CLOUDFLARE

ホワイトペーパー

SaaSアプリケーションの保護方法の簡素化

Zero Trustアプローチで
ユーザーとデータを
保護する方法

本文

はじめに

現在、Software as a Service（SaaS）アプリケーションを使用した分散型環境によって、企業は世界中の社員や請負業者をより柔軟にサポートすることができるようになりました。現在、最も代表的なSaaSアプリケーション・スイートには、コミュニケーション（メール配信、チャット・プラットフォーム）、生産性（文書、スプレッドシート）、コラボレーション（オンライン・ストレージ）などがあります。ガートナー社は、2025年までに85%の企業がクラウドファーストの原則でビジネスを展開すると予測しており、SaaSをアクセス管理の展開手段として推奨しています[1]。

しかし、SaaSアプリケーションによって企業はより機敏性を維持できるようになる一方で、クラウドへの移行にはセキュリティとパフォーマンスのリスクが伴います。特に、互いに独立して動作するように設計されたポイントソリューションを複数使い分けている企業にとってこのリスクは顕著に現れます。このようなアプリケーションを数百とはいかないまでも、数十も実装し管理しなければならならず、セキュリティ、ネットワーク、ITチームは時間に追われ、組織全体の可視化に苦労し、また、本来連携するように設計されていないサービスによって生じるセキュリティや接続性のギャップとの格闘を強いられます。

その結果、多くの組織がSaaS環境全体でセキュリティ製品を一本化するためのより良い方法（効率性を向上させ、管理と導入の複雑さを軽減し、統合的なサポートが受けられる）を模索するようになりました

ガートナー社は、2025年までに企業の80%が、セキュリティサービスエッジ（SSE）プラットフォームから、ウェブ、クラウドサービス、プライベートアプリケーションへのアクセスを、1つにまとめた単一のベンダーソリューションへ移行するだろうと予測しています[2]。

SaaSセキュリティの簡素化には、いくつかの重要な考慮事項があります。現在、従業員のコミュニケーション手段や業務を遂行するための手段には、新たなリスクに先手を打ち、SaaSアプリケーションに起因するインシデントを減らし、セキュリティチームが組織に降りかかる脅威を容易に監視・防止できるように設計された、セキュリティに対するシンプルでスケーラブルなアプローチが必要です。

クラウドアクセスセキュリティブローカー（CASB）とクラウドメールセキュリティ（CES）の機能を統合したZero Trustプラットフォームが提供する、データ損失、フィッシング、ランサムウェア、シャドーIT、組織全体にわたるラテラルムーブメントなどを阻止する最も簡単な方法について紹介します。

[1] ガートナー、「予測分析：世界規模での情報セキュリティおよびリスクマネジメント。」アナリスト：Shailendra Upadhyay、Mark Driver、Christian Canales、Ruggero Contu、Lawrence Pingree、Elizabeth Kim、John A。Wheeler、Nat Smith、Rahul Yadav、Swati Rakheja、Dave Messett、Mark Wah、Shawn Eftink。2021年8月12日、ガートナー[2]。ガートナー、「2022年予測：これからは統合セキュリティプラットフォームの時代。」アナリスト：Charlie Winckless、Joerg Fritsch、Peter Firstbrook、Neil MacDonald、Brian Lowans。2021年12月1日。ガートナー。

CASBの進化

包括的なSaaSセキュリティには、セキュリティチームがSaaSの全体像を把握し、容易に脅威の監視と緩和ができ、機密データやシステムに対してセキュリティで保護されたアクセスを実現するなどの、いくつかの重要な技術が必要になります。SaaSのセキュリティ戦略において最も重要なコンポーネントの1つが、クラウド・アクセス・セキュリティ・ブローカー（CASB）であり、これは組織のクラウドにホスティングされたサービスとアプリケーションに対するデータセキュリティ制御と可視性を提供します。

SaaSセキュリティ入門：CASB

CASBが採用されたSaaSを利用することで、ITおよびセキュリティチームは、単一のダッシュボードからすべてのデータ設定とユーザーアクティビティを確認することができます。その機能はプロバイダーによって異なりますが、通常、次のような属性があります[1]：

