WatchGuard®

進化するセキュリティ対策を
より安全で、シンプルに

Smart Security, Simply Done.

ウォッチガード・テクノロジー・ジャパン株式会社

ウォッチガードの使命:

それはサイバー攻撃からビジネスを**「守り抜く」**こと。

現代のビジネスはオンラインのネットワーク抜きでは考えられません。本社をはじめとして支社／支店、店舗、校舎、自宅、提携先、データセンター、あるいはノートPCやタブレット、スマートフォンなど、あらゆる拠点や個人デバイスがつながり、膨大な量の機密情報や個人情報がやり取りされています。

また今日、リモートワーカーが急増しており、勤務地が分散化しているため、攻撃対象領域が拡大しています。こうした環境の中、ランサムウェアやボットネットなどサイバー攻撃も多様化、巧妙化しており、不正アクセスが多発しています。このように、現在では有線無線を問わず、すべてのゲートウェイとエンドポイントに対して、外部や内部からの攻撃を未然に阻止する事前対策、並びに被害の拡大を防止する事後対策が求められています。ウォッチガードは包括的な情報セキュリティのプロフェッショナルとして、こうしたサイバー攻撃による「情報漏えい」や「業務停止」による被害／損失を防ぐことを使命としています。

Unified Security Platform (USP)

ウォッチガードの統合型セキュリティプラットフォーム

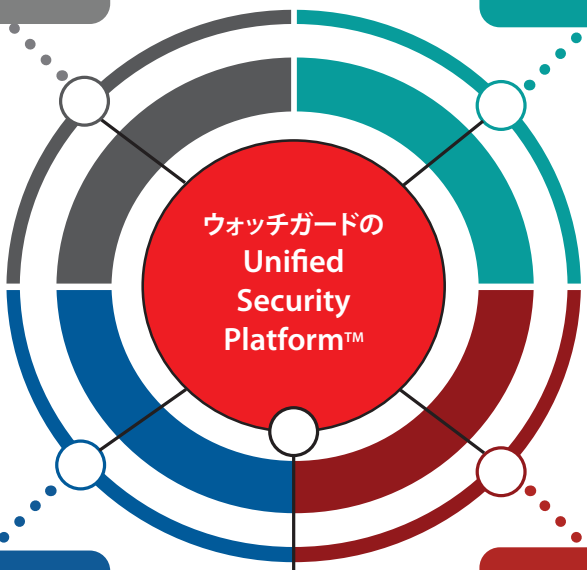
運用効率を高めつつ、拡張性とスピードを向上させる強力なセキュリティサービスを実現します。

包括的なセキュリティ

環境、ユーザー、デバイスを保護するためのエンドポイント、多要素認証、ネットワークセキュリティ製品／サービスの総合ポートフォリオ

明確な管理と制御

WatchGuard Cloud による一元的なセキュリティポリシー管理、可視化、高度なレポート機能



ニーズに応じた運用拡張

API連携、テクノロジーパートナー製品とのエコシステム連携、および合理化されたポイント消費システムモデルによる効率運用

ナレッジ共有

ゼロトラストセキュリティを採用し、ThreatSyncによる脅威の検知と修復のための真のXDRベースのアプローチを展開するための完全統合プラットフォーム

自動化

単一のプラットフォームに統合された複数のサービスで様々なタスクを自動化することで、セキュリティ機能の提供、配信、管理などあらゆる側面を簡素化

なぜウォッチガードなのか?

ウォッチガードの統合型セキュリティソリューションは、Unified Security Platform（USP）を基盤として、WatchGuard Cloudによる一元管理の元、**「ネットワークセキュリティ」、「多要素認証（MFA）」、「セキュアWi-Fi」、「エンドポイントセキュリティ」**の4つを柱を基盤として、あらゆる攻撃対象領域をカバーしています。

ウォッチガードの統合型セキュリティソリューション体系図

Unified Security Platform

WATCHGUARD CLOUD

管理：顧客や拠点単位など、マルチティア／マルチアカウント方式でアプライアンスを管理し、多要素認証やエンドポイント製品も一元管理できます。
* DNSWatch/DNSWatchGO は現在管理対象外

可視化：豊富なレポート機能でネットワークの利用状況やセキュリティトレンドを把握できます。

ネットワークセキュリティ

既知／未知にかかわらず、あらゆる脅威に対応するエンタープライズクラスの多層防御機能により、巧妙化する脅威を強力に防御し、鉄壁のゲートウェイで社内ネットワークを保護します。

ファイアウォールアプライアンス（OS: Fireware）

Firebox T Series
- NV5
- T25/T25-W
- T45/T45-POE/T45-W-POE
- T85-POE

Firebox M Series
- M290
- M390
- M590
- M690
- M4800
- M5800

仮想アプライアンス
- FireboxV
- Firebox Cloud

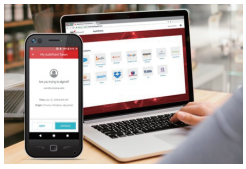
セキュア Wi-Fi

有線ネットワークだけでなく、無線 LAN のセキュリティも確保します。アクセスポイントは全モデルがクラウド管理型であり、セキュアでスケーラブルな無線 LAN の構築が可能です。

Wi-Fi 6 アクセスポイント
- AP130
- AP330
- AP432
- AP332CR
- AP430CR

多要素認証（MFA）

今では 1 つの認証方法は脆弱であり、認証手段を複数用意することにより、社員 PC のログイン情報の窃取による機密データへの不正アクセスを見抜き、回避することができます。



専用スマホアプリ／トークン
- AuthPoint

エンドポイントセキュリティ

エンドポイントへの高度なサイバー攻撃に対する防御、検知、レスポンスや高機能レポート、パッチ管理、フル暗号化、DNS セキュリティなど、ゼロトラストのアプローチで端末を保護します。

シングルエージェント
- WatchGuard EPP
- WatchGuard EDR
- WatchGuard EPDR
- Advanced Reporting Tool
- Patch Management
- Full Encryption
- DNS WatchGO
- Panda Security 製品

オンプレミス管理／可視化ツール：WatchGuard Dimension

パッケージソリューション：WatchGuard Passport（P12）Total Security Suite、Basic Security Suite、Standard Support（P14）

独自OSに統合されたベストオブブリードのセキュリティ技術

ウォッチガードの独自OSであるFireware上で、最新の技術を駆使したベストオブブリードの各種セキュリティ機能が1台のアプライアンスに統合されています。

モジュール形式を採用しており、必要に応じて各機能のライセンスを購入することですぐに利用開始できます。ウォッチガードのUTM（統合脅威管理）/NGFW（次世代ファイアウォール）アプライアンスは容易に設定・管理することができ、SOHO、中小中堅企業、大企業といったあらゆる規模の組織に対応しており、それぞれ適正なアプライアンスが用意されています。また、仮想環境やモバイル無線LAN環境にも対応しており、包括的かつ柔軟性に富んだ情報セキュリティソリューションの実現を支援しています。

Fireboxアプライアンス

Firewareセキュリティ機能

Gateway AntiVirus

ゲートウェイアンチウイルス

ウイルス、ワーム、トロイの木馬、スパイウェア、アドウェアなどのセキュリティの脅威を最新のシグネチャとヒューリスティックエンジン及び最新の振る舞いベースのスキャニングでブロックします。シグネチャの自動更新により最新のウイルスにも対応。ZIP、RAR、TAR、GZIP、ARC、CABなどの圧縮ファイルのスキャンも実行し、高速なネットワークパフォーマンスを実現します。

IntelligentAV

インテリジェントアンチウイルス

進化するマルウェアからの保護を実現する強力なマシンラーニングエンジンを備えており、クラウド接続、シグネチャ、または行動分析を必要とせずに、評価済みの数学的統計モデルを使用して、ネットワークに侵入しようとするマルウェアを撃退します。シグネチャの定期的なアップデートが困難となるクローズの環境においても安全性を確保します。Firebox T40/80およびM270以上の現行モデルの場合、Total Security Suiteを購入することで、BitdefenderとCylanceのデュアルスキャンエンジンを実装可能です。

