WHITE PAPER

FortiCloud による Security-as-a-Service

IT インフラストラクチャの保護と管理を強化する主なポイントとユースケース

目次

概要 3

SECaaS（Security-as-a-Service）に対するニーズ 3

FortiCloud SECaaS の主な機能 4

FortiGate Cloud 4

FortiWeb Cloud 4

FortiCWP 5

FortiCASB 5

FortiMail Cloud 5

FortiSandbox Cloud 5

FortiCloud の代表的なユースケース 6

クラウドベースの管理 6

クラウドのみで構成されるインフラの保護と管理 6

中小企業のセキュリティ 6

FortiCloud を活用したオンプレミスのセキュリティ強化 7

FortiCloud が提供するソリューション 7

終わりに 7

概要

企業の規模を問わず、インフラの保護にあたってのコストと複雑さが大きな課題となっています。「SECaaS（Security-as-a-Service）」として提供されるセキュリティを採用することで、全体的なセキュリティ態勢が向上しクラウドベースのワークロードの保護が可能になり、セキュリティポリシーの管理作業が軽減されます。さらには、グローバルなデプロイやポリシー管理が簡素化され、管理システム用にハードウェアを追加するためのコストも必要ありません。

FortiCloud は、オンプレミスとクラウドのどちらにおいても、アプリケーションとインフラストラクチャを効率的かつ効果的な方法で保護したいと考える、あらゆる規模の企業のニーズに対応します。

SECaaS（Security-as-a-Service）に対するニーズ

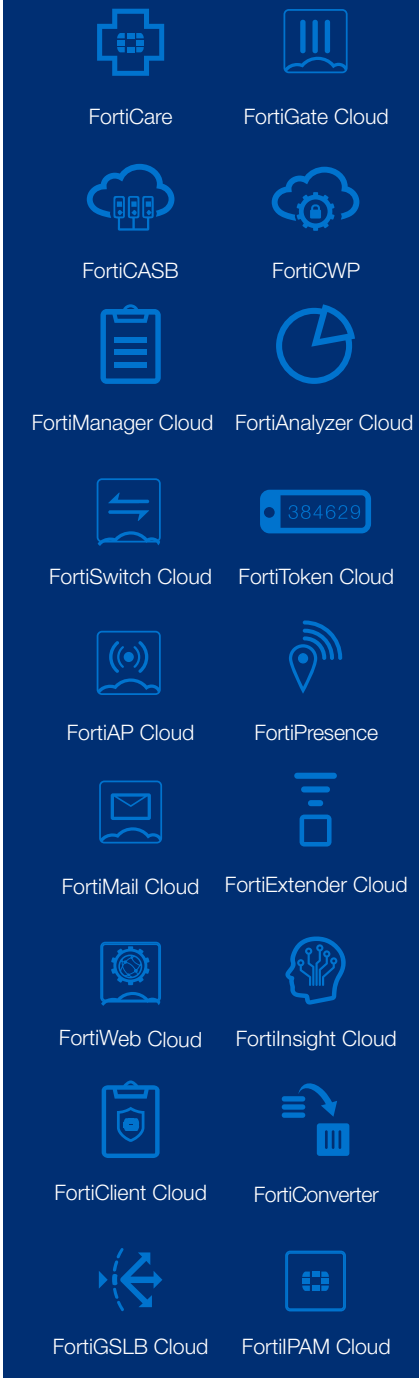
IoT やモバイルコンピューティングの普及によって、「境界」がゲートウェイデバイスからほぼすべてのデバイスへと移行したことで、境界ベースのセキュリティの概念、すなわちすべての出入口のセキュリティ強化に重点を置くシステムは時代遅れになったと言われることが多くなりました。多くのセキュリティのプロフェッショナルが指摘するように、あらゆる場所に境界が存在するようになっています。クラウド、データセンター、デバイスを明確に区別することが困難になった今、オンプレミスのセキュリティの概念にも進化が求められています。今日、デスクトップ、ノート PC、さらにはモバイルデバイスさえもが、オフィス拠点の場所やユーザーがインターネットに接続する場所に関係なく、コンテンツを受け取り、処理できるようになりました。境界だけでなく、クラウドそのものもあらゆる場所に存在するため、セキュリティもあらゆる場所に存在する必要があります。