- **データ保護：**CASBは、機密データを保護し、企業管理のシステムからデータが流出することを防ぎます。
- **アクセス制御：**CASB は、企業管理のアプリケーション内で、ユーザーが閲覧および実行できる内容を制御するのに役立ちます。また、ユーザーが本人であることを確認するための本人確認機能を提供することもあります。
- **シャドーITの検出：**CASBは、従業員が業務目的で使用している未承認のシステムやサービス（一般に「シャドーIT」と呼ばれる）を特定するのにも役立ちます。これらのシステムをカタログ化することで、これまで知られていなかったセキュリティリスクを検出し、軽減することができます。
- **脅威対策：**CASBは、マルウェア対策による検知、サンドボックス、パケットインスペクションなどの技術により、データ漏えいや外部からの攻撃をブロックすることができます。
- **動態管理：**CASBは、ユーザーの行動分析への洞察とアプリケーションの動態の制御をセキュリティチームに提供し、SaaS環境全体の動向を簡単に調査して脅威を追跡することを可能にします。
- **コンプライアンス：**CASBは、不適切な設定を特定することで組織が規制要件（SOC 2、HIPAA、GDPRなど）を満たすことに役立ちます。これによってコンプライアンス違反に伴う罰則や罰金を回避します。

[3]このリストはCASBの提供内容として含まれる可能性のある機能を網羅したものではありません。

現代におけるCASBの課題を理解する

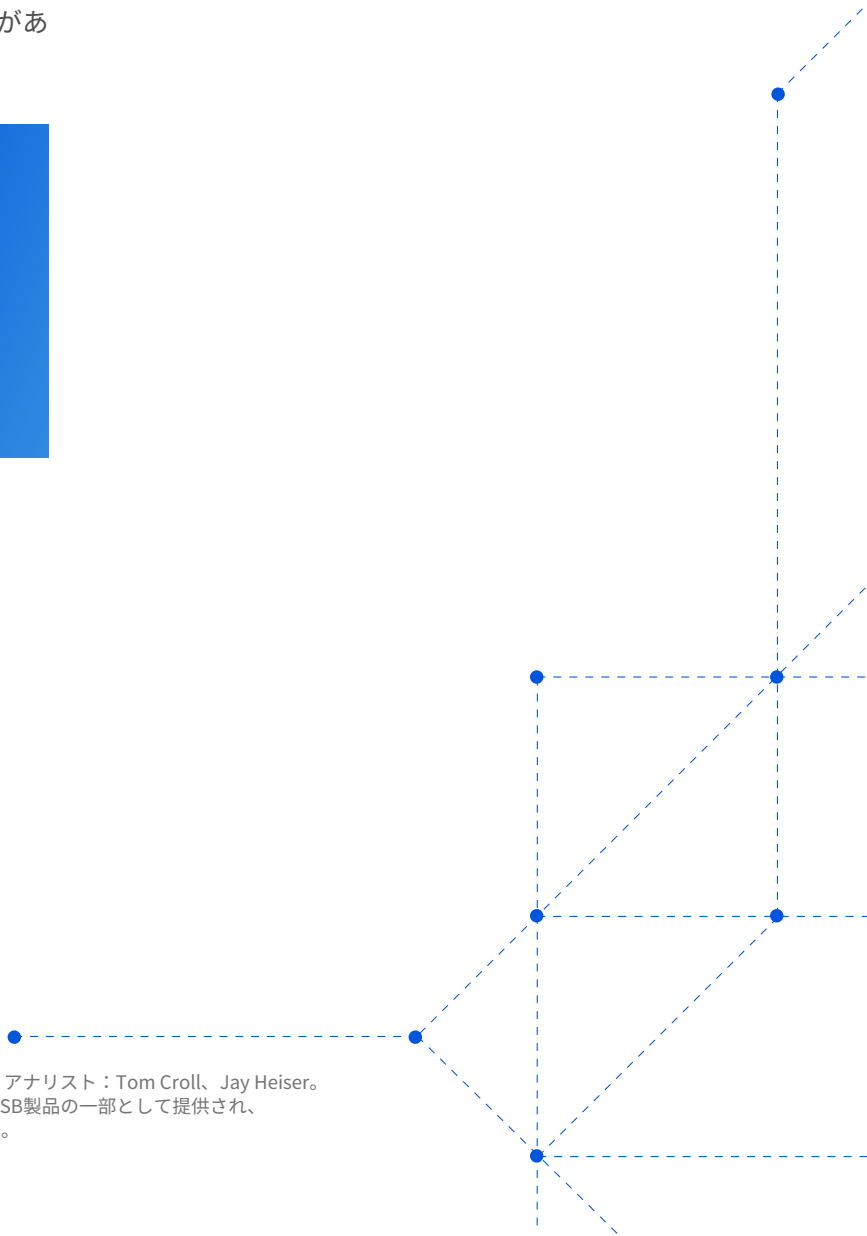
SaaSの導入が進むにつれ、組織が保護すべき攻撃対象領域も増えていきます。貴重なデータが入った単一のデータベースではなく、そのデータは企業で使用するためにサンドボックス化されているかどうかに関わらず、サードパーティが管理するアプリケーション（Dropbox、Google Driveなど）に分散されています。

