

SOLUTION BRIEF

# FortiSASE — あらゆる場所のすべてのユーザーに、クラウドからセキュリティを提供

## 概要

複数のリモートオフィスを持ち、ハイブリッドに働く従業員を多く抱える企業では、分散したネットワーク全体で一貫したセキュリティポリシーを適用し、実施することが困難です。新しいネットワークエッジが増加し、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）ソリューションは、あらゆる場所のユーザーに安全なアクセスと高性能の接続性を提供します。しかし、SASE ソリューションの中には、リモートのユーザーや拠点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いものや、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ツールやセキュリティツールとシームレスに統合できないものが多くあります。

そのような状況で、FortiSASE は独自のアプローチをとっています。

FortiOS に支えられたフォーティネットならではのセキュリティ ドリブン ネットワーキング戦略によって、セキュリティとネットワーク機能を単一の統合システムに融合させ、エッジ全体で一貫したセキュリティとユーザーエクスペリエンスを提供することが可能になっています。そして今、クラウドに拡張された FortiOS によって、組織の中核で展開されているのと同じエンタープライズクラスのセキュリティを、ハイブリッドに働く従業員にも提供できるようになりました。クラウド向けの FortiSASE は、セキュリティ、ネットワーク、接続機能をシームレスに統合し、同じレベルの保護、可視性、制御を、場所を問わず、すべてのデバイス、すべてのユーザーに提供します。

## FortiSASE

クラウド向けの FortiSASE ソリューションは、市場で最も広範な物理 / クラウドの統合セキュリティソリューションを提供し、実現します。その起点となるのは、FortiGuard Labs の脅威インテリジェンスサービスによりサポートおよび強化された、業界をリードする NGFW（次世代ファイアウォール）と FWaaS（Firewall-as-a-Service）のソリューションです。これらは、FortiOS が提供するセキュリティ ドリブン ネットワーキング機能の基本的要素であり、FortiSASE ソリューションの中核を成します。これによって、クラウドネイティブの FortiSASE アーキテクチャが高性能なセキュリティと接続性を大規模に実現できるため、マルチクラウドの環境を含むあらゆる構成と環境で最大限の柔軟性とセキュリティが可能になります。

FortiSASE は、全世界で最も広範に導入されているセキュリティ OS である FortiOS に組み込まれているため、迅速かつ容易に展開できます。また、すべての要素がシームレスに動作するように設計されているため、直感的に操作できます。さらに、フォーティネットセキュリティ ファブリックの一部として、どのような環境も一元的に管理でき、完全なオーケストレーションが可能です。

FortiSASE は、フォーティネットの先進的なエンタープライズクラスのセキュリティと強力な FortiOS をサービスとしてクラウドで提供し、すべてのエッジにわたって一貫したセキュリティとユーザーエクスペリエンスを実現します。

FortiSASEに加えて、FortiOS は以下のサービスを提供します。これらはすべて、SASE ソリューションの一環として機能します。

- **次世代ファイアウォール (NGFW)** : NGFW は、ディープインスペクションと高度な手法を組み合わせる安全な接続を確立 / 維持し、インバウンドとアウトバウンドのトラフィックを分析します。
- **侵入防止システム (IPS)** : IPS は、既知の脆弱性を利用しようとする悪意のある活動を検出するため、ネットワークを監視します。
- **データ漏えい対策 (DLP)** : DLP 機能は、エンドユーザーが重要情報をネットワーク外に持ち出すことを防止します。
- **DNS (Domain Name System)** : DNS は、悪意のあるドメインを識別して隔離し、悪意のある脅威がネットワークに侵入することを防止します。
- **セキュア Web ゲートウェイ (SWG)** : SWG は、Web トラフィックからマルウェアをフィルタリングし、企業や規制当局のポリシーに対するコンプライアンスを確保します。
- **ゼロトラストネットワークアクセス (ZTNA)** : ZTNA は、ユーザーとデバイスを認証し、コンテキストとポリシーに基づいて特定のネットワークリソースに限定したアクセスを提供します。

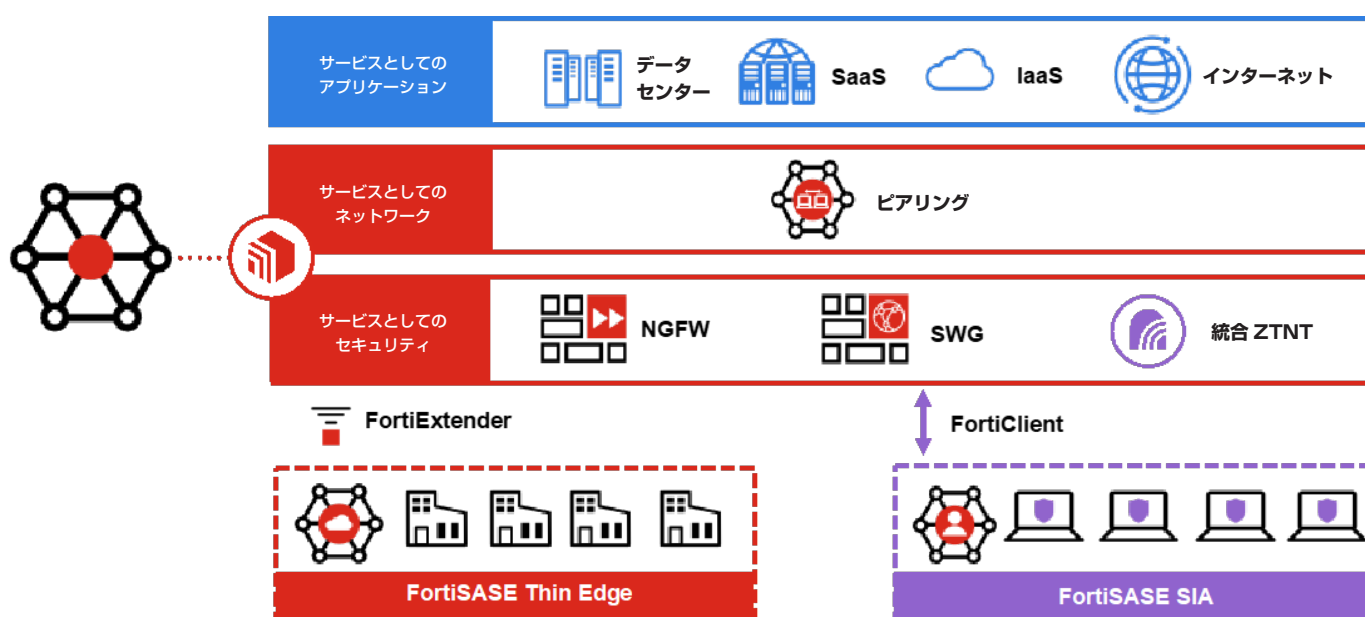


図 1: FortiSASE の概要

フォーティネットの SASE ソリューションには、以下の 2 つのタイプの主要フォームファクターがあります。

- **FortiSASE Secure Internet Access (SIA)** は、高性能な常時接続の脅威対策をクラウドからリモートユーザーに提供します。FWaaS、IPS、DLP、DNS、SWG、ZTNA、サンドボックスなど、仮想プライベートネットワーク (VPN) を超えた統合的なネットワークキングとセキュリティの機能を、遅延やユーザーエクスペリエンスの阻害を引き起こすことなく実現します。

このアプローチにより、エンドユーザーは場所を問わず、常に一貫したファイアウォールとセキュリティポリシーによる保護を受けることができます。この常時接続の戦略は、オフネットワークのユーザーを含む包括的なセキュリティを適用します。これによって、企業ネットワークとオンプレミスの資産に対するサイバー攻撃の防止が支援されます。

- **FortiSASE Thin Edge** は、FortiSASE SIA と同様の、クラウドで提供される高性能な常時接続の脅威対策を、シンエッジのユーザーに提供します。この製品は、セキュリティサービスを CapEx(設備投資)から OpEx(運用コスト)へと移すことを計画している場合を含め、必要なアプライアンスを削減できる簡素なエッジソリューションを求める組織向けに設計されたものです。FortiExtender により 5G / LTE 上で容易に展開可能な FortiSASE Thin Edge を使用することで、インフラストラクチャのリーダーは SECaaS (Security-as-a-Service) を迅速に拡張できます。

