

サービス利用手順書 かんたんネットワークプロテクション編

目 次

# 内容

改訂履歴	2
はじめに	3
1. サービスについて	4
(1)サービス提供内容	4
(2)サービス提供範囲	4
(3)サービス利用条件	6
①ご利用環境	6
②推奨導入構成	6
③サイジング	7
(4)サービス利用の流れ	7
(5)サービス提供範囲外の機能について	8
2. ご利用環境の構成	9
3. ネットワークプロテクション機能の初期設定	10
3-1.ファイアウォール	10
(1)初期ポリシーの設定手順	10
(2)ライブログの確認手順	12
3 – 2 . NAT	13
(1)マスカレード設定手順	13
(2)DNAT の設定手順	14
3 – 3.侵入検知(IPS)	17
(1)グローバル設定手順	17
(2)攻撃パターン設定手順	19
(3)DoS フラッド防御設定手順	21
(4)ポートスキャン防御設定手順	22
3 – 4.高度な防御(Advanced Threat Protection)	23
(1)高度な防御(Advanced Threat Protection)設定手順	23

さくらのクラウド「Sophos UTM」 サービス利用手順書 かんたんネットワークプロテクション編

# 改訂履歴

版数	更新日	更新内容	更新者
1.0	2018/1/25	初版作成	興安計装株式会社

サービス利用手順書 かんたんネットワークプロテクション編

# はじめに

### 本手順書に関する注意事項

この手順書は、一般的な評価環境を簡単なステップで構築するための補助資料です。導入に際して必要な全てのトピックについての網羅的な解説は意図しておりません。個々の トピックについての詳細は、管理者ガイドをご確認頂くようお願い致します。

本サービスにおけるお問い合わせは、さくらインターネット株式会社が提供するサポート窓口 をご利用いただくか、技術情報にて公開されたナレッジをご参照ください。本サービスの製品 SophosUTM9の開発元であるソフォス株式会社への直接の問い合わせを固く禁じます。

## 本手順書の目的と位置づけ

目的: Sophos UTM9 の配下に展開された保護対象システム(サーバ若しくはクライアント) をネットワークプロテクションの各機能で保護する基本設定手順をご提供すること。

本手順の順番に沿って設定を進めて頂くことにより、Sophos UTM9 によるシステムの保護に必要な初期構成が可能となります。

本手順書ではサービス利用手順【初期導入編】に従い、セットアップされていることを 前提としております。またネットワークプロテクション以外の機能については、本手順書 には記載しておりません。

# 1. サービスについて

# (1)サービス提供内容

提供項目	内容
Sophos UTM9 アーカイブイメージ	一部機能を除き、動作検証及び初期設定が完了した状態の アーカイブイメージを提供します。
Sophos UTM9 利用ライセンス	当社が提供したアーカイブイメージから展開した SophosUTM9 のみが適用可能なライセンスを提供します。

# (2)サービス提供範囲

本サービスで提供される SophosUTM9の機能は以下の通りです。

サービス項目	機能
	• DNS • DHCP
ネットワークサービス	・NTP 上記に付随する各種オプション
	Uモートアクセスサービスを提供するブラウザベースアプリケーショ
ユーザポータル	ンと付随する各種オプション
	・ファイアウォール
ネットワークプロテクション	・侵入防御(IPS)
	・高度な防御機能(ATP)
	上記に付随する各種オプション
	・Web フィルタリング
Web プロテクション	・アプリケーションコントロール
	上記に付随する各種オプション
	・SMTP プロキシ
E メールプロテクション	・POP3 プロキシ
	上記に付随する各種オプション
高度な防御	よりリスクの高い通信の防御
Web #_バプロテクション	Web Application Firewall (WAF)
	上記に付随する各種オプション

サービス利用手順書 かんたんネットワークプロテクション編

	• IPsec
サイト間 VPN	• SSL
	• Amazon VPC
	• SSL
	• РРТР
リモートアクセス	• L2TP over IPsec
	• IPsec
	・HTML5 VPN ポータル
	・Cisco™ VPN クライアント
	・各サービスのログ取得
ログとレポート	・各サービスのレポート作成
	・エグゼクティブサマリーレポートの作成

本サービスで提供される SophosUTM9の詳細機能については Owlook セキュリティマネジメン

トサービス仕様書内の3.提供機能の詳細をご参照ください。

サービス利用手順書 かんたんネットワークプロテクション編

## (3) サービス利用条件

本サービスの利用条件は以下の通りです。

## ①ご利用環境

さくらのクラウドサービス内の全てのリージョンよりご利用可能です。

### ②推奨導入構成

Sophos UTM9 はご利用の環境における外部(インターネット)との接続点への導入し、内部 はスイッチを利用しセグメントを構築してください。



また以下のように、ルーター+スイッチ機能で SophosUTM9 へ任意の IP アドレスを設定する



\$6\$ Copyright© 2017 KOANKEISO CO., LTD. All rights reserved.

