SOLUTION BRIEF

FortiOS：フォーティネット セキュリティ ファブリック

はじめに

世界中の企業組織が、新しいテクノロジーを次々と採用して急速に拡大するデジタルトランスフォーメーション（DX）に追いつこうと格闘しています。DX によって新たな可能性が無限に広がりますが、攻撃対象領域も拡大し、結果として単機能のセキュリティソリューションの寄せ集めとなり、相互連携することのない細分化されたネットワークが形成されることになります。

フォーティネットのセキュリティオペレーティングシステムである FortiOS によって、セキュリティ ファブリックがネットワークインフラストラクチャ全体のセキュリティデバイスを相互接続できるようになり、単一の適応型オペレーティングシステムによる効果的な保護が実現します。FortiOS の最新リリースには、攻撃対象領域全体の可視性と制御を強化し、人工知能（AI）を活用したセキュリティ侵害防止機能をネットワーク全体に統合する数百もの新機能が追加されているため、シームレスな保護と脅威の検知が実現し、オペレーション、オーケストレーション、レスポンスの自動化が実現します。

多くの企業が、スキルのある人材の明らかな不足と限られた予算という問題を抱える中で、高度なサイバー脅威は今も増え続けています。複数のセキュリティ製品がネットワークに導入され、法規制やセキュリティ標準のコンプライアンスに伴う新たな要件への対応が求められるようになっていることで、エンタープライズセキュリティのリーダーを取り巻く環境は、ますます複雑化し続けています。ビジネスのあらゆる分野で DX が進むことで、ネットワークにも急速な進化が求められ、アプリケーション、データ、およびサービスの高速化と、多様なユーザー、ドメイン、デバイスへの対応が必要とされるようになりました。さらには、モノのインターネット（IoT）デバイスやクラウドインフラストラクチャの登場によって攻撃対象領域が拡大し、IT 部門が把握していない部分に対する攻撃にも備えなければならなくなりました。

セキュリティ ファブリックのアプローチ

これらの課題の解決方法として、複数の単機能ソリューションやプラットフォームを使用するアプローチがありますが、これとは対照的な、組織内の異なる環境に存在するすべてのデータやセキュリティの要素を縫い目のない 1 枚の生地（ファブリック）のように密接に統合、一体化するアプローチがあったとしたらどうでしょうか。このようなアプローチであれば、ネットワークからクラウドまでのインフラストラクチャ全体のセキュリティの可視化、制御、統合、管理を可能にする、セキュアデジタルビジネスモデルが実現します。これによって、ワークロードやデータの増加に合わせた拡張や変更が可能になると同時に、IoT、スマートデバイス、境界のないネットワーク、そしてクラウド環境を行き来するデータ、ユーザー、アプリケーションを簡単に追跡して保護できるようになります。

フォーティネット セキュリティ ファブリックは、単機能製品やプラットフォームソリューションに代わる、有効な手段を提供します。セキュリティ ファブリック内のすべてのセキュリティコンポーネントがリアルタイムで相互に通信できるようにすることで、高度な脅威に対する広範かつ強力な自動保護が実現します。FortiOS は、フォーティネット セキュリティ ファブリックを構築する上で基盤となるネットワークオペレーティングシステムです。その最新リリースである FortiOS 6.2 には、300 を超える新機能が追加されており、ネットワークパフォーマンスに影響を与えたりセキュリティを低下させたりすることなく、DX を推進することができます。

IoT デバイスを標的とする攻撃がすべての攻撃に占める割合は、2020 年までに 25% になると予測されています。[1]

エンタープライズワークロードの 83% が、2020 年までにクラウドで処理されるようになると考えられています。[2]

FortiOS 6.2 では、セキュアな DX の可能性を無限に広げる 300 以上の新機能が追加されています。

企業の 4 分の 3 以上は、デジタルイノベーションの進化があまりに急速で、サイバー攻撃への自らの対策が追いついていないと認めています。[3]

