24 時間有人監視でネットを守る

あんしんネットワーク警備

Owlook®

【BOX 型 UTM】

マネジメントサービス仕様書

第 1.1 版

2018 年 4 月 5 日

愛媛綜合警備保障株式会社

目　次

改訂履歴

版数	更新日	更新内容	更新者
1.0	2017/11/15	制定	三浦
1.1	2018/04/05	レポートの仕様を修正	吉田

はじめに

本仕様書は、興安計装株式会社（以下「サービス提供事業者」とする）が提供する「BOX 型 UTM マネジメントサービス」（以下「本サービス」とする）の利用申込を行ったお客様（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「BOX 型 UTM 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。

1. BOX 型 UTM マネジメントサービスについて

1-1.サービス構成

本サービスは、UTM のセキュリティ機能および、監視・運用保守サービスをサービス提供事業者が提供するものです。各機能およびサービスの構成は以下の通りです。

※サービス詳細については「2.サービス内容」を参照ください。

※サービス適用対象は UTM のみとなります。その他の機器・設備については保守対象外となります。

基本サービス	・24 時間 365 日の死活監視 ・重大インシデント発生連絡 ・各種設定変更 ・故障申告受付窓口 ・定期バックアップ ・ファームウェアバージョンアップ対応 ・保守（センドバック/オンサイト保守） ・レポート閲覧（※1）
セキュリティ機能	・ステートフル Firewall ・侵入検知／防御（IPS） ・高度な脅威検知（ATP） ・URL フィルタリング（※1） ・アプリケーションコントロール（※1） ・E メールプロテクション ホワイトリスト/ブラックリスト登録（※1）
有料オプションサービス	・訪問設置サービス

※1「URL フィルタリング」・「E メールのホワイトリスト/ブラックリスト登録」・「レポート閲覧」・「アプリケーションコントロール」は利用者で登録・確認頂く項目となります。

1-2.サービス提供範囲

本サービスの提供範囲は以下となります。サービス提供事業者は UTM に関するサポートを実施いたします。

回線提供事業者	ONU/ホームゲートウェイ/ビジネスフォン機器/事業者様機器　等
サービス提供事業者	UTM （SG105、SG115、SG125、SG135、SG210、SG230、SG310、SG330）
利用者設備	ルータ/アクセスポイント/パソコン/タブレット端末/プリンタ　等

※サービス提供時に LAN ケーブルを 1 本同梱いたします。経年劣化等で故障した場合は、利用者様にてご用意いただきます。

※本サービスがご利用いただけない状況が発生した場合は、利用規約に基づき対応を行います。

1-3.サービス提供責任範囲

提供者	責任範囲
利用者	利用者様所有機器
サービス提供事業者	UTM

1-4.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。

項目	条件
インターネット回線	ご利用いただく回線およびプロバイダに制限はございません。
PPPoE 接続機器（ホームゲートウェイ・ビジネスフォン機器・ルータ等）	サービス利用にあたっては、UTM 上位に設置するルータ機能を持つ機器をご用意ください。UTM はブリッジモードにて動作いたします。 ※上位機器のファイアーウォール等で通信が遮断される場合は、PPPoE 接続機器の設定変更をお願いする場合がございます。
Wi-Fi 機器をご利用の場合	利用者が Wi-Fi 機器を利用されている場合、利用者の Wi-Fi 機器と利用者端末とで Wi-Fi 接続を実施してください。
VPN 接続について	UTM の監視および設定変更作業のみに使用いたします。