ことが可能です。

#### サービス利用手順書 かんたんネットワークプロテクション編

#### **③サイジング**

さくらのクラウドサービス環境へ SophosUTM9 を展開した場合のスペック目安は以下の通り です。あくまで目安でありパフォーマンスを保証する数値ではありません。ハイパーバイザーの ご利用環境によって最大 10%までのパフォーマンスの低下が予想されます。

vCPU	2	2	4	4	2*6	2*10
メモリ(GB)	4	8	12	16	24	48
HDD(GB)	100※1					
FW 最大※2 (Mbps)	3,100	13,000	20,000	25,000	40,000	60,000
IPS 最大 (Mbps)	750	3,000	6,000	7,000	12,000	16,000
FW + ATP + IPS 最 大 (Mbps)	680	2,850	5,890	6,650	11,980	14,600
新規最大 TCP 接続/秒	24,000	70,000	120,000	130,000	160,000	190,000
同時最大 TCP 接続数	2,000,000	4,000,000	6,000,000	8,000,000	12,000,000	20,000,000
同時最大接続 IPsec VPN トンネル数	175	500	1,200	1,600	2,200	2,800
同時接続 SSL VPN トンネル数	75	200	250	280	340	420

※1 Disk サイズの推奨は 100GB です。ログの保持には Syslog サーバへの転送機能を推奨します。

※2 1518 バイトのパケットサイズ、デフォルトのルールセット環境の目安値です。

# (4) サービス利用の流れ

本サービスご利用までの流れは以下の通りとなります。実施内容についての詳細手順はさくら インターネットより技術情報として公開されています。

提供ステップ	実施内容
	本サービスはさくらのクラウドサービス上で提供可能なサービスと
①さくらのクラウトリーヒスの アカウント取得	なります。その為、利用者はさくらのクラウドサービスが利用でき
	る状態であることが前提となります。
	さくらのクラウドサービスより本サービスより提供される
②SophosUTM9の展開	SophosUTM9 のアーカイブイメージをパブリックアーカイブから展
	開します。
③利田相約へ同音	SophosUTM9へ初回ログイン時に表示される URL より利用規約を確
	認し、同意頂きます。

サービス利用手順書 かんたんネットワークプロテクション編

@ライヤンフサーバーへの培結	SophosUTM9 へ当社が提供するライセンスサーバへ接続設定を行い
ゆうれ ビンスリーバーパの接続	ます。
	SophosUTM9 がライセンスサーバへ接続後、利用ライセンスが有効
⑤利用ライセンスの有効化	になります。利用ライセンスの有効化処理はご利用環境によって 30
	分程お待ちいただく事があります。
	SophosUTM9の機能がご利用いただけるようになり、利用者にて設
©小小川用」如	定が可能となります。
②利田牧乙	SophosUTM9を一定期間停止、または削除した場合、ライセンスは
נ ≋אודעיאי⊘	破棄され利用終了となります。

### (5) サービス提供範囲外の機能について

本サービスで提供される Sophos UTM9 利用ライセンスはほぼすべての機能をご利用いただ く事が可能なライセンスです。その為、本サービス仕様書に記載のない機能も利用ライセンスに 含まれます。

またさくらのクラウドサービス環境では、Sophos UTM9 に搭載された HA クラスタ機能及び ブリッジインターフェイスの構成をご利用いただく事ができません。

本サービス仕様書に記載がある機能は、推奨導入構成において動作確認ができている機能となります。

本サービス仕様書に記載のない機能または、推奨外の構成でご利用いただく場合、本サービス 内でサポートすることはできません。本サービス仕様書に記載のない機能または、推奨外の構成 は、利用者の責任でご利用いただきますようお願いいたします。

# 2. ご利用環境の構成

本手順書では以下の構成であることを前提に記載いたします。



# 【構成要件】

- > Sophos UTM9 はご利用の環境におけるインターネットとの接続点へ導入します。
- Sophos UTM9 はインターネットセグメント(WAN) 側とプライベートセグメント(LAN)
   側の 2 つの NIC を持ちます。プライベートセグメント(LAN) 側の IP アドレスは
   192.168.0.1/24 を持ちます。
- ▶ プライベートセグメント(LAN)は192.168.0.0/24のネットワーク帯域で構成します。
- プライベートセグメント(LAN)はスイッチを利用しセグメントを構築します。
- > 保護対象システムの IP アドレスは 192.168.0.2/24 を持ちます。
- 保護対象システムのデフォルトゲートウェイは Sophos UTM9 のプライベートセグメント (LAN) 側の IP アドレス 192.168.0.1/24 を向いています。

