
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.
WatchGuard
ウォッチガード・テクノロジー・ジャパン株式会社

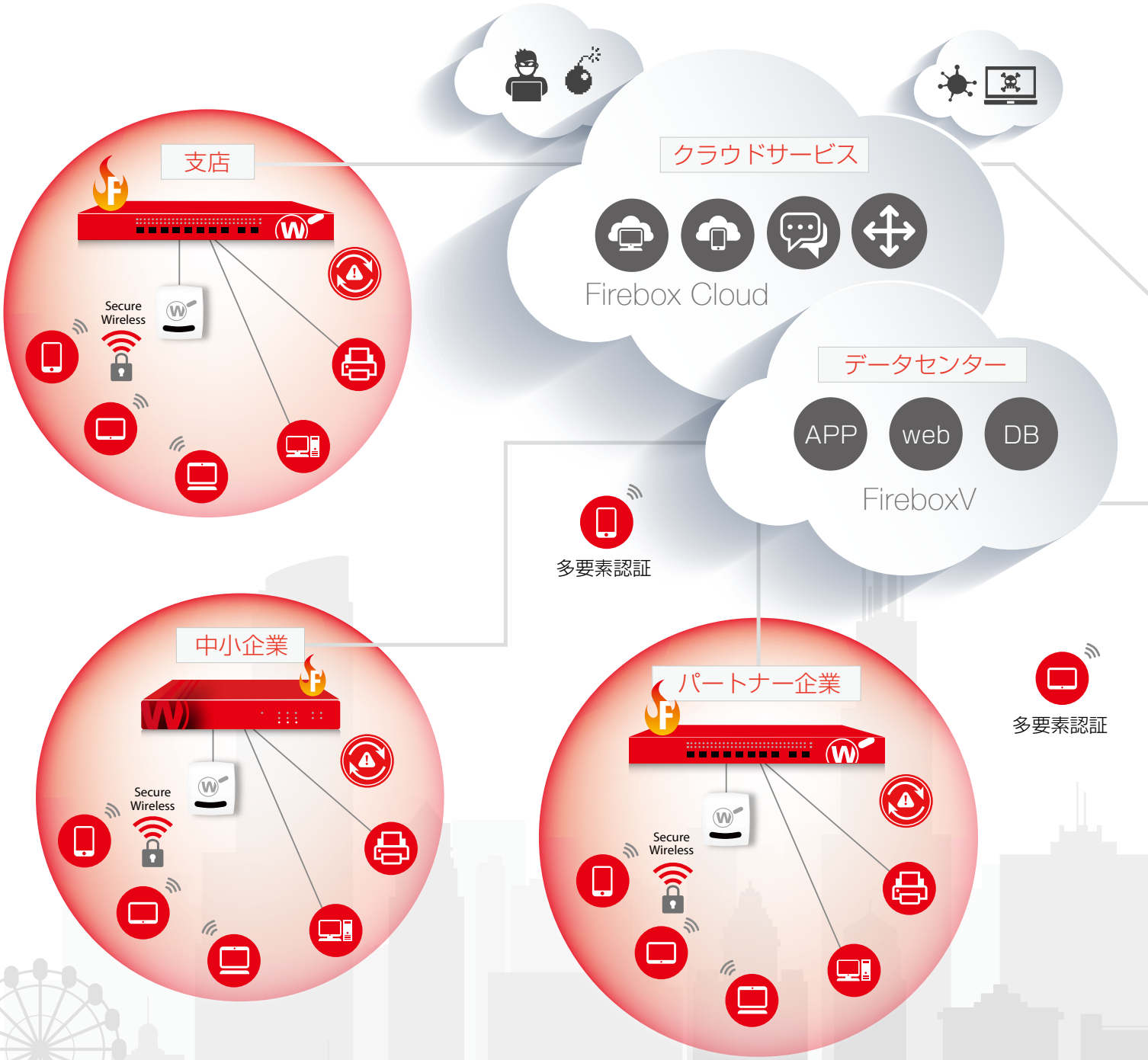
ウォッチガードの使命:

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、提携先、データセンター、あるいはノートPCやタブレット、スマートフォンといった個人の無線デバイスなど、あらゆる拠点／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。

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しており、さらには攻撃の糸口となる無線デバイスの急激な普及により、不正アクセスも多発しています。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、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。



