Owlook®

BOX 型 UTM（WatchGuard 版）

マネジメント仕様書

第 1.7 版

2020 年 8 月 4 日

目　次

改訂履歴

版数	更新日	更新内容	更新者
1.0	2019/4/15	新規作成	松永
1.1	2019/5/14	重大インシデント発生連絡の条件を修正	松永
1.2	2019/5/22	マルウェアスキャン最大ファイルサイズを 5MB から 10MB へ変更	松永
		セキュリティ機能に標的型攻撃対策サンドボックスと DNS セキュリティを追加	
1.3	2019/07/12	レポート詳細説明の文言を修正	末岡
		サービス提供範囲の文言を T15 から T シリーズに変更	
		機器スペック一覧、物理仕様一覧を削除	
1.4	2020/06/10	保守内容にオンサイト保守を追加	松永
		重大インシデント発生連絡の通知先をお客様から申込書記載の通知先メールアドレスへ変更	
		設定変更サービスを追加	
		通知メール例を修正	
		サービス開始前問合せ先部署名を修正	
1.5	2020/06/26	サービス提供形態の管理インターフェイス IP を修正	末岡
		10.x.x.x 帯のアドレスではサービスを利用できない旨を注意事項へ追加	
1.6	2020/07/10	セキュリティ機能に Basic プラン/Total プランの機能分けを追加	松永
		管理インターフェースの説明文を修正	
		注意事項に UTM が直接インターネットへ接続する必要がある旨を追記	
1.7	2020/8/4	サービス名称を修正	浅野

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（WatchGuard 版）マネジメント」（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。

※セキュリティ機能は Basic プランと Total プランの 2 種類あり、標的型攻撃対策サンドボックス（APT Blocker）と DNS セキュリティ（DNS Watch）は Total プランの場合のみ利用可能です。

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 ・レポート送信 ・構成管理 ・故障申告受付窓口 ・保守（センドバック/オンサイト保守） ・ファームウェアバージョンアップ対応
セキュリティ機能	・ステートフル Firewall ・侵入検知／防御（IPS） ・レピュテーションセキュリティ&ボットネット検知 ・URL フィルタリング（WebBlocker） ・アプリケーション制御（Application Control） ・迷惑メール対策（spamBlocker） ・ゲートウェイアンチウィルス（Gateway AntiVirus） ・標的型攻撃対策サンドボックス（APT Blocker）※total プランのみ利用可 ・DNS セキュリティ（DNS Watch）※total プランのみ利用可

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（T シリーズ）
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

※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。

※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。

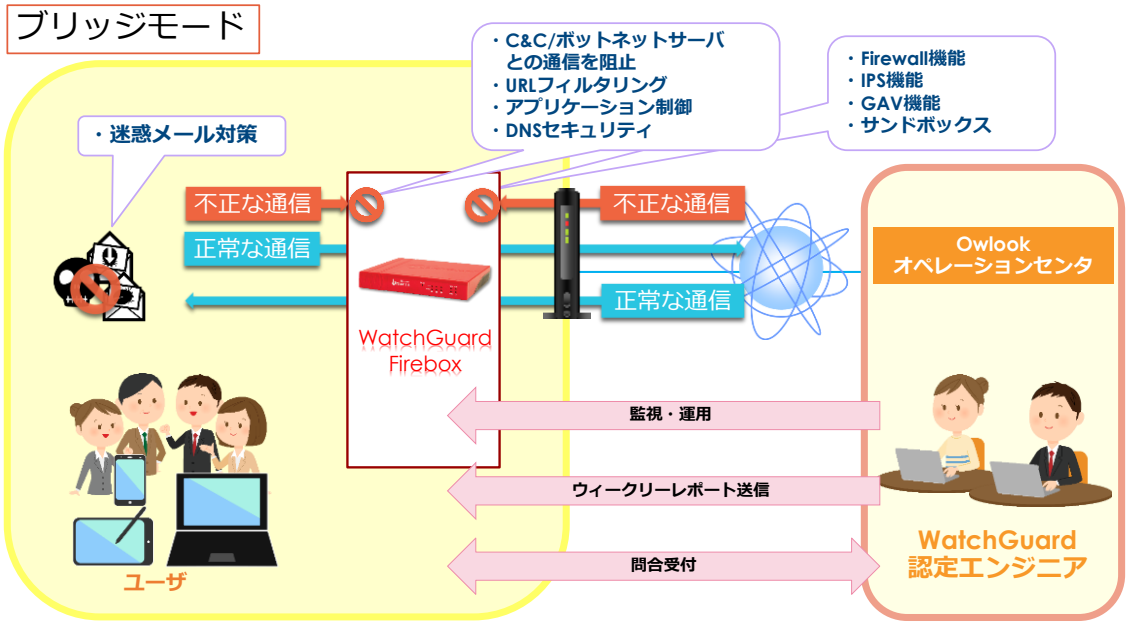
※UTM からサービス提供事業者の設備へ定期的にログを送信いたします。

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 にはお客様環境の DHCP により自動的に IP アドレスが割り振られます。