サービス利用手順書 かんたんネットワークプロテクション編

# 3. ネットワークプロテクション機能の初期設定

## 3-1. ファイアウォール

#### (1)初期ポリシーの設定手順

ファイアウォールは初期状態ですべての通信を「拒否」します。その為、通信を許可するポリシ ーを追加する必要があります。

①ネットワークプロテクション > ファイアウォール >ルールタブより、「新規ルール」を押下

します。

₽検索	ファイアウォール
ダッシュボード	ルール 😵 送受信国別 送受信国除外 ICMP 詳細
マネジメント	▲ 新規ルール マ ペ い
定義とユーザ	
インタフェースとルーティング	2.5イフログを開く 衣小. 10 ♥ 0-0 010
ネットワークサービス	□ アクション III▼ ソート應 優先順位 asc ▼
ネットワークプロテクション	
ファイアウォール	
侵入防御(IPS)	
サーバロードバランシング	
VOIP 詳細	そのようなファイアウォールルレールは定義されていません。
a十初以	

②「ルールを追加」画面に遷移します。以下の通り、設定を入力し、「+」ボタンを押下し詳細 メニューを展開します。

グループ:グループなし 優先順位:最下位 送信元:Internal (Network) サービス:Any 宛先:Any アクション:許可

優先順位:	最下位			¥
送信元:			-	+
	DND		DND	
サービス:				+
	DND		DND	-
対象・		DHD	-	
7670-			_	+
				D.K
アクション:	許可			~
コメント:				

サービス利用手順書 かんたんネットワークプロテクション編

この時、送信元、サービス、宛先のフォルダアイコンを押下すると、左メニューにオブジェクト が転嫁されます。オブジェクトの一覧からドラック&ドロップで設定が可能です。

© Any IPv6 転 ec2-52-68-241-41.ap-north	📄 ライブログを開く			
🛤 External (Address)	ルールを追加			×
🔝 External (Broadcast)	ガループ・	・・ グリープナ	N . ••	J
External (Network)				
🔝 Internal (Address)	優先順位:	最下位		~
🔝 Internal (Broadcast)	送信元:			+
🔝 Internal (Network)				
🗊 Internet IPv4	$\rightarrow$	🛤 Internal (	Network)	
🚅 Internet IPv6				
🛤 kanshi_test (Address)	H 137.	DN		DNI
kanshi_test (Broadcast)	J-EA.			+
🖾 kanshi_test (Network)				
E KOAN				DN
so NTP Server Pool				DAU
NWC-SUM02	宛先:		<b>-</b>	+
🔤 ryosuke-isobe (User Netw		DND	DND	
🔝 smtp.ocn.ne.jp				DN
🖙 emtrioca ne ini 2				

③「詳細」より以下の通り、設定を入力し、「保存」ボタンを押下します。

時間帯:常時 トラフィックをログ:チェック 送信元 MAC アドレス:なし

時間帯:	<< 常時 >>	~
トラフィックをログ:	2	
送信元MACアドレス	::なし ::	~

④ポリシー作成直後は、「無効」状態になっているため、有効化ボタンを押下し、ポリシーを有 効にします。

□ アクション III▼	ソート順: 優先順位 asc	<b>~</b>		
🗌 📝 編集	<u>0</u> 11	Internal (Network) 🔝 💶	🕸 Any	0
🗙 削除		🖊 Any		
自複製				

サービス利用手順書 かんたんネットワークプロテクション編

□ アクション ■▼	ソート順: 優先順位 asc	•		
🗌 📝 編集	11	Internal (Network) 🔛 💶	🛶 🙎 Any	0
★ 削除		💉 Any		
自複製				

以上で、初期ポリシーの設定手順は完了です。

# (2)ライブログの確認手順

ファイアウォールの動作状況をライブログで確認するには、下記の手順を実行します。 ①「ライブログを開く」ボタンを押下します。

UTM 9	👤 admin   🗾   🕜 🧲 🔅	
ファイアウォール		
ルール 😢 送受信国別 送受信	国除外 ICMP 詳細	
+ 新規ルール	ユーザ作成ファイアウォール	« »
	<b>●</b> 検索 検索 +=.	
🛐 ライフログを開く	衣小.	10 💙 1-1 01 1
□ アクション Ⅲ▼ ソート順: 優先順位	asc 🗸	
□ 🛛 編集 🛛 🚺 11	Internal (Network) 📭 💶 💭 🔊 💭 Any	0
★ 削除	💉 Any	
自複製		
	UTM 9 ファイアウォール ルール ②送受信国別 送受信 + 新規ルール ライブログを開く アクション 国 マ ソート縣 優先順位 深編集 11 X 削除 福製	UTM9 ↓ ▲ admin   ②   ② C ☆ ファイアウォール ルール ②送受信国別 送受信国除外 ICMP 詳細 + 新規ルール ユーザ作成ファイアウォール マ ●検索 検索 表示: アクション ■ マ ソート庵 優先順位 asc マ ■ 244 ※ 副除 ● 複製 11 Internal (Network) ■ ▲ Any ※ Any ● 複製

