ソリューションガイド

目次

ウォッチガードの使命:

スマートなセキュリティを「簡単」に実現。

ウォッチガードは、およそ30年間にわたり、最先端のサイバーセキュリティ技術を開発し、導入と管理が容易なソリューションとして提供してきました。業界をリードするネットワークおよびエンドポイントセキュリティ、セキュアWi-Fi、多要素認証、ネットワークインテリジェンスの製品とサービスにより、ウォッチガードは世界中の250,000社を超える中小企業に活用されており、1,000万台を超えるエンドポイントを含む最も重要な資産を保護できるよう支援しています。

サイバーセキュリティの状況は常に変化し、日々新たな脅威が出現する世界において、ウォッチガードはあらゆる企業がエンタープライズグレードのサイバーセキュリティ技術を利用できるようにしています。ウォッチガードはワシントン州シアトルに本社を置き、北米、ヨーロッパ、アジア太平洋、ラテンアメリカにオフィスを構えています。

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

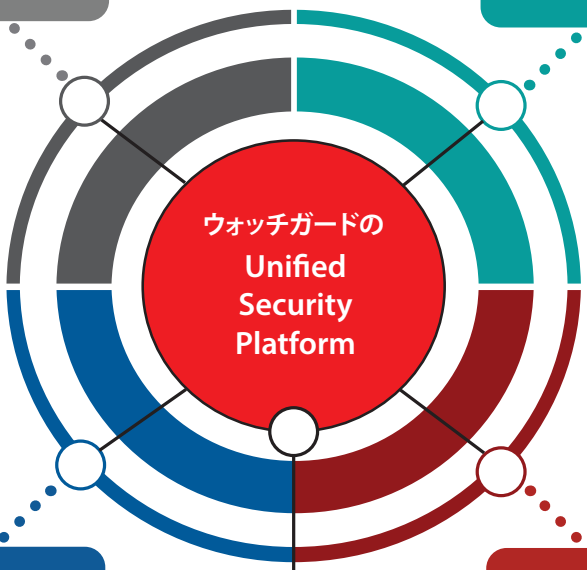
運用効率を高めつつ、拡張性とスピードを向上させる強力なセキュリティサービスを実現します。

