

さくらのクラウド「Sophos UTM」

Owlook

セキュリティマネジメントサービス仕様書

第 1.2 版

2019 年 2 月 12 日



興安計装株式会社

目次

内容

改訂履歴.....	3
はじめに.....	4
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. ライセンスについて.....	9
(1) ライセンスのカウント方法.....	9
(2) ライセンス違反となるケース.....	12
3. 提供機能の詳細について.....	13
3-1. ユーザポータル.....	13
3-2. ネットワークサービス.....	14
(1) DNS.....	14
(2) DHCP.....	14
(3) NTP.....	15
3-3. ネットワークプロテクション.....	15
(1) ファイアウォール.....	15
(2) NAT.....	15
(3) 侵入検知 (IPS).....	16
3-4. Web プロテクション.....	16
(1) Web フィルタリング.....	17
(2) HTTPS.....	18

(3) Web フィルタリングポリシー	18
(4) アプリケーション コントロール.....	19
3 – 5. E メールプロテクション	20
(1) SMTP プロキシ.....	20
(2) SMTP スпам対策.....	20
(3) SMTP その他.....	21
(4) POP3 プロキシ	21
(5) POP3 スпам対策.....	22
(6) POP3 その他.....	22
(7) 隔離レポート.....	23
(8) メールマネージャ	23
3 – 6. 高度な防御.....	24
Advanced Threat Protection	24
3 – 7. Web サーバプロテクション	24
(1) WAF	24
(2) 仮想 Web サーバ.....	24
(3) その他.....	26
3 – 8. サイト間 VPN	27
詳細.....	28
3 – 9. リモートアクセス.....	29
詳細.....	29
3 – 10. ログとレポート.....	30
(1) ログファイルの閲覧.....	30
(2) エグゼクティブレポート.....	33
(3) ログ設定	34

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
1.1	2018/11/1	2. ライセンスについて (1) ライセンスのカウント方法 上項のライセンス取り扱いにおける初期バンドル数を 5IP から 1IP に変更。	興安計装株式会社
1.2	2019/2/12	ファームウェアバージョン 9.6 における機能を追加 3 – 5. Eメールプロテクション (3) SMTP その他 透過モードの対応ポート追加 3 – 7. Web サーバプロテクション (3) その他 ブロックページのカスタマイズ機能追加 Let's Encrypt™証明書の機能追加	興安計装株式会社

はじめに

本仕様書は、興安計装株式会社（以下「当社」とする）が提供する「Owlook セキュリティマネジメントサービス」（以下「本サービス」とする）の提供を受ける者（以下「利用者」とする）に対する、本サービスの機能、サービス内容、その他の諸条件について記載するものです。

また、本仕様書は「Owlook セキュリティマネジメントサービス利用規約」の一部を構成するものとします。

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。

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
ネットワークサービス	<ul style="list-style-type: none"> ・ DNS ・ DHCP ・ NTP 上記に付随する各種オプション
ユーザポータル	リ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ンと付随する各種オプション

ネットワークプロテクション	<ul style="list-style-type: none"> ・ファイアウォール ・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 プロテクション	<ul style="list-style-type: none"> ・Web フィルタリング ・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
Eメールプロテクション	<ul style="list-style-type: none"> ・SMTP プロキシ ・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 サーバプロテクション	<ul style="list-style-type: none"> ・Web Application Firewall (WAF) 上記に付随する各種オプション
サイト間 VPN	<ul style="list-style-type: none"> ・IPsec ・SSL ・Amazon VPC
リモートアクセス	<ul style="list-style-type: none"> ・SSL ・PPTP ・L2TP over IPsec ・IPsec ・HTML5 VPN ポータル ・Cisco™ VPN クライアント
ログとレポート	<ul style="list-style-type: none"> ・各サービスのログ取得 ・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 3. 提供機能の詳細をご参照ください。

(3) サービス利用条件

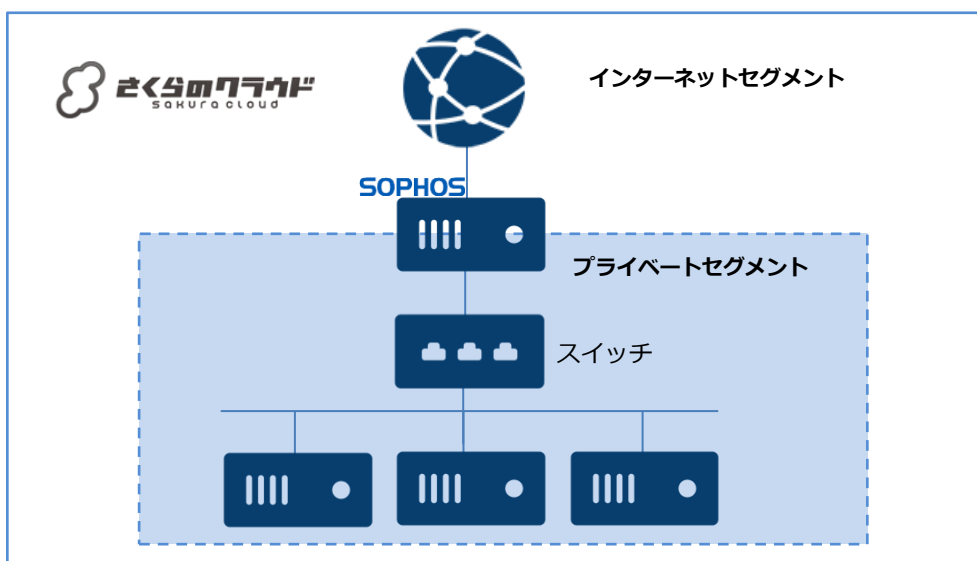
本サービスの利用条件は以下の通りです。

①ご利用環境

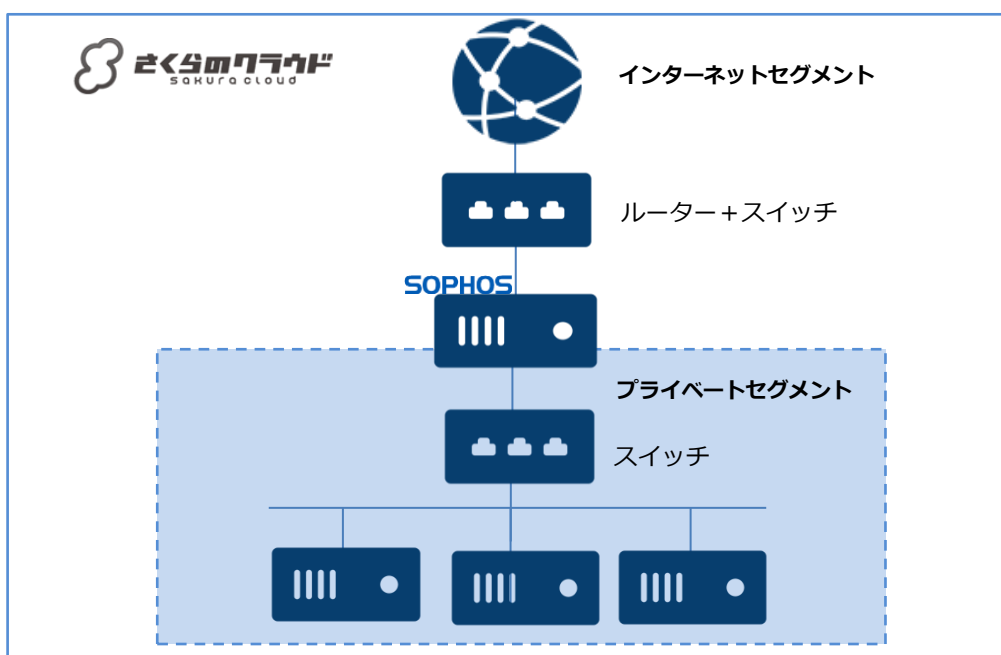
さくらのクラウドサービス内の全てのリージョンよりご利用可能です。

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ことが可能です。



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 packetsize、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
①さくらのクラウドサービスのアカウント取得	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。
②SophosUTM9 の展開	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 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利用規約へ同意	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。