②別ウィンドウでログ画面が立ち上がります。ルールに一致したもの、拒否したもの等の通信状態をリアルタイムに確認することができます。

6	WebA		
🛈 🗞 https:// <b>192.168.12.1</b> :4444/logwin	.html		
ライブログ: ファイアウォール Filter:			
14:57:02 パケットフィルタルール#11 TCP			
14:57:02 パケットフィルタルール#11 TCP			
14:57:02 NATルール#3 TCP			
14:57:04 デフォルト破棄 TCP			
14:57:05 デフォルト破棄 TCP			
14:57:05 デフォルト破棄 CLD	AP		
14:57:23 NATJレーJレ#3 TCP			
14:57:29 デフォルト破棄 TCP			
14:57:33 デフォルト破棄 TCP			
14:57:35 デフォルト破棄 TCP			
14:57:41 デフォルト破棄 TCP			
14:57:44 NATJレーJレ#3 TCP			

ファイアウォールルールをオンにしたりオフにしたりして通信されているパケットの状態をご 確認ください。

サービス利用手順書 かんたんネットワークプロテクション編

3-2. NAT

(1)マスカレード設定手順

マスカレードの機能を利用して内部ネットワークから外部のネットワークへアクセスするには、 下記の手順を実行します。

①ネットワークプロテクション > NAT > マスカレードタブより「新規マスカレードルール」ボタンを押下します。

▶検察	NAT					
ダッシュボード	マスカレード NAT					
マネジメント	➡ 新想マスカレードルール	▶検索	検索			// »
定義とユーザ		12				··· //
インタフェースとルーティング				表示:	10 🔻	0-0 of 0
ネットワークサービス	□ アクション Ⅲ▼ ソート順: 個	医先順位 asc ▼				
ネットワークプロテクション						
ファイアウォール						
NAT						
侵入防御(IPS)						
サーバロードバランシング						
VoIP		マスカレードルールが定義されて	ていません。			
詳細		新しく作成するには新規 マスカレード ルート	ヽボタンをクリック	します。		
Webプロテクション						
Eメールプロテクション						
高度な防御						

②「マスカレードルール」を追加より、以下の通り入力し、「保存」ボタンを押下します。

ネットワーク : Internal(Network) 優先順位 : 最下位 I/F : External 使用アドレス : プライマリアドレス

•	マスカレードルールを注	追加 ×
	ネットワーク: 📋 🖡	🗈 Internal (Netw 🚞 🕂
	優先順位 最下位	位 🔻
	I/F: Exter	rnal 🔹
	使用アドレス: << ブ	゚ライマリアドレス×▼
	1	保存 🗙 キャンセル

③有効化ボタンを押下しマスカレードルールを有効にします。

■ アクション II▼	ソート順: 優先順位 asc ▼	
🗌 📝 編集	□ Internal (Network) → I External	0
🗙 削除		
自複製		

サービス利用手順書 かんたんネットワークプロテクション編

アクション III	<ul> <li>✓ ソート順: 優先順位 asc ▼</li> </ul>	
🗌 📝 編集	IIIII Internal (Network) → III External	0
★ 削除		
■ 複製		

#### (2) DNAT の設定手順

DNAT(Destination NAT)ルールを設定するには、以下の手順を実行します。 ここではインターネット上の任意のユーザから、保護対象システム(Windows Server2012R2) にカスタマイズしたポート番号でリモートデスクトップ接続する想定の手順となります。

①ネットワークプロテクション > NAT > NAT タブより「新規マスカレードルール」ボタン
 を押下します。

▶検索	NAT	
ダッシュボード		
マネジメント	+ 新規NATルール	« »
定義とユーザ	検索 ★ / 0	
インタフェースとルーティング	茲示. 10 ▼	1-4 01 4
ネットワークサービス	□ <b>アク</b> ション Ⅲ▼ ソート順: 優先順位 asc ▼	
ネットワークプロテクション	□ ☑ 編集 □ ○ 1 DNAT	0
	★ 削除 トラフィックセレクタ: Q Any → ✓ SSH → N External (Address)	
NAT	宛先変換: ■ 192.168.12.4 ✓ SSH	
	自動ファイアウォールルール: 🗸	
キーパロードバランシング	初期パケットのログ: 🗙	

②「NAT ルールを追加」より、以下の通り入力します。

グループ・グループなし	NATルールを追加	×
優先順位:最下位	グループ: [:: グループなし ::	<b>•</b>
ルールタイプ:DNAT(宛先)	伝先順位: <u> </u>	<u>•</u>

③マッチング条件の欄は以下の通り入力します。

トラフィック送信元:Any					
サービス : 53389					
トラフィック宛先:	External	(Address)			

マッチング条件					
	トラフィック送信元:	📋  ฎ Any	<b>=</b> +		
	サービス:	DND DN	🗎 +		
	トラフィック宛先:	DND DN	<b>=</b> +		