CASBはSaaSアプリケーション内の企業データとユーザーの保護に役立ちますが、それでも脅威を完璧に捕らえるものではありません。SaaSアプリケーションではより多くの貴重なデータが処理されるため、これらのアプリケーションは攻撃者がデータ漏えいやその他の脅威を仕掛けるためターゲットとされることが多くなっています。また、単純な設定ミスやユーザーのミスでも、このような攻撃に対して無防備になってしまう可能性があります。

ガートナー社は、2025年までにクラウド上で発生する侵害の99%以上は、ユーザーによる予防可能な設定ミスや間違いに起因するものであると予測しています[4]。

ユーザーの設定ミスや最新のSaaS攻撃を予測して対処することに関して、多くのCASBはまだ不十分です。この問題に対処するため、一部のベンダーは、制御プレーンにおいて設定とコンプライアンス観点のエラーを追跡するように設計されたクラウドまたはSaaSのセキュリティ動態管理（CSPMまたはSSPM[5]）サービスの提供を開始しています。しかし、このようなサービスはすべてが網羅された状態で提供されているわけではなく、多くの組織では必要な検出と修正の機能がないままになっています。

さらに、一部のCASBはデータ漏えいを事前に特定できないため、セキュリティチームが攻撃者に追いつくための修復コストやデータ損失が増大します。



[4]ガートナー、「クラウド・セキュリティのハイプ・サイクル：2021年」。アナリスト：Tom Croll、Jay Heiser。2021年7月27日。ガートナー[5]。これらのサービスや機能は、多くの場合CASB製品の一部として提供され、アプリケーションのインライン保護とAPIベースの保護の両方を提供します。

CASBの実装と統合に関する問題点

SaaSベンダーがビルトインのセキュリティ機能を強化する一方で、「連携」と「可視化」という2つの大きなハードルが残っています。これらのベンダーは、データへのアクセスと利用を容易にしますが、管理しやすくするために行うセキュリティ機能の統合は、組織に未だに負担をかけるものになっています。
複数のポイントソリューションを採用している組織では、これらのソリューションが相互に連携できるように設計されていなかったり、可視性のレベルが異なったりすると、異なるプラットフォーム間で脅威を追跡することはより困難なものになります。

このことは、アプリケーション環境を複雑にします。攻撃者は検出されずに攻撃を実行するためのセキュリティプラットフォーム間にあるギャップを特定するだけで良く、そのため基本的な攻撃でさえも予測・軽減することが難しくなります。CASBを利用することで、組織は一か所からセキュリティ製品にアクセスすることができ、セキュリティ・スタック全体の可視性と軽減する能力を向上させることができます。