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

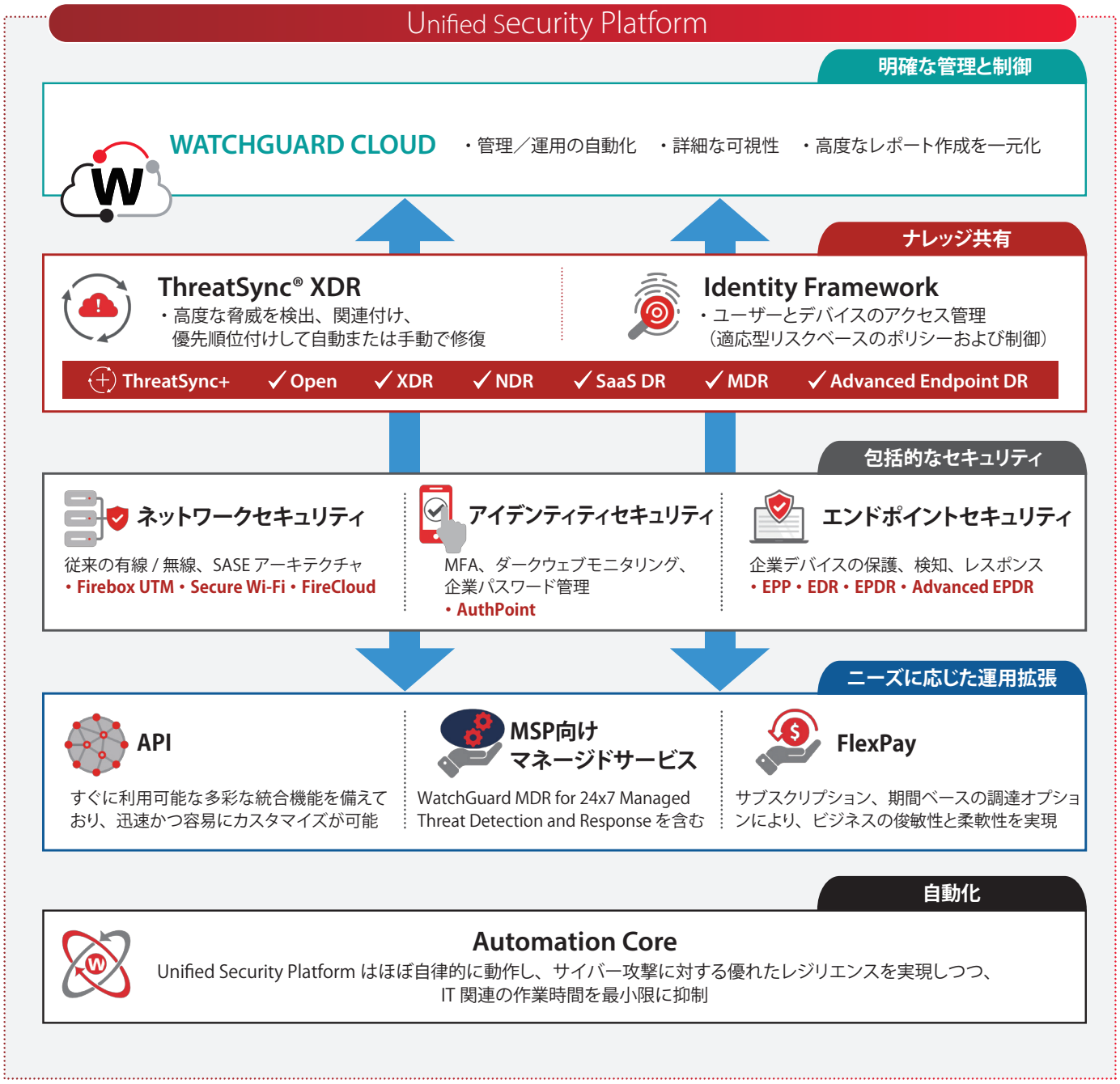
自動化

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)を基盤としており、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)」、「エンドポイントセキュリティ」**の3つの柱を基軸として、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



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。

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、シグネチャの自動更新により最新のウイルスにも対応します。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及びスコアリングすることで、脅威の早期発見や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。

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。

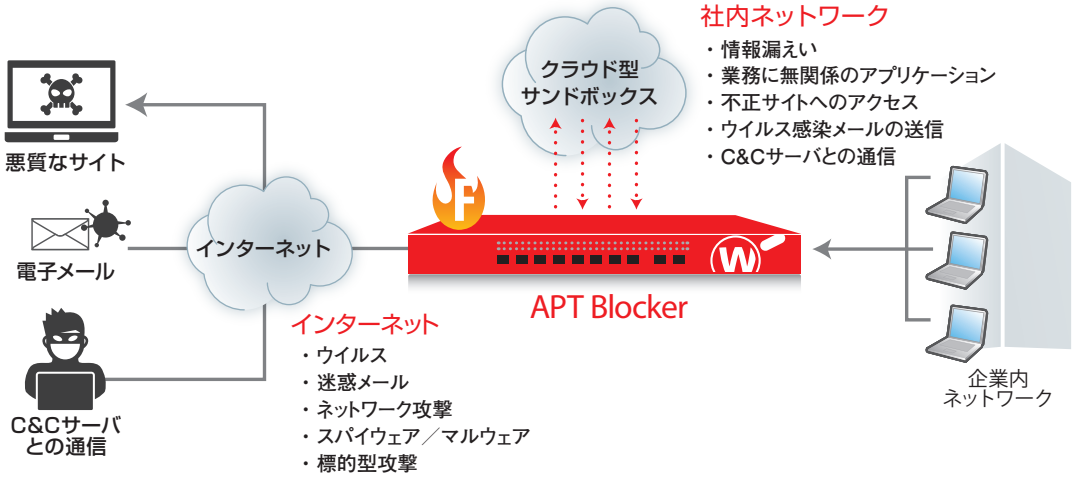
Solution1 変異し続ける悪質マルウェアからの防御（APT Blocker / IntelligentAV）

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

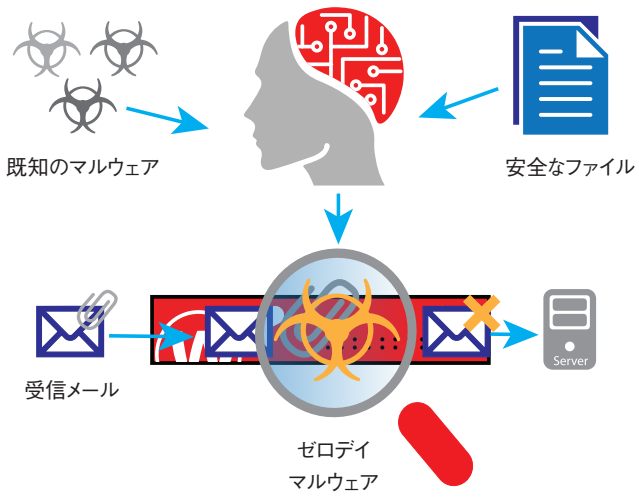
- APT Blocker: 標的型攻撃やゼロデイアタックを検出する業界で最も洗練されたセキュリティプラットフォーム
- シグネチャによる既知のマルウェア検知に加え、ファイル内部に埋め込まれた行動を詳細に分析し、回避行動をとる巧妙なマルウェアも的確に検出
- クラウドベースの次世代型サンドボックスと連携し、ファイルの正確なコード分析により標的型攻撃につながる脅威を検出



