統合脅威管理（UTM）アプライアンス

TM-BOX

TMB-2550／TMB-2530

進化するサイバー脅威に備える
スモールオフィスの
スタンダードソリューション

https://www.muratec.jp/ce/

様々なセキュリティー脅威からネットワークをガード

ファイアウォール

インターネットと社内ネットワークの間で通信を監視し、許可してよい通信以外はすべて遮断。ファイアウォール業界のパイオニアCheck Point社の特許技術「ステートフル・インスペクション」により、通信のヘッダー情報だけでなく通信制御まで検査し、「なりすましパケット」などの偽装侵入もしっかり防ぎます。

IPS（侵入防止）

悪意のあるコマンドや有害な実行コードなどが通信に含まれていないか解析し、ウイルスやDoS攻撃といった不正アクセスをブロックします。OSやアプリケーションの脆弱性を狙って仕掛けられるゼロデイ攻撃に対しても有効です。

アンチウイルス

最新の脅威情報を世界中の情報源から収集しているCheck Point社のナレッジベース「ThreatCloud™」で、ウイルスやランサムウェア、ワーム、トロイの木馬といったマルウェアや不正サイトを検出。ネットワークの入口で遮断して侵入を防ぎます。

アンチスパム

メールの送信元が悪意のあるIPアドレスではないか、また既知のスパムメールのパターンと一致していないかをデータベースで照合し、高精度なスパム判定を行います。個別に許可/拒否リストも作成できるので、よりきめ細かいフィルタリングも可能です。

※ POP3sによる暗号化通信は検査対象外です。

アプリケーション制御&URLフィルタリング

業界最大規模のライブラリを活用して、ネットワーク内部からの悪意のあるアプリケーションや不正サイトへのアクセスを規制します。ボットネットやフィッシングなどの高リスクアプリケーションは初期設定でブロック。また特定のアプリケーションやWebサイトのアクセス許可/ブロックも個別に設定できます。

アンチボット

PCに侵入して外部の指令元からの遠隔操作でネットワーク内部のデータを盗み出したり、侵入したPCからスパムメールを大量送信するなどの二次攻撃を行う「ボット」プログラム。
アンチボット機能ではボットの指令元をデータベースから判別し、通信パターンを解析して感染PCを検出。指令元への通信を遮断して遠隔操作を阻止します。

Threat Emulation（サンドボックス） TEモデル

送信されてきた対象ファイル※をネットワークの入口で一旦止めて、不審と判定されると「ThreatCloud™」に送信。仮想環境で実行させて、不正な動作を検知したら即座にブロックし、ネットワークへの侵入を防ぎます。未知の脆弱性を狙ったゼロデイ攻撃や標的型攻撃による被害を防ぐのに有効です。

※ 初期設定：pdf、doc、docx、xls、xlsx、ppt、pptx

CHECK POINT

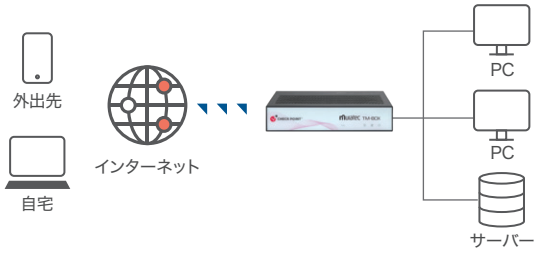
チェック・ポイント・ソフトウェア・テクノロジーズ社は、インターネットセキュリティーにおけるトップ企業として妥協のないセキュリティー機能を実現。ネットワークセキュリティー製品の元祖であるFireWall-1と特許技術のステートフル・インスペクションを開発した、業界きってのリーディングカンパニーです。

安心・快適なネットワーク運用を支える充実の機能

外出先から安全にリモートアクセス

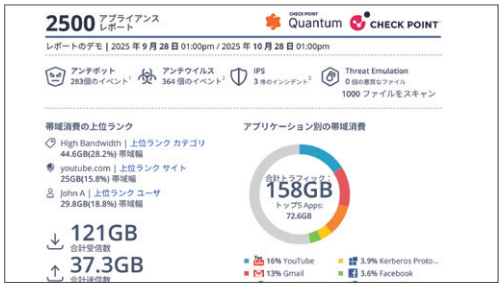
自宅や外出先のモバイル端末から社内ネットワークにVPNで安全に接続できるリモートアクセスVPN機能を標準搭載。社外にいても社内にいるのと同じ感覚でネットワーク内の機器にアクセスできるので、テレワークにとても便利です。

※ 本機能の利用にはルーターモードで接続する必要があります。
※ 本機能の利用可能期間は製品ライセンス期間に準じます。



セキュリティーレポート

TM-BOXの稼働状況をいつでもWeb画面上で確認できます。阻止したマルウェアの詳細やボット感染PCなどの情報に加え、よく利用するアプリケーションやWebサイトの状況も分かるので、不要なサイトへのアクセス制限をかける判断材料としても利用できます。



