SOLUTION BRIEF

FortiSASE：包括的な SASE ソリューションでリモートユーザーにセキュリティとネットワーキングをクラウドから提供

概要

ほとんどの企業がハイブリッドワークを導入し、少なくとも週の何日かをオフィス以外で働くことを従業員に認めるようになりました。結果として、ホームオフィスやモバイルワーカーにまで攻撃対象領域が拡大し、ネットワーク、アプリケーション、デジタルリソースの保護がこれまで以上に困難になりました。リモートオフィスやハイブリッドワーカーが多い組織では、オン / オフ両方のネットワークに一貫性ある方法でセキュリティポリシーを適用し、最適なユーザーエクスペリエンスを従業員に提供するのは、容易なことではありません。

理由の 1 つとして、このような変化が綿密に計画された戦略の一部としてではなく、組織的に発生したものであることが挙げられます。新しいネットワークエッジとリモートユーザーが急増し、それらは往々にして個別のプロジェクトとして実装されていることから、サイバー犯罪者にとっては非常に魅力的なセキュリティのギャップが生まれています。

SASE（セキュアアクセスサービスエッジ）アーキテクチャは、あらゆる場所のユーザーに安全なアクセスと高パフォーマンスの接続を提供することで、これらの問題の解決に役立ちますが、多くの SASE ソリューションで解決されるのは一部の問題だけであり、リモートユーザーにエンタープライズクラスのセキュリティを提供できなかったり、ネットワークエッジに展開された多様な物理 / 仮想のネットワークやセキュリティのツールとシームレスに統合できなかったり、あるいはそのどちらもできなかったりします。結果として、あらゆる場所に一貫性あるセキュリティ態勢や最適なユーザーエクスペリエンスを提供することができません。

FortiSASE は、フォーティネットの単一ベンダーによる SASE アプローチを採用して、クラウドから提供する SD-WAN（ソフトウェア制御による WAN）接続とクラウドから提供する SSE（セキュリティサービスエッジ）を統合することで、ネットワーキングとセキュリティのコンバージェンスをネットワークエッジからリモートユーザーにまで拡大する、包括的な SASE ソリューションを提供します。

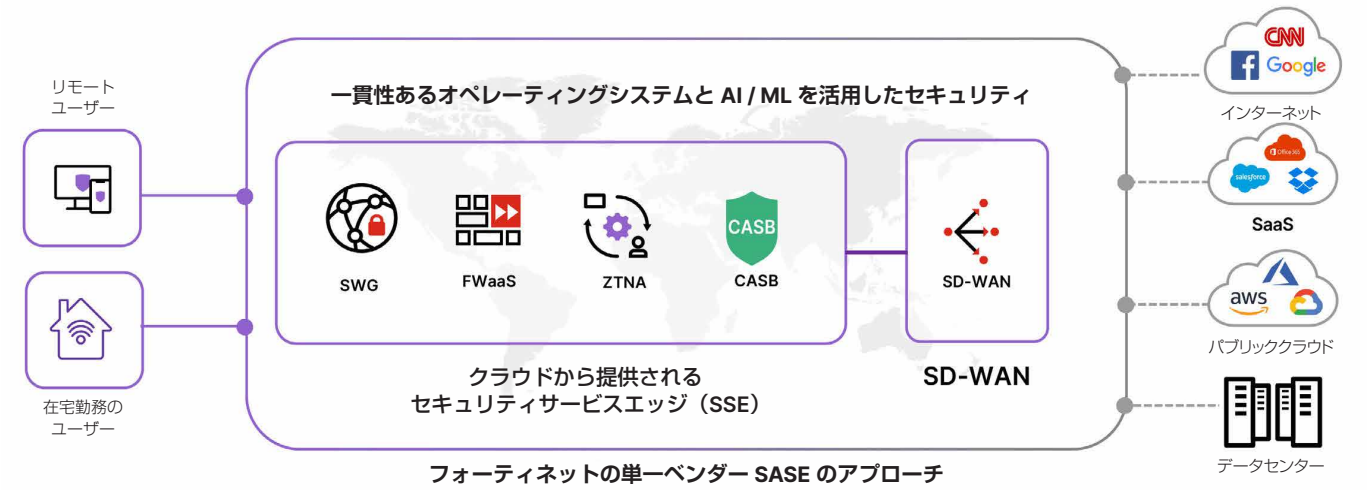
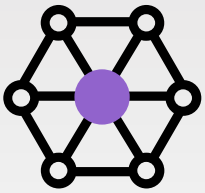


図 1：FortiOS を活用した一貫性あるセキュリティ態勢と優れたユーザーエクスペリエンスをあらゆる場所のユーザーに提供

FortiSASE は、ネットワーキングとセキュリティを 1 つに統合し、ネットワークエッジからリモートユーザーまでのすべてに最適かつ安全な接続を保証することを前提に設計されたソリューションです。フォーティネットの 20 年以上にわたる有機的なイノベーションから生まれた FortiSASE が提供する、SWG（セキュア Web ゲートウェイ）、ZTNA（ゼロトラストネットワークアクセス）、次世代 CASB（クラウドアクセスセキュリティブローカー）、クラウドベースの FWaaS（Firewall-as-a-Service）、セキュア SD-WAN が、CAPEX から OPEX のビジネスモデルへの移行を可能にします。

フォーティネット独自のセキュリティ ドリブン ネットワーキング戦略と単一のオペレーティングシステムである FortiOS の組み合わせにより、セキュリティとネットワーキングの機能を単一の統合システムに融合させ、あらゆる場所のあらゆるユーザーへの一貫したセキュリティとユーザーエクスペリエンスの提供を可能にしています。FortiSASE は、エンタープライズクラスのセキュリティと優れたユーザーエクスペリエンスを独自の方法で両立させることで、あらゆる場所の Web、クラウド、アプリケーションへのセキュアアクセスを可能にします。



FortiOS と FortiGuard の AI を活用するセキュリティサービスを FortiSASE に組み込むことで、シンプルかつスケーラブルなセキュリティをクラウドから提供し、一貫性あるセキュリティと優れたユーザーエクスペリエンスをあらゆる場所のユーザーに対して実現しています。

FortiSASE：シンプルかつシームレスで スケーラブルなセキュリティをクラウドから提供

FortiSASE は、セルフサービス設計のシンプルなクラウドベースの管理、ユーザーの容易なオンボーディング、業界で最も柔軟な階層型でユーザー単位のライセンスモデルを提供します。これにより、CAPEX から OPEX のビジネスモデルへの移行と、今日の非常に動的なネットワークとインフラストラクチャのコストの予測が可能になります。

FortiSASE は、ソリューションのセキュリティ制御が米国公認会計士協会（AICPA）の TSP（Trust Services Principle and Criteria）に準拠していることを検証する SOC 2（Service Organization Control Type 2）認定を取得しています。この SOC 2 標準の認定は、お客様の多様なコンプライアンス要件に確実に対応するというフォーティネットのコミットメントを実証するものです。さらには、SWG、ユニバーサル ZTNA、次世代デュアルモード CASB、FWaaS、高度脅威防御などのエンタープライズクラスのセキュリティ機能がすでに完全統合された包括的なソリューションを提供することで、以下の 3 つの重要なユースケースに対応します。

- **セキュアインターネットアクセス：**

  企業の境界の外で働くリモートユーザーがインターネットに直接アクセスすると、攻撃対象領域やリスクが拡大します。FortiSASE は、SWG と FWaaS の包括的な機能を提供し、エージェントまたはエージェントレスの両方のアプローチをサポートすることで、管理対象と管理対象外の両方のデバイスを保護します。

- **セキュアプライベートアクセス：**

  ハイブリッドワークが新たな標準となりつつある現状で、従来の VPN のスケーラビリティで十分とは言えません。VPN トンネルにはインスペクションや高度な保護機能がないため、VPN トンネルの侵害によって、あらゆるアプリケーションへのアクセスが可能になり、攻撃対象領域が拡大し、脅威のラテラルムーブメント（水平移動）のリスクが増大する可能性があります。FortiSASE セキュアプライベートアクセスは、企業のアプリケーションへの業界で最も柔軟なセキュア接続を提供します。ユニバーサル ZTNA アプローチを使用することで、きめ細かいアプリケーションアクセスが実装され、アプリケーション単位の明示アクセスを可能にすることで、暗黙のトラストモデルから安全性の高い明示的なトラスト戦略へとセキュリティ戦略の移行が容易になります。FortiSASE セキュアプライベートアクセスと SD-WAN ネットワークのシームレスな統合により、FortiSASE のインテリジェントステアリングと動的ルーティング機能を利用して企業アプリケーションへの最短パスの自動検索も可能になりました。

- **セキュア SaaS アクセス：**

  SaaS の採用の急速な拡大に伴い、多くの企業がシャドー IT の課題やデータ流出の防止といった難題に直面しています。FortiSASE セキュア SaaS アクセスとインラインと API ベースの両方をサポートする次世代デュアルモード CASB により、重要な SaaS アプリケーションを特定してリスクのあるアプリケーションをレポートすることで包括的に可視化し、シャドー IT の課題を解決できます。次世代 CASB は、アプリケーションのきめ細かい制御を可能にすることで、機密データを保護し、管理対象と管理対象外の両方のデバイスでのアプリケーションに潜むマルウェアの検知と修復を可能にします。

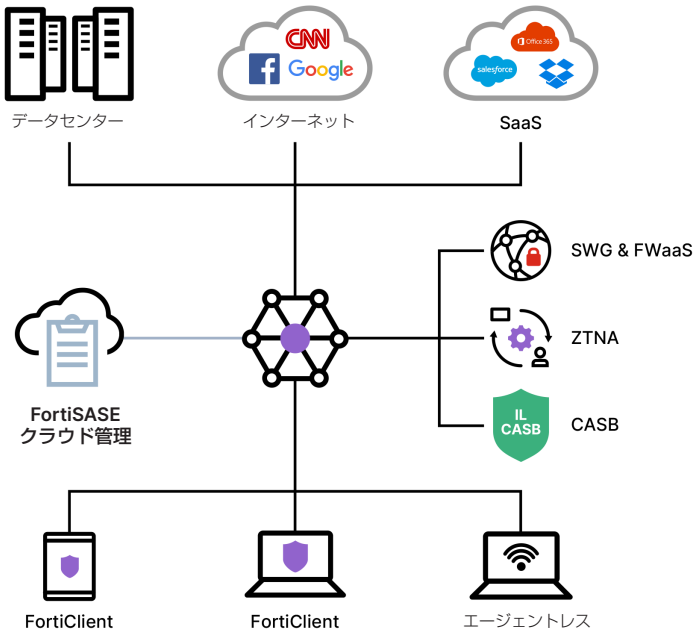


図 2：FortiSASE があらゆるアプリケーションに対する安全で信頼できるクラウドベースの接続を提供

包括的でスケーラブルなセキュリティ機能の提供

FortiSASE は、インターネット、プライベートデータセンター、SaaS アプリケーションのトラフィックを保護する包括的なセキュリティ機能を提供します。

セキュア Web ゲートウェイ：暗号化されたトラフィックを含む Web トラフィックを保護する幅広い機能により、最も高度な Web の脅威からの保護を可能にします。Web フィルタリング、アンチウイルス、ファイルフィルタリング、データ漏洩防止などの連携により、管理対象と管理対象外の両方のデバイスの縦深防御を実現します。

FaaS（Firewall-as-a-Service）：業界をリードするフォーティネット セキュリティ ファブリック戦略の中核である FortiOS の実績ある独自の機能を活用することで、クラウドのトラフィック、アプリケーション、サービスの高パフォーマンス SSL インスペクションと高度な脅威検知手法が可能になります。フォーティネットの FWaaS は、安全かつ安定した接続を確立してリモートユーザーに提供しつつ、インバウンドとアウトバウンドのトラフィックをユーザーエクスペリエンスに影響することなく分析します。

ユニバーサル ZTNA：ZTNA は、IT のチームによるビジネスクリティカルなアプリケーションへのユーザー単位、セッション単位のアクセスの認証、保護、監視を可能にします。ユニバーサル ZTNA によって、この機能があらゆる場所のあらゆるユーザーとデバイスにまで拡大されるため、暗黙のアクセスアプローチから、継続的なアイデンティティとコンテキストの検証に基づく安全性の高い明示的なアクセス戦略への移行が実現します。

次世代デュアルモード CASB:インラインと API ベースの両方をサポートする CASB により、FortiSASE は、重要な SaaS アプリケーションやシャドー IT アプリケーションを特定し、認可された SaaS アプリケーションへのアクセスを保護し、SaaS アプリケーションへのアクセスを信頼できるエンドポイントだけに制限し、同時にアプリケーションアクセスの ZTNA ポスチャーチェックも可能にします。

DNS（Domain Name System）：DNS トンネリング、DNS プロトコルの悪用、DNS 侵入、C2 サーバーの識別、ドメイン生成アルゴリズム（DGA）などの DNS ベースの高度な脅威からの保護を可能にします。DNS トラフィックを完全に可視化し、悪意のある新規登録ドメイン（NRD）やパークドメインなどの高リスクのドメインをブロックします。

IPS（侵入防止システム）：リアルタイムの脅威インテリジェンスを活用し、パフォーマンスへの影響を最小限にしつつ、新規と既存の両方の脆弱性からの保護を可能にします。

サンドボックス:脅威を安全な環境で特定、活性化、分析して、リアルタイムの防止と検知を可能にすることで、未知の高度な脅威からファイルを保護します。

フォーティネットの優位性

FortiSASE は、隔離されたクラウドのみのアプローチから脱却し、フォーティネット セキュリティ ファブリックに組み込まれたサービスを提供します。FortiOS の機能の拡張と活用により、フォーティネット セキュリティファブリックは、幅広い可視性、きめ細かい制御、一貫性あるプロアクティブな保護をあらゆる場所に提供します。

一貫性あるセキュリティによるオン / オフネットワークのユーザーの保護：FortiSASE は、包括的なセキュリティをクラウドから提供し、ZTNA をネイティブに統合することで、一貫性ある保護をローカルとリモートの両方のユーザーに提供します。

統合されたエージェント：フォーティネットの統合されたエージェントである FortiClient は、ZTNA、トラフィックの SASE へのリダイレクト、デュアルモードの次世代 CASB、堅牢なエンドポイント保護などの複数のユースケースをサポートしているため、ユースケースごとに個別のエージェントは必要ありません。

シンプルな管理と利用：容易な導入、オンボーディング、管理をセルフサービス設計と業界で最も柔軟なユーザーベースのライセンスモデルで利用できるため、IT チームは、包括的で一貫性あるセキュリティをハイブリッドワーカーに実装することができます。さらには、すでに IT のチームの大きな負担となっている可能性のある、異なるネットワークエコシステムに展開されたシステムの管理、監視、調整、最適化といった負担を増やすことなく、これが実現します。

これらのテクノロジーと単一の FortiOS オペレーティングシステムの組み合わせにより、ユーザー、アプリケーション、エンドポイントデバイスを保護しつつ、分散ネットワークの他の要素とのシームレスな相互運用を可能にする、クラウドベースの統合 SASE ソリューションを提供します。ネットワーキングとセキュリティの統合を可能にするシームレスなエンドツーエンドのこのアプローチにより、今日の急速に進化するデジタル市場での高い競争力の獲得に必要とされる適応型の戦略が確立されます。

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

Copyright© 2022 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-FortiSASE-Cloud-Delivered-Security-202211-R1