※UTM のファームウェアアップデート作業の際、サービス停止を伴う計画的な作業があります。

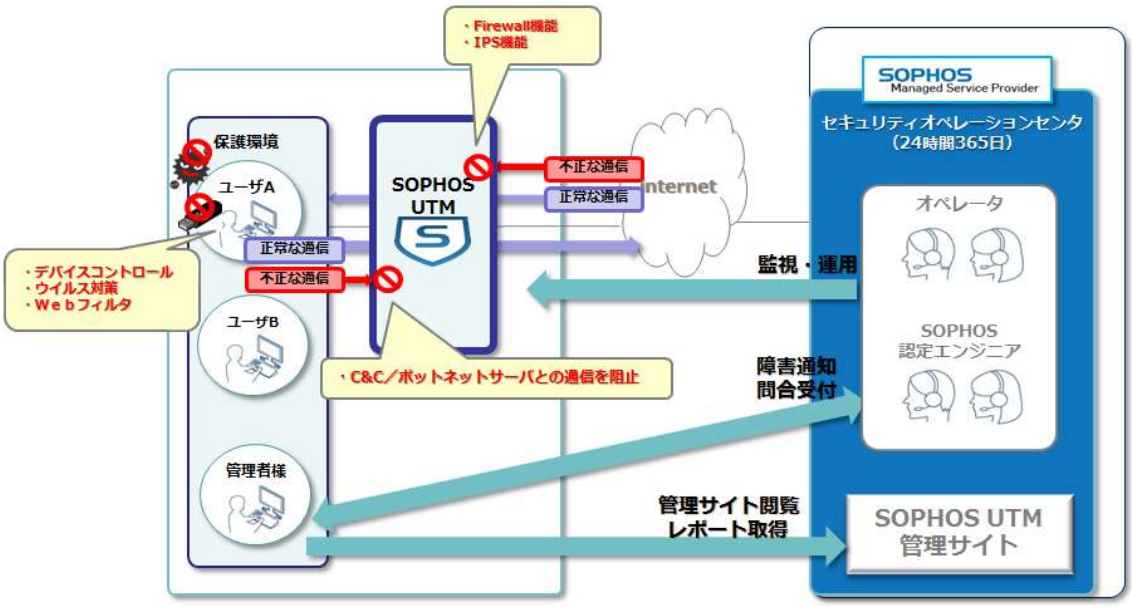
1-5.サービス提供形態

本サービスでは、UTM を既存のお客様ネットワーク内にブリッジとして設置いたします。UTM に対してお客様ネットワークアドレスより、固定の IP アドレスを 1 つ提供していただく必要がございます。

WAN インタフェースについて　・・・ プライベート、グローバルアドレス共に対応可能です。
PPPoE の終端には対応しておりません。

LAN インタフェースについて　・・・ WAN インタフェースとブリッジインタフェースを構成することで、WAN セグメントと同ネットワークアドレスを使用することが可能となります。

提供イメージ



※UTM 上位にルータ機能を持つ機器（ホームゲートウェイ等）をご用意いただき、その機器で PPPoE 接続を実施ください。

※利用者ルータの配下にブリッジモードで UTM を設置いたします。

※Wi-Fi をご利用される場合、UTM の配下に利用者の Wi-Fi 機器を設置してください。

1-6.サービス提供レベル一覧

サービス項目	提供時間	提供レベル	通知仕様
死活監視	24 時間 365 日	検知後即時	メールにて自動通知 ※希望により電話通知も可（※1）
重大インシデント発生連絡	24 時間 365 日	メールは検知後 20 分以内に送付	メールにて通知 ※希望により電話通知も可（※2）
レポート	随時	随時	利用者がログインして確認
各種設定変更	24 時間 365 日	最大 5 日以内(※3)に実施	メールにて通知 ※希望により電話通知も可
故障申告受付窓口	24 時間 365 日	1 次回答を 24 時間以内に実施	電話にて受付後 メールまたは電話にて通知
定期バックアップ	毎日夜間	自動取得	通知なし
ファームウェア バージョンアップ対応	都度案内	メンテナンス実施 2 週間前までにメールにて告知	メールにて通知

