(config-virtual)# access-log 127.0.0.1 23.4
```

通常のアクセスログ設定とは異なり、syslog サーバーのアドレスは外部の IP アドレスではなく、本製品自身を指定します。また、ファシリティとレベル（local7. LOG_WARNING）を指定します。

ポイント

アクセスログ機能は L7 負荷分散機能の一部です。アクセスログ機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

2.21.5 クラウド WAF 情報表示

クラウド WAF の情報を表示します。

2.21.5.1 クラウド WAF 設定情報表示

クラウド WAF の設定情報を確認するには、以下のコマンドを使用します。

```
netwiser> show cloud-waf [-d]
```

表示例を以下に示します。

```
netwiser> show cloud-waf
Manager-Address: 3.114.226.161
                Port: 10024
                 Key: ID: 002, Name: SVB000000024, IP: any
             Enable: yes
```

各項目は以下のようになっています。

■Manager-Address：クラウド WAF マネージャーの IP アドレス

■Port：クラウド WAF マネージャーの宛先ポート番号

■Key：クラウド WAF マネージャーより発行されたエージェントキーの内容

■Enable：クラウド WAF の設定状態です。有効の場合 yes と表示。

現在ブロックされている IP アドレスを表示するには、-d オプションを付けます。

```
netwiser> show cloud-waf -d
Manager-Address: 3.114.226.161
                Port: 10024
                 Key: ID: 002, Name: SVB000000024, IP: any
             Enable: yes
--- Block IP List ---
163.49.52.30/32
```

■Block IP List：ブロックされている IP アドレス

2.21.5.2 アクセスログ表示

本製品を通過した HTTP のアクセスログを表示するには、以下のコマンドを使用します。

```
netwiser> show access-log
```

以下に表示例を示します。

```
netwiser> show access-log
163.49.52.30 - - [27/Mar/2023:10:40:43 +0900] "GET
/railsgoat/forgot_password)%20or%20exists%20(%20select%20%22java.lang.T
hread.sleep%22(15000)%20from%20INFORMATION_SCHEMA.SYSTEM_COLUM
NS%20where%20TABLE_NAME%20=%20'SYSTEM_COLUMNS'%20and%20COL
UMN_NAME%20=%20'TABLE_NAME')%20--%20 HTTP/1.1" 404 1492
192.168.0.3 - - [27/Mar/2023:10:30:06 +0900] "GET /.env HTTP/1.0" 404 202
192.168.0.3 - - [27/Mar/2023:10:30:06 +0900] "GET / HTTP/1.0" 200 28067
```

アクセスログをクリアするには、config モードに移り以下のコマンドを使用します。

```
netwiser(config)# clear access-log
```

2.21.1 クラウド WAF における防御対象

本製品において防御可能な攻撃を下表に例示します。

攻撃手法
● サーバサイドインクルードインジェクション
● HTTP インジェクション
● LDAP インジェクション
● XML 外部エンティティ
● サーバサイドリクエストフォージェリ
● デシリアライゼーション
● クロスサイトスクリプティング
● SQL インジェクション
● NoSQL インジェクション
● OS コマンドインジェクション

- 改行コードインジェクション
- ディレクトリトラバーサル
- ファイルインクルード攻撃
- URL エンコード攻撃
- ブラックリスト UA
- その他の WEB 攻撃全般
- ミドルウェアなどの脆弱性を突いた攻撃（Apache Struts2 の脆弱性等）

⚠ 注意 これらの攻撃に対し 100%の防御を保証するものではございません

2.21.2 クラウド WAF における制限事項

● 本製品から監視センターへの通信は UDP プロトコルを利用します。プロトコルの性質上、通信経路で検査対象のログが Drop する可能性があります（監視センターではエージェントからの全ログを受信することを保証していません）。

● 遮断処理は、監視センターに送信されたログを検査後、検知対象の送信元 IP アドレスを遮断対象に登録します（IP アドレスベース遮断）。遮断対象に登録されるまでのリクエストは検知のみを実施します。

● 本製品と監視センター間のステータスが、オフラインからオンラインに変化した場合、オフライン期間のログ情報が監視センターへまとめて送信されます。一度に大量のログが送信された場合、しきい値系のシグネチャで検知/遮断される可能性があります。

2.22 ヘルスチェックの設定

サーバーの稼働状態をチェックするにはヘルスチェックの設定を行います。
本章ではヘルスチェックに関する設定方法を例とともに記します。

ヘルスチェックを行うには特権モードの *probe* コマンドでヘルスチェックポリシーを定義します。

```
①ICMP ヘルスチェック
netwiser(config)# probe <ﾎﾟﾘｼｰ名> <ｻｰﾊﾞｰ IP ｱﾄﾞﾚｽ>
②L4/7 ヘルスチェック
netwiser(config)# probe <ﾎﾟﾘｼｰ名> <ｻｰﾊﾞｰ IP ｱﾄﾞﾚｽ>.<ﾎﾟｰﾄ>.{udp|tcp|ssl}
③ヘルスチェック組み合わせ設定
netwiser(config)# probe <ﾎﾟﾘｼｰ名> <"組み合わせ文字列">
```

probe コマンドを実行すると、ヘルスチェック設定モードに遷移します。
ヘルスチェック設定モードではヘルスチェックに関する詳細設定を行います。
既に作成済みのヘルスチェックポリシーを指定する場合、ポリシー名を指定するだけでヘルスチェック設定モードに遷移します。

ヘルスチェック設定モードの *interval* コマンドでヘルスチェックの間隔（1～255 秒）を設定することができます。

```
netwiser(config-probe)# interval <時間(ms)>
```

ヘルスチェック設定モードの *retry* コマンドによりヘルスチェックで異常検知と判断するまでのリトライ回数を設定することができます。

```
netwiser(config-probe)# retry <回数>
```

ヘルスチェックポリシーを定義しただけでは、ヘルスチェックは開始されません。
ヘルスチェックポリシーを有効にするにはヘルスチェック設定モードで *enable* コマンドを実行します。また、無効に戻すには *no* を指定します。

```
netwiser(config-probe)# enable
netwiser(config-probe)# no enable
```

特権モードでの *enable probe* コマンドの実行でもヘルスチェックを有効にすることが可能です。無効に戻すには *no* を指定します。

```
netwiser(config)# enable probe <ﾎﾟﾘｼｰ名>
netwiser(config)# no enable probe <ﾎﾟﾘｼｰ名>
```

2.22.1 サーバー復旧時動作

デフォルト設定では、ヘルスチェックDOWN状態からALIVE状態に変化した際、該当サーバーは即時に負荷分散対象に復帰します。

ヘルスチェック設定モードで *manual-failback* コマンドを実施することで、ヘルスチェック DOWN 状態から ALIVE 状態に変化しても、該当実サーバーを負荷分散対象から除外したままにしておくことが可能です。

設定を解除するには *no* を指定します。

```
netwiser(config-probe)# manual-failback
netwiser(config-probe)# no manual-failback
```

manual-failback 設定でヘルスチェック DOWN 状態になると、該当の実サーバーは無効状態へと変化します。*enable real* コマンドで有効状態にするまで、実サーバーは負荷分散対象から除外されます。

以下の例では、実サーバー192.168.1.10.80.tcp がヘルスチェック DOWN 状態から ALIVE 状態に変化した後、負荷分散対象に復帰するまでの手順を記します。

```
*** 192.168.1.10.80.tcp がヘルスチェック DOWN  ***
netwiser(config)# show real
Address: 192.168.1.10
                              Port: 80            Curcon: 0
                             Proto: tcp         PeakCon: 100
                            MaxCon: 0            TotCon: 1102
                            Enable:                Fail: 0
*** 手動で該当のサーバーを負荷分散対象に復帰させる ***
netwiser(config)# enable real 192.168.1.10.80.tcp
netwiser(config)# show real
Address: 192.168.1.10
                              Port: 80            Curcon: 0
                             Proto: tcp         PeakCon: 100
                            MaxCon: 0            TotCon: 1102
                            Enable: yes            Fail: 0
```

変化

以下のように、既にICMPヘルスチェックで登録されているIPアドレスを使用して、更にLayer4以上のヘルスチェックポリシーを登録する場合、それぞれのポリシー間で *manual-failback* 設定を合わせる必要があります。

```
probe icmp_probe 192.168.1.10          ; ICMP ヘルスチェック
probe http_probe 192.168.1.10.80.tcp   ; TCP ヘルスチェック
```

manual-failback 設定が異なる場合、先にダウンした方の動作が適用されます。

2.22.2 ICMP ヘルスチェック

ICMP の echo 要求をサーバーIP アドレスに送信します。規定回数連続して echo 応答を受信しない、または応答データが異常であるとサーバーダウンと判断します。

以下の例では、サーバー192.168.1.10 に対して ICMP ヘルスチェックを実行します。

```
netwiser(config)# probe icmp_probe 192.168.1.10
netwiser(config-probe)# enable
```

⚠ 注意

1つの実サーバーに対して、ICMP ヘルスチェックを複数登録しないでください。登録すると、2 台目以降のサーバーに対するヘルスチェックが失敗します。

ポイント

ポート番号 0 を指定した実サーバーのヘルスチェックは、ICMP ヘルスチェックが必要です。

2.22.3 TCP ヘルスチェック

TCP ヘルスチェックでは、コネクション要求をサーバーAP に送信します。
コネクションが確立されれば正常と判断し、規定回数連続してコネクションが確立できなければサーバーダウンと判断します。

以下の例では、サーバー192.168.1.10 の 80 番ポートに対して TCP ヘルスチェックを実行します。

```
netwiser(config)# probe tcp_probe 192.168.1.10.80.tcp
netwiser(config-probe)# enable
```

2.22.4 UDP ヘルスチェック

UDP ヘルスチェックでは、1 バイトのデータ(0xff)をサーバーAP に送信します。
ICMP Port Unreachable を受信しなければ正常と判断します。

以下の例では、サーバー192.168.1.10 の 561 番ポートに対して UDP ヘルスチェックを実行します。

```
netwiser(config)# probe udp_probe 192.168.1.10.561.udp
netwiser(config-probe)# enable
```

ポイント

同一サーバーの同一ポートに対して複数の *probe* 設定を行わないでください。

2.22.5 HTTP ヘルスチェック

HTTP ヘルスチェックでは、HTTP リクエストをサーバーAP に送信しレスポンスをチェックします。

```
netwiser(config-probe)# http <"ﾘｸｴｽﾄ"> {status <ｽﾃｰﾀｽｺｰﾄﾞ> ... |
string <"ﾚｽﾎﾟﾝｽ"> }
```

TCP コネクション確立後<"ﾘｸｴｽﾄ">をサーバーAP に送信します。
応答パケットの内容が、指定の<ｽﾃｰﾀｽｺｰﾄﾞ>または<"ﾚｽﾎﾟﾝｽ">と合致すれば正常と判断されます。

■*<"ﾘｸｴｽﾄ">*
HTTP リクエストとして送信する文字列です。

■*<ｽﾃｰﾀｽｺｰﾄﾞ>*
指定された HTTP ステータスコードがサーバーからのレスポンスに含まれていれば正常と判断します。値は最大 4 パターンまで指定可能です。数字は空白で区切ってください。また、値をハイフン(-)で連結すると範囲指定が可能になります。
必ず 3 桁の数字を使用してください。

■*<"ﾚｽﾎﾟﾝｽ">*
指定された文字列がサーバーからのレスポンスに含まれていれば正常と判断します。

デフォルト設定では TCP コネクションの確立と解放を毎回行います。確立したコネクションをそのまま維持する場合は、*persist* コマンドを実行してください。

```
netwiser(config-probe)# persist
```

以下の例では、HTTP サーバー192.168.1.10 への GET リクエストに対して、ステータスコード 200～202 もしくは 304 が返答されれば正常と判断します。

```
netwiser(config)# probe http_probe_st 192.168.1.10.80.tcp
netwiser(config-probe)# http "GET / HTTP/1.0¥r¥n¥r¥n" status 200-202
 304
```

ポイント

リクエスト文字列の末尾の改行は省略しても構いません。その場合、本製品が自動で改行を付加して HTTP リクエストを送信します。

以下の例では、HTTP サーバー192.168.1.10 の"/test.html"への GET リクエストに対して、サーバーからのレスポンス内に”It works.”という文字列が含まれていれば正常と判断します。また、コネクション維持設定を行います。

```
netwiser(config)# probe http_probe_res 192.168.1.10.80.tcp
netwiser(config-probe)# http "GET /test.html HTTP/1.0¥r¥n¥r¥n" string "It works."
netwiser(config-probe)# persist
```

ポイント

指定したリクエストが HTTP1.0 で、かつ *persist* が設定された場合、HTTP リクエスト内に"Connection: Keep-Alive"ヘッダーを自動で挿入します。

2.22.6 SSL ヘルスチェック

SSL ヘルスチェックでは、コネクション要求から SSL ネゴシエーション完了までが動作すれば正常と判断します。
probe コマンドのプロトコルに *ssl* を指定すれば、SSL ヘルスチェックのヘルスチェックポリシーを定義することができます。

```
netwiser(config)# probe dns_probe 192.168.1.10.443.ssl
netwiser(config-probe)# enable
```

また、SSL ヘルスチェックポリシー上で HTTP ヘルスチェックを設定すると、サーバーへリクエストが暗号化されますので HTTPS ヘルスチェックとなります。

HTTP ヘルスチェックの詳細は「2.22.5HTTP ヘルスチェック」を参照してください。

2.22.7 DNS ヘルスチェック

DNS ヘルスチェックでは、DNS リクエストをサーバーAP に送信しレスポンスをチェックします。
問い合わせるドメイン名とクエリを指定して *dns* コマンドを実行します。

```
netwiser(config-probe)# dns <ﾄﾞﾒｲﾝ名> {A | AAAA}
```

サーバーから DNS レスポンスを受信し、レスポンスの QR ビットが 1, Opcode が 0, RCODE が 0 ならば正常と判断します。
以下の例では、DNS サーバー192.168.1.10 に対して DNS ヘルスチェックを実行します。

```
netwiser(config)# probe dns_probe 192.168.1.10.53.tcp
netwiser(config-probe)# dns www.server1.com A
netwiser(config-probe)# enable
```

2.22.8 その他アプリケーションヘルスチェック

その他アプリケーションプロトコルに対するヘルスチェックを以下に明記します。

■FTP ヘルスチェック

設定するにはヘルスチェック設定モードで *ftp* コマンドを実行します。

TCP コネクション確立後、サーバーからのメッセージを待ちます。

ステータス 220 で始まるメッセージを interval 以内に受信すれば正常と判断します。

```
netwiser(config-probe)# ftp
```

■IMAP4 ヘルスチェック

設定するにはヘルスチェック設定モードで *imap4* コマンドを実行します。

TCP コネクション確立後、サーバーからのメッセージを待ちます。

"*OK"で始まるﾒｯｾｰｼﾞを interval 以内に受信すれば正常と判断します。

```
netwiser(config-probe)# imap4
```

■NTP ヘルスチェック

設定するにはヘルスチェック設定モードで *ntp* コマンドを実行します。

サーバービットが ON であり、かつ LI（Leap Indicator）ビットが"11"以外である NTP 応答を interval 以内に受信すれば正常と判断します。

```
netwiser(config-probe)# ntp
```

■POP3 ヘルスチェック

設定するにはヘルスチェック設定モードで *pop3* コマンドを実行します。

TCP コネクション確立後、サーバーからのメッセージを待ちます。

"+OK"で始まるﾒｯｾｰｼﾞを interval 以内に受信すれば正常と判断します。

```
netwiser(config-probe)# pop3
```

■SMTP ヘルスチェック

設定するにはヘルスチェック設定モードで *smtp* コマンドを実行します。

TCP コネクション確立後、サーバーからのメッセージを待ちます。

ステータスコード 220 で始まるメッセージを interval 以内に受信すれば正常と判断します。

```
netwiser(config-probe)# smtp
```

2.22.9 ヘルスチェックの組み合わせ

複数のヘルスチェックポリシーを組み合わせたヘルスチェックポリシーを登録することが可能です。

別に設定されたヘルスチェックポリシーを最大４つまで、論理演算子 AND(&&)と OR(||)を使用して組み合わせます。演算子の前後はブランクが必要です。

AND で結ばれたサーバーはどれかひとつでもダウンすると、全てダウン状態にセットされます。

OR で結ばれたサーバーはどれかひとつでもヘルスチェックにパスすれば、全てアップ状態にセットされます。

以下の例では、ヘルスチェックポリシーP1、P2 の両方がダウンするか、P3 がダウンした場合、P1、P2、P3 全てのヘルスチェックがダウンにセットされます。

```
netwiser(config)# probe nest_probe "(P1 || P2) && P3"
```

⚠ 注意

以下のように、ヘルスチェックポリシー(P1)を複数の組み合わせ設定に登録しないでください。

```
netwiser(config)# probe nest_probe1 "P1 && P2 && P3"
netwiser(config)# probe nest_probe2 "P1 && P4"
```

2.23 冗長構成の設定

本製品は冗長構成で動作します。
本章では冗長構成に関する設定方法を例とともに記します。
冗長構成は、同一機種、同一バージョン間で構成してください。

⚠ 注意 SX-3940/3920 を冗長構成でご使用の場合、本体前のスルースイッチを必ず OFF にしてください。

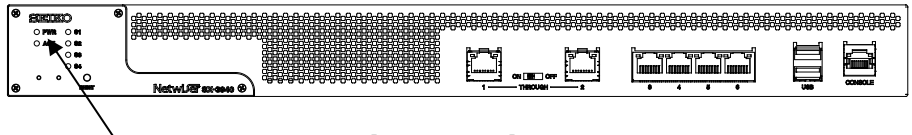
2.23.1 概要

2.23.1.1 アクティブ/スタンバイ方式

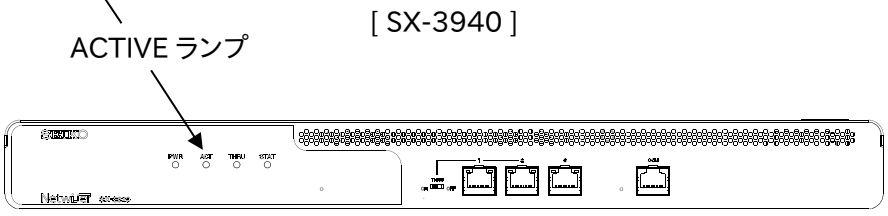
本装置で冗長構成を組む場合、アクティブ／スタンバイ方式での冗長構成となります。
2 台のうち、負荷分散を行っている機器を“マスター機”あるいは“マスター状態”と呼び、待機している機器を“バックアップ機”あるいは“バックアップ状態”と呼びます。
SX-3950,SX-3945,SX-3940,SX-3920 では、冗長構成で動作している場合、マスター機は前面パネルの ACTIVE ランプが点灯し、バックアップ機は消灯します。

■ACTIVE ランプ（緑）
冗長構成でない場合は常に点灯しています。
冗長構成時はマスター機が点灯、バックアップ機が消灯します。

＊SX-3950、SX-3945 の ACTIVE ランプも同じ位置になります。



[SX-3940]



[SX-3920]

2.23.1.2 VRRP プロトコル

本製品で採用している VRRP(Virtual Router Redundancy Protocol)プロトコルは IPv4 と IPv6 アドレスをサポートするバージョン3(v3)です。VRRP プロトコルは、冗長構成を組む 2 台の機器間で VRRP 広告パケットを交換することにより動作します。

基本的には、以下のように動作します。

① マスター機は VRRP 広告パケットを一定間隔で送出し続ける。

② バックアップ機はマスター機からの VRRP 広告パケットを受信する。

③ バックアップ機は VRRP 広告パケットを一定時間受信できなくなると、マスター機に異常が発生したと判断し、自身をマスター状態に遷移する。

ポイント

本製品では、

1. マスター機の VRRP 広告パケットは仮想ルーターID(VRID)を設定した VLAN からデフォルトでは 1 秒に 1 回送信します。(送信インターバルは変更できます)
2. バックアップ機は送信インターバルの約 3 倍の時間 VRRP 広告パケットが受信できなければマスター状態に遷移します。

VRRP に関連する設定の詳細は「2.23.5VRRP 設定」を参照してください。

2.23.2 冗長構成の有効化

VRRP を有効にするには、VRRP 広告パケットをやり取りする VLAN 毎に仮想ルーターID（VRID）を設定します。仮想ルーターID は、マスター機とバックアップ機で同じ ID を割り振ってください。
後述する VRRP 設定の順序に関係なく、VRID を設定したタイミングで VRRP が有効になります。

ポイント

VRRP では、同一仮想ルーターID の機器がマスター／バックアップの関係になりますので、当該ロードバランサー以外の VRRP 機器とは異なる仮想ルーター ID を割り振ってください。

以下の例では、VLAN1 に対して VRID「100」を割り振ります。

```
netwiser(config)# interface vlan 1
netwiser(config-vlan)# vrrp vrid 100
vrrp instance 0 created.
```

ポイント

仮想ルーターID の設定のみでは、コマンドやセッション情報の同期は行われません。相手機器との同期状態を確立するための設定が必要です。
詳細は「2.23.7冗長同期設定」を参照してください

show vrrp コマンドで、VRRP 状態や VRRP 関連の統計情報を参照することができます。詳しくは**「SX-3990_3950_3945_3940_3920 コマンドリファレンス」（別紙）**を参照してください。

2.23.3 L2 ループの防止

デフォルト設定では、バックアップ状態の機器でも L2 フォワーディングを行います。よって、ネットワークの接続が物理的に L2 ループを含んでいる場合、バックアップ機の MAC フレームの中継によりブロードキャストストームが発生します。冗長構成に伴う L2 ループの防止策として以下の 2 つの方法のうちどちらかを設定します。

① L2 フォワーディングの停止設定
② スパニングツリー設定

以下、それぞれについて詳しく述べます。

2.23.3.1 L2 フォワーディングの停止設定

任意の VLAN における L2 フォワーディングの停止設定をするには *no vrrp backup-l2forward* コマンドを実行します。
本コマンドを実行した機器の VLAN は、バックアップ状態になると L2 フォワーディングを行わなくなります。(マスター状態ではフォワーディングします)

no vrrp backup-l2forward を実行すると、本製品がバックアップ状態になった際に VLAN1 の L2 フォワーディングが停止します。

```
netwiser(config)# interface vlan 1
netwiser(config-vlan)# no vrrp backup-l2forward
```

L2 フォワーディングの停止設定を解除するには *vrrp backup-l2forward* を実行します。

```
netwiser(config-vlan)# vrrp backup-l2forward
```

ポイント

no vrrp backup-l2forward が設定された VLAN では、管理 IP アドレスへのアクセスは継続して行えますが、パケットの送信には下記の制限があります。

1. 本製品からのパケットの送信は、VLAN に割り当てられたイーサネットポートのうち、ポート番号が最も小さいリンクアップしているポートから行われます。
2. トランクポート(tagged 設定されたポート)がある場合は、ポート VLAN のポートを優先して使用します。

2.23.3.2 スパニングツリー設定

L2 ループを防止する 2 つ目の方法は、スパニングツリー設定です。
機器全体に反映されるスパニングツリーの設定を変更します。
イーサネットポートスパニングツリーの設定は「2.9スパニングツリーの設定」を参照してください。
本製品のスパニングツリーは Rapid Spanning-Tree Protocol（RSTP）で動作します。対向機器との関係でレガシーな STP で動作することはありますが、レガシーな STP 動作を設定で強制することはできません。

2.23.3.2.1 ブリッジプライオリティーの設定

VRRP 状態に連動させて、スパニングツリーのブリッジプライオリティーを変更することができます。これにより、接続スイッチがスパニングツリーに未対応の場合でも本製品同士で STP を構成することができます。
スパニングツリーのブリッジプライオリティーを変更するには、特権モードで *spanning-tree priority* コマンドを実行します。
デフォルト設定に戻すには *no* を指定します。

```
netwiser(config)# spanning-tree [master | backup] priority <プライオリティー値>
```

オプションに *master* を指定した場合は、マスター状態時のプライオリティーを、*backup* を指定した場合はバックアップ状態時のプライオリティーをそれぞれ設定します。省略した場合、マスター・バックアップの両プライオリティーをともに同じ値に設定します。

2.23.3.2.2 Bridge Protocol Data Unit 送信間隔の設定

STP 動作が、レガシーな STP で動作する場合、本製品が送信する Bridge Protocol Data Unit(BPDU)フレームの送信間隔はデフォルトで 2 秒です。
設定を変更するには *spanning-tree hello-time* コマンドを実行します。
デフォルト設定に戻すには *no* を指定します。

```
netwiser(config)# spanning-tree hello-time <BPDU 送信間隔(s)>
```

2.23.3.2.3 Bridge Protocol Data Unit タイムアウト時間の設定

STP 動作が、レガシーな STP で動作する場合、BPDU フレームのタイムアウト時間はデフォルトで 20 秒です。
設定を変更するには *spanning-tree max-age* コマンドを実行します。
デフォルト設定に戻すには *no* を指定します。

```
netwiser(config)# spanning-tree max-age <タイムアウト時間(s)>
```

2.23.3.2.4 状態遅延時間の設定

STP 動作が、レガシーな STP で動作する場合、本製品がフォワーディング状態に遷移する際の遅延時間はデフォルトで 15 秒です。
設定を変更するには *spanning-tree forward-delay* コマンドを実行します。
デフォルト設定に戻すには *no* を指定します。

```
netwiser(config)# spanning-tree forward-delay <遅延時間 (s)>
```

2.23.4 強制バックアップ

マスター状態で動作する機器を、強制的にバックアップ状態にすることが可能です。強制的にバックアップ状態にするには *vrrp force-backup* コマンドを実行します。

```
netwiser(config)# vrrp force-backup
```

強制バックアップ状態を解除すると、再び VRRP 状態の判定処理を行い、両機器間で VRRP 状態の決定がなされます。

```
netwiser(config)# no vrrp force-backup
```

⚠ 注意

vrrp force-backup の設定を行った場合はマスターに昇格しなくなります。冗長構成で運用を行う際は解除を行って下さい。

2.23.5 VRRP 設定

2.23.5.1 VRRP インスタンスの作成

VRRP に関する詳細設定を行う場合、VRRP インスタンスを作成して VRRP 設定モードに遷移します。

VRRP インスタンスは *vrrp instance* コマンドで作成します。

```
netwiser(config)# vrrp instance [<インスタンス No.>]
netwiser(config-vrrp)#
```

VRRP インスタンスを削除する場合、*no* を指定します。

```
netwiser(config)# no vrrp instance [<インスタンス No.>]
```

現在、VRRP インスタンスはシステムで 1 つしか作成できませんので、<インスタンス No.>パラメーターは省略可能です。指定する場合は必ず 0 を指定してください。

ポイント

冗長構成を有効にする場合、システムには必ず VRRP インスタンスが存在している必要があります。VLAN 設定モードで VRID を登録する際、VRRP インスタンス設定が存在しない場合は、システムが自動で VRRP インスタンス(No. 0)を生成します。

⚠ 注意

VRID 設定が存在する状態（冗長構成が有効状態）で VRRP インスタンスを削除すると、全ての VLAN から VRID 設定を削除し、冗長機能を無効にしてしまいますので注意してください。

2.23.5.2 プリエンプト機能の設定

本製品はフェイルオーバーが発生した後のフェイルバック動作として以下の 2 つをサポートしています。

① プリエンプトモード

機器に設定したプライオリティー値にしたがって、常にその値が高い方がマスター機となります。

② 非プリエンプトモード

先に起動した機器がプライオリティー値とは関係なくマスター機として動作し続けます。また、フェイルオーバーが発生後、バックアップ状態に遷移した機器が復旧しても、フェイルバック（切り戻し動作）が発生することなく動作し続けます。

プリエンプトモードを有効にするには、VRRP 設定モード内で、***preempt*** コマンドを実行します。

```
netwiser(config-vrrp)#  preempt
```

プリエンプトモードを無効にするには、***no*** を指定してコマンドを実行します。

```
netwiser(config-vrrp)#  no preempt
```

2.23.5.3 VRRP プライオリティーの設定

プリエンプトモードが有効な場合、VRRP プライオリティー値を適切に設定する必要があります。
デフォルト設定では、プライオリティー100 に設定されています。変更するには *priority* コマンドを実行します。

```
netwiser(config-vrrp)# priority <プライオリティー>
```

後述の設定情報の同期機能(「2.23.7.1 設定とセッション情報の同期」参照)が有効である場合、*priority* コマンドは冗長相手機器に同期されます。
冗長相手機器のプライオリティー値を自機器と異なる値で同期させるには *peer* オプションを指定します。

```
netwiser(config-vrrp)# priority <自プライオリティー> peer <相手プライオリティー>
```

設定同期が無効な場合、*peer* オプションを指定しても無視されます。

プライオリティー値をデフォルトに戻すには *no* を指定します。

```
netwiser(config-vrrp)# no priority
```

⚠ 注意

マスター・バックアップ両機器でプリエンプト設定が異なっていると正常に動作しなくなる恐れがあります。両機器間でプリエンプト機能の有効/無効を合わせてください。

ポイント

マスター、バックアップ機のプライオリティー値が等しい場合、先にマスター状態に遷移した機器がマスター状態でありつづけます。
たとえば、マスター状態の機器 A の故障によって機器 B がマスターに遷移したとすると、機器 A を復旧させても機器 B がマスター状態のままになります。

2.23.5.4 リンク監視機能の設定

自機のイーサネットポートのリンク状態を監視し、VRRP 広告パケットを動的に変更する機能です。イーサネットポートのリンク状態を監視し、フェイルオーバーのタイミングをコントロールすることができます。
SX-3990 では、ホストマシン内部の仮想ブリッジ（または仮想スイッチや TAP）に本製品が接続されている限り、動的なリンク DOWN が発生し得ないケースがあります。この場合、自らイーサネットポートを停止状態にしない限りは、リンク状態が DOWN になることがないため、本機能を使用することはできません。

設定により以下のようなことができます。

① VRRP 広告パケットの送信停止
リンク監視設定のグループに指定した全ての監視対象リンクがダウンした場合、マスター機は VRRP 広告パケットの送信を停止します。
広告パケット送信が停止しますので、フェイルオーバーが起こります。

② プライオリティー値の動的な変更
リンク監視設定のグループに含まれる監視対象ポートの何れかがリンクダウンする度にプライオリティー値を減少させることができます。
たとえば、
(ア) プリエンプトモードの冗長構成。
(イ) リンク監視対象グループとしてポート 1～3。
(ウ) マスター機のプライオリティー設定は 107。バックアップ機の設定は 100。
(エ) リンクダウン時の減算値は 5。
と設定した場合、マスター機のスイッチポートのリンク状態により以下のようにプライオリティー値を動的に変更します。

ケース①

設定 priority 値=107

ポート 1	LINK DOWN
ポート 2	LINK UP
ポート 3	LINK UP

実際の priority 値 =107−5
=**102**

ケース②

設定 priority 値=107

ポート 1	LINK DOWN
ポート 2	LINK UP
ポート 3	LINK DOWN

実際の priority 値 =107−5−5
=**97**

ケース①の場合は、減算後のプライオリティー値が 102 であるため、フェイルオーバーは起こりませんが、ケース②のように 2 ポートがダウンすると、プライオリティー値が 97 となる（バックアップ機より小さい）ので、フェイルオーバーが起こります。

リンク監視機能を設定するには VRRP 設定モード内で、*track* コマンドを実行します。

```
netwiser(config-vrrp)# track group <ｸﾞﾙｰﾌﾟ番号> ethernet <ﾎﾟｰﾄ番号情報> [decrement <減少値>]
```

以下の例では、マスター機のポート 1, 3, 5 がすべてリンクダウンすると、VRRP 広告パケットの送信を停止します。

```
netwiser(config-vrrp)# track group 1 ethernet 1,3,5
```

decrement オプションを指定することで、ポートがリンクダウンする度に VRRP プライオリティー値を減算します。
以下の例では、マスター機のポート 1, 3, 5 がリンクダウンする度に VRRP プライオリティー値を 5 ずつ減算します。

```
netwiser(config-vrrp)# track group 1 ethernet 1,3,5  decrement 5
```

すべてがリンクダウンすると、VRRP 広告パケットの送信を停止するのは同じです。

ポイント

リンク監視のグループは複数設定することができます。グループごとにプライオリティー減算値を独立に設定できます。ただし、複数グループに同一ポート番号を含めることはできません。

リンク監視機能を解除するには、グループ毎に *no* を指定します。

```
netwiser(config-vrrp)# no track group <ｸﾞﾙｰﾌﾟ番号>
```

2.23.5.5 VRRP 広告パケットの送信間隔

VRRP 広告のパケットは、1 秒間隔で送信されます。
VRRP 設定モードの *interval* コマンドで送信間隔を変更することが可能です。
時間は入力値×10(msec)が設定されます。
以下、VRRP 広告パケットの送信間隔を 3 秒に設定します。

```
netwiser(config-vrrp)# interval 300
```

Bacukp から Master 状態への遷移時間は、送信インターバルの約 3 倍の時間になります。
遷移時間の最小値は 200ms です。
<interval>に 1 から 6 を設定した場合でも遷移時間は 200ms となります。

2.23.5.6 VRRP 広告パケットの受信遅延設定

スパニングツリー設定によって L2 ループの防止を行っている場合、ツリー構成が収束するまでに数十秒かかることがあります。
収束までの間 VRRP 広告パケットを受信できなくなりますので、正常な状態であるにも関わらずバックアップ機がマスター状態に遷移してしまうことがあります。

これを避けるためには、VRRP 設定モード内で、*delay* コマンドを実行します。

```
netwiser(config-vrrp)# delay <遅延時間 (s)>
```

バックアップ状態に遷移した時には、*delay* コマンドで設定した時間だけ VRRP 広告パケットの受信開始を遅らせることができます。

本設定をデフォルト状態（無効）にするには、*no* を指定します。

```
netwiser(config-vrrp)# no delay
```

2.23.6 冗長 IP アドレス（Redundant IP アドレス）の設定

VLAN インターフェイスに冗長用の IP アドレス（以下、冗長 IP アドレス）を設定することが可能です。冗長 IP アドレスは、冗長構成でマスター状態になった場合にのみ有効になるアドレスです。

冗長 IP アドレスを設定することで、VLAN インターフェイスへの外部機器からのアクセスを一元的にマスター機側で受け付けることが可能になります。

```
netwiser(config-vlan)# ip redundant-address <IP ｱﾄﾞﾚｽ>
```

*<IP ｱﾄﾞﾚｽ>*には、IPv4 アドレスと IPv6 アドレスを一件ずつ登録することが可能です。

以下の例では、10.168.1.110 を VLAN2 の冗長アドレスとして設定します。

```
netwiser(config)# interface vlan 2
netwiser(config-vlan)# ip redundant-address 10.168.1.110
```

冗長 IP アドレスの使用用途として、たとえば、クライアント側とサーバー側のネットワークが別のセグメントである場合、サーバーからの戻りパケットのゲートウェイアドレスとして冗長 IP アドレスを登録します。

他にも、冗長 IP アドレスにアクセスすれば、現在マスター状態の機器にアクセスすることが可能になります。

2.23.7 冗長同期設定

2.23.7.1 設定とセッション情報の同期

マスター、バックアップ機器間で設定およびセッション情報の同期を行うには、VRRP 設定モードの *peer* コマンドで冗長相手先のアドレスを設定します。

```
netwiser(config-vrrp)# peer-address <IP ｱﾄﾞﾚｽ>
```

これにより、

① 操作中の機器で実行されたコマンドが、冗長相手機器でも実行されます。

② 負荷分散用のセッション情報がマスター機と同期します。

冗長同期は、マスター、バックアップの両機器に、

① *peer-address* 設定

② 仮想ルーターID（VRID）設定

の両方を設定すると機能します。

⚠ 注意 冗長同期はマスター、バックアップ間の同期用 TCP コネクションの状態によっては、コマンドやセッション情報を喪失することがありますので注意してください。

2.23.7.2 設定同期

マスター、バックアップの両機器に仮想ルーターID（VRID）設定、*peer-address* 設定を設定すると、現在設定中の機器で入力したコマンドを冗長相手機器でも即時実行します。

設定を変更するコマンドが同期対象となります。しかし、以下のコマンドは冗長相手に同期されません。

同期対象外コマンド	
特権モード	*clear *1*
	copy
	hostname
	import all
	import config
	import firmware

	passwd
	sync config
	write erase
VLAN 設定モード	*ip address*
イーサネット設定モード	*mirror-port*
	monitor
SSL 設定モード	*csr* *2
VRRP 設定モード	*peer-address*

*1 *clear content* を除く

*2 *csr* コマンド実行時に生成される署名要求書は冗長相手先に同期されませんが、同時に生成される秘密鍵は、冗長構成相手に同期されます。

2.23.7.2.1 設定情報の一括同期

sync config all コマンドを実行すると、一括同期対象外の設定を除く全ての設定情報・ユーザーアカウント情報を冗長相手機器にコピーします。
「全ての設定情報」には、SSL 関連ファイルや sorry コンテンツも含まれます。

```
netwiser(config)# sync config all
```

一括同期対象外コマンド	
特権モード	*hostname*
	terminal
VLAN 設定モード	*ip address*
VRRP 設定モード	*peer-address*

sync config all コマンドを実行後、冗長相手機器でその設定を有効にするには再起動をする必要があります。

⚠ 注意

コマンド実行後は、冗長相手機器を再起動するまではマスター機でもバックアップ機でも *write memory* を実行しないでください。
write memory してしまうと、一括同期した内容が現在の設定で上書きされてしまいます。

ポイント

sync config all を実行すると、自機器の VLAN の機器 IP アドレスを±1 したアドレスが、冗長相手側の VLAN の機器 IP アドレスとして設定されます。
+1 か−1 かは、自機器の VLAN の機器 IP と *peer-address* の大小関係から

決定します。(比較する自機器の IP アドレスは、コマンド同期に使用している VLAN の機器 IP アドレスです。)
たとえば、「自機器の IP アドレス ＞ *peer-address* で設定されている IP アドレス」であれば、−1 されます。

2.23.7.2.2 設定の非同期設定

冗長同期相手の IP アドレスと VRID が設定されている状態であっても、設定情報の同期を行わないように設定を変更することが可能です。
設定情報の同期を停止させるには、*no sync config* を実行します。
設定情報の同期を再開するには、*sync config* を実行します。

```
①コマンド同期の停止
netwiser(config)# no sync config
②コマンド同期の再開
netwiser(config)# sync config
```

2.23.7.3 セッション情報同期

セッション情報同期では、マスター機で生成される以下の負荷分散セッション情報を定期的にバックアップ機に送信します。

① L4 負荷分散用セッション情報
② IP アドレスセッション維持情報
③ Cookie セッション維持情報
④ SSL セッション維持情報
⑤ X-Forwarded-For セッション維持情報

ポイント

各セッション情報は 1 秒に 1 回、前回の送信からの差分情報をマスター機からバックアップ機へと送信します。

show session-sync コマンドで、セッション同期の送受信統計情報を参照することができます。詳しくは**「SX-3990_3950_3945_3940_3920 コマンドリファレンス」(別紙)**を参照してください。

2.23.7.3.1 全セッション情報の一括同期

*sync session all*コマンドを実行すると、実行時のマスター機とバックアップ機のセッション情報を一括同期します。

```
netwiser(config)# sync session all
```

⚠ 注意

本コマンドは、マスター機でもバックアップ機でも実行できます。
実行すると、バックアップ機のセッション情報をすべて破棄し、その後、マスター機の全セッション情報をコピーします。
このため、一括同期中はマスター機の負荷分散機能がほぼ停止状態になります（最大 1 分程度）ので注意してください。

ポイント

後述のセッション情報の非同期設定が有効であっても、一括同期は実行できます。

2.23.7.3.2 システム起動時のセッション同期

冗長同期が有効な場合、デフォルトでは、システム起動後に最初にバックアップ状態に遷移したタイミングでマスター機との全セッション同期を実施します。

全セッション同期は、前述（「2.23.7.3.1全セッション情報の一括同期」参照）の通り、マスター機の負荷分散停止を伴いますので注意が必要です。
本機能を無効にするには、*no sync startup-session*を実行します。
有効に戻すには、*sync startup-session*を実行します。

```
①起動時セッション同期の停止
netwiser(config)# no sync startup-session
②起動時セッション同期の開始
netwiser(config)# sync startup-session
```

2.23.7.3.3 セッション情報の非同期設定

peer-address と VRID が設定されている状態である場合、マスター機とバックアップ機は定期的にセッション情報の同期を行いますが、セッション情報の同期を行わないように設定を変更することが可能です。
同期を停止させるには、*no sync session* を実行します。
同期を再開するには、*sync session* を実行します。

```
①セッション同期の停止
netwiser(config)# no sync session
②セッション同期の再開
netwiser(config)# sync session
```

ポイント

システム起動時のセッション同期は、全セッション情報の同期と同等であるため、システム起動時のセッション同期が有効ならば、セッション情報非同期設定をしていたとしても初めてバックアップに遷移したタイミングで全セッションの同期を行います。
これを無効にするためには、システム起動時のセッション同期を無効に設定してください。

2.24 フェイルスルーの設定

SX-3940,SX-3920 では、本製品に何らかの障害が発生し処理が継続出来ない場合、ポート 1 とポート 2 をハードウェアにより直結することができます。これにより、万が一機器に障害が発生しても、提供中のサービスを止めることなく継続することが可能です。

フェイルスルー機能を有効にするには、仮想サーバーに関連付ける実サーバーのうち1台の実サーバーの IP アドレスに、仮想サーバーと同一 IP アドレスを定義します。
これによりフェイルスルー設定であることをシステムが自動で検知し、フェイルスルー機能が有効になります。また、仮想 IP と同一 IP の実サーバー(以下、フェイルスルー対象サーバーと呼称)を仮想サーバーとの関連付けから解除すると、フェイルスルー機能は無効になります。

以下の例では、仮想サーバー192.168.1.100.80.tcp と同一の IP アドレスを一台の実サーバーに定義し、フェイルスルー機能を有効にします。

```
netwiser(config)# real 192.168.1.100.80.tcp
netwiser(config)# real 192.168.1.101.80.tcp
netwiser(config)# virtual 192.168.1.100.80.tcp
netwiser(config-virtual)# bind 192.168.1.100.80.tcp
netwiser(config-virtual)# bind 192.168.1.101.80.tcp
netwiser(config-virtual)# enable
```

以上の設定により、本製品に障害が発生した場合でも、実サーバー 192.168.1.100 への接続性だけは確保された状態になります。

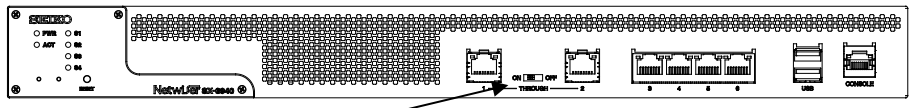
■スルースイッチ

フェイルスルー機能を使用する場合は、スルースイッチをONにしてください（左方向にスライドさせる）。

フェイルスルー機能を使用しない場合スルースイッチを OFF にしてください。

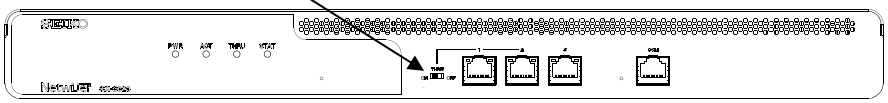
工場出荷状態でスルースイッチは ON に設定されています。

スルー スイッチ	フェイル スルー設定	電源 OFF 時 または故障発生時	通常時
ON	有効	ポート 1-2 間が接続されます	ポート１とポート２は、それぞれ内部の通信用ＩＣに接続され通信が行われます
OFF	無効	ポート 1-2 間は接続されません	



[SX-3940]

スルースイッチ



[SX-3920]

show ethernet コマンドで、スルースイッチの状態を参照することができます。

詳しくは**「SX-3990_3950_3945_3940_3920 コマンドリファレンス」（別紙）**を参照してください。

■接続するイーサネットポートについての制限
フェイルスルー機能を使用する場合は、ポート1にクライアント側ネットワーク、ポート2にサーバー側ネットワークを接続してください。また、イーサネットポートの接続先ネットワーク種別が以下のように設定されている必要があります。
ポート1　network
ポート2　server
この設定は、フェイルスルー機能が有効になった際にシステムが自動で設定します。ただし、フェイルスルー対象サーバーを仮想サーバーとの関連付けから解除しても、接続先ネットワーク種別の設定は元の設定に戻りませんので注意してください。元に戻すにはイーサネット設定モードの ***slb*** コマンドを実施します。
詳細は「2.15接続先ネットワーク種別」を参照してください。
ポート 1、2 以外のポートも負荷分散に使用することは可能ですが、フェイルスルー対象サーバーは必ずポート 2 に接続してください。

■ヘルスチェックポリシーについての制限
フェイルスルー設定を行った場合、必ずフェイルスルー対象サーバーに対する icmp ヘルスチェックが登録されている必要があります。

⚠ 注意

フェイルスルー機能には他にもいくつかの制約事項があります。
以下に全ての制約事項を記しますので、フェイルスルー機能を使用する場合は必ず確認してください。

1. 仮想サーバーと同一の IP アドレスである実サーバーが 1 台バインドされていること
2. イーサネットポートの接続先種別（***slb*** コマンド）が正しく設定されていること
3. スルースイッチが ON になっていること
4. ポート 1 とポート 2 のリンク速度、VLAN ID、802.1Q タグ設定の有効/無効が一致していること
5. スパニングツリープロトコル、リンク集約が設定されていないこと
6. 冗長構成でないこと
7. 仮想サーバーにソース NAT が設定されていないこと
8. 仮想サーバーに ***dsr*** オプション付きでバインドされた実サーバーが存在しないこと
9. 仮想サーバーと関連付けている全ての実サーバーの IP バージョンが一致

していること

10. フェイルスルー対象サーバーに対する icmp ヘルスチェックの登録がされており、かつサービス開始前に必ず一度はヘルスチェックが成功していること

■フェイルスルー対象サーバーの交換

フェイルスルー対象サーバーのヘルスチェック DOWN を検出した後、フェイルスルー対象サーバーの交換や、それ準ずる作業により該当の IP アドレスに紐付く MAC アドレスが変更される場合、対象サーバーの接続性が復旧した後でも本製品から対象サーバーに実施している ICMP ヘルスチェックは DOWN 判定のままとなります。

この状態を復旧するには、対象サーバーの交換が済んだ後に、対象サーバーへのヘルスチェックポリシーを起動し直す必要があります。

ヘルスチェックポリシーは特権モードの *enable probe* コマンドか、ヘルスチェック設定モードの *enable* コマンドで起動し直すことができます。

特権モードの場合、以下のようにヘルスチェックポリシーを再起動します。

```
netwiser(config)# no enable probe <ヘルスチェック名>      ; 停止する
netwiser(config)# enable probe <ヘルスチェック名>         ; 起動する
```

ヘルスチェック設定モードの場合、以下のようにヘルスチェックポリシーを再起動します。

```
netwiser(config)# probe <ヘルスチェック名>      ; モード遷移する
netwiser(config-probe)# no enable          ; 停止する
netwiser(config-probe)# enable             ; 起動する
```

2.25 TRACEROUTE

本製品では traceroute コマンドを使用することができます。
宛先ホストまでのネットワーク経路をリスト表示します。

宛先ホストが IPv4 アドレスの場合は *traceroute* を使用します。

```
netwiser> traceroute {<IPv4 ｱﾄﾞﾚｽ> | <ﾎｽﾄ名>} [source-ip-addr <IPv4 ｱﾄﾞﾚｽ> [route-id <ﾙｰﾄ ID>] | source-virtual {<仮想ｻｰﾊﾞｰ ID> | <仮想ｻｰﾊﾞｰ名>}] [hop <ﾎｯﾌﾟ数>]
```

宛先ホストが IPv6 アドレスの場合は *traceroute6* を使用します

```
netwiser> traceroute6 {<IPv6 ｱﾄﾞﾚｽ> | <ﾎｽﾄ名>} [source-ip-addr <IPv6 ｱﾄﾞﾚｽ> [route-id <ﾙｰﾄ ID>] | source-virtual {<仮想ｻｰﾊﾞｰ ID> | <仮想ｻｰﾊﾞｰ名>}] [hop <ﾎｯﾌﾟ数>]
```

宛先ホストには IP アドレス、IP アドレス名、またはホスト名を指定することができます。
送信元を指定したい場合は、IP アドレス、仮想サーバーID、または仮想サーバー名を指定することができます。
送信元に IP アドレスを指定した場合はルート ID を指定することが出来ます。
仮想サーバーID、または仮想サーバー名を指定した場合は該当の仮想サーバーに設定されているルート ID が自動的に使用されます。
最大ホップ数を指定できます。設定できる最大ホップ数の範囲は 1 から 32 です。
省略した場合、8 に設定されます。

ポイント

ルート ID を指定した場合は、指定したルート ID と同一の ID を持つルーティングテーブルに従います。ルート ID を指定しない場合はルート ID 0 が使用されます。

ポイント

送信元 IP アドレスは以下のアドレスのみ使用可能です。

1. VLAN の管理 IP アドレス(VLAN 設定モードの *ip address* 設定)
2. 冗長アドレス(VLAN 設定モードの *ip redundant-address* 設定)
3. 仮想サーバードレス(特権モードの *virtual* 設定)
4. NAT プールアドレス(特権モードの *nat-pool* 設定)

NAT プールアドレスを送信元アドレスとして使用するには、リバース NAT 登録またはソース NAT の設定がされている必要があります。

2.26 ライブマイグレーション（SX-3990 のみ）

稼働中の仮想マシンを停止することなく別のホストマシン上に移動させる機能をライブマイグレーション機能と呼称します。
SX-3990 をライブマイグレーションさせる場合、その動作は各ハイパーバイザーの仕様に依存します。

ライブマイグレーションが正常に完了すると、ハイパーバイザーが自発的に、仮想 NIC の MAC アドレスを送信元とした MAC フレーム（RARP など）を送出し、隣接機器に対して、ARP キャッシュの更新を促します。
ただし、ここで通知される MAC フレームは、仮想 NIC の MAC アドレスを送信元とした MAC フレームであり、装置 IP や仮想 IP アドレスに紐付く MAC アドレスが通知されるわけではありません。装置 IP および仮想 IP に紐付く MAC アドレスを通知するには、*advertise-mode* コマンドを使用し近隣機器の ARP キャッシュを更新します。

GARP/UNA の送信を開始するには、*advertise-mode on* を実行します。
GARP/UNA の送信を停止させるには、*advertise-mode off* を実行します。

