



# 分散環境における Webアプリケーションと APIの保護

包括的で使いやすいSaaS型セキュリティソリューションを使用し、マルチクラウドとオンプレミスのインフラストラクチャに導入されたWebアプリケーションとAPIを保護します。



## KEY BENEFITS

### 包括的で使いやすい SaaS 型セキュリティ

単一の SaaS 型セキュリティソリューションを使用し、あらゆるクラウドとオンプレミスで Web アプリケーションと API を保護します。

### 分散アプリケーションとマルチクラウド環境のためのソリューションにより、どこにでも導入可能

F5 Distributed Cloud Services は、最新のモジュール化が進んだ分散アプリケーションに対し、高度で利用しやすいセキュリティを提供します。

### エンドツーエンドの可観測性とポリシー適用により、SecOps の業務を効率化、高速化

クラウドでもオンプレミスでも、ポータブルな可視化と統一されたセキュリティポリシーを提供することにより、SecOps チームの効率性を向上させます。

### 統合型サービス、SaaS フォームファクタおよび柔軟な導入により TCO を削減

異なるクラウドセキュリティソリューションを単一のクラウドセキュリティスタックに集約することで、個別のポリシーやインフラストラクチャを維持する必要がなくなり、総所有コストを削減できます。

### 開発者体験を向上し、サービス提供までの時間を短縮

既存の CI/CD ワークフローや DevOps ツールに簡単にプラグインできるので、通常のプロセスの一端としてセキュリティワークロードの導入と検証を自動化でき、開発者体験を最適化できます。

## マルチクラウドおよびエッジ環境においてアプリケーションと API のセキュリティを拡張

現在のアプリケーションを中心とした世界では、アプリケーションのセキュリティは事業継続に不可欠です。

アプリケーションを保護することは、ビジネス、顧客、収益源を保護することを意味します。そのため、オンラインでの商取引を運営または促進する組織はセキュリティを軽視できません。アプリケーションに対する脅威はどこにでも存在し、アプリケーションセキュリティの技術や専門知識を習得、実装、維持することは従来どおり困難です。開発モデルやアプリケーションアーキテクチャが進化し、マルチクラウドでの導入、API の急増、自動スケーリング、サーバーレスの実装が関連するようになったことで、この問題はさらに困難になっています。

最新のマイクロサービスは、アプリケーション使用量の増加に対応し、パフォーマンス向上を実現するために、分散型アプリケーションアーキテクチャを使用して構築されることが増えています。可用性とパフォーマンスに対するユーザーの期待が変化するにつれ、企業は、データへのアクセスや重要なテレメトリーの処理を高速化するために、元のクラウドに長い時間戻るのはなく、軽量アプリケーションをブランチおよびサテライトで実行するようになっています。しかし、このような分散型アプリケーションインスタンスに対して一貫した効果的なセキュリティを提供することは、企業にとって困難です。

NetOps と SecOps はこのような急速な変化から遅れを取っています。DevOps チームは、このような状況、そしてそこで使われているセキュリティツールキットを、ビジネスが求める革新を阻害するものと見なしています。さらに、最新のマイクロサービスベースのアプリケーションと API が増加したことで、アプリケーションの攻撃対象は拡大し、従来のソリューションでは一貫した保護を提供できなくなっています。SecOps チームは、異なるレガシーセキュリティソリューションを活用し維持しなければならず、その努力の成果は本来よりも少なくなっています。

このような課題の結果、TCO が増加し、進化する攻撃に対抗するためのセキュリティの有効性が低下しています。また、リソースが限られていて、ツールが非効率的であるため、攻撃が発生した場合、SecOps の対応は手作業になることが多く、すでに逼迫したリソースにかかる負担はさらに大きくなります。

セキュリティを軽視する組織は、ビジネスそのものをリスクにさらしています。しかし、このような複雑性を緩和し、サイバー犯罪を受けづらくする方法はあります。機械学習とグローバルな脅威インテリジェンスを適応、拡張、活用できるセキュリティ中心のインフラストラクチャに投資を行うことで、ビジネスを推進する Web アプリケーションと API の保護は、不満ではなく効果を生み出すようになります。

## KEY FEATURES

### どこにあるアプリケーションにも 対応するフル機能の

#### セキュリティソリューション

ネットワークエッジ、パブリッククラウド、オンプレミスなど、アプリケーションやワークロードがどこに導入されていても、一元化されたコントロールプレーンを介して、自己修復やヘルスマonitoringによる漸進的なロールアウトなど、セキュリティプロビジョニングを自動化します。

### ニーズに合わせてスケールする 強力な保護機能

高度な Web アプリケーションファイアウォール、DDoS 軽減、ボット検知、API セキュリティなどの堅牢な適応型セキュリティサービスは、組織のニーズまたは個々のアプリケーションのニーズに応じたレイヤー化が可能です。