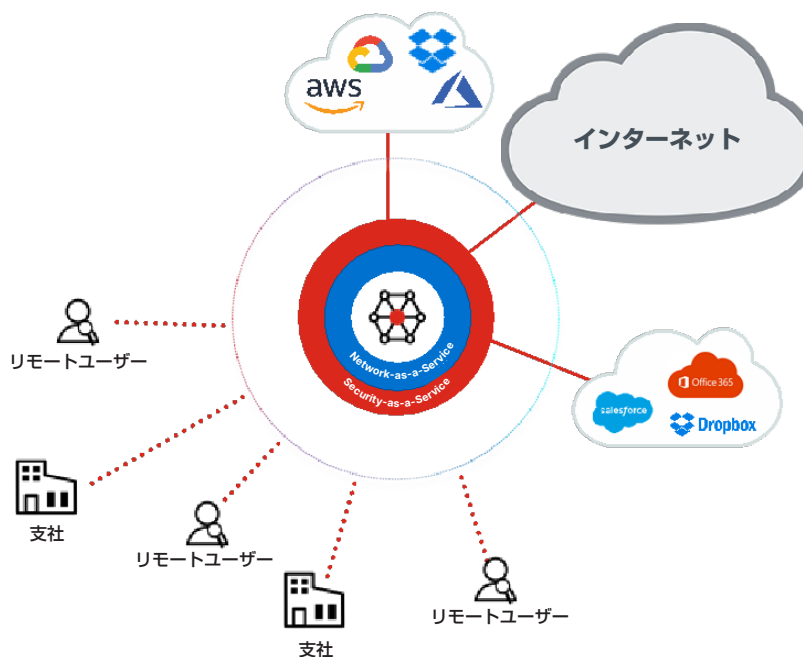


図 2 : SIA とシンクライアントのユースケース

## フォーティネット セキュリティ ファブリックを介して SASE を拡張

フォーティネット セキュリティ ファブリックにより、FortiSASE をはじめとするセキュリティソリューションを、すべてのネットワーク、エンドポイント、クラウドにわたって一貫した形で提供 / オーケストレーションできます。フォーティネット セキュリティ ファブリックのすべての要素は、共通のオペレーティングシステムである FortiOS 上で動作するか、または FortiOS に接続するため、管理者の可視性と制御性が向上します。これにより、セキュリティポリシーの一貫した展開と実施、および分散したネットワーク全体での一元管理を確実に実現できます。

FortiSASE は、フォーティネット セキュリティ ファブリックの一部であることから、エッジに展開されたセキュリティやネットワークのソリューションともシームレスに統合でき、セキュリティとアクセス管理のための単一でシームレスなソリューションを実現します。組織のニーズはそれぞれ異なりますが、SASE ソリューションを中核の機能のみに限定すると、ネットワークが無用なリスクを負い複雑化します。より包括的なネットワークとセキュリティのアプローチでは、分散したネットワーク全体を単一エコシステムの一部として理解します。そこでは、すべてのエッジの全要素が連携して、より豊かなビジネス成果をもたらされます。

このアプローチによって一貫性のある動的なセキュリティ態勢が実現され、あらゆる場所に展開されたアプリケーション、リソース、データ、サービスに対して、ユーザーやデバイスが世界中のどこからでも迅速にアクセスできます。そのために、脅威を自動的に評価し、リスクに合わせてシステムを自動調整するセキュリティが使用されます。

## フォーティネットの優位性

フォーティネットは、セキュリティドリブン ネットワーキング戦略に基づいて、ネットワークエッジ全体で一貫したエンタープライズクラスの保護を提供している唯一の SASE ベンダーです。FortiSASE は、クラウドベースで利用できる高度なセキュリティを提供し、ワークフローの運用に影響を与えずに一般的なセキュリティギャップを解消します。また、各要素が同じ FortiOS 環境の一部であるため、すべての機能を備えた FortiSASE ソリューションも迅速に展開して直感的に管理できます。

FortiSASE は、フォーティネット セキュリティ ファブリックのメリットを実現するため、リスクプロファイルを低減してハイブリッドな企業ネットワークを最適化し、場所を問わずユーザーを支援および保護します。これにより、あらゆるネットワークエッジで一貫した保護が提供されます。しかも、企業ネットワークとサービスプロバイダーネットワークの両方の要求に対応しているため、インフラの管理者はクラウドを介して同一のセキュリティを提供することにより、既存セキュリティインフラに対する投資を拡張できます。

## フォーティネットのイノベーション

フォーティネットは、20年以上にわたるセキュリティイノベーションを通じて、以下のメリットを実現しています。

- フォーティネットは、セキュリティを SD-WAN に完全統合した最初のセキュリティベンダーです。これは、フォーティネットが長年にわたるセキュリティとネットワークングの経験を単一の統合ソリューションへと集約することによって実現したものです。この戦略は「セキュリティ ドリブン ネットワーキング」と呼ばれます。このアプローチを基盤として、クラウド向け FortiSASE ソリューションが実現しました。
- FortiGuard Labs チームは、業界有数の洗練された人工知能 (AI) システムを活用して、世界中のインテリジェンスを相関させ、新たな脅威を特定、調査、分類しています。FortiSASE をはじめとするフォーティネットのソリューションは、このインテリジェンスを直接活用することで、コンポーネントを更新し、分散したネットワーク全体で一貫して脅威に対する防御を強化しています。
- フォーティネットは、2020 年のガートナー社 WAN エッジインフラストラクチャ マジック・クアドラント<sup>1</sup> およびネットワークファイアウォール マジック・クアドラント<sup>2</sup> の両部門で、リーダー・クアドラントの 1 社に位置づけられました。このように、単一ベンダーとして両レポートで評価されたのは、フォーティネットのアプライアンスだけです。
- また、フォーティネットのセキュリティソリューションは、業界で最も多くのテストや検証を実施されています。NSS Labs の NGFW テストで「Recommended (推奨)」の評価を 6 回連続で受けているほか、ICSA Labs、Virus Bulletin など、多数の機関のテストで最高評価を受けています。

## フォーティネットの優位性

フォーティネットは、ネットワークングとセキュリティに対する長年のアプローチの一環として、テスト / 検証されたネットワークングとセキュリティのテクノロジーを統合ソリューションに組み合わせることにより、今日の企業が必要とする包括的 SASE ソリューションを提供しています。また、業界で最も広範な先進の接続とセキュリティのテクノロジーにより、どのようなソリューションもカスタマイズできる点において、他のベンダーとは一線を画しています。したがって、それぞれ独自の環境に合わせて SASE ソリューションが設計され、要件の変化に応じた適合も容易です。

さらに、FortiSASE ソリューションはフォーティネット セキュリティ ファブリックの一部であるため、オンプレミスかクラウドかを問わず、あらゆるネットワークエッジに展開された他のフォーティネットやフォーティネット ファブリック レディ パートナーのソリューションと簡単に統合 / 接続できます。それだけではありません。これらすべてに一元管理システムで対応できるので、分散したネットワーク全体の広範な可視性ときめ細かな制御が保証されています。

<sup>1</sup> [Gartner Magic Quadrant for WAN Edge Infrastructure], Jonathan Forest / Andrew Lerner / Naresh Singh 共著、2020 年 9 月 23 日 (英語) : <https://www.fortinet.com/jp/solutions/gartner-wan-edge>

<sup>2</sup> [Gartner Magic Quadrant for Network Firewalls], Rajpreet Kaur / Adam Hills / Jeremy D'Hoinne 共著、2020 年 11 月 9 日 (英語) : <https://www.fortinet.com/jp/solutions/gartner-network-firewalls>



### 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](http://www.fortinet.com/jp/contact)

お問い合わせ