それでも、CASBは大きなSaaSのセキュリティ戦略の一部でしかありません。SaaS全体をカバーするためには、不必要に複雑化したり、セキュリティチームに各ツールの手動での設定・保守を強いることなく、CASBの機能を他のZero Trustテクノロジーと融合させる必要があります。大規模なSaaSの管理を手動のプロセスで成功させることはできません。SaaSの管理プラットフォームとCASBツールを補完し、チームの疲弊やユーザーの設定ミスやエラーのリスクを排除し、組織が幅広い脅威を効果的に軽減できるようにするためには、自動化が必要です。

メールセキュリティの進化

多くのSaaSサービスと同様に、メールによるコミュニケーションは、あらゆる規模の組織にとって不可欠なビジネスアプリケーションとして発展してきました。クラウドやリモートワークへの移行に伴い、Microsoft 365やGoogle Workspaceなどのクラウドメールソリューションへ移行する組織が増えており、ガートナー社の調べでは、利用する組織は世界中の70%にも及びます[6]。

その結果、メールは現在最も広く採用されているSaaSアプリケーションであり、フィッシング、マルウェア、スプーフィング、ビジネスメール詐欺（BEC）などの最新の脅威を引き寄せる、最大の攻撃対象領域の一つになっています。

しかし、攻撃者が無防備な従業員に対して手口をより巧妙化させ続ける中、メール攻撃からの保護はセキュリティチームにとってうんざりするような負担のかかる作業となります。これらの脅威からユーザとデータを保護するために、セキュリティリーダーは、SaaSセキュリティプラットフォームへのメールの統合を、より視覚的かつより強固で簡素な保護を提供する方法で検討する必要があります。

SaaSセキュリティ入門：メールセキュリティ

現代のメールセキュリティには、悪意のある攻撃や不正アクセスからメールアカウントとコンテンツを保護するための一連のツール、プロセス、技術が包含されています。メールのセキュリティ技術として代表的なものには、以下のようなものがあります。

- **セキュアメールゲートウェイ（SEG）：**SEGはSMTPトラフィックを処理およびフィルタリングします。また、メール転送エージェントを指すようにMXレコードを変更する必要があります。
- **クラウドメールセキュリティ（CES）：**CESは、MXレコードを変更することなく、（クラウドメールプロバイダーへのAPIアクセスを介して）メールの内容を分析します。（注：ガートナー社では、このカテゴリを「ICES」または「統合されたCES」と呼んでいます）。
- **ドメインベースのメッセージ認証・報告・適合（DMARC）：**DMARCでは、ドメインの送信者ポリシーフレームワーク（SPF）とドメインキー認識メール（DKIM）レコードをチェックすることでメールを認証します。このシステムでは、SPFまたはDKIMのチェックに失敗したメールは、スパムとしてマークされるか、意図した受信者に到達しないようにブロックされます。
- **メールデータ保護（EDP）：**EDPソリューションでは、暗号化することで、不慮のデータ損失やメールコンテンツへの不正アクセスを防止します。

[6]ガートナー社、「マーケットガイド（Eメールセキュリティ）。」アナリスト：Mark Harris、Peter Firstbrook、Ravisha Chugh、Mario de Boer。2021年10月7日。ガートナー社。

現代におけるメールセキュリティの課題を理解する

当初、メールはオンプレミスのソフトウェアプラットフォームで配信されていましたが、クラウドネイティブの配信システムへの移行が進んでいます。多くの組織では、ユーザーがより効率的に作業やコラボレーションを行うことができるMicrosoft 365やGoogle Workspaceなどの機能豊富なプロダクティビティスイートへと切り替えています。

電子メールは長い間使われてきたため、ライトユーザーでも、不審なメールや悪意のあるリンクなどの電子メールを介して遭遇する可能性のあるより一般的な脅威については、認識があると思います。その結果、攻撃者は、正当なメッセージと悪意のあるメッセージをより見分けづらくするための戦略を進化させてきました。多くの場合、これらの複合型の脅威は、より正当なものであるように見せるように複数の通信チャネル（例えば、ビッシング、スミッシングなど）を横断して、ユーザーを騙して機密情報を開示させようとします。

