SOLUTION BRIEF

拡大する攻撃対象領域を保護する次世代ファイアウォール：FortiGate NGFW

概要

新しいデジタルイノベーションの普及により、企業ネットワークが変化しています。画期的な機能が追加されると同時に、新たな脆弱性も見つかっています。モバイルワーカー、複数のパブリッククラウドやプライベートクラウド、IoT デバイスの急増に伴い、ネットワークの攻撃対象領域が劇的に拡大しています。これにより、成長を続ける企業はセキュリティの確保がさらに困難になります。フォーティネットの次世代ファイアウォール（NGFW）ソリューションでは、新たな脅威やますます複雑化するネットワークに対し、広範にわたる統合型の自動保護を実現します。進化するネットワークを保護することができるエンドツーエンドのセキュリティアーキテクチャを有するフォーティネット セキュリティ ファブリックと一体となって機能します。

フォーティネットの NGFW

- 高性能な脅威保護
- 立証済みのセキュリティ効果
- ミッションクリティカルなアプリケーションの保護
- セキュリティレーティングと自動化による継続的なリスク評価
- フォーティネット セキュリティ ファブリックとの統合
- エンタープライズクラスのセキュリティ管理

ネットワークの分散による攻撃対象の拡大

新しいテクノロジーは企業ネットワークの拡大をもたらしています。これにより、クラウド環境、地理的に分散したオフィス、エンドポイントデバイスの増加や多様化が進展しています。80% 近くの組織が、デジタルイノベーションの導入に対してサイバー攻撃の防御能力が追いついていないと回答しています [1]。

攻撃者はこうした無防備な状況を十分に把握しています。そして彼らは、これまで拡大してきたネットワーク領域の最大の弱点に狙いを定めています。高度な戦略（マルチベクター攻撃、多形攻撃など）や自動化されたプロセスで防御を突破し、機密情報を盗み出したり、身代金と引き換えにオペレーションをロックダウンしたりします。

ネットワークエンジニアリングやオペレーションのリーダーは状況を乗り切ろうにも、暗号化データを完全に可視化できないだけでなく、アプリケーション、データ、ユーザー、複数のネットワークエッジにわたるネットワークインフラストラクチャの制御もできないことへの不安が拭えません。多くの組織において、ネットワークのサイロ内で動作するポイントセキュリティ製品はばらばらに運用されており、しかも数が非常に多く、複雑さが増すだけになってしまっています。平均的な企業では 75 種類のセキュリティソリューションが使用されていますが、その多くは単一の攻撃ベクターまたはコンプライアンス要件のみに対応しています [2]。その結果、セキュリティ態勢の効果が低下しています。

ネットワークセキュリティの進化を促進

セキュリティの効果を向上させるために、ネットワークエンジニアリングやオペレーションのリーダーは、組織全体に展開されているさまざまなセキュリティソリューション間の互換性を強化することが求められます。彼らに必要なのは、脅威インテリジェンスをリアルタイムで共有できるセキュリティ、安定した信頼性の高いネットワークパフォーマンス、レスポンスを調整および自動化するオープン API（アプリケーションプログラミングインタフェース）、一体化されたコンソールでの簡素化されたセキュリティ管理です。

企業としては、IoT から複数のクラウドまで、さらにユーザーからデータまで、拡大する攻撃対象領域全体を保護することが求められます。具体的には、SSL（セキュアソケットレイヤー）インスペクション / TLS（トランスポートレイヤーセキュリティ）インスペクションを実施し、暗号化されたフロー内のマルウェアを検知することが挙げられます。

フォーティネットの FortiGate NGFW ソリューションでは、IT インフラストラクチャ全体でより連携的で統合型のアプローチを採用することで、こうしたニーズにすべて対応することができます。