### 一元化された可観測性： ネットワーク + アプリケーション + セキュリティ

アプリケーション導入、インフラストラクチャの健全性、セキュリティ、可用性、パフォーマンスといった詳細なステータスなど、異種混在のエッジおよびクラウド導入において、アプリケーションからインフラストラクチャまでの統合的な可視化が可能です。

### 専用のグローバルネットワーク

F5 は、アプリケーション間の接続とグローバルなアプリケーション配信に最適化された 13 のメトロマーケットにまたがる、20 以上のグローバル PoP が配備された高性能なグローバルバックボーンを提供しています。

### ID とシークレットの管理

証明書の自動ローテーションにより、アプリケーションインスタンスごとに ID ライフサイクルを管理し、異なるマルチクラウドやエッジ環境にあるアプリケーションに対して統一された ID サービスを提供します。

## 一元的なセキュリティとグローバルな運用を簡素化

F5は、比類ないパフォーマンスとグローバルなスケールで、最新のアプリケーションを保護し、セキュリティを確保します。F5のクラウドネイティブセキュリティサービスは、世界中のあらゆる規模の組織におけるあらゆる規模のさまざまなアプリケーションを保護してきた数十年の経験に裏付けられています。

これらのサービスは、機械学習とグローバルに収集された脅威インテリジェンスを活用し、アプリケーションを標的とする可能性のある進化し続ける脅威から保護します。セキュリティに対するレイヤー化されたモジュール式のアプローチにより、必要なコントロールのみを取得して実装できるため、コストを削減し、全体的な有効性を向上できます。

また、F5 Distributed Cloud Servicesを利用することで、データセンターからクラウドやエッジに至るまで、クラウドネイティブな管理、一貫したセキュリティ、エンドツーエンドの可観測性を備えた最新のコンテナ型アプリケーションの導入と実行が可能になります。数分以内に効率的に導入される共通のポリシーとサービスのセットにより、世界中の多くのユーザーが、重要なアプリケーションを利用できるようになります。

## ソリューションコンポーネント

F5 Distributed Cloud Web Application and API Protection (WAAP) ソリューションは、データセンターのグローバルなネットワーク上にクラウドネイティブなアプリケーションインフラストラクチャを構築し、堅牢で効果的なアプリケーションおよびAPI保護サービスを広範囲に提供します。

- **Web Application Firewall (WAF)**: 中間プロキシとして機能し、アプリケーションのリクエストとレスポンスを検査して、ハッキング、ゼロデイ攻撃、L7サービス拒否など、広範なリスクをブロックおよび軽減することで、Webベースのアプリケーションを無数の脅威から保護します。
- **API保護**: アプリケーションプログラミングインターフェイスを悪用し、侵入やその他のサービス停止を狙う脅威アクターから保護します。API保護は、WAFと同様の機能を実行します。しかし、従来のWAFは、その性質上、APIのプロトコルやデータフローを十分にカバーできないのが一般的でした。このため、WAFを導入しただけでは、多くのアプリケーションで深刻なセキュリティギャップが発生しています。
- **ボット対策**: 悪意のある自動化を管理および回避し、正当なマシン間のコミュニケーションを仲介して、Web不正行為、知的財産権の盗難、クレデンシャルスタッフィングやアカウント乗っ取り、産業スパイ、サービス拒否などのビジネスロジックのリスクから防御します。
- **DDoSプロテクション**: スプーフィングトラフィックや不正なトラフィック、リクエストフラッドなど、サービスに過剰な負荷をかけてオフラインにしたり、信頼やサービスへのアクセスが損なわれる方法でサービスを中断させようとする悪用をフィルタリングすることで、大規模なサービス拒否攻撃に対するネットワークレベルのシールドを提供します。

アプリケーションを保護することは、ビジネス、顧客、収益源を保護することを意味します。

どこに導入されるアプリケーションにも、これらの保護のいずれか（またはすべて）をシームレスに追加できます。また、インジェクション、クロスサイトスクリプティング、ソフトウェアの脆弱性などの一般的な脅威に対抗するために、必要に応じて保護を実装および進化できます。

さらに、F5 Distributed Cloud WAAP は、グローバルに分散したアプリケーションの運用インサイトとパフォーマンスデータを一元的に提供し、全体の効率性を高め、サポートを合理化し、顧客の拡大と維持に役立つビジネスインテリジェンスメトリクスを向上させます。

F5の一元管理されたクラウドプラットフォームは、他にも利点があり、監査を簡単にする、アプリケーションのポリシーを大規模に徹底する、アプリケーションが直面するリスクや脅威にポリシーを適用させるなどが可能です。