※1　作業によるアラームの検知を考慮し、以下の条件に当てはまった場合電話連絡します。

・営業時間（平日 9 時～17 時）帯の 14 時以前に発生

・・・アラーム検知後 3 時間経っても復旧アラームを検知しない場合に連絡

・営業時間（平日 9 時～17 時）帯の 14 時以降に発生

・・・アラーム検知後 17 時までに復旧アラームを検知しない場合に連絡

・営業時間外（平日 17 時～9 時及び土日祝）に発生

・・・アラーム検知後翌営業日の 12 時まで復旧アラームを検知しない場合に連絡

◇大規模障害の場合はこの限りではありません。

◇電話が繋がらなかった場合はメールにてご連絡いたします。

（留守番電話サービスを利用されている場合はメッセージを残します）

※2　お客様希望時間帯に連絡します。

※3　受付受領通知は担当者確認後 24 時間以内、作業実施は受領通知後 72 時間以内、作業結果通知は作業完了後 24 時間以内

2. サービス内容

2-1. セキュリティ機能

（1）セキュリティ機能一覧

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。

※セキュリティ機能は SOPHOS 社が提供する UTM 仕様に準ずるものです。

機能項目	機能内容
ファイアウォール	UTM を通過するパケットを監視し、フィルタルールに従ってパケットを制御します。ポートの設定は「全開放」又は「全閉塞」のどちらかになります。
侵入防御 （IPS）	IPS パターン / ディープパケットのインスペクションを組み合わせて攻撃を特定しブロックします。また Dos／フラッド、ポートスキャンなどからの通信から保護することが可能です。
高度な脅威検知 （ATP）	ネットワークから出ていくトラフィックをモニターし内部の感染したコンピューターを検出し C&C/ボットネットとの不正通信を遮断します。
URL フィルタリング	Web アクセス時に予め設定した処理に従いアクセス制御を行います。管理者がアクセスさせたくないサイトや有害なサイトへのアクセスをブロックし、警告メッセージを表示させます。
アプリケーション コントロール	すべてのネットワークトラフィックが、アプリケーションの分類に応じて分類またはロギングされます。twitter や Facebook などアプリケーション単位でのアクセス制御が可能です。
アンチスパム	スパムメールを警告（Subject にスパムマーカを付与）します。
アンチフィッシング	メールに含まれるフィッシング URL を検出しブロックします。
ウィルス検知	メール添付ファイル及び Web サイトからのダウンロードデータをスキャンし、マルウェアをブロックします。
レポート閲覧	ネットワークの利用状況をはじめ、パケットフィルタ/ファイアーウォールのブロック状況などをご確認頂けます。

（2）セキュリティ機能詳細

※E メールプロテクション以外のすべての機能において初期設定はメーカーの推奨値で設定します。※１

①ファイアウォール※２、※３

ファイアウォールルールは上位からチェックされます。最初のルールが一致するまでチェックを続けます。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。以降の他のルールはすべて無視されます。

②侵入防御（IPS）※4、※５

シグニチャに基づく IPS ルールセットを利用して攻撃を認識します。UTM を通過する通信に適用されます。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。

DoS/フラッド防御機能は、TCP SYN フラッド、UDP フラッド、ICMP フラッドに対応しており、通信レートの上限を超えたパケットを遮断します。

ポートスキャン機能は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ブロックします。

③高度な脅威検知※６

侵入防御および Web プロテクションとの連携により、UTM を通過する通信に適用されます。

④URL フィルタリング※７、※８、※９

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 サイトを検出する、ウイルス対策が含まれています。また、カテゴリ毎の Web サイトへのアクセスを制御できますので、管理者は、ギャンブル、ポルノ、ショッピングといったものへのアクセスに関するポリシを強制し、これらのサイトのブロックすることが可能です。

⑤アプリケーションコントロール※１０、※１１

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ブロックすることができます。URL フィルタリングとは異なり、アプリケーション制御分類エンジンを使用すると、ネットワークトラフィックをプロトコルや URL 単位ではなく、よりきめ細かい基準で識別することができます。