フォーティネットの FortiGate NGFW

FortiGate NGFW は、セキュリティの複雑さを軽減し、アプリケーション、ユーザー、ネットワークの可視化を実現します。また、FortiGuard Labs が提供する専用のセキュリティプロセシングユニット（SPU）と脅威インテリジェンスのサービスを活用し、既知の攻撃に対する最高レベルのセキュリティと高パフォーマンスの脅威保護（侵入防御、Web フィルタリング、マルウェア防御、アプリケーション制御など）を提供します。未知の攻撃は、フォーティネットのオンプレミスおよびクラウドベースの高度な脅威防御ソリューションによって検知および防御されます。

広範なフォーティネット セキュリティ ファブリック アーキテクチャと一体化した FortiGate NGFW は、自動化されたポリシーベースのレスポンスを活用するため、解決までの時間が短縮されます。FortiGate NGFW がイベントを検知すると、セキュリティ ファブリックで情報交換が行われ、企業全体で共有される情報が決定されます。たとえば、組織の一部でマルウェアが検知された場合、セキュリティ ファブリックはその組織の他の IT インフラストラクチャと脅威インテリジェンスを共有します。別の例では、あるセキュリティソリューションに対してポリシーが作成されると、セキュリティ ファブリックはコンテキストに応じて、同じポリシーをアーキテクチャ内の他のセキュリティソリューションに適用させ、一貫性のある組織的な制御を実現します。

企業によっては、パフォーマンスの低下を最小限に抑えながら SSL / TLS インスペクション、IPS、アンチウイルスなどのセキュリティ機能を個別または複数同時に実行する必要がある場合もあります。FortiGate NGFW では、こうした企業特有のセキュリティニーズに合わせた柔軟な展開が可能です。組織のネットワークインフラストラクチャで展開される FortiGate デバイスは、すべてセキュリティ ファブリックを介して相互接続されます。この統合により、包括的なリアルタイム保護が実現すると同時に、展開が簡素化されるため、企業全体で複数のタッチポイントやポリシーの必要性が軽減されます。

フォーティネット NGFW のユースケース

- **複雑さを軽減：**製品とサービスを統合してコストを削減し、ROI（投資収益率）を最大化します。
- **暗号化されたクラウドアクセス：**クリアテキストから暗号化（SSL / TLS）まで、あらゆる種類のトラフィックをインスペクションすることで、透明性と制御を実現します。
- **可視化と自動化：**ネットワークやセキュリティイベントにアクセスしてコンテキストの可視性を確保しながら、自動化されたプロセスで運用を簡素化します。

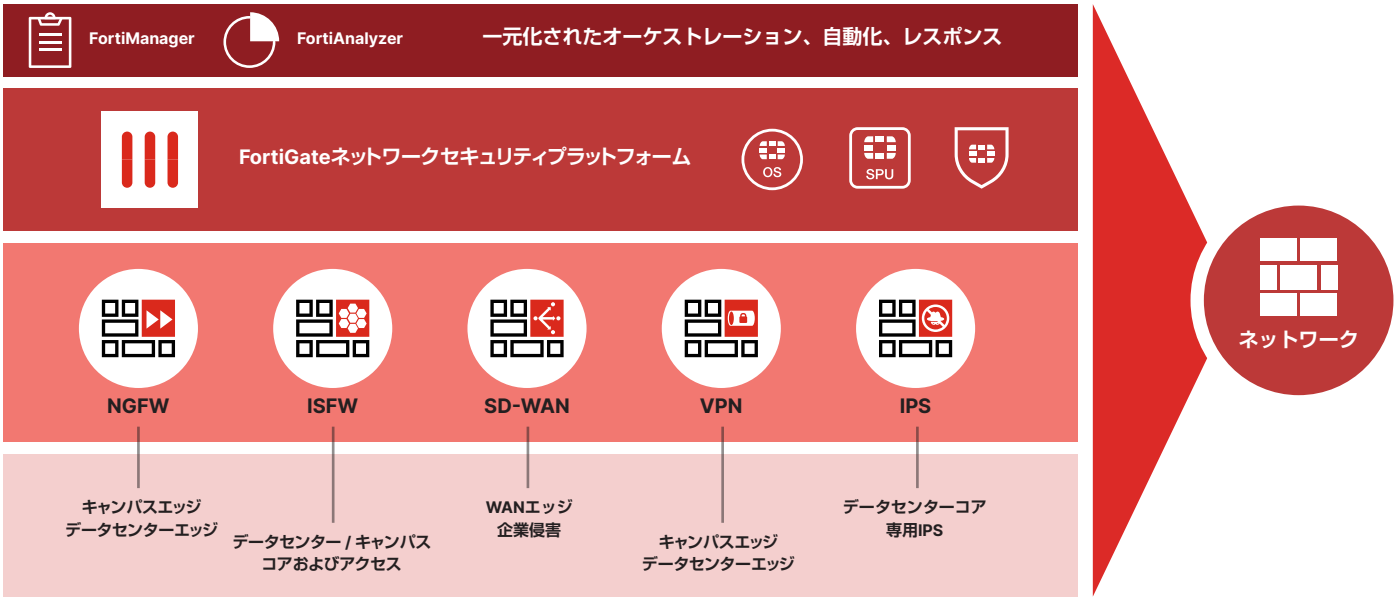

図 1：フォーティネットの次世代ファイアウォール（NGFW）ソリューション

業界トップのセキュリティ効果

脅威の状況に関する広範な知識と複数のレベルで迅速に対応する能力の連携は、効果的なネットワークセキュリティを実現する基盤となります。こうしたことから、FortiGuard 脅威インテリジェンス（多数のゼロデイ脅威や脆弱性を発見して高い評価を獲得 [3]）のサービスが重要な成功要因となって、フォーティネットの NGFW 機能は世界クラスを維持しています。

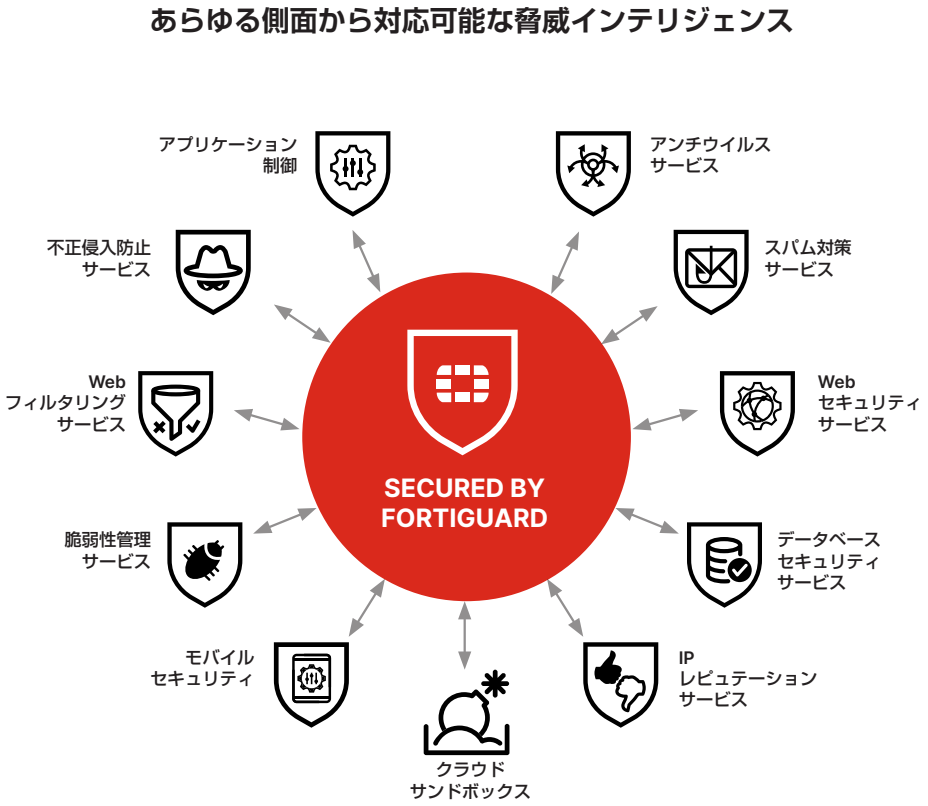

図 2：あらゆる側面から対応可能な FortiGuard Labs の脅威インテリジェンス

FortiGuard のグローバルな脅威リサーチチームは、フォーティネットの製品開発チームと緊密に連携し、動的なセキュリティインテリジェンスのサービスを提供しています。セキュリティの更新は瞬時に実行され、自動的にサードパーティの研究ラボで独立的に検証されます。これにより、極めて正確かつ効果的な脅威インテリジェンスを可能にします。