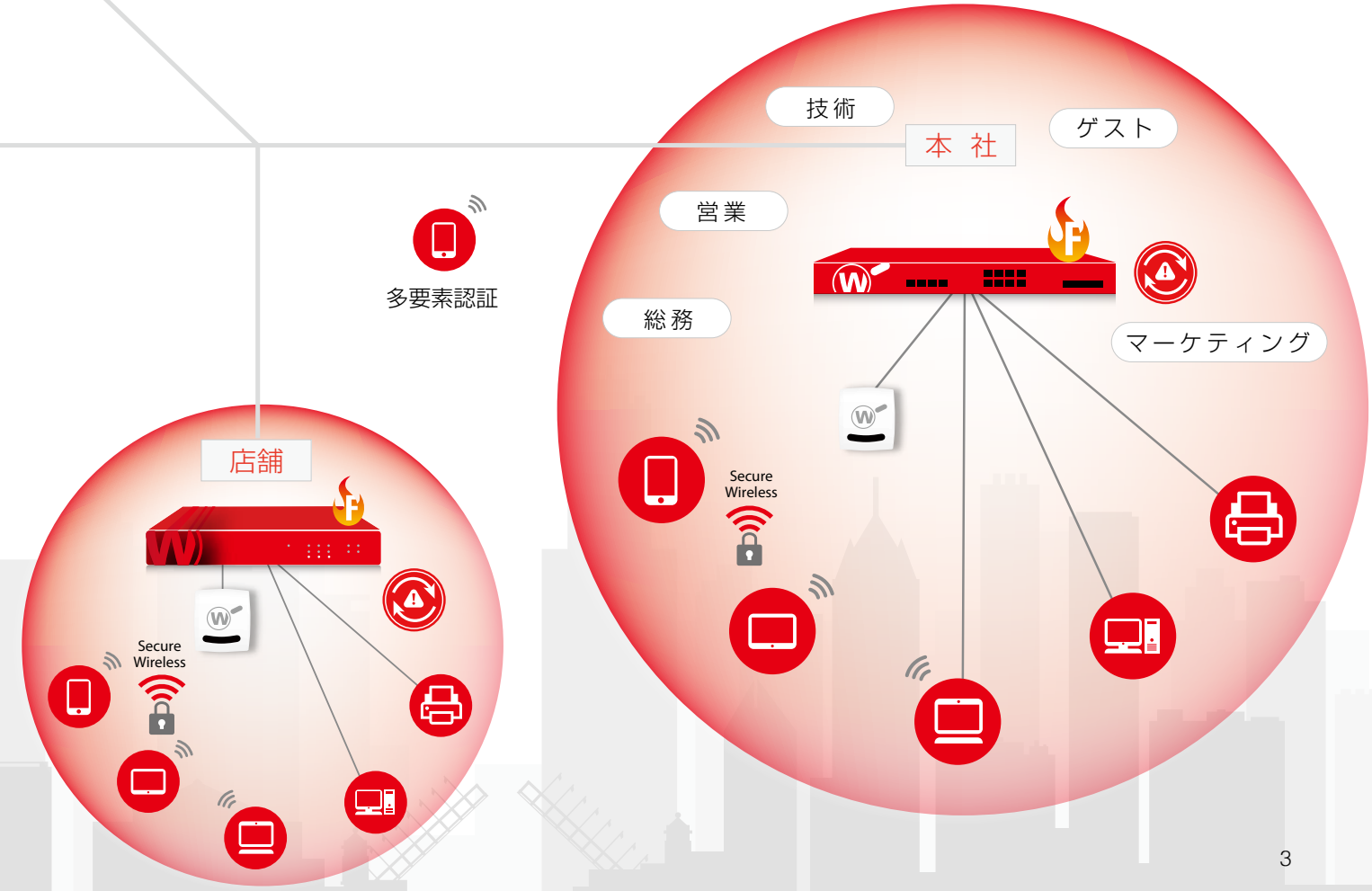
なぜウォッチガードなのか?

求められる「高性能」、「シンプル」、「低コスト」の三要素を兼ね備えた渾身のセキュリティアプライアンス。

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、ベストオブブリードの最先端技術が1台のハードウェアに統合されており、SOHO、中小／中堅規模、大規模といったあらゆる組織に対して、それぞれ適正なアプライアンスをご用意しています。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。また、Threat Detection & Response(TDR)機能によって、Fireboxのネットワークセキュリティと、Host Sensor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、ネットワークとエンドポイントそれぞれ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。また、アプライアンスとは別にモバイルデバイス向け多要素認証ソリューション(AuthPoint)*も利用することができます。*詳細はデータシートをご覧下さい。

WatchGuard Firebox はネットワークのすべての脅威に有効なソリューションです。

- 企業のネットワークの保護に必要なすべてのセキュリティ機能を1台に集約
- 各セキュリティ機能を有効にしつつ高いスループットを実現
- ウイルス感染、不正アクセス、迷惑メール、ネットワーク攻撃など、さまざまな脅威をブロック
- Webフィルタリング、アプリケーション制御により、企業の生産性の向上を支援
- 個別のセキュリティ機能を組合せる場合に比べて、優れたROI(費用対効果)を実現
- 導入・運用・管理がシンプルで、手間がかからず専門的な知識も不要
- グラフィカルなレポート機能により、複雑なセキュリティ管理を分かりやすく「見える化」
- 広範かつ強力な防御を可能にするアプリケーションプロキシを採用
- 未知の脅威からネットワークを守る標的型攻撃対策
- モバイルを含む接続デバイスをセキュアに管理



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

最新の技術を駆使したベストオブブリードのセキュリティ機能群が、ウォッチガードの独自OSであるFirewareで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。

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 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ブロックし、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ブロック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。

Threat Detection & Response (TDR)

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Host Sensor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。

DLP: Data Loss Prevention

情報漏えい対策

企業内ネットワークから外部ネットワークへの個人情報や機密情報の漏えいを防止します。外部に送信されようとしているテキスト本文や添付されたドキュメント内をスキャンし、特定のキーワードを含む情報が外部に送信されないように未然にブロックします。

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。

Mobile Security

モバイルセキュリティ

MUVPN(IPSec/SSL)またはWi-Fi接続時にコンプライアンスをチェックすることで、安全なモバイルデバイスのみネットワーク接続を許可します。iOSやAndroidが搭載されたスマートデバイスにFireboxと連携する専用アプリのFireClientをインストールして、デバイスのセキュリティ状況を把握し、安全と判断されたデバイスのみ接続を許可することで強固なセキュリティを確保します。

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。

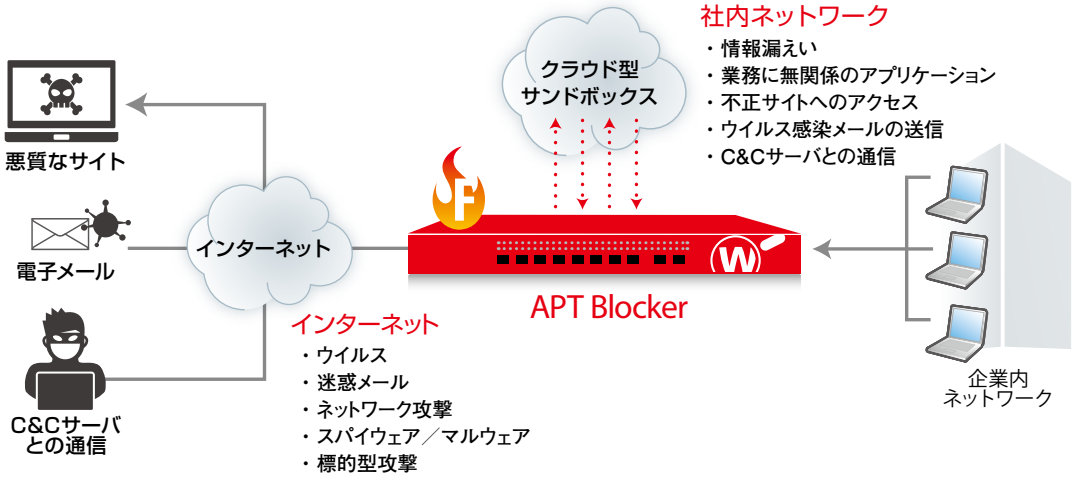
Solution1 変異し続ける悪質マルウェアからの防御

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

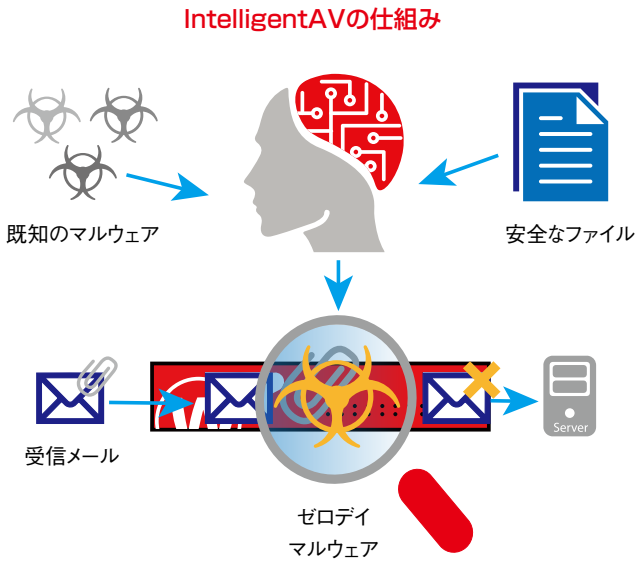
UTM/NGFWによる多層防御／APT Blockerによる標的型攻撃対策

- 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

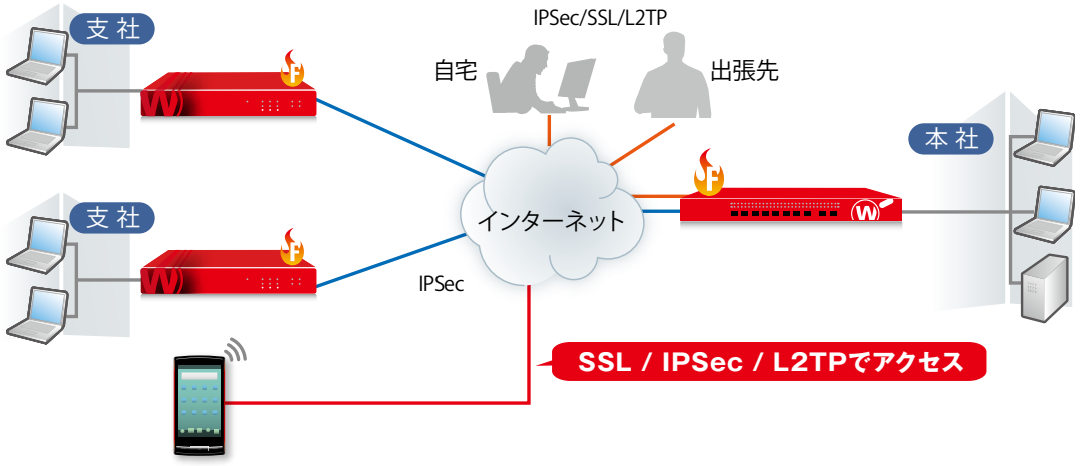


Solution2 拠点間の安全かつ高速な接続

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

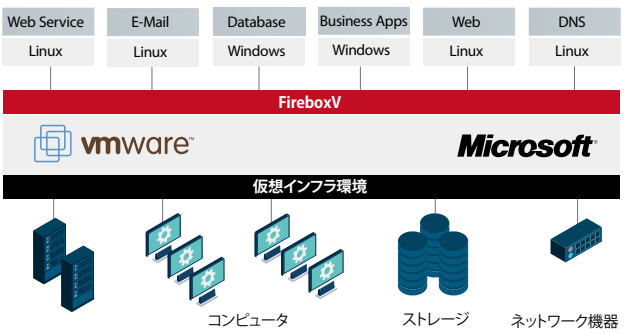


Solution3 仮想環境への導入と効率的な運用

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。

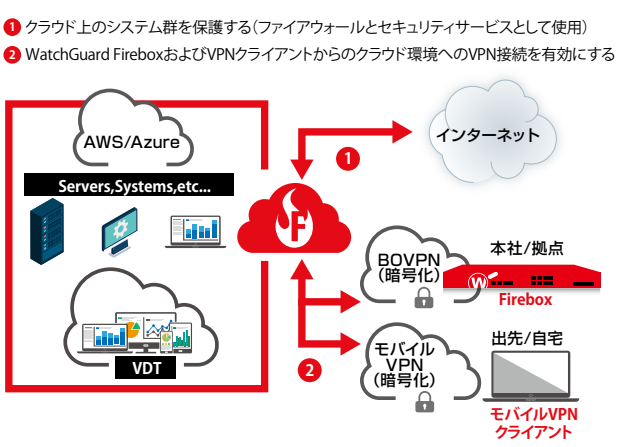
WatchGuard FireboxV（仮想アプライアンス）による仮想環境への対応

- 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 無線LANのセキュリティ対策／クラウド管理型無線LANソリューション

タブレット、スマートフォンおよびノートPCなどからの無線接続やBYOD（Bring Your Own Device）の普及により、無線LANネットワークに対するセキュリティの課題が増大しています。IT管理者やセキュリティ管理者には企業内の有線と無線LANの両者の安全性を確保することが求められています。

WatchGuardアクセスポイントによるセキュリティ

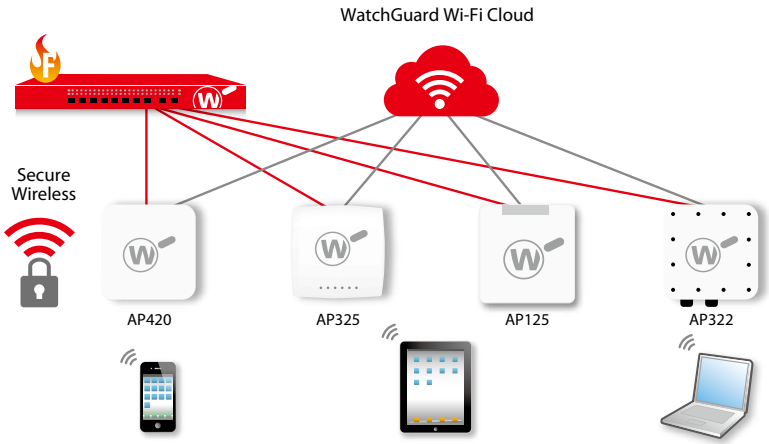
- ウォッチガード製品と連携し、シームレスに無線LANアクセスにもセキュリティを適用
- セキュリティポリシーの順守とデバイスの一元管理により管理負荷を大幅に軽減
- 先進のWatchGuard WIPS（特許取得済:ワイヤレス侵入防止システム）機能（※Wi-Fi Cloud利用時）

Mobile Security機能

- MUVPN（IPSec/SSL）またはWi-Fi接続時にコンプライアンスチェック
- Jailbreak（脱獄）の有無
- 端末内のマルウェア（Android端末）
- OSバージョン

WatchGuard Wi-Fi Cloud

- 大規模なWi-Fiネットワークの統合管理
- 階層化グルーピング、多拠点一括管理が可能な管理アーキテクチャ
- 無線の電波強度の状況を直感的に確認できるヒートマップ機能
- SNS認証の強化でビジネス分析を可視化
- カスタマイズされたスプラッシュページを通じたプロモーション施策



無線関連ソリューション

無線LANアクセスポイント

AP420/AP325/AP125/AP322

クラウド管理型ソリューションで
実現するセキュアな無線LAN

今日の市場における真のゲームチェンジャーであるWatchGuard Wi-Fi Cloudソリューションは、Wi-Fi環境に安全かつ保護された区域を提供するように設計されています。また、管理者の労力を取り除き、導入、管理コストを大幅に低減することが可能なソリューションです。特色のある包括的なエンゲージメントツールとビジネス分析の可視化ツールにより、ビジネスが成功するために必要な競争上の優位性を実現できます。

【主な特長（Wi-Fi Cloud 利用時）】

- 先進のWatchGuard WIPS（特許取得済:ワイヤレス侵入防止システム）を採用
- 大規模なWi-Fiネットワークの統合管理を実現
- パフォーマンスとセキュリティを同時に追求
- オンプレミスでの管理も可能
- SNS認証の強化でビジネス分析を可視化
- GO MobileAppを活用してモバイルデバイスから無線LANネットワークを管理
- カスタマイズされたスプラッシュページや特別なプロモーション施策を簡単に設定
- 無線の電波強度の状況を直感的に確認できるヒートマップ機能が利用可能
- RESTful API を採用したWatchGuard Wi-Fi Cloudにより大規模無線LANにも柔軟に対応
- 階層化グルーピング、多拠点一括管理が可能な管理アーキテクチャにより、無線LANの管理を簡素化
- クラウド管理型APとして屋内用・屋外用双方をラインアップ
- AP322は防塵防水規格IP67対応で屋外利用に最適

Mobile Security

Fireboxと接続し、無線LANアクセスポイント
でセキュアな企業内無線環境を構築

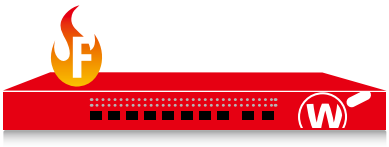
- 安全なモバイルデバイスのみネットワーク接続を許可
  - MUVPN（IPSec/SSL）またはWi-Fi接続時にコンプライアンスチェック
  - OSバージョン: 指定OSバージョン以外からは接続不可
  - Jailbreak（脱獄）の有無
  - マルウェア/ウイルスの有無（Androidのみ）
- Network Discoveryとの連携
  - ネットワークマップ上で、モバイルデバイスのコンプライアンスステータスが確認可能
- モバイルデバイスの利用状況とデバイスの状況を把握
- ライセンス（※別途購入オプション「FireClient」が必要）
  - ユーザ数に応じたWatchGuard FireClientライセンスの購入でMobile Security機能が利用可能
- モバイルデバイス向けアプリFireClient（ダウンロード無償）
  - モバイルデバイスへFireClientのインストールが必要
  - iOS 8以上、Android 4.1以上に対応

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

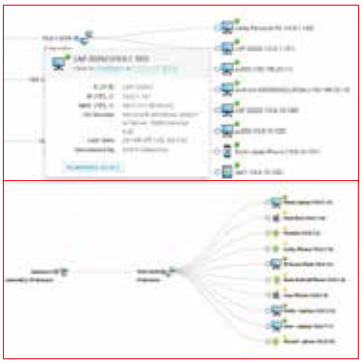
万が一、セキュリティの事故やマルウェアによる情報漏えいが発見されれば、企業の信頼性や収益にも大きな影響が出ます。セキュリティ管理者は常に企業ネットワーク内を監視し、不正なトラフィックを識別して迅速かつ的確な対処が求められます。

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、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）

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

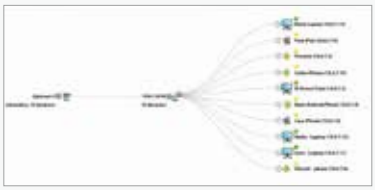
2. WatchGuard System Manager

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）

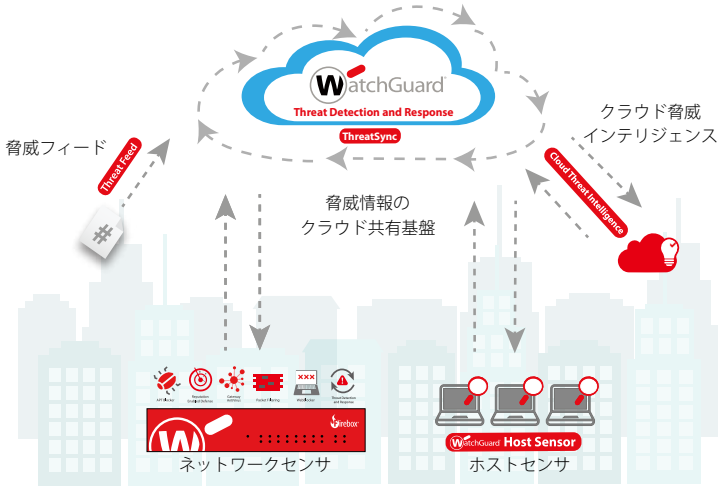


Solution6 相関分析、優先順位付け、レスポンス（Threat Detection & Response：TDR）

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、Host Sensor、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 Host Sensor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 Host Sensor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Host Sensor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 クラウドアプリケーションへの強力な認証ポータルシステム（Access Portal）

クラウドベースのアプリケーションによる業務の効率化やコスト削減が普及するなか、それらのアプリケーションへの認証を迅速かつ容易に実現する認証システムが必須となっています。クラウドリソースを活用する企業や組織のために開発されたWatchGuard Access Portalは、低コストでの認証システムを実現します。SAMLを始め各種認証機能と連携させる事が可能なため、Access Portalを企業のアイデンティティストア（認証ポータル）として活用できます。また、企業のイントラネット内へのRDPおよびSSHリソースへの一元的なアクセスを可能にするIT管理者のための認証ポータルとしても利用できます。

互換認証プロバイダの製品例

- Shibboleth
- OneLogin
- Okta
- ADFS（Active Directory Federation Services）

組み合わせ可能なソフトウェアトークン例

- RSA SecureID
- Duo Mobile
- OneLogin Protect
- Google Authenticator
- Okta Mobile

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

トランスペアレントモード

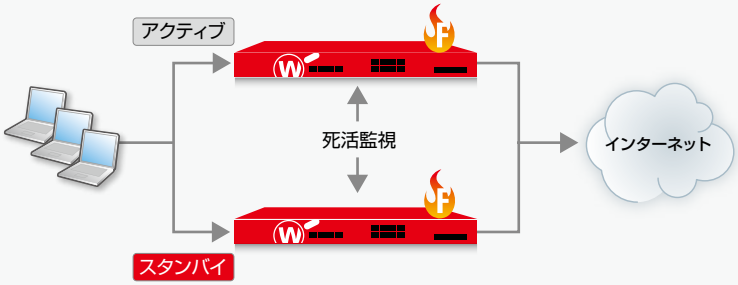
トランスペアレントモードを利用すれば、既存のネットワーク構成に変更を加えることなく、簡単に透過性をもたせることができます。必要な機能だけを容易に適用できるため、新規導入時のセキュリティ構成など、安心してネットワークセキュリティの構築が可能となり、他のネットワークサービスへの影響を考慮した導入プロセス計画を策定することができます。

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。

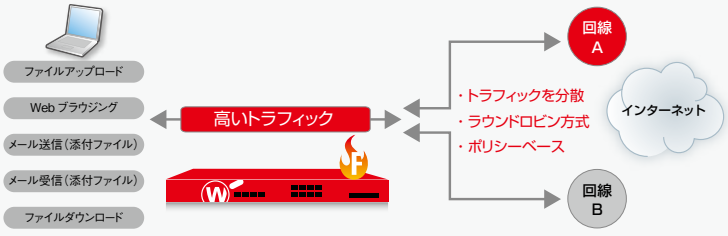
ハイアベイラビリティ（HA構成）

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。



マルチ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。ウォッチガードのマルチWAN負荷分散を導入し、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。アクセスする回線毎に重み付けの選択が可能で、高速回線:低速回線=2:1に設定するといったカスタマイズも自由に行えます。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、「Total Security Suite」と「Basic Security Suite」、「Support」の3タイプから選択可能です。

製品	Support	TOTAL SECURITY	Basic Security
ステートフルファイアウォール	✓	✓	✓
モバイルVPN	✓	✓	✓
ブランチオフィスVPN	✓	✓	✓
アプリケーションプロキシ	✓	✓	✓
不正侵入検知・防御（IPS）		✓	✓
アプリケーション利用の可視化と制御		✓	✓
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）		✓	✓
Network Discovery		✓	✓
標的型攻撃対策（サンドボックス）		✓	
情報漏えい対策（DLP）		✓	
Dimension Command		✓	
相関分析、優先順位付け、レスポンス（TDR）		✓	
Access Portal ※		✓	
DNSWatch		✓	
IntelligentAV ※		✓	
サポート	スタンダード（24x7）	ゴールド（24x7）	スタンダード（24x7）

※平日(9:00~18:00)以外は英語でのサポートとなります。
※Mobile Security機能の利用には、FireClientライセンスの購入が別途必要となります。
※IntelligentAV、Access Portal：Firebox M270以上で利用できます。

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 / Data Loss Prevention / Threat Detection & Response（TDR）/ DNSWatch / IntelligentAV
LiveSecurity Service/ 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	**T15/T15-W**	**T35/T35-W**	**T55/T55-W**	**T70**
スループットと接続				
FW スループット	400 Mbps	940 Mbps	1 Gbps	4 Gbps
VPN スループット	150 Mbps	560 Mbps	360 Mbps	740 Mbps
AV スループット	120 Mbps	325 Mbps	636 Mbps	1.2 Gbps
IPS スループット	160 Mbps	573 Mbps	636 Mbps	1.5 Gbps
UTM スループット	90 Mbps	278 Mbps	523 Mbps	1 Gbps
インターフェイス 10/100/1000	3	5	5	8
I/O インターフェイス	1 Serial / 1 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）	100,000	1,300,000	1,300,000	800,000
新規セッション数	2,400	6,800	9,500	27,000
VLAN サポート	10	50	75	75
認証ユーザ数	200	500	500	500
VPNトンネル数				
Branch Office VPN	5	25	40	50
モバイル VPN IPSec	5	25	50	60
モバイル VPN SSL/ L2TP	5	25	50	60
TDR Host Sensor 数※ （Total Security Suite 発注時バンドル数）	5	20	35	60
無線AP管理台数（参考値）※1 ※2 ※1 無線LANコントローラとして利用時 ※2 制限を設けているわけではありません	4	20	40	50

※Host Sensorアドオンオプション: 次に記載の数で追加可能です。10/25/50/100/250/500/1,000/2,500/5,000個のHost Sensors

	AP125	AP325	AP420	AP322
				
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）	2.400-2.474GHz、5.150-5.250GHz、5.250-5.350GHz、5.470-5.725GHz、5.725-5.850GHz		2.4-2.4835GHz、4.9-5.0GHz、5.15-5.25GHz(UNII-1)、5.25-5.35GHz、5.47-5.6GHz、5.650-5.725GHz(UNII-2)、5.725-5.85GHz(UNII-3)	2.400-2.474GHz、5.15-5.25GHz、5.25-5.35GHz、5.47-5.725GHz、5.725-5.825GHz
アンテナ数	4（内蔵、全方向性）	6（内蔵、全方向性）	10（内蔵、全方向性）	6（内蔵、全方向性）
周波数帯	5GHz / 2.4GHz			
Tx/Rx ストリーム	2x2 MIMO		4x4 MIMO	3x3 MIMO
最大転送速度	11ac(866 Mbps)、11n(300 Mbps)		11ac(1.3 Gbps)、11n(450 Mbps)	
最大送信出力	20 dBm		27 dBm	20 dBm
SSID	8			
セキュリティ	WPA-PSK、WPA2-PSK、WPA-PSK/WPA2-PSK (Mixed)、WPA-802.1X (Enterprise) WPA2-802.1X (Enterprise)、WPA-802.1X/WPA2-802.1X (Mixed)、TKIP、AES、TKIP/AES、Captive Portal、MAC whitelist/blacklist、VLAN Tagging			
イーサネット	2 x 1 Gb			
電源	PoEインジェクタ（オプション）、A/Cアダプタ（オプション）			PoEインジェクタ（オプション）
IEEE準拠規格	802.11a/b/g/n/ac、802.11i、802.1q、802.1X、802.3af/at（AP125除く）、802.3af（AP125のみ）、802.11e、802.11ac Wave2 対応			802.11a/n/ac, 802.11b/g/n, 802.3at

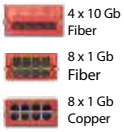
WatchGuard Network Security Products（中規模オフィス向け）

Firebox M Series

Firebox M270/M370

Firebox M440

Firebox M470/M570/M670



モデル	M270	M370	M440	M470	M570	M670
スループットと接続						
FW スループット	4.9 Gbps	8 Gbps	6.7 Gbps	19.6 Gbps	26.6 Gbps	34 Gbps
VPN スループット	1.6 Gbps	4.6 Gbps	3.2 Gbps	5.2 Gbps	5.8 Gbps	7.6 Gbps
AV スループット	2.1 Gbps	3.0 Gbps	2.2 Gbps	3.5 Gbps	5.4 Gbps	6.2 Gbps
IPS スループット	2.3 Gbps	4.8 Gbps	2.2 Gbps	5.7 Gbps	8.0 Gbps	10.4 Gbps
UTM スループット	1.6Gbps	2.6 Gbps	1.6 Gbps	3.1 Gbps	4.4 Gbps	5.4 Gbps
インターフェイス 10/100/1000	8	8	25 1G copper 2 10G SFP +	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	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	制限なし	制限なし
同時接続（双方向）	2,000,000	3,300,000	4,000,000	3,800,000	8,300,000	8,500,000
新規セッション数	40,000	51,000	62,000	62,000	115,000	140,000
VLAN サポート	100	200	400	300	500	750
認証ユーザ数	制限なし	制限なし	制限なし	制限なし	制限なし	制限なし
VPNトンネル数						
Branch Office VPN	50	100	300	250	500	750
モバイル VPN IPSec	75	100	300	250	500	750
モバイル VPN SSL /L2TP	75	100	300	250	500	750
TDR Host Sensor 数※ （Total Security Suite 発注時バンドル数）	60	150	250	200	250	250
無線AP管理台数（参考値）※1 ※2 ※1 無線LANコントローラとして利用時 ※2 制限を設けているわけではありません	60	80	100	100	150	175

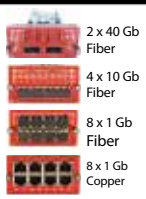
※Host Sensorアドオンオプション：次に記載の数で追加可能です。10/25/50/100/250/500/1,000/2,500/5,000個のHost Sensors

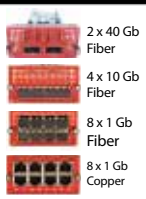
FireboxV

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	M4600	M5600
スループットと接続		
FW スループット	40 Gbps	60 Gbps
VPN スループット	10 Gbps	10 Gbps
AV スループット	9 Gbps	12 Gbps
IPS スループット	13 Gbps	18 Gbps
UTM スループット	8 Gbps	11 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	2 Serial / 2 USB
ノード数（LAN IPs）	制限なし	制限なし
同時接続（双方向）	7,500,000	12,700,000
新規セッション数	160,000	240,000
VLAN サポート	1,000	制限なし
認証ユーザ数	制限なし	制限なし
VPNトンネル数		
Branch Office VPN	5,000	制限なし
モバイル VPN IPSec	10,000	制限なし
モバイル VPN SSL / L2TP	10,000	制限なし
TDR Host Sensor 数※ （Total Security Suite 発注時バンドル数）	250	250
無線AP管理台数（参考値）※1 ※2 ※1 無線LANコントローラとして利用時 ※2 制限を設けているわけではありません	200	300

※Host Sensorアドオンオプション：次に記載の数で追加可能です。10/25/50/100/250/500/1,000/2,500/5,000個のHost Sensors

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

進化するセキュリティ対策をより安全で、シンプルに

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

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）

サポート&メンテナンス

LiveSecurity Service/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

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

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、業界標準ハードウェア、ベストオブブリードセキュリティ、ポリシーベースの管理ツールを独自アーキテクチャにより統合したビジネスセキュリティソリューションを提供するグローバルリーダとして、全世界の企業にエンタープライズクラスのセキュリティソリューションを提供しています。本社を米国ワシントン州シアトルに置き、北米、ヨーロッパ、アジア太平洋地区、中南米に支社を展開しています。日本法人であるウォッチガード・テクノロジー・ジャパン株式会社は、多くのパートナーを通じて、アプライアンス製品、セキュリティの「可視化」、セキュリティとネットワークの「管理」など拡大するニーズへのソリューションを提供しています。詳細は https://www.watchguard.co.jp をご覧下さい。

WatchGuard

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

■ お問い合わせ先

PN201903