この時、サービスについては新たにサービスを定義する必要があります。「+」ボタンを押下して「サービス定義の追加」を開き以下の通り入力し「保存」を押下します。

サービス利用手順書 かんたんネットワークプロテクション編

名前:53389 ※任意 定義タイプ:TCP 宛先ポート:53389 送信元ポート:1:65535

マッチング条件			サービス定義の	追加 🔀	
トラフィック送信元:	🗍 💲 Any	<b>i</b> +	名前:	53389	68
サービス:	DND	DN 🚞 🕂 🗲	定義タイノ: 宛先ポート:	53389	J
トラフィック宛先:	DND	DNI 🚞 🕇	送信元ポート:	1:65535	•0.
アクション			コメント:		
変更後の宛先:	DND	DNI 🚔 🕇		✔ 保存 🗙 キャンセル	

④アクションの欄、詳細は以下の通り入力します。

変換後の宛先: 192.168.0.2
 サービス: Microsoft Remote Desktop
 自動ファイアウォールルール:チェック
 初期パケットのログ:チェック

アクション			
変更後の宛先:	DND	DNI 🚞 🕂	
変更後のサービス:	DND	DNI 🚞 🕂	
✓ 自動ファイアウォールルール			
אלאב			
□ 詳細			
✔ 初期パケットのログ			

この時、変換後の宛先については新たにネットワークオブジェクトを追加する必要があります。 「+」ボタンを押下して「ネットワークオブジェクトを追加」を開き以下の通り入力し「保存」 を押下します。

名前:保護対象 ※任意	アクション	ネットワークオブジェクトを追加 ※	
タイプ : ホスト	変更後の現先: DND DN 🚞 🗲	名前:保護対象	
101/1 アドレフ・19216802	変更後のサービス: DND DN 🚔 🕇	IPv4 アドレス: 192.168.0.2	
IF V4 7 1 VX : 132.100.0.2	□ 自動ファイアウォールルール	Ⅲ DHCP 設定	
	34KE	B ONSIDE	
	E [其編		
	√ 保存 🗙 キヤンセル		
		✓ 保存 X キャンセル	
	on Limited. All clother operated		

 $<sup>15\</sup>$  Copyright© 2017 KOANKEISO CO., LTD. All rights reserved.

サービス利用手順書 かんたんネットワークプロテクション編

NATルールを追加	×
グループ: 📰	グループなし :: 🔹 🔻
優先順位: 最	下位 ▼
ルールタイプ: DI	NAT(宛先) ▼
マッチング条件	
トラフィック送信元: 📋	💱 Any 🚞 🕇
サービス: 📋	🖌 53389 📄 🕂
トラフィック宛先: 📋	🖾 External (Add 🚞 🕂
アクション	
変更後の宛先: 📋	📮 保護対象 📄 🛨
変更後のサービス: 📋	🖌 Microsoft Ren 🚞 🕂
☑ 自動ファイアウォールルール	٧
コメント:	
∃ 詳細	
	✔ 保存 🗙 キャンセル

⑤入力が完了したら「保存」ボタンを押下します。

⑥有効化ボタンを押下し DNAT ルールを有効にします。

<ul> <li>□ 編集</li> <li>※ 削除</li> <li>□ 複製</li> </ul>	5 DNAT トラフィックセレクタ: ♀ Any → ✔ 53389 → № External (Address) 宛先変換: ■ 保護対象 ✔ Microsoft Remote Desktop (RDP) 自動ファイアウォールルール: ✔ 初期パケットのログ: ✔	0
<ul> <li>□ 評編集</li> <li>× 削除</li> <li>□ 複製</li> </ul>	S DNAT     トラフィックセレクタ: ♀ Any → ✔ 53389 → № External (Address)     宛先変換: ■ 保護対象 ✔ Microsoft Remote Desktop (RDP)     自動ファイアウォールレール: ✔     初期パケットのログ: ✔	0

⑦設定をテストします。WAN 側クライアント PC から Sophos UTM9 の WAN 側インタフェースの公開用 IP アドレスに 53389 ポートでアクセスすることで、保護対象システム(Windows Server2012R2)にアクセスすることができます。

サービス利用手順書 かんたんネットワークプロテクション編

## 3-3. 侵入検知 (IPS)

ここでは、外部ネットワークから内部ネットワークに対する不正アクセスに対する防御機能である、「侵入防御(IPS)」について説明します。

## (1) グローバル設定手順

①ネットワークプロテクション > 侵入検知(IPS) > グローバルタブより「IPS ステータス」
 ボタンを押下します。

SOPHOS	UTM 9	上 admin   🗊   🕜 C 🔅
▶検索	侵入防御(IPS)	
ダッシュボード	<b>8 グローバル</b> 攻撃パターン DoS/フラッド防御	◎ ポートスキ 除外 詳細
マネジメント	IPSステータス	
定義とユーザ		
インタフェースとルーティング	- クロー/UIPS設定	
ネットワークサービス		IPSをスタートするには、ローカルネットワークと攻撃が検知さ
ネットワークプロテクション	External (Address)	れた際に適用するポリシーを指定してください。
ファイアウォール	Internal (Network)	
NAI 侵入防御(IPS)		
<u> </u>		
VoIP =***m		
計構 Wobプロークション		
	ポリシー: 破棄 ▼	
ヒスールノロナクション	再起動ポリシー: すべてのパケットをドロッ▼	
局度な防御	-	
エンドポイントプロテクション		✓ 適用
ワイヤレスプロテクション		