④ライセンスサーバーへの接続	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ます。
⑤利用ライセンスの有効化	SophosUTM9 がライセンスサーバへ接続後、利用ライセンスが有効になります。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。
⑥利用開始	SophosUTM9 の機能がご利用いただけるようになり、利用者にて設定が可能となります。
⑦利用終了	SophosUTM9 を一定期間停止、または削除した場合、ライセンスは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ます。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. ライセンスについて

本サービスで提供される Sophos UTM9 利用ライセンスはパブリックアーカイブで提供されるイメージに **1ライセンスがバンドル**されています。ライセンスは保護対象となるシステムがもつ IP アドレスに対して発生する為、初期状態で 1つの IP アドレスを保護することができます。1つ以上の IP アドレスが Sophos UTM9 の配下に属する場合、追加でライセンスの購入が必要となります。

(1) ライセンスのカウント方法

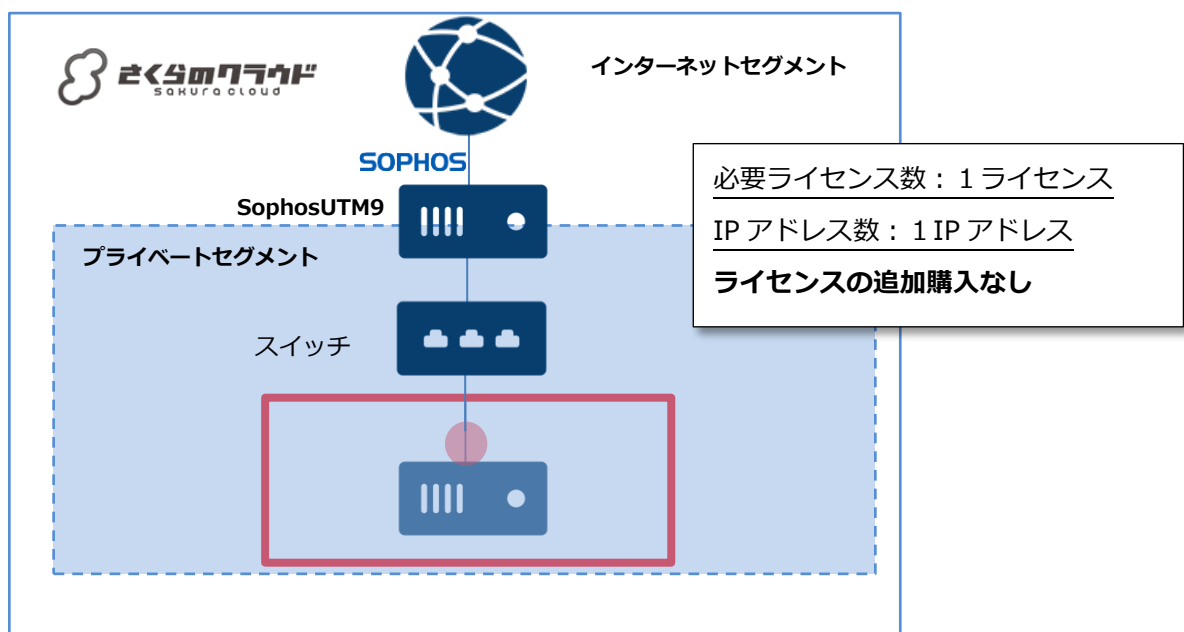
SophosUTM9 のライセンスは **保護対象の IP アドレス** に対して発生します。保護対象は外部との通信において **SophosUTM9 を通過するサーバー** です。よって保護対象のデフォルトゲートウェイアドレスは、SophosUTM9 のプライベートセグメント側の IP アドレスを向いていることとなります。その保護対象が持つ、**SophosUTM9 のプライベートセグメントに属する IP アドレス** に対してライセンスが発生します。