フォーティネットが、NSS Labs、Virus Bulletin、AV-Comparatives [4] などの実際のセキュリティ効果テストで、一貫して高い評価を得ている主な理由の 1 つとして、社内調査、業界専門の情報、高度な機械学習機能の組み合わせが挙げられます。

運用の簡素化

柔軟な展開オプションを備えるフォーティネット NGFW 独自の単一プラットフォームアプローチは、購入、展開、管理が容易なエンドツーエンドの保護を実現します。一元化されたセキュリティ管理と可視性により、複数の管理コンソールが一体化され、自動化された管理が可能になります。特に、アプリケーション、ユーザー、デバイス、脅威、クラウドサービスの使用状況、詳細なインスペクションにおいては、ネットワークエンジニアリングおよびオペレーションリーダーが極めて直感的に、ネットワーク上で起こっていることをより的確に把握できるようになります。こうした戦略的なビューにより、セキュリティやネットワークのリソースを最適化できるポリシーをより詳細に作成したり管理したりすることが簡単にできるようになります。

図 3：FortiManager のダッシュボードビュー

ネットワークリーダーは、トラフィックをクリアに監視したり、詳細なセキュリティ制御で統合型のポリシーを設定したりすることができます。ネットワーク管理は、ログ作成、レポート、一元管理を行う単一のコンソールを介して、自動化と分析の両方に対応します。

拡大する企業全体で 1 つの NGFW ソリューション

フォーティネット セキュリティ ファブリックの基盤となる FortiGate NGFW は、高パフォーマンスな企業ネットワーキングの要求が高まった場合でも保護することができます。FortiGate NGFW は、専用のセキュリティプロセッサテクノロジーを採用し、これにより、業界をリードするセキュリティ効果や統合を実現しながら、極めて高いスループットと並外れた低レイテンシーを実現します。