```
①GARP/UNA の送信開始
netwiser(config)# advertise-mode on
②GARP/UNA の送信停止
netwiser(config)# advertise-mode off
```

ポイント

advertise-mode on を実行後、10 分経過すると自動で送信を停止します。

第3章　コンフィグレーションガイド（WEB 管理画面編）

3.1 概要

本章では、本製品の設定作業について、WEB 管理画面での設定方法を例とともに記します。
SX-3990 では、設定作業を開始する前に、Netwiser をハイパーバイザー上にインストールする必要があります。詳しくは**「SX-3990 インストールガイド」**（別紙）を参照してください。
また、CLI（コマンドラインインターフェイス）を使用した設定方法は「第2章コンフィグレーションガイド（CLI 編）」を参照してください。
各項目の必須・任意設定や各入力値の入力範囲、入力制限等の情報は、WEB 管理画面各項目を参照してください。（「3.1.3.4入力値チェック」参照）

3.1.1 はじめに

本製品の WEB 管理画面は、Microsoft Internet Explorer 11.0 で動作確認を行っております。
その他のブラウザでは正しく動作しない場合があります。

ポイント

本製品の WEB 管理画面は JavaScript を使用しています。
正常に動作させるため、ブラウザの JavaScript 設定を有効にしてください。
＜Internet Explorer 11.0 の場合＞
右上に表示されている歯車アイコンをクリックして下さい。
表示されたメニューの中から［インターネットオプション］を選択します。
［インターネットオプション］画面で［セキュリティ］タブをクリックします。
［レベルのカスタマイズ］ボタンを押します。
［スクリプト］項目の［アクティブスクリプト］を［有効にする］を選択します。

ポイント

複数のブラウザから同時に設定変更を行わないでください。
設定が正しく反映されない場合があります。

3.1.2 WEB 管理画面概要

WEB 管理画面におけるトップ画面と各種メインメニューについて、以下に説明します。

メニュー項目	説明
トップ画面	WEB 管理画面へログインすると初めに表示される画面で、システム情報や簡易的な機器状態を表示します。 画面左上の Netwiser ロゴをクリックすると、どの画面からでもトップ画面に遷移することが可能です。
	各種設定を行います。コマンドラインインターフェイス（CLI）で設定する場合と同様に、使用条件に合わせた詳細な設定が可能です。
	各種モジュールの状態や統計値など詳細な機器情報が参照できます。
	システムのリソースや負荷分散におけるネットワークトラフィック負荷等のリアルタイムな情報をグラフィカルに表示します。
	システムのリソースや負荷分散におけるネットワークトラフィック等の統計情報をグラフィカルに表示します。 また、統計情報データを CSV 形式のファイルでダウンロードできます。
	機器内部に保持するログデータの参照やダウンロードを行います。

3.1.3 基本説明

基本的な操作や WEB 管理画面の機能について説明します。

3.1.3.1 ユーザーアカウント

WEB 管理画面のユーザーアカウントは、コマンドラインインターフェイス（以下、CLI）のユーザーアカウントと共用されます。

3.1.3.2 自動ログアウト

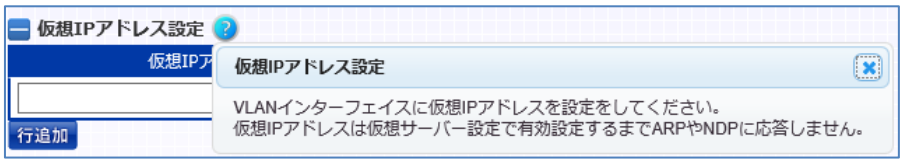
WEB 管理画面へログインしてから一定時間アクセスがない場合、自動的にログアウトします。自動ログアウト時間はデフォルトで 10 分です。

CLI を使用して自動ログアウト時間の変更や自動ログアウト機能の無効化が可能です。

詳細は「3.8.1.1自動ログアウト」を参照してください。

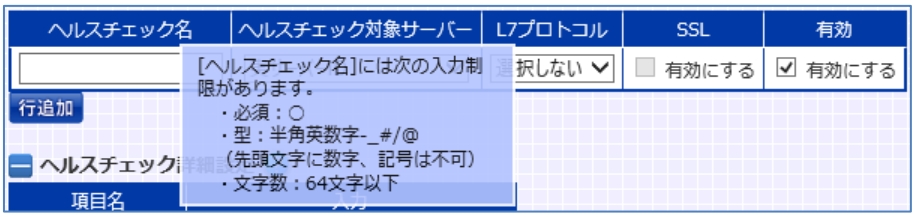
3.1.3.3 ヘルプボタン

WEB 管理画面の設定画面には、項目毎にヘルプボタンが用意されています。クリックすると、項目説明が表示されます。

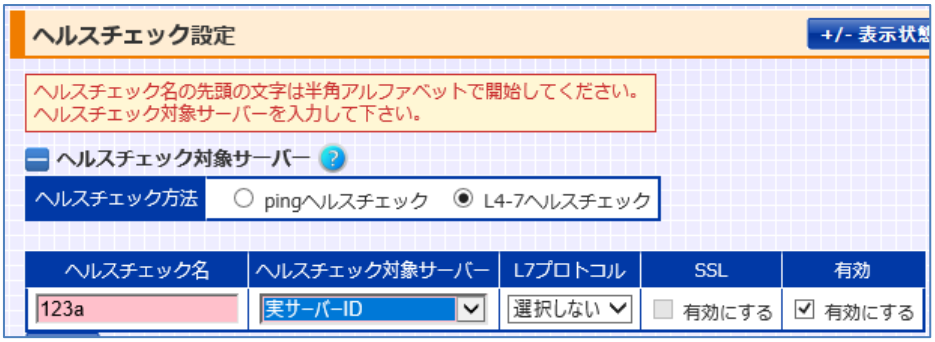


3.1.3.4 入力値チェック

各設定テーブルの項目名にマウスオーバーすると、該当項目の入力範囲や入力制限が表示されます。

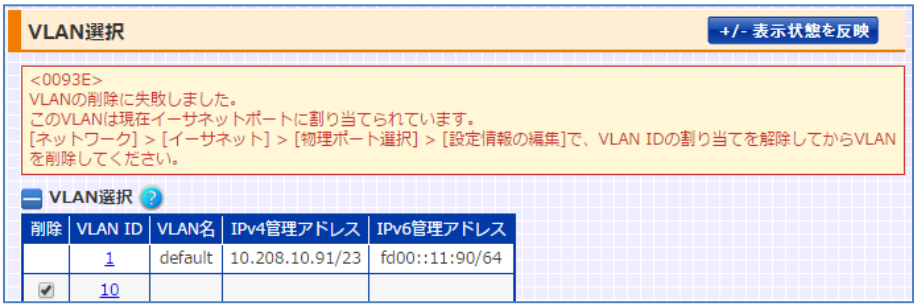


また、入力制限に違反する入力には、設定画面上部にエラーメッセージが表示されます。



3.1.3.5 コマンド実行エラー

設定の依存関係や、機器の内部エラー等により設定変更が失敗した場合、以下のように設定画面上部にエラーメッセージが表示されます。



3.1.4 入力制限

■入力できる文字
入力値に全角文字は使用できません。

■引用符を使用する際の制限
入力文字列内に単一引用符(')や二重引用符(")を使用する場合は、バックスラッシュ(¥)でエスケープし、更に二重引用符で囲んで使用してください。
例）"aaa¥"bbb"

■文字列パラメーター末尾の入力制限
入力文字列の末尾にバックスラッシュ(¥)を入力することできません。
例）abc¥　　←失敗します

ポイント

入力のミス等により画面に異常が見られた場合、再度同じ画面に入り直してください。

3.2 トップ画面

WEB 管理画面へログインすると初めに表示される画面で、システム情報や簡易的な機器状態を表示します。また、画面左上の Netwiser ロゴをクリックすると、どの画面からでもトップ画面に遷移することが可能です。

■システム情報

ホスト名	本製品のホスト名
ユーザーアカウント名	ログイン時に指定したユーザーアカウント名
シリアル番号	本製品のシリアル番号
ファームウェアバージョン	ファームウェアバージョンと、ファームウェアの作成された日付
ブート領域	起動システムのブート領域
冗長状態	現在の VRRP 状態 ※「無効」、「Master」、「Backup」
現在の時刻	本製品のシステムクロック
システム起動時間	起動してからの時間

■デバイス情報
現在の CPU 使用率とメモリー使用率をグラフで表示します。
本数値はトップ画面にアクセスした時点での数値です。

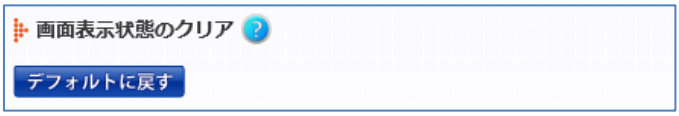
■負荷分散状態一覧
構成した仮想サーバーの負荷分散状態を表示します。
本数値はトップ画面にアクセスした時点での数値です。

■ヘルスチェック情報
DOWN 状態にあるヘルスチェックポリシーを表示します。
本表示はトップ画面にアクセスした時点でのヘルスチェック状態です。

■画面表示状態の一括定義
お使いのネットワーク環境に沿った設定ポリシーを入力する事で、設定画面における不必要な設定項目を非表示にし、設定画面の表示をより簡潔にします。
本項目は Admin 権限でログインした場合にのみ表示されます。
詳しくは、「3.6画面カスタマイズ機能」を参照してください。

■画面表示状態（ログ参照）の定義
Admin 権限以外の権限のユーザーをログ参照画面へ遷移できないように画面の表示状態を変更することが可能です。
詳しくは、「3.6.3ログ参照画面へのアクセス制限」を参照してください。

■画面表示状態のクリア
Admin 権限のユーザーは、上述した「画面表示状態の一括定義」や、後述する設定画面カスタマイズ機能（「3.6画面カスタマイズ機能」参照）により、設定画面の各項目に対して表示/非表示を定義できます。
これらの表示状態を一括で初期状態（全て表示）に戻すには、本項目の「デフォルトに戻す」ボタンを押下します。



■ログアウト

「ログアウト」ボタンをクリックしてください。ログアウトページを表示しWEB 管理画面よりログアウトします。また、他のユーザーでログインしなおす場合は、ログアウト後に Web ブラウザーを一旦終了させてから再度ログインしてください。

3.3 設定画面について

本製品の WEB 管理画面では、設定メニューのサブメニュー項目から各設定画面に遷移して設定変更を行います。ただし、設定モードが設けられているコマンドなどでは、設定ポリシーを選択してから設定画面に遷移する場合もあります。本項では、設定ポリシー等の選択画面が設けられている画面について、設定画面への遷移方法を説明します。

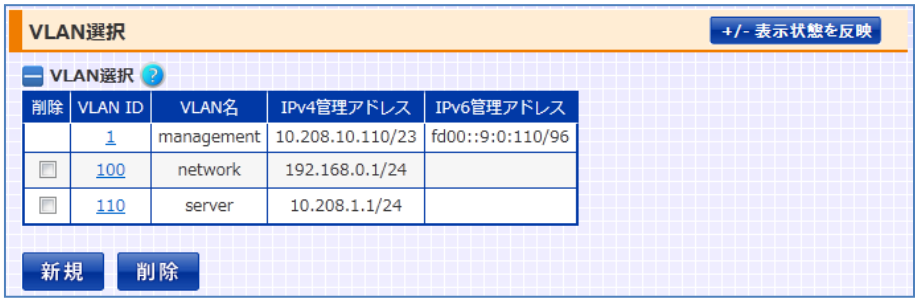
3.3.1 VLAN 選択

場所: 設定 ＞ ネットワーク ＞VLAN

VLAN 設定画面へ遷移するための画面です。

新規の VLAN ID を登録する場合は「新規」ボタンを押下します。設定済みの VLAN ID に対して設定を変更する場合、VLAN ID のリンクを押下します。

以上により、VLAN 設定画面への遷移が可能です。



また、削除する場合は任意の VLAN ID を選択して「削除」ボタンを押下します。

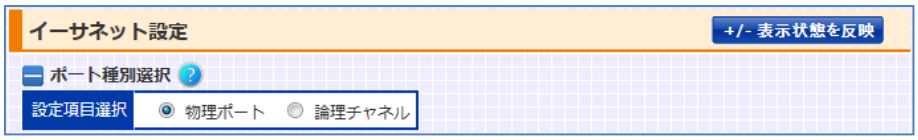
3.3.2 イーサネット設定

場所: 設定 > ネットワーク > イーサネット

イーサネットポート、または論理チャネルの設定画面へ遷移するための画面です。(SX-3990 は設定不要となります)

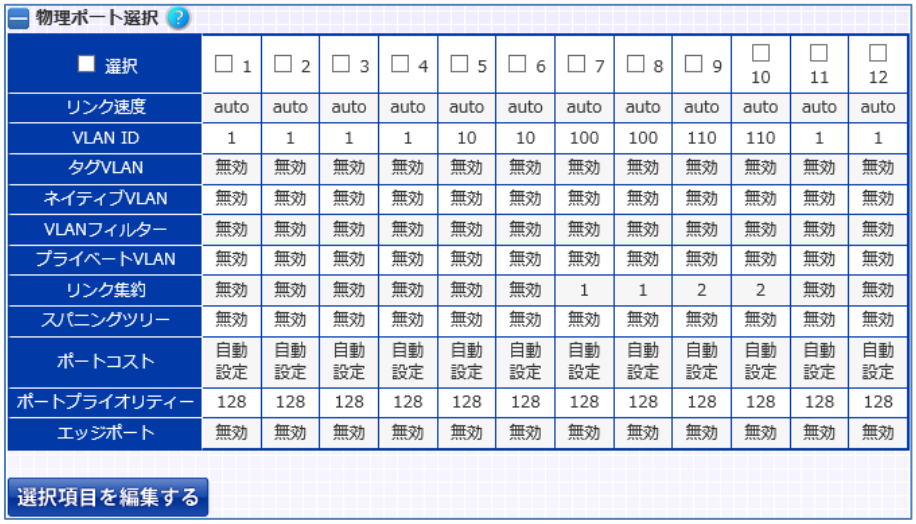
■ポート種別選択

変更する設定について、イーサネットポートか、論理チャネルかを選択します。
「論理チャネル」は、登録済みの論理チャネル設定が存在する場合のみ選択肢として表示されます。



■イーサネットポート選択

「ポート種別選択」で「イーサネットポート」が選択された場合表示されます。
全てのイーサネットポートの設定を一覧表示します。
「選択」欄から設定したいイーサネットポートを選択します。
イーサネットポートは複数選択可能で、「選択」チェックボックスを選択した場合、全てのイーサネットポートが選択されます。
任意のイーサネットポートを選択し、「選択項目を編集する」を押下すると、設定情報の変更画面が表示されます。
「選択項目を編集する」押下後は、「ポート種別選択」、「イーサネットポート選択」ともに変更不可になります。


物理ポート選択

選択	1	2	3	4	5	6	7	8	9	10	11	12
リンク速度	auto	auto	auto	auto	auto	auto	auto	auto	auto	auto	auto	auto
VLAN ID	1	1	1	1	10	10	100	100	110	110	1	1
タグVLAN	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効
ネイティブVLAN	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効
VLANフィルター	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効
プライベートVLAN	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効
リンク集約	無効	無効	無効	無効	無効	無効	1	1	2	2	無効	無効
スパニングツリー	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効
ポートコスト	自動設定	自動設定	自動設定	自動設定	自動設定	自動設定	自動設定	自動設定	自動設定	自動設定	自動設定	自動設定
ポートプライオリティー	128	128	128	128	128	128	128	128	128	128	128	128
エッジポート	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効	無効

選択項目を編集する

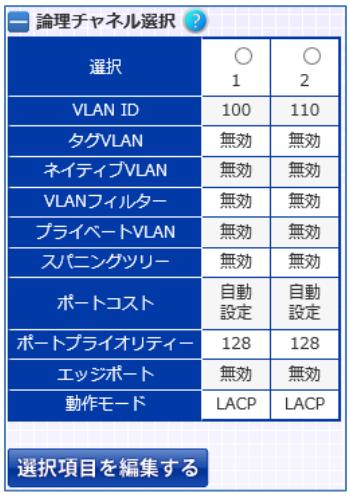
■論理チャネル選択

「ポート種別選択」で「論理チャネル」が選択された場合表示されます。

全ての論理チャネルの設定を一覧表示します。

「選択」欄から設定したい論理チャネルを選択します。

任意の論理チャネルを選択し、「選択項目を編集する」を押下すると、設定情報の変更画面が表示されます。


論理チャネル選択

選択	1	2
VLAN ID	100	110
タグVLAN	無効	無効
ネイティブVLAN	無効	無効
VLANフィルター	無効	無効
プライベートVLAN	無効	無効
スパニングツリー	無効	無効
ポートコスト	自動設定	自動設定
ポートプライオリティー	128	128
エッジポート	無効	無効
動作モード	LACP	LACP

選択項目を編集する

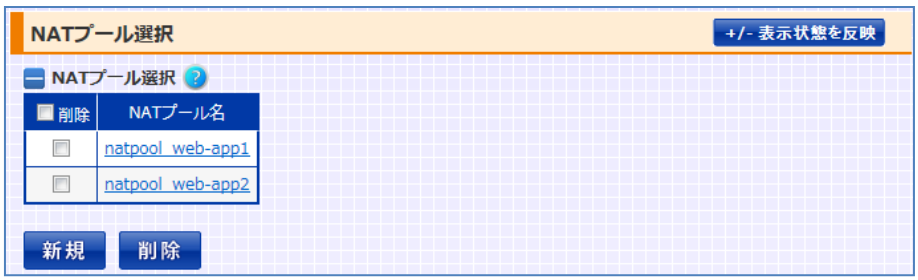
3.3.3 NAT プール選択

場所: 設定 ＞ バランシング ＞NAT プール ＞NAT プール

NAT プール設定画面へ遷移するための画面です。

新規の NAT プールポリシーを登録する場合は「新規」ボタンを押下します。設定済みの NAT プールポリシーに対して設定を変更する場合、NAT プール名のリンクを押下します。

以上により、NAT プール設定画面への遷移が可能です。



また、削除する場合は任意の NAT プール名を選択して「削除」ボタンを押下します。

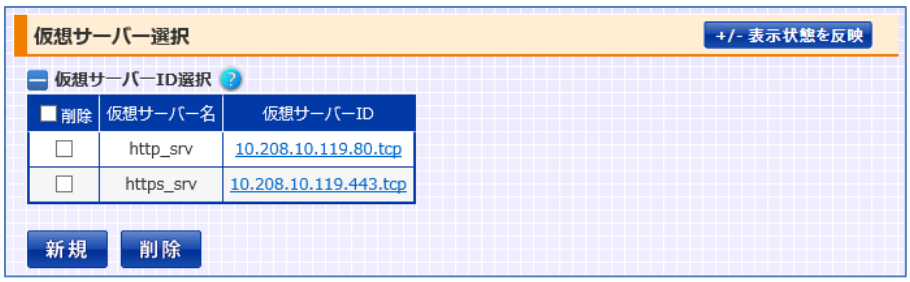
3.3.4 仮想サーバー選択

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー

仮想サーバー設定画面へ遷移するための画面です。

新規の仮想サーバーを登録する場合は「新規」ボタンを押下します。設定済みの仮想サーバーに対して設定を変更する場合、仮想サーバーID のリンクを押下します。

以上により、仮想サーバー設定画面への遷移が可能です。



また、削除する場合は任意の仮想サーバーID を選択して「削除」ボタンを押下します。

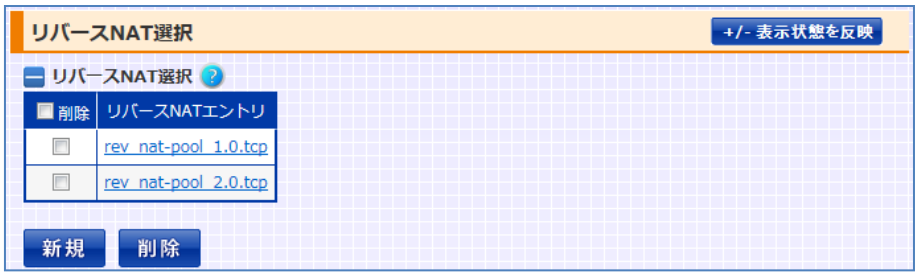
3.3.5 リバース NAT 選択

場所: 設定 > バランシング > 仮想サーバー > リバース NAT

リバース NAT 設定画面へ遷移するための画面です。

新規のリバース NAT を登録する場合は「新規」ボタンを押下します。設定済みの仮想サーバーに対して設定を変更する場合、リバース NAT エントリーのリンクを押下します。

以上により、リバース NAT 設定画面への遷移が可能です。



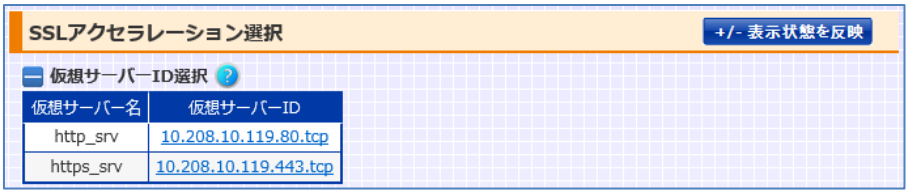
また、削除する場合はリバース NAT エントリーを選択して「削除」ボタンを押下します。

3.3.6 SSL アクセラレーション選択

場所: 設定 ＞ バランシング ＞SSL アクセラレーション ＞SSL アクセラレーション

SSL アクセラレーション設定画面に遷移するための画面です。
SSL アクセラレーションを行う際、SSL アクセラレーション設定画面で仮想サーバーへの SSL ポリシー割り当てや使用する暗号スイート等の詳細設定を行う必要があります。

任意の仮想サーバーへのリンクを押下することで、SSL アクセラレーション設定画面への遷移が可能です。



3.3.7 ヘルスチェック選択

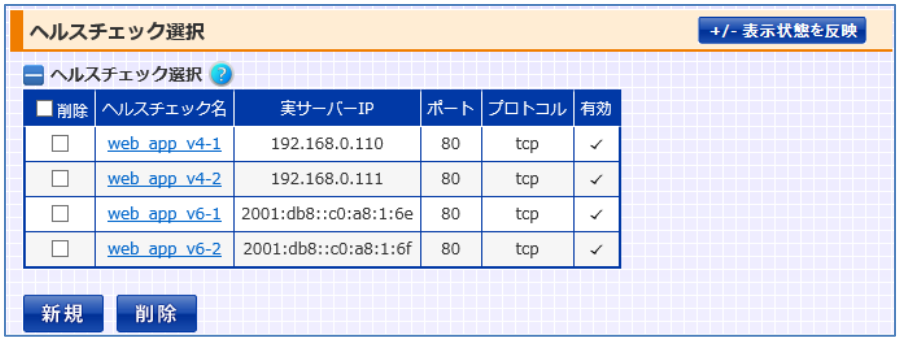
場所: 設定 > ヘルスチェック > ヘルスチェック設定

ヘルスチェック設定画面へ遷移するための画面です。

新規のヘルスチェックポリシーを登録する場合は「新規」ボタンを押下します。

設定済みのヘルスチェックポリシーに対して設定を変更する場合、ヘルスチェック名のリンクを押下します。

以上により、ヘルスチェック設定画面への遷移が可能です。



また、削除する場合はヘルスチェック名を選択して「削除」ボタンを押下します。

3.4 設定数制限

本項では、各種設定の登録件数制限をまとめて記します。

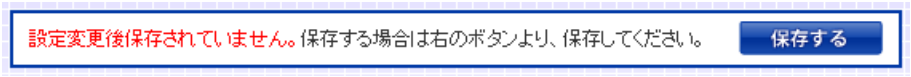
ネットワーク		
	VLAN ID	128 件
	仮想 IP アドレス	512 件 ＊ IPv4 256 件 IPv6 256 件
	MAC テーブル	128 件
	ARP テーブル	128 件
	NDP テーブル	128 件
	ルーティングテーブル	128 件
パケットフィルタリング		
	IPv4 アクセスリスト	128 件 ＊ IPv4, IPv6 合計
	IPv4 アクセスリストルール	128 件 ＊アクセスリストポリシー毎
	IPv6 アクセスリスト	128 件 ＊ IPv4, IPv6 合計
	IPv6 アクセスリストルール	128 件 ＊アクセスリストポリシー毎
	MAC アクセスリスト	128 件
	MAC アクセスリストルール	128 件 ＊アクセスリストポリシー毎
ファイアウォール		
	VLAN リスト	128 件 ＊ VLAN, イーサネットポート合計
	VLAN リストルール	127 件 ＊ルールリストポリシー毎
	イーサネットポートリスト	128 件 ＊ VLAN, イーサネットポート合計
	イーサネットポートリストルール	127 件 ＊ルールリストポリシー毎
SSL		
	SSL 証明書	256 件
バランシング		
実サーバー		
	実サーバーID	512 件 ＊ IPv4 256 件 IPv6 256 件
	sorry コンテンツインポート	32 件
NAT プール		

NAT プール設定	
NAT プール名	256 件
NAT プールアドレス設定	16 件 *1
仮想サーバー	
仮想サーバー設定	
仮想サーバーID 設定	512 件 ＊ IPv4 256 件 IPv6 256 件
IP スイッチングルール	256 件 ＊ 仮想サーバー毎
URL スイッチングルール	32 件 ＊ 仮想サーバー毎
URL リダイレクト設定	
403 応答設定	
実サーバーバインド	256 件 ＊ 仮想サーバー毎
ソース NAT フィルター設定	256 件
URL スイッチングルール設定	1024 件
location ルール設定	
リバース NAT	
リバース NAT エントリー	256 件
リバース NAT バインド登録	256 件 ＊リバース NAT ポリシー毎
SSL アクセラレーション	
SSL アクセラレーション設定（SNI 登録数）	32 件 ＊ 仮想サーバー毎
ヘルスチェック	
ヘルスチェック設定	1024 件
ヘルスチェック組み合わせ設定	
システム	
ネットワーク	
IP アドレス名の定義	512 件
SNMP 設定	
SNMP マネージャー設定	4 件
SNMP トラップトリガー設定	16 件
SYSLOG 設定	
SYSLOG サーバーIP アドレス	4 件
宛先メールアドレス	16 件
NTP サーバー	4 件
ユーザー管理	
ユーザーアカウント	4 件
リモートアクセス制御	
web リモートアクセス制御	32 件
telnet リモートアクセス制御	32 件
ssh リモートアクセス制御	32 件

*1 システム全体で登録可能な件数（ただし、仮想サーバーIP アドレスとして登録されているアドレスは登録制限に含まれない）

3.5 設定の保存

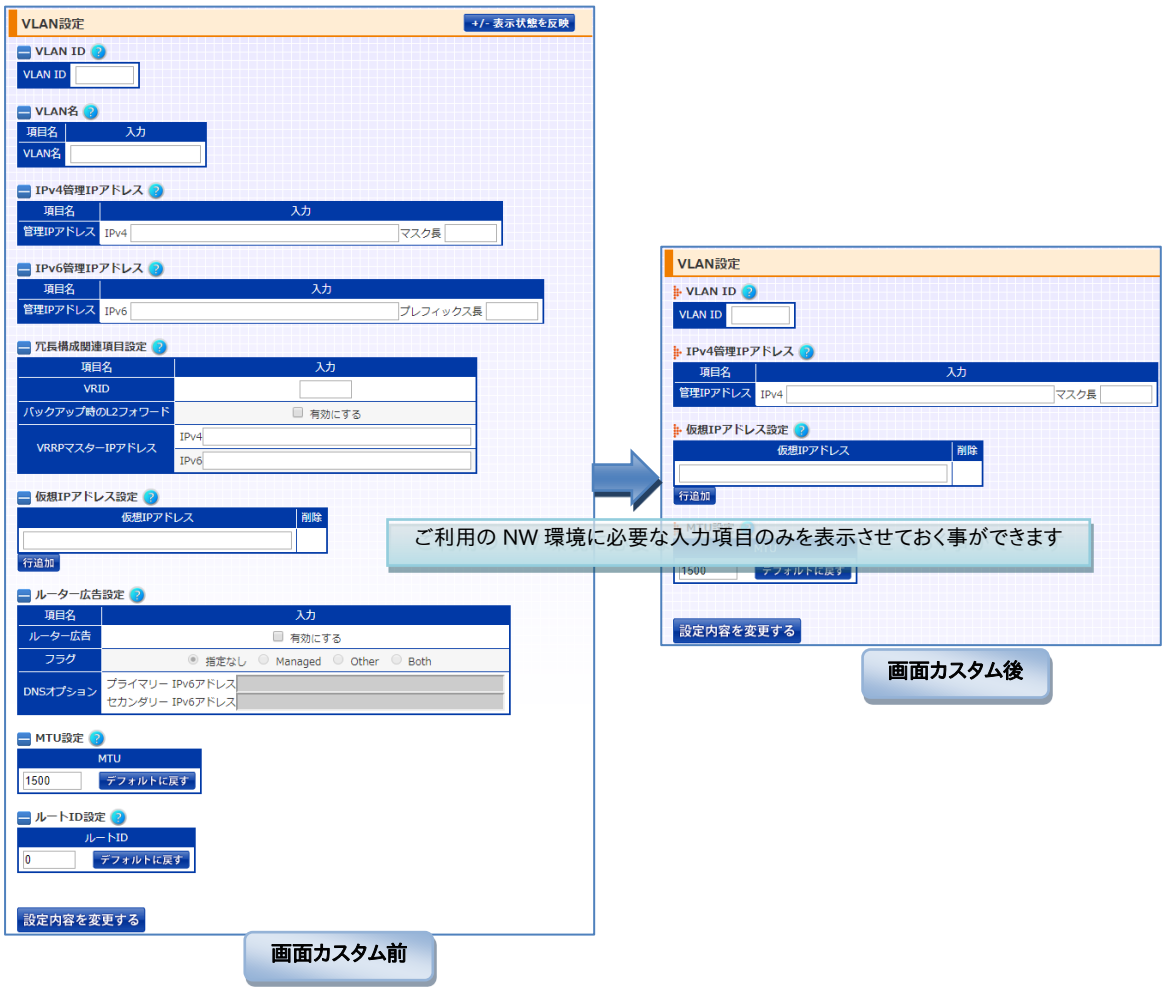
設定が変更された場合、画面上部に以下のメッセージが表示されます。
「保存する」ボタンで設定内容を保存してください。



3.6 画面カスタマイズ機能

設定画面の各項目に関して、表示状態または非表示状態にする事が可能です。

ユーザーは、任意の項目のみを表示させる事により、設定画面をより簡潔でわかり易い画面にしておくことができます。



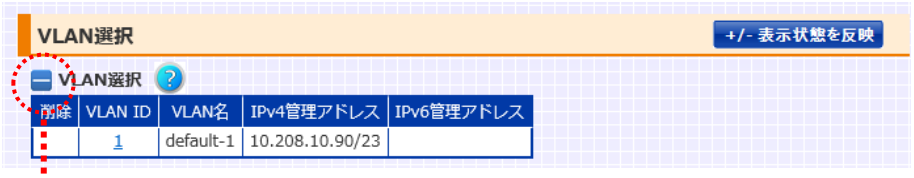
自ら設定変更する場合においても、第三者に設定指示を出す場合においても、より簡潔な画面にしておく事は、設定ミスや勘違いを減らす上で重要です。

ただし、本機能は、画面の表示内容をカスタマイズするための機能であり、Netwiser のネットワーク機器としての動作内容に影響するものではありません。

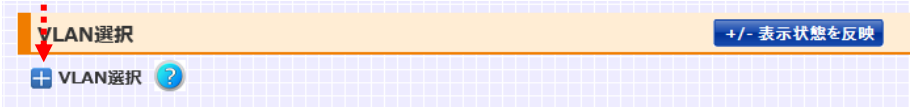
設定を変更する上で必須の操作ではありません。

3.6.1 個別カスタム

設定画面の各表示項目に、「＋」または「－」ボタンが用意されています。
全ての設定項目に初期状態として「－」ボタンが表示されています。
「－」ボタンを押下すると、ボタンは「＋」に変化し、項目表示は非表示状態へと変化します。
これにより、必要のない設定項目やメニュー項目をあらかじめ非表示状態にすることができ、設定画面をより簡潔な表示にしておく事が可能になります。



[表示状態]



[非表示状態]

ポイント

ただし、ユーザーアカウント権限によって、カスタムした際の画面表示に違いがあります。たとえば、Sub-Admin 権限のユーザーにおいては、項目タブも含めた完全な非表示状態となります。
詳細は「3.6.5画面表示とユーザー権限」を参照してください。

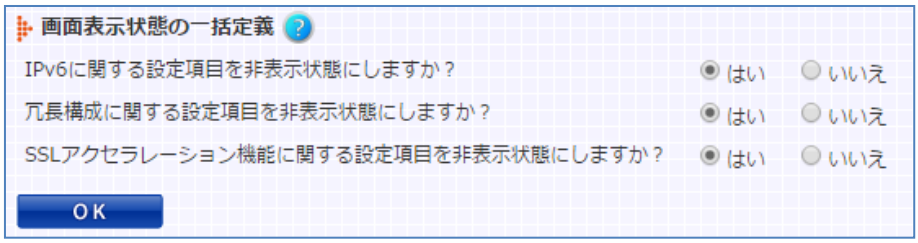
3.6.2 グループカスタム

WEB 管理画面のトップ画面にて、お使いのネットワーク環境に沿った設定ポリシーを入力できます。

WEB 管理画面は、本項目の回答内容を加味し、不必要な設定項目を設定画面上で非表示状態にします。

たとえば、「IPv6 に関する設定項目を非表示状態にしますか？」の設問で「いいえ」を選択した場合、IPv6 を利用する環境でのみ設定が必要な項目は、非表示状態になります。

デフォルト設定では、全ての設問に対して「いいえ」が選択されています。



設問内容について説明します。

- **IPv6 に関する設定項目を非表示状態にしますか？**
  お使いのネットワーク環境で IPv6 をご使用にならない場合、「はい」を選択します。
- **冗長構成に関する設定項目を非表示状態にしますか？**
  本製品は、機器間で冗長構成を形成する事が可能です。
  本製品を冗長構成で利用しない場合、「はい」を選択します。
- **SSL アクセラレーション機能に関する設定項目を非表示状態にしますか？**
  本製品は、SSL アクセラレーション機能があります。
  SSL アクセラレーション機能を利用しない場合、「はい」を選択します。

これらの設問に対する入力内容によって設定画面の表示状態が変化します。

本機能は画面表示に関する操作であり、機器の動作に直接影響するものではありませんので未回答でも問題ありません。

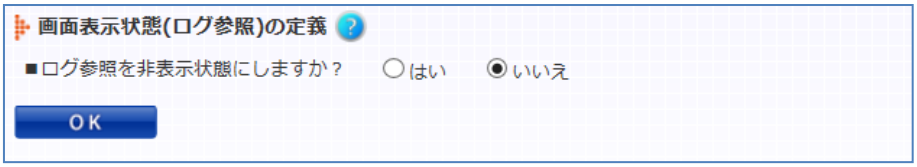
その場合、設定画面上の全ての項目が表示状態のままとなります。

3.6.3 ログ参照画面へのアクセス制限

Admin 権限のユーザーにのみログ情報の参照を許可するよう設定することが可能です。

設定を変更する場合、WEB 管理画面に Admin 権限でログインし、トップ画面を表示します。

トップ画面には以下の通り、「画面表示状態（ログ参照）の定義」の項目が表示されます。



デフォルト設定では、設問「ログ参照を非表示状態にしますか？」に対して「いいえ」が選択されています。

「はい」を選択し「OK」ボタンを押下することで、設定変更が完了します。

設定変更後に、Admin 権限以外の権限で WEB 管理画面にログインした場合、以下のように画面上部の「ログ参照」メニューが非表示となります。

ポイント

本設定は、WEB 管理画面の表示状態を操作するための設定です。

CLI にログインした際の動作には影響しません。

3.6.4 表示状態の反映と保存

設定画面タイトルバーの右側に、「+/- 表示状態を反映」ボタンがあります。
表示、非表示状態を操作し、「+/- 表示状態を反映」ボタンを押下すると、画面更新後も画面の表示状態が反映されたままになります。

また、「設定内容を変更する」ボタンの押下など、設定変更に関する操作を実施した際にも、画面表示状態が反映されます。
ただし、再起動後も画面状態を保持しておく場合、設定保存する必要があります。
設定の保存は「3.5設定の保存」を参照してください。

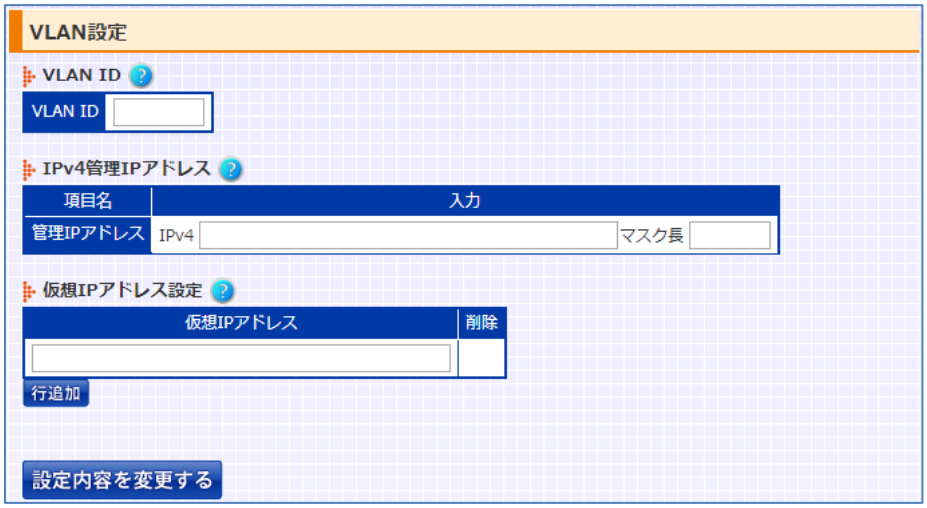
3.6.5 画面表示とユーザー権限

WEB 画面の表示状態を変更できない Sub-Admin 権限のユーザーアカウントを作成できます。
「＋」または「－」ボタンは、Admin 権限のユーザーであればいつでも変更できますが、Sub-Admin 権限のユーザーアカウントは、画面表示状態の変更を行う事ができません。
ユーザーアカウントの作成は「3.7.2パスワードの変更・ユーザーアカウントの管理」を参照してください。

Sub-Admin 権限のユーザーが WEB 設定画面にログインすると、非表示状態にされた設定項目が完全に画面表示されなくなります。

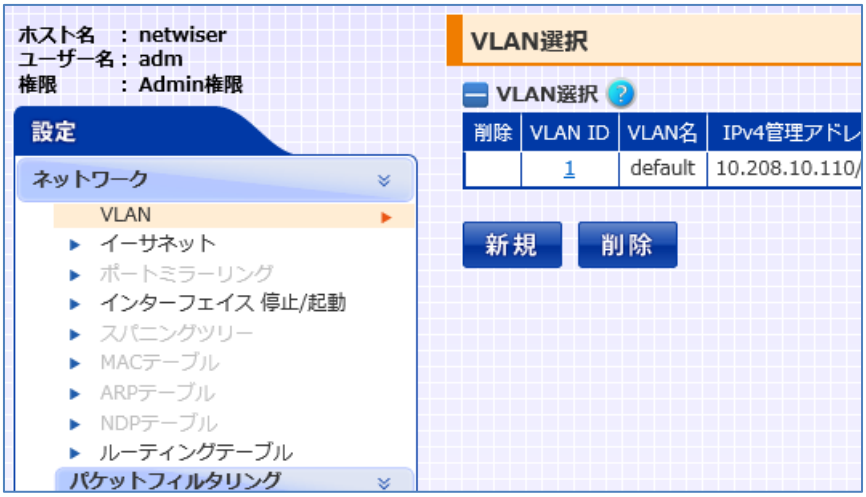
たとえば、VLAN 設定画面で、「VLAN ID」、「IPv4 管理 IP アドレス」、「仮想 IP アドレス」のみを表示状態にした場合において、Admin 権限と Sub-Admin 権限の画面表示の違いを比較します。

[Admin 権限ユーザーの表示]

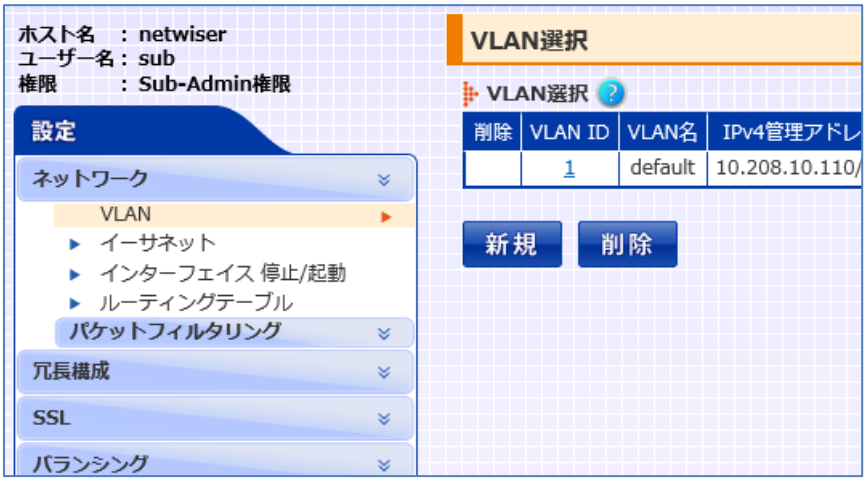


[Sub-Admin 権限ユーザーの表示]

また、各画面内の全項目を非表示状態にした場合、画面左のサブメニューに変化が加わります。
以下では、「ポートミラーリング」、「スパニングツリー」、「MAC テーブル」、「ARP テーブル」、「NDP テーブル」の画面内の全項目を非表示状態にした場合において、Admin 権限と Sub-Admin 権限の画面表示の違いを比較します。



[Admin 権限ユーザーの表示]



[Sub-Admin 権限ユーザーの表示]

Admin 権限ユーザーの場合、メニュー項目の文字列がグレーに変化し、任意のメニュー項目が見え難くなります。
Sub-Admin 権限ユーザーの場合、任意のメニュー項目が表示されなくなります。

3.6.6 表示状態のインポート/エクスポート

現在の画面表示状態が格納された設定ファイルを取り出したり、取り出した設定ファイルを取り込む事ができます。

画面表示状態の取り出しは「5.3.2.2画面表示情報のエクスポート」を参照してください。
画面表示状態の取り込みは「5.3.1.2画面表示情報のインポート」を参照してください。

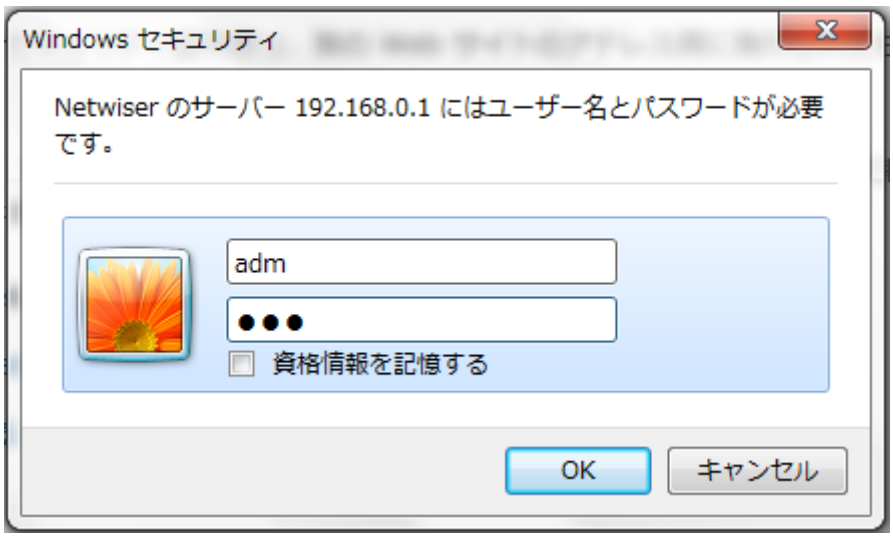
ポイント 画面表示状態の設定情報は「全ての設定情報」に含まれます。

3.7 初期設定

本章では、システムの初期状態から設定を始める場合について、本製品に対してネットワーク経由でアクセス可能にするまでの流れを説明します。

3.7.1 デフォルトユーザーアカウント / デフォルトアドレス

本製品には、初期ユーザーアカウントとして"adm"が登録されています。
パスワードも同様に"adm"です。
また、初期状態では全てのイーサネットポートに対してアドレス
'192.168.0.1/24'（VLAN 1）が割り当てられています。



ブラウザを開き、アドレスにシステム IP アドレスを指定するとトップページが表示されます。
WEB 管理画面へは HTTP および HTTPS プロトコルでのアクセスが可能ですが、システムの初期状態では HTTP でのアクセスは全て HTTPS へリダイレクトされます。
リダイレクト機能の解除はリモートアクセス制御画面で行うことが可能です。
詳細は、「3.7.5リモートアクセスの許可」を参照してください。

3.7.2 パスワードの変更・ユーザーアカウントの管理

場所: 設定 > システム > ユーザー管理 > ユーザーアカウント

WEB 管理画面からユーザーアカウントの追加、削除を行います。

■ユーザーアカウント追加

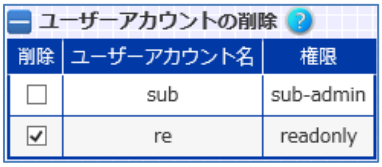
① ユーザーアカウント名
新規に登録するアカウント名を入力します。

② 権限
新規に登録するユーザーアカウントの権限を選択します。
Admin 権限のユーザーは WEB 管理画面の権限制限において、一切の制限を受けません。
Readonly 権限のユーザーは機器の設定変更を実施する事ができません。
Subadmin 権限のユーザーは、画面カスタム操作を行う事ができません。
その他は Admin 権限のユーザーと同等の権限を持ちます。
画面カスタム操作については、「3.6画面カスタマイズ機能」を参照してください。

③ 新規パスワード、パスワード再入力（確認）
ログインパスワードを定義します。

■ユーザーアカウント削除

削除したいユーザーアカウントを選択します。



ポイント

自アカウント（現在自らログインしているアカウント）は削除できません。
自アカウントを削除したい場合、別アカウントでログインし直す必要があります。

ポイント

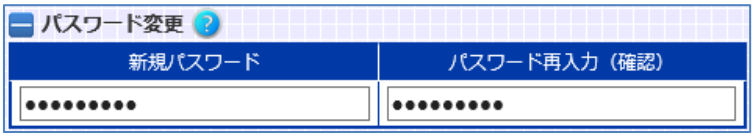
登録済みのユーザーアカウントに関して、権限を変更することはできません。
一度削除してから再度登録し直してください。

また、自アカウントのパスワードを変更したい場合はパスワード画面へ遷移します。

場所：設定 ＞ システム ＞ ユーザー管理 ＞ パスワード変更

■パスワード変更

自アカウントのパスワードを変更します。



3.7.3 機器 IP アドレスの変更

システムの初期状態では全てのポートが VLAN 1 に定義されています。
VLAN に設定されている管理 IP アドレスは、削除または変更することが可能です。

場所: 設定 ＞ ネットワーク ＞VLAN＞VLAN 選択 ＞VLAN 設定

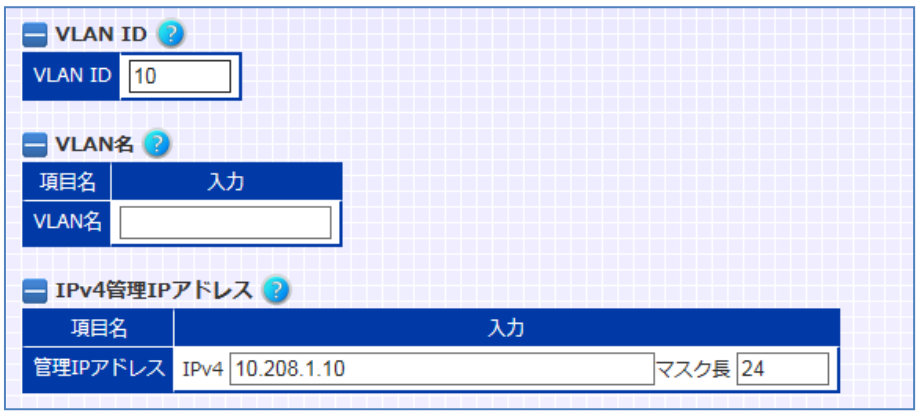
VLAN 選択画面から、「新規」ボタンで VLAN 設定画面に遷移し、VLAN ID の作成と、管理 IP アドレスの設定を行います。

① VLAN ID
任意の VLAN ID を入力します。

② VLAN 名
VLAN を任意の文字列で名前付けします。設定しなくても問題ありません。

③ 管理 IP アドレス（IPv4）、管理 IP アドレス（IPv6）
IPv4 アドレスとサブネットマスク長か IPv6 アドレスとプレフィックス長、またはその全てを入力します。

以下、例として VLAN 10 に管理用の IPv4 アドレスを割り当て、さらにイーサネットポート10を VLAN 10 に割り当てます。また、最後に VLAN 1 の IP アドレスを削除します。



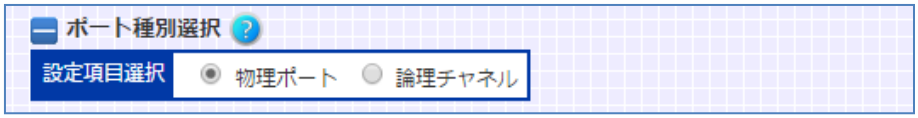
場所：設定 ＞ ネットワーク ＞ イーサネット

イーサネットポート10に VLAN10 を割り当てます。

① ポート種別選択

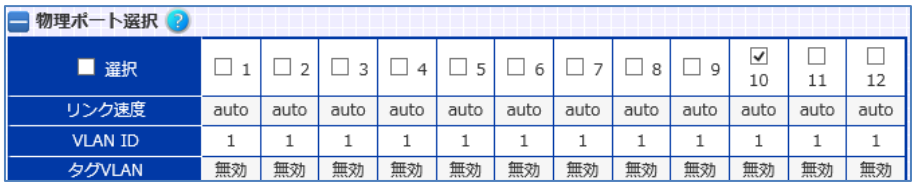
設定変更を行うインターフェイス種別として「イーサネットポート」を選択します。

論理チャネル設定がされていない場合、「論理チャネル」の選択項目は表示されません。



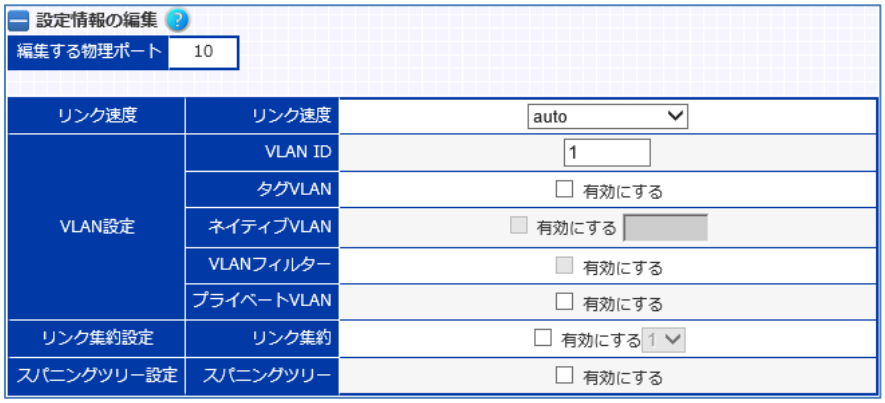
② イーサネットポート選択

設定変更したいイーサネットポート番号を選択します。



③ 設定情報の編集 ＞VLAN 設定 ＞VLAN ID

ポートに割り当てたい VLAN ID を入力します。

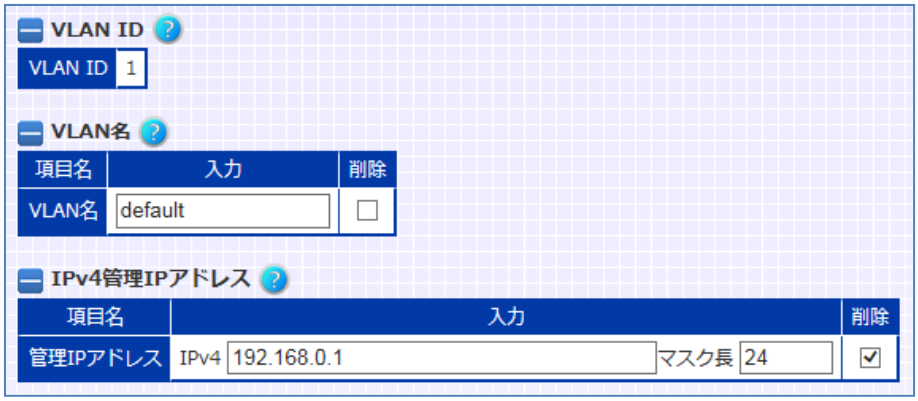


場所: 設定 > ネットワーク > VLAN > VLAN 選択 > VLAN 設定

VLAN1に登録されているシステムの初期アドレスを削除します。

■VLAN 設定 > 管理 IP アドレス

削除したい IP アドレス行の「削除」を選択します。



VLAN インターフェイスの割り当て状況は、機器情報画面の「ネットワーク > VLAN」で確認できます。

注意

IP アドレスにリンクローカルアドレス（IPv4：169.254.0.0/16, IPv6：fe80::/10）を指定しないでください。

これは、機器 IP アドレスだけではなく、IP アドレスを指定する必要のある全ての設定において共通の制限です。

3.7.3.1 管理専用ポートの定義

任意の単一ポートを管理専用ポートとして設定できます。管理専用ポートは管理 IP アドレスへのアクセスや、そのポートを経由するアクセスを制限します。

場所: 設定 > バランシング > ネットワーク > バランシングポート定義

■バランシングポート定義（イーサネットポート）

① 定義

管理専用ポートとして定義したいポートで「管理専用ポート」を選択します。

その他の選択肢についての詳細は「3.17 接続先ネットワーク種別」を参照してください。

以下、例としてイーサネットポート10を管理専用ポートとして定義します。

バランシングポート定義（物理ポート）

物理ポート番号	定義
1	クライアント/サーバーポート
2	クライアント/サーバーポート
3	クライアント/サーバーポート
4	クライアント/サーバーポート
5	クライアント/サーバーポート
6	クライアント/サーバーポート
7	クライアント/サーバーポート
8	クライアント/サーバーポート
9	クライアント/サーバーポート
10	管理専用ポート
11	クライアント/サーバーポート
12	クライアント/サーバーポート

以下、管理専用ポートの動作を説明します。

■管理 IP アドレスへのアクセスを制限する

管理専用ポートに指定されたポートが所属する VLAN の管理 IP アドレス、または冗長アドレスへは、管理専用ポートからのみアクセス可能であり、その他のポートからアクセスすることはできません。

また、管理専用ポートでないポートが所属する VLAN の管理 IP アドレスへは、管理専用ポートからアクセスすることはできません。

■管理専用ポートを経由するアクセスを制限する
管理専用ポート以外のポートで受信したパケットを、管理専用ポートへ転送しません。
また、管理専用ポートで受信したパケットを、管理専用ポート以外のポートへ転送しません。

■負荷分散パケットの遮断
管理専用ポートでは、負荷分散パケットを送受信しません。

管理専用ポートを定義する際には、以下のような制限があります。
- ✓ 管理専用ポートは任意の 1 ポートにのみ設定可能です
- ✓ 管理専用ポートが所属する VLAN に、その他のポートを割り当てることはできません
- ✓ 管理専用ポートが所属する VLAN には、必ず管理 IP アドレスが設定されている必要があります
- ✓ 管理専用ポートが所属するVLAN に、仮想サーバーIP を設定することはできません
- ✓ 管理専用ポートはアクセスポートである必要があります
- ✓ 管理専用ポートは論理チャネルに所属することはできません
- ✓ 管理専用ポートに対してスパニングツリーの設定をすることはできません

⚠ 注意

管理専用ポートの設定が存在し、かつ特定のポートをトランクポートに設定する場合は、VLAN フィルターの設定より、許可する VLAN タグの ID を明示的に設定し、その際に、管理専用ポートの所属するVLAN の ID を除外してください。
VLAN フィルターの設定は「3.9.3 タグ VLAN の設定」を参照してください。

3.7.4 デフォルトルーターと経路情報の設定

機器のルーティングテーブルを設定するにはルーティングテーブル設定画面に遷移します。

場所: 設定 > ネットワーク > ルーティングテーブル

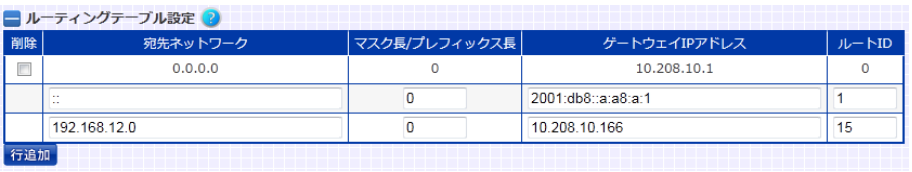
WEB 管理画面から経路情報の設定を行います。

■ルーティングテーブル設定

① 宛先ネットワーク、マスク/プレフィックス長
宛先ネットワークアドレスを入力します。
デフォルトルーターの IPv4 アドレスを設定する場合、「宛先ネットワークアドレス」に'0.0.0.0'、「マスク/プレフィックス長」に 0 を入力します。
IPv6 アドレスであればそれぞれ':: '、0 を入力します

② ゲートウェイアドレス
ゲートウェイアドレスを入力します。

③ ルート ID
ルーティングテーブルのルート ID を設定します。



本製品ではルーティングテーブルをルート ID 単位に複数持つことができます。
設定できるルート ID の範囲は 0 から 15 です。
ルート ID を指定しない場合はルート ID 0 が設定されます。
ルート ID は VLAN 設定モード、仮想サーバー設定モード、またはリバース NAT 設定モードで使用することができます。
各モードでは使用するルーティングテーブルのルート ID を指定できます。

ポイント

ルート ID は VLAN 設定画面、仮想サーバー設定画面、リバース NAT 設定画面で使用することができます。
各画面では使用するルーティングテーブルのルート ID を指定できます。

ポイント

TRACEROUTE テストを除き、自機発のパケット(PING テスト, ヘルスチェック等)にはルート ID を指定することができません。ルート ID 0 が使用されます。

ポイント

Netwiser に設定されているどの VLAN のネットワークアドレスにも合致しない IP アドレスを、ゲートウェイアドレスに指定することはできません。
また、ルーティングエントリー登録後に、ゲートウェイアドレスが合致するネットワークを持つ VLAN に対して以下の変更を行いたい場合、該当のルーティングエントリーを削除してから設定を変更する必要があります。

- ✓ 該当の VLAN を削除したい場合
- ✓ 該当の VLAN に設定された IP アドレスを削除したい場合
- ✓ 該当の VLAN に設定された IP アドレスを、別のネットワークアドレスへ変更したい場合

ポイント

本製品の管理 IP アドレスへの接続は VLAN に設定されているルート ID が使用されません。ルート ID 0 が使用されます。
PING への応答は VLAN に設定されているルート ID が使用されます。

3.7.5 リモートアクセスの許可

デフォルト設定では、telnet を使用した本製品へのリモートアクセスは許可されていません。更に、WEB 管理画面への HTTP アクセスは HTTPS へリダイレクトされます。
本製品への telnet でのアクセスや、WEB 管理画面への HTTP アクセスを許可するには、リモートアクセス制御画面に遷移します。

場所: 設定 > システム > ユーザー管理 > リモートアクセス制御

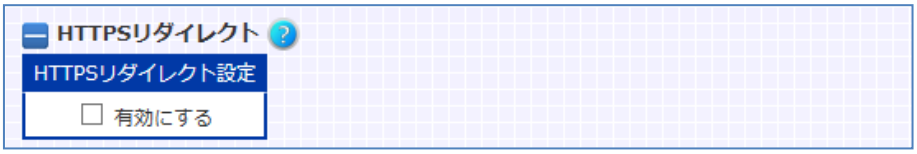
■リモートアクセス制御

① 制御種別
制御対象となるリモートアクセス先の種別を指定します。
「web」、「ssh」、「telnet」はそれぞれ「WEB 管理画面へのアクセス」、「ssh を利用した CLI へのアクセス」、「telnet を利用した CLI へのアクセス」を指します。

② 送信元 IP アドレス、マスク/プレフィックス長
許可するネットワークドレスを定義します。
送信元アドレスに'0.0.0.0'、マスク長に 0 を指定することで、全ての端末か

らのアクセス（IPv4）を許可します。
IPv6も同様に送信元アドレスに'::'、プレフィックス長に0を指定することで、全ての端末からのアクセス（IPv6）を許可します。

■HTTPS リダイレクト
「HTTPS リダイレクト設定」の選択を外すことで、HTTP アクセスに対するリダイレクト機能を無効にします。



ポイント

リモートアクセスフィルターの設定をしても、アクセスリストを使用したフィルタリング設定と相反するルールとなる場合（かつ該当のアクセスリストのフィルタリング設定が有効である場合）、アクセスリストのフィルタリングルールが優先されます。

3.7.6 設定ファイルをインポートする場合

あらかじめ本製品からエクスポートしておいた設定情報を取り込むことが可能です。
本製品への設定情報のインポートは「5.3.1設定情報のインポートとファームウェアアップグレード」を参照してください。

3.8 基本設定

3.8.1 リモート端末設定

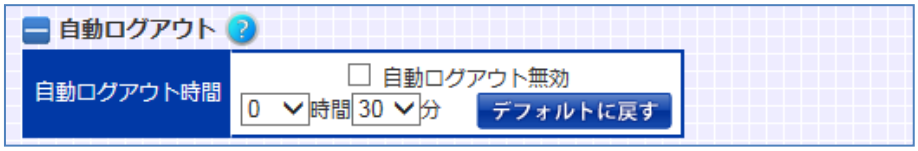
3.8.1.1 自動ログアウト

本製品へのログイン後、WEB 管理画面に対して一定時間操作されなければ自動的にログアウトします。
自動ログアウト時間の変更や無効化を行うには、自動ログアウト画面に遷移します。

場所: 設定 > システム > ユーザー管理 > 自動ログアウト

■自動ログアウト

① 自動ログアウト時間
デフォルトは 10 分です。セキュリティポリシーに合う間隔を設定してください。
自動ログアウト機能を無効にする場合、「自動ログアウト無効」を選択してください。



設定した自動ログアウトタイマーは CLI ログイン時にも適用されます。
WEB 管理画面では、自動ログアウト時間が経過した場合再度パスワードの入力が求められます。

3.8.2 リモートアクセスフィルターの設定

任意のネットワークセグメントからのみ、telnet/ ssh/ web でのアクセスを許可する場合リモートアクセス制御画面に遷移します。

■リモートアクセス制御

① 制御種別

制御対象となるリモートアクセス先の種別を指定します。

「web」、「ssh」、「telnet」はそれぞれ「WEB 管理画面へのアクセス」、「ssh を利用した CLI へのアクセス」、「telnet を利用した CLI へのアクセス」を指します。

② 送信元 IP アドレス、マスク/プレフィックス長

許可するネットワークドレスを定義します。

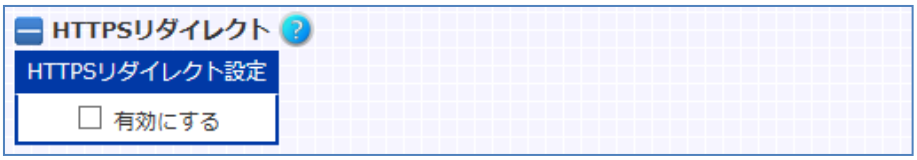
例として、以下のセキュリティポリシーを基に設定例を示します。

- telnet での接続は 192.168.1.110 と 2001:db8::c0:a8:1:6e からのみ許可する
- ssh と HTTP での接続は 192.168.1.0/24 と 2001:db8::/32 のネットワークからのみ許可する

■HTTPS リダイレクト

① HTTPS リダイレクト設定

WEB 管理画面への HTTP アクセスを HTTPS にリダイレクトするには「有効にする」を選択します。



ポイント

リモートアクセスフィルターの設定をしても、アクセスリストを使用したフィルタリング設定と相反するルールとなる場合（かつ該当のアクセスリストのフィルタリング設定が有効である場合）、アクセスリストのフィルタリングルールが優先されます。

3.8.3 日時の設定

本製品のシステムクロックを変更するには日時変更画面へ遷移します。

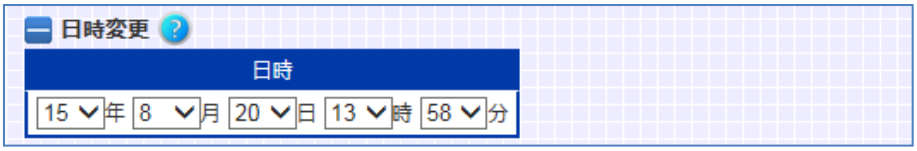
場所: 設定 > システム > 機器情報 > 日時変更

■日時変更

① 日時

画面にアクセスした時点での時刻を表示しています。

変更する場合、任意の日時を選択してください。



3.8.4 サーバーの名前付け

IP アドレスに名前付けすることで、以降の入力を簡略化することが可能です。
名前付けを行うと、設定ファイルに記述される文字列も、名前付け設定で指定した文字列で表示されます。

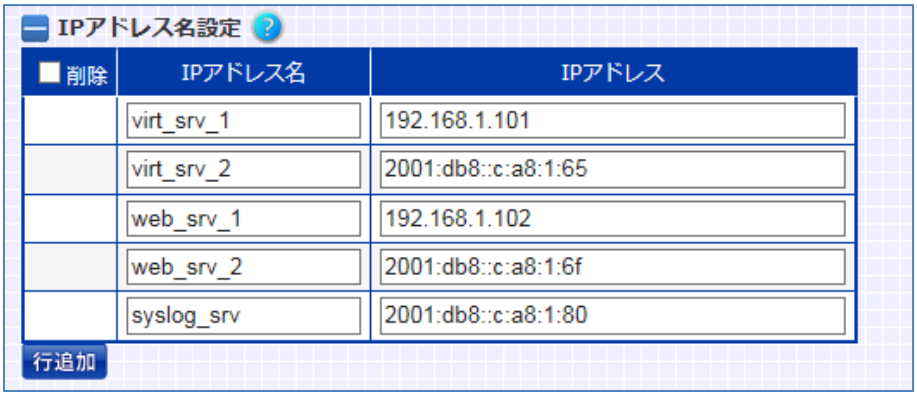
場所: 設定 > システム > ネットワーク > IP アドレス名の定義

IP アドレスの名前付け設定を行います。

■IP アドレス名設定

① IP アドレス名
IP アドレスに付ける名前を入力します。

② IP アドレス
IP アドレス名に紐付ける IP アドレスを入力します。



ポイント

機器IPアドレスやルーティングテーブルエントリーの登録などのように、ネットワークアドレスやサブネットマスク、IPv6 プレフィクスを必要とするアドレスの場合、名前を使用した設定ができません。それらの入力項目は IP アドレス形式で入力してください。

3.8.5 DNS の設定

SSL アクセラレーション機能をお使いの際、クライアント証明書の失効リストを取得するため、取得先サーバーの URL を入力を必要とする場合があります。この際に、本製品が FQDN を使用してサーバーへアクセスするためには、DNS サーバーの IP アドレスを本製品に設定する必要があります。
（失効リストの取得を行わない場合、DNS の設定は不要です）
DNS サーバーの設定を行うには DNS サーバー画面に遷移します。

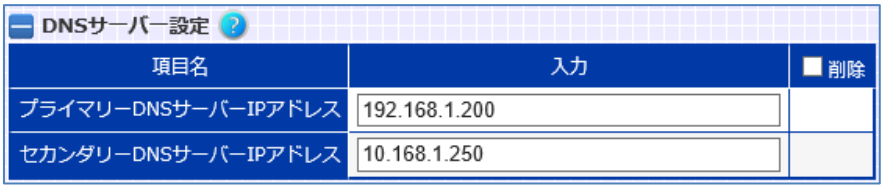
場所: 設定 > システム > ネットワーク > DNS サーバー

DNS サーバーを定義します。

■DNS サーバー設定

① プライマリーDNS サーバーIP アドレス
プライマリーDNS サーバーの IP アドレス（または IP アドレス名）を入力します。

② セカンダリー
セカンダリーDNS サーバーの IP アドレス（または IP アドレス名）を入力します。



ポイント

セカンダリーDNS サーバーの設定は必須ではありませんが、プライマリーDNS サーバーの設定がなく、セカンダリーDNS サーバーのみが設定されている状態では動作しません。

3.8.6 NTP サーバーの設定

NTP サーバーの IP アドレスを設定するには NTP サーバー画面に遷移します。

場所: 設定 > システム > ネットワーク > NTP サーバー

■NTP サーバー設定

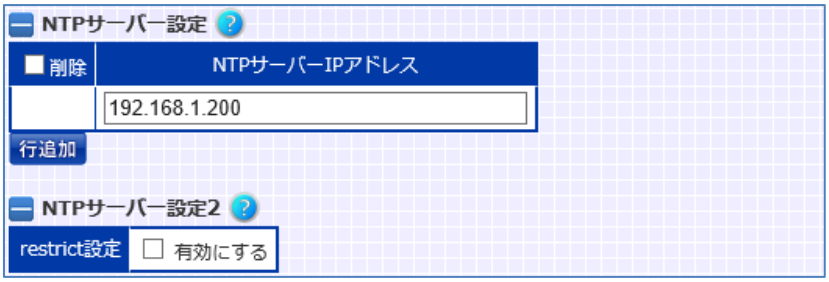
① NTP サーバーIP アドレス

NTP サーバーの IP アドレス（または IP アドレス名）を入力します。

② restrict 設定

本製品は、デフォルト設定では自身が NTP サーバーとしても動作しています。ただし、restrict 設定を有効にすると、設定した NTP サーバー以外との時刻情報の交換を行いません。

restrict 設定は、本製品を NTP サーバーとして利用しない場合において、NTP のセキュリティを確保するために有効です。

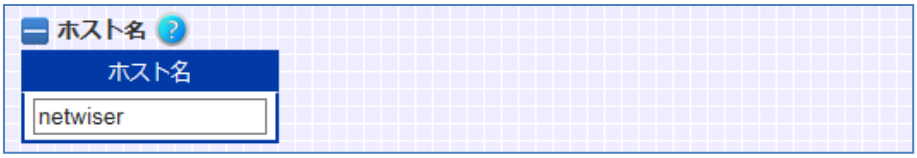


3.8.7 ホスト名の設定

本製品のホスト名はデフォルトで"netwiser"が設定されています。
変更する場合はホスト名画面に遷移します。

場所: 設定 > システム > 機器情報 > ホスト名

■ホスト名
設定したいホスト名を入力します。



3.8.8 LAN ポートの速度固定設定

SX-3950,SX-3945,SX-3940,SX-3920 の場合、LAN ポートのリンク速度はデフォルトでオートネゴシエーションに設定されています。速度を固定する場合はイーサネットポート設定画面に遷移してリンク速度の設定変更を行います。
(SX-3990 では、LAN ポートの速度固定設定は動作しません)

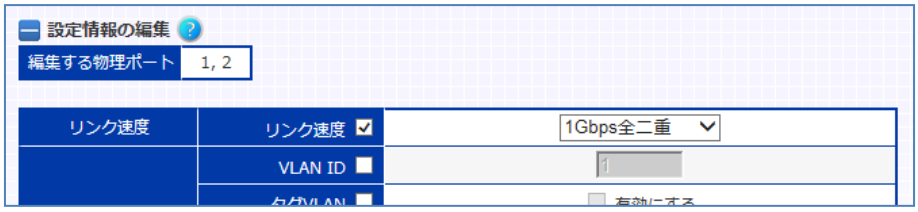
場所: 設定 > ネットワーク > イーサネット

■設定情報の編集(イーサネットポート)

① リンク速度

リンク速度を選択します。

以下の例では、複数のイーサネットポートが指定されているので、項目「リンク速度」を選択してから速度種別を選択しています。



ポイント

speed auto/1000full 設定時には auto MDI/MDI-X で動作しますが、それ以外の設定時は MDI-X で動作します。この場合、他のスイッチと接続する際はクロスケーブルで接続してください。

SX-3950 のポート 11 および 12 の回線速度はオートネゴシエーションに設定されており変更できません。

3.8.9 SYSLOG の設定

起動中に機器背面の電源スイッチを OFF したり等で、電源供給が急に断たれると、syslog メッセージは消えてしまいます。リモートの syslog サーバーに常時メッセージを送信するには SYSLOG 設定画面に遷移します。

場所: 設定 > システム > ネットワーク > SYSLOG 設定

■SYSLOG 関連設定

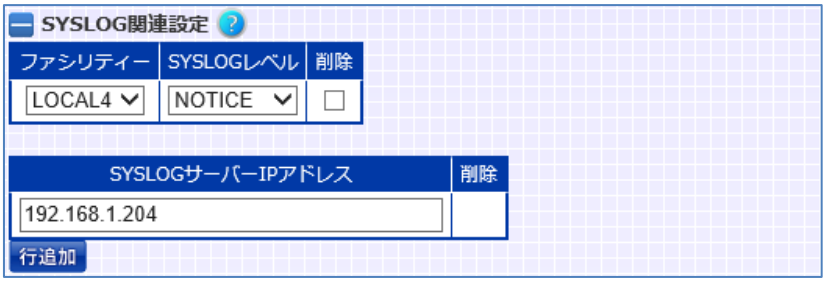
① ファシリティー、SYSLOG レベル

syslog サーバーに送信されるメッセージのファシリティーと、送信するログの下限レベルを選択します。デフォルトに戻す場合削除を選択します。

syslog サーバーに送信されるメッセージのファシリティーはデフォルトで LOCAL4 (20)、下限レベルはデフォルトで notice です。

② SYSLOG サーバーIP アドレス

SYSLOG サーバーの IP アドレス（または IP アドレス名）を設定します。



ファシリティー、ログレベルを表す数値の対応を以下に明記します。

ファシリティー		レベル	
LOCAL0	16	emerg	0
LOCAL1	17	alert	1
LOCAL2	18	crit	2
LOCAL3	19	err	3
LOCAL4	20	warn	4
LOCAL5	21	notice	5
LOCAL6	22	info	6
LOCAL7	23	debug	7

syslog サーバー設定とは別に、syslog メッセージをメールで配信することも可能です。この場合、以下のコマンドを使用してメールサーバーの IP アドレス、送信元メールアドレス、宛先メールアドレスの設定を行います。

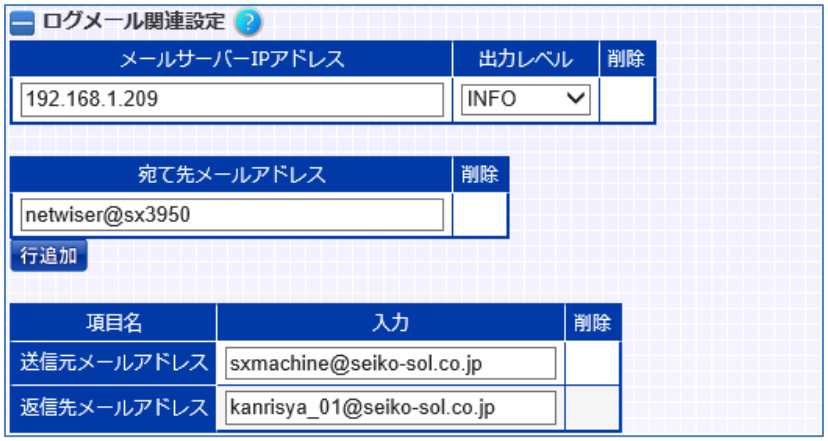
■ログメール関連設定

① メールサーバーIP アドレス、出力レベル
メールサーバーの IP アドレス（または IP アドレス名）と検出対象とするログの下限レベルを設定します。

② 宛先メールアドレス
ログ検出時の配信先メールアドレスを設定します。

③ 送信元メールアドレス
メール受信時の送信元アドレスを設定します。本メールアドレスは架空のアドレスを入力してください。

④ 返信先メールアドレス
本メールへの返信先メールアドレスを設定します。



本製品にはメール受信の機能はありませんので、送信元メールアドレスには netwiser@sx3950 のような架空のアドレスを設定してください。

syslog サーバーと宛先メールアドレスは複数設定することが可能です。その他の項目は 1 件のみ設定します。

3.8.10 SNMP の設定

SNMP の設定をするには、SNMP 設定画面に遷移します。

場所: 設定 > システム > ネットワーク > SNMP 設定

■SNMP マネージャー設定

SNMP マネージャーの IP アドレス（または IP アドレス名）と、SNMP バージョンを設定します。

■コミュニティー、コンタクト、ロケーション

SNMP のシステム情報を設定します。

■SNMP トラップトリガー設定

任意の syslog が出力された際に SNMP トラップを送信することも可能です。
その場合、検出対象となる syslog 文字列を設定します。
「初回のみ」を選択すると、当該コマンドが実行された後、任意の文字列が最初に検出された際にのみ、SNMP トラップを送信します。

■SNMP トラップエージェントアドレス設定

SNMPv1 トラップ発行時のエージェントアドレスの設定を行うには、エージェントアドレスとして使用する VLAN ID を指定します。指定した VLAN に設定されている IPv4 管理アドレスがエージェントアドレスとして使用されます。
VLAN ID の設定がない場合は SNMPv1 トラップの agent-addr に 0.0.0.0 が設定されます。

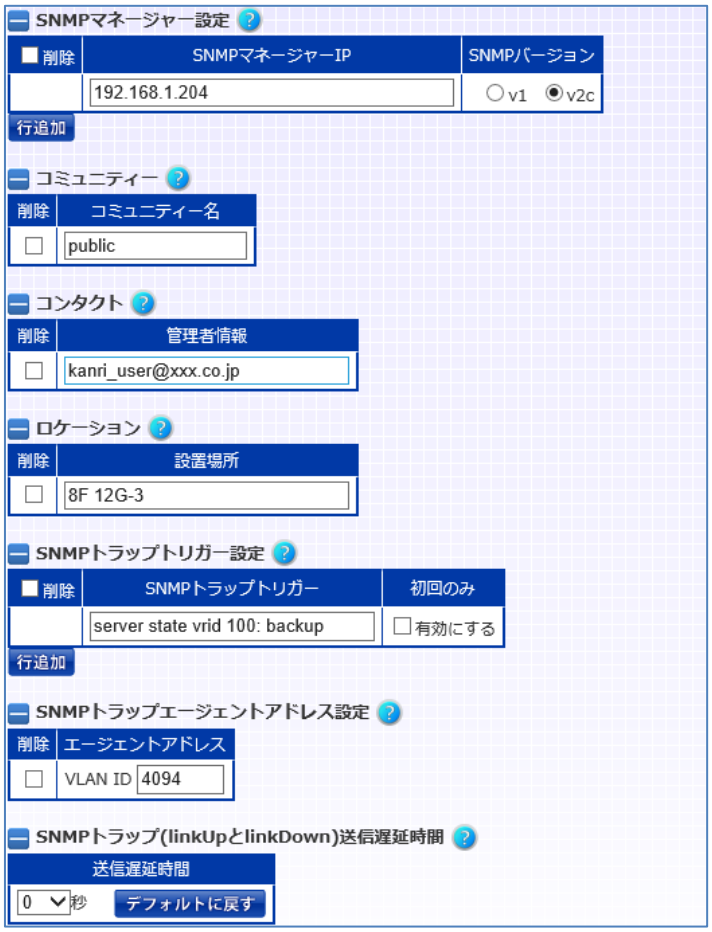
ポイント

- 作成されていない VLAN を指定することはできません。
- IPv4 管理 IP アドレスの設定がない VLAN を指定することはできません。
- VLAN ID 設定後、該当 VLAN の IPv4 管理 IP アドレスを変更した場合、SNMPv1 トラップ発行時のエージェントアドレスも自動的に変更されます。

■SNMP トラップ(linkUp と linkDown)送信遅延時間

lacp 論理チャネルなど、リンク状態の変化に伴い状態の収束に一定の時間が生じるポートからトラップが送信される可能性がある場合、リンクアップまたはリンクダウンのトラップ送信が失敗する場合があります。
本設定を実施する事で、リンクアップまたはリンクダウントラップの送信を、指定

した秒数だけ遅らせることが可能です。
これにより、該当トラップの送信失敗を防ぎます。



プライベート MIB の定義ファイルを取り出すには設定エクスポート画面に遷移します。詳細は「5.3.2.5MIB 定義ファイルのエクスポート」を参照してください。

3.9 VLAN の設定

3.9.1 ポート VLAN の設定

全てのイーサネットポートはデフォルトで VLAN 1 に割り当てられています。
変更するにはイーサネット設定画面に遷移して、イーサネットポートに任意の VLAN を割り当てます。

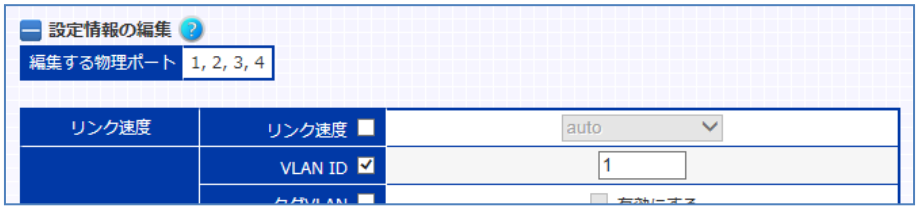
場所: 設定 > ネットワーク > イーサネット

■設定情報の編集（イーサネットポート）

ポート種別とイーサネットポートの選択を行い、設定情報の編集項目を表示させます。

① VLAN 設定 > VLAN ID
　選択したイーサネットポートに割り当てる VLAN ID を入力します。

下の例では、ポート1～4 を VLAN 2 に割り当てます。
ここでは、複数のイーサネットポート番号を指定しているので、入力フォーム横のチェックボックスを選択してから設定の入力を行います。



3.9.2 プライベート VLAN の設定

プライベート VLAN に設定することで同一 VLAN に属する全てのポート間の通信を禁止します。1 つの VLAN 内でブロードキャストドメインを分割できるので、同一サブネット上でのセキュリティが確保されます。

プライベート VLAN はデフォルトで無効になっています。変更するには、イーサネット設定画面に遷移して、プライベート VLAN を有効にします。

場所: 設定 > ネットワーク > イーサネット

■設定情報の編集（イーサネットポート）

① VLAN 設定 > プライベート VLAN

「有効にする」を選択すると、該当のイーサネットポートがプライベート VLAN に設定されます。

また、タグ VLAN、ネイティブ VLAN、VLAN フィルターが選択不可になります。

3.9.3 タグ VLAN の設定

デフォルトでは送受信パケットに 802.1q タグを付けません(アクセスポート)。
802.1q タグを有効(トランクポート)にするにはイーサネット設定画面に遷移して、タグ VLAN を有効にします。

場所: 設定 > ネットワーク > イーサネット

■設定情報の編集(イーサネットポート)

① VLAN 設定 > タグ VLAN
トランクポートに設定する場合「有効にする」を選択します。
タグ VLAN の「有効にする」を選択すると、「ネイティブ VLAN」、「VLAN フィルター」が設定可能になります。
ただし、トランクポートをプライベート VLAN に設定することはできませんので、プライベート VLAN は選択不可になります。
タグ VLAN 有効の状態から解除した場合、アクセスポートに変更され、ポートは VLAN1 に割り当てられます。

② VLAN 設定 > ネイティブ VLAN
タグ付パケットは、タグ内の VLAN ID を使用し、タグなしパケットは、ネイティブ VLAN に設定された VLAN ID を使用します。
ネイティブ VLAN はデフォルトで 1 ですが、変更することもできます。
変更する場合は、「有効にする」を選択して任意の VLAN ID を入力します。

③ VLAN 設定 >VLAN フィルター
特定の VLAN ID のパケットのみ通過させる場合は「有効にする」を選択し、許可する VLAN ID を選択します。
指定のない場合は、全てのパケットが通過します。

ポイント

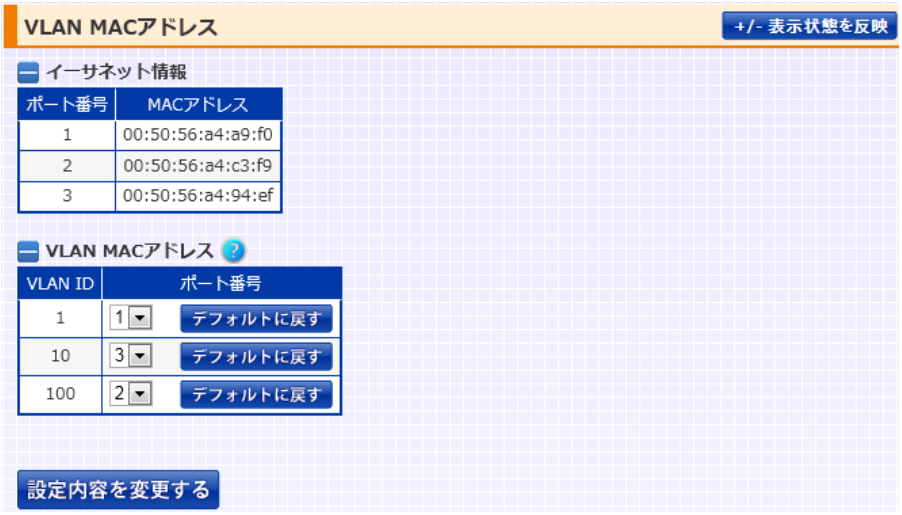
イーサネットポート、または論理チャネルにタグ VLAN の設定がされている場合、MTU サイズは全ての VLAN で統一されている必要があります。
本製品では、タグ VLAN を設定した際、設定されている MTU サイズの中で最小の値が各 VLAN に対して自動で設定されます。
ただし、VLAN に IPv6 アドレスが設定されている場合、該当の VLAN に設定可能な MTU 値の範囲を下回って設定されることがあります。手動で適切な値に変更してください。
MTU 設定の詳細は「3.12MTU 値の変更」を参照してください。

3.9.4 VLAN MAC アドレスの設定（SX-3990 のみ）

すべての VLAN インターフェースはデフォルトでポート1の MAC アドレスが割り振られます。そのため、VLAN に割り当てた IP アドレスあるいは仮想 IP アドレスが使用する MAC アドレスは、ポート1の MAC アドレスに設定されます。仮想 NIC のプロミスキャスモード(promiscuous mode）を無効にしたとき、仮想 NIC はその NIC 向けのフレームのみを受信するため、バランシング動作可能な構成は One-Arm 構成のみとなります。複数のポートを使用した構成の場合は、仮想 IP アドレスの MAC アドレスと仮想 NIC の MAC アドレスとが異なるため、仮想 IP 向けのフレームを受信できません。このとき、仮想 NIC をプロミスキャスモードで動作させる必要があります。

1つの VLAN に1つのポートを割り当てたルーター構成の場合は、プロミスキャスモードを無効にしたまま、VLAN MAC アドレス画面で MAC アドレスを変更することでバランシング動作が可能になります。

場所：設定 ＞ ネットワーク ＞VLAN MAC アドレス



ポイント

以下の場合は、仮想 NIC のプロミスキャスモードを有効化してください。

- 1 つの VLAN に複数のポートを割り当てる
- 冗長構成

3.10 リンク集約

本章ではリンク集約設定に関する設定方法を例とともに記します。
（SX-3990 では、リンク集約機能は動作しません）

リンク集約設定を行うと、複数のイーサネットポートを集約し 1 つの論理チャネルとして扱うことが可能になり、帯域幅が増幅します。
論理チャネルの設定を行うには、イーサネット設定画面に遷移します。ただし、事前にイーサネット設定画面で論理チャネルの生成を行っておく必要があります。

論理チャネル設定の項目は、「動作モード」を除き、全てがイーサネット設定モードで設定する項目名と同一です。各項目のデフォルト値や使用方法も同じです。
以下に、論理チャネル設定モードで設定可能な項目について記載します。

WEB 管理画面上の表記	対応する CLI コマンド
VLAN ID	vlan
タグ VLAN	tagged
ネイティブ VLAN	native-vlan
VLAN フィルター	allowed-vlan
プライベート VLAN	protected
スパニングツリー	spanning-tree
動作モード	mode
バランシングポート定義 *1	slb

*1 「バランシングポート定義」の WEB 管理画面上の場所は[バランシング ＞ ネットワーク ＞ バランシングポート定義]。その他の項目は[ネットワーク ＞ イーサネット]です。

3.10.1 論理チャネルの生成

リンク集約を設定するには、イーサネット設定画面のイーサネットポート設定で論理チャネルを割り当てます。
(SX-3990 では、論理チャネルの生成は不要となります)

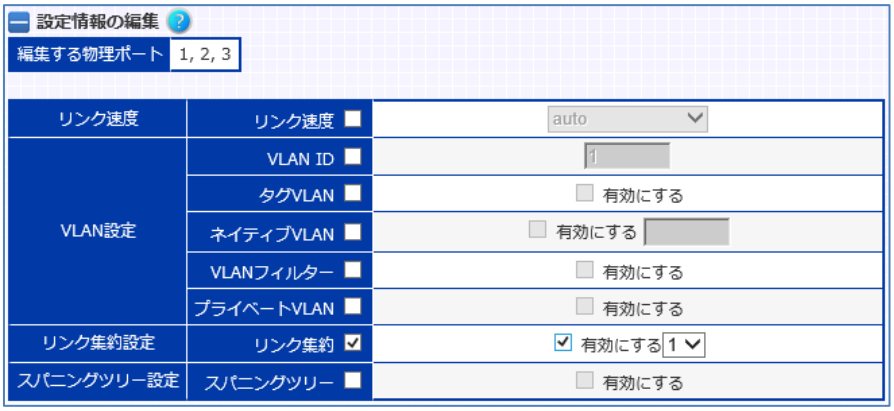
場所: 設定 > ネットワーク > イーサネット

■設定情報の編集(イーサネットポート)

① リンク集約設定 > リンク集約

「有効にする」を選択し、更に任意の論理チャネル番号を選択ます。
設定可能なチャネル数は SX-3950/3945 が最大4(チャネル番号 1-4)、SX-3940 が最大2(チャネル番号 1-2)、SX-3920 が1(チャネル番号 1)となります。

下の例では、ポート1～3 を集約し、論理チャネル 1 を生成します。
複数のイーサネットポート番号を指定しているので、入力フォーム横のチェックボックスを選択してから設定の入力を行います。
※1G I/F と 10G I/F でリンク集約の設定をすることはできません。



以下に挙げる設定をチャネルモードで設定変更した場合、所属する全てのイーサネットポートに設定変更が反映されます。

WEB 管理画面上の表記	対応する CLI コマンド
VLAN ID	(vlan)
タグ VLAN	(tagged)
ネイティブ VLAN	(native-vlan)
VLAN フィルター	(allowed-vlan)
プライベート VLAN	(protected)
スパニングツリー	(spanning-tree)
バランシングポート定義	(slb)

これらの設定、またはリンク速度が異なるポート同士で論理チャネルを形成しないでください。また、ミラーポートを論理チャネルに含めることはできません。

ポイント

論理チャネル生成前にイーサネット設定画面のイーサネットポート指定でこれらの設定を実施した場合、論理チャネル生成時の設定内容に、これらの設定が反映されます。
また、論理チャネル生成後に、イーサネット設定画面のイーサネットポート指定でこれらの設定項目を変更することはできませんので注意してください。
論理チャネル生成後は、イーサネット設定画面の論理チャネル指定でこれらの設定項目を変更してください。

ポイント

リンク集約で使用するポートを速度固定で使用する場合、100MbpsFull、または 1GbpsFull で使用してください。
half 設定では動作しません。

⚠ 注意

リンク集約設定からリンク集約をしない設定にする際、ネットワークがループします。
ケーブルを外してから設定を変更してください。

3.11 スパニングツリーの設定

デフォルトで Spanning-Tree Protocol （STP）は停止状態になっています。
STP を開始するにはイーサネット設定画面に遷移して、スパニングツリー設定を行います。

場所: 設定 > ネットワーク > イーサネット

■設定情報の編集（イーサネットポート）

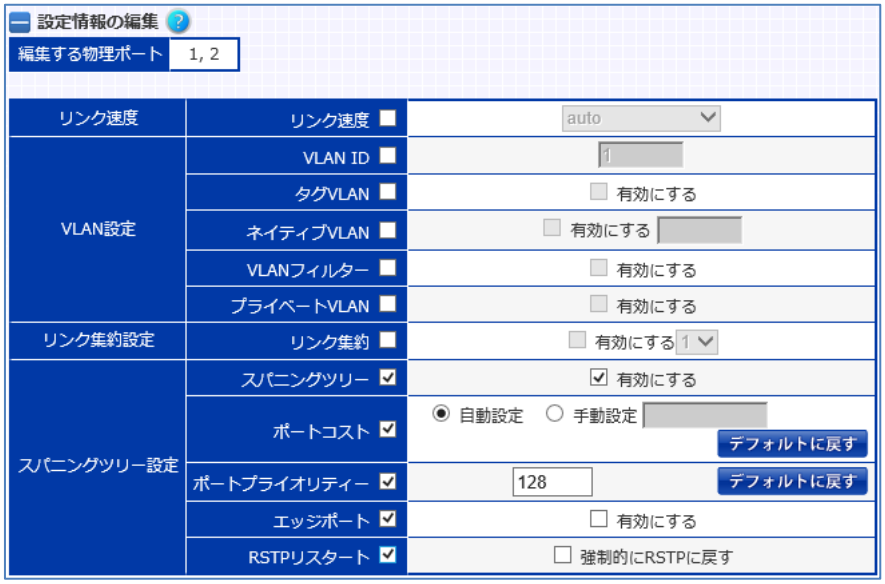
① スパニングツリー設定 > スパニングツリー
「有効にする」を選択すると、詳細な設定が設定可能になります。

② スパニングツリー設定 > ポートコスト
ポートコストを入力します。範囲は 1 から 200000000 です。

③ スパニングツリー設定 > ポートプライオリティー
ポートプライオリティーを入力します。範囲は 0 から 240 で、16 の倍数で登録する必要があります。

④ スパニングツリー設定 > エッジポート
Rapid Spanning-Tree Protocol（RSTP）はスイッチ以外の装置が接続されたエッジポートを自動的に検出し 3 秒後に forwarding(転送)状態へ移行します。3 秒の遅延なく直ちに forwarding 状態に移行させるには、「有効にする」を選択します。

⑤ スパニングツリー設定 > RSTP リスタート
リンク集約設定時のデフォルトの動作モードは RSTP であり変更できません。
しかし、以下の場合は 802.1D 互換モードで動作します。
・ RSTP 未対応のスイッチを検出
・ バス接続されている(半二重リンク)
802.1D 互換モードで動作中のポートを強制的に RSTP に戻すには、「強制的に RSTP に戻す」を選択します。



3.12 MTU 値の変更

本製品の MTU サイズのデフォルトは 1500 です。MTU サイズを変更するには VLAN 設定画面に遷移して、MTU サイズの変更を行います。

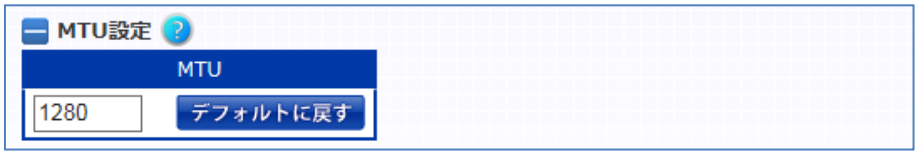
場所: 設定 ＞ ネットワーク ＞VLAN＞VLAN 選択 ＞VLAN 設定

■MTU 設定

① MTU

設定したい MTU サイズに変更します。

設定できる MTU サイズの範囲は 576 から 1500 ですが、該当の VLAN に IPv6アドレスが設定されている場合、1280 が最小になります。



ポイント

イーサネットポート、または論理チャネルにタグ VLAN の設定がされている場合、MTU サイズは全ての VLAN で統一されている必要があります。

タグ VLAN の設定がある状態で MTU サイズの変更を行うと、全 VLAN の MTU サイズが、指定した値に変更されます。ただし、タグ VLAN 設定がされていても、

新規に VLAN を作成した場合、MTU サイズはデフォルトの 1500 に設定されます。手動で他の VLAN の MTU サイズに合わせてください。

注意

MTU を小さい値から大きい値に変更する場合、再起動する必要があります。

3.13 ルーティングテーブルの設定

VLAN で使用するルーティングテーブルのルート ID を設定することができます。

VLAN で使用するルーティングテーブルのルート ID を設定するには VLAN 設定画面に遷移してルート ID の設定を行います。ルート ID が設定されている場合は、VLAN で受信したパケットは VLAN に設定されたルート ID と同一の ID を持つルーティングテーブルに従います。

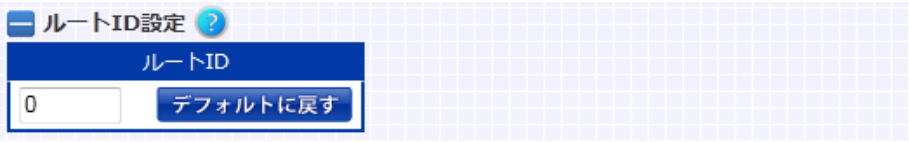
場所: 設定 > ネットワーク > VLAN > VLAN 選択 > VLAN 設定

■ルート ID

① ルート ID

VLAN で使用するルーティングテーブルのルート ID を設定します。

設定できるルート ID の範囲は 0 から 15 です。



ポイント

1. パケットを受信したポートがトランクポートの場合は、タグ情報の VLAN ID を読み取り、該当する VLAN に設定されているルート ID のルーティングテーブルに従います。
2. タグ情報の VLAN ID が本製品に設定されていない VLAN ID の場合は、ルート ID 0 が使用されます。
3. パケットにタグ情報がない場合はネイティブ VLAN に設定されている VLAN のルート ID が使用されます。

ポイント

負荷分散対象、またはリバース NAT の対象となるパケットは各設定画面で設定されているルート ID に従います。

⚠ 注意

本製品の管理 IP アドレスへの接続は VLAN に設定されているルート ID が使用されません。ルート ID 0 が使用されます。
PING への応答は VLAN に設定されているルート ID が使用されます。

3.14 ルーター広告の設定

Router Advertisement（RA）機能を有効にするには、VLAN 設定画面に遷移して、ルーター広告の設定を行います。

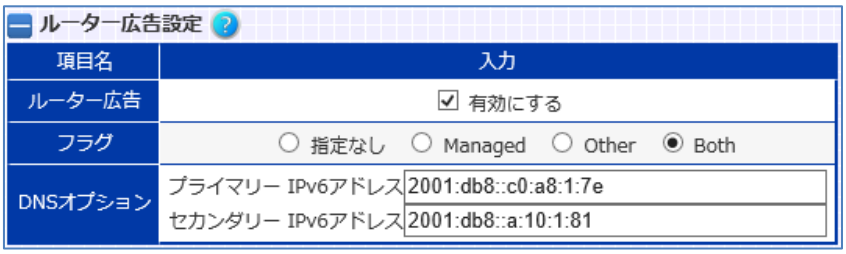
場所: 設定 ＞ ネットワーク ＞VLAN＞VLAN 選択 ＞VLAN 設定画面

■ルーター広告設定

① ルーター広告
「有効にする」を選択すると、RA 機能が有効になります。

② フラグ
RA パケット中の M フラグ(Managed)、O フラグ(Other)、またはその両方(Both)をセットします。
M フラグが指定されている場合、DHCPv6 サーバーから IPv6 アドレスを取得します。また、O フラグが指定されている場合、アドレス以外の情報も DHCP サーバーから取得します。
「指定なし」が選択された場合、どちらのフラグもセットされません。

③ DNS オプション
RA の DNS オプションを有効にし、プライマリーDNS サーバーとセカンダリーDNS サーバーを設定します。
「プライマリーIPv6 アドレス」、「セカンダリーIPv6 アドレス」ともに省略可能ですが、「セカンダリーIPv6 アドレス」のみを指定することはできません。
入力がない場合は、RA の DNS オプションが無効になります。



3.15 フィルタリングの設定

本章では、本製品のフィルタリングに関する設定を例とともに説明します。

3.15.1 リモートアクセスフィルタリング

telnet、ssh を使用したアクセスや、WEB 管理画面へのアクセスといった、本製品へのリモートアクセスに関して、アクセスフィルターを設定することが可能です。

詳細は「3.8.2リモートアクセスフィルターの設定」を参照してください。

3.15.2 VLAN ID フィルタリング

トランクポートはデフォルトで全 VLAN のパケットを通過させます。特定の VLAN ID のみ許可するにはイーサネット設定画面に遷移して、VLAN フィルター設定を行います。

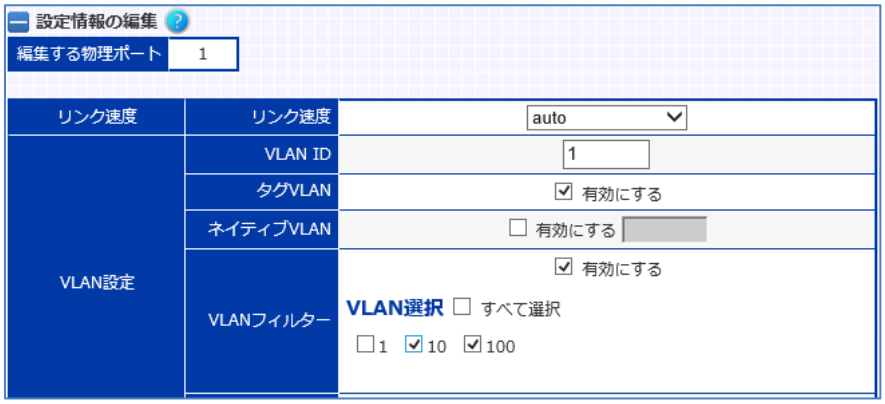
場所: 設定 > ネットワーク > イーサネット

■設定情報の編集

① VLAN フィルター

「有効にする」を選択し、更に VLAN ID を選択すると、任意の VLAN ID のパケットのみを許可する設定になります。

VLAN フィルター設定を有効にするには、タグ VLAN で「有効にする」が選択されている必要があります。



3.15.3 L2 パケットフィルタリング

MAC アクセスリスト設定画面で L2 パケットに対するアクセス制御リスト(Access Control List、以下 ACL)を作成します。

場所: 設定 > ネットワーク > パケットフィルタリング > MAC アクセスリスト

■MAC アクセスリスト設定

① アクセスリスト名
作成する ACL のポリシー名を入力します。

② 行番号
ACL に登録するルールのルール番号を入力します。
指定可能な行番号の範囲は 1-65534 で、省略した場合は最後のルールに 10 を加えた番号が割り当てられます。
デフォルトルールとして行番号 65535 に全ての受信拒否が設定されています。

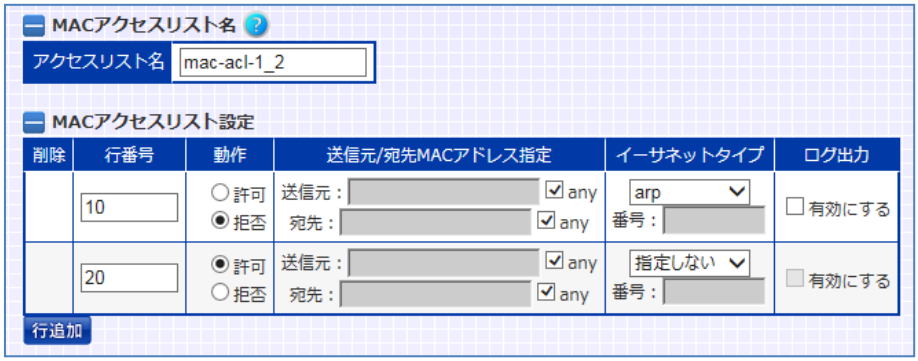
③ 動作
「許可」、「拒否」のいずれかを選択します。

④ 送信元/宛先 MAC アドレス指定
登録するルールの送信元 MAC アドレスと、宛先 MAC アドレスを入力します。
それぞれ、「any」を選択すると、全ての MAC アドレスをフィルタリングの対象とします。

⑤ イーサネットタイプ
イーサネットタイプを選択し、ルールにマッチさせるイーサネットタイプを指定します。「指定しない」を選択した場合、全てのイーサネットタイプが対象となります。
ip、ipv6、arp、bpdu の中から選択するか、選択肢以外のイーサネットタイプを指定する場合、「番号を指定」を選択して、イーサネットタイプ番号を入力します。
イーサネットタイプ番号は 5dd から ffff までの 16 進数で入力してください。

⑥ ログ出力
「有効にする」を選択すると、ルールに一致した場合に syslog メッセージを生成します。
動作で「拒否」を選択した場合にのみ指定可能です。

たとえば、ARP リクエストを拒否する ACL を作成するには、以下のようにします。



まず、行番号 10 で ARP リクエストを拒否し、その他のパケットは行番号 20 によってアクセスが許可されます。
上述した通り、全てのアクセスリストには、デフォルトルールとして行番号 65535 に全ての受信拒否が設定されています。よって行番号 20 がない場合は全パケットのアクセスが遮断されてしまいます。

フィルタリングを開始する場合は、MAC パケットフィルター起動画面で L2 フィルタリングの設定を行います。

場所：設定 ＞ ネットワーク ＞ パケットフィルタリング ＞ MAC パケットフィルター起動

■MAC パケットフィルター起動

① 受信パケットフィルター起動
「起動する」を選択すると、「受信アクセスリスト」が選択可能になります。

② 受信アクセスリスト
受信パケットに対するフィルタリングとして、設定したいアクセスリストのポリシー名を選択します。

③ 送信パケットフィルター起動
「起動する」を選択すると、「送信アクセスリスト」が選択可能になります。

④ 送信アクセスリスト
送信パケットに対するフィルタリングとして、設定したいアクセスリストのポリシー名を選択します。

以下の例では、ポート1とポート２の受信パケットに対して mac-acl-1_2 を適用します。


MACパケットフィルター起動

ポート番号	受信パケットフィルター起動	受信アクセスリスト	送信パケットフィルター起動	送信アクセスリスト
1	☑ 起動する	mac-acl-1_2	☐ 起動する	未選択
2	☑ 起動する	mac-acl-1_2	☐ 起動する	未選択
3	☐ 起動する	未選択	☐ 起動する	未選択
4	☐ 起動する	未選択	☐ 起動する	未選択
5	☐ 起動する	未選択	☐ 起動する	未選択
6	☐ 起動する	未選択	☐ 起動する	未選択
7	☐ 起動する	未選択	☐ 起動する	未選択
8	☐ 起動する	未選択	☐ 起動する	未選択
9	☐ 起動する	未選択	☐ 起動する	未選択
10	☐ 起動する	未選択	☐ 起動する	未選択
11	☐ 起動する	未選択	☐ 起動する	未選択
12	☐ 起動する	未選択	☐ 起動する	未選択

送信フィルターと受信フィルターに、異なるフィルタリングルールを設定することも可能です。

ポイント

MAC パケットフィルター起動画面で、フィルタリングルールを適用した後、MAC アクセスリスト設定画面で ACL ルールを変更しても設定は反映されません。MAC アクセスリスト設定画面で ACL ルールを変更した後、再度 MAC パケットフィルター起動画面で、フィルタリングルールを適用し直してください。

3.15.4 L3/L4 パケットフィルタリング

L3/L4 パケットに対するアクセス制御リスト(Access Control List、以下 ACL)を作成するには、IPv4 アクセスリスト設定画面、または IPv6 アクセスリスト設定画面に遷移します。

場所: 設定 > ネットワーク > パケットフィルタリング > IP アクセスリスト

■IPv4 アクセスリスト設定

① アクセスリスト名
作成する ACL のポリシー名を入力します。

② 行番号
ACL に登録するルールのルール番号を入力します。
省略した場合は最後のルールに 10 を加えた番号が割り当てられます。
デフォルトルールとして行番号 65535 に全ての受信拒否が設定されています。

③ 動作
「許可」、「拒否」のいずれかを選択します。

④ プロトコル
ルールにマッチさせる送信元のプロトコルを選択します。
選択肢以外のプロトコルを指定したい場合、「プロトコル番号で指定する」を選択し、入力欄にプロトコル番号を入力します。
プロトコル番号は 0 から 255 までの 10 進数を入力します。
プロトコル番号 0 または選択肢"ip"は、全ての IP パケットを表します。

⑤ 送信元/宛先 IPv4 アドレス指定
登録するルールの送信元 IP アドレス(またはネットワークアドレス)と、宛先 IP アドレス(またはネットワークアドレス)を入力します。
それぞれ、「any」を選択すると、全ての IPv4 アドレスをフィルタリングの対象とします。

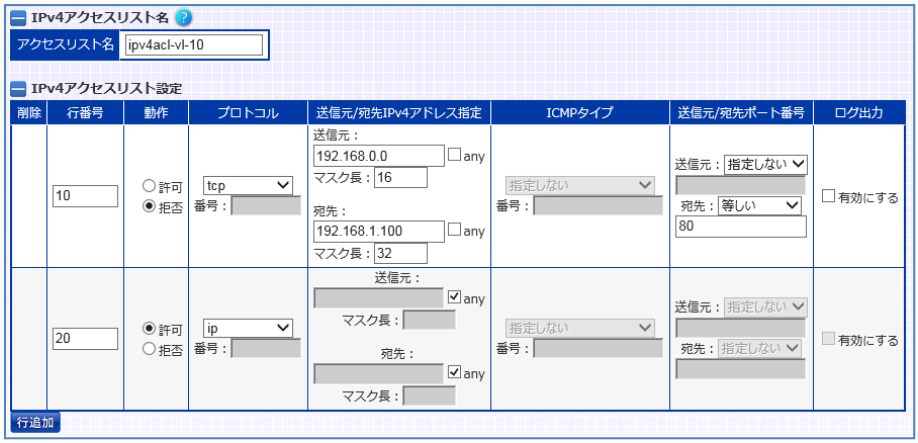
⑥ ICMP タイプ
プロトコルで"icmp"または"icmpv6"が選択されている場合、ICMP タイプの選択が可能になります。
ルールにマッチさせる ICMP タイプを指定したい場合、ICMP タイプを選択します。「指定しない」を選択すると、全ての ICMP タイプが対象となります。
選択肢以外の ICMP タイプを指定する場合、「番号を指定」を選択して、

ICMP タイプ番号を入力します。
番号は 0 から 255 までの 10 進数を入力します。

⑦ 送信元/宛先ポート番号
プロトコルに”tcp”または”udp”が入力された場合にのみ、フィルタリングの対象とする送信元ポート番号、宛先ポート番号を指定できます。
ポート番号を使用しない場合、「指定しない」を選択します。
ポート番号は、「等しい」、「異なる」、「より大きい」、「より小さい」、「範囲指定」のいずれかが選択可能です。

⑧ ログ出力
「有効にする」を選択すると、ルールに一致した場合に syslog メッセージを生成します。
動作で「拒否」を選択した場合にのみ指定可能です。

以下の例では、ネットワークアドレス 192.168.0.0/16 からの 192.168.1.100（ポート 80）に対するアクセスを拒否します。



まず、行番号 10 で任意のアクセスを拒否するルールを規定します。その他のパケットは行番号 20 によってアクセスが許可されます。
上述した通り、全てのアクセスリストには、デフォルトルールとして行番号 65535 に全ての受信拒否が設定されています。よって行番号 20 がない場合は全パケットのアクセスが遮断されてしまいます。

フィルタリングを開始する場合は、IPv4(IPv6)パケットフィルター起動画面で L3/L4 フィルタリングの設定を行います。

場所: 設定 > ネットワーク > パケットフィルタリング > IP パケットフィルター起動

■IPv4 パケットフィルター起動/IPv6 パケットフィルター起動

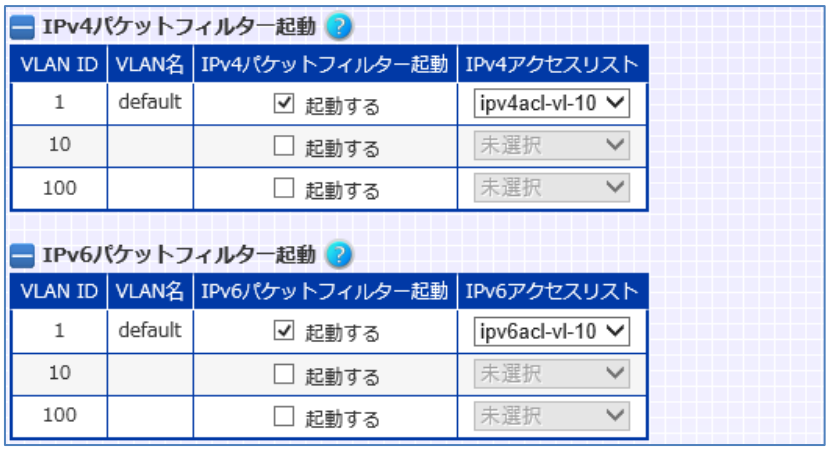
① IPv4パケットフィルター起動
「起動する」を選択すると、「IPv4 アクセスリスト」が選択可能になります。

② IPv4 アクセスリスト
受信パケットに対するフィルタリングとして、設定したいアクセスリストのポリシー名を選択します。

③ IPv6 パケットフィルター起動
「起動する」を選択すると、「IPv6 アクセスリスト」が選択可能になります。

④ IPv6 アクセスリスト
受信パケットに対するフィルタリングとして、設定したいアクセスリストのポリシー名を選択します。

以下の例では、VLAN 1 に対して ipv4acl-vl-10、ipv6acl-vl-10 を適用します。



ポイント

IP パケットフィルター設定は、受信パケットにのみ適用されます。送信パケットには適用されません。

ポイント

IP パケットフィルター起動画面で、フィルタリングルールを適用した後、IPv4(または IPv6)アクセスリスト設定画面で ACL ルールを変更しても設定は反映されません。
IPv4(または IPv6)アクセスリスト設定画面で ACL ルールを変更した後、再度 IP パケットフィルター起動画面で、フィルタリングルールを起動し直してください。

3.16 ファイアウォールの設定

本章では、本製品のファイアウォール機能に関する設定を例とともに説明します。

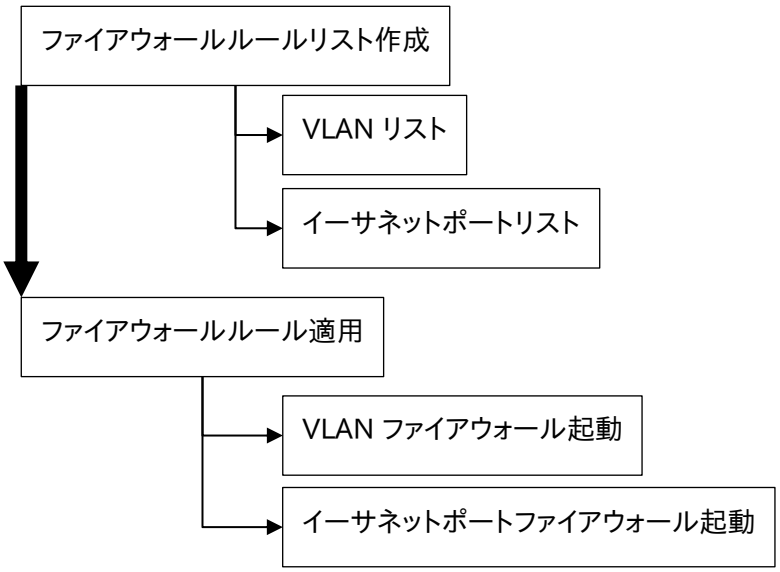
3.16.1 ファイアウォール機能

ファイアウォール機能を使用すると、本製品を流れる着信トラフィックと発信トラフィックをフィルタリングできます。

ファイアウォール機能は、1 つ以上の「ルール」のセットを使用して、ネットワークパケットを送受信するときにネットワークパケットを検査し、トラフィックの通過を許可またはブロックします。

ファイアウォール機能のルールは、プロトコルタイプ、送信元または宛先のホストアドレス、送信元または宛先のポートなど、パケットの 1 つ以上の特性を検査できます。

設定の流れを以下に示します。



3.16.2 ファイアウォールルール作成

ファイアウォールルール制御リストを作成するには、VLAN リスト設定画面、またはイーサネットポートリスト設定画面に遷移します。

ルールリストの最大設定数は 128 件、各リストのルール最大設定数は 127 件です。

3.16.2.1 VLAN リスト設定

特定の vlan にファイアウォールルールを設定したい場合は「VLAN リスト設定画面」を選択してください。

場所: 設定 > ネットワーク > ファイアウォール > VLAN リスト

■IPFW VLAN リスト設定

① IPFW VLAN リスト名
作成するファイアウォールルールのリスト名を入力します。
リスト名は、1 から 64 文字まで文字列を付けることができます。
半角英数、ハイフン(-)、アンダーバー(_)、シャープ(#)、スラッシュ(/)、コマーシャルアット(@)が使用可能です。先頭文字に数字、記号を使用することはできません。

② 行番号
ファイアウォールルールリストに登録するルールのルール番号を入力します。
省略した場合は最後のルールに 10 を加えた番号が割り当てられます。
デフォルトルールとして行番号 65535 に全ての受信許可が設定されています。

③ 動作
「送信許可」、「受信許可」、「送信拒否」、「受信拒否」のいずれかを選択します。

④ プロトコル
ルールにマッチさせるプロトコルを選択します。
選択肢以外のプロトコルを指定したい場合、「プロトコル番号で指定する」を選択し、入力欄にプロトコル番号を入力します。
プロトコル番号は 0 から 255 までの 10 進数を入力します。

プロトコル番号 0 または選択肢"ip"は、全ての IP パケットを表します。

⑤ 送信元/宛先 IP アドレス指定

登録するルールの送信元 IP アドレス（またはネットワークアドレス）と、宛先 IP アドレス（またはネットワークアドレス）を入力します。

それぞれ、「any」を選択すると、全ての IPv4 アドレスあるいは IPv6 アドレスをフィルタリングの対象とします。「me」を指定した場合は自局 IP アドレスに一致します。

⑥ ICMP タイプ

プロトコルで"icmp"または"icmp6"が選択されている場合、ICMP タイプの選択が可能になります。

ルールにマッチさせる ICMP タイプを指定したい場合、ICMP タイプを選択します。「指定しない」を選択すると、全ての ICMP タイプが対象となります。

選択肢以外の ICMP タイプを指定する場合、「番号を指定」を選択して、ICMP タイプ番号を入力します。

番号は 0 から 255 までの 10 進数を入力します。

⑦ 送信元/宛先ポート番号

プロトコルに”tcp”または”udp”が選択された場合にのみ、フィルタリングの対象とする送信元ポート番号、宛先ポート番号を指定できます。

ポート番号を使用しない場合、「指定しない」を選択します。

ポート番号は、「等しい」、「異なる」、「範囲指定」のいずれかが選択可能です。

⑧ オプション

■ログ出力

ルールに一致した場合に syslog メッセージを生成します。

動作で「送信拒否」、「受信拒否」を選択した場合に選択可能です。

■established

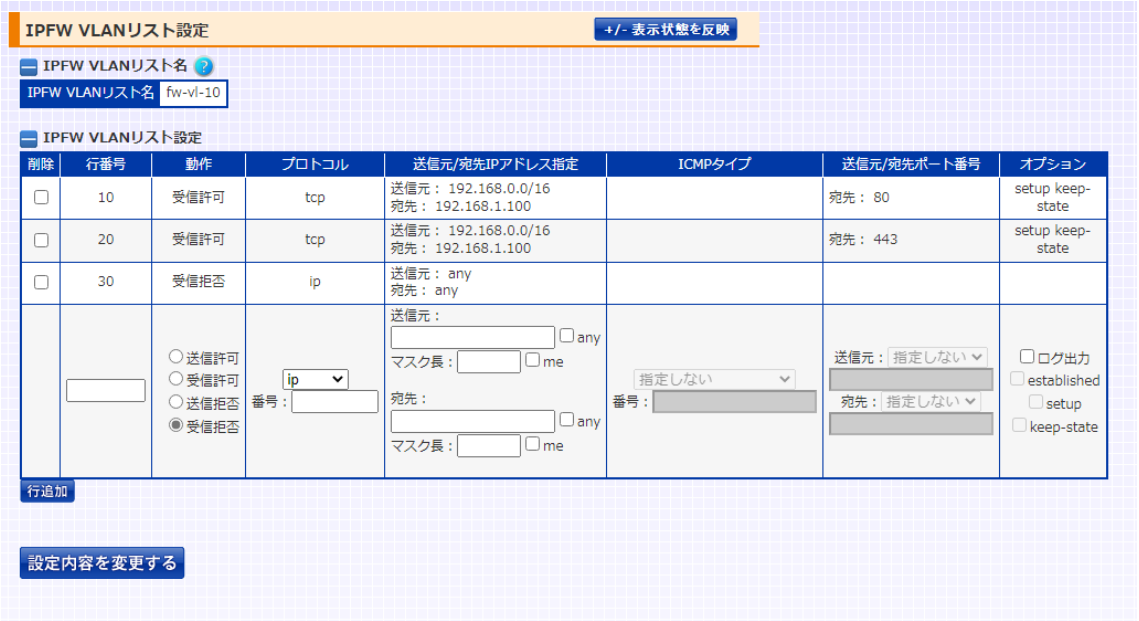
“プロトコル”に“tcp”または“tcp6”が選択されたときパケットがすでに確立されている TCP コネクションの一部であれば(RST または ACK ビットがセットされていれば)マッチします。

■setup

“プロトコル”に“tcp”または“tcp6”が選択されたときコネクション確立要求(SYN=1)の TCP パケットにマッチします。”keep-state”と組み合わせて指定することでコネクション確立要求に合わせて動的ルールを作成します。

■keep-state
動作に「送信許可」、「受信許可」を選択、“プロトコル”に“tcp”、“tcp6”、”icmp”、”icmp6”が選択したとき指定可能です。
ルールに一致するとファイアウォールは、一致したルールと同じプロトコルを使用して送信元アドレスと宛先アドレスおよびポート間の双方向トラフィックを一致させる動的ルールを作成します。

以下の例では、ネットワークアドレス 192.168.0.0/16 からの 192.168.1.100（ポート 80 および 443）に対するアクセスを許可し、それ以外のトラヒックを拒否します。



まず、行番号 10 および20でネットワークアドレス 192.168.0.0/16 から 192.168.1.100 へのポート 80 および 443 にアクセスするルールを規定します。その他のパケットは行番号30によってアクセスが拒否されます。
全てのアクセスリストには、デフォルトルールとして行番号 65535 に全ての受信許可が設定されています。よって行番号30 がない場合は全パケットのアクセスが許可されてしまいます。

3.16.2.2 イーサネットポートリスト設定

特定のイーサネットポート、または論理チャネルにファイアウォールルールを設定したい場合は「イーサネットポート設定画面」を選択してください。

場所: 設定 > ネットワーク > ファイアウォール > イーサネットポートリスト

■IPFW イーサネットポートリスト設定

① IPFW イーサネットポートリスト名
作成するファイアウォールルールのリスト名を入力します。

② 行番号
ファイアウォールルールリストに登録するルールのルール番号を入力します。
省略した場合は最後のルールに 10 を加えた番号が割り当てられます。
デフォルトルールとして行番号 65535 に「全て受信許可」が設定されています。

③ 動作
「受信許可」、「受信拒否」のいずれかを選択します。

④ プロトコル
ルールにマッチさせる送信元のプロトコルを選択します。
選択肢以外のプロトコルを指定したい場合、「プロトコル番号で指定する」を選択し、入力欄にプロトコル番号を入力します。
プロトコル番号は 0 から 255 までの 10 進数を入力します。
プロトコル番号 0 または選択肢"ip"は、全ての IP パケットを表します。

⑤ 送信元/宛先 IP アドレス指定
登録するルールの送信元 IP アドレス（またはネットワークアドレス）と、宛先 IP アドレス（またはネットワークアドレス）を入力します。
それぞれ、「any」を選択すると、全ての IPv4 アドレスあるいは IPv6 アドレスをフィルタリングの対象とします。それぞれ、「any」を選択すると、全ての IPv4 アドレスあるいは IPv6 アドレスをフィルタリングの対象とします。「me」を指定した場合は自局 IP アドレスに一致します

⑥ ICMP タイプ
プロトコルで"icmp"または"icmp6"が選択されている場合、ICMP タイプの選択が可能になります。
ルールにマッチさせる ICMP タイプを指定したい場合、ICMP タイプを選択します。「指定しない」を選択すると、全ての ICMP タイプが対象となります。
選択肢以外の ICMP タイプを指定する場合、「番号を指定」を選択して、ICMP タイプ番号を入力します。
番号は 0 から 255 までの 10 進数を入力します。

⑦ 送信元/宛先ポート番号

プロトコルに”tcp”または”udp”が入力された場合にのみ、フィルタリングの対象とする送信元ポート番号、宛先ポート番号を指定できます。
ポート番号を使用しない場合、「指定しない」を選択します。
ポート番号は、「等しい」、「異なる」、「範囲指定」のいずれかが選択可能です。

⑨ オプション

■ログ出力
ルールに一致した場合に syslog メッセージを生成します。
動作で「送信拒否」、「受信拒否」を選択した場合に選択可能です。

■established
“プロトコル”に“tcp”または“tcp6”が選択されたときパケットがすでに確立されている TCP コネクションの一部であれば(RST または ACK ビットがセットされていれば)マッチします。

■setup
“プロトコル”に“tcp”または“tcp6”が選択されたときコネクション確立要求(SYN=1)の TCP パケットにマッチします。”keep-state”と組み合わせて指定することでコネクション確立要求に合わせて動的ルールを作成します。

■keep-state
動作に「送信許可」、「受信許可」を選択、“プロトコル”に“tcp”、“tcp6”、”icmp”、”icmp6”が選択したとき指定可能です。
ルールに一致するとファイアウォールは、一致したルールと同じプロトコルを使用して送信元アドレスと宛先アドレスおよびポート間の双方向トラフィックを一致させる動的ルールを作成します。

以下の例では、ネットワークアドレス 192.168.0.0/16 からの 192.168.1.100（ポート 80 および 443）に対するアクセスを許可し、それ以外のトラヒックを拒否します。

まず、行番号 10 および20でネットワークアドレス 192.168.0.0/16 から 192.168.1.100 へのポート 80 および 443 にアクセスするルールを規定します。その他のパケットは行番号30によってアクセスが拒否されます。
全てのアクセスリストには、デフォルトルールとして行番号 65535 に全ての受信許可が設定されています。よって行番号30 がない場合は全パケットのアクセスが許可されてしまいます。

ポイント

IPFW イーサネットポートリスト設定のフィルタリング設定は、受信パケットにのみ適用されます。送信パケットには適用されません。

3.16.3 ファイアウォールルール適用

作成したファイアウォールルール制御リストを適用するには、「VLAN ファイアウォール起動画面」、または「イーサネットポートファイアウォール起動画面」に遷移します。

3.16.3.1 VLAN ファイアウォール起動

特定の VLAN にファイアウォールルールを適用する場合は、VLAN ファイアウォール起動画面で設定を行います。

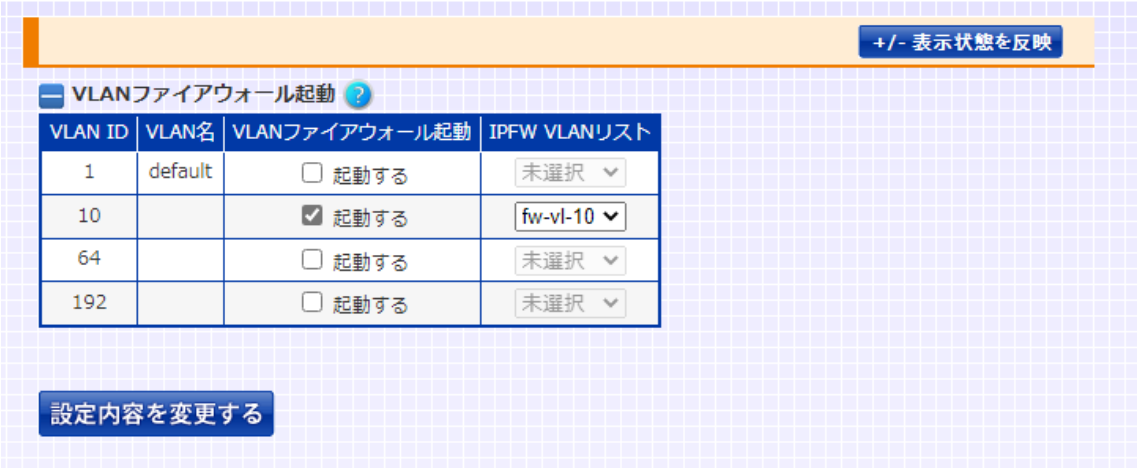
場所: 設定 > ネットワーク >ファイアウォール > VLAN ファイアウォール起動

■VLAN ファイアウォール起動

① VLAN ファイアウォール起動
「起動する」を選択すると、「IPv4 アクセスリスト」が選択可能になります。

② IPFW VLAN リスト
パケットに対するフィルタリングとして、設定したい VLAN リストのポリシー名を選択します。

以下の例では、VLAN 10 に対して fw-vl-10 を適用します。



ポイント VLAN ファイアウォール起動画面でルールの適用を開始した後、VLAN リスト設

定画面で、ファイアウォールルールを変更しても、起動中のファイアウォール処理には反映されません。
ファイアウォールルール変更後は、再度 VLAN ファイアウォール起動画面でルールを起動し直してください。

3.16.3.2 イーサネットポートファイアウォール起動

特定のイーサネットポート、または論理チャネルにファイアウォールルールを適用する場合は、イーサネットポートファイアウォール起動画面で設定を行います。

場所: 設定 > ネットワーク >ファイアウォール > イーサネットポートファイアウォール起動

■イーサネットポートファイアウォール起動

① イーサネットポートファイアウォール起動
「起動する」を選択すると、「IPFW イーサネットポートリスト」が選択可能になります。

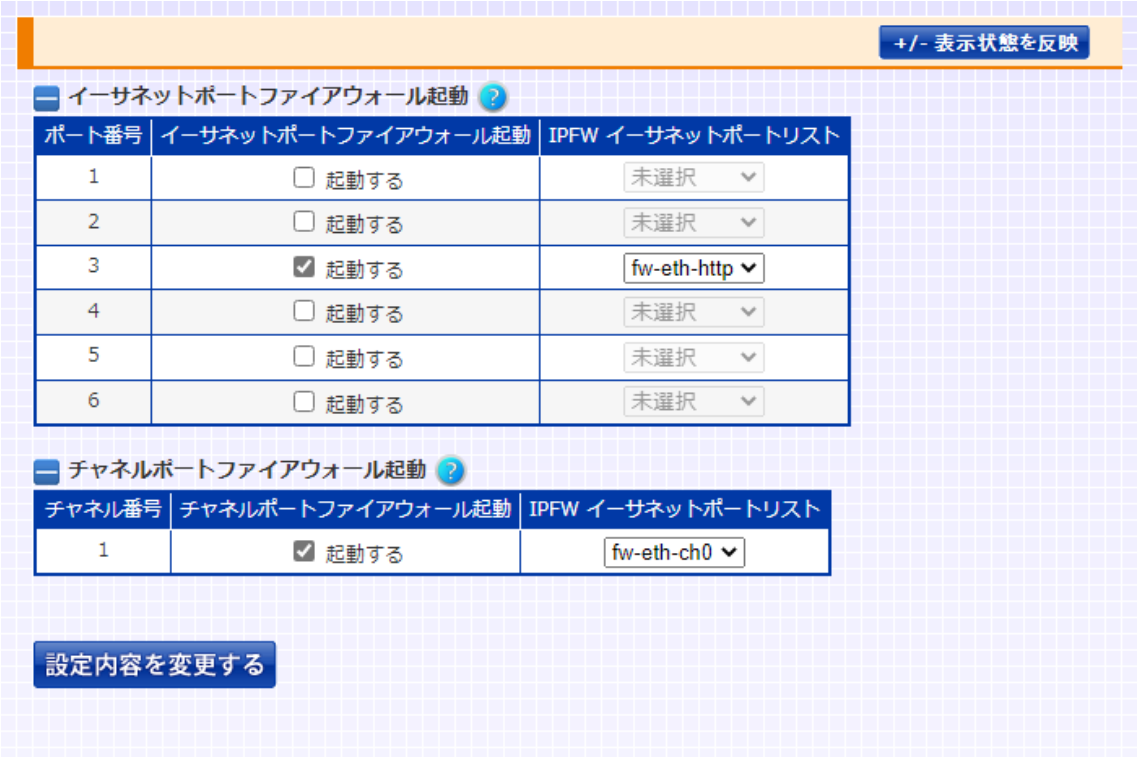
② IPFW イーサネットポートリスト
パケットに対するフィルタリングとして、設定したいイーサネットポートリストリストのポリシー名を選択します。

■チャネルポートファイアウォール起動

① チャネルポートファイアウォール起動
「起動する」を選択すると、「IPFW イーサネットポートリスト」が選択可能になります。

② IPFW イーサネットポートリスト
パケットに対するフィルタリングとして、設定したいイーサネットポートリストのポリシー名を選択します。

以下の例では、イーサネットポート 3 に対して fw-eth-http を適用し、論理チャネル1に対して fw-eth-ch0 を適用します。



ポイント

イーサネットポートファイアウォール起動でルールの適用を開始した後、イーサネットポートリスト設定でファイアウォールルールを変更しても、起動中のファイアウォール処理には反映されません。
ファイアウォールルール変更後は、再度イーサネットポートファイアウォール起動画面でルールを起動し直してください。

3.17 接続先ネットワーク種別

バランシングポート定義画面で、イーサネットポートまたは論理チャネルの接続先ネットワーク種別を定義することが可能です。

場所: 設定 > バランシング > ネットワーク > バランシングポート定義

■バランシングポート定義（イーサネットポート）

① 定義

該当のポートの接続先ネットワーク種別を選択します。

■クライアント/サーバーポート

クライアント側ネットワークとサーバー側ネットワークのどちらも接続可能な設定となります。

■クライアントポート

クライアント側ネットワークが接続されていることを意味します。

フェイルスルー設定がされている場合、ポート 1 を本設定にする必要があります。

フェイルスルー設定でない場合、本設定を行っても動作に影響はないため、デフォルト設定のままで問題ありません。

■サーバーポート

サーバーネットワークが接続されていることを意味します。

フェイルスルー設定がされている場合、ポート 2 を本設定にする必要があります。

フェイルスルー設定でない場合、本設定を行っても動作に影響はないため、デフォルト設定のままで問題ありません。

■管理ポート

管理ネットワークに接続されていることを意味します。

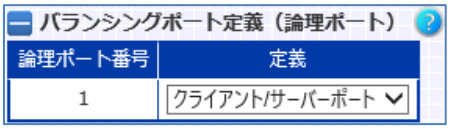
管理ポートでは、受信した仮想サーバーへの ARP/NDP 問い合わせには答えません。

■管理専用ポート

管理ネットワークに接続されており、かつ当該ポートとその他のイーサネットポート間の通信が遮断されることを意味します。

管理専用ポートでは、管理専用ポートへのアクセスや、管理専用ポートを経由するアクセスを制限します。
管理専用ポートの詳しい説明は「3.7.3.1 管理専用ポートの定義」を参照してください。

また、論理チャネルに所属しているイーサネットポートの設定を変更するには、論理チャネルの設定テーブルで変更してください。



ポイント

フェイルスルー設定がされた場合、システムが自動的にポート1を'クライアントポート'、ポート 2 を'サーバーポート'に設定します。
ただし、フェイルスルー設定が解除されても本設定はそのままですので注意してください。

ポイント

デフォルト設定は「クライアント/サーバーポート」です。非フェイルスルー状態でも設定変更は可能ですが、必須ではありません。

3.18 ポートミラーリングの設定

ミラーリング設定を行うことで、本製品の送受信するネットワークパケットを任意のイーサネットポートにミラーリングすることができます。
ミラーリングを設定するにはポートミラーリング設定画面に遷移します。

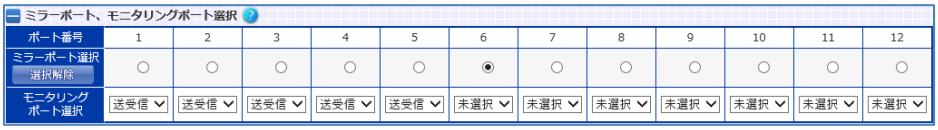
場所: 設定 > ネットワーク > ポートミラーリング

■ミラーポート、モニタリングポート選択

① ミラーポート選択
ミラーリングポートに設定するイーサネットポート番号を選択します。
ミラーポートは単一ポートにのみ適用できます。また、ミラーポートを論理チャネルに含めることはできません。

② モニタリングポート選択
モニタリングポートに設定するイーサネットポート番号を選択します。
イーサネットポート番号は、複数選択可能です。
また、フィルタリング対象とするパケットの種別を「送信」、「受信」、または「送受信」の中から選択します。
監視対象は複数設定することができますが、複数ポートを監視する対象とした場合にミラーポートはデータをロストする場合があります。

以下の例では、ポート 1～5 の送受信パケットをポート 6 にミラーリングします。



3.19 MAC アドレスの追加・削除

MAC アドレステーブルに静的エントリーを追加するには MAC テーブル設定画面に遷移します。

場所: 設定 > ネットワーク > MAC テーブル

■静的 MAC アドレスエントリー設定

① MAC アドレス

テーブルに追加したい MAC アドレスを入力します。

② イーサネットポート番号、論理チャネル番号

MAC アドレスの存在するネットワークに割り当てられているイーサネットポート、または論理チャネルを選択します。

③ VLAN ID

対象となるイーサネットポート、または論理チャネルがトランクポートである場合指定します。そうでない場合省略可能です。

動的 MAC エントリーの生存時間や、テーブルエントリー最大数を変更する事も可能です。

■動的エントリー保持時間設定

① 動的エントリー保持時間

動的 MAC テーブルエントリーの生存時間を設定します。

② テーブルエントリー最大数

動的 MAC テーブルエントリーの最大保持数を設定します。

3.20 ARP、NDP

3.20.1 ARP テーブルエントリーの追加・削除

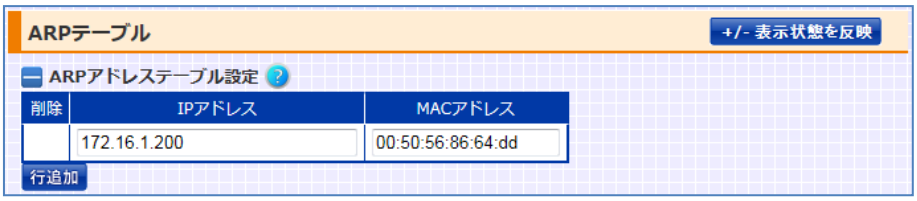
ARP テーブルに静的エントリーを追加するには ARP テーブル設定画面に遷移します。

場所: 設定 > ネットワーク > ARP テーブル

静的 ARP テーブルの追加、削除を行います。

■ARP アドレステーブル設定

テーブルに追加したい IPv4 アドレス（または IP 名）と MAC アドレスを入力します。



その他に、動的 ARP テーブルの生存時間を変更する事が可能です。

■動的エントリー保持時間設定

動的 ARP エントリーの生存時間はデフォルトで 20 分です。

変更するには、任意の時間を選択します。

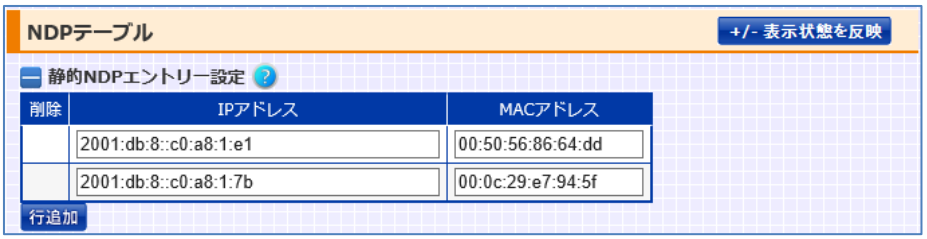
3.20.2 NDP テーブルエントリーの追加・削除

NDP テーブルに静的エントリーを追加するには、NDP テーブル設定画面に遷移します。

場所: 設定 > ネットワーク > NDP テーブル

■静的 NDP エントリー設定

テーブルに追加したい IPv6 アドレス（または IP 名）と MAC アドレスを入力します。



3.21 サーバー負荷分散の設定

本章ではサーバー負荷分散に関する設定方法を例とともに記します。
更に具体的な設定例については「第4章設定例」を参照してください。

3.21.1 同時に設定できない機能

以下に挙げる機能は、同一の仮想サーバーに対して同時に設定することができません。ご注意ください。

機能	同時に設定できない機能
Cookie によるセッション維持 ［３．２１．１５．５］ ［３．２１．１５．６］	･複数のサーバーにまたがるセッション維持（仮想サーバーグループの設定） ・DSR モード
SSL セッション ID によるセッション維持 ［３．２１．１５．４］	･複数のサーバーにまたがるセッション維持（仮想サーバーグループの設定） ・DTLS プロトコル ・DSR モード ・URL スイッチング ・HTTP リダイレクトの送信 ・403 レスポンスの送信 ・URL スイッチング設定 ・Fallback-url の設定 ・Location ヘッダー書き換え設定 ・発信元 IP アドレス、プロトコル情報の挿入 ・sorry コンテンツの設定 ・X-Forwarded-For セッション維持設定 ・X-Forwarded-For スイッチング設定
複数のサーバーにまたがるセッション維持（仮想サーバーグループの設定） ［３．２１．１５．１］	・Cookie によるセッション維持 ・SSL セッション ID によるセッション維持
X-Forwarded-For ヘッダーに明示された IP アドレス情報によるセッション維持 ［３．２１．１５．２］	・DSR モード
DSR モード（dsr オプション） ［３．２１．１６．９］	・Cookie によるセッション維持 ・SSL セッション ID によるセッショ

	ン維持 ・URL スイッチング ・HTTP リダイレクトの送信 ・403 レスポンスの送信 ・Location ヘッダーの書き換え ・ソース NAT ・発信元 IP アドレス、プロトコル情報の挿入 ・アクセスログの生成 ・SSL アクセラレーション ・フェイルスルー ・IPv4/IPv6 変換 ・sorry コンテンツの設定 ・X-Forwarded-For セッション維持設定 ・X-Forwarded-For スイッチング設定
発信元 IP アドレスに基づく負荷分散 ［３．２１．１６．２］	・URL スイッチング ・HTTP リダイレクトの送信 ・403 レスポンスの送信 ・Location ヘッダーの書き換え
URL スイッチング ［３．２１．１６．４］ HTTP リダイレクトの送信 ［３．２１．１６．５］ 403 レスポンスの送信 ［３．２１．１６．５］	・発信元 IP アドレスに基づく負荷分散 ・DSR モード ・SSL セッション ID によるセッション維持
Location ヘッダーの書き換え ［３．２１．１６．６］	・発信元 IP アドレスに基づく負荷分散 ・DSR モード
発信元 IP アドレス、プロトコル情報の挿入 ［３．２１．１２］	・DSR モード
アクセスログ ［３．２１．１３］	・DSR モード
SSL アクセラレーション ［３．２２］	・DSR モード
sorry コンテンツの設定 ［３．２１．１６．７］	・DSR モード

※ 表中の「Cookie によるセッション維持」は、cookie セッション維持と cookie 挿入機能の両方を指します。

※ 表中の「発信元 IP アドレスに基づく負荷分散」は、送信元 IP アドレスによる負荷分散と X-Forwarded-For ヘッダー情報の内容による負荷分散の両方を

指します。

3.21.2 実サーバーの設定

負荷分散対象となるサーバーの設定を行うには、実サーバー設定画面に遷移します。

場所: 設定 > バランシング > 実サーバー > 実サーバー設定

WEB 管理画面から実サーバーの登録を行います。

■実サーバー設定

① 実サーバーIP、ポート、プロトコル
登録する実サーバーIP（または IP アドレス名）、ポート、プロトコルを入力します。

② 最大コネクション
システム全体で実サーバーが受け付けるコネクションの最大数を設定します。
デフォルトは 0 で、無制限となります。

⚠ 注意 接続中のコネクションがある状態で最大コネクション数を変更した場合、現在接続中のコネクションが切れてから設定が反映されますので注意してください。

ポイント コネクション接続とコネクション切断のタイミングによっては、設定より小さい値で最大コネクション数に達することがあります。

ポイント 最大コネクション数に達した実サーバーへは、新規コネクションを確立することができません。ただし、セッション維持機能により生成されたセッション情報に合致する新規コネクションに関しては、最大コネクション制限の対象になりません。

ポイント 仮想サーバー毎に実サーバーの最大コネクションを指定することも可能です。詳しくは「3.21.16仮想サーバーと実サーバーの関連付け」を参照してください。

③ 有効

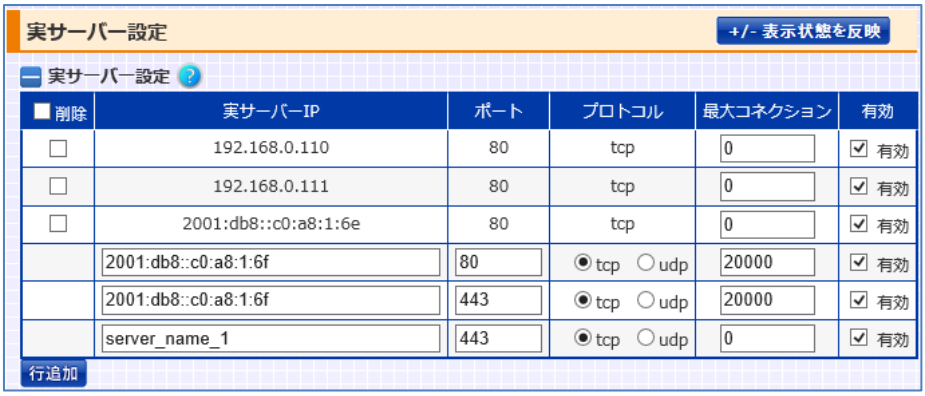
設定直後のデフォルトでは実サーバーは稼動状態です。停止状態にするには

選択を外します。

ポイント

ヘルスチェック設定で、「手動復旧」に設定している実サーバーは、ヘルスチェックが DOWN すると、当該画面の「有効」チェックボックスが自動的に未選択状態になり、負荷分散対象から外れます。

実サーバーを負荷分散対象に戻す場合、再び「有効」を選択し直す必要があります。



仮想サーバーにバインドされている実サーバーID を削除することはできません。仮想サーバー設定画面に遷移して、仮想サーバーとの対応を解除してから削除してください。

また、実サーバーID を削除すると、そのサーバーとの間で確立中のコネクションに関する情報は失われます。

機器情報画面の「バランシング ＞ 実サーバー」で、実サーバー情報を参照することができます。

3.21.3 仮想サーバーの設定

仮想サーバーを設定するにはあらかじめ仮想サーバーIP アドレスの設定を行わなければなりません。
仮想サーバーIP アドレスの設定を行うには、VLAN 設定画面に遷移します。

場所: 設定 > ネットワーク > VLAN > VLAN 選択 > VLAN 設定

■仮想 IP アドレス設定

① 仮想 IP アドレス
使用する仮想サーバーの IP アドレス(または IP アドレス名)を入力します。

仮想サーバーIP アドレスの設定が完了した後、仮想サーバーの設定を行います。
仮想サーバーの設定を行うには、仮想サーバー設定画面に遷移します。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■仮想サーバーID 設定

① 仮想サーバー名
仮想サーバーに名前付けして管理することが可能です。
任意の仮想サーバー名を入力します。
本設定は設定を管理し易くするための設定であり必須ではありません。

② 仮想サーバーIP アドレス、ポート、プロトコル
仮想サーバーIP アドレスを選択し、ポートの入力、プロトコルの選択を行います。
仮想サーバーIP アドレスを選択するには、VLAN 設定画面で事前に仮想サーバーIP を登録しておく必要があります。

③ 有効
仮想サーバーはデフォルトで停止状態です。稼働状態にするには有効を選択します。

停止状態の仮想サーバーは新規のコネクション要求を受け付けません。ただし稼動中に確立したコネクションはそのまま維持されます。

FTP パケットはデータ部分に IP アドレス情報を含むため、負荷分散するには特殊な処理が必要になります。FTP サーバーの制御ポートとしてデフォルトの 21 以外を使用する場合はプロトコルに ftp と設定してください。
tftp の負荷分散をするには、ポート番号に 69、プロトコルに udp と設定してください。

「機器情報 ＞ バランシング ＞ 仮想サーバー」で、仮想サーバー情報を参照することができます。

⚠ 注意

ポート番号 0 を指定した仮想サーバーに対して、以下の設定はできません。

- アクセスログ設定
- SSL アクセラレーション設定
- SSL セッション維持設定
- cookie セッション維持設定
- URL スイッチング設定
- URL リダイレクト設定、または 403 応答の設定
- Fallback-url の設定
- Location ヘッダー書き換え設定
- ヘッダー挿入設定
- sorry コンテンツの設定
- IPv4/IPv6 変換設定
- X-Forwarded-For セッション維持設定
- X-Forwarded-For スイッチング設定

3.21.4 仮想サーバー状態の設定

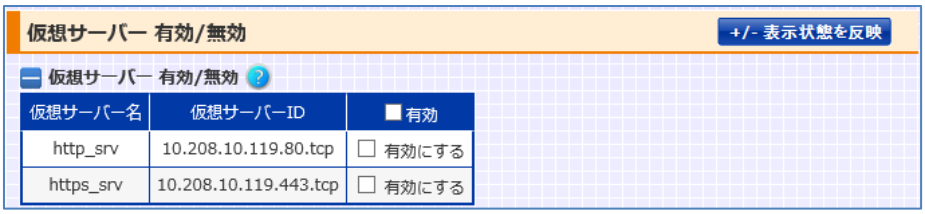
仮想サーバーはデフォルトで停止状態です。仮想サーバー設定画面で稼働状態を変更する事もできますが、全ての仮想サーバーエントリーの稼働状態を一括で変更する場合、仮想サーバー有効/無効設定画面に遷移します。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー有効/無効

■仮想サーバー有効/無効

① 有効

有効にする場合選択します。



停止状態の仮想サーバーは新規のコネクション要求を受け付けません。ただし稼動中に確立したコネクションはそのまま維持されます。

3.21.5 MSL タイマーの設定

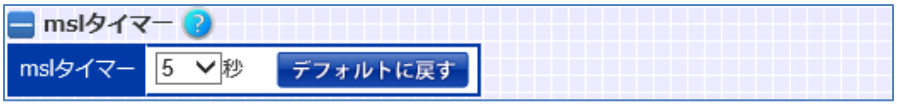
本製品における TCP コネクションの MSL タイマー（Maximum Segment Lifetime） はデフォルトで 2 秒です。
MSL タイマーを変更することで、本製品が管理する TCP コネクションの TIME_WAIT 状態における待ち時間（=MSL タイマーの 2 倍）が変化します。

場所： 設定 ＞ バランシング ＞ 仮想サーバー ＞ msl タイマー

■mslタイマー

① msl タイマー
タイマー値を変更する場合 1～60 秒の範囲で選択します。
「デフォルトに戻す」ボタンを押下した場合 60 秒が選択されます。

以下では、MSL タイマーを 5 秒に設定することで、TIME_WAIT 状態の待ち時間（=MSL タイマーの 2 倍）が 10 秒に変更されます。



注意 MSL タイマー値の変更は負荷分散動作だけでなく、TCP ヘルスチェック時の動作など、システム全体に影響します。

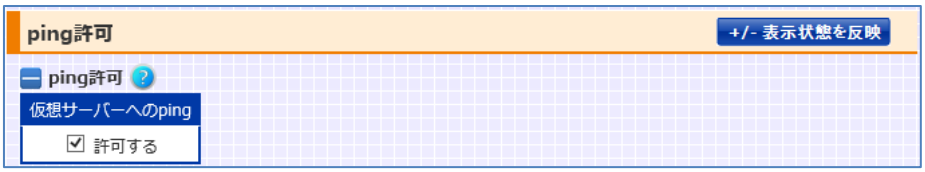
3.21.6 仮想サーバーへの ping 許可設定

デフォルトでは、仮想サーバーIP アドレスへの ping には応答しません。
仮想サーバーIP アドレスへの ping に応答するには、ping 許可設定画面に遷移します。

場所: 設定 > バランシング > 仮想サーバー > ping 許可

■ping 許可

① 仮想サーバーへの ping
仮想サーバーIP アドレスへの ping を許可する場合、「許可する」を選択します。



⚠ 注意

同一 IP アドレスの仮想サーバーが複数登録されており、ルート ID がそれぞれの仮想サーバーで異なる場合は、応答パケットは最初に登録されている仮想サーバーのルート ID のルーティングテーブルに従います。

3.21.7 負荷分散方式の変更

負荷分散方式の設定を変更するには、仮想サーバー設定画面に遷移して、分散アルゴリズムの設定を行います。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■仮想サーバー基本設定

① 分散アルゴリズム

最小コネクション、またはラウンドロビンのいずれかを選択します。

UDP 仮想サーバーの場合、最小コネクションは設定できません。

プロトコルが tcp、または ftp の仮想サーバーは、デフォルトで最小コネクションが設定されます。

プロトコルが udp の仮想サーバーは、ラウンドロビンのみ設定可能です。

3.21.8 アイドルタイマー値の変更

コネクションタイムアウト時間を変更するには、仮想サーバー設定画面に遷移して、コネクションタイムアウト設定を行います。

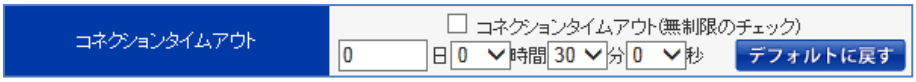
場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■仮想サーバー基本設定

① コネクションタイムアウト

アイドル状態（無通信状態）の L4 コネクションを破棄する時間を、範囲内から選択します。

アイドル状態（無通信状態）の L4 コネクションを破棄する時間はデフォルトで、tcp が 30 分、udp が 5 分です



ポイント

この設定は L7 コネクションには適用されません。

L7 コネクションとは、以下のいずれかの設定がされた仮想サーバーが処理するコネクションのことを指します。

- SSL アクセラレーション設定
- SSL セッション維持設定
- cookie セッション維持設定
- URL スイッチング設定
- HTTP リダイレクト設定
- Location ヘッダー書き換え設定
- Fallback-url の設定
- sorry コンテンツの設定
- アクセスログ設定
- ヘッダー挿入設定
- IPv4/IPv6 変換設定
- X-Forwarded-For スイッチング設定
- X-Forwarded-For セッション維持設定

3.21.9 送信元アドレスの変換

実サーバーへの送信元アドレスの変換を仮想サーバーで行うには、事前に登録した NAT プールを仮想サーバーへ割り当てます。
NAT プールを登録するには、NAT プール設定画面に遷移して、プールアドレスの登録を行います。

場所: 設定 ＞ バランシング ＞NATプール ＞NATプール選択 ＞NATプール設定

■NAT プール設定

① NAT プール名
NAT プールのポリシー名を入力します。

② 開始 IP アドレス、終了 IP アドレス
プールアドレスを入力します。
範囲指定で登録する場合、終了 IP アドレスも入力します。

ポイント

範囲指定でアドレスを登録する場合、範囲内に仮想サーバーIP アドレスを含めることはできません。「開始 IP アドレス」のみを入力する事で 1 件だけ登録できます。仮想サーバーIP アドレスは1件ずつ登録してください。

ポイント

NAT プールのポリシーは 256 件まで登録可能です。しかし、プールアドレスの最大登録数はシステム全体で 16 件です。ただし、仮想サーバーIP アドレスは登録制限に含まれません。
また、NAT プールアドレスにはリンクローカルアドレスを設定しないでください。

ポイント

仮想サーバー設定に割り当てられている状態の NAT プールポリシーを削除することはできません。NAT プールポリシーを削除する場合、仮想サーバーでの割り当てを解除してから削除してください。

送信元アドレスの変換機能を有効にするには、仮想サーバー設定画面に遷移して、作成済みの NAT プールポリシーを仮想サーバーに割り当てます。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■仮想サーバー基本設定

① ソース NAT プール

ソース NAT 設定を有効にするには登録済みの NAT プールポリシーを選択します。

ポイント

NAT プール設定モードでプールアドレスの追加・削除を行うだけで、該当の NAT プールポリシーを割り当てている仮想サーバーにも設定が反映されます。

ポイント

ソース NAT 設定を実施した場合、該当の仮想サーバーに対する全てのアクセスの送信元アドレスが、プールアドレスに変換されます。特定のネットワークからのアクセスにのみ送信元アドレスの変換機能を適用したい場合は NAT フィルター設定を実施します。

NAT フィルター設定は「3.21.11ソース NAT フィルタリングの設定」を参照してください

NAT プールアドレスの使用状況を統計情報として参照できます。

機器情報画面の「バランシング > NAT プール」で、仮想サーバー情報を参照することができます。

3.21.10 ワンアームゲートウェイモードの設定

ワンアーム構成でソース NAT 設定を使用せずに負荷分散するにはワンアームゲートウェイモード設定を使用します。

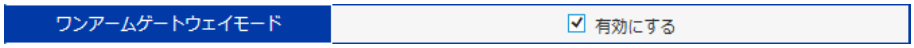
ワンアームゲートウェイモードを使用するには、仮想サーバー設定画面に遷移して、ワンアームゲートウェイモードの設定を有効にします。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■仮想サーバー基本設定

① ワンアームゲートウェイモード

ワンアームゲートウェイモード設定を有効にする場合選択します。



ポイント

ワンアームゲートウェイモードで使用する場合、実サーバーのデフォルトゲートウェイを本製品の管理 IP アドレス、または冗長 IP アドレス(冗長構成の場合)に設定する必要があります。

ポイント

この設定はソース NAT 設定、ソース NAT フィルタリング設定と併用することで、指定した任意のクライアントアドレスのみソース NAT させることが可能です。
仮想サーバーと同じ VLAN に存在するクライアントからアクセスする場合は、ソース NAT 設定、ソース NAT フィルタリング設定が必須となります。
詳しくはワンアーム構成の構成例「4.7.3構成例 3(ソース NAT+ワンアームゲートウェイモード)」を参照してください。

3.21.11 ソース NAT フィルタリングの設定

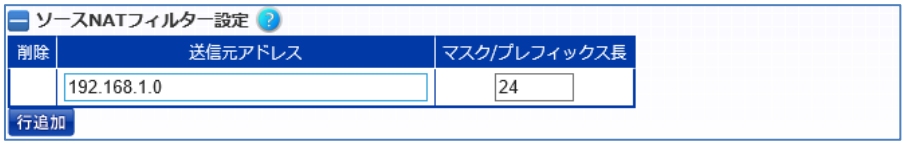
仮想サーバーに対して、特定のネットワークアドレスからのアクセスにのみ、送信元アドレスの変換機能（ソース NAT 設定）を適用するには、仮想サーバー設定画面でソース NAT フィルター設定を登録します。また、ソース NAT フィルタールールを登録するには、事前に送信元アドレス変換機能（ソース NAT 設定）が有効である必要があります。
送信元アドレス変換機能の設定は「3.21.9送信元アドレスの変換」を参照してください。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■ソース NAT フィルター設定

① 送信元アドレス、マスク/プレフィックス長
任意のネットワークアドレス、マスク長（またはプレフィックス長）を入力します。

以下では、192.168.1.0/24 からのアクセスにのみ、送信元アドレス変換機能（ソース NAT 設定）が適用され、その他のネットワークからのアクセスには、送信元アドレス変換機能（ソース NAT 設定）が適用されません。



仮想サーバーの送信元アドレス変換機能（ソース NAT 設定）が無効に設定された場合は、該当の仮想サーバーに設定された全てのソース NAT フィルター設定が自動で削除されます。

ポイント

ソース NAT フィルター設定は、新規コネクションから適用されるものであり、既存コネクションには影響しません。

3.21.12 発信元 IP アドレス、プロトコル情報のヘッダーおよび Cookie 属性の挿入

仮想サーバーが HTTP サーバーの場合、変換前の発信元 IP アドレス、プロトコルを HTTP リクエストに挿入することが可能です。
HTTP リクエストにヘッダー情報を挿入するには、仮想サーバー設定画面に遷移してヘッダー挿入機能設定を変更します。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

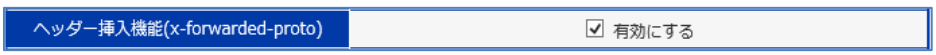
■仮想サーバー基本設定

① ヘッダー挿入機能(x-forwarded-for)
変換前の発信元 IP アドレスを HTTP リクエストヘッダーに挿入します。
有効にする事で、該当の仮想サーバーに対する全てのリクエストに以下のヘッダーを挿入して実サーバーに送信します。