凡例

-  : 保護対象となるサーバー
-  : 保護対象の IP アドレス
-  : 保護対象とならない IP アドレス

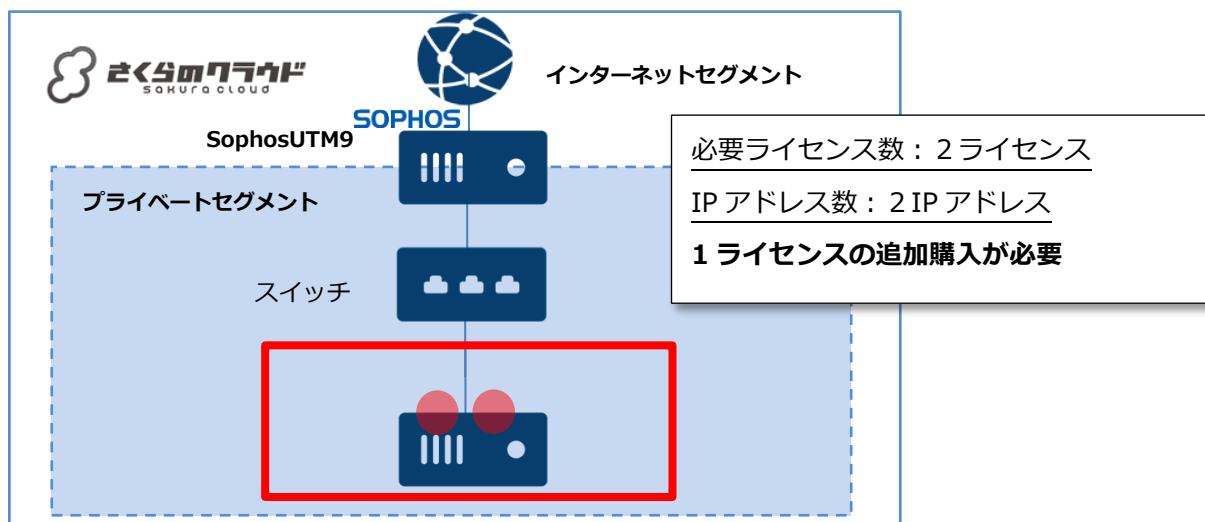
①基本構成

パブリックアーカイブで提供されるイメージに 1ライセンス分が含まれます。その為、以下の構成の場合、ライセンスの追加購入は必要ありません。



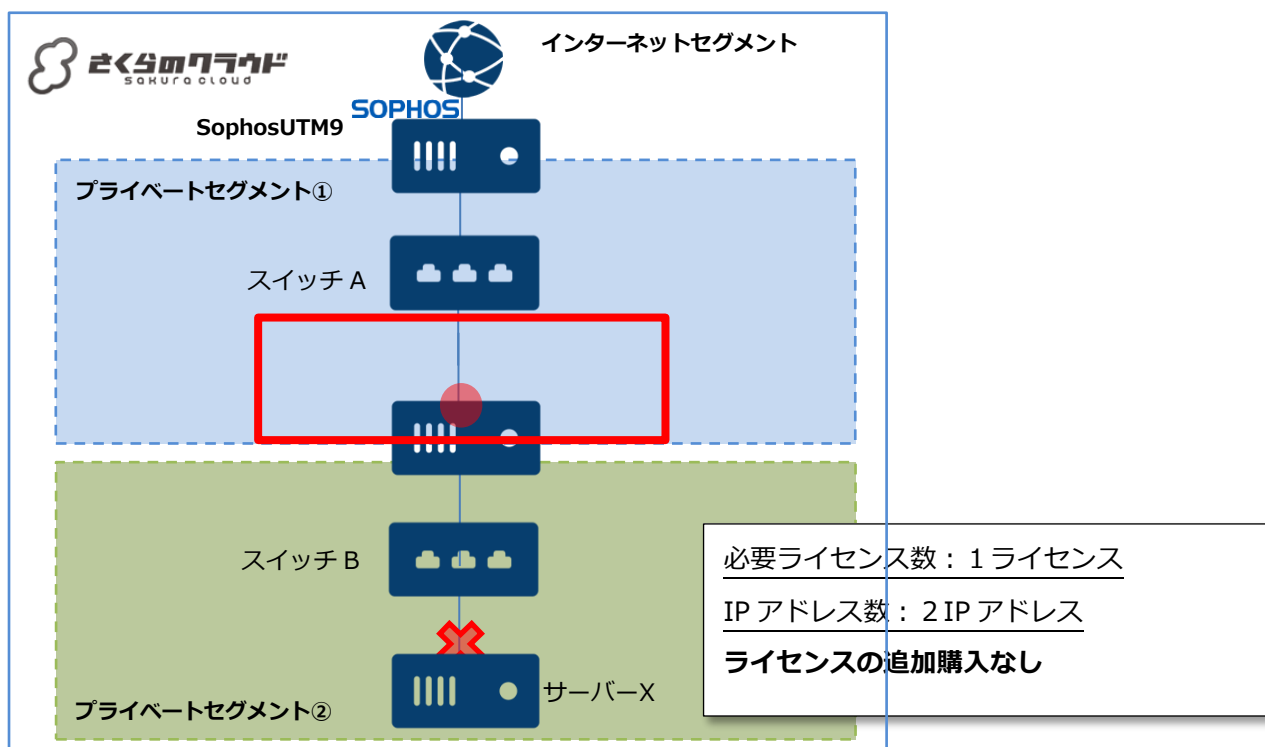
②保護対象が複数の IP アドレスを持つケース

以下のようにサーバーが 1 台であっても保護対象が全て SophosUTM9 を通過する場合、追加ライセンスとカウントされます。



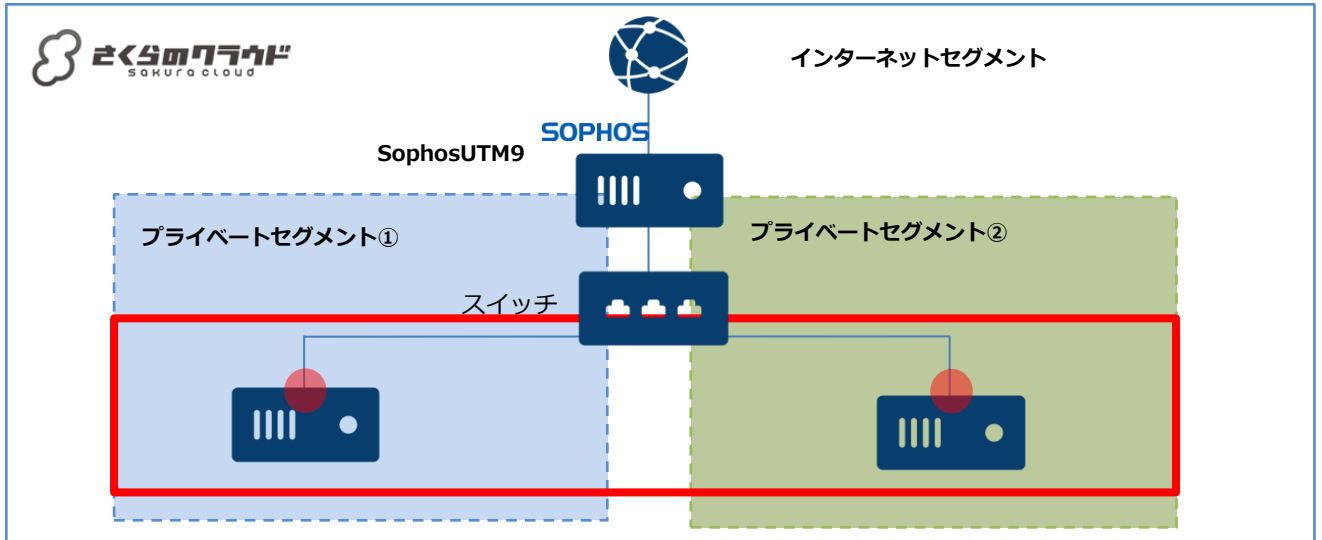
③直列多層構成の場合

以下の構成は多層構成のケースです。多層構成となった場合、「サーバー-X」が「プライベートセグメント②」内だけでの通信であれば（SophosUTM9 を通過することは無い）ライセンス数は 1 ライセンスとなります



④ 並列多層構成の場合

以下の構成は多層構成のケースですが、SophosUTM9 が「プライベートセグメント①」「プライベートセグメント②」の2つに対し、ゲートウェイを提供する並列構成となる為、ライセンス数は7ライセンスとなります。



必要ライセンス数：2ライセンス

IP アドレス数：2 IP アドレス

1ライセンス追加購入が必要

(2) ライセンス違反となるケース

本サービスは以下のようなケースにおいてライセンス違反となります。ライセンス違反が検出された場合、当社からのライセンス提供を停止させていただきます。ライセンス違反に伴う利用者への影響について当社では一切の保証をいたしませんのでご注意ください。

違反ケース	違反内容
①利用ライセンス適用後に SophosUTM9 の複製を行い、複数起動させる。	ライセンスの不正複製となります。SophosUTM9 を複数利用される場合、都度パブリックアーカイブより作成を行い、ライセンス手続きを行ってください。
②利用ライセンス適用後にさくらのクラウドサービス以外の環境に SophosUTM9 の複製を持ち出し、起動させる。	ライセンスの不正複製となります。本サービスはさくらのクラウドサービス内のみでご利用ください。
③さくらのクラウドサービス以外の環境からライセンスサーバに接続する。	ライセンスの不正利用となります。本サービスはさくらのクラウドサービス内のみでの提供となる為、外部環境からのライセンスサーバへの接続行為は禁止しております。
④追加ライセンスを購入せずに保護対象を追加する。	ライセンスの不正利用となります。保護対象に変更があった場合、速やかに手続きをお願いします。
⑤利用者が本サービス以外で入手した SophosUTM9 のライセンスを、本サービスから提供されるアーカイブイメージに適用する。	本サービスはさくらのクラウドサービス向けにカスタマイズされているため、正しく動作しない場合であっても一切の保証はいたしません。

3. 提供機能の詳細について

本サービスが提供するセキュリティ機能の詳細は以下の通りとなります。

3-1. ユーザポータル

ユーザポータルは、許可されたユーザにパーソナルなメールおよびリモートアクセスサービスを提供するユニットの特別なブラウザベースアプリケーションです。Sophos UTM9 で提供されるユーザポータル機能は以下の通りです。

機能項目	機能内容
SMTP 隔離	ユーザは隔離場所に保持されているメッセージを表示したり、リリースが可能です。
SMTP ログ	ユーザはメールトラフィックの SMTP ログを表示可能です。
POP3 隔離	ユーザは隔離場所に保持されているメッセージを表示したり、リリースが可能です。
POP3 アカウント	ユーザは使用する POP3 アカウントの資格情報を入力が可能です。
送信者ホワイトリスト	ユーザは送信者をホワイトリストに追加することで、それらの送信者から送信されたメッセージがスパムとして分類されないように設定することが可能です。
送信者ブラックリスト	ユーザはメール送信者をブラックリスト化することが可能です。ブラックリストは、システム内で SMTP と POP3 が使用されていれば、SMTP と POP3 の両方のメールに適用されます。
クライアント認証	ユーザはここから Sophos Authentication Agent (SAA) のセットアップファイルをダウンロードできます。
リモートアクセス	ユーザはリモートアクセスクライアントソフトウェアおよびそれらに付属する設定ファイルをダウンロードが可能です。
HTML5 VPN ポータル	ユーザは、定義済みのサービスを使用して定義済みのホストへの VPN 接続を確立することが可能です。
パスワードの変更	ユーザはユーザポータルにアクセスするためのパスワード変更が可能です。
HTTPS プロキシ	ユーザは HTTP/S プロキシ CA 証明書をインポートし、セキュア Web サイトへの訪問時に表示されるエラーメッセージを回避することが可能です。

3-2. ネットワークサービス

Sophos UTM9 で提供されるネットワーク機能は以下の通りです。

(1) DNS

DNS は、ドメイン名（コンピュータのホスト名）を IP アドレスに変換するために主に使用されます。

機能項目	機能内容
DNS リゾルバ	DNS リゾルバ機能として動作します。
DNSSEC	受信 DNS 要求の DNSSEC 署名を確認し、署名ゾーンからの、正しく署名されたレコードだけを受け入れます。
フォワーダ	外部 DNS 名に関する DNS クエリを当該ネットワーク外の DNS サーバに転送します。
リクエストルーティング	DNS フォワーダに解決させたくないドメインがある場合、そのドメインへのクエリをフォワーダではなく内部サーバに処理させることができます。
スタティックエントリ	独自の DNS サーバをセットアップせず、ネットワーク内のいくつかのホストに対してスタティック DNS マッピングが必要な場合は、これらのマッピングを入力することができます。
DynDNS	ダイナミック DNS（略して DynDNS）は、可変 IP アドレスを持つコンピュータにスタティックインターネットドメイン名を割り当てることができます。

(2) DHCP

DHCP は、定義された IP アドレスプールからクライアントコンピュータにアドレスを自動的に割り当てます。

機能項目	機能内容
DHCP リレー	DHCP リレーを使用すると、ネットワークセグメントをまたいで DHCP 要求および応答を転送することが可能です。
スタティックマッピング	一部または全部のクライアントの IP アドレスとクライアント間のスタティックマッピング作成が可能です。

(3) NTP

NTP は、IP ネットワーク経由でコンピュータシステムのクロックを同期するために使用するプロトコルです。Sophos UTM9 の時刻の同期先を設定することができます。

3-3. ネットワークプロテクション

Sophos UTM9 で提供されるネットワークプロテクション機能は以下の通りです。

(1) ファイアウォール

ゲートウェイのファイアウォールルールを定義し管理することができます。以下の機能を提供します。

機能項目	機能内容
ルール定義	デフォルトのセキュリティポリシーでは、すべてのネットワークトラフィックをブロックしてログに記録されます。ファイアウォールルールの処理順序は位置番号によって処理されます。1つのファイアウォールルールが一致すると、他のすべてのルールは無視されます。
送受信国別ブロック	特定国から、または特定国へのトラフィックをブロックすることが可能です。ホストの IP アドレスの GeoIP 情報に基づきます。
国ブロックの例外	ブロックされる国の例外を定義可能です。
ICMP	ICMP を使用して、ホスト間で接続関連のステータス情報のやり取りについての設定が可能です。

(2) NAT

NAT ルールを定義し、管理することができます。以下の機能が設定可能です。

機能項目	機能内容
マスカレード	1つのグローバル IP アドレスの背後にある内部ネットワークをマスカレード機能の提供が可能です。
DNAT	データパケットの宛先アドレスが書き換えが可能です。 ※PPTP VPN アクセスは DNAT に対応していません。

SNAT	接続を開始したコンピュータの IP アドレスが可能です。 ※PPTP VPN アクセスは DNAT に対応していません。
------	---

(3) 侵入検知 (IPS)

侵入防御システム (IPS) は、シグニチャに基づく IPS ルールセットを利用し、トラフィックを完全に分析し、ネットワークに到達する前に攻撃を自動的にブロックします。既存のルールセットと攻撃パターンは、パターン更新によって最新状態に更新されます。IPS 攻撃パターンのシグニチャは、IPS ルールとしてルールセットに自動的にインポートされます。以下の機能を提供します。

機能項目	機能内容
攻撃パターン管理	オペレーティングシステム固有の攻撃、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、プロトコル異常、マルウェアが攻撃グループとしてカテゴリ化され、各カテゴリに対し破棄または警告の動作指定が可能です。
ルールの有効期間設定	デフォルトでは、IPS ルールの有効期間は 12 か月です。他の期間の選択が可能です。
追加の警告ルールを有効化	各攻撃パターンに警告レベルのルールを追加します。
通知	検知した IPS イベントを E メールまたは SNMP トラップで管理者に通知が可能です。 ※通知設定の変更が有効になるまでは最大 5 分かかる場合があります。
除外	侵入防御のスキャンから除外する送信元、送信先のネットワーク、ホスト及びサービスの定義が可能です。
DoS/フラッド防御	DoS (サービス拒否) 攻撃と DDoS (分散型サービス拒否) 攻撃からの防御が可能です。特定時間内にネットワークに対して送信される SYN (TCP)、UDP、ICMP パケットの数を制限します。
ポートスキャン防御	ネットワーク上のホストまたはサービスのスキャンを検出し防御します。

3-4. Web プロテクション

Sophos UTM9 で提供される Web プロテクション機能は以下の通りです。

(1) Web フィルタリング

送受信 Web トラフィックをスキャンし、スパイウェアから保護し、悪意のある Web サイトを検出し防御します。認証機能の利用も可能です。以下のオペレーションモードを提供します。

