バイヤーズガイド

# クラウドベースのセキュア Web ゲートウェイの選び方

テレワーカーを保護し、エンタープライズセキュリティをシンプル化

# 目次


**先進的なエンタープライズのセキュリティ確保：データセンターのバックホールを見直す** 2

**テレワークの拡大が IT とセキュリティにもたらす新たな需要** 3

**なぜクラウドベースのセキュア Web ゲートウェイが必要なのか** 5

**セキュア Web ゲートウェイの主な要件** 6

- すべての DNS 要求および URL 要求の評価 6
- 複数のペイロード分析手法 7
- ゼロデイフィッシング検知 7
- 暗号化トラフィックの検査 7
- データ損失防止機能の統合 8
- シャドー IT の識別と管理 8
- 場所を問わずあらゆるデバイスを保護する機能 9
- すべてのエンタープライズアプリケーションへのセキュアなアクセス 9
- 最適なパフォーマンス 11
  - Office 365 の統合 11

**セキュリティをエッジに移動** 12


# 先進的なエンタープライズのセキュリティ確保：データセンターのバックホールを見直す

クラウドコンピューティング、Software as a Service（SaaS）、モビリティ、そして最新のネットワークアーキテクチャは、ビジネスの手法に大きな変化をもたらしました。しかし、これらの新しいテクノロジーのメリットを制約なく提供しながら従業員のセキュリティ確保に努める IT チームにとって、これは悪夢のような状況とも言えます。そして今、私たちは新たな課題に直面しています。2020 年には、デジタル変革がどれだけ進行しているかに関係なく、多くの企業がリモートユーザーの劇的な増加に急いで対応せざるを得ませんでした。

セキュア Web ゲートウェイは、従業員を保護するための重要なコンポーネントですが、多くの企業は依然としてデータセンター内の物理機器を使用しています。こうしたハードウェアは、継続的な管理、保守、アップグレードを要するだけでなく、Web トラフィックの検査と制御に複雑なトラフィックバックホールを使用するため、最終的にはパフォーマンスが低下します。

分散した企業環境という新たな現実のもとでセキュリティを確保するためには、最新の合理的なアプローチが必要となります。その方法は、ハードウェア機器を排除することと、セキュア Web ゲートウェイ機能をクラウドに移行することです。

このバイヤーズガイドでは、クラウドベースのセキュア Web ゲートウェイの利点と、最新の Web ゲートウェイテクノロジーに求められる機能について説明します。

# テレワークの拡大が IT とセキュリティにもたらす新たな需要

過去 10 年の間に、テレワーカーは着実に増えてきました。COVID-19 の流行は、この傾向に拍車をかけたにすぎません。この流れはパンデミック終息後も続くと考えられます。Gartner 社の調査では、回答した CFO の 74% が、パンデミック終息後に、以前オンサイト勤務だった従業員の 5% 以上を恒久的にテレワークのポジションに移すつもりであることがわかりました。[1]

フィッシング、ランサムウェア、マルウェアなどの高度な標的型攻撃の数も急増しています。最近の調査では、回答者の 53% が、COVID-19 パンデミックが始まって以降、フィッシングを目にすることが多くなったと答えています。[2] 米国財務省も、最近出した勧告のなかで、サイバー攻撃者はビジネスの継続を左右するオンラインシステムを標的にしており、今回の COVID-19 パンデミック下でランサムウェアの支払い要求が増加していると述べています。[3]

これまで多くの企業は、セキュア Web ゲートウェイなどのセキュリティ機器をデータセンターに配置し、本社やブランチオフィスにいるオンサイトユーザーにも、テレワークのリモートユーザーにも、同じ方法でインターネットアクセスのセキュリティを確保していました。この方法で検査と制御を行うには、すべての Web トラフィックを中央にバックホールすることになります。

この方式のセキュア Web ゲートウェイは、ユーザーが開始した Web トラフィックから望ましくないマルウェアをフィルタリングし、ユーザーが悪性 Web サイトにアクセスするのを防ぎ、社内ポリシーや規制を遵守するために、エンタープライズによって使用されてきました。

