SOLUTION BRIEF

# FortiCloud で実現する、クラウドインフラとアプリケーションの保護

## 概要

**クラウドインフラやアプリケーションの適切な保護にあたっては、クラウドを前提に構築され、クラウドからサービスとして提供されるソリューションが必要です。FortiCloud とその傘下のソリューションは、先行投資やハードウェアを必要とすることなく、アプリケーション、ワークロード、データ、E メールの保護を可能にします。セキュリティを低下させることなく、クラウドコンピューティングの俊敏性と柔軟性を実現したいと考える組織に最適のソリューションです。**

**クラウドコンピューティングは、管理やオーケストレーション、分析のための多くのシステムのホストとして機能し、アプリケーションやユーザーが安全なネットワークの外側に存在することになるため、攻撃対象領域がこれまで以上に拡大します。**

## クラウドネイティブアプリケーションの保護にあたっての課題

設備投資を抑制し、俊敏性を向上させ、人工知能（AI）エンジンや高度な分析ツールなどの強力なサービスを利用するといった理由から、コンピューティングリソースのクラウドへの移行を進める企業が増えています。あらゆる規模の企業が、クラウドを利用すればデータセンターを自社で構築して管理することなく、高度なアプリケーションを活用できることに気付きました。

クラウドコンピューティングでは、オンプレミスのインフラストラクチャと変わらないセキュリティを確保することはできますが、クラウドに固有の新たなセキュリティの課題にも直面することになります。攻撃対象範囲の拡大に加えて、複数のクラウドや、場合によってはクラウドとデータセンターの両方に存在する複数のアプリケーションの保護が必要になること、さらにはクラウドセキュリティの十分なスキルを持つプロフェッショナルが業界全体で不足していることなどが挙げられます。

攻撃対象領域とは、攻撃者によるコンピューティングシステムへの侵入、変更、あるいは混乱を可能にする、さまざまなベクトルの総称です。クラウドコンピューティングは、管理やオーケストレーション、分析のための多くのシステムのホストとして機能し、アプリケーションやユーザーが安全なネットワークの外側に存在することになるため、攻撃対象領域がこれまで以上に拡大します。さらには、API（アプリケーションプログラミングインタフェース）を活用するクラウドネイティブアプリケーションは、プログラムによる管理が可能であるため、新たな攻撃ベクトルを生み出すことにもなります。また、クラウドアプリケーション開発に DevOps 手法が取り入れられるようになっていることから、高い権限を付与された開発チームが、セキュリティプロフェッショナルチームによるレビューを受けることなく新しいアプリケーションや変更されたアプリケーションを投入する可能性があります。

クラウドの採用によって新たに発生する脆弱性を解決するため、多くの組織が統合されていないポイントセキュリティ製品を次々と導入するようになりました。平均的な企業では 75 種類以上のセキュリティソリューションが利用されていると言われていますが、それらの多くはリスクやコンプライアンス要件のひとつのみを解決するものです。継続的な設備投資によって新たなポイント製品を次々と購入する必要があるだけでなく、これらの異なるソリューションの多くは相互に連携する機能が欠如しているため管理の負担が増大し、新たなセキュリティギャップが発生して脅威が防御をすり抜ける可能性が高くなります。クラウドインフラやアプリケーションの管理にあたっては、セキュリティチームの負担を軽減し、ROI が高く、継続的なコンプライアンス、安全性、耐障害性の維持を可能にする一貫したアプローチが不可欠です。

## フォーティネットでクラウドネイティブアプリケーションを保護する

従来のセキュリティソリューションは、ネットワークの周囲に安全な境界を構築するという発想で設計されています。ところが、「境界」があらゆる場所に存在するクラウドの時代、この手法は利用できなくなっています。クラウドネイティブアプリケーションの保護には、クラウドを前提に構築され、クラウドから提供できるソリューションが必要です。クラウドセキュリティは、以下をはじめとする要素で構成されます。

- アプリケーションの保護
- ワークロードとストレージの保護
- E メールの保護
- Microsoft 365 や Salesforce などの SaaS アプリケーションの保護
- 構成やコンプライアンスの管理
- サンドボックス
- 機械学習と人工知能を採用したリアルタイムの脅威フィードによる高度な脅威保護
- 一元的な管理と分析

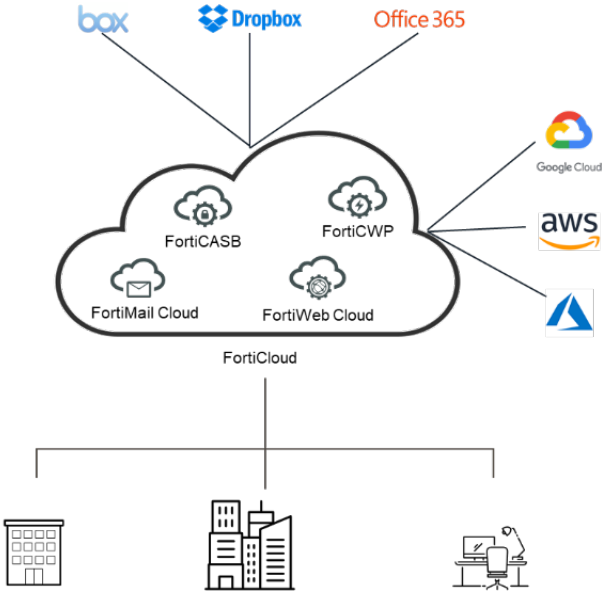


図 1：フォーティネットによるクラウドネイティブアプリケーションの保護

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 には、FortiWeb Cloud や FortiCASB などの SECaaS（Security-as-a-Service）を提供するツールに加えて、FortiGate Cloud や FortiManager Cloud などのセキュリティツールの管理、さらにはアセット、ライセンス、RMA の追跡に使用される FortiCare などへのアクセスも提供されています。

万全なソリューションである FortiCloud がフォーティネット セキュリティ ファブリックの重要な要素として加わることで、フォーティネットの各セキュリティソリューションが連携し、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。

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。FortiCloud には、クラウドセキュリティに関連する次の主要コンポーネントが含まれています。

### 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、DevOps チームとセキュリティアーキテクトは高額な設備投資を行うことなく、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しなければならず、すでに多くの負担を強いられているチームの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環境を活用し、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 Security-as-a-Service（SECaaS）ソリューションを提供します。

**フル装備のフォーティネット セキュリティ ファブリックが対応する領域**

- 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

FortiWeb の中核である AI ベース検知エンジンは、ML 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し、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 を保護します。FortiWeb Cloud は、クラウドから提供される真の SECaaS 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。

### 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 は、Microsoft Office 365、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。**

### 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、行動、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。FortiCASB は、Microsoft Office 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 [1]。 SECaaS ソリューション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 ML 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。

### 次のステップ

FortiCloud は、セキュリティを低下させることなくクラウドコンピューティングの俊敏性と柔軟性を実現したいと考える組織に最適のソリューションです。FortiCloud は、SECaaS や他のセキュリティツールの管理、ライセンスなどのアセットを追跡する機能を提供し、万全なソリューションとしてクラウドネイティブアプリケーションの保護を実現します。特にフル装備のフォーティネット セキュリティ ファブリックの一部として提供される場合は、そのメリットが最大限に活かされます。

[1] 「Email Security Services Protection」、SE Labs、2020 年 1 ～ 3 月（英語）：https://www.fortinet.com/content/dam/fortinet/assets/white-papers/selabs2020.pdf

* 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。

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