⑥E メールプロテクション※１２、※１３、※１４、※１５、※１６、※１７、※１８、※１９

SMTP、POP3 プロキシを設定し保護します。送受信される E メールに対してウイルススキャンおよびメールフィルタサービスを提供します。

※1　パフォーマンスに影響がでる可能性があるためデフォルト設定を推奨しております。
※2　サービス提供事業者が指定した定義および適用ルールに基づき処理を行います。初期設定は「全開放」ですが、侵入防御機能と連動しているため、一部不正なパケットを遮断することがあります。
※3　利用者の UTM 操作を推奨しておりません。ルール追加・変更・削除・除外、SSL 証明書の設定は監視・運用サービスにて提供します。
※4　情報流出等の防止を完全に保証する機能ではございません。
※5　ポートスキャン機能は初期設定では無効となっております。
※6　侵入防御もしくは Web プロテクションとの連携は必須要件となります。
※7　フィルタリングリング設定は、お客様で設定して頂きます。
※8　http は URL、ファイルのダウンロードに対しフィルタを掛けます。
※9　https は URL に対しフィルタを掛けます。
※10　アプリケーションコントロール設定は、お客様で設定して頂きます。
※11　初期設定では「全開放」となっております。
※12　送信メールは 25 番ポートあて、受信メールは 110 番、995 番ポートあてのメールを監視します。ポート番号が異なる場合は監視できません。また送信メールにおいて 25 番ポートで監視をするためには、UTM を SMTP プロキシとして動作させる必要がある為、利用者でご利用のメールソフトの設定変更が必要となります。
※13　すべてのドメインが同じ設定を共有している環境での動作を前提としております。
※14　メールクライアントの設定でサーバータイムアウト設定を長くすることが必要になる場合があります。
※15　スパムマーカは 2 バイト文字に対応しておりますが、環境依存文字があった場合、優先文字コードが UTF-8 以外に設定されている際に変換できず、スパムマーカが文字化けする場合があります。
※16　アンチウィルススキャンの最大スキャンサイズは 50Mbyte です。
※17　E メールのホワイトリスト/ブラックリスト、スパムメールの隔離設定はお客様にて設定頂きます。
※18　スパムメールの隔離設定もお客様にて設定頂きます。
※19　隔離されたメールはメールマネジャー機能から管理者が閲覧可能です。また、利用者に対しても隔離されたことを通知するレポートを 1 日最大 2 回まで発報することができます。但し、添付メールのスキャンについてはオンデマンドでレポートが送信されます。

2-2. 監視・運用保守サービス

（1）監視・運用保守サービス一覧

本サービスが提供する監視・運用サービスの詳細は以下の通りとなります。

- サービス提供事業者が提供する UTM を対象とします。

サービス項目	サービス内容
死活監視	UTM を 24 時間 365 日死活監視し利用者へ通知します。
重大インシデント発生連絡	重大なインシデントが発生した際に利用者へ通知します。
レポート	UTM で扱った脅威のサマリ（ブロックした通信など）等をお客様にて UTM へログインしていただきご覧いただけます。
各種設定変更	UTM が提供するセキュリティ機能に対する設定変更作業を行います。
故障申告受付窓口	利用者からの UTM の故障申告を 24 時間 365 日受け付けます。
故障対応	① オンサイト保守（平日 9:00~17:00 対応） ② オンサイト保守（24 時間 365 日対応） ③ センドバック保守
定期バックアップ	UTM 設定内容のバックアップを取得します。
ファームウェア バージョンアップ対応	UTM のファームウエアバージョンアップを行います。

（2）監視・運用保守サービス詳細

① 死活監視

サービス提供事業者監視システムと UTM とを VPN で接続し監視を行います。また、UTM の管理用 IP アドレスに対し、サービス提供事業者監視システムより 64Bytes の ICMP echo パケットを 10 分間隔で送信して監視します。タイムアウトが発生した場合、10 分後にリトライし、再度結果がタイムアウトであった場合、障害と判定し利用者へ通知を行います。