次世代ファイアウォールやエンドポイント保護などの従来のセキュリティソリューションは、キャンパスやデータセンターの保護においては常に重要な役割を果たしますが、これらの従来型のソリューションがその役割を引き続き発揮できるようにするには、クラウドベースのセキュリティソリューションによる拡張が必要です。

クラウドベースのツールによるローカル環境のセキュリティ強化という考え方は、新しいものではありません。たとえば、20 年前から販売されてきたアンチウイルスソリューションのほとんどで、クラウドから配信される更新されたシグネチャファイルやさまざまな種類の脅威フィードが利用されてきました。しかしながら、対象がオンプレミスかクラウドかという違いが残されてはいるものの、クラウドベースのセキュリティソリューションに対するニーズは増え続けています。

クラウドベース、少なくともクラウドを利用したセキュリティの強化には、あらゆる場所からアクセスや管理が可能であるということだけでなく、拡張性の高さという優位性があります。クラウドから提供される E メールセキュリティは、オンプレミスのアプライアンスとは異なり、E メールの急増に対応できなくなることはありません。また、クラウドベースのサンドボックスであれば、検査するファイルの数や複雑さの増加に合わせた拡張も可能です。オンプレミスのソリューションであっても、クラウドを活用した人工知能（AI）ベースの脅威分析などのツールと統合することで多くのメリットが追加されます。そして、多くの組織が Microsoft 365 や Salesforce、Google Drive などのクラウドベースのサービスを何らかの形で利用するようになった今、クラウドアクセスセキュリティブローカー（CASB）ソリューションの利用こそが、これらのアプリケーションを保護する最適な方法なのです。

FortiCloud 傘下のソリューション



FortiCloud SECaaS の主な機能

FortiCloud は、SECaaS（Security-as-a-Service）を提供する広範なプラットフォームです。他社のアプローチとは異なり、FortiCloud はクラウドネイティブアプリケーションの保護に必要なあらゆる要素を備えており、クラウド環境において効果的で拡張性の高い保護を実現しています。FortiCloud では、次の 3 つに分類されるツールが提供されています。

- SECaaS を提供するツール：FortiWeb Cloud、FortiCASB など
- セキュリティデバイスを管理するツール：FortiGate Cloud、FortiManager Cloud など
- サポート情報を管理するツール（アセット、ライセンス、RMA、サポートチケットなど）：FortiCare

FortiCloud は、フォーティネット セキュリティ ファブリックで重要な役割を担っています。フォーティネット セキュリティ ファブリックがフォーティネットのセキュリティソリューションを緊密に連携させることで、あらゆる場所で発生する悪意のある振る舞いの情報収集、調整、レスポンスが可能になります。

FortiCloud は、フォーティネット セキュリティ ファブリックで重要な役割を担っています。フォーティネット セキュリティ ファブリックがフォーティネットのセキュリティソリューションを緊密に連携させることで、あらゆる場所で発生する悪意のある振る舞いの情報収集、調整、レスポンスが可能になります。

セキュリティ ファブリックの中核となるのは、ネットワークのエッジに配備されるアップストリーム用の FortiGate と、内部セグメンテーションファイアウォール（ISFW）として機能する、ネットワーク内部に配備された複数の FortiGate です。セキュリティ ファブリックを使用することで、FortiAnalyzer、FortiManager、FortiClient、FortiClient EMS、FortiWeb、FortiSwitch、FortiAP といったフォーティネット製品の動作を調整できます。

セキュリティ ファブリックは、他のセキュリティベンダーと一線を画すフォーティネットの大きな差別化要素です。フォーティネット セキュリティ ファブリックは、次の領域に対応します。

- エンドポイントクライアントのセキュリティ
- セキュアな有線、無線、VPN アクセス
- ネットワークセキュリティ
- データセンターセキュリティ（物理、仮想）
- アプリケーション（OTS：市販品、カスタム）セキュリティ
- クラウドセキュリティ
- コンテンツ（E メール、Web）セキュリティ
- インフラストラクチャ（スイッチング、ルーティング）セキュリティ