②IPS の検知を有効にするネットワーク及び、インターフェイスを指定します。

今回は、外部からの不正アクセス及び内部ネットワークの不正アクセスに対する防御を有効にす るため、以下のポリシーを適用します。

External (Address)

Internal (Network)

フォルダアイコンをクリックし該当のオブジェクトをドラックアンドドロップします。

サービス利用手順書 かんたんネットワークプロテクション編

Networks (CTRL+Z)	★ 侵入防御(IPS)
All  External (Address) External (Broadcast)	<ul> <li>● グローバル 攻撃パターン DoS/フラッド防御 ● ポートスキ 除外 詳細</li> <li>IPSステータス</li> </ul>
External (Network)	グローバルPS設定
🔝 Internal (Address)	
🖾 Internal (Broadcast)	ローカルネットワーク IPSをスタートするには、ローカルネットワークと攻撃が検知さ
internar (Network)	れた際に適用するボリシーを指定してください。
🗊 Internet IPv4	🔲 🔝 Internal (Network)
🚅 Internet IPv6	
kanshi_test (Address)	DND DND DND
🔛 kanshi_test (Broadcast)	DND DND DND
kanshi_test (Network)	DND DND DND
E KOAN	
so license.owlook.ne.jp	
so NTP Server Pool	再起動ボリシー: _ すべてのパケットをドロ、▼
NWC-SUM02	✓ 適用
nyosuke-isobe (User Netwo	

③ポリシー及び再起動ポリシーはデフォルトのまま、「適用」ボタンを押下し設定を保存します。



以上で、グローバル設定手順は完了です。

サービス利用手順書 かんたんネットワークプロテクション編

# (2) 攻撃パターン設定手順

①ネットワークプロテクション > [侵入防御(IPS) > 攻撃パターンタブを開きます。 攻撃の種類は大きく分けて以下の 6 種類があり、それらに対する詳細な攻撃パターンに対して 個別に設定できます。

- ・ OS 固有の攻撃
- ・ サーバに対する攻撃
- ・ クライアントソフトウェアに対する攻撃
- ・ プロトコルアノマリー
- ・マルウェア

▶検索	侵入防御(IPS)
ダッシュボード	● クローバル ┃ <b>牧肇パターン</b>
マネジメント	下記のテーブルは、利 <mark>序、</mark> 能なIPSルールグループを表示しています。パフォーマンスを向上させる際には、使用していないサービスやソフ
定義とユーザ	トウェアに関するグレープは除外してください。有効にしたグループでは次の4つのオプションが設定可能です:
インタフェースとルーティング	<ul> <li>アクション・デフォルトにより、グループ内の各ルールには実用的なデフォルトアクションがあります。 警告 または 破棄のどちらかを</li> </ul>
ネットワークサービス	・ クリーブに設定することにより、これらのテフォルトを無効にすることかできます。 ・ リリースされてからの保持期間:デフォルトでは、IPSパターンファイルは直近12ヶ月を使用することを推奨しています。これは、全体
ネットワークプロテクション	のパッチレベル、レガシーシステムの利用、その他セキュリティ要件等の要因により変更することができます。
ファイアウォール	<ul> <li>追加の警告ルールを有効化:このオブションを有効にすると、警告目的のみに使用される追加ルールも含まれます。これらのルールは 警告のフォルフボシティブ(評論物)を引き起こす可能性があっため、デフォルトでは含まれていません。</li> </ul>
NAT	■日のフォルスパンフィン (Bellixiu) を引きたとう 引起生いのなんし、フラオルド (Cladeshi Chile Chile) • 通知:このオブションを有効にすると、グループ内の各ルールに該当した全てのインシデントに対して通知が送られます。
侵入防御(IPS)	変更が完了したら、グループの下にある適用ボタンをクリックしてください。
VolP	
詳細	フェータフルガループタ フカション, リリースされてオプション,
Webプロテクション	へ マクション からの保持期間 <sup>212 ノヨン</sup>
Eメールプロテクション	✓ OS固有の攻撃 (309 攻撃イベント、265 警告) 改善▼ 12ヶ月以下▼ 追加の警告ルール ✔ 通知
高度な防御	L ✔ Windows (266 攻撃イベント, 191 警告) · · · · · <sub>改善</sub> ▼ □ 追加の警告ルール ✔ 通知
エンドポイントプロテクション	└────────────────────────────────────
ワイヤレスプロテクション	└ 🖉 その他 (33 攻撃イベント, 42 警告) ・・・・・ <sub>改善</sub> ▼ 📄 追加の警告ルール 🖉 通知
Webサーバプロテクション	ぜ サーバに対する攻撃(1230 攻撃イベント、3201 警告)     日本     12ヶ月以下▼     追加の警告ルール     通知     通知     追加の     「     」     追加の     「     」     」     追加の     「     」     」     」     」     」     」     」     」     」     」     」     」     」     」     」     」     」     」     □
REDマネジメント	L @ HTTPサーバ (344 攻撃イベント, 1154 警告)
サイト間VPN	. └ 2 一般的 (6 攻撃イベント, 51 警告) ・ ・ ・ ・
リエートアクセス	· · · · · · · · · · · · · · · · · · ·
	L @ PHP (183 攻撃イベント, 483 警告) · · · · · · · · · · · · · · · · · · ·
<u> サ</u> ホート	L @ CGI (109 攻撃イベント, 275 警告) · · · · · <sub>改勇</sub> ▼ □ 追加の警告ルール @ 通知
ログオフ	└ 🖉 メールサーバ (14 攻撃イベント, 261 警告) 🛛 🙀 ▼ 📄 追加の警告ルール 🖉 通知