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

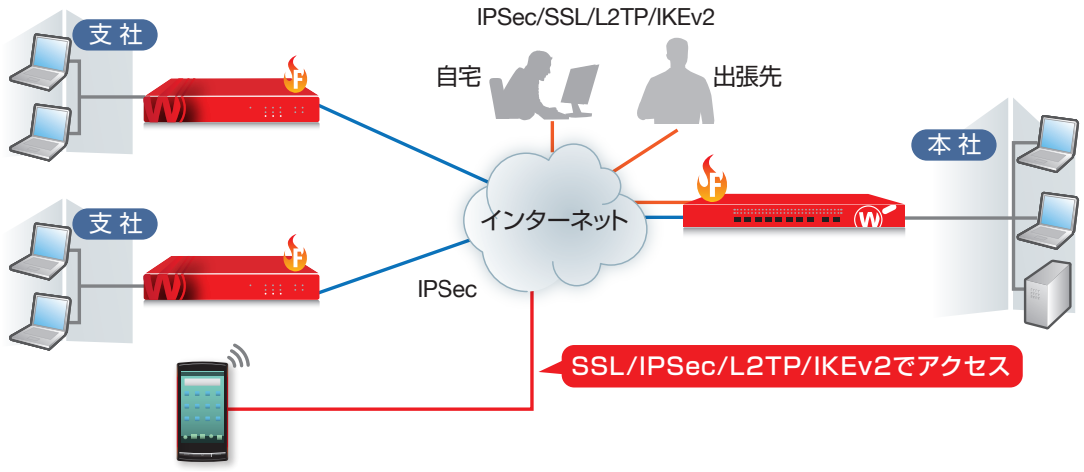


Solution2 拠点間の安全かつ高速な接続（VPN）

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

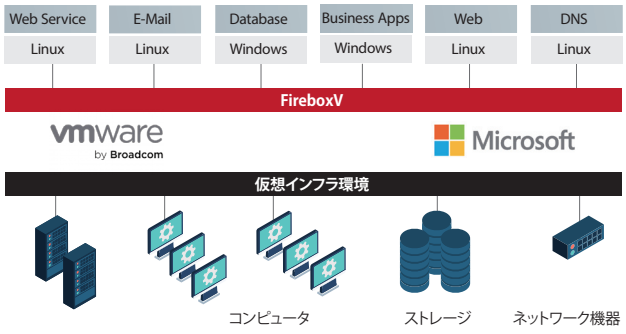


Solution3 仮想環境への導入と効率的な運用（FireboxV / Firebox Cloud）

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。

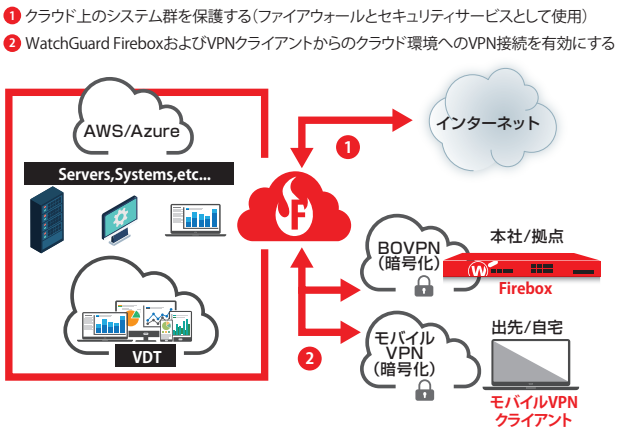
WatchGuard FireboxV（仮想アプライアンス）による仮想環境への対応

- 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



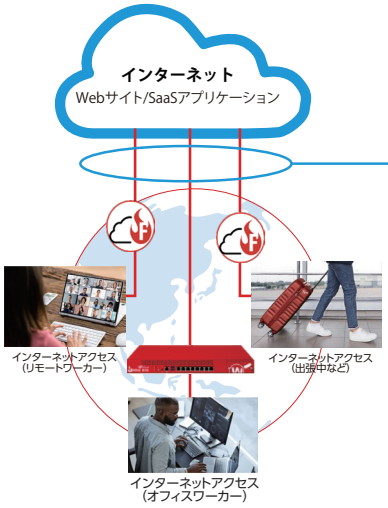
クラウド環境へ対応した仮想アプライアンス WatchGuard Firebox Cloud

- 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 Firebox UTMを補完するSASEソリューション（FireCloud）

FireCloud Internet Accessは、WatchGuard Cloudを通じて管理されるFWaaSおよびSWGによるエンタープライズグレードのセキュリティを提供します。グローバルポリシーを即時に適用し、場所を問わずあらゆるデバイスでに対してシームレスで安全なアクセスを保証します。また、リモートユーザーにゼロトラストセキュリティを提供し、ファイアウォールレベルの保護と安全なアプリアクセスも可能にし、すべてウォッチガードのクラウドネイティブプラットフォームを通じて管理します。



Firewall-as-a-Service（FWaaS）
- DNSフィルタリング
- ボットネット検知
- IPS（侵入防御）
- APT Blocker（サンドボックス）
- TLSインスペクション
- ジオブロッキング
- ゲートウェイアンチウイルス（GAV）

Secure Web Gateway（SWG）
- WebBlocker / URLフィルタリング
- アプリケーション制御

ユーザー認証
- 接続管理
- アイデンティティプロバイダー（idP）

マネジメントサービス
- 共通のポリシー／構成
- 容易なセットアップウィザード
- idP用のSMAL連携
- 一つのプラットフォーム
（UTM、ID、エンドポイント保護）

【ライセンス】

	FWaaS	SWG	ZTNA	どちらを選ぶべきか?
内容	クラウド型ファイアウォール（トラフィックインスペクション、ポリシー）	Webアクセスを安全に行うゲートウェイ	アプリケーション単位でアクセス許可（最小特権アクセス）必要なアプリケーションだけに安全に接続（VPN代替）	
Internet Access	○	○		リモートユーザー
Total Access	○	○	○	ハイブリッド（VPN代替＋社内リソース利用）