クラウドセキュリティは、サイバーセキュリティという広範な枠組みの一部に過ぎないかもしれませんが、その重要性は計り知れないものです。クラウドセキュリティを提供する FortiCloud は、以下をはじめとする主要コンポーネントで構成されています。

FortiGate Cloud

FortiGate Cloud は、ご利用中の FortiGate を管理するためのクラウドベースのプラットフォームです。導入環境全体を可視化すると共に、初期導入、セットアップ、継続的な管理をすべて簡素化します。SD-WAN、UTM（統合脅威管理）機能、そして FortiSwitch や FortiAP の導入環境を FortiGate で管理可能となり、機能を拡張すると同時に詳細な分析情報や実用的なレポートを提供します。FortiGate Cloud は、一般的に中小規模企業におけるフォーティネットソリューションの管理に利用されます。

FortiWeb Cloud

極めて高度な保護が要求される Web アプリケーション向けに設計された FortiWeb Cloud は、導入と管理が容易で、コスト効率に優れた堅牢なセキュリティを提供します。FortiWeb Cloud を利用することで、高額な設備投資を行うことなく、DevOps チームとセキュリティアーキテクトはハードウェアアプライアンスや仮想アプライアンスなどの FortiWeb で使用されている実績ある検知テクノロジーを活用可能になります。顧客毎に仮想マシンを作成することで管理ワークロードをさらに増加させるソリューションとは異なり、FortiWeb Cloud は主要なパブリッククラウドを活用し、優れた拡張性を備えた低遅延のアプリケーションセキュリティを実現する、真の SECaaS（Securitu-as-a-Service）ソリューションを提供します。

FortiWeb の中核である AI ベース検知エンジンは、機械学習を利用して通常のパターンから逸脱する要求を特定して対策を実行することで、既知および未知のゼロデイ脆弱性の脅威からアプリケーションを保護します。さらに、FortiWeb と FortiSandbox の統合によって、新しい脅威や未知の脅威の AI を活用した検知や、MITRE ATT&CK フレームワーク、OWASP トップ 10 の脆弱性のインスペクション、FortiGuard Labs からのリアルタイムの脅威フィードにも対応します。

FortiWeb は、Web ベースのアプリケーションとそれらのアプリケーションで使用されている API（アプリケーションプログラミングインタフェース）を保護します。FortiWeb Cloud は、クラウドから提供される真の SECaaS（Security-as-a-Service）であるため、従量制で利用できハードウェアを追加する必要もありません。

FortiWeb の中核である AI ベース検知エンジンは、機械学習を利用して通常のパターンから逸脱する要求を特定して対策を実行することで、既知および未知のゼロデイ脆弱性の脅威からアプリケーションを保護します。

FortiCWP

FortiCWP は、セキュリティ管理者と DevOps チームによる、クラウド構成のセキュリティ態勢の評価、クラウドリソースの構成ミスに起因する潜在的な脅威の検知、クラウドリソース（クラウドの内部と外部）のトラフィックの分析、ベストプラクティスとの比較によるクラウド構成の評価を可能にします。FortiCWP のこれらの豊富な機能を利用することで、マルチクラウドインフラストラクチャ全体のリスク管理、法規制のコンプライアンスレポートの作成、クラウドインフラストラクチャのライフサイクルおよび自動化フレームワークへの修復機能の統合が可能になります。

FortiCASB

FortiCASB はフォーティネットが開発したクラウドネイティブのクラウドアクセスセキュリティブローカー（CASB）サブスクリプションサービスで、企業が使用するクラウドベースのサービスに対して、可視性、コンプライアンス、データセキュリティ、および脅威保護を提供する、広範な CSPM（Cloud Security Posture Management：クラウドセキュリティ状態管理）の機能セットを備えています。FortiCASB は、主要 SaaS アプリケーションに対して、ユーザー、振る舞い、格納データに関するポリシーベースの洞察と包括的なレポートツールを提供します。Microsoft 365、Microsoft OneDrive、Google Drive、Salesforce.com、Dropbox、Box をはじめとする主要な SaaS / クラウドサービスとの API ベースの完全な統合に加えて、コンプライアンスレポートやシャドー IT の検知が可能です。