②アクションの設定が完了したら、「適用」ボタンを押下します。

サービス利用手順書 かんたんネットワークプロテクション編

<ul> <li>クライアントソフトウェアに対する攻撃()</li> </ul>	破棄 ▼	12ヶ日以下 ▼	□ 追加の警告ルール	☑ 通知
└ ♥ Office (MS Office) () · · · · · · ·	 · 破棄 ▼		□ 追加の警告ルール	☑ 通知
└ 🖉 ブラウザ(Internet Explorer、Mozilla) () · ·	 · 破棄 ▼	]	□ 追加の警告ルール	☑ 通知
L 🖉 メール、SMTP、POP3、IMAP (Outlook) ()・	· <sub>破棄</sub> ▼	]	🗌 追加の警告ルール	☑ 通知
L 🖉 マルチメディア (WMP、iTunes、RealPlayer) ()	· <sub>破棄</sub> ▼	]	🗌 追加の警告ルール	☑ 通知
L 🖉 メッセンジャー(AOL, MSN) () ・ ・ ・	· <sub>破棄</sub> ▼	]	🗌 追加の警告ルール	✓ 通知
	te <del>n</del> T		□ 追加の警告ルール	☑ 通知
	 10(共 )		<ul> <li>追加の宣告ルール</li> <li>追加の警告ルール</li> </ul>	☑ 通知
	HXH	]		
マルウェア (2146 攻撃イベント, 9421 警告)	破棄 ▼	12ヶ月以7 ▼	🗌 追加の警告ルール	☑ 通知
				海田
				v ™

以上で、攻撃パターン設定手順は完了です。デフォルトでは全ての攻撃を検知する設定になって います。細かいチューニングについては管理者ガイドを参考に環境に合わせチューニングしてみ てください。

サービス利用手順書 かんたんネットワークプロテクション編

### (3) DoS フラッド防御設定手順

②アクションの設定が完了したら、「適用」ボタンを押下します。

ネットワークプロテクション > 侵入防御(IPS) >DoS フラッド防御タブを開きます。

DoS フラッド防御の種類は以下の3種類があり、それぞれ個別の設定を行うことができます。

- ・ TCP SYN フラッド防御
- ・UDP フラッド防御
- ・ICMP フラッド防御

設定が終了したら、項目ごとに「適用」ボタンを押下し設定内容を反映させてください。

₽検索	侵入防御(IPS)		
ダッシュボード		■ ◎ ポートスキ 除外 詳細	
マネジメント			
定義とユーザ			
インタフェースとルーティング	- ■ TCPStNフラッド防御 を使用	TCP SYNフラッド防御はTCP SYNパケットフラッドを検知しブ	
ネットワークサービス		ロックします。	
ネットワークプロテクション			
ファイアウォール			
侵入防御(IPS)	送信元パケットレート (パケット/秒): 100		
サーバロードバランシング	宛先パケットレート (パケット/秒):200		
VoIP 詳細		ノ海田	
Webプロテクション			
Eメールプロテクション	- UDPフラッド防御		
高度な防御			
エンドポイントプロテクション	_ UDPフラット防御 を使用	UDPフラット防御はUDPバグットによるフラット攻撃を使知およ びブロックします。	
ワイヤレスプロテクション	モード: 送信元及び宛先アドレス 🔹		
Webサーバプロテクション	ログ: 制限 🔹		
REDマネジメント	送信元パケットレート (パケット/秒): 200		
サイト間VPN	宛先パケットレート (パケット/秒): 300		
リモートアクセス			
ログとレポート			
サポート	ICMPフラッド防御		
ログオフ			
	☑ ICMPフラッド防御 を使用	ICMPフラッド防御はICMPパケットによるフラッド攻撃を検知お とびゴロックレます	
	モード: 送信元及び宛先アドレス	よいノロックします。	
	ログ: 制限 🔹		
	洋信寺 パケットレート (パケットが)・10		
	9世元ハウットレート ハイグット/791:20		
		✓ 適用	