```
X-Forwarded-For: 変換前の発信元 IP アドレス
```

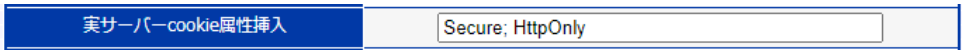
② ヘッダー挿入機能(x-forwarded-proto)
変換前の宛先プロトコルを HTTP リクエストヘッダーに挿入します。
有効にすることで、該当の仮想サーバーに対する全てのリクエストに以下のヘッダーを挿入して実サーバーに送信します。

```
X-Forwarded-Proto: 変換前の宛先プロトコル
```



③ 実サーバ Cookie 属性挿入機能
実サーバーが発行した Set-Cookie ヘッダーに任意の Cookie 属性を挿入することが可能です。

以下のように、HttpOnly 属性が設定された cookie は JavaScript からアクセスできなくなり、Secure 属性が設定された cookie は HTTPS 通信時だけその cookie を送信します。



注意 cookie 属性で指定した文字列についてはチェックせずにそのまま付加します。指定文字列が属性として正しいことをご確認ください。

ポイント ヘッダー挿入機能はL7 負荷分散機能の一部です。ヘッダー挿入機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

3.21.13 アクセスログ

仮想サーバーが HTTP サーバーの場合、アクセスログを生成し外部の syslog サーバーへ送信することが可能です。仮想サーバー設定画面に遷移して、アクセスログ送信先サーバーを設定します。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

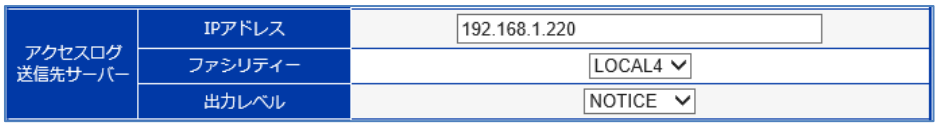
■仮想サーバー基本設定 > アクセスログ送信先サーバー

① IP アドレス

アクセスログ送信先のログサーバーIP アドレス（または IP アドレス名）を入力します。

② ファシリティー、出力レベル

メッセージのファシリティーと出力ログの下限レベルを選択します。



ファシリティー、ログレベルを表す数値の対応を以下に明記します。

ファシリティー		レベル	
LOCAL0	16	emerg	0
LOCAL1	17	alert	1
LOCAL2	18	crit	2
LOCAL3	19	err	3
LOCAL4	20	warn	4
LOCAL5	21	notice	5
LOCAL6	22	info	6
LOCAL7	23	debug	7

本製品は以下の例のような NCSA 共通形式のメッセージを生成します。形式を変更することはできません。

<送信元アドレス> --[<日時分>] "<アクセス先 URL パス>" <ステータスコード> <応答メッセージのボディサイズ>

以下に実際に送出されるメッセージの例を示します。

```
127.0.0.1 - - [15/Aug/2012:18:15:05 +0900] "/cgi-bin/index.cgi" 200
1050
```

本設定はシスログ設定と関連していません。また、生成されたログは本製品内部のシスログファイルには残りません。

ポイント

アクセスログ機能は L7 負荷分散機能の一部です。アクセスログ機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

3.21.14 ルーティングテーブルの設定

仮想サーバーで使用するルーティングテーブルのルート ID を設定できます。

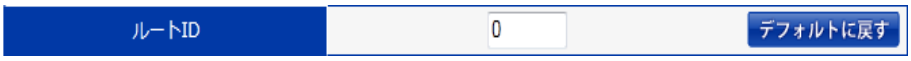
仮想サーバーで使用するルーティングテーブルのルート ID を設定するには仮想サーバー設定画面に遷移してルート ID の設定を行います。ルート ID が設定されている場合は、負荷分散対象となるパケットが仮想サーバーに設定されたルート ID と同一の ID を持つルーティングテーブルに従います。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■仮想サーバー基本設定

① ルート ID

仮想サーバーで使用するルーティングテーブルのルート ID を設定します。
設定できるルート ID の範囲は 0 から 15 です。



3.21.15 セッション維持機能の設定

仮想サーバー設定画面でセッション維持設定を実施すると、同一クライアントからの通信が一定時間同一のサーバーに割り振られるようになります。たとえば、クライアントがオンラインで何かのフォームを記入するような場合、一定の時間通信を同一のサーバーに割り振ることにより、トランザクションを完結させることができます。
セッションの維持に使用可能な情報は IP アドレス、X-Forwarded-For ヘッダー、cookie、SSL セッション ID の 4 種類です。

セッションタイムアウト値として指定する時間は、あるクライアントからのコネクションが全て終了したアイドル状態で、セッション維持機能が有効である時間を指します。たとえば 5 分と設定すると、コネクション要求が 5 分以内に発生すれば前と同じサーバーに送信されますが、5 分を経過すると別のサーバーに割り振られる可能性があります。
範囲は 1 分から 365 日です。ただし、cookie 挿入機能の場合、0 分を指定することが可能です。

3.21.15.1 IP アドレスセッション維持

クライアントの IP アドレスに基づいたセッション維持を設定するには仮想サーバー設定画面のセッション維持設定項目で「IP アドレス」セッション維持を設定します。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■仮想サーバー基本設定 > セッション維持設定

① セッション維持方法

IP アドレスセッション維持を設定するには、「IP アドレス」を選択します。

IP アドレスセッション維持を無効にするには「セッション維持 無効」を選択します。

② マスク/プレフィックス長

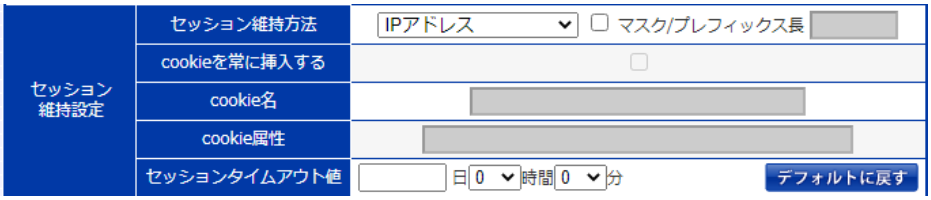
IP アドレス単位ではなくサブネット単位でセッションを維持したい場合、チェックボックスを選択したうえで、任意のマスク/プレフィックス長を入力します。

本設定を行うと、送信元 IP アドレスを任意のマスク長でマスクし、同じサブネットとなるクライアントからのアクセスに関して振り分け先サーバーを統一します。

③ セッションタイムアウト値

セッション維持のタイムアウト間隔は日時分で指定します。

「デフォルトに戻す」ボタンを押下した場合 15 分に設定されます。



IP アドレスセッション維持情報を参照するには、機器情報画面の「バランシング > IP アドレスセッション維持」で確認できます。

更に、仮想サーバーグループを作成することで、複数の仮想サーバー間で IP セッション維持情報を共有することが可能です。仮想サーバーグループ設定の詳細は「3.21.15.3 仮想サーバーグループの形成」を参照してください。

3.21.15.2 X-Forwarded-For セッション維持

X-Forwarded-For ヘッダー情報に明示されている IP アドレス情報に基づいてセッション維持を行うことが可能です。これにより、X-Forwarded-For ヘッダーにクライアントの IP アドレス情報が埋め込まれてさえいれば、プロキシサーバーを経由するなどして IP アドレスが隠蔽されている場合においても、クライアント IP アドレスに基づくセッション維持が可能です。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■仮想サーバー基本設定 > セッション維持設定

① セッション維持方法

X-Forwarded-For セッション維持を設定するには、「XFF ヘッダー」を選択します。

X-Forwarded-For セッション維持を無効にするには「セッション維持 無効」を選択します。

② マスク/プレフィックス長

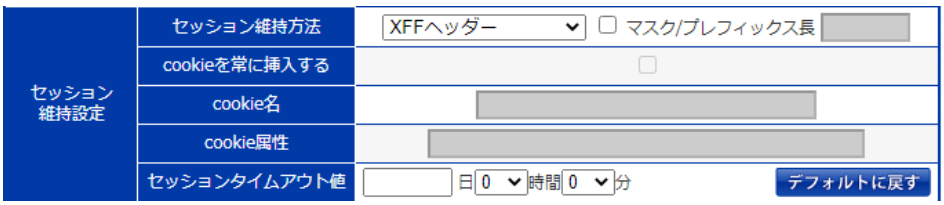
IP アドレス単位ではなくサブネット単位でセッションを維持したい場合、チェックボックスを選択したうえで、任意のマスク/プレフィックス長を入力します。

本設定を行うと、X-Forwarded-For ヘッダーに明示された IP アドレス情報を任意のマスク長でマスクし、同じサブネットとなるクライアントからのアクセスに関して振り分け先サーバーを統一します。

③ セッションタイムアウト値

セッション維持のタイムアウト間隔は日時分で指定します。

「デフォルトに戻す」ボタンを押下した場合 15 分に設定されます。



IP アドレスセッション維持情報を参照するには、機器情報画面の「バランシング > IP アドレスセッション維持」で確認できます。

更に、仮想サーバーグループを作成することで、複数の仮想サーバー間で

X-Forwarded-For セッション維持情報を共有することが可能です。
仮想サーバーグループ設定の詳細は「3.21.15.3 仮想サーバーグループの形成」を参照してください。

ポイント

HTTP リクエスト内に X-Forwarded-For ヘッダーが存在しない場合、IP ヘッダーの送信元アドレス情報を基にセッション維持情報が生成されます。また、X-Forwarded-For ヘッダーに複数の IP アドレス情報が明示されている場合は、先頭の IP アドレス情報を参照します。

ポイント

X-Forwarded-For ヘッダー情報に基づいて生成されたセッション維持情報は、IP アドレスセッション維持情報と同等に扱われ、IP アドレスセッション維持設定と同様にタイムアウト間隔やサブネット単位でのセッション維持、仮想サーバーグループの形成が可能です。ただし、X-Forwarded-For セッション維持設定は L7 負荷分散機能の一部であるため、設定された仮想サーバーに対する全てのリクエストは L7 レベルで処理されます。その点で、IP アドレスセッション維持設定とは異なります。
なお、X-Forwarded-For セッション維持設定がされている状態から、IP アドレスセッション維持設定に切り替えた場合、その時点における該当仮想サーバーの IP セッション情報は全て削除されるのでご注意ください。

⚠ 注意

IP ヘッダーに明示されている送信元 IP アドレスのアドレスファミリーと、X-Forwarded-For ヘッダーにセットされた IP アドレスのアドレスファミリーが一致しない場合、セッション維持情報が正常に生成されません。

3.21.15.3 仮想サーバーグループの形成

IP セッション維持設定、または X-Forwarded-For セッション維持設定で動作する仮想サーバー同士をグループ化することで、異なる仮想サーバー同士でセッション維持情報を共有することが可能です。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバーグループ

仮想サーバーグループを定義し、複数の仮想サーバーを所属させます。

■仮想サーバーグループ設定

① グループ名
　仮想サーバーグループに付ける任意の名前を入力します。

② 仮想サーバーID 選択
　グルーピングする仮想サーバーID を選択します。

以下の例では my_app という名前のグループを作り、HTTP 仮想サーバー（my_app_http=192.168.1.100.80.tcp）と HTTPS 仮想サーバー（my_app_https=192.168.1.100.443.tcp）を所属させます。ただし、双方の仮想サーバーには IP セッション維持、あるいは X-Forwarded-For セッション維持が設定されているものとします。

以上により、セッション維持設定が、仮想サーバーグループ全体に対して有効となるので、クライアントが仮想サーバーmy_app_http へアクセス後、my_app_https へアクセスすると、そのリクエストは my_app_http が振り分けた実サーバーと同じサーバーに割り振られます（逆の順番でも同じです）。
ひとつのグループには最大で 5 つの仮想サーバーを追加することができます。
ただし、一つの仮想サーバーが複数グループに所属することはできません。

ポイント

タイムアウト設定、マスク設定に関して、buddy グループ内の各仮想サーバーは共通の設定値を使用して動作します。このとき、IP セッション維持設定がされている仮想サーバーの中で、buddy グループの最初に指定されている仮想サーバーの設定情報が buddy グループ内で共有されます。

上の設定例では、my_app_https は my_app_http に設定されたセッション維持設定情報を基に動作します。
これは、my_app_https に設定されたタイムアウト設定やマスク設定が my_app_http と異なる場合や、my_app_https に、セッション維持設定がされていない場合においても同様です。ただし、my_app_http にセッション維持設定がされていない場合は、my_app_https のセッション維持設定情報が buddy グループ内で共有されます。
更には、IP セッション維持が設定されている仮想サーバーと X-Forwarded-For セッション維持が設定されている仮想サーバー間で仮想サーバーグループを形成した場合も、同様に buddy グループの最初に指定されている仮想サーバーのセッション維持設定が有効になります。
buddy グループ内のどの仮想サーバーにもセッション維持設定がされていない場合、buddy グループの各仮想サーバー間でセッション情報を共有することはできません。

3.21.15.4 SSL セッション維持

SSL セッション ID に基づいたセッション維持を設定するには、仮想サーバー設定画面のセッション維持設定項目で「SSL セッション ID」を選択します。

場所: 設定 ＞ バランシング ＞ 仮想サーバー ＞ 仮想サーバー選択 ＞ 仮想サーバー設定

■仮想サーバー基本設定 ＞ セッション維持設定

① セッション維持方法

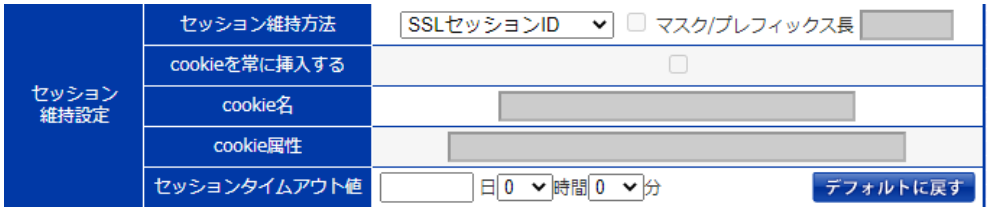
SSL セッション維持を設定するには、「SSL セッション ID」を選択します。

セッション維持を無効にするには「セッション維持 無効」を選択します。

② セッションタイムアウト値

セッション情報のアイドルタイマーを設定範囲から選択します。

「デフォルトに戻す」ボタンを押下した場合 15 分に設定されます。



SSL セッション維持情報は、機器情報画面の「バランシング ＞ SSL セッション維持」で確認できます。

3.21.15.5 cookie セッション維持

cookie に基づいたセッション維持を設定するには、仮想サーバー設定画面のセッション維持設定項目で「cookie」を指定します。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

cookie 情報を基にセッション維持を行うには Cookie セッション維持設定を行います。

仮想サーバー設定画面に遷移してセッション維持設定を変更します。

■仮想サーバー基本設定 > セッション維持設定

① セッション維持方法

Cookie セッション維持を設定するには、「cookie」を選択します。

② cookie 名

cookie 名は実サーバーによって生成され、Set-Cookie ヘッダーで通知される cookie の名前です。

255 文字以内に設定してください。

③ セッションタイムアウト値

セッション情報のアイドルタイマーを設定範囲から選択します。

「デフォルトに戻す」ボタンを押下した場合 30 分に設定されます。

ポイント

cookie 情報は、cookie セッション維持が設定されている全ての仮想サーバー間で共有されます。

URL によるセッション維持は cookie によるセッション維持設定を行うことによって同時に使用可能になります。この場合も web サーバーからのレスポンスに Set-Cookie ヘッダーが含まれていなければなりません。URL によるセッション維持は、cookie セッション維持が設定してあり、クライアントからのリクエストに cookie ヘッダーがなかった場合に行われます。

URLとパラメーターの区切り文字には”;”(セミコロン),“?”(疑問符)が使用できます。パラメーター同士の区切り文字には”&”（アンパサンド）, “?”(疑問符)が使用できます。

cookie 名を sessionid と設定した場合、HTTP リクエストに下記のような URL が含まれると下線部を HTTP cookie と同等のものとして解釈します。
例）
/page.html?sessionid=abcdefg
/page.html;sessionid=abcdefg
/page.html;sessionid=abcdefg?dummy=xxxx
/page.html?dummy=xxxx?sessionid=abcdefg
/page.html?dummy=xxxx&sessionid=abcdefg
/page.html?dummy=xxxx&dummy2=yyyy&sessionid=abcdefg

cookie セッション維持情報は、機器情報画面の「バランシング ＞ cookie セッション維持」で確認できます。

3.21.15.6 cookie 挿入機能

本製品が実サーバーの代わりに生成した cookie をセッション維持に利用するには、仮想サーバー設定画面のセッション維持設定項目で「cookie 挿入」を選択します。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

実サーバーの代わりに生成した cookie をセッション維持に利用するには cookie 挿入機能を設定します。
仮想サーバー設定画面に遷移してセッション維持設定を変更します。

■仮想サーバー基本設定 > セッション維持設定

① セッション維持方法
cookie 挿入機能を有効にするには、「cookie 挿入」を選択します。

② cookie を常に挿入する
「cookie を常に挿入する」を選択した場合、アクセスのたびに cookie の有効期限を更新します。
「cookie を常に挿入する」を選択しなければ、cookie の有効期限は最初のアクセスからの経過時間になります。

③ cookie 名
Set-Cookie ヘッダーで通知される cookie 名を入力します。

④ cookie 属性
Set-Cookie ヘッダーに付加する属性を入力します。

⑤ セッションタイムアウト値
セッション情報のアイドルタイマーを設定範囲から選択します。
0 を選択すると、cookie の保持期間はクライアントがブラウザを閉じるまでとなります。
「デフォルトに戻す」ボタンを押下した場合 0 分に設定されます。

⚠ 注意 cookie 属性で指定した文字列についてはチェックせずにそのまま付加します。指定文字列が属性として正しいことをご確認ください。

3.21.16 仮想サーバーと実サーバーの関連付け

仮想サーバーに実サーバーを関連付けるには、仮想サーバー設定画面の実サーバーバインド設定項目で実サーバーを選択します。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■実サーバーバインド設定

① スイッチングルール
登録したバインド ID を選択します。
スイッチングルールに基づく負荷分散を行わない場合、「設定しない」が選択されます。

② 実サーバーIP、ポート
仮想サーバーに紐づける実サーバーを選択します。
仮想サーバープロトコルと異なるプロトコルであるサーバーを選択しないでください。

③ DSR オプション
DSR(Direct Server Return)構成での負荷分散を行う場合有効にします。

④ 重み
負荷分散の重みづけを行います。
重みに 0 を指定すると、バインド解除と同等の動作になります。重みに 0 指定した場合はバインドを解除した場合と違い、設定ファイル上に設定情報が残ります。そのため、サーバーメンテナンスなどで一時的に仮想サーバーとの関連付けから解除する場合などで使用します。

⑤ backup
バックアップサーバーとして待機させておく場合に選択します。
バックアップサーバーとはプライマリーサーバーが DOWN 状態に変化したときに、プライマリーサーバーに代わって負荷分散対象となるサーバーです。

⑥ overflow

オーバーフローサーバーとして待機させておく場合に選択します。
オーバーフローサーバーとはプライマリーサーバーが最大コネクションに達したときに、プライマリーサーバーに代わって負荷分散対象となるサーバーです。

⑦ 最大コネクション
実サーバーの最大コネクションを設定します。

以下の例では、実サーバー192.168.1.11.80.tcp と実サーバー192.168.1.12.80.tcp に対して 3 対 1 で負荷分散し、かつ実サーバー192.168.1.13.80.tcp をバックアップサーバーとして待機させます。(負荷分散で使用されるプロトコルは、仮想サーバーのプロトコルに依存します)

以下の例では、実サーバー192.168.1.11.80.tcp と実サーバー192.168.1.12.80.tcp に対して最大コネクション数を指定して負荷分散し、かつ実サーバー192.168.1.13.80.tcp をオーバーフローサーバーとして待機させます。

ポイント

同一の実サーバーを複数のバインドグループに所属させる場合、最大コネクションの値は同じである必要があります。そのため最大コネクションの値を設定した場合は、同一の実サーバーの最大コネクションの値が全て最新の値で上書きされます。
以下の設定例では、実サーバー192.168.1.11.80 の最大コネクションの値は全て 3000 に設定されます。

実サーバーバインド設定

削除	スイッチングルール	バインド選択					
		実サーバーIP.ポート	DSR	重み	backup	overflow	最大コネクション
	バインドID：1	192.168.1.11.80	有効		有効	有効	1000
	バインドID：2	192.168.1.11.80	有効		有効	有効	2000
	バインドID：3	192.168.1.11.80	有効		有効	有効	3000

行追加

重みの値も同様に、同一の実サーバーの重みの値が全て最新の値で上書きされます。
また、以下のように、実サーバー192.168.1.11.80 の最大コネクションの値を省略した場合は、同一の実サーバーの最大コネクションの値が適用されます。

実サーバーバインド設定

削除	スイッチングルール	バインド選択					
		実サーバーIP.ポート	DSR	重み	backup	overflow	最大コネクション
	URLスイッチング バインドID：1	192.168.1.11.80		1	有効	有効	1000
	URLスイッチング バインドID：2	192.168.1.11.80		1	有効	有効	1000
	バインドID：3	192.168.1.11.80	有効		有効	有効	

行追加

ポイント

システム全体で実サーバーの受け付ける最大コネクション数を設定することも可能です。このシステム全体の最大コネクション数に達している場合、実サーバーバインド設定で指定した最大コネクション数に達していなくても、コネクション数が制限されます。詳しくは「3.21.2実サーバーの設定」を参照してください。

IP アドレスを基に負荷分散を行う場合「3.21.16.2IP スイッチングの設定」を参照してください。
HTTP ヘッダー情報を基に負荷分散を行う場合「3.21.16.4URL スイッチングの設定」を参照してください。

全ての仮想サーバーと実サーバーの関連付けは、機器情報画面の「バランシング ＞ バインド」で確認できます。

3.21.16.1 バックアップサーバー・オーバーフローサーバーの動作

待機系サーバーの挙動に関して設定を変更するには、仮想サーバー設定画面の基本設定項目で「バックアップポリシー」と「フェイルバック時動作」を設定します。

待機系のサーバーとはバックアップサーバー、またはオーバーフローサーバーに設定された実サーバーを指します。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■仮想サーバー基本設定

① バックアップポリシー

待機系サーバーが active 状態になるタイミングとして、以下のいずれかを選択できます。

■*single*

バックアップサーバー	全てのプライマリーサーバーが DOWN すると、バックアップサーバーが起動（プライマリーへ昇格）します。
オーバーフローサーバー	全てのプライマリーサーバーが最大コネクション数に達すると、オーバーフローサーバーが稼働（プライマリーへ昇格）します。

■*multi*

バックアップサーバー	プライマリーサーバーが 1 台 DOWN すると、バックサップサーバーが起動（プライマリーへ昇格）します。
オーバーフローサーバー	プライマリーサーバーが 1 台最大コネクション数に達すると、オーバーフローサーバーが稼働（プライマリーへ昇格）します。

② フェイルバック時動作

プライマリーに昇格したサーバーが再び待機系に降格した場合の動作を選択します。

「セッション維持情報を使用しない」を選択すると、フェイルバックした際に以降の新規接続要求を強制的にプライマリーサーバーに戻します。

「セッショ維持情報を使用する」を選択すると、待機系サーバーへのセッション維持情報（sticky 情報）を保持したまま、新規セッションからプライマリーサーバーに振り分けます。

ポイント

バックアップポリシーやフェイルバック時動作でどのように設定しても、バックアップサーバーを複数台登録する事が可能です。

待機系サーバーは登録した順に起動（プライマリーへ昇格）します。

更に、ヘルスチェック設定画面で手動復旧を設定することで、ヘルスチェックで DOWN 状態になったサーバーが ALIVE 状態に復帰した際も、負荷分散対象から外したままにしておくことが可能です。

詳細は「3.23クラウド WAF

本章では、本製品のクラウド WAF 連携機能について説明します。

3.21.17 クラウド WAF 連携

クラウド WAF 連携機能を使用すると、本製品を流れる着信トラフィックと発信トラフィックをフィルタリングできます。

クラウド WAF 連携機能は、L7 負荷分散のアクセスログ機能（3.21.13）を使用して、WAF センタールールとシグネチャマッチングをおこないます。攻撃検知対象の場合は、センターから本製品へ遮断命令を送信し、遮断対象 IP アドレスをブロックします。

遮断対象 IP アドレスは IPv4 アドレスとなります。

3.21.18 クラウド WAF 動作イメージ

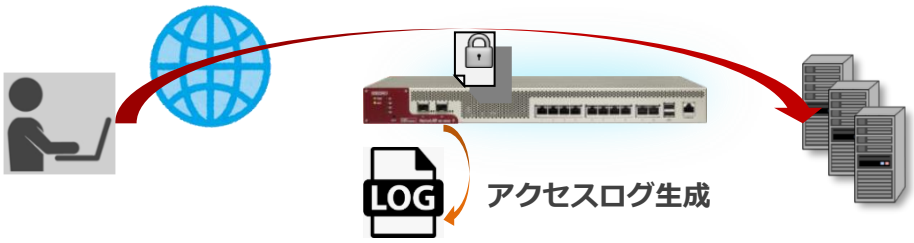
攻撃検知の遮断動作イメージにを以下に示します。

3.21.18.1 アクセスログの生成

① クライアントから Web サーバーへ HTTP リクエストを送信

② Web アプリケーションが HTTP レスポンスを送信

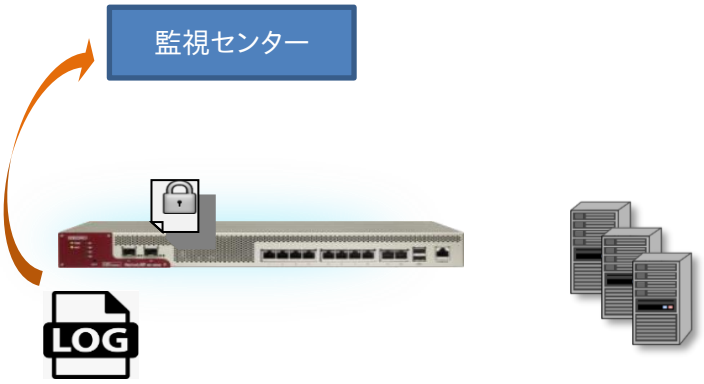
③ 本製品がアクセスログを生成



3.21.18.2 監視センターへログ送信

① アクセスログを収集

② 監視センターへログを送信（UDP）

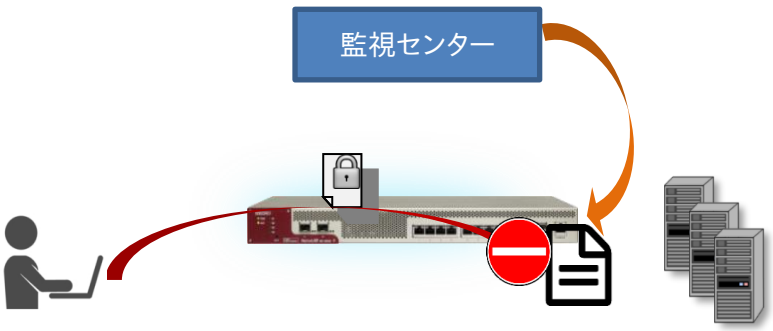


3.21.18.3 遮断命令の送信

① 監視センターで、ログを WAF センタールールとシグネチャマッチング

② 攻撃検知対象の場合は、監視センターから本製品へ遮断命令を送信

③ 遮断対象 IP アドレスを引数に遮断ルールを追加（接続元 IP アドレスの拒否）

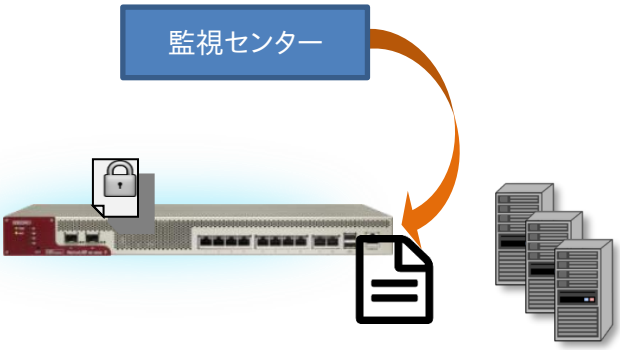


フィルタでブロック

3.21.18.4 ブロック解除命令の送信

① 遮断時間（初期値：10 分間）を経過した場合は、本製品へ遮断解除命令を送信

② 対象 IP アドレスを引数に遮断ルールを削除（接続元 IP アドレスのブロック解除）



ブロック解除

3.21.19 クラウド WAF 連携の有効

クラウド WAF を設定するには、クラウド WAF 設定画面に遷移します。

場所: 設定 > ネットワーク > クラウド WAF

■マネージャーアドレス

マネージャーの IP アドレスまたは IP 名を入力します。

■ポート

マネージャーのポート番号を入力します。

■エージェントキー

エージェントキーを入力します。

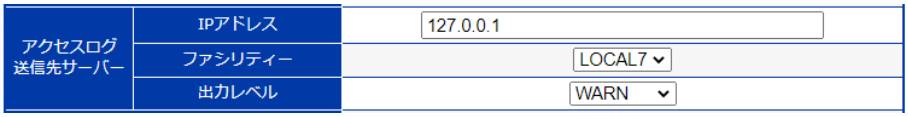
■有効

設定が完了し、クラウド WAF を使用開始するときに有効にします。

クラウド WAF を有効化するとき、設定やネットワーク状況により最大で1分程度時間がかかることがあります。

3.21.20 アクセスログ設定

クラウド WAF を使用する場合は、クラウド WAF を適用する仮想サーバーの設定に以下のようにアクセスログ（3.21.13）を設定します。



通常のアクセスログ設定とは異なり、syslog サーバーのアドレスは外部の IP アドレスではなく、本製品自身(127.0.01)を指定します。また、ファシリティとレベル（local7. LOG_WARNING）を指定します。

アクセスログ機能は L7 負荷分散機能の一部です。アクセスログ機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

3.21.21 アクセスログ表示

本製品で生成されたアクセスログ（3.34.2）を表示するには、**場所: ログ参照 > アクセスログ**を参照ください。

3.21.22 クラウド WAF における防御対象

本製品において防御可能な攻撃を下表に例示します。

攻撃手法
● サーバサイドインクルードインジェクション
● HTTP インジェクション
● LDAP インジェクション
● XML 外部エンティティ
● サーバサイドリクエストフォージェリ
● デシリアライゼーション
● クロスサイトスクリプティング
● SQL インジェクション
● NoSQL インジェクション
● OS コマンドインジェクション
● 改行コードインジェクション
● ディレクトリトラバーサル
● ファイルインクルード攻撃
● URL エンコード攻撃
● ブラックリスト UA
● その他の WEB 攻撃全般
● ミドルウェアなどの脆弱性を突いた攻撃（Apache Struts2 の脆弱性等）

これらの攻撃に対し 100%の防御を保証するものではございません

3.21.23 クラウド WAF における制限事項

● 本製品から監視センターへの通信は UDP プロトコルを利用します。プロトコルの性質上、通信経路で検査対象のログが Drop する可能性があります（監視センターではエージェントからの全ログを受信することを保証していません）。

● 遮断処理は、監視センターに送信されたログを検査後、検知対象の送信元 IP アドレスを遮断対象に登録します（IP アドレスベース遮断）。遮断対象に登録されるまでのリクエストは検知のみを実施します。

● 本製品と監視センター間のステータスが、オフラインからオンラインに変化した場合、オフライン期間のログ情報が監視センターへまとめて送信されます。一度に大量のログが送信された場合、しきい値系のシグネチャで検知/遮断される可能性があります。

ヘルスチェックの設定」を参照してください。

ポイント

複数のサーバーをバックアップサーバー、かつオーバーフローサーバーとして登録して、更にバックアップポリシーで「multi」を選択した場合の待機系サーバーの昇格動作を説明します。

以下の例では

- 実サーバー1(Server1.80)が DOWN 状態になり、実サーバー2(Server2.80)が最大コネクションに達した場合、実サーバー3(Server3.80)がプライマリーサーバーに昇格しバックアップサーバーおよびオーバーフローサーバーとして動作します。
- 実サーバー1 および実サーバー2 が DOWN 状態になった場合、実サーバー3 および実サーバー4(Server4.80)がプライマリーサーバーに昇格しバックアップサーバーとして動作します。
- 実サーバー1 およびサーバー2 が最大コネクションに達した場合、実サーバー3 および実サーバー4 がプライマリーサーバーに昇格しオーバーフローサーバーとして動作します。

実サーバーバインド設定

削除	スイッチングルール	バインド選択					
		実サーバーIP.ポート	DSR	重み	backup	overflow	最大コネクション
☐		Server1.80		1	☐ 有効	☐ 有効	2000
☐		Server2.80		1	☐ 有効	☐ 有効	2000
☐		Server3.80		1	☑ 有効	☑ 有効	0
☐		Server4.80		1	☑ 有効	☑ 有効	0
	バインドID：設定なし	指定しない	☐ 有効		☐ 有効	☐ 有効	

行追加

3.21.23.1 IP スイッチングの設定

クライアントの IP アドレスを基に負荷分散先を決定するには、仮想サーバー設定画面の「バインド ID 登録」で IP アドレス負荷分散のルールと、バインド ID を登録してから、仮想サーバーと実サーバーを関連付けます。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■バインド ID 登録

① 負荷分散方法選択

IP アドレス負荷分散を設定する場合、「バインド ID 登録」で、「バインド ID を登録する（IP アドレス負荷分散）」を選択します。

■バインド ID 登録（IP アドレス負荷分散）

① XFF ヘッダー情報の参照

X-Forwarded-For スイッチングを行う場合「有効」を選択します。

詳細は「3.21.23.2 X-Forwarded-For スイッチングの設定」を参照してください。

② バインド ID

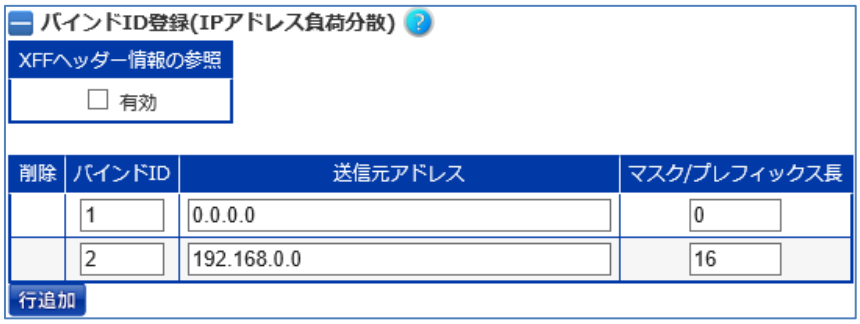
バインド設定時に使用するための ID を定義します。

③ 送信元アドレス、マスク/プレフィックス長

送信元ネットワークアドレスを定義します。

送信元アドレスとマスク/プレフィックス長に 0.0.0.0/0 や::/0 を設定すると、それぞれのアドレスファミリーのデフォルトルールを設定することができます。デフォルトルールの設定を行うことで、任意のスイッチングルール以外のアクセスに対する振り分け先グループを設定することが可能です。

以下の例では、クライアントの IP が 192.168.0.0/16 のアクセスをバインド ID 2 として登録し、その他の IP からのアクセスをバインド ID 1 とする IP スイッチングルールを登録します。



ポイント

一つの仮想サーバーID に対して IP スイッチングと URL スイッチングを同時に設定することはできません。

ポイント

IP スイッチングの設定をした場合、グループ ID を指定して実サーバーと仮想サーバーを関連付けないと負荷分散対象になりません。

ポイント

範囲が重複するネットワークアドレスが複数登録された場合、ネットワーク範囲の一番狭い設定行から優先して評価されます。

⚠ 注意

仮想サーバーのアドレスファミリーと異なるアドレスファミリーのスイッチングルールを設定すると、IP アドレス負荷分散は正しく動作しません。

次に、バインド ID を指定して仮想サーバーと実サーバーを関連付けます。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■実サーバーバインド設定

① スイッチングルール
「バインド ID 登録(IP アドレス負荷分散)」で設定した ID を選択します。

② 実サーバーIP、ポート
仮想サーバーに紐づける実サーバーを選択します。
仮想サーバープロトコルと異なるプロトコルであるサーバーを選択しない

でください。

③ DSR オプション
DSR(Direct Server Return)構成での負荷分散を行う場合有効にします。

④ 重み
負荷分散の重みづけを行います。

⑤ backup
バックアップサーバーとして待機させておく場合に選択します。

⑥ overflow
オーバーフローサーバーとして待機させておく場合に選択します。

⑦ 最大コネクション
実サーバーの最大コネクションを設定します。

以下の例では、バインド ID 1 にマッチしたアクセスは 192.168.1.10.80 に、バインド ID 2 にマッチしたアクセスは 192.168.1.11.80 か 192.168.1.12.80 に負荷分散されます。

3.21.23.2 X-Forwarded-For スイッチングの設定

X-Forwarded-For ヘッダー情報に明示された IP アドレスを基に IP アドレススイッチングを行うことが可能です。これにより、X-Forwarded-For ヘッダーにクライアントの IP アドレス情報が埋め込まれてさえいれば、プロキシサーバーを経由するなどして IP アドレスが隠蔽されている場合においても、クライアント IP アドレスに基づく負荷分散先の決定が可能です。

X-Forwarded-For スイッチングを設定するには、IP スイッチングの設定を行う際に、「XFF ヘッダー情報の参照」を有効にします。
IP スイッチングの設定の詳細は「3.21.23.1 IP スイッチングの設定」を参照してください。

HTTP リクエスト内に X-Forwarded-For ヘッダーが存在しない場合、IP ヘッダーの送信元アドレス情報を基に負荷分散先が決定されます。また、
X-Forwarded-For ヘッダーに複数の IP アドレス情報が明示されている場合は、先頭の IP アドレス情報を参照します

ポイント

X-Forwarded-For スイッチング設定は L7 負荷分散機能の一部であるため、設定された仮想サーバーに対する全てのリクエストは L7 レベルで処理されます。その点で IP アドレススイッチング設定とは異なります。

ポイント

一つの仮想サーバーID に対して X-Forwarded-For スイッチングと URL スイッチングを同時に設定することはできません。

⚠ 注意

仮想サーバーIP のアドレスファミリーと、X-Forwarded-For ヘッダーにセットされた IP アドレスのアドレスファミリーが一致しない場合、X-Forwarded-For スイッチングは正しく動作しません。

3.21.23.3 URL スイッチングの設定

URL や HTTP ヘッダーに含まれる文字列によって負荷分散を行う場合、事前に URL スイッチングルール設定画面で、スイッチングルールの登録を行います。

場所: 設定 > バランシング > 仮想サーバー > URL スイッチングルール設定

■URL スイッチングルール設定

① ルール名

スイッチングルールのポリシー名を定義します。

② ルールタイプ

スイッチングルールのタイプを選択します。

■ホストヘッダー

HTTP リクエストヘッダーの Host ヘッダー値によるルールを定義します。

ルール内容入力例: www.seiko-sol.co.jp

■HTTP メソッド

HTTP リクエストヘッダーのメソッド種別によるルールを定義します。

ルール内容入力例: GET

■パス

HTTP リクエストヘッダーのリクエストパスによるルールを定義します。

ルール内容入力例: /home.html

■ユーザーエージェント

HTTP リクエストヘッダーの User-Agent ヘッダー値によるルールを定義します。

ルール内容入力例: !mozilla/4.*

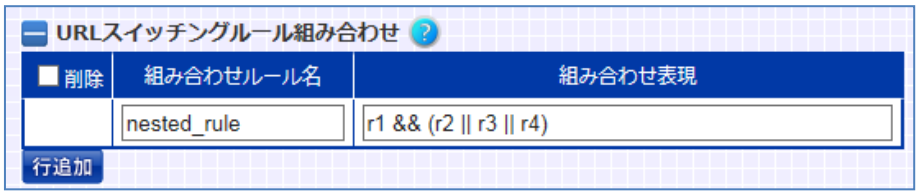
③ ルール内容

スイッチングルールのタイプに沿った任意の文字列を入力します。

ポイント

文字列が HTTP メソッドの場合、大文字と小文字を区別します。また、文字列が HTTP メソッドの場合、ワイルドカード（＊）を含んではなりません。
ワイルドカード（＊）は以下のように使用します。
　例）　"string*"(前方一致)、"*string(後方一致) "、"*string*" (部分一致)
また、先頭に NOT (!) を付けるとその文字列以外を表します。

また、複数のルールを組み合わせて別のルールを定義することも可能です。
■URL スイッチングルール組み合わせ
① 組み合わせルール
　組み合わせルールのポリシー名を定義します。
② 組み合わせ表現
　最大 4 個までのルールを以下のように AND (&&) または OR (||) 演算子で組み合わせることで設定します。
　AND で結ばれたルールは全てがマッチした際に真と判断されます。
　OR で結ばれたルールはどれかひとつでもマッチすると真と判断されます。



ポイント

ルールを AND (&&) や OR (||) 演算子で組み合わせる場合、演算子の前後はブランクが必要です。

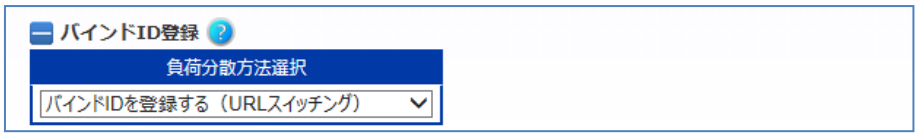
次に、仮想サーバー設定画面の「バインドID登録」で、使用するURLスイッチングルールと、バインド ID を登録してから、仮想サーバーと実サーバーを関連付けます。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■バインド ID 登録

① 負荷分散方法選択

URL スイッチングを設定する場合、「バインド ID 登録」で、「バインド ID を登録する（URL スイッチング）」を選択します。



■バインド ID 登録（URL スイッチング）

① バインド ID

バインド設定時に使用するための ID を定義します。

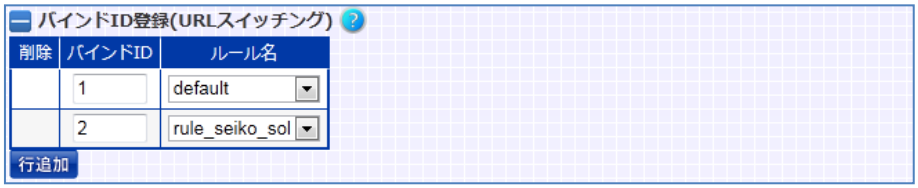
② ルール名

登録済みの URL スイッチングルールを選択します。

ルール名に「default」を選択することでデフォルトルールのバインド ID を定義できます。

ひとつの仮想サーバーに最大 31 個のルールを登録することができます。

以下の例では、rule_seiko_sol にマッチするアクセスをバインド ID 2 として登録し、その他のアクセスをバインド ID 1 として登録します。



次に、バインド ID を指定して仮想サーバーと実サーバーを関連付けます。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■実サーバーバインド設定

① スイッチングルール
「バインド ID 登録（URL スイッチング）」で設定した ID を選択します。

② 実サーバーIP、ポート
仮想サーバーに紐づける実サーバーを選択します。
仮想サーバープロトコルと異なるプロトコルであるサーバーを選択しないでください。

③ DSR オプション
DSR(Direct Server Return)構成での負荷分散を行う場合有効にします。
ただし、URL スイッチングと同時に設定することはできません。

④ 重み
負荷分散の重みづけを行います。

⑤ backup
バックアップサーバーとして待機させておく場合に選択します。

⑥ overflow
オーバーフローサーバーとして待機させておく場合に選択します。

⑦ 最大コネクション
実サーバーの最大コネクションを設定します。

以下の例では、バインド ID 1 にマッチしたアクセスは 192.168.1.10.80 に、バインド ID 2 にマッチしたアクセスは 192.168.1.11.80 か 192.168.1.12.80 に負荷分散されます。

ポイント

リクエストがどのルールにも一致せず、かつデフォルトルールのバインド ID が割り当てられたサーバーがない場合、そのリクエストは破棄されます。

ポイント

リクエスト受信時に、振り分け先候補として複数グループが該当する場合は、「バインド ID 登録（URL スイッチング）」テーブルにて入力した設定順序（グループ ID を割り当てた順序）で、負荷分散対象のバインドグループが選定されます。

3.21.23.4 HTTP リダイレクションとエラーレスポンスの設定

特定のルールに合致した HTTP リクエストを本製品が別の URL にリダイレクトさせたり、403 エラーレスポンスを返すように設定することができます。

リダイレクト設定や 403 応答設定を行うには、初めに「URL スイッチングルール」を登録します。URL スイッチングルールの登録は「3.21.23.3URL スイッチングの設定」を参照してください。

次に、リダイレクト設定を行う場合は、仮想サーバー設定画面の「URL リダイレクト設定」項目を設定します。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

URL スイッチングルールの登録後、URL リダイレクトの設定を行います。

■URL リダイレクト設定

① ルール名
スイッチングルールのポリシー名を選択します。
「default」を選択した場合、デフォルトルールが適用されます。

② プロトコル
リダイレクト先スキームを選択します。

③ ドメイン
リダイレクト先のドメインを指定します。
ドメインにワイルドカード（＊）を指定すると、リダイレクト先のドメインは元のリクエストと同じになります。
ドメインに IPv6 アドレスを使用する場合は大括弧（[ ]）で囲う必要があります。

④ リダイレクト先パス
リダイレクト先のパスを指定します。
ワイルドカード（＊）を指定すると、リダイレクト先の URL パスは元のリクエストと同じになります。

⑤ リダイレクト先ポート
リダイレクト先スキームが http で 80 以外のポート、または https で 443 以外のポートにリダイレクトしたい場合に任意のポート番号を指定します。

以下の例では、仮想サーバーへのリクエストがルール r2 に合致する場合、リクエストを http://newdomain.com/newurl.html へリダイレクトします。
また、仮想サーバーへのリクエストがルール r3 に合致する場合、リクエストを https へリダイレクトします（このとき、ドメインやパスは変更しません）。

更に、403 応答設定を行う場合は、仮想サーバー設定画面の「403 応答設定」項目を設定します。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

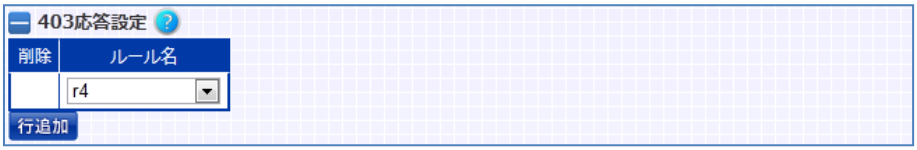
■403応答設定

① ルール名

スイッチングルールのポリシー名を選択します。

選択したルールに合致したリクエストに対して403エラーレスポンスを応答します。

以下の例では、仮想サーバーへのリクエストがルール r4 に合致する場合、クライアントに 403 レスポンスが応答されます。



仮想サーバーに対し、URL スイッチング、HTTP リダイレクション、403 応答を同時に設定することができます。

ポイント

これらの設定を行う場合、実サーバーバインド設定には必ずグループ番号を割り当てる必要があります。グループ番号は任意の数字で構いません。

3.21.23.5 Location ヘッダーの書き換え

本製品の SSL アクセラレーション機能を使用すると、実サーバーが返す 300 番台のレスポンスのリダイレクト先が https ではなく http になってしまうことがあります。
この問題を回避するには location ルール設定画面で location ルールを定義し、仮想サーバー設定画面の URL リダイレクト設定項目で正しい URL を設定します。

初めに、location ルール設定画面で、サーバーのリダイレクト応答に含まれる Location ヘッダーを置換するためのルールを定義します

場所: 設定 > バランシング > 仮想サーバー > location ルール設定

■location ルール設定

① ルール名
ルールにマッチさせたいスイッチングルールのポリシー名を定義します。

② プロトコル
ルールにマッチさせたいリダイレクト先のスキームを選択します。

③ ドメイン
ルールにマッチさせたいリダイレクト先のドメインを入力します。

④ パス
ルールにマッチさせたいリダイレクト先のパスを入力します。

以下の例では、Location ヘッダーの値が http://www.seiko-sol.co.jp/bar/ で始まる場合にマッチするルールを登録します。

ポイント location ルールのドメインとパスは大文字と小文字を区別しません。また、文

字列の前後にワイルドカード（＊）を付けて、先頭、末尾または任意の部分を指定することができます。更に、先頭に NOT (!) を付けるとその文字列以外を表します。ワイルドカード（＊）だけの場合は任意の文字列を表します。

次に、仮想サーバー設定画面の URL リダイレクト設定項目で正しい URL を設定します。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

次に、仮想サーバー設定画面に遷移して「URL リダイレクト設定」を設定します。

■URL リダイレクト設定

① ルール名
登録した location ルールのポリシー名を選択します。

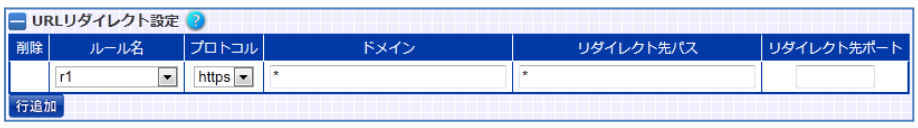
② プロトコル
リダイレクト先スキームを選択します。

③ ドメイン
リダイレクト先を変更させたい場合は、任意のドメインを指定します。
ドメインにワイルドカード（＊）を指定すると、リダイレクト先を書き換えません。

④ リダイレクト先パス
リダイレクト先のパスを変更させたい場合は、任意の URL パスを指定します。URL にワイルドカード（＊）を指定すると、リダイレクト先のパスを書き換えません。

⑤ リダイレクト先ポート
リダイレクト先スキームが http で 80 以外のポート、または https で 443 以外のポートにリダイレクトしたい場合に任意のポート番号を指定します。
省略するとポート番号の書き換えは行いません。

以下の例では、Location ヘッダーの値が事前に登録したルール r1 に合致する場合、https に書き換えます。「ドメイン」、「リダイレクト先パス」にはワイルドカード（＊）を指定しているため、書き換えは行いません。



ポイント

これらの設定を行う場合、実サーバーバインド設定には必ずグループ番号を割り当てる必要があります。グループ番号は任意の数字で構いません。

3.21.23.6 sorry コンテンツの設定

実サーバーの障害時や過負荷状況、またはメンテナンスなど、なんらかの理由で HTTP リクエストの振り分けが出来ない場合、サービスが提供できない旨の代替コンテンツを本製品から返信することが可能です。当該コンテンツを「sorry コンテンツ」と呼称します。
本製品は、以下のいずれかの状況になると sorry コンテンツでの応答を行います。

- 仮想サーバーに実サーバーが1台もバインドされていない
- バインドされている全ての実サーバーが DOWN 状態になっている
- バインドされている全ての実サーバーが無効設定になっている
- バインドされている全ての実サーバーのコネクション数が最大コネクション数に達してしまっている

この機能を有効にするには、sorry コンテンツインポート画面で代替コンテンツを本製品にインストールします。
sorry コンテンツのインポートは「5.3.1.5sorry コンテンツのインポート」を参照してください。

インポートが完了したら、仮想サーバー設定画面の基本設定項目で、仮想サーバーと sorry コンテンツを関連付けます。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■仮想サーバー基本設定

① sorry コンテンツを使用する
　インポートした sorry コンテンツを選択します。

ポイント

sorry コンテンツ機能は L7 負荷分散機能の一部です。sorry コンテンツをバインドすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

ポイント

バインド中の sorry コンテンツと同じ名前のコンテンツ名を指定して新規にファイルをインポートした場合、仮想サーバーから当該コンテンツを解除し、仮想サーバーへ割り当て直してください。

ポイント

代替コンテンツは HTML 形式のみサポートします。また、以下の制約があります。

■コンテンツ名

コンテンツ名は 16 文字以内の半角英数字または半角記号で、先頭は数字であってはいけません。また、使用可能な記号はハイフン(-)、アンダーバー(_)のみです。

■コンテンツサイズ

インポートするコンテンツサイズは 4500 バイト以内でなければなりません。

■コンテンツ内容

コンテンツ内に、画像ファイルなどへのリンクを含んではなりません。

コンテンツは、以下の例のようにコンテンツの文字コードを表す META タグと、ブラウザにキャッシュされるのを防ぐための META タグを HEAD 部に含めてください。

```
<HTML>
    <HEAD>
        <TITLE>OUT OF SERVICE</TITLE>
        <META http-equiv="Content-Type" content="text/html; ch
arset=shift_jis">
        <META http-equiv="Pragma" content="no-cache">
        <META http-equiv="Cache-Control" content="no-cache">
        <META http-equiv="Expires" content="0">
    </HEAD>
    <BODY>
        <H2>ただいまサーバーが混雑しています。しばらく経ってか
ら再度接続してください。</H2>
    </BODY>
</HTML>
```

インポートしたsorryコンテンツはそのままで使用可能な状態ですが、フラッシュ

メモリーには保存されていません。
ファイルインポート後は、「保存する」ボタンで設定を保存してください。

3.21.23.7 全実サーバーDOWN 時のリダイレクト先 URL

実サーバーの障害時や過負荷状況、またはメンテナンスなど、なんらかの理由で HTTP リクエストの振り分けが出来ない場合に 302 レスポンスを返し、任意の URL にリダイレクトさせることが可能です。

以下のいずれかの状況になると 302 応答を行います。

- ✓ 仮想サーバーに実サーバーが1台もバインドされていない
- ✓ バインドされている全ての実サーバーが無効になっている
- ✓ バインドされている全ての実サーバーが DOWN 状態、またはコネクション数が最大数に達した状態のいずれかの状態になっている

この機能を有効にするには、仮想サーバー設定画面の基本設定項目で、リダイレクト先の URL を設定します。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■仮想サーバー基本設定

① 全実サーバーDOWN 時のリダイレクト先 URL

リダイレクト先 URL

ポイント

sorry コンテンツの設定と全実サーバーDOWN 時のリダイレクト先 URL の設定が同時に設定されている場合は、全実サーバーDOWN 時のリダイレクト先 URL の設定が優先されます。

ポイント

全実サーバーDOWN 時のリダイレクト機能は L7 負荷分散機能の一部です。全実サーバーDOWN 時のリダイレクト先 URL の設定をすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

3.21.23.8 DSR（Direct Server Return）

仮想サーバーに関連付ける実サーバーを DSR モードで動作させた場合、実サーバーからの送信パケットはロードバランサーを経由せず直接クライアントコンピュータへ返送されます。このため、ロードバランサーの処理を軽減させることが可能となります。

実サーバーを DSR モードで動作させる場合、仮想サーバー設定画面の実サーバーバインド設定項目で、実サーバーと仮想サーバーを関連付ける際に DSR オプションを有効にします。

場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■実サーバーバインド設定

① スイッチングルール
登録したバインド ID を選択します。
スイッチングルールに基づく負荷分散を行わない場合、「設定なし」を選択します。
実サーバーを DSR モードで動作させる場合、URL スイッチングは設定できません。

② 実サーバーIP、ポート
仮想サーバーに紐づける実サーバーを選択します。
仮想サーバープロトコルと異なるプロトコルであるサーバーを選択しないでください。

③ DSR オプション
DSR(Direct Server Return)構成での負荷分散を行う場合有効にします。

④ 重み
負荷分散の重みづけを行います。

⑤ backup
バックアップサーバーとして待機させておく場合に選択します。

⑥ overflow
オーバーフローサーバーとして待機させておく場合に選択します。

⑦ 最大コネクション
実サーバーの最大コネクションを設定します。

ポイント

DSR モードで使用する場合、実サーバーのループバックアドレスに仮想サーバーIP アドレスを登録する必要があります。
また、ループバックインターフェイスは ARP リクエストの送信、ARP リクエストへの応答を行わないよう設定する必要があります。
詳しくは「4.9.1DSR 実サーバーの設定例」を参照してください。

ポイント

DSR モードで使用する場合バインドする実サーバーに対して、ヘルスチェックを必ず設定してください。

3.21.23.9 FTP-DATA ポート

設定は仮想サーバ設定画面で実施します。

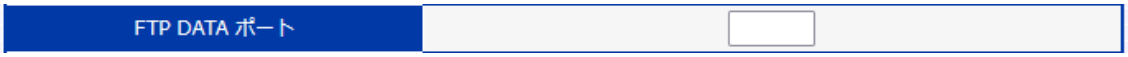
場所: 設定 > バランシング > 仮想サーバー > 仮想サーバー選択 > 仮想サーバー設定

■FTP-DTA ポート設定

FTP のアクティブモード接続時、FTP サーバーから接続される FTP データコネクトの発ポートを指定します。通常は指定不要です。

・指定がないとき（初期値）は、制御ポートから1を引いたポート番号を使用します。

・仮想サーバが FTP 設定ではないとき(ポートが 21 以外かつプロトコルが ftp 以外)、入力された値は意味を持ちません。



3.21.24 実サーバーIP アドレスの変換

実サーバーから開始されるコネクションの送信元 IP アドレスを任意の NAT プールアドレスに変換するには、リバース NAT の設定を行います。

変換に使用するアドレスは、事前に NAT プールアドレスとして登録されている必要があります。
NAT プールアドレスの登録は「3.21.9送信元アドレスの変換」を参照してください。

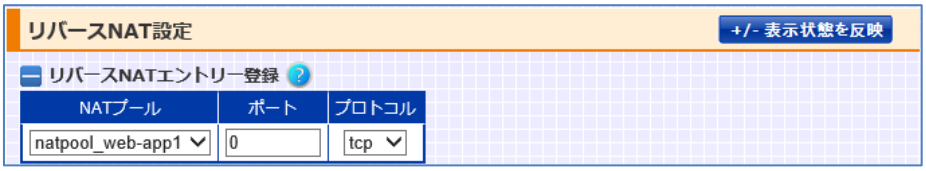
次に、リバース NAT 設定画面で、登録済み NAT プールを使用してリバース NAT 設定を定義します。

場所: 設定 > バランシング > 仮想サーバー > リバース NAT

■リバース NAT エントリー登録

① NAT プール
登録済みの NAT プールエントリーを選択します。
指定した NAT プールエントリー内で定義されたアドレスプールが変換に使用されます。

② ポート、プロトコル
変換に使用する送信元ポート番号、プロトコルを定義します。



次に、変換対象となるサーバーを登録します。

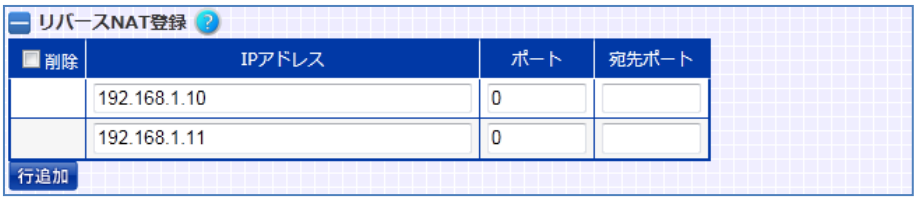
■リバース NAT 登録

① IP アドレス
変換対象とするサーバーの IP アドレスを指定します。
ただし、指定した NAT プールアドレスと異なるアドレスファミリーのサーバ IP を登録しても動作しません。

② ポート

変換対象とする送信元ポート番号を指定します。
0 を指定すると、全てのポート番号を変換対象にします。

③ 宛先ポート
変換対象とする宛先元ポート番号を指定します。
省略可能です。



リバース NAT 設定では、送信元ポート番号を以下のルールで変換します。

「リバース NAT エントリー登録」で指定するポート番号（VP）	「リバース NAT 登録」で指定するポート番号（RP）	変換ルール
任意の数値	任意の数値	送信元ポート番号が RP なら VP に変換
任意の数値	0	送信元ポート番号が 1024 未満ならそのままで、1024 以上なら VP に変換
0	任意の数値	送信元ポート番号が RP なら 1024 以上の未使用ポート番号に変換
0	0	送信元ポート番号が 1024 未満ならそのままで、1024 以上なら 1024 以上の未使用ポート番号に変換

ポイント

リバース NAT 登録で設定したサーバーのポート番号が 0 ではなく、かつそのサーバーが実サーバーとして定義されているサーバーに対して、ポート番号、プロトコル含めて合致する場合、サーバーから発信されるコネクションもそのサーバ

一のコネクション数にカウントされるため、負荷分散や最大コネクション数に影響します。

機器情報画面の「バランシング ＞NATプール」で、NATプールアドレスの使用状況を参照できます。

また、リバースNATの有効/無効やルートID、リバースNATセッションのアイドルタイムを設定することができます。

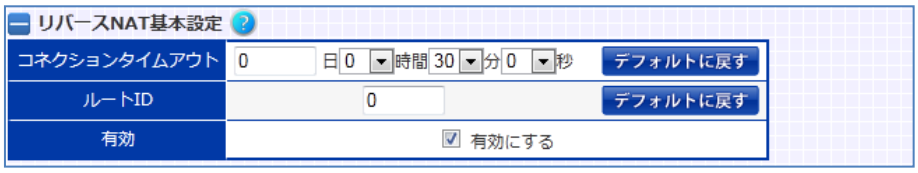
リバースNAT設定画面ではリバースNATで使用するルーティングテーブルのルートIDを設定できます。ルートIDが設定されている場合は、リバースNATの対象となるパケットがリバースNATに設定されたルートIDと同一のIDを持つルーティングテーブルに従います。

■リバースNAT基本設定

① コネクションタイムアウト
リバースNATセッションのアイドルタイムを選択します。

② ルートID
リバースNATで使用するルーティングテーブルのルートIDを設定します。
設定できるルートIDの範囲は0から15です。

③ 有効
リバースNAT設定を有効にする場合選択します。



ポイント

ワンアーム構成の場合には実サーバーIPアドレスの変換は動作しません。
インライン構成の場合にのみ利用可能です。

3.21.25 NAT ログ情報の送信

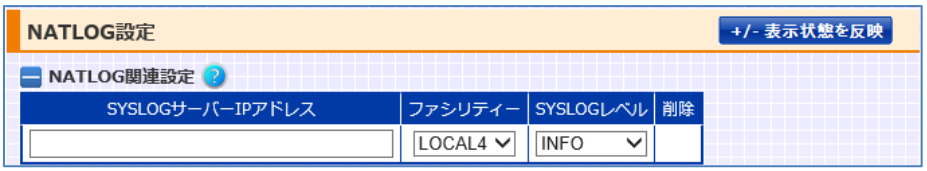
本製品の負荷分散機能によって NAT 変換された IP アドレスのログを外部の syslog サーバーへ送信することが可能です。
設定は NATLOG 設定画面で実施します。

場所: 設定 > システム > NATLOG 設定

■NATLOG 設定

① SYSLOG サーバーIP アドレス
送信先に指定する SYSLOG サーバーの IP アドレス（または IP アドレス名）を設定します。

② ファシリティー、SYSLOG レベル
syslog サーバーに送信されるメッセージのファシリティーと、送信するログの下限レベルを選択します。



ファシリティー、ログレベルを表す数値の対応を以下に明記します。

ファシリティー		レベル	
LOCAL0	16	emerg	0
LOCAL1	17	alert	1
LOCAL2	18	crit	2
LOCAL3	19	err	3
LOCAL4	20	warn	4
LOCAL5	21	notice	5
LOCAL6	22	info	6
LOCAL7	23	debug	7

以下の形式でメッセージを生成します。形式を変更することはできません。

<日時分> <ﾎｽﾄ名> PCB CREATED: <ﾌﾟﾛﾄｺﾙ> <送信元 IP>.<ﾎﾟｰﾄ> -> <仮想サーバーIP>.< ﾎﾟｰﾄ> -> <仮想サーバーIP>.< 送信元ﾎﾟｰﾄ> -> <実サーバーIP>.<ﾎﾟｰﾄ>

以下に、実際に送出されるメッセージの例を示します。

```
Sep  2 16:56:24 netwiser PCB CREATED: tcp 10.208.11.146.49278
-> 10.208.10.95.80 -> 10.208.10.95.1025 -> 10.208.11.145.80
```

ポイント

本設定は SYSLOG 設定状態と関連していません。また、生成されたログは本製品内部の SYSLOG ファイルには残りません。

3.22 SSL アクセラレーションの設定

SSL による暗号通信を復号化し各サーバーに負荷分散することで、サーバーの SSL 通信による処理負荷を軽減させます。
本章では SSL アクセラレーションに関する設定方法を例とともに記します。

3.22.1 SSL アクセラレーション機能の仕様

本製品で対応する公開鍵方式、SSL バージョン、暗号スイート、証明書形式について、以下に明記します。

■対応する暗号スイート

暗号スイート	SSL 3.0	TLS 1.0	TLS 1.2	DTLS 1.0	DTLS 1.2
DES-CBC-SHA	○	○	×	○	×
DES-CBC3-SHA	○	○	○	○	○
AES128-SHA	○	○	○	○	○
AES256-SHA	○	○	○	○	○
DHE-RSA-AES128-SHA	×	×	○	×	○
DHE-RSA-AES256-SHA	×	×	○	×	○
AES128-SHA256	×	×	○	×	○
AES256-SHA256	×	×	○	×	○
DHE-RSA-AES128-SHA256	×	×	○	×	○
DHE-RSA-AES256-SHA256	×	×	○	×	○
AES128-GCM-SHA256	×	×	○	×	×
AES256-GCM-SHA384	×	×	○	×	×
DHE-RSA-AES128-GCM-SHA256	×	×	○	×	×
DHE-RSA-AES256-GCM-SHA384	×	×	○	×	×
ECDHE-RSA-AES256-GCM-SHA384	×	×	○	×	×
ECDHE-ECDSA-AES256-GCM-SHA384	×	×	○	×	×
ECDHE-RSA-AES256-SHA384	×	×	○	×	○
ECDHE-ECDSA-AES256-SHA384	×	×	○	×	○
ECDHE-RSA-AES256-SHA	×	×	○	×	○
ECDHE-ECDSA-AES256-SHA	×	×	○	×	○
ECDHE-RSA-AES128-GCM-SHA256	×	×	○	×	×

ECDHE-ECDSA-AES128-GCM-SHA256	×	×	○	×	×
ECDHE-RSA-AES128-SHA	×	×	○	×	○
ECDHE-RSA-AES128-SHA256	×	×	○	×	○
ECDHE-ECDSA-AES128-SHA	×	×	○	×	○
ECDHE-ECDSA-AES128-SHA256	×	×	○	×	○

※ SX-3920 では ECDHE 系の暗号スイートに対応していません

※ DTLS1.2 では、クライアント認証が有効の時だけ "DHE-RSA-AES128-SHA"、"DHE-RSA-AES256-SHA"をサポートします。クライアント認証が無効の時は、これらの暗号スイートは SSL ネゴシエーション時に選択されません。

■対応する証明書形式

- DER Encoded Binary X.509（鍵・証明書）。
- Base64 Encoded X.509（鍵・証明書）。
- PKCS#12（鍵＋証明書）
- Base64 Encoded PKCS#10（署名要求のエクスポート）

⚠ 注意 テスト証明書では ECDHE-ECDSA 系の暗号スイートを利用することは出来ません。

3.22.2 SSL ポリシーの作成

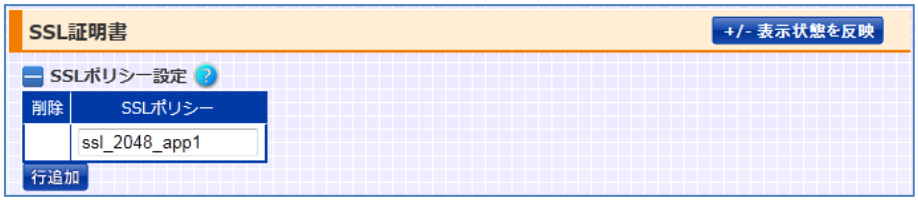
SSL アクセラレーションの設定を行うにはまず SSL 関連ファイルを管理するための SSL ポリシーを作成する必要があります。
SSL ポリシーの作成は、SSL ポリシー設定画面で実施します。

場所: 設定 > SSL > SSL 証明書

SSL アクセラレーションを行うための事前準備として、SSL ポリシーを作成します。

■SSL ポリシー設定

① SSL ポリシー
SSL ポリシーのための名前を入力します。



test オプションを指定して SSL ポリシーを作成すると、テスト用の証明書、秘密鍵、中間証明書がインポートされた状態の SSL ポリシーを作成することができます。
テスト用の証明書や鍵は、"SSL ポリシー名 test"という形式でポリシー名を入力する事で作成できます。

ポイント

テスト用証明書は正規の認証局が発行した証明書ではありません。SSL アクセラレーション機能の動作テスト以外の目的には使用しないでください。

⚠ 注意

WEB 画面では、SSL 証明書自動更新のプレフィックスにマッチする SSL ポリシーを追加、変更、削除することは出来ません。
どうしても必要な場合は CLI 画面から行ってください。

3.22.3 電子証明書と鍵のインポート

Web サーバーが OpenSSL を用いた Apache, Apache-SSL, stronghold の場合は既存のサーバーの鍵と電子証明書を取得する方法が公開されていますので、サーバー情報を取得し本製品にインポートして使用します。
鍵ファイル、電子証明書ファイル、中間証明書ファイルの取得は各サーバー用のソフトウェアマニュアルを参照してください。
ファイルの転送をするためにはネットワークを使用して本製品にインポートする必要があります。
署名アルゴリズム SHA-1,MD5,SHA-2 ファミリー(SHA224, SHA256, SHA384, SHA512)で署名されたサーバー電子証明書のインポートが可能です。

Web サーバーから鍵ファイル、電子証明書ファイル、中間証明書を取得しメンテナンス用パソコンに保存します。

まず、SSL ポリシーが作成されている必要があります。SSL ポリシーの作成は「3.22.2SSL ポリシーの作成」を参照してください。
次に、SSL インポート画面から電子証明書や秘密鍵のインポートを実施します。

場所: 設定 > SSL > SSL インポート
SSL 証明書や秘密鍵を機器にインポートします。
■ファイル選択
① SSL ポリシー名
任意の登録済み SSL ポリシーを選択します。
② PKCS12 形式
インポートする PKCS12 形式のファイルを選択します。
PKCS12 形式のファイルを選択した場合、「秘密鍵」や「サーバー証明書」、「中間証明書」は選択しないでください。
③ 秘密鍵
インポートする秘密鍵のファイルを選択します。
RSA 秘密鍵は 1024bit、2048bit、4096bit に対応します。
ECC 秘密鍵は EC 名前付き曲線 secp256r1、secp384r1 に対応します。
秘密鍵を選択した場合、「PKCS 形式」は選択しないでください。

④ パスフレーズ

PKCS12 形式、または秘密鍵のいずれかをインポートする場合で、かつファイルがパスワードで守られている場合、パスフレーズを入力してください。

⑤ サーバー証明書

インポートするサーバー証明書ファイルを選択します。

サーバー証明書を選択した場合、「PKCS 形式」は選択しないでください。

⑥ 中間証明書

インポートする中間証明書ファイルを選択します。

中間証明書を選択した場合、「PKCS 形式」は選択しないでください。

既に中間証明書がインポートされている場合、「上書き」または「階層化」が選択可能です。

「上書き」を選択した場合、既存の中間証明書を上書きしてインポートます。

「階層化」を選択した場合、既存の中間証明書にチェーンします。

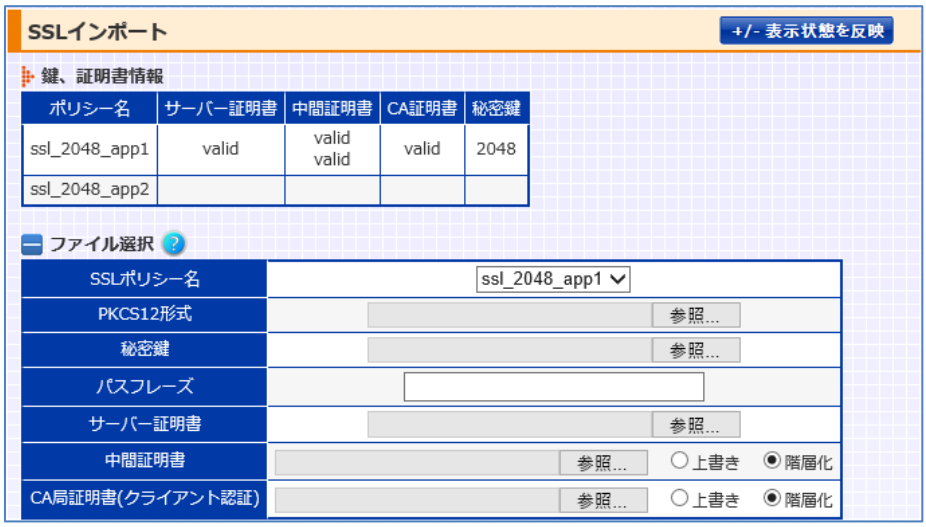
⑦ CA 証明書（クライアント認証）

インポートする CA 証明書ファイルを選択します。

既に中間証明書がインポートされている場合、「上書き」または「階層化」が選択可能です。

「上書き」を選択した場合、既存の CA 証明書を上書きしてインポートます。

「階層化」を選択した場合、既存の CA 証明書にチェーンします。



ポイント

冗長構成で、かつ冗長相手とコマンドの同期が可能な状態であれば、自機器にインポートした証明書や鍵はピア側の機器にコピーされます。

ポイント

証明書を多段インポートする場合、必ず以下の順序で証明書のインポートを行ってください。

- 一段目の証明書： サーバー証明書（あるいはクライアント証明書）を署名する証明書
- 二段目の証明書： 一段目の証明書を署名する証明書

インポートした鍵や証明書ファイルを取り出す事ができます。詳細は「5.3.2.4 SSL 関連ファイルのエクスポート」を参照してください。
また、機器情報画面の「SSL > SSL アクセラレーション」で、証明書や秘密鍵のインポート状態と SSL アクセラレーション処理の統計情報を参照することができます。

ポイント

二段にチェーンされた中間証明書（あるいはクライアント CA 証明書）を 1 ファイルにまとめてインポートすることも可能です
ただし、以下の例に示す通り、PEM 形式の証明書であり、かつ一段目の証明書の終端ラベル（"----- END <label> -----"）と二段目の証明書の開始ラベル（"----- BEGIN <label> -----"）が改行コードで繋がれている必要があります。

```
-----BEGIN CERTIFICATE-----

〈証明書データ〉

-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

〈証明書データ〉

-----END CERTIFICATE-----
```

3.22.4 電子署名要求の作成と取り出し

本製品で電子証明書署名要求（CSR）を作成し、認証局で認証をしてもらい、その電子証明書を利用します。

CSR の作成は、SSL 証明書署名要求作成画面で実施します。

場所： 設定 ＞ SSL ＞ SSL 証明書署名要求作成

■CSR(署名要求)設定

① SSL ポリシー名

事前に作成しておいた SSL ポリシーを選択します。

② ECC 証明書

ECC 証明書用の CSR を作成する場合選択します。

③ 公開鍵長

RSA 秘密鍵の鍵長を選択します。

④ 楕円曲線パラメーター

任意の EC 名前付き曲線を選択します。

⑤ サーバーの FQDN

サーバーの FQDN（Common Name）を入力します。

⑥ 国名、都道府県、区市町村

それぞれ、適切な所在地を入力します。

⑦ 組織名、部門名、メールアドレス

それぞれ、適切な管理者情報を入力します。

下記の例では SSL ポリシー"TEST_1"に csr と秘密鍵の作成を行います。

入力項目は適切な情報を入力してください。

ポイント 作成した秘密鍵、署名要求書は必ず保管しておいてください。

ポイント 認証局から発行された証明書は、事前に作成しておいた SSL ポリシーに対してインポートしてください。
また、必要に応じて中間証明書をインポートしてください。

⚠ 注意 Netwiser で CSR を行った場合、秘密鍵は Netwiser 以外の機器にインポートすることは出来ません。

CSR の作成が完了すると、作成した CSR を機器から取り出す事ができます。詳細は「5.3.2.4SSL 関連ファイルのエクスポート」を参照してください。

3.22.5 仮想サーバーへの割り当て

SSL アクセラレーション機能を有効にするには、必要な証明書や鍵ファイルをインポートした後、任意の仮想サーバーに対して SSL ポリシーを割り当てます。

ただし、仮想サーバーに SSL ポリシーを割り当てるためには、該当の SSL ポリシーに秘密鍵、サーバー証明書の両方がインポートされている必要があります。
証明書、秘密鍵のインポートは「3.22.3電子証明書と鍵のインポート」を参照してください。

仮想サーバーへの SSL ポリシーの割り当ては、SSL アクセラレーション設定画面で実施します。

場所: 設定 > バランシング > SSL アクセラレーション > 仮想サーバーID 選択> SSL アクセラレーション設定

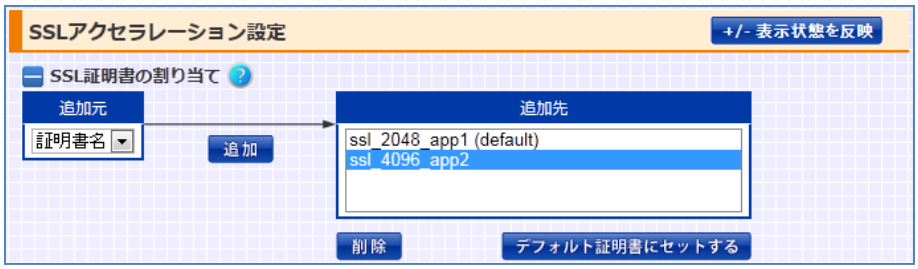
■SSL 証明書の割り当て

① 追加元
「追加元」から任意の SSL ポリシーを選択し、「追加」ボタンで「追加先」テーブルに追加します。
文字列" (default)"が付加されている SSL ポリシーの証明書がデフォルト証明書として動作します。

② 追加先

デフォルト証明書を変更したい場合、「追加先」から SSL ポリシーを選択して「デフォルト証明書にセットする」ボタンをクリックすると、任意の SSL ポリシーをデフォルト証明書に設定することができます。

仮想サーバーの割り当てから解除したい場合、任意の SSL ポリシーを選択して「削除」ボタンで割り当てを解除します。



ポイント

仮想サーバーに割り当てられた SSL ポリシーは、SSL ポリシー設定画面で削除を実施しても削除することはできません。

SSL ポリシーの削除を実施する場合、仮想サーバーへの割り当てを解除してから行ってください。

ポイント

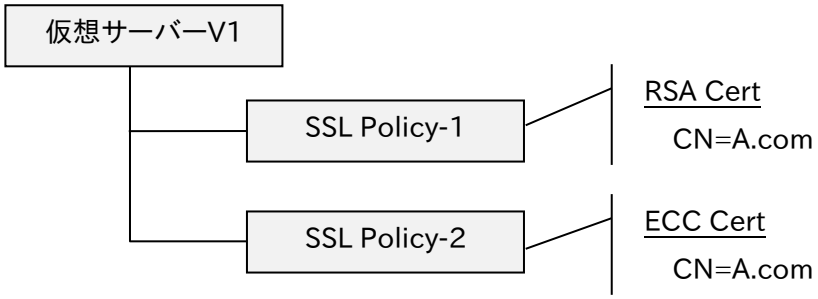
本製品は SSL/TLS の拡張仕様の一つである SNI に対応しています。

仮想サーバーに対して複数の証明書を割り当てた場合や、複数の CN（Common Name）がセットされている証明書（拡張領域"Subject Alternative Names"を利用した証明書）を割り当てた場合、SNI ヘッダの内容によって証明書を使い分けることが可能になります。

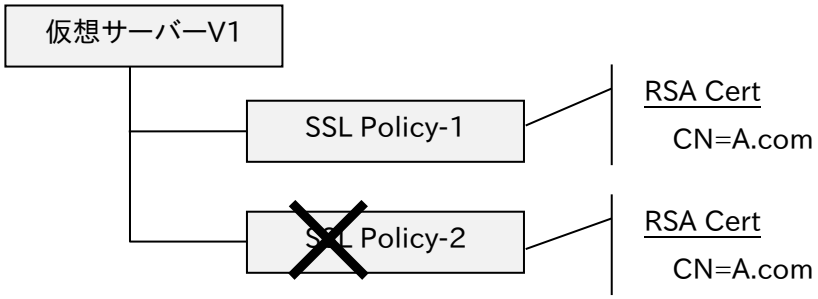
SNI に対応しないアクセスがあった場合は、SNI デフォルト証明書がサーバー証明書として使用されます。

ポイント

単一の仮想サーバーにおいて RSA/ECDSA 両方の署名方式に対応させたい場合、同じ CN（Common Name）の RSA 証明書と ECC 証明書を別々の SSL ポリシーにインポートし、それらを同一の仮想サーバーにバインドする必要があります。



ただし、同じ署名方式（RSA 証明書同士、あるいは ECC 証明書同士）で、かつ同じ CN（Common Name）であるサーバー証明書を同一仮想サーバーに対して複数バインドすると、正常に動作しなくなることがあるため、このような操作はしないでください。



もし、このような操作を行ってしまった場合は、該当の仮想サーバーにバインドされている SSL ポリシーを全てアンバインドしてからバインドし直してください。

ポイント

仮想サーバーに割り当てられた状態のままでも、SSL ポリシーに秘密鍵や証明書をインポートし更新することが可能です。ただし、秘密鍵とサーバー証明書を更新する場合、「秘密鍵」→「サーバー証明書」の順で更新してください。
正しい順序で更新しなかった場合は、SSL ポリシーの割り当てを一旦解除してから、再度割り当てを行ってください。

ポイント

SSL サーバー証明書の拡張領域"Subject Alternative Names"で指定する CN（Common Name）にはワイルドカード（＊）を使用することが可能です。
ただし、ワイルドカードは先頭のサブドメインのみが対象となります。

⚠ 注意

仮想サーバーに割り当てられている状態の SSL ポリシーに対して秘密鍵や証明書の更新を行う場合、証明書と秘密鍵の更新の間（1～数秒程度）その仮想

サーバーに割り当てられた全ての SSL ポリシーに対して新規に SSL セッションが作れない状態になりますので注意してください。

機器情報画面の「SSL > SSL アクセラレート」で、証明書や秘密鍵のインポート状態と SSL アクセラレーション処理の統計情報を参照することができます。

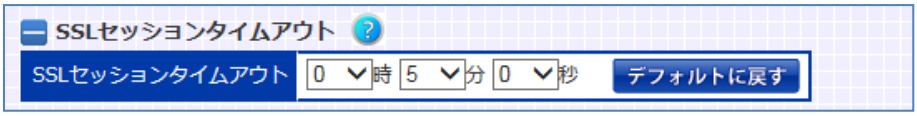
3.22.6 SSL セッションタイムアウト

SSL セッション情報の保持時間はデフォルトで 5 分です。
SSL セッション情報の保持時間の変更は、SSL アクセラレーション選択画面で実施します。

場所: 設定 > バランシング > SSL アクセラレーション

■SSL セッションタイムアウト

① SSL セッションタイムアウト
SSL セッション情報の保持時間を選択します。



3.22.7 クライアント認証

クライアント認証を有効にするには、クライアント証明書を発行した CA 局の自己署名証明書（self-signed certificate）を本製品にインストールする必要があります。更に、自己署名証明書がインストールされたSSLポリシーを仮想サーバーに割り当てます。
クライアント認証のためにインポートする自己署名証明書に、ECC 証明書を利用することはできません。

本製品への証明書のインストールは SSL インポート画面で実施します。
詳細は、「3.22.3電子証明書と鍵のインポート」を参照してください。

仮想サーバーへの SSL ポリシーの割り当ては、SSL アクセラレーション設定画面で実施します。詳細は「3.22.5仮想サーバーへの割り当て」を参照してください。

ポイント

SNI 利用時にクライアント認証を行う SSL ポリシーを割り当てた場合、その他すべての SSL ポリシーでクライアント認証が行われます。
また、仮想サーバーID に対して、クライアント証明書がインポートされている SSL ポリシーを複数件割り当てることはできません。

3.22.7.1 証明書失効時リスト(CRL)の更新

有効期限前に失効したクライアント証明書のチェックは CA 局が発行する証明書失効リスト(CRL)を用いて行います。本製品が CRL を使用してクライアント証明書の期限前失効をチェックする必要がある場合は、CRL の配布元 URL を設定します。CRL は PEM 形式、DER 形式の何れでもかまいません。

場所: 設定 > SSL > 証明書失効リスト

CRL の配布元 URL を設定します。

■証明書失効リスト

① SSL ポリシー
任意の SSL ポリシーを選択します。

② 証明書失効リストダウンロード先 URL
証明書失効リストのダウンロード先 URL を指定します。

③ 更新間隔
証明書失効リストのダウンロード間隔を選択します。

以下の例では、192.168.1.251:8009 から MyCRL.der ファイルを 10 分毎にダウンロードします。

ポイント

URL に IPv6 アドレスを使用する場合は、以下のように[ ]で囲んでください。
"http://[2001:db8::c0:a8:1:fb]:8009/MyCRL.der"

プロキシサーバー経由で CRL の配布元 URL へアクセスする場合、本製品にプロキシサーバーの登録をする必要があります。
プロキシサーバーの登録はプロキシサーバー設定画面で実施します。

場所: 設定 > SSL > プロキシサーバー

プロキシサーバーを登録します。

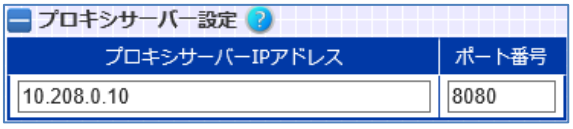
■プロキシサーバー設定

① プロキシサーバーIP アドレス

登録するプロキシサーバーの IP アドレスを入力します。

② ポート番号

接続先のプロキシサーバーのポート番号を指定します。



3.22.7.2 クライアント証明書の挿入

クライアント認証を使用すると、本製品で認証を行った後 HTTP リクエスト（GET、POST）に以下のデータを追加してサーバーへ送ることができます。

- base64 形式、または pem 形式に変換されたクライアント証明書
- base64 形式に変換された SSL セッション ID

ポイント

SSL セッション ID はクライアント認証なしであっても、設定することが可能です。

クライアント証明書は SSL ハンドシェーク終了後、最初の HTTP リクエストにセットされます。SSL セッション ID は同一の TCP コネクションで複数の GET、POST メソッドが発生する場合にもセットされます。

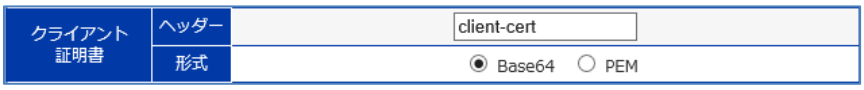
クライアント証明書と SSL セッション ID はデフォルトでは送信されません。クライアント証明書と SSL セッション ID をサーバーへ送る必要がある場合は、HTTP ヘッダーに追加されるタグ名を設定します。設定を行うには、SSL アクセラレーション設定画面に遷移します。

場所: 設定 > バランシング > SSL アクセラレーション > 仮想サーバーID 選択> SSL アクセラレーション設定

■SSL アクセラレーション設定

① クライアント証明書ヘッダー

HTTP リクエストに挿入するクライアント証明書ヘッダー、形式を定義します。



② SSL セッション ID ヘッダー

HTTP リクエストに挿入する SSL セッション ID を定義します。

3.22.7.3 クライアント認証失敗時の動作

クライアント証明書が提示されない、または証明書の期限切れ、失効などの理由により認証に失敗した場合の動作を設定することが出来ます。

本製品のデフォルト設定では、SSL alert メッセージを送信しコネクションを終了します。デフォルト以外の処理を設定するには SSL アクセラレーション設定画面に遷移します。

場所: 設定 > バランシング > SSL アクセラレーション > 仮想サーバーID 選択> SSL アクセラレーション設定

SSL アクセラレーション設定画面に遷移し、クライアント認証失敗時の動作を設定します。

■クライアント認証失敗時動作

① 動作

クライアント認証に失敗した際の動作を選択します。

■***SSL ハンドシェーク強制終了***

alert を送信し SSL ハンドシェークを強制終了します。

■***403 レスポンス返送***

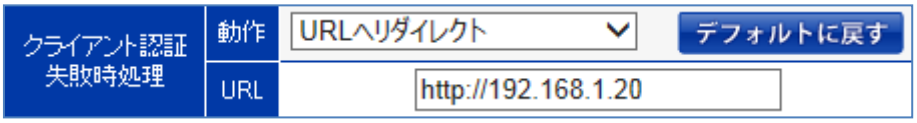
403 Forbidden レスポンスを返します。

■***URL へリダイレクト***

302 レスポンスを返し***<URL>***で指定されたページへリダイレクトします。

② URL

URL へリダイレクトを選択した際、リダイレクト先の URL を指定します。



ポイント

CRL の取得が成功するまで、証明書の期限切れ、失効に関してはチェックされません。

3.22.8 使用する暗号スイートの選択

SSL アクセラレーションで使用する暗号スイートを指定できます。

デフォルト設定として、以下の暗号スイートの許可/拒否をしています。

許可する暗号スイート
DES-CBC3-SHA
AES128-SHA
AES128-SHA256
AES256-SHA
AES256-SHA256
AES128-GCM-SHA256
AES256-GCM-SHA384
DHE-AES128-SHA
DHE-AES128-SHA256
DHE-AES128-GCM-SHA256
DHE-AES256-SHA
DHE-AES256-SHA256
DHE-AES256-GCM-SHA384
拒否する暗号スイート
DES-CBC-SHA
ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES128-SHA256
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-SHA
ECDHE-RSA-AES256-SHA384
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES128-SHA
ECDHE-ECDSA-AES128-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-SHA
ECDHE-ECDSA-AES256-SHA384
ECDHE-ECDSA-AES256-GCM-SHA384

使用する暗号スイートの選択を行うには、SSL アクセラレーション設定画面に遷移します。

場所: 設定 > バランシング > SSL アクセラレーション > 仮想サーバーID 選択> SSL アクセラレーション設定

■SSL アクセラレーション詳細設定

① サーバーが許可する暗号スイート

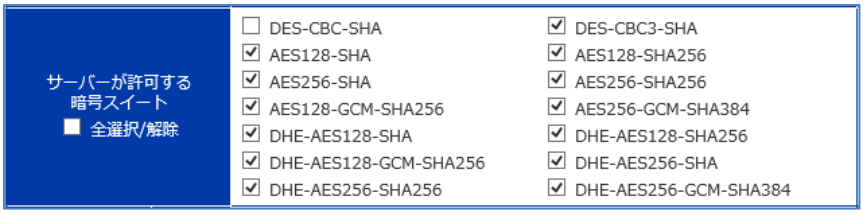
サーバーが許可する暗号スイートを選択します。

「全選択/解除」を選択すると、全ての項目を選択状態にします。

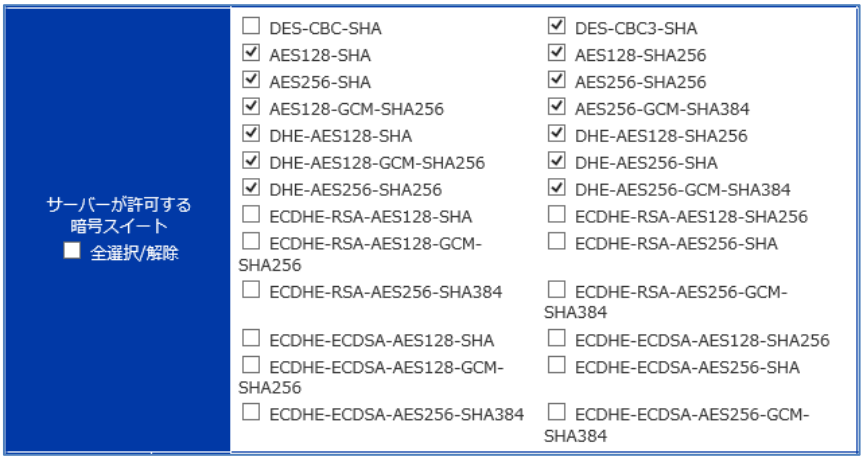
「全選択/解除」の選択を外すと、全ての項目の選択が解除されます。

ただし、SX-3920 では、ECDHE 系の暗号スイートをサポートしていないため、ECDHE 系の暗号スイートは選択肢から除外されています。

以下は、SX-3920 の表示



以下は、SX-3920 以外の機種での表示



該当の仮想サーバーは、指定された暗号スイート内のいずれかを SSL アクセラレーションの際に使用します。

3.22.9 SSL3.0 の有効化

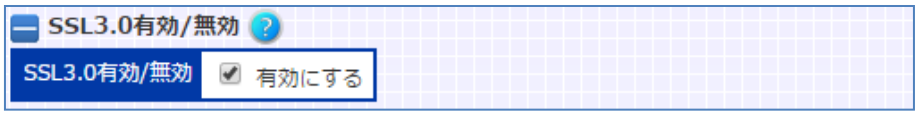
SSL 3.0 はデフォルトで無効化されています。SSL 3.0 での SSL アクセラレーションを有効化するためには SSL アクセラレーション設定画面に遷移します。

場所: 設定 > バランシング > SSL アクセラレーション

■SSL3.0 有効/無効

① SSL3.0 有効/無効

SSL3.0 を有効化する場合、選択します。



注意 SSL 3.0 を有効化すると脆弱性 CVE-2014-3566 に該当しますので、設定変更の際は注意してください。

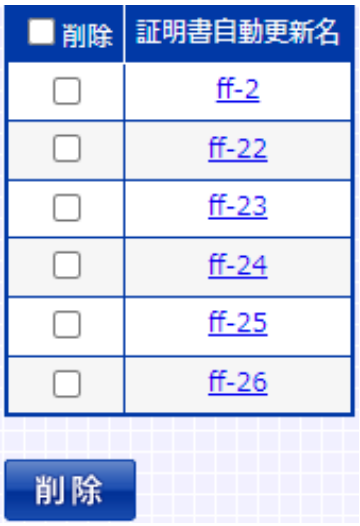
3.22.10 SSL 証明書自動更新

SSL 証明書自動更新は、証明書の有効期限が設定した日数以内になると CSR を作成し、サーバーへアップロードします。
その後指定したサーバーから証明書をダウンロードし、SSL アクセラレートで使用する証明書を自動的に更新します。
SSL 証明書自動更新を有効化するためには SSL 証明書自動更新設定画面に遷移します。

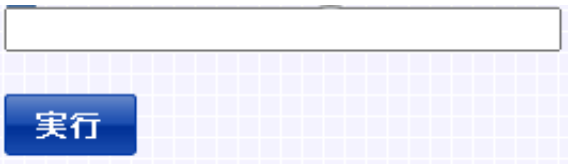
場所: 設定 > SSL

■証明書自動更新プレフィックス一覧

SSL 証明書自動更新の設定を変更する場合、証明書自動更新名を選択します。
削除したいときは、チェックボックスを有効にして削除ボタンを押します。



新規の時はプレフィックスを入力して実行ボタンを押してください。



■証明書自動更新設定

証明書自動更新名を選択すると以下の画面が表示されます。

① 有効

証明書自動更新の設定が完了し自動更新を開始するときチェックボックスを有効にします。

② 電子証明書署名要求(CSR)作成期日

証明書の有効期限の何日前に CSR を作成するか設定します。0の時は CSR なしとなります。

③ 国名

国名を 2 文字で入力します。

④ 都道府県（州）

都道府県名を入力します。

⑤ 区市町村

区市町村名を入力します。

⑥ 組織名
組織名を入力します。

⑦ サーバーの fqdn
fqdn を入力します。
※重要: この fqdn はクライアントがサーバーにアクセスするときに、サーバーの正当性を確認するために使用します。

⑧ 公開鍵
鍵長を指定します。
256 : secp256r1
384 : secp384r1
※上記の 2 つは ecc が使えない機種は指定不可
1024 : rsa 1024
2048 : rsa 2048
4096 : rsa 4096

⑨ メールアドレス
メールアドレスを入力します。

⑩ CSR アップロード url
CSR アップロード先、‘upload.php’ 等スクリプトまで入力します。

⑪ 証明書ダウンロード url
ダウンロードするサーバー上のフォルダの url を入力します。

⑫ ユーザー認証アカウント
アップロード／ダウンロード時にユーザー認証が必要な時入力します。

⑬ ユーザー認証パスワード
アップロード／ダウンロード時にユーザー認証が必要な時入力します。

⑭ 秘密鍵パスフレーズ
CSR なしのとき、ダウンロードする秘密鍵にパスフレーズが掛かっている場合に入力します。

⑮ CN (fqdn)チェック
ダウンロードした証明書がサーバーの fqdn で入力したものに相違ないか確認する場合はチェックボックスを有効にします。
※このチェックボックスが有効なとき、証明書のダウンロード完了前にサーバー名を変更すると、ダウンロードが失敗するので注意してください

⑯ 証明書自動更新の状態を初期化
CSR 設定の変更等により CSR 作成からやり直したい場合にチェックします。

⚠ 注意　設定例及び注意事項は、CLI 編 2.20.10SSL 証明書自動更新に記載していますので、必ず目を通してください。

3.23 クラウド WAF

本章では、本製品のクラウド WAF 連携機能について説明します。

3.23.1 クラウド WAF 連携

クラウド WAF 連携機能を使用すると、本製品を流れる着信トラフィックと発信トラフィックをフィルタリングできます。
クラウド WAF 連携機能は、L7 負荷分散のアクセスログ機能（3.21.13）を使用して、WAF センタールールとシグネチャマッチングをおこないます。攻撃検知対象の場合は、センターから本製品へ遮断命令を送信し、遮断対象 IP アドレスをブロックします。

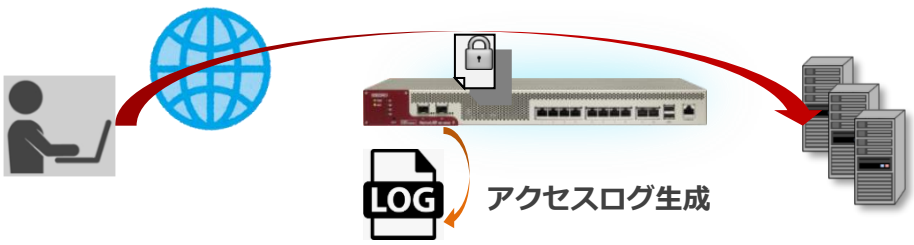
注意 遮断対象 IP アドレスは IPv4 アドレスとなります。

3.23.2 クラウド WAF 動作イメージ

攻撃検知の遮断動作イメージにを以下に示します。

3.23.2.1 アクセスログの生成

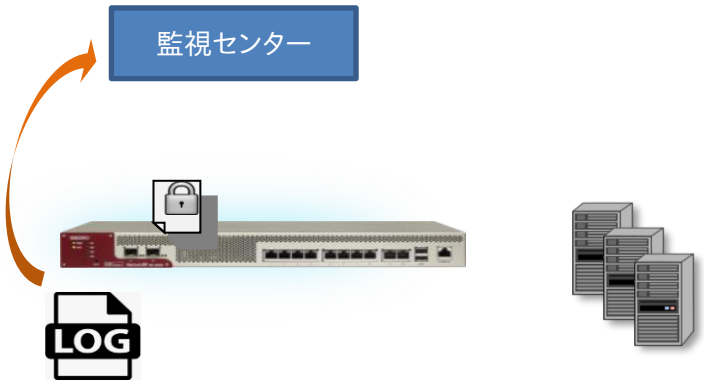
④ クライアントから Web サーバーへ HTTP リクエストを送信
⑤ Web アプリケーションが HTTP レスポンスを送信
⑥ 本製品がアクセスログを生成



3.23.2.2 監視センターへログ送信

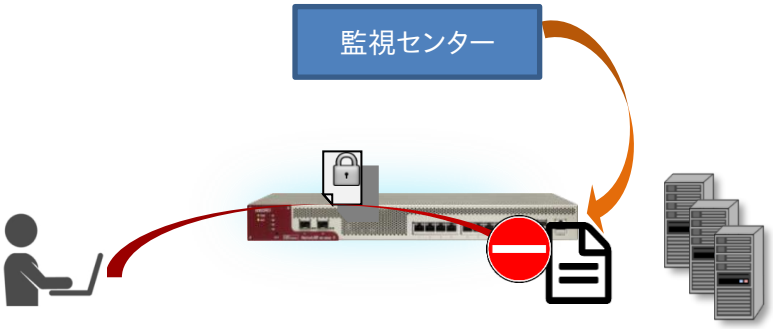
③ アクセスログを収集

④　監視センターへログを送信（UDP）



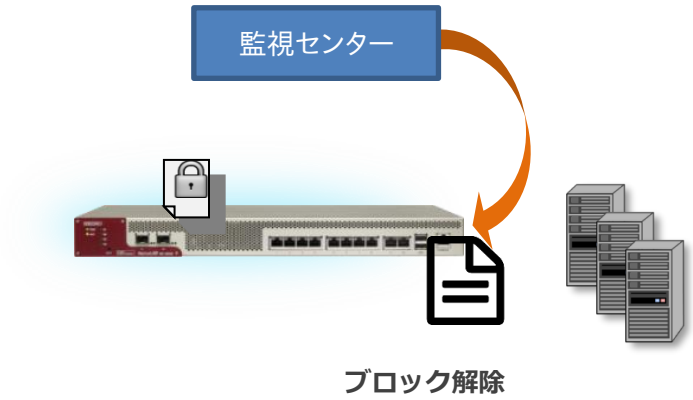
3.23.2.3 遮断命令の送信

④　監視センターで、ログを WAF センタールールとシグネチャマッチング
⑤　攻撃検知対象の場合は、監視センターから本製品へ遮断命令を送信
⑥　遮断対象 IP アドレスを引数に遮断ルールを追加（接続元 IP アドレスの拒否）



3.23.2.4 ブロック解除命令の送信

③　遮断時間（初期値：10 分間）を経過した場合は、本製品へ遮断解除命令を送信
④　対象 IP アドレスを引数に遮断ルールを削除(接続元 IP アドレスのブロック解除)



ブロック解除

3.23.3 クラウド WAF 連携の有効

クラウド WAF を設定するには、クラウド WAF 設定画面に遷移します。

場所: 設定 > ネットワーク > クラウド WAF

■マネージャーアドレス

マネージャーの IP アドレスまたは IP 名を入力します。

■ポート

マネージャーのポート番号を入力します。

■エージェントキー

エージェントキーを入力します。

■有効

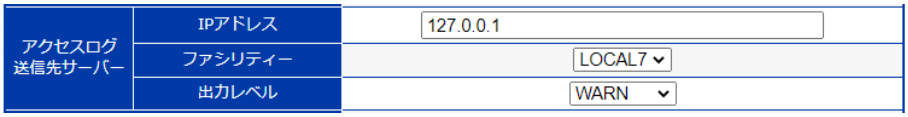
設定が完了し、クラウド WAF を使用開始するときに有効にします。

注意

クラウド WAF を有効化するとき、設定やネットワーク状況により最大で1分程度時間がかかることがあります。

3.23.4 アクセスログ設定

クラウド WAF を使用する場合は、クラウド WAF を適用する仮想サーバーの設定に以下のようにアクセスログ（3.21.13）を設定します。



通常のアクセスログ設定とは異なり、syslog サーバーのアドレスは外部の IP アドレスではなく、本製品自身(127.0.01)を指定します。また、ファシリティとレベル（local7. LOG_WARNING）を指定します。

ポイント

アクセスログ機能は L7 負荷分散機能の一部です。アクセスログ機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

3.23.5 アクセスログ表示

本製品で生成されたアクセスログ（3.34.2）を表示するには、**場所: ログ参照 > アクセスログ**を参照ください。

3.23.6 クラウド WAF における防御対象

本製品において防御可能な攻撃を下表に例示します。

攻撃手法
● サーバサイドインクルードインジェクション
● HTTP インジェクション
● LDAP インジェクション
● XML 外部エンティティ
● サーバサイドリクエストフォージェリ
● デシリアライゼーション
● クロスサイトスクリプティング
● SQL インジェクション
● NoSQL インジェクション
● OS コマンドインジェクション
● 改行コードインジェクション
● ディレクトリトラバーサル
● ファイルインクルード攻撃
● URL エンコード攻撃
● ブラックリスト UA
● その他の WEB 攻撃全般
● ミドルウェアなどの脆弱性を突いた攻撃（Apache Struts2 の脆弱性等）

⚠ 注意

これらの攻撃に対し 100%の防御を保証するものではございません

3.23.7 クラウド WAF における制限事項

● 本製品から監視センターへの通信は UDP プロトコルを利用します。プロトコルの性質上、通信経路で検査対象のログが Drop する可能性があります（監視センターではエージェントからの全ログを受信することを保証していません）。

● 遮断処理は、監視センターに送信されたログを検査後、検知対象の送信元 IP アドレスを遮断対象に登録します（IP アドレスベース遮断）。遮断対象に登録されるまでのリクエストは検知のみを実施します。

● 本製品と監視センター間のステータスが、オフラインからオンラインに変化した場合、オフライン期間のログ情報が監視センターへまとめて送信されます。一度に大量のログが送信された場合、しきい値系のシグネチャで検知/遮断される可能性があります。

3.24 ヘルスチェックの設定

サーバーの稼働状態をチェックするにはヘルスチェックの設定を行います。
本章ではヘルスチェックに関する設定方法を例とともに記します。

ヘルスチェック設定を行うには、ヘルスチェック設定画面に遷移します。
初めに、「ヘルスチェック対象サーバー」項目で、ヘルスチェックポリシーの概要を定義します。
場所: 設定 > ヘルスチェック > ヘルスチェック設定

■ヘルスチェック対象サーバー

① ヘルスチェック方法
ICMP ヘルスチェックを行う場合「ping ヘルスチェック」を選択します。
その他のヘルスチェックでは「L4-7 ヘルスチェック」を選択します。

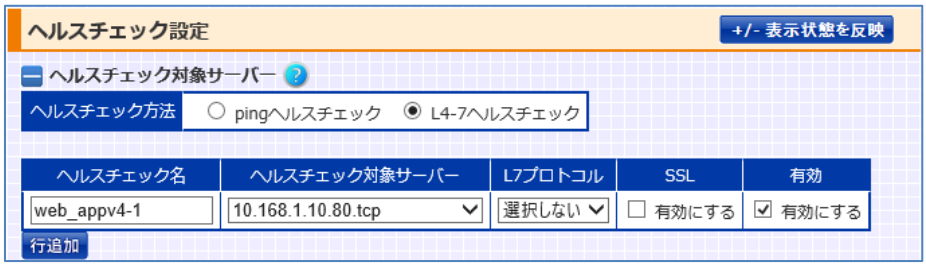
② ヘルスチェック名
任意のヘルスチェックポリシー名を定義します。

③ ヘルスチェック対象サーバー
ヘルスチェック対象サーバーを選択します。
実サーバー登録されているサーバーが選択肢になります。
実サーバーの登録は「3.21.2実サーバーの設定」を参照してください。

④ L7 プロトコル
ヘルスチェック対象のアプリケーション種別を選択します。
ヘルスチェック方法で「L4-7 ヘルスチェック」を指定した場合に選択可能になります。
TCP コネクションでのヘルスチェック、または UDP エコーでのヘルスチェックを行う場合、「選択しない」を選択します。

⑤ SSL
ヘルスチェックで SSL ハンドシェイクを行う場合選択します。
ヘルスチェック対象サーバーのプロトコルが tcp の場合に選択可能になります。

⑥ 有効
ヘルスチェックを有効状態にする場合選択します。



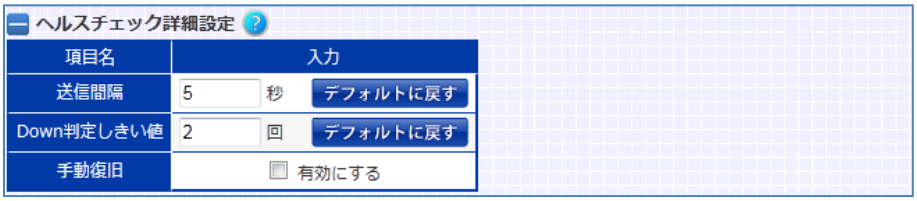
次に、ヘルスチェック詳細設定を定義します。
本項では全てのヘルスチェックポリシーに共通する設定項目を説明します。
L7 プロトコル選択時の各アプリケーションに対するヘルスチェックの詳細設定は各項目で確認してください。

■ヘルスチェック詳細設定

① 送信間隔
ヘルスチェックの送信間隔を定義します。

② Down 判定しきい値
ヘルスチェックで異常検知と判断するまでのリトライ回数を設定することができます。

③ 手動復旧
サーバーがヘルスチェック DOWN 状態から ALIVE 状態に変化した際の復旧動作を選択します。
無効である場合、ALIVE 状態に変化したサーバーは即時に負荷分散対象に復帰します。
有効にした場合、ヘルスチェック状態が ALIVE 変化しても該当サーバーを負荷分散対象から除外したままにします。



ポイント

手動復旧設定が有効な状態でヘルスチェック DOWN した場合、実サーバー状態は自動で無効状態に変化します。これに伴い、実サーバー設定画面でも「有効」のチェックボックスが未選択状態へと変化します。
この時、実サーバーを負荷分散対象へ復帰させるには、実サーバー設定画

面の「有効」チェックボックスを選択し、実サーバーを有効状態に変化させます。
実サーバー状態の変更は「3.21.2実サーバーの設定」を参照してください。

3.24.1 ヘルスチェック一括設定

通常のヘルスチェック設定とは異なり、仮想サーバーにバインドされた全ての実サーバーに対して、一括でヘルスチェックポリシーを定義することが可能です。

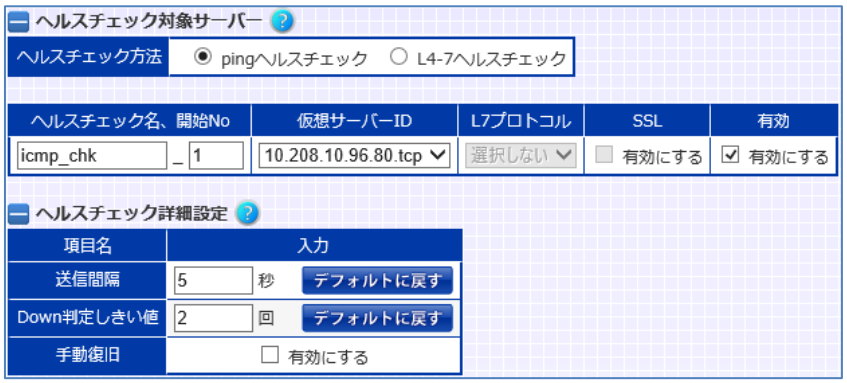
場所: 設定 > ヘルスチェック > ヘルスチェック一括設定

■ヘルスチェック対象サーバー

① ヘルスチェック名、開始 No
任意のヘルスチェックポリシー名を定義します。
通常のヘルスチェックポリシー名と違い 60 文字以内で定義してください。
開始 No はヘルスチェックポリシー名の末尾にアンダースコア(_)付きで付加される番号です。

② 仮想サーバーID
仮想サーバーを選択します。
選択した仮想サーバーにバインドされている全ての実サーバーがヘルスチェック定義の範囲となります。

以下の例では、仮想サーバーID"10.208.10.96.80.tcp"にバインドされている実サーバーに対して、入力内容に沿った ICMP ヘルスチェックが登録されます。
たとえば、"10.208.10.96.80.tcp"に 3 台の実サーバーがバインドされている場合、ヘルスチェック名は、それぞれバインド登録順に icmp_chk_1, icmp_chk_2, icmp_chk_3 となります。



3.24.2 ICMP ヘルスチェック

ICMP の echo 要求をサーバーIP アドレスに送信します。規定回数連続して echo 応答を受信しない、または応答データが異常であるとサーバーダウンと判断します。

ICMP ヘルスチェックポリシーの定義と詳細設定は「3.23クラウド WAF
本章では、本製品のクラウド WAF 連携機能について説明します。

3.24.3 クラウド WAF 連携

クラウド WAF 連携機能を使用すると、本製品を流れる着信トラフィックと発信トラフィックをフィルタリングできます。
クラウド WAF 連携機能は、L7 負荷分散のアクセスログ機能（3.21.13）を使用して、WAF センタールールとシグネチャマッチングをおこないます。攻撃検知対象の場合は、センターから本製品へ遮断命令を送信し、遮断対象 IP アドレスをブロックします。

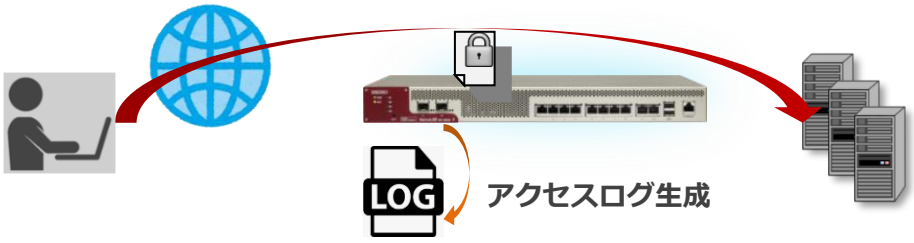
遮断対象 IP アドレスは IPv4 アドレスとなります。

3.24.4 クラウド WAF 動作イメージ

攻撃検知の遮断動作イメージにを以下に示します。

3.24.4.1 アクセスログの生成

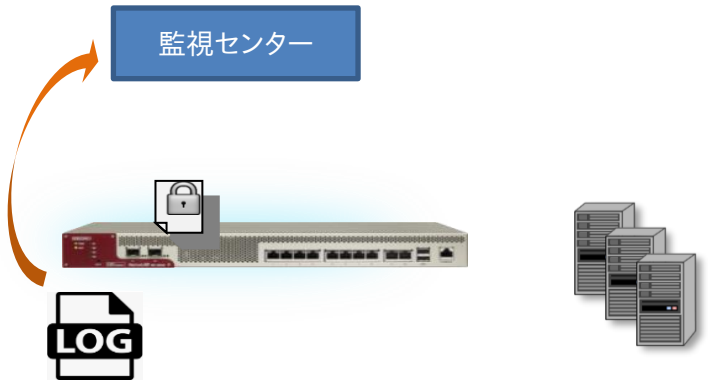
⑦ クライアントから Web サーバーへ HTTP リクエストを送信
⑧ Web アプリケーションが HTTP レスポンスを送信
⑨ 本製品がアクセスログを生成



3.24.4.2 監視センターへログ送信

⑤ アクセスログを収集

⑥ 監視センターへログを送信（UDP）

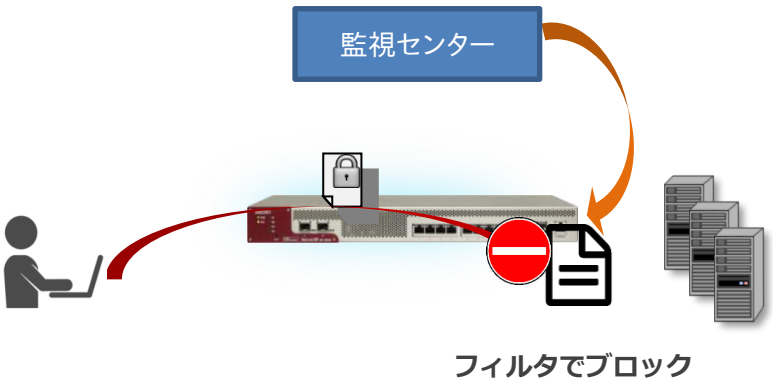


3.24.4.3 遮断命令の送信

⑦ 監視センターで、ログを WAF センタールールとシグネチャマッチング

⑧ 攻撃検知対象の場合は、監視センターから本製品へ遮断命令を送信

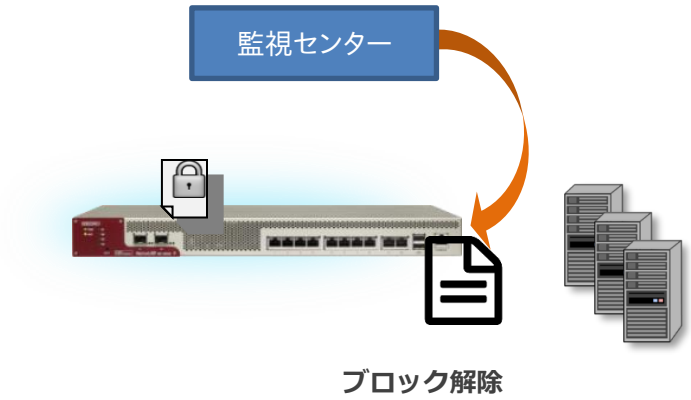
⑨ 遮断対象 IP アドレスを引数に遮断ルールを追加（接続元 IP アドレスの拒否）



3.24.4.4 ブロック解除命令の送信

⑤　遮断時間（初期値：10 分間）を経過した場合は、本製品へ遮断解除命令を送信

⑥　対象 IP アドレスを引数に遮断ルールを削除（接続元 IP アドレスのブロック解除）



3.24.5 クラウド WAF 連携の有効

クラウド WAF を設定するには、クラウド WAF 設定画面に遷移します。

場所: 設定 > ネットワーク > クラウド WAF

■マネージャーアドレス

マネージャーの IP アドレスまたは IP 名を入力します。

■ポート

マネージャーのポート番号を入力します。

■エージェントキー

エージェントキーを入力します。

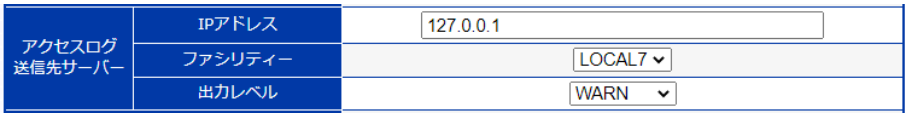
■有効

設定が完了し、クラウド WAF を使用開始するときに有効にします。

クラウド WAF を有効化するとき、設定やネットワーク状況により最大で1分程度時間がかかることがあります。

3.24.6 アクセスログ設定

クラウド WAF を使用する場合は、クラウド WAF を適用する仮想サーバーの設定に以下のようにアクセスログ（3.21.13）を設定します。



通常のアクセスログ設定とは異なり、syslog サーバーのアドレスは外部の IP アドレスではなく、本製品自身(127.0.01)を指定します。また、ファシリティとレベル（local7. LOG_WARNING）を指定します。

アクセスログ機能は L7 負荷分散機能の一部です。アクセスログ機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

3.24.7 アクセスログ表示

本製品で生成されたアクセスログ（3.34.2）を表示するには、**場所: ログ参照 > アクセスログ**を参照ください。

3.24.8 クラウド WAF における防御対象

本製品において防御可能な攻撃を下表に例示します。

攻撃手法
● サーバサイドインクルードインジェクション
● HTTP インジェクション
● LDAP インジェクション
● XML 外部エンティティ
● サーバサイドリクエストフォージェリ
● デシリアライゼーション
● クロスサイトスクリプティング
● SQL インジェクション
● NoSQL インジェクション
● OS コマンドインジェクション
● 改行コードインジェクション
● ディレクトリトラバーサル
● ファイルインクルード攻撃
● URL エンコード攻撃
● ブラックリスト UA
● その他の WEB 攻撃全般
● ミドルウェアなどの脆弱性を突いた攻撃（Apache Struts2 の脆弱性等）

これらの攻撃に対し 100%の防御を保証するものではございません

3.24.9 クラウド WAF における制限事項

● 本製品から監視センターへの通信は UDP プロトコルを利用します。プロトコルの性質上、通信経路で検査対象のログが Drop する可能性があります（監視センターではエージェントからの全ログを受信することを保証していません）。

● 遮断処理は、監視センターに送信されたログを検査後、検知対象の送信元 IP アドレスを遮断対象に登録します（IP アドレスベース遮断）。遮断対象に登録されるまでのリクエストは検知のみを実施します。

● 本製品と監視センター間のステータスが、オフラインからオンラインに変化した場合、オフライン期間のログ情報が監視センターへまとめて送信されます。一度に大量のログが送信された場合、しきい値系のシグネチャで検知/遮断される可能性があります。

ヘルスチェックの設定」を参照してください。

⚠ 注意　1つの実サーバーに対して、ICMP ヘルスチェックを複数登録しないでください。登録すると、2 台目以降のサーバーに対するヘルスチェックが失敗します。

ポイント　ポート番号 0 を指定した実サーバーのヘルスチェックは、ICMP ヘルスチェックが必要です。

3.24.10 TCP ヘルスチェック

TCP ヘルスチェックでは、コネクション要求をサーバーAP に送信します。
コネクションが確立されれば正常と判断し、規定回数連続してコネクションが確立できなければサーバーダウンと判断します。

TCP ヘルスチェックポリシーの定義と詳細設定は「3.23クラウド WAF
本章では、本製品のクラウド WAF 連携機能について説明します。

3.24.11 クラウド WAF 連携

クラウド WAF 連携機能を使用すると、本製品を流れる着信トラフィックと発信トラフィックをフィルタリングできます。
クラウド WAF 連携機能は、L7 負荷分散のアクセスログ機能（3.21.13）を使用して、WAF センタールールとシグネチャマッチングをおこないます。攻撃検知対象の場合は、センターから本製品へ遮断命令を送信し、遮断対象 IP アドレスをブロックします。

遮断対象 IP アドレスは IPv4 アドレスとなります。

3.24.12 クラウド WAF 動作イメージ

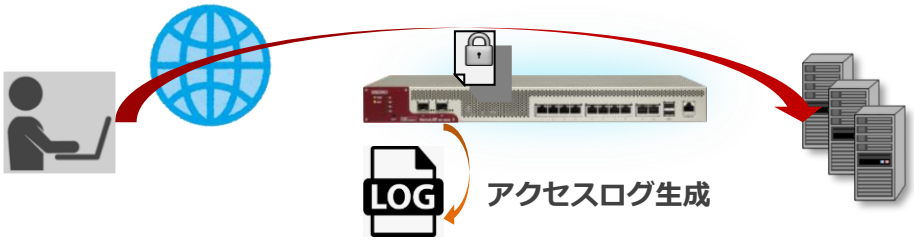
攻撃検知の遮断動作イメージにを以下に示します。

3.24.12.1 アクセスログの生成

⑩　クライアントから Web サーバーへ HTTP リクエストを送信

⑪　Web アプリケーションが HTTP レスポンスを送信

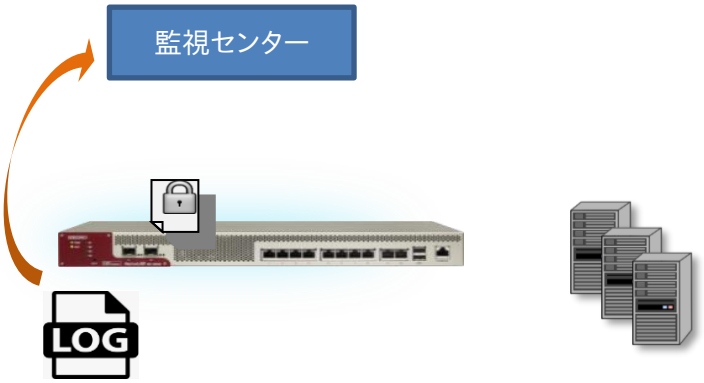
⑫　本製品がアクセスログを生成



3.24.12.2 監視センターへログ送信

⑦　アクセスログを収集

⑧　監視センターへログを送信（UDP）

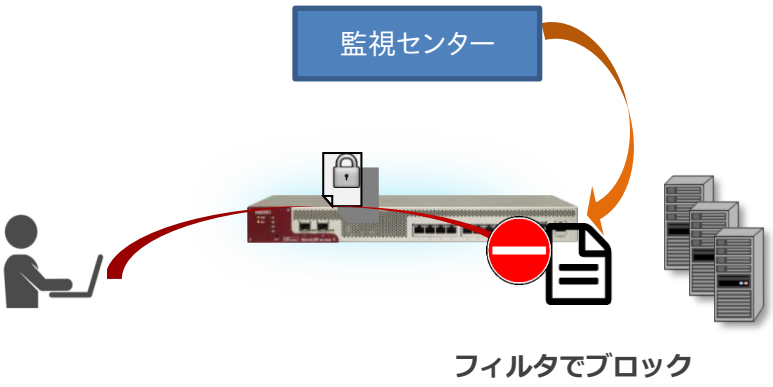


3.24.12.3 遮断命令の送信

⑩　監視センターで、ログを WAF センタールールとシグネチャマッチング

⑪　攻撃検知対象の場合は、監視センターから本製品へ遮断命令を送信

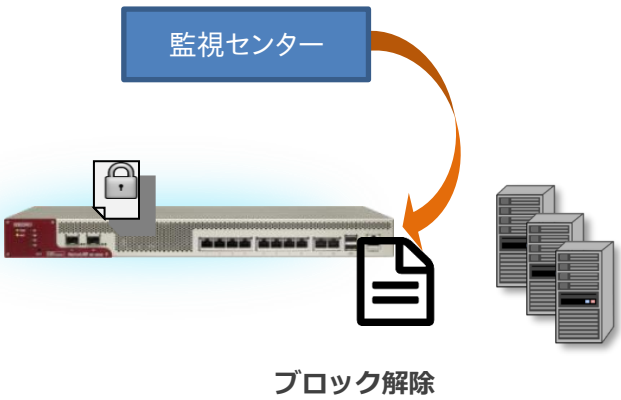
⑫　遮断対象 IP アドレスを引数に遮断ルールを追加（接続元 IP アドレスの拒否）



3.24.12.4 ブロック解除命令の送信

⑦ 遮断時間（初期値：10 分間）を経過した場合は、本製品へ遮断解除命令を送信

⑧ 対象 IP アドレスを引数に遮断ルールを削除(接続元 IP アドレスのブロック解除)



3.24.13 クラウド WAF 連携の有効

クラウド WAF を設定するには、クラウド WAF 設定画面に遷移します。

場所: 設定 > ネットワーク > クラウド WAF

■マネージャーアドレス

マネージャーの IP アドレスまたは IP 名を入力します。

■ポート

マネージャーのポート番号を入力します。

■エージェントキー

エージェントキーを入力します。

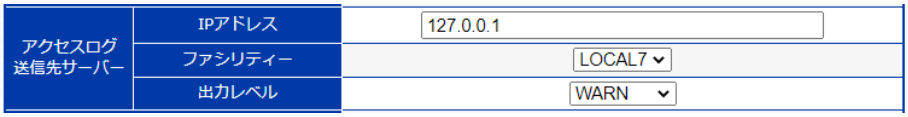
■有効

設定が完了し、クラウド WAF を使用開始するときに有効にします。

クラウド WAF を有効化するとき、設定やネットワーク状況により最大で1分程度時間がかかることがあります。

3.24.14 アクセスログ設定

クラウド WAF を使用する場合は、クラウド WAF を適用する仮想サーバーの設定に以下のようにアクセスログ（3.21.13）を設定します。



通常のアクセスログ設定とは異なり、syslog サーバーのアドレスは外部の IP アドレスではなく、本製品自身(127.0.01)を指定します。また、ファシリティとレベル（local7. LOG_WARNING）を指定します。

アクセスログ機能は L7 負荷分散機能の一部です。アクセスログ機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

3.24.15 アクセスログ表示

本製品で生成されたアクセスログ（3.34.2）を表示するには、**場所: ログ参照 > アクセスログ**を参照ください。

3.24.16 クラウド WAF における防御対象

本製品において防御可能な攻撃を下表に例示します。

攻撃手法
● サーバサイドインクルードインジェクション
● HTTP インジェクション
● LDAP インジェクション
● XML 外部エンティティ
● サーバサイドリクエストフォージェリ
● デシリアライゼーション
● クロスサイトスクリプティング
● SQL インジェクション
● NoSQL インジェクション
● OS コマンドインジェクション
● 改行コードインジェクション
● ディレクトリトラバーサル
● ファイルインクルード攻撃
● URL エンコード攻撃
● ブラックリスト UA
● その他の WEB 攻撃全般
● ミドルウェアなどの脆弱性を突いた攻撃（Apache Struts2 の脆弱性等）

これらの攻撃に対し 100%の防御を保証するものではございません

3.24.17 クラウド WAF における制限事項

● 本製品から監視センターへの通信は UDP プロトコルを利用します。プロトコルの性質上、通信経路で検査対象のログが Drop する可能性があります（監視センターではエージェントからの全ログを受信することを保証していません）。

● 遮断処理は、監視センターに送信されたログを検査後、検知対象の送信元 IP アドレスを遮断対象に登録します（IP アドレスベース遮断）。遮断対象に登録されるまでのリクエストは検知のみを実施します。

● 本製品と監視センター間のステータスが、オフラインからオンラインに変化した場合、オフライン期間のログ情報が監視センターへまとめて送信されます。一度に大量のログが送信された場合、しきい値系のシグネチャで検知/遮断される可能性があります。

ヘルスチェックの設定」を参照してください。

3.24.18 UDP ヘルスチェック

UDP ヘルスチェックでは、1 バイトのデータ(0xff)をサーバーAP に送信します。
ICMP Port Unreachable を受信しなければ正常と判断します。

UDP ヘルスチェックポリシーの定義と詳細設定は「3.23クラウド WAF
本章では、本製品のクラウド WAF 連携機能について説明します。

3.24.19 クラウド WAF 連携

クラウド WAF 連携機能を使用すると、本製品を流れる着信トラフィックと発信トラフィックをフィルタリングできます。
クラウド WAF 連携機能は、L7 負荷分散のアクセスログ機能（3.21.13）を使用して、WAF センタールールとシグネチャマッチングをおこないます。攻撃検知対象の場合は、センターから本製品へ遮断命令を送信し、遮断対象 IP アドレスをブロックします。

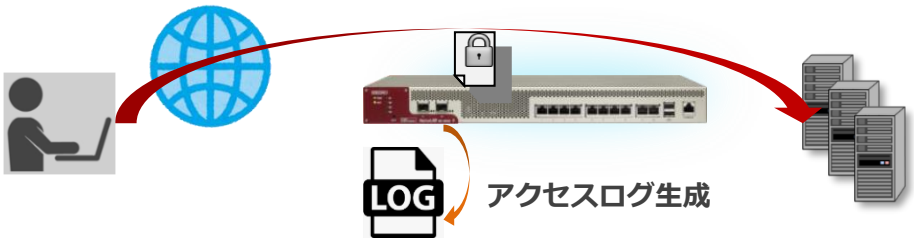
遮断対象 IP アドレスは IPv4 アドレスとなります。

3.24.20 クラウド WAF 動作イメージ

攻撃検知の遮断動作イメージにを以下に示します。

3.24.20.1 アクセスログの生成

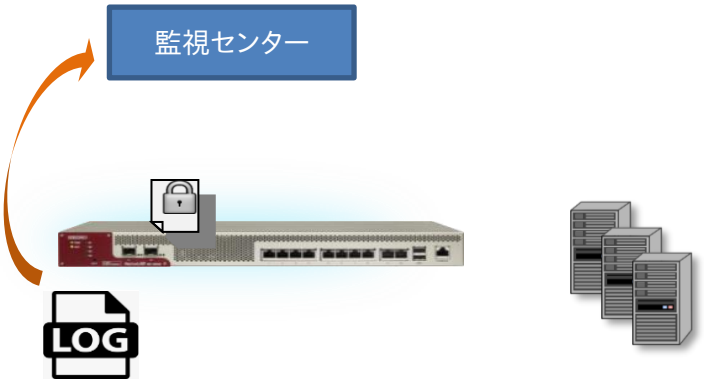
⑬ クライアントから Web サーバーへ HTTP リクエストを送信
⑭ Web アプリケーションが HTTP レスポンスを送信
⑮ 本製品がアクセスログを生成



3.24.20.2 監視センターへログ送信

⑨ アクセスログを収集

⑩ 監視センターへログを送信（UDP）

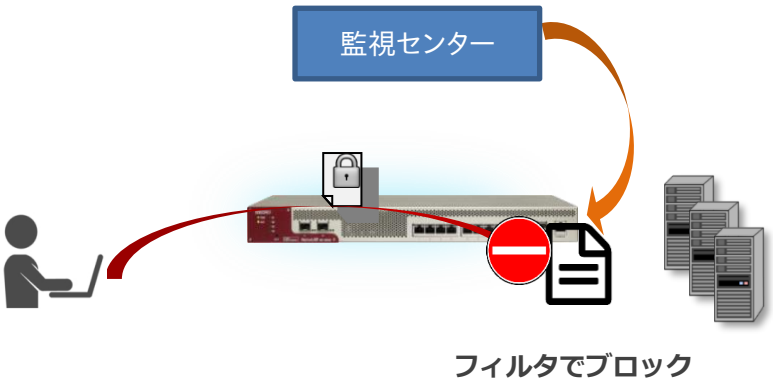


3.24.20.3 遮断命令の送信

⑬ 監視センターで、ログを WAF センタールールとシグネチャマッチング

⑭ 攻撃検知対象の場合は、監視センターから本製品へ遮断命令を送信

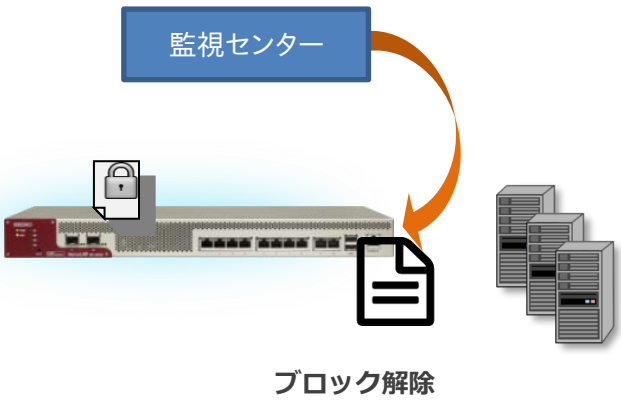
⑮ 遮断対象 IP アドレスを引数に遮断ルールを追加（接続元 IP アドレスの拒否）



3.24.20.4 ブロック解除命令の送信

⑨ 遮断時間（初期値：10 分間）を経過した場合は、本製品へ遮断解除命令を送信

⑩ 対象 IP アドレスを引数に遮断ルールを削除(接続元 IP アドレスのブロック解除)



3.24.21 クラウド WAF 連携の有効

クラウド WAF を設定するには、クラウド WAF 設定画面に遷移します。

場所: 設定 > ネットワーク > クラウド WAF

■マネージャーアドレス

マネージャーの IP アドレスまたは IP 名を入力します。

■ポート

マネージャーのポート番号を入力します。

■エージェントキー

エージェントキーを入力します。

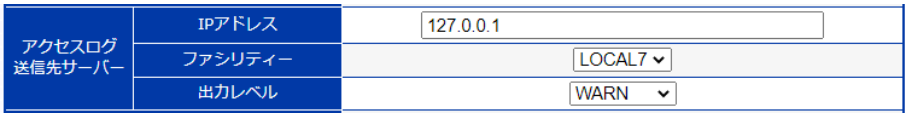
■有効

設定が完了し、クラウド WAF を使用開始するときに有効にします。

クラウド WAF を有効化するとき、設定やネットワーク状況により最大で1分程度時間がかかることがあります。

3.24.22 アクセスログ設定

クラウド WAF を使用する場合は、クラウド WAF を適用する仮想サーバーの設定に以下のようにアクセスログ（3.21.13）を設定します。



通常のアクセスログ設定とは異なり、syslog サーバーのアドレスは外部の IP アドレスではなく、本製品自身(127.0.01)を指定します。また、ファシリティとレベル（local7. LOG_WARNING）を指定します。

アクセスログ機能は L7 負荷分散機能の一部です。アクセスログ機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

3.24.23 アクセスログ表示

本製品で生成されたアクセスログ（3.34.2）を表示するには、**場所: ログ参照 > アクセスログ**を参照ください。

3.24.24 クラウド WAF における防御対象

本製品において防御可能な攻撃を下表に例示します。

攻撃手法
● サーバサイドインクルードインジェクション
● HTTP インジェクション
● LDAP インジェクション
● XML 外部エンティティ
● サーバサイドリクエストフォージェリ
● デシリアライゼーション
● クロスサイトスクリプティング
● SQL インジェクション
● NoSQL インジェクション
● OS コマンドインジェクション
● 改行コードインジェクション
● ディレクトリトラバーサル
● ファイルインクルード攻撃
● URL エンコード攻撃
● ブラックリスト UA
● その他の WEB 攻撃全般
● ミドルウェアなどの脆弱性を突いた攻撃（Apache Struts2 の脆弱性等）

これらの攻撃に対し 100%の防御を保証するものではございません

3.24.25 クラウド WAF における制限事項

● 本製品から監視センターへの通信は UDP プロトコルを利用します。プロトコルの性質上、通信経路で検査対象のログが Drop する可能性があります（監視センターではエージェントからの全ログを受信することを保証していません）。

● 遮断処理は、監視センターに送信されたログを検査後、検知対象の送信元 IP アドレスを遮断対象に登録します（IP アドレスベース遮断）。遮断対象に登録されるまでのリクエストは検知のみを実施します。

● 本製品と監視センター間のステータスが、オフラインからオンラインに変化した場合、オフライン期間のログ情報が監視センターへまとめて送信されます。一度に大量のログが送信された場合、しきい値系のシグネチャで検知/遮断される可能性があります。

ヘルスチェックの設定」を参照してください。

⚠ 注意

同一サーバーの同一ポートに対して複数の UDP ヘルスチェックポリシーを設定すると、正しくヘルスチェックが動作しなくなる可能性がありますので注意してください。

3.24.26 HTTP ヘルスチェック

HTTP ヘルスチェックでは、HTTP リクエストをサーバーAP に送信しレスポンスをチェックします。

HTTP ヘルスチェックポリシーの定義と詳細設定の一部は「3.23クラウド WAF
本章では、本製品のクラウド WAF 連携機能について説明します。

3.24.27 クラウド WAF 連携

クラウド WAF 連携機能を使用すると、本製品を流れる着信トラフィックと発信トラフィックをフィルタリングできます。
クラウド WAF 連携機能は、L7 負荷分散のアクセスログ機能（3.21.13）を使用して、WAF センタールールとシグネチャマッチングをおこないます。攻撃検知対象の場合は、センターから本製品へ遮断命令を送信し、遮断対象 IP アドレスをブロックします。

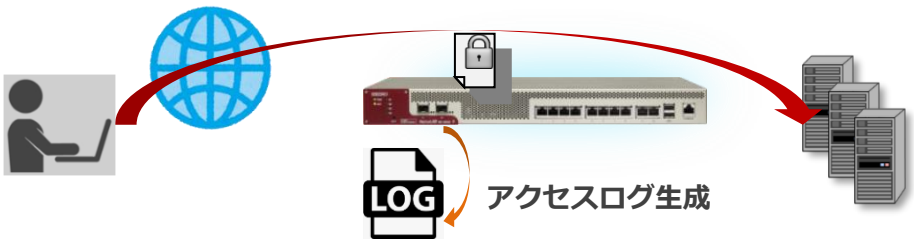
遮断対象 IP アドレスは IPv4 アドレスとなります。

3.24.28 クラウド WAF 動作イメージ

攻撃検知の遮断動作イメージにを以下に示します。

3.24.28.1 アクセスログの生成

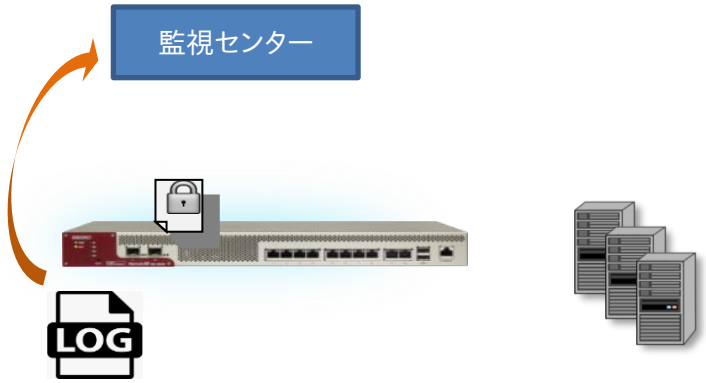
⑯ クライアントから Web サーバーへ HTTP リクエストを送信
⑰ Web アプリケーションが HTTP レスポンスを送信
⑱ 本製品がアクセスログを生成



3.24.28.2 監視センターへログ送信

⑪ アクセスログを収集

⑫ 監視センターへログを送信（UDP）

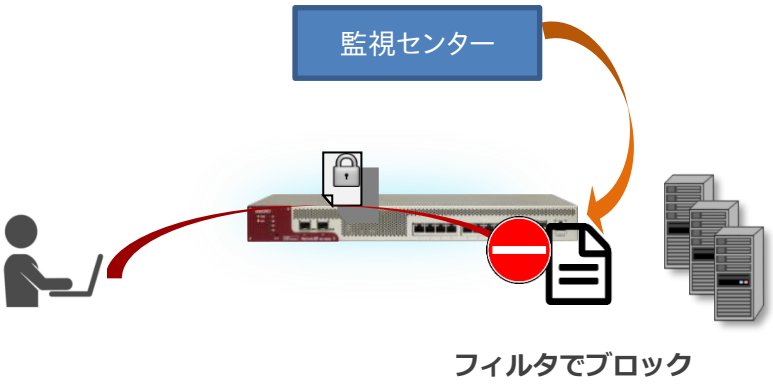


3.24.28.3 遮断命令の送信

⑯ 監視センターで、ログを WAF センタールールとシグネチャマッチング

⑰ 攻撃検知対象の場合は、監視センターから本製品へ遮断命令を送信

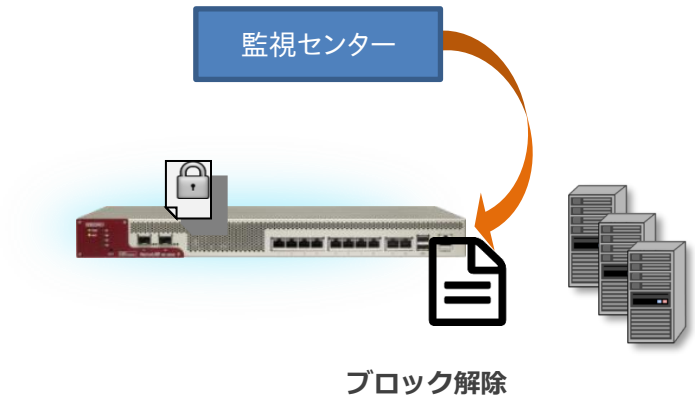
⑱ 遮断対象 IP アドレスを引数に遮断ルールを追加（接続元 IP アドレスの拒否）



3.24.28.4 ブロック解除命令の送信

⑪　遮断時間（初期値：10 分間）を経過した場合は、本製品へ遮断解除命令を送信

⑫　対象 IP アドレスを引数に遮断ルールを削除（接続元 IP アドレスのブロック解除）



3.24.29 クラウド WAF 連携の有効

クラウド WAF を設定するには、クラウド WAF 設定画面に遷移します。

場所: 設定 > ネットワーク > クラウド WAF

■マネージャーアドレス

マネージャーの IP アドレスまたは IP 名を入力します。

■ポート

マネージャーのポート番号を入力します。

■エージェントキー

エージェントキーを入力します。

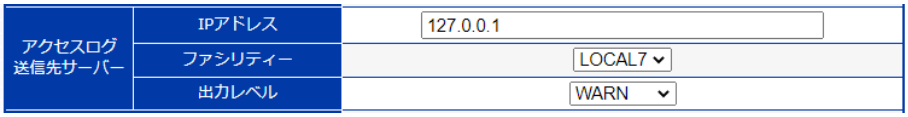
■有効

設定が完了し、クラウド WAF を使用開始するときに有効にします。

クラウド WAF を有効化するとき、設定やネットワーク状況により最大で1分程度時間がかかることがあります。

3.24.30 アクセスログ設定

クラウド WAF を使用する場合は、クラウド WAF を適用する仮想サーバーの設定に以下のようにアクセスログ（3.21.13）を設定します。



通常のアクセスログ設定とは異なり、syslog サーバーのアドレスは外部の IP アドレスではなく、本製品自身(127.0.01)を指定します。また、ファシリティとレベル（local7. LOG_WARNING）を指定します。

アクセスログ機能は L7 負荷分散機能の一部です。アクセスログ機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

3.24.31 アクセスログ表示

本製品で生成されたアクセスログ（3.34.2）を表示するには、**場所: ログ参照 > アクセスログ**を参照ください。

3.24.32 クラウド WAF における防御対象

本製品において防御可能な攻撃を下表に例示します。

攻撃手法
● サーバサイドインクルードインジェクション
● HTTP インジェクション
● LDAP インジェクション
● XML 外部エンティティ
● サーバサイドリクエストフォージェリ
● デシリアライゼーション
● クロスサイトスクリプティング
● SQL インジェクション
● NoSQL インジェクション
● OS コマンドインジェクション
● 改行コードインジェクション
● ディレクトリトラバーサル
● ファイルインクルード攻撃
● URL エンコード攻撃
● ブラックリスト UA
● その他の WEB 攻撃全般
● ミドルウェアなどの脆弱性を突いた攻撃（Apache Struts2 の脆弱性等）

これらの攻撃に対し 100%の防御を保証するものではございません

3.24.33 クラウド WAF における制限事項

● 本製品から監視センターへの通信は UDP プロトコルを利用します。プロトコルの性質上、通信経路で検査対象のログが Drop する可能性があります（監視センターではエージェントからの全ログを受信することを保証していません）。

● 遮断処理は、監視センターに送信されたログを検査後、検知対象の送信元 IP アドレスを遮断対象に登録します（IP アドレスベース遮断）。遮断対象に登録されるまでのリクエストは検知のみを実施します。

● 本製品と監視センター間のステータスが、オフラインからオンラインに変化した場合、オフライン期間のログ情報が監視センターへまとめて送信されます。一度に大量のログが送信された場合、しきい値系のシグネチャで検知/遮断される可能性があります。

ヘルスチェックの設定」を参照してください。
HTTP ヘルスチェック特有の設定項目について、以下に説明します。

場所: 設定 > ヘルスチェック > ヘルスチェック設定

■ヘルスチェック詳細設定

① HTTP 接続維持
一度確立したコネクションをそのまま維持してヘルスチェックを行います。

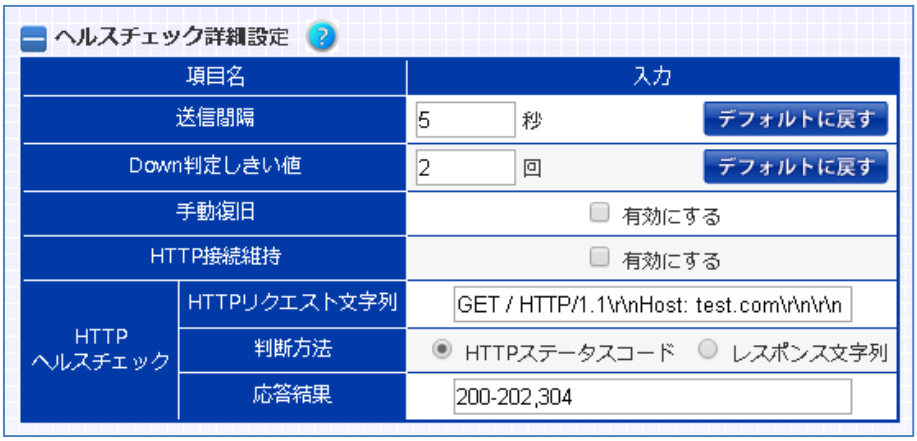
② HTTP ヘルスチェック > HTTP リクエスト文字列
ヘルスチェックで使用する HTTP リクエストの内容を定義します。

③ HTTP ヘルスチェック > 判別方法
HTTP ヘルスチェックの判定方法を選択します。
ステータスコードで判定するには「HTTP ステータスコード」を、レスポンスに含まれる文字列で判定するには「レスポンス文字列」を選択します。

④ HTTP ヘルスチェック > 応答結果
HTTP ヘルスチェックに対する応答を定義します。
定義した内容と異なる場合ヘルスチェックが失敗と判定されます。
応答結果は、③で指定した判定方法に沿った内容を入力します。
「HTTP ステータスコード」を選択した場合、指定された HTTP ステータスコードがサーバーからのレスポンスに含まれていれば正常と判断します。
値は最大 4 パターンまで指定可能です。数字は空白で区切ってください。
また、値をハイフン(-)で連結すると範囲指定が可能になります。
必ず 3 桁の数字を使用してください。

「レスポンス文字列」を選択した場合、指定された文字列がサーバーからのレスポンスに含まれていれば正常と判断します。

以下の例では、
GET / HTTP/1.1
Host: test.com
の HTTP リクエストを対象のサーバーに対して送信し、ステータスコード 200, 201, 202, 304 のいずれかが応答されれば正常と判断します。



ポイント リクエスト文字列の末尾の改行は省略しても構いません。その場合、本製品が自動で改行を付加して HTTP リクエストを送信します。

ポイント 指定したリクエストが HTTP1.0 で、かつ「HTTP 接続維持」が有効にされた場合、HTTP リクエスト内に"Connection: Keep-Alive"ヘッダーを自動で挿入します。

3.24.34 SSL ヘルスチェック

SSL ヘルスチェックでは、コネクション要求から SSL ネゴシエーション完了までが動作すれば正常と判断します。
SSL ヘルスチェックを実施するにはヘルスチェック対象サーバー設定欄の「SSL」を有効にします。
SSL ヘルスチェックポリシーの定義と詳細設定は「3.23クラウド WAF
本章では、本製品のクラウド WAF 連携機能について説明します。

3.24.35 クラウド WAF 連携

クラウド WAF 連携機能を使用すると、本製品を流れる着信トラフィックと発信トラフィックをフィルタリングできます。

クラウド WAF 連携機能は、L7 負荷分散のアクセスログ機能（3.21.13）を使用して、WAF センタールールとシグネチャマッチングをおこないます。攻撃検知対象の場合は、センターから本製品へ遮断命令を送信し、遮断対象 IP アドレスをブロックします。

遮断対象 IP アドレスは IPv4 アドレスとなります。

3.24.36 クラウド WAF 動作イメージ

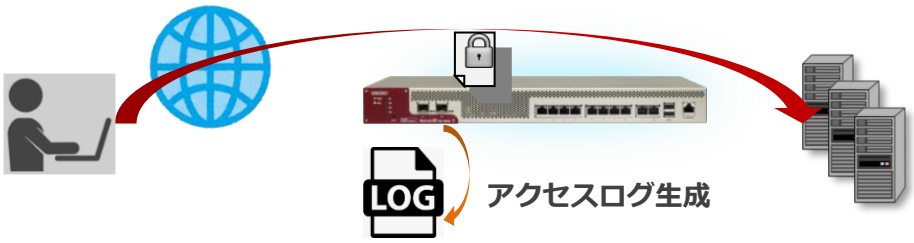
攻撃検知の遮断動作イメージにを以下に示します。

3.24.36.1 アクセスログの生成

⑲ クライアントから Web サーバーへ HTTP リクエストを送信

⑳ Web アプリケーションが HTTP レスポンスを送信

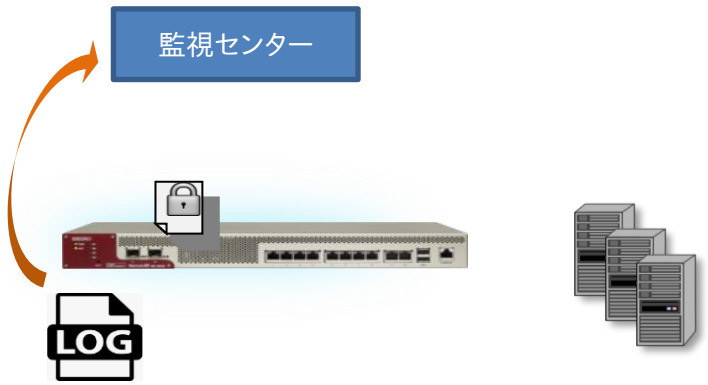
21 本製品がアクセスログを生成



3.24.36.2 監視センターへログ送信

⑬ アクセスログを収集

⑭ 監視センターへログを送信（UDP）

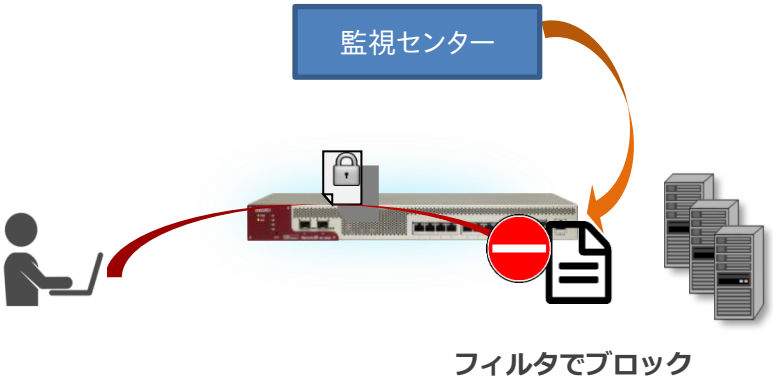


3.24.36.3 遮断命令の送信

⑲ 監視センターで、ログを WAF センタールールとシグネチャマッチング

⑳ 攻撃検知対象の場合は、監視センターから本製品へ遮断命令を送信

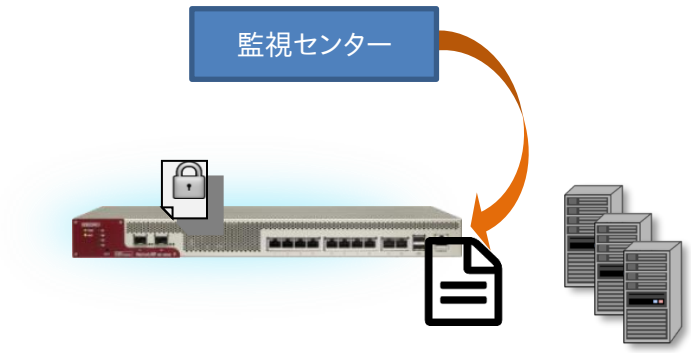
21 遮断対象 IP アドレスを引数に遮断ルールを追加（接続元 IP アドレスの拒否）



3.24.36.4 ブロック解除命令の送信

⑬ 遮断時間（初期値：10 分間）を経過した場合は、本製品へ遮断解除命令を送信

⑭ 対象 IP アドレスを引数に遮断ルールを削除(接続元 IP アドレスのブロック解除)



ブロック解除

3.24.37 クラウド WAF 連携の有効

クラウド WAF を設定するには、クラウド WAF 設定画面に遷移します。

場所: 設定 > ネットワーク > クラウド WAF

■マネージャーアドレス

マネージャーの IP アドレスまたは IP 名を入力します。

■ポート

マネージャーのポート番号を入力します。

■エージェントキー

エージェントキーを入力します。

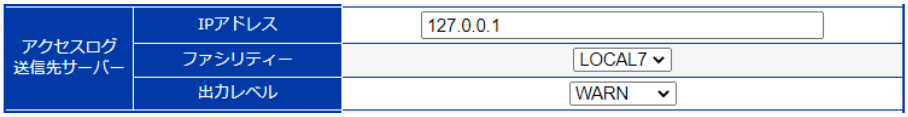
■有効

設定が完了し、クラウド WAF を使用開始するときに有効にします。

クラウド WAF を有効化するとき、設定やネットワーク状況により最大で1分程度時間がかかることがあります。

3.24.38 アクセスログ設定

クラウド WAF を使用する場合は、クラウド WAF を適用する仮想サーバーの設定に以下のようにアクセスログ（3.21.13）を設定します。



通常のアクセスログ設定とは異なり、syslog サーバーのアドレスは外部の IP アドレスではなく、本製品自身(127.0.01)を指定します。また、ファシリティとレベル（local7. LOG_WARNING）を指定します。

アクセスログ機能は L7 負荷分散機能の一部です。アクセスログ機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

3.24.39 アクセスログ表示

本製品で生成されたアクセスログ（3.34.2）を表示するには、**場所: ログ参照 > アクセスログ**を参照ください。

3.24.40 クラウド WAF における防御対象

本製品において防御可能な攻撃を下表に例示します。

攻撃手法
● サーバサイドインクルードインジェクション
● HTTP インジェクション
● LDAP インジェクション
● XML 外部エンティティ
● サーバサイドリクエストフォージェリ
● デシリアライゼーション
● クロスサイトスクリプティング
● SQL インジェクション
● NoSQL インジェクション
● OS コマンドインジェクション
● 改行コードインジェクション
● ディレクトリトラバーサル
● ファイルインクルード攻撃
● URL エンコード攻撃
● ブラックリスト UA
● その他の WEB 攻撃全般
● ミドルウェアなどの脆弱性を突いた攻撃（Apache Struts2 の脆弱性等）

これらの攻撃に対し 100%の防御を保証するものではございません

3.24.41 クラウド WAF における制限事項

● 本製品から監視センターへの通信は UDP プロトコルを利用します。プロトコルの性質上、通信経路で検査対象のログが Drop する可能性があります（監視センターではエージェントからの全ログを受信することを保証していません）。

● 遮断処理は、監視センターに送信されたログを検査後、検知対象の送信元 IP アドレスを遮断対象に登録します（IP アドレスベース遮断）。遮断対象に登録されるまでのリクエストは検知のみを実施します。

● 本製品と監視センター間のステータスが、オフラインからオンラインに変化した場合、オフライン期間のログ情報が監視センターへまとめて送信されます。一度に大量のログが送信された場合、しきい値系のシグネチャで検知/遮断される可能性があります。

ヘルスチェックの設定」を参照してください。

HTTPS でのヘルスチェックを行う場合「SSL」を有効にして、HTTP ヘルスチェックを設定します。HTTP ヘルスチェックの詳細は「3.24.26HTTP ヘルスチェック」を参照してください。

3.24.42 DNS ヘルスチェック

DNS ヘルスチェックでは、DNS リクエストをサーバーAP に送信しレスポンスをチェックします。
サーバーから DNS レスポンスを受信し、レスポンスの QR ビットが 1, Opcode が 0, RCODE が 0 ならば正常と判断します。

DNS ヘルスチェックを設定するには、ヘルスチェック対象サーバー設定欄の「L7 プロトコル」で「dns」を選択します。
ヘルスチェックポリシーの定義と詳細設定の一部は「3.23クラウド WAF
本章では、本製品のクラウド WAF 連携機能について説明します。

3.24.43 クラウド WAF 連携

クラウド WAF 連携機能を使用すると、本製品を流れる着信トラフィックと発信トラフィックをフィルタリングできます。
クラウド WAF 連携機能は、L7 負荷分散のアクセスログ機能（3.21.13）を使用して、WAF センタールールとシグネチャマッチングをおこないます。攻撃検知対象の場合は、センターから本製品へ遮断命令を送信し、遮断対象 IP アドレスをブロックします。

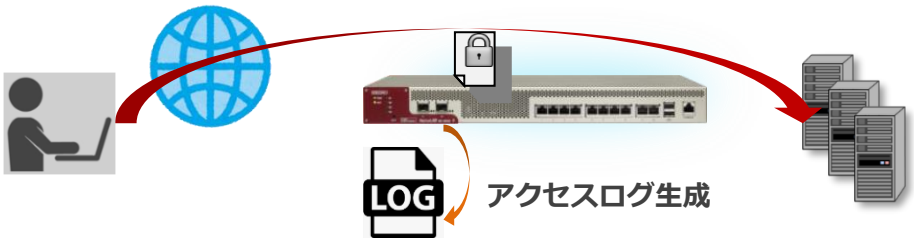
遮断対象 IP アドレスは IPv4 アドレスとなります。

3.24.44 クラウド WAF 動作イメージ

攻撃検知の遮断動作イメージにを以下に示します。

3.24.44.1 アクセスログの生成

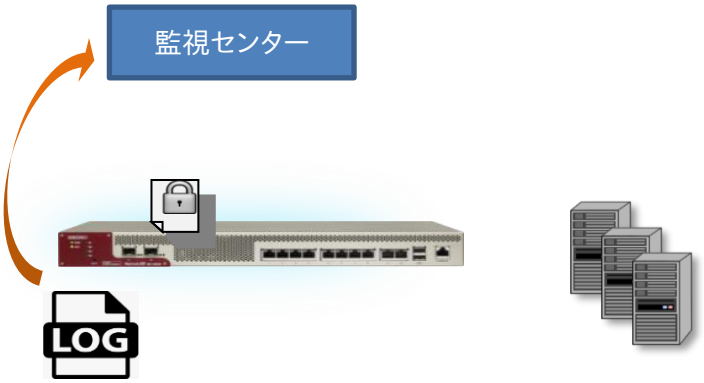
22　クライアントから Web サーバーへ HTTP リクエストを送信
23　Web アプリケーションが HTTP レスポンスを送信
24　本製品がアクセスログを生成



3.24.44.2 監視センターへログ送信

⑮　アクセスログを収集

⑯　監視センターへログを送信（UDP）

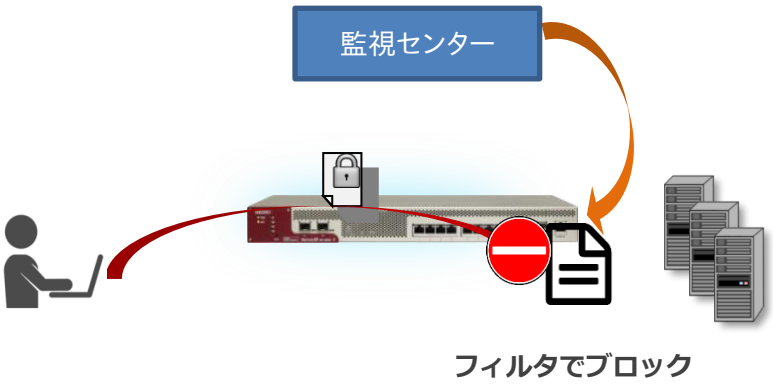


3.24.44.3 遮断命令の送信

22　監視センターで、ログを WAF センタールールとシグネチャマッチング

23　攻撃検知対象の場合は、監視センターから本製品へ遮断命令を送信

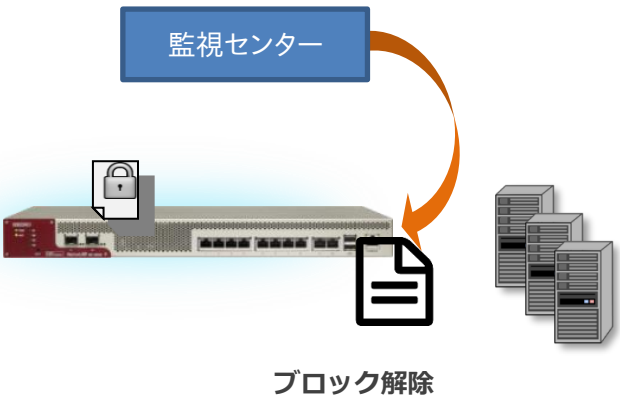
24　遮断対象 IP アドレスを引数に遮断ルールを追加（接続元 IP アドレスの拒否）



3.24.44.4 ブロック解除命令の送信

⑮ 遮断時間（初期値：10 分間）を経過した場合は、本製品へ遮断解除命令を送信

⑯ 対象 IP アドレスを引数に遮断ルールを削除(接続元 IP アドレスのブロック解除)



3.24.45 クラウド WAF 連携の有効

クラウド WAF を設定するには、クラウド WAF 設定画面に遷移します。

場所: 設定 > ネットワーク > クラウド WAF

■マネージャーアドレス

マネージャーの IP アドレスまたは IP 名を入力します。

■ポート

マネージャーのポート番号を入力します。

■エージェントキー

エージェントキーを入力します。

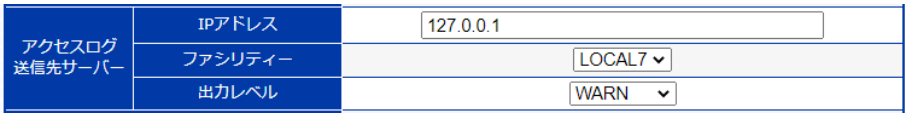
■有効

設定が完了し、クラウド WAF を使用開始するときに有効にします。

クラウド WAF を有効化するとき、設定やネットワーク状況により最大で1分程度時間がかかることがあります。

3.24.46 アクセスログ設定

クラウド WAF を使用する場合は、クラウド WAF を適用する仮想サーバーの設定に以下のようにアクセスログ（3.21.13）を設定します。



通常のアクセスログ設定とは異なり、syslog サーバーのアドレスは外部の IP アドレスではなく、本製品自身(127.0.01)を指定します。また、ファシリティとレベル（local7. LOG_WARNING）を指定します。

アクセスログ機能は L7 負荷分散機能の一部です。アクセスログ機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

3.24.47 アクセスログ表示

本製品で生成されたアクセスログ（3.34.2）を表示するには、**場所: ログ参照 > アクセスログ**を参照ください。

3.24.48 クラウド WAF における防御対象

本製品において防御可能な攻撃を下表に例示します。

攻撃手法
● サーバサイドインクルードインジェクション
● HTTP インジェクション
● LDAP インジェクション
● XML 外部エンティティ
● サーバサイドリクエストフォージェリ
● デシリアライゼーション
● クロスサイトスクリプティング
● SQL インジェクション
● NoSQL インジェクション
● OS コマンドインジェクション
● 改行コードインジェクション
● ディレクトリトラバーサル
● ファイルインクルード攻撃
● URL エンコード攻撃
● ブラックリスト UA
● その他の WEB 攻撃全般
● ミドルウェアなどの脆弱性を突いた攻撃（Apache Struts2 の脆弱性等）

これらの攻撃に対し 100%の防御を保証するものではございません

3.24.49 クラウド WAF における制限事項

● 本製品から監視センターへの通信は UDP プロトコルを利用します。プロトコルの性質上、通信経路で検査対象のログが Drop する可能性があります（監視センターではエージェントからの全ログを受信することを保証していません）。

● 遮断処理は、監視センターに送信されたログを検査後、検知対象の送信元 IP アドレスを遮断対象に登録します（IP アドレスベース遮断）。遮断対象に登録されるまでのリクエストは検知のみを実施します。

● 本製品と監視センター間のステータスが、オフラインからオンラインに変化した場合、オフライン期間のログ情報が監視センターへまとめて送信されます。一度に大量のログが送信された場合、しきい値系のシグネチャで検知/遮断される可能性があります。

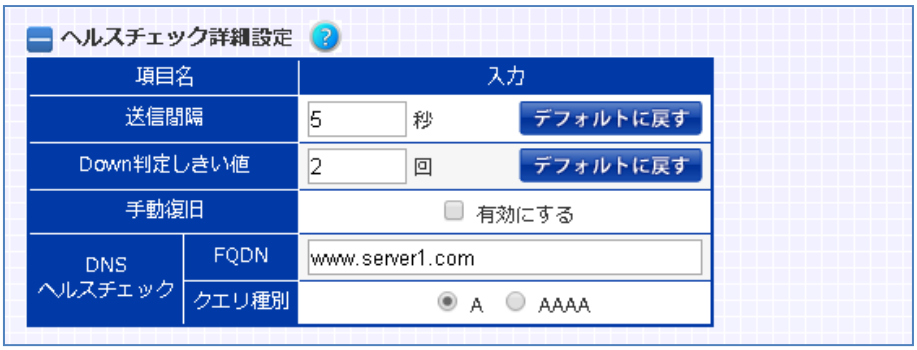
ヘルスチェックの設定」を参照してください。

場所: 設定 > ヘルスチェック > ヘルスチェック設定

■ヘルスチェック詳細設定

① DNS ヘルスチェック ＞FQDN
問い合わせるドメイン名を定義します。

② DNS ヘルスチェック ＞ クエリ種別
ヘルスチェックに使用する DNS クエリ種別を選択します。



3.24.50 その他アプリケーションヘルスチェック

その他アプリケーションプロトコルに対するヘルスチェックを以下に明記します。
各種ヘルスチェックポリシーの定義と詳細設定は「3.23クラウド WAF
本章では、本製品のクラウド WAF 連携機能について説明します。

3.24.51 クラウド WAF 連携

クラウド WAF 連携機能を使用すると、本製品を流れる着信トラフィックと発信トラフィックをフィルタリングできます。
クラウド WAF 連携機能は、L7 負荷分散のアクセスログ機能（3.21.13）を使用して、WAF センタールールとシグネチャマッチングをおこないます。攻撃検知対象の場合は、センターから本製品へ遮断命令を送信し、遮断対象 IP アドレスをブロックします。

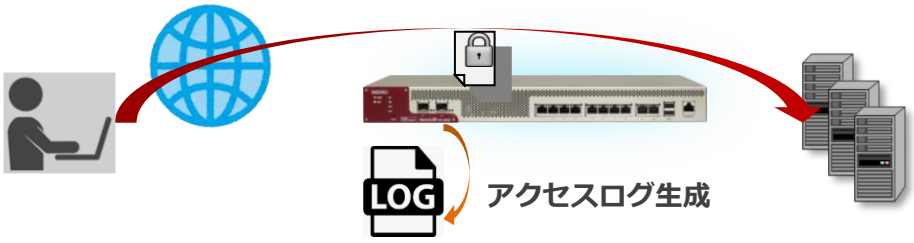
遮断対象 IP アドレスは IPv4 アドレスとなります。

3.24.52 クラウド WAF 動作イメージ

攻撃検知の遮断動作イメージにを以下に示します。

3.24.52.1 アクセスログの生成

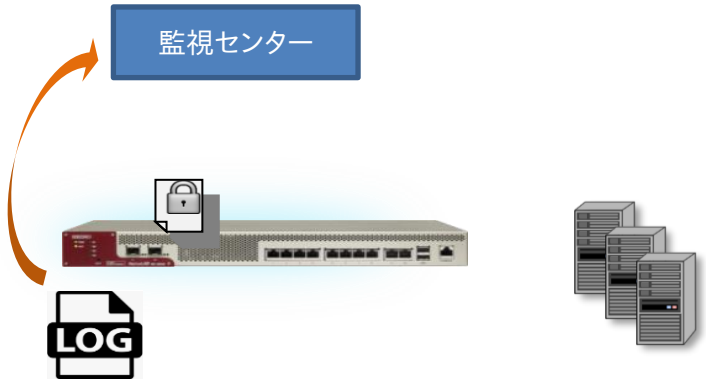
25　クライアントから Web サーバーへ HTTP リクエストを送信
26　Web アプリケーションが HTTP レスポンスを送信
27　本製品がアクセスログを生成



3.24.52.2 監視センターへログ送信

⑰　アクセスログを収集

⑱　監視センターへログを送信（UDP）

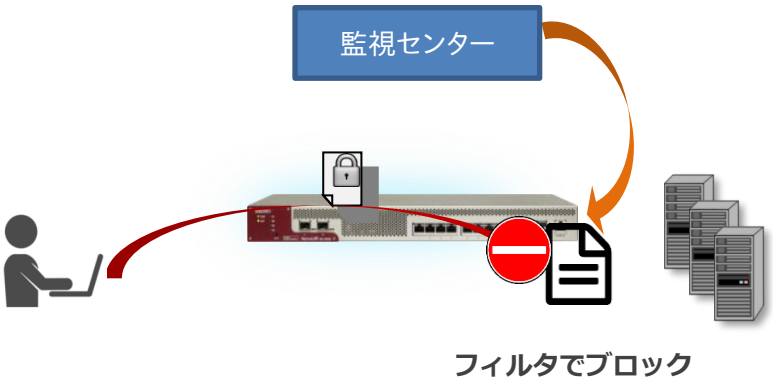


3.24.52.3 遮断命令の送信

25　監視センターで、ログを WAF センタールールとシグネチャマッチング

26　攻撃検知対象の場合は、監視センターから本製品へ遮断命令を送信

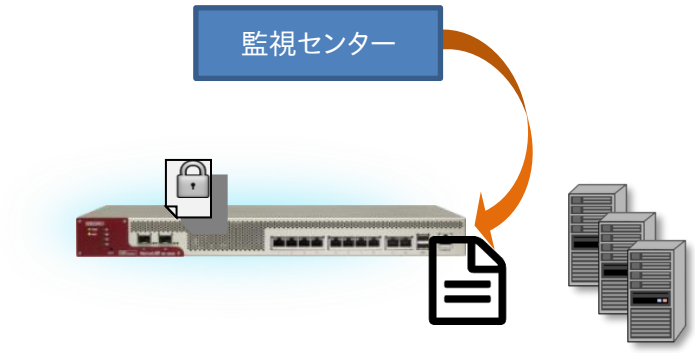
27　遮断対象 IP アドレスを引数に遮断ルールを追加（接続元 IP アドレスの拒否）



3.24.52.4 ブロック解除命令の送信

⑰　遮断時間（初期値：10 分間）を経過した場合は、本製品へ遮断解除命令を送信

⑱　対象 IP アドレスを引数に遮断ルールを削除（接続元 IP アドレスのブロック解除）



ブロック解除

3.24.53 クラウド WAF 連携の有効

クラウド WAF を設定するには、クラウド WAF 設定画面に遷移します。

場所: 設定 > ネットワーク > クラウド WAF

■マネージャーアドレス

マネージャーの IP アドレスまたは IP 名を入力します。

■ポート

マネージャーのポート番号を入力します。

■エージェントキー

エージェントキーを入力します。

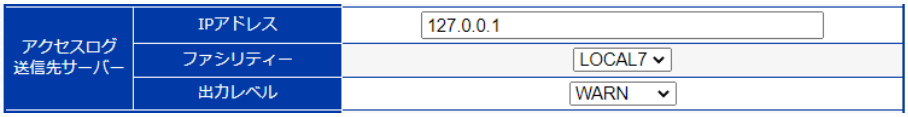
■有効

設定が完了し、クラウド WAF を使用開始するときに有効にします。

クラウド WAF を有効化するとき、設定やネットワーク状況により最大で1分程度時間がかかることがあります。

3.24.54 アクセスログ設定

クラウド WAF を使用する場合は、クラウド WAF を適用する仮想サーバーの設定に以下のようにアクセスログ（3.21.13）を設定します。



通常のアクセスログ設定とは異なり、syslog サーバーのアドレスは外部の IP アドレスではなく、本製品自身(127.0.01)を指定します。また、ファシリティとレベル（local7. LOG_WARNING）を指定します。

アクセスログ機能は L7 負荷分散機能の一部です。アクセスログ機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

3.24.55 アクセスログ表示

本製品で生成されたアクセスログ（3.34.2）を表示するには、**場所: ログ参照 > アクセスログ**を参照ください。

3.24.56 クラウド WAF における防御対象

本製品において防御可能な攻撃を下表に例示します。

攻撃手法
● サーバサイドインクルードインジェクション
● HTTP インジェクション
● LDAP インジェクション
● XML 外部エンティティ
● サーバサイドリクエストフォージェリ
● デシリアライゼーション
● クロスサイトスクリプティング
● SQL インジェクション
● NoSQL インジェクション
● OS コマンドインジェクション
● 改行コードインジェクション
● ディレクトリトラバーサル
● ファイルインクルード攻撃
● URL エンコード攻撃
● ブラックリスト UA
● その他の WEB 攻撃全般
● ミドルウェアなどの脆弱性を突いた攻撃（Apache Struts2 の脆弱性等）

これらの攻撃に対し 100%の防御を保証するものではございません

3.24.57 クラウド WAF における制限事項

● 本製品から監視センターへの通信は UDP プロトコルを利用します。プロトコルの性質上、通信経路で検査対象のログが Drop する可能性があります（監視センターではエージェントからの全ログを受信することを保証していません）。

● 遮断処理は、監視センターに送信されたログを検査後、検知対象の送信元 IP アドレスを遮断対象に登録します（IP アドレスベース遮断）。遮断対象に登録されるまでのリクエストは検知のみを実施します。

● 本製品と監視センター間のステータスが、オフラインからオンラインに変化した場合、オフライン期間のログ情報が監視センターへまとめて送信されます。一度に大量のログが送信された場合、しきい値系のシグネチャで検知/遮断される可能性があります。

ヘルスチェックの設定」を参照してください。

■FTP ヘルスチェック
設定するには、ヘルスチェック対象サーバー設定欄の「L7 プロトコル」で「ftp」を選択します。
TCP コネクション確立後、サーバーからのメッセージを待ちます。
ステータス 220 で始まるメッセージをヘルスチェック送信間隔以内に受信すれば正常と判断します。

■IMAP4 ヘルスチェック
設定するにはヘルスチェック対象サーバー設定欄の「L7 プロトコル」で「imap4」を選択します。
TCP コネクション確立後、サーバーからのメッセージを待ちます。
"*OK"で始まるﾒｯｾｰｼﾞをヘルスチェック送信間隔以内に受信すれば正常と判断します。

■NTP ヘルスチェック
設定するにはヘルスチェック対象サーバー設定欄の「L7 プロトコル」で「ntp」を選択します。
サーバービットが ON であり、かつ LI（Leap Indicator）ビットが"11"以外である NTP 応答をヘルスチェック送信間隔以内に受信すれば正常と判断します。

■POP3 ヘルスチェック
設定するにはヘルスチェック対象サーバー設定欄の「L7 プロトコル」で「pop3」を選択します。
TCP コネクション確立後、サーバーからのメッセージを待ちます。
"+OK"で始まるﾒｯｾｰｼﾞをヘルスチェック送信間隔以内に受信すれば正常と判断します。

■SMTP ヘルスチェック
設定するにはヘルスチェック対象サーバー設定欄の「L7 プロトコル」で「smtp」を選択します。
TCP コネクション確立後、サーバーからのメッセージを待ちます。
ステータスコード 220 で始まるメッセージをヘルスチェック送信間隔以内に受

信すれば正常と判断します。

3.24.58 ヘルスチェックの組み合わせ

複数のヘルスチェックポリシーを組み合わせたヘルスチェックポリシーを登録することが可能です。

別に設定されたヘルスチェックポリシーを最大４つまで、論理演算子 AND(&&)と OR(||)を使用して組み合わせます。演算子の前後はブランクが必要です。
AND で結ばれたサーバーはどれかひとつでもダウンすると、全てダウン状態にセットされます。(全て ALIVE 状態の時だけアップと判断されます)
OR で結ばれたサーバーはどれかひとつでもヘルスチェックにパスすれば、全てアップ状態にセットされます。(全て DOWN 状態の時だけダウンと判断されます)

場所: 設定 > ヘルスチェック > ヘルスチェック組み合わせ設定

ヘルスチェックの組み合わせポリシーを定義します。

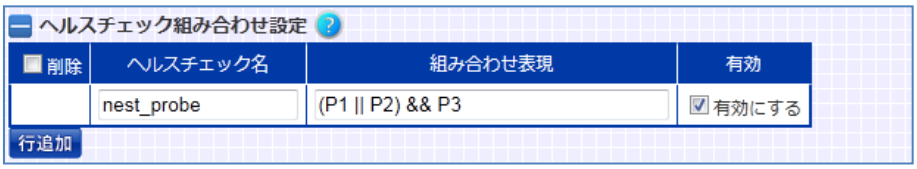
■ヘルスチェック組み合わせ設定

① ヘルスチェック名
ヘルスチェックポリシー名を定義します。

② 組み合わせ表現
ヘルスチェックポリシーの組み合わせ表現を定義します。

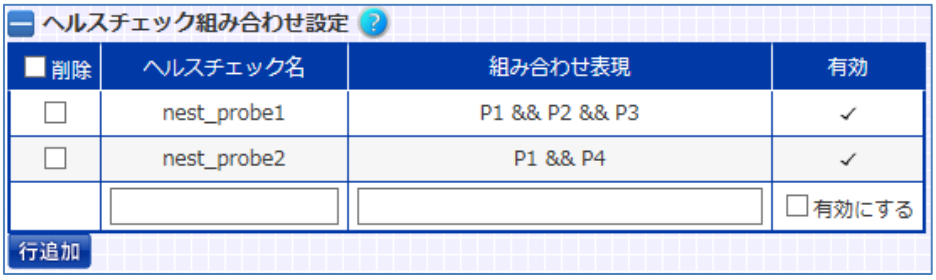
③ 有効
ヘルスチェック組み合わせポリシーを有効にします。

以下の例では、ヘルスチェックポリシーP1、P2 の両方がダウンするか、P3 がダウンした場合、P1、P2、P3 全てのヘルスチェックがダウンにセットされます。



⚠ 注意

以下のように、ヘルスチェックポリシー(P1)を複数の組み合わせ設定に登録しないでください。



3.25 冗長構成の設定

本製品は冗長構成で動作します。
本章では冗長構成に関する設定方法を例とともに記します。
冗長構成は、同一機種、同一バージョン間で構成してください。

⚠ 注意 SX-3940/3920 を冗長構成でご使用の場合、本体前のスルースイッチを必ず OFF にしてください。

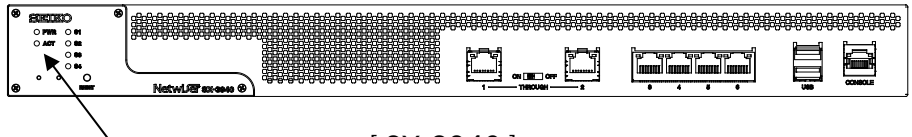
3.25.1 概要

3.25.1.1 アクティブ/スタンバイ方式

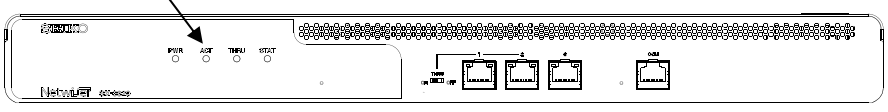
本装置で冗長構成を組む場合、アクティブ／スタンバイ方式での冗長構成となります。
2 台のうち、負荷分散を行っている機器を“マスター機”あるいは“マスター状態”と呼び、待機している機器を“バックアップ機”あるいは“バックアップ状態”と呼びます。
SX-3950,SX-3945,SX-3940,SX-3920 では、冗長構成で動作している場合、マスター機は前面パネルの ACTIVE ランプが点灯し、バックアップ機は消灯します。

■ACTIVE ランプ（緑）
冗長構成でない場合は常に点灯しています。
冗長構成時はマスター機が点灯、バックアップ機が消灯します。

＊SX-3950、SX-3945 の AVTIVE ランプも同じ位置になります。



[SX-3940]



[SX-3920]

3.25.1.2 VRRP プロトコル

本製品で採用している VRRP プロトコルは冗長構成を組む 2 台の機器間で VRRP 広告パケットを交換することにより動作します。
基本的には、以下のように動作します。

① マスター機は VRRP 広告パケットを一定間隔で送出し続ける。
② バックアップ機はマスター機からの VRRP 広告パケットを受信する。
③ バックアップ機は VRRP 広告パケットを一定時間受信できなくなると、マスター機に異常が発生したと判断し、自身をマスター状態に遷移する。

ポイント

本製品では、

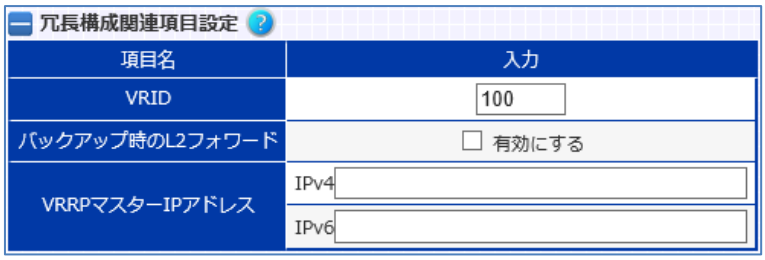
1. マスター機の VRRP 広告パケットは仮想ルーターID(VRID)を設定した VLAN からデフォルトでは 1 秒に 1 回送信します。(送信インターバルは変更できます)
2. バックアップ機は送信インターバルの約 3 倍の時間 VRRP 広告パケットが受信できなければマスター状態に遷移します。

VRRP に関連する設定の詳細は「3.25.5VRRP 設定」を参照してください。

3.25.2 冗長構成の有効化

VRRP を有効にするには、VRRP 広告パケットをやり取りする VLAN 毎に仮想ルーターID（VRID）を設定します。仮想ルーターID は、マスター機とバックアップ機で同じ ID を割り振ってください。
後述する VRRP 設定の順序に関係なく、VRID を設定したタイミングで VRRP が有効になります。
VRID の設定は VLAN 設定画面で実施します。

場所： 設定 ＞ ネットワーク ＞VLAN＞VLAN 選択 ＞VLAN 設定
任意の VLAN ID に対して、仮想ルーターID（VRID）を設定します。
■冗長構成関連項目設定
① VRID
該当の VLAN で VRRP を有効にするため、任意の VRID を入力します。



ポイント

VRRP では、同一仮想ルーターID の機器がマスター／バックアップの関係になるので、当該ロードバランサー以外の VRRP 機器とは異なる仮想ルーターID を割り振ってください。

ポイント

仮想ルーターID の設定のみでは、コマンドやセッション情報の同期は行われません。相手機器との同期状態を確立するための設定が必要です。
詳細は「3.25.7冗長同期設定」を参照してください。

機器情報画面の「ネットワーク ＞ VRRP」で VRRP 情報を参照できます。

3.25.3 L2 ループの防止

デフォルト設定では、バックアップ状態の機器でも L2 フォワーディングを行います。よって、ネットワークの接続が物理的に L2 ループを含んでいる場合、バックアップ機の MAC フレームの中継によりブロードキャストストームが発生します。冗長構成に伴う L2 ループの防止策として以下の 2 つの方法のうちどちらかを設定します。

① L2 フォワーディングの停止設定
② スパニングツリー設定

以下、それぞれについて詳しく述べます。

3.25.3.1 L2 フォワーディングの停止設定

バックアップ状態において、任意の VLAN の L2 フォワーディングを停止することで、L2 ループを防止できます。

L2 フォワーディングの停止設定は VLAN 設定画面で実施します。

場所: 設定 > ネットワーク > VLAN > VLAN 選択 > VLAN 設定

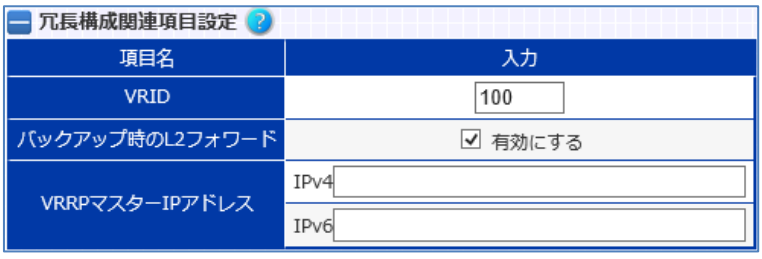
任意の VLAN ID に対して、バックアップ時の L2 フォワード設定を変更します。

■冗長関連項目設定

① バックアップ時の L2 フォワード

「有効にする」を選択すると、VRRP 状態にかかわらず、L2 フォワーディングを行います。

「有効にする」の選択を外すと、バックアップ時に L2 フォワーディングを行いません。(マスター状態では L2 フォワーディングを行います)



ポイント バックアップ時の L2 フォワードが無効にされた VLAN では、管理 IP アドレスへ

のアクセスは継続して行えますが、パケットの送信には以下の制限があります。

1. 本製品からのパケットの送信は、VLAN に割り当てられたイーサネットポートのうち、ポート番号が最も小さいリンクアップしているポートから行われます。
2. トランクポート(tagged 設定されたポート)がある場合は、ポート VLAN のポートを優先して使用します。

3.25.3.2 スパニングツリー設定

L2 ループを防止する 2 つ目の方法は、スパニングツリー設定です。
機器全体に反映されるスパニングツリーの設定を変更します。
イーサネットポートや論理チャネル毎のスパニングツリーの設定は「3.11スパニングツリーの設定」を参照してください。
本製品のスパニングツリーは Rapid Spanning-Tree Protocol（RSTP）で動作します。対向機器との関係でレガシーな STP で動作することはありますが、レガシーな STP 動作を設定で強制することはできません。
スパニングツリー設定はスパニングツリー設定画面で実施します。

場所: 設定 > ネットワーク > スパニングツリー

■スパニングツリー設定

① Bridge Priority
VRRP 状態に連動させて、スパニングツリーのブリッジプライオリティーを変更することができます。これにより、接続スイッチがスパニングツリーに未対応の場合でも本製品同士で STP を構成することができます。
ここでは、機器がマスター状態の際のブリッジプライオリティーを設定します。

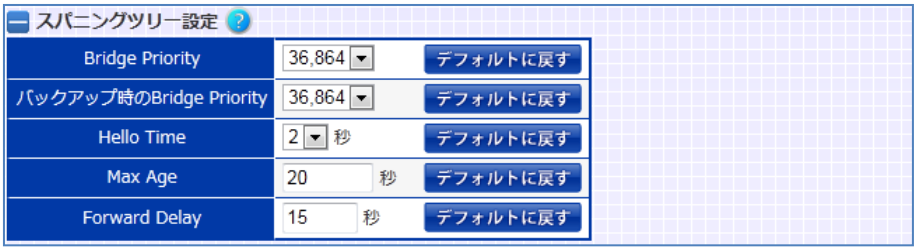
② バックアップ時の Bridge Priority
ここでは、機器がバックアップ状態の際のブリッジプライオリティーを設定します。

③ Hello Time
STP 動作がレガシーな STP で動作する場合、本製品が送信する Bridge Protocol Data Unit(BPDU)フレームの送信間隔はデフォルトで 2 秒です。
ここでは、送信する BPDU フレームの送信間隔を設定します。

④ Max Age
STP 動作がレガシーな STP で動作する場合、BPDU フレームのタイムアウ

ト時間はデフォルトで 20 秒です。
ここでは、BPDU フレームのタイムアウト時間を設定します。

⑤ Forward Delay
STP 動作がレガシーな STP で動作する場合、本製品がフォワーディング状態に遷移する際の遅延時間はデフォルトで 15 秒です。
ここでは、本製品がフォワーディング状態に遷移する際の遅延時間を設定します。



3.25.4 強制バックアップ

マスター状態で動作する機器を、強制的にバックアップ状態にすることが可能です。強制バックアップ実行画面で実施します。

場所: 設定 > 冗長構成 > 強制バックアップ

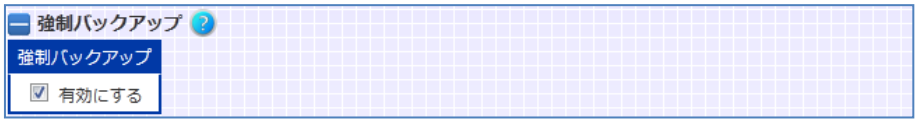
マスター状態で動作する機器を強制的にバックアップ状態にする。

■強制バックアップ

① 強制バックアップ

「有効にする」を選択して実行すると、強制的にバックアップ状態にすることができます。

「有効にする」の選択を外して実行すると、強制バックアップ状態が解除され、再び VRRP 状態の判定処理を行い、両機器間で VRRP 状態の決定がなされます。



注意 vrrp force-backup の設定を行った場合はマスターに昇格しなくなります。冗長構成で運用を行う際は解除を行って下さい。

3.25.5 VRRP 設定

VRRP を利用して、相手機器と冗長状態を形成します。
VRRP を設定するには、任意の VLAN で VRID の登録がされている必要があります。VRID の登録は「3.25.2 冗長構成の有効化」を参照してください。
VRRP に関する詳細設定は VRRP 設定画面で実施します。

場所: 設定 > 冗長構成 > VRRP

■VRRP 設定

① 冗長構成相手
冗長構成相手先 IP アドレスを入力します。

② プリエンプション
「有効にする」を選択して登録すると、プリエンプトモードを有効にします。
「有効にする」の選択を外して登録すると、プリエンプトモードを無効にします。

③ プライオリティー
VRRP プライオリティー値を入力します。

④ プライオリティー(peer)
冗長構成相手側に設定する VRRP プライオリティーを設定します。
本設定はコマンド同期できる状態でないと、冗長相手に反映されません。

⑤ 送信間隔
VRRP 広告の送信間隔を入力します。
時間は入力値×10(msec)が設定されます。

⑥ 状態遷移遅延
状態遷移の遅延時間を入力します。
バックアップ状態に遷移した時に、VRRP 広告パケットの受信開始を任意の時間だけ遅らせることができます。

3.25.5.1 プリエンプト機能の設定

本製品はフェイルオーバーが発生した後のフェイルバック動作として以下の 2 つをサポートしています。

① プリエンプトモード

機器に設定したプライオリティー値にしたがって、常にその値が高い方がマスター機となります。

② 非プリエンプトモード

先に起動した機器がプライオリティー値とは関係なくマスター機として動作し続けます。また、フェイルオーバーが発生後、バックアップ状態に遷移した機器が復旧しても、フェイルバック（切り戻し動作）が発生することなく動作し続けます。

また、プリエンプトモードが有効な場合は、VRRP プライオリティー値を適切に設定する必要があります。

デフォルト設定では、プライオリティー100 に設定されています。

後述の設定情報の同期機能（「3.25.7冗長同期設定」参照）が有効である場合、冗長相手のプライオリティー値を自機器から変更できます。ただし、設定同期が無効な場合無視されます。

⚠ 注意

マスター・バックアップ両機器でプリエンプト設定が異なっていると正常に動作しなくなる恐れがあります。両機器間でプリエンプト機能の有効/無効を合わせてください。

ポイント

マスター、バックアップ機のプライオリティー値が等しい場合、先にマスター状態に遷移した機器がマスター状態でありつづけます。

たとえば、マスター状態の機器 A の故障によって機器 B がマスターに遷移したとすると、機器 A を復旧させても機器 B がマスター状態のままになります。

プリエンプト機能の有効/無効や VRRP プライオリティーの設定は VRRP 設定画面で実施します。画面詳細は「3.25.5VRRP 設定」を参照してください。

3.25.5.2 VRRP 広告パケットの送信間隔

VRRP 広告のパケットは、1 秒間隔で送信されます。
送信間隔の変更は VRRP 設定画面で実施します。画面詳細は「3.25.5VRRP 設定」を参照してください。

3.25.5.3 VRRP 広告パケットの受信遅延設定

スパニングツリー設定によって L2 ループの防止を行っている場合、ツリー構成が収束するまでに数十秒かかることがあります。
収束までの間 VRRP 広告パケットを受信できなくなりますので、正常な状態であるにも関わらずバックアップ機がマスター状態に遷移してしまうことがあります。
これを避けるためには、状態遷移遅延時間を設定します。
状態遷移遅延時間の設定は、VRRP 設定画面で実施します。画面詳細は「3.25.5VRRP 設定」を参照してください。

3.25.5.4 リンク監視機能の設定

自機のイーサネットポートのリンク状態を監視し、VRRP 広告パケットを動的に変更する機能です。イーサネットポートのリンク状態を監視し、フェイルオーバーのタイミングをコントロールすることができます。
SX-3990 では、ホストマシン内部の仮想ブリッジ（または仮想スイッチや TAP）に本製品が接続されている限り、動的なリンク DOWN が発生し得ないケースがあります。この場合、自らイーサネットポートを停止状態にしない限りは、リンク状態が DOWN になることがないため、本機能を使用することはできません。

設定により以下のようなことができます。

① VRRP 広告パケットの送信停止
リンク監視設定のグループに指定した全ての監視対象リンクがダウンした場合、マスター機は VRRP 広告パケットの送信を停止します。
広告パケット送信が停止しますので、フェイルオーバーが起こります。

② プライオリティー値の動的な変更
リンク監視設定のグループに含まれる監視対象ポートの何れかがリンク

ダウンする度にプライオリティー値を減少させることができます。
たとえば、
(ア) プリエンプトモードの冗長構成。
(イ) リンク監視対象グループとしてポート 1～3。
(ウ) マスター機のプライオリティー設定は 107。バックアップ機の設定は 100。
(エ) リンクダウン時の減算値は 5。
と設定した場合、マスター機のスイッチポートのリンク状態により以下のようにプライオリティー値を動的に変更します。

ケース①

設定 priority 値=107

ポート 1	LINK DOWN
ポート 2	LINK UP
ポート 3	LINK UP

実際の priority 値 =107−5
=**102**

ケース②

設定 priority 値=107

ポート 1	LINK DOWN
ポート 2	LINK UP
ポート 3	LINK DOWN

実際の priority 値 =107−5−5
=**97**

ケース①の場合は、減算後のプライオリティー値が 102 であるため、フェイルオーバーは起こりませんが、ケース②のように 2 ポートがダウンすると、プライオリティー値が 97 となる（バックアップ機より小さい）ので、フェイルオーバーが起こります。

リンク監視機能は VRRP 設定画面で実施します。
（SX-3990 は、ハイパーバイザー上にインストールされていることにより、自らイーサネットポートを停止状態にしない限りはリンク状態が DOWN になることはないため、リンク監視機能を使用することはできません。）

場所: 設定 > 冗長構成 >VRRP

VRRP 設定画面で、リンク監視機能の設定をします。

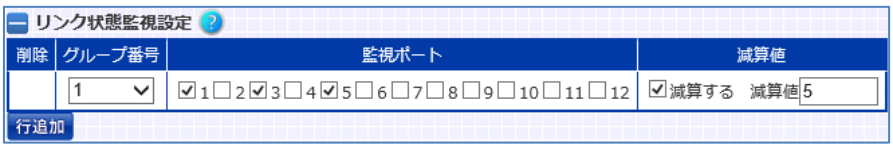
■リンク状態監視設定

① グループ番号
状態監視ルールに付けるグループ番号を選択します。

② 監視ポート
監視対象のイーサネットポート番号を選択します。

③ 減算値
リンクダウン時に VRRP プライオリティーの減算を行う場合、「減算する」を選択し、減算値を入力します。

以下の例では、マスター機のポート 1, 3, 5 がすべてリンクダウンすると、VRRP 広告パケットの送信を停止します。更に、マスター機のポート 1, 3, 5 がリンクダウンする度に VRRP プライオリティー値を 5 ずつ減算します。



ポイント

リンク監視のグループは複数設定することができます。グループごとにプライオリティー減算値を独立に設定できます。ただし、複数グループに同一ポート番号を含めることはできません。

3.25.6 冗長 IP アドレス（Redundant IP アドレス）の設定

VLAN インターフェイスに冗長用の IP アドレス（以下、冗長 IP アドレス）を設定することが可能です。冗長 IP アドレスは、冗長構成でマスター状態になった場合にのみ有効になるアドレスです。

冗長 IP アドレスを設定することで、VLAN インターフェイスへの外部機器からのアクセスを一元的にマスター機側で受け付けることが可能になります。

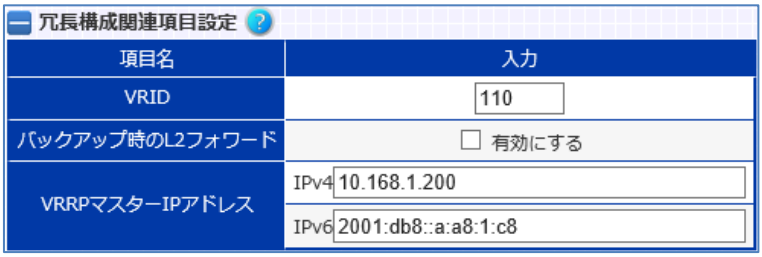
冗長 IP アドレスの設定は VLAN 設定画面で実施します。

場所：設定 ＞ ネットワーク ＞VLAN＞VLAN 選択 ＞VLAN 設定

■冗長構成関連項目設定

① VRRP マスタ IP アドレス

冗長構成でマスター状態になった場合にのみ有効になるアドレスを登録します。



冗長 IP アドレスの使用用途として、たとえば、クライアント側とサーバー側のネ

ットワークが別のセグメントである場合、サーバーからの戻りパケットのゲートウェイアドレスとして冗長 IP アドレスを登録します。
他にも、冗長 IP アドレスにアクセスすれば、現在マスター状態の機器にアクセスすることが可能になりますので、管理画面へのアクセス先 IP としても利用できます。

3.25.7 冗長同期設定

3.25.7.1 設定とセッション情報の同期

マスター、バックアップ機器間で設定およびセッション情報の同期を行うには、冗長相手先のアドレス設定は VRRP 設定画面で実施します。
画面詳細は「3.25.5VRRP 設定」を参照してください。

これにより、
① 操作中の機器で実行されたコマンドが、冗長相手機器でも実行されます。
② 負荷分散用のセッション情報がマスター機と同期します。

冗長同期は、マスター、バックアップの両機器に、
① *peer-address* 設定
② 仮想ルーターID（VRID）設定
の両方を設定すると機能します。

⚠ 注意 冗長同期はマスター、バックアップ間の同期用 TCP コネクションの状態によっては、コマンドやセッション情報を喪失することがありますので注意してください。

3.25.7.2 設定同期

マスター、バックアップの両機器に仮想ルーターID（VRID）設定と冗長相手 IP アドレスを設定すると、現在設定中の機器で入力したコマンドを冗長相手機器でも即時実行します。
設定を変更するコマンドが同期対象となります。しかし、以下のコマンドは冗長相手に同期されません。

同期対象外コマンド	
特権モード	*clear* *1
	copy
	hostname
	import all
	import config
	import firmware
	passwd

	sync config
	write erase
VLAN 設定モード	*ip address*
イーサネット設定モード	*mirror-port*
	monitor
SSL 設定モード	*csr* *2
VRRP 設定モード	*peer-address*

*1 *clear content* コマンドを除く

*2 *csr* コマンド実行時に生成される署名要求書は冗長相手先に同期されませんが、同時に生成される秘密鍵は、冗長構成相手に同期されます。

3.25.7.2.1 設定情報の一括同期

情報同期実行画面で、全設定情報の同期を実行すると、一括同期対象外の設定を除く全ての設定情報・ユーザーアカウント情報を冗長相手機器にコピーします。

場所: 設定 > 冗長構成 > 情報同期実行

■情報同期実行

① 全設定情報を同期する

「同期する」を選択すると、現在設定中の機器の設定情報・ユーザーアカウント情報を冗長相手機器にコピーします。

全設定情報には、SSL 関連ファイルや sorry コンテンツも含まれます。

冗長相手機器でその設定を有効にするには再起動をする必要があります。

「全設定情報」には、SSL 関連ファイルや sorry コンテンツも含まれます。

ただし、以下の設定項目は冗長相手に同期されません。

一括同期対象外の設定項目	
特権モード	ホスト名
	端末設定 （自動ログアウト、コマンド履歴保存件数など）
VLAN 設定モード	機器 IP アドレス

VRRP 設定モード	冗長相手 IP アドレス

ポイント

全設定情報の同期を実行すると、自機器の VLAN の機器 IP アドレスを±1 したアドレスが、冗長相手側の VLAN の機器 IP アドレスとして設定されます。
+1 か−1 かは、自機器の VLAN の機器 IP と冗長相手の IP アドレスの大小関係から決定します。(比較する自機器の IP アドレスは、コマンド同期に使用している VLAN の機器 IP アドレスです。)
「自機器の IP アドレス ＞ 現在冗長相手で設定されている IP アドレス」であれば、自機器の IP アドレスから−1 されたアドレスが冗長相手の機器 IP アドレスとしてセットされます。

3.25.7.2.2 設定情報の非同期設定

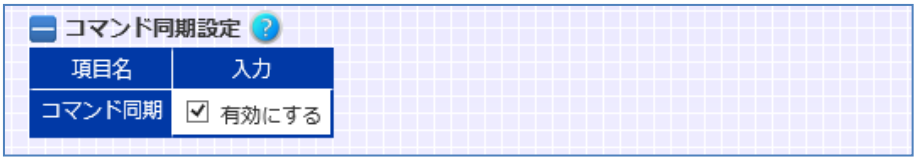
冗長同期相手の IP アドレスと VRID が設定されている状態であっても、設定情報の同期を行わないように設定を変更することが可能です。
設定情報の同期停止は同期設定画面で実施します。

場所: 設定 ＞ 冗長構成 ＞ 同期設定

■コマンド同期設定

① コマンド同期

設定情報の同期を停止させるには、「有効にする」の選択を解除します。



3.25.7.3 セッション情報同期

セッション情報同期では、マスター機で生成される以下の負荷分散セッション情報を定期的にバックアップ機に送信します。

① L4 負荷分散用セッション情報
② IP アドレスセッション維持情報
③ Cookie セッション維持情報

ポイント

各セッション情報は 1 秒に 1 回、前回の送信からの差分情報をマスター機からバックアップ機へと送信します。

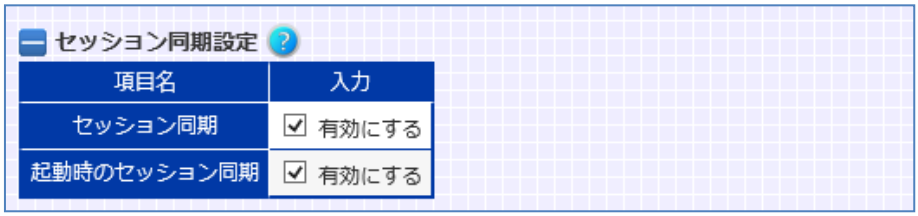
起動時のセッション同期が有効な場合、デフォルトでは、システム起動後に最初にバックアップ状態に遷移したタイミングでマスター機との全セッション同期を実施します。ただし、全セッション情報の同期は後述（「セッション情報の一括同期3.25.7.3.1」参照）の通り、マスター機の負荷分散停止を伴いますので注意が必要です。
同期設定画面で、起動時のセッション同期を無効にする事が可能です。

場所: 設定 > 冗長構成 > 同期設定

■セッション同期設定

① セッション同期
セッション情報の同期を停止させるには、「有効にする」の選択を解除します。

② 起動時のセッション同期
「有効にする」を選択した場合、システム起動時にマスター機との全セッション情報の同期を実施します。
「有効にする」の選択を外すと、システム起動時にマスター機とのセッション情報の同期を実施しません。



機器情報画面の「ネットワーク > セッション同期」で、セッション同期に関する統計情報を参照できます。

3.25.7.3.1 セッション情報の一括同期

実行時のマスター機とバックアップ機のセッション情報を一括同期する事が可能です。

場所: 設定 > 冗長構成 > 情報同期実行

■情報同期実行

① 全セッション情報を同期する

「同期する」を選択すると、マスター機の全セッション情報をバックアップ機にコピーします。

注意

本機能は、マスター機でもバックアップ機でも実行できます。
実行すると、バックアップ機のセッション情報をすべて破棄し、その後、マスター機の全セッション情報をコピーします。
このため、一括同期中はマスター機の負荷分散機能がほぼ停止状態になります（最大 1 分程度）ので注意してください。

ポイント

後述のセッション情報の非同期設定が有効であっても、一括同期は実行できます。

3.26 フェイルスルーの設定

SX-3940,SX-3920 では、本製品に何らかの障害が発生し処理が継続出来ない場合、ポート1とポート2をハードウェアにより直結することができます。これにより、万が一機器に障害が発生しても、提供中のサービスを止めることなく継続することが可能です。

フェイルスルー機能を有効にするには、仮想サーバーに関連付ける実サーバーのうち1台の実サーバーの IP アドレスに、仮想サーバーと同一 IP アドレスを定義します。
これによりフェイルスルー設定であることをシステムが自動で検知し、フェイルスルー機能が有効になります。また、仮想 IP と同一 IP の実サーバー(以下、フェイルスルー対象サーバーと呼称）を仮想サーバーとの関連付けから解除すると、フェイルスルー機能は無効になります。

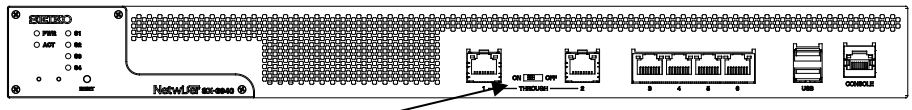
■スルースイッチ

フェイルスルー機能を使用する場合は、スルースイッチをONにしてください（左方向にスライドさせる）。

フェイルスルー機能を使用しない場合スルースイッチを OFF にしてください。

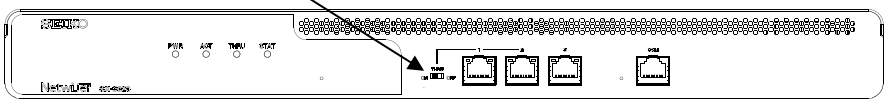
工場出荷状態でスルースイッチは ON に設定されています。

スルー スイッチ	フェイル スルー設定	電源 OFF 時 または故障発生時	通常時
ON	有効	ポート 1-2 間が接続されます	ポート１とポート２は、それぞれ内部の通信用ＩＣに接続され通信が行われます
OFF	無効	ポート 1-2 間は接続されません	



[SX-3940]

スルースイッチ



[SX-3920]

機器情報画面の「ネットワーク ＞ イーサネット」でスルースイッチの状態を参照することができます。

■接続するイーサネットポートについての制限
フェイルスルー機能を使用する場合は、ポート1にクライアント側ネットワーク、ポート2にサーバー側ネットワークを接続してください。また、イーサネットポートの接続先ネットワーク種別が以下のように設定されている必要があります。
ポート1　network
ポート2　server
この設定は、フェイルスルー機能が有効になった際にシステムが自動で設定します。ただし、フェイルスルー対象サーバーを仮想サーバーとの関連付けから解除しても、接続先ネットワーク種別の設定は元の設定に戻りませんので注意してください。
元に戻すには、バランシングポート定義画面で設定を変更します。詳細は「3.17 接続先ネットワーク種別」を参照してください。
ポート 1、2 以外のポートも負荷分散に使用することは可能ですが、フェイルスルー対象サーバーは必ずポート 2 に接続してください。

■ヘルスチェックポリシーについての制限
フェイルスルー設定を行った場合、必ずフェイルスルー対象サーバーに対する icmp ヘルスチェックが登録されている必要があります。

⚠ 注意

フェイルスルー機能には他にもいくつかの制約事項があります。
以下に全ての制約事項を記しますので、フェイルスルー機能を使用する場合は必ず確認してください。

1. 仮想サーバーと同一の IP アドレスである実サーバーが 1 台バインドされていること
2. イーサネットポートの接続先種別（バランシングポート定義）が正しく設定されていること
3. スルースイッチが ON になっていること
4. ポート 1 とポート 2 のリンク速度、VLAN ID、802.1Q タグ設定の有効/無効が一致していること
5. スパニングツリープロトコル、リンク集約が設定されていないこと
6. 冗長構成でないこと
7. 仮想サーバーにソース NAT が設定されていないこと
8. 仮想サーバーに DSR オプション付きでバインドされた実サーバーが存在しないこと

9. 仮想サーバーと関連付けている全ての実サーバーの IP バージョンが一致していること
10. フェイルスルー対象サーバーに対する icmp ヘルスチェックの登録がされており、かつサービス開始前に必ず一度はヘルスチェックが成功していること

フェイルスルー設定を有効にするには、仮想サーバーと同一 IP アドレスのサーバーを登録して、仮想サーバーにバインドします。
実サーバーの登録は「3.21.2実サーバーの設定」を参照してください。
実サーバーと仮想サーバーとの関連付け設定は「3.21.16仮想サーバーと実サーバーの関連付け」を参照してください。

■フェイルスルー対象サーバーの交換
フェイルスルー対象サーバーに関するヘルスチェック DOWN を検出した後、フェイルスルー対象サーバーの機器交換や、それ準ずる作業により該当の IP アドレスに紐付く MAC アドレスが変更される場合、対象サーバーの接続性が復旧した後でも本製品から対象サーバーに実施している ICMP ヘルスチェックは DOWN 判定のままとなります。
この状態を復旧するには、対象サーバーの交換が済んだ後に、対象サーバーへのヘルスチェックポリシーを起動し直す必要があります。
ヘルスチェックポリシーを起動し直すには、「無効」に設定した後でもう一度「有効」にする必要があります。詳しくは「3.23 クラウド WAF
本章では、本製品のクラウド WAF 連携機能について説明します。

3.26.1 クラウド WAF 連携

クラウド WAF 連携機能を使用すると、本製品を流れる着信トラフィックと発信トラフィックをフィルタリングできます。
クラウド WAF 連携機能は、L7 負荷分散のアクセスログ機能（3.21.13）を使用して、WAF センタールールとシグネチャマッチングをおこないます。攻撃検知対象の場合は、センターから本製品へ遮断命令を送信し、遮断対象 IP アドレスをブロックします。

遮断対象 IP アドレスは IPv4 アドレスとなります。

3.26.2 クラウド WAF 動作イメージ

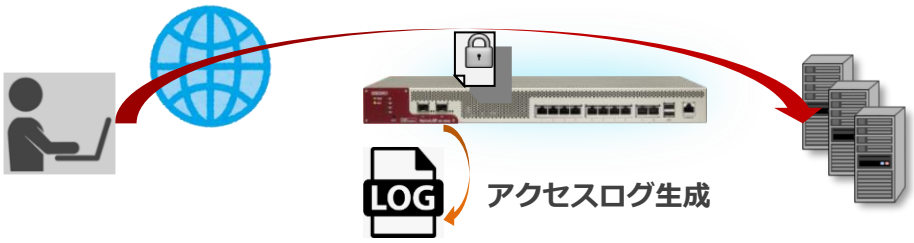
攻撃検知の遮断動作イメージにを以下に示します。

3.26.2.1 アクセスログの生成

28　クライアントから Web サーバーへ HTTP リクエストを送信

29　Web アプリケーションが HTTP レスポンスを送信

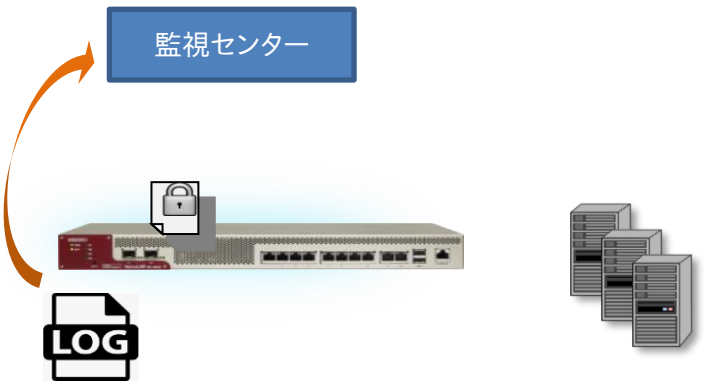
30　本製品がアクセスログを生成



3.26.2.2 監視センターへログ送信

⑲　アクセスログを収集

⑳　監視センターへログを送信（UDP）

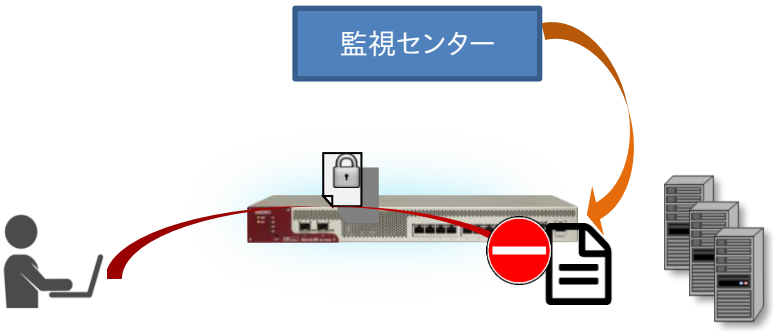


3.26.2.3 遮断命令の送信

28　監視センターで、ログを WAF センタールールとシグネチャマッチング

29　攻撃検知対象の場合は、監視センターから本製品へ遮断命令を送信

30　遮断対象 IP アドレスを引数に遮断ルールを追加（接続元 IP アドレスの拒否）

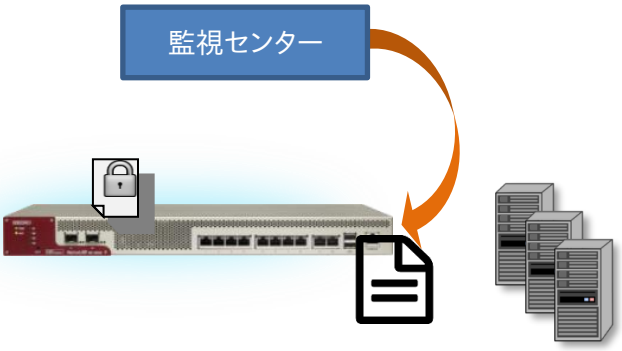


フィルタでブロック

3.26.2.4 ブロック解除命令の送信

⑲　遮断時間（初期値：10 分間）を経過した場合は、本製品へ遮断解除命令を送信

⑳　対象 IP アドレスを引数に遮断ルールを削除(接続元 IP アドレスのブロック解除)



ブロック解除

3.26.3 クラウド WAF 連携の有効

クラウド WAF を設定するには、クラウド WAF 設定画面に遷移します。

場所: 設定 > ネットワーク > クラウド WAF

■マネージャーアドレス

マネージャーの IP アドレスまたは IP 名を入力します。

■ポート

マネージャーのポート番号を入力します。

■エージェントキー

エージェントキーを入力します。

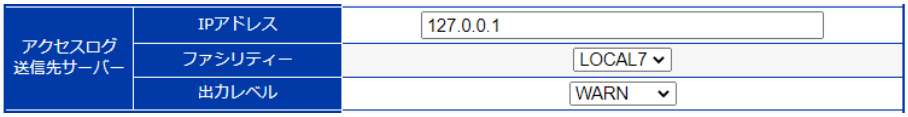
■有効

設定が完了し、クラウド WAF を使用開始するときに有効にします。

クラウド WAF を有効化するとき、設定やネットワーク状況により最大で1分程度時間がかかることがあります。

3.26.4 アクセスログ設定

クラウド WAF を使用する場合は、クラウド WAF を適用する仮想サーバーの設定に以下のようにアクセスログ（3.21.13）を設定します。



通常のアクセスログ設定とは異なり、syslog サーバーのアドレスは外部の IP アドレスではなく、本製品自身(127.0.01)を指定します。また、ファシリティとレベル（local7. LOG_WARNING）を指定します。

アクセスログ機能は L7 負荷分散機能の一部です。アクセスログ機能を有効にすると、仮想サーバーに URL スイッチングや cookie スティッキー設定がされていなくてもリクエストは L7 レベルで処理されます。

3.26.5 アクセスログ表示

本製品で生成されたアクセスログ（3.34.2）を表示するには、**場所: ログ参照 > アクセスログ**を参照ください。

3.26.6 クラウド WAF における防御対象

本製品において防御可能な攻撃を下表に例示します。

攻撃手法
● サーバサイドインクルードインジェクション
● HTTP インジェクション
● LDAP インジェクション
● XML 外部エンティティ
● サーバサイドリクエストフォージェリ
● デシリアライゼーション
● クロスサイトスクリプティング
● SQL インジェクション
● NoSQL インジェクション
● OS コマンドインジェクション
● 改行コードインジェクション
● ディレクトリトラバーサル
● ファイルインクルード攻撃
● URL エンコード攻撃
● ブラックリスト UA
● その他の WEB 攻撃全般
● ミドルウェアなどの脆弱性を突いた攻撃（Apache Struts2 の脆弱性等）

これらの攻撃に対し 100%の防御を保証するものではございません

3.26.7 クラウド WAF における制限事項

● 本製品から監視センターへの通信は UDP プロトコルを利用します。プロトコルの性質上、通信経路で検査対象のログが Drop する可能性があります（監視センターではエージェントからの全ログを受信することを保証していません）。

● 遮断処理は、監視センターに送信されたログを検査後、検知対象の送信元 IP アドレスを遮断対象に登録します（IP アドレスベース遮断）。遮断対象に登録されるまでのリクエストは検知のみを実施します。

● 本製品と監視センター間のステータスが、オフラインからオンラインに変化した場合、オフライン期間のログ情報が監視センターへまとめて送信されます。一度に大量のログが送信された場合、しきい値系のシグネチャで検知/遮断される可能性があります。

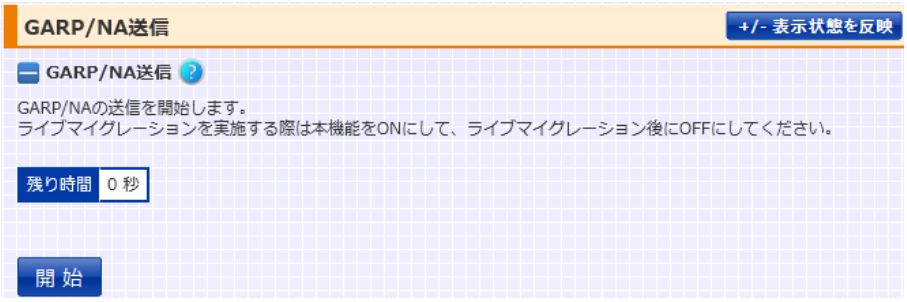
ヘルスチェックの設定」を参照してください。

3.27 ライブマイグレーション（SX-3990 のみ）

稼働中の仮想マシンを停止することなく別のホストマシン上に移動させる機能をライブマイグレーション機能と呼称します。
SX-3990 をライブマイグレーションさせる場合、その動作は各ハイパーバイザーの仕様に依存します。

ライブマイグレーションが正常に完了すると、ハイパーバイザーが自発的に、仮想 NIC の MAC アドレスを送信元とした MAC フレーム（RARP など）を送出し、隣接機器に対して、ARP キャッシュの更新を促します。
ただし、ここで通知される MAC フレームは、仮想 NIC の MAC アドレスを送信元とした MAC フレームであり、装置 IP や仮想 IP アドレスに紐付く MAC アドレスが通知されるわけではありません。装置 IP および仮想 IP に紐付く MAC アドレスを通知するには、GARP/NA 送信を開始し近隣機器の ARP キャッシュを更新します。

場所：設定 ＞ システム ＞ 機器管理 ＞GARP/NA 送信



ポイント

GARP/NA 送信開始後、10 分経過すると自動で送信を停止します。

3.28 機器テスト

3.28.1 ICMP リクエスト送信

ICMP リクエストを任意の機器に送信できます。

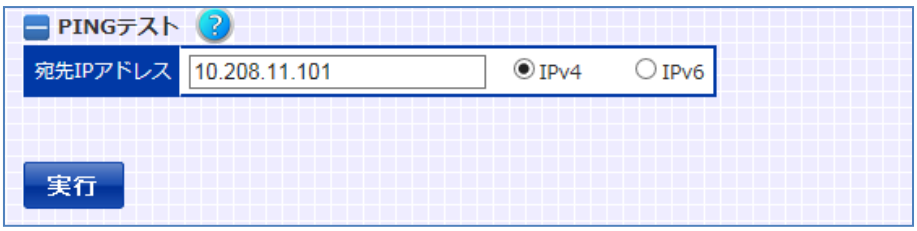
場所: 設定 > システム > 機器管理 > 機器テスト > PING テスト

■PING テスト

① 宛先 IP アドレス

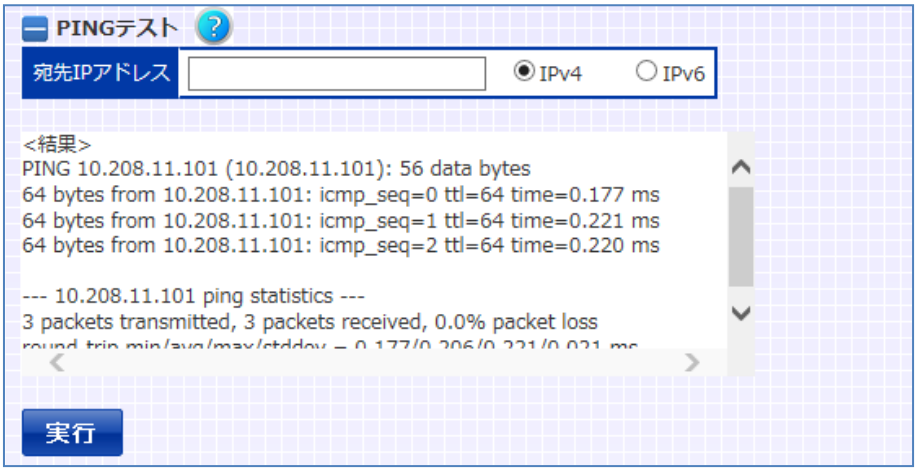
任意の IP アドレスまたは IP アドレス名のいずれかを入力します。

指定した IP アドレスまたは IP アドレス名が IPv4 アドレスであれば「IPv4」を、IPv6 アドレスであれば「IPv6」を選択します。



「実行」ボタンを押下すると、任意のアドレスへ ICMP リクエストを送信します。

送信完了後、結果が入力項目の下に表示されます。



3.28.2 シスログ出力

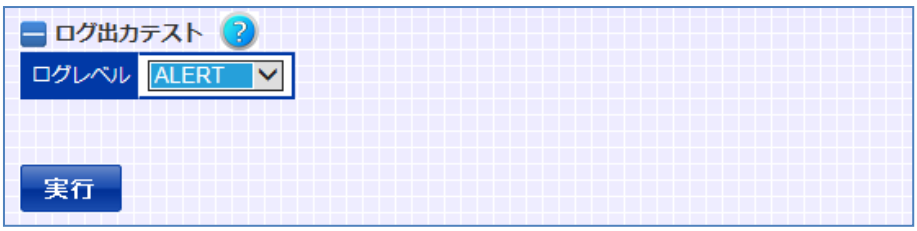
任意のログレベルや任意のタイミングで、テスト用のシスログを出力できます。
本製品は、システムログの出力によって、ログサーバーへログ情報を送信したり、
メールでシステム管理者へ送信したりする事が可能です。
これらの設定をテストする際に本機能を使用してください。

場所: 設定 > システム > 機器テスト > SYSLOG テスト

■ログ出力テスト

① ログレベル

任意のログレベルを選択して「実行」ボタンを押下します。



テスト用シスログは以下のフォーマットで出力されます。

<Mon> <Day> <Time>　<host 名> lbconfigd: [++++ FOR DEBUG ++++] LOG LEVEL "<ログレベル>"　<ランダムな数値>

例）

Aug 3 15:34:47　netwiser lbconfigd: [++++ FOR DEBUG ++++] LOG LEVEL "ALERT"　<007b8bed0>

3.28.3 TRACEROUTE

宛先ホストまでのネットワーク経路をリスト表示します。

場所: 設定 > システム > 機器管理 > 機器テスト > TRACEROUTE テスト

■TRACEROUTE テスト

① プロトコル

宛先ホストのアドレスが IPv4 アドレスであれば「IPv4」を、IPv6 アドレスであれば「IPv6」を選択します。

② 宛先ホスト

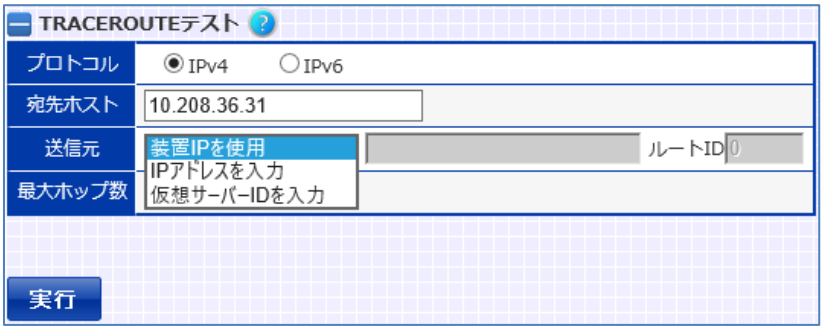
任意の IP アドレス、IP アドレス名、またはホスト名のいずれかを入力します。

③ 送信元

送信元を指定したい場合は、管理 IP アドレス、IP アドレス、仮想サーバーID、または仮想サーバー名を指定することができます。

送信元が IP アドレスであれば「IP アドレスを入力」を、送信元が仮想サーバーID、または仮想サーバー名であれば「仮想サーバーID を入力」を選択します。

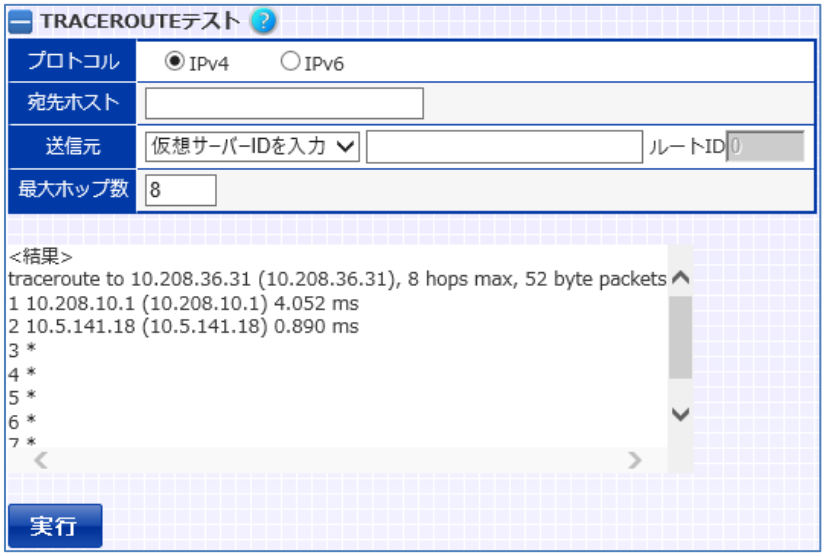
送信元に「IP アドレスを入力」を選択した場合はルート ID を指定することが出来ます。「仮想サーバーID を入力」を選択した場合は該当の仮想サーバーに設定されているルート ID が自動的に使用されます。



④ 最大ホップ数

最大ホップ数を指定できます。設定できる最大ホップ数の範囲は 1 から 32 です。

「実行」ボタンを押下すると、経路の調査が開始されます。
完了後、結果が入力項目の下に表示されます。



ポイント

ルート ID を指定した場合は、指定したルート ID と同一の ID を持つルーティングテーブルに従います。ルート ID を指定しない場合はルート ID 0 が使用されます。

ポイント

送信元 IP アドレスは以下のアドレスのみ使用可能です。

1. VLAN の管理 IP アドレス(VLAN 設定画面の管理 IP アドレス設定)
2. 冗長アドレス(VLAN 設定画面の VRRP マスターIP アドレス設定)
3. 仮想サーバードレス(仮想サーバー設定画面の仮想サーバーID 設定)
4. NAT プールアドレス(NAT プール設定画面の NAT プールアドレス設定)

NAT プールアドレスを送信元アドレスとして使用するには、リバース NAT 登録またはソース NAT の設定がされている必要があります。

⚠ 注意

宛先ホストに到達できない場合は、最大 32 秒間の応答待ち時間が発生します。

3.29 システム起動/停止操作

3.29.1 システム停止

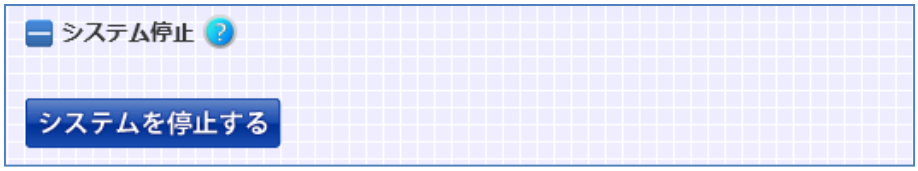
本製品を停止します。

場所: 設定 > システム > 機器管理 > システム停止

■システム停止

「システムを停止する」ボタンを押下します。

確認画面が表示されるので、システムを停止させるには「はい」を押下します。



3.29.2 再起動

本製品を再起動します。

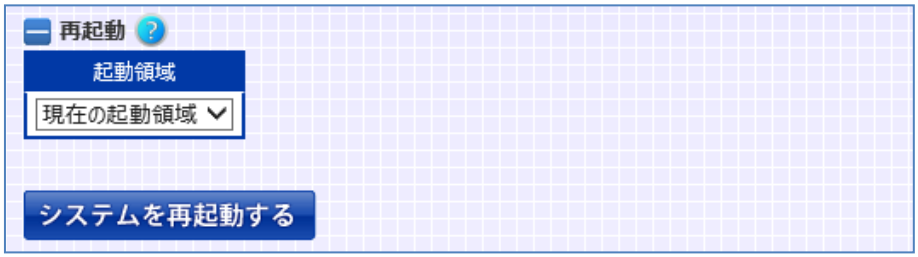
場所: 設定 > システム > 機器管理 > 再起動

■再起動

① 起動領域

再起動後に参照する起動領域を選択し、「システムを再起動する」ボタンを押下します。

確認画面が表示されるので、再起動させるには「はい」を押下します。



3.29.3 工場出荷時設定

本製品の設定情報を初期化します。

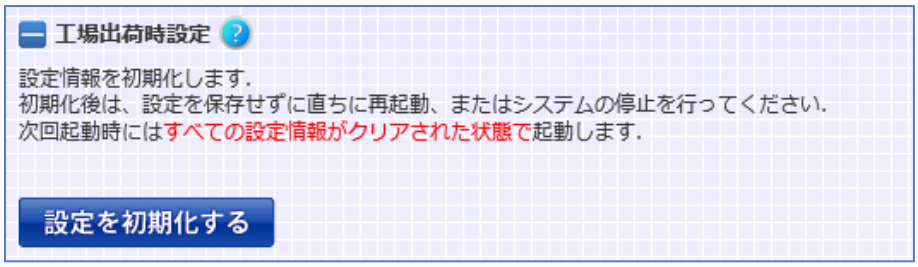
場所: 設定 > システム > 機器管理 > 再起動

■工場出荷時設定

「設定を初期化する」ボタンを押下します。

確認画面が表示されるので、初期化するには「はい」を押下します。

次回起動時にはすべての設定情報がクリアされた状態で起動します。

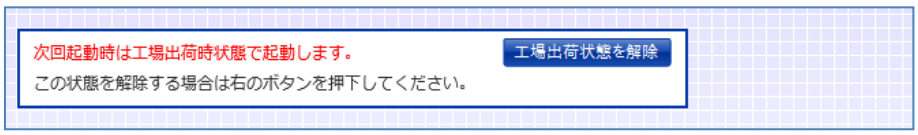


初期化後は、設定を保存せずに直ちに再起動(「3.29.2再起動」参照)、またはシステムの停止(「3.29.1システム停止」参照)を行ってください。

「設定を初期化する」ボタンを押下後は、次回起動時に初期状態となりますが、この状態を解除する事も可能です。

「設定を初期化する」ボタンを押下後に、画面上部に以下の表示が出力されるようになります。

初期化設定を解除する場合は「工場出荷状態を解除」を押下してください。



3.30 かんたん設定

SX-3920 には「かんたん設定」が設けられています。
「かんたん設定」では、負荷分散の設定が一画面で行えます。
本章は「かんたん設定」画面での設定方法について、例とともに説明します。

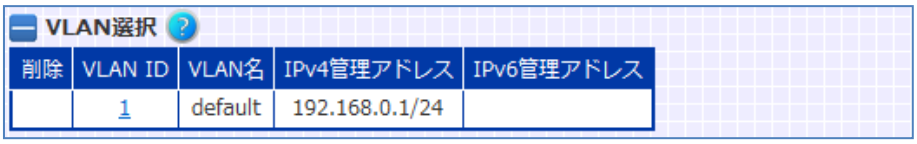
3.30.1.1 はじめに

「かんたん設定」で設定作業を行う際は、VLAN 1 の IP アドレスが設定されている状態であることが前提となっています。
VLAN 1 の IP アドレスの設定手順を以下に説明します。

A) VLAN ID の選択

場所: 設定 > ネットワーク > VLAN 選択

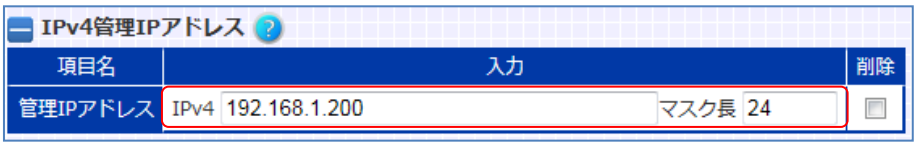
VLAN 選択のテーブルから、VLAN ID 1 のリンクをクリックし、VLAN 設定画面に遷移します。



B) 管理 IP アドレスの入力

場所: 設定 > ネットワーク > VLAN 選択 > VLAN 設定

「管理 IP アドレス」の IPv4 アドレス入力欄に、本製品の VLAN 1 に設定する IP アドレスを入力し更に、「マスク長」にはサブネットマスクの長さを入力します。
画面下部の「設定内容を変更する」をクリックすると、設定が完了します。

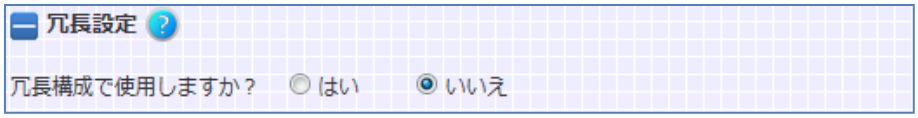


3.30.1.2 各設定項目の説明

「かんたん設定」画面の各設定項目について説明します。

3.30.1.2.1 冗長設定

冗長構成で本製品を使用するには、「はい」を選択します。
そうでない場合「いいえ」を選択します。



ポイント

かんたん設定では、冗長を組む場合、ネットワーク上に L2 ループが存在しないような構成を想定しています。
ネットワーク上にループが存在するような構成で冗長ネットワークを構成する場合、かんたん設定後に L2 ループの防止を考慮し、設定変更を加える必要があります。L2 ループの防止については、「3.25.3L2 ループの防止」を参照してください。

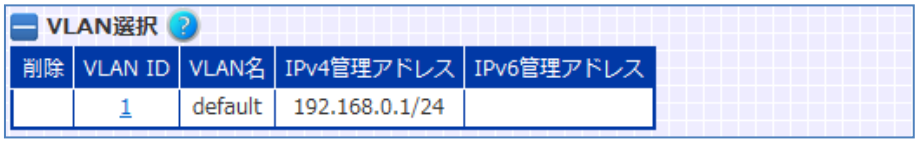
更に、冗長構成で本製品を使用する場合、かつ冗長相手の設定を同時に行う場合、冗長相手先と設定情報の同期が可能な状態になっている必要があります。

以下の例では、負荷分散用のイーサネットポートを、同期用のポートとしても使用することで、設定情報の同期が可能な状態にします。

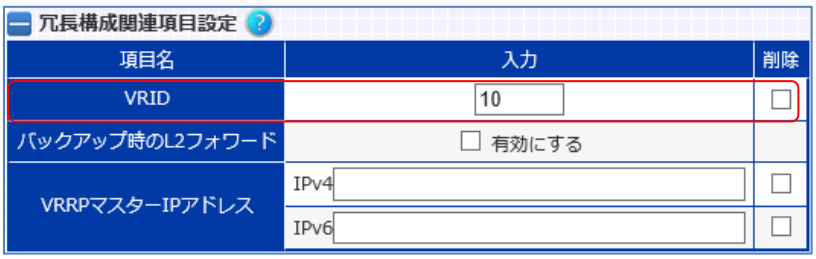
A) VRID の割り当て

場所: 設定 ＞ ネットワーク ＞VLAN 選択

VLAN 選択画面で VLAN1 のリンクをクリックし、VLAN 設定画面に遷移します。



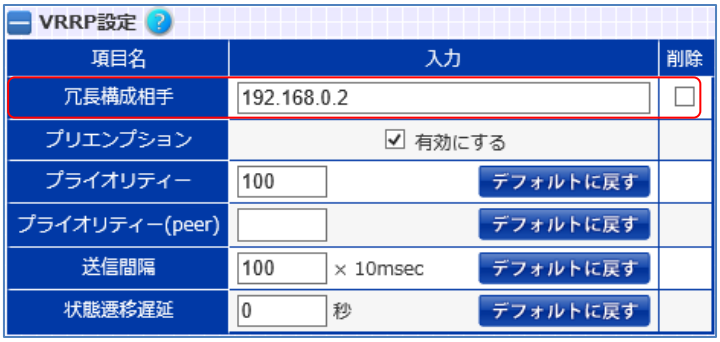
次に、本製品を冗長構成で使用するために VRID の設定をします。画面下部の「設定内容を変更する」をクリックすると、設定が完了します。



B) 冗長相手先 IP アドレスの設定

場所: 設定 > ネットワーク > 冗長構成 > VRRP

冗長構成相手先の IP アドレスを入力します。画面最下部の「設定内容を変更する」をクリックすると、設定が完了します。



C) 冗長相手への設定

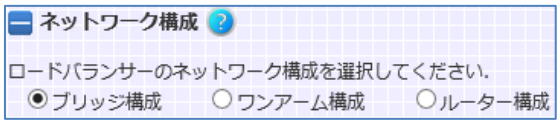
冗長構成相手にも事前に以下の 2 点を設定しておく必要があります。

- VLAN 1 の IP アドレス（本例では'192.168.0.2'となります）
- 上記 A)～B)と同様の設定

以上の設定を行い冗長相手先と LAN ケーブルで接続することで、設定情報の同期が可能になります。

3.30.1.2.2 ネットワーク構成

ロードバランサーのネットワーク構成を選択します。



■ブリッジ構成

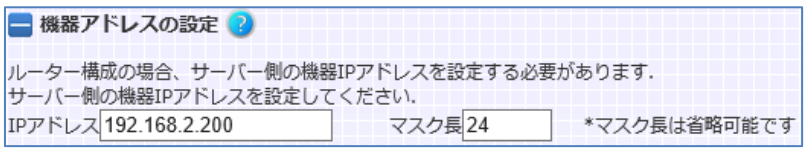
同一ネットワークセグメント間の負荷分散を行います。

■ワンアーム構成

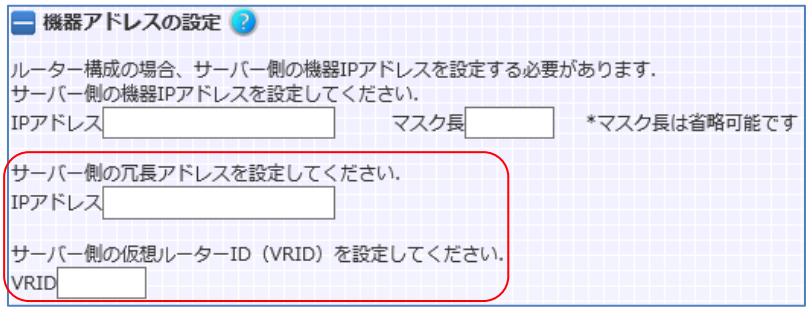
負荷分散パケットの送受信が、ロードバランサーの単一ポートで行われます。
ワンアームを構成選択すると、NAT プールポリシーが自動で設定されます。
NATプールポリシー名の文字列には、"np_<年><月><日><時><分>"が使用されます。
例) np_1409111404
また、NAT プールのプールアドレスには、「ロードバランシング設定」項目で指定する仮想サーバーIP アドレスが使用されます。

■ルーター構成

異なるネットワークセグメント間で負荷分散を行います。
ルーター構成を選択した場合、サーバー側の機器に設定する IP アドレスを入力する必要があります。ルーター構成では VLAN1 にクライアント側ネットワーク、VLAN2 にサーバー側ネットワークが設定されます。また、イーサネットポート2がサーバー側ネットワークとして割り当てられます。

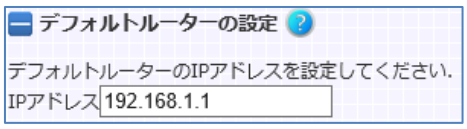


また、「冗長設定」で「はい」を選択した場合、VRRP マスター状態の際に有効になる機器 IP アドレスを VLAN2に設定します。
更に、VLAN 2 側の仮想ルーターID（VRID）を入力します。



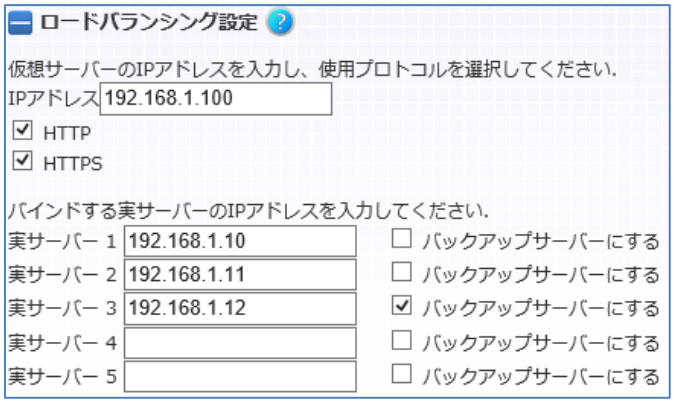
3.30.1.2.3 デフォルトルーターの設定

本製品に設定するデフォルトルーターの IP アドレスを入力します。



3.30.1.2.4 ロードバランシングの設定

仮想サーバーの定義と、仮想サーバーに関連付ける実サーバーを設定します。



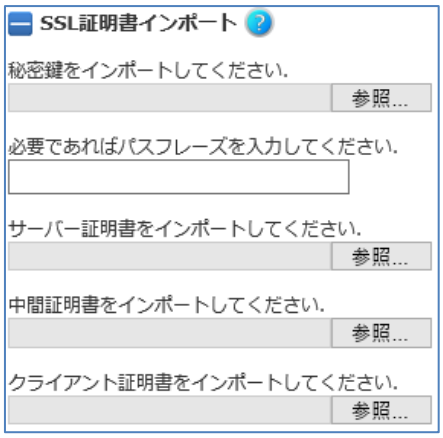
プロトコルに HTTP を選択すると 80 番ポート、HTTPS を選択すると 443 番ポートの仮想サーバーを定義することができます。HTTP、HTTPS は同時に選択可能ですが、その場合、バインドする実サーバーは HTTP 仮想サーバー、HTTPS 仮想サーバーで同一のサーバーをバインドすることになります。
実サーバーは 5 台まで登録可能で、「バックアップサーバーにする」を選択することで、任意の実サーバーをバックアップサーバーに設定できます。
また、登録した実サーバーへの TCP ヘルスチェック設定が自動的に登録されます。プロトコルに HTTP を選択すると 80 番ポート、HTTPS を選択すると 443

番ポートに対して、各実サーバーへの TCP ヘルスチェックを開始します。
ヘルスチェックポリシー名の文字列には、"pr_<年><月><日><時><分>-<No.>"が使用されます。
<No.>には 0～10 の値が割り振られます。
例) pr_1409111404-0

プロトコルで HTTPS を選択した場合、443 番ポートへのアクセスに対して SSL アクセラレーションを行うかどうかを選択します。
SSL アクセラレーション機能を有効にする場合「はい」を選択します。
そうでない場合、「いいえ」を選択します。

3.30.1.2.5 SSL 証明書インポート

SSL アクセラレーションを行う場合、使用する鍵や証明書ファイルを本製品にインポートする必要があります。



多段証明書をインポートする場合、「設定」＞「SSL」＞「SSLインポート」から、続けて設定します。
詳細は「3.22.3電子証明書と鍵のインポート」を参照してください。

3.31 機器情報

[機器情報]メニューの各画面では、システム情報や負荷分散状況を表示することができます。

■更新ボタン

表示は、画面にアクセスがあった時点での情報です。情報を更新するには、再度画面に入り直すか、「更新ボタン」をクリックします。

■データのクリア

機器情報を表示する画面には、「データのクリア」ボタンがあります。
データをクリアしたい場合、「データのクリア」ボタンをクリックします。

以下に、データのクリアが可能な画面を明記します。

画面名	クリアできるデータ
ネットワーク >イーサネット情報	イーサネットポートで送受信されたパケット数やエラー数の統計値
ネットワーク > VRRP	送受信した VRRP 広告数や、VRRP 状態遷移の統計値
ネットワーク >セッション同期	送受信した同期セッションの統計値
ネットワーク > MAC テーブル	動的 MAC エントリー *1
ネットワーク > ARP テーブル	動的 ARP エントリー *1
ネットワーク > NDP テーブル	動的 NDP エントリー
ネットワーク > L2/L3 フォワード	L2 フォワーディングと L2 フラッディングの統計値
SSL > SSL アクセラレート	SSL ボードオプションの有無 SSL セッション情報 SSL アクセラレーションの統計値
SSL > SSL 証明書自動更新	クリア不可
バランシング > 仮想サーバー	仮想サーバーの処理したコネクション数の統計情報
バランシング > 実サーバー	実サーバーの処理したコネクション数の統計値
バランシング > 負荷分散概要	セッション数、スティッキー情報数の統計値
ヘルスチェック	ヘルスチェック成功/失敗数の統計

＞ ヘルスチェック	値

*1 全件削除、または任意のテーブルエントリーの削除が可能

⚠ 注意 冗長構成時 BACKUP 機は負荷分散(バランシング、SSL アクセラレート) および SSL 証明書自動更新、クラウド WAF は停止しているため、これらのカウンターやステータスなどは MASTER 機で確認してください。

3.32 リアルタイム情報

[リアルタイム]メニューをクリックすると、リアルタイム情報画面に遷移します。
リアルタイム情報画面では機器リソースやネットワークトラフィック等の状態をリアルタイムに描画します。

3.32.1 システム情報

場所: リアルタイム情報 > システム情報

開始ボタンをクリックすると、グラフの描画が開始されます。

■CPU 使用率
現在の CPU 使用率を表示します。

■メモリー使用率
現在のメモリー使用率を表示します。

■RSA 演算処理数
本製品が1秒間に処理している SSL コネクション数を表示します。

■L4 コネクション数
現在の L4 コネクション数を表示します。

■L7 コネクション数
現在の L7 コネクション数を表示します。

■SSL セッション数
現在の SSL セッション数を表示します。

3.32.2 仮想サーバー情報

場所: リアルタイム情報 > 仮想サーバー情報

仮想サーバーIDを選択し、開始ボタンをクリックすると、グラフの描画が開始されます。

■コネクション数

該当の仮想サーバーが現在処理しているコネクション数。

■受信パケット数

該当の仮想サーバーが現在処理している受信処理パケット数。

■送信パケット数

該当の仮想サーバーが現在処理している送信処理パケット数。

■受信バイト数

該当の仮想サーバーが現在処理している受信処理バイト数。

■送信バイト数

該当の仮想サーバーが現在処理している送信処理バイト数。

3.32.3 実サーバー情報

場所: リアルタイム情報 > 実サーバー情報

実サーバーID を選択し、開始ボタンをクリックすると、グラフの描画が開始されます。

■コネクション数

該当の実サーバーが現在処理しているコネクション数。

■受信パケット数

該当の実サーバーが現在処理している受信処理パケット数。

■送信パケット数

該当の実サーバーが現在処理している送信処理パケット数。

■受信バイト数

該当の実サーバーが現在処理している受信処理バイト数。

■送信バイト数

該当の実サーバーが現在処理している送信処理バイト数。

3.33 統計情報

メインメニュー「統計情報」の選択により、システム情報、仮想サーバー情報、実サーバー情報のリソース、ネットワークトラフィック等の日付別統計情報（対象となる日付の時間毎の総和）、月別統計情報(対象となる月の日付毎の総和)を表示します。また、表示している情報のデータファイルをダウンロードすることが可能です。表示可能な情報は過去2ヶ月分です。

ポイント

統計情報は、装置の ON/OFF により初期化されます。
定期的に情報をダウンロードしてください。

3.33.1 システム情報

場所: 統計情報 > システム情報

「日付別」または「月別」と、任意の期間を選択し「描画」をクリックします。

■RSA 演算処理数

RSA 演算処理数におけるシステム全体の統計値です。

■L4 コネクション数

システム全体で処理した L4 コネクション数の統計値です。

■L7 コネクション数

システム全体で処理した L7 コネクション数の統計値です。

■SSL セッション数

システム全体で処理した SSL セッション数の統計値です。

3.33.2 仮想サーバー情報

場所: 統計情報 > 仮想サーバー情報

「日付別」または「月別」と、任意の期間を選択し、更に任意の仮想サーバーIDを選択し、「描画」をクリックします。

■コネクション数

該当の仮想サーバーが現在処理しているコネクション数。

■受信パケット数

該当の仮想サーバーが現在処理している受信処理パケット数。

■送信パケット数

該当の仮想サーバーが現在処理している送信処理パケット数。

■受信バイト数

該当の仮想サーバーが現在処理している受信処理バイト数。

■送信バイト数

該当の仮想サーバーが現在処理している送信処理バイト数。

3.33.3 実サーバー情報

場所: 統計情報 > 実サーバー情報

「日付別」または「月別」と、任意の期間を選択し、更に任意の実サーバーID を選択し、「描画」をクリックします。

■コネクション数

該当の実サーバーが現在処理しているコネクション数。

■受信パケット数

該当の実サーバーが現在処理している受信処理パケット数。

■送信パケット数

該当の実サーバーが現在処理している送信処理パケット数。

■受信バイト数

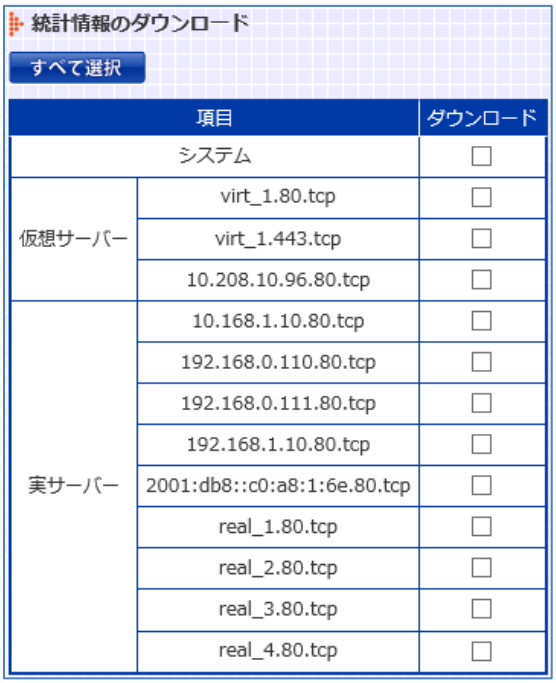
該当の実サーバーが現在処理している受信処理バイト数。

■送信バイト数

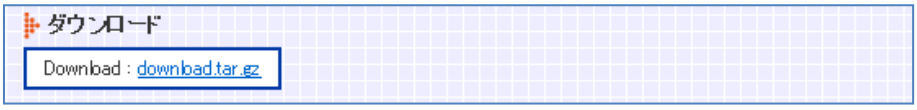
該当の実サーバーが現在処理している送信処理バイト数。

3.33.4 ダウンロード

ダウンロードする統計情報を選択します。「すべて選択」をクリックすると、全ての項目が選択されます。再度「すべて選択」をクリックすると、選択が解除されます。選択し、画面下部の「OK」をクリックするとダウンロード画面に遷移します。



ダウンロード画面に遷移後、表示されたダウンロードファイル名を左クリックで保存します。



3.34 ログ参照

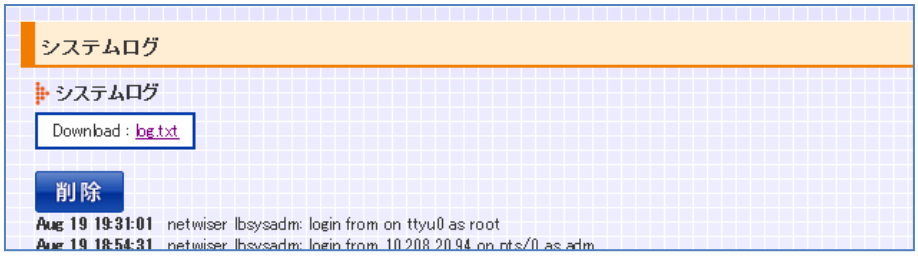
機器内部に保持するログの参照やダウンロードが可能です。

3.34.1 システムログ

場所: ログ参照 > システムログ

本製品のシステムログが表示されます。また、シスログファイルへのリンクが表示されます。

必要な場合は右クリックでダウンロードしてください。

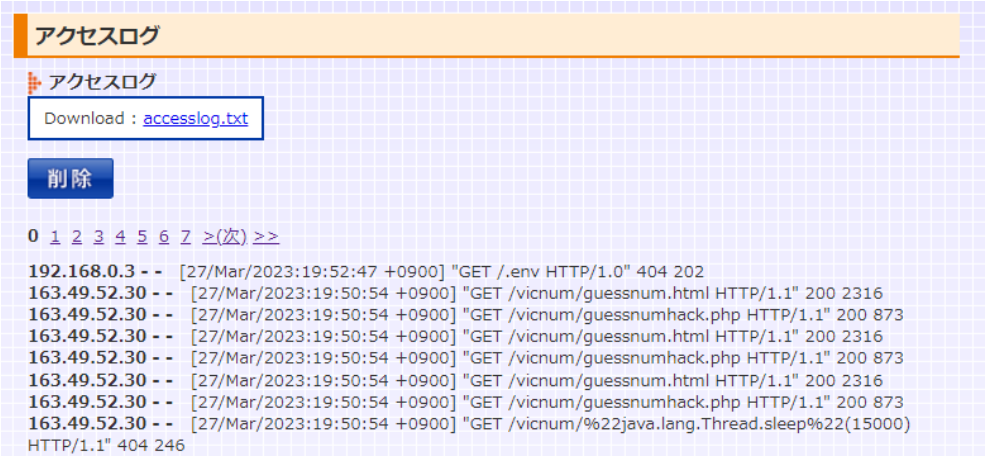


3.34.2 アクセスログ

場所: ログ参照 > アクセスログ

クラウド WAF が有効の場合、HTTP アクセスログが表示されます。また、アクセスログファイルへのリンクが表示されます。

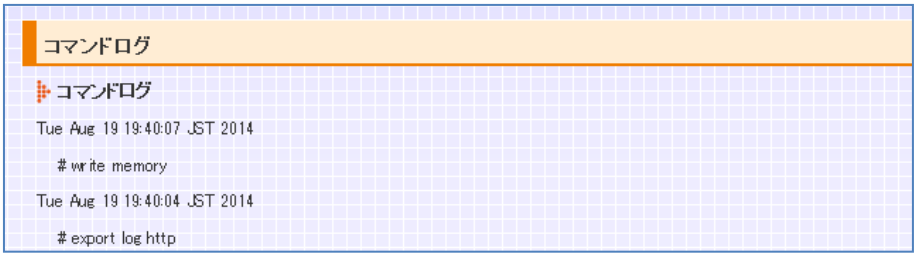
必要な場合は右クリックでダウンロードしてください。



3.34.3 コマンドログ

場所: ログ参照 > コマンドログ

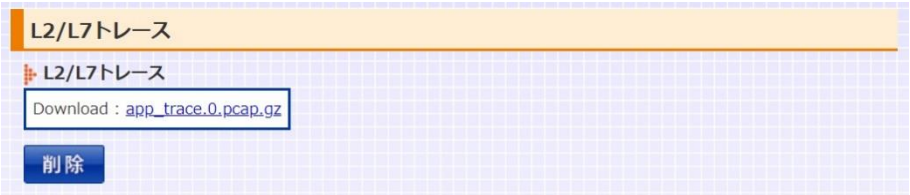
WEB 管理画面からの操作により発行したコマンドの履歴を表示します。



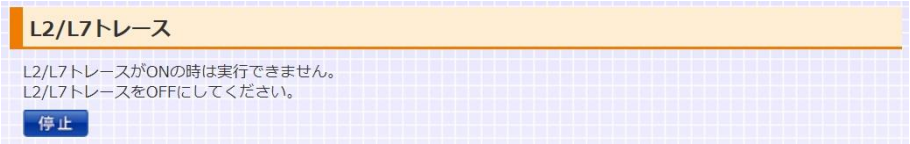
3.34.4 L2/L7 トレース情報

場所: ログ参照 ＞L2/L7 トレース

本装置は、解析用の機能として L2 パケット/L7 負荷分散パケットに関するパケットトレースを実施し、キャプチャデータを生成する機能があります。
本画面では、機器内部に保存されているキャプチャファイルへのリンクを表示します。
「削除」ボタンで削除することができます。



パケットトレースを実行している最中に本画面を表示した場合、「停止」ボタンが表示されます。「停止」ボタンでトレース機能を停止させるとダウンロードリンクが表示されます。



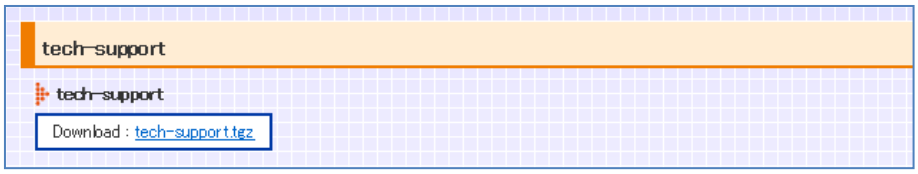
WEB 管理画面からパケットトレースを開始することはできません。
詳細は「5.3.3 L7 トレース機能」または「5.3.4 L2 トレース機能」を参照してください。

3.34.5 テクニカルサポートファイル

場所: ログ参照 > tech-support > tech-support

テクニカルサポートファイルへのリンクを表示します。

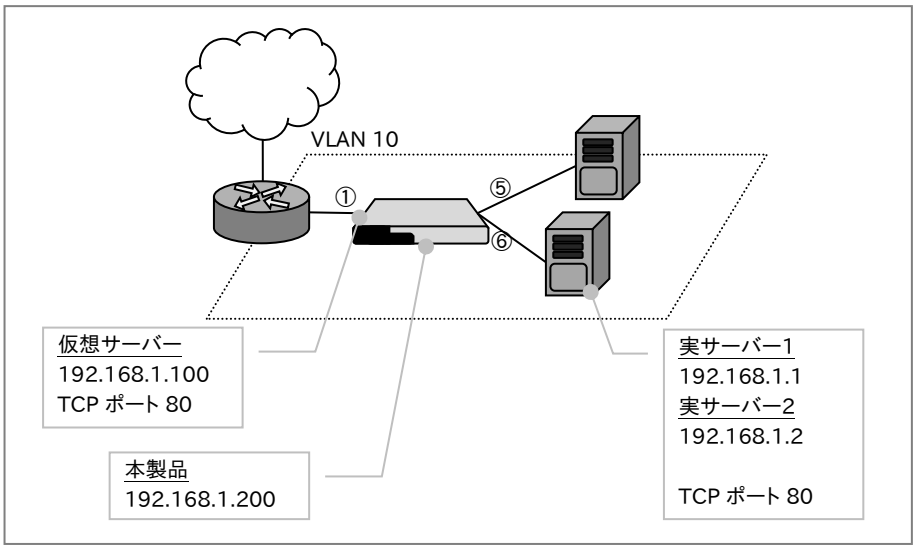
必要な場合は右クリックでダウンロードしてください。



第4章　設定例

4.1 仮想サーバーと実サーバーが同じ VLAN の場合

仮想サーバーと実サーバーがすべて同じ VLAN 内(VLAN 10)に存在する場合の設定例を下記に示します。



A)　各 IP アドレスに名前付けします。（必須ではありません）