WebBlocker

Webフィルタリング

業務に関係のないWebサイトへのアクセスを規制•管理し、生産性を高めるとともに、ウイルス感染や情報漏えいなどを未然に防ぎます。130以上のブロックカテゴリとサブカテゴリから選択し、HTTPとHTTPSの両方でフィルタリングします。出口対策として、C&Cサーバやボットネットなどを含む、危険なサイトへのアクセスをブロックします。ホワイトリスト/ブラックリストでのカスタマイズ、カテゴリ単位でユーザ/グループへの制御スケジュール機能に対応しています。

spamBlocker

迷惑メール対策

有害なスパムメールをリアルタイムで拒否及び検知し、マルウェア感染を未然に防ぎます。迷惑メールを一掃することで、日々の業務効率を高め、ネットワークインフラにかかる負荷を軽減します。世界的に広く導入されている検知エンジンを採用し、高い検知率で不要メールを拒否及び検知することができます。

IPS: Intrusion Prevention Service

不正侵入検知•防御

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脆弱性を突くあらゆるネットワーク攻撃をブロックします。シグネチャアップデートを常時行うことで最新の脅威にも対応し、TCP、UDPの主要プロトコルをすべてスキャンします。また、攻撃元として識別されたIPアドレスを自動的にブロックします。

Application Control

アプリケーション利用の可視化と制御

アプリケーション利用を可視化し、不要なアプリケーションを制御し、禁止することができます。主要なアプリケーションに対応し、アプリケーション内の機能を個々に制御することもできます。(例:メッセンジャーのチャット機能は「許可」のまま、ファイル転送機能を「禁止」にする)。アプリケーション単位でユーザ/グループ への制御を可能にしたり、スケジュール機能により制御する時間帯を定めたりと柔軟なポリシー設定ができます。

Firewareセキュリティ機能

ThreatSync

相関分析、優先順位付け、レスポンス

Fireboxのネットワークセキュリティと、新たに追加されたホストセンサによるエンドポイントセキュリティ機能により脅威を検知するとともに、個々の脅威情報をクラウドで相関分析およびスコアリングすることにより、脅威の早期発見、インシデントレスポンスの自動化が可能となります。

APT Blocker

標的型攻撃対策

ウイルス対策や不正侵入検知などシグネチャ型のセキュリティ対策で対応が困難な未知のマルウェアを、クラウド上のサンドボックスと連携することで検知/ブロックします。先進のフルシステムエミュレーションによるサンドボックス技術を活用した詳細な検知プロセスにより、高度な技術を持つ悪質なマルウェアによる攻撃を阻止します。

Reputation Enabled Defense

レピュテーションセキュリティ(RED)

クラウドベースのWebレピュテーション(評判照合)サービスとして、アンチウイルスエンジンを含む複数のソースから情報を収集し、サイト毎のレピュテーションにより、Webサイトからのリアルタイム保護を実現します。ポイントに応じて、トラフィックをクラウド上にて判定し、ブロック/バイパスが可能で、アプライアンス負担を軽減、パフォーマンスを最大50%高めます。

Botnet Detection

ボットネット検知

ボットネットを利用した不正行為から守り、DoS攻撃、スパム/ウイルスの送信、機密情報の漏えいなどを阻止します。ボットネットサイトリストはIPアドレスベースでリアルタイムに更新され、HTTP/HTTPSだけでなく、すべてのポートとプロトコルに対応しており、送信先IPアドレスと送信元IPアドレスの両方をチェックします。

DNSWatch

DNSWatch

アウトバウンドのDNSリクエストを監視し、悪意のあるサイトのリストとの照合を行い、既知の不正なドメインへの接続を防止します。悪意あると判断されたリクエストはブロックされ、安全なページにユーザをリダイレクトします。DNSWatchは接続の種類やプロトコル、ポートにかかわらずクリックジャック攻撃やフィッシングサイトへの誘導からユーザを保護します。

包括的なソリューション
多彩なニーズにお応えする各種先進機能をご用意しています。

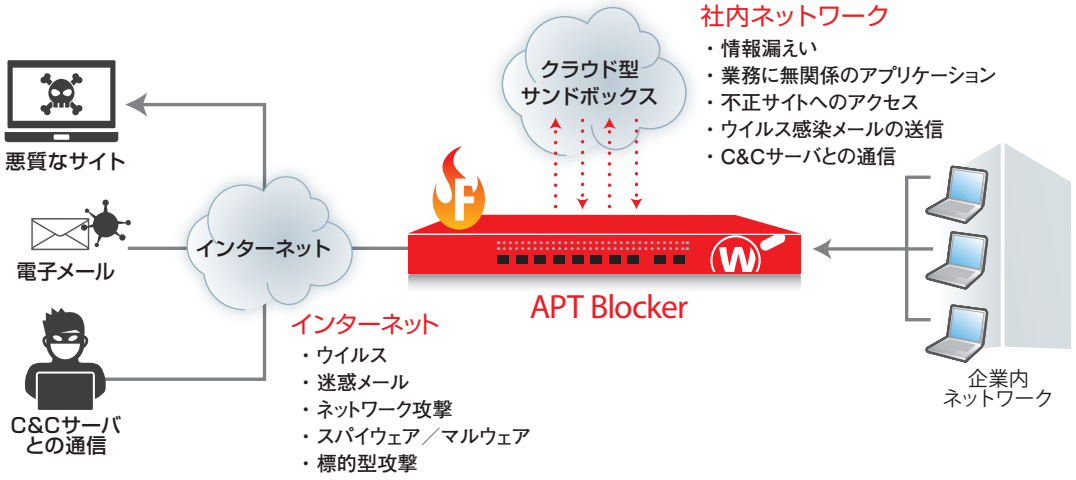
Solution1 変異し続ける悪質マルウェアからの防御

現代では、攻撃者はシグネチャベースのセキュリティ対策を容易にすり抜ける変異型やゼロデイ攻撃※を利用したマルウェアを利用し、さまざまな手段で企業情報へのアクセスを試みるため、従来のウイルス対策やスパムメール対策などの単体の製品だけで防御することが難しくなっています。企業のIT環境は、直接の攻撃対象となるリスク以外に、関連企業への踏み台にされ、知らぬ間に加害者になっている可能性もあり、すべての企業に対策が必要となっています。

※ ソフトウェアの修正情報、シグネチャが用意できていない脆弱性への攻撃

UTM/NGFWによる多層防御／APT Blockerによる標的型攻撃対策

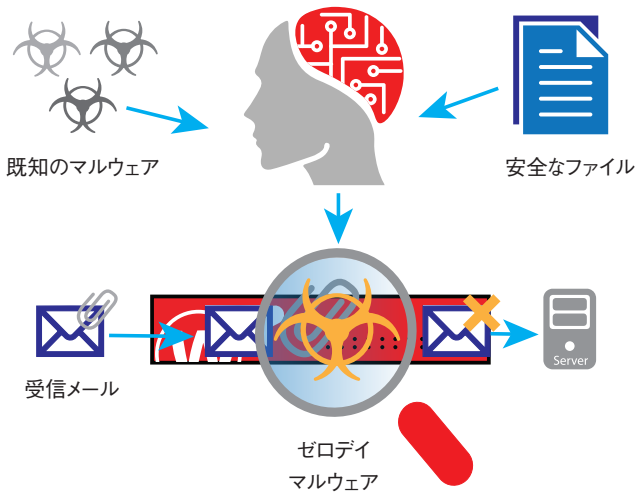
- APT Blocker: 標的型攻撃やゼロデイアタックを検出する業界で最も洗練されたセキュリティプラットフォーム
- シグネチャによる既知のマルウェア検知に加え、ファイル内部に埋め込まれた行動を詳細に分析し、回避行動をとる巧妙なマルウェアも的確に検出
- クラウドベースの次世代型サンドボックスと連携し、ファイルの正確なコード分析により標的型攻撃につながる脅威を検出