このようなゲートウェイソリューションは元来、ほとんどの従業員が会社の管理下に置かれたデバイスを自分のデスクで使用する環境で設計され、展開されていました。しかし、テレワークユーザーやブランチオフィスのユーザーが増えるにつれて、SaaS アプリケーションにアクセスするためにパブリックインターネットへ出るトラフィックが増大しました。これに対応して十分なパフォーマンスを維持するために、中央のデータセンターに複数の重複するセキュア Web ゲートウェイが導入されていきます。こうした機器の購入や管理が複雑化し、多大なコストと時間を要するようになりました。

> **「データセンターに費やされた IT 予算の割合は、過去数年間で減少し、今では全体のわずか 17% になっています」**
>
> — Gartner、2019 IT Key Metrics Data

一方、すべてのリモートユーザーのトラフィックをバックホールしながら、セキュア Web ゲートウェイ機器をブランチサイトに追加する企業もありました。このような冗長アプローチは、機器の無秩序な拡大につながり、付随するコストも、展開や管理の手間も増大します。

さらに、多数のサイトで一貫したセキュリティポリシーを維持することは、ますます困難になります。仮想機器を導入して機器数を減らしても、余分なハードウェアを展開し管理しなければならない状況は解消されません。

3 つ目のアプローチとして、ハイブリッド構成を採用する企業もありました。これは、主要サイトでは引き続きオンプレミスのセキュア Web ゲートウェイを使用し、ブランチの Web トラフィックはクラウドベースのセキュア Web ゲートウェイに送信する方法です。この方法でも、やはりリモートサイトの従業員のトラフィックはバックホールされます。このアプローチでは、オンプレミスの機器に対する既存のハードウェア投資が無駄になることはありません。しかし、結局、異種システムを管理することになるため複雑さが増します。機器数と管理作業が増えて、純粋なクラウドアプローチよりもはるかにコストがかかるだけでなく、ローカルシステムとクラウドベースシステムの間で一貫したポリシーを維持することも困難です。

> **Gartner は、2025 年までに 80% のエンタープライズが従来のデータセンターを閉鎖すると予測しています。**[4]

さらに悪いことに、導入するソリューションが複雑化の一途をたどると同時に、サイバーセキュリティのリソースが不足する傾向にあります。(ISC)[2] の調査から、現在米国で必要とされるセキュリティワーカーの不足を埋めるためには、こうした人材を 62% 増やす必要があることが明らかとなっています。[5]

# なぜクラウドベースのセキュア Web ゲートウェイが必要なのか

今必要とされているのは、企業のクラウド戦略に対応し、効果的なテレワークを可能にする先進的な Web セキュリティアプローチです。クラウドベースのセキュア Web ゲートウェイは、インターネットに直接接続することで、複数の機器やバックホールの必要性を排除し、複雑さを軽減しながら、高度なセキュリティも提供します。

クラウドベースのセキュア Web ゲートウェイには、以下のようなメリットがあります。

**セキュリティの複雑さの軽減：**このようなセキュア Web ゲートウェイはクラウドのサービスであるため、ハードウェアや仮想機器を配置する必要がなくなり、これらの設定や管理、および 3 年ごとの交換やアップグレードも不要となります。

**パフォーマンスのボトルネックの最小化:**インターネットベースのセキュア Web ゲートウェイを使用すると、Web トラフィックの負荷や暗号化トラフィックが増大しても、機器を追加する必要がなくなります。必要に応じてサービスを追加すれば済むので、パフォーマンスへの影響を最小限に抑えることができます。

**トラフィックのバックホール／折り返しにかかるコストの削減：**クラウドベースのセキュア Web ゲートウェイは、インターネットへの直接接続を可能にすることで、トラフィックをバックホールすることなく Web トラフィックにセキュリティを適用します。そのため、Multiprotocol Label Switching のネットワークコストを削減できます

**セキュリティチームの効率の向上:**クラウドセキュア Web ゲートウェイは、ハードウェアやソフトウェアの継続的な保守が不要です。そのため、ただでさえ不足しているセキュリティ担当者の貴重な時間をその他の予防的なセキュリティ対策に使うことができます。

**一貫したセキュリティポリシー：**組織はポリシーを中央で管理しながら世界中に展開し、接続に使用するデバイスに関係なくすべてのユーザーにポリシーを適用できるようになります。地域によって適用するポリシーが異なっていても、同じ UI を使用してすべてのポリシーを管理できます。