メールの使用が増加するにつれ、組織はより多くの侵害の危険にさらされることになります。攻撃者が一旦誰かのメールアカウントへのアクセス権を取得すると、組織の内部を横方向に移動し、機密データの侵害や盗難などの行為が簡単にできるようになります。また、クラウドメールプロバイダーは、スパム、マルウェア、フィッシングなどの一般的な脅威を軽減するためのビルトインの限られたセキュリティ機能を提供していますが、侵害された内部送信者からの、受信トレイから受信トレイへと横方向に移動する攻撃には脆弱であることがよく知られています。

これらの脅威に対抗するため、メールセキュリティソリューションも進化を続けています。クラウドネイティブメールプラットフォームは、一般的なスパムやマルウェアの攻撃に対処できる基本レベルのビルトインのセキュリティ機能を備えています。

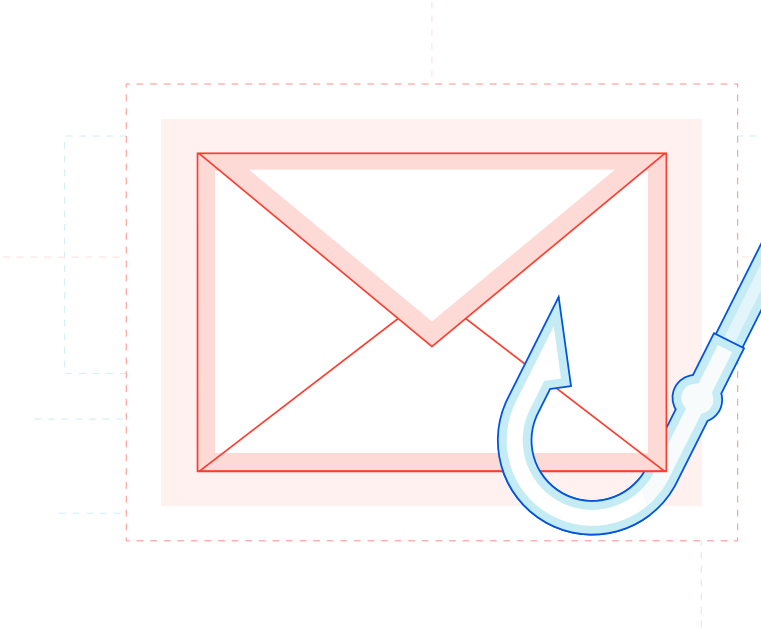
ガートナー社は、2023年までに全組織の少なくとも40%が、SEGのような個別のツールを採用するのではなく、このビルトイン型の保護対策に傾注すると予測しています[7]。

多くの組織は、SEGを使用せずに、巧妙なフィッシング攻撃やBEC攻撃を阻止し、APIを介してクラウドメール環境と緊密に統合できるセキュリティ製品を探すことで、メールセキュリティスタックを簡素化することを選択しています。ガートナー社は、2023年までにフィッシング対策ソリューションの20%が、メールプラットフォームとのAPI統合によって提供されると予測しています[8]。

[7]ガートナー社、「マーケットガイド（Eメールセキュリティ）。」アナリスト：Mark Harris、Peter Firstbrook、Ravisha Chugh、Mario de Boer。2021年10月7日。ガートナー社。[8]ガートナー社、「マーケットガイド（Eメールセキュリティ）。」

メールセキュリティの実装と統合に関する問題点

これらのビルトイン型の機能は、組織にある程度の安心感を与えますが、現代のメールの脅威に対抗するには十分とは言えません。スピアフィッシングやBECなど、あらゆる種類の攻撃には、電子メールプロバイダーが提供していない専用のセキュリティプラットフォームが必要です。また、従来のメールセキュリティソリューションは、拡張性、クラウドネイティブの課題への対応、高度な標的型攻撃への対処に対応できるようには設計されていません。