IntelligentAV（AIによるマルウェア対策）

- 強力なマシンラーニングエンジンを活用し、進化するマルウェアに対する予測ベースでのプロアクティブな防御
- インターネットに接続する前にマルウェアを検知、防御（シグネチャやクラウド接続に依存しない）
- Fireboxにおけるマルウェア検知に、新たな強力なレイヤーを追加し、多層防御をさらに強化

IntelligentAVの仕組み

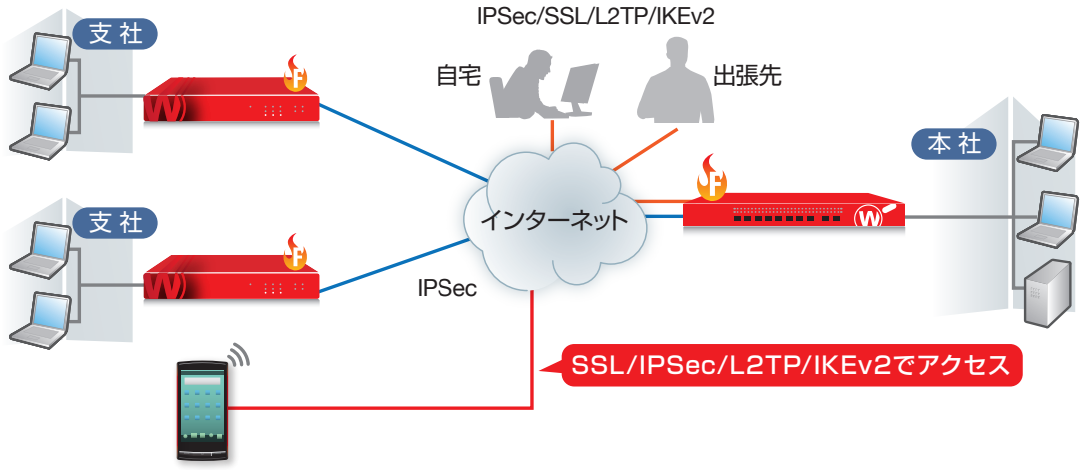


Solution2 拠点間の安全かつ高速な接続

インターネットが必須となるすべてのビジネスにおいて、回線コストの削減とセキュリティ対策の実現は大きな課題となっています。このような課題の解決手段としてインターネットを専用線のように使用することのできるVPN接続は、多くの企業で導入されています。

WatchGuard VPN（Virtual Private Network）ソリューション

- 複数のVPN機能を搭載しており、回線コスト削減に大きな効果を発揮し、セキュアで高速なVPNネットワークを構築
- 洗練された管理インターフェイスにより、ドラッグ&ドロップで簡単にVPN設定が可能なため、複数の複雑なVPNトンネルの作成も容易で管理者の負荷を軽減
- オフィスとビジネスパートナー間で安全なネットワーク通信を実現し、ウォッチガードのアプライアンスとIPSec対応デバイスの間で暗号化されたトンネルを柔軟に作成

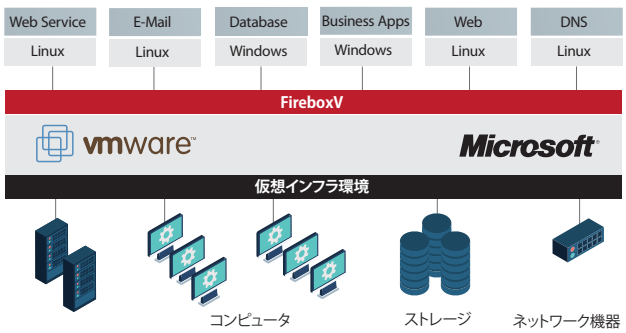


Solution3 仮想環境への導入と効率的な運用

様々な業種・規模の企業が仮想化技術により、ハードウェアや運用コストを削減しています。さらに、物理的な制約、電気容量の削減要求、発熱量の制限などにより、ネットワーク機器やセキュリティアプライアンスにも仮想アプライアンスを利用するケースが増えています。しかし、多くの管理者は運用方法やパフォーマンスの違いを懸念しています。それに対し、ウォッチガードの仮想アプライアンスでは、ハードウェアアプライアンスと同レベルの高いセキュリティ機能、共通の管理機能を提供できるため、安心して導入をご検討いただけます。

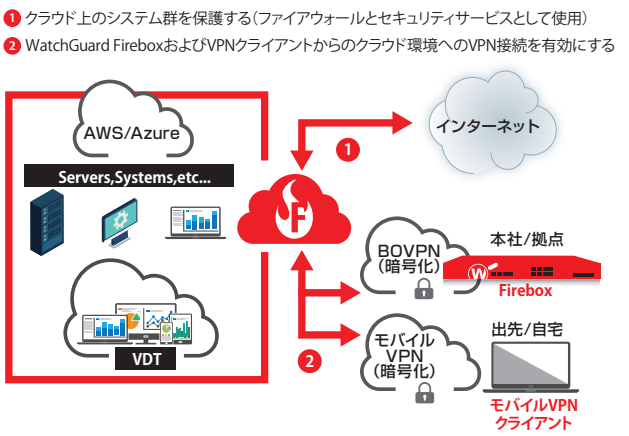
WatchGuard FireboxV（仮想アプライアンス）による仮想環境への対応

- ハードウェアアプライアンスと同様に高いセキュリティ機能と共通の管理機能を提供
- 共通のセキュリティ機能や管理機能に加え、柔軟な導入方法により管理者の負荷を軽減
- ホスティング、クラウドなどのサービスプロバイダによるFireboxVインスタンスをセキュリティサービスとして提供



クラウド環境へ対応した仮想アプライアンス WatchGuard Firebox Cloud

- AWS（Amazon Web Services）、Microsoft Azure環境に合わせたセキュリティ機能と管理機能を提供
- 一部の機能を除き、ハードウェアアプライアンスと同様に高いセキュリティ機能と共通の管理機能を提供
- クラウド上のサーバ群、各種システム、DBなどのセキュリティを確保