FortiMail Cloud *

FortiMail Cloud は、従業員とデータをサイバー攻撃から保護する包括的な E メールセキュリティを実現します。そのセキュリティの有効性は、第三者機関から業界トップクラスの評価を得ています。SECaaS（Security-as-a-Service）として提供されるため容易に利用を開始可能で、継続的な管理の負荷が最小限に抑制されると同時に、セキュリティサービスの大半はエンドユーザーへの容易な拡張が可能です。FortiMail は、99.5% 以上のスパム検知率と多層型マルウェア検知を実現すると同時に、極めて低い誤検知率を達成しています。完全なマネージドサービスである FortiMail Cloud を利用することで、E メールの保護をフォーティネットに委ね、安心してビジネスに集中できるようになります。

FortiSandbox Cloud

トップクラスの評価を得ている FortiSandbox は、フォーティネットが提供するセキュリティ侵害対策ソリューションの一部であり、フォーティネット セキュリティ ファブリック プラットフォームと統合することで、広範なデジタル攻撃領域のランサムウェアやクリプトマルウェアをはじめとする、急速に進化する標的型攻撃の脅威からの保護が可能になります。ゼロデイ、高度なマルウェアの検知とレスポンスの自動化によって、実用的なインテリジェンスをリアルタイムで提供します。FortiSandbox は、特許出願中のブーストツリーによる拡張ランダムフォレストと最小二乗法による最適化という 2 つの機械学習モデルを、疑わしいオブジェクトの静的 / 動的分析に適用することでゼロデイ脅威の検知効率とパフォーマンスを向上させます。また、MITRE ATT&CK フレームワークに基づく標準をマルウェアレポートに採用しており、脅威の調査と管理のプロセスを高速化します。

* FortiMail Cloud は 電気通信事業者の免許をお持ちのパートナーを経由してご契約の上、ご利用いただくことが可能です。詳細はフォーティネットジャパンまでお問い合わせください。

FortiCloud の代表的なユースケース

クラウドベースの管理

あらゆる規模の組織が、より効率的でコスト効率も高いデバイスのアクセスや管理方法を模索しています。FortiCloud では、Web ベースのポータルからオンプレミスとクラウド両方のフォーティネット製品（物理デバイス、仮想デバイス）を管理できます。さらに、デバイスベースのサポートを提供する FortiCare にアクセスし、ファームウェアアップデート、テクニカルサポート、動的なポリシーに対応する基本的な FortiGuard サブスクリプションを活用することができます。このユースケースで利用されている以下のコンポーネントは、個別に購入する必要があります。

主要なコンポーネント

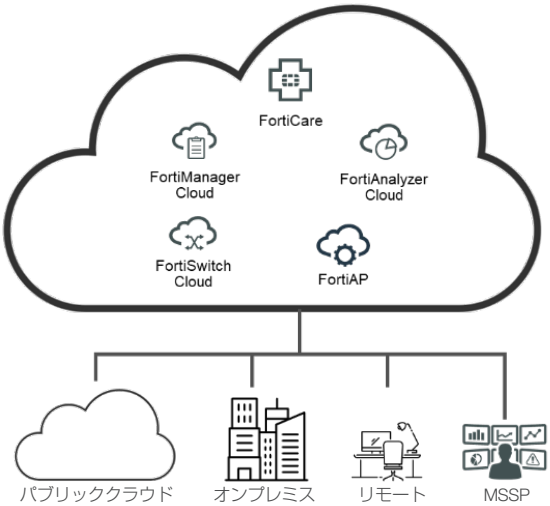
FortiCare：フォーティネット製品、アカウントベースサービスの管理、プロフェッショナルサービス、ライセンス、サポートチケット、RMA などへのアクセス

FortiManager Cloud：簡素化されたゼロタッチプロビジョニングや豊富なツールセットを活用する管理機能により、デバイスの台数を問わず単一のコンソールから一元管理が可能