以上で、DoS フラッド防御設定手順は完了です。デフォルトではこの機能は無効になっていま す。細かいチューニングについては管理者ガイドを参考に環境に合わせチューニングしてみてく ださい。

サービス利用手順書 かんたんネットワークプロテクション編

# (4) ポートスキャン防御設定手順

①ネットワークプロテクション > 侵入防御(IPS) > ポートスキャン防御)タブを開きます。 デフォルトでは、機能はオフの状態ですのでをクリックして機能をオンにします。 アクションのプルダウンリストから、ポートスキャンに対するアクションを選択し 「適用」を 押下します。

₽検索	侵入防御(IPS)
ダッシュボード	
マネジメント	ポートスキャン検知
定義とユーザ	
インタフェースとルーティング	クロー/01設定
ネットワークサービス	アクション・「トラフィックを破棄 マ アンチポートスキャンを検出し、必要に応じてポートスキャンを
ネットワークプロテクション	プロックすることができます。 アクションは、検出されたボート
ファイアウォール	<ul> <li>ビ ロン (2 m) RR</li> <li>ノギヤンのトラノイックをどのように処理するかを定義します。</li> <li>これは、ドロップされるか、または拒否することができます。</li> </ul>
NAI <mark>侵入防御(IPS)</mark> サーハロートバランシング	グのみに設定されている場合、トラフィックは引き続き許可され ますが、ポートスキャンインシデントが記録されます。
VoIP 詳細	✓ 適用
Webプロテクション	
Eメールプロテクション	
高度な防御	
エンドポイントプロテクション	
ワイヤレスプロテクション	
Webサーバプロテクション	
REDマネジメント	
サイト間VPN	
リモートアクセス	
ログとレポート	
サポート	
ログオフ	

以上で、ポートスキャン設定手順は完了です。デフォルトではこの機能は無効になっています。 細かいチューニングについては管理者ガイドを参考に環境に合わせチューニングしてみてくだ さい。

サービス利用手順書 かんたんネットワークプロテクション編

## 3-4. 高度な防御 (Advanced Threat Protection)

高度な防御(Advanced Threat Protection)機能を有効にすることでより、高度な検知が可能となります。侵入検知と合わせて有効にすることを推奨します。

## (1) 高度な防御(Advanced Threat Protection) 設定手順

①高度な防御 > 高度な脅威防御(ATP) > グローバルタブを開きます。デフォルトでは、機能はオフの状態ですのでをクリックして機能をオンにし「適用」を押下します。

▶検索	高度な脅威防御(ATP)	
ダッシュボード	⊘ グローバル	
マネジメント	ATP Z	
定義とユーザ		
インタフェースとルーティング	- 馬度な脅威防御(ATP)設定	
ネットワークサービス	ポリシー: )渡艇 ▼	高度な脅威防御が、UTMを通過するすべてのトラフィックに対し
ネットワークプロテクション		て有効になっています。脅威スキャンの対象から特定のソースホ
Webプロテクション	除外するネットワーク/ホスト: 💼 +	ストまたはネットワークをスキップしたい場合は、ネットワーク/ ホスト例外でそれらを定義することができます
Eメールプロテクション	DND DND DND DND	宛先を脅威に対するスキャンからスキップする、または、検出さ
高度な防御	DND DND DND	れた脅威を回避するには、脅威の例外中のドメインまたはIPアド
Sophosサンドフトーム		レスに入力することがにきます。それは、コマンド&コンドロー ルサーバに感染したコンピュータを公開し、ハッカーが、潜在的
高度な脅威防御(ATP)		にコンピュータを制御し、ネットワークにアクセスするため <mark></mark> に使
エンドポイントプロテクション	除外する習販: + □	用できるようになるので、検出された脅威をスキップすることは
ワイヤレスプロテクション		
Webサーバプロテクション		高度な脅威防御を最大化: この機能は、得入防止とWebプロテクションを相互作用させるこ
REDマネジメント		とができます。保護を最大化するために、それらを有効にしてく
サイト間VPN		ださい。
リモートアクセス		IPSは、現在、 <b>IPS_STATUS_ENABLED_DISABLED</b> で <mark></mark> す
ログとレポート		Web保護は、現在、 WEBPROTECTION STATUS ENABLED DISABLED STAT
サポート		
ログオフ		✓ 適用
	ライブログ	
	🍺 ライブログを開く	<b>高度な脅威防御</b> ライブログを閉くにはここをクリックしてください。

以上で、高度な防御(Advanced Threat Protection)設定手順は完了です。