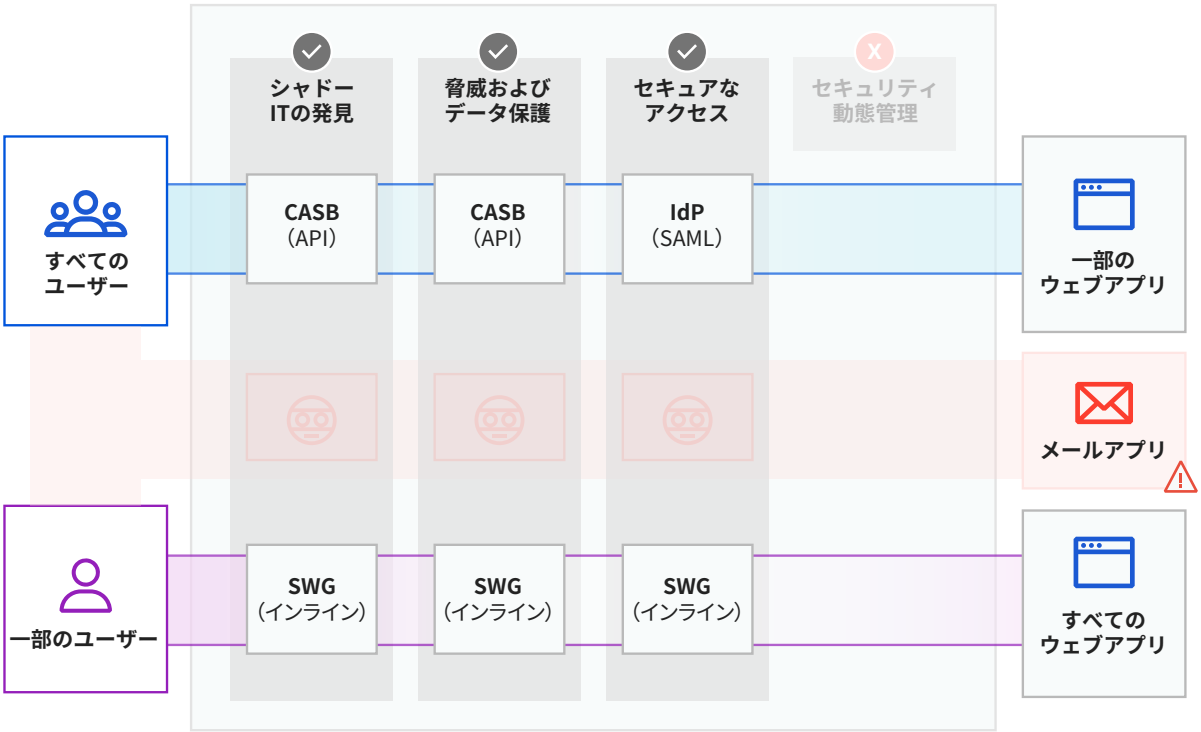
セキュリティチームが最新の脅威を捉えるように設計されたメールセキュリティツールを選定した場合でも、設定要件が複雑であったり、導入プロセスに時間がかかったり、ポリシーのメンテナンスが面倒であるなど、さらなる問題に直面することがあります。例えば、あらゆる種類の攻撃を阻止するために、増え続けるポリシーのリストを維持することは現実的ではなく、拡張性もないことから、メール攻撃に対してSEG製品を展開することは難しいという風評があります。巧妙化された攻撃を検知するためには、クラウドネイティブサービスのみが対応できる大規模なアルゴリズムを使用する必要があります。

企業のメールシステムをこうした攻撃から守るには、セキュリティチームに過度の負担を強いたり、従来のハードウェア製品を階層化したり、悪意のあるメッセージをすべて捕捉することを従業員頼みにするのではなく、クラウドネイティブのメールセキュリティ機能が一本化された、メールベースのコミュニケーションに対する暗黙の信頼を減らすZero Trustのアプローチが必要になります。