提供モード	内容
標準モード	標準モードでは、Web フィルタはデフォルトでクライアント要求をポート 8080 で待ち受けます。
透過モード	透過モードでは、ポート 80(SSL を使用している場合はポート 443) でクライアントブラウザアプリケーションが行うすべての接続はインターセプトします。

提供可能な認証モードは以下の通りです。

認証モード	内容
なし	認証をしない場合に使用します。
エージェント	Sophos Authentication Agent (SAA) を使用する場合に選択します。
Apple OpenDirectory SSO	Apple OpenDirectory を使用する場合に選択します。 ※キャッシュできるのはグループ情報のみです。
基本ユーザ認証	各クライアントはプロキシを使用する前にこのプロキシに対して自己認証する場合に選択します。
ブラウザ	Web フィルタへの自己認証のためのログインダイアログがユーザのブラウザに表示されます
eDirectory SSO	eDirectory を使用する場合に選択します。 ※Web フィルタはアクセス先の IP アドレスと資格情報を最大 15 分間キャッシュします。

※アクセスしているユーザのログインステータスの変更が Web フィルタによって反映されるまで、最大 15 分かかります。

(2) HTTPS

HTTPS トラフィックの検出方法は以下の通りです。

検出モード	内容
復号化してスキャン	HTTPS は復号化されスキャンされます。 またタグ、分類による指定スキャンも可能です。
透過モードで HTTPS トラフィックをプロキシしない	すべての HTTPS トラフィックに対する Web フィルタリングが無効にします。
URL フィルタリングのみ	URL フィルタリングのみスキャンします。

(3) Web フィルタリングポリシー

Web フィルタリングポリシーの割り当てを作成、管理します。提供される機能は以下の通りです。

機能項目	機能内容
カテゴリ	Web サイトは予め以下のカテゴリに分類されてます。 IT、Suspicious(疑わしい)、インフォメーションとコミュニケーション、エンターテイメント/カルチャー、オンライン売買、ゲーム/ギャンブル、コミュニティ/教育/宗教、ドラッグ、ヌード、ファイナンス/投資、ライフスタイル、交通・移動(機関)、個人ホームページ、極端論、過激論的サイト、武器・兵器、求人情報、薬 違法行為 カテゴリ毎に個別に許可かブロックの動作を設定可能です。未分類の Web サイト、評判に基づく Web サイトに対しても設定可能です。
Web サイト	特定の URL や Web サイト、または特定のドメインにある複数の Web ページを、そのカテゴリに関わらず、個別に許可かブロックの動作を設定可能です。(ブラックリスト、ホワイトリスト)
ダウンロード	どのファイルタイプおよび MIME タイプをブロックまたは警告するか設定可能です。またダウンロードのサイズ制限も可能です。
ウイルス対策	ウイルス対策用の Web フィルタ設定およびアクティブコンテンツの削除が設定可能です。またウイルス対策エンジンはシングルスキャン、デュアル

	スキャンから選択可能です。不要と思われるアプリケーションのブロック機能、スキャンサイズの制限機能が設定可能です。
アクティブコンテンツ除去	Web ページに埋め込まれたオブジェクトなど特定の Web コンテンツの自動削除設定が可能です。
セーフサーチ	検索プロバイダより提供されるセーフサーチ機能を強制することが可能です。
親プロキシ	親プロキシを設定することが可能です。
画像検索結果にライセンスを強制する	検索エンジンが、共有、変更および再利用が可能であるとラベル付けされた画像の結果のみ、表示することが可能です。 ※親プロキシを有効化した場合は、SSL スキャニングを有効にした状態での透過モードでの HTTPS 要求は行えません。
Google Apps の許可ドメインを強制する	Google Apps の許可ドメインを強制することが可能です。
アクティビティ記録	アクセスしたページのログ、ブロックしたページのログについて記録するかを選択が可能です。

(4) アプリケーション コントロール

Sophos UTM9 で提供されるアプリケーションコントロールはネットワークトラフィックの分類にレイヤ7パケット検査を使用し、トラフィックの種類に基づいてネットワークトラフィックをシェーピングおよびブロックします。提供されるは機能以下の通りです。

機能項目	機能内容
ネットワーク可視化	すべてのネットワークトラフィックが、その分類に応じて分類またはロギングされフローモニタに、タイプに関する詳細な情報表示が可能です。
アプリケーションコントロールルール	アプリケーショントラフィックに対してブロックするか、または明示的に許可するか定義が可能です。デフォルトでは、アプリケーションコントロールを有効にするとすべてのネットワークトラフィックが許可されます。

3-5. Eメールプロテクション

Sophos UTM9 で提供される Eメールプロテクション機能は以下の通りです。

(1) SMTP プロキシ

Sophos UTM9 は SMTP プロキシを提供します。すべてのドメインが同じ設定を共有するシングルモードでの使用を推奨します。マルウェア対策についての機能は以下の通りです。

機能項目	機能内容
マルウェアスキャン	ウイルス、トロイの木馬、疑わしいファイルタイプなどスキャンが可能です。スキャンされたメールは破棄、隔離のアクション選択が可能です。隔離されたメッセージは、メールの隔離場所に保存されます。ウイルス対策エンジンはシングルスキャン、デュアルスキャンから選択可能です。
MIME タイプフィルタ	オーディオコンテンツ、ビデオコンテンツ、実行形式コンテンツ等の MIME タイプのフィルタリングが可能です。
ファイル拡張子フィルタ	ファイル拡張子に基づいて特定タイプのファイルを含むメールのフィルタリングが可能です。
マルウェア チェックフッタ	各送信・受信メールでは、メールが悪意あるコンテンツであるかについてすでにスキャン済みであることをユーザに知らせる、特別なフッタを追加することが可能です。

※悪意のあるコンテンツを含むメッセージはブロックされ、メール隔離場所に保存されます。ユーザはユーザポータルまたは、毎日の隔離レポートで、隔離されたメッセージの確認やリリースが可能です。ただし、悪意のあるコンテンツを含むメッセージのリリースは、メールマネージャで管理者のみが実施できます。

(2) SMTP スпам対策

スパム対策の機能は以下の通りです。

機能項目	機能内容
スパムフィルタ	スパムの可能性があるとして分類されたメッセージに対する対策の定義が可能です。確実性の高いスパム、疑わしいスパム、これら2種類のスパムに対する処理を、警告、隔離、スキャンしない設定が可能です。

送信者ブラックリスト	個別にブロックしたい送信者の設定が可能です。ブラックリストは外部からの SMTP セッションの送信者を参照します。
表現フィルタ	メッセージの件名や本文を特定の表現をスキャンすることが可能です。

(3) SMTP その他

その他の機能は以下の通りです。

機能項目	機能内容
除外	アンチスパム、マルウェア、またはその他のセキュリティチェックから除外するホワイトリストのホスト、ネットワーク、送信者、および受信者の定義が可能です。
リレー	SMTP プロキシはメールリレーとして使用可能です。
ヘッダ変更	UTM を通過するメールの SMTP ヘッダコンテンツを変更または削除設定が可能です。
透過モード	透過モードは、ポート 25、465、587 のトラフィックを傍受し、それをプロキシに再ルーティングします。
TLS 設定	TLS ハンドシェイクを実行する際、このシステムを識別するために使用されます。
DomainKeys Identified Mail (DKIM)	DKIM 署名の設定が可能です。DKIM 署名を使用するには、RSA 鍵と対応する鍵の設定とドメインの設定が必要です。
機密性表明フッタ	メールに機密情報や部外秘の情報が含まれていることなどをユーザーに知らせる、機密フッタの追加・カスタマイズが可能です。

(4) POP3 プロキシ

受信メールの POP3 プロキシを設定が可能です。POP3 プロキシは透過的に機能し、ポート 110 または 995 (TLS による暗号化) で内部ネットワークから受信するすべての POP3 通信をスキャンします。提供される機能は以下の通りです。

機能項目	機能内容
------	------

マルウェアスキャン	ウイルス、トロイの木馬、疑わしいファイルタイプなどスキャンが可能です。スキャンされたメールは破棄、隔離のアクション選択が可能です。隔離されたメッセージは、メールの隔離場所に保存されます。ウイルス対策エンジンはシングルスキャン、デュアルスキャンから選択可能です。
ファイル拡張子フィルタ	ファイル拡張子に基づいて特定タイプのファイルを含むメールのフィルタリングが可能です。

(5) POP3 スпам対策

スパム対策の機能は以下の通りです。

機能項目	機能内容
スパムフィルタ	スパムの可能性があるとして分類されたメッセージに対する対策の定義が可能です。確実性の高いスパム、疑わしいスパム、これら2種類のスパムに対する処理を、警告、隔離、スキャンしない設定が可能です。
送信者ブラックリスト	個別にブロックしたい送信者の設定が可能です。受信する POP3 セッションのエンベロープの送信者が、このブラックリストのアドレスと照合されます。
表現フィルタ	メッセージの件名や本文を特定の表現をスキャンすることが可能です。

(6) POP3 その他

その他の機能は以下の通りです。

機能項目	機能内容
除外	アンチスパム、マルウェア、またはその他のセキュリティチェックから除外するホワイトリストのホスト、ネットワーク、送信者、および受信者の定義が可能です。
透過モード スキップリスト	透過モード時にスキップするホストとネットワークを設定することが可能です。
POP3 サーバと プリフェッチ設定	指定の POP3 サーバへ対するプリフェッチ設定が可能です。

優先文字コード	優先文字コードの設定が可能です。
TLS 設定	TLS 暗号化された POP3 トラフィックのスキャンが可能です。

(7) 隔離レポート

Eメールプロテクションには、さまざまな理由からブロックされ、配信待ちのメッセージ、悪意あるソフトウェアに感染したメッセージ、疑わしい添付ファイルを含むメッセージ、スパムと特定されたもの、または単に不要な表現を含むメッセージが含まれます。隔離レポートで提供される機能は以下の通りです。

機能項目	機能内容
レポート送信時刻	隔離レポートの送信時刻及び追加のレポートの設定が可能です。
カスタマイズ可能なメッセージテキスト	隔離レポートの序文となるテキストのカスタマイズが可能です。
除外	隔離レポートを受信する E メールアドレスの除外設定が可能です。
リリースオプション	ユーザがリリース可能な隔離メッセージのタイプを設定可能です。

(8) メールマネージャ

メールマネージャは、機器に現在保存されているすべてのメールメッセージを管理および整理するための管理ツールです。配信待ちのメッセージや、悪意あるソフトウェアに感染している隔離メッセージ、疑わしい添付ファイルが添付されている隔離メッセージ、スパムとして識別された隔離メッセージ、または好ましくない表現が含まれている隔離メッセージなどが表示されます。メッセージをダウンロード、リリース、削除する前に、メールマネージャを使用してすべてのメッセージをレビューすることができます。メールマネージャは UTF-8 に完全に対応しています。
 ※データベースログは 3 日経過後に削除されます。許可される最大日数は 30 日です。
 ※隔離メッセージは 14 日経過後に削除されます。許可される最大日数は 999 日です。

※データベースログと隔離の両方に対して許可される最低日数は 1 日です。

3 – 6. 高度な防御

Sophos UTM9 で提供される高度な防御機能は以下の通りです。

Advanced Threat Protection

Sophos UTM9 はすべてのネットワークとの間でやり取りされる IP パケットを精査し、Sophos Labs からフィードされる CnC/Botnet データによって継続的に更新されるデータベースを参照しよりリスクの高い感染したホストや、そのコマンド・アンド・コントロール（CnC） サーバとの通信を防御します。

3 – 7. Web サーバプロテクション

Sophos UTM9 で提供される Web サーバプロテクション機能は以下の通りです。

(1) WAF

Sophos UTM9 はリバースプロキシ及び Web アプリケーションファイアウォール（WAF） 機能を提供します。保護される仮想サーバは、DNAT ルールを使用する代わりに定義します。UTM のこのエリアでは、Web サーバから送受信されるリクエストに、利用条件を適用することができます。また、複数のターゲットに対する負荷分散が可能です。

(2) 仮想 Web サーバ

これらの仮想 Web サーバは、UTM の一部としてインターネットと Web サーバ間のファイアウォールを構築します。UTM は Web サーバへのリクエストをピックアップし、実際の Web サーバを様々な攻撃から保護します。それぞれの仮想 Web サーバは バックエンド Web サーバにマッピングされており、適用する保護レベルが設定されます。これにより、バックエンド Web サーバのロードバランシングを実行できます。ファイアウォールプロファイルとして提供される機能は以下の通りです。

機能項目	機能内容
実行モード	すべての HTTP リクエストをモニタリングし、ログに記録するモニターモ

	ードと、ルールに応じて HTTP リクエストを拒否する拒否モードの設定が可能です。
スタティック URL ハードニング	URL の書き換えから保護します。クライアントが Web サイトを要求すると、Web サイトのすべてのスタティック URL に対して署名が行われます。
フォームハードニング	URL の書き換えから保護します。Web フォームのオリジナル構造を維持したまま署名します。
Cookie 署名	Web サーバを Cookie の悪用から保護します。
低レピュテーションのクライアントをブロック	GeoIP および RBL 情報に基づいて、評判の悪いクライアントを分類に従ってブロックすることが可能です。
共通脅威フィルタ	複数の脅威から Web サーバを保護できます。 ※詳細は次項にて記載します。
Rigid フィルタリング	ルールのいくつかがより厳しくスキャンされます。
フィルタルールをスキップ	脅威カテゴリに誤検出につながるルールが含まれている場合、スキップしたいルール番号の設定が可能です。
アンチウイルススキャン有効化	Web サーバをウイルスから防御します。ウイルス対策エンジンはシングルスキャン、デュアルスキャンから選択できます。対象ダウンロード、アップロードいずれかまたは両方を設定することが可能です。
MIME タイプによるブロックアップロード	MIME タイプで定義されたアップロードをスキャンしたりブロックすることが可能です。

共通脅威フィルタの詳細は以下の通りです。

機能項目	機能内容
プロトコル違反	HTTP プロトコルの RFC 標準仕様の遵守を強制します。
プロトコル異常	共有使用パターンを検索し、パターンが欠けている場合、多くは悪意のあるリクエストを示しています。
リクエスト制限	リクエスト引数の量と範囲に妥当な制限を強制します。

HTTP ポリシー	HTTP プロトコルの許可された使用を制限します。
不良ロボット	ロボットやクローラの使用パターンの特性をチェックします。
ジェネリック攻撃	大半の攻撃に共通するコマンド実行の試みを検索します。
SQL インジェクション攻撃	埋め込み SQL コマンドやリクエスト引数にあるエスケープ文字をチェックします。
クロスサイトスクリプティング (XSS) 攻撃	埋め込みスクリプトのタグやリクエスト引数のコードをチェックします。
嚴重なセキュリティ	禁止されているパストラバーサルを試行をチェックするなど、リクエストに関して嚴重なセキュリティチェックを実行します。
トロイの木馬	トロイの木馬が特徴とする使用パターンをチェックします。
アウトバウンド検査	Web サーバからクライアントへの情報の漏えいを防ぎます。

(3) その他

その他の機能は以下の通りです。

機能項目	機能内容
サイトパスルーティング	外部から受信したリクエストを転送する本 Web サーバの設定が可能です。
リクエストリダイレクト	受信リクエストを転送する URL の定義が可能です。
SlowHTTP 保護	リクエストヘッダのタイムアウトを設定が可能です。
プロキシプロトコル	プロキシプロトコルがサポートされます。
セッションストレージ	Web アプリケーションファイアウォールでのユーザセッションの制限が可能です。

Cookie 署名	Cookie 署名用の署名キーとして使用できるカスタムシークレットの設定が可能です。
スタティック URL ハードニング	URL ハードニング用の署名キーとして使用されるカスタムシークレットの設定が可能です。
フォーム ハードニング	フォームハードニングトークンの暗号キーとして使用されるカスタムシークレットの設定が可能です。
除外	特定のチェックから除外される Web リクエストや送信元ネットワークの設定が可能です。
リバース認証	認証プロファイルによって、リバース認証を使用して、特定の認証設定をそれぞれのサイトパスルータに割り当てることが可能です。
フォームテンプレート	リバース認証のために HTML フォームをアップロードすることが可能です。またブロックページのアップロードや HTML の編集が可能です。
証明書管理	Sophos UTM9 内で使用する証明書関連オプションを管理することが可能です。X.509 証明書の作成またはインポート、および CRL のアップロードなどを行うことが可能です。
Let's Encrypt™証明書	Let's Encrypt が発行する証明書の自動生成と自動更新が可能です。Let's Encrypt の利用規約に同意しご利用いただくことになります。

3-8. サイト間 VPN

Sophos UTM9 で提供されるサイト間 VPN 機能は以下の通りです。

機能項目	機能内容
Amazon VPC	Amazon VPC との IPsec 接続が可能です。
IPsec	IPsecVPN 接続が可能です。標準的なトランスポートモード、トンネルモード及び AH (認証ヘッダ) 認証プロトコル、ESP (カプセル化セキュリティペイロード) 暗号化 (および認証) プロトコルを定義することが可能です。
SSL	SSL 接続を介した SSL VPN 接続が可能です。

詳細

暗号化設定、圧縮設定、デバッグ設定など、各種の高度なサーバーオプションを設定できます。

その他の機能は以下の通りです。

機能項目	機能内容
暗号化アルゴリズム	VPN トンネルを通して送信されるデータの暗号化に使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。 DES-EDE3-CBC AES-128-CBC (128 ビット) AES-192-CBC (192 ビット) AES-256-CBC (256 ビット) BF-CBC (Blowfish (128 ビット))
認証アルゴリズム	VPN トンネルを通して送信されるデータの完全性チェックに使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。 MD5 (128 ビット) SHA1 (160 ビット) SHA2 256 (256 ビット) SHA2 384 (384 ビット) SHA2 512 (512 ビット)
鍵サイズ	Diffie-Hellman 鍵交換の長さをビット単位で指定可能です。1024、2048、3072 または 4096 ビットの鍵サイズを選択できます。
サーバ証明書	SSL VPN サーバがクライアントに対して自らの身元を証明するために使用するローカル SSL 証明書を設定可能です。 ※UTM はワイルドカード証明書および SSL VPN の中間 CA により署名された証明書をサポートしていません。
鍵の有効期限	鍵の有効期限を設定可能です。デフォルトは 28,800 秒です。
圧縮設定	SSL VPN トンネルを通して送信されるすべてのデータを暗号化の前に圧縮設定が可能です。
デバッグ設定	デバッグ情報を SSL VPN ログファイルに含めることが可能です。
証明書管理	UTM の証明書関連のあらゆる操作を一元管理することが可能です。

3-9. リモートアクセス

Sophos UTM9 で提供されるリモートアクセス機能は以下の通りです。

機能項目	機能内容
SSL	OpenVPN によるリモートアクセスが可能です。セキュアなユーザポータルから、カスタマイズされた SSL VPN クライアントソフトウェアバンドルをダウンロードできます。このバンドルには無料の SSL VPN クライアント、SSL 証明書、および簡単なワンクリックでインストールできる設定が含まれています。
PPTP	PPTP によるリモートアクセスが可能です。
L2TP over IPsec	機密性、認証、完全性を提供する IPsec と L2TP を組み合わせた L2TP over IPsec によるリモートアクセスが可能です。
iOS デバイス	ユーザポータルで iOS デバイスユーザに対する自動 L2TP over IPsec 設定を提供することが可能です。
IPsec	IPsec によるリモートアクセスが可能です。標準的なトランスポートモード、トンネルモード及び AH（認証ヘッダ）認証プロトコル、ESP（カプセル化セキュリティペイロード）暗号化（および認証）プロトコルを定義することが可能です。
HTML5 VPN ポータル	HTML5 VPN ポータル機能によるリモートアクセスが可能です。外部ネットワークのユーザは、ブラウザのみをクライアントとして使用して、あらかじめ設定されているコネクションタイプで内部リソースにアクセスすることができます。
Cisco VPN クライアント	Cisco VPN クライアント経由の IPsec リモートアクセスが可能です。

詳細

暗号化設定、圧縮設定、デバッグ設定など、各種の高度なサーバーオプションについてはサイト間 VPN と同様です。

3-10. ログとレポート

Sophos UTM9 で提供されるログとレポート機能は以下の通りです。

(1) ログファイルの閲覧

機能項目	機能内容
今日のログファイル	当日時点で出力されるすべてのログにアクセス可能です。
アーカイブログファイル	すべてのログファイルはデイリーベースでアーカイブされます。アーカイブしたログファイルは、閲覧したり、zip ファイル形式でダウンロードできます。UTM システム ID を含め、記載されたすべてのログファイルを一度にダウンロードするには、すべてのログのエクスポートをクリックします。 ※512 MB を超える未圧縮のログファイルを表示・ダウンロードはできません。
ログファイルの検索	さまざまな期間のローカルログファイルを検索することが可能です。