Solution5 安心して無線LANに接続（Secure Wi-Fi）

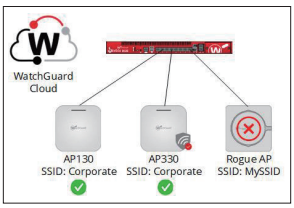
場所を問わないワーキングスタイルの普及により、ノートPC、タブレット、スマートフォンなど多くのデバイスが無線LANネットワークにつながっており、今ではオフィス内や在宅でさえもWi-Fi接続が主流になっています。また、社内管理が十分に行き届いていないBYOD（個人所有デバイス）も増加しており、セキュリティリスクがこれまでになく高まっています。

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

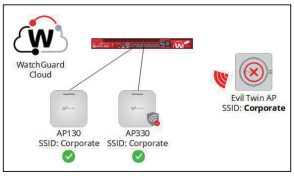
- 一元管理が可能な専用アクセスポイント（AP）をラインナップ
- 最新世代のWi-Fi 6と強力なWPA3暗号化を採用
- セキュリティベンダーならではの有線と同様のセキュリティを実現
- 統合型プラットフォーム上で容易に導入、設定、レポーティング
- 複数のロケーションにわたり1台のアクセスポイントから無制限に拡張管理
- ロケーション、ビル、フロア、顧客、リモートユーザー単位など、アクセスポイントを多様な方法でグループ化
- 分散型ネットワークを横断して一貫したポリシーを適用
- エアスペースモニタリング機能（不正アクセス検知／悪魔の双子アクセスポイント検知）

クラウドでセキュアな一元管理を実現

不正アクセスポイントを検出



悪魔の双子
アクセスポイントを検出



専用アクセスポイント（AP）

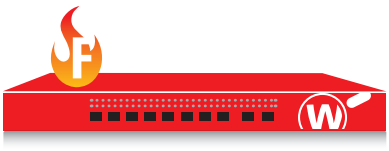
AP130	スモールオフィスやリモートワーク環境など、低密度の屋内環境向けに最適化
AP330	中小企業や中堅企業など、中密度の屋内環境向けに最適化
AP432	大企業や大規模施設など、高密度の屋内環境向けに最適化
AP332CR	中規模施設など、屋外の過酷な環境や気象条件に最適化
AP430CR	大規模施設など、屋外の過酷な環境や気象条件に最適化
AP230W	スモールオフィスやリモートワーク環境など、低密度の屋内環境向けに最適化（壁掛け型）

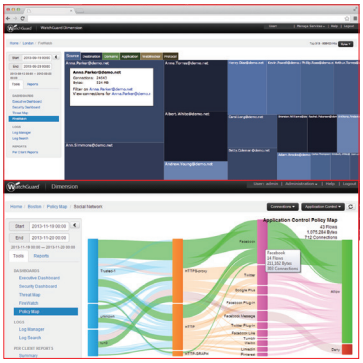
Solution6 ネットワークセキュリティの可視化（WatchGuard Cloud）

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。

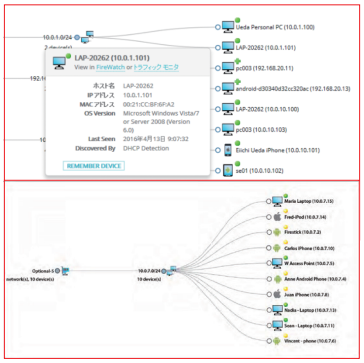
WatchGuard DimensionとWatchGuard Cloud Visibilityによるネットワークセキュリティの監視

- 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



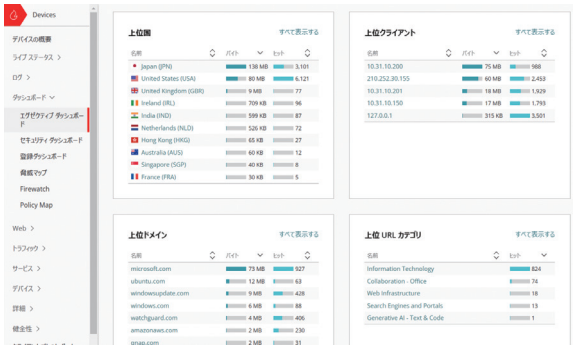
Network Discovery

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

WatchGuard Cloud の強力なプラットフォームでは、セキュリティに関する優れた管理およびレポート機能を提供しています。

- 集中化と可視化によるシンプルな管理
- インフラ不要によるコストと時間を削減
- FireboxアプライアンスにRapidDeploy機能を標準装備（実装、設定ツール）
- 多階層管理、遠隔によるファームウェアバージョンアップ
- ネットワークセキュリティの可視化（100以上のレポート、ダッシュボード、ログ）



【集中化と可視化によるシンプルな管面】
（例）エグゼクティブダッシュボード画面

【コストと時間を節約（保守とセットアップのための管理画面）】

Solution7 相関分析、優先順位付け、レスポンス（ThreatSync+、ThreatSync+ NDR、ThreatSync XDR）

セキュリティ運用を簡素化し、スピードと効率性でサイバー攻撃を特定し、修復に必要な情報を収集します。

脅威のスコアリングと優先順位付け

- さまざまなセキュリティレベルのアクティビティデータを相関させ、最も重要な脅威の優先順位付けを行います。

簡素化された統合セキュリティ

- 環境、ユーザ、デバイスからの統合脅威インテリジェンスにより、セキュリティ運用を合理化します。

コンテキストに基づく脅威インテリジェンス

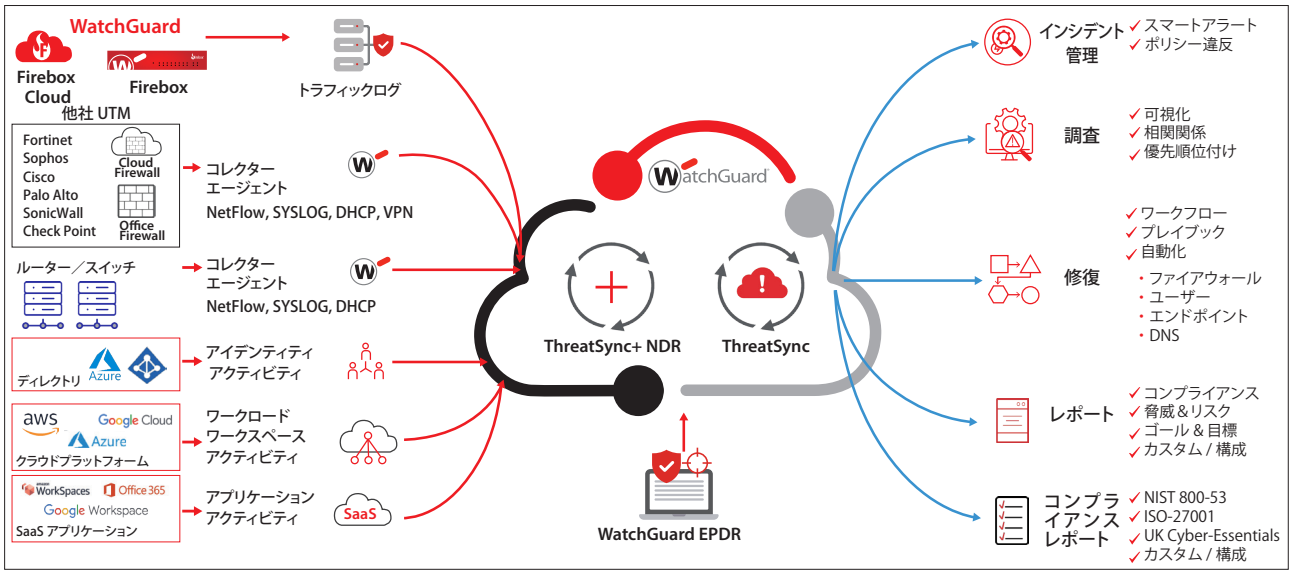
- 個々のイベントに関する集合知は、全体としてインシデントの指標となり、XDRは、より洞察力の高いデータとクロスドメインのコンテキスト化を可能にし、脅威の検知を迅速化します。

スピードと確実性

- より素早い検知、より信頼性の高い迅速な対応、より強固なセキュリティを可能にする高度な機能を提供します。

ThreatSync+ NDR:シンプルな統合ネットワークセキュリティ

- クラウドネイティブアーキテクチャによるコスト削減
- 最先端のAIで脅威を検知
- 隠れたネットワークリスクを明確化
- 迅速なレスポンスを実行



【ライセンス】

	XDR プラットフォームの基盤	NDR	SaaS	XDR
内容	Firebox、EDR、AuthPointなどからのイベントを統合し、脅威の相関分析とアラート管理を提供 (例)端末隔離など	ネットワーク脅威検知機能:ネットワークフロー解析により、異常なトラフィックを検知し、他社NW機器とも連携 (例)隔離や遮断の自動化	SaaSアプリの可視化・制御機能を追加:クラウドの利用状況を監視／可視化	リスクスコアリング機能: 異常な通信やデバイス、認証・ポリシー違反などに反応し、リスクレベルを数値化してアラートや対策に活用 コンプライアンスレポート機能: ISO、NIST、CISAなど
ThreatSync+	○			
Total Access	○	○		
ThrearSync+ SaaS	○		○	
Total XDR	○	○	○	○

Solution8 クラウドベースの多要素認証（AuthPoint）

巧妙化するサイバー攻撃に対し、多層防御により、侵入を防ぐことができます。ゼロトラストの第一歩であるAuthPointは、IDとアクセスを徹底検証することにより、境界防御に頼らず、すべてのアクセスを検証します。

- ✓ クラウドベースで簡単に導入でき、ユーザーへのプッシュ通知などスムーズな認証を実現
- ✓ スマートフォンを活用し、パスワード+スマートフォン認証により、セキュリティを強化
- ✓ パスワードの流出／漏えいやフィッシングなど不正アクセスやなりすましに対応
- ✓ VPNやクラウドサービスへの安全なアクセスが可能

【ライセンス】

	多要素認証	リスクベース	シングルサインオン	ダークウェブ監視
内容	パスワード&追加要素（認証方法） ✓ プッシュ通知 ✓ QRコード ✓ ワンタイムパスワード	モバイルDNA、位置情報、アプリケーション名等からの要求認証を確認	複数クラウドサービス等に一度のログインでアクセス可能	資格情報などの漏えいを検知し、ユーザー等に通知
AuthPoint MFA	○	○	○	
Total Identity Security	○	○	○	○

【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、プッシュ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/プッシュ通知/QRコードのいずれかを使用して認証することで、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、プッシュ通知に対する承認を義務付けてセキュアなリモートアクセスを実現。

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。

Solution9 ゼロトラスト（Passport）

自由な働き方への Passport

【ライセンス】

機能	ライセンス	内容
多要素認証	Authpoint	MFAライセンス、スマートフォン認証
常時保護	FireCloud	VPN接続不要のユーザー保護（SASE）
迅速なレスポンス	EPDR	エンドポイント保護、初動検知

多要素認証

従業員の認証において、クラウドアプリケーション、VPN、エンドポイントなどに強力な多要素認証を適用し、シングルサインオンを実現します。

常時保護

VPN接続することなくインターネット上のユーザーの保護、フィッシングのブロックを可能にし、モバイルユーザーにも社内で規定されたものと同様のWebポリシーを適用できます。

迅速なレスポンス

ランサムウェアと関連するC&C（コマンド&コントロール）を封じ込めつつ、マルウェアをはじめ多様な脅威を検知し、自動レスポンスで対応します。

Solution10 エンドポイントセキュリティ：不正なダウロードを防止（DNSWatchGO）

DNSレベルでユーザーを保護

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。

Solution11 エンドポイントセキュリティ：末端のPCまで保護（WatchGuard EPP/EDR/EPDR）

「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

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。

WatchGuard Advanced EPDR
（高度なエンドポイント保護/検知/レスポンス）

EPDR搭載の全機能の他、感染したエンドポイントのプロアクティブな検知、および一般的なマルウェアを使用しない脅威を発見する機能を備えています。高度なIOAやイベント、STIXやYaraルールと互換性のあるIOCの一元管理、高度なセキュリティポリシー、インシデントの検知、封じ込め、修復するためのリモートアクセスなど、検知／レスポンスの高機能でセキュリティ効果を高めることができます。

【オプション】セキュリティ IT 運用のオプションモジュール

Patch Management(脆弱性管理:システムに対するパッチの適用)

更新されていないアプリケーションのパッチを検知し、最新のパッチを適用します。Windows、Mac、Linuxに対応し、ソフトウェアの脆弱性攻撃を未然に防ぎます。

Full Encryption(フルディスク暗号化:暗号化によるデータ保護)

Windows、Macを対象に、ディスクの暗号化と復号化、回復キーの管理、リストやレポートを一元管理します。

Advanced Reporting tool
(モニタリングと実用的な洞察:検知とアラート)

エンドポイント製品によって収集したコンテキスト情報を保存し、関連付けます。セキュリティインテリジェンスを自動的に生成し、組織が攻撃や異常な動作を特定できるツールを提供することで、企業システムやネットワークの内部の誤用を検知してセキュリティ調査を深掘りします。

	EDR Core	WATCHGUARD EPP	WATCHGUARD EDR	WATCHGUARD EPDR	WATCHGUARD ADVANCED EPDR
ウォッチガードのUnified Security Platformアーキテクチャ内のプロアクティブなエンドポイントセキュリティ		✓	✓	✓	✓
軽量なクラウドベースのエージェント		✓	✓	✓	✓
ゼロトラストアプリケーションサービス:実行前、実行中、実行後			✓	✓	✓
メモリ内動作のエクスプロイト対策		✓	✓	✓	✓
エンドポイントのリスク監視		✓	✓	✓	✓
脅威ハンティングサービス:動作分析MITRE ATT&CKに忠実にマッピングされた高度なIOA検知			✓	✓	✓
永続的なマルウェアの検知に関するナレッジに基づいたリアルタイム検索				✓	✓
IDS、ファイアウォール、デバイス制御		✓		✓	✓
Webブラウジング保護とカテゴリベースのURLフィルタリング		✓		✓	✓
STIX、YARA、IOCルールに基づくエンドポイントでの検索					✓
脅威ハンティングサービス:動作分析MITRE ATT&CKにマッピングされた非決定論的なIOA検知					✓
非決定的なIoA調査を可能にするコンテキストテレメトリ					✓
攻撃対象領域を削減する高度なセキュリティポリシー					✓
クラウドからのリモートシェル:クリックして接続し、エンドポイントのプロセス、サービス、構成ミス、ファイルなどを管理					✓
オプション:Advanced Reporting Tool			✓	✓	✓
オプション:Patch Management		✓	✓	✓	✓
オプション:Full Encryption		✓	✓	✓	✓

Solution12 MSPパートナー向け24/7の脅威監視／レスポンスプラットフォーム（WatchGuard MDR）

WatchGuard MDRは、企業のワークロードを増やすことなく、正確で強力な保護を提供します。ウォッチガードのエンドポイント、ファイアウォール、ID管理、ネットワーク製品、そして主要なサードパーティ製クラウドサービスまで、フルスタックのセキュリティを単一の統合プラットフォームで管理できます。

24時間365日体制のSOCは、AI主導の自動化とエキスパートによる専門スキルを組み合わせ、ノイズを排除して脅威をより迅速に阻止します。アラートの繰り返しや時間の無駄をなくし、組織のビジネスにシームレスに適合する真のセキュリティを実現します。

誤検知数 1件以下
1カ月あたり

平均6アラート
1カ月あたり

6分
平均初回対応時間

10ミリ秒
脅威の自動ブロック速度

MDR サービス内容	Core MDR	Core MDR for MS	Total MDR
24/7 SOCモニタリング	✓	✓	✓
AI/MLベースの脅威検出	✓	✓	✓
自動脅威レスポンス／リアルタイムアラート	✓	✓	✓
根本原因分析	✓	✓	✓
脅威ハンター	✓	✓	✓
インシデントレスポンス			✓
ディフェンスポータル	✓	✓	✓
パートナーのテクニカルアカウントマネージャへのアクセス	✓	✓	✓
エンドポイントインテグレーション	WatchGuard 製品 EDR/EPDR/AEPDR	Microsoft Defender	WatchGuard製品 EDR/EPDR/AEPDR
ThreatSync+ XDR			✓
ネットワークインテグレーション			Firebox,Firebox CloudThreatSync+ NDR
アイデンティティインテグレーション			WatchGuard AuthPoint
Google Workspace			✓
Microsoft 365	✓	✓	✓
AWS CloudTrailカバレッジ			✓

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

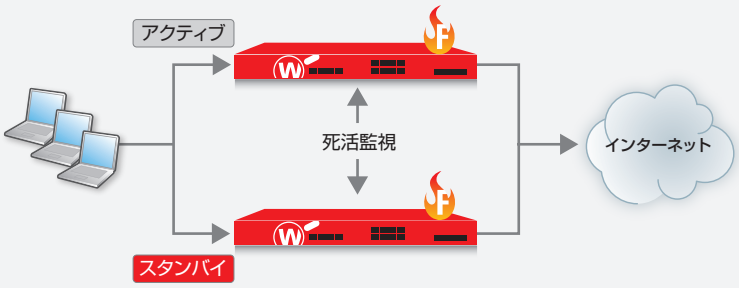
トランスペアレントモードを利用すれば、既存のネットワーク構成に変更を加えることなく、簡単に透過性をもたせることができます。必要な機能だけを容易に適用できるため、新規導入時のセキュリティ構成など、安心してネットワークセキュリティの構築が可能となり、他のネットワークサービスへの影響を考慮した導入プロセス計画を策定することができます。

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。

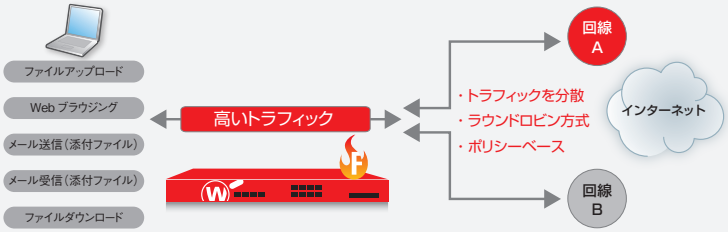
ハイアベイラビリティ（HA構成）

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		✓	✓
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***		✓	
WatchGuard Cloud ログデータ保持／レポートデータ保持		365日/30日	90日/1日

* Firebox T115-W、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 T115-W、T20/T20-W、T25/T25-W、T35-Rではご利用いただけません。
*** Fireboxモデルによって付属数が異なります。

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	**T115-W**	**T125/125-W**	**T145/145-W**	**T185**
スループットと接続				
FW スループット	1.02 Gbps	2.28 Gbps	3.90 Gbps	7.90 Gbps
VPN スループット	640 Mbps	1.44 Gbps	1.94 Gbps	2.20 Gbps
AV スループット	450 Mbps	880 Mbps	1.06 Gbps	2.80 Gbps
IPS スループット	375 Mbps	725 Mbps	1.03 Gbps	2.40 Gbps
UTM スループット	280 Mbps	510 Mbps	710 Mbps	1.83 Gbps
インターフェイス	3 (10/100/1000)	1 x 2.5 GbE, 4 x 1 GbE	1 x 2.5 GbE, 4 x 1 GbE, 1 x SFP/SFP+	4 x 1 GbE, 4 x 2.5 GbE, (2PoE+PSE, 802.3at) 1 x SFP/SFP+
I/O インターフェイス	1 Serial/1 USB-A 3.2	1 Serial/2 USB-A 3.2	1 Serial/2 USB-A 3.2	1 Serial/2 USB-A 3.2
ノード数（LAN IP）	制限なし	制限なし	制限なし	制限なし
同時接続（双方向）	3,850,000	3,850,000	3,850,000	3,850,000
新規セッション数	26,500	26,500	26,500	26,500
VLAN サポート	無制限	無制限	無制限	無制限
VPN トンネル数				
ブランチオフィス	5	10	25	100
モバイル	5	10	25	100

Access Point	AP130	AP330	AP230W
			
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		2400 - 2483.5 MHz、5.15 - 5.825 GHz
アンテナ数	4(内蔵)	6(内蔵)	4(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		23 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	1 x 2 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	**NV5**	**T25/T25-W**	**T45/T45-POE/T45-W-POE**
スループットと接続			
FW スループット	410 Mbps	3.14 Gbps	3.94 Mbps
VPN スループット	200 Mbps	1.02 Gbps	1.58 Gbps
AV スループット	-	472 Mbps	874 Mbps
IPS スループット	-	525 Mbps	716 Mbps
UTM スループット	-	403 Mbps	557 Mbps
インターフェイス	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	3,850,000
新規セッション数	8,500	16,000	26,500
VLAN サポート	10	10	50
VPN トンネル数			
ブランチオフィス	10	10	30
モバイル	10	10	30

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		
			
モデル	**M295**	**M395**	**M495**
スループットと接続			
FW スループット	7.90 Gbps	20.00 Gbps	37.00 Gbps
VPN スループット	5.80 Gbps	8.10 Gbps	16.20 Gbps
AV スループット	3.00 Gbps	5.90 Gbps	6.30 Gbps
IPS スループット	2.41 Gbps	4.50 Gbps	7.40 Gbps
UTM スループット	1.85 Gbps	3.00 Gbps	6.30 Gbps
インターフェイス	4x2.5Gb, 4x1Gb, 2xSFP+	2.5 Gbps RJ45 x 12, 1 Gbps SFP x 2, 10 Gbps SFP+ x	2.5 Gbps RJ45 x 12, 10 Gbps RJ45 x 2, 1 Gbps SFP x 2, 10 Gbps SFP+ x 2
I/O インターフェイス	1 Serial/2 USB-A 3.2	1 Serial/2 USB-A 3.2	1 Serial/2 USB-A 3.2
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）	6,000,000	6,000,000	6,000,000
新規セッション数	60,000	124,000	152,000
VLAN サポート	無制限	無制限	無制限
VPN トンネル数			
ブランチオフィス	100	350	800
モバイル	100	350	800

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	
		
モデル	**M595**	**M695**
スループットと接続		
FW スループット	43.00 Gbps	45.00 Gbps
VPN スループット	19.80 Gbps	23.20 Gbps
AV スループット	7.60 Gbps	11.50 Gbps
IPS スループット	9.40 Gbps	10.80 Gbps
UTM スループット	7.20 Gbps	10.20 Gbps
インターフェイス	2.5 Gbps RJ45 x 12, 10 Gbps RJ45 x 2, 1 Gbps SFP x 2, 10 Gbps SFP+ x 4	2.5 Gbps RJ45 x 12, 10 Gbps RJ45 x 2 1 Gbps SFP x 4, 10 Gbps SFP+ x 4
I/O インターフェイス	1 Serial/2 USB-A 3.2	1 Serial/2 USB-A 3.2
ノード数（LAN IP）	制限なし	制限なし
同時接続（双方向）	15,000,000	30,000,000
新規セッション数	212,000	245,000
VLAN サポート	無制限	無制限
VPN トンネル数		
ブランチオフィス	1,200	2,000
モバイル	1,200	2,000

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

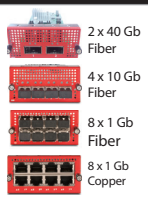
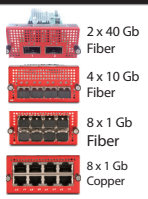
	Firebox M Series			
	 Firebox M290/M390		 Firebox M590/M690	
モデル	**M290**	**M390**	**M590**	**M690**
スループットと接続				
FW スループット	5.8 Gbps	18 Gbps	20 Gbps	29.7 Gbps
VPN スループット	2.4 Gbps	5.2 Gbps	6.84 Gbps	10.0 Gbps
AV スループット	1.47 Gbps	3.1 Gbps	5.0 Gbps	6.2 Gbps
IPS スループット	1.3 Gbps	3.3 Gbps	4.6 Gbps	5.8 Gbps
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	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 IP）	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				
ブランチオフィス	75	250	500	1000
モバイル	75	250	500	1,000

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。

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, Inc.は、統合型サイバーセキュリティにおけるグローバルリーダーです。Unified Security Platform®（統合型セキュリティプラットフォーム）は、マネージドサービスプロバイダー向けに独自に設計されており、世界トップクラスのセキュリティを提供することで、ビジネスのスケールとスピード、運用効率の向上に貢献しています。17,000社を超えるセキュリティのリセラーやサービスプロバイダと提携しており、25万社以上の顧客を保護しています。実績豊富な製品とサービスは、ネットワークセキュリティとインテリジェンス、高度なエンドポイント保護、多要素認証、セキュアWi-Fiで構成されています。これらの製品では、包括的なセキュリティ、ナレッジの共有、明快さと制御、運用の整合性、自動化という、セキュリティプラットフォームに不可欠な5つの要素を提供しています。ワシントン州シアトルに本社を置き、北米、欧州、アジア太平洋地域、ラテンアメリカにオフィスを構えています。日本法人では、多彩なパートナーを通じて、国内で拡大する多様なセキュリティニーズに応えるソリューションを提供しています。

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　x.com/watchguardjapan

■ お問い合わせ先

2026年1月
PIN202601