WAN インタフェース（0 番）	・・・	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（1 番）	・・・	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。
管理インタフェース（2 番）	・・・	緊急時に UTM へ接続するための管理用として使用いたします。お客様は通常使用できません。 ※お客様 LAN 環境が DHCP の場合、「10.0.1.1/24」が設定されています。

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	毎週日曜日		メールにて送付
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
構成管理		UTM 設定内容を最大 10 世代まで保管	
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
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 WatchGuard 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	プラン	
		Basic	Total
ステートフル Firewall	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。	○	○
侵入検知／防御（IPS）	既知の攻撃をシグネチャベースのセキュリティ対策で防御します。	○	○
レピュテーションセキュリティ&ボットネット検知	ネットワークから出ていくトラフィックをモニターし、評価の悪い Web サイトや 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（WebBlocker）	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。有害なサイト（危険なコンテンツを含むサイト、アダルトサイト）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。	○	○
アプリケーション制御（Application Control）	P2P アプリケーション、ランサムウェアに関連するアプリケーションをブロックします。	○	○
迷惑メール対策（spamBlocker）	言語、内容、フォーマットに 関わらず迷惑メールを認識し、スパムメールを警告（Subject にスパムマーカを付与）します。	○	○
ゲートウェイアンチウィルス（Gateway AntiVirus）	メール添付ファイル及び Web サイト、FTP サーバ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。 ※SSL/TLS で暗号化された通信は検査しません。	○	○
標的型攻撃対策サンドボックス（APT Blocker）	ランサムウェア、ゼロデイ脅威などの複雑な攻撃や回避型の攻撃を検出しブロックします。		○
DNS セキュリティ（DNS Watch）	悪意のある DNS 要求を検出してブロックします。		○

（2）セキュリティ機能詳細

① ステートフル Firewall

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、1 つのファイアウォールルールが一致すると、以降の他のルールはすべて無視されます。Default Threat Protection 機能により、受信したパケットの発信元及び宛先を調査し、SYN フラッド攻撃、スプーフィング攻撃、ポートスキャン等の攻撃から保護します。

※QUIC プロトコル（UDP80 番、443 番）は拒否しています。

② 侵入検知／防御（IPS）

継続的に更新されるシグネチャを使用して全ての主要プロトコルのトラフィックをスキャンすることで、スパイウェア、SQL インジェクション、クロスサイトスクリプティング、バッファオーバーフローなどのネットワークの脅威からリアルタイムに保護します。ただし、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。

③ レピュテーションセキュリティ&ボットネット検知

Web サイト(URL)に「良」「悪」「不明」のスコアを付ける評判チェックを利用して、セキュアなウェブブラウジングを実現します。評価スコアが明白に悪い URL への接続は即時に遮断します。また、既知のボットネットサイト IP アドレスもリスト化されているので、パケットレベルでこれらのサイトをブロックできるようになります。

④ URL フィルタリング（WebBlocker）

常時更新されるデータベースを使用することにより、WebBlocker は悪意のあるサイトへのアクセスをブロックし、スパイウェア、ファーミングおよびフィッシングサイトなど危険な Web コンテンツからネットワークを保護します。また、カテゴリ毎の Web サイトへのアクセスも制御できます。本サービスでは前述にあるような危険なコンテンツを含むサイトとアダルトに分類されるサイトをブロックします。

⑤ アプリケーション制御（Application Control）

ネットワーク上で稼動するアプリケーションを制限します。本サービスでは P2P アプリケーション、ランサムウェアに関連するアプリケーションからの外部へのアクセスを遮断する事によってネットワークが危険にさらされる事態を防ぎます。