② 重大インシデント発生連絡

UTM が提供する各セキュリティ機能において、サービス提供事業者があらかじめ規定した設定に準ずる重大なインシデントが発生した際に、利用者へメール（希望により電話）にて通知します。

③ レポート

利用者に対して、レポートを閲覧するための ID/パスワードを発行いたします。利用者にてレポートを確認頂くことができます。なお、ご希望があればサービス提供事業者指定のフォーマットにてメール通知させて頂くことも可能です。尚、UTM のディスク容量により、古い記録が削除される場合があります。

④ 各種設定変更

対象となる設定変更作業はファイアウォールのルール設定追加・変更・削除、バックアップのリストア作業です。

利用者からの設定変更依頼については、電話・メールにて受付いたします。依頼受領から 72 時間以内に変更作業を実施します。変更作業が完了後、対応結果を電話、メールにて利用者へ通知します。

⑤ 故障申告受付窓口

故障申告窓口は電話・メールにて 24 時間 365 日受付可能となります。申告を受けた内容について UTM の状態確認およびサービス提供事業者にて定めた 1 次対応を実施し、実施結果を利用者へ電話、メールにて通知します。

⑥　保守対応

利用者との契約内容に従い、UTM の保守対応を実施いたします。

1.　オンサイト保守（平日 9:00~17:00 対応）

サービス提供事業者サポートセンターにて機器故障と判断した場合、代替機器を持参した作業員が、平日 9:00~17:00 間でご訪問し対応を実施いたします。

※交通事情などにより遅延する場合がございますが、サービス提供事業者にてオンサイト保守が必要と判断した時点から、7 時間以内に訪問できるよう対応いたします。

2. オンサイト保守（24 時間 365 日対応）

サービス提供事業者サポートセンターにて機器故障と判断した場合、代替機器を持参した作業員が、24 時間 365 日でご訪問し対応を実施いたします。

※交通事情などにより遅延する場合がございますが、サービス提供事業者にてオンサイト保守が必要と判断した時点から、7 時間以内に訪問できるよう対応いたします。

3.　センドバック保守

サービス提供事業者サポートセンターにて機器故障と判断した場合、先行して代替機器を送付いたします。故障回復後に、サービス提供事業者指定の宛先まで故障機を送付ください。なお、受付時間帯によっては、当日発送ができない場合がございますので、予めご了承ください。

※故障機の返却は機器交換後から 1 週間以内に指定の住所へ着払いにてご返却ください。ご返却いただけない場合、その時点の交換機器の定価を請求させていただきます。

⑦　定期バックアップ

UTM の設定内容を毎日夜間帯に取得し、利用者毎に 10 世代の設定を管理します。リストア作業については各種設定変更サービスにて受付け、即時実施します。

⑧　ファームウェアバージョンアップ対応

ファームウエアバージョンアップまたは緊急のメンテナンス等で、UTM の再起動が必要になる場合は事前に利用者へメール、ポータルサイトにて通知後に実施します。

2-3.訪問設置サービス（オプション）

（1）訪問設置サービス一覧

本サービスは利用者が UTM 設置作業について、訪問での対応を希望された場合に実施する有料サービスとなります。

サービス項目	サービス内容
UTM 訪問設置サービス	UTM の設置工事をサービス提供事業者にて対応いたします。 ※訪問費用については別紙をご参照ください

※ご訪問時は、インターネット回線が開通していること。もしくはインターネット回線工事との同時訪問対応が前提となります。

3．各種受付窓口

3－1．各種窓口について

本サービスは利用者または利用前のユーザから、以下の仕様で各種問合せを受け付けます。

◇サービス開始前のお問合せ

部署名	内容	
ICT 技術サービス部門 関西営業所 UTM 担当	受付時間	平日 9:00~18:30
	連絡先	06-6459-7506
	メール	contact-nw@koan.co.jp

◇事業者様・利用者様向け

受付窓口	内容		
Owlook オペレーションセンター	サービス開始後のお問い合わせ	受付時間	24 時間 365 日
		連絡先	03-5295-3121
		メール	osms-support@koan.jp

別紙 1：機器スペック一覧

機器スペック一覧（1）：

パフォーマンス		SG105	SG115	SG125	SG135
ファイアウォール最大 ※1（Mbps）		1,500	2,300	3,100	6,000
ファイアウォール実環境 (Mbps) ※2		1,140	1,630	2,100	3,650
ATP 実環境(Mbps) ※2		1,060	1,470	1,490	2,680
IPS 最大（Mbps） ※1		350	500	750	1,500
IPS 全ルール（Mbps）		175	200	320	590
FW + ATP + IPS 最大 (Mbps) ※1		310	450	680	1,340
FW + ATP + IPS 実環境(Mbps) ※2		160	190	310	445
HTTP リクエスト数/秒 ※3		360	500	900	1,650
最大推奨接続数	新規 TCP 接続/秒	15,000	20,000	24,000	36,000
	同時 TCP 接続数	1,000,000	1,000,000	2,000,000	2,000,000
イーサネットインターフェース (固定)		4 GE copper	4 GE copper	8 GE copper	8 GE copper
I/O ポート（背面）		USB 2.0 x 2 COM (RJ45) x 1 VGA x 1			
電源		外部オートレンジ DC：12V、100-240VAC、 50-60 Hz			

機器スペック一覧（2）：

パフォーマンス		SG210	SG230	SG310	SG330
ファイアウォール最大 ※1（Mbps）		11,000	13,000	17,000	20,000
ファイアウォール実環境 (Mbps) ※2		5,970	7,140	8,265	9,760
ATP 実環境(Mbps) ※2		4,415	5,390	7,123	8,550
IPS 最大（Mbps） ※1		2,000	3,000	5,000	6,000
IPS 全ルール（Mbps）		630	910	1,390	1,420
FW + ATP + IPS 最大 (Mbps) ※1		1,910	2,850	4,790	5,890
FW + ATP + IPS 実環境(Mbps) ※2		590	780	980	1,110
HTTP リクエスト数/秒 ※3		2,100	2,300	3,100	4,200
最大推奨接続数	新規 TCP 接続/秒	60,000	70,000	100,000	120,000
	同時 TCP 接続数	4,000,000	4,000,000	6,000,000	6,000,000
イーサネットインターフェース (固定)		6 GE copper	6 GE copper	8 GE copper 2 GE SFP	8 GE copper 2 GE SFP
I/O ポート		USB 3.0 x 2（前面） Micro USB x 1（前面） USB 3.0 x 1（背面） COM (RJ45) x 1（前面） HDMI x 1（背面）			
電源		90-264VAC、50-60 Hz (内部で自動切替)			

本表はあくまで参考値となるため、実際の数値とは異なる場合があります。

※1　1518 バイト パケットサイズ (UDP)、デフォルトのルールセット

※2　NSS Perimeter Mix (TCP/UCP)

※3　スループット:　100k バイト ファイル、リクエスト / 秒: 1K バイト ファイル (記載されている数字はシングルスキャンによるもので、デュアルスキャンが有効な場合にスループットは 15-20%

減少)