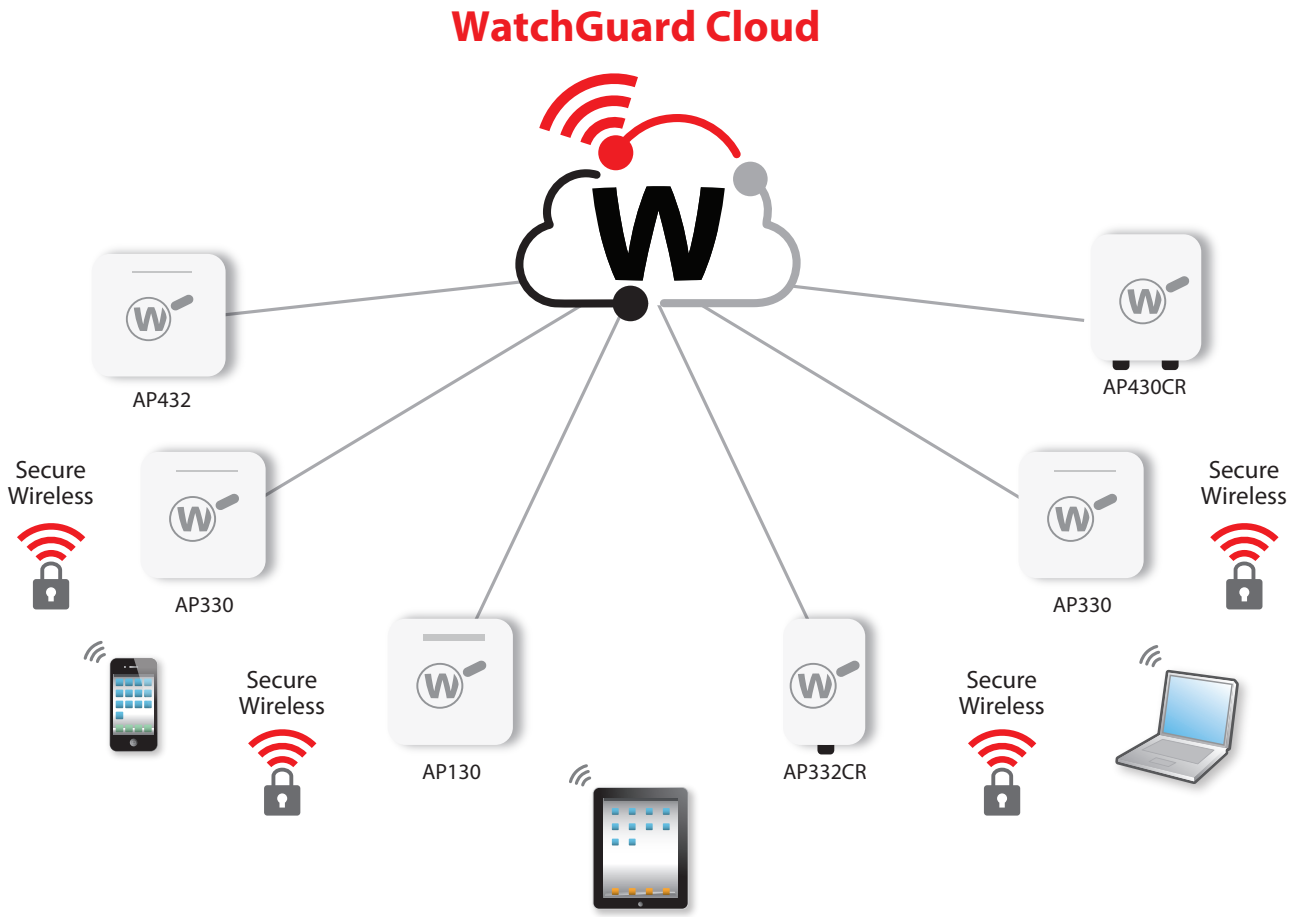


Solution4 セキュアWi-Fi：安心して無線LANに接続

場所を問わないワーキングスタイルの普及により、ノートPC、タブレット、スマートフォンなど多くのデバイスが無線LANネットワークにつながっており、今ではオフィス内や在宅でさえもWi-Fi接続が主流になっています。また、社内管理が十分に行き届いていないBYOD（個人所有デバイス）も増加しており、セキュリティリスクがこれまでになく高まっています。

WatchGuard Cloudを活用したクラウド管理型のセキュアな無線LANソリューション

- 一元管理が可能な専用アクセスポイント（AP）をラインナップ
- 最新世代のWi-Fi 6と強力なWPA3暗号化を採用
- セキュリティベンダーならではの有線と同様のセキュリティを実現
- 統合型プラットフォーム上で容易に導入、設定、レポーティング
- 複数のロケーションにわたり1台のアクセスポイントから無制限に拡張管理
- ロケーション、ビル、フロア、顧客、リモートユーザー単位など、アクセスポイントを多様な方法でグループ化
- 分散型ネットワークを横断して一貫したポリシーを適用



クラウドでセキュアな一元管理を実現

専用アクセスポイント（AP）

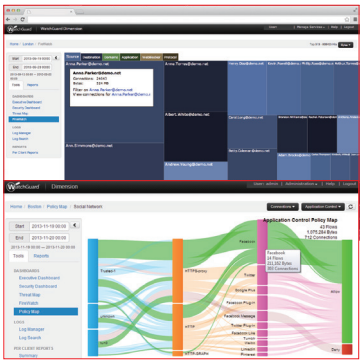
AP130	スモールオフィスやリモートワーク環境など、 低密度の屋内環境向けに最適化
AP330	中小企業や中堅企業など、中密度の屋内環境向けに最適化
AP432	大企業や大規模施設など、高密度の屋内環境向けに最適化
AP332CR	中規模施設など、屋外の過酷な環境や気象条件に最適化
AP430CR	大規模施設など、屋外の過酷な環境や気象条件に最適化

Solution5 ネットワークセキュリティの可視化（WatchGuard Dimension / Network Discovery）

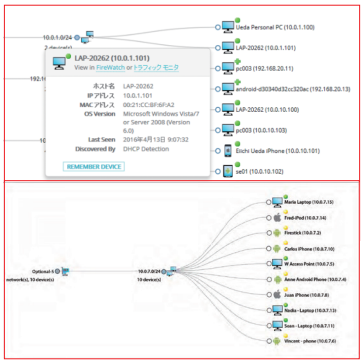
万が一、セキュリティの事故やマルウェアによる情報漏えいが発見されれば、企業の信頼性や収益にも大きな影響が出ます。セキュリティ管理者は常に企業ネットワーク内を監視し、不正なトラフィックを識別して迅速かつ的確な対処が求められます。

WatchGuard DimensionとWatchGuard Cloud Visibilityによるネットワークセキュリティの監視

- すべてのトラフィックをリアルタイムで分析し、ネットワークセキュリティの可視化と最適なセキュリティポリシーの策定を支援
- 豊富なレポーティング機能により、役職に応じたサマリおよび詳細レポートを生成
- クライアント端末情報、ユーザやアプリケーションの相関ビュー、ピンポイントのトレンド情報など、ネットワークアクティビティを高次元でビジュアル化
- 必要に応じて個別のログデータまで簡単にドリルダウンして確認



WatchGuard Dimension



Network Discovery

Network DiscoveryでFirebox配下の社内ネットワークを可視化

- 社内ネットワークに接続しているデバイスを探索し、Web UIにネットワークマップとして表示
- デバイス毎に次の情報を取得: IPアドレス、MACアドレス、OSおよびService Pack、デバイス/ホスト名、開放ネットワークポートおよび動作プロトコル

管理ソフトウェア

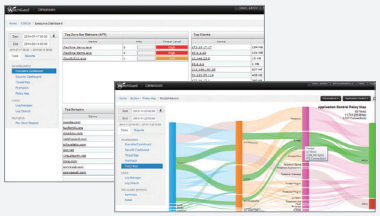
1. WatchGuard Dimension

セキュリティ対策にリアルタイムの可視化ツールで一歩先のインテリジェンスを実装

必須要件:ハイパーバイザ（VMware ESXi/Windows Hyper-V）仮想環境
Dimensionは仮想インスタンスとしてOVF/VHDファイル形式にて提供

WatchGuard Dimensionによるログ収集とレポート機能

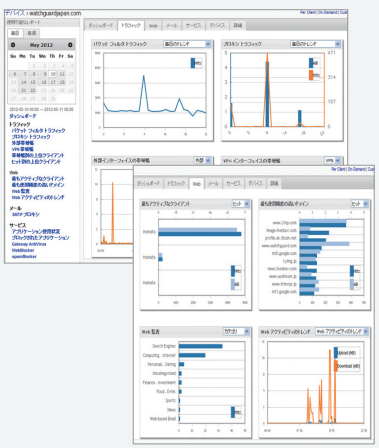
- 複数アプライアンスからのログを集約
- パブリック、プライベートクラウドに対応
- 100種類のレポート形式、エグゼクティブサマリーレポート
- FireWatchおよびThreatMapなどの可視化ツール
- HIPAA、PCIコンプライアンスの特別レポート
- SNMP v2 & v3、Syslog
- 暗号化されたログチャネル
- PDF/CSV形式レポートのメール送信



2. WatchGuard System Manager

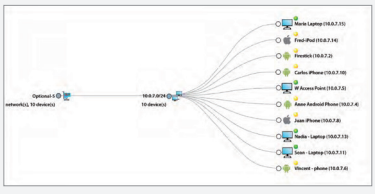
ネットワーク、セキュリティ、アプライアンス全ての設定・運用管理を支援する洗練された統合管理ツール

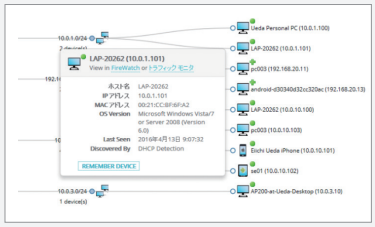
- アプライアンスに直接接続、スクリプトによるコマンドラインインターフェイス
- Webブラウザによる単一デバイスを管理するためのWeb UI
- 対話型でリアルタイムでのモニタリングとロギングを提供する中央コンソール
- ドラッグ&ドロップによるVPNの設定、豊富な履歴レポートの提供
- RapidDeployによる容易な設定と導入



3. Network Discovery

- 社内ネットワークに接続しているデバイスを探索し、Web UIにネットワークマップとして表示
- デバイス毎に次の情報を取得: IPアドレス、MACアドレス、OSおよびService Pack、デバイス／ホスト名、開放ネットワークポートおよび動作プロトコル、デバイスのapprove状況（承認／未承認）、Mobile Security機能によるコンプライアンス結果（モバイルデバイス）



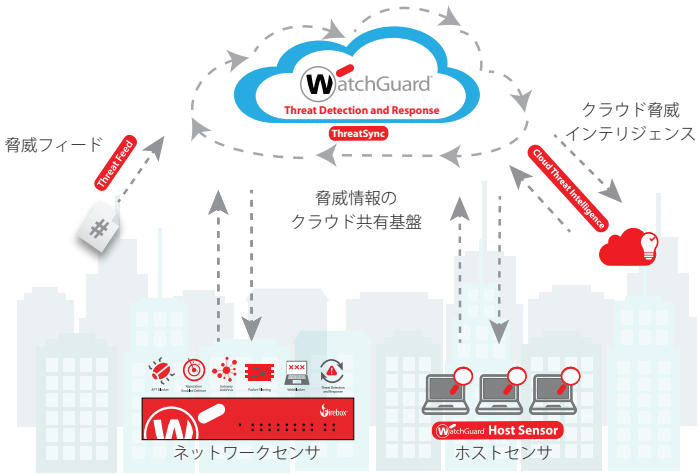


Solution6 相関分析、優先順位付け、レスポンス（ThreatSync：XDR）

サイバー犯罪者は、企業ネットワークにアクセスするために、あらゆる接続ポイントから様々な手法を複合的に駆使して複雑かつ高度な攻撃を行います。効果的なセキュリティ対策には、ネットワークとエンドポイント両方でのセキュリティ検知機能だけでなく、攻撃者の目的や活動も含めた相関分析が必要です。

ネットワークとエンドポイントイベントの相関分析

- 脅威情報のクラウド共有基盤であるThreatSyncにて、全脅威情報を集約、相関分析し、脅威を早期に発見
- ThreatSync上ではFirebox、ホストセンサ、脅威インテリジェンス等からの脅威情報を集約し、相関分析を行い、脅威をスコアリング
- ネットワークとエンドポイント全体におけるインシデントレスポンス能力を向上



可視化機能をエンドポイントまで拡張

- WatchGuardホストセンサにより、デバイスに負荷をかけることなく、脅威を監視および検知
- クラウドで一元管理されるため、MSSPやIT管理者はあらゆる場所から容易に更新・管理

高度なランサムウェア対策

- WatchGuardホストセンサに実装されているランサムウェアに特化したモジュール、Host Ransomware Prevention（HRP）を活用
- 挙動分析エンジンとデコイディレクトリ（ハニーポット）により、特定の動作や処理がランサムウェア攻撃に関連しているかどうか判別し、エンドポイントでの様々な特性を監視
- 悪意ある脅威と判定した場合に、ファイルが暗号化される前に自動的にランサムウェア攻撃を防止

インシデントレスポンスの自動化

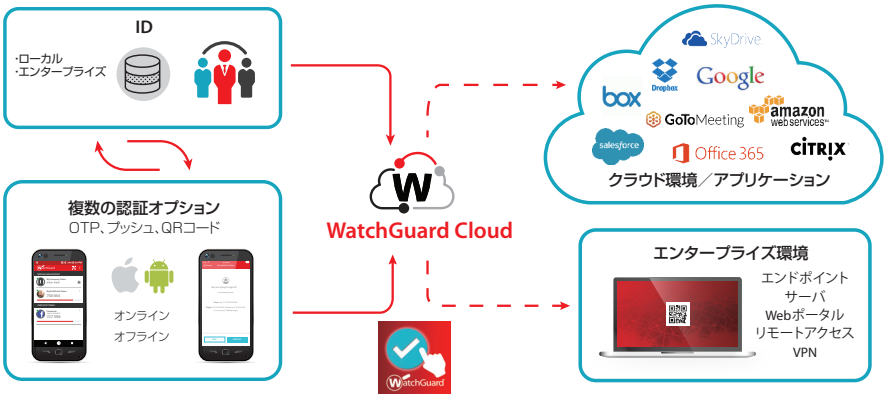
- 脅威情報のクラウド共有基盤であるThreatSyncには、ネットワークとエンドポイント全体の脅威情報が集約、相関分析され、脅威スコア生成により重大度をランク付け
- 分析の結果、ファイルの隔離、プロセス停止、レジストリ値の削除などの対応をホストセンサに指示
- 脅威を検知するまでの時間を短縮し、迅速なインシデントレスポンスを自動化

Solution7 クラウドベースの多要素認証（AuthPoint）

昨今の情勢下によりテレワークが普及する中で、攻撃者は企業が支給するPCもしくは個人用PCのログイン情報の窃取を通じて、企業の機密情報にアクセスしようとしています。こうした攻撃を防ぐには、認証手段を2種類以上に分散させることで認証を強化することが有効です。

モバイルアプリも利用可能なクラウドソリューション

AuthPointはクラウドベースのシンプルかつ強力な多要素認証ソリューションであり、VPN 、クラウドアプリケーション（SAMLベース） 、PC（Windows/Mac/Linux）ログイン時に認証強化を図ることができます。ユーザにとって馴染みのあるスマートフォンの専用アプリ（iOS/Android対応）およびウォッチガードやサードパーティのトークンを通じて利用することが可能です。



【ユースケース】

PCログイン - オンライン

- Windowsログオン認証に加え、Push通知による確認と承認のステップを追加。

クラウドアプリケーションのSSO

- IdPポータルにアクセスし、OTP/Push通知/QRコードのいずれかを使用して認証すると、連携しているすべてのアプリにシングルサインオンを実現。

VPN/リモートアクセス

- 通常のユーザー名とパスワードによる認証に加えPush通知に対する承認を義務付けてリモートアクセスをセキュアに。

PCログイン - オフライン

- Windowsログオン認証に加え、AuthPointアプリでQRコードをスキャンすることにより、オフラインでも多要素認証が可能。

Solution8 エンドポイントセキュリティ：末端のPCまで保護

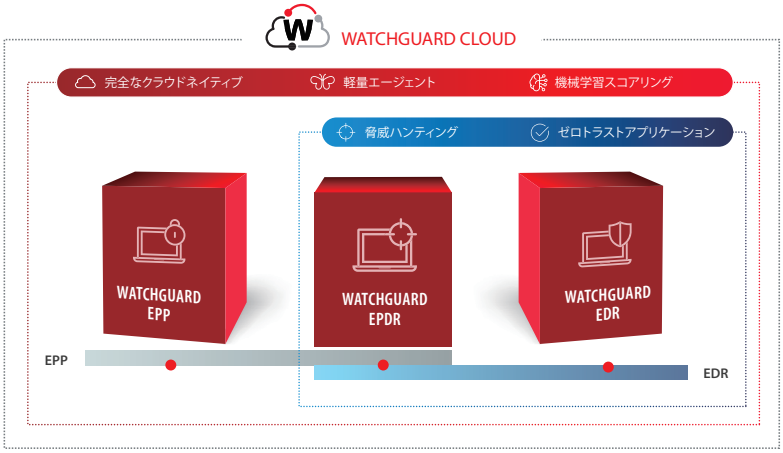
「ゼロトラスト」で高度な脅威に対する防御、検知、レスポンス（WatchGuard EPP/EDR/EPDR）

攻撃者は主にエンドポイント（個人が利用するPCやモバイルデバイスなど）を標的として脅威を拡散しようと試みています。昨今の攻撃は巧妙化、複雑化しており、常にエンドポイントの状態を監視する必要があり、万一感染が検知された場合、速やかに脅威を最小限に止めるための対応を施す必要があります。

WatchGuard EPP(エンドポイント保護プラットフォーム):
個々の端末における既知の脅威を検知・防御することで、感染を未然に防ぎます。

WatchGuard EDR(エンドポイント検知／レスポンス):
感染することを前提として全ての端末の挙動を把握し、感染範囲の確認、原因の特定、封じ込めにより、二次被害の拡大を防ぎます。原因を特定した後、対応策を全ての端末に適用し、動作記録の証拠を保全します。

WatchGuard EPDR(エンドポイント保護／検知／レスポンス):
EPPとEDRの機能に加えて、パッチ管理、フル暗号化、高機能レポーティングツールといったセキュリティIT運用のオプションモジュールも利用することができます。



クラウドでセキュアな一元管理を実現

WatchGuard Passport

セキュリティソリューションパッケージには、WatchGuard EPDR、DNSファイアウォールのDNSWatchGO、そして多要素認証のAuthPointが含まれています。

Solution9 エンドポイントセキュリティ：不正なダウロードを防止

DNSレベルでユーザを保護（DNSWatchGO）

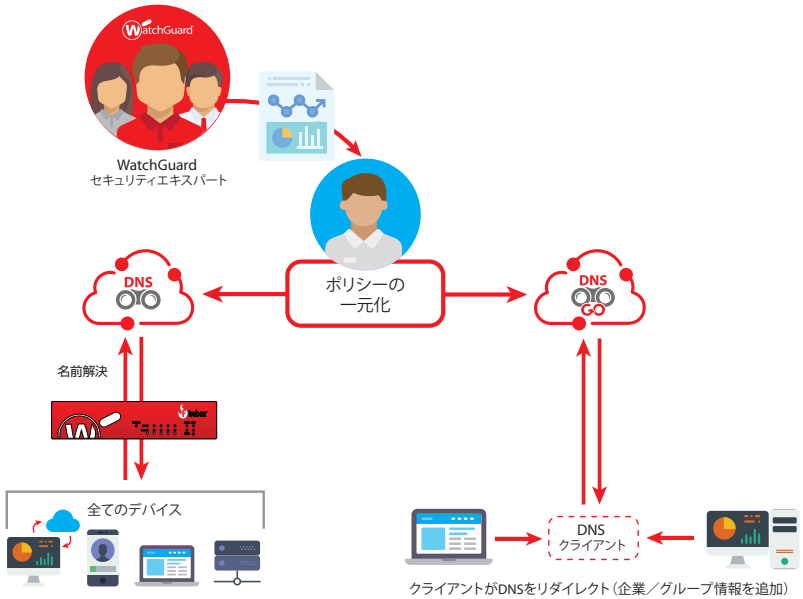
ユーザは標的型攻撃メールやフィッシングメールなどを通じて、多種多様な悪意のあるWebサイトへのアクセスを試みる可能性があります。このようなWebサイトはマルウェアなど不正なコンテンツをダウンロードさせる意図があり、一度ダウンロードしてしまうとPC内に潜伏し、機密情報を漏えいさせたり、他のPC/サーバ攻撃の踏み台にされたりする可能性があります。

DNSWatchGOは、ハードウェアを不要とする100%クラウドベースのソリューションであり、こうした悪意のあるWebサイトを宛先としたDNSリクエストのトラフィックを監視・分析し、不正なドメインへの接続をブロックすることで、マルウェアのダウンロードを防止することができます。

【主な特長】

- DNSレベルの検知機能を備えており、悪意のあるWebサイトへの接続をブロックするため、追加でセキュリティレイヤーを提供
- フィッシング攻撃や C2（C&C）接続からユーザを自動的に保護
- 130種類に及ぶ事前定義されたブロックカテゴリにより、Webの危険な領域へのアクセスを制限するコンテンツフィルタリングを実施
- 攻撃をブロックした後で、ユーザの意識を高めるために速やかにセキュリティ教育を提供
- 高速で常時有効なセキュリティ機能を提供
- VPNが不要

※Fireboxアプライアンス配下にDNSWatchGOクライアントが存在する場合、FireboxのDNSWatch機能が優先して機能します。



DNSWatch（Firebox経由）　DNSWatchGO（オフプレミス）

円滑なビジネスを推進する各種ネットワーク機能

ウォッチガードでは最先端のセキュリティ機能を提供するだけでなく、ネットワークを快適に利用し、ビジネスの安全性と俊敏性を最大化するための各種ネットワーク機能が用意されています。

ネットワーク機能

ブリッジモード

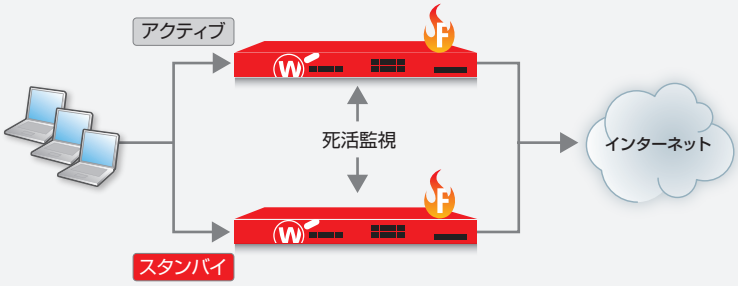
トランスペアレントモードを利用すれば、既存のネットワーク構成に変更を加えることなく、簡単に透過性をもたせることができます。必要な機能だけを容易に適用できるため、新規導入時のセキュリティ構成など、安心してネットワークセキュリティの構築が可能となり、他のネットワークサービスへの影響を考慮した導入プロセス計画を策定することができます。

ロードバランス／トラフィックシェイピング

インターネットの普及に伴い、Webサーバへのアクセス増大と負荷の集中が課題となっています。複数台のサーバで負荷を分散するロードバランス機能により、1台のアプライアンスでルータ機能、ファイアウォール機能、ロードバランス機能が提供できるため、管理面での負荷と導入コストを大幅に軽減することができます。また、優先度の高いトラフィックに対して、ネットワーク帯域を優先的に割り当てるトラフィックシェイピングを適用することにより、さらに詳細なトラフィック管理が可能になります。

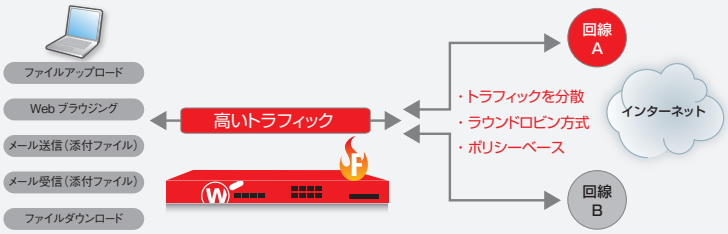
ハイアベイラビリティ（HA構成）

企業の基幹システムやネットワークは24時間365日稼動し続けることが求められています。ウォッチガードのHA構成を導入することで、ダウンタイムを最小化して稼働率を限りなく100%に近づけることができます。万一のハードウェア障害時にもスタンバイ機へ自動的にフェイルオーバすることでダウンタイムを限りなく短くし、業務の継続を維持します。アクティブ／アクティブ構成を採用し、トラフィックの負荷を分散しながら冗長構成による高可用性を提供します。



SD-WAN 負荷分散

インターネットの普及によって業務はよりリアルタイムな活動が求められています。ウォッチガードのSD-WAN機能を使用し、企業のインターネットアクセスを複数の回線に分散することで、より高速で信頼性の高い業務の遂行を実現します。ラウンドロビンによる負荷分散や、アクセスする回線ごとに重み付けすることが可能です。さらに回線を切り替えるしきい値としてパケットロス、遅延、ジッターを指定できます。また、ポリシー毎に利用回線を振り分けることもできます。



Oneアプライアンス、Oneパッケージのトータルセキュリティ

ウォッチガードのコンセプトは、製品設計からパッケージ化までのあらゆる段階で「シンプル」を追求しており、「STANDARD SUPPORT」、「BASIC SECURITY」、「TOTAL SECURITY」の3タイプから選択可能です。

製品	Standard Support	TOTAL SECURITY	Basic Security
ステートフルファイアウォール	✓	✓	✓
VPN	✓	✓	✓
SD-WAN	✓	✓	✓
アクセスポータル*	✓	✓	✓
不正侵入検知·防御(IPS)		✓	✓
アプリケーション制御		✓	✓
Webフィルタリング		✓	✓
迷惑メール対策		✓	✓
ゲートウェイアンチウイルス		✓	✓
レピュテーションセキュリティ(RED)		✓	✓
ネットワークディスカバリ		✓	✓
標的型攻撃対策(サンドボックス)		✓	
相関分析/優先順位付け/レスポンス (ThreatSync:XDR)		✓	
DNSWatch		✓	
インテリジェントAV(AI)**		✓	
EDRコア		5	
WatchGuard Cloud Visibility/ データ保存		30日	1日
サポート	スタンダード(24X7)***	スタンダード(24X7)***	スタンダード(24X7)***

* Firebox T20/T20-W、T25/T25-W、T35-Rではご利用いただけません。M270、M370、M470、M570、M670、FireboxV、Firebox CloudではTotal Security Suiteが必要です。
** Firebox T20/T20-W、T25/T25-W、T35-Rではご利用いただけません。
*** 平日日中(9:00–18:00)は日本語対応、それ以外は英語での対応となります。

すべてのWatchGuard Fireboxシリーズでは、以下の機能をご利用いただけます。(サブスクリプションのライセンス追加により機能が有効になります)

OS機能	
標準	IP address 割り当て: スタティック、DynDNS、PPPoE、DHCP (サーバ、クライアント、リレー) / 独立ポート / VLANサポート / トランスペアレント / ドロップインモード
拡張ネットワーク [b]	ダイナミックルーティング(BGP、OSPF、RIPv1、2) / ポリシーベースルーティング / ナット : スタティック、ダイナミック、1:1、IPSecトラバーサル、ポリシーベースPAT / トラフィックシェイピング & QoS : 8優先キュー、DiffServ、modified strict queuing / バーチャル IP (サーバロードバランス) [a]
可用性 [b]	ハイアベイラビリティ (アクティブ/パッシブ、アクティブ/アクティブクラスタリング) / VPNフェイルオーバ / マルチWANフェイルオーバ / マルチWANロードバランス / リンクアグリゲーション(802.3adダイナミック、スタティック、アクティブ/バックアップ) / 無線WANフェイルオーバ (ブロードバンド無線ブリッジアクセサリを使用)
無線	
Integrated無線	802.11 a/b/g/n(T15-W)、802.11 a/b/g/n/ac(T35-W、T55-W)対応
無線アクセスポイント	すべてのモデルが無線LANにUTMセキュリティ機能を拡張するために無線アクセスポイントをサポート / MACフィルタリングを含む、クライアントレポート、キャプティブポータル技術、802.1X認証、PCIに準拠したスキャンおよびレポート
無線WAN	すべてのモデルが携帯接続への無線ブリッジデバイスを拡張するWatchGuard Broadband Extendをサポート / 一部ダイレクトコネクトUSBをサポート
サブスクリプション	
セキュリティサービス	Application Control / Intrusion Prevention Service / WebBlocker / Gateway AntiVirus / APT Blocker / spamBlocker / Reputation Enabled Defense / ThreatSync / DNSWatch / IntelligentAV
Standard Support Service	ハードウェア保障、ソフトウェアアップデート、技術サポート、アラートサービスが含まれます。 複数年契約のサービスはすべてのモデルで使用可能。受付時間:24時間365日 (休日および夜間は英語対応のみ)

[a]サーバの負荷分散は、Firebox T15のアプライアンスでは使用できません。 [b]クラスタリングを含む一部の機能は、Firebox T15では使用できません。

WatchGuard Network Security Products（小規模オフィス向け）

	Firebox T Series		
			
モデル	**NV5**	**T25/T25-W**	**T35-R**
スループットと接続			
FW スループット	410 Mbps	3.14 Gbps	940 Mbps
VPN スループット	200 Mbps	1.02 Gbps	560 Mbps
AV スループット	-	472 Mbps	325 Mbps
IPS スループット	-	525 Mbps	300 Mbps
UTM スループット	-	403 Mbps	203 Mbps
インターフェイス 10/100/1000	3	5	5
I/O インターフェイス	1 Serial / 1 USB	1 Serial / 2 USB	1 serial / 2 USB
ノード数（LAN IP）	制限なし	制限なし	制限なし
同時接続（双方向）	73,000	1,300,000	1,300,000
新規セッション数	8,500	16,000	6,800
VLAN サポート	10	10	50
VPNトンネル数			
Branch Office VPN	10	10	25
モバイルVPN	10	10	25

Access Point	AP130	AP330
		
設置環境（屋内 / 屋外）	屋内	
サポートする周波数帯（GHz）	2400 - 2483.5 MHz、4.92 - 5.825 GHz	
アンテナ数	4(内蔵)	6(内蔵)
周波数帯	5 GHz / 2.4 GHz	
Tx/Rx ストリーム	2x2:2 OFDMA	
最大転送速度	1201 Mbps(5 GHz帯)、574 Mbps(2.4 GHz帯)	
最大送信出力	21 dBm	
SSID	8	
セキュリティ	Wi-Fi 6 WPA3 およびそれ以前のセキュリティと暗号化方式	
イーサネット	1 x 1 Gb	1 x 2.5 Gb
電源	12V/2A DC、802.3at（PoE+）	
IEEE準拠規格	IEEE 802.11 a/b/g/n/ac/ax	

WatchGuard Network Security Products（小規模オフィス向け）

	Firebox T Series	
		
モデル	**T45/T45-POE/T45-W-POE**	**T85-POE**
スループットと接続		
FW スループット	3.94 Gbps	4.96 Gbps
VPN スループット	1.58 Gbps	2.04 Gbps
AV スループット	874 Mbps	1.53 Gbps
IPS スループット	716 Mbps	1.28 Gbps
UTM スループット	557 Mbps	943 Mbps
インターフェイス 10/100/1000	5	8
I/O インターフェイス	1 Serial / 2 USB	1 Serial / 2 USB
ノード数（LAN IPs）	制限なし	制限なし
同時接続（双方向）	3,850,000	3,850,000
新規セッション数	26,500	35,500
VLAN サポート	50	75
VPNトンネル数		
Branch Office VPN	30	60
モバイルVPN	30	60

Access Point	AP432	AP332CR	AP430CR
			
設置環境（屋内 / 屋外）	屋内	屋外(IP67対応)	
サポートする周波数帯（GHz）	2400 - 2483.5 MHz、5.15 - 5.825 GHz	2400 - 2473.5 MHz、5.15 - 5.825 GHz	2412 - 2472 MHz、5.15 - 5.85 MHz
アンテナ数	8	4（無指向性外部SMA型ｱﾝﾃﾅ）	6（外部Nｺﾈｸﾀ）
周波数帯	5 GHz / 2.4 GHz		
Tx/Rx ストリーム	4x4:4 OFDMA	2x2 OFDMA	4x4 OFDMA
最大転送速度	2.4 Gbps(5 GHz帯)、1148 Mbps(2.4 GHz帯)	1201 Mbps(5GHz帯)、574 Mbps(2.4GHz帯)	2402 Mbps(5 Ghz帯)、574 Mbps(2.4 Ghz帯)
最大送信出力	23 dBm	25 dBm	24 dBm
SSID	8		
セキュリティ	Wi-Fi 6 WPA3 およびそれ以前のセキュリティと暗号化方式		
イーサネット	1 x 2.5 Gbs	2.5 Gbps	1 x 1 Gbs、1 x 5 Gbs
電源	12V DC/2A、802.3at（PoE+）	802.3at（PoE+）	
IEEE準拠規格	IEEE 802.11 a/b/g/n/ac/ax		