⑥　迷惑メール対策（spamBlocker）

受信される E メールに対してスパムスキャンを提供します。メッセージ中の単語を評価するのではなく、迷惑メール発生の重要な特徴を評価するので、メールの言語やフォーマットにかかわらず迷惑メールを特定することができます。POP3（110 番）、IMAP（143 番）の受信メールをスキャン対象としており、これらのポート番号と異なる場合は監視できません。スパム検知されたメールは件名にマーカを付けそのまま受信します。

⑦　ゲートウェイアンチウィルス（Gateway AntiVirus）

HTTP、FTP、SMTP、POP3 などの標準的なプロトコルにおいて、断続的に更新されるシグネチャを活用して、既知のスパイウェア、ウイルス、トロイの木馬、ワーム、ローグウェアはもちろん、既知のウイルスの亜種も含め、複合型の脅威を識別しブロックします。マルウェアスキャンの最大スキャンサイズは送受信ともに 10MB です。SMTP、POP3 でマルウェアファイルが検知された場合は、検知内容を記したファイルへと置き換えてメールを配信します。本サービスでは SSL/TLS で暗号化された通信は検査しません。

⑧　標的型攻撃対策サンドボックス（APT Blocker）

実績豊富な次世代型サンドボックスにより、ランサムウェア、ゼロデイ脅威などの複雑な攻撃や回避型の攻撃を検出しブロックします。

⑨　DNS セキュリティ（DNS Watch）

悪意のある DNS 要求を検出してブロックし、セキュリティベストプラクティスを提供する安全なページにユーザーをリダイレクトします。

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	レベルの高いアラートを検知した際に、申込書記載の通知先メールアドレスへ通知します。
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）等をお客様へ毎週日曜日にメール送信します。
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。
構成管理	UTM の設定情報を最大 10 世代まで保管します。
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（平日 9:00~17:00 対応）
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

UTM からサービス事業者側の管理システムに定期的にログが送信されています。定期的なログの送信が確認されない場合、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

URL フィルタリングの機能でボットネットの C&C（コマンド＆コントロール）サーバへのアクセスを検知した際、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

UTM からサービス事業者側へ送信されたログをもとにレポートを作成し、利用者に対してレポートを毎週日曜日にメール送信します。初回のレポートのみ、初期構築作業時の通信ログを含んだ状態で作成されますが、ご了承ください。なお、ログ記録は過去 30 日間分の保管になります。

④ 各種設定変更

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 構成管理

構成管理としてサービス提供事業者側で UTM の設定内容（コンフィグファイル）を最大 10 世代、5MB の容量まで保管します。 1 世代分のコンフィグファイルの大きさにより保管できる世代数は変わります。

⑥ 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。

⑦ 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。

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にて通知後に実施します。

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 営業部門 営業部	受付時間	平日 9:00~18:30
	連絡先	03-5295-8800
	メール	contact-nw@koan.co.jp

◇サービス開始後のお問合せ（販売パートナー企業様・利用者様向け）

受付窓口	内容	
ICT 技術サービス部門 Owlook オペレーションセンタ	受付時間	24 時間 365 日
	連絡先	03-5295-3121
	メール	osms-support@koan.jp

４．注意事項

- UTM の運用中は定期的に各種メンテナンス作業が発生いたします。
- メンテナンス作業には UTM の再起動等一時的に通信断が発生する場合があります。
- メンテナンス作業時に UTM がお客様ネットワークに接続されていない場合、お客様に UTM の接続をお願いする場合があります。
- UTM からサービス提供事業者へ定期的にログが送信されます。ログはレポートの作成、UTM の監視、トラブルシューティング等に使用されます。
- お客様の LAN ネットワーク帯が「10.X.X.X」の場合は本サービスをご利用になれません。
- UTM はサービス提供事業者のログ送信や各種セキュリティ機能を維持するために（プロキシサーバ経由ではなく）直接インターネットへ接続する必要があります。そのため、お客様 LAN ネットワークに HTTP プロキシサーバがあり、LAN ネットワークからのインターネット接続が HTTP プロキシサーバ経由に限定されている場合、お客様インターネット環境を修正していただく場合があります。

別紙 1：通知メール例

・UTM 通信断発生の通知

送信元	osms-support@koan.jp
宛先	申込書記載の通知先メールアドレス
Cc	osms-support@koan.jp
件名	【異常通知】_ノード名
本文	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 ステータス：異常 UTM でアラートを検知しました。 機器の状態を確認の上、問題が御座いましたら、 Owlook オペレーションセンターまでご連絡ください。 -------------------------------- Owlook オペレーションセンター TEL： 03-5295-3121 E-MAIL： osms-support@koan.jp