```
netwiser> config
netwiser(config)# name v-www 192.168.1.100
netwiser(config)# name www1 192.168.1.1
netwiser(config)# name www2 192.168.1.2
```

B)　VLAN 10 に管理用アドレスと仮想アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.200/24
netwiser(config-vlan)# ip virtual-address v-www
netwiser(config-vlan)# exit
```

C)　使用するポートを VLAN 10 のメンバに設定します。

```
netwiser(config)# interface ethernet 1,5,6
netwiser(config-if)# vlan 10
netwiser(config-if)# exit
```

D) 実サーバーを登録します。

```
netwiser(config)# real www1.80.tcp
netwiser(config)# real www2.80.tcp
```

E) 実サーバーへのヘルスチェックを設定します。

ここでは TCP コネクション確立によるヘルスチェックの設定を例示しています。

設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。

起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-www1 www1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-www2 www2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

F) 仮想サーバーを設定します。

ここでは仮想サーバーへの名前付け、セッション維持設定、実サーバーのバインド、仮想サーバーの有効化を設定します。

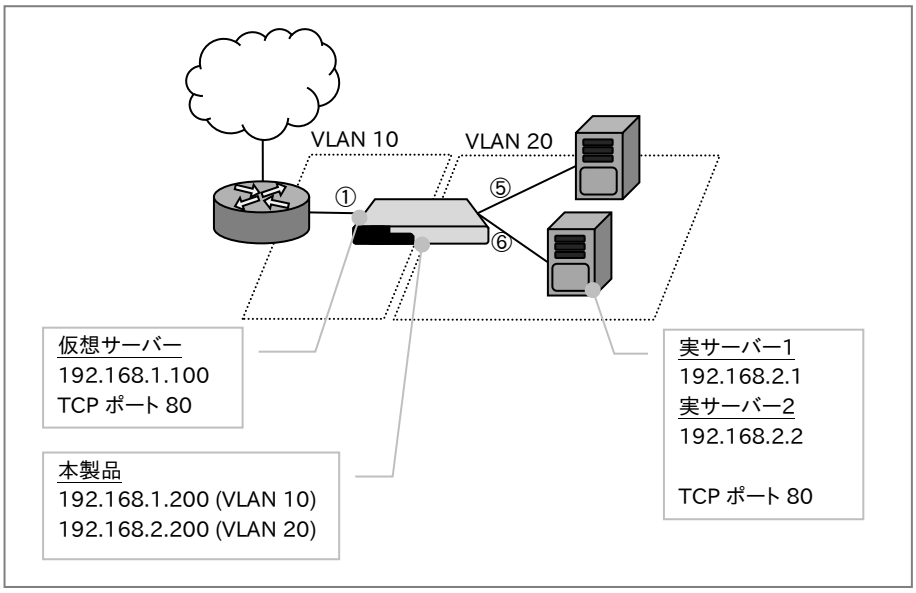
```
netwiser(config)# virtual v-www.80.tcp
netwiser(config-virtual)# name v-http
netwiser(config-virtual)# sticky generic
netwiser(config-virtual)# bind www1.80
netwiser(config-virtual)# bind www2.80
netwiser(config-virtual)# enable
netwiser(config-virtual)# exit
```

G) 設定を保存します。

```
netwiser(config)# write memory
```

4.2 仮想サーバーと実サーバーが異なる VLAN の場合

仮想サーバーと実サーバーが異なる VLAN(VLAN 10、VLAN 20)に存在する場合の設定例を下記に示します。



A) 各 IP アドレスに名前付けします。（必須ではありません）

```
netwiser> config
netwiser(config)# name v-www 192.168.1.100
netwiser(config)# name www1 192.168.2.1
netwiser(config)# name www2 192.168.2.2
```

B) VLAN に管理用アドレスと仮想アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.200/24
netwiser(config-vlan)# ip virtual-address v-www
netwiser(config-vlan)# exit
netwiser(config)# interface vlan 20
netwiser(config-vlan)# ip address 192.168.2.200/24
netwiser(config-vlan)# exit
```

C) 使用するポートを VLAN のメンバに設定します。

```
netwiser(config)# interface ethernet 1
netwiser(config-if)# vlan 10
netwiser(config-if)# exit
netwiser(config)# interface ethernet 5,6
```

```
netwiser(config-if)# vlan 20
netwiser(config-if)# exit
```

D)　実サーバーを登録します。

```
netwiser(config)# real www1.80.tcp
netwiser(config)# real www2.80.tcp
```

E)　実サーバーへのヘルスチェックを設定します。

ここでは TCP コネクション確立によるヘルスチェックの設定を例示しています。

設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。

起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-www1 www1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-www2 www2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

F)　仮想サーバーを設定します。

ここでは仮想サーバーへの名前付け、セッション維持設定、実サーバーのバインド、仮想サーバーの有効化を設定します。

```
netwiser(config)# virtual v-www.80.tcp
netwiser(config-virtual)# name v-http
netwiser(config-virtual)# sticky generic
netwiser(config-virtual)# bind www1.80
netwiser(config-virtual)# bind www2.80
netwiser(config-virtual)# enable
netwiser(config-virtual)# exit
```

G)　設定を保存します。

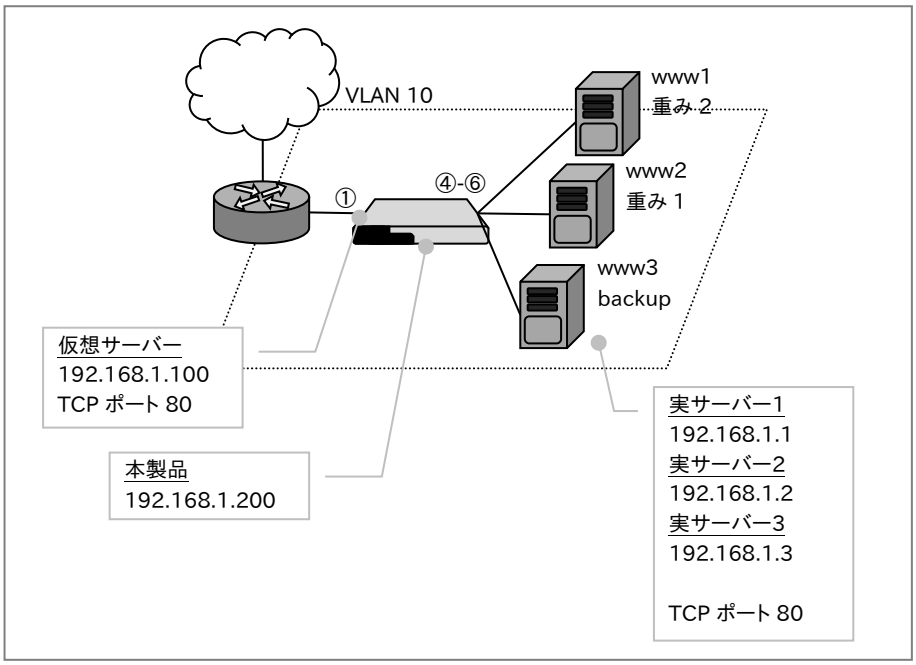
```
netwiser(config)# write memory
```

ポイント

仮想サーバーと実サーバーの VLAN が同じでも、異なっていても設定上の違いはほとんどありませんが、VLAN が異なっている場合では実サーバーのデフォルトルートを本製品の管理 IP アドレスに設定する必要があります。

4.3 重み付け負荷分散、backup サーバー設定

仮想サーバーと実サーバーが同じVLAN 内(VLAN 10)に存在する場合の設定例を下記に示します。VLAN が異なる場合は[4.2仮想サーバーと実サーバーが異なる VLAN の場合]を参考に読み替えてください。



A) 各 IP アドレスに名前付けします。（必須ではありません）

```
netwiser> config
netwiser(config)# name v-www 192.168.1.100
netwiser(config)# name www1 192.168.1.1
netwiser(config)# name www2 192.168.1.2
netwiser(config)# name www3 192.168.1.3
```

B) VLAN 10 に管理用アドレスと仮想アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.200/24
netwiser(config-vlan)# ip virtual-address v-www
netwiser(config-vlan)# exit
```

C) 使用するポートを VLAN 10 のメンバに設定します。

```
netwiser(config)# interface ethernet 1,4-6
netwiser(config-if)# vlan 10
netwiser(config-if)# exit
```

D) 実サーバーを登録します。

```
netwiser(config)# real www1.80.tcp
netwiser(config)# real www2.80.tcp
netwiser(config)# real www3.80.tcp
```

E) 実サーバーへのヘルスチェックを設定します。

ここでは TCP コネクション確立によるヘルスチェックの設定を例示しています。

設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。

起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-www1 www1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-www2 www2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-www3 www3.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

F) 仮想サーバーを設定します。

ここでは仮想サーバーへの名前付け、セッション維持設定、実サーバーのバインド、仮想サーバーの有効化を設定します。

```
netwiser(config)# virtual v-www.80.tcp
netwiser(config-virtual)# name v-http
netwiser(config-virtual)# sticky generic
netwiser(config-virtual)# bind www1.80 weight 2
netwiser(config-virtual)# bind www2.80
netwiser(config-virtual)# bind www3.80 backup
netwiser(config-virtual)# enable
netwiser(config-virtual)# exit
```

ポイント

bind 設定で *weight* を指定しない場合はデフォルトの *1* が設定されます。

上記の設定では www1,2 がヘルスチェックにより ALIVE と判断されている間は 2:1 の割合で負荷分散し、実サーバーがすべて DOWN になると www3 が動作します。

www1,2 のいずれかが DOWN した際に www3 を稼働させることも可能です。

この場合は仮想サーバー設定モードで *backup-policy* を *multi* に設定します。

```
netwiser(config)# virtual v-www.80.tcp
netwiser(config-virtual)# backup-policy multi
netwiser(config-virtual)# exit
```

デフォルトの動作では、実サーバーが DOWN から ALIVE になると自動的に負荷分散に加わり始めます。復旧を手動で行いたい場合はヘルスチェックに *manual-failback* を設定します。

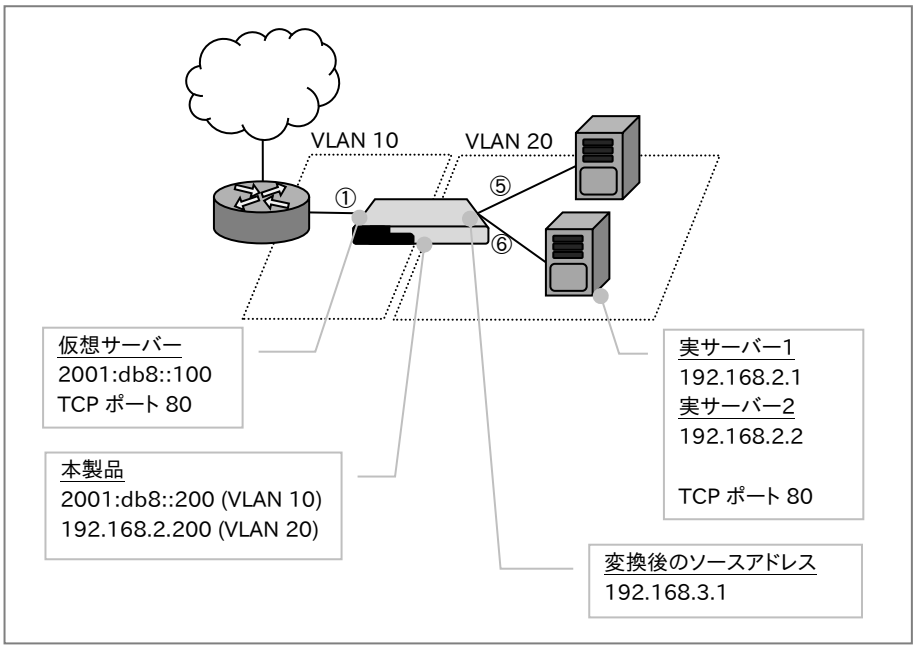
```
netwiser(config)# probe hc-www1
netwiser(config-virtual)# manual-failback
netwiser(config-virtual)# exit
netwiser(config)# probe hc-www2
netwiser(config-virtual)# manual-failback
netwiser(config-virtual)# exit
```

G)　設定を保存します。

```
netwiser(config)# write memory
```

4.4 IPv6 / IPv4 変換

仮想サーバーと実サーバーが異なる VLAN(VLAN 10、VLAN 20)に存在する場合の設定例を下記に示します。IPv6←→IPv4 変換においても同一 VLAN 内での動作が可能です。



A) 各 IP アドレスに名前付けします。（必須ではありません）

```
netwiser> config
netwiser(config)# name v-www 2001:db8::100
netwiser(config)# name www1 192.168.2.1
netwiser(config)# name www2 192.168.2.2
netwiser(config)# name xlat1 192.168.3.1
```

B) VLAN に管理用アドレスと仮想アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 2001:db8::200/64
netwiser(config-vlan)# ip virtual-address v-www
netwiser(config-vlan)# exit
netwiser(config)# interface vlan 20
netwiser(config-vlan)# ip address 192.168.2.200/24
netwiser(config-vlan)# exit
```

C) 使用するポートを VLAN のメンバに設定します。

```
netwiser(config)# interface ethernet 1
```

```
netwiser(config-if)# vlan 10
netwiser(config-if)# exit
netwiser(config)# interface ethernet 5,6
netwiser(config-if)# vlan 20
netwiser(config-if)# exit
```

D) 実サーバーを登録します。

```
netwiser(config)# real www1.80.tcp
netwiser(config)# real www2.80.tcp
```

E) 実サーバーのヘルスチェックを設定します。

ここでは TCP コネクション確立によるヘルスチェックの設定を例示しています。

設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。

起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-www1 www1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-www2 www2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

F) NAT プールを定義し、プールにアドレスを設定します。

```
netwiser(config)# nat-pool xlat_pool
netwiser(config-natpool)# ip address xlat1
netwiser(config-natpool)# exit
```

ポイント

NAT プールアドレスは IPv6→IPv4 変換後のソース IP アドレスとして使用されます。NAT プールには複数の IP アドレスを設定することができます。同時接続数が多い場合は複数の IP アドレスを設定してください。

G) 仮想サーバーを設定します。

ここでは仮想サーバーの名前付け、セッション維持設定、実サーバーのバインド、仮想サーバーの有効化を設定します。

```
netwiser(config)# virtual v-www.80.tcp
netwiser(config-virtual)# name v-http
netwiser(config-virtual)# source-nat xlat_pool
netwiser(config-virtual)# sticky cookie SESSIONID
netwiser(config-virtual)# bind www1.80
netwiser(config-virtual)# bind www2.80
netwiser(config-virtual)# enable
netwiser(config-virtual)# exit
```

ポイント

IP バージョン変換は *nat-pool*、*source-nat* 設定を追加するのみで、基本的な負荷分散の設定とほとんど同じです。同一 VLAN 内に IPv4 仮想サーバーと IPv6 仮想サーバーを共存させることもできますので、簡単にデュアルスタックのサイトを構築することができます。

ポイント

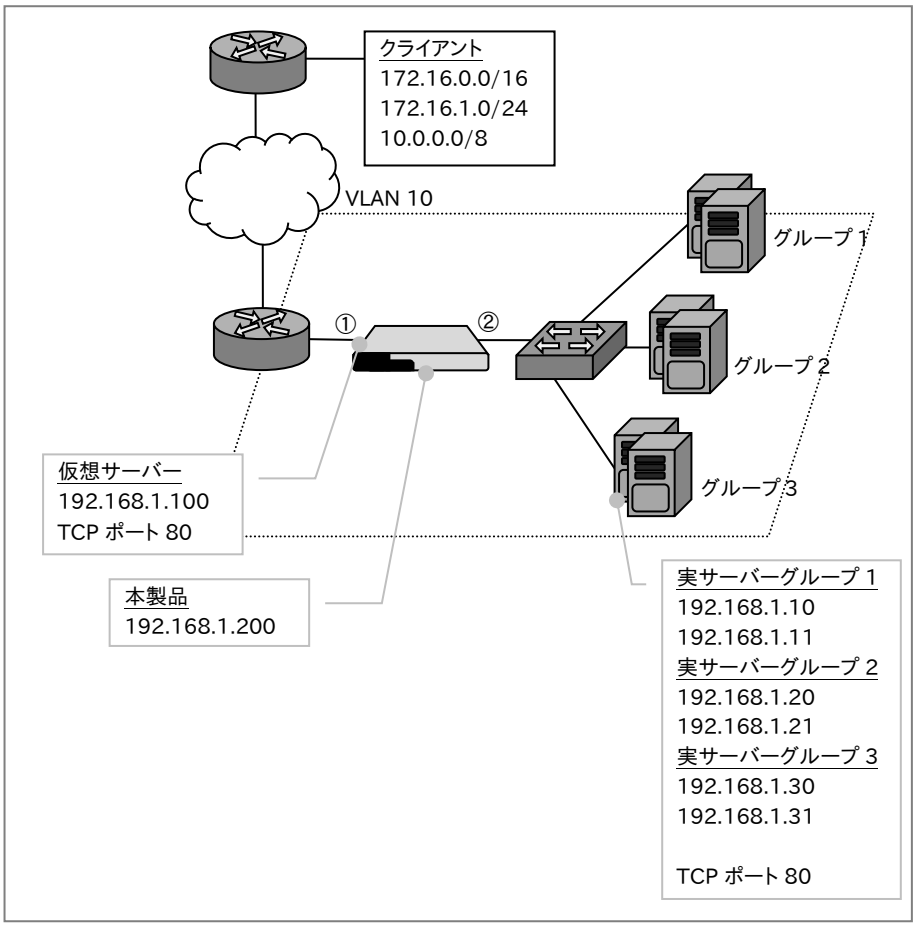
本装置で NAT した全ての履歴は *nat-log* コマンドで外部ログサーバーに送信するように設定することができます。
nat-log コマンドの詳細は「2.19.21NAT ログ情報の送信」を参照してください。

H)　設定を保存します。

```
netwiser(config)# write memory
```

4.5 IP アドレス負荷分散

仮想サーバーと実サーバーが同じVLAN 内(VLAN 10)に存在する場合の設定例を下記に示します。VLAN が異なる場合は[4.2仮想サーバーと実サーバーが異なる VLAN の場合]を参考に読み替えてください。



送信元アドレス	仮想 IP アドレス	分散先アドレス
172.16.0.0/16	192.168.1.100	192.168.1.10 192.168.1.11
172.16.1.0/24 10.0.0.0/8	192.168.1.100	192.168.1.20 192.168.1.21
その他	192.168.1.100	192.168.1.30 192.168.1.31

本設定例ではクライアントの IP アドレスによって負荷分散先を変えるものです。

172.16.0.0/16 のクライアントからのリクエストはサーバーグループ 1 に、172.16.1.0/24 と 10.0.0.0/8 からのリクエストをサーバーグループ 2 に、その他のクライアントからのアクセスをサーバーグループ 3 に負荷分散します。

A) 各 IP アドレスに名前付けします。（必須ではありません）

```
netwiser> config
netwiser(config)# name v-www 192.168.1.100
netwiser(config)# name siteA-1 192.168.1.10
netwiser(config)# name siteA-2 192.168.1.11
netwiser(config)# name siteB-1 192.168.1.20
netwiser(config)# name siteB-2 192.168.1.21
netwiser(config)# name siteC-1 192.168.1.30
netwiser(config)# name siteC-2 192.168.1.31
```

B) VLAN 10 に管理用アドレスと仮想アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.200/24
netwiser(config-vlan)# ip virtual-address v-www
netwiser(config-vlan)# exit
```

C) 使用するポートを VLAN 10 のメンバに設定します。

```
netwiser(config)# interface ethernet 1,2
netwiser(config-if)# vlan 10
netwiser(config-if)# exit
```

D) 実サーバーを登録します。

```
netwiser(config)# real siteA-1.80.tcp
netwiser(config)# real siteA-2.80.tcp
netwiser(config)# real siteB-1.80.tcp
netwiser(config)# real siteB-2.80.tcp
netwiser(config)# real siteC-1.80.tcp
netwiser(config)# real siteC-2.80.tcp
```

E) 実サーバーへのヘルスチェックを設定します。

ここでは TCP コネクション確立によるヘルスチェックの設定を例示しています。

設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。

起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-siteA-1 siteA-1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-siteA-2 siteA-2.80.tcp
netwiser(config-probe)# enable
```

```
netwiser(config-probe)# exit
netwiser(config)# probe hc-siteB-1 siteB-1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-siteB-2 siteB-2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-siteC-1 siteC-1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-siteC-2 siteC-2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

F)　仮想サーバーを設定します。

ここでは仮想サーバーへの名前付け、IP アドレスマッチングルールの定義、実サーバーのバインド、仮想サーバーの有効化を設定します。

```
netwiser(config)# virtual v-www.80.tcp
netwiser(config-virtual)# name v-http
netwiser(config-virtual)# match 172.16.0.0/16 group 1
netwiser(config-virtual)# match 172.16.1.0/24 group 2
netwiser(config-virtual)# match 10.0.0.0/8 group 2
netwiser(config-virtual)# match 0.0.0.0/0 group 3
netwiser(config-virtual)#
netwiser(config-virtual)# bind siteA-1.80 group 1
netwiser(config-virtual)# bind siteA-2.80 group 1
netwiser(config-virtual)# bind siteB-1.80 group 2
netwiser(config-virtual)# bind siteB-2.80 group 2
netwiser(config-virtual)# bind siteC-1.80 group 3
netwiser(config-virtual)# bind siteC-2.80 group 3
netwiser(config-virtual)#
netwiser(config-virtual)# enable
netwiser(config-virtual)# exit
```

ポイント

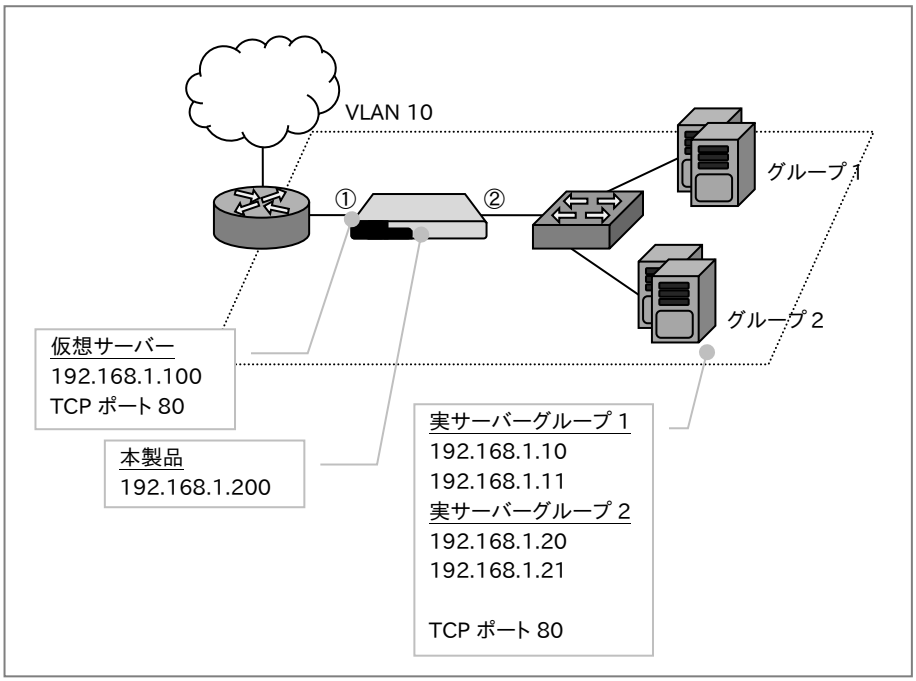
本設定では 172.16.0.0/16 マッチングルールは 172.16.1.0/24 マッチングルールを含んでいますが、IP アドレス負荷分散ではビットマスクが長い順に評価されるため 172.16.1.0/24 からのアクセスは常にサーバーグループ２に負荷分散されます。

G)　設定を保存します。

```
netwiser(config)# write memory
```

4.6 URL スイッチング

仮想サーバーと実サーバーが同じVLAN 内(VLAN 10)に存在する場合の設定例を下記に示します。VLAN が異なる場合は[4.2仮想サーバーと実サーバーが異なる VLAN の場合]を参考に読み替えてください。



本設定例では、"?service_id=group1"または"?service_id=grp1"を URL に含むリクエストをサーバーグループ 1 に、その他のリクエストをサーバーグループ 2 に負荷分散します。

A)　各 IP アドレスに名前付けします。（必須ではありません）

```
netwiser> config
netwiser(config)# name v-www 192.168.1.100
netwiser(config)# name siteA-1 192.168.1.10
netwiser(config)# name siteA-2 192.168.1.11
netwiser(config)# name siteB-1 192.168.1.20
netwiser(config)# name siteB-2 192.168.1.21
```

B)　VLAN 10 に管理用アドレスと仮想アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.200/24
netwiser(config-vlan)# ip virtual-address v-www
```

```
netwiser(config-vlan)# exit
```

C) 使用するポートを VLAN 10 のメンバに設定します。

```
netwiser(config)# interface ethernet 1,2
netwiser(config-if)# vlan 10
netwiser(config-if)# exit
```

D) 実サーバーを登録します。

```
netwiser(config)# real siteA-1.80.tcp
netwiser(config)# real siteA-2.80.tcp
netwiser(config)# real siteB-1.80.tcp
netwiser(config)# real siteB-2.80.tcp
```

E) 実サーバーへのヘルスチェックを設定します。

ここでは TCP コネクション確立によるヘルスチェックの設定を例示しています。

設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。

起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-siteA-1 siteA-1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-siteA-2 siteA-2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-siteB-1 siteB-1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-siteB-2 siteB-2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

F) マッチングルールを定義します。

仮想サーバーを設定する前に *rule* コマンドで L7 マッチングルールをあらかじめ定義しておきます。

```
netwiser(config)# rule mr-1 path "*?service_id=group1"
netwiser(config)# rule mr-2 path "*?service_id=grp1"
```

G) 仮想サーバーを設定します。

ここでは仮想サーバーへの名前付け、L7 マッチングルールの定義、実サーバーのバインド、仮想サーバーの有効化を設定します。

```
netwiser(config)# virtual v-www.80.tcp
```

```
netwiser(config-virtual)# name v-http
netwiser(config-virtual)# match mr-1 group 1
netwiser(config-virtual)# match mr-2 group 1
netwiser(config-virtual)# match default group 2
netwiser(config-virtual)#
netwiser(config-virtual)# bind siteA-1.80 group 1
netwiser(config-virtual)# bind siteA-2.80 group 1
netwiser(config-virtual)# bind siteB-1.80 group 2
netwiser(config-virtual)# bind siteB-2.80 group 2
netwiser(config-virtual)#
netwiser(config-virtual)# enable
netwiser(config-virtual)# exit
```

ポイント

本設定では"?service_id=group1"または"?service_id=grp1"という文字列が HTTP のリクエストパスに含まれていなければ、常にサーバーグループ 2 に負荷分散されます。

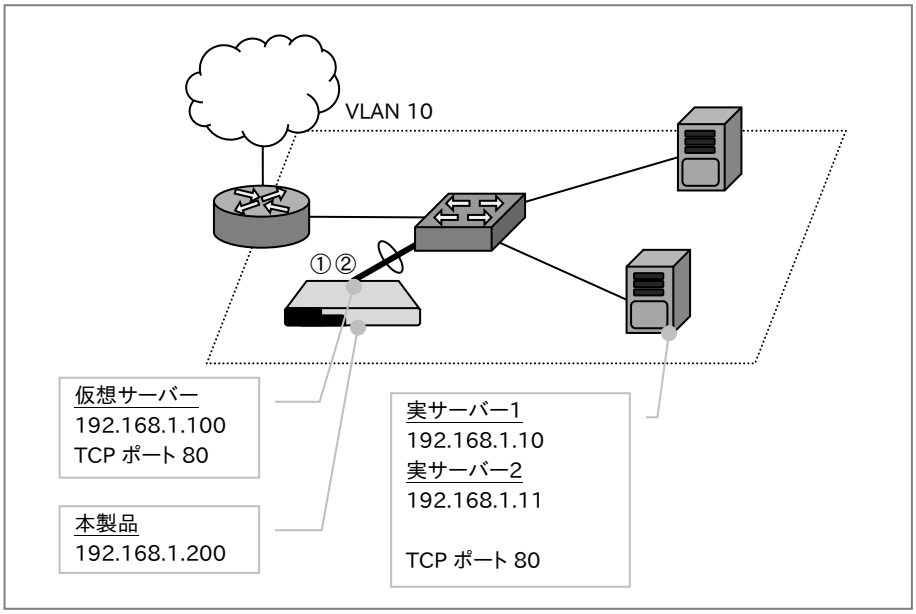
H)　設定を保存します。

```
netwiser(config)# write memory
```

4.7 ワンアーム構成

4.7.1 構成例 1(ソース NAT)

仮想サーバーと実サーバーが同じVLAN 内(VLAN 10)に存在する場合の設定例を下記に示します。



本設定例では、以下の説明をします。

① 一本の論理チャネルでスイッチと接続する、ワンアーム構成です。

② ソース NAT 設定を使用してクライアントの送信元アドレスの変換を行います。

A) 各 IP アドレスに名前付けします。（必須ではありません）

```
netwiser> config
netwiser(config)# name v-www 192.168.1.100
netwiser(config)# name www1 192.168.1.10
netwiser(config)# name www2 192.168.1.11
```

B) VLAN 10 に管理用アドレスと仮想アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.200/24
netwiser(config-vlan)# ip virtual-address v-www
netwiser(config-vlan)# exit
```

C) 使用するポート 1,2 で論理チャネルを形成し、論理チャネルを VLAN10 の

メンバに設定します。

```
netwiser(config)# interface ethernet 1,2
netwiser(config-if)# channel 1
netwiser(config-if)# exit
netwiser(config)# interface channel 1
netwiser(config-channel)# vlan 10
netwiser(config-channel)# exit
```

D) 実サーバーを登録します。

```
netwiser(config)# real www1.80.tcp
netwiser(config)# real www2.80.tcp
```

E) 実サーバーへのヘルスチェックを設定します。

ここでは TCP コネクション確立によるヘルスチェックの設定を例示しています。

設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。

起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-www1 www1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-www2 www2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

F) NAT プールを定義し、プールにアドレスを設定します。

```
netwiser(config)# nat-pool snat_pool
netwiser(config-natpool)# ip address v-www
netwiser(config-natpool)# exit
```

ポイント

ここではプールアドレスに仮想 IP アドレスを設定しています。本製品から実サーバーへのパケットのソース IP アドレスは、仮想 IP アドレスに変換されます。実サーバーでアクセスログを取得する場合、すべてのアクセスが仮想アドレスからのアクセスに見えます。実サーバーに真のクライアント IP アドレスを知らせるためには仮想サーバー設定モードの *header insert x-forwarded-for* コマンドをご使用ください。

header insert x-forwarded-for コマンドの詳細は「2.19.14発信元 IP アドレス、プロトコル情報のヘッダーおよび Cokkie 属性挿入」を参照してください。

G) 仮想サーバーを設定します。

ここでは仮想サーバーへの名前付け、ソース NAT、セッション維持設定、実サー

バーのバインド、仮想サーバーの有効化を設定します。

```
netwiser(config)# virtual v-www.80.tcp
netwiser(config-virtual)# name v-http
netwiser(config-virtual)# source-nat snat_pool
netwiser(config-virtual)# sticky cookie SESSIONID
netwiser(config-virtual)# bind www1.80
netwiser(config-virtual)# bind www2.80
netwiser(config-virtual)# enable
netwiser(config-virtual)# exit
```

ポイント

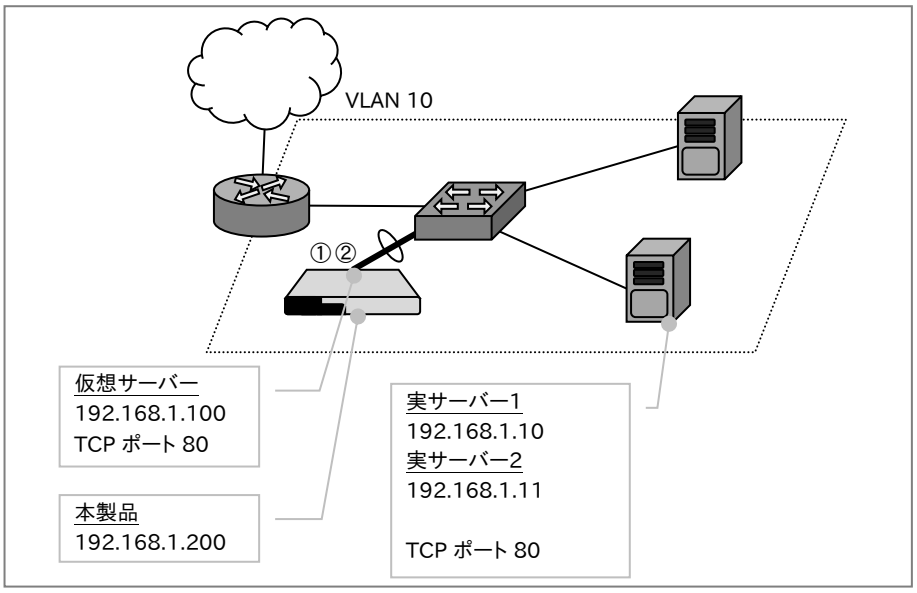
本装置で NAT した全ての履歴は *nat-log* コマンドで外部ログサーバーに送信するように設定することができます。
nat-log コマンドの詳細は「2.19.21NAT ログ情報の送信」を参照してください。

H)　設定を保存します。

```
netwiser(config)# write memory
```

4.7.2 構成例 2(ワンアームゲートウェイモード)

仮想サーバーと実サーバーが同じVLAN 内(VLAN 10)に存在する場合の設定例を下記に示します。



本設定例では、以下の説明をします。

① 一本の論理チャネルでスイッチと接続する、ワンアーム構成です。

② ワンアームゲートウェイモード設定を使用してクライアントの送信元アドレスの変換を行いません。

A) 各 IP アドレスに名前付けします。（必須ではありません）

```
netwiser> config
netwiser(config)# name v-www 192.168.1.100
netwiser(config)# name www1 192.168.1.10
netwiser(config)# name www2 192.168.1.11
```

B) VLAN 10 に管理用アドレスと仮想アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.200/24
netwiser(config-vlan)# ip virtual-address v-www
netwiser(config-vlan)# exit
```

C) 使用するポート 1,2 で論理チャネルを形成し、論理チャネルを VLAN10 のメンバに設定します。

```
netwiser(config)# interface ethernet 1,2
netwiser(config-if)# channel 1
netwiser(config-if)# exit
netwiser(config)# interface channel 1
netwiser(config-channel)# vlan 10
netwiser(config-channel)# exit
```

D)　実サーバーを登録します。

```
netwiser(config)# real www1.80.tcp
netwiser(config)# real www2.80.tcp
```

E)　実サーバーへのヘルスチェックを設定します。

ここでは TCP コネクション確立によるヘルスチェックの設定を例示しています。

設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。

起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-www1 www1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-www2 www2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

F)　仮想サーバーを設定します。

ここでは仮想サーバーへの名前付け、ワンアームゲートウェイモード、セッション維持設定、実サーバーのバインド、仮想サーバーの有効化を設定します。

```
netwiser(config)# virtual v-www.80.tcp
netwiser(config-virtual)# name v-http
netwiser(config-virtual)# onearm-gateway-mode
netwiser(config-virtual)# sticky cookie SESSIONID
netwiser(config-virtual)# bind www1.80
netwiser(config-virtual)# bind www2.80
netwiser(config-virtual)# enable
netwiser(config-virtual)# exit
```

ポイント

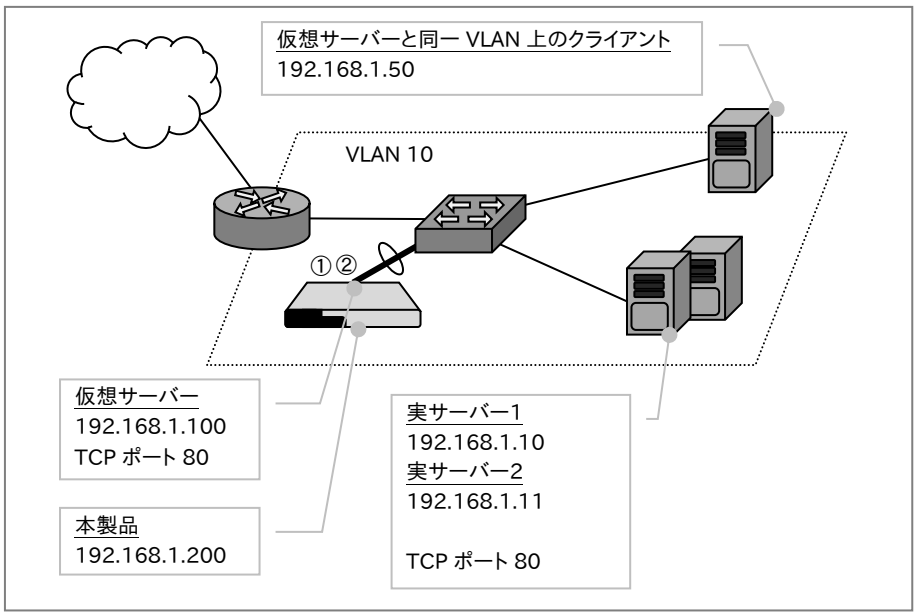
ワンアームゲートウェイモードで使用する場合、実サーバー1,2 のデフォルトゲートウェイを本製品の管理 IP アドレス、または冗長 IP アドレス(冗長構成の場合)に設定する必要があります。

G)　設定を保存します。

```
netwiser(config)# write memory
```

4.7.3 構成例 3(ソース NAT+ワンアームゲートウェイモード)

仮想サーバーと実サーバーが同じ VLAN 内(VLAN 10)に存在し、ルーター経由のクライアント、及び仮想サーバーと同一 VLAN 上のクライアントが存在する場合の設定例を下記に示します。



本設定例では、以下の説明をします。

① 一本の論理チャネルでスイッチと接続する、ワンアーム構成です。

② ワンアームゲートウェイモード設定を使用してルーターを経由したクライアントの送信元アドレスの変更は行いません。

③ ソース NAT 設定、ソース NAT フィルタリング設定を使用して仮想サーバーと同一 VLAN 上にあるクライアントの送信元アドレスのみ変換を行います。

A) 各 IP アドレスに名前付けします。（必須ではありません）

```
netwiser> config
netwiser(config)# name v-www 192.168.1.100
netwiser(config)# name www1 192.168.1.10
netwiser(config)# name www2 192.168.1.11
```

B) VLAN 10 に管理用アドレスと仮想アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.200/24
netwiser(config-vlan)# ip virtual-address v-www
netwiser(config-vlan)# exit
```

C) 使用するポート 1,2 で論理チャネルを形成し、論理チャネルを VLAN10 のメンバに設定します。

```
netwiser(config)# interface ethernet 1,2
netwiser(config-if)# channel 1
netwiser(config-if)# exit
netwiser(config)# interface channel 1
netwiser(config-channel)# vlan 10
netwiser(config-channel)# exit
```

D) 実サーバーを登録します。

```
netwiser(config)# real www1.80.tcp
netwiser(config)# real www2.80.tcp
```

E) 実サーバーへのヘルスチェックを設定します。

ここでは TCP コネクション確立によるヘルスチェックの設定を例示しています。

設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。

起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-www1 www1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-www2 www2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

F) NAT プールを定義し、プールにアドレスを設定します。

```
netwiser(config)# nat-pool snat_pool
netwiser(config-natpool)# ip address v-www
netwiser(config-natpool)# exit
```

G) 仮想サーバーを設定します。

ここでは仮想サーバーへの名前付け、ソース NAT、ソース NAT フィルタリング、ワンアームゲートウェイモード、セッション維持設定、実サーバーのバインド、仮想サーバーの有効化を設定します。

```
netwiser(config)# virtual v-www.80.tcp
netwiser(config-virtual)# name v-http
netwiser(config-virtual)# source-nat snat_pool
netwiser(config-virtual)# permit-nat-filter 192.168.1.50/32
netwiser(config-virtual)# onearm-gateway-mode
netwiser(config-virtual)# sticky cookie SESSIONID
netwiser(config-virtual)# bind www1.80
```

```
netwiser(config-virtual)# bind www2,80
netwiser(config-virtual)# enable
netwiser(config-virtual)# exit
```

ポイント

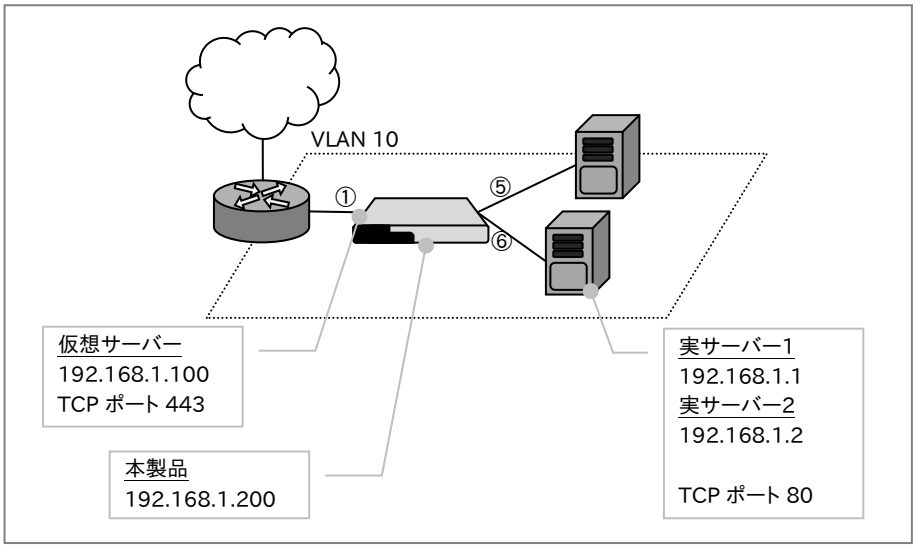
ここではプールアドレスに仮想 IP アドレスを設定しています。ソース NAT フィルタリング設定で指定されたクライアントのソース IP アドレスのみが、仮想 IP アドレスに変換されます。

H)　設定を保存します。

```
netwiser(config)# write memory
```

4.8 SSL アクセラレーション

本装置で SSL アクセラレーションを行う場合の設定例を下記に示します。
例として、仮想サーバーと実サーバーがすべて同じ VLAN 内(VLAN 10)に存在する場合で説明します。



A) 各 IP アドレスに名前付けします。（必須ではありません）

```
netwiser> config
netwiser(config)# name v-www 192.168.1.100
netwiser(config)# name www1 192.168.1.1
netwiser(config)# name www2 192.168.1.2
```

B) VLAN 10 に管理用アドレスと仮想アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.200/24
netwiser(config-vlan)# ip virtual-address v-www
netwiser(config-vlan)# exit
```

C) 使用するポートを VLAN 10 のメンバに設定します。

```
netwiser(config)# interface ethernet 1,5,6
netwiser(config-if)# vlan 10
netwiser(config-if)# exit
```

D) 実サーバーを登録します。

```
netwiser(config)# real www1.80.tcp
netwiser(config)# real www2.80.tcp
```

E)　実サーバーへのヘルスチェックを設定します。

ここでは TCP コネクション確立によるヘルスチェックの設定を例示しています。

設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。

起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-www1 www1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-www2 www2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

F)　SSL ポリシーを登録します。

```
netwiser(config)# ssl www-ssl-site-A
netwiser(config-ssl)# exit
```

G)　秘密鍵、サーバー証明書、中間証明書をインポートします。

ここでは秘密鍵、サーバー証明書、中間証明書をインポートします。任意の SSL ポリシーを指定することで、インポートする SSL 関連ファイルと SSL ポリシーとを紐づけます。

以下では、*import* コマンド実行時に転送方法を省略しているので、ファイル転送に tftp を使用します。*import* コマンド実行後に、ローカル PC から tftp を使用して任意の SSL 関連ファイルを送信します。

```
netwiser(config)# import ssl www-ssl-site-A key
Ready to TFTP receive.
Press 'q[ENTER]' to cancel: .

Transfer is complete.
Enter Import Password:
netwiser(config)#
netwiser(config)# import ssl www-ssl-site-A cert
Ready to TFTP receive.
Press 'q[ENTER]' to cancel: .

Transfer is complete.
netwiser(config)# import ssl www-ssl-site-A chain
Ready to TFTP receive.
Press 'q[ENTER]' to cancel: .