FortiAnalyzer Cloud：クラウドベースのシステム分析、イベント管理、状態監視サービスを提供

FortiAP Cloud：直感的で使いやすいシンプルなクラウドインタフェースで、スタンドアロンの FortiAP のライフサイクル管理を一元化

FortiSwitch Cloud：直感的で使いやすいシンプルなクラウドインタフェースで、スタンドアロンの FortiSwitch のライフサイクル管理を一元化



クラウドのみで構成されるインフラの保護と管理

クラウドによって、組織は迅速に作業を進めて俊敏性を向上させると同時に、設備投資を削減できます。このようなメリットを最大限に活かすために、ハードウェアの増設ではなくクラウドベースのサービスを優先的に選択する組織が増えています。FortiCloud は、SECaaS（Security-as-a-Service）をクラウドから提供します。FortiCloud では、クラウドベースのデータやワークロードを保護し、Salesforce や Microsoft 365 などの SaaS ベースのアプリケーションを安全に利用するためのツールも提供されています。また、クラウドからフォーティネットの物理デバイスや仮想デバイスを管理することも可能になります。このユースケースで利用されている以下のコンポーネントは、個別に購入する必要があります。

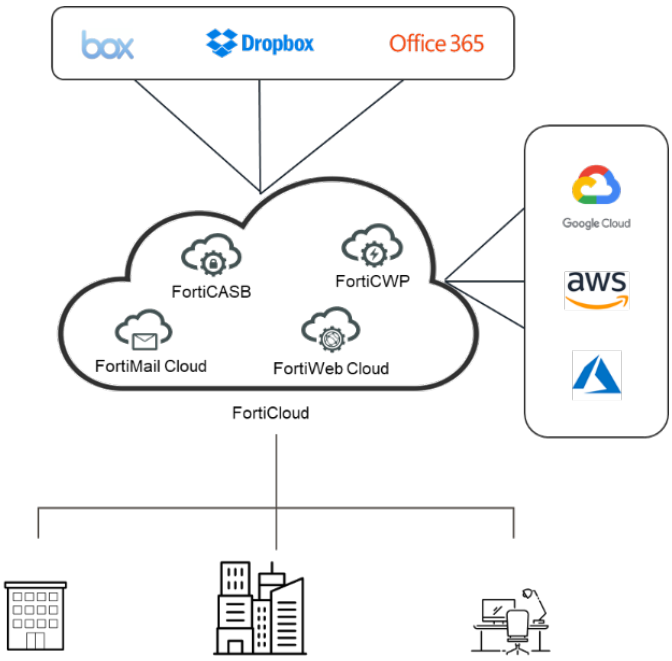
主要なコンポーネント

FortiWeb Cloud：SECaaS ベースの Web アプリケーションファイアウォール

FortiCWP：SECaaS ベースでクラウドワークロードやクラウドデータを保護

FortiCASB：Microsoft 365 や Salesforce などの SaaS アプリケーションを保護し、シャドー IT を検知

FortiMail Cloud *：トップクラスの評価を得ている SECaaS ベースのセキュア E メールゲートウェイ



* FortiMail Cloud は 電気通信事業者の免許をお持ちのパートナーを経由してご契約の上、ご利用いただくことが可能です。詳細はフォーティネットジャパンまでお問い合わせください。

中小企業のセキュリティ

中小規模の企業には、大企業と同じ脅威に直面するものの脅威に対処するリソースや人員が少ないというさらなる課題が存在します。FortiCloud は、Security-as-a-Service をクラウドから提供します。さらに、クラウドベースのデータやワークロードを保護し、Salesforce や Microsoft 365 などの SaaS ベースのアプリケーションを安全に利用するための、構成が容易で使いやすいツールも提供されています。また、クラウドからフォーティネットの物理デバイスや仮想デバイスを管理することも可能になります。このユースケースで利用されている以下のコンポーネントは、個別に購入する必要があります。

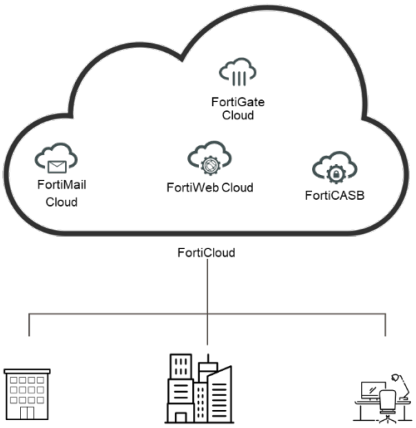
主要なコンポーネント

FortiGate Cloud：FortiGate を管理する、クラウドベースの軽量のプラットフォームです。FortiGate Cloud を使用することで、SD-WAN や UTM の機能、さらには FortiSwitch や FortiAP の導入環境の管理が可能になり、機能性が拡張されます。FortiGate Cloud は、豊富な分析機能と実用的なレポートも提供可能です。

FortiWeb Cloud：SECaaS ベースの Web アプリケーションファイアウォール

FortiCASB：SaaS アプリケーションの保護とシャドー IT の検知

FortiMail Cloud *：トップクラスの評価を得ているSECaaSベースのセキュアEメールゲートウェイ



FortiCloud を活用したオンプレミスのセキュリティ強化

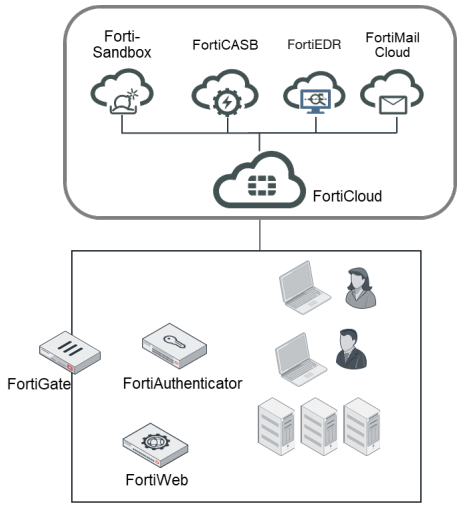
多くの組織では、クラウドへのアプリケーションの移行や付随するセキュリティのクラウドへの移行が進行していますが、引き続きデータセンターやオフィス、支社を維持している企業が大半を占めています。FortiCloud は、リアルタイムの脅威フィード、AI ベースの脅威分析、クロスプラットフォーム管理、拡張性の高いセキュリティ製品群を提供し、オンプレミスのセキュリティを強化します。

主要なコンポーネント

FortiSandbox Cloud：フォーティネットのデバイスや他のネットワーク機器から不審なファイルを受信して、安全なスキャンと実行を通じて検証します。FortiSandbox は、リアルタイムの脅威フィード、人工知能、MITRE ATT&CK フレームワークを使用して、既知と未知の両方の脅威を検知します。

FortiEDR：エンドポイントの感染前と感染後に高度な脅威保護をリアルタイムで実現します。プロアクティブに攻撃対象領域を減らし、マルウェアによる感染を防止すると同時に、潜在的な脅威をリアルタイムで検知して無効化し、カスタマイズ可能なプレイブックによってレスポンスと修復の手順を自動化します。FortiEDRは、クラウドでのマルチテナント管理、クラウドベースの脅威フィードの受信、オンプレミスあるいはクラウドでの FortiSandbox の統合を可能にします。

* FortiMail Cloud は 電気通信事業者の免許をお持ちのパートナーを経由してご契約の上、ご利用いただくことが可能です。詳細はフォーティネットジャパンまでお問い合わせください。



オンプレミスの施設
（データセンター、キャンパス、支社）

FortiCASB：Microsoft 365 や Salesforce などの SaaS アプリケーションを保護し、シャドー IT を検知

FortiMail Cloud *：トップクラスの評価を得ているSECaaSベースのセキュアEメールゲートウェイ

FortiCloud が提供するソリューション

FortiCloud は、クラウドから Security-as-a-Service を提供すると同時に、オンプレミスに対しても最新の脅威フィードや AI ベースの脅威分析、クロスプラットフォーム管理、統合されたサービス管理機能を提供し、セキュリティを強化します。

終わりに

従来型のセキュリティツールは、クラウドから提供されるサービスで強化することができます。これと同時に、当然ながら従来のセキュリティデバイスはクラウドベースのアプリケーションやデータの保護に適したものではありません。したがって、セキュリティや脅威インテリジェンスのフィード、管理をすべてクラウドから提供するソリューションが不可欠です。セキュリティの未来は、脅威の検知と修復の優れた機能だけでなく、クラウドネイティブの新しいアーキテクチャによって実現します。そのようなアーキテクチャでは、あらゆるデバイスの保護をセキュリティ ファブリックに集約し、実行場所を問わずすべてのアプリケーションを統一されたセキュリティで保護可能になります。

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

WP-SaaS-FortiCloud-202009-R1