ログとレポートは機能毎の参照が可能です。参照可能な情報は以下の通りです。

機能項目	機能内容
ハードウェア	ハードウェアの使用状況に関する以下の情報が表示されます。 CPU 使用率 メモリ/スワップ使用率 パーティション使用率 表示される期間は以下の通りです。 デイリー：過去 24 時間の統計概観を示します。 ウィークリー：過去 7 日間の概要的な統計を示します。 マンスリー：過去 4 週間の概要的な統計を示します。 年次：過去 12 か月間の概要的な統計を示します。
ネットワーク使用状況	各インタフェースを通過したトラフィックに関する概要的な統計が表示されます。各チャートのデータは、以下の単位を使用して示されます。 u (マイクロ、 10^{-6})

	<p>m (ミリ、10^{-3}) k (キロ、10^3) M (メガ、10^6) G (ギガ、10^9)</p> <p>10^{-18}~10^8 の範囲内でスケーリング可能です。</p> <p>各ヒストグラムには、受信、送信の 2 つのグラフが表示されます。</p> <p>同時接続チャートは、同時接続の合計を示します。表示される期間は以下の通りです。</p> <p>デイリー：過去 24 時間の統計概観を示します。</p> <p>ウィークリー：過去 7 日間の概要的な統計を示します。</p> <p>マンスリー：過去 4 週間の概要的な統計を示します。</p> <p>年次：過去 12 か月間の概要的な統計を示します。</p>
帯域使用状況	<p>デバイスから転送されたネットワークトラフィック、デバイスに転送されたネットワークトラフィック、デバイスを経由して転送されたネットワークトラフィックについての包括的なデータが表示されます。データを PDF あるいは Excel 形式でダウンロードできます。</p>
Network Protection	<p>ネットワークプロテクションイベントについての概要的な以下の統計が表示されます。</p> <p>ファイアウォール違反 侵入防止の統計</p> <p>表示される期間は以下の通りです。</p> <p>デイリー：過去 24 時間の統計概観を示します。</p> <p>ウィークリー：過去 7 日間の概要的な統計を示します。</p> <p>マンスリー：過去 4 週間の概要的な統計を示します。</p> <p>年次：過去 12 か月間の概要的な統計を示します。</p>
ファイアウォール	<p>ファイアウォールアクティビティに関する包括的なデータが、送信元 IP、送信元ホスト、受信パケット数、サービス数に従って分類されて表示されます。データを PDF あるいは Excel 形式でダウンロードできます。</p> <p>※TTL (生存時間) が 1 以下のパケットは、ログされることなくドロップされます。</p>
Advanced Threat Protection	<p>ネットワークでの脅威の詳細に関する包括的なデータが表示されます。データを PDF あるいは Excel 形式でダウンロードできます。</p>

IPS	ネットワークでの侵入防御アクティビティに関する包括的なデータが表示されます。データを PDF あるいは Excel 形式でダウンロードできます。
Web Protection	最もアクティブな Web ユーザと最もよく表示されている Web サイトに関する概要的な統計が表示されます。
Web 使用状況レポート Web サーフィンデータ 統計	ネットワークトラフィックやユーザの Web 使用状況に関する包括的なデータが表示されます。
検索エンジンレポート	ユーザが使用している検索エンジンやユーザが行った検索に関する情報が表示されます。
部門	ユーザまたはホストおよびネットワークを仮想部門にグループ化することが可能です。これらの部門を使用して Web 使用状況レポートや検索エンジンレポートをフィルタすることが可能です。
スケジュールレポート	定期的に E メールで送信したい保存済みレポートを定義することができます。スケジュールレポートを作成するには、あらかじめ保存済みのレポートが少なくとも 1 つ必要です
アプリケーション コント ロール	様々な期間における最もアクティブな送信元、最も訪問が頻繁な宛先、最も人気の高いアプリケーションについての総合的な統計が表示されます。
Email Protection 使用状況グラフ	さまざまな時間枠内に UTM を通過したメールフローの概要的な統計が表示されます。表示される期間は以下の通りです。 デイリー：過去 24 時間の統計概観を示します。 ウィークリー：過去 7 日間の概要的な統計を示します。 マンスリー：過去 4 週間の概要的な統計を示します。 年次：過去 12 か月間の概要的な統計を示します。
メール使用状況	さまざまな時間帯で最もアクティブに使用された E メールアドレスやアドレスドメインに関する包括的な統計が表示されます。
ブロックメール	ウイルス対策およびアンチスパムによってブロックされたすべてのメール要求に関する包括的な統計が表示されます。データを PDF あるいは Excel 形式でダウンロードできます。
リモートアクセス	リモートアクセスアクティビティおよびセッション情報に関する全体的な統計を提供します。 表示される期間は以下の通りです。 デイリー：過去 24 時間の統計概観を示します。

	<p>ウィークリー：過去 7 日間の概要的な統計を示します。</p> <p>マンスリー：過去 4 週間の概要的な統計を示します。</p> <p>年次：過去 12 か月間の概要的な統計を示します。</p>
セッション	<p>さまざまな時間範囲について、完了したセッション、失敗したログイン、および現在のユーザに関する包括的な統計を提供します。</p>
Webserver Protection 使用状況グラフ	<p>Web サーバの要求、警告、アラートに関する概要的な統計を表示します。表示される期間は以下の通りです。</p> <p>デイリー：過去 24 時間の統計概観を示します。</p> <p>ウィークリー：過去 7 日間の概要的な統計を示します。</p> <p>マンスリー：過去 4 週間の概要的な統計を示します。</p> <p>年次：過去 12 か月間の概要的な統計を示します。</p>
Webserver Protection 詳細	<p>さまざまな時間枠内で最もアクティブだったクライアント、仮想ホスト、バックエンド、応答コード、および様々な攻撃に関する包括的な統計が表示されます。</p>

(2) エグゼクティブレポート

各サービスのネットワーク使用状況を表示するために重要なレポートングデータをグラフィカルな形式にまとめることができます。エグゼクティブレポート機能は以下の通りです。

機能項目	機能内容
アーカイブ エグゼクティブレポート	アーカイブされたすべてのエグゼクティブレポートの概要表示が可能です。
デイリー エグゼクティブレポート	デイリーエグゼクティブレポートの作成が可能です。エグゼクティブレポートは PDF、HTML によるメール送信が可能です。
ウィークリー エグゼクティブレポート	ウィークリーエグゼクティブレポートの作成が可能です。エグゼクティブレポートは PDF、HTML によるメール送信が可能です。このレポートでは、エグゼクティブレポートがデータの収集を開始する曜日も選択できます。
マンスリー エグゼクティブレポート	マンスリーエグゼクティブレポートの作成が可能です。エグゼクティブレポートは PDF、HTML によるメール送信が可能です。

(3) ログ設定

ローカルおよびリモートログの基本的な設定を構成できます。提供される機能は以下の通りです。

機能項目	機能内容
ローカルログ	ローカルログの出力が可能です。デフォルトではローカルログは有効になっています。ログファイルの自動消去設定も可能です。
リモート Syslog サーバ	他のホストにログメッセージの転送が可能です。選択したホストは、Syslog プロトコルと互換性のあるログデーモンを実行する必要があります。
リモートログファイル アーカイブ	前日のログファイルは1つのファイルに集約・圧縮され、リモートログファイルのストレージに転送することが可能です。
レポート設定	レポートの出力機能の有効化/無効化やデータ保持時間/量の設定が可能です。
除外	特定のドメインやアドレスをレポートから除外することが可能です。

以上