# セキュア Web ゲートウェイの主な要件

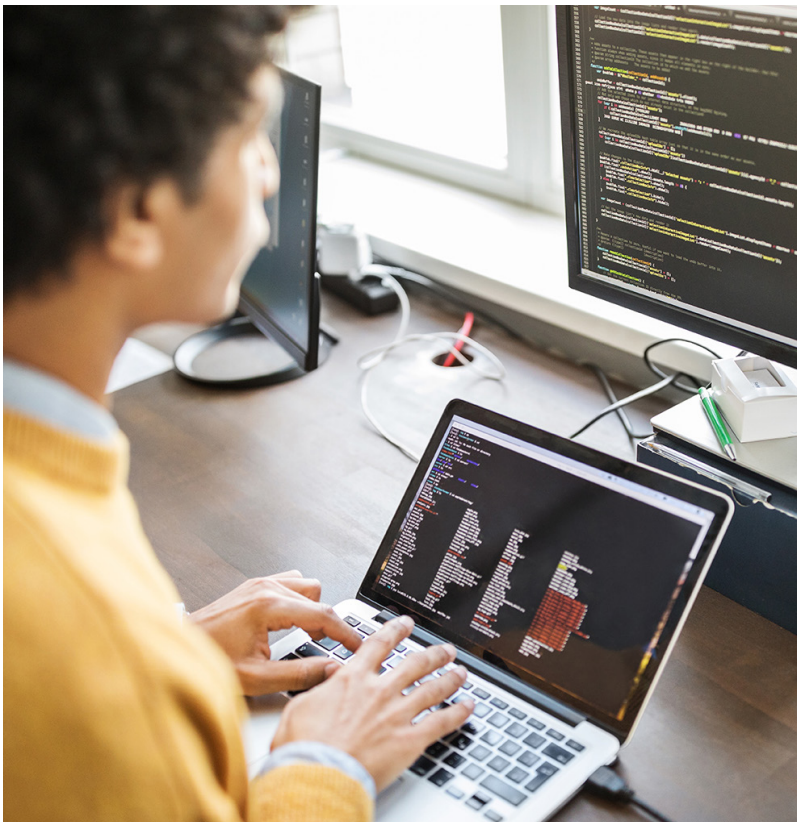
クラウドベースのセキュア Web ゲートウェイを選ぶ際に重要なのは、セキュリティを中心的な要件として認識することです。多くの場合、古いセキュア Web ゲートウェイには、今はもう存在しない問題を解決するための機能が含まれています。たとえば、帯域幅の制御機能は、帯域幅のコストが高かった時代に設計されたものです。また、勤務時間中に従業員が YouTube や Facebook を使用できないようにする機能もあります。今はこうした機能は不要になりました。帯域幅は十分にありますし、多くの従業員が自分のモバイルデバイスを使用するため、会社のデバイスで YouTube などのサービスを利用することについては、特に問題視されなくなりました。

現在、組織が必要としているのは、新しいセキュリティ問題に対応できるように設計されたセキュア Web ゲートウェイです。特に、多層防御戦略に基づき、複数のセキュリティ対策を使用して高度な防御を提供できるソリューションであることが重要です。そのためには、あらゆる角度からサイバーセキュリティに対抗し、冗長方式のセキュリティ対策を提供できなければなりません。このようにすれば、1 つの防御ラインが破られても、その亀裂から入り込まれないように別の防御層が攻撃を阻止します。こうした階層型のアプローチでは、マルウェア、ランサムウェア、フィッシングなどの脅威が早期に迅速にブロックされるので、ユーザーのデバイスが侵害されることはありません。

多層防御戦略に基づくセキュア Web ゲートウェイは、次の機能を提供します。

## すべての DNS 要求および URL 要求の評価

クラウドベースのセキュア Web ゲートウェイソリューションには、すべての URL 要求および DNS 要求をリアルタイムの脅威インテリジェンスと照合して評価し、悪性の要求をキルチェーンの初期



段階でブロックする機能が必要です。セキュア Web ゲートウェイによって発信接続が確立する前に脅威をブロックできれば、Web リソースを使用して、返されたコンテンツを開いたり検査したりする必要はありません。この効率的な手法により、膨大な計算を要するプロセスが回避され、ペイロード段階でセキュア Web ゲートウェイが分析しなければならないトラフィック量が軽減されます。結果、セキュア Web ゲートウェイ全体のパフォーマンスが向上します。

