FortiSASE

ハイライト

- セキュア SaaS アクセス
- セキュアインターネットアクセス
- セキュアプライベートアクセス
- AI 活用セキュリティ
- クラウドから管理

ハイブリッドワーキングに最適なセキュリティとネットワーキングのスケーラブルな機能をクラウドから提供

ハイブリッドワークがほとんどの企業で新しい現実になったことで、攻撃対象領域が拡大し、リモートユーザーの保護がさらに困難になるという新たな課題に直面しています。新しいネットワークエッジとリモートユーザーが増加し、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。同時に、多数のリモートオフィスやハイブリッドワーカーを抱える企業の多くが、オン / オフネットワークのユーザーに一貫性ある方法でセキュリティポリシーを適用しつつ、優れたユーザーエクスペリエンスをすべてのユーザーに提供するという難題を抱えています。

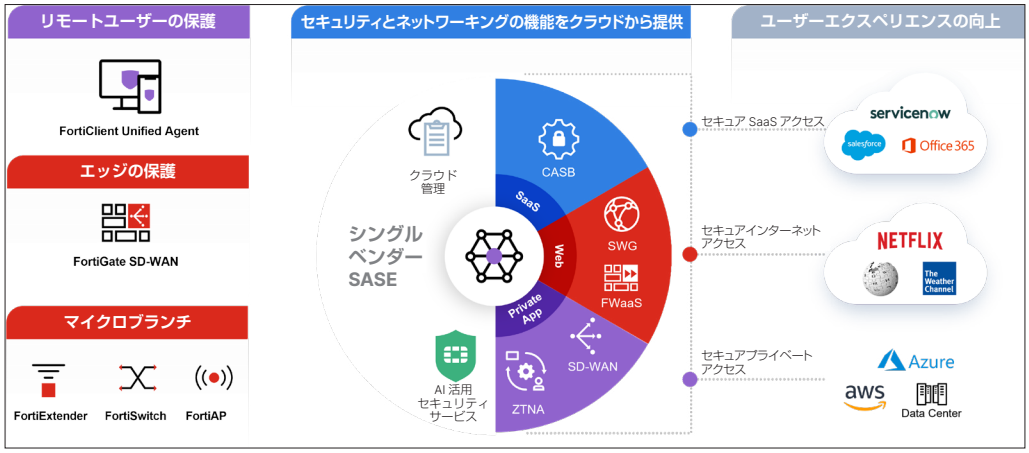
提供形態

クラウド

はじめに

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、ネットワーキングとセキュリティの多くの問題を解決しますが、クラウドから提供される多くのセキュリティソリューションは、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ワークのユーザーに提供できていません。また、ネットワークエッジに置かれた物理 / 仮想ネットワークやセキュリティのさまざまなツールとシームレスに統合して、あらゆる場所に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提供することもできません。

フォーティネットのシングルベンダー SASE アプローチは、統一されたオペレーティングシステムとエージェントでのネットワーキングとセキュリティのコンバージェンスにより、エンタープライズグレードのセキュリティと優れたユーザーエクスペリエンスのあらゆるエッジへの一貫性ある適用を可能にします。FortiSASE は、FortiGuard セキュリティサービスをシンエッジ、セキュアエッジ、リモートユーザーに拡張し、オンネットとオフネットワークの両方のユーザーのセキュアアクセスを可能にします。



20 年以上にわたる有機的なイノベーション、共通の FortiOS オペレーティングシステム、FortiGuard の AI を活用したセキュリティサービスが組み込まれた FortiSASE は、SWG（セキュア Web ゲートウェイ）、ユニバーサル ZTNA（ゼロトラストネットワークアクセス）、次世代デュアルモード CASB（クラウドアクセスセキュリティブローカー）、FWaaS（Firewall-as-a-Service）、クラウドから提供する SD-WAN 接続を可能にすることで、CAPEX から OPEX のビジネスモデルへの移行を支援し、オーバーヘッドの大幅な削減、ユーザーエクスペリエンスと保護の強化を実現します。FortiSASE は、エンタープライズクラスのセキュリティの完全統合により、あらゆる場所に展開される Web、クラウド、アプリケーションへのユーザー単位、セッション単位のセキュアアクセスを可能にします。

セキュリティとネットワーキングのシームレスなコンバージェンスにより、同じレベルの保護、可視性、ユーザーエクスペリエンスをあらゆる場所のあらゆるユーザーに提供します。組織のコンプライアンスを支援するため、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。

ハイライト

FortiOS

FortiOS は、20 年以上にわたって業界をリードしてきたフォーティネットのイノベーションが結集された、統合オペレーティングシステムです。セキュリティ ドリブンの独自のアプローチの採用により、ネットワーキングとセキュリティをシームレスに統合し、クラウドからの提供を実現しています。

FortiGuard AI 活用セキュリティサービス

AI を活用したセキュリティサービスをアプリケーション、コンテンツ、Web トラフィック、デバイス、ユーザーに適用することで、最新の攻撃からの一貫性あるリアルタイムの防御を実現し、迅速かつリアルタイムの検知とレスポンスを保証します。

クラウドベースの管理

クラウドベースのシンプルな管理により、さまざまな場所に分散するユーザーやアプリケーションの一元的な可視化と制御を、業界をリードする SLA で提供します。

主なビジネスの成果

あらゆる場所で一貫したセキュリティ態勢を実現

同じ FortiOS による一貫したセキュリティ態勢が実現することで、セキュリティギャップが解消され、攻撃対象領域が最小化されます。

優れたユーザーエクスペリエンス

インテリジェントなアプリケーションステアリングと動的ルーティングをネイティブに利用できるフォーティネットのセキュア SD-WAN は、優れたユーザーエクスペリエンスをリモートユーザーに提供します。

運用の効率化

シンプルな管理にセキュリティとネットワーキングの強力な分析が加わることで、運用の簡素化を実現します。

OPEX ビジネスモデルへの移行

シンプルな階層型ライセンスモデルで利用できるため、CAPEX から OPEX への移行が可能になります。

主要なユースケース

セキュアインターネットアクセス

企業の境界で保護されないリモートユーザーや支社のユーザーがインターネットに直接アクセスすると、攻撃対象領域も関連するリスクも拡大します。FortiSASE は、エージェントと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、SWG（セキュア Web ゲートウェイ）と FWaaS（Firewall-as-a-Service）の包括的な機能を管理対象と管理対象外の両方のデバイスに提供します。

セキュアプライベートアクセス

今日のハイブリッドワークで直面する課題を従来の VPN で解決することはできません。VPN では接続がインスペクションされないため、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）のリスクが高くなります。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可能にします。企業は、アプリケーションへのきめ細かいアクセスをユニバーサル ZTNA で適用することで、アプリケーション単位の明示的なアクセスを可能にし、暗黙ではなく明示的な信頼への移行を実現することができます。FortiSASE セキュアプライベートアクセスは、SD-WAN ネットワークとのシームレスな統合に加えて、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の機能による最短パスの自動探索を活用した企業アプリケーションへのアクセスのメリットを提供します。

セキュア SaaS アクセス

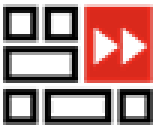
SaaS の採用の急速な拡大に伴い、多くの企業がシャドー IT の課題やデータ流出の防止といった難題に直面しています。FortiSASE セキュア SaaS アクセスとインラインと API ベースの両方をサポートする次世代デュアルモード CASB により、重要な SaaS アプリケーションを特定してリスクのあるアプリケーションをレポートすることで包括的に可視化し、シャドー IT の課題を解決できます。次世代 CASB は、アプリケーションのきめ細かい制御を可能にすることで、機密データを保護し、管理対象と管理対象外の両方のデバイスでアプリケーションに潜むマルウェアの検知と修復を可能にします。

主な機能と特長

SaaS（Security as a Service）

セキュア Web ゲートウェイ（SWG）

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。SWG は、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、DLP（データ漏洩防止）による縦深防御を管理対象と管理対象外の両方のデバイスで実現します。



FWaaS（Firewall-as-a-Service）

フォーティネットの FWaaS テクノロジーは、第三者機関による認定で高評価を獲得している FortiOS の機能を活用し、高パフォーマンスの SSL インスペクションと高度な脅威検知手法をクラウドから提供します。安全かつ安定した接続を確立し、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

あらゆる場所のあらゆるユーザーとデバイスに ZTNA を提供することで、暗黙のアクセスから明示的な制御への移行を可能にします。アプリケーション単位で適用されるきめ細かい制御により、ユーザーの認証、アイデンティティとコンテキストの継続的な検証、監視を組み合わせて提供します。

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次世代 CASB が、重要な SaaS アプリケーションとシャドー 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セキュアアクセスを提供し、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、アプリケーションアクセスの ZTNA 態勢チェックを可能にします。

NaaS（Networking as a Service）

SD-WAN（ソフトウェア制御による WAN）

フォーティネットのクラウドから提供する SD-WAN には、アプリケーションステアリングと動的ルーティングの機能が組み込まれているため、企業アプリケーションへの最短パスを特定し、それらの接続の整合性が変化した場合はそれを修正することで、優れたユーザーエクスペリエンスが常に提供されるようにすることができます。

アプリケーションの可視化と制御

FortiSASE は、5,000 以上のアプリケーションシグネチャ、ファーストパケット識別、ディープパケットインスペクション、カスタムアプリケーションシグネチャ、SSL 復号、採用が義務付けられている暗号を使用する TLS1.3、ディープインスペクションにより、アプリケーションに対する詳細な可視性ときめ細かい制御を常に可能にします。

SASE の拡大によるすべてのユーザー、エッジ、デバイスの保護

フォーティネットは、SASE ソリューションに新たなイノベーションをもたらします。フォーティネットの SASE は、業界で最も包括的な SASE として、あらゆる場所のユーザー、アクセス、エッジ、デバイスを保護しつつ、最高の ROI、一貫したセキュリティ態勢、優れたユーザーエクスペリエンスを提供します。セキュリティとネットワーキングのコンバージェンスにフォーティネット独自のアプローチを採用することで、SASE に向けたシンプルなセキュアネットワーキングを実現します。

フォーティネット SASE のイノベーションは、ユニバーサル ZTNA、SD-WAN 統合、OT / IoT セキュリティ、LAN / WLAN / 5G セキュリティ、デジタルエクスペリエンス監視、柔軟なライセンスモデルなどの包括的な機能により、ハイブリッドワークのユーザー、クラウドの利用、統合管理、ログを考慮して専用に設計された最先端の AI 活用ソリューションを強化します。フォーティネットの新しい SASE ソリューションは、Web、企業アプリケーション、SaaS アプリケーションのいずれにアクセスする場合も、すべてのエッジ、デバイス、ユーザーで最高のセキュリティを保証します。

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 ファブリックの拡張機能として提供されるため、フォーティネットのセキュリティソリューションのポートフォリオ全体を連携する共通のオペレーティングシステムである FortiOS のパワーがあらゆる場所に拡張されます。このソリューションには、次のようなメリットがあります。

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

包括的なセキュリティとネットワーキングをクラウドから提供し、ユニバーサル ZTNA であらゆる場所のユーザーに対応します。

単一の統合されたエージェント

統合されたエージェントで複数のユースケースをサポートします。FortiClient を、ZTNA、トラフィックの SASE へのリダイレクト、CASB、エンドポイント保護などのユースケースに利用でき、他のソリューションのようにユースケースごとに複数のエージェントが必要になることはありません。

シンプルな管理と利用

独自のセルフサービス設計によるシンプルなオンボーディングと管理を、業界で最も柔軟なユーザーベースの階層型ライセンスモデルで利用できます。

ライセンス情報

REMOTE USERS	BANDS	USER LICENSE
FortiSASE Remote	50-499	FC2-10-EMS05-547-02-DD
	500-1999	FC3-10-EMS05-547-02-DD
	2000-9999	FC4-10-EMS05-547-02-DD
	10 000+	FC5-10-EMS05-547-02-DD

機能リスト

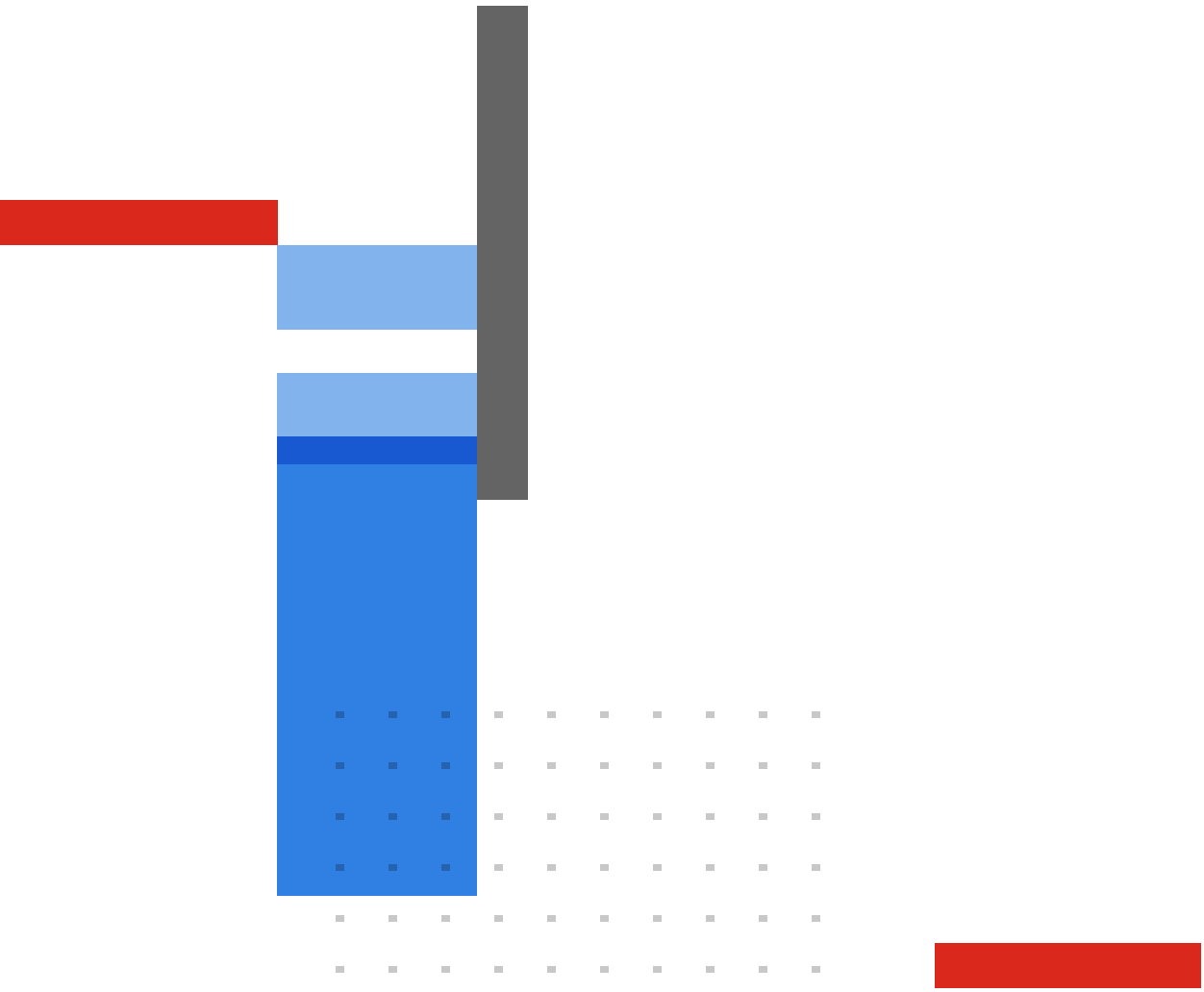
	機能	説明
セキュア SD-WAN	アプリケーションの識別と制御	きめ細かいアプリケーションポリシー、アプリケーション SLA ベースのパス選択、SD-WAN パスの動的帯域幅測定、アクティブ / アクティブおよびアクティブ / スタンバイの転送、暗号化された転送のオーバーレイサポート、アプリケーションセッションベースのステアリング、プローブベースの SLA 測定。産業用制御シグネチャを含む 8,000 以上のアプリケーションの制御。
	高度なルーティング	アプリケーション識別型のルーティング、静的ルーティング、内部ゲートウェイ（iBGP、OSPF v2/v3、RIP v2）、外部ゲートウェイ（eBGP）、VRF、ルート再分散、ルートリーク、BGP コンフェデレーション、ルータリフレクター、サマライズとルートアグリゲーション、非対称ルーティング。
	ネットワークとセキュリティのコンバージェンス	有機的に開発され、専用設計構築で ASIC を搭載する業界唯一の SD-WAN により、シンエッジ（SD-WAN、ルーティング）や WAN エッジ（SD-WAN、ルーティング、NGFW）で、支社のすべてのアプリケーション、ユーザー、データの保護を可能にし、FortiSASE との統合により、あらゆる場所のユーザーへの一貫性ある堅牢なセキュリティの提供が実現します。
	セキュアプライベートアクセス	SASE PoP から複数の SD-WAN ハブにへの IPSec トンネルを確立することで、リモートユーザーをプライベートアプリケーションに安全に接続します（セキュアプライベートアクセス）。
クラウドから提供されるセキュリティ	API-CASB	主要 SaaS プロバイダーに直接接続し、クラウドの利用状況や保存データにアクセスします。これにより、プロビジョニングされたクラウドリソースの構成に潜在する脅威や、SaaS アプリケーションのデータに含まれる脅威、独自情報、機密性の高い顧客レコードを管理者がスキャンできるようになります。さらには、ロケーションやデバイスの区別なく企業の SaaS アプリケーションの全ユーザーを確実に監視し、保護できます。
	インライン CASB	クラウドアプリケーションの移動データや保存データを保護し、データシャドー IT レポートの作成、リスク評価の実行、リスクのトレンドやイベントの可視性を拡張します。
	FWaaS	FortiOS を活用する FortiSASE FWaaS は、Web フィルタリング、高度な脅威保護（ATP）、侵入防止システム（IPS）、ドメインネームシステム（DNS）セキュリティなどのハイパースケールの次世代ファイアウォール（NGFW）機能を提供するクラウドベースのサービスです。FortiGate Firewall に匹敵するセキュリティの有効性を提供します。
	SWG	FortiSASE SWG は、FortiOS の明示的 Web プロキシ、キャプティブポータル、認証機能を利用して、Web トラフィックを保護します。
	ZTNA	ZTNA は、ZTA（ゼロトラストアクセス）においてアプリケーションへのアクセスを制御する機能であり、ZTA の原則を拡張して、すべてのアプリケーションセッションの前にユーザーとデバイスを検証し、組織が定めたそのアプリケーションにアクセスするためのポリシーを満足していることを確認します。
高度な脅威検知	アンチウイルス（AV）	FortiSASE アンチウイルスは、セキュリティアップデートを自動配信して、最新のポリモーフィック型攻撃、ウイルス、スパイウェア、その他コンテンツレベルの脅威から保護します。特許取得済みの Content Pattern Recognition Language（CPRL）ベースのアンチマルウェアエンジンは、既知および未知のウイルス亜種の防止を目的に設計されており、毎週 180 万の新しいアンチウイルス定義が追加されています。
	アンチスパム	FortiGuard アンチスパムは、組織の処理対象となるスパムを包括的かつ多層的なアプローチで検知およびフィルタリングします。二重パスを使用する検知テクノロジーによってネットワークの境界でスパムメールを大幅に削減するため、メールによる攻撃や感染に対する卓越した制御が可能になります。
	アプリケーション制御	FortiSASE は、既知のアプリケーションに加えて、カスタムアプリケーションによって生成されるネットワークトラフィックも認識できます。アプリケーション制御は、IPS プロトコルデコーダーを使用しているため、トラフィックが非標準のポートやプロトコルを使用している場合も、ネットワークトラフィックを分析することでアプリケーショントラフィックを検知できます。個別のアプリケーションや特定タイプのアプリケーションへのアクセスを許可、拒否、または制限するポリシーをすばやく作成できます。
	データ漏洩防止（DLP）	DLP により、複数のクラウドベースシステムの機密情報の特定、データの偶発的な共有の防止、データの監視と保護が可能になります。SOX、GDPR、PCI、HIPAA、NIST、ISO27001 などの標準に対応する FortiCASB の事前定義済レポートを利用してポリシー違反を可視化することで、違反を追跡し、修復できます。
	DNS フィルタリング	DNS フィルタリングは、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。DoT（DNS over TLS）、DoH（DNS over HTTPS）、DNS フラッド保護、DNS トンネリング、DNS 侵入、C2 サーバーの識別、DGA（ドメイン生成アルゴリズム）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。
	侵入防止システム（IPS）	AI / ML を活用する IPS サービスが、ほぼリアルタイムのインテリジェンスと数千の侵入防止ルールの提供し、ネットワークトラフィックのディープパケットインスペクションにより、既知や不審な脅威をデバイスに到達する前に検知してブロックします。フォーティネットのリサーチチームが、このサービスの強化に継続的に取り組んでいます。
	AI を活用する次世代サンドボックス	AI / ML テクノロジーを活用して、高度な脅威をリアルタイムで特定し、隔離します。ファイル、Web サイト、URL、ネットワークトラフィックのインスペクションを実行して、ゼロデイ脅威などの不正活動を検知し、サンドボックステクノロジーを使用して、安全な仮想環境で不審なファイルを分析します。
	SSL インスペクション / 復号	FortiSASE は、ディープインスペクションを使用して、発信元 SSL セッションの受信者になりすまし、コンテンツを復号してインスペクションすることで、脅威を検知し、ブロックします。その後、コンテンツを再暗号化して、実際の受信者に送信します。ディープインスペクションは、HTTPS を使用する攻撃だけでなく、SMTPS、POP3S、IMAPS、FTPS などの一般的に使用される SSL 暗号化プロトコルからも保護します。
	Web フィルタリング	Web フィルタリングは、90 以上のカテゴリに分類された数億件の URL のデータベースを利用することで、きめ細かい Web 制御とレポートを強化します。TLS 1.3 サポートにより、暗号化されたトラフィックの分析も可能になり、未知の不正 URL をほぼ即座にブロックします。クラウド対応により、Web ベースの脅威からの完全な保護、AI ドリブンの検知、分析、適用を提供することで、既知および未知の脅威からのリアルタイムの保護を実現します。
	アウトブレイクアラート	最新のサイバーセキュリティ攻撃の時系列、影響を受けたテクノロジー、適用可能なパッチ / 減災の推奨事項などの包括的で詳細な情報が提供されます。攻撃シーケンスの分析に役立つフォーティネット製品や影響の有無の判断に役立つ脅威ハンティングツールも含まれています。

機能リスト（続き）

	機能	説明
接続	統一されたエージェント	統一されたエージェントで複数のユースケースをサポートします。FortiClient エージェントを、ZTNA、SASE へのトラフィックのリダイレクト、エンドポイント保護などに利用でき、ユースケースごとにエージェントが必要になることはありません。
	エージェントレス接続	BYOD デバイスやエージェントをダウンロードできないデバイス（Chromebook など）においては、PAC ファイルを使用することでエージェントレスセキュリティを利用できます。
	エンドポイント保護	フォーティネットの FortiClient は、セキュリティ、コンプライアンス、承認済アクセスの制御を単一のクライアントで提供します。FortiClient は、スマートフォンやタブレットなどのエンドポイントで直接動作するエンドポイント保護ソフトウェアを提供しています。FortiClient がフォーティネット セキュリティ ファブリックに接続して、デバイスをシステムの他の部分にフィードするため、エンドポイントのセキュリティ情報や可視性が提供され、各デバイスにアクセスする人や物を制御できるようになります。 FortiSASE は、LAN 拡張機能として構成された FortiExtender の管理と統合をサポートします。このソリューションは、FortiClient の代わりに FortiExtender を利用して FortiSASE へのセキュア接続を処理することで、シングルユーザー、シングルデバイスの FortiClient エンドポイントのケースをマルチユーザー、マルチデバイスの LAN 環境に拡張します。
	シンエッジ	業界をリードするフォーティネットのセキュア WLAN / LAN 製品ファミリーは、フォーティネットのシングルベンダー SASE ソリューションとも統合されるため、LAN ソリューションが導入されているセキュアマイクロブランチから FortiSASE ソリューションにトラフィックを送信し、単一の管理コンソールでサイトのすべてのデバイスの包括的なセキュリティを確保できます。
	セキュアエッジ	ユーザーエクスペリエンスを最適化するため、FortiSASE では、ローカルの FortiGate でセキュリティを実行する方法、または支社を FortiSASE に接続して FortiGate NGFW とフォーティネットのセキュア SD-WAN を使用してクラウドでセキュリティインスペクションを実行する方法を選択できます。
	API 接続	FortiSASE は、FortiAnalyzer（分析）、FortiMonitor（DEM）、FortiSIEM（脅威の検知）とのシームレスな統合が可能です。オープン REST API を利用でき、インバウンド API 統合に使用できます。
	認証	SAML ベース認証をサポートし、ネイティブ FortiTrust ID のサポートに加えて、Microsoft Entra ID や Okta などのサードパーティのアイデンティティプロバイダーとのシームレスな統合も可能です。
	専用 IP のサポート	追加ライセンスを利用することで、FortiSASE による専用パブリック IP のサポートが可能になり、ソース IP アンカリングによる IP レピュテーションとジオロケーションサービスをお客様が利用できるようになります。
AI 活用サービス	FortiGuard セキュリティサービス	FortiSASE は、ボットネット保護をデフォルトで提供し、AV、IPS、Web フィルタリング、DLP などのすべてのセキュリティサービスが FortiGuard AI / ML 活用セキュリティにより有効になります。シグネチャのすべてのアップデートと定義がほぼリアルタイムで更新されます。フォーティネットは、630,000 以上の膨大な顧客ベースから得られるインテリジェンスを活用して最新の脅威インテリジェンスを FortiGuard Labs に配信しているため、新しいゼロデイ脅威のシグネチャがすべてのお客様にリアルタイムベースで反映されます。
監視と管理	単一コンソール	管理者は、SASE コンソールを集中管理プラットフォームの単一ダッシュボードとして使用することで、すべてのユースケース（Web、プライベート、SaaS セキュリティ）でオールインワンの構成と可視性が可能になり、セキュリティサービスの導入と管理、ネットワークパフォーマンスの監視、セキュリティイベントの分析を効率的に実行できるようになります。実用的なインテリジェンスとカスタマイズ可能なレポートにより、情報に基づく意思決定や、セキュリティとネットワークの戦略の継続的な最適化が可能になります。
	MSSP ポータル	MSSP ポータルによる一元的な管理と構成の機能により、MSSP が顧客ベースに SASE サービスを効率的に展開し、管理できるようになります。MSSP は、単一画面から、セキュリティポリシー、ネットワーク設定、ユーザーアクセスを構成できるため、複数のクライアント環境で一貫性ある統一されたセキュリティが保証されます。 FortiSASE ソリューションを利用することで、顧客がレポートを生成したり、ログを表示したりすることもできます。レポートとログは、ネットワークで何が起きているかの理解や、ウイルスの検知、無効な Web サイトへの訪問、侵入、ログイン試行の失敗などのネットワークアクティビティの情報の取得に役立ちます。
	レポート	レポート機能を利用することで、ログからデータレポートを生成できます。FortiSASE を構成してスケジュールした間隔で定期的にレポートを実行することも、必要に応じて手動でレポートを実行することもできます。 ログと監視は、ネットワークで何が起きているかの理解や、ウイルスの検知、無効な Web サイトへの訪問、侵入、ログイン試行の失敗などのネットワークアクティビティの情報の取得にも役立ちます。
	分析	レポート機能を利用することで、ログからデータレポートを生成できます。FortiSASE を構成してスケジュールした間隔で定期的にレポートを実行することも、必要に応じて手動でレポートを実行することもできます。

フォーティネット CSR ポリシー

フォーティネットは、サイバーセキュリティを通じてあらゆるお客様の進歩と持続可能性を推進し、人権を尊重する倫理的な方法でビジネスを遂行し、常に信頼できるデジタル世界を実現することをお約束します。お客様には、フォーティネットの製品およびサービスを使用して、違法な検閲、監視、拘留、または過剰な武力行使などの人権の侵害または乱用に関与したり、何らかの形で支援したりしないことをフォーティネットに表明し、保証していただくことになります。フォーティネット製品の利用にあたっては、フォーティネットの EULA（エンドユーザー使用許諾契約）を遵守し、EULA に違反すると疑われる場合は、フォーティネット不正告発規定に概要が記載されている手順で報告する必要があります。



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

DS-FSI-R13-202309-R1