SaaSセキュリティのためのより良いアプローチ

SaaSアプリケーションは、コミュニケーションプラットフォームからメール配信システムまで、現在のビジネス運営のかなりの部分を占めています。しかし、複雑化する脅威からこれらのアプリケーションを保護することは、多くの場合、互いにネイティブに連携するように設計されていない、または組織のSaaS環境全体を可視化することができない複数のツールを使いこなさなければならないため、セキュリティチームにとって悪夢のようなものとなります。

従来のSaaSセキュリティ

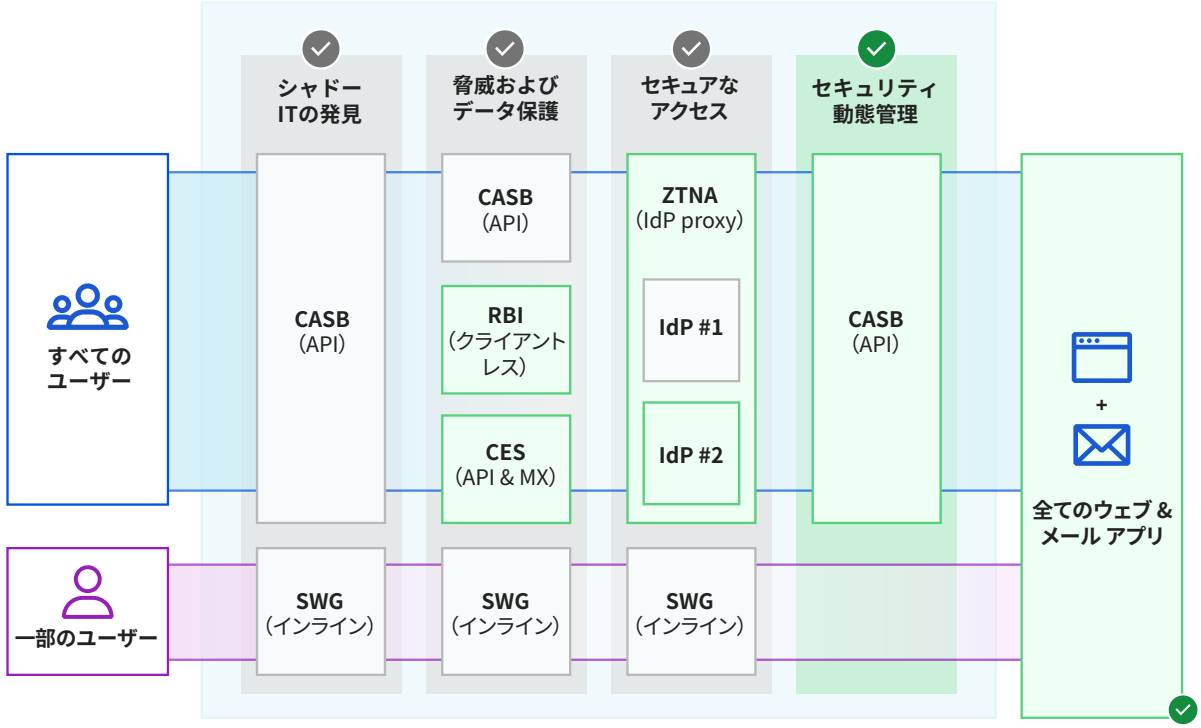


SWG = セキュア・ウェブ・ゲートウェイ | CASB = クラウド・アクセス・セキュリティ・ブローカー | IdP = ID プロバイダー

ベンダーがより強固なSaaSセキュリティツールを開発するにつれ、ITおよびセキュリティチームには、これらのクラス最高のソリューションを組み合わせて、アプリケーションとデータのセキュリティを確保するという任務が発生します。これには、多くの場合、導入と管理にかなりの時間と社内リソースが必要でした。また、ポイントソリューションが個々のレベルの脅威に対処することはできる一方で、マルチベンダー対応や組織全体の可視性を提供する包括的なプラットフォームは存在しませんでした。