脅威インテリジェンスは、マルウェア、ランサムウェア、フィッシング、および低スループットの DNS ベースデータ窃盗に対する防御を提供できる必要があります。また、現在の問題に適した最新の防御を提供できる設計であること、誤検知率が低いことも必要です。

## 複数のペイロード分析手法

脅威は多様であり、1 つの検知手法やアプローチであらゆるタイプのマルウェアに対応するのは不可能です。したがって、セキュア Web ゲートウェイソリューションには、複数のマルウェア分析エンジンが搭載されている必要があります。また、これらのエンジンは、シグネチャ、シグネチャレス、機械学習、サンドボックスなど、さまざまな識別手法を使用して、インラインまたはオフラインで HTTP および HTTPS のペイロードをスキャンできなければなりません。こうした分析によって、実行可能ファイルやドキュメントファイルなどの悪性ファイルに対する包括的なゼロデイ防御が可能となります。

## ゼロデイフィッシング検知

テレワーカーは、COVID-19 の発生以降、フィッシング攻撃の増加に直面し続けています。攻撃者は、メール、ソーシャルメディア、インスタント・メッセージング・アプリや、オンラインファイルの共有およびコラボレーションチャネルを通じてフィッシング攻撃を開始し、認証情報を盗んで、エンタープライズネットワークに侵入します。さらにそこから、横方向に移動し、データや知的財産を見つけて流出させたり、ランサムウェアキャンペーンを仕掛けたりすることもできます。

ほとんどのセキュリティベンダーは、次の方法でフィッシングページへのアクセスを識別し、ブロックしています。

1. **あるドメインにヒットする異常なトラフィックを観察する**
2. **そのドメインを分析する**
3. **フィッシングドメインかどうかを判断する**
4. **そのドメインをブロックリストに追加する**
5. **ブロックリストの更新を顧客にプッシュする**

このプロセスは時間がかかる可能性があります。さらに悪いことに、今日のサイバー犯罪者はフィッシングキットを使用し、短寿命の攻撃を簡単に作成して開始するので、検知はさらにいっそう難しくなっています。フィッシングドメインや URL が見つかった時点で、攻撃は終了しているのです。実際、より巧妙で標的を絞り込んだフィッシング攻撃ほど、攻撃期間は短くなっています。

しかし、たとえキャンペーンがすぐに終了するとしても、高度なゼロデイフィッシング検知エンジンなら、それらを特定してブロックできます。このようなキットベースの攻撃の反復要素は、フィッシングページのコードで確認できます。この情報を使用すると、これらのページの「フィンガープリント」を特定することで、正確な識別が可能となります。

セキュア Web ゲートウェイソリューションには、要求された Web ページを分析し、以前に確認されたフィッシングページの「フィンガープリント」と比較できるゼロデイフィッシング検知エンジンが含まれていなければなりません。

## 暗号化トラフィックの検査

インターネットは元来、データ転送用チャネルとしては安全ではありません。そのため、攻撃者によるトラフィックの盗聴、偽造、改ざんを阻止するために Web トラフィックの暗号化が一般的となりました。Transport Layer Security（TLS）は、安全な Web ブラウジングを提供するための暗号化について定めた事実上の業界標準です。TLS は、クライアントブラウザーと Web サーバーなど、2 つのエンドポイント間にセキュアなトンネルを作成します。

> **インターネット上の暗号化された Web トラフィックの割合は、2014 年には約 50% でしたが、現在は 80% から 90% となり、着実に増加してきました。世界のトップ 100 サイトのほとんど（96%）がデフォルトで HTTPS に設定されています。**
>
> — Google Transparency Report、2020 年

ただし、すべての HTTPS トラフィックが安全というわけではありません。攻撃者やマルウェア作成者も、暗号化によってアクティビティを隠し、ユーザーが（ランサムウェアを介して）ファイルにアクセスするのを防ぎ、悪性のネットワーク通信を保護しています。最近の調査から、インターネット接続を確立したマルウェアの約 4 分の 1 が通信に TLS を使用していたことが判明しました。[6]

HTTPS Web トラフィックを事前に検査し、制御するためには、プロキシサーバー（信頼できる中間サーバー）を使用してセキュアトンネル内を観察し、暗号化されたトラフィックを調べる必要があります。プロキシサーバーは、HTTPS トラフィックをプレーンテキストに復号化し、分析してから、そのトラフィックを再び暗号化したうえで、中間者（MITM）と呼ばれる手法で別のセキュアな接続を確立する必要があります。MITM は要求された URL を検査して、それらが安全か悪性かを判断します。さらに TLS 暗号化トラフィックを可視化してエンタープライズを脅威から守るとともに、オリジン Web サイトへのトラフィックの機密性と整合性を維持します。

MITM の検査には、かなりの処理能力が必要であるため、遅延によって Web ブラウジングが遅くなる可能性があります。したがって、セキュア Web ゲートウェイは、アプリケーションのパフォーマンスを高めるサービスを提供できなければなりません。世界各地のユーザーやデータセンターの近くに配置されたサーバーとインテリジェントソフトウェアによるグローバル分散ネットワークを活用し、アプリケーションのパフォーマンスと可用性を改善する Web 最適化機能が必要となります。

また、適切に機能せず迂回が必要なドメインと URL のリストを、クラウドセキュア Web ゲートウェイのベンダーが一元的に管理し、維持しているかどうかも MITM は確認しなければなりません。さらに、クラウドセキュア Web ゲートウェイには、金融サービスやヘルスケアなど、機密性の高い Web コンテンツの MITM 検査を回避できる機能も必要です。

## データ損失防止機能の統合

個人を特定できる情報（PII）やその他のビジネス上の機密データの損失を積極的に予防することは、経済的損失や評判の失墜を防ぐためにも重要です。クラウドセキュア Web ゲートウェイには、設定が簡単で迅速に展開できるデータ損失防止機能が統合されていなければなりません。ディクショナリが頻繁に更新され、PII、PCI DSS、HIPAA などのデータプライバシーおよび保護規制に対応していることや、カスタムディクショナリを簡単に作成できることも必要です。

## シャドー IT の識別と管理

ユーザーは、セキュリティチームに気づかれずに、自分の手で膨大な数のアプリケーションを会社の管理下に置かれたデバイスにダウンロードし、インストールして使用できます。しかし、未承認のアプリケーションを使用すると、その組織のアタックサーフェスが大きく拡大し、リスクプロファイルが増す可能性があります。

> **平均的な企業では、1,295 を超えるアプリとクラウドサービスを使用しています。これらの 95% 以上が管理されず、IT 管理者権限もありません。**
>
> — Cybersecurity Insiders、Cloud Security Report、2019 年

クラウドセキュア Web ゲートウェイには、使用されているアプリケーションを特定する機能や、特定のアプリケーションをインストールしたユーザーの数を検出する機能、重大なセキュリティリスクをもたらす可能性のあるアプリケーションについて注意を喚起する機能が必要です。また、このようなアプリケーションを特定するだけでなく、そのアプリケーション全体のブロックや、そのアプリケーションの特定の動作のブロック（アップロードは許可するがダウンロードは許可しないなど）ができることも必要です。

## 場所を問わずあらゆるデバイスを保護する機能

この 10 年でワークスタイルの柔軟性は大きく拡大してきました。ユーザーは、どこにいても、どのようなデバイスでも仕事ができます。また、パンデミックによる在宅勤務の増加に伴い、エンタープライズのエンドユーザーコンピューティングの 59% がモバイルデバイスに移行し、PC やノートパソコンの代わりとして、またはこれらを補完するために使用されています。この変化は、従業員がオフィス勤務に戻っても継続すると予測されています。[7]

モバイルデバイスへの移行と Wi-Fi ネットワークの利用拡大は、あらゆる組織のセキュリティ体制に亀裂をもたらす可能性があります。デバイスのパフォーマンスを低下させることなく、統一されたユニバーサルレベルのセキュリティを適用できることが必要です。

クラウドセキュア Web ゲートウェイには、ユーザーが使用するあらゆるネットワークのあらゆるデバイス（iOS、Android OS、Chrome OS）に対する標的型脅威（マルウェア、ランサムウェア、フィッシング、DNS データ窃盗、ゼロデイ攻撃など）を事前に特定、ブロック、緩和する機能が必要です。ゲートウェイソリューションは、最適なデバイスパフォーマンスを維持しながら、ユビキタスな制御と合理化された管理をグローバルに提供できなければなりません。

## すべてのエンタープライズアプリケーションへのセキュアなアクセス

クラウドセキュア Web ゲートウェイは、パブリックインターネットにアクセスするときにユーザーとデバイスをマルウェアから保護します。しかし、エンタープライズにとっては、これはセキュリティパズルの 1 つのピースにすぎません。