Transfer is complete.
netwiser(config)#
```

H)　仮想サーバーを設定します。

ここでは仮想サーバーへの名前付け、セッション維持設定、実サーバーのバインド、SSL ポリシーのバインド、仮想サーバーの有効化を設定します。

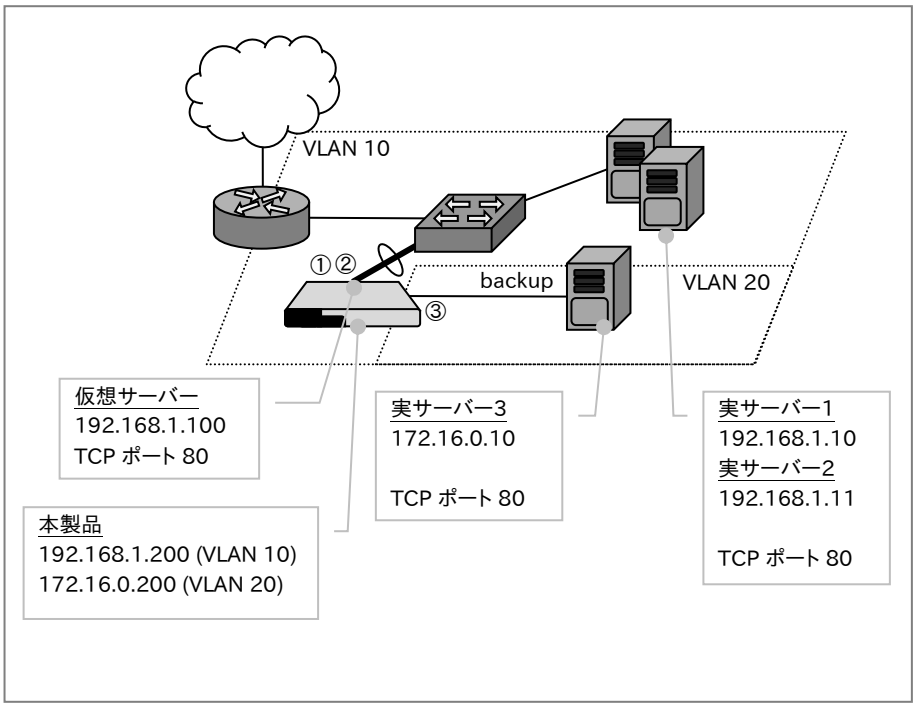
```
netwiser(config)# virtual v-www.443.tcp
netwiser(config-virtual)# name v-https
netwiser(config-virtual)# sticky generic
netwiser(config-virtual)# bind www1.80
netwiser(config-virtual)# bind www2.80
netwiser(config-virtual)# ssl www-ssl-site-A
netwiser(config-virtual)# enable
netwiser(config-virtual)# exit
```

I)　設定を保存します。

```
netwiser(config)# write memory
```

4.9 DSR

仮想サーバーと実サーバーが同じ VLAN 内(VLAN 10)と異なる VLAN(VLAN 20)に混在する場合の設定例を下記に示します。



本設定例では、一本の論理チャネルでスイッチと接続する、シングルアーム構成で DSR サーバーを配置し、VLAN 20 内に DSR サーバーのバックアップサーバーを配置しています。

A) 各 IP アドレスに名前付けします。（必須ではありません）

```
netwiser> config
netwiser(config)# name v-www 192.168.1.100
netwiser(config)# name www1 192.168.1.10
netwiser(config)# name www2 192.168.1.11
netwiser(config)# name www-backup 172.16.0.10
```

B) VLAN 10、VLAN20 に管理用アドレスと仮想アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.200/24
netwiser(config-vlan)# ip virtual-address v-www
netwiser(config-vlan)# exit
netwiser(config)# interface vlan 20
```

```
netwiser(config-vlan)# ip address 172.16.0.200/24
netwiser(config-vlan)# exit
```

C) 使用するポート 1,2 で論理チャネルを形成し、論理チャネルを VLAN10 のメンバに設定します。

```
netwiser(config)# interface ethernet 1,2
netwiser(config-if)# channel 1
netwiser(config-if)# exit
netwiser(config)# interface channel 1
netwiser(config-channel)# vlan 10
netwiser(config-channel)# exit
netwiser(config)# interface ethernet 3
netwiser(config-if)# vlan 20
netwiser(config-if)# exit
```

D) 実サーバーを登録します。

```
netwiser(config)# real www1.80.tcp
netwiser(config)# real www2.80.tcp
netwiser(config)# real www-backup.80.tcp
```

E) 実サーバーへのヘルスチェックを設定します。

ここでは TCP コネクション確立によるヘルスチェックの設定を例示しています。

設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。

起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-www1 www1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-www2 www2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-backup www-backup.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

F) 仮想サーバーを設定します。

ここでは仮想サーバーへの名前付け、セッション維持設定、実サーバーのバインド、仮想サーバーの有効化を設定します。

```
netwiser(config)# virtual v-www.80.tcp
netwiser(config-virtual)# name v-http
netwiser(config-virtual)# sticky generic
netwiser(config-virtual)# bind www1.80 dsr
netwiser(config-virtual)# bind www2.80 dsr
```

```
netwiser(config-virtual)# bind www-backup.80 backup
netwiser(config-virtual)# enable
netwiser(config-virtual)# exit
```

G) 設定を保存します。

```
netwiser(config)# write memory
```

4.9.1 DSR 実サーバーの設定例

DSR で負荷分散する場合、動作する全ての実サーバーのループバックインターフェイスに、仮想サーバーIP アドレスを設定する必要があります。
各ループバックインターフェイスに対する ARP リクエストへの応答や、ループバックインターフェイスの IP アドレスを送信元アドレスとした ARP リクエストの送信は停止させる必要があります。
以下に示す設定方法、設定手順は OS 種別や OS バージョンによって異なる場合があります。ご利用環境の設定手順を確認し、正しく設定してください。

4.9.1.1 Linux サーバー

A)　ループバックインターフェイスに仮想 IP アドレスを設定します。

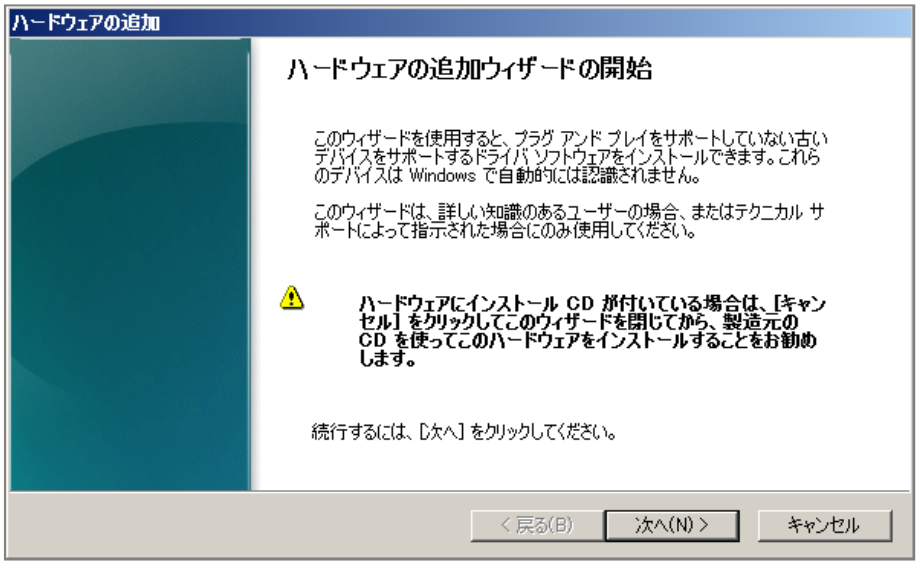
```
# ifconfig lo:1 192.168.1.100 netmask 255.255.255.255 -arp up
```

B)　ループバック上の ARP 応答や ARP 要求を停止します。

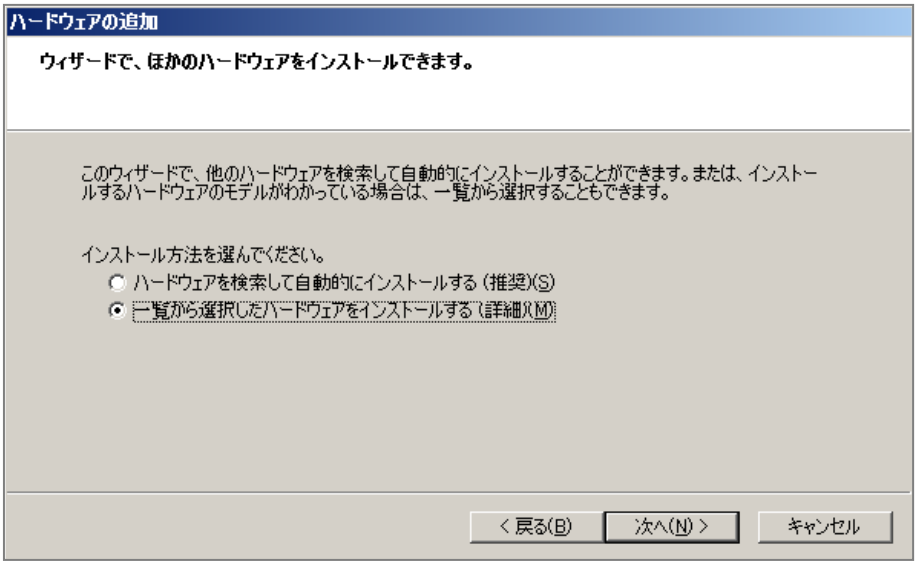
```
# sysctl net.ipv4.conf.all.arp_ignore=1
# sysctl net.ipv4.conf.all.arp_announce=2
```

4.9.1.2 Windows サーバー

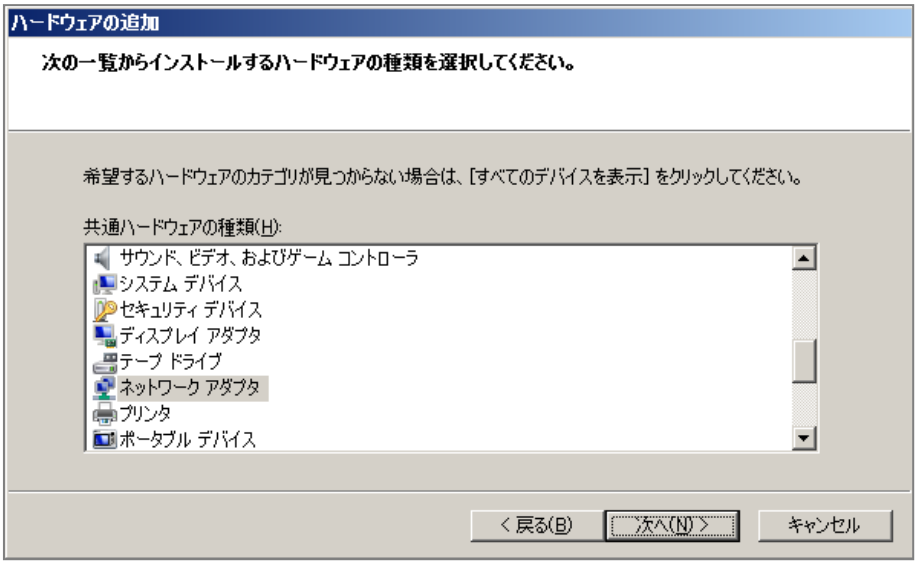
A)　ループバックインターフェイスを追加します。
「コントロールパネル」から「ハードウェアの追加」を選択し、「次へ」をクリックします。



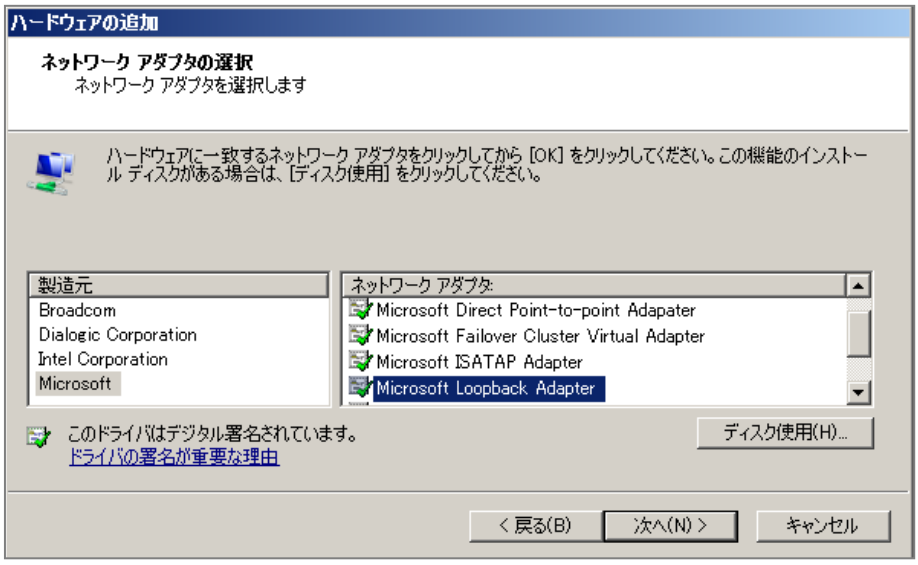
「一覧から選択したハードウェアをインストールする」を選択し、「次へ」をクリックします。



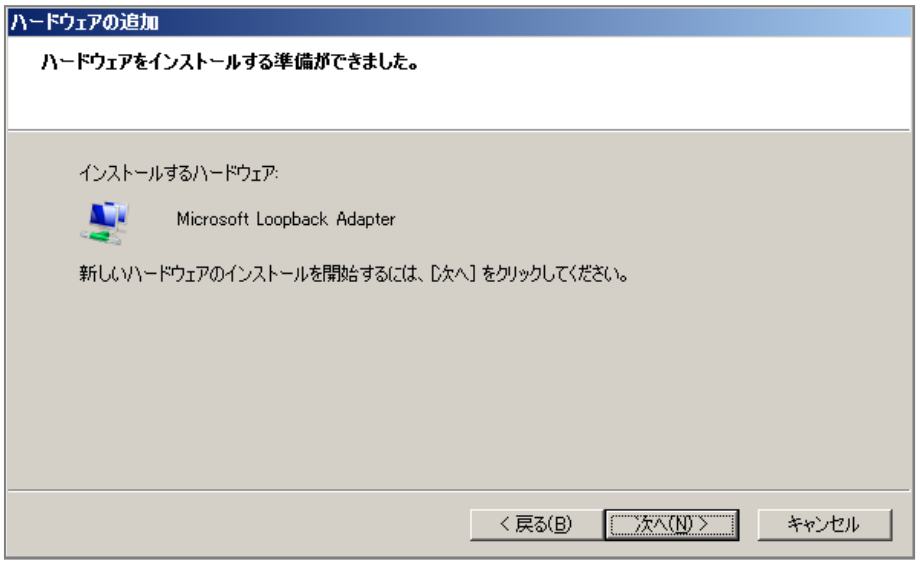
「ネットワークアダプタ」を選択し、「次へ」をクリックします。



「製造元」一覧で、「Microsoft」をクリックします。 続いて、「ネットワーク アダプタ」の一覧から「Microsoft Loopback Adapter」を選択し、「次へ」をクリックします。



インストール開始画面で「次へ」をクリックします。



最後に「完了」をクリックするとインストールが完了します。

B)　ファイアウォールの設定を変更します

利用するポートのトラフィックを遮断しないよう設定するか、ファイアウォールを無効にする必要があります。

C)　インターフェイスのオプションを変更します

コマンドプロンプトを起動し下記のコマンドを実行します。

本設定例では、既存のネットワークインターフェイスに「ローカル エリア接続」があり、新規のループバックインターフェイスとして「ローカル エリア接続 2」が作られた場合を説明します。

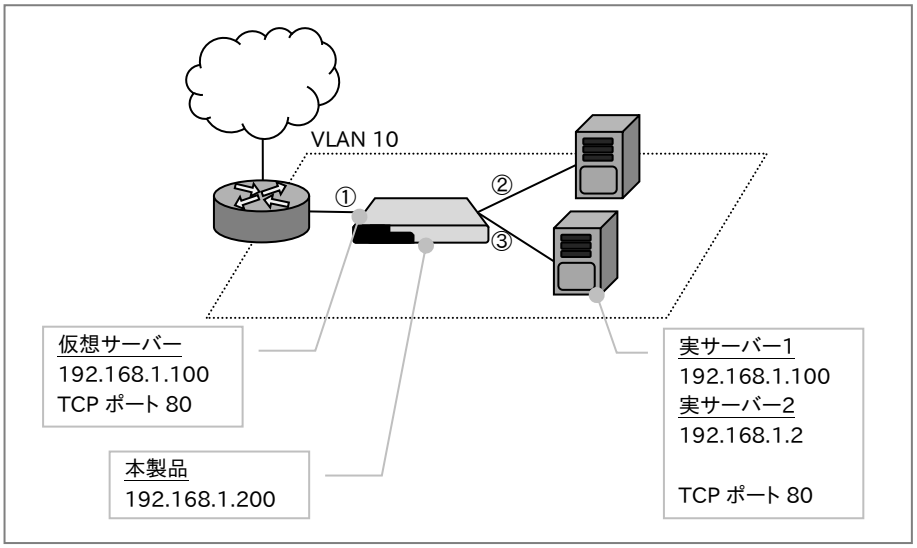
```
> netsh interface ipv4 set interface "ローカル エリア接続" weakhostreceive=enabled
> netsh interface ipv4 set interface "ローカル エリア接続 2" weakhostreceive=enabled
> netsh interface ipv4 set interface "ローカル エリア接続 2" weakhosttsend=enabled
```

D) ループバック上の ARP 応答や ARP 要求

Windows Server のループバックインターフェイスは、デフォルトで ARP 応答や ARP 要求が禁止されているため、設定を変更する必要はありません。

4.10 フェイルスルー構成

SX-3940,SX-3920 は、仮想サーバーと実サーバーの IP アドレスを同じアドレスに設定することができます。これにより本装置に障害が発生した場合でも、該当する実サーバーへの通信のみは継続させることができます。



ポイント

フェイルスルー構成の場合、イーサネットポート 1 はクライアントネットワークに固定されます。またイーサネットポート 2 の先にスルーサーバー(仮想 IP アドレスと同じアドレスを持つ実サーバー)が接続されるよう機器を配置してください。ポート 3 以降に実サーバーを接続することも可能ですが、スルー動作は行いません。

⚠ 注意

フェイルスルー構成では本体前面にあるスルースイッチを ON に設定する必要があります。ON になっていないとスルー機能が働きませんので注意してください。

A)　各 IP アドレスに名前付けします。（必須ではありません）

```
netwiser> config
netwiser(config)# name v-www 192.168.1.100
netwiser(config)# name www2 192.168.1.2
```

B) VLAN 10 に管理用アドレスと仮想アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.200/24
netwiser(config-vlan)# ip virtual-address v-www
netwiser(config-vlan)# exit
```

C) 使用するポートを VLAN 10 のメンバに設定します。

```
netwiser(config)# interface ethernet 1-3
netwiser(config-if)# vlan 10
netwiser(config-if)# exit
netwiser(config)#
```

D) 実サーバーを登録します。

```
netwiser(config)# real v-www.80.tcp
netwiser(config)# real www2.80.tcp
```

E) 実サーバーへのヘルスチェックを設定します。

ここでは ICMP echo によるヘルスチェックの設定を例示しています。

設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。

起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-www1 v-www
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-www2 www2
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

ポイント

フェイルスルー対象サーバーに対しては ICMP echo によるヘルスチェックの設定が必須となります。TCP やアプリケーションレイヤーでのヘルスチェックが必要な場合は上記設定に加えて別途設定を追加してください。

F) 仮想サーバーを設定します。

ここでは仮想サーバーへの名前付け、セッション維持設定、実サーバーのバインド、仮想サーバーの有効化を設定します。

```
netwiser(config)# virtual v-www.80.tcp
netwiser(config-virtual)# name v-http
netwiser(config-virtual)# sticky generic
netwiser(config-virtual)# bind v-www.80
netwiser(config-virtual)# bind www2.80
netwiser(config-virtual)# enable
```

```
netwiser(config-virtual)# exit
```

G) 設定を保存します。

```
netwiser(config)# write memory
```

4.11 冗長構成

本製品の冗長構成の典型的な設定パターンを 3 つ説明します。

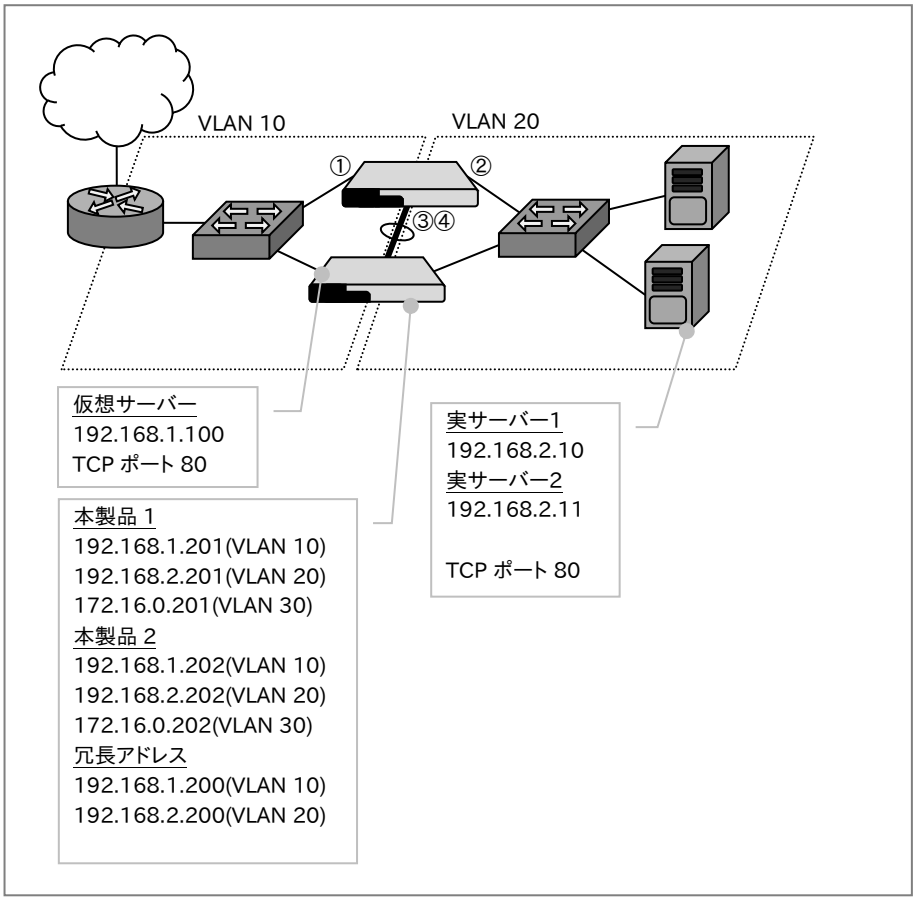
1. 仮想サーバーと実サーバーの VLAN が異なり、上下スイッチが冗長化されていない構成
2. 仮想サーバー、実サーバーの VLAN が同じで、上下スイッチが冗長化されている構成(STP 無し)
3. 仮想サーバー、実サーバーの VLAN が同じで、上下スイッチが冗長化されている構成(STP 有り)

⚠ 注意

フェイルスルー機能が使用できる機器(SX-3940 や SX-3920)では、本体前面にあるスルースイッチを OFF に設定する必要があります。ON になっていると本製品の電源が落ちた時にネットワーク上でループが形成されてしまう可能性があります。

4.11.1 構成例 1

仮想サーバーと実サーバーの VLAN が異なる場合の構成例です。本構成ではネットワーク上にループが無いので後述の *backup-l2forward* や、各スイッチの STP 設定について考慮する必要はありません。



ポイント

冗長構成の設定は、先に片方の機器を最後まで設定し、完了後に同期コマンド *sync config all* を実行して同期する方法と、両方の機器の設定を同時に進めていく方法があります。本設定例では同時に進める方法で説明します。

ポイント

はじめに、冗長構成を組むための最低限の設定情報を投入し、コマンド同期ができるところまで設定します。設定が完了するまでは LAN ケーブルを接続しないでください。

A)　各 VLAN に管理 IP アドレスを設定します。

■装置 1

```
netwiser> config
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.201/24
netwiser(config-vlan)# vrrp vrid 10
netwiser(config-vlan)# exit
netwiser(config)# interface vlan 20
netwiser(config-vlan)# ip address 192.168.2.201/24
netwiser(config-vlan)# vrrp vrid 20
netwiser(config-vlan)# exit
netwiser(config)# interface vlan 30
netwiser(config-vlan)# ip address 172.16.0.201/24
netwiser(config-vlan)# exit
```

■装置 2

```
netwiser> config
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.202/24
netwiser(config-vlan)# vrrp vrid 10
netwiser(config-vlan)# exit
netwiser(config)# interface vlan 20
netwiser(config-vlan)# ip address 192.168.2.202/24
netwiser(config-vlan)# vrrp vrid 20
netwiser(config-vlan)# exit
netwiser(config)# interface vlan 30
netwiser(config-vlan)# ip address 172.16.0.202/24
netwiser(config-vlan)# exit
```

B)　使用するポートを各 VLAN のメンバに設定します。

■装置 1, 2 共通

```
netwiser(config)# interface ethernet 1
netwiser(config-if)# vlan 10
netwiser(config-if)# exit
netwiser(config)# interface ethernet 2
netwiser(config-if)# vlan 20
netwiser(config-if)# exit
netwiser(config)# interface ethernet 3,4
netwiser(config-if)# channel 1
netwiser(config-if)# exit
netwiser(config)# interface channel 1
netwiser(config-channel)# vlan 30
netwiser(config-channel)# exit
```

C) 冗長構成相手を設定します。

■装置 1

```
netwiser(config)# vrrp instance
netwiser(config-vrrp)# peer-address 172.16.0.202
netwiser(config-vrrp)# exit
```

■装置 2

```
netwiser(config)# vrrp instance
netwiser(config-vrrp)# peer-address 172.16.0.201
netwiser(config-vrrp)# exit
```

ポイント

ここまでの設定でケーブルを接続すると、装置 1,2 が Master-Backup の冗長構成になります。以降のコマンドは Master 機または Backup 機のどちらかで実行することで、ピア側にコマンドが同期されます。

D) 各 IP アドレスに名前付けします。（必須ではありません）

```
netwiser(config)# name lb1 172.16.0.201
netwiser(config)# name lb2 172.16.0.202
netwiser(config)# name v-www 192.168.1.100
netwiser(config)# name www1 192.168.2.10
netwiser(config)# name www2 192.168.2.11
```

E) 各 VLAN に仮想アドレスと冗長アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip virtual-address v-www
netwiser(config-vlan)# ip redundant-address 192.168.1.200
netwiser(config-vlan)# exit
netwiser(config)# interface vlan 20
netwiser(config-vlan)# ip redundant-address 192.168.2.200
netwiser(config-vlan)# exit
```

F) 実サーバーを登録します。

```
netwiser(config)# real www1.80.tcp
netwiser(config)# real www2.80.tcp
```

G) 実サーバーへのヘルスチェックを設定します。

ここでは TCP コネクション確立によるヘルスチェックの設定を例示しています。
設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。
起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-www1 www1.80.tcp
netwiser(config-probe)# enable
```

```
netwiser(config-probe)# exit
netwiser(config)# probe hc-www2 www2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

H) 仮想サーバーを設定します。

ここでは仮想サーバーへの名前付け、セッション維持設定、実サーバーのバインド、仮想サーバーの有効化を設定します。

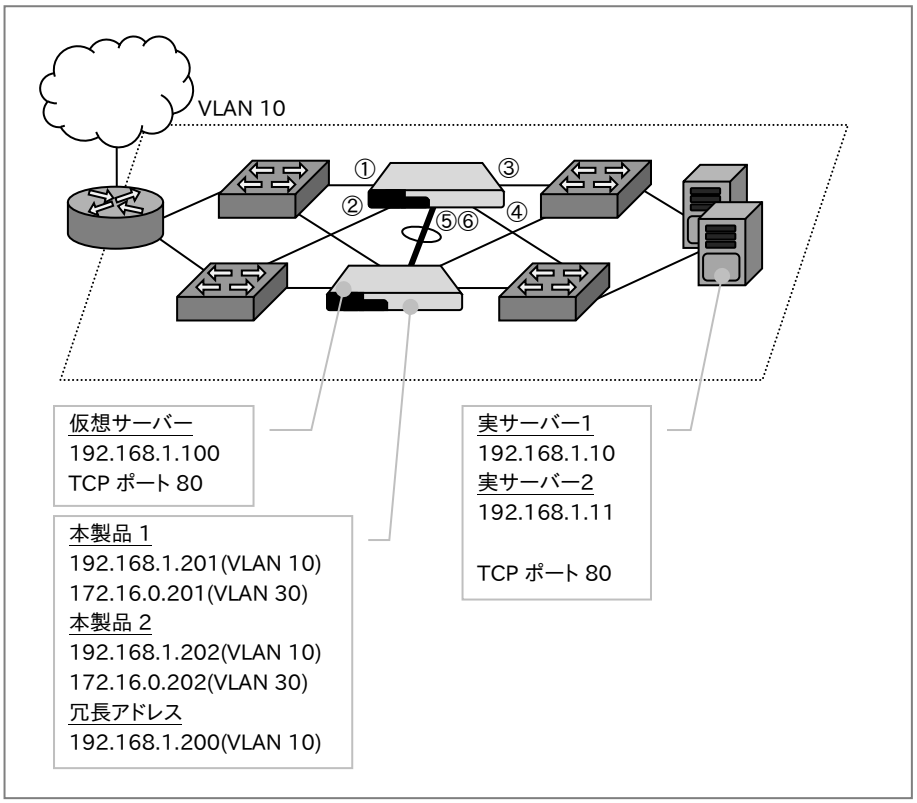
```
netwiser(config)# virtual v-www.80.tcp
netwiser(config-virtual)# name v-http
netwiser(config-virtual)# sticky generic
netwiser(config-virtual)# bind www1.80
netwiser(config-virtual)# bind www2.80
netwiser(config-virtual)# enable
netwiser(config-virtual)# exit
```

I) 設定を保存します。

```
netwiser(config)# write memory
```

4.11.2 構成例 2

仮想サーバーと実サーバーの VLAN が同じの構成例です。設定例 1 に加えて上下スイッチが冗長化されています。本構成ではネットワーク上にループが存在するため、*no vrrp backup-l2forward* 設定でループが発生しないよう配慮する必要があります。



ポイント

冗長構成の設定は、先に片方の機器を最後まで設定し、完了後に同期コマンド *sync config all* を実行して同期する方法と、両方の機器の設定を同時に進めていく方法があります。本設定例では同時に進める方法で説明します。

ポイント

はじめに、冗長構成を組むための最低限の設定情報を投入し、コマンド同期ができるところまで設定します。設定が完了するまでは LAN ケーブルを接続しないでください。

A)　各 VLAN に管理 IP アドレスを設定します。

■装置 1

```
netwiser> config
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.201/24
netwiser(config-vlan)# vrrp vrid 10
netwiser(config-vlan)# no vrrp backup-l2forward
netwiser(config-vlan)# exit
netwiser(config)# interface vlan 30
netwiser(config-vlan)# ip address 172.16.0.201/24
netwiser(config-vlan)# exit
```

■装置 2

```
netwiser> config
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.202/24
netwiser(config-vlan)# vrrp vrid 10
netwiser(config-vlan)# no vrrp backup-l2forward
netwiser(config-vlan)# exit
netwiser(config)# interface vlan 30
netwiser(config-vlan)# ip address 172.16.0.202/24
netwiser(config-vlan)# exit
```

⚠ 注意

*no vrrp backup-l2forward*設定が無いと、LAN ケーブル接続後ループが発生しますので注意してください。

B)　使用するポートを各 VLAN のメンバに設定します。

■装置 1, 2 共通

```
netwiser(config)# interface ethernet 1-4
netwiser(config-if)# vlan 10
netwiser(config-if)# exit
netwiser(config)# interface ethernet 5,6
netwiser(config-if)# channel 1
netwiser(config-if)# exit
netwiser(config)# interface channel 1
netwiser(config-channel)# vlan 30
netwiser(config-channel)# exit
```

C)　冗長構成相手を設定します。

■装置 1

```
netwiser(config)# vrrp instance
```

```
netwiser(config-vrrp)# peer-address 172.16.0.202
netwiser(config-vrrp)# exit
```

■装置 2

```
netwiser(config)# vrrp instance
netwiser(config-vrrp)# peer-address 172.16.0.201
netwiser(config-vrrp)# exit
```

ポイント

ここまでの設定でケーブルを接続すると、装置 1,2 が Master-Backup の冗長構成になります。以降のコマンドは Master 機または Backup 機のどちらかで実行することで、ピア側にコマンドが同期されます。

D) リンク監視機能で、上下スイッチへの経路が途絶えた際にフェイルオーバーするように設定します。

```
netwiser(config)# vrrp instance
netwiser(config-vrrp)# track group 1 ethernet 1,2
netwiser(config-vrrp)# track group 2 ethernet 3,4
netwiser(config-vrrp)# exit
```

ポイント

同一の *track group* 内の全ての物理リンクがダウンすると本製品は VRRP 広告の送信を停止します。

E) 各 IP アドレスに名前付けします。 (必須ではありません)

```
netwiser(config)# name lb1 172.16.0.201
netwiser(config)# name lb2 172.16.0.202
netwiser(config)# name v-www 192.168.1.100
netwiser(config)# name www1 192.168.1.10
netwiser(config)# name www2 192.168.1.11
```

F) 各 VLAN に仮想アドレスと冗長アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip virtual-address v-www
netwiser(config-vlan)# ip redundant-address 192.168.1.200
netwiser(config-vlan)# exit
```

G) 実サーバーを登録します。

```
netwiser(config)# real www1.80.tcp
netwiser(config)# real www2.80.tcp
```

H) 実サーバーへのヘルスチェックを設定します。

ここでは TCP コネクション確立によるヘルスチェックの設定を例示しています。

設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。

起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-www1 www1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-www2 www2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

I) 仮想サーバーを設定します。

ここでは仮想サーバーへの名前付け、セッション維持設定、実サーバーのバインド、仮想サーバーの有効化を設定します。

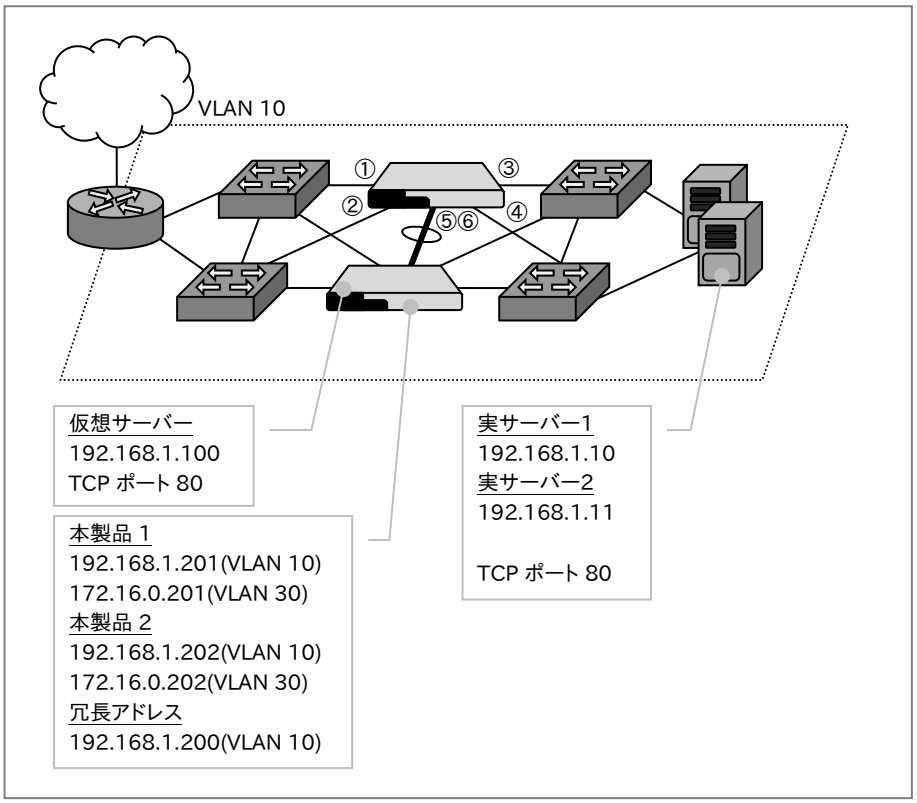
```
netwiser(config)# virtual v-www.80.tcp
netwiser(config-virtual)# name v-http
netwiser(config-virtual)# sticky generic
netwiser(config-virtual)# bind www1.80
netwiser(config-virtual)# bind www2.80
netwiser(config-virtual)# enable
netwiser(config-virtual)# exit
```

J) 設定を保存します。

```
netwiser(config)# write memory
```

4.11.3 構成例 3

仮想サーバーと実サーバーの VLAN が同じの構成例です。設定例 2 に加えて冗長化されたスイッチ間の渡りが接続されています。本構成では *no vrrp backup-l2forward* 設定ではループ状態を回避することができないため、全てのスイッチでスパニングツリーを動作させる必要があります。



ポイント

冗長構成の設定は、先に片方の機器を最後まで設定し、完了後に同期コマンド *sync config all* を実行して同期する方法と、両方の機器の設定を同時に進めていく方法があります。本設定例では同時に進める方法で説明します。

ポイント

はじめに、冗長構成を組むための最低限の設定情報を投入し、コマンド同期ができるところまで設定します。設定が完了するまでは LAN ケーブルを接続しないでください。

A) 各 VLAN に管理 IP アドレスを設定します。

■装置 1

```
netwiser> config
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.201/24
netwiser(config-vlan)# vrrp vrid 10
netwiser(config-vlan)# exit
netwiser(config)# interface vlan 30
netwiser(config-vlan)# ip address 172.16.0.201/24
netwiser(config-vlan)# vrrp vrid 30
netwiser(config-vlan)# exit
```

■装置 2

```
netwiser> config
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip address 192.168.1.202/24
netwiser(config-vlan)# vrrp vrid 10
netwiser(config-vlan)# exit
netwiser(config)# interface vlan 30
netwiser(config-vlan)# ip address 172.16.0.202/24
netwiser(config-vlan)# vrrp vrid 30
netwiser(config-vlan)# exit
```

B) 使用するポートを各 VLAN のメンバに設定し、スパニングツリーを有効に設定します。

■装置 1, 2 共通

```
netwiser(config)# interface ethernet 1-4
netwiser(config-if)# vlan 10
netwiser(config-if)# spanning-tree
netwiser(config-if)# exit
netwiser(config)# interface ethernet 5,6
netwiser(config-if)# channel 1
netwiser(config-if)# exit
netwiser(config)# interface channel 1
netwiser(config-channel)# vlan 30
netwiser(config-channel)# exit
```

ポイント

スパニングツリーの設定をする場合、本製品がルートブリッジにならないように注意してください。本製品をルートブリッジにする必要がある場合は、*spanning-tree backup-priority* を設定し、VRRP 状態と STP 状態を連携させてください。

C) 冗長構成相手を設定します。

■装置 1

```
netwiser(config)# vrrp instance
netwiser(config-if)# peer-address 172.16.0.202
netwiser(config-if)# exit
```

■装置 2

```
netwiser(config)# vrrp instance
netwiser(config-if)# peer-address 172.16.0.201
netwiser(config-if)# exit
```

ポイント

ここまでの設定でケーブルを接続すると、装置 1,2 が Master-Backup の冗長構成になります。以降のコマンドは Master 機または Backup 機のどちらかで実行することで、ピア側にコマンドが同期されます。

D) リンク監視機能で、上下スイッチへの経路が途絶えた際にフェイルオーバーするように設定します。

```
netwiser(config)# vrrp instance
netwiser(config-vrrp)# track group 1 ethernet 1,2
netwiser(config-vrrp)# track group 2 ethernet 3,4
netwiser(config-vrrp)# exit
```

ポイント

同一の *track group* 内の全ての物理リンクがダウンすると本製品は VRRP 広告の送信を停止します。

E) 各 IP アドレスに名前付けします。(必須ではありません)

```
netwiser(config)# name lb1 172.16.0.201
netwiser(config)# name lb2 172.16.0.202
netwiser(config)# name v-www 192.168.1.100
netwiser(config)# name www1 192.168.1.10
netwiser(config)# name www2 192.168.1.11
```

F) 各 VLAN に仮想アドレスと冗長アドレスを設定します。

```
netwiser(config)# interface vlan 10
netwiser(config-vlan)# ip virtual-address v-www
netwiser(config-vlan)# ip redundant-address 192.168.1.200
netwiser(config-vlan)# exit
```

G) 実サーバーを登録します。

```
netwiser(config)# real www1.80.tcp
netwiser(config)# real www2.80.tcp
```

H) 実サーバーへのヘルスチェックを設定します。

ここでは TCP コネクション確立によるヘルスチェックの設定を例示しています。

設定直後のヘルスチェックエントリーはデフォルトで無効状態になっています。

起動する場合は *enable* 設定が必要になります。

```
netwiser(config)# probe hc-www1 www1.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
netwiser(config)# probe hc-www2 www2.80.tcp
netwiser(config-probe)# enable
netwiser(config-probe)# exit
```

I) 仮想サーバーを設定します。

ここでは仮想サーバーへの名前付け、セッション維持設定、実サーバーのバインド、仮想サーバーの有効化を設定します。

```
netwiser(config)# virtual v-www.80.tcp
netwiser(config-virtual)# name v-http
netwiser(config-virtual)# sticky generic
netwiser(config-virtual)# bind www1.80
netwiser(config-virtual)# bind www2.80
netwiser(config-virtual)# enable
netwiser(config-virtual)# exit
```

J) 設定を保存します。

```
netwiser(config)# write memory
```

第5章　運用ガイド

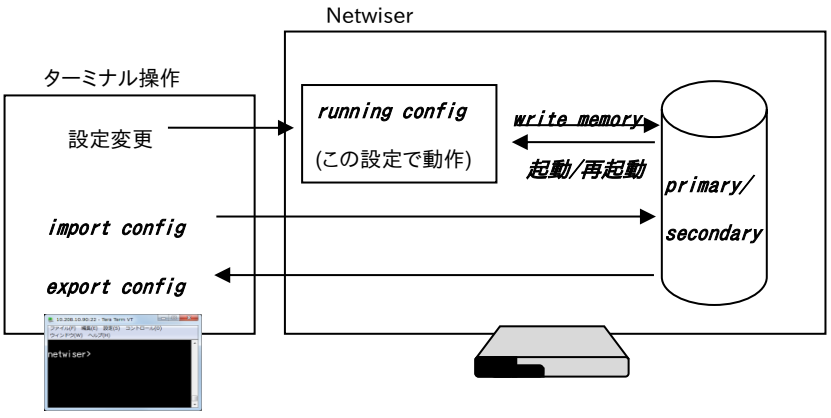
5.1 概要

本章では、本製品の運用、メンテナンスに関わる設定やコマンド、または操作手順について説明します。

5.1.1 設定情報とシステムの起動領域について

本製品は、システムの起動領域として primary 領域/secondary 領域の 2 面持ちます。システムの全設定情報をそれぞれの領域に別々に保持することが可能です。システムの初期状態では、primary 領域の設定情報(以下、primary config)で起動します。再起動時に指定することで、secondary 領域の設定情報(以下、secondary config)で起動することが可能です。
このように、システムの起動領域と設定情報の間で、primary/secondary が対応付けて動作します。

起動時に参照した設定ファイルは、起動後に running config としてコピーされます。本製品は、running config を使用して動作します。
設定の変更は running config ファイルに反映され、設定に従って動作が開始されます。ただし、running config は一時的な設定情報ファイルになりますので電源 OFF/ON することで設定情報は消去されてしまいます。
設定変更後は ***write memory*** コマンドまたは、***copy*** コマンドで設定情報を保存してください。特別に指定しない限り、設定情報の保存は起動した時点での領域に対して行われます。



5.2 設定データやファームウェアのコピー

primary/secondary 起動領域間で設定ファイルやファームウェアファイルをコピーすることができます。
本機能を使用することで、ファームウェアや設定情報を更新する前に、primary 起動領域の情報を secondary 起動領域にバックアップしておくことが可能となります。また、primary 起動領域の情報を更新した後で secondary 起動領域を同じ状態に更新することも簡単に実現できます。(secondary 起動領域から primary 起動領域へのコピーも可能です)

CLI で設定ファイルやファームウェアファイルをコピーする場合、*copy* コマンドを使用します。

```
netwiser(config)# copy {startup-config | firmware } {primary secondary | secondary primary}
```

■ *startup-config*

起動時に参照される設定ファイルを primary/secondary 起動領域間でコピーします。

■ *firmware*

ファームウェアファイルを primary/secondary 起動領域間でコピーします。

■ *primary, secondary*

コピー元起動領域とコピー先起動領域を指定します。
"<コピー元起動領域> <コピー先起動領域>"の順に指定してください。

[WEB 管理画面]

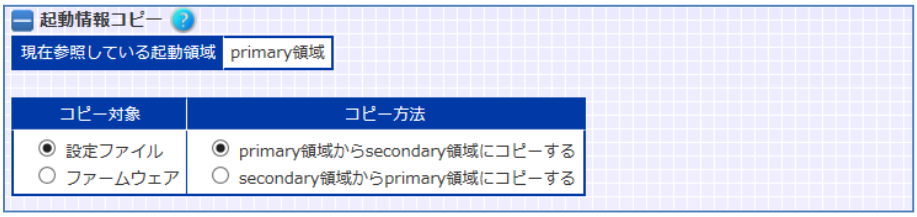
場所: 設定 > システム > 機器情報 > 起動ファイル情報複製

■起動情報コピー

① 現在参照している起動領域
　現在参照している起動領域を表示します。

② コピー対象
　コピーしたいファイル種別を選択します。

③ コピー方法
　コピー元起動領域とコピー先起動領域の組み合わせを選択します。



5.3 ファイルの取り込みと取り出し

本章では、本製品に対する設定情報やファームウェアファイルの取り込み（以下、インポート）、設定情報やログ情報などの取り出し（以下、エクスポート）に関する操作手順について説明します。

5.3.1 設定情報のインポートとファームウェアアップグレード

設定ファイルやファームウェアを本製品へインポートするには *import* コマンドを実行します。

ファイルの転送には tftp または zmodem を使用します。このため、tftp または zmodem が動作するパソコンを使用してネットワーク経由で行ってください。

WEB 管理画面から行う場合は、WEB ブラウザからファイルの取り込みを行うので、特別な転送プロトコルに対応している必要はありません。

tftp、zmodem で行うファイル転送の例として、設定ファイルのインポート手順を説明します。

■tftp を使用する場合

① *import* コマンドの実行

telnet または ssh で本製品にログインし、*import* コマンドを実行します。

```
netwiser(config)# import config tftp
Ready to TFTP receive.
Press 'q[ENTER]' to cancel:
```

転送プロトコルオプションは省略可能で、省略した場合 tftp が選択されます。

”Ready to TFTP receive.” と表示されたら、ローカル端末側で、tftp コマンドを実行してください。

② tftp コマンドの実行

Windows 系の場合

```
tftp -i 〈IP アドレス〉 put 〈ファイル名〉
```

UNIX 系 OS の場合

```
tftp〉 put 〈IP アドレス〉:slb.primary.conf
Received 3508 bytes during 0.0 seconds in 7 blocks
```

tftp コマンドは OS やバージョンの違いにより使用方法に差異がある場合があります。ご使用の環境での使用方法を確認し、操作を行ってください。
転送が成功すると、CLI 上に" Transfer is complete."と表示されます。
再起動して設定を有効にしてください。

```
netwiser(config)# import config tftp
Ready to TFTP receive.
Press 'q[ENTER]' to cancel: .

Transfer is complete.
'import config primary' done.
Reboot is required for changes to take effect.
```

■zmodem を使用する場合

① *import* コマンドの実行

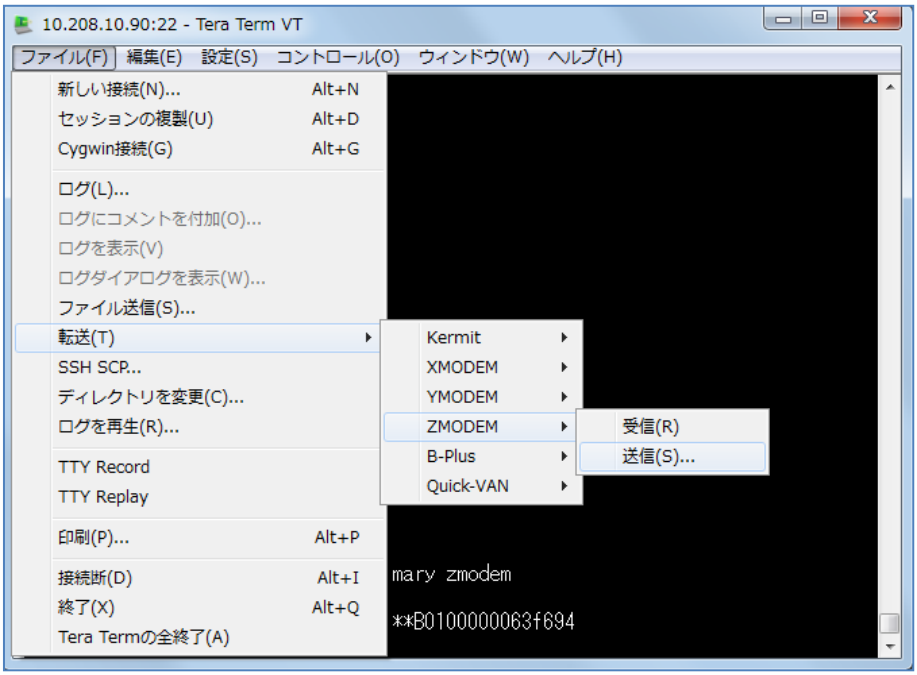
telnet または ssh で本製品にログインし、*zmodem* オプションを指定して *import* コマンドを実行します。

```
netwiser(config)# import config zmodem
Ready to TFTP receive.
Press 'q[ENTER]' to cancel:
```

”Ready to ZMODEM receive.” と表示されたら、ローカル端末側で、zmodem を実行してください。

② zmodem の実行

ZMODEM を使用して機器にファイルを転送します。



import コマンド実行時は「送信」を、*export* コマンド実行時は「受信」を選択します。
OS や VT100 エミュレータの種別により差異がある場合があります。ご使用の環境での使用方法を確認し、操作を行ってください。
転送が成功すると、CLI 上に" Transfer is complete."と表示されます。
再起動して設定を有効にしてください。

```
netwiser(config)# import config zmodem
Ready to ZMODEM receive.
Press '^X' several time to cancel: **B0100000063f694

Transfer is complete.
'import config primary' done.
Reboot is required for changes to take effect.Reboot is required
 for changes to take effect.
```

import config コマンドの詳細や、WEB 管理画面からのインポート手順については「5.3.1.1設定ファイルのインポート」を参照してください。

5.3.1.1 設定ファイルのインポート

設定ファイルをインポートする場合は *import config* コマンドを使用します。
インポート完了後は、設定を有効にするために本製品を再起動してください。

```
adm(config)# import config [primary | secondary | current] [tftp | zmodem]
```

■*primary, secondary, current*

インポート先の起動領域を選択します。
current を指定した場合、または本パラメーターを省略した場合、現在の起動領域になります。

■*tftp, zmodem*

ファイルの転送方法を選択します。省略した場合、tftp を使用します。
それぞれのプロトコルに応じた転送手順については、「5.3.1設定情報のインポートとファームウェアアップグレード」を参照してください。

ポイント

ファイルのインポート後は、設定保存せず直ちに機器を再起動してください。設定の保存を行うと、次回起動時に使用されるはずの設定情報が、現在の設定情報で上書きされてしまいます。

ポイント

import config コマンドでは SSL 証明書、鍵ファイル、sorry コンテンツ等の設定以外のファイルはインポートされませんので注意してください。それらのファイルも含めた全ての設定情報をインポートする場合、*import all* コマンドを使用します。詳細は「5.3.1.3全ての設定情報のインポート」を参照してください。

⚠ 注意

テキストエディタ等で独自に編集した設定ファイルを本製品にインポートする場合、以下の注意点を守り正しい形式の設定ファイルをインポートしてください。

・ 設定ファイル上に記述される設定行の文字列と、設定時にコマンドとして実行する際の文字列とでは、文法が異なるケースがあります。

例）

```
real 192.168.1.100.80.tcp is      ; 設定ファイル上の記述形式
real 192.168.1.100.80.tcp         ; コマンド文法
```

設定行が設定ファイルの記述形式と異なると、インポートエラーとなるか、またはシステムに正しく認識されない恐れがあります。

show config コマンドや *show running-config* コマンド、または WEB 設定画面の「設定エクスポート画面」で設定ファイルの記述形式を確認し、正しく編集してください。

・ 設定ファイル内にコメント文を埋め込むことはできません。以下のように、各設定行の初めに記号をいれないでください。

```
!
real 192.168.0.100.80.tcp is
# this real-server-id is test
# real 192.168.0.101.80.tcp is
!
```

ただし、!は設定種別毎の区切りのマークとして必須ですので、取り除かないでください。

・ エクスポートしたファイルを編集して *user-mgmt* 設定行を追加したとしても、新規のユーザーアカウントは作成されません。
ユーザーアカウントを追加する場合は、必ず CLI、または WEB 設定画面から設定してください。ユーザーアカウントを削除する場合も同様です。

・ 編集後、設定ファイルを保存する際には、改行コードを"LF"または"CR-LF"にして保存してください。その他の改行コードは正しく認識されません。

ポイント

SSL 証明書自動更新は設定インポート時は無効(no enable)になっています。
再起動後自動更新の進捗状況を確認してから有効にしてください。
詳しくは、「2.20.10.7 SSL 証明書自動更新設定上の注意」を確認してください。

[WEB 管理画面]

場所: 設定 ＞ システム ＞ 機器情報 ＞ 設定インポート

事前にエクスポートした設定情報を、本製品にインポートします。

■設定インポート

① 設定ファイル

機器にインポートしたいファイルを選択します。

② 起動領域

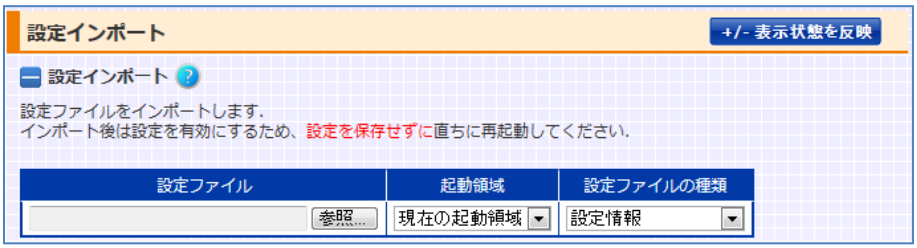
インポート先のブート領域を選択します。

③ 設定ファイルの種類

インポートするファイルの種別を選択します。

「設定情報」を選択すると、設定ファイルのインポートを行います。

「全設定情報」を選択すると、SSL 証明書、鍵ファイル、sorry コンテンツ等の設定ファイル以外のファイルも含めた全ての設定情報のインポートを行います。



5.3.1.2 画面表示情報のインポート

画面カスタム操作で変更した画面の表示状態は、設定ファイルとして
画面表示の設定情報をインポートする場合は *import webconf* コマンドを使用します。

```
adm(config)# import webconf [tftp | zmodem]
```

■ *tftp, zmodem*

ファイルの転送方法を選択します。省略した場合、tftp を使用します。
それぞれのプロトコルに応じた転送手順については、「5.3.1設定情報のインポートとファームウェアアップグレード」を参照してください。

ポイント

インポート完了後、画面を更新する事で表示状態が反映しますが、そのままでは再起動後に有効になりません。再起動後も画面表示状態を保持したい場合は設定を保存してください。

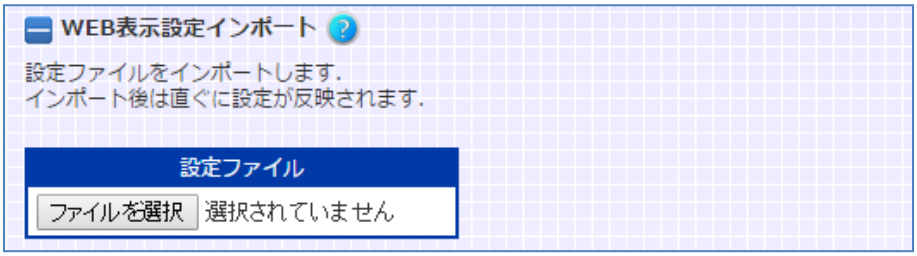
[WEB 管理画面]

場所: 設定 > システム > 機器管理 > WEB 表示設定インポート

事前にエクスポートした画面表示情報を、本製品にインポートします。

■WEB 表示設定インポート

① 設定ファイル
機器にインポートしたいファイルを選択します。



画面表示操作用の設定情報の定義は「5.3.5WEB 管理画面表示用設定ファイル」を参照してください。

5.3.1.3 全ての設定情報のインポート

SSL 証明書、鍵ファイル、sorry コンテンツ等の設定ファイル以外のファイルも含めた全ての設定情報を本製品にインポートする場合 *import all* コマンドを使用します。

```
adm(config)# import all [primary | secondary | current] [tftp | zmodem]
```

■*primary, secondary, current*

インポート先の起動領域を選択します。

current を指定した場合、または本パラメーターを省略した場合、現在の起動領域になります。省略した場合 *current* が選択されます。

■*tftp, zmodem*

ファイルの転送方法を選択します。省略した場合、tftp を使用します。

それぞれのプロトコルに応じた転送手順については、「5.3.1設定情報のインポートとファームウェアアップグレード」を参照してください。

ポイント

ファイルのインポート後は、設定保存せず直ちに機器を再起動してください。設定保存を行うと、次回起動時に使用されるはずの設定情報が、現在の設定情報で上書きされてしまいます。

[WEB 管理画面]

場所: 設定 > システム > 機器情報 > 設定インポート

事前にエクスポートした全設定情報を、本製品にインポートします。

画面説明は「5.3.1.1設定ファイルのインポート」を参照してください。

ポイント

SSL 証明書自動更新は設定インポート時は無効(no enable)になっています。

再起動後自動更新の進捗状況を確認してから有効にしてください。

詳しくは、「2.21.10.7 SSL 証明書自動更新設定上の注意」を確認してください。

5.3.1.4 SSL 関連ファイルのインポート

本製品に証明書や秘密鍵などの SSL 関連ファイルをインポートする場合、*import ssl* コマンドを使用します。
詳細は「2.20.3電子証明書と鍵のインポート」を参照してください。

5.3.1.5 sorry コンテンツのインポート

実サーバーの障害時や過負荷状況、またはメンテナンスなど、なんらかの理由で HTTP リクエストの振り分けが出来ない場合、サービスが提供できない旨の代替コンテンツを本製品から返信することが可能です。当該コンテンツを「sorry コンテンツ」と呼称します。
本製品に sorry コンテンツファイルをインポートする場合、*import content* コマンドを使用します。ファイル転送後は直ちに設定を保存してください。

```
netwiser(config)# import content <content-name> [ tftp | zmodem ]
```

■ *tftp, zmodem*

ファイルの転送方法を選択します。省略した場合、tftp を使用します。
それぞれのプロトコルに応じた転送手順については、「5.3.1設定情報のインポートとファームウェアアップグレード」を参照してください。

ポイント

冗長構成で、かつ冗長相手とコマンドの同期が可能な状態であれば、自機器にインポートした sorry コンテンツはピア側の機器にコピーされます。

show content コマンドでインポートされた sorry コンテンツの内容を表示させることができます。
詳しくは**「SX-3990_3950_3945_3940_3920 コマンドリファレンス」（別紙）**を参照してください。

[WEB 管理画面]

場所：設定 ＞ バランシング ＞ 実サーバー ＞ sorry コンテンツインポート

実サーバーのサービスが何らかの理由で停止した際、クライアントからのリクエストに代替コンテンツで応答することが可能です。

初めに、代替コンテンツをインポートインポートします。

■sorry コンテンツインポート

① sorry コンテンツ

インポートするコンテンツファイルを選択します。

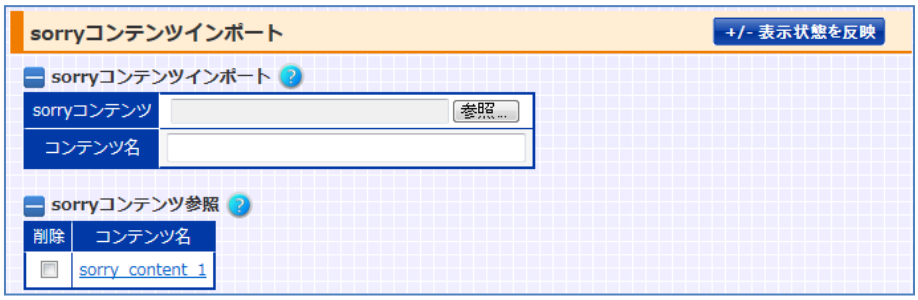
② コンテンツ名

インポートする際にコンテンツ名を定義します。

■sorry コンテンツ参照

インポートしたコンテンツは本画面上にリンクで表示されます。

リンクを押下することでコンテンツ内容を確認できます。



5.3.1.6 ファームウェアのインポート

本製品のファームウェアバージョンを更新するには、*import firmware* コマンドを使用し、ファームウェアファイルを機器に取り込みます。
バージョンアップを有効にするには、インポート後再起動します。

```
adm(config)# import firmware [primary | secondary | current] [tftp | zmodem]
```

■*primary, secondary, current*
インポート先の起動領域を選択します。
current を指定した場合、または本パラメーターを省略した場合、現在の起動領域になります。省略した場合 *current* が選択されます。

■*tftp, zmodem*
ファイルの転送方法を選択します。省略した場合、tftp を使用します。
それぞれのプロトコルに応じた転送手順については、「5.3.1設定情報のインポートとファームウェアアップグレード」を参照してください。

ポイント

Netwiser version 7(SX-38 シリーズ)の設定ファイルを Netwiser version 8(SX-39 シリーズ)にインポートして使用することが可能です。

[WEB 管理画面]
場所: 設定 > システム > 機器情報 > 設定インポート
ファームウェアファイルを、本製品にインポートします。

■設定インポート
① ファームウェアファイル
ファームウェアファイルを選択します。

② 起動領域
インポート先のブート領域を選択します。

5.3.2 機器情報のエクスポート

本製品の設定情報やインポート済みの SSL 証明書ファイル等を取り出すには、*export* コマンドを実行します。

telnet や ssh で本製品にアクセスして行う場合、ファイルの転送には tftp または zmodem を使用します。このため、tftp または zmodem が動作するパソコンを使用してネットワーク経由で行ってください。

WEB 管理画面から行う場合は、WEB ブラウザからファイルの取り出しを行うので、特別な転送プロトコルに対応している必要はありません。

readonly 権限のユーザーアカウントでログインした場合、WEB 管理画面から設定情報のエクスポートを行うことはできませんので注意してください。

ファイル転送の例として、「5.3.1設定情報のインポートとファームウェアアップグレード」で設定ファイルの転送手順を説明していますので参照してください。

5.3.2.1 設定ファイルのエクスポート

設定ファイルをエクスポートする場合は *export config* コマンドを使用します。

```
adm(config)# export config [primary | secondary | current] [tftp | zmodem]
```

■*primary, secondary, current*

エクスポート元の起動領域を選択します。

current を指定した場合、または本パラメーターを省略した場合、現在の起動領域から設定ファイルを取り出します。

■*tftp, zmodem*

ファイルの転送方法を選択します。省略した場合、tftp を使用します。

それぞれのプロトコルに応じた転送手順については、「5.3.1設定情報のインポートとファームウェアアップグレード」を参照してください。

⚠ 注意 エクスポートした設定ファイルをテキストエディタ等で編集し、再度本製品にインポートすることは可能ですが、正しい記述形式で編集された設定ファイルをインポートしてください。設定ファイルをインポートする際の注意点は「5.3.1.1設定ファイルのインポート」を参照してください。

[WEB 管理画面]
場所: 設定 > システム > 機器情報 > 設定エクスポート
本製品の設定情報ファイルを取り出します。

■設定エクスポート

① 現在参照している起動領域
現在使用している起動領域を表示します。

② 現在の設定情報
現在動作している設定ファイル（running-config）へのハイパーリンクです。

③ primary 領域の設定情報
primary 起動領域に保存されている設定ファイルへのハイパーリンクです。

④ secondary 領域の設定情報
secondary 起動領域に保存されている設定ファイルへのハイパーリンクです。

⑤ primary 領域の全設定情報
primary 起動領域に保存されている全設定情報へのハイパーリンクです。全設定情報には、設定ファイル、sorry コンテンツ、 証明書や鍵等の SSL 情報、 SNMP 起動情報が含まれます。

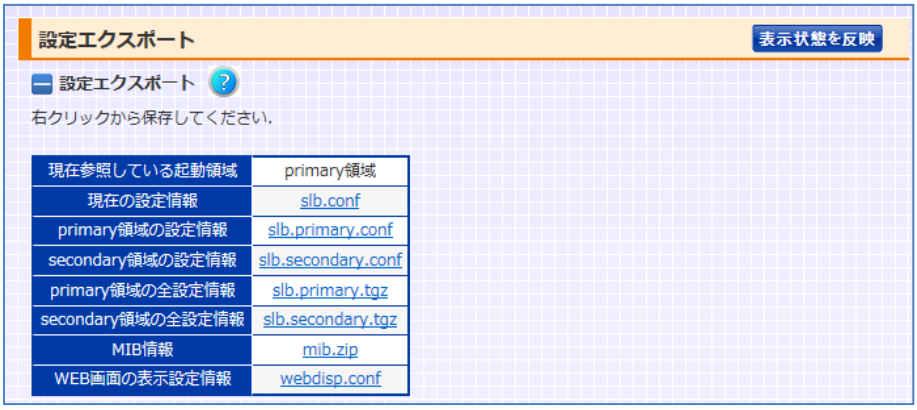
⑥ secondary 領域の全設定情報
secondary 起動領域に保存されている全設定情報へのハイパーリンクです。

⑦ MIB 情報

拡張 MIB 定義ファイルへのハイパーリンクです。

⑧ WEB 画面の表示設定情報

WEB 管理画面の表示設定を格納したファイルへのハイパーリンクです。



5.3.2.2 画面表示情報のエクスポート

本製品は、WEB 管理画面の設定画面に関して、表示状態をカスタマイズする事が可能です。(「3.6画面カスタマイズ機能」参照)

現在の画面表示状態を本製品からエクスポートする場合 ***export webconf*** コマンドを使用します。

```
adm(config)# export webconf [tftp | zmodem]
```

■ ***tftp, zmodem***

ファイルの転送方法を選択します。省略した場合、tftp を使用します。

それぞれのプロトコルに応じた転送手順については、「5.3.1設定情報のインポートとファームウェアアップグレード」を参照してください。

[WEB 管理画面]

場所: 設定 > システム > 機器情報 > 設定エクスポート

本製品の WEB 管理画面における表示状態を格納した設定ファイルを取り出します。画面詳細は「5.3.2.1設定ファイルのエクスポート」を参照してください。

画面表示操作用の設定情報の定義は「5.3.5WEB 管理画面表示用設定ファイル」を参照してください

5.3.2.3 全ての設定情報のエクスポート

SSL 証明書、鍵ファイル、sorry コンテンツ等の設定以外のファイルも含めた全ての設定情報を本製品からエクスポートする場合 *export all* コマンドを使用します。

```
adm(config)# export all [primary | secondary | current] [tftp | zmodem]
```

■*primary, secondary, current*

エクスポート元の起動領域を選択します。

current を指定した場合、または本パラメーターを省略した場合、現在の起動領域からエクスポートします。省略した場合 *current* が選択されます。

■*tftp, zmodem*

ファイルの転送方法を選択します。省略した場合、tftp を使用します。

それぞれのプロトコルに応じた転送手順については、「5.3.1設定情報のインポートとファームウェアアップグレード」を参照してください。

[WEB 管理画面]

場所: 設定 > システム > 機器情報 > 設定エクスポート

本製品の設定情報ファイルを取り出します。

詳細は「5.3.2.1設定ファイルのエクスポート」を参照してください。

5.3.2.4 SSL 関連ファイルのエクスポート

本製品から証明書や秘密鍵などの SSL 関連ファイルをエクスポートする場合、*export ssl* コマンドを使用します。

```
adm(config)# export ssl <policy-name> { cert | chain | client | crl | csr | key | pkcs12 } [ tftp | zmodem ]
```

エクスポートするファイルの種別とファイルの転送方法を選択します。

■*cert, chain, client, crl, csr, key, pkcs12*

エクスポートするファイルの種別を選択します。

中間証明書や CA 証明書など、証明書がチェーンされている場合、チェーンされた全ての証明書を取り出します。

■ *tftp, zmodem*
ファイルの転送方法を選択します。省略した場合、tftp を使用します。
それぞれのプロトコルに応じた転送手順については、「5.3.1設定情報のインポートとファームウェアアップグレード」を参照してください。

[WEB 管理画面]
場所: 設定 > システム > 機器情報 > 設定エクスポート
本製品の設定情報ファイルを取り出します。

■ファイル選択
任意の SSL ポリシーにインポートされている証明書や鍵ファイルのハイパーリンクを表示します。リンクをクリックすると、ファイル内容が表示されます。
エクスポートするには、右クリックから保存してください。

① SSL ポリシー名
設定済みの SSL ポリシー名。

② 秘密鍵
秘密鍵ファイルへのハイパーリンクです。

③ 証明書
サーバー証明書へのハイパーリンクです。

④ 中間証明書
中間証明書へのハイパーリンクです。証明書がチェーンされている場合、チェーンされた全ての証明書を取り出します。

⑤ CA 局証明書（クライアント認証）
CA 局証明書へのハイパーリンクです。証明書がチェーンされている場合、チェーンされた全ての証明書を取り出します。

⑥ CSR（署名要求）
証明書署名要求書へのハイパーリンクです。

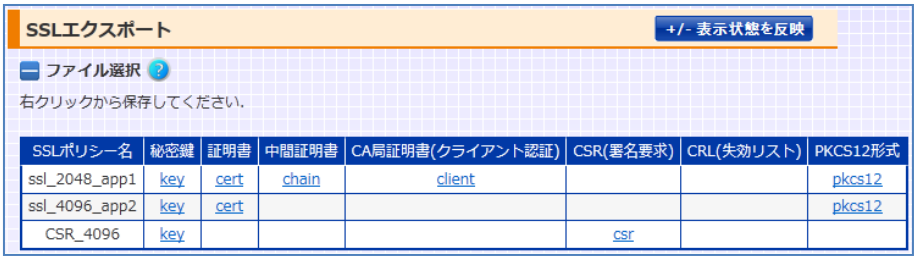
⑦ CRL（失効リスト）

証明書失効リストへのハイパーリンクです。

⑧ PKCS12 形式

PKCS12 形式ファイルへのハイパーリンクです。

インポートした秘密鍵、サーバー証明書、中間証明書をまとめて、PKCS12 形式ファイルに変換しています。



SSLポリシー名	秘密鍵	証明書	中間証明書	CA局証明書(クライアント認証)	CSR(署名要求)	CRL(失効リスト)	PKCS12形式
ssl_2048_app1	key	cert	chain	client			pkcs12
ssl_4096_app2	key	cert					pkcs12
CSR_4096	key				csr		

5.3.2.5 MIB 定義ファイルのエクスポート

プライベート MIB の定義ファイルをエクスポートする場合は ***export mib*** コマンドを使用します。

```
adm(config)# export mib [tftp | zmodem]
```

■ ***tftp, zmodem***

ファイルの転送方法を選択します。省略した場合、tftp を使用します。

それぞれのプロトコルに応じた転送手順については、「5.3.1設定情報のインポートとファームウェアアップグレード」を参照してください。

[WEB 管理画面]

場所: 設定 > システム > 機器情報 > 設定エクスポート

本製品の設定情報ファイルを取り出します。

詳細は「5.3.2.1設定ファイルのエクスポート」を参照してください。

5.3.2.6 シスログのエクスポート

シスログファイルをエクスポートする場合は *export log* コマンドを使用します。

```
adm(config)# export log [tftp | zmodem]
```

■ *tftp, zmodem*

ファイルの転送方法を選択します。

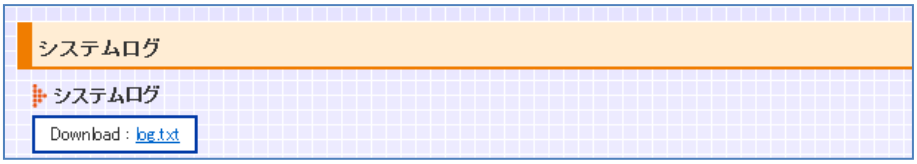
それぞれのプロトコルに応じた転送手順については、「5.3.1設定情報のインポートとファームウェアアップグレード」を参照してください。

[WEB 管理画面]

場所: ログ参照 > システムログ

本製品に保存されているシステムログの表示と、シスログファイルのダウンロードができます。

シスログファイルへのハイパーリンクが表示されるので、右クリックで保存してください。



5.3.3 L7 トレース機能

本装置には、解析用の機能として L7 負荷分散パケットに関するパケットトレースを実施し、キャプチャデータを生成する機能があります。

⚠ 注意

本コマンドは使い方によって disk の消耗速度を早める危険性があります。
必ず、弊社技術サポートエンジニアの指示の下で使用してください。

本コマンドと l2-trace コマンドを同時に実行することは出来ません。

L7 負荷分散パケットトレースを開始するには *packet-trace* コマンドを使用します。

```
adm(config)# packet-trace on [ { deny | permit } ip <ip-address> ]
adm(config)# packet-trace on [ { deny | permit } port <num> ]
adm(config)# packet-trace on [ { deny | permit } ip <ip-address> por
t <num> [ and-policy | or-policy ] ]
adm(config)# packet-trace off
```

■ *on/off*

パケットトレースを開始する場合は *on* を、停止する場合は *off* を指定してください。
パケットトレースを停止した時点でキャプチャデータを圧縮して内部ディスクに保存するため、トレースの停止処理が完了するまで数十秒～1 分程度の時間を要する場合があります。

■ *deny/permit*

任意のルールでフィルタリングする場合、フィルタールールの適用方法を選択します。
deny の場合、任意のフィルタールールに合致しないパケット情報のみキャプチャファイルに保存します。
permit の場合、任意のフィルタールールに合致するパケット情報のみキャプチャファイルに保存します。
フィルタールールを指定しない場合省略します。

■ *ip/port*

フィルタールールとして、IP アドレスかポート番号、またはその両方の組み合わ

せを 1 パターンだけ定義することが可能です。
IP アドレス、ポート番号ともに送信元、宛先情報の両方を検索対象とします。

■*and-policy/or-policy*
IP アドレスとポート番号の両方をフィルタールールに含める場合、二つのフィルター情報の組み合わせ条件を指定することができます。
AND 条件であれば *and-policy*、OR 条件であれば *or-policy* を指定します。
省略された場合、AND 条件が適用されます。

一度に取得可能なキャプチャデータは最大 1.5GB であり、最大サイズを取得するとトレース機能は自動で停止します。ただし、自動停止された状態では、採取したキャプチャデータをダウンロードすることはできません。
自動停止された場合においても、*packet-trace off* コマンドを実施してください。

L7 トレース機能の状態は *show packet-trace-state* コマンドで確認することができます。
show packet-trace-state コマンドの詳細は
「SX-3990_3950_3945_3940_3920 コマンドリファレンス」（別紙）を参照してください。

保存したキャプチャデータは、WEB 管理画面からダウンロードすることが可能です。詳しくは「3.34.4 L2/L7 トレース情報」を参照してください。
また、テクニカルサポートファイルにも取得したキャプチャデータを格納します。
テクニカルサポートファイルの取得方法は「5.8異常があった時」を参照してください。

5.3.4 L2 トレース機能

本装置には、解析用の機能として L2 パケットに関するパケットトレースを実施し、キャプチャデータを生成する機能があります。

⚠ 注意 本コマンドは使い方によって disk の消耗速度を早める危険性があります。
必ず、弊社技術サポートエンジニアの指示の下で使用してください。

本コマンドと packet-trace コマンドを同時に実行することは出来ません。

L2 パケットトレースを開始するには *l2-trace* コマンドを使用します。

```
adm(config)# l2-trace on { rx | tx } ethernet <port-num>
adm(config)# l2-trace on permit ip [<ip-address>] ethernet <port-num
>
adm(config)# l2-trace off
```

■*on/off*

パケットトレースを開始する場合は *on* を、停止する場合は *off* を指定してください。
パケットトレースを停止した時点でキャプチャデータを圧縮して内部ディスクに保存するため、トレースの停止処理が完了するまで数十秒～1 分程度の時間を要する場合があります。

■*rx/tx*

rx の場合、受信パケット情報のみキャプチャファイルに保存します。
tx の場合、送信パケット情報のみキャプチャファイルに保存します。
省略された場合、送受信 L2 パケット情報をキャプチャファイルに保存します。

■*ip <ip-address>*

IP アドレスでフィルターリングしたい場合、任意のアドレスを入力します。 送信元アドレス、宛先アドレスのいずれも検索対象となります。
Iアドレスが省略された場合、全ての IP パケット情報をキャプチャファイルに保存します。

■*ethernet <port-num>*

パケットトレースを行うイーサネットポートのポート番号を入力します。

一度に取得可能なキャプチャデータは最大 1.5GB であり、最大サイズを取得するとトレース機能は自動で停止します。ただし、自動停止された状態では、採取したキャプチャデータをダウンロードすることはできません。
自動停止された場合においても、*l2-trace off* コマンドを実施してください。

L2 トレース機能の状態は *show packet-trace-state* コマンドで確認することができます。
show packet-trace-state コマンドの詳細は
「SX-3990_3950_3945_3940_3920 コマンドリファレンス」（別紙）を参照してください。

保存したキャプチャデータは、WEB 管理画面からダウンロードすることが可能です。詳しくは「3.34.4 L2/L7 トレース情報」を参照してください。
また、テクニカルサポートファイルにも取得したキャプチャデータを格納します。
テクニカルサポートファイルの取得方法は「5.8異常があった時」を参照してください。

5.3.5 WEB 管理画面表示用設定ファイル

本製品の WEB 管理画面は、ユーザーの設定ポリシーに合わせて任意の項目のみを表示させる事ができます。(詳しくは「3.6画面カスタマイズ機能」を参照してください)

各画面項目は画面表示用の設定ファイルにて、その状態が保管されています。たとえば、VLAN 設定画面にある VLAN ID 入力テーブルの表示状態を変更した場合、以下のように設定行が変更されます。

```
nw-vlan-id on     ; 表示状態
  ↓
nw-vlan-id off    ; 非表示状態
```

以下に、当該設定ファイルの各設定行と対応する項目名の定義を明記します。

ネットワーク		
	VLAN	
		VLAN 選択 / nw-vlan-select {on | off}
		VLAN ID / nw-vlan-id {on | off}
		VLAN 名 / nw-vlan-basic {on | off}
		IPv4 管理 IP アドレス / nw-vlan-ip-v4 {on | off}
		IPv6 管理 IP アドレス / nw-vlan-ip-v6 {on | off}
		冗長構成関連項目設定 / nw-vlan-vrrp {on | off}
		仮想 IP アドレス設定 / nw-vlan-redundant {on | off}
		ルーター広告設定 / nw-vlan-rtadv {on | off}
		MTU 設定 / nw-vlan-mtu {on | off}
		ルート ID 設定 / nw-vlan-route_id {on | off}
	イーサネット	
		ポート種別選択 / nw-eth-type-select {on | off}
		イーサネットポート選択 / nw-eth-port-select {on | off}
		論理チャネル選択 / nw-eth-channel-select {on | off}
		設定情報の編集 ※イーサネットポート用 / nw-eth-port-settings {on | off}
		設定情報の編集 ※論理チャネル用 / nw-eth-channel-settings {on | off}
	ポートミラーリング	
		ミラーポート、モニタリングポート / nw-monitoring {on | off}

選択	
インターフェイス停止/起動	
イーサネットポートの有効/無効選択	nw-shutdown {on | off}
スパニングツリー	
スパニングツリー設定	nw-stp {on | off}
MAC テーブル	
静的 MAC アドレスエントリー設定	nw-mac-table {on | off}
動的エントリー保持時間設定	nw-mac-aging {on | off}
ARP テーブル	
ARP アドレステーブル設定	nw-arp-table {on | off}
動的エントリー保持時間設定	nw-arp-aging {on | off}
NDP テーブル	
静的 NDP エントリー設定	nw-ndp-table {on | off}
ルーティングテーブル	
ルーティングテーブル設定	nw-routing-table {on | off}
パケットフィルタリング	
IP アクセスリスト	
IPv4 アクセスリスト選択	nw-v4acl-select {on | off}
IPv4 アクセスリスト名	nw-v4acl-name {on | off}
IPv4 アクセスリスト設定	nw-v4acl-rule {on | off}
IPv6 アクセスリスト	
IPv6 アクセスリスト選択	nw-v6acl-select {on | off}
IPv6 アクセスリスト名	nw-v6acl-name {on | off}
IPv6 アクセスリスト設定	nw-v6acl-rule {on | off}
MAC アクセスリスト	
MAC アクセスリスト選択	nw-macl-select {on | off}
MAC アクセスリスト名	nw-macl-name {on | off}
MAC アクセスリスト編集	nw-macl-settings {on | off}
IP パケットフィルター起動	
IPv4 パケットフィルター起動	nw-ip4filter-start {on | off}
IPv6 パケットフィルター起動	nw-ip6filter-start {on | off}
MAC パケットフィルター起動	
MAC パケットフィルター起動	nw-macfil-start {on | off}

冗長構成		
	VRRP	
		VRRP 設定 sync-vrrp-settings {on | off}
		リンク状態監視設定 sync-track {on | off}
	情報同期実行	
		情報同期実行 sync-session-config {on | off}
	強制バックアップ	
		強制バックアップ sync-force-backup {on | off}
	同期設定	
		コマンド同期設定 sync-command-settings {on | off}
		セッション同期設定 sync-session-settings {on | off}
SSL		
	SSL 証明書	
		SSL ポリシー設定 ssl-create {on | off}
	証明書失効リスト	
		証明書失効リスト ssl-crl {on | off}
	プロキシサーバー	
		プロキシサーバー設定 ssl-proxy {on | off}
	SSL 証明書署名要求	
		CSR（署名要求）設定 ssl-csr {on | off}
	SSL インポート	
		ファイル選択 ssl-import {on | off}
	SSL エクスポート	
		ファイル選択 ssl-export {on | off}
	鍵、証明書の削除	
		ファイル選択 ssl-del {on | off}
バランシング		
	実サーバー	
		実サーバー設定
			実サーバー設定 slb-real {on | off}
			sorry コンテンツインポート slb-sorry-import {on | off}
			sorry コンテンツ参照 slb-sorry-disp {on | off}
	NAT プール	
		NAT プール
			NAT プール選択 slb-npool-select {on | off}

NAT プール名	slb-npool-name {on | off}
NAT プールアドレス設定	slb-npool-addr {on | off}
仮想サーバー	
仮想サーバー	
仮想サーバーID 選択	slb-virtid-select {on | off}
仮想サーバーID 設定	slb-virtid-settings {on | off}
仮想サーバー基本設定	slb-vserver-basic {on | off}
ソース NAT フィルター設定	slb-snat-filter {on | off}
バインド ID 登録（バインドグループ登録）	slb-bind-group {on | off}
バインド ID 登録(IP アドレス負荷分散)	slb-bind-id-ip {on | off}
バインド ID 登録(URL スイッチング)	slb-bind-id-url {on | off}
実サーバーバインド設定	slb-bind {on | off}
URL リダイレクト設定	slb-redirect {on | off}
403 応答設定	slb-forbid {on | off}
ルート ID 設定	slb-route_id {on | off}
URL スイッチングルール設定	
URL スイッチングルール設定	slb-usw-rule {on | off}
URL スイッチングルール組み合わせ	slb-usw-nest {on | off}
location ルール	
location ルール設定	slb-location-rule {on | off}
仮想サーバーグループ	
仮想サーバーグループ設定	slb-virt-group {on | off}
リバース NAT	
リバース NAT 選択	slb-revnat-select {on | off}
リバース NAT エントリー登録	slb-revnat-entry {on | off}
リバース NAT 登録	slb-revnat-bind {on | off}
リバース NAT 基本設定	slb-revnat-basic {on | off}
仮想サーバー 有効/無効	
仮想サーバー 有効/無効	slb-enable {on | off}
ping 許可	
ping 許可	slb-alowping {on | off}

SSL アクセラレーション		
	SSL アクセラレーション	
		仮想サーバーID 選択 / slb-virtid-ssl-select {on | off}
		SSL セッションタイムアウト / slb-ssl-timer {on | off}
		SSL3.0 有効/無効 / slb-sslv3-enable {on | off}
		SSL 証明書の割り当て / slb-ssl-assign {on | off}
		SSL アクセラレーション詳細設定 / slb-ssl-advanced-setting {on | off}
	ネットワーク	
		バランシングポート定義
		バランシングポート定義（イーサネットポート） / slb-eth-role {on | off}
		バランシングポート定義（論理ポート） / slb-chan-role {on | off}
ヘルスチェック		
	ヘルスチェック設定	
		ヘルスチェック選択 / probe-select {on | off}
		ヘルスチェックコピー / probe-copy {on | off}
		ヘルスチェック対象サーバー / probe-set-server {on | off}
		ヘルスチェック詳細設定 / probe-advanced-setting {on | off}
		ヘルスチェック一括設定
		ヘルスチェック対象サーバー / probe-set-server-bulk {on | off}
		ヘルスチェック詳細設定 / probe-advanced-setting-bulk {on | off}
		ヘルスチェック組み合わせ設定
		ヘルスチェックデータ参照 / probe-nest-show {on | off}
		ヘルスチェック組み合わせ設定 / probe-nest-settings {on | off}
		ヘルスチェック 有効/無効
		ヘルスチェック 有効/無効 / probe-enable {on | off}
システム		
	ネットワーク	
		IP アドレス名の定義
		IP アドレス名設定 / sys-ipname {on | off}
		SNMP 設定

SNMP マネージャー設定	sys-snmp-host {on | off}
コミュニティー	sys-snmp-commu {on | off}
コンタクト	sys-snmp-contact {on | off}
ロケーション	sys-snmp-location {on | off}
SNMP トラップトリガー設定	sys-snmp-trigger {on | off}
SYSLOG 設定	
SYSLOG 関連設定	sys-logging {on | off}
ログメール関連設定	sys-mail {on | off}
NATLOG 設定	
NATLOG 関連設定	sys-natlog {on | off}
DNS サーバー	
DNS サーバー設定	sys-dns {on | off}
NTP サーバー	
NTP サーバー設定	sys-ntp {on | off}
NTP サーバー設定 2	sys-restrict {on | off}
ユーザー管理	
ユーザーアカウント	
ユーザーアカウントの追加	sys-add-account {on | off}
ユーザーアカウントの削除	sys-del-account {on | off}
パスワード変更	
パスワード変更	sys-passwd {on | off}
リモートアクセス制御	
リモートアクセス制御	sys-remote {on | off}
HTTPS リダイレクト	sys-auto-redirect {on | off}
自動ログアウト	
自動ログアウト	sys-auto-logout {on | off}
機器管理	
ホスト名	
ホスト名	sys-hostname {on | off}
日時変更	
日時変更	sys-date {on | off}
設定インポート	
設定インポート	sys-import {on | off}
画面表示状態インポート	
画面表示状態インポート	sys-webdispconf-import {on | off}

設定エクスポート	
設定エクスポート	sys-export {on | off}
起動ファイル情報複製	
起動情報コピー	sys-copy {on | off}
ファームウェアアップデート	
ファームウェアアップデート	sys-upgrade {on | off}
システム停止	
システム停止	sys-halt {on | off}
再起動	
再起動	sys-reboot {on | off}
工場出荷時設定	
工場出荷時設定	sys-erase {on | off}
機器テスト	
PING テスト	
PING 実行	sys-ping-test {on | off}
SYSLOG テスト	
ログ出力テスト	sys-logging-test {on | off}
TRACEROUTE テスト	
TRACEROUTE 実行	sys-traceroute-test {on | off}

5.4 機器情報の参照

本製品の設定や動作状況を確認するには、CLI 上で show コマンドを使用するか、WEB 管理画面から「機器情報」画面を参照します。
本章では、本製品の設定情報やネットワークに関する統計情報、リアルタイム情報について、その参照方法を説明します。

5.4.1 設定情報の参照

show コマンドで現在の設定情報（running-config）を確認するには show running-config コマンドを使用します。

```
netwiser> show running-config
# Netwiser SX-3950 v6.90.81
!
hostname netwiser
allow-ping
!
sync config
sync session
sync startup-session
!
user-mgmt adm permission admin
!
--More--(byte 142)
```

また、show running-config コマンドに所定のパラメーターを指定することで、任意の設定のみを表示させることが可能です。
以下の例では VLAN 設定のみを表示させます。

```
netwiser(config)# show running-config interface vlan
!
interface vlan 1
 name default
 ip address 10.208.10.90/23
 no ip redundant-address
 ip virtual-address virt_1
 mtu 1500
 no rtadv
 vrrp vrid 192
 no vrrp backup-l2forward
!
interface vlan 10
```