IPv6回線サービス対応

幅広いIPv6 IPoEおよびIPv4 over IPv6（DS-Lite/IPIP/MAP-E）接続サービスに対応。IPv6対応ルーターを個別に設置する必要なく、シンプルな構成でIPv4/IPv6両環境でのセキュリティー検査が可能です。

※ 対応VNE事業者の情報は弊社ホームページをご確認ください。

Fast Accel機能

動画ストリーミングやWeb会議など信頼性の高いサービスへの通信を検査対象から除外することで、機器の負荷を低減しパフォーマンスを向上させます。また特定端末のMACアドレスを除外指定することも可能です。

※ 初期設定：有効
※ 対象サービス：動画ストリーミング（Youtube、Netflixなど）、大手コーポレートサービス（Microsoft、Googleなど）、SNS（Facebookなど）、Web会議（Zoom、Webexなど）（2025年11月時点）

SSLトラフィックインスペクション

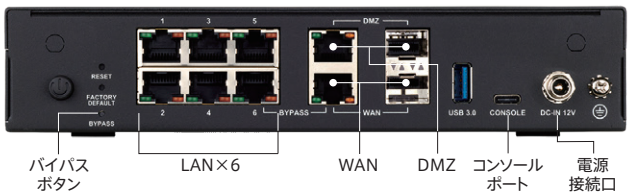
httpsで構成されたWebサイトへの接続やファイルダウンロード、POP3sやIMAP4sによるメール受信など、SSL/TLS暗号化された通信も検査対象とすることができ、通信内に潜む様々な脅威を検知、遮断します。

※ アンチスパム機能は対象外です。
※ 暗号化通信の解析処理を行うため、環境により処理負荷が増す場合があります。

バイパス機能

本機能をアクティブに設定することで、TM-BOXの電源やソフトウェアに異常が発生した際でもWANポートとLAN6ポート間の通信経路を確保します。UTMを経由せず一時的にネットワークを通過させることで、通信障害の切り分けや復旧作業の際に役立ちます。

本体インターフェース



製品構成

モデル	ライセンス期間		Threat Emulation機能※1
TMB-2550	5年	6年	ー
TMB-2550TE	5年	6年	標準
TMB-2530	5年	6年	ー
TMB-2530TE	5年	6年	標準
オプション品			
1年延長ライセンス※2			

※1 標準モデルにThreat Emulation機能を後日追加することはできません。
※2 脅威対策機能を最新状態に維持するライセンスを1年延長するオプション。6年ライセンスモデルには適用できません。

主な仕様

	TMB-2550	TMB-2530
テスト環境におけるパフォーマンス		
脅威対策スループット※1	1,000 Mbps	750 Mbps
パフォーマンス(RFC3511,2544,2647,1242 に基づくラボ・テスト環境)		
ファイアウォールスループット 1518 bytes UDP	4,000 Mbps	3,000 Mbps
VPNスループット AES-GCM 1452 bytes	1,400 Mbps	1,400 Mbps
秒間セッション接続数	20,000	16,000
同時セッション接続数	1,000,000	
リモートアクセス数(同時接続ユーザー数)※2	100	
ハードウェア		
WAN	1000BASE-T RJ45 / SFP x 1	
DMZ	1000BASE-T RJ45 / SFP x 1	
LAN	1000BASE-T RJ45 x 6	
コンソール・ポート	USB-C x 1	
USBポート※3	USB3.0 x 1	
大きさ	幅210mm x 奥行き170mm x 高さ42mm	
質量	0.87 kg	
環境要件		
電源	AC100V(50/60Hz)	
最大消費電力	26.01W	
動作環境	温度0～40℃、湿度5～95%(結露なきこと)	

※1 すべての脅威対策機能(Threat Emulation含む)をONにした状態での実効値
※2 環境によって接続数が低減する場合があります。
※3 ファームウェアの更新等に使用

TM-BOX の詳しい情報はこちら
www.muratec.jp/ce/products/network/tmb2550_2530/

⚠ ご使用上の注意
●ご使用の際は、取扱説明書をよくお読みのうえ正しくお使いください。
●水・湿気・ほこり・油煙等の多い場所、屋外、振動の多い場所、不安定な場所などには設置しないでください。故障や感電、火災の原因になることがあります。

村田機械株式会社 情報機器事業部
ムラテックフロンティア株式会社
本 社／営業本部
〒612-8686　京都市伏見区竹田向代町136
TEL. 075(672)8136
https://www.muratec.jp/ce/

お問い合わせ先:

製品の仕様・操作方法やアフターサービスに関するご相談は
インフォメーションセンター
フリーダイヤル **0120-610-917**
※ 電話番号をお間違えないようにご確認の上おかけください。

※このカタログの記載内容は2025年11月現在のものです。
KATM25-5115112002VT