また、従来のSaaSセキュリティ対策では、保護対象をメールプラットフォームにまで広げることができない場合が多く、ビジネスに不可欠なワークフローを複製されたり、信頼できるパートナーやユーザーになりすまし、既存の電子メール分類システムやビルトイン型の制御を簡単に回避する標的型攻撃に対して組織は脆弱なままとなっていました。また、これらのソリューション間のネイティブな統合や、脅威の全体像の可視化もないため、最新の脅威からアプリケーションを保護するために、セキュリティチームが修正すべきギャップがさらに多くなっています。

現代のSaaSセキュリティ



SWG = セキュアウェブゲートウェイ | CASB = クラウドアクセスセキュリティブローカー | IdP = IDプロバイダー | RBI = リモートブラウザ分離
CES = クラウドメールセキュリティ | ZTNA = Zero Trustネットワークアクセス

従来のSaaSセキュリティと管理ソリューションに残されたギャップを解消するために、組織にはインターネットネイティブな単一プラットフォームでアプリケーションとデータを保護するように設計された最新の脅威対策が必要です。この最新のアプローチに欠かせないのが、堅牢なセキュリティ動態管理です。これにより、セキュリティチームは、ユーザーに重要なリソースへどのようにアクセスさせるかをより的確に判断し、外部および内部の脅威を可視化して制御できるようになります。

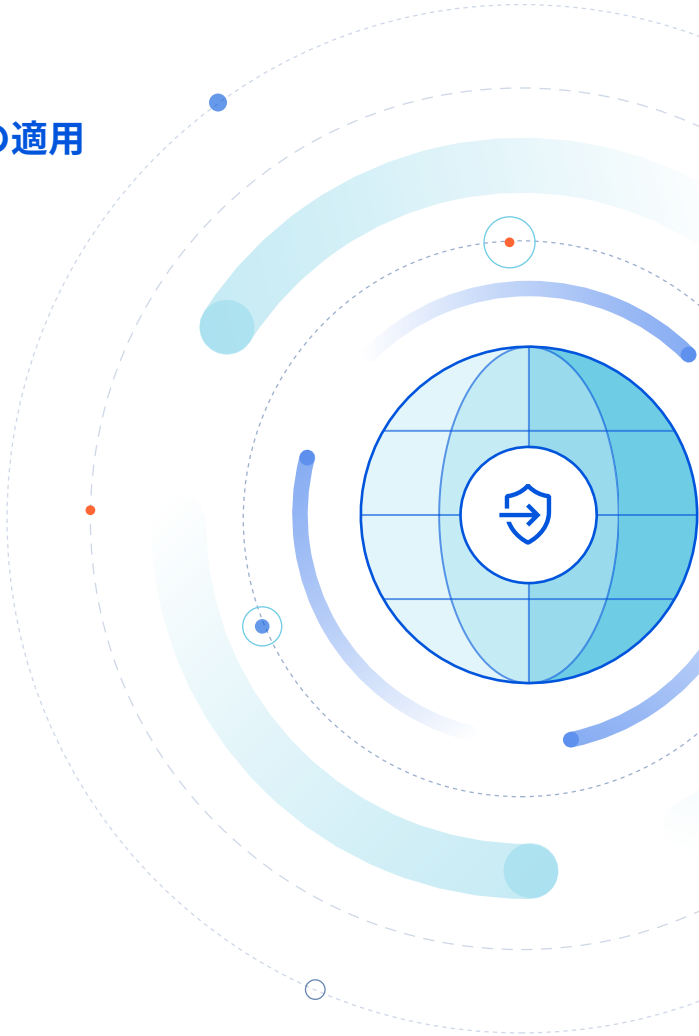
SaaSセキュリティプラットフォームでは、単一のソリューションツールを運用して個々の脅威を修復する必要はなく、アプリケーションをスキャンして設定、権限、共有の異常を検出して、セキュリティチームがアプリケーションへのアクセスを管理し、メール攻撃を軽減し、内部脅威や危険なデータ共有をブロックできるようにします。

このアプローチによって、組織はSaaSアプリケーションをより堅牢かつ包括的に保護できるだけでなく、チケットのトリアージにかかる時間を短縮し、セキュリティプロセスