

DATA SHEET

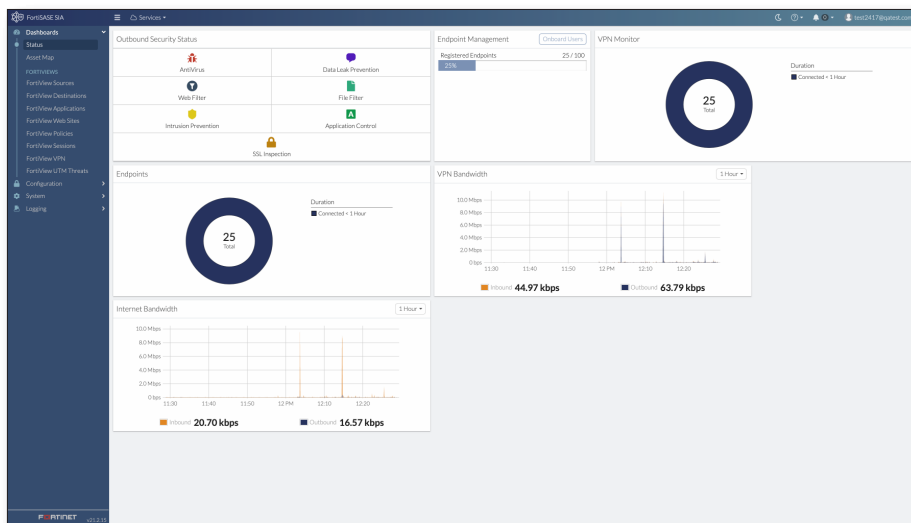
# FortiSASE セキュアインターネットアクセス

提供形態：



クラウド

## リモートワーク向けにクラウドからセキュリティを提供



FortiSASE SIA は、リモートワークのユーザー向けにクラウドから**セキュリティを提供する、専用設計のサービス**です。このスケーラブルなクラウドベースのプラットフォームは、FortiOS の採用により FWaaS (Firewall-as-a-Service)、IPS、DLP、SWG、サンドボックスをリモートワークに拡張することを可能にします。

FortiSASE SIA は**最新のリアルタイム保護**を提供し、クライアントのトラフィックのターミネーション、トラフィックのスキャンによる既知および未知の脅威の検知、あらゆる場所で働くユーザーへの企業セキュリティポリシーの適用を実現します。

FortiSASE SIA は、業界をリードする脅威保護サービスをクラウドから提供することにより、オフィスの外からアクセスするユーザーの管理と保護を**簡素化**します。FortiClient Agent がユーザーのトラフィックを最も近くにある FortiSASE SIA データセンターにトンネリングすることで、**セキュリティの適用と保護**を可能にします。

## リモートワーク向けセキュリティの課題

### 課題

リモートワークのユーザーは、オフィスでは利用可能なファイアウォールやセキュリティによって保護されることなく、自宅や外出先からビジネスクリティカルアプリケーションにアクセスします。このようなユーザーは、サイバー脅威の標的になるだけでなく、デバイスを VPN で接続したり、オフィスに接続されたりすると、企業ネットワークや他のユーザーに大きな脅威をもたらすことにもなります。

### ソリューション

FortiSASE SIA でオンプレミスのポリシーをリモートユーザーとそのデバイスにまで拡張することで、すべてのネットワークエッジに統一されたネットワーキング / セキュリティポリシーを実装し、適用します。

### 主な利点

ユーザーの場所に関係なく、常に一貫性あるファイアウォール / セキュリティポリシーを提供します。

セキュリティポリシーをリモートワーカーにも適用することで企業ネットワークの感染を防止し、優れたユーザーエクスペリエンスを実現します。

## ハイライト



### SASE デリバリモデル

FortiSASE SIA は、フォーティネット セキュリティ ファブリックのコンポーネントを活用してクラウドから提供される SaaS (Security-as-a-Service) ソリューションです。あらゆる場所にいるユーザーが、FWaaS (Firewall-as-a-Service) や SWG (セキュア Web ゲートウェイ) などのセキュリティ機能を容易に利用することが可能になります。



### FortiOS によるアクセラレーション

FortiOS は、フォーティネット セキュリティ ファブリックの核心となるオペレーティングシステムです。セキュリティやネットワークの複数のテクノロジーをあらゆる環境でシームレスに連携させることで、クラス最高の脅威インテリジェンスに基づくユーザーの保護を可能にし、ユーザーエクスペリエンスも向上させます。この包括的アプローチにより、リモートワークのセキュリティギャップが解消され、攻撃や侵害への迅速なレスポンスが実現します。



### 世界トップレベルの保護

FortiSASE SIA は、業界をリードする調査研究機関である FortiGuard Labs の活用により、リアルタイムの保護をリモートワークのユーザーに提供します。世界中に分散する 560 万以上のセンサーから収集した実世界の脅威インテリジェンスを FortiGuard Labs が継続的に分析し、高度な AI を活用して異常や不審なパターンを特定します。これらの情報に基づいて生成された新しい保護が FortiOS とネイティブに統合されて、自動的に配布されます。この完全統合された自動化アプローチにより、攻撃のライフサイクル全体での既知および未知の脅威に対するタイムリーで協調型の保護が実現します。



### スケーラブルな運用コストモデル

デバイス単位の年額課金モデルで利用できるため、過剰なハードウェアに投資することなく、ビジネスの成長に合わせて必要なセキュリティを予測して利用できます。

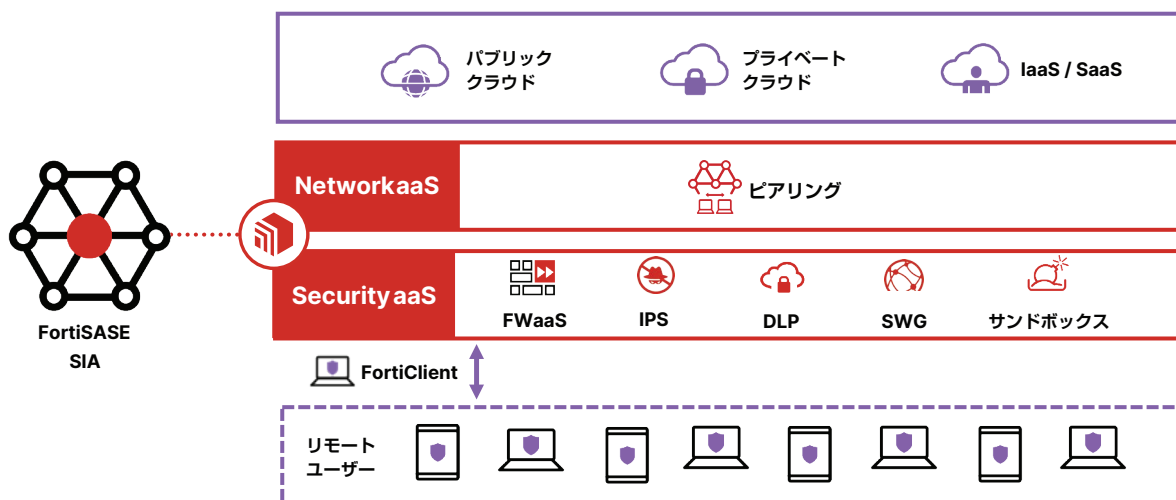
## 概要

### エンタープライズグレードのセキュリティ

Web と E メールは、マルウェアを組織に送り込むために使われる最も一般的な攻撃ベクトルであり、オフィスの外にいるユーザーには多くの場合、組織のネットワークにいる場合と同じレベルの十分な保護は提供されません。リモートユーザーの場合も、組織のネットワークと同じレベルのセキュリティが提供されるようにすることが重要です。

### リモートワークのセキュリティを最適化

FortiSASE SIA は、企業ネットワークの保護下でないリモートワークのユーザーに、SaaS (Security-as-a-Service) を提供します。FortiClient は、ユーザーがネットワークの外にいること検知し、企業のセキュリティポリシーを適用できる FortiSASE SIA サービスにトラフィックをトンネリングすることで、企業が管理するデバイスが保護されない状態でインターネットに公開されてしまうリスクを解消します。



## 主な特長

### マルウェアやエクスプロイトの防止

自動化されたコンテンツアップデート機能、マルウェア / ヒューリスティック検知エンジン、プロアクティブなライブラリ脅威保護を**アンチウイルス**に採用し、すべての既知の脅威と亜種からの保護を実現します。Content Pattern Recognition Language (CPRL) と特許取得済みの新しいコード認識ソフトウェアによって未知の亜種からの保護を可能にすることで、深刻度の高いマルウェア脅威からの保護を実現し、SLA の達成を保証します。

FortiSandbox Cloud は、動的分析を使用して未知の攻撃からの保護を可能にし、自動的な減災を実現します。FortiSandbox Cloud は、不審なファイルを隔離し、実行時の動作を確認できます。有害ファイルと判断された場合は FortiSandbox Cloud によって新しいシグネチャが作成されるため、以降の攻撃をファイアウォールが直ちにブロックします。

FortiClient および FortiSandbox をご利用いただいている世界中の何百万人ものユーザーが、FortiGuard のクラウドベースの脅威インテリジェンスプラットフォームを介して既知および未知のマルウェアに関する情報を共有しています。FortiGuard は、FortiClient エンドポイントと自動的にインテリジェンスを共有し、新たなマルウェア脅威からの保護を可能にします。

FortiClient のランサムウェア対策は、振る舞い分析を活用して、ランサムウェアに見られる不審な振る舞いを検知します。このような振る舞いが検知された場合、FortiClient がランサムウェアをブロックして管理者に警告し、オプションで感染したエンドポイントを自動隔離してネットワークから切断することで、他のエンドポイントの感染を防止します。

### 暗号化トラフィックの分析

インターネットのアプリケーショントラフィックの 95% が暗号化されるようになったことから、攻撃者も暗号化を悪用し、検知を逃れてネットワークに脅威を侵入させるようになりました。**SSL / TLS インспекション**は、暗号化トラフィックの内部のコンテンツをインスペクションすることで、隠れた脅威を検知します。ディープインспекション証明書が自動的にエンドポイントに配布されるため、管理が簡素化されます。

### 継続的な脅威モニタリング

FortiGuard の**侵入防止システム (IPS)** は、ネットワークベースの脅威に対する最新の保護対策を提供します。数千のシグネチャによる包括的な IPS ライブラリ、攻撃検知方法の完全な制御によって複雑なセキュリティアプリケーションにも対応する柔軟なポリシー、そして NSS Labs によって高く評価されたセキュリティ回避手法への対抗機能を活用する、最新の脅威からの保護が実現します。

### フィルタリングサービス

インターネットはビジネスの遂行にあたり重要な役割を果たすようになりましたが、インターネットの不適切な使用は、生産性の低下、企業のリソースの浪費、迷惑行為、法的責任、人事などの問題に発展しかねません。フォーティネットの**FortiGuard Web フィルタリングサービス**は、すべての Web アクティビティを監視し、価値ある実用的インテリジェンスを提供し、新たな法規制、教育関連のコンプライアンス、人事規定、企業のインターネット利用ポリシーの順守を支援します。

FortiGuard は、業界で最も高精度の Web フィルタリングサービスの 1 つを活用し、80 以上のコンテンツカテゴリに分類された Web コンテンツ評価データベースを継続的に更新し、クラウドから提供します。

### アプリケーション制御

**FortiGuard のアプリケーション制御**は、ネットワークアプリケーションの使用を制御して管理対象の企業資産を保護します。高度な検知シグネチャを活用してアプリケーション、DB アプリケーション、Web アプリケーション、プロトコルを識別し、ブロックリストと許可リストの両方を使用するアプローチによってトラフィックを許可または拒否できます。柔軟なポリシーによって攻撃検知方法を完全に制御できます。

### リスクの検知

**データ漏洩防止 (DLP)** は、ネットワークトラフィックを監視してネットワークから持ち出されてはならない機密情報を特定します。FortiSASE SIA は、トラフィックをファイル形式やコンテンツの定義と照合し、標準データタイプと管理者が定義したカスタムエントリの両方を利用して、ファイルの外部への持ち出しを特定し、防止します。

### イベントログ管理

FortiSASE SIA が提供する**リアルタイムのログと分析**の機能を、接続の問題のトラブルシューティング、インシデントの調査、コンプライアンスの監査に利用できます。地域の法規制への対応を支援するため、ログを保存する地域を選択できます。オプションですべてのログを外部のログサービスに転送できます。



## ライセンス詳細

ライセンス名	内容
FortiSASE SIA – 25 Endpoints	License Subscription for 25 Roaming Endpoints. Includes: FortiClient ZTNA Agent, EPP/APT and FortiSASE SIA Subscriptions (EMS hosted by FortiCloud) and 24×7 FortiCare, plus FortiCare Best Practice Service
FortiSASE SIA – 500 Endpoints	License Subscription for 500 Roaming Endpoints. Includes: FortiClient ZTNA Agent, EPP/APT and FortiSASE SIA Subscriptions (EMS hosted by FortiCloud) and 24×7 FortiCare, plus FortiCare Best Practice Service
FortiSASE SIA – 2,000 Endpoints	License Subscription for 2,000 Roaming Endpoints. Includes: FortiClient ZTNA Agent, EPP/APT and FortiSASE SIA Subscriptions (EMS hosted by FortiCloud) and 24×7 FortiCare, plus FortiCare Best Practice Service
FortiSASE SIA – 10,000 Endpoints	License Subscription for 10,000 Roaming Endpoints. Includes: FortiClient ZTNA Agent, EPP/APT and FortiSASE SIA Subscriptions (EMS hosted by FortiCloud) and 24×7 FortiCare, plus FortiCare Best Practice Service

**FORTINET**

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

お問い合わせ