ビジネス全体に総合的なセキュリティアプローチを適用するためには、会社が所有・管理しているアプリケーションが社内のデータセンターにあろうと IaaS 環境にあろうと、これらを不正行為から保護する必要があります。従来のネットワークセキュリティツールは、ネットワーク境界を保護します。しかし、ユーザーの認証情報を盗んだり、ユーザーのデバイスにマルウェアをインストールするなどの方法によって境界が破られると、攻撃者はネットワーク内を自由に移動できます。

組織には、ゼロトラスト・ネットワーク・アクセス（ZTNA）テクノロジーによってコーポレートアプリケーションを保護するようなクラウドセキュア Web ゲートウェイが必要です。ZTNA は、ゼロトラスト・セキュリティに不可欠なコンポーネントであり、ユーザーのアイデンティティに基づいて特定のアプリケーションのみ（ネットワーク全体またはセグメント全体ではなく）に対するアクセス権をユーザーに付与します。このソリューションは、アイデンティティおよびアクセス管理、多要素認証（MFA）、およびシングル・サインオン・テクノロジーとの統合を通じて、ユーザーのアイデンティティを保護します。ZTNA ツールを使用することで、デバイスの安全な管理や、複合的なワイド・エリア・ネットワークまたは仮想プライベートネットワークの接続維持に伴う複雑さを回避できます。適切に認証されたユーザーがアクセスできるのは、必要なアプリケーションとデータのみであるため、アプリケーションのアタックサーフェスをゼロにするとともに、ラテラルムーブメ

**エンタープライズフィッシング攻撃が増加している**

**観察された攻撃件数 – 2020 年 3 月～10 月**

**64%**

**エンタープライズを標的とした攻撃**

**の増加**

**17%**

**消費者を標的とした攻撃**

**の増加**

出典：Akamai Enterprise Threat Protector セキュア Web ゲートウェイ

ント（横方向の移動）リスクを最小限に抑えることができます。クラウドセキュア Web ゲートウェイを評価する際には、そのベンダーが提供する ZTNA サービスの機能を考慮する必要があります。そのサービスでは、最新の Web アプリケーションと従来の非 Web アプリケーションへのアクセスが提供されますか？そのサービスでは、組織の既存のアイデンティティ・プロバイダー・サービスとの統合が可能ですか？ MFA に対応していますか？

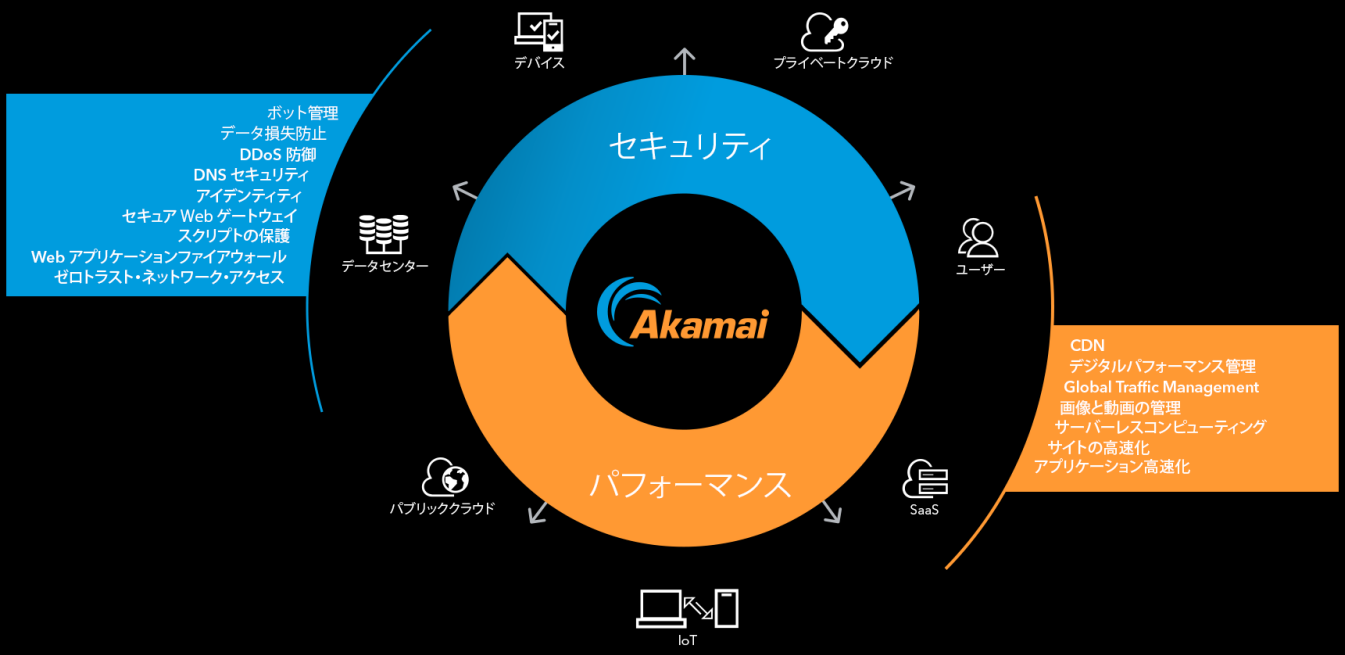
セキュア Web ゲートウェイには、ZTNA サービスと統合、連係して、侵害されたことがわかっているデバイスからは、どのコーポレートアプリケーションにもアクセスできないようにする機能が必要です。また、セキュア Web ゲートウェイのログは、他の脅威信号の補強として、デバイスのセキュリティポスチャをより正確に把握するために役立ちます。たとえば、デバイスがコマンドサーバーと制御サーバーを呼び出している場合、それを信号として使用し、そのデバイスが修復されるまでアプリケーションアクセスを制限するといった機能が必要です。

セキュア Web ゲートウェイと ZTNA 機能を追加することで、組織は、Secure Access Service Edge（SASE）フレームワークの導入へと一歩踏み出すことになります。SASE は、組織のセキュリティ対策の中心を、今日の高度に分散した作業環境やビジネス環境では機能しなくなったデータセンターやハードウェア機器を中心としたセキュリティアーキテクチャから切り離します。その代わりに、ユーザーやデバイスのアイデンティティに応じたポリシーベースのアクセスを提供します。また、SASE は、Web アプリーションファイアウォール、API セキュリティ、ボット管理、Web にアクセスするアプリケーションへの分散型サービス妨害（DoS）防御など、多様なセキュリティ制御も提供します。

> **ZTNA は、アプリケーションの柔軟性、アジリティ、スケーラビリティを改善します。デジタルビジネスは、社内アプリケーションを直接インターネットにさらさずにビジネスを推進し、攻撃のリスクを減らすことができます。**
>
> Gartner 社、Market Guide for Zero Trust Network Access、Steve Riley、Neil MacDonald、Lawrence Orans、2020 年 6 月 8 日

しかも、セキュリティ制御は、ユーザーから 1 インターネットホップしか離れていない SASE プラットフォームで提供されるので、ユーザー、デバイス、クラウドサービスの場所に関係なく、低レイテンシーのアクセスが可能です。

## Akamai のクラウド配信型 SASE



## パフォーマンスの最適化

セキュリティは最優先事項ですが、そのためにパフォーマンスを低下させて、ユーザー体験を損なうわけにはいきません。クラウドベースのセキュア Web ゲートウェイは、セキュリティに対する多層防御アプローチを提供するだけでなく、レイテンシーを発生させずに、こうしたサービスを提供できなくてはなりません。

レイテンシーを回避するためには、あらゆるユーザーが近くで接続できるように、クラウドセキュア Web ゲートウェイをグローバルに展開する必要があります。結局、バックホールのタイプを別の方式に替えても意味はないのです。

クラウドプラットフォームは、ピーク時にもエンドユーザー体験に影響しないように、即座に拡張できなければなりません。特に HTTPS トラフィックの検査においては、キャパシティが重要となります。HTTPS トラフィックは急激に増加しており、最終的には Web トラフィックの 100% 近くが HTTPS になると見込まれます。今ではマルウェアでさえ、ほとんどが HTTPS で配信されています。したがって、エンドユーザーへの影響を最小限に抑えながら暗号化トラフィックを検査する機能は非常に重要です。また、プラットフォームが 100% の可用性を保証する SLA を提供していることも必要です。

> **今では組織全体の 81% がクラウドサービスに移行し、そのうち半数以上を Office 365 のユーザーが占めています。[8]**

**Office 365 の統合：**Microsoft Office 365（O365）は不可欠な生産性スイートとして多くの組織に使用されています。そのため、このサービスのセキュリティとパフォーマンスを高いレベルに保つことは大変重要です。ユーザーが TLS MITM 検査を実行するフォワードプロキシ経由でアプリケーションにアクセスすると、他の多くの一般的な SaaS アプリケーションと同様、O365 のパフォーマンスも低下します。これは、クラウドセキュア Web ゲートウェイを展開する際の課題の 1 つとなっています。

O365 のパフォーマンスへの影響を避けるためには、クラウドセキュア Web ゲートウェイが、以下の条件を満たすグローバル・エッジ・プラットフォームを介して提供されることが重要です。

- リクエストのソース IP を使用して、地理的に最も近い Microsoft O365 データセンターにリクエストを送信します。これは、社内の DNS リゾルバーに最も近いデータセンターにリクエストを転送するバックホール方式の DNS ソリューションとは異なります。たとえば、シンガポールから O365 にアクセスするユーザーがニューヨークの O365 サーバーにルーティングされた場合、ユーザー体験は極度に悪化します。

- セキュア Web ゲートウェイサーバーを Microsoft O365 データセンターの近くに配置します。これらのサーバーとデータセンターが相互接続されていれば理想的です。

- Microsoft が発行および更新する O365 ドメインと IP アドレスのリストを使用して、ワンクリックで O365 トラフィックの最適化を設定する機能を提供します。これらのドメインへの要求は、Microsoft の推奨に従い、O365 サーバーに直接送信する必要があります。これにより、Microsoft が新しいドメインまたは IP アドレスを追加する際にファイアウォールやその他のセキュリティ製品を手動で更新する必要がなくなり、時間と労力を節約できます。

# セキュリティをエッジに移動

テレワーカーが急増したことで、サイバー攻撃に対してますます脆弱な状況となっています。その結果、サイバー攻撃は頻度が増し、深刻化しています。最も効果的なクラウドベースセキュア Web ゲートウェイは、実証済みの多層防御機能を提供し、最新のセキュリティ要件を満たすことに特化したソリューションです。このようなソリューションは、ゼロトラストや SASE などの最新のエンタープライズ・セキュリティ・モデルにも対応できるので、場所を問わずすべてのユーザーがインターネットに安全にアクセスできます。

包括的なクラウドセキュア Web ゲートウェイに求められる機能は、すべての DNS および URL 要求の評価、複数のペイロード分析手法の提供、ゼロデイフィッシングへの対処、暗号化トラフィックの検査、データ損失防止の統合、シャドー IT の特定と管理、場所を問わずあらゆるデバイスを保護すること、そして、これらすべてを高いパフォーマンスを維持し、エンタープライズ・アプリケーション・セキュリティ・テクノロジーと統合しながら実現できることです。このようなソリューションを使用すれば、セキュリティの複雑さを軽減し、コストのかかるバックホールを排除し、セキュリティチームの効率を高めて、一貫したセキュリティポリシーを適用できます。

**Akamai のクラウドセキュア Web ゲートウェイであるセキュア・インターネット・アクセスの詳細と無料トライアルについて、akamai.com をご覧ください。**


1. https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2
2. https://www.helpnetsecurity.com/2020/09/02/phishing-attacks-pandemic/
3. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
4. https://blogs.gartner.com/david_cappuccio/2018/07/26/the-data-center-is-dead/
5. https://www.brinknews.com/a-global-shortage-of-cybersecurity-professionals-leaves-businesses-at-risk/
6. https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/
7. https://www.mobolize.com/2020/10/29/mobolize-announces-technology-partnership-with-akamai-to-enable-security-on-mobile-devices/
8. https://blog.goptg.com/microsoft-office-365-statistics#:~:text=According%20to%20Bitglass%2C%20usage%20of,the%20shift%20to%20cloud%20services



Akamai はオンラインライフのカとなり、守っています。世界中のトップ企業が Akamai を選び、安全なデジタル体験を構築して提供することで、毎日、いつでもどこでも、世界中の人々の人生をより豊かにしています。クラウドからエッジまで、世界で最も分散されたコンピューティングプラットフォームにより、Akamai は、アプリケーションの開発や実行を容易にし、同時に、体験をユーザーに近づけ、脅威を遠ざけます。Akamai のセキュリティ、コンピューティング、デリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。公開日：2022 年 6 月。