```
 ip address 172.16.1.101/24
 no ip redundant-address
 no ip virtual-address
 mtu 1500
 no rtadv
 vrrp vrid 193
 no vrrp backup-l2forward
!
```

show running-config コマンドの詳細は
「SX-3990_3950_3945_3940_3920 コマンドリファレンス」(別紙)を参照してください。

5.4.2 その他機器情報の参照

設定情報以外にも、負荷分散情報や統計情報、ARP テーブルなどの機器情報を ***show*** コマンドで確認することができます。
また、***show*** コマンドで参照できる統計値やテーブルエントリーの一部は、***clear*** コマンドで削除することが可能です。

以下、show コマンドの一覧を記載します。

show access-list ipv4	機器に適用されている IPv4 アクセスリストの一覧を表示します。
show access-list ipv6	機器に適用されている IPv6 アクセスリストの一覧を表示します。
show access-list mac	機器に適用されている MAC アクセスリストの一覧を表示します。
show access-list mgmt	機器に適用されている管理アクセスリストを表示します。
show arp	ARP キャッシュを表示します。 ***clear arp*** コマンドで、動的 ARP エントリーを削除できます。
show bind	仮想サーバーと、仮想サーバーにバインドされた実サーバーのコネクション情報を表示します。
show cert-update	SSL 証明書自動更新の進捗状況や各種統計情報を表示します。
show channel	論理チャネルの状態を表示します。
show content	システムにインポートした sorry コンテンツを表示します。 ***clear content*** コマンドで、任意の sorry コンテンツを削除できます。
show connection	負荷分散に関連するセッション情報の現在値とピーク値を表示します。
show ethernet	イーサネットポートの送受信パケット数の累積値を表示します。 ***clear statistics ethernet*** コマンドで、イーサネットの統計情報をクリアできます。
show forward	L2/L3 フォワーディングの統計情報を表示します。 ***clear statistics l2forward*** コマンドで、L2 フォワーディング、L2 フラッディングの

	統計情報をクリアできます。
show history	実行したコマンドの履歴を表示します。

show logging	機器のシステムログを表示します。 *clear logging* コマンドで、機器に保存されているシステムログを削除できます。
show login-session	現在のログインユーザーの一覧を表示します。 *clear login-session* コマンドで、現在ログインしている任意のユーザーを強制的にログアウトさせることができます。
show mac	MAC アドレステーブルを表示します。 *clear mac* コマンドで、動的 MAC テーブルエントリーを削除できます。
show nat-pool	NAT プールの統計情報を表示します。
show ndp	IPv6 近隣キャッシュを表示します。
show ntp	NTP サーバーとの同期状態を表示します。
show probe	サーバーヘルスチェックの状態を表示します。 *clear statistics probe* コマンドで、サーバーヘルスチェックに関連する統計情報をクリアできます。
show real	実サーバー毎の統計情報を表示します。 *clear statistics real* コマンドで、実サーバーが保持する統計情報をクリアできます。
show route	ルーティングテーブルを表示します。
show session	Layer4 セッションテーブルを表示します。 *clear statistics session* コマンドで、負荷分散に関する統計情報をクリアできます。
show socket	TCP/UDP セッションの接続状況を表示します。
show spanning-tree	スパニングツリーの状態を表示します。

show ssl	証明書の有効性を SSL ポリシー毎に表示し、同時に統計情報も表示します。また、ポリシー名を指定し、ファイルの内容を表示することもできます。 *clear statistics ssl* コマンドで、SSL アクセラレーションに関する統計情報をクリアできます。 また、*clear ssl-session* コマンドで、SSL アクセラレーション機能で生成した SSL セッション情報を削除できます。
show sticky	セッション維持情報テーブルを表示します。
show session-sync	冗長構成でのセッション情報の同期に関する統計情報を表示します。 *clear statistics session-sync* コマンドで、冗長構成での同期に関する統計情報をクリアできます。
show system	システムのリアルタイム統計情報を表示します。
show tech-support	本製品の技術サポートを受ける場合に必要となるファイルを取り出します。
show traffic	負荷分散に関連するトラフィック統計を表示します。
show version	フラッシュメモリーに保存されているファームウェアのバージョン情報を表示します。
show virtual	仮想サーバー毎の統計情報を表示します。 *clear statistics virtual* コマンドで、仮想サーバーが保持する統計情報をクリアできます。
show vlan	各 VLAN に所属するイーサネットポートや論理チャネルの一覧を表示します。
show vrrp	VRRP の状態や関連する統計情報を表示します。 *clear statistics vrrp* コマンドで、VRRP に関連する統計情報をクリアできます。

show コマンドのパラメーターや表示内容の詳細は
「SX-3990_3950_3945_3940_3920 コマンドリファレンス」(別紙)を参照してください。

[WEB 管理画面]

場所： 機器情報

[機器情報]メニューの各画面では、システム情報や負荷分散状況を表示することができます。また、機器情報画面には「更新ボタン」や「データのクリア」ボタンがあります。

■更新ボタン

表示は、画面にアクセスがあった時点での情報です。情報を更新するには、再度画面に入り直すか、「更新ボタン」をクリックします。

■データのクリア

データによっては、統計情報をクリアする事が可能です。それらの統計情報を表示する画面には、「データのクリア」ボタンがあります。

画面に表示中の統計情報を一旦クリアしたい場合、「データのクリア」ボタンをクリックします。

5.5 CLI エラーメッセージ

本製品のコマンドラインインターフェイス上に出力されるエラーメッセージとエラー番号の一覧を、以下に列挙します。

No.	エラーメッセージ / 説明
0001E	access-list <str>: No such settings.
	access-list 設定モードの情報が取得できません。 '*exit*' コマンドを実施して、access-list 設定モードに入り直してください。
0002E	Operator is valid only for TCP/UDP rule.
	フィルタリングルールにポート番号を使用する場合、プロトコルに TCP、または UDP を指定してください。
0003E	<num>: out of range(1-65535).
	送信元、または宛先ポート番号に、規定外の値が入力されました。 ポート番号は 1-65535 の範囲で設定してください。
0004E	<num>: Unknown port.
	送信元、または宛先ポート番号に、規定外の値が入力されました。 ポート番号は 1-65535 の範囲で設定してください。
0005E	<num>: out of range(0-65534).
	送信元、または宛先ポート番号に、規定外の値が入力されました。 ポート番号範囲指定の開始値は、0-65534 の範囲で設定してください。
0006E	<num>: out of range(1-65535).
	送信元、または宛先ポート番号に、規定外の値が入力されました。 ポート番号範囲指定の終了値は、1-65535 の範囲で設定してください。
0007E	<num>: Unknown port.
	送信元、または宛先ポート番号に、規定外の値が入力されました。 ポート番号は 1-65535 の範囲で設定してください。

0008E	<num>: 2nd port must be greater than 1st one.
	送信元、または宛先ポート番号に、規定外の値が入力されました。 ポート番号範囲指定の終了値は、ポート番号範囲指定の開始値より大きい値で設定してください。
0009E	<num>: out of range(0-32).
	アドレス形式文字列に誤りがあるか、マスク長に規定外の値が入力されました。 ネットワークアドレスは<ip-addr/len>のように入力します。 （例：192.168.1.0/24） IPv4 アドレスのマスク長は 0-32 の範囲で設定してください。
0010E	<num>: out of range(0-128).
	アドレス形式文字列に誤りがあるかプレフィックス長に規定外の値が入力されました。 ネットワークアドレスは<ip-addr/len>のように入力します。 （例：fd:80:701::/64） IPv6 アドレスのプレフィックス長は 0-128 の範囲で設定してください。
0011E	<str>: invalid address.
	アドレス形式文字列に誤りがあります。 IP アドレス、またはネットワークアドレス（例：192.168.1.0/24）形式で入力してください。 また、文字列"any"は、全てのアドレスを意味します。 IP 名の使用はできません。
0012E	too many rules.
	アクセスリストに登録されているフィルタリングルール数が登録限度に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0013E	line number exhausted.
	規定値を超えてしまうため、フィルタリングルール番号の自動割り振りに失敗しました。 第一パラメーター'*line*'を省略せず、任意のルール番号（1-65535）を指定したうえでフィルタリングルールを登録してください。

0014E	<num>: out of range(0-255). プロトコルをプロトコル番号で指定する場合、0-255 の範囲で設定してください。
0015E	<str>: Unknown protocol. 規定外のプロトコル文字列が入力されました。 入力値を確認してください。
0016E	<str>: Can not use this protocol in IPv4. IPv4 アクセスリストのフィルタリングルールでは、プロトコルに icmpv6 を指定することはできません。
0017E	Type is valid only for ICMP rule. プロトコルに icmp が指定されていなければ、ICMP タイプを指定する事はできません。
0018E	<num>: out of range(0-255). ICMP タイプを番号で指定する場合、0-255 の範囲で設定してください。
0019E	<str>: Unknown icmp type. 規定外の ICMP タイプ文字列が入力されました。 もう一度入力値を確認してください。
0020E	parameter 'log' is valid when the deny rules settings. フィルタリングルールの登録に失敗しました。 'log'オプションは、アクセス許可設定の際には指定できません。
0021E	Settings already exists. フィルタリングルールの登録に失敗しました。 登録した設定は既に存在します。 全てのアクセスを拒否するフィルタリングルールは、デフォルトでアクセスリストの最後尾(行番号 65535)に登録されています。 もう一度設定内容や入力値を確認し、やり直してください。
0022E	too many rules. アクセスリストに登録されているフィルタリングルール数が登録限度に達しています。 設定を追加する場合は、既存の設定情報を削除してください。

0023E	line number exhausted. 規定値を超えてしまうため、フィルタリングルール番号の自動割り振りに失敗しました。 第一パラメーター'*line*'を省略せず、任意のルール番号（1-65535）を指定したうえでフィルタリングルールを登録してください。
0024E	<num>: out of range(0-255). プロトコルをプロトコル番号で指定する場合、0-255 の範囲で設定してください。
0025E	<str>: Unknown protocol. 規定外のプロトコル文字列が入力されました。 入力値を確認してください。
0026E	<str>: Can not use this protocol in IPv6. IPv6 アクセスリストのフィルタリングルールでは、プロトコルに icmp を指定することはできません。
0027E	Type is valid only for ICMPv6 rule. プロトコルに icmpv6 が指定されていなければ、ICMP タイプを指定する事はできません。
0028E	<num>: out of range(0-255). ICMP タイプを番号で指定する場合、0-255 の範囲で設定してください。
0029E	<str>: Unknown icmp type. 規定外の ICMP タイプ文字列が入力されました。 入力値を確認してください。
0030E	parameter 'log' is valid when the deny rules settings. フィルタリングルールの登録に失敗しました。 'log'オプションは、アクセス許可設定の際には指定できません。
0031E	Settings already exists. フィルタリングルールの登録に失敗しました。 登録した設定は既に存在します。 全てのアクセスを拒否するフィルタリングルールは、デフォルトでアクセスリストの最後尾(行番号 65535)に登録されています。 もう一度設定内容や入力値を確認し、やり直してください。

0032E	<num>: out of range(1-65534). フィルタリングルールの行番号は 1-65534 の範囲で設定してください。
0033E	<str>: Settings already exists. フィルタリングルールの登録に失敗しました。 指定された行番号は既に登録されています。
0034E	<str>: No such settings. フィルタリングルールの削除に失敗しました。 設定は存在しません。 設定内容や入力値を、もう一度確認してください。
0035E	<str>: Settings already exists. フィルタリングルールの登録に失敗しました。 指定された行番号は既に登録されています。
0036E	<str>: No such settings. フィルタリングルールの削除に失敗しました。 設定は存在しません。 設定内容や入力値を、もう一度確認してください。
0037E	<str>: parameter error. アクセスリスト設定モードへの遷移に失敗しています。 exit コマンドで、一旦特権モード(config モード)から遷移し直してください。
0038E	invalid address. 不正なネットワークアドレス形式を検出しました。 もう一度入力値を確認してください。
0039E	<str>: invalid address. 不正なネットワークアドレス形式を検出しました。 もう一度入力値を確認してください。
0040E	<str>: invalid address. 不正なアドレス形式を検出しました。 もう一度入力値を確認してください。

0041E	invalid address. 不正なアドレス形式を検出しました。 もう一度入力値を確認してください。
0042E	invalid address. v6 プレフィックスのアドレス指定は許可されません。 ネットワークアドレス形式で指定してください。
0043E	invalid address. 不正なアドレス形式（マスクアドレス）を検出しました。 もう一度入力値を確認してください。
0044E	Address already in use. 入力した管理 IP アドレスは、既に仮想サーバーIP アドレスとして使用されているアドレスです。 設定内容や入力値を、もう一度確認してください。
0045E	Address already in use. 入力した管理 IP アドレスは、既に管理 IP アドレスとして使用されているアドレスです。 もう一度入力値を確認してください。
0046E	Address already in use. 入力した管理 IP アドレスは、既に管理 IP アドレスとして使用されているアドレスです。 もう一度入力値を確認してください。
0047E	Network address already in use. 入力したネットワークアドレスと同一ネットワークアドレスが既に登録済みです。 もう一度入力値を確認してください。
0048E	Address already in use. 入力した管理 IP アドレスは、既に管理 IP アドレスとして使用されているアドレスです。 もう一度入力値を確認してください。
0049E	Network address already in use. 入力したネットワークアドレスと同一ネットワークアドレスが既に登録済みです。 もう一度入力値を確認してください。

0050E	can not delete the address. please delete the vrrp settings on this vlan. VLAN に VRID が設定されている状態で、ip address の削除はできません。 "no vrrp vrid"コマンドで、VRID 設定を削除してから、管理 IP アドレスを削除してください。
0051E	No such settings. (mask length unmatch) 入力したネットワークアドレス設定は存在しません。 マスク長が間違っています。
0052E	No such settings. (ip address unmatch) 入力した IP アドレス設定は存在しません。 入力値を確認してください。
0053E	No such settings. (prefix length unmatch) 入力したネットワークアドレス設定は存在しません。 プレフィックス長が間違っています。
0054E	No such settings. (ip address unmatch) 入力した IP アドレス設定は存在しません。 入力値を確認してください。
0055E	ip virtual-address settings is exist on this vlan. 仮想サーバーIP アドレスが設定されている VLAN の管理 IP アドレスは削除できません。 仮想サーバーIP アドレス設定を削除してからやり直してください。
0056E	ip redudant-address settings is exist on this vlan. 管理 IP アドレスの削除に失敗しました。 VRRP マスターIP アドレス(redundant-address)が設定されている VLAN の管理 IP アドレスは、削除できません。 VRRP マスターIP アドレス(redundant-address)設定を削除してからやり直してください。

0057E	can not modify the same network vlan ip as the peer-address. 管理 IP アドレスの削除に失敗しました。 この VLAN は、冗長構成の同期用 VLAN として使用されています。 同期用に使用されている VLAN の管理 IP アドレスは削除することができません。
0058E	this vlan network and peer-address is must be same network address. 管理 IPv4 アドレスの削除に失敗しました。 この VLAN は、冗長構成の同期用 VLAN として使用されています。 同期用に使用されている VLAN の管理 IP アドレスを変更する場合は、同一ネットワークアドレス内での変更でなければなりません。 VRRP 設定モードの'peer-address'コマンドで、冗長相手先 IP アドレスを別 VLAN のネットワークになるように変更するか、'no peer-address'コマンドで、冗長相手先 IP アドレスを削除してから、もう一度やり直してください。
0059E	this vlan network and peer-address is must be same network address. 管理 IPv6 アドレスの削除に失敗しました。 この VLAN は、冗長構成の同期用 VLAN として使用されています。 同期用に使用されている VLAN の管理 IP アドレスを変更する場合は、同一ネットワークアドレス内での変更でなければなりません。
0060E	vlan name already has been changed. please re-enter 'interface vlan' mode by typing 'inerface vlan {<new-name> | <vlan-id>}' in config mode. VLAN 名の変更があったにもかかわらず、VLAN 設定モードへ遷移し直していません。 exit コマンドを実行し、特権モード（config モード）からもう一度設定し直してください。
0061E	<str>: invalid address. 仮想サーバーIP アドレス設定の変更に失敗しました。 不正な IP アドレスを検出しました。 もう一度入力値を確認してください。

0062E	<str>: Settings already exists. 仮想サーバーIP アドレスの登録に失敗しました。 同一設定が既に存在しています。 もう一度入力値を確認してください。
0063E	<str>: Address already in use. 仮想サーバーIP アドレスの登録に失敗しました。 入力したアドレスは、管理 IP アドレスとして既に使用されています。 もう一度入力値を確認してください。
0064E	<str>: Address already in use. 仮想サーバーIP アドレスの登録に失敗しました。 入力したアドレスは、静的 ARP テーブルエントリーとして登録されています。 もう一度入力値を確認してください。
0065E	management IPv6 address not configured. 仮想サーバーIP アドレスの登録に失敗しました。 仮想サーバードレスに IPv6 を使用したい場合は、管理 IP アドレスに IPv6 アドレスを登録してください。
0066E	management IPv4 address not configured. 仮想サーバーIP アドレスの登録に失敗しました。 仮想サーバードレスに IPv4 を使用したい場合は、管理 IP アドレスに IPv4 アドレスを登録してください。
0067E	number of {ipv4|ipv6} virtual addresses cannot exceed 256. 仮想サーバーIP アドレスの登録に失敗しました。 IPv4（または IPv6）仮想サーバードレスは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0068E	<str>: No such settings. 仮想サーバーIP アドレスの削除に失敗しました。 入力された設定は存在しません。 もう一度入力値を確認してください。

0069E	<str>: Address already in use. 仮想サーバーIP アドレスの削除に失敗しました。 指定したアドレスは仮想サーバーとして使用されています。 'no virtual'コマンドで仮想サーバー設定を削除してから、もう一度やり直してください。
0070E	<str>: Address already in use. 仮想サーバーIP アドレスの削除に失敗しました。 指定したアドレスは NAT プールアドレスで使用されています。 NAT プール設定モードの'no ip address' コマンドで該当のプールアドレス設定を削除してから、もう一度やり直してください。
0071E	<str>: invalid address. VRRP マスターIP アドレスの変更に失敗しました。 入力したアドレス形式に誤りがあるか、存在しない IP 名を指定しています。 入力値を確認してください。
0072E	<str>: Settings already exists. VRRP マスターIP アドレスの登録に失敗しました。 入力したアドレスは VRRP マスターIP アドレスとして既に登録されています。 入力値を確認してください。
0073E	management IPv4 address not configured. VRRP マスターIP アドレスの登録に失敗しました。 VRRP マスターIP アドレスに IPv4 を使用したい場合は、管理 IP アドレスに IPv4 アドレスを登録してください。
0074E	management IPv6 address not configured. VRRP マスターIP アドレスの登録に失敗しました。 VRRP マスターIP アドレスに IPv6 を使用したい場合は、管理 IP アドレスに IPv6 アドレスを登録してください。
0075E	<str>: No such settings. VRRP マスターIP アドレスの削除に失敗しました。 入力された設定は存在しません。 もう一度入力値を確認してください。

0076E	<str>: Invalid access-list.(unmatch ip version)
	IPv6 アクセスリストが指定されたため、IPv4 アクセスフィルターの設定に失敗しました。 IPv4 アクセスフィルターを設定するには、IPv4 アクセスリストを指定してください。
0077E	<str>: Invalid access-list.(list empty)
	指定されたアクセスリストがルール未設定のアクセスリストであるため、IPv4 アクセスフィルターの設定に失敗しました。 フィルタリングルールが登録されたアクセスリストを指定してください。
0078E	<str>: Invalid access-list.(unmatch ip version)
	IPv4 アクセスリストが指定されたため、IPv6 アクセスフィルターの設定に失敗しました。 IPv6 アクセスフィルターを設定するには、IPv6 アクセスリストを指定してください。
0079E	<str>: Invalid access-list.(list empty)
	指定されたアクセスリストがルール未設定のアクセスリストであるため、IPv6 アクセスフィルターの設定に失敗しました。 フィルタリングルールが登録されたアクセスリストを指定してください。
0080E	<num>: out of range(<min>-<max>).
	MTU 値の変更に失敗しました。 MTU 値の範囲規定は、管理 IP アドレスに IPv6 アドレスが設定されているかどうかで変動します。 管理 IP アドレスに IPv6 アドレスが設定されている場合、1280-1500 の範囲で設定してください。 管理 IP アドレスに IPv6 アドレスが設定されていない場合、576-1500 の範囲で設定してください。
0081E	<str>: Settings already exists.
	VLAN 名の登録に失敗しました。 入力された名前は既に別 VLAN で登録されています。 入力値を確認してください。
0082E	<str>: invalid address.
	ルーター広告設定の登録に失敗しました。 プライマリーDNS アドレスのアドレス形式に誤りがあるか、存在しない IP 名を指定しています。 入力値を確認してください。

0083E	<str>: invalid address. ルーター広告設定の登録に失敗しました。 DNS アドレスは IPv6 アドレス形式で指定してください。
0084E	<str>: invalid address. ルーター広告設定の登録に失敗しました。 セカンダリーDNS アドレスのアドレス形式に誤りがあるか、存在しない IP 名を指定しています。 入力値を確認してください。
0085E	<str>: invalid address. ルーター広告設定の登録に失敗しました。 DNS アドレスは IPv6 アドレス形式で指定してください。
0086E	<num>: invalid argument. VRID の登録に失敗しました。 VRID は 1-255 の数値で入力してください。
0087E	<num>: out of range(1-255). VRID の登録に失敗しました。 VRID は 1-255 の範囲で設定してください。
0088E	management ip address not configured. VRID の登録に失敗しました。 VRID の登録を行うには、管理 IP アドレスが設定されている必要があります。
0089E	vrrp id not configured. バックアップ時 L2 フォワード設定の変更に失敗しました。 設定を変更するには、VRID が設定されている必要があります。
0090E	<num>: out of range(1-4094). VLAN ID の登録に失敗しました。 VLAN ID は 1-4094 の範囲で設定してください。

0091E	number of vlan IDs cannot exceed 128. VLAN ID の登録に失敗しました。 VLAN ID は登録可能な最大設定数に達しています。 設定を追加する場合は既存の VLAN 設定を削除してください。
0092E	Operation not permitted. VLAN の削除に失敗しました。 VLAN1（デフォルト VLAN）は削除することができません。
0093E	this vlan is in use by ethernet port. VLAN の削除に失敗しました。 この VLAN は現在イーサネットポートに割り当てられています。 イーサネット設定モードの vlan コマンドで、VLAN ID の割り当てを解除してから VLAN を削除してください。
0094E	Device busy. Virtual ip <str> is in use on virtual server. VLAN の削除に失敗しました。 この VLAN に登録されている仮想サーバーIP アドレスを使用した仮想サーバーが存在します。 '*no virtual*コマンドで仮想サーバーを削除しないと VLAN は削除できません。
0095E	Device busy. Virtual ip <str> is in use on nat-pool. VLAN の削除に失敗しました。 この VLAN に登録されている仮想サーバーIP アドレスをプールアドレスとして使用している NAT プール設定が存在します。 NAT プール設定モードの'*no ip address*' コマンドで該当のプールアドレス設定を削除してから、もう一度やり直してください。
0096E	can not delete the same network vlan ip as the peer-address network. VLAN の削除に失敗しました。 この VLAN は冗長構成の同期用 VLAN として使用しています。 VRRP 設定モードの'*peer-address*'コマンドで、冗長相手先 IP アドレスを別 VLAN のネットワークになるように変更するか、'*no peer-address*'コマンドで、冗長相手先 IP アドレスを削除してから、もう一度やり直してください。

0097E	<str>: No such settings. 仮想サーバー設定の登録に失敗しました。 入力されたサーバーID に誤りがあります。 入力値を確認してください。
0098E	Operation not supported. 仮想サーバー設定の登録に失敗しました。 仮想サーバープロトコル文字列に"ssl"は指定できません。 "tcp"を指定してください。
0099E	<str>: No such address on any vlan. 仮想サーバー設定の登録に失敗しました。 VLAN 設定モードの'*ip virtual-address*'コマンドで、仮想サーバーIP を登録してから、仮想サーバーの登録を実施してください。
0100E	<str>: Settings already exists. 仮想サーバー設定の登録に失敗しました。 入力された仮想サーバーID は登録済みです。 設定内容や入力値を、もう一度確認してください。
0101E	number of {ipv4|ipv6} virtual server cannot exceed 256. 仮想サーバー設定の登録に失敗しました。 IPv4（または IPv6）仮想サーバーは登録可能な最大設定数に達しています。 設定を追加する場合は既存設定を削除してください。
0102E	invalid port number. 仮想サーバーの登録に失敗しました。 プロトコルに ftp を指定する場合、ポート番号に 0 を設定することはできません。
0103E	virtual-server name already has been changed. please re-enter 'virtual' mode by typing 'virtual {<new-name> | <virtual-id>}' in config mode. 仮想サーバー名の変更があったにもかかわらず、仮想サーバー設定モードへ遷移し直していません。 *'exit'*コマンドを実行し、特権モード（config モード）からもう一度設定し直してください。

0104E	bind server cannot exceed 256 on system.
	実サーバーのバインドに失敗しました。 サーバーバインド数はシステムで登録可能な最大設定数に達しています。 設定を追加する場合は既存のバインドポリシーを削除してください。
0105E	total policies of bind and redirect cannot exceed 512 per virtual server ID.
	実サーバーのバインド設定、リダイレクト設定、403 応答設定は仮想サーバー毎に計 512 件までしか登録できません。 設定を追加する場合は既存設定を削除してください。
0106E	Operation not supported for non-HTTP servers.
	アクセスログ設定の登録に失敗しました。 アクセスログ設定は、UDP 仮想サーバーや FTP 仮想サーバーには設定できません。 設定内容や入力値を、もう一度確認してください。
0107E	access log is not available with DSR.
	アクセスログ設定の登録に失敗しました。 仮想サーバーが DSR 設定で動作しています。 アクセスログは DSR 設定との併用はできません。 もう一度入力値を確認してください。
0108E	<str>: invalid address.
	アクセスログ設定の登録に失敗しました。 不正なアドレスを検出しました。 もう一度入力値を確認してください。
0109E	invalid argument. <facility.level>: <16-23>.<0-7>
	アクセスログ設定の登録に失敗しました。 ファシリティーとレベルはドット(.)で繋ぎます。 もう一度入力値を確認してください。
0110E	invalid argument. <facility.level>: <16-23>.<0-7>
	アクセスログ設定の登録に失敗しました。 レベルは 0-7 の範囲で設定してください。

0111E	invalid argument. 　　<facility.level>: <16-23>.<0-7>
	アクセスログ設定の登録に失敗しました。 ファシリティーは 16-23 の範囲で設定してください。
0112E	<str>: No such file or derectory.
	ソーリーコンテンツ設定に失敗しました。 指定されたソーリーコンテンツが、存在しない、または内部エラーにより読み込めません。 ソーリーコンテンツがインポートされている事と、入力値が正しい事をもう一度確認してください。
0113E	L7 balancing is not available with dsr option.
	ソーリーコンテンツ設定に失敗しました。 仮想サーバーは DSR で動作しています。 ソーリーコンテンツ設定は DSR 設定と併用できません。 設定内容や入力値を、もう一度確認してください。
0114E	<str>: invalid address.
	実サーバーのバインドに失敗しました。 不正な実サーバーID が検出されました。 設定内容や入力値を、もう一度確認してください。
0115E	<str>: not equal to virtual server's proto.
	実サーバーのバインドに失敗しました。 バインドする実サーバーのプロトコルは、仮想サーバープロトコルと同じでなければいけません。 設定内容や入力値を、もう一度確認してください。
0116E	<str>: invalid address.
	実サーバーのバインドに失敗しました。 不正な実サーバーID が検出されました。 設定内容や入力値を、もう一度確認してください。

0117E	If you want to use the service port 0 of the server, virtual server protocol must be tcp or udp.
	実サーバーのバインドに失敗しました。 ポート番号 0 の実サーバーをバインドする場合、仮想サーバープロトコルが ftp であってはいけません。 設定内容や入力値を、もう一度確認してください。
0118E	<str>: No such settings.
	実サーバーのバインドに失敗しました。 指定された実サーバーは登録されていません。 設定内容や入力値を、もう一度確認してください。
0119E	If you want to use the service port 0 of the server, virtual server and real server must be same service port.
	実サーバーのバインドに失敗しました。 ポート番号 0 の実サーバーをバインドする場合、仮想サーバーのポート番号も 0 でなければいけません。 設定内容や入力値を、もう一度確認してください。
0120E	If you want to use the service port 0 of the server, virtual server and real server must be same service port.
	実サーバーのバインドに失敗しました。 ポート番号 0 の実サーバーをバインドする場合、仮想サーバーのポート番号も 0 でなければいけません。 設定内容や入力値を、もう一度確認してください。
0121E	group <num>: out of range(1-31).
	実サーバーのバインドに失敗しました。 グループ番号は 1-31 の範囲で設定してください。
0122E	weight <num>: out of range(0-255).
	実サーバーのバインドに失敗しました。 重みは 1-255 の範囲で設定してください。

0123E	L7 balancing is not available with dsr option. 実サーバーのバインドに失敗しました。 仮想サーバーは L7 バランシングの設定がされています。 DSR 設定は L7 バランシング設定と併用できません。 設定内容や入力値を、もう一度確認してください。
0124E	source-nat is not available with dsr option. 実サーバーのバインドに失敗しました。 仮想サーバーはソース NAT 設定がされています。 DSR 設定はソース NAT 設定と併用できません。 設定内容や入力値を、もう一度確認してください。
0125E	not equal to virtual server's port number. 実サーバーのバインドに失敗しました。 DSR 設定を有効にするには、バインドする実サーバーのポート番号と仮想サーバーのポート番号が等しくなければいけません。 設定内容や入力値を、もう一度確認してください。
0126E	dsr option ummatch. 実サーバーのバインドに失敗しました。 同一の実サーバーを複数のバインドグループに所属させる場合、DSR オプションの有無は統一されていなければいけません。 設定内容や入力値を、もう一度確認してください。
0127E	weight value unmatch. 実サーバーのバインドに失敗しました。 同一の実サーバーを複数のバインドグループに所属させる場合、重み付けの値は共通でなければいけません。 設定内容や入力値を、もう一度確認してください。
0128E	NATPT switch is not available with DSR. 実サーバーのバインドに失敗しました。 仮想サーバーには DSR 設定がされています。 IPv4<-->IPv6 変換設定は、DSR で動作する仮想サーバーには設定できません。 設定内容や入力値を、もう一度確認してください。

0129E	unmach tagged settings port1 and port2. 実サーバーのバインドに失敗しました。 イーサネットポートイーサネットポート 1 とイーサネットポート 2 のタグ VLAN 設定の有無が食い違っています。 フェイルスルー設定を行う場合、イーサネットポート 1 とイーサネットポート 2 のタグ VLAN 設定の有無を統一してください。
0130E	port<num> is settings spanning-tree. 実サーバーのバインドに失敗しました。 スパニングツリーが設定されている場合、フェイルスルーモードで動作させることはできません。 イーサネット設定モードからスパニングツリー設定を無効にしてから、フェイルスルー設定を行ってください。
0131E	port<num> is settings channel. 実サーバーのバインドに失敗しました。 論理チャネルリンクが存在する場合、フェイルスルーモードで動作させることはできません。 イーサネット設定モードから論理チャネル設定を無効にしてから、フェイルスルー設定を実施してください。
0132E	No such settings. 実サーバーバインド設定の解除に失敗しました。 実サーバーは一台もバインドされていません。 設定内容や入力値を、もう一度確認してください。
0133E	<str>: No such settings. 実サーバーバインド設定の解除に失敗しました。 指定された実サーバーはバインドされていません。 設定内容や入力値を、もう一度確認してください。
0134E	<str>: invalid address. ソース NAT フィルタリング設定の変更に失敗しました。 不正なアドレスを検出しました。 設定内容や入力値を、もう一度確認してください。

0135E	<str>: invalid address. ソース NAT フィルタリング設定の変更に失敗しました。 不正なアドレスを検出しました。 設定内容や入力値を、もう一度確認してください。
0136E	address family must be the same as virtual server address family. ソース NAT フィルタリング設定の変更に失敗しました。 フィルタリングルールに指定するアドレスは、仮想サーバードレスのアドレスファミリーと同じでなければいけません。 設定内容や入力値を、もう一度確認してください。
0137E	mask(or prefix) length must be larger than 0. ソース NAT フィルタリング設定の変更に失敗しました。 フィルタリングルールに指定するマスク長（またはプレフィックス長）に 0 を指定することはできません。 設定内容や入力値を、もう一度確認してください。
0138E	must be configured 'source-nat' settings before configuring the permit-nat-filter settings on this virtual server. ソース NAT フィルタリング設定の登録に失敗しました。 ソース NAT 設定がされていない仮想サーバーに、ソース NAT フィルタリングルールを登録することはできません。 'source-nat'コマンドでソース NAT 設定を実施してから、やり直してください。
0139E	Settings already exists. ソース NAT フィルタリング設定の登録に失敗しました。 同一設定が既に登録されています。 設定内容や入力値をもう一度確認してください。
0140E	number of nat-filter rules cannot exceed 256. ソース NAT フィルタリング設定の登録に失敗しました。 ソース NAT フィルタリング設定は、仮想サーバーに登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。

0141E	No such settings. ソース NAT フィルタリング設定の削除に失敗しました。 指定されたネットワークアドレスに合致するルールが存在しません。 設定内容や入力値をもう一度確認してください。
0142E	<str>: invalid address. IP アドレス負荷分散設定の変更に失敗しました。 不正なネットワークアドレスを検出しました。 入力値をもう一度確認してください。
0143E	<str>: invalid address. IP アドレス負荷分散設定の変更に失敗しました。 不正なネットワークアドレスを検出しました。 入力値をもう一度確認してください。
0144E	<str>: invalid address. IP アドレス負荷分散設定の変更に失敗しました。 不正なマスクアドレスを検出しました。 入力値をもう一度確認してください。
0145E	group <num>: out of range(1-31). IP アドレス負荷分散設定の変更に失敗しました。 グループ番号は 1-31 の範囲で設定してください。
0146E	Settings already exists. IP アドレス負荷分散設定の登録に失敗しました。 同一設定が既に登録されています。 設定内容や入力値をもう一度確認してください。
0147E	number of ip balancing policies cannot exceed 256. IP アドレス負荷分散設定の登録に失敗しました。 IP アドレス負荷分散設定は、仮想サーバー毎に設定できる最大登録数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。

0148E	No such settings. IP アドレス負荷分散設定の削除に失敗しました。 入力内容に合致するルールが存在しません。 設定内容や入力値をもう一度確認してください。
0149E	No such settings. IP アドレス負荷分散設定の削除に失敗しました。 入力内容に合致するルールが存在しません。 設定内容や入力値をもう一度確認してください。
0150E	Operation not supported for non-HTTP servers. URL スイッチンググループ ID 設定、または URL リダイレクト設定、または 403 応答設定のいずれかで、設定の変更に失敗しました。 これらの設定は TCP 仮想サーバーでなければ設定できません。 設定内容や入力値をもう一度確認してください。
0151E	URL switch is not available with DSR. URL スイッチンググループ ID 設定、または URL リダイレクト設定、または 403 応答設定のいずれかで、設定の変更に失敗しました。 これらの設定は DSR 設定がされている仮想サーバーに対して設定できません。 設定内容や入力値をもう一度確認してください。
0152E	<str>: No such settings. URL スイッチンググループ ID 設定、または URL リダイレクト設定、または 403 応答設定のいずれかで、設定の変更に失敗しました。 指定されたルールはシステムに登録されていません。 特権モードの'*rule*'コマンドを使用して、任意のルールを登録してください。
0153E	cannot specify more than 31 rules per virtual server. URL スイッチンググループ ID 設定、または URL リダイレクト設定、または 403 応答設定のいずれかで、設定の登録に失敗しました。 これらの設定は、全て合わせて仮想サーバー毎に 31 件までしか登録できません。 設定を追加する場合は、既存の設定情報を削除してください。

0154E	group <num>: out of range(1-31). URL スイッチンググループ ID 設定の登録に失敗しました。 グループ番号は 1-31 の範囲で設定してください。
0155E	<str>: invalid domain. URL リダイレクト設定の登録に失敗しました。 リダイレクト先のドメインの指定で、不正な文字列を検出しました。 ワイルドカード(*)は単体で使用し、他の文字列と組み合わせないでください。
0156E	domain name too long. URL リダイレクト設定の登録に失敗しました。 リダイレクト先のドメインで指定可能な文字列は最大 255 文字です。 もう一度入力値を確認してください。
0157E	<str>: invalid path. URL リダイレクト設定の登録に失敗しました。 URL パスに不正な文字列を検出しました。 ワイルドカード(*)は単体で使用し、他の文字列と組み合わせないでください。
0158E	url path too long. URL リダイレクト設定の登録に失敗しました。 URL パスで指定可能な文字列は最大 255 文字です。 もう一度入力値を確認してください。
0159E	<num>: out of range(1-65535). URL リダイレクト設定の登録に失敗しました。 リダイレクト先ポート番号は 1-65535 の範囲で設定してください。
0160E	<str>: No such settings. URL スイッチンググループ ID 設定、または URL リダイレクト設定、または 403 応答設定のいずれかで、設定の削除に失敗しました。 これらの設定は、仮想サーバーに登録されていません。 設定内容や入力値をもう一度確認してください。

0161E	UDP virtual server cannot setting predictor load. バランシングアルゴリズム設定の変更に失敗しました。 UDP 仮想サーバーに最小コネクション設定を登録することはできません。
0162E	<str>: No such settings. ソース NAT 設定に失敗しました。 指定された NAT ポリシーは存在しません。 設定内容や入力値をもう一度確認してください。
0163E	source nat is not available with DSR settings. ソース NAT 設定に失敗しました。 DSR 設定されている仮想サーバーに対してソース NAT を適用することはできません。 設定内容や入力値をもう一度確認してください。
0164E	<str>: file open error. クライアント CA 証明書ファイルの読み込みに失敗しました。 恐れ入りますが、一度クライアント CA 証明書を削除して、もう一度クライアント CA 証明書のインポートからやり直してください。
0165E	<str>: file close error. クライアント CA 証明書ファイルのクローズに失敗しました。 恐れ入りますが、一度クライアント CA 証明書を削除して、もう一度クライアント CA 証明書のインポートからやり直してください。
0166E	ssl acceleration is not available with DSR. SSL アクセラレーション設定に失敗しました。 DSR 設定がされている仮想サーバーに対して、SSL アクセラレーション設定はできません。
0167E	<str>: No such settings. SSL アクセラレーション設定に失敗しました。 指定された名前の SSL ポリシーが存在しません。 設定内容や入力値をもう一度確認してください。

0168E	ssl key file not found. SSL アクセラレーション設定に失敗しました。 指定した SSL ポリシーには SSL 鍵ファイルがインポートされていません。 SSL 鍵ファイルをインポートしてから設定し直してください。
0169E	ssl certificate file not found. SSL アクセラレーション設定に失敗しました。 指定した SSL ポリシーには SSL 証明書ファイルがインポートされていません。 SSL 証明書ファイルをインポートしてから設定し直してください。
0170E	Already bound ssl-policy for client-authentication. SSL アクセラレーション設定に失敗しました。 同じ仮想サーバーに対して、クライアント証明書がインポートされた SSL ポリシーを複数バインドすることはできません。 設定内容や入力値をもう一度確認してください。
0172E	number of bind ssl policies cannot exceed 32. SSL アクセラレーション設定に失敗しました。 SSL ポリシーのバインド設定は、仮想サーバーに登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0173E	invalid argument. (1m-365d) 不正なセッション維持タイムアウト値を検出しました。 セッション維持タイムアウト値は日付型の文字列で 1m-365d の範囲で設定してください。
0174E	out of range. (1m-365d) IP アドレスセッション維持設定、または SSL セッション維持設定のタイムアウト値が規定値の範囲外です。 1m-365d の範囲で設定してください。

0175E	Operation not supported sticky ssl on ftp or udp server.
	SSL セッション維持設定に失敗しました。 SSL セッション維持設定は tcp 仮想サーバーのみ設定可能です。 設定内容や入力値をもう一度確認してください。
0176E	ssl option cannot be used on virtual-server in a buddy group.
	SSL セッション維持設定に失敗しました。 この仮想サーバーは仮想サーバーグループに属しています。 SSL セッション維持設定を行う場合は、仮想サーバーグループから解除してください。
0177E	SSL sticky is not available with DSR.
	SSL セッション維持設定に失敗しました。 この仮想サーバーは DSR 設定で動作しています。 SSL セッション維持設定を行う場合は、バインドサーバーの DSR オプションを解除してください。
0178E	Operation not supported sticky cookie on ftp or udp server.
	cookie セッション維持設定に失敗しました。 cookie セッション維持設定は tcp 仮想サーバーのみ設定可能です。 設定内容や入力値をもう一度確認してください。
0179E	cookie option cannot be used on virtual-server in a buddy group.
	cookie セッション維持設定に失敗しました。 この仮想サーバーは仮想サーバーグループに属しています。 cookie 維持設定を行う場合は、仮想サーバーグループから解除してください。
0180E	cookie sticky is not available with DSR.
	cookie セッション維持設定に失敗しました。 この仮想サーバーは DSR 設定で動作しています。 cookie セッション維持設定を行う場合は、バインドサーバーの DSR オプションを解除してください。

0181E	cookie name length cannot exceed 256 characters.
	cookie セッション維持設定に失敗しました。 不正な cookie 名を検出しました。 cookie 名は 255 文字以内で設定してください。
0182E	invalid argument. (1m-365d)
	不正な cookie セッション維持設定のタイムアウト値を検出しました。 cookie セッション維持設定のタイムアウトは日付型の文字列で 1m-365d の範囲で設定してください。
0183E	<date>: out of range. (1m-365d)
	cookie セッション維持設定のタイムアウト値が規定の範囲外です。 1m-365d の範囲で設定してください。
0184E	invalid argument. (0s-365d)
	TCP セッションタイムアウト値が規定の範囲外です。 TCP セッションタイムアウトは 0s-365d の範囲で設定してください。
0185E	out of range. (0s-365d)
	TCP セッションタイムアウト値が規定の範囲外です。 TCP セッションタイムアウトは 0s-365d の範囲で設定してください。
0186E	Operation not supported for non-HTTP servers.
	ヘッダー挿入設定(X-Forwarded)に失敗しました。 ヘッダー挿入機能は、tcp 仮想サーバーにのみ設定可能です。 もう一度設定内容や入力値を確認してください。
0187E	header insert is not available with DSR.
	ヘッダー挿入設定(X-Forwarded)に失敗しました。 この仮想サーバーは DSR 設定で動作しています。 ヘッダー挿入設定を行う場合は、バインドサーバーの DSR オプションを解除してください。

0188E	URL is too long. クライアント認証失敗時処理設定の変更に失敗しました。 不正な URL 文字列を検出しました。 リダイレクト先に指定する URL 文字列は 512 文字以内で入力してください。
0189E	header length is too long. クライアント証明書ヘッダー挿入設定の登録に失敗しました。 不正なヘッダー名文字列を検出しました。 ヘッダー名文字列は 16 文字以内で入力してください。
0190E	<str>: cipher-expression is too long. 暗号スイート許可設定の変更に失敗しました。 不正な暗号スイート文字列を検出しました。 暗号スイート文字列は 256 文字以内で入力してください。
0191E	syntax error - <"cipher-expression"> is must be chained by comma(,). can not use the space. 暗号スイート許可設定の変更に失敗しました。 不正な暗号スイート文字列を検出しました。 暗号スイート文字列は、各暗号スイート文字列をカンマ(,)で繋ぎます。 また、文字列内にスペースは含めないでください。
0192E	<str>: Unknown suite. 暗号スイート許可設定の変更に失敗しました。 不正な暗号スイート文字列を検出しました。 もう一度入力値を確認してください。
0193E	<str>: Unknown suite. 暗号スイート許可設定の変更に失敗しました。 不正な暗号スイート文字列を検出しました。 もう一度入力値を確認してください。
0194E	header length is too long. SSL セッション ID ヘッダー挿入設定に失敗しました。 不正なヘッダー名文字列を検出しました。 ヘッダー名文字列は 16 文字以内で入力してください。

0195E	<str>: No such settings. SSL 設定モードの情報が取得できません。 exit コマンドを実施して、SSL 設定モードに入り直してください。
0196E	<num>: Invalid types. Please type '1024' or '2048' or '4096'. CSR の登録に失敗しました。 不正な鍵長が指定されました。 鍵長は 1024, 2048, 4096 のいずれかを指定してください。
0197E	failed create file. CSR の登録時に内部エラーが発生し、CSR ファイルの生成に失敗ました。 入力値を確認して、もう一度登録し直してください。
0198E	failed to sync key file. CSR の登録時に内部エラーが発生しました。 CSR の登録には成功しましたが、鍵ファイルのパスワード生成に失敗しました。 入力値を確認して、もう一度登録し直してください。
0199E	failed to sync key file. CSR の登録時に内部エラーが発生しました。 CSR の登録には成功しましたが、鍵ファイルの同期に失敗しました。 もう一度 CSR を登録し直すか、生成された鍵ファイルを取り出し、冗長相手へインポートしてください。
0200E	URL is too long. 証明書失効リスト設定の登録に失敗しました。 不正な URL 文字列を検出しました。 失効リストのダウンロード先に指定するURL 文字列は 512 文字以内で入力してください。
0201E	scheme not supported. 証明書失効リスト設定の登録に失敗しました。 不正な URL 文字列を検出しました。 URL 文字列は"http://"または"https://"で開始してください。

0202E	scheme not supported. 証明書失効リスト設定の登録に失敗しました。 不正な URL 文字列を検出しました。 URL 文字列は"http://"または"https://"で開始してください。
0203E	host is empty. 証明書失効リスト設定の登録に失敗しました。 不正な URL 文字列を検出しました。 ホストアドレス部が空になっています。 入力値を確認して、もう一度登録し直してください。
0204E	path is empty. 証明書失効リスト設定の登録に失敗しました。 不正な URL 文字列を検出しました。 URL パス部が空になっています。 入力値を確認して、もう一度登録し直してください。
0205E	path is empty. 証明書失効リスト設定の登録に失敗しました。 不正な URL 文字列を検出しました。 URL パスのアクセス先ファイルが指定されていません。 入力値を確認して、もう一度登録し直してください。
0206E	invalid argument. (0m-365d) CRL 更新間隔の指定に不正な文字列を検出しました。 日付型の文字列で 1m-365d の範囲で設定してください。
0207E	out of range. (0m-365d) CRL 更新間隔が規定の範囲外です。 1m-365d の範囲で設定してください。
0208E	reverse-nat <str>: No such settings. リバース NAT 設定モードの情報が取得できません。 exit コマンドを実施して、リバース NAT 設定モードに入り直してください。

0209E	<str>: invalid argument. リバース NAT バインド設定に失敗しました。 不正なサーバードレスを検出しました。 入力値を確認して、もう一度登録し直してください。
0210E	<num>: out of range. (0-65535) リバース NAT バインド設定に失敗しました。 不正な宛先ポート番号を検出しました。 宛先ポート番号は 1-65535 の範囲で設定してください。
0211E	number of reverse-nat bind policies cannot exceed 256. リバース NAT バインド登録に失敗しました。 リバース NAT エントリーにバインドされているサーバーID は、登録可能な最大設定数に達しています。 設定を追加する場合は既存の設定を削除してください。
0212E	Settings already exists. リバース NAT バインド登録に失敗しました。。 同一設定が既に存在しています。 もう一度入力値を確認してください。
0213E	No such settings. リバース NAT バインド削除に失敗しました。。 入力されたバインド設定は存在しません。 もう一度入力値を確認してください。
0214E	invalid argument. (0s-365d) リバース NAT コネクションタイマーの設定変更に失敗しました。 タイマー値は日付型の文字列で 0s-365d の範囲で設定してください。
0215E	out of range. (0s-365d) リバース NAT コネクションタイマーの設定変更に失敗しました。 タイムアウト値は 0s-365d の範囲で設定してください。

0216E	Argument list too long. ヘルスチェック組み合わせ設定の登録に失敗しました。 組み合わせ文字列に指定できるヘルスチェックポリシーは最大 4 つです。 もう一度入力値を確認してください。
0217E	<str>: No such settings. ヘルスチェック組み合わせ設定の登録に失敗しました。 入力されたヘルスチェックポリシーは存在しません。 もう一度設定内容や入力値を確認して、やり直してください。
0218E	nested probe cannot be used within "expression" of another nested probe. ヘルスチェック組み合わせ設定の登録に失敗しました。 入力されたヘルスチェックポリシーが、既に別の組み合わせヘルスチェック内で使用されている可能性があります。 設定内容をもう一度確認してください。 登録したい場合は、該当のヘルスチェック組み合わせ設定を削除してください。
0219E	invalid argument. ヘルスチェック組み合わせ設定の登録に失敗しました。 組み合わせ表現に誤りがあります。 組み合わせ表現文字列では、別に設定されたヘルスチェックポリシーを最大 4 つまで、論理演算'&&'と'||'を使用して組み合わせてください。演算子の前後にはスペースが必要です。 もう一度入力値を確認してください。
0220E	number of probe policies cannot exceed 1024. ヘルスチェック設定の登録に失敗しました。 ヘルスチェックポリシーは、登録可能な最大設定数に達しています。 設定を追加する場合は既存の設定を削除してください。
0221E	<num>: invalid address. ヘルスチェック設定の登録に失敗しました。 不正なサーバードレスを検出しました。 もう一度入力値を確認してください。

0222E	<num>: invalid address. ヘルスチェック設定の登録に失敗しました。 不正なサーバードレスを検出しました。 もう一度入力値を確認してください。
0223E	<num>: invalid address. ヘルスチェック設定の登録に失敗しました。 不正なサーバードレスを検出しました。 もう一度入力値を確認してください。
0224E	invalid argument. ヘルスチェック設定の登録に失敗しました。 不正なポート番号を検出しました。 もう一度入力値を確認してください。
0225E	<num>: out of range. (1-65535) ヘルスチェック設定の登録に失敗しました。 不正なポート番号を検出しました。 ポート番号は 1-65535 の範囲で設定してください。 もう一度入力値を確認してください。
0226E	probe <str>: No such settings. ヘルスチェック設定モードの情報が取得できません。 exit コマンドを実施して、ヘルスチェック設定モードに入り直してください。
0227E	invalid argument. DNS ヘルスチェック設定の登録に失敗しました。 不正なパラメーターを検出しました。 もう一度入力値を確認してください。
0228E	Protocol error. DNS ヘルスチェック設定の登録に失敗しました。 このヘルスチェックポリシーは、既に別のアプリケーションヘルスチェックとして登録されています。 DNS ヘルスチェック設定を実施する場合は、既存のアプリケーション設定を解除してからもう一度設定し直してください。

0229E	FQDN length too long. DNS ヘルスチェック設定の登録に失敗しました。 不正な FQDN 文字列を検出しました。 FQDN は 256 文字以内で入力してください。
0230E	probe <str>: No such settings. ヘルスチェック設定モードの情報が取得できません。 ‘*exit*’ コマンドを実施して、ヘルスチェック設定モードに入り直してください。
0231E	Protocol error. 設定の変更に失敗しました。 このヘルスチェックポリシーは、既に別のアプリケーションヘルスチェックとして登録されています。 設定を実施する場合は、既存のアプリケーション設定を解除してからもう一度設定し直してください。
0232E	probe <str>: No such settings. ヘルスチェック設定モードの情報が取得できません。 exit コマンドを実施して、ヘルスチェック設定モードに入り直してください。
0233E	Protocol error. 設定の変更に失敗しました。 このヘルスチェックポリシーは、既に別のアプリケーションヘルスチェックとして登録されています。 設定を実施する場合は、既存のアプリケーション設定を解除してからもう一度設定し直してください。
0234E	invalid argument. TSP ヘルスチェック設定の変更に失敗しました。 リクエストパラメーターに文字列が指定されていません。 もう一度入力値を確認してください。
0235E	request strings too long. TSP ヘルスチェック設定の変更に失敗しました。 リクエストパラメーターに指定する文字列長は最大で 256 文字までで入力してください。

0236E	<num>: out of range. (0-20)
	TSP ヘルスチェック設定の変更に失敗しました。 タイムスタンプの許容誤差は 1-20 の範囲で設定してください。
0237E	<num>: out of range. (0-2000000000)
	TSP ヘルスチェック設定の変更に失敗しました。 Nonce オプションで指定する値は 0-2000000000 の範囲で設定してください。
0238E	probe <str>: No such settings.
	ヘルスチェック設定モードの情報が取得できません。 ‘*exit*’コマンドを実施して、ヘルスチェック設定モードに入り直してください。
0239E	Protocol error.
	設定の変更に失敗しました。 このヘルスチェックポリシーは、既に別のアプリケーションヘルスチェックとして登録されています。 設定を実施する場合は、既存のアプリケーション設定を解除してからもう一度設定し直してください。
0240E	request strings too long.
	HTTP ヘルスチェック設定の変更に失敗しました。 HTTP リクエストパラメーターに指定できる文字列長は最大で 256 文字までです。 もう一度入力値を確認してください。
0241E	invalid argument.
	HTTP ヘルスチェック設定の変更に失敗しました。 不正な HTTP リクエスト文字列を検出しました。 もう一度入力値を確認してください。
0242E	bad status code.
	HTTP ヘルスチェック設定の変更に失敗しました。 不正なステータスコード文字列を検出しました。 ステータスコードは最大 4 パターンまで指定可能です。 数字は空白で区切ってください。また、値をハイフン(-)で連結すると範囲指定が可能になります。 必ず 3 桁の数字を使用してください。

0243E	bad status code. HTTP ヘルスチェック設定の変更に失敗しました。 不正なステータスコード文字列を検出しました。 ステータスコードは最大 4 パターンまで指定可能です。 数字は空白で区切ってください。また、値をハイフン(-)で連結すると範囲指定が可能になります。 必ず 3 桁の数字を使用してください。
0244E	bad status code. HTTP ヘルスチェック設定の変更に失敗しました。 不正なステータスコード文字列を検出しました。 ステータスコードは最大 4 パターンまで指定可能です。 数字は空白で区切ってください。また、値をハイフン(-)で連結すると範囲指定が可能になります。 必ず 3 桁の数字を使用してください。
0245E	bad status code. HTTP ヘルスチェック設定の変更に失敗しました。 不正なステータスコード文字列を検出しました。 ステータスコードは最大 4 パターンまで指定可能です。 数字は空白で区切ってください。また、値をハイフン(-)で連結すると範囲指定が可能になります。 必ず 3 桁の数字を使用してください。
0246E	response strings too long. HTTP ヘルスチェック設定の変更に失敗しました。 HTTP 応答文字列に指定できる文字列長は最大で 256 文字までです。 もう一度入力値を確認してください。
0247E	probe <str>: No such settings. ヘルスチェック設定モードの情報が取得できません。 ‘*exit*’ コマンドを実施して、ヘルスチェック設定モードに入り直してください。

0248E	Operation not supported for non-HTTP health-check policies.
	HTTP 接続維持設定の変更に失敗しました。 HTTP 接続維持設定は HTTP ヘルスチェックポリシーにしか設定できません。 もう一度設定内容を確認してください。
0249E	probe <str>: No such settings.
	ヘルスチェック設定モードの情報が取得できません。 ‘*exit*’コマンドを実施して、ヘルスチェック設定モードに入り直してください。
0250E	<num>: out of range. (0-255)
	Down 判定しきい値設定の変更に失敗しました。 Down 判定しきい値は 1-255 の範囲で設定してください。
0251E	probe <str>: No such settings.
	ヘルスチェック設定モードの情報が取得できません。 ‘*exit*’コマンドを実施して、ヘルスチェック設定モードに入り直してください。
0252E	invalid argument. (1s-255s)
	送信間隔設定で不正な値を検出しました。 送信間隔設定は日付型の文字列で 1s-255s の範囲で設定してください。
0253E	out of range. (1s-255s)
	送信間隔設定の変更に失敗しました。 送信間隔は 1s-255s の範囲で設定してください。
0254E	probe <str>: No such settings.
	ヘルスチェック設定モードの情報が取得できません。 ‘*exit*’コマンドを実施して、ヘルスチェック設定モードに入り直してください。
0255E	probe <str>: No such settings.
	ヘルスチェック設定モードの情報が取得できません。 ‘*exit*’コマンドを実施して、ヘルスチェック設定モードに入り直してください。
0256E	natpool <str>: No such settings.
	NAT プール設定モードの情報が取得できません。 ‘*exit*’コマンドを実施して、NAT プール設定モードに入り直してください。

0257E	<str>: invalid address. プールアドレスの登録に失敗しました。 範囲指定の開始アドレスで不正値を検出しました。 もう一度入力値を確認してください。
0258E	<str>: invalid address. プールアドレスの登録に失敗しました。 範囲指定の終了アドレスで不正値を検出しました。 もう一度入力値を確認してください。
0259E	Start IP and end IP is different IP type. プールアドレスの登録に失敗しました。 範囲指定の開始アドレスと終了アドレスで、異なるアドレスファミリーが使用されています。 もう一度入力値を確認してください。
0260E	<str>: invalid address. プールアドレスの登録に失敗しました。 プールアドレスで不正値を検出しました。 もう一度入力値を確認してください。
0261E	Can not set the IPv6 link-local address in nat-pool. プールアドレスの登録に失敗しました。 プールアドレスで不正値を検出しました。 プールアドレスに IPv6 リンクローカルアドレスを登録することはできません。
0262E	Settings already exists. プールアドレスの登録に失敗しました。 プールアドレスで不正値を検出しました。 入力されたアドレスは、既にプールアドレスとして登録されている可能性があります。 もう一度設定内容や入力値を確認して、設定し直してください。
0263E	No such settings. プールアドレスの削除に失敗しました。 入力されたプールアドレスは、NAT プールに登録されていません。
0264E	mac access-list <str>: No such settings. MAC アクセスリスト設定モードの情報が取得できません。 ‘*exit*’ コマンドを実施して、MAC アクセスリスト設定モードに入り直してください。

0265E	too many rules. MAC アクセスリストに登録されているフィルタリングルール数が登録限度に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0266E	line number exhausted. 規定値を超えてしまうため、フィルタリングルール番号の自動割り振りに失敗しました。 第一パラメーター'line'を省略せず、任意のルール番号（1-65535）を指定したうえでフィルタリングルールを登録してください。
0267E	<str>: invalid Ethernet address. フィルタリングルールの登録に失敗しました。 不正な送信元 MAC アドレスが入力されました。 もう一度入力値を確認してください。
0268E	<str>: invalid Ethernet address. フィルタリングルールの登録に失敗しました。 不正な宛先 MAC アドレスが入力されました。 もう一度入力値を確認してください。
0269E	parameter 'log' is valid when the deny rules settings. フィルタリングルールの登録に失敗しました。 '*log*'オプションは、アクセス許可設定の際には指定できません。 アクセス許可設定である場合にのみ、指定することができます。
0270E	Settings already exists. フィルタリングルールの登録に失敗しました。 登録した設定は既に存在します。 全てのアクセスを拒否するフィルタリングルールは、デフォルトでアクセスリストの最後尾(行番号 65535)に登録されています。 もう一度設定内容や入力値を確認し、やり直してください。
0271E	<num>: out of range. (1-65534) フィルタリングルールの登録に失敗しました。 フィルタリングルールの行番号は 1-65534 の範囲で設定してください。

0272E	Settings already exists. フィルタリングルールの登録に失敗しました。 指定された行番号は既に登録されています。
0273E	No such settings. フィルタリングルールの削除に失敗しました。 指定された行番号は存在しません。
0274E	failed to send data for config-sync. 内部エラーにより、コマンド同期用ソケットの生成に失敗しました。 自機器への設定変更は成功しましたが、コマンドの同期に失敗しています。 恐れ入りますが、一旦 exit コマンドで設定モードを抜け、特権モード（config モード）に入り直してください。
0275E	failed to execute command on peer machine. 設定の同期に失敗しました。 自機器への設定変更は成功しましたが、冗長相手へのコマンドの同期に失敗しています。 ・ Master/Backup 状態の切り替りが発生していませんか？ Master/Backup 状態の切り替りが発生した場合、再度特権モードに入り直す必要があります。 ・ 自機器と冗長相手機器の設定情報に矛盾がありませんか？ 「冗長先アドレス（peer アドレス）の設定や、VRID の設定が食い違っている」、または「冗長相手先に存在しない設定に対して削除設定を実施した」など、設定情報に矛盾がある場合、設定同期処理は失敗します。 ・ 最後に実行されたコマンドは正常に実行されましたか？ 正常にコマンド同期がされないまま（コマンド同期に失敗したまま）設定変更を続けた場合、同期先との接続が遮断されてしまう恐れがあります。 これらの理由、またはその他の何らかの理由により冗長相手との接続性が損なわれた可能性があります。 恐れ入りますが、冗長相手との接続性を確認してから、一旦 ***'exit'*** コマンドで設定モードを抜け、特権モード（config モード）に入り直して設定をやり直してください。

0276E	could not send commands to the peer machine. 設定の同期に失敗しました。 自機器への設定変更は成功しましたが、冗長相手へのコマンドの同期に失敗しています。 ・ Master/Backup 状態の切り替りが発生していませんか？ Master/Backup 状態の切り替りが発生した場合、再度特権モードに入り直す必要があります。 ・ 自機器と冗長相手機器の設定情報に矛盾がありませんか？ 「冗長先アドレス（peerアドレス）の設定や、VRID の設定が食い違っている」、または「冗長相手先に存在しない設定に対して削除設定を実施した」など、設定情報に矛盾がある場合、設定同期処理は失敗します。 ・ 最後に実行されたコマンドは正常に実行されましたか？ 正常にコマンド同期がされないまま（コマンド同期に失敗したまま）設定変更を続けた場合、同期先との接続が遮断されてしまう恐れがあります。 これらの理由、またはその他の何らかの理由により冗長相手との接続性が損なわれた可能性があります。 恐れ入りますが、冗長相手との接続性を確認してから、一旦 '*exit*' コマンドで設定モードを抜け、特権モード（config モード）に入り直して設定をやり直してください。

0277E	failed to execute command on peer machine. 設定の同期に失敗しました。 自機器への設定変更は成功しましたが、冗長相手へのコマンドの同期に失敗しています。 ・ Master/Backup 状態の切り替りが発生していませんか？ Master/Backup 状態の切り替りが発生した場合、再度特権モードに入り直す必要があります。 ・ 自機器と冗長相手機器の設定情報に矛盾がありませんか？ 「冗長先アドレス（peer アドレス）の設定や、VRID の設定が食い違っている」、「または冗長相手先に存在しない設定に対して削除設定を実施した」など、設定情報に矛盾がある場合、設定同期処理は失敗します。 ・ 最後に実行されたコマンドは正常に実行されましたか？ 正常にコマンド同期がされないまま（コマンド同期に失敗したまま）設定変更を続けた場合、同期先との接続が遮断されてしまう恐れがあります。 これらの理由、またはその他の何らかの理由により冗長相手との接続性が損なわれた可能性があります。 恐れ入りますが、冗長相手との接続性を確認してから、一旦 '*exit*' コマンドで設定モードを抜け、特権モード（config モード）に入り直して設定をやり直してください。

0278E	failed to execute command on peer machine. ** please re-enter 'config' mode by typing 'config' in normal mode. ** probably one of the following situation - failover (i.e. master <-> backup switching) occured. - local configuration state differs from the peer machine's. - the last synced command was not properly done.
	設定の同期に失敗しました。 自機器への設定変更は成功しましたが、冗長相手へのコマンドの同期に失敗しています。 ・ Master/Backup 状態の切り替りが発生していませんか？ Master/Backup 状態の切り替りが発生した場合、再度特権モードに入り直す必要があります。 ・ 自機器と冗長相手機器の設定情報に矛盾がありませんか？ 「冗長先アドレス（peerアドレス）の設定や、VRID の設定が食い違っている」、または「冗長相手先に存在しない設定に対して削除設定を実施した」など、設定情報に矛盾がある場合、設定同期処理は失敗します。 ・ 最後に実行されたコマンドは正常に実行されましたか？ 正常にコマンド同期がされないまま（コマンド同期に失敗したまま）設定変更を続けた場合、同期先との接続が遮断されてしまう恐れがあります。 これらの理由、またはその他の何らかの理由により冗長相手との接続性が損なわれた可能性があります。 また、このメッセージは冗長相手先アドレスの設定後にも出力されます。 恐れ入りますが、冗長相手との接続性を確認してから、一旦 '*exit*' コマンドで設定モードを抜け、特権モード（config モード）に入り直して設定をやり直してください。
0279E	Invalid argument. (space is not permited.)
	不正な文字列を検出しました。 文字列に空白が使用されています。 このパラメーターでは、空白の仕様は禁止されています。 入力内容をもう一度確認してください。

0280E	Invalid argument. (double quote is not permited.)
	不正な文字列を検出しました。 文字列に二重引用符が使用されています。 このパラメーターでは、二重引用符の仕様は禁止されています。 入力内容をもう一度確認してください。
0281E	illegal name - max 16 characters exceeded.
	不正な文字列を検出しました。 16 文字以内で指定してください。
0282E	illegal name - must start with an alphabetic character.
	不正な文字列を検出しました。 アルファベットで開始してください。
0283E	illegal name - only alphanumeric, hyphen(-) or underscore(_) allowed.
	不正な文字列を検出しました。 ハイフンまたはアンダーバー以外の記号の使用は認められていません。
0284E	illegal name - only alphanumeric, hyphen(-) or underscore(_) or square(#) or slash(/) or commercial at(@) allowed.
	不正な文字列を検出しました。 ハイフン、アンダーバー、ドット、スラッシュ、シャープ、アット以外の記号の使用は認められていません。
0287E	<str>: invalid time expression.
	不正な文字列を検出しました。 タイマー値は日付型の文字列で設定してください。
0288E	<str>: invalid time expression.
	不正な文字列を検出しました。 タイマー値は日付型の文字列で設定してください。
0289E	<str>: invalid time expression.
	不正な文字列を検出しました。 タイマー値は日付型の文字列で設定してください。
0290E	<str>: invalid time expression.
	不正な文字列を検出しました。 タイマー値は日付型の文字列で設定してください。

0291E	<str>: invalid time expression. 不正な文字列を検出しました。 タイマー値は日付型の文字列で設定してください。
0292E	group cannot contain more than five virtual servers. 仮想サーバーグループ設定に失敗しました。 仮想サーバーグループ設定で 5 件以上の仮想サーバーを検出しました。 仮想サーバーグループに指定できる仮想サーバーは 4 件までです。 入力値を確認し、もう一度設定し直してください。
0293E	<str>: No such settings. 仮想サーバーグループの登録に失敗しました。 不正な仮想サーバーID または仮想サーバー名を検出しました。 入力された仮想サーバーは存在しません。 設定内容や入力値を確認し、もう一度設定し直してください。
0294E	virtual cannot be in more than one group. 仮想サーバーグループの登録に失敗しました。 既に他の仮想サーバーグループに所属している仮想サーバーが指定されています。 仮想サーバーを複数の仮想サーバーグループに所属させることはできません。 設定内容や入力値を確認し、もう一度設定し直してください。
0295E	Operation not supported for ssl/cookie sticky associations. 仮想サーバーグループの登録に失敗しました。 cookie セッション維持設定、cookie 挿入設定、SSL セッション維持設定のいずれかが設定されている仮想サーバーを、仮想サーバーグループに所属させることはできません。 設定内容や入力値を確認し、もう一度設定し直してください。
0296E	<str>: No such settings. 仮想サーバーグループの削除に失敗しました。 不正な仮想サーバーID または仮想サーバー名を検出しました。 入力された仮想サーバーは存在しません。 設定内容や入力値を確認し、もう一度設定し直してください。

0297E	<str>: No such settings. 仮想サーバーグループの削除に失敗しました。 入力された仮想サーバーは、指定した仮想サーバーグループに所属していません。 設定内容や入力値を確認し、もう一度設定し直してください。
0298E	usage : help <command> help コマンドで、不正なパラメーターを検出しました。 パラメーターには存在するコマンドを入力してください。
0299E	Command '<str>' unknown. help コマンドで、不正なパラメーターを検出しました。 パラメーターには存在するコマンドを入力してください。
0300E	other user is configuring the system. (Terminal id <num>). 設定の変更に失敗しました。 既に特権モードにログインしているユーザーがいるか、または何らかの理由により、システム内部のログイン情報がクリアされないままでいます。 設定変更を続けるには、特権モードに遷移中のユーザーをログアウトさせます。 任意のログインユーザーを強制的にログアウトさせるには、'*show login-session*' コマンドでアスタリスク(*)が表示されている端末 ID を確認し、更に'*clear login-session*' コマンドを実施してください。

0301E	failed to execute config command on peer machine. ** please re-enter 'config' mode by typing 'config' in normal mode. **
	設定の同期に失敗しました。 冗長相手へのコマンドの同期に失敗しています。 ・ Master/Backup 状態の切り替りが発生していませんか？ Master/Backup 状態の切り替りが発生した場合、設定同期用のコネクションがクリアされてしまいます。 ・ 自機器と冗長相手機器の設定情報に矛盾がありませんか？ 「冗長先アドレス（peer アドレス）の設定や、VRID の設定が食い違っている」、または「冗長相手先に存在しない設定に対して削除設定を実施した」など、設定情報に矛盾がある場合、設定同期処理は失敗します。 ・ 最後に実行されたコマンドは正常に実行されましたか？ 正常にコマンド同期がされないまま（コマンド同期に失敗したまま）設定変更を続けた場合、同期先との接続が遮断されてしまう恐れがあります。 これらの理由、またはその他の何らかの理由により冗長相手との接続性が損なわれた可能性があります。 この状態では冗長相手へ設定の同期がされません。 恐れ入りますが、自機器や冗長相手機器の設定内容、冗長相手との接続性などを確認してから、一旦 '***exit***' コマンドで設定モードを抜け、特権モード（config モード）に入り直して設定をやり直してください。
0302E	probe <str>: No such settings.
	ヘルスチェックポリシーの有効化、または無効化に失敗しました。 指定されたヘルスチェックポリシーは存在しません。 設定内容や入力値を確認し、もう一度設定し直してください。
0303E	virtual <str>: No such settings.
	仮想サーバー設定の有効化、または無効化に失敗しました。 指定された仮想サーバーID は存在しません。 設定内容や入力値を確認し、もう一度設定し直してください。

0304E	virtual <str>: No such settings. 仮想サーバー設定の有効化、または無効化に失敗しました。 指定された仮想サーバー名は存在しません。 設定内容や入力値を確認し、もう一度設定し直してください。
0305E	Must be full directory path. Please start at slash. テクニカルサポートログの取得に失敗しました。 ローカルディレクトリパスは、絶対パスでなければいけません。パス文字列は必ずスラッシュ(/)で開始してください。
0306E	<str>: No such settings. SSL 情報のエクスポートに失敗しました。 入力された SSL ポリシーは存在しません。 設定内容や入力値を確認し、もう一度実施してください。
0307E	Invalid ssl directory structure. Please reconstruct the setting of ssl. SSL 情報のエクスポートに失敗しました。 内部エラーにより、SSL ディレクトリ構造が正しく形成されていません。 恐れ入りますが、'*no ssl* コマンドで該当の SSL ポリシーを削除してから再度 SSL ポリシーを生成し直してください。
0308E	version file open failure. バージョン番号が記述されている内部ファイルの読み込みに失敗しました。
0309E	serial-no file open failure. シリアル番号が記述されている内部ファイルの読み込みに失敗しました。
0310E	config file open error. 設定ファイルの読み込みに失敗しました。
0311E	config file close error. 設定ファイルのクローズに失敗しました。
0312E	config file close error. 設定ファイルのクローズに失敗しました。
0313E	config file close error. 設定ファイルのクローズに失敗しました。
0314E	config file close error. 設定ファイルのクローズに失敗しました。

0315E	failed to get the history data. コマンドヒストリの取得に失敗しました。
0316E	command history file close error. コマンドヒストリ取得時の終了処理に失敗しました。
0317E	hash file open error. ユーザーアカウントデータの変更に失敗しました。 内部エラーにより、パスワードファイルの読み込みに失敗しています。 もう一度設定をやり直してください。
0318E	hash file close error. ユーザーアカウントデータの変更に失敗しました。 内部エラーにより、パスワード変更の終了処理に失敗しています。 もう一度設定をやり直してください。
0319E	web password file open error. ユーザーアカウントデータの変更に失敗しました。 内部エラーにより、WEB 用パスワードファイルの読み込みに失敗しています。 もう一度設定をやり直してください。
0320E	web password file close error. ユーザーアカウントデータの変更に失敗しました。 内部エラーにより、WEB 用パスワードの変更処理に失敗しています。 もう一度設定をやり直してください。
0321E	web password file open error. ユーザーアカウントデータの変更に失敗しました。 内部エラーにより、WEB 用パスワードの更新処理に失敗しています。 もう一度設定をやり直してください。
0322E	web password file close error. ユーザーアカウントデータの変更に失敗しました。 内部エラーにより、WEB 用パスワードの変更処理に失敗しています。 もう一度設定をやり直してください。
0323E	empty password is not permitted. パスワードの変更に失敗しました。 空のパスワードは許可されていません。

0324E	password length too long. パスワードの変更に失敗しました。 パスワードは 32 文字以内で入力してください。
0325E	password length too long. パスワードの変更に失敗しました。 パスワードは 32 文字以内で入力してください。
0326E	Operation not supported on this user. パスワードの変更に失敗しました。 パスワード変更が認められない特殊なユーザーです。
0327E	failed to create local socket. STP 統計情報の取得に失敗しました。 もう一度やり直してください。
0328E	failed to get statistical data for ssl. SSL 統計情報の取得に失敗しました。 もう一度やり直してください。
0329E	<str>: No such file or directory. 証明書の表示に失敗しました。 もう一度やり直してください。
0330E	failed to create local socket. VLAN 情報の取得に失敗しました。 もう一度やり直してください。
0331E	failed to create local socket. MAC テーブル情報の取得に失敗しました。 もう一度やり直してください。
0332E	I got the corrupted data for real server. 実サーバー統計情報の取得に失敗しました。 もう一度やり直してください。
0333E	no data at the same real server address. 実サーバー統計情報の取得に失敗しました。 もう一度やり直してください。
0334E	no data at the same real server address. 実サーバー統計情報の取得に失敗しました。 もう一度やり直してください。

0335E	<str>: parameter error. サーバーバインド統計情報の取得に失敗しました。 不正ないアドレスを検出しました。 入力値をもう一度確認してください。
0336E	processing failed. ルーティングテーブル情報の取得に失敗しました。 もう一度やり直してください。
0337E	processing failed. L7 セッション情報（ipv4）の取得に失敗しました。 もう一度やり直してください。
0338E	processing failed. L7 セッション情報（ipv6）の取得に失敗しました。 もう一度やり直してください。
0339E	failed debug trace fetch. トレース情報の取得に失敗しました。
0340E	strings too long. トレーストリガー設定に失敗しました。 不正なトリガー文字列を検出しました。 トリガー文字列は 256 文字以内で設定してください。
0341E	Settings already exists. トレーストリガー設定に失敗しました。 入力された設定は既に存在します。 設定内容や入力値を確認し、もう一度設定し直してください。
0342E	number of trace trigger settings cannot exceed 16. トレーストリガー設定は登録可能な最大設定数に達しています。 設定を追加する場合は既存の設定を削除してください。
0343E	No such settings. トレーストリガー設定の削除に失敗しました。 入力された設定は存在しません。 設定内容や入力値を確認し、もう一度設定し直してください。

0344E	Must be full directory path. Please start at slash.
	ダンプデータの取得に失敗しました。 ローカルディレクトリパスは、絶対パスでなければいけません。パス文字列は必ずスラッシュ（/）で開始してください。
0345E	<str>: parameter error.
	ダンプ取得設定の変更に失敗しました。 不正なパラメーターを検出しました。 入力値を確認してもう一度やり直してください。
0346E	no virtual server data.
	仮想サーバー情報が取得できません。
0347E	no virtual server data.
	イーサネット情報が取得できません。
0348E	config file open error.
	設定ファイルの読み込みに失敗しました。
0349E	config file close error.
	設定ファイルのクローズ処理に失敗しました。
0350E	config file open error.
	設定ファイルの読み込みに失敗しました。
0351E	config file close error.
	設定ファイルのクローズ処理に失敗しました。
0352E	config file open error.
	設定ファイルの読み込みに失敗しました。
0353E	config file close error.
	設定ファイルのクローズ処理に失敗しました。
0354E	config file open error.
	設定ファイルの読み込みに失敗しました。
0355E	config file close error.
	設定ファイルのクローズ処理に失敗しました。
0356E	config file open error.
	設定ファイルの読み込みに失敗しました。
0357E	config file close error.
	設定ファイルのクローズ処理に失敗しました。

0358E	<str>: syntax error. イーサネット情報が取得できません。 ポート番号の指定に誤りがあります。 入力値を確認してやり直してください。
0359E	Argument list too long. イーサネット情報が取得できません。 ポート番号の指定に誤りがあります。 入力値を確認してやり直してください。
0360E	<num>: out of range. (1-<num>) イーサネット情報が取得できません。 ポート番号の指定に誤りがあります。 入力値を確認してやり直してください。
0361E	<num>: out of range. (1-<num>) イーサネット情報が取得できません。 ポート番号の指定に誤りがあります。 入力値を確認してやり直してください。
0362E	config file open error. 設定ファイルの読み込みに失敗しました。
0363E	<num>: No such settings. 論理チャネル情報が取得できません。 存在しないチャネル番号が入力されました。 入力値を確認してやり直してください。
0364E	<str>: No such settings. VLAN 情報が取得できません。 存在しない VLAN ID または VLAN 名が入力されました。 入力値を確認してやり直してください。
0365E	config file close error. 設定ファイルのクローズ処理に失敗しました。
0366E	config file open error. 設定ファイルの読み込みに失敗しました。
0367E	config file close error. 設定ファイルのクローズ処理に失敗しました。
0368E	config file open error. 設定ファイルの読み込みに失敗しました。

0369E	config file close error. 設定ファイルのクローズ処理に失敗しました。
0370E	config file open error. 設定ファイルの読み込みに失敗しました。
0371E	config file close error. 設定ファイルのクローズ処理に失敗しました。
0372E	config file open error. 設定ファイルの読み込みに失敗しました。
0373E	<str>: No such settings. 仮想サーバー情報が取得できません。 存在しない仮想サーバーID または仮想サーバー名が入力されました。 入力値を確認してやり直してください。
0374E	config file close error. 設定ファイルのクローズ処理に失敗しました。
0375E	config file open error. 設定ファイルの読み込みに失敗しました。
0376E	config file close error. 設定ファイルのクローズ処理に失敗しました。
0377E	config file open error. 設定ファイルの読み込みに失敗しました。
0378E	config file close error. 設定ファイルのクローズ処理に失敗しました。
0379E	config file open error. 設定ファイルの読み込みに失敗しました。
0380E	config file close error. 設定ファイルのクローズ処理に失敗しました。
0381E	failed to estimate arp data. ARP テーブル情報の取得に失敗しました。 入力値を確認してやり直してください。
0382E	failed to retrieval of routing table. ARP テーブル情報の取得に失敗しました。 入力値を確認してやり直してください。

0383E	failed to create socket. ARP テーブル情報の取得に失敗しました。 入力値を確認してやり直してください。
0384E	failed to startup internal process. シスログ情報の取得に失敗しました。 入力値を確認してやり直してください。
0385E	config file close error. 設定ファイルのクローズ処理に失敗しました。
0386E	failed to create socket. チャネル情報の取得に失敗しました。 入力値を確認してやり直してください。
0387E	out of range. (1-<num>) チャネル情報の取得に失敗しました。 不正な論理チャネル番号を検出しました。 入力値を確認してやり直してください。
0388E	failed to get the ndp data. NDP テーブル情報の取得に失敗しました。 入力値を確認してやり直してください。
0389E	failed to create socket. NDP テーブル情報の取得に失敗しました。 入力値を確認してやり直してください。
0390E	<str>: invalid address. 静的 ARP エントリーの変更に失敗しました。 不正なアドレスを検出しました。 入力値を確認してやり直してください。
0391E	<str>: invalid address. 静的 ARP エントリー情報の変更に失敗しました。 不正なアドレスを検出しました。 入力値を確認してやり直してください。
0392E	<str>: Settings already exists. 静的 ARP エントリー情報の登録に失敗しました。 指定されたアドレスは既に登録されています。 設定内容や入力値を確認し、もう一度設定し直してください。

0393E	Address already in use for vlan ip or virtual ip or redundant ip. 静的 ARP エントリー情報の登録に失敗しました。 指定されたアドレスは、装置 IP、または仮想サーバーIP で使用されています。 設定内容や入力値を確認し、もう一度設定し直してください。
0394E	Network is unreachable. 静的 ARP エントリー情報の登録に失敗しました。 指定されたアドレスは到達性がないため ARP テーブルに登録されませんでした。 設定内容や入力値を確認し、もう一度設定し直してください。
0395E	static arp table has already become full. 静的 ARP エントリー情報の登録に失敗しました。 静的 ARP エントリーは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0396E	<str>: No such settings. 静的 ARP エントリー情報の削除に失敗しました。 指定された静的 ARP エントリーは存在しません。 設定内容や入力値をもう一度確認してください。
0397E	out of range. (1m-1d) ARP エントリー生存時間の変更に失敗しました。 不正なパラメーターを検出しました。 日付型の文字列で 1m-365d の範囲で設定してください。
0398E	out of range. (1m-1d) ARP エントリー生存時間の変更に失敗しました。 不正なパラメーターを検出しました。 日付型の文字列で 1m-365d の範囲で設定してください。
0399E	hostname is too long. ホスト名の変更に失敗しました。 不正な文字列を検出しました。 ホスト名は 16 文字以内で入力してください。

0400E	syntax error - <portnum> must be either a single port, multiple ports separated by a comma(,), or a range of ports separated by a hyphen(-)
	イーサネット設定モードへ遷移できませんでした。 不正な文字列を検出しました。 ポート番号を複数指定する場合はカンマ(,)で区切るか、ハイフン(-)で繋げて指定してください。
0401E	port <num>: No such data.
	イーサネット設定モードへ遷移できませんでした。 入力されたポートは本装置の規定範囲外です。 本装置のイーサネットポート数を確認し、もう一度やり直してください。
0402E	failed to ethernet mode.
	イーサネット設定モードへ遷移できませんでした。 内部エラーが発生しました。 恐れ入りますが、設定モードから一旦抜けて、特権モードに入り直してからもう一度コマンドを実行してください。
0403E	<str>: invalid channel number.
	チャネル設定モードへ遷移できませんでした。 不正な値を検出しました。 入力値をもう一度確認してください。
0404E	<num>: No such settings.
	チャネル設定モードへ遷移できませんでした。 入力されたチャネル番号は存在しません。 論理チャネルはイーサネット設定モードの’*channel* コマンドで登録します。 設定内容や入力値をもう一度確認してください。
0405E	failed to channel mode.
	チャネル設定モードへ遷移できませんでした。 内部エラーが発生しました。 恐れ入りますが、設定モードから一旦抜けて、特権モードに入り直してからもう一度コマンドを実行してください。

0406E	<str>: No such settings. VLAN 設定モードへ遷移できませんでした。 入力された VLAN 名は存在しません。 設定内容や入力値をもう一度確認してください。
0407E	vlan <num>: No such data. VLAN の削除に失敗しました。 入力された VLAN は存在しません。 設定内容や入力値をもう一度確認してください。
0408E	failed to vlan mode. VLAN 設定モードへ遷移できませんでした。 内部エラーが発生しました。 恐れ入りますが、設定モードから一旦抜けて、特権モードに入り直してからもう一度コマンドを実行してください。
0409E	Detected invalid file. ファイルのインポートに失敗しました。 ファイル転送が中断されました。 'q'の入力により転送中断が発生したか、もしくは不正な設定ファイルを検出しました。 'q'の入力による任意の転送中断でない場合、設定ファイル内容を確認してください。
0410E	failed to rewrite configuration file. ファイルのインポートに失敗しました。 不正な設定ファイルが検出され、ファイル転送が中断されました。 インポート対象の設定ファイルの内容を確認してから、再度インポートし直してください。
0411E	Detected invalid files or failed to import files for internal error. ファイルのインポートに失敗しました。 不正な設定ファイルが検出され、ファイル転送が中断されました。 インポート対象の設定ファイルの内容を確認してから、再度インポートし直してください。

0412E	number of sorry contents cannot exceed 32.
	ソーリーコンテンツファイルのインポートに失敗しました。 ソーリーコンテンツはインポート可能な最大数に達しています。 ソーリーコンテンツを追加する場合は、'*clear content*'コマンドを実施し、既存のコンテンツを削除してください。
0413E	failed to import the sorry content.
	ソーリーコンテンツファイルのインポートに失敗しました。 内部エラーが発生しました。 恐れ入りますが、もう一度インポートし直してください。
0414E	file size too large.
	ソーリーコンテンツファイルのインポートに失敗しました。 コンテンツサイズが規定値を超えています。 コンテンツサイズを 4500byte 以内にして、もう一度インポートし直してください。
0415E	<str>: No such settings.
	SSL 関連ファイルのインポートに失敗しました。 入力された SSL ポリシー名は存在しません。 設定内容や入力値をもう一度確認してください。
0416E	Invalid ssl directory structure. Please reconstruct the ssl settings.
	SSL 関連ファイルのインポートに失敗しました。 SSL ディレクトリ構造が正しくありません。 該当の SSL ポリシーを一旦削除して、SSL ポリシーの作成からやり直してください。
0417E	invalid input value.
	SSL 関連ファイルのインポートに失敗しました。 入力値をもう一度確認してください。
0418E	invalid input value.
	SSL 関連ファイルのインポートに失敗しました。 入力値をもう一度確認してください。

0419E	Already bound ssl-policy for client-authentication. Please unbind ssl-policy "<str>" from virtual-server.
	SSL 関連ファイルのインポートに失敗しました。 クライアント CA 証明書がインポートされた SSL ポリシーは仮想サーバーに対して1つまでしかバインドできません。 この SSL ポリシーにクライアント CA 証明書をインポートする場合、仮想サーバー設定モードに遷移して、既にクライアント CA 証明書がインポートされている SSL ポリシーを、該当の仮想サーバーからアンバインドしてください。
0420E	failed to import the ssl files. Please re-import the files.
	SSL 関連ファイルのインポートに失敗しました。 内部エラーが発生しました。 恐れ入りますが、もう一度インポートし直してください。
0421E	<str>: invalid address.
	シスログサーバーのホストアドレスが不正です。 入力値をもう一度確認してください。
0422E	<str>: Settings already exists.
	シスログサーバーのホストアドレスの登録に失敗しました。 該当のアドレスは既に登録されています。 設定内容や入力値をもう一度確認してください。
0423E	number of syslog server cannot exceed 4.
	シスログサーバーのホストアドレスの登録に失敗しました。 シスログホストは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0424E	<str>: No such settings.
	シスログサーバーのホストアドレスの削除に失敗しました。 該当のホストアドレスは登録されていません。 設定内容や入力値をもう一度確認してください。

0425E	invalid argument. シスログファシリティー、シスログレベルの登録に失敗しました。 不正なファシリティー値を検出しました。 ファシリティーは 16-23 の範囲で設定してください。
0426E	facility <num>: out of range. (16-23) シスログファシリティー、シスログレベルの登録に失敗しました。 不正なファシリティー値を検出しました。 ファシリティーは 16-23 の範囲で設定してください。
0427E	invalid argument. シスログファシリティー、シスログレベルの登録に失敗しました。 不正なログレベル値を検出しました。 ログレベルは 0-7 の範囲で設定してください。
0428E	level <num>: out of range. (0-7) シスログファシリティー、シスログレベルの登録に失敗しました。 不正なログレベル値を検出しました。 ログレベルは 0-7 の範囲で設定してください。
0429E	<str>: invalid address. メールホストの登録に失敗しました。 不正なアドレスを検出しました。 入力値をもう一度確認してください。
0430E	invalid argument. メールホストの登録に失敗しました。 不正なログレベル値を検出しました。 ログレベルは 0-7 の範囲で設定してください。
0431E	level <num>: out of range. (0-7) メールホストの登録に失敗しました。 不正なログレベル値を検出しました。 ログレベルは 0-7 の範囲で設定してください。
0432E	number of logging-to mail address cannot exceed 16. 宛先メールアドレスの登録に失敗しました。 宛先メールアドレスは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。

0433E	mail address too long. 宛先メールアドレスの登録に失敗しました。 URL 文字列は 256 文字以内で入力してください。
0434E	invalid mail address. 宛先メールアドレスの登録に失敗しました。 不正な URL を検出しました。 入力値をもう一度確認してください。
0435E	Settings already exists. 宛先メールアドレスの登録に失敗しました。 入力されたメールアドレスは既に登録されています。 設定内容や入力値をもう一度確認してください。
0436E	<str>: No such settings. 宛先メールアドレスの削除に失敗しました。 入力されたメールアドレスは登録されていません。 設定内容や入力値をもう一度確認してください。
0437E	mail address too long. 送信元メールアドレスの登録に失敗しました。 URL 文字列は 256 文字以内で入力してください。
0438E	invalid mail address. 送信元メールアドレスの登録に失敗しました。 不正な URL を検出しました。 入力値をもう一度確認してください。
0439E	mail address too long. 返信先メールアドレスの登録に失敗しました。 URL 文字列は 256 文字以内で入力してください。
0440E	invalid mail address. 返信先メールアドレスの登録に失敗しました。 不正な URL を検出しました。 入力値をもう一度確認してください。

0441E	<num>: Available number is only 0. VRRP インスタンスの登録に失敗しました。 インスタンス ID は 0 のみ指定可能です。 入力値をもう一度確認してください。
0442E	failed to moving vrrp mode. VRRP 設定モードへ遷移できませんでした。 内部エラーが発生しました。 恐れ入りますが、設定モードから一旦抜けて、特権モードに入り直してからもう一度コマンドを実行してください。
0443E	<num>: Available number is only 0. VRRP インスタンスの削除に失敗しました。 インスタンス ID は 0 のみ指定可能です。 入力値をもう一度確認してください。
0444E	vrrp instance <num>: No such settings. VRRP インスタンスの削除に失敗しました。 VRRP インスタンスは存在しません。 設定内容をもう一度確認してください。
0445E	file open error vrrp process. 強制バックアップに失敗しました。 VRRP プロセスが応答しません。 VRRP 状態を確認してからもう一度実施してください。
0446E	<str>: invalid ethernet address. 不正な MAC アドレスを検出しました。 もう一度入力値を確認してください。
0447E	Invalid argument. 静的 MAC アドレスエントリーの登録に失敗しました。 不正な入力値を検出しました。 もう一度入力値を確認してください。
0448E	<str>: Settings already exists. 静的 MAC アドレスエントリーの登録に失敗しました。 該当の MAC アドレスは既に登録済みです。 設定内容や入力値をもう一度確認してください。

0449E	<num>: out of range. (1-<num>) 静的 MAC アドレスエントリーの登録に失敗しました。 不正なイーサネットポート番号の入力を検出しました。 設定内容や入力値をもう一度確認してください。
0450E	<num>: out of range. (1-<num>) 静的 MAC アドレスエントリーの登録に失敗しました。 不正な論理チャネル番号の入力を検出しました。 設定内容や入力値をもう一度確認してください。
0451E	chan<num>: No such settings. 静的 MAC アドレスエントリーの登録に失敗しました。 該当の論理チャネルは存在しません。 設定内容や入力値をもう一度確認してください。
0452E	<str>: invalid parameter. 静的 MAC アドレスエントリーの登録に失敗しました。 不正なパラメーターを検出しました。 入力値をもう一度確認してください。
0453E	static mac address table has already become full. 静的 MAC アドレスエントリーの登録に失敗しました。 静的 MAC アドレスエントリーは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0454E	add mac-table entry failed. 静的 MAC アドレスエントリーの登録に失敗しました。 内部エラーが発生しました。 恐れ入りますが、もう一度設定し直してください。
0455E	<str>: No such settings. 静的 MAC アドレスエントリーの削除に失敗しました。 該当の MAC エントリーは存在しません。 設定内容や入力値をもう一度確認してください。

0456E	out of range. (1m-2h) MAC テーブルのタイムアウト値の変更に失敗しました。 MAC テーブルのタイムアウト値が規定の範囲外です。 1m-2h の範囲で設定してください。
0457E	<num>: out of range. (0-4096) MAC テーブルサイズの変更に失敗しました。 MAC テーブルサイズが規定の範囲外です。 0-4096 の範囲で設定してください。
0458E	<str>: Settings already exists. IP アドレスの名前付けに失敗しました。 入力された名前は既に登録されています。 設定内容や入力値をもう一度確認してください。
0459E	<str>: invalid address. IP アドレスの名前付けに失敗しました。 不正なアドレス文字列を検出しました。 入力値を確認して、もう一度設定し直してください。
0460E	<str>: Settings already exists. IP アドレスの名前付けに失敗しました。 入力された IP アドレスは既に登録されています。 設定内容や入力値をもう一度確認してください。
0461E	number of server-name settings cannot exceed 512. IP アドレスの名前付けに失敗しました。 IP アドレスの名前付け設定は登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0462E	Invalid argument. IP アドレスの名前付け設定の削除に失敗しました。 不正な入力値を検出しました。 もう一度入力値を確認し、正しい文法で設定してください。

0463E	<str>: No such settings. IP アドレスの名前付け設定の削除に失敗しました。 該当の設定は存在しません。 設定内容や入力値をもう一度確認してください。
0464E	<str>: invalid address. 静的 ndp テーブルエントリーの登録に失敗しました。 不正なアドレス文字列を検出しました。 入力値を確認して、もう一度設定し直してください。
0465E	<str>: Settings already exists. 静的 ndp テーブルエントリーの登録に失敗しました。 入力された ndp エントリーは既に登録されています。 設定内容や入力値をもう一度確認してください。
0466E	Address already in use. 静的 ndp テーブルエントリーの登録に失敗しました。 入力されたアドレスは、装置 IP アドレスまたは仮想サーバードレスとして既に登録されています。 設定内容や入力値をもう一度確認してください。
0467E	Network is unreachable. 静的 ndp テーブルエントリーの登録に失敗しました。 入力されたアドレスへの到達性を確認できませんでした。 設定内容や入力値をもう一度確認してください。
0468E	static ndp table is full. 静的 ndp テーブルエントリーの登録に失敗しました。 静的 ndp テーブルエントリーは登録可能な最大数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0469E	<str>: No such settings. 静的 ndp テーブルエントリーのの削除に失敗しました。 該当の設定は存在しません。 設定内容や入力値をもう一度確認してください。

0470E	<str>: invalid address. ntp サーバーの登録に失敗しました。 不正なアドレス文字列を検出しました。 入力値を確認して、もう一度設定し直してください。
0471E	<str>: Settings already exists. ntp サーバーの登録に失敗しました。 入力された ntp サーバードレスは既に登録されています。 設定内容や入力値をもう一度確認してください。
0472E	number of ntp server addresses cannot exceed 4. ntp サーバーの登録に失敗しました。 ntp サーバー設定は登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0473E	<str>: No such settings. ntp サーバー設定の削除に失敗しました。 該当の設定は存在しません。 設定内容や入力値をもう一度確認してください。
0474E	<num>: out of range. (0-65535) プロキシサーバー設定の登録に失敗しました。 不正なポート番号が指定されています。 ポート番号は 1-65535 の範囲で入力してください。 入力値を確認して、もう一度設定し直してください。
0475E	<str>: invalid address. プロキシサーバー設定の登録に失敗しました。 不正なアドレス文字列を検出しました。 入力値を確認して、もう一度設定し直してください。
0476E	<str>: No such settings. ヘルスチェック設定モードへの遷移に失敗しました。 入力されたヘルスチェックポリシーは存在しません。 設定内容や入力値をもう一度確認してください。

0477E	<str>: Already exists. ヘルスチェック組み合わせ設定の登録に失敗しました。 入力されたヘルスチェックポリシー名は既に存在しています。 設定内容や入力値をもう一度確認してください。
0478E	<str>: invalid address. ヘルスチェック設定モードへの遷移に失敗しました。 不正なアドレス文字列を検出しました。 入力値を確認して、もう一度設定し直してください。
0479E	<str>: Already exists. (not same ID) ヘルスチェック設定モードへの遷移に失敗しました。 不正なサーバーID 文字列を検出しました。 入力値を確認して、もう一度設定し直してください。
0480E	<str>: Already exists. (not same protocol) ヘルスチェック設定モードへの遷移に失敗しました。 不正なサーバーID 文字列を検出しました。 入力値を確認して、もう一度設定し直してください。
0481E	<str>: Already exists. (not same protocol) ヘルスチェック設定モードへの遷移に失敗しました。 不正なサーバーID 文字列を検出しました。 入力値を確認して、もう一度設定し直してください。
0482E	failed to moving probe mode. 内部エラーにより、ヘルスチェック設定モードへの遷移に失敗しました。 恐れ入りますが、一旦 exit コマンドで設定モードを抜け、特権モード（config モード）に入り直してください。
0483E	<str>: No such settings. ヘルスチェックポリシーの削除に失敗しました。 入力されたヘルスチェックポリシーは存在しません。 設定内容や入力値をもう一度確認してください。

0484E	<str>: this is undeletable entry.
	ヘルスチェックポリシーの削除に失敗しました。 該当のポリシーは、ヘルスチェック組み合わせ設定で参照されています。 削除したい場合は、該当ポリシーを参照しているヘルスチェック組み合わせ設定を削除してください。
0485E	invalid input value.
	システムの再起動に失敗しました。 再起動は応答形式で実行されます。 再起動する場合は'y'を入力してください。
0486E	<str>: invalid address.
	最大コネクション数の設定に失敗しました。 不正なサーバーID 文字列を検出しました。 入力値を確認して、もう一度設定し直してください。
0487E	<str>: Operation not supported. (protocol is only allowed 'tcp')
	最大コネクション数の設定に失敗しました。 UDP サーバーが指定されています。 最大コネクション数は TCP サーバーにのみ設定可能です。 入力値を確認して、もう一度設定し直してください。
0488E	<str>: No such settings.
	最大コネクション数の設定に失敗しました。 入力された実サーバーID は存在しません。 設定内容や入力値をもう一度確認してください。
0489E	<num>: out of range. (0-65535)
	最大コネクション数の設定に失敗しました。 入力されたコネクション数が規定の範囲外です。 0-65535 の範囲で設定してください。
0490E	<str>: invalid address.
	実サーバーの登録に失敗しました。 不正なサーバーID 文字列を検出しました。 入力値を確認して、もう一度設定し直してください。

0491E	Operation not supported. 実サーバーの登録に失敗しました。 不正なプロトコル文字列を検出しました。 入力値を確認して、もう一度設定し直してください。
0492E	Operation not supported. 実サーバーの登録に失敗しました。 不正なプロトコル文字列を検出しました。 入力値を確認して、もう一度設定し直してください。
0493E	<str>: Operation not supported. (protocol is only allowed 'tcp') 実サーバーの登録に失敗しました。 UDP サーバーに対して最大コネクション数が指定されています。 最大コネクション数は TCP サーバーにのみ設定可能です。 入力値を確認して、もう一度設定し直してください。
0494E	<num>: out of range. (0-65535) 実サーバーの登録に失敗しました。 入力された最大コネクション数が規定の範囲外です。 0-65535 の範囲で設定してください。
0495E	<str>: Settings already exists. 実サーバーの登録に失敗しました。 入力された実サーバーは既に登録されています。 設定内容や入力値をもう一度確認してください。
0496E	Number of {ipv4 | ipv6} real server cannot exceed 256. 実サーバーの登録に失敗しました。 実サーバーは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0497E	<str>: No such settings. 実サーバーの削除に失敗しました。 入力された実サーバーID は登録されていません。 設定内容や入力値をもう一度確認してください。

0498E	<str>: Device busy. 実サーバーの削除に失敗しました。 該当の実サーバーは仮想サーバーにバインドされています。 設定を削除する場合は、仮想サーバー設定モードの no bind コマンドで、該当の実サーバーを解除してください。
0499E	<str>: invalid mask or prefix. ルーティングテーブルの変更に失敗しました。 マスク長、またはプレフィックス長で不正な値を検出しました。 設定内容や入力値をもう一度確認してください。
0500E	<str>: invalid address. ルーティングテーブルの変更に失敗しました。 不正なアドレス文字列を検出しました。 入力値を確認して、もう一度設定し直してください。
0501E	<str>: invalid address. ルーティングテーブルの変更に失敗しました。 不正なゲートウェイアドレス検出しました。 入力値を確認して、もう一度設定し直してください。
0502E	address family is unmatch. ルーティングテーブルの変更に失敗しました。 宛先アドレスとゲートウェイアドレスで同一のアドレスファミリーを使用してください。
0503E	Network is unreachable. ルーティングテーブルの変更に失敗しました。 ゲートウェイアドレスの到達性が確認できません。 ゲートウェイアドレスは、VLAN に登録済みのネットワークアドレスの範囲に沿って指定してください。
0504E	<str>: invalid address. ルーティングテーブルの変更に失敗しました。 不正なマスクアドレス文字列を検出しました。 入力値を確認して、もう一度設定し直してください。

0505E	<str>: invalid address. ルーティングテーブルの変更に失敗しました。 不正な宛先アドレス文字列を検出しました。 入力値を確認して、もう一度設定し直してください。
0506E	<str>: invalid address. ルーティングテーブルの変更に失敗しました。 不正なゲートウェイアドレス文字列を検出しました。 入力値を確認して、もう一度設定し直してください。
0507E	Network is unreachable. ルーティングテーブルの変更に失敗しました。 ゲートウェイアドレスの到達性が確認できません。 ゲートウェイアドレスは、VLAN に登録済みのネットワークアドレスの範囲に沿って指定してください。
0508E	The network address is already exist on the VLAN network. ルーティングテーブルの登録に失敗しました。 宛先ネットワークアドレスが、VLAN に登録済みのネットワークアドレスと完全一致します。 VLAN に登録済みのネットワークアドレスと異なるネットワークアドレスを指定してください。
0509E	Settings already exists. ルーティングテーブルの登録に失敗しました。 入力されたルーティングエントリーは既に登録されています。 設定内容や入力値をもう一度確認してください。
0510E	number of routing table entry cannot exceed 128. ルーティングテーブルの登録に失敗しました。 ルーティングテーブルは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。

0511E	No such settings. ルーティングテーブルの削除に失敗しました。 入力されたルーティングエントリーは登録されていません。 設定内容や入力値をもう一度確認してください。
0512E	invalid argument. スパニングツリー設定の変更に失敗しました。 特権モードの spanning-tree コマンドには、パラメーターが必須です。 もう一度入力値を確認してください。
0513E	<num>: out of range. (0-61440 in steps of 4096) スパニングツリープライオリティーの変更に失敗しました。 不正なプライオリティー値が入力されました。 プライオリティー値は 0-61440 の範囲で、4096 の倍数で入力してください。
0514E	<num>: out of range. (0-61440 in steps of 4096) スパニングツリーのバックアッププライオリティーの変更に失敗しました。 不正なプライオリティー値が入力されました。 プライオリティー値は 0-61440 の範囲で、4096 の倍数で入力してください。
0515E	out of range. (1s-2s) HelloTime(BPDU 送信間隔)の設定変更に失敗しました。 不正な値が入力されました。 HelloTime は 1s-2s の範囲で入力してください。
0516E	out of range. (4s-30s) ForwardDelay の設定変更に失敗しました。 不正な値が入力されました。 ForwardDelay は 4s-30s の範囲で入力してください。
0517E	out of range. (6s-40s) MaxAge の設定変更に失敗しました。 不正な値が入力されました。 MaxAge は 6s-40s の範囲で入力してください。

0518E	out of range. (0s-1d) SSL セッションタイムアウト値の変更に失敗しました。 SSL セッションタイムアウトは 0s-1d の範囲で入力してください。
0519E	<str>: invalid argument. 不正なパラメーターが入力されました。 パラメーター文字列内に、使用できない記号が含まれています。 入力値を確認して、もう一度設定し直してください。
0520E	<str>: invalid address. SNMP ホストアドレスの登録に失敗しました。 アドレス形式に誤りがあるか、存在しない IP 名を指定しています。 入力値を確認してください。
0521E	Operation not supported ipv6 host address. SNMP ホストアドレスの登録に失敗しました。 SNMP ホストアドレスに IPv6 アドレスを指定する事はできません。 入力値を確認して、もう一度設定し直してください。
0522E	<str>: Settings already exists. SNMP ホストアドレスの登録に失敗しました。 入力されたホストアドレスは登録済みです。 設定内容や入力値を、もう一度確認してください。
0523E	number of snmp manager ip addresses cannot exceed 4. SNMP ホストアドレスの登録に失敗しました。 SNMP ホストアドレスは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0524E	<str>: No such settings. SNMP ホストアドレスの削除に失敗しました。 入力されたホストアドレスは存在しません。 設定内容や入力値を、もう一度確認してください。

0525E	<str>: strings too long. SNMP トラップトリガー設定の登録に失敗しました。 入力されたトリガー文字列は長すぎます。 入力値を確認して、もう一度設定し直してください。
0526E	<str>: Settings already exists. SNMP トラップトリガー設定の登録に失敗しました。 入力されたトリガー文字列は登録済みです。 設定内容や入力値を、もう一度確認してください。
0527E	number of trap trigger settings cannot exceed 16. SNMP トラップトリガー設定の登録に失敗しました。 SNMP トラップトリガー設定は登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0528E	Please escape quote by the backslash(¥¥) if you using double quotes into a strings. And the strings should be enclosed in double quotes in this case. SNMP トラップトリガー設定の登録に失敗しました。 文字列に二重引用符(")を含める場合、必ずバックスラッシュでエスケープし、かつその文字列を二重引用符で囲む必要があります。 （例： "aaa¥"bbb"） 入力値を確認して、もう一度設定し直してください。
0529E	<str>: No such settings. SNMP トラップトリガー設定の削除に失敗しました。 入力された設定は存在しません。 設定内容や入力値を、もう一度確認してください。
0530E	<str>: strings too long. (length:1-<num>) SNMP 設定の登録に失敗しました。 パラメーターとして入力された文字列が長すぎます。 入力値を確認して、もう一度設定し直してください。

0531E	number of ssl-policy cannot exceed 256. SSL 証明書ポリシーの登録に失敗しました。 SSL 証明書ポリシーは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0532E	<str>: detected to invalid ssl directory. SSL 証明書ポリシーの登録に失敗しました。 内部エラーにより、SSL 証明書ポリシーのためのディレクトリ構造が正しく形成されませんでした。 恐れ入りますが、設定内容や入力値を確認し、もう一度設定し直してください。
0533E	failed to moving ssl mode. 内部エラーにより SSL 設定モードへの遷移に失敗しました。 恐れ入りますが、一旦ログアウトして、もう一度 CLI にログインし直してください。
0534E	<str>: No such settings. SSL ポリシーの削除に失敗しました。 入力された設定は存在しません。 設定内容や入力値を、もう一度確認してください。
0535E	<str>: This ssl-policy is used in virtual-server. SSL ポリシーの削除に失敗しました。 該当の SSL ポリシーは仮想サーバーにバインドされています。 設定を削除する場合は、仮想サーバー設定モードの no ssl コマンドで、該当の SSL ポリシーのバインドを解除してください。
0536E	This ssl-policy is used in virtual-server. SSL 関連ファイルの削除に失敗しました。 該当の SSL ポリシーは仮想サーバーにバインドされています。 設定を削除する場合は、仮想サーバー設定モードの no ssl コマンドで、該当の SSL ポリシーのバインドを解除してください。
0537E	out of range. (0-500) コマンドヒストリー保持件数の変更に失敗しました。 不正な値が入力されました。 コマンドヒストリー保持件数は 0-500 の範囲で入力してください。

0538E	out of range. (0m-1d) 自動ログアウト時間の変更に失敗しました。 不正な値が入力されました。 自動ログアウト時間は 0m-1d の範囲で入力してください。
0539E	out of range. (0m-1d) 自動ログアウト時間の変更に失敗しました。 不正な値が入力されました。 自動ログアウト時間は 0m-1d の範囲で入力してください。
0540E	failed to moving virtual mode. 内部エラーにより仮想サーバー設定モードへの遷移に失敗しました。 恐れ入りますが、一旦ログアウトして、もう一度 CLI にログインし直してください。
0541E	<str>: No such settings. 仮想サーバーの削除に失敗しました。 入力された設定は存在しません。 設定内容や入力値を、もう一度確認してください。
0542E	virtual server is not deletable. (because belong a buddy group) 仮想サーバーの削除に失敗しました。 この仮想サーバーポリシーは、仮想サーバーグループに所属しています。 仮想サーバーを削除する場合は、no buddy コマンドで、該当の仮想サーバーグループから解除してください。
0544E	number of MAC access-list cannot exceed <num>. MAC アクセスリストの登録に失敗しました。 MAC アクセスリストは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0545E	<str>: No such settings. MAC アクセスリストの削除に失敗しました。 入力された設定は存在しません。 設定内容や入力値を、もう一度確認してください。

0546E	<str>: Can't delete this entry. MAC アクセスリストの削除に失敗しました。 このアクセスリストはイーサネット設定で使用しています。 このアクセスリストを削除する場合は、イーサネット設定モードの no filter コマンドで、フィルタリング設定を解除してください。
0547E	number of IP access-list cannot exceed <num>. IP アクセスリストの登録に失敗しました。 IP アクセスリストは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0548E	<str>: policy name is already used in the IPv6 access list. IP アクセスリストの登録に失敗しました。 入力されたポリシー名は、IPv6 アクセスリストで既に使用されています。
0549E	<str>: policy name is already used in the IPv4 access list. IP アクセスリストの登録に失敗しました。 入力されたポリシー名は、IPv4 アクセスリストで既に使用されています。
0550E	<str>: No such settings. IP アクセスリストの削除に失敗しました。 入力された設定は存在しません。 設定内容や入力値を、もう一度確認してください。
0551E	<str>: Can't delete this entry. IP アクセスリストの削除に失敗しました。 このアクセスリストは VLAN 設定で使用しています。 このアクセスリストを削除する場合は、VLAN 設定モードの no filter コマンドで、フィルタリング設定を解除してください。
0552E	Failed to moving access-list mode. 内部エラーによりアクセスリスト設定モードへの遷移に失敗しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。

0553E	Failed to set data for kernel. 内部エラーにより PING 許可設定に失敗しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0554E	invalid address. 不正なアドレスを検出しました。 もう一度入力値を確認してください。
0555E	<str>: No such data. プライマリーDNS サーバー設定の削除に失敗しました。 入力された設定は存在しません。 設定内容や入力値を、もう一度確認してください。
0556E	<str>: No such data. セカンダリーDNS サーバー設定の削除に失敗しました。 入力された設定は存在しません。 設定内容や入力値を、もう一度確認してください。
0557E	invalid input value. 機器の停止に失敗しました。 不正な入力値を検出しました。 機器の停止時には、応答形式で'y'または'n'を入力してください。
0558E	config file close error. 内部エラーにより設定ファイルのクローズ処理に失敗しました。
0559E	config file close error. 内部エラーにより設定ファイルのクローズ処理に失敗しました。
0560E	number of nat-pool cannot exceed <num>. NAT プールポリシーの登録に失敗しました。 NAT プールは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0561E	Failed to moving nat-pool mode. 内部エラーにより NAT プール設定モードへの遷移に失敗しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。

0562E	<str>: No such settings. NAT プール設定の削除に失敗しました。 入力された設定は存在しません。 設定内容や入力値を、もう一度確認してください。
0563E	<str>: nat-pool used in source-nat. NAT プール設定の削除に失敗しました。 この NAT プールは仮想サーバー設定で使用しています。 この NAT プールを削除する場合は、仮想サーバー設定モードの no source-nat コマンドで、ソース NAT 設定を解除してください。
0564E	<str>: nat-pool used in reverse-nat. NAT プール設定の削除に失敗しました。 この NAT プールはリバース NAT 設定で使用しています。 この NAT プールを削除する場合は、no reverse-nat コマンドで、ソース NAT 設定を解除してください。
0565E	<str>: No such settings. 仮想サーバーグループ設定の削除に失敗しました。 入力された設定は存在しません。 設定内容や入力値を、もう一度確認してください。
0566E	number of url rule exceed <num>. URL スイッチングルールの登録に失敗しました。 URL スイッチングルールは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0567E	Invalid argument. URL スイッチングルールの登録に失敗しました。 不正な文字列を検出しました。 もう一度入力値を確認してください。
0568E	method string may not contain "*". URL スイッチングルールの登録に失敗しました。 不正な文字列を検出しました。 HTTP メソッドでは、文字列にアスタリスク(*)を含める事はできません。 もう一度入力値を確認してください。

0569E	number of url rule exceed <num>. URL スイッチングルールの登録に失敗しました。 URL スイッチングルールは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0570E	Invalid argument. URL スイッチングルールの登録に失敗しました。 不正な文字列を検出しました。 もう一度入力値を確認してください。
0571E	"*" may appear only at the beginning or end of the string. URL スイッチングルールの登録に失敗しました。 不正な文字列を検出しました。 アスタリスク(*)は、ルール文字列の先頭、または末尾にのみ指定可能です。 もう一度入力値を確認してください。
0572E	number of location rule exceed <num>. Location ルールの登録に失敗しました。 Location ルールは、URL スイッチングルールと合わせて登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0573E	Invalid argument. Location ルールの登録に失敗しました。 不正な文字列を検出しました。 もう一度入力値を確認してください。
0574E	"*" may appear only at the beginning or end of the string. Location ルールの登録に失敗しました。 不正な文字列を検出しました。 URL 文字列のアスタリスク(*)は、文字列の先頭、または末尾にのみ指定可能です。 もう一度入力値を確認してください。

0575E	"*" may appear only at the beginning or end of the string.
	Location ルールの登録に失敗しました。 不正な文字列を検出しました。 パス文字列のアスタリスク(*)は、文字列の先頭、または末尾にのみ指定可能です。 もう一度入力値を確認してください。
0576E	number of rule exceed <num>.
	組み合わせルールの登録に失敗しました。 組み合わせルールは、Location ルール、URL スイッチングルールと合わせて登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0577E	Argument list too long.
	組み合わせルールの登録に失敗しました。 組み合わせルールで指定可能なルール数は最大で 4 件までです。 もう一度入力値を確認してください。
0578E	<str>: No such settings.
	組み合わせルールの登録に失敗しました。 指定されたルール名が、既存の設定に存在しません。 設定内容や入力値を、もう一度確認してください。
0579E	nested rule cannot be used within "expression" of another nested rule.
	組み合わせルールの登録に失敗しました。 組み合わせルール文字列内に組み合わせルールを含める事はできません。 設定内容や入力値を、もう一度確認してください。
0580E	location rule cannot be used within nested rules.
	組み合わせルールの登録に失敗しました。 組み合わせルール文字列内に Location ルールを含める事はできません。 設定内容や入力値を、もう一度確認してください。

0581E	Invalid argument. 組み合わせルールの登録に失敗しました。 不正な文字列を検出しました。 もう一度入力値を確認してください。
0582E	<str>: Settings already exists. ルールの登録に失敗しました。 ルール名"default"は、システムに予約されています。 ルール名を変更して、もう一度登録し直してください。
0583E	<str>: Settings already exists. ルールの登録に失敗しました。 同一ルール名の設定が既に存在しています。 もう一度入力値を確認してください。
0584E	Invalid argument. Location ルールの登録に失敗しました。 入力値の文法が正しくありません。 もう一度入力値を確認してください。
0585E	<str>: No such settings. ルールの削除に失敗しました。 指定されたルール名が、既存の設定に存在しません。 設定内容や入力値を、もう一度確認してください。
0586E	<str>: rule in use. ルール設定の削除に失敗しました。 このルールは仮想サーバー設定で使用しています。 このルールを削除する場合は、仮想サーバー設定モードの no match コマンドで設定を解除してください。
0587E	<str> is undeletable entry. ルール設定の削除に失敗しました。 このルールは組み合わせルール設定で使用しています。 このルールを削除する場合は、no rule nested コマンドで、該当の組み合わせルール設定を削除してください。

0588E	<str>: parameter error. リバース NAT エントリーの登録に失敗しました。 リバース NAT ポリシー文字列の文法に誤りがあります。 もう一度入力値を確認してください。
0589E	<str>: parameter error. リバース NAT エントリーの登録に失敗しました。 リバース NAT ポリシー文字列の文法に誤りがあります。 もう一度入力値を確認してください。
0590E	<num>: out of range. (0-65535) リバース NAT エントリーの登録に失敗しました。 不正なポート番号を検出しました。 ポート番号は 0-65535 の範囲で入力してください。
0591E	<str>: parameter error. リバース NAT エントリーの登録に失敗しました。 不正なプロトコル文字列を検出しました。 リバース NAT エントリーのプロトコルには、tcp、udp、ftp のいずれかを指定してください。
0592E	<str>: No such settings. リバース NAT エントリーの登録に失敗しました。 指定された NAT プールポリシーは存在しません。 設定内容や入力値を、もう一度確認してください。
0593E	<str>: Can not be registered at the same NAT pool and port number. リバース NAT エントリーの登録に失敗しました。 使用する NAT プールと、指定するポート番号が同一である場合、プロトコルが tcp のリバース NAT エントリーとプロトコルが ftp のリバース NAT エントリーは排他的です。 設定内容や入力値を、もう一度確認してください。

0594E	number of reverse-nat entry exceed <num>. リバース NAT エントリーの登録に失敗しました。 リバース NAT エントリーは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0595E	failed to moving reverse-nat mode. 内部エラーによりリバース NAT 設定モードへの遷移に失敗しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0596E	failed to moving reverse-nat mode. 内部エラーによりリバース NAT 設定モードへの遷移に失敗しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0597E	No such settings. リバース NAT エントリーの削除に失敗しました。 指定されたリバース NAT エントリーは存在しません。 設定内容や入力値を、もう一度確認してください。
0598E	<str>: parameter error. 実サーバーの有効化に失敗しました。 不正な実サーバーID を検出しました。 もう一度、入力値を確認してください。
0599E	No such settings. 実サーバーの有効化に失敗しました。 指定された IP アドレスの実サーバーは存在しません。 設定内容や入力値を、もう一度確認してください。
0600E	No such settings. 実サーバーの有効化に失敗しました。 指定された実サーバーは存在しません。 設定内容や入力値を、もう一度確認してください。
0601E	<str>: parameter error. 仮想サーバーの有効化に失敗しました。 不正な仮想サーバーID を検出しました。 もう一度、入力値を確認してください。

0602E	No such settings. 仮想ーバの有効化に失敗しました。 指定された IP アドレスの仮想サーバーは存在しません。 設定内容や入力値を、もう一度確認してください。
0603E	No such settings. 仮想サーバーの有効化に失敗しました。 指定された仮想サーバーは存在しません。 設定内容や入力値を、もう一度確認してください。
0604E	Failed to set data for kernel. 内部エラーにより ARP テーブル情報の取得に失敗しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0605E	Failed to set data for kernel. 内部エラーにより ARP テーブル情報の取得に失敗しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0606E	<str>: Address could not delete. 内部エラーにより ARP テーブルエントリーの削除に失敗しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0607E	This file is bind virtual-server. Please unbind to remove. ソーリーコンテンツの削除に失敗しました。 このソーリーコンテンツは仮想サーバー設定で使用しています。 コンテンツを削除する場合は、仮想サーバー設定モードの no bind content コマンドで、該当のコンテンツを仮想サーバー設定から解除してください。
0608E	No such settings. ソーリーコンテンツの削除に失敗しました。 入力されたコンテンツファイルが存在しません。 機器情報や入力値を、もう一度確認してください。

0609E	<str>: parameter error. リモートアクセスフィルター設定の変更に失敗しました。 不正なパラメーター文字列を検出しました。 もう一度、入力値を確認してください。
0610E	number of token error. リモートアクセスフィルター設定の変更に失敗しました。 サブネットマスクアドレスの指定がされていません。 もう一度、入力値を確認してください。
0611E	invalid address. リモートアクセスフィルター設定の変更に失敗しました。 不正なマスクアドレスを検出しました。 もう一度、入力値を確認してください。
0612E	<str>: invalid address. リモートアクセスフィルター設定の変更に失敗しました。 不正なアドレスを検出しました。 もう一度、入力値を確認してください。
0613E	<str>: Settings already exists. リモートアクセスフィルター設定の登録に失敗しました。 該当のフィルター設定は既に登録済みです。 設定内容や入力値をもう一度確認してください。
0614E	number of remote-mgmt settings exceed <num>. リモートアクセスフィルター設定の登録に失敗しました。 リモートアクセスフィルター設定は登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0615E	<str>: No such settings. リモートアクセスフィルター設定の削除に失敗しました。 入力された設定は存在しません。 設定内容や入力値を、もう一度確認してください。

0616E	<str>: account-name too long. (length:1-16)
	ユーザーアカウント設定の変更に失敗しました。 入力されたアカウント名が規定文字列長より長いため、設定の変更に失敗しました。 もう一度、入力値を確認してください。
0617E	number of user-account cannot exceed <num>.
	ユーザーアカウントの登録に失敗しました。 ユーザーアカウントは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0618E	Settings already exists.
	ユーザーアカウントの登録に失敗しました。 該当のユーザーアカウント名は既に登録済みです。 設定内容や入力値をもう一度確認してください。
0619E	Invalid argument.
	ユーザーアカウント設定の変更に失敗しました。 不正な入力値、または不正なコマンド文法を検出しました。 もう一度、入力値を確認してください。
0620E	password strings should be enclosed in double quotes.
	ユーザーアカウントの登録に失敗しました。 パスワードに二重引用符を含めたい場合、バックスラッシュ(¥)でエスケープし、かつパスワード文字列を二重引用符で囲んでください。
0621E	number of user-account cannot exceed <num>.
	ユーザーアカウントの登録に失敗しました。 ユーザーアカウントは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0622E	Settings already exists.
	ユーザーアカウントの登録に失敗しました。 該当のユーザーアカウント名は既に登録済みです。 設定内容や入力値をもう一度確認してください。

0623E	Sorry. 'web-account' is reserve name for system. ユーザーアカウントの登録に失敗しました。 該当のユーザーアカウント名はシステムに予約されています。 ユーザー名を変更して、もう一度登録してください。
0624E	Sorry. 'root' is reserve name for system. ユーザーアカウントの登録に失敗しました。 該当のユーザーアカウント名はシステムに予約されています。 ユーザー名を変更して、もう一度登録してください。
0625E	Sorry. 'seikoce' is reserve name for system. ユーザーアカウントの登録に失敗しました。 該当のユーザーアカウント名はシステムに予約されています。 ユーザー名を変更して、もう一度登録してください。
0626E	Sorry. 'confchk' is reserve name for system. ユーザーアカウントの登録に失敗しました。 該当のユーザーアカウント名はシステムに予約されています。 ユーザー名を変更して、もう一度登録してください。
0627E	password is too long. (length:1-32) ユーザーアカウントの登録に失敗しました。 不正なパスワードを検出しました。 パスワード文字列の最大長は 32 文字です。
0628E	The end of the password string can not be a blank. ユーザーアカウントの登録に失敗しました。 不正なパスワードを検出しました。 二重引用符で囲んだ場合であっても、パスワード文字列の末尾に、空白を指定する事はできません。
0630E	<str>: failed to create the account. 内部エラーにより、ユーザーアカウントの登録に失敗しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。

0631E	<str>: No such settings. ユーザーアカウントの削除に失敗しました。 入力されたアカウント名は存在しません。 設定内容や入力値を、もう一度確認してください。
0632E	your account data not found. 内部エラーにより、ユーザーアカウントの登録に失敗しました。 現在ログイン中のアカウントに関して、アカウント名をシステムから取得できません。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0633E	Operation not supported to delete the own account. ユーザーアカウントの削除に失敗しました。 自ユーザーアカウントを削除する事はできません。 設定内容や入力値を、もう一度確認してください。
0634E	<str>: failed to delete the account. 内部エラーにより、ユーザーアカウントの削除に失敗しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0635E	<str>: length over. 内部エラーにより、強制ログアウトが失敗しました。 不正な端末 ID を検出しました。 端末 ID は 0-99 の範囲で指定してください。
0636E	terminal-id <num>: clear error 内部エラーにより、強制ログアウトが失敗しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0637E	The static MAC address, please delete the "no mac address". 内部エラーにより、強制ログアウトが失敗しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0638E	<num>: socket error occurred. イーサネット統計情報のクリアに失敗しました。 内部エラー（Socket エラー）が発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。

0639E	forward packet number clear error. L2 フォワード統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0640E	forward byte number clear error. L2 フォワード統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0641E	flood packet number clear error. L2 フラッディング統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0642E	flood byte number clear error. L2 フラッディング統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0643E	IPv4 statistics clear error. L3 フォワード(ipv4)統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0644E	IPv6 statistics clear error. L3 フォワード(ipv6)統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0645E	L4 session clear error. L4 セッション情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。

0646E	L7 session clear error. L7 セッション情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0647E	SSL session clear error. SSL セッション情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0648E	SSL statistics clear error. SSL 統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0649E	SSL statistics clear error. SSL 統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0650E	VRRP statistics clear error. VRRP 統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0651E	HA statistics clear error. 同期統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0652E	PROBE statistics clear error. ヘルスチェック統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。

0653E	Server statistics clear error. サーバー統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0654E	Server statistics clear error. サーバー統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0655E	No such settings. サーバー統計情報のクリアに失敗しました。 指定された実サーバーID は存在しません。 設定内容や入力値をもう一度確認してください。
0656E	statistical data not found. 仮想サーバー統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0657E	<str>: parameter error. 仮想サーバー統計情報のクリアに失敗しました。 不正なパラメーターを検出しました。 もう一度、入力値を確認してください。
0658E	No such settings. 仮想サーバー統計情報のクリアに失敗しました。 指定された仮想サーバーID は存在しません。 設定内容や入力値をもう一度確認してください。
0659E	statistical data not found. 実サーバー統計情報のクリアに失敗しました。 内部エラーが発生しました。 恐れ入りますが、一旦ログアウトして、もう一度ログインし直してください。
0660E	<str>: parameter error. 実サーバー統計情報のクリアに失敗しました。 不正なパラメーターを検出しました。 もう一度、入力値を確認してください。

0661E	No such settings. 実サーバー統計情報のクリアに失敗しました。 指定された実サーバーID は存在しません。 設定内容や入力値をもう一度確認してください。
0662E	out of range. (1s-10m) システム変数の変更に失敗しました。
0663E	out of range. (1s-10m) システム変数の変更に失敗しました。
0664E	out of range. (1-10000000) システム変数の変更に失敗しました。
0665E	<str>: invalid address. NAT ログ設定の登録に失敗しました。 不正なアドレス形式を検出しました。 もう一度入力値を確認してください。
0666E	<str>: invalid argument. <facility.level>: <16-23>.<0-7> NAT ログ設定の登録に失敗しました。 不正なパラメーターを検出しました。 もう一度入力値を確認してください。
0667E	<str>: invalid argument. <facility.level>: <16-23>.<0-7> NAT ログ設定の登録に失敗しました。 不正なパラメーターを検出しました。 もう一度入力値を確認してください。
0668E	<str>: invalid argument. <facility.level>: <16-23>.<0-7> NAT ログ設定の登録に失敗しました。 不正なパラメーターを検出しました。 ログレベルは 0-7 の範囲で指定してください。
0669E	<str>: invalid argument. <facility.level>: <16-23>.<0-7> NAT ログ設定の登録に失敗しました。 不正なパラメーターを検出しました。 ファシリティーは 16-23 の範囲で指定してください。

0670E	channel <num>: No such settings. 指定された論理チャネル設定は存在しません。 設定内容や入力値をもう一度確認してください。
0671E	Argument list is too long. VLAN フィルタリング設定の登録に失敗しました。 VLAN ID は 640 文字以内で指定してください。
0672E	syntax error - <vlan-id> must be either a single vlan, multiple vlans separated by a comma(,), or a range of vlans separated by a hyphen(-) VLAN フィルタリング設定の登録に失敗しました。 VLAN ID を複数指定する場合は、ハイフン(-)またはカンマ(,)で VLAN ID 文字列を繋いでください。
0673E	<num>: out of range. (1-4094) VLAN フィルタリング設定の登録に失敗しました。 VLAN ID の範囲は 1-4094 です。 もう一度入力値を確認してください。
0674E	<num>: out of range. (1-4094) VLAN フィルタリング設定の登録に失敗しました。 VLAN ID の範囲は 1-4094 です。 もう一度入力値を確認してください。
0675E	Operation not supported on untagged channel. VLAN フィルタリング設定の登録に失敗しました。 タグ VLAN の設定がない場合、VLAN フィルターの設定はできません。 設定内容や入力値をもう一度確認してください。
0676E	Argument list is too long. VLAN フィルタリング設定の登録に失敗しました。 VLAN ID は 640 文字以内で指定してください。

0677E	syntax error - <vlan-id> must be either a single vlan, multiple vlans separated by a comma(,), or a range of vlans separated by a hyphen(-)
	VLAN フィルタリング設定の登録に失敗しました。 VLAN ID を複数指定する場合は、ハイフン(-)またはカンマ(,)で VLAN ID 文字列を繋いでください。
0678E	Argument list is too long.
	VLAN フィルタリング設定の登録に失敗しました。 VLAN ID を複数指定する場合は、ハイフン(-)またはカンマ(,)で VLAN ID 文字列を繋いでください。 また、区切り文字は 127 回まで使用する事ができます。
0679E	<num>: out of range. (1-4094)
	VLAN フィルタリング設定の登録に失敗しました。 VLAN ID の範囲は 1-4094 です。 もう一度入力値を確認してください。
0680E	<num>: out of range. (1-4094)
	VLAN フィルタリング設定の登録に失敗しました。 VLAN ID の範囲は 1-4094 です。 もう一度入力値を確認してください。
0681E	port<num>: Operation not supported on untagged channel.
	指定したポートの一部、または全てに対して、VLAN フィルタリング設定の登録に失敗しました。 タグ VLAN の設定がない場合、VLAN フィルターの設定はできません。 設定内容や入力値をもう一度確認してください。
0682E	Operation not supported on mirror port. (port<num>)
	チャネル設定の登録に失敗しました。 ミラーポートを論理チャネルとして設定する事はできません。 設定内容や入力値をもう一度確認してください。

0683E	port<num>: <mismatch-settings>… port<num>: <mismatch-settings>…
	チャネル設定の登録に失敗しました。 論理チャネルを形成するポート群に、設定上のミスマッチが発生しています。 以下に挙げる設定は、論理チャネルを形成するイーサネットポート間で同一である必要があります。 ・VLAN ID (vlan) ・タグ VLAN (tagged) ・ネイティブ VLAN (native-vlan) ・VLAN フィルター (allowed-vlan) ・プライベート VLAN (protected) ・スパニングツリー (spanning-tree) ・バランシングポート定義 (slb) 設定内容や入力値をもう一度確認してください。
0684E	port<num>: <mismatch-settings>… port<num>: <mismatch-settings>…
	チャネル設定の登録に失敗しました。 論理チャネルを形成するイーサネットポート間では VLAN ID を同一にする必要があります。 設定内容や入力値をもう一度確認してください。
0685E	port<num>: <mismatch-settings>… port<num>: <mismatch-settings>…
	チャネル設定の登録に失敗しました。 論理チャネルを形成するイーサネットポート間では VLAN フィルタリング設定を同一にする必要があります。 設定内容や入力値をもう一度確認してください。
0686E	port<num>: <mismatch-settings>… port<num>: <mismatch-settings>…
	チャネル設定の登録に失敗しました。 論理チャネルを形成するイーサネットポート間ではスパニングツリー設定を同一にする必要があります。 設定内容や入力値をもう一度確認してください。

0687E	port<num>: <mismatch-settings>… port<num>: <mismatch-settings>…
	チャネル設定の登録に失敗しました。 論理チャネルを形成するイーサネットポート間では接続先ポート種別設定を同一にする必要があります。 設定内容や入力値をもう一度確認してください。
0688E	Operation not supported on transparent mode.
	チャネル設定の登録に失敗しました。 フェイルスルー設定がされている場合、論理チャネルを設定する事はできません。 設定内容や入力値をもう一度確認してください。
0689E	<num>: do not permit the channel number other than 1.
	チャネル設定の登録に失敗しました。 本機種で指定可能な論理チャネル番号は 1 のみです。 もう一度入力値を確認してください。
0690E	<num>: out of range. (1-<num>)
	チャネル設定の登録に失敗しました。 不正な論理チャネル番号を検出しました。 本製品で指定可能な論理チャネル番号を確かめて、もう一度登録し直してください。
0691E	Multiple mirror ports not supported.
	ミラーポートの設定に失敗しました。 複数のポートをミラーポートに設定する事はできません。 もう一度入力値を確認してください。
0692E	port<num>: Operation not permitted on monitor port.
	ミラーポートの設定に失敗しました。 モニタリングポートをミラーポートに設定する事はできません。 設定内容や入力値をもう一度確認してください。
0693E	port<num>: Operation not permitted on aggregated port.
	ミラーポートの設定に失敗しました。 論理チャネルを形成するポートをミラーポートに設定する事はできません。 設定内容や入力値をもう一度確認してください。

0694E	vlan <num>: No such settings. 論理チャネルに対する VLAN の設定に失敗しました。 入力された VLAN ID は存在しません。 設定内容や入力値をもう一度確認してください。
0695E	Operation not supported on tagged port. 論理チャネルに対する VLAN の設定に失敗しました。 タグ VLAN 設定がされているチャネルに対して VLAN ID の設定はできません。 設定内容や入力値をもう一度確認してください。
0696E	vlan <num>: No such settings. イーサネットポートに対する VLAN の設定に失敗しました。 入力された VLAN ID は存在しません。 設定内容や入力値をもう一度確認してください。
0697E	port<num>: Operation not supported on tagged port. イーサネットポートに対する VLAN の設定に失敗しました。 タグ VLAN 設定がされているポートに対して VLAN ID の設定はできません。 設定内容や入力値をもう一度確認してください。
0698E	port<num>: Operation not permitted on aggregated port. イーサネットポートに対する VLAN の設定に失敗しました。 このイーサネットポートは論理チャネルを形成しています。 ポートの属する VLAN ID を変更する場合は、論理チャネル設定モードから実施してください。
0699E	port<num>: Operation not permitted on mirror port. モニタリングポートの設定に失敗しました。 ミラーポートをモニタリングポートに設定する事はできません。
0700E	<num>: No such settings. L2 フィルタリング設定の起動に失敗しました。 入力された MAC アクセスリストは存在しません。 設定内容や入力値をもう一度確認してください。

0701E	<num>: List empty. L2 フィルタリング設定の起動に失敗しました。 入力された MAC アクセスリストには、フィルタリングルールの登録がありません。 このアクセスリストを適用するには、MAC アクセスリスト設定モードでフィルタリングルールを登録してください。
0702E	chan<num>: Operation not supported on untagged channel. 論理チャネルに対するネイティブ VLAN の設定に失敗しました。 ネイティブ VLAN を設定するには、タグ VLAN が設定されている必要があります。 設定内容や入力値をもう一度確認してください。
0703E	<num>: out of range. (1-4094) 論理チャネルに対するネイティブ VLAN 設定の登録に失敗しました。 VLAN ID の範囲は 1-4094 です。 もう一度入力値を確認してください。
0704E	<num>: out of range. (1-4094) イーサネットポートに対するネイティブ VLAN 設定の登録に失敗しました。 VLAN ID の範囲は 1-4094 です。 もう一度入力値を確認してください。
0705E	port<num>: Operation not supported on untagged channel. イーサネットポートに対するネイティブ VLAN の設定に失敗しました。 ネイティブ VLAN を設定するには、タグ VLAN が設定されている必要があります。 設定内容や入力値をもう一度確認してください。
0706E	Operation not supported on tagged port. 論理チャネルに対するプライベート VLAN の設定に失敗しました。 タグ VLAN 設定がされているチャネルに対してプライベート VLAN の設定はできません。 設定内容や入力値をもう一度確認してください。

0707E	port<num>: Operation not supported on tagged port. イーサネットポートに対するプライベート VLAN の設定に失敗しました。 タグ VLAN 設定がされているポートに対してプライベート VLAN の設定はできません。 設定内容や入力値をもう一度確認してください。
0708E	port<num>: Operation not permitted on aggregated port. イーサネットポートに対するプライベート VLAN の設定に失敗しました。 このイーサネットポートは論理チャネルを形成しています。 プライベート VLAN 設定を変更する場合は、論理チャネル設定モードから実施してください。
0709E	port<num>: Operation not permitted on aggregated port. イーサネットポートに対する接続先ポート設定の変更に失敗しました。 このイーサネットポートは論理チャネルを形成しています。 接続先ポート設定を変更する場合は、論理チャネル設定モードから実施してください。
0710E	<num>: out of range. (0-240 in steps of 16) スパニングツリープライオリティーの設定に失敗しました。 不正なプライオリティー値を検出しました。 プライオリティーは 0-240 の範囲、かつ 16 の倍数で設定してください。
0711E	port<num>: stp not enabled on port. スパニングツリープライオリティーの設定に失敗しました。 このポートではスパニングツリー設定が有効になっていません。 設定内容や入力値をもう一度確認してください。
0712E	port<num>: Operation not permitted on aggregated port. スパニングツリープライオリティーの設定に失敗しました。 このイーサネットポートは論理チャネルを形成しています。 スパニングツリー設定を変更する場合は、論理チャネル設定モードから実施してください。

0713E	<num>: out of range. (0-240 in steps of 16)
	スパニングツリープライオリティーの設定に失敗しました。 不正なプライオリティー値を検出しました。 プライオリティーは 0-240 の範囲、かつ 16 の倍数で設定してください。
0714E	chan<num>: stp not enabled on channel.
	スパニングツリープライオリティーの設定に失敗しました。 このチャネルではスパニングツリー設定が有効になっていません。 設定内容や入力値をもう一度確認してください。
0715E	<num>: out of range. (1-200000000)
	STP コストの設定に失敗しました。 不正な STP コストを検出しました。 STP コストは 1-200000000 の範囲で設定してください。 設定内容や入力値をもう一度確認してください。
0716E	port<num>: stp not enabled on port.
	STP コストの設定に失敗しました。 このポートではスパニングツリー設定が有効になっていません。 設定内容や入力値をもう一度確認してください。
0717E	port<num>: Operation not permitted on aggregated port.
	STP コストの設定に失敗しました。 このイーサネットポートは論理チャネルを形成しています。 スパニングツリー設定を変更する場合は、論理チャネル設定モードから実施してください。
0718E	<num>: out of range. (1-200000000)
	STP コストの設定に失敗しました。 不正な STP コストを検出しました。 STP コストは 1-200000000 の範囲で設定してください。 設定内容や入力値をもう一度確認してください。
0719E	chan<num>: stp not enabled on channel.
	STP コストの設定に失敗しました。 この論理チャネルではスパニングツリー設定が有効になっていません。 設定内容や入力値をもう一度確認してください。

0720E	port<num>: stp not enabled on port. STP コストの設定に失敗しました。 このポートではスパニングツリー設定が有効になっていません。 設定内容や入力値をもう一度確認してください。
0721E	port<num>: Operation not permitted on aggregated port. STP エッジポート設定に失敗しました。 このイーサネットポートは論理チャネルを形成しています。 STP エッジポート設定を変更する場合は、論理チャネル設定モードから実施してください。
0722E	chan<num>: stp not enabled on channel. STP コストの設定に失敗しました。 この論理チャネルではスパニングツリー設定が有効になっていません。 設定内容や入力値をもう一度確認してください。
0723E	port<num>: stp not enabled on port. スパニングツリーのリスタートに失敗しました。 このポートではスパニングツリー設定が有効になっていません。 設定内容や入力値をもう一度確認してください。
0724E	port<num>: Operation not permitted on aggregated port. スパニングツリーのリスタートに失敗しました。 このイーサネットポートは論理チャネルを形成しています。 スパニングツリーをリスタートする場合は、論理チャネル設定モードから実施してください。
0725E	chan<num>: stp not enabled on channel. スパニングツリーのリスタートに失敗しました。 この論理チャネルではスパニングツリー設定が有効になっていません。 設定内容や入力値をもう一度確認してください。
0726E	<num>: out of range. (1-200000000) STP コストの設定に失敗しました。 不正な STP コストを検出しました。 STP コストは 1-200000000 の範囲で設定してください。 設定内容や入力値をもう一度確認してください。

0727E	Operation not supported in transparent mode. スパニングツリー設定に失敗しました。 フェイルスルー設定がされている場合、スパニングツリーを有効にできません。 設定内容や入力値をもう一度確認してください。
0728E	port<num>: Operation not permitted on aggregated port. スパニングツリー設定に失敗しました。 このイーサネットポートは論理チャネルを形成しています。 スパニングツリーを設定する場合は、論理チャネル設定モードから実施してください。
0729E	unmatch tagged settings on port1 and port2. (cannot start transparent mode) タグ VLAN 設定に失敗しました。 フェイルスルー設定である場合、イーサネットポート 1 とイーサネットポート 2 のタグ VLAN の有効/無効は同一である必要があります。
0730E	port<num>: Operation not permitted on aggregated port. タグ VLAN 設定に失敗しました。 このイーサネットポートは論理チャネルを形成しています。 タグ VLAN を設定する場合は、論理チャネル設定モードから実施してください。
0731E	<num>: out of range. (1-200000000) STP コストの設定に失敗しました。 不正な STP コストを検出しました。 STP コストは 1-200000000 の範囲で設定してください。 設定内容や入力値をもう一度確認してください。
0732E	Operation not supported in transparent mode. スパニングツリー設定に失敗しました。 フェイルスルー設定がされている場合、スパニングツリーを有効にできません。 設定内容や入力値をもう一度確認してください。
0733E	out of range. (0s-100s) VRRP 遅延時間設定の変更に失敗しました。 遅延時間は 0s-100s の間で設定してください。

0734E	<num>: out of range. (1s-4095s) VRRP 送信間隔の変更に失敗しました。 送信間隔は 1s-4095s の間で設定してください。
0735E	<str>: invalid address. 冗長構成相手機器のアドレス設定に失敗しました。 不正な IP アドレスを検出しました。 もう一度入力値を確認してください。
0736E	not exist same network address. 冗長構成相手機器のアドレス設定に失敗しました。 入力されたアドレスは、既存 VLAN に設定されているどのネットワークアドレスにも合致しません。 冗長構成相手機器のアドレスには、本製品に設定されているネットワークアドレス内のアドレスを設定してください。 設定内容や入力値をもう一度確認してください。
0737E	<num>: out of range. (1-10) ポート監視設定に失敗しました。 ポート監視グループは 1-10 の範囲で設定してください。
0738E	<num>: out of range. (1-253) ポート監視設定に失敗しました。 プライオリティー減算値は 1-253 の範囲で設定してください。
0739E	group <num>: No such settings. ポート監視設定の削除に失敗しました。 指定されたグループ ID は既存設定に存在しません。 設定内容や入力値をもう一度確認してください。
0740E	<num>: out of range. (1-254) VRRP プライオリティー設定の変更に失敗しました。 VRRP プライオリティーは 1-254 の範囲で設定してください。
0741E	<num>: out of range. (1-254) VRRP プライオリティー設定の変更に失敗しました。 VRRP プライオリティーは 1-254 の範囲で設定してください。

0742E	<str>: No such settings. 仮想サーバー名の設定に失敗しました。 入力された仮想サーバー名は、既に存在します。 設定する場合は、既存設定を変更、または削除してください。
0743E	level <num>: out of range. (0-7) テスト用ログの出力に失敗しました。 ログレベルは 0-7 の範囲で指定してください。
0744E	config-sync process failed to connect. 全設定情報の同期に失敗しました。 同期通信にエラーが発生しました。 設定情報の同期には、以下の設定がされている必要があります。 ・VRID の設定 ・冗長相手先アドレスの設定 これらの設定を見直してください。 また、これらの設定が正しい場合は内部エラーが発生した可能性があります。 恐れ入りますが、ログインし直してもう一度実行してください。
0745E	webconfig file not found. 内部エラーにより、WEB 表示用設定ファイルの同期に失敗しました。 恐れ入りますが、ログインし直してもう一度実行してください。
0747E	This ssl-policy is used in virtual-server. (But the csr.pem was delete.) SSL ポリシーに紐づく CSR ファイルの削除に成功しました。 しかし、この SSL ポリシーは仮想サーバーにバインドされているため、CSR 生成時に作成された鍵ファイルは削除できません。 削除する場合は仮想サーバー設定モードの no ssl コマンドで、該当の SSL ポリシーを解除してください。
0748E	illegal name - only alphanumeric, hyphen(-) or underscore(_) or square(#) or commercial at(@) allowed. 不正な文字列を検出しました。 ハイフン、アンダーバー、ドット、シャープ、アット以外の記号の使用は認められていません。 もう一度入力値を確認してください。

0749E	Argument list is too long. VLAN フィルタリング設定の登録に失敗しました。 VLAN ID を複数指定する場合は、ハイフン(-)またはカンマ(,)で VLAN ID 文字列を繋いでください。 また、区切り文字は 127 回まで使用する事ができます。
0750E	Multiple mirror ports not supported. イーサネットポートに対するミラーリング設定に失敗しました。 既にミラーポートに設定されているイーサネットポートが存在します。 ミラーポートに設定できるイーサネットポートは 1 ポートのみです。 設定内容や入力値をもう一度確認してください。
0751E	peer-address settings not found on this machine. 冗長相手機器への情報同期に失敗しました。 冗長相手先アドレスの設定がされていません。 設定内容や入力値をもう一度確認してください。
0752E	webconfig file not found. 内部エラーにより、WEB 表示用設定ファイルの同期に失敗しました。 WEB 管理画面から実行された同様のコマンド要求が完結されないままでいます。 恐れ入りますが、WEB 表示用設定ファイルをインポートする場合、一旦、WEB 管理画面の[システム] > [機器管理] > [画面表示状態インポート]画面から操作してください。
0753E	failed to import webconfig file. 内部エラーにより、WEB 表示用設定ファイルの同期に失敗しました。 恐れ入りますが、ログインし直してもう一度実行してください。
0754E	invalid address. IPv4NAT プールの変更に失敗しました。 不正なプールアドレスを検出しました。 もう一度入力値を確認してください

0755E	invalid address range. IPv4NAT プールの変更に失敗しました。 不正なアドレス範囲を検出しました。 プールアドレスは 16 件まで範囲指定可能です。 範囲指定でなく、1 件のプールアドレスのみを設定する場合は「開始 IP アドレス」にだけ入力してください。
0756E	There is a virtual IP in the range. IPv4NAT プールの変更に失敗しました。 不正なアドレス範囲を検出しました。 アドレス範囲を指定する場合は、仮想 IP アドレスがその範囲に含まれてはいけません。 仮想 IP アドレスを設定する場合は、「開始 IP アドレス」にのみ入力して設定してください。
0757E	have exceeded the upper limit of the setting range. IPv4NAT プールの変更に失敗しました。 プールアドレスは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0758E	invalid address. IPv6NAT プールの変更に失敗しました。 不正なプールアドレスを検出しました。 もう一度入力値を確認してください。
0759E	invalid address range. IPv6NAT プールの変更に失敗しました。 不正なアドレス範囲を検出しました。 プールアドレスは 16 件まで範囲指定可能です。 範囲指定でなく、1 件のプールアドレスのみを設定する場合は「開始 IP アドレス」にだけ入力してください。
0760E	There is a virtual IP in the range. IPv6NAT プールの変更に失敗しました。 不正なアドレス範囲を検出しました。 アドレス範囲を指定する場合は、仮想 IP アドレスがその範囲に含まれてはいけません。 仮想 IP アドレスを設定する場合は、「開始 IP アドレス」にのみ入力して設定してください。

0761E	have exceeded the upper limit of the setting range. IPv6NAT プールの変更に失敗しました。 プールアドレスは登録可能な最大設定数に達しています。 設定を追加する場合は、既存の設定情報を削除してください。
0800E	host name too long. ホストまでの経路確認に失敗しました。 ホスト名で指定可能な文字数は最大 255 文字です。 入力値を、もう一度確認してください。
0801E	Host name search is required DNS settings. ホストまでの経路確認に失敗しました。 DNS サーバーが設定されていません。 ホスト名を使用する場合は、[システム] > [ネットワーク] > [DNS サーバー]画面で、 DNS サーバーを設定してください。
0802E	<str>: invalid address. ホストまでの経路確認に失敗しました。 不正なアドレス文字列を検出しました。 入力値を、もう一度確認してください。
0803E	<str>: invalid address. ホストまでの経路確認に失敗しました。 不正なアドレス文字列を検出しました。 入力値を、もう一度確認してください。
0804E	<num>: out of range. (0-15) ルーティング番号に、規定外の値が入力されました。 ルーティング番号は 0-15 の範囲で設定してください。
0805E	<str>: No such data. ホストまでの経路確認に失敗しました。 存在しない仮想サーバーのアドレスが入力されました。 入力値を、もう一度確認してください。
0806E	<str>: invalid address. ホストまでの経路確認に失敗しました。 不正なアドレス文字列を検出しました。 入力値を、もう一度確認してください。
0807E	<num>: out of range. (0-15) ルーティング番号に、規定外の値が入力されました。 ルーティング番号は 0-15 の範囲で設定してください。

0808E	<num>: out of range. (0-15) ルーティング番号に、規定外の値が入力されました。 ルーティング番号は 0-15 の範囲で設定してください。
0809E	<num>: out of range. (0-15) ルーティング番号に、規定外の値が入力されました。 ルーティング番号は 0-15 の範囲で設定してください。
0810E	<num>: out of range. (0-15) ルーティング番号に、規定外の値が入力されました。 ルーティング番号は 0-15 の範囲で設定してください。
0811E	<num>: out of range. (0-15) ルーティング番号に、規定外の値が入力されました。 ルーティング番号は 0-15 の範囲で設定してください。
0812E	<num>: out of range. (0-15) ルーティング番号に、規定外の値が入力されました。 ルーティング番号は 0-15 の範囲で設定してください。
0813E	please specify any of the management-address or redundant-address or virtual-address or NAT pool-address. ホストまでの経路確認に失敗しました。 送信元 IP には「管理 IP アドレス」か「冗長 IP アドレス」か「仮想 IP アドレス」か「NAT プールアドレス」のいずれかを選択してください。
0814E	alphanumeric and following symbols"!#$%&'*+.^_`\|~-" allowed. クッキー名の設定に失敗しました。 クッキー名の指定で、不正な文字を検出しました。 『!#$%&'*+.^_`|~-』以外の記号の使用は認められていません。
0815E	<num>: out of range. (1-32) ホストまでの経路確認に失敗しました。 ホップ数は 1-32 の範囲で選択してください。
0816E	access log is not available with TCP Port 0. アクセスログ設定の登録に失敗しました。 TCP ポート 0 指定の仮想サーバーに対して、アクセスログ設定はできません。
0817E	sorry contents is not available with TCP Port 0. ソーリーコンテンツ設定に失敗しました。 TCP ポート 0 指定の仮想サーバーに対して、ソーリーコンテンツ設定はできません。

0818E	NATPT switch is not available with TCP Port 0. 実サーバーのバインドに失敗しました。 TCP ポート 0 指定の仮想サーバーに対して、IPv4<-->IPv6 変換設定はできません。
0819E	URL switch is not available with TCP Port 0. URL スイッチンググループ ID 設定、または URL リダイレクト設定、または 403 応答設定のいずれかで、設定の変更に失敗しました。 TCP ポート 0 指定の仮想サーバーに対して、これらの設定はできません。
0820E	ssl acceleration is not available with TCP Port 0. SSL アクセラレーション設定に失敗しました。 TCP ポート 0 指定の仮想サーバーに対して、SSL アクセラレーション設定はできません。
0821E	SSL sticky is not available with TCP Port 0. SSL セッション維持設定に失敗しました。 TCP ポート 0 指定の仮想サーバーに対して、SSL セッション維持設定はできません。
0822E	cookie sticky is not available with TCP Port 0. cookie セッション維持設定に失敗しました。 TCP ポート 0 指定の仮想サーバーに対して、cookie セッション維持設定はできません。
0823E	header insert is not available with TCP Port 0. ヘッダー挿入設定(X-Forwarded)に失敗しました。 TCP ポート 0 指定の仮想サーバーに対して、ヘッダー挿入設定(X-Forwarded)はできません。
0824E	URL is too long. 全実サーバーDOWN 時のリダイレクト先 URL 設定の変更に失敗しました。 不正な URL 文字列を検出しました。 リダイレクト先に指定する URL 文字列は 512 文字以内で入力してください。
0825E	scheme not supported. 全実サーバーDOWN 時のリダイレクト先 URL 設定の登録に失敗しました。 不正な URL 文字列を検出しました。 URL 文字列はhttp://またはhttps://で開始してください。
0826E	scheme not supported. 全実サーバーDOWN 時のリダイレクト先 URL 設定の登録に失敗しました。 不正な URL 文字列を検出しました。 URL 文字列はhttp://またはhttps://で開始してください。

0827E	host is empty. 全実サーバーDOWN 時のリダイレクト先 URL 設定の登録に失敗しました。 不正な URL 文字列を検出しました。 ホストアドレス部が空になっています。 入力値を確認して、もう一度登録し直してください。
0830E	maxconns <num>: out of range. (0-65535) 最大コネクション数の設定に失敗しました。 入力されたコネクション数が規定の範囲外です。 0-65535 の範囲で設定してください。
0835E	failed to get L7 session info. L7 セッション情報の取得に失敗しました。
0836E	Deny and permit rules can not be mixed. 拒否ルールと許可ルールを混在させることはできません。
0837E	Execution is impossible when packet trace is ON. Please turn off packet-trace. パケットトレースが ON の時は実行できません。 パケットトレースを OFF にしてください。
0838E	<str>: parameter error. 不正なアドレスを検出しました。 入力値をもう一度確認してください。
0839E	<num>: out of range. (0-32) マスク長に規定外の値が入力されました。 IPv4 アドレスのマスク長は 0-32 の範囲で設定してください。
0840E	<num>: out of range. (0-128) プレフィックス長に規定外の値が入力されました。 IPv6 アドレスのプレフィックス長は 0-128 の範囲で設定してください。
0841E	<num>: out of range. (1-65535) ポート番号に、規定外の値が入力されました。 ポート番号は 1-65535 の範囲で設定してください。
0842E	filter list4: No such settings. 内部エラーにより、パケットトレース設定モードの情報が取得できませんでした。 設定に失敗した恐れがあります。 もう一度、パケットトレース設定画面へ入り、設定をやり直してください。

0843E	<str>: parameter error. 不正なサーバー名、サーバーID を検出しました。 入力値をもう一度確認してください。
0844E	<str>: parameter error. 不正なサーバーID を検出しました。 入力値をもう一度確認してください。
0845E	<str>: parameter error. 不正な IP アドレス、ポート番号を検出しました。 入力値をもう一度確認してください。
0846E	<str>: parameter error. 不正なヘルスチェック名を検出しました。 入力値をもう一度確認してください。
0847E	<num>: Invalid types. Please type '256' or '384'. CSR の登録に失敗しました。 不正な鍵長が指定されました。 鍵長は 256, 384 のいずれかを指定してください。
0848E	failed to create keylen file. 内部エラーにより、CSR の作成に失敗しました。 入力値をもう一度確認し、やり直してください
0851E	Address already in use. 入力した管理 IP アドレスは、既に冗長 IP アドレスとして使用されているアドレスです。 もう一度入力値を確認してください。
0853E	<str>: Address already in use. 入力した仮想 IP アドレスは、既に冗長 IP アドレスとして使用されているアドレスです。 もう一度入力値を確認してください。
0855E	Address already in use. 入力した冗長 IP アドレスは、既に仮想 IP アドレスとして使用されているアドレスです。 もう一度入力値を確認してください。
0856E	<str>: Address already in use. 入力したアドレスは、NAT プールアドレスに登録されています。 もう一度入力値を確認してください。

0857E	<str>: Address already in use. 入力した冗長 IP アドレスは、静的 ARP テーブルエントリーとして登録されています。 もう一度入力値を確認してください。
0858E	Address that is registered in the static arp table is included. 入力した NAT プールアドレスは、静的 ARP テーブルエントリーとして登録されています。 もう一度入力値を確認してください。
0859E	<str>: Address already in use. 入力したアドレスは、NAT プールアドレスに登録されています。 もう一度入力値を確認してください。
0860E	<str>: Address already in use. 入力した仮想 IP アドレスは、静的 NDP テーブルエントリーとして登録されています。 もう一度入力値を確認してください。
0861E	<str>: Address already in use. 入力した冗長 IP アドレスは、静的 NDP テーブルエントリーとして登録されています。 もう一度入力値を確認してください。
0862E	Address that is registered in the static ndp table is included. 入力した NAT プールアドレスは、静的 NDP テーブルエントリーとして登録されています。 もう一度入力値を確認してください。
0863E	Address already in use. 入力した管理 IP アドレスは、静的 ARP テーブルエントリーとして登録されています。 もう一度入力値を確認してください。
0864E	Address already in use. 入力した管理 IP アドレスは、静的 NDP テーブルエントリーとして登録されています。 もう一度入力値を確認してください。
0865E	Address already in use. 入力した管理 IP アドレスは、NAT プールアドレスに登録されています。 もう一度入力値を確認してください。

0866E	<str>: Address already in use. 入力した冗長 IP アドレスは、NAT プールアドレスに登録されています。 もう一度入力値を確認してください。
0869E	Address is already in use as the MIP. 入力したアドレスは、既に管理 IP アドレスとして登録されています。 もう一度入力値を確認してください。
0870E	Address is already in use as the MIP. 入力したアドレスは、既に管理 IP アドレスとして登録されています。 もう一度入力値を確認してください。
0871E	Address is already in use as the Redundant IP. 入力したアドレスは、既に冗長 IP アドレスとして登録されています。 もう一度入力値を確認してください。
0872E	Address is already in use as the Redundant IP. 入力したアドレスは、既に冗長 IP アドレスとして登録されています。 もう一度入力値を確認してください。
0873E	vlan <num>: No such settings. SNMP トラップエージェントアドレスの設定に失敗しました。 入力された VLAN ID は存在しません。 設定内容や入力値をもう一度確認してください。
0874E	There is no MIPv4 settings in the selected VLAN. SNMP トラップエージェントアドレスの設定に失敗しました 入力された VLAN に IPv4 アドレスが設定されていません。 設定内容や入力値をもう一度確認してください。
0875E	VLAN is in use as "snmp trap agent-address". VLAN の削除に失敗しました。 この VLAN は現在 SNMP トラップエージェントアドレスに割り当てられています。 [システム] > [ネットワーク] > [SNMP 設定] > [SNMP トラップエージェントアドレス設定]で、VLAN ID の割り当てを解除してから VLAN を削除してください。
0876E	MIPv4 is in use as "snmp trap agent-address". 管理 IP アドレスの削除に失敗しました。 この VLAN は、現在 SNMP トラップエージェントアドレスとして使用されています。 [システム] > [ネットワーク] > [SNMP 設定] > [SNMP トラップエージェントアドレス設定]で、VLAN ID の割り当てを解除してから管理 IP アドレスを削除してください。

0877E	Operation not supported for non-HTTP servers.
	全実サーバーDOWN 時のリダイレクト先 URL の設定に失敗しました。 UDP、または FTP 仮想サーバーに対して該当の設定はできません。 設定内容や入力値をもう一度確認してください。
0878E	Operation not supported for non-HTTP servers.
	ソーリーコンテンツ設定に失敗しました。 UDP、または FTP 仮想サーバーに対して該当の設定はできません。 設定内容や入力値をもう一度確認してください。
0879E	Operation not supported for non-HTTP servers.
	クライアント証明書ヘッダー挿入の設定に失敗しました。 UDP、または FTP 仮想サーバーに対して該当の設定はできません。 設定内容や入力値をもう一度確認してください。
0880E	Operation not supported for non-HTTP servers.
	SSL セッション ID ヘッダー挿入の設定に失敗しました。 UDP、または FTP 仮想サーバーに対して該当の設定はできません。 設定内容や入力値をもう一度確認してください。
0881E	fallback-url is not available with DSR.
	全実サーバーDOWN 時のリダイレクト先 URL の設定に失敗しました。 仮想サーバーが DSR 設定で動作しています。 全実サーバーDOWN 時のリダイレクト先 URL の設定は DSR 設定と併用できません。 もう一度入力値を確認してください。
0882E	out of range. (1-<32 or 128>)
	マスク／プレフィックス長に規定外の値が入力されました。 IPv4 アドレスのマスク長は 1-32 の範囲で設定してください。 IPv6 アドレスのプレフィックス長は 1-128 の範囲で設定してください。
0883E	address family is unmatch.
	仮想サーバーグループの設定に失敗しました。 グループ内の各仮想サーバーは全て同じアドレスファミリーである必要があります。 設定内容や入力値を確認し、もう一度設定し直してください。
0884E	out of range. (1s-10s)
	送信遅延時間の設定に失敗しました。 送信遅延時間は 1s-10s の範囲で設定してください。

0885E	This vlan is necessary for route and can not be deleted. この VLAN はルート設定に必要であり、削除することはできません。
0886E	ECDHE is unsupported cipher suites. この機器は ECDHE 系の暗号スイートに対応していません。 設定内容や入力値をもう一度確認してください。
0887E	ECDHE is unsupported cipher suites. この機器は ECDHE 系の暗号スイートに対応していません。 設定内容や入力値をもう一度確認してください。
0888E	ECDHE is unsupported cipher suites. この機器は ECDHE 系の暗号スイートに対応していません。 設定内容や入力値をもう一度確認してください。
0889E	This management IPv4 address is necessary for the route and can not be changed. この管理 IPv4 アドレスはルート設定に必要であり、異なるネットワークアドレスに変更することはできません。 IPv4 アドレスをもう一度確認してください。
0890E	This management IPv6 address is necessary for the route and can not be changed. この管理 IPv6 アドレスはルート設定に必要であり、異なるネットワークアドレスに変更>することはできません。 IPv6 アドレスをもう一度確認してください。
0891E	This management IPv4 address is necessary for the route and can not be deleted. この管理 IPv4 アドレスはルート設定に必要であり、削除することはできません。 IPv4 アドレスをもう一度確認してください。
0892E	This management IPv6 address is necessary for the route and can not be deleted. この管理 IPv6 アドレスはルート設定に必要であり、削除することはできません。 IPv6 アドレスをもう一度確認してください。
0893E	Detected invalid key type. 不正な鍵ファイルを検出したため、ファイルのインポートに失敗しました。 インポート対象のファイルを確認し、もう一度インポートし直してください。

0894E	must be configured 'IP rule' settings before configuring the xff-balancing settings on this virtual server.
	XFF スイッチング（XFF ヘッダ情報の参照）設定の変更に失敗しました。 XFF スイッチング設定をするには、IP アドレス負荷分散ルールが設定されている必要があります。 IP アドレス負荷分散ルールを設定してから、やり直してください。
0920E	Option 'secure'　must be set to a single port.
	管理専用ポート設定に失敗しました。 複数のポートが指定されています。 管理専用ポートは任意の単一ポートにのみ設定可能です。
0921E	A secure management port can not belong to a VLAN in which a management IP address is not set.
	管理専用ポート設定に失敗しました。 このポートが所属する VLAN に、装置 IP アドレスが設定されていません。 管理専用ポートの所属するVLANは装置IPアドレスが設定されている必要があります。 装置 IP アドレスの設定をした後に、もう一度設定し直してください。
0922E	A secure management port can not belong to a VLAN in which a virtual server IP address is set.
	管理専用ポート設定に失敗しました。 このポートが所属する VLAN に、仮想サーバーIP アドレスが設定されています。 管理専用ポートの所属するVLANには仮想サーバーIPアドレスが設定されていない必要があります。 仮想サーバーIP アドレスを削除して、もう一度設定し直してください。
0923E	A secure management port can not belong to a VLAN to which other ports belong.
	管理専用ポート設定に失敗しました。 このポートが所属する VLAN には、複数のポートが割当たっています。 管理専用ポートの所属する VLAN には、管理専用ポートのみ所属している必要があります。 該当の VLAN からその他のポートを除外して、もう一度設定し直してください。
0924E	Secure management port(portX) is already configured.
	管理専用ポート設定に失敗しました。 本システムには、既に管理専用ポートが存在します。 該当ポートの管理専用ポート設定を解除してから、もう一度設定し直してください。

0925E	Can not configure a tagged port as a secure management port. 管理専用ポート設定に失敗しました。 トランクポートを管理専用ポートに設定することはできません。 タグ VLAN の設定を解除してから、もう一度設定し直してください。
0926E	Spanning tree can not be set on the secure management port. スパニングツリー設定に失敗しました。 指定されたポートに管理専用ポートが含まれています。 管理専用ポートにスパニングツリーを設定することはできません。 該当ポートの管理専用ポート設定を解除してから、もう一度設定し直してください。
0927E	Cannot set 'the virtual server IP address' for the VLAN to which the secure management port(port<num>) belongs. 仮想サーバーIP アドレスの設定に失敗しました。 管理専用ポートが所属する VLAN には、仮想サーバーIP アドレスを設定することはできません。 該当ポートの管理専用ポート設定を解除してから、もう一度設定し直してください。
0928E	Can not delete the management IP address from the VLAN to which the secure management port(port<num>) belongs. 装置 IP アドレスの削除に失敗しました。 管理専用ポートが所属する VLAN には、必ず装置 IP アドレスが設定されている必要があります。 この VLAN の装置 IP アドレスを削除する場合、該当ポートの管理専用ポート設定を解除してから、もう一度設定し直してください。
0929E	port<num> is secure management port. Other ports can not belong to the VLAN to which the secure management port belongs. 割り当て VLAN の変更に失敗しました。 指定された複数ポートの中に、管理専用ポートが含まれています。 管理専用ポートが所属する VLAN は、管理専用ポート以外が所属することはできません。 個別にポート番号を指定したうえで、VLAN の変更を実施してください。

0930E	Cannot set 'tagged' on secure management port.
	タグ VLAN の設定に失敗しました。 管理専用ポートをトランクポートにすることはできません。 該当ポートの管理専用ポート設定を解除してから、もう一度設定し直してください。
0932E	Cannot assign another port to the VLAN(vlan<num>) to which the secure management port belongs.
	割り当て VLAN の変更に失敗しました。 割当先の VLAN には、管理専用ポートが所属しています。 この VLAN に変更したい場合は、管理専用ポートの所属する VLAN を変更してから、もう一度設定し直してください。
0933E	A secure management port(port<num>) can not belong to a VLAN to which another port belongs.
	割り当て VLAN の変更に失敗しました。 指定された VLAN には既に別のポートが所属しています。 管理専用ポートが所属する VLAN は、管理専用ポート以外が所属することはできません。 該当のポートの所属 VLAN を変更した上で、もう一度設定し直してください。
0934E	A secure management port can not belong to a VLAN for which a management IP address is not set.
	割り当て VLAN の変更に失敗しました。 割当先の VLAN には、装置 IP アドレスが設定されていません。 管理専用ポートが所属するVLANには、装置IPが必ず設定されている必要があります。 該当 VLAN の IP アドレスを設定してから、もう一度設定し直してください。
0935E	A secure management port can not belong to a VLAN in which a virtual server IP address is set.
	割り当て VLAN の変更に失敗しました。 割当先の VLAN には、仮想サーバーIP アドレスが設定されています。 管理専用ポートが所属する VLAN には、仮想サーバーIP アドレスが設定されていない必要があります。 該当 VLAN の仮想サーバーIP アドレス設定を削除してから、もう一度設定し直してください。

0936E	Cannot set 'channel' on secure management port.
	チャネル設定に失敗しました。 管理専用ポートが、論理チャネルに所属することはできません。 管理専用ポート設定を解除してから、もう一度設定し直してください。
0937E	Cannot set the spanning tree port to the secure management port.
	管理専用ポート設定に失敗しました。 スパニングツリーが設定されているポートを管理専用ポートに設定することはできません。 スパニングツリー設定を解除してから、もう一度設定し直してください。
0940E	Operation not supported on software load balancer.
	仮想アプライアンス版 LB では、当該操作をサポートしていません。
0941E	failed to mode change.
	特権モードへの遷移に失敗しました。 メイン画面からもう一度やり直してください。
0942E	internal error.
	内部エラーが発生しました。 メイン画面からもう一度やり直してください。
0943E	internal error.
	内部エラーが発生しました。 メイン画面からもう一度やり直してください。
0944E	The 10Gb Ethernet interface does not support forcing a speed and duplex option.
	リンク速度の設定変更に失敗しました。 指定されたポートに 10G I/F が含まれています。 設定内容や入力値をもう一度確認してください。
0945E	out of range. (1s-1m)
	msl タイマー設定の変更に失敗しました。 msl タイマーは 1s-1m の範囲で設定してください。
0946E	The 10Gb Ethernet interface does not support link aggregation settings.
	リンク集約設定の変更に失敗しました。 指定されたポートに 10G I/F が含まれています。 設定内容や入力値をもう一度確認してください。

0947E	out of range. (1-12)
	リンク状態監視設定の変更に失敗しました。 監視ポート番号に、規定外の値が入力されました。 設定内容や入力値をもう一度確認してください。
0948E	Operation not supported on ftp or udp server.
	XFF スイッチング（XFF ヘッダ情報の参照）設定の変更に失敗しました。 XFF スイッチング（XFF ヘッダ情報の参照）設定は tcp 仮想サーバのみ設定可能です。 設定内容や入力値をもう一度確認してください。
0949E	Operation not supported on ftp or udp server.
	XFF セッション維持設定の変更に失敗しました。 XFF セッション維持設定は tcp 仮想サーバのみ設定可能です。 設定内容や入力値をもう一度確認してください。
0960E	out of range. (0-90)
	証明書更新のタイミング変更に失敗しました。 タイミングは 0-90 の範囲で設定してください。
0961E	country is 2 characters.
	国コードの変更に失敗しました。 国コードは 2 文字で設定してください。
0962E	Models that do not support ECC cannot select 256 or 384.
	鍵長の変更に失敗しました。 ECC 非対応機種は 256、384 を選択できません。
0963E	out of range. (0-2)
	中間証明書の数の変更に失敗しました。 中間証明書の数は 0-2 の範囲で設定してください。
0964E	config file open error.
	設定ファイルの読み込みに失敗しました。
0965E	config file close error.
	設定ファイルのクローズ処理に失敗しました。
0966E	‘ssl: *XXXX*_<num>' is reserved for 'cert-update: *プレフィックス*'.
	SSL ポリシーの削除に失敗しました。 指定された名前の SSL ポリシーは、SSL 証明書自動更新の既存のポリシーによって使用されているため削除することはできません。
0967E	'ssl: *XXXX*_<num>' is reserved for 'cert-update: *プレフィックス*'
	SSL ポリシーの作成に失敗しました。

	指定された名前の SSL ポリシーは、SSL 証明書自動更新の既存のポリシーによって予約されているため作成することはできません。
0968E	cert-update *プレフィックス*': No such settings.
	cert-update の初期化に失敗しました。 指定された cert-update は存在しません。 設定内容や入力値を確認し、もう一度設定し直してください。
0969E	*SSL 証明書自動更新モジュールのエラーメッセージ*.
	cert-update [*プレフィックス*] not found.
	指定された cert-update は存在しません。
	cert-update [*プレフィックス*] ssl not found.
	指定された cert-update に関連する SSL ポリシーが存在しません。
	cert-update [*プレフィックス*] update was completed.
	証明書の更新が、証明書のダウンロードまで完了しているため初期化できません。
	cert-update [*プレフィックス*] ssl [*SSL ポリシー*] in use.
	SSL ポリシーが仮想サーバーに割り当てられているため初期化できません。
0970E	'ssl: *SSL ポリシー*' Already exists.
	SSL 証明書自動更新ポリシーの作成に失敗しました。 指定された名前の SSL 証明書自動更新ポリシーは、使用する SSL ポリシーがすでに存在するため作成することはできません。
0971E	failed to moving cert-update mode.
	cert-update 設定モードへ遷移できませんでした。 内部エラーが発生しました。 恐れ入りますが、設定モードから一旦抜けて、特権モードに入り直してからもう一度コマンドを実行してください。
0972E	*プレフィックス*': No such settings.
	cert-update の削除に失敗しました。 入力された cert-update は存在しません。 設定内容や入力値をもう一度確認してください。

5.6 syslog メッセージ

5.6.1 イーサネット - port

5.6.1.1 notice

link state changed to UP <speed> Mbps <duplex>

イーサネットポートがリンクアップした

link state changed to DOWN

イーサネットポートがリンクダウンした

dropped 802.1q packet from <macaddr>

<macaddr>からタグ付きパケットを受信し破棄した

5.6.1.2 info

denied <src> -> <dst> type <ethertype> count <n>

MAC アクセスリストにより該当パケットが破棄された

5.6.2 リンク集約 - chan

5.6.2.1 notice

active aggregator found

論理チャネル内に有効な集約グループが形成された

Link state changed to UP

論理チャネルがリンクアップに変化した

Link state changed to DOWN

論理チャネルの状態がダウンに変化した

5.6.3 VLAN - vlan

5.6.3.1 crit

cannot create vlan id = 0.

内部エラーが発生した

port1 does not exist on system.
内部エラーが発生した

packet dropped. <port> is not a VLAN interface
内部エラーが発生した

receive interface not found on <vlan>
内部エラーが発生した

invalid receive interface(<port>).
内部エラーが発生した

invalid ipv<n> interface type(<m>)
内部エラーが発生した

5.6.3.2 notice

mac address table became full(<n>)
MAC アドレステーブルのエントリー数が最大に達した

stp: state changed to <state> on <port>
<port>の STP 状態が<state>に変化した

5.6.4 lbcommon 負荷分散共通 - lb

5.6.4.1 alert

system reached sticky session limit <n>
IP セッション維持で使用するテーブルのエントリー数が上限に達した

system reached L4 connection limit <n>
L4 負荷分散で使用するテーブルのエントリー数が上限に達した

5.6.4.2 crit

negative proxy connection count
内部状態の異常を検出した

negative server connection count

内部状態の異常を検出した

bitmap is corrupt <n> <m>
内部状態の異常を検出した

nat addr <ipaddr> proto <n> not found
内部状態の異常を検出した

port already freed
内部状態の異常を検出した

negative sticky ref count
内部状態の異常を検出した

natpool not found
内部状態の異常を検出した

negative natpool ref count
内部状態の異常を検出した

nat rule not found
内部状態の異常を検出した

negative curcons counter <string>
内部状態の異常を検出した

5.6.4.3 error

socreate error <reason> <string>
通信ソケット生成処理が異常終了した

soconnect error <reason> <string>
実サーバーとのコネクション確立処理が異常終了した

sosend error <reason> <string>
データ送信処理が異常終了した

5.6.4.4 warn

server <ipaddr> port <port> reached its connection limit <n>

実サーバーのコネクション数が上限に達した

server <ipaddr> port <port> is up

実サーバーが通信を開始した

server <ipaddr> port <port> is down

実サーバーが通信を停止した

5.6.5 IPv4 L4 負荷分散 - lb

5.6.5.1 crit

vlan not found <n> <mem> <mem>

内部状態の異常を検出した

no leading space for ethernet header

内部データの異常を検出した

5.6.5.2 warn

upper-layer protocol header not found

L4 ヘッダーのない不正なパケットを受信した

5.6.5.3 notice

FTP 227 reply with different address <ipaddr>(<ipaddr>)

受信した FTP 227 レスポンスに含まれる IP アドレスが FTP 実サーバーのアドレスと異なっている

FTP PORT command with different address <ipaddr>(<ipaddr>)

受信した FTP PORT コマンドに含まれる IP アドレスが FTP クライアントのアドレスと異なっている

5.6.6 IPv6 L4 負荷分散 - lb6

5.6.6.1 crit

vlan not found <n> <mem> <mem>

内部状態の異常を検出した

packet is not contiguous

内部データの異常を検出した

icmp packet is not contiguous

内部データの異常を検出した

5.6.6.2 warn

upper-layer protocol header not found

L4 ヘッダーのない不正なパケットを受信した

5.6.6.3 notice

FTP EPRT command with different address <ipaddr>(<ipaddr>)

受信した FTP EPRT コマンドに含まれる IP アドレスが FTP クライアントのアドレスと異なっている

5.6.7 L7 負荷分散 - lb

5.6.7.1 alert

system reached L7 connection limit <n>

L7 負荷分散で使用するテーブルのエントリー数が上限に達した

cookie table became full

cookie セッション維持で使用するテーブルのエントリー数またはテーブルのサイズが上限に達した

5.6.7.2 crit

invalid socket state <n>

内部状態の異常を検出した

5.6.7.3 error

socreate error <reason> <string>

通信ソケット生成処理が異常終了した

sobind error <reason> <string>

通信ソケットへのアドレスバインド処理が異常終了した

solisten error <reason> <string>

コネクション要求の受信開始処理が異常終了した

could not bind local address. check configuration.

ソース NAT 設定がないため通信ソケットへローカルアドレスをバインドできなかった

soconnect error <reason> <string>

実サーバーとのコネクション確立処理が異常終了した

soreceive error <reason> <string>

データの受信処理が異常終了した

sosend error <reason> <string>

データ送信処理が異常終了した

invalid tcp client state <n>

内部状態の異常を検出した

invalid tcp server state <n>

内部状態の異常を検出した

could not connect to <ipaddr>:<port>

実サーバーとのコネクション確立が失敗した

timeout in invalid tcp state <n> <m>

内部状態の異常を検出した

invalid udp server state <n>

内部状態の異常を検出した

so_setsockopt(level=<n>,optname=<m>) error <reason> <string>
ソケットオプションのセットが異常終了した

5.6.7.4 notice

ssl client hello timed out
一定時間内に Client Hello メッセージを受信しなかった

5.6.8 HTTP 負荷分散 - http

5.6.8.1 crit

scb <n> has unexpected null proxy config
仮想サーバー情報の異常を検出した

scb <n> has unexpected null server config
実サーバー情報の異常を検出した

scb <n>, invalid state[<state>:CLOSED]
FIN 送信に失敗した

5.6.8.2 error

check configuration
HTTP アクセスログ指定の異常を検出した

access log socreate error (<n>)
ログサーバー用ソケット作成に失敗した

access log soconnect error (<n>)
ログサーバーへの接続に失敗した

hostname parameter too long(<n>)
アクセスログ用ホスト名の異常を検出した

status code is not included in a first mbuf
Status-Line の異常を検出した

location header too big!(<n>)

Location ヘッダーの異常を検出した

Cannot send access log message [<n>:<m>]

アクセスログの送信に失敗した

scb unexpectedly NULL!

内部状態のエラーを検出した

unknown direction (<n>)

内部状態のエラーを検出した

5.6.8.3 notice

Invalid timed out in state[<state>:<state>]

内部状態[<state>:<state>]でタイマー満了の異常を検出した

response header too big. size = <size1> should be < <size2>

HTTP のレスポンスヘッダーのサイズが大きすぎる

5.6.8.4 info

FIN timed out, scb <n>

FIN タイマーの満了を検出した

HTTP request <ipaddress>.<port> -> <ipaddress>.<port> timed out

HTTP リクエストのタイムアウトを検出した

found <CR><LF> before HTTP request

HTTP リクエストヘッダーの前に空白行を検出した

rejected HTTP request from <ipaddress> because its size (<n>)
exceeds the maximum (16384)

16k バイトより大きい HTTP リクエストヘッダーを受信した

parse http scheme error for location header(response)

サポートされていないスキームが指定された Location ヘッダーを受信し

た

parse host error for response location header
Location ヘッダーの異常を検出した

URL is too long for response location header
Location ヘッダーの異常を検出した

lost an access log message
アクセスログの異常を検出した

switching protocols
HTTP から WebSocket にスイッチした

5.6.9 SSL アクセラレーション - ssl

5.6.9.1 error

sosend error <reason> <string>
データ送信処理が異常終了した

cannot create session while stickiness is enabled
SSL セッション ID によるセッション維持設定が有効の時に SSL セッションが生成できなかった

certificate not found
サーバー証明書が見つからなかった

tmp key not found
exportable な暗号スイートで使用する一時的 RSA 鍵が見つからなかった

Input/output error <reason>
暗号処理ハードウェアで異常が発生した

No space left on device
暗号処理ハードウェアでメモリー確保異常が発生した

5.6.9.2 notice

too big for cert header <n>

クライアント証明書のサイズが大きすぎて HTTP ヘッダーに挿入できない

bad record length <n> <string>

SSL レコード長の値が異常なパケットを受信した

record too long <n>

SSL レコード長の値が異常なパケットを受信した

bad ccs length <n>

SSL レコード長の値が異常なパケットを受信した

bad alert length <n>

SSL レコード長の値が異常なパケットを受信した

state <n> unexpected message <m>

予期しない SSL ハンドシェークを受信した

bad version <n>

SSL バージョンの値が異常な Client Hello を受信した

bad cipher spec length <n>

cipher spec 長の値が異常な Client Hello を受信した

bad message length <n> <string>

パケット長が短すぎる、または SSL レコード長の値と一致しない

bad session-id length <n> <m>

session-id 長の値が異常な Client Hello を受信した

bad cipher suites length <n> <m>

cipher suites 長の値が異常な Client Hello を受信した

bad compression methods length <n> <m>

compression methods 長の値が異常な Client Hello を受信した

null method not found
compression methods リストに必須メソッドの null が含まれていない

bad extension length <n> <m>
extension 長の値が異常な Client Hello を受信した

bad renegotiation info <n> <m>
renegotiation info 拡張の値が異常な Client Hello を受信した

bad server name list length <n> <m>
SNI 拡張の値が異常な Client Hello を受信した

bad server name length <n> <m>
SNI 拡張の値が異常な Client Hello を受信した

required cipher missing
異なる暗号スイートでセッション再利用を要求する異常な Client Hello を受信した

certificate for <string> not found
SNI 拡張のサーバー名と CN が一致するサーバー証明書が見つからなかった

no ciphers passed
cipher_suites リストに対応可能な暗号スイートが含まれていない

bad certificate list length <n> <m>
certificate list 長の値が異常な Certificate を受信した

bad certificate length <n> <m>
certificate 長の値が異常な Certificate を受信した

bad client key length <n> <m>
client key 長の値が異常な Client Key Exchange を受信した

bad signature length <n> <m>

signature 長の値が異常な Certificate Verify を受信した

incorrect version <n> <m>

プレマスターシークレットの先頭 2 バイトが Client Hello のバージョンと一致しない

5.6.10 セッション情報同期 - ha

5.6.10.1 alert

LBHA command queue full. [<function_name>]

内部状態の異常を検出した。

5.6.10.2 crit

Cannot bind local addr with a socket [<n>]. [<function_name>]

HA 用通信ソケットがローカルアドレスに bind できなかった。<n>は理由コード。

Failed to close a socket [<n>].

HA 用通信ソケットの閉塞に失敗した。<n>は理由コード。

Failed to close a listen socket [<n>].

HA 用通信ソケットの閉塞に失敗した。<n>は理由コード。

Cannot set REUSEPORT socket option [<n>].

HA 用通信ソケットのオプション設定に失敗した。<n>は理由コード。

Cannot set ACCEPTFILTER socket option [<n>].

HA 用通信ソケットのオプション設定に失敗した。<n>は理由コード。

Cannot listen on a socket [<n>].

HA 通信用ソケット上で接続待受けに失敗した。<n>は理由コード。

tsleep() failed.

内部状態の異常を検出した。

Failed to close a socket [<n>].
旧通信ソケットを閉塞しようとしたが失敗した。<n>は理由コード。

5.6.10.3 error

Invalid data structure for new sync_interval is specified.
内部状態の異常を検出した。

Invalid data structure for new state is specified.
内部状態の異常を検出した。

Invalid data structure for new localaddr is specified.
内部状態の異常を検出した。

Invalid data structure for new peeraddr is specified.
内部状態の異常を検出した。

Invalid data structure for new stat is specified.
内部状態の異常を検出した。

Invalid data structure for new sync_request is specified.
内部状態の異常を検出した。

Unexpected ID(<n>) for HA instances. [<function_name>]
内部状態の異常を検出した。

Invalid data structure for old sync_interval is specified.
内部状態の異常を検出した。

Invalid data structure for old state is specified.
内部状態の異常を検出した。

Invalid data structure for old localaddr is specified.
内部状態の異常を検出した。

Invalid data structure for old peeraddr is specified.

内部状態の異常を検出した。

Invalid data structure for old stat is specified.

内部状態の異常を検出した。

Invalid data structure for old sync_request is specified.

内部状態の異常を検出した。

Invalid VRRP state.

異常な（MASTER、BACKUP、無効以外）の VRRP ステート変更が行われた。あるいは現在のステートが異常。

Unexpected type[<n>] for socket creation.

内部状態の異常を検出した。

Failed to receive data [<n>].

データの受信処理に失敗した。<n>は理由コード。

Failed to send data [<n>]. [<function_name>]

データの送信処理に失敗した。<n>は理由コード。

Failed to send sync command [<n>].

セッション一括同期命令の送信処理に失敗した。<n>は理由コード。

Unexpected LBHA PCB add/update/del command.

内部状態の異常を検出した。

Unexpected LBHA sticky add/del command.

内部状態の異常を検出した。

Unexpected LBHA cookie add/del command.

内部状態の異常を検出した。

Unexpected HA message type.

内部状態の異常を検出した。

Session receive buffer over flow.

セッション情報受信用バッファが溢れてしまった。

Unexpected MSG type(<n>) was received.

想定外のセッション情報を受信した。あるいは受信データが壊れている。
<n>は受信データのタイプコード。

Cannot start Backup. Not set local address.

ローカル IP アドレスが未設定のため、BACKUP 処理を開始できない。

Cannot start Master. Not set local address.

ローカル IP アドレスが未設定のため、MASTER 処理を開始できない。

Unexpected LBHA command.

内部状態の異常を検出した。

Invalid type "NONE" has received.

内部状態の異常を検出した。

Unexpected type(<n>) for LBHA_CMD_MODVAR command.

内部状態の異常を検出した。

5.6.10.4 warn

VRRP state unchanged.

現在と同じ VRRP ステートへの変更が行われた。

Unexpected VRRP state transition.

VRRP 無効からいきなり MASTER へと遷移した。

No such virtual/real server for L4 PCB.

受信した L4 セッション情報の仮想／実サーバー情報は本製品には未登録だった。

No such virtual/real server for IP sticky.

受信した IP セッション維持情報の仮想／実サーバー情報は本製品には

未登録だった。

No such virtual/real server for cookie sticky.

受信した Cookie セッション維持情報の仮想／実サーバー情報は本製品には未登録だった。

HA resources are still not retrieved. [<function_name>]

MASTER/BACKUP の開始に必要な資源がまだ準備できていなかった。

5.6.10.5 notice

Failed to send all sessions. Reset Master

一括同期のためのセッション情報の送信に失敗したので、MASTER 処理を再起動する。

Cannot connect the peer [<n>].

HA 用通信ソケットで冗長相手に接続できなかった。<n>は理由コード。

Unexpected VRRP state (not Backup). [<function_name>]

データ受信時に VRRP ステートが BACKUP ではなかった。

Failed to connect to Master [<n>].

MASTER 機との接続が切断された。<n>は理由コード。

Unexpected VRRP state (not Master). [<function_name>]

データ送信時に VRRP ステートが MASTER ではなかった。

Failed to accept connection [<n>].

接続受入れに失敗した。<n>は理由コード。

The socket is no longer available. [<function_name>]

データを送受信あるいは MASTER 機に再接続しようとしたが、当該 HA 用通信ソケットはすでに無効だった。

The connection is already closed [<n>].

データを受信しようとしたが、当該 TCP コネクションはすでに閉塞していた。<n>は理由コード。

Not ready to send data [<n>].

データを送信するための準備が整っていなかった。<n>は理由コード。

Failed to receive/send packets. Reset Backup

セッション情報の送受信に失敗したので、BACKUP 処理を再起動する。

Failed to send packets. Reset Master

セッション情報の送信に失敗したので、MASTER 処理を再起動する。

Failed to receive/send packets. Reset Master

パケット情報の送受信に失敗したので、MASTER 処理を再起動する。

Failed to send a sync request. Reset Backup

セッション一括同期命令の送信に失敗したので、BACKUP 処理を再起動する。

5.6.10.6 info

Starting Backup process.

BACKUP 処理を開始する。

Starting Master process.

MASTER 処理を開始する

Peer address unchanged.

現在と同じ冗長相手機器 IP アドレスへの変更しようとした。

The socket is already closed [<n>].

閉塞しようとした HA 用通信ソケットはすでに閉塞済みだった。<n>は閉塞理由コード。

L4 PCB update or delete message was discarded in other than Backup state.

L4 セッション情報を受信したが、VRRP 状態がすでに BACKUP ではないため受信メッセージを破棄した。

IP sticky update or delete message was discarded in other than Backup state.

IP セッション維持情報を受信したが、VRRP 状態がすでに BACKUP ではないため受信メッセージを破棄した。

Already changed to other than Backup state. [<function_name>]

VRRP ステートがすでに BACKUP ではないため、処理を停止した。

Already changed to other than Master state. [<function_name>]

VRRP ステートがすでに MASTER ではないため、処理を停止した。

VRRP state transition and a TCP event occur simultaneously at resetting Backup.

VRRP ステート遷移と BACKUP 処理の再起動が同時に発生した。再起動処理は行わない。

VRRP state transition and a TCP event occur simultaneously at resetting Master.

VRRP ステート遷移と MASTER 処理の再起動が同時に発生した。再起動処理は行わない。

VRRP state transition and a TCP event occur simultaneously at receiving/sending packets in Backup.

VRRP ステート遷移と BACKUP 用パケット送受信が同時に発生した。送受信処理は行わない。

VRRP state transition and a TCP event occur simultaneously at receiving/sending packets in Master.

VRRP ステート遷移と MASTER 用パケット送受信が同時に発生した。送受信処理は行わない。

VRRP state transition and a TCP event occur simultaneously at sending packets in Master.

VRRP ステート遷移と MASTER 用パケット送信が同時に発生した。送信処理は行わない。

Retrying Backup process after <n> msec.

BACKUP 開始処理を<n>ミリ秒後に再度行う。

Retrying Master process after <n> msec.

MASTER 開始処理を<n>ミリ秒後に再度行う。

Session sync interval is zero. Never send sessions.

セッション情報を送信しようとしたが、送信間隔が 0 に設定されたので送信しない。

Obsoleted session all sync request. No connection to peer.

冗長相手に未接続だったため、セッション一括同期命令を送信せずに破棄した。

The old socket is already closed. (reset by peer)

旧通信ソケットを閉塞しようとしたが、すでに閉塞済みであった。

5.6.11 内部トレース - trace

5.6.11.1 crit

Trace snapshot <snap-no> : <function> <line>

カーネルによるスナップショット・イベントが発生した

5.6.11.2 error

trace no get request <n> - <m>

スナップショット番号、n から m 間のトレースデータが取得されないまま破棄した

5.6.12 プロセス共通

5.6.12.1 error

cannot call lstat (<filename>): <reason> [<func>]

<filename>に対する lstat 関数が失敗した

<filename> is not a regular file [<func>]

<filename>のファイル形式が正常でない

<mac-addr>: Invalid mac address

不正な MAC アドレスを検出

<filename> open error: <reason> [<func>(<line>)]

<filename>のファイルオープンに失敗した

x509 file decode error.[<func>(<line>)]

SSL 証明書のデコードに失敗した

<filename> close error: <reason> [<func>(<line>)]

<string>のファイルクローズに失敗した

5.6.13 CLI/WebUI - lbconfigd

5.6.13.1 crit

failed to unbind channel(port<n>, chan<m>)

論理チャネル<m>に対するポート<n>の割り当てに失敗した

failed to unbind channel(port<n>, vlan<m>)

VLAN<m>に対するポート<n>の割り当てに失敗した

no existence nat-pool.

NAT プールが存在しない

not found current channel number

現在遷移している channel モードの設定情報が取得できない

redirect rule exists. but rule policy not found.

リダイレクトルールが存在しますが、ルールポリシーが見つからない。

sourcenat address list empty.

ソース NAT アドレスリストが空

5.6.13.2 error

<filename> open error: <reason> [<func>(<line>)]

<filename>オープンエラー

<real-id>: no data at the same real server address. [<func>(line)]
指定された実サーバーID 情報がカーネル情報に存在しない

<reason> [<func>(<line>)]
netstat コマンド実行に失敗した

<string> error [<func>(<line>)]
<string>が失敗した

<string>: <reason> [<func>(<line>)]
ネットマスク長またはプレフィックス長が不正

<string>: lbu_lookup_npool error [<func>(<line>)]
nat-pool(<string>)が存在しない

<string>: lbu_lookup_real error [<func>(<line>)]
<string>の実サーバー設定が存在しない

<string>: lbu_lookup_virtual error [<func>(<line>)]
<string>の仮想サーバー設定が存在しない

<string>: parameter error [<func>(<line>)]
未定義のコマンド

add mac-table entry failed.
静的 mac エントリーの追加に失敗した

bad SEQUECE id[0x<n>]
シーケンス番号不正

config sync connection has not been established: <reason>
コマンド同期用コネクションが確立できない状態である

exist ipsw balancing settings. but not found ipsw rule.

IPSW 分散設定が存在しますが、IPSW ルールが見つからない。

failed bind the sorry contents. contents not found.
コンテンツがみつからず、sorry コンテンツのバインドに失敗した。

failed receive polling event: <reason>
ポーリング処理が異常終了した

failed ssl bind settings for initializing.
初期化するための SSL バインドの設定に失敗した

failed to get statistical data for ssl.
SSL 統計情報データの取得に失敗した

failed to get the environment value for the config-file update.
カーネル環境変数に対する変更が失敗した

failed to get the virtual server option data.
仮想サーバーオプションデータの取得に失敗した

failed to get the virtual server statistical data.
仮想サーバー統計データの取得に失敗した

failed to get your account-name. (priv_id=<n>)
アカウント名の取得に失敗しパスワードの変更ができなかった

failed to laggport settings.("chan<n>") [(<line>)]
論理チャネル<n>の設定に失敗した

file(csr.pem)=<string>
<string>に csr.pem ファイル作成に失敗した

get lbstat error
lbu_get_stat_lbstat が失敗した

hosts file read open error.

"hosts"の書き込みオープンエラー

httpd.conf file read open error.
"httpd.conf"の読み込みオープンエラー

httpd.conf file write open error.
"httpd-tmp.conf"の書き込みオープンエラー

Invalid ssl directory structure.(err=<n>)
無効な ssl ディレクトリ構造のため、異常終了した

Invalid ssl directory structure: <reason>
SSL に関するディレクトリ構造が不正

ioctl error on cli: <reason> [<func>(<line>)]
cli 処理でデバイス制御に失敗した

ioctl error on cli: <reason> [<func>(<line>)]
cli 処理でデバイス制御に失敗した

key length write error. (<string>)
キー長の書き込みに失敗した

lbu_lookup_channel error [<func>(<line>)]
lbu_lookup_channel が失敗した

lbu_set_sockstorage error [<func>(<line>)]
lbu_set_sockstorage が失敗した

lbu_set_sockstorage error [<func>(<line>)]
lbu_set_sockstorage が失敗した

lbu_set_strings_addr error [<func>(<line>)]
lbu_set_strings_addr が失敗した

not found current mac acl entry.

現在の MAC アクセスリストエントリーが見つからない

not found current nat-pool entry.(<string>)
現在の NAT プールエントリーが見つからない

not found current reverse-nat entry.
現在のリバース NAT エントリーが見つからない

ready_load_config_ip error [<func>(<line>)]
ready_load_config_ip が失敗した

rtadv conf file write open error.
"rtadvd.conf"の読み込みオープンエラー

sclips.conf file read open error.
"sclips.conf"の読み込みオープンエラー

socket error on cli: <reason> [<func>(<line>)]
socket の作成に失敗した

statd is not started
lbstatd が起動していない

statistics clear waiting time over [<func>(<line>)]
統計情報クリア処理がタイムアウトした

syncd is not started
lbsyncd が起動していない

sysctlbyname error on cli: <reason> [<func>(<line>)]
cli 処理でシステム情報の取得に失敗した

your account data not found. [myname:<user-name1>,
uname:<user-name2>, priv_id:<id>, tty:<n>]
自ユーザーアカウント情報が取得できない

5.6.13.3 info

cannot delete the own account. [myname:<user-name1>, uname:<user-name2>, priv_id:<id>, tty:<n>]

自ユーザーアカウントを削除しようとした

certificate file <string> is not include common-name data.

証明書ファイル<string>は common-name データを含んでいない。

key file <string> is not include common-name data.

鍵ファイル<string>は common-name データを含んでいない。

5.6.14 設定ファイル検査 - lbconfchk

設定ファイル検査 - lbconfchk

5.6.14.1 error

<filename> open error: <reason> [<func>(<line>)]

<filename>オープンエラー

<filename> open error: <reason> [<func>(<line>)]

<filename>クローズエラー

detected command error in checking '<reason>'.[line <n>]

<reason>の検査によりエラーが検知された （設定ファイルの行番号<n>によってエラーが発生）

command write error, probably sysadm has gone, reason=<reason>[<func>(<line>)]

設定行の検査時に内部エラーが発生した

select error, ret=<n>, reason=<reason> [<func>(<line>)]

<reason>によりイベント待機処理が異常終了した

failed to read internal cli response.

設定行の検査時に内部エラーが発生した

5.6.14.2 debug

select error, reason=<reason>[<func>(<line>)]

不正な設定行により検査処理がタイムアウトした

process of config-check is succeed, read=<command>.

設定行"<command>"は検査にパスした

process of config-check is failed, read=<command>.

設定行"<command>"はエラーと判断された

5.6.15 設定情報同期 - lbsyncd

5.6.15.1 crit

unknown ha state(<n>) returned

セッション同期機能が不正な状態を返却した

command write error, probably sysadm has gone, reason=<reason>

受信側: コマンド実行プロセスへのコマンド送信が失敗した

5.6.15.2 error

pidfile <filename> open error: <reason>

PID ファイルの生成に失敗した

received unknown signal(<n>)

不正なシグナルを受信した

<state> socket select error: <reason>

<state>状態でのイベント待機処理が異常終了した

<type> socket create error: <reason>

通信ソケット<type>の生成処理が異常終了した

master socket set option error: <reason>

master 状態でのソケットオプションのセットが異常終了した

<type> socket listen error: <reason>

ソケット<type>の LISTEN が異常終了した

socket fcntl <type> error: <reason>
ソケットに対する fcntl 処理が異常終了した

<type> socket accept error: <reason>
コネクション<type>の受け入れ処理が異常終了した

recv unknown message type(<n>) on <type> socket
ソケット<type>で未知のメッセージを受信した

popen(<string>) error: <reason>
受信側: コマンド実行プロセスの起動に失敗した

output buffer size is not enough
受信側: コマンド実行処理用のバッファサイズが不十分だった

synced file(<filename>) create error, reason=<reason>
受信側: ファイルの同期処理が失敗した

synced file(<filename>) write error, reason=<reason>
受信側: ファイルの同期処理が失敗した

import file(<filename>) get size error: <reason>
送信側: ファイルの同期処理が失敗した

unexpected send file header size(<n>): <reason>
送信側: ファイルの同期処理が失敗した

open <filename> error: <reason>
送信側: ファイルの同期処理が失敗した

unexpected <type> file size(<n>): <reason>
送信側: ファイルの同期処理が失敗した

unexpected <type> send error. command=<string>, header size=<n>,

reason=<reason>
送信側: コマンドの同期処理が失敗した

unexpected respond error. command=<string>, respond size=<n>, reason=<reason>
送信側: コマンド同期の応答確認が失敗した

5.6.15.3 warn

<type> socket bind error: <reason>
ソケット<type>のバインド処理が異常終了した

import file(<filename>) open error: <reason>
送信側: ファイルの同期処理が失敗した

5.6.15.4 notice

debugging mode changed to <n> -> <m>
デバッグモードが<n>から<m>に変化した

backup socket connect error: <reason>
peer への接続処理が失敗した

old accepted connection closed
master 側に接続要求が複数来たため、古い方の接続を破棄した

command '<string>' failed to sync
送信側: コマンド<string>の同期に失敗した

command request '<string>' discarded
送信側: コマンド<string>の送信要求が失敗し、コマンドが破棄された

5.6.15.5 info

state changed to <state>
<state>状態に移行した

command sync connection established(<n>)
peer への接続が成功した

command sync connection accepted
コネクションの受け入れが正常に完了した

command '<string>' successfully done
受信側: コマンド<string>が正常に実行された

command '<string>' failed
受信側: コマンド<string>が失敗した

5.6.16 冗長構成 - lbvrrpd

5.6.16.1 error

cannot allocate memory [<string>]: <reason>
メモリー確保に失敗した

cannot open socket for setting vrid(mac address) of interface <device>: <reason>
vrid 設定用のソケットのオープンに失敗した

cannot set vrid(mac address) for interface <device>, vrid=<n> (ioctl SIOCSDRVSPEC): <reason>
vrid の設定に失敗した

cannot open socket for setting reply ip address of interface <device>: <reason>
応答 IP アドレス設定用のソケットのオープンに失敗した

cannot set reply ip address for interface <device>, addr=<ipaddr> (ioctl SIOCSDRVSPEC(<n>)): <reason>
応答 IP アドレスの設定に失敗した

cannot open socket for setting L2forward of interface <device>: <reason>
L2forward 設定用のソケットのオープンに失敗した

cannot set L2forward for interface <device>, l2forward=<n> (ioctl SIOCSDRVSPEC): <reason>

L2forward の設定に失敗した

cannot set sysctl net.lb.ha.state=<n>: <reason>

LB_HA の状態設定に失敗した

cannot open socket for getting portlink status: <reason>

ポートのリンク状態取得用のソケットのオープンに失敗した

your NIC doesn't support SIOCGIFMEDIA ioctl: <reason>

NIC が未サポート

<device>: cannot do ioctl, intertface is faulty: <reason>

NIC が故障している

getifaddrs error: <reason> [<string>]

getifaddrs に失敗した

cannot open vrrpd pid file: <reason>

VRRPD の PID ファイルのオープンに失敗した

cannot transition to daemon mode: <reason>

デーモン化に失敗した

vrid [<n>] cannot open socket, disabled

VRRP の通信ソケットのオープンに失敗した

cannot open mib info socket : <reason>

MIB 情報の通信ソケットのオープンに失敗した

cannot bind for mib info socket : <reason>

MIB 情報の通信ソケットのバインドに失敗した

cannot listen for mib info socket: <reason>

MIB 情報の通信ソケットのリッスンに失敗した

failed to select of mib info: <reason>
MIB 情報のイベント待機に失敗した

failed to accept of mib info: <reason>
MIB 情報のイベント受付に失敗した

send error of mib info(SIGPIPE)
MIB 情報の送信に失敗した（SIGPIPE）

send error of mib info: <reason>
MIB 情報の送信に失敗した（その他）

cannot get the time with gettimeofday: <reason>
時刻の取得に失敗した

failed to open syncd.pid
syncd の PID ファイルのオープンに失敗した

failed to create a socket for devd: <reason>
devd 向けのソケットの生成に失敗した

failed to connect a socket for devd: <reason>
devd 向けのソケットの接続に失敗した

vrrpd[<n>]: IPv4 mcast setsockopt(<m>) error: <reason>
IPv4 マルチキャスト関係のソケットオプションの設定に失敗した

vrrpd[<n>]: IPv6 mcast setsockopt(<m>) error: <reason>
IPv6 マルチキャスト関係のソケットオプションの設定に失敗した

cannot open raw socket for VRRP protocol [AF_INET/AF_INET6, SOCK_RAW, IPPROTO_VRRP]: <reason>
VRRP パケット向けのソケットのオープンに失敗した

cannot set SO_RCVTIMEO option on the IPPROTO_VRRP raw socket:

<reason>
VRRP パケット向けのソケットオプションの設定に失敗した
（SO_RCVTIMEO）

cannot set IPV6_RECVPKTINFO option on the IPPROTO_VRRP raw socket: <reason>
VRRP パケット向けのソケットオプションの設定に失敗した
（IPV6_RECVPKTINFO）

vrrpd[<n>]: sendmsg error (<reason>)
パケットの送信に失敗した

vrrpd[<n>]: recvmsg error (<reason>)
パケットの受信に失敗した

vrid [<n>] cannot send advertisement packet
VRRP 広告が送信できない

vrid [<n>] cannot send sub advertisement packet
サブの VRRP 広告が送信できない

ip ttl of vrrp packet isn't set to 255. Packet is discarded
受信した VRRP 広告を破棄した（TTL 不一致）

vrrp version of vrrp packet is not valid or not compatible with this daemon. Packet is discarded
受信した VRRP 広告を破棄した（プロトコルバージョン不一致）

vrrp type of vrrp packet is not valid with this daemon. Packet is discarded
受信した VRRP 広告を破棄した（タイプ不一致）

invalid vrrp packet received (invalid size). Packet is discarded
受信した VRRP 広告を破棄した（受信サイズ異常）

checksum of vrrp packet is invalid. Packet is discarded

受信した VRRP 広告を破棄した（IPv4 チェックサム異常）

The number of the IPv4 redundant address is different
受信した VRRP 広告と IPv4 冗長アドレスの数が不一致だった

IPv4 redundant address mismatch
受信した VRRP 広告と IPv4 冗長アドレスの値が不一致だった

The number of the IPv6 redundant address is different
受信した VRRP 広告と IPv6 冗長アドレスの数が不一致だった

IPv6 redundant address mismatch
受信した VRRP 広告と IPv6 冗長アドレスの値が不一致だった

detection of misconfigured server on the network for vrid = <n> and priority = <m>
冗長構成の設定不一致を検知した（冗長アドレス）

this server is not a master virtual router. Packet is discarded
受信した VRRP 広告を破棄した（冗長アドレス不一致）

the advertisement interval set on received vrrp packet isn't same local. Packet is discarded
受信した VRRP 広告を破棄した（インターバル不一致）

(<state>) socket select error: <reason>
<state>状態でのイベント待機に失敗した

(<state>) Not received packets: <reason>
<state>状態での受信パケットは無い

5.6.16.2 notice

stopped VRRPD with signal=<n>
VRRPD を停止した

VRRP force-backup

強制的な BACKUP 状態にした

VRRP no force-backup

強制的な BACKUP 状態を解除した

server state vrid <n>: <state> (priority <m>)

<state>状態へ遷移した

was waiting <n> seconds for the spanning tree latency

STP 向けの状態遷移遅延時間が経過した

5.6.16.3 info

vrrpd[<n>]: recvmsg is not AF_INET

受信パケットは IPv4 ではない

vrrpd[<n>]: recvmsg is not AF_INET6

受信パケットは IPv6 ではない

peer and local MIP is same. vid=<n> vrid=<m>

冗長構成の peer と local の管理 IP アドレスが同じ

waiting <n> useconds for the forwarding delay

フォワーディング遅延処理をしている

5.6.17 ヘルスチェック - lbhcd

5.6.17.1 error

Cannot allocate memory for config <reason>

設定読み込み時にメモリー取得失敗

Cannot allocate memory for dns <reason>

dns 用ワークメモリー取得失敗

Cannot allocate memory for tsp <reason>

tsp 用ワークメモリー取得失敗

socket error <proto>

ヘルスチェック用 socket の取得失敗

setsockopt error <proto> [RCVBUF]

setsockopt によるレシーブバッファサイズの設定が失敗

Cannot set server state <reason>

カーネルへの server state (up/down) 通知が失敗

socket error <reason>[transparent_flag]

transparent 処理で必要な socket の取得失敗

ioctl error <reason> [transparent_flag]

transparent 処理時、フラグの操作に失敗

write error <reason> [put_server_status]

他プロセスへのヘルスチェック状態の書き出しが失敗

5.6.17.2 notice

server <ip><port> failed a health check; count=<n>, reason=<reason>

ヘルスチェックがシーケンス通りに完了しなかった

vip unknown <ip>

transparent 処理時、該当する仮想 IP のエントリーを検出できなかった

vlan unknown <ip>

transparent 処理時、仮想 IP が属する vlan を検出できなかった

mac unknown <ip>

transparent 処理時、仮想 IP と一致する実サーバーの mac address を検出できなかった

5.6.17.3 info

health check daemon start

ヘルスチェックプロセスが開始された

5.6.18 ログ関連 - lblogd

5.6.18.1 error

lblogd no type

type が指定されていない

lblogd -t <type> exit.

<type>モードの logd プロセスが終了した

no filename

type : rotate でファイルが指定されていない

[<type>:<pid>] poll error <reason>

ログ待ち中に異常が発生した

[<type>:<pid>] open error [rotate] <reason>

ログローテートのファイル open 失敗

[<type>:<pid>] write error [rotate] <reason>

ログローテートのファイル書き込み失敗

[<type>:<pid>] popen error [sendmail] <reason>

sendmail への pipe open 失敗

[<type>:<pid>] malloc error [logd_trap] <reason>

トラップ用ワークエリアの取得失敗

[<type>:<pid>] socket error [logd_trap_listen] <reason>

トラップ用 socket 作成失敗

[<type>:<pid>] bind error [logd_trap_listen] <reason>

トラップ用 socket の初期化失敗

[<type>:<pid>] accept error [logd_trap_accept] <reason>

トラップ用 socket の接続受け入れ失敗

[<type>:<pid>] write error [logd_trap_accept] <reason>
トラップ用 socket の書き出し失敗

[<type>:<pid>] sysctlnametomib error [logd_cap] <reason>
トレースデータ取得失敗

[<type>:<pid>] sysctl error [logd_cap] <reason>
トレースデータ取得失敗

[<type>:<pid>] open error [logd_cap] <reason>
トレースデータファイル open 失敗

[<type>:<pid>] write error [logd_cap_file_header] <reason>
トレースデータファイル書き出し失敗

[<type>:<pid>] write error [logd_cap] <reason>
トレースデータファイル書き出し失敗

5.6.18.2 info

lblogd -t <type> start.
logd プロセスが<type>モードで開始した

5.6.19 SSL クライアント認証 - lbssld

5.6.19.1 warn

warning, not much extra random data
十分なランダム性を確保できなかった

5.6.19.2 info

can't decode certificate <string>
クライアント証明書のデコード失敗 string はクライアント証明書の CN

Cannot decrypt signature for <string>
クライアント証明書の verify が失敗 string はクライアント証明書の CN

Can't decode certificate(CA) <string>

中間 CA の証明書のデコード失敗 string は証明書の CN

Client certificate for <string> <reason>

クライアント証明書は認証されなかった string はクライアント証明書の CN

load crl <ssl 名>

CRL を読み込んだ

5.6.20 CRL 取得 - lbcrld

5.6.20.1 error

getaddrinfo: <reason>

crl で指定された host の ip アドレスが取得できない

socket: <reason>

socket の取得失敗

connect <url>: <reason>

url で指定された host への接続失敗

SSL_new: <reason>

ssl 接続のためのエリア取得失敗

SSL_set_fd: <reason>

ssl 接続のためのエリア初期化失敗

SSL_connect: <reason>

ssl 接続失敗

write: <reason>

crl 取得リクエスト送信失敗

SSL_write: <reason>

ssl 接続での crl 取得リクエスト送信失敗

file write: <reason>

crl ファイルの保存失敗

poll: <reason>

crl 取得レスポンス待ちで異常発生

read: <reason>

crl 取得レスポンス受信失敗

SSL_read: <reason>

ssl 接続での crl 取得レスポンス受信失敗

CONNECT method failed <status>

proxy 経由での接続失敗

open <filename>: <reason>

crl ファイルの open 失敗

Cannot allocate memory <n>

crl 取得レスポンス受信用ワークエリア取得失敗

<status> response from <host:port>

host から 200 および 301,302,304,307 以外の レスポンスを受信した

SSL_CTX_new: <reason>

ssl 処理のためのエリア取得失敗

5.6.20.2 info

<status> response from <host:port>

host から 301,302,304,307 レスポンスを受信した

redirected to <host>:<port>/<path>

host へリダイレクトした

downloaded CRL[<ssl 名>] from <host.port>

crl 取得が成功した

5.6.21 統計情報取得 - lbstatd

5.6.21.1 error

socket chmod error: <reason>

ソケットファイルの権限変更に失敗した

socket listen error: <reason>

ソケットのリッスンに失敗した

Statistics file <filename> open error: <reason> <string>

統計情報ファイルのオープンに失敗した

Statistics file <filename> read error: <reason> <string>

統計情報ファイルの読み込みに失敗した

Statistics file <filename> write error: <reason> <string>

統計情報ファイルの書き出しに失敗した

Statistics file <filename> re-read error: <reason> <string>

統計情報ファイルの再読み込みに失敗した

Statistics file <filename> re-write error: <reason> <string>

統計情報ファイルの再書き出しに失敗した

pidfile <filename> open error: <reason>

PID ファイルの生成に失敗した

5.6.21.2 warn

socket select error: <reason>

ソケットのイベント待機に失敗した

socket bind error: <reason>

ソケットのバインドに失敗した

5.6.21.3 notice

Statistics file <filename> update timing error

統計情報ファイルの更新タイミング異常を検知した

5.6.21.4 info

statistics daemon started

統計情報デーモンが起動した

statistics daemon terminated

統計情報デーモンが停止した

5.6.22 内部状態表示 - systat

5.6.22.1 error

Failed to get SX machine port

イーサネットポート数の取得に失敗した

Failed to get CPU time

CPU 時間の取得に失敗した

Failed to get Memory info

メモリー情報の取得に失敗した

Failed to get CPU temperature

全 CPU コアの平均温度(℃)の取得に失敗した

Failed to get TCP stat

L4 統計の取得に失敗した

Failed to get LB stat

グローバル統計情報の取得に失敗した

Failed to get SSL stat

SSL 統計情報の取得に失敗した

Failed to get Bridge stat

L2 統計の取得に失敗した

Failed to get IPv4 stat

L3 統計(IPv4)の取得に失敗した

Failed to get IPv6 stat

L3 統計(IPv6)の取得に失敗した

Failed to get Ethernet info

EHTER 情報の取得に失敗した

5.6.23 SNMP 関連 - snmp

5.6.23.1 error

snHardware: abort(<n>)

snHardware オブジェクトに対して不正なリクエストを受信した

snHardware: <string>

snHardware オブジェクトの内部処理で異常終了した

snChassisFanTableEntry: abort(<n>)

snChassisFanTableEntry オブジェクトに対して不正なリクエストを受信した

snChassisFanTableEntry: <string>

snChassisFanTableEntry オブジェクトの内部処理で異常終了した

snChassisTemperatureTableEntry: abort(<n>)

snChassisTemperatureTableEntry オブジェクトに対して不正なリクエストを受信した

snChassisTemperatureTableEntry: <string>

snChassisTemperatureTableEntry オブジェクトの内部処理で異常終

了した

snVirtualTableEntry: abort(<n>)
snVirtualTableEntry オブジェクトに対して不正なリクエストを受信した

snVirtualTableEntry: <string>
snVirtualTableEntry オブジェクトの内部処理で異常終了した

snRealTableEntry: abort(<n>)
snRealTableEntry オブジェクトに対して不正なリクエストを受信した

snRealTableEntry: <string>
snRealTableEntry オブジェクトの内部処理で異常終了した

cpu time get error: <string>
CPU 時間取得処理内で異常終了した

vrrpv3OperationsEntry: abort(<n>)
vrrpv3OperationsEntry オブジェクトに対して不正なリクエストを受信した

vrrpv3Router: abort(<n>)
vrrpv3Router オブジェクトに対して不正なリクエストを受信した

vrrpv3Router: <string>
vrrpv3Router オブジェクトの内部処理で異常終了した

vrrpv3StatisticsEntry: abort(<n>)
vrrpv3StatisticsEntry オブジェクトに対して不正なリクエストを受信した

vrrpv3StatisticsEntry: <string>
vrrpv3StatisticsEntry オブジェクトの内部処理で異常終了した

5.6.23.2 notice

snHardware: Undefined OID(<n>)
snHardware オブジェクトにはない OID を検知した

snChassisFanTableEntry: Undefined OID(<n>)

snChassisFanTableEntry オブジェクトにはない OID を検知した

snChassisTemperatureTableEntry: Undefined OID(<n>)

snChassisTemperatureTableEntry オブジェクトにはない OID を検知した

snVirtualTableEntry: Undefined OID(<n>)

snVirtualTableEntry オブジェクトにはない OID を検知した

snRealTableEntry: Undefined OID(<n>)

snRealTableEntry オブジェクトにはない OID を検知した

vrrpv3OperationsEntry: Undefined OID(<n>)

vrrpv3OperationsEntry オブジェクトにはない OID を検知した

vrrpv3Router: Undefined OID(<n>)

vrrpv3Router オブジェクトにはない OID を検知した

vrrpv3StatisticsEntry: Undefined OID(<n>)

vrrpv3StatisticsEntry オブジェクトにはない OID を検知した

5.6.24 TFTP 関連 - tftp

5.6.24.1 error

getaddrinfo: <reason>

ネットワークのアドレスとサービスを変換に失敗した

socket: <reason>

ソケットの作成に失敗した

setsockopt: <reason>

ソケットオプションの設定に失敗した

bind: <reason>

ソケットの bind に失敗した

could not allocate memory for sockets: <reason>

ソケットにメモリーの割り当てに失敗した

select: <reason>

select システムコールの実行に失敗した

5.6.25 内部監視 - lbsvcmon

5.6.25.1 error

popen failed.

実行中のプロセスのリスト取得に失敗した

process <process> is stopped <n> times

プロセス<process>が連続<n>回停止した

SSL Error: System is restarted.

SSL 基板の異常が進行したためシステムが再起動された

5.6.25.2 warn

lbsvcmon is already running, pid: <n>

PID<n>で lbsvcmon が既に起動している

can't open pid file
PID ファイルの生成に失敗した

can't daemonize
lbsvcmon のデーモン化に失敗した

can't write pid
PID ファイルへの書き込みに失敗した

sysctl failed
net.lb.trace_timeout の値の更新に失敗した

process <process> is stopped
プロセス<process>が停止した

process <process> is restarted
停止したプロセス<process>が起動された

process <process> failed restart
停止したプロセス<process>の起動に失敗した

get request_counts failed
SSL 基板が処理したリクエスト数の取得に失敗した

get error_counts failed
SSL 基板で処理エラーとなった数の取得に失敗した

System has changed to debug mode.
SSL 基板に異常を検知したためデバッグモードに移行した

5.6.25.3 notice

SSL Error: Request:<n> Error:<m>
SSL 通信でリクエスト数<n>に対して<m>回の処理エラーが発生した

5.6.25.4 info

received SIGPIPE
シグナル SIGPIPE を受信した

received SIGNAL : No.=<n>
シグナル(No.=<n>)を受信した

<filename> file is found.
コアダンプファイル<filename>が生成された

save core file failed
コアダンプファイルの保存に失敗した

5.6.26 SSL 証明書自動更新 - lbcertupd

5.6.26.1 error

Cannot allocate memory for <発生箇所>
メモリの取得に失敗

Can't create ssl <ssl ポリシー名> for certificate update.
自動更新用の ssl ポリシーが作成できない

Can't entering config mode. check other terminal.
他の端末が特権モードに入っているため自動更新できない
・冗長構成の時はスタンバイ機との同期も必要

popen error: for sysadm <発生箇所>
CLI との接続に失敗

unknown certificate found. <プレフィックス> create a new ssl.
プレフィックスにマッチする最新の ssl ポリシーの証明書が使用できないためダウンロード用に新しい ssl を作成した

HA state get failed
冗長構成のとき冗長構成の状態を取得できない

<ファイル名> open error: <発生箇所>
必要な証明書にアクセスできない

<ファイル名> close error: <発生箇所>
証明書をクローズできない

x509 file decode error. <発生箇所>
証明書を解析できない

Can't write memory for ssl <ssl ポリシー名> CSR upload.
CSR 作成後保存ができない
※秘密鍵が保存されない可能性があるので注意

deccode pass: decode error <発生箇所,内容>
アカウントまたは秘密鍵のパスワード取得失敗

5.6.26.2 warn

unable to write to csr *xxxx* <ssl ポリシー名>
CSR 作成でテンポラリーファイルが作成できない

unable to create to key. ssl= <ssl ポリシー名> keylen= <鍵長>
自動更新用の秘密鍵が作成できない

CSR upload problem : <発生箇所/エラー詳細>
CSR アップロード失敗

CERT/KEY download problem : <発生箇所/エラー詳細>
(鍵、)証明書のダウンロード失敗
※鍵は CSR なしモード時のみ

interprocess communication problem : <発生箇所/エラー詳細>
CLI との通信エラー

key type, ssl <ssl ポリシー名> was changed. check virtual's cipher-suite.
自動更新する証明書は公開鍵のタイプ(rsa/ecc)が変わるため仮想サーバーの cipher-suite に注意が必要

Certificate, ssl <ssl ポリシー名>　expiring soon
証明書の期限切れが近い

Certificate, ssl <ssl ポリシー名>　expired
証明書の期限が切れた

5.6.26.3 notice

ssl name <プレフィックス> not found, created a new one.
プレフィックスにマッチする ssl ポリシーが無いため、ダウンロード用に新規に ssl ポリシーを作成した
※この場合 ssl ポリシーは仮想サーバーに割り当てられていないので、証明書のダウンロード完了後、仮想サーバーに割り当てる必要があります

CSR uploaded. Certificate update time has come. ssl <ssl ポリシー名>
証明書の期限切れが迫って来たため、CSR を指定した url にアップロードした

unable cleate csr <プレフィックス> please set <設定>.
<設定>.が抜けているため CSR を作成できない

downloaded <プレフィックス>, key and certificate mismatch
ダウンロードした証明書が鍵と一致しない

downloaded <プレフィックス>, certificate was bad.
ダウンロードした証明書が使用不可または期限切れ

New certificate <ssl ポリシー名> was ready.
ダウンロードが正常に終了した

New SSL <ssl ポリシー名> was effect to virtual. <適用した virtual 数>

更新した ssl ポリシーの、仮想サーバーへの適用が完了した

ssl <ssl ポリシー名> was deleted

プレフィックスにマッチする ssl ポリシーが世代管理により、3 世代以上前の ssl を削除した

exit_cud <PID> sig=<要因番号>

自動更新デーモンが終了した

5.6.26.4 info

[CLI] <エラー情報>

自動更新デーモンが CLI に発行したコマンドのエラーレスポンス
5.5 CLI エラーメッセージ 参照

cannot decode account password. ssl <ssl ポリシー名>

ダウンロード時にアカウントのパースワードのデコード失敗

cannot decode account password. (csr_upload) ssl <ssl ポリシー名>

CSR アップロード時にアカウントのパースワードのデコード失敗

ssl <ssl ポリシー名> was used.

ssl が仮想サーバーで使用中のため削除できない

cud_cert_comp: Can't get temporary.

証明書比較のためのテンポラリーが確保できない

5.7 SNMP

本章では本製品の実装する拡張 MIB について記述します。

5.7.1 独自 MIB

ssolNetwiserObjects = enterprises.955.1.22.1

オブジェクト ID	オブジェクト名	意味
ssolNetwiserObjects.1	snHardware	-
ssolNetwiserObjects.1.1	snCpuUtilization	CPU 使用率(×0.1%)
ssolNetwiserObjects.1.2	snMemorySize	総メモリーバイト数
ssolNetwiserObjects.1.3	snMemoryAvailable	空きメモリーバイト数
ssolNetwiserObjects.1.4	snMemoryUtilization	メモリー使用率(×0.1%)
ssolNetwiserObjects.1.7	snChassisFanTable	-
ssolNetwiserObjects.1.7.1	snChassisFanTableEntry	-
ssolNetwiserObjects.1.7.1.1	snChassisFanIndex	-
ssolNetwiserObjects.1.7.1.2	snChassisFanState	シャーシファン状態 (1) good (2) bad (3) notpresent
ssolNetwiserObjects.1.8	snChassisTemperatureTable	-
ssolNetwiserObjects.1.8.1	snChassisTemperatureTable Entry	-
ssolNetwiserObjects.1.8.1.1	snChassisTemperatureIndex	-
ssolNetwiserObjects.1.8.1.2	snChassisTemperature	シャーシ温度(℃)
ssolNetwiserObjects.1.9	snChassisPsuTable	-
ssolNetwiserObjects.1.9.1	snChassisPsuTableEntry	-
ssolNetwiserObjects.1.9.1.1	snChassisPsuIndex	-
ssolNetwiserObjects.1.9.1.2	snChassisPsuState	冗長電源状態 (1) good (2) fault (3) fanfault (4) notpresent
ssolNetwiserObjects.2	snVirtualTable	-
ssolNetwiserObjects.2.1	snVirtualTableEntry	仮想サーバー
ssolNetwiserObjects.2.1.1	snVirtualIndex	-
ssolNetwiserObjects.2.1.2	snVirtualIpAddress	IP アドレス
ssolNetwiserObjects.2.1.3	snVirtualPort	ポート番号
ssolNetwiserObjects.2.1.4	snVirtualProtocol	プロトコル
ssolNetwiserObjects.2.1.5	snVirtualState	設定状態 (1) enabled

			(2) disabled
	ssolNetwiserObjects.2.1.6	snVirtualCurrentConnections	現在のコネクション数
	ssolNetwiserObjects.2.1.7	snVirtualPeakConnections	ピークコネクション数
	ssolNetwiserObjects.2.1.8	snVirtualTotalConnections	総コネクション数
	ssolNetwiserObjects.2.1.9	snVirtualTotalTxPackets	クライアントへの 送信パケット数
	ssolNetwiserObjects.2.1.10	snVirtualTotalTxBytes	クライアントへの 送信バイト数
	ssolNetwiserObjects.2.1.11	snVirtualTotalRxPackets	クライアントからの 受信パケット数
	ssolNetwiserObjects.2.1.12	snVirtualTotalRxBytes	クライアントからの 受信バイト数
ssolNetwiserObjects.3		snRealTable	-
ssolNetwiserObjects.3.1		snRealTableEntry	実サーバー
	ssolNetwiserObjects.3.1.1	snRealIndex	-
	ssolNetwiserObjects.3.1.2	snRealIpAddress	IP アドレス
	ssolNetwiserObjects.3.1.3	snRealPort	ポート番号
	ssolNetwiserObjects.3.1.4	snRealProtocol	プロトコル
	ssolNetwiserObjects.3.1.5	snRealAdminState	設定状態 (1) enabled (2) disabled
	ssolNetwiserObjects.3.1.6	snRealOperState	稼動状態 (1) up (2) down
	ssolNetwiserObjects.3.1.7	snRealLastChange	稼動状態が変化したときの sysUpTime
	ssolNetwiserObjects.3.1.8	snRealCurrentConnections	現在のコネクション数
	ssolNetwiserObjects.3.1.9	snRealPeakConnections	ピークコネクション数
	ssolNetwiserObjects.3.1.10	snRealTotalConnections	総コネクション数
	ssolNetwiserObjects.3.1.11	snRealTotalTxPackets	クライアントへの 送信パケット数
	ssolNetwiserObjects.3.1.12	snRealTotalTxBytes	クライアントへの 送信バイト数
	ssolNetwiserObjects.3.1.13	snRealTotalRxPackets	クライアントからの 受信パケット数
	ssolNetwiserObjects.3.1.14	snRealTotalRxBytes	クライアントからの 受信バイト数

5.7.2 標準 MIB

本製品が対応している標準 MIB のオブジェクトを明記します。

system =1.3.6.1.2.1.1

オブジェクト ID	オブジェクト名	意味
systems	system	-
systems.1	sysDescr	機器情報 （ホスト名、カーネル ID、機種名、バージョン数）
systems.2	sysObjectID	ベンダ OID
systems.3	sysUpTime	SNMP プロセスが起動（または再起動）してからの UpTime
systems.4	sysContact	SNMP コンタクト値
systems.5	sysName	ホスト名
systems.6	sysLocation	SNMP ロケーション値
systems.7	sysServices	本装置のサービス種別

interfaces =1.3.6.1.2.1.2

オブジェクト ID	オブジェクト名	意味
interfaces	intrefaces	-
interfaces.1	ifNumber	ネットワークインターフェイス数
interfaces.2	ifTable	-
interfaces.2.1	ifEntry	-
interfaces.2.1.1	ifIndex	ネットワークインターフェイス固有値
interfaces.2.1.2	ifDescr	ネットワークインターフェイス名
interfaces.2.1.3	ifType	ネットワークインターフェイス種別
interfaces.2.1.4	ifMtu	MTU 値
interfaces.2.1.5	ifSpeed	帯域幅
interfaces.2.1.6	ifPhysAddress	MAC アドレス
interfaces.2.1.7	ifAdminStatus	設定状態 (1) up (2) down (3) testing
interfaces.2.1.8	ifOperStatus	動作状態

					(1) up (2) down (3) testing (4) unknown (5) dormant (6) notPresent (7) lowerLayerDown
			interfaces.2.1.9	ifLastChange	現在の状態に遷移した際の UpTime
			interfaces.2.1.10	ifInOctets	受信したパケットのオクテット数
			interfaces.2.1.11	ifInUcastPkts	受信したユニキャストパケット数
			interfaces.2.1.12	ifInNUcastPkts	受信した非ユニキャストパケット数
			interfaces.2.1.13	ifInDiscards	エラー以外の理由で破棄された受信パケット数
			interfaces.2.1.14	ifInErrors	エラーになった受信パケット数
			interfaces.2.1.15	ifInUnknownProtos	非サポートプロトコルの受信パケット数
			interfaces.2.1.16	ifOutOctets	転送したパケットのオクテット数
			interfaces.2.1.17	ifOutUcastPkts	送信したユニキャストパケット数
			interfaces.2.1.19	ifOutDiscards	エラー以外の理由で破棄された送信パケット数
			interfaces.2.1.20	ifOutErrors	エラーになった送信パケット数
			interfaces.2.1.21	ifOutQLen	送信キューに溜まっているパケット数
			interfaces.2.1.22	ifSpecific	追加情報への参照

vrrpv3Objects = 1.3.6.1.2.1.207

オブジェクト ID			オブジェクト名	意味
vrrpv3Objects			vrrpv3MIB	-
	vrrpv3Objects.1.1.1.1.12		vrrpv3OperationsUpTime	仮想ルーターの UpTime
	vrrpv3Objects.1.2		vrrpv3Statistics	-
		vrrpv3Objects.1.2.1	vrrpv3RouterChecksumErrors	無効なチェックサム値の VRRP パケット受信数
		vrrpv3Objects.1.2.2	vrrpv3RouterVersionErrors	無効なバージョン番号の VRRP パケット受信数
		vrrpv3Objects.1.2.3	vrrpv3RouterVrIdErrors	無効な VRID の VRRP パケット受信数

		vrrpv3Objects.1.2.5		vrrpv3StatisticsTable	-
			vrrpv3Objects.1.2.5.1.1	vrrpv3StatisticsMasterTransitions	VRRP マスターへの移行数
			vrrpv3Objects.1.2.5.1.2	vrrpv3StatisticsNewMasterReason	マスターへ移行した際の理由 (0) 移行なし、または現在バックアップ状態である (1) プライオリティー (2) プリエンプション (3) 不明
			vrrpv3Objects.1.2.5.1.3	vrrpv3StatisticsRcvdAdvertisements	VRRP 広告受信数
			vrrpv3Objects.1.2.5.1.4	vrrpv3StatisticsAdvIntervalErrors	不正な間隔で受信した VRRP 広告パケット数
			vrrpv3Objects.1.2.5.1.5	vrrpv3StatisticsIpTtlErrors	TTL エラー発生数
			vrrpv3Objects.1.2.5.1.6	vrrpv3StatisticsProtoErrReason	プロトコルエラー (0) noError (1) ipTtlError (2) versionError (3) checksumError (4) vrIdError
			vrrpv3Objects.1.2.5.1.7	vrrpv3StatisticsRcvdPriZeroPackets	優先度 0 の不正な VRRP 広告受信数
			vrrpv3Objects.1.2.5.1.8	vrrpv3StatisticsSentPriZeroPackets	優先度 0 の不正な VRRP 広告送信数
			vrrpv3Objects.1.2.5.1.9	vrrpv3StatisticsRcvdInvalidTypePackets	不正な type フィールドを持つ VRRP 広告受信数
			vrrpv3Objects.1.2.5.1.10	vrrpv3StatisticsAddressListErrors	不正なアドレスの仮想ルーターから受信したパケット数
			vrrpv3Objects.1.2.5.1.11	vrrpv3StatisticsPacketLengthErrors	不正なサイズの VRRP 広告受信数

5.7.3 独自 TRAP オブジェクト一覧

ssolNetwiserNotifications = enterprises. 955.1.22.0

オブジェクト ID	オブジェクト名	意味
ssolNetwiserNotifications.2	snChassisFanStateChange	シャーシファン状態が変化
ssolNetwiserNotifications.3	snRealOperStateChange	実サーバー状態が変化
ssolNetwiserNotifications.4	snLogOutPut	任意のログ文字列の出力
ssolNetwiserNotifications.5	snChassisPsuStateChange	冗長電源状態が変化

5.8 異常があった時

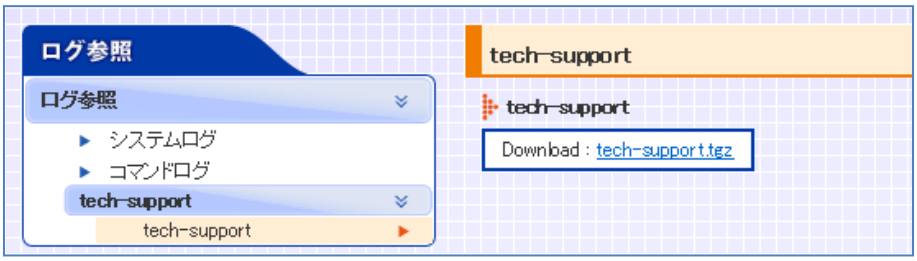
本製品に障害が発生した際は、弊社テクニカルサポートを受けるための機器情報（以下、テクニカルサポートログ）を取得し、弊社サービス取扱所宛てにお送りください。

telnet、ssh を使用して本製品にアクセスしテクニカルサポートログの取得を行う場合、***export tech-support*** コマンドを実行します。
export tech-support コマンドでは、ftp または scp を使用して、テクニカルサポートログファイルを任意のリモートホストに転送します。