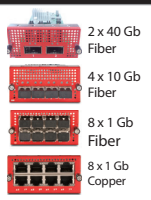
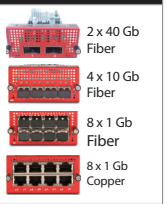
WatchGuard Network Security Products（中規模オフィス向け）

	Firebox M Series			
	 Firebox M290/M390		 Firebox M590/M690	
モデル	**M290**	**M390**	**M590**	**M690**
スループットと接続				
FW スループット	5.8 Gbps	18 Gbps	20 Gbps	29.7 Gbps
VPN スループット	2.4 Gbps	5.2 Gbps	6.84 Gbps	10.0 Gbps
AV スループット	1.47 Gbps	3.1 Gbps	5.0 Gbps	6.2 Gbps
IPS スループット	1.3 Gbps	3.3 Gbps	4.6 Gbps	5.8 Gbps
UTM スループット	1.18 Gbps	2.4 Gbps	3.3 Gbps	4.6 Gbps
インターフェイス 10/100/1000	8	8	8	8
I/O インターフェイス	1 serial / 2 USB	1 serial / 2 USB	1 serial / 2 USB	1 serial / 2 USB
ノード数（LAN IPs）	制限なし	制限なし	制限なし	制限なし
同時接続（双方向）	3,500,000	4,500,000	6,000,000	15,000,000
新規セッション数	34,000	98,000	132,000	146,000
VLAN サポート	100	250	750	1,000
VPNトンネル数				
Branch Office VPN	75	250	500	1000
モバイル VPN	75	250	500	1,000

FireboxV

モデル名	CPU コア上限	ファイアウォール (Mbps)	VPN (Mbps)	VPN ユーザ数	VLAN
Small	2	2,000	400	50	50
Medium	4	4,000	1,500	600	300
Large	8	8,000	3,000	6,000	750
XLarge	16	制限なし	制限なし	10,000	1,500

WatchGuard Network Security Products（大規模オフィス向け）

	Firebox M Series	
	 Firebox M4800  2 x 40 Gb Fiber 4 x 10 Gb Fiber 8 x 1 Gb Fiber 8 x 1 Gb Copper	 Firebox M5800  2 x 40 Gb Fiber 4 x 10 Gb Fiber 8 x 1 Gb Fiber 8 x 1 Gb Copper
モデル	**M4800**	**M5800**
スループットと接続		
FW スループット	49.6 Gbps	87.0 Gbps
VPN スループット	16.4 Gbps	18.8 Gbps
AV スループット	12.5 Gbps	22.0 Gbps
IPS スループット（フルスキャン）	8.1 Gbps	12.5 Gbps
UTM スループット（フルスキャン）	6.8 Gbps	11.3 Gbps
インターフェイス 10/100/1000	8 x 1 Gb	8 x 1 Gb / 4 x 10 Gb
I/O インターフェイス	1 Serial / 2 USB	1 Serial / 2 USB
ノード数（LAN IPs）	制限なし	制限なし
同時接続（双方向）	15,000,000	30,800,000
新規セッション数	254,000	328,000
VLAN サポート	1,000	制限なし
VPNトンネル数		
Branch Office VPN	5,000	制限なし
モバイルVPN	10,000	制限なし

Firebox Cloud

モデル名	CPU コア上限	ファイアウォール (Mbps)	VPN (Mbps)	VPN ユーザ数
Small	2	2,000	400	50
Medium	4	4,000	1,500	600
Large	8	8,000	3,000	6,000
XLarge	16	制限なし	制限なし	10,000

*1 ネットワークインターフェイスの数は仮想環境に依存します。VMware vSphereは10、Microsoft Hyper-Vは8までのアダプタをサポートします。
[a]ファイバーポートは10GBase-SR/SWまたは1000BASE-SXとして動作することができます。

Fireboxセキュリティ仕様

セキュリティ

ファイアウォール機能	ステートフルパケットインスペクション、ディープパケットインスペクション、プロキシファイアウォール
アプリケーションプロキシ	HTTP、HTTPS、SMTP、FTP、DNS、TCP、POP3、TFTP
脅威保護	スパイウェア、DoS攻撃、フラグメンテッドパケット、マルフォームパケット、複合型脅威、標的型攻撃
VoIP	H.323、、SIP、コールセットアップ、セッションセキュリティ
セキュリティサービス	WebBlocker、spamBlocker、Gateway AntiVirus、Intrusion Prevention Service、Reputation Enabled Defense、Application Control、DLP（Data Loss Prevention）、APT Blocker、TDR（Threat Detection & Response）、DNSWatch、IntelligentAV
ゲートウェイアンチウイルス	最新のシグネチャとヒューリスティックエンジン及び最新の振る舞いベースのスキャニング
迷惑メール対策	1バイト文字、2バイト文字、画像ベース、ウイルスアウトブレイクなどに対応
Webフィルタリング	130以上のブロックカテゴリ、HTTP、HTTPSに対応
IPS	TCP、UDPの主要プロトコルをすべてスキャン
アプリケーション利用の可視化と制御	Firebox製品を通過するアプリケーションを制御 主要なアプリケーションに対応、アプリケーション内の機能制御も可能

VPNおよび認証

暗号化	DES、3DES、AES 128/192/256ビット
IPSec	SHA-1、MD5、IKE pre-shared key、3rd party cert
VPNフェイルオーバ	あり
SSL	シンクライアント、Outlook Web Access (OWA)
PPTP	サーバおよびパススルー
シングルサインオン	トランスペアレントActive Directory認証
XAUTH	Radius、LDAP、Secure LDAP、Windows Active Directory
その他ユーザ認証	VASCO、RSA SecurID、Webベース、ローカル、Microsoft Terminal Service、Citrix XenApp

管理

リアルタイム監視、レポート	WatchGuard Dimension
管理プラットフォーム	WatchGuard System Manager（WSM）
アラームと通知	SNMP v2/v3、メール、管理システムアラート
サーバサポート	ログ、レポート、検疫、WebBlocker、管理
Web UI	Windows、Mac、Linux、Solaris OSをサポート
コマンドラインインターフェイス	ダイレクトコネクト、スクリプト含む

標準ネットワーク

QoS	8 優先キュー、DiffServ、modified strict queuing
IPアドレスアサインメント	静的、DynDNS、PPPoE、DHCP（サーバ、クライアント、リレー）

認証・基準

QoS	8 優先キュー、DiffServ、modified strict queuing
セキュリティ	ICSA、FIPS 140-2、EAL 4+
安全	NRTL/C、CB
ネットワーク	IPv6 Ready Gold（ルーティング）
特定有害物質指令	WEEE、RoHS、REACH

【WatchGuard Technologiesについて】

WatchGuard® Technologiesは25年以上にわたり、最先端のサイバーセキュリティテクノロジーの開発におけるパイオニアとして、導入・管理が容易なソリューションを提供し続けてきました。ネットワークセキュリティ、セキュアWi-Fi、多要素認証、エンドポイントセキュリティなど、ネットワークインテリジェンスを駆使した製品やサービスを元に、日々新たな脅威が台頭するサイバーセキュリティ情勢において、グローバル規模で250,000以上の顧客に対して最も重要なアセットを保護するために支援しています。

ウォッチガード・テクノロジー・ジャパン株式会社

〒106-0041 東京都港区麻布台1-11-9 BPRプレイス神谷町5階　TEL:03-5797-7205　FAX:03-5797-7207

www.watchguard.co.jp　JPNSales@watchguard.com

www.facebook.com/watchguard.jp　twitter.com/watchguardjapan

■ お問い合わせ先

PN202304