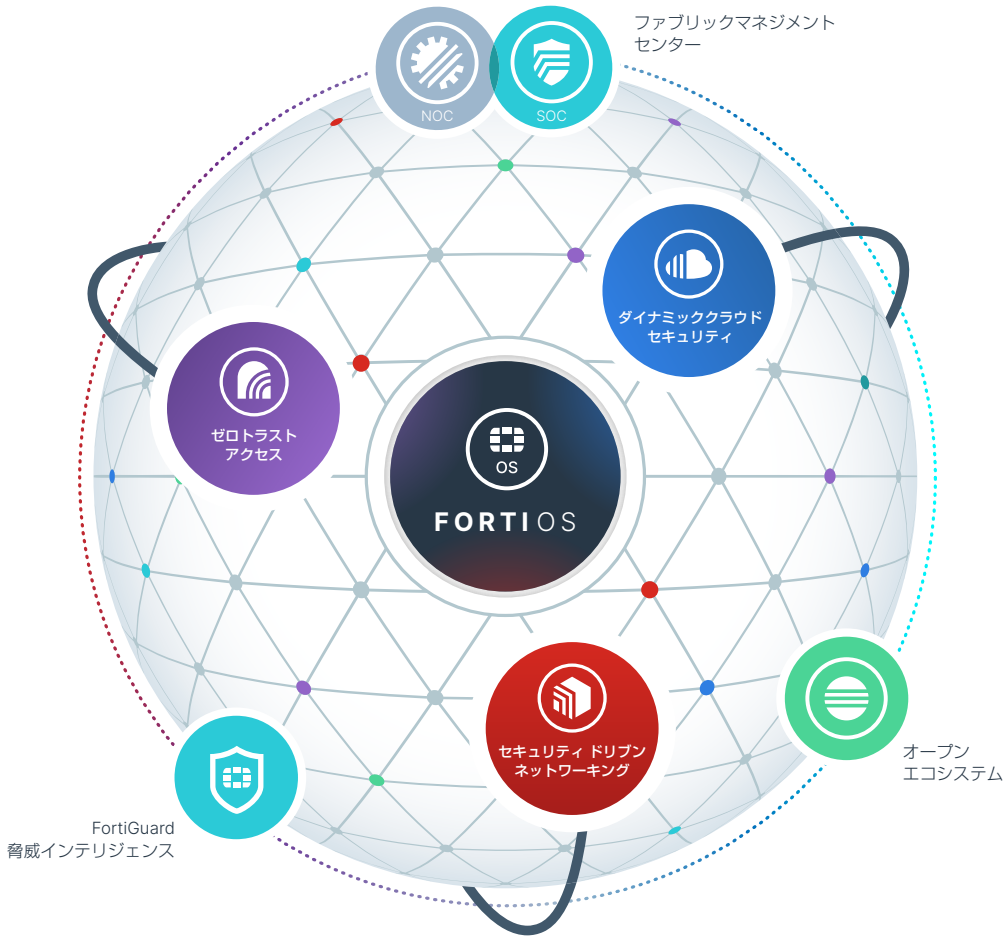

図 4：フォーティネット セキュリティ ファブリック アーキテクチャ

FortiGate NGFW ファミリーには、さまざまな価格 / パフォーマンス別に柔軟性の高い一連のプラットフォームが用意されています。エンタープライズエッジ、データセンターエッジ、分散型企業の支社に展開することができ、複数のクラウドへの安全なアクセスを提供します。さらに、FortiGate NGFW は、インテント ベースト セグメンテーションソリューションの一部としてデータセンター内に展開することもできます。インテント ベースト セグメンテーションは、フラットネットワークやオープンネットワークにパーティションを作成して、攻撃対象領域を減らします。

また、適応型アクセス制御を適用し、ユーザーとデバイスの継続的な信頼を確立します。これは、ユーザーとエンティティの行動分析（UEBA）に基づいて行われます。

長期にわたる広範かつ動的な防御戦略の実現

フォーティネットの NGFW では、あらゆるタイプの展開に対応するユニバーサルプラットフォームサポートが利用でき、拡張されたエンタープライズインフラストラクチャにおいて優れた柔軟性を提供します。また、FortiGate ファミリーのソリューション全体で利用される単一のネットワークセキュリティオペレーティングシステムは、攻撃者に対抗するために必要な可視性と制御をもたらします。

さらに、FortiGate アプライアンスはフォーティネット セキュリティ ファブリックを介してすべて相互接続され、コンテキストセキュリティポリシーと脅威インテリジェンスが組織全体に自動配布されます。

単一のダッシュボードにより、管理ビューが統合され、可視性が向上し、セキュリティポリシーの実装が簡素化されています。

フォーティネットは実際のセキュリティ効果において高評価を獲得

NSS LABS RECOMMENDED

AV comparatives

vb 100 VIRUS virusbtn.com

ICSA labs CERTIFIED FIREWALL - SMB

COMMON CRITERIA

[1]「The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study」、Kelly Bissell 他共著、Accenture and Ponemon、2019 年 3 月 6 日（英語）：https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[2]「Defense in depth: stop spending, start consolidatin」、Kacy Zurkus 著、CSO Online、2016 年 3 月 14 日（英語）：https://www.csoonline.com/article/3042601/security/defense-in-depth-stop-spending-start-consolidating.html

[3]「Zero-Day Research | Fixes Available」、FortiGuard Labs、2019 年 5 月 16 日（英語）：https://fortiguard.com/zeroday

[4]「Certifications」、フォーティネット、2019 年 5 月 16 日（英語）：https://www.fortinet.com/corporate/about-us/product-certifications.html

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

SB-NGFW-Network-Leader-Solution-Selection-202204-R1