今日のハイブリッド環境に適したセキュアな接続

はじめに

リモートワークとハイブリッドネットワーク（オンプレミスとクラウドソリューション）への移行は、サイバーセキュリティの状況を大きく変えました。オンプレミスのファイアウォールやVPN に依存する従来のネットワークセキュリティモデルでは、分散した従業員を効果的に保護することは困難です。

ウォッチガードの FireCloud Internet Access は、ウォッチガードのセキュアサービスエッジ（SASE）戦略における第一弾のリリースであり、世界中の様々な場所からインターネットやクラウドアプリケーションにアクセスするリモートワーカーを保護するという課題に対応しています。このソリューションは、Firebox ファイアウォールの強固な保護機能をリモート従業員に拡張し、ユーザーエクスペリエンスを向上させるとともに、グローバル規模でセキュリティポリシーを統一し、管理を大幅に簡素化することができます。

課題：分散したワーカーの安全を守る

リモートワークやハイブリッドワークの拡大により、異なるネットワーク間でのセキュリティポリシーの一貫性の欠如、保護されていないホームネットワークやパブリックネットワークによる攻撃対象領域の拡大、従来の VPN ソリューションに伴うパフォーマンスのボトルネック、および IT チームに求められる複雑な管理要件など、新たなセキュリティ上の課題が発生しています。企業がクラウドベースのアプリケーションやサービスを利用するようになるにつれ、場所に関係なくシームレスで安全な接続を保証するセキュリティソリューションの必要性が高まっています。

ソリューション概要：ウォッチガードの FireCloud Internet Access

FireCloud Internet Access は、インターネットやクラウドアプリケーションにアクセスするリモートワーカーを、場所に関係なく保護するために設計されたクラウド配信型の SASE ソリューションです。グローバルな PoP（ポイントオブプレゼンス）ネットワーク上に構築され、一貫したセキュリティの実行と最適化されたパフォーマンスを提供します。機能として、クラウド配信型のファイアウォール保護を提供するファイアウォール・アズ・ア・サービス、URL フィルタリング、マルウェアスキャン、アプリケーション制御を含むセキュア Web ゲートウェイ、そして悪意のあるドメインをブロックし、DNS ベースの攻撃を防止する DNS フィルタリングなどがあります。

主な特長とメリット

高度なセキュリティ

FireCloud Internet Access は、マルウェア、ランサムウェア、フィッシング攻撃などの脅威がユーザーに到達する前に防御することで、プロアクティブに脅威を防止します。そしてグローバル規模のセキュリティポリシーを適用し、ユーザーとデバイスが承認された Web サイトやアプリケーションにのみアクセスできるようにするため、マルウェア感染の可能性を最小限に抑えます。

- **Web ブロッキングとコンテンツフィルタリング：**リモートワークとハイブリッドネットワーク（オンプレミスとクラウドソリューション）への移行は、サイバーセキュリティの状況を大きく変えました。オンプレミスのファイアウォールや VPN に依存する従来のネットワークセキュリティモデルでは、分散した従業員を効果的に保護することは困難です。

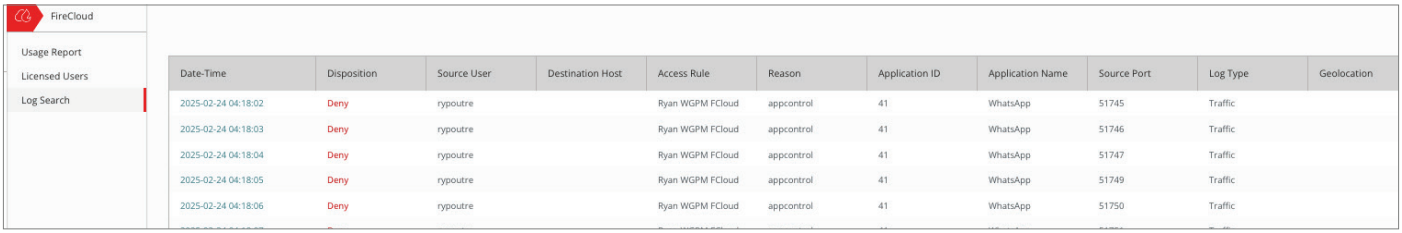

図1：FireCloudログUI（ブロックされたトラフィックのフィルタリング表示）

- **ジオロケーションフィルタリング：**FireCloud 独自のジオロケーション機能により、管理者は地理的な場所に基づいてネットワークトラフィックを検知し、制御することができます。ジオロケーションフィルタリングを有効にすることで、特定の国や地域からのアクセスをブロックし、リスクの高い場所から発信される潜在的なサイバー脅威にさらされる機会を減らすことができます。この機能は、信頼できる地理的な地域のみに接続を制限することでセキュリティを高め、サイバー攻撃に対する組織の防御能力をさらに強化します。

- **ボットネット検知とネットワークブロッキング：**FireCloud は、ボットネット検知や侵入防止などの高度なネットワークブロッキング機能を提供します。ボットネット検知機能は、既知のボットネット IP アドレスの最新リストを維持し、自動的にブロックサイトリストに追加することで、ユーザーが悪意のあるドメインに接続できないようにします。さらに、FireCloud の侵入防止サービス（IPS）は、リアルタイムのシグネチャベースの検知機能を利用して、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攻撃を防御します。管理者は、脅威が検知されたときに適切なアクションを実行するように IPS 設定を構成し、プロアクティブにネットワークを保護できます。

シンプルな導入と管理

FireCloud のセキュリティポリシーは、WatchGuard Cloud で集中管理することで Firebox のポリシーを強化します。管理者は単一のインターフェイスからセキュリティポリシーを設定・適用することができ、Firebox と FireCloud の両方で一貫したポリシー構造と用語を用いることで管理を簡素化することができます。

管理者は、WatchGuard Cloud から FireCloud エージェントをターゲットデバイスとして簡単に設定することができます。セキュリティの設定が保存されると、WatchGuard がホストする世界中のすべての PoP に自動的に展開されるため、ユーザーの所在地に関係なく、一貫したポリシーの適用が保証されます。

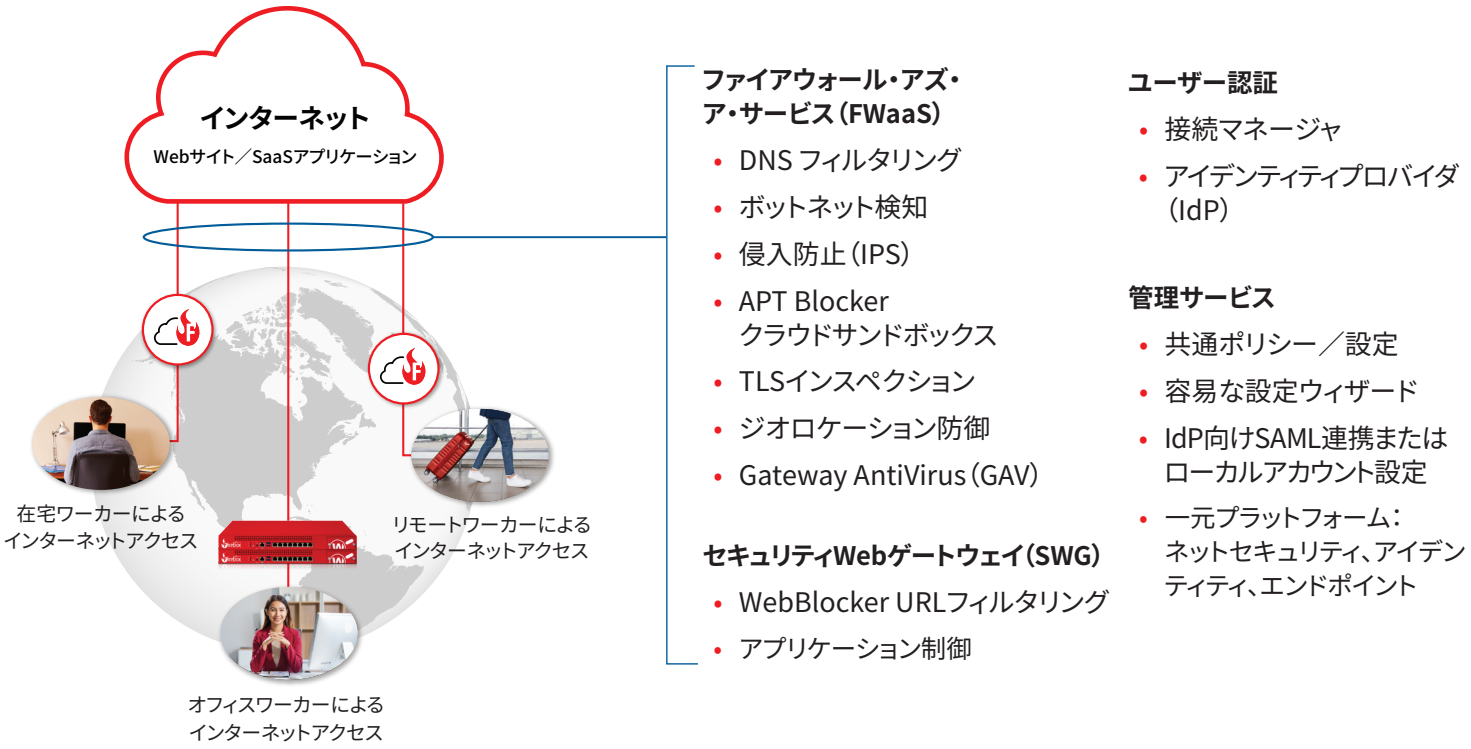

図2：FireCloud Internet Accessでリモートワーカーにfirebox保護機能を拡張

ユーザーエクスペリエンスの向上

PoP のグローバルネットワークを介した最適化されたルーティングが遅延時間を短縮し、クラウドベースのアプリケーションやサービスへのシームレスなアクセスを可能にします。また、スケーラブルなアーキテクチャにより、企業は増加する帯域幅需要に難なく対応できます。従業員は、接続やセキュリティ保護に支障をきたすことなく、オフィスやリモート勤務に関係なく同一の環境で業務を遂行することができます。

ダッシュボードとレポーティング

FireCloud のレポーティング機能では、直感的なダッシュボードを通じて、ネットワークアクティビティ、セキュリティイベント、ユーザー接続に関する包括的な知見データを提供します。FireCloud の利用状況レポートはリアルタイムおよび履歴データを提供し、管理者はトラフィックパターンの監視、セキュリティポリシーの適用、そしてパフォーマンスの最適化を行うことができます。

- **セキュリティ分析ビュー：**セキュリティタブでは、ネットワーク脅威とブロックされたトラフィックに関する詳細なデータを提供します。管理者は、FireCloud によって阻止された攻撃試行や防御されたマルウェア脅威の頻度を示す折れ線グラフなどで攻撃防御の状態を把握できるなど、特定のセキュリティイベントを調べることができます。APT Blocker によって特定されたゼロデイマルウェアは、WebBlocker によりブロックされた URL カテゴリの内訳とともにハイライト表示されます。また、ブロックされたアプリケーション、ブロックされたユーザーリクエスト、および最も頻繁にブロックされた宛先と通信プロトコルの上位を特定します。ジオロケーションフィルタリングは、ブロックされたトラフィックの国別の地理的内訳を表示し、管理者が場所に基づいてセキュリティアクションを評価できるようにします。

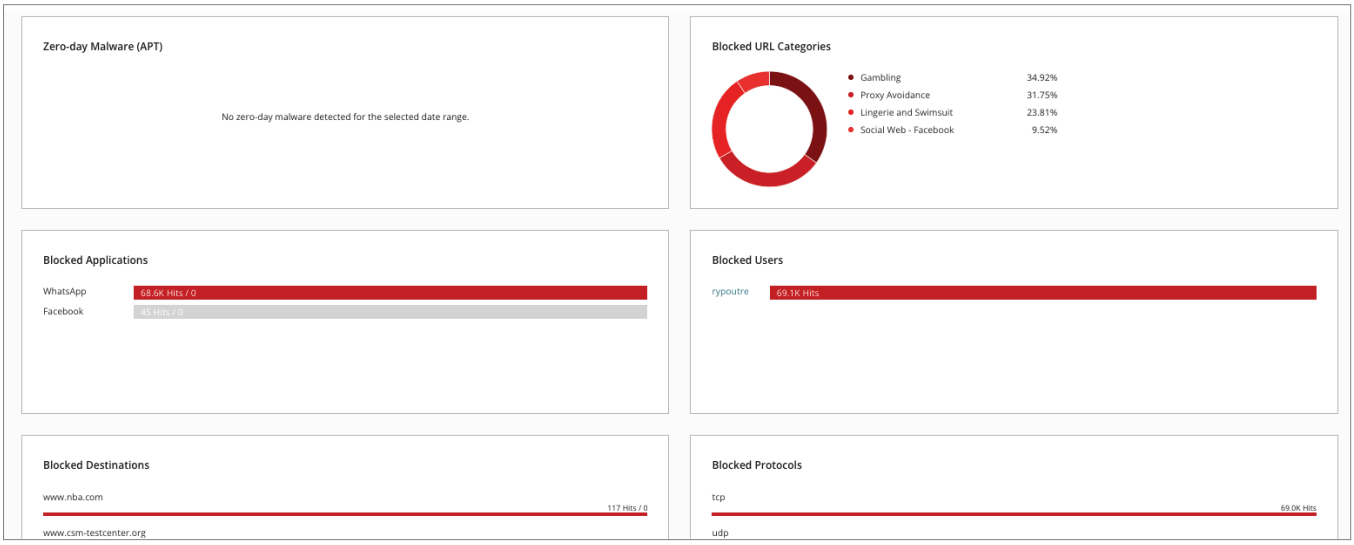

図3：FireCloudセキュリティレポートで防御されたトラフィックとユーザーの詳細を表示

- **トラフィックインサイトビュー：**トラフィックタブには、許可されたネットワークアクティビティの概要が表示され、ユーザーの行動やアプリケーションの利用状況についての知見データが得られます。最もアクセスされているアプリケーションのカテゴリや個々のアプリケーション、頻繁にアクセスされている Web サイトやドメインの詳細が表示されます。最もアクティブな FireCloud ユーザーに関する情報は、頻繁にアクセスされる場所や通信プロトコルに関するデータとともに表示されます。承認されている接続の地理的な表示も可能で、さまざまな地域におけるネットワークアクティビティの程度を知ることができます。

- **ユーザーアクティビティとデバイス監視ビュー：**ユーザータブは、認証されたユーザーの詳細、デバイス情報、およびユーザーグループのメンバーを含む、ユーザー固有のデータを追跡できます。管理者は、ユーザーが接続したデバイス、グループに基づいた各ユーザーに適用されているセキュリティポリシー、および接続デバイスで実行されているクライアントとオペレーティングシステムのバージョンを確認できます。フィルタを適用してユーザリストを絞り込むことができるため、非アクティブユーザーやインストールされているクライアントバージョンをユーザーごとに容易に特定できます。

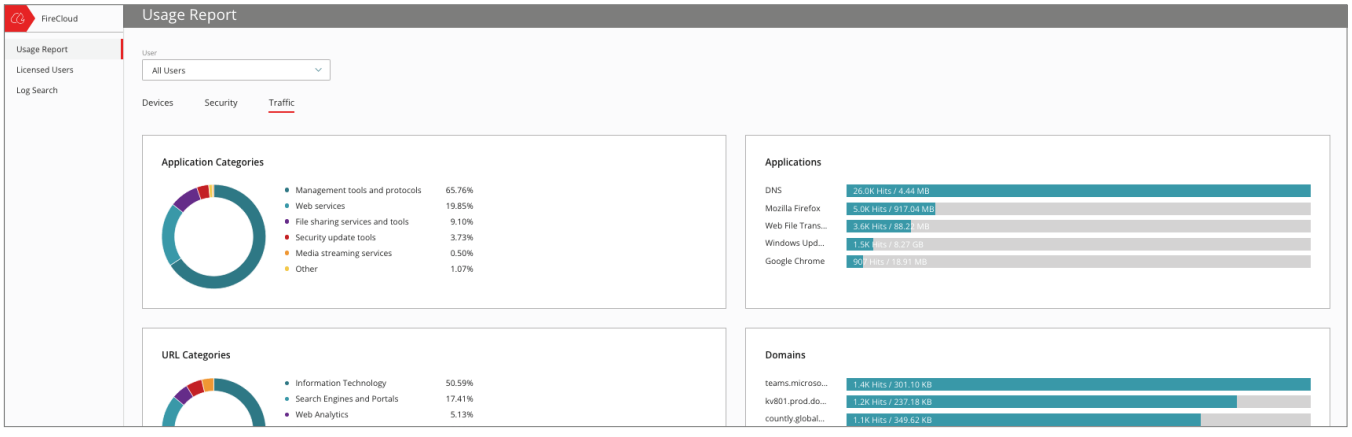

図4：FireCloudの利用状況レポートで、アプリケーションや宛先における上位のユーザーアクティビティの詳細を表示

あらゆるユースケースに対応

リモートワークの安全を確保

リモートワークを導入する組織では、従来の VPN に頼ることなく従業員を保護するセキュリティソリューションが必要です。FireCloud Internet Access は、クラウドアプリケーションへのセキュアかつダイレクトな接続を可能にし、パフォーマンスのボトルネックを解消するとともに、従業員がどこで作業しているかに関係なく、統一されたセキュリティを適用することができます。

巧妙な脅威から保護

ランサムウェア、フィッシング、マルウェアなどの最新のサイバー脅威には、プロアクティブなセキュリティ対策が必要です。FireCloud Internet Access は、ネットワークトラフィックをリアルタイムで検査し、悪意のあるアクティビティがユーザーに到達する前にブロックします。クラウドベースの脅威インテリジェンスを活用することで、新たなサイバー脅威に対抗できるように継続的に更新され、データ漏洩やサイバー攻撃のリスクを最小限に抑えます。

統一されたセキュリティポリシーを適用

分散した従業員全体で一貫したセキュリティポリシーを維持することは困難です。FireCloud Internet Access は、すべてのユーザーとデバイスにセキュリティルールを設定・適用することで、ポリシーの適用を簡素化します。WatchGuard Cloud を介した一元管理により、シームレスなポリシーの展開と、組織全体に対する統一されたセキュリティ基準が保証されます。

FireCloud の特長

- **ハイブリッド：**FireCloud Internet Access の大きな特長として、導入されている既存の WatchGuard Firebox とシームレスに統合できるハイブリッドセキュリティアプローチを提供していることが挙げられます。導入が容易で一元管理できるため、IT 管理が簡素化されます。また、費用対効果の高い価格モデルにより、Zscaler や Fortinet といった競合他社に代わる魅力的な選択肢となっています。
- **優れた包括性：**ファイアウォール・アズ・ア・サービス、セキュア Web ゲートウェイ、DNS フィルタリングの組み合わせにより、今日の職場環境に適した包括的なセキュリティソリューションを提供します。
- **容易な管理：**FireCloud は Firebox や WatchGuard Cloud と統合されているため、オンプレミスとクラウド／ SaaS アプリケーションの両方で、オフィス内とリモートワーカーを問わず単一のセキュリティポリシーを定義することができます。少人数の IT チームや MSP にとって、このアプローチは他の SASE 製品に比べ、より容易な管理、一貫したセキュリティ制御、および低コスト化を実現します。
- **容易な導入：**FireCloud は WatchGuard EPDR と同じユニバーサルエージェントを使用しており、軽量で安定した SASE クライアントを実現しています。WatchGuard のグローバル PoP インフラと WatchGuard Cloud の集中管理方式と組み合わせることで、FireCloud はよりシンプルで容易に導入することができます。
- **卓越した統合性：**ウォッチガードの脅威検知／レスポンススタックへの統合により、セキュリティがさらに強化されます。FireCloud のログは ThreatSync に取り込まれ、リモートワーカーのユースケースに対応する統一された相関性のある脅威検知／レスポンスを実現します。これにより、MSP はリスクと脅威対策として既存環境を継続的に監視しつつ、優れた SASE ソリューションを提供することができます。

まとめ

企業がリモートワークやクラウドベースのアプリケーションを採用し続ける中、分散したワーカーのセキュリティ確保が優先事項となっています。ウォッチガードの FireCloud Internet Access は、包括的でクラウドネイティブなセキュリティを提供し、保護能力を強化、IT 管理の簡素化、そしてネットワークパフォーマンスの向上を可能にします。FireCloud は、主要なセキュリティ機能を単一の管理しやすいプラットフォームに統合することで、マネージドサービスプロバイダーが優れたリモートワーク向けのセキュリティサービスを提供し、組織が今日のサイバーセキュリティの課題に自信を持って対処できるようになります。

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。ウォッチガードの 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、および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。ウォッチガードの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。同社は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。詳細は https://www.watchguard.co.jp をご覧下さい。

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　Email：jpnsales@watchguard.com　www.watchguard.co.jp

本資料では明示的および暗示的な保証は一切しておりません。全ての製品、特徴、機能性の仕様は将来必要に応じて変更される可能性があります。© 2025 WatchGuard Technologies, Inc. All rights reserved.
WatchGuard、WatchGuard ロゴ、Firebox は米国および／またはその他の国の WatchGuard Technologies の商標または登録商標です。その他の商標は各社に帰属します。作成日：2025 年 4 月