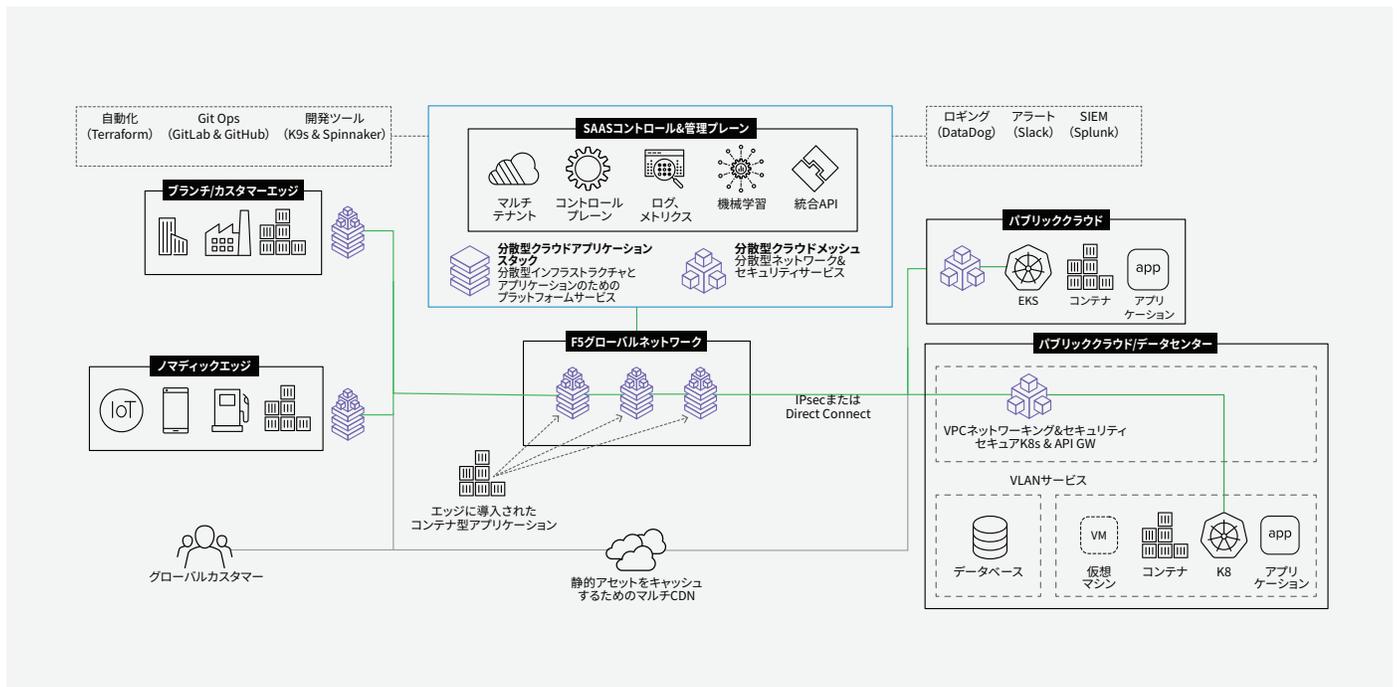


図1: F5 Distributed Cloud Services

F5 DISTRIBUTED CLOUD WEB APPLICATION AND API PROTECTION ソリューションは、データセンターのグローバルなネットワーク上にクラウドネイティブなアプリケーションインフラストラクチャを構築し、堅牢で効果的なアプリケーションおよび API 保護サービスを広範囲に提供します。

## 高性能かつ効果的で、スケーラブルなセキュリティにより優れたデジタル体験を提供

アプリケーションはビジネスの生命線であり、サイバー犯罪者もそのことを十分に理解しています。現代の脅威に対抗するには、スケーラブルで適応性の高いセキュリティソリューションが必要です。アプリケーションのモジュール化と分散化が進んだことで、どこにでも導入でき、一元化された SaaS 型インフラストラクチャで管理される、安全なサービスが必要になっています。

F5 Distributed Cloud Services は、今日のアプリケーションアーキテクチャに必要なセキュリティの有効性と使いやすさを提供します。より優れた方法で、比類ないパフォーマンスと可用性を備えた最新のアプリケーションサービスを大規模に提供できます。データセンターやコロケーションサイトからクラウドパートナーやエッジに至るまで、顧客の要望に応じてどこにでも、コンテナやマイクロサービスアプリケーションを導入および実行でき、クラウドネイティブな運用、一貫したセキュリティ、エンドツーエンドの可観測性を提供します。

一貫した再現性のある結果、グローバルなセキュリティ、ポリシー適用を実現する「write-once, run anywhere（一度書けば、どこでも実行できる）」セキュリティポリシーのメリットを体験してください。F5 の API ドリブンによるアプリケーション保護アプローチは、ネットワーク、セキュリティ運用、開発者間の連携を強化し、クラウドにとらわれないアプリケーションの導入と管理インフラストラクチャは、アプリケーションが導入される場所を問わず、クラウド間での運用、パフォーマンス、分析、脅威の可視化を実現します。

この革新的で利用しやすいプラットフォームは、アプリケーション保護のセキュリティギャップを減らし、アプリケーションポートフォリオ全体で一貫したセキュリティを確保できます。F5 Distributed Cloud WAAP を使用することで、効果的なセキュリティを簡単に手に入れることができるだけでなく、ビジネスと顧客が求める革新を促進できます。

## 次のステップ

詳しくは、[f5.com/waap](https://f5.com/waap) をご覧ください。