```
netwiser> export tech-support {ftp | scp} <転送先ｱﾄﾞﾚｽ> <転送先ﾊﾟｽ> <ﾛｸﾞｲﾝﾕｰｻﾞｰ名>
```

WEB 管理画面からテクニカルサポートログの取得を行う場合 tech-support 画面からログ情報を取得します。

場所：ログ参照 > tech-support > tech-support
テクニカルサポートログファイルへのリンクから、右クリックでダウンロードしてください。



5.9 その他参考情報

よくある質問、技術資料、構成例に関しては、下記ホームページにも記載がございます。

http://www.seiko-sol.co.jp/products/loadbalancer/

ライセンス

以下に本製品で使用しているソフトウェアのライセンス条項の一覧を示します.

【FreeBSD】

【Apache】

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the

Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its

distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
   agreed to in writing, Licensor provides the Work (and each
   Contributor provides its Contributions) on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
   implied, including, without limitation, any warranties or conditions
   of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
   PARTICULAR PURPOSE. You are solely responsible for determining the
   appropriateness of using or redistributing the Work and assume any
   risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
   whether in tort (including negligence), contract, or otherwise,
   unless required by applicable law (such as deliberate and grossly
   negligent acts) or agreed to in writing, shall any Contributor be
   liable to You for damages, including any direct, indirect, special,
   incidental, or consequential damages of any character arising as a
   result of this License or out of the use or inability to use the
   Work (including but not limited to damages for loss of goodwill,
   work stoppage, computer failure or malfunction, or any and all
   other commercial damages or losses), even if such Contributor
   has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
   the Work or Derivative Works thereof, You may choose to offer,
   and charge a fee for, acceptance of support, warranty, indemnity,
   or other liability obligations and/or rights consistent with this
   License. However, in accepting such obligations, You may act only
   on Your own behalf and on Your sole responsibility, not on behalf
   of any other Contributor, and only if You agree to indemnify,
   defend, and hold each Contributor harmless for any liability
   incurred by, or claims asserted against, such Contributor by reason
   of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following
boilerplate notice, with the fields enclosed by brackets "[]"
replaced with your own identifying information. (Don't include
the brackets!) The text should be enclosed in the appropriate
comment syntax for the file format. We also recommend that a
file or class name and description of purpose be included on the
same "printed page" as the copyright notice for easier
identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

【Driver for the Intel(R) PRO/1000 Family of Adapters】

Copyright (c) 2001-2010, Intel Corporation
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

【Driver for the Intel XL710 Ethernet Controller Family】

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the Intel Corporation nor the names of its
   contributors may be used to endorse or promote products derived from
   this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

【libFTDI】

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change

free software--to make sure the software is free for all its users.

  This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

  When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

  To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

  For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

  We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

  To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is

modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to

encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs

(which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the

entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library

facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not

excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new

versions of the Lesser General Public License from time to time.
Such new versions will be similar in spirit to the present version,
but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library
specifies a version number of this License which applies to it and
"any later version", you have the option of following the terms and
conditions either of that version or of any later version published by
the Free Software Foundation. If the Library does not specify a
license version number, you may choose any version ever published by
the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free
programs whose distribution conditions are incompatible with these,
write to the author to ask for permission. For software which is
copyrighted by the Free Software Foundation, write to the Free
Software Foundation; we sometimes make exceptions for this. Our
decision will be guided by the two goals of preserving the free status
of all derivatives of our free software and of promoting the sharing
and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO
WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW.
EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR
OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY
KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE
LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME
THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN
WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY
AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU

FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

```
    You should have received a copy of the GNU Lesser General Public
    License along with this library; if not, write to the Free Software
    Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA  02110-1301  USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary.  Here is a sample; alter the names:

  Yoyodyne, Inc., hereby disclaims all copyright interest in the
  library `Frob' (a library for tweaking knobs) written by James Random Hacker.

  <signature of Ty Coon>, 1 April 1990
  Ty Coon, President of Vice

That's all there is to it!
```

SEIKO
セイコーソリューションズ株式会社
〒261-8507 千葉県千葉市美浜区中瀬 1-8
support@seiko-sol.co.jp