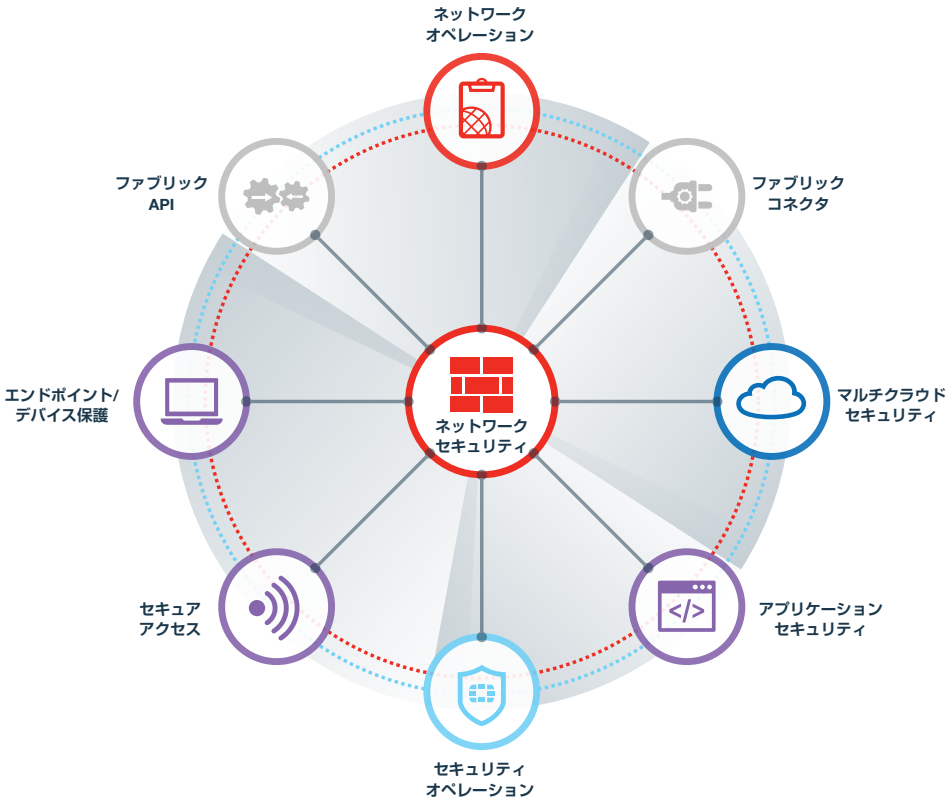

図 1：フォーティネット セキュリティ ファブリック

Broad（幅広い）：デジタル攻撃対象領域の可視化

ネットワークに分散するデバイスを単独の隔離されたものとして処理するセキュリティソリューションでは、今日のビジネスを保護することはできません。フォーティネット セキュリティ ファブリックは、攻撃対象全体を保護することで、複数の場所で脅威の影響を食い止めます。この目標を達成するため、FortiOS 6.2 は、エンドポイント、アクセスポイント、ネットワーク機器、データセンター、クラウド、さらにはアプリケーションやデータそのものを含めた環境全体の可視化と制御を可能にします。セキュリティ ファブリックは、データとリソースを論理的に分離する動的ネットワークセグメンテーションとの組み合わせによって、あらゆる攻撃ベクトルに対応し、ネットワークゾーン間の移動を試みる脅威を検知して、封じ込めます。これにより、ネットワークとデータの保護が可能になります。

セキュリティ ファブリックの拡張ネイティブクラウド / クラウドコネクタにより、プライベート、IaaS（Infrastructure-as-a-Service）、およびネイティブのクラウド制御機能が含まれるマルチクラウド環境全体の完全な可視化が可能になりました。さらに、FortiCASB-SaaS（クラウドアクセスセキュリティブローカー）によって SaaS（Software-as-a-Service）アプリケーションの可視化と高度な脅威保護が実現します。マルチクラウドの可視化により、統合セキュリティ管理コンソールを使用した、オン / オフ両方のネットワークトラフィックの相互の相関付けが可能になります。

FortiOS 6.2 は、セキュリティ ファブリック内部に統合されたフォーティネットのセキュア SD-WAN もサポートしており、SaaS や VoIP（Voice over IP）をはじめとするビジネスクリティカルアプリケーションに優先度を設定し、きめ細かく制御できます。これ以外にも、トラフィックシェーピングによるクリティカルアプリケーションの帯域幅の保証、ゼロタッチ展開によるプラグアンドプレイの SD-WAN ロケーション管理、ワンタッチ VPN による一般的なクラウド VPN アクセスの活用などの新機能が追加されました。また、FortiOS 6.2 に追加された、ユーザーの QoE（Quality of Experience）を保証するよう設計された機能によって、さまざまなメリットが提供されます。環境内で何らかの問題が発生した場合でも、QoE によってサービスの品質低下を回避できます。

Integrated（統合化）：AI ドリブンの侵害保護

多くの組織にとって、セキュリティ対策は極めて複雑になっています。新たなセキュリティギャップを解消し、攻撃対象を保護する目的で、多くの単機能製品が次々と追加導入されています。多数の製品を導入、管理、監視するプロセスは人手に頼ることも多く、結果として定常的なリソース不足に悩まされることになります。また、新しい法規制の制定によってコンプライアンスやレポート作成の要件が厳しくなる一方で、こうした複雑な状況をさらに悪化させる要因となっているのが、スキルのあるセキュリティプロフェッショナルの世界的な不足であり、特にクラウドセキュリティ、DevSecOps、インシデント対応などの分野においては深刻な問題となっています。[4,5]

複雑化し続ける環境を包括的に保護するには、企業のセキュリティインフラストラクチャの異なる部分を、一つの統合システムとして連携させることが不可欠です。セキュリティ ファブリックは、すべてのデバイス、そして分散ネットワークを保護するシステムの統合セキュリティとしてだけでなく、高度な最新の脅威を迅速に検知するように設計されています。FortiOS 6.2 には、インフラストラクチャ全体での正確な脅威検知を可能にする、高度な新機能が数多く統合されています。AI を活用したインテリジェンスは、セキュリティ ファブリック全体から収集され、FortiGuard Labs から提供されます。そして、このインテリジェンスを一体型でエンドツーエンドのセキュリティアーキテクチャによって共有することで、自動化の可能性が最大限に広がり、人材不足の影響が軽減されます。具体的には、セキュリティ ファブリックでは人手による監視や介入の制約なく、信頼性の高い分析結果に基づいて自動アクションを実行するとともに、脅威情報の効率的なコミュニケーションや迅速なパッチ適用が実現します。

フォーティネットでは、継続的に最先端の新しいテクノロジーや機能をセキュリティ ファブリックに追加しているため、お客様のニーズに合わせて強化や拡張が可能です。FortiOS 6.2 は、TLS（トランスポートレイヤセキュリティ）1.3 をネイティブでサポートしているため、シームレスで安全なインターネットトラフィックエクスペリエンスと FortiDeceptor によるディセプションベースのセキュリティを提供し、不正侵入や犯罪者の活動の検知が可能になります。

Automated（自動化）：オペレーション、オーケストレーション、レスポンス

統合化と自動化の連携は極めて重要です。脅威が検知されてから、セキュリティイベントへのレスポンスまでの時間を可能な限り短縮し、侵害のリスクを最小限に抑制しなければなりません。フォーティネット セキュリティ ファブリックは、侵入から検知までの時間はもちろん、検知からレスポンスまでの時間も短縮するよう設計されています。フォーティネット セキュリティ ファブリックは、脅威インテリジェンスの相関付けによってリスクレベルを判断し、協調的レスポンスを自動的に同期します。さらに、新たに発見された脅威に関するインテリジェンスの共有、脅威の影響を受けたデバイスの動的な隔離、ネットワークセグメントの分割、ルールの更新、新しいポリシーの展開、およびマルウェアの削除も可能です。また、侵害リスクの軽減だけでなく、人手によるセキュリティプロセスを自動化することで、予算の削減や人材不足の問題を解決できます。

セキュリティ ファブリックの新機能

フォーティネット セキュリティ ファブリックは、複雑さのホリスティックな軽減に役立つよう設計された、さまざまな機能も提供しています。具体的には、デバイス別のアプリケーションインベントリ作成、およびフォーティネットのスイッチや無線アクセスポイントで発生したイベントへのセキュリティレスポンスを自動化できます。自動化されたワークフローではリスクが継続的に診断されるため、システムイベント、脅威アラート、ユーザーやデバイスのステータスなどの事前定義されたトリガーに基づき、ユーザーが容易にレスポンスを設定することができます。さらに、隔離、通知、構成の調整、カスタムレポートなどのさまざまなレスポンスを利用して、ワークフロー環境をリアルタイムで制御できます。自動監査では、セキュリティのコンプライアンス状態に関するトレンドデータを提供し、規模や業種が類似する企業とのベンチマーク比較によるランク付けを提示します。

フォーティネットは、フォーティネット独自のソリューション、パートナーの広範なエコシステム、さらにはサードパーティのソリューションまでのすべての要素をセキュリティ ファブリックに統合し、インフラストラクチャで利用されているすべてのソリューションの一元管理を可能にする唯一のベンダーであり、このような一元管理機能によって、ポリシーやルールの自動化にとどまらない、オペレーションとレスポンスのさらなる簡素化を実現しています。

FortiOS 6.2 には、これ以外にも数多くの新機能が追加されており、監査およびコンプライアンスのベストプラクティスをサポートすることで、PCI DSS（Payment Card Industry Data Security Standard）などの最新の標準や法規制へのコンプライアンスを容易にしています。さらに、事前設定されたルールが用意されているため、複雑なルールの作成、適用、追跡に要する時間を削減できます。

FortiOS 6.2 の新機能：

- インテント ベースト セグメンテーション
- セキュア SD-WAN
- エンドユーザー QoE
- AI を活用した脅威インテリジェンス
- ディセプションベースのセキュリティ
- インシデント対応の自動化
- 監査とコンプライアンスのベストプラクティス
- セキュリティの一元管理

1 日に検知される新しいマルウェアに占めるゼロデイまたは未知のマルウェアの割合が 40%を超えるようになったことから、高度な脅威とブリーチの検知が不可欠となりました。[6]

自動化、人工知能、機械学習を採用している組織の割合は 38%に過ぎません。[7]

終わりに

DX が進むに伴って、企業は多くのセキュリティの課題に直面しています。コンピューティングとネットワーキングのトレンドが、ビジネスインフラストラクチャ、アーキテクチャ、そしてビジネスの現場に変化をもたらす一方で、サイバー犯罪においても発見された脆弱性を悪用するために新たな攻撃手法の採用や改良が続いています。このような変化に対応するためには、ビジネスリーダーが分散インフラストラクチャ全体の確実な保護を可能にする、新たなアプローチを採用することが不可欠です。フォーティネット セキュリティ ファブリックは、スケーラブルで相互接続されたセキュリティと高度な検知能力、実用的な脅威インテリジェンス、およびオープン API 標準規格によって、最も要件の厳しいエンタープライズ環境の保護にも対応するよう設計された、インテリジェントなアーキテクチャを提供します。

FortiOS 6.2 は、フォーティネットが提供する最新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です。この最新バージョンで採用された数百もの機能強化と機能の追加によって、セキュリティ ファブリックが拡張され、企業全体の攻撃対象の可視性と制御のさらなる強化が実現します。また、AI を活用したセキュリティ侵害防止機能をネットワーク全体に統合することで、シームレスな保護と脅威の検知を実現するとともに、オペレーション、オーケストレーション、レスポンスの自動化によってセキュリティの問題の迅速な特定と解決を可能にすると同時に、複雑さを軽減して DX の促進を支援します。

[1]「25% Of Cyberattacks Will Target IoT In 2020（2020 年にはサイバー攻撃の 25% が IoT を標的にするようになる）」、Retail TouchPoints、2019 年 3 月 21 日時点の情報（英文）：https://www.retailtouchpoints.com/resources/type/infographics/25-of-cyberattacks-will-target-iot-in-2020

[2] Louis Columbus 著、「83% Of Enterprise Workloads Will Be In The Cloud by 2020（2020 年にはエンタープライズワークロードの 83% がクラウドで処理されるようになる）」、Forbes、2018 年 1 月 7 日（英文）：https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#53fe895c6261

[3] Kelly Bissell 他著、「The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study（サイバー犯罪の被害額：第 9 回 サイバー犯罪の年間被害額調査）」、Accenture と Ponemon の共同調査、2019 年 3 月 6 日（英文）：https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

[4]「Cybersecurity Skills Shortage Soars, Nearing 3 Million（サイバーセキュリティのスキル不足が深刻化し、その数は 300 万人に）」（ISC）[2]、2018 年 10 月 18 日（英文）：https://blog.isc2.org/isc2_blog/2018/10/cybersecurity-skills-shortage-soars-nearing-3-million.html

[5] Dawn Kawamoto 著、「Top 8 Cybersecurity Skills IT Pros Need in 2018(2018 年に IT プロに必要とされるサイバーセキュリティのスキル TOP 8)」、Dark Reading、2017 年 12 月 18 日（英文）：https://www.darkreading.com/careers-and-people/top-8-cybersecurity-skills-it-pros-need-in-2018/d/d-id/1330657

[6] FortiGuard Labs の内部データによる

[7] Kelly Bissell 他著、「The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study（サイバー犯罪の被害額：第 9 回 サイバー犯罪の年間被害額調査）」、Accenture と Ponemon の共同調査、2019 年 3 月 6 日（英文）：https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

フォーティネットジャパン株式会社

〒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

Copyright© 2019 Fortinet, Inc. All rights reserved. この文書のいかなる部分も、いかなる方法によっても複製、または電子媒体に複写することを禁じます。この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。Fortinet®、FortiGate®、FortiCare®、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。その他の製品または社名は各社の商標です。

SB-FortiOS6.2-201906-R1