物理仕様一覧（1）：

物理仕様	SG105/SG115	SG125/SG135
設置方式	ラックマウントキット入手可能 (個別に発注していただく必要があります)	
サイズ 幅　×　奥行　×　高さ	225 x 150 x 44 mm 8.86 x 5.91 x 1.73 インチ	288 x 186.8 x 44 mm 11.38 x 7.35 x 1.73 インチ
重さ	1.19 kg / 2.62 lbs (本体) 2.185 kg / 4.82 lbs (梱包時)	1.7 kg / 3.75 lbs (本体) 2.82 kg / 6.22 lbs (梱包時)
環境	SG105/SG115	SG125/SG135
電力消費量	12.46W、49.3 BTU/hr (アイドル時)26.16W、89.2 BTU/hr (フルロード時)	12.46W、49.3 BTU/hr (アイドル時)26.16W、89.2 BTU/hr (フルロード時)
稼働気温	0 - 40°C (動作時)-20 - +80°C (非動作時)	
湿度	10%-90% (結露なきこと)	
安全規格	SG105/SG115	SG125/SG135
認定資格	CE、FCC Class B、CB、VCCI、C-Tick、UL、CCC	

物理仕様一覧（2）

物理仕様	SG210/SG230	SG310/SG330
設置方式	1Uラックマウント （2 ラックマウント用のイヤーも付属）	
サイズ 幅　×　奥行　×　高さ	438 x 292 x 44 mm 17.24 x 11.5 x 1.75 インチ	
重さ	5.1 kg / 11.24 lbs (本体) 7.05 kg / 15.54 lbs (梱包時)	5.2 kg / 11.46 lbs (本体) 7.15 kg / 15.76 lbs (梱包時)
環境	SG210/SG230	SG310/SG330
電力消費量	20W、69BTU/hr (アイドル時)26.16W SG210：30W、103BTU/hr (フルロード時) SG230：34W、117BTU/hr (フルロード時)	12.46W、49.3 BTU/hr (アイドル時)26.16W、89.2 BTU/hr (フルロード時)
稼働気温	0 - 40°C (動作時)-20 - +80°C (非動作時)	
湿度	10%-90% (結露なきこと)	
安全規格	SG210/SG230	SG310/SG330
認定資格	CE、FCC Class A、CB、VCCI、C-Tick、UL、CCC	

別紙２：通知メール例

・UTM 通信断発生の通知

From:　osms-support@koan.jp
To:　ご登録済のお客様メールアドレス
Subject:　【異常通知】●●_xxx.xxx.xxx.xxx
発生年月日：YYYY/MM/DD
発生時刻　：HH:MM:SS
ノード名　：●●
IP アドレス：xxx.xxx.xxx.xxx
障害内容　：ICMP CRITICAL
ステータス：異常

・UTM 通信復旧の通知

From:　osms-support@koan.jp
To:　ご登録済のお客様メールアドレス
Subject:　【回復通知】●●_xxx.xxx.xxx.xxx
回復年月日：YYYY/MM/DD
回復時刻　：HH:MM:SS
ノード名　：●●
IP アドレス：xxx.xxx.xxx.xxx
障害内容　：ICMP OK
ステータス：正常

・重大インシデント発生の通知

From: "Firewall Notification System" <do-not-reply@fw-notify.net>
To: osms-service@koan.jp
Subject: [●●][CRIT-861] Advanced Threat Protection Alert
Advanced Threat Protection
A threat has been detected in your network
The source IP/host listed below was found to communicate with a potentially malicious site outside your company.
Details about the alert:
Threat name....: C2/Generic-A
Details.....: http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/C2~Generic-A.aspx
Time.....: YYYY-MM-DD HH:MM:SS
Traffic blocked: no
Source IP address or host: xxx.xxx.xxx.xxx

--
System Uptime : x days x hours x minutes
System Load : 0.10
System Version : Sophos UTM 9.315-2
Please refer to the manual for detailed instructions.
The send limit for this notification has been reached. No further notifications of this type will be sent during this period.

■本仕様書の著作権およびその他知的財産権について

本仕様書内の各文章、画像その他著作物等についての著作権およびその他知的財産権は、当社が利用者に対して本サービスを提供することに関して、契約に基づき当社に対して本サービスを提供する興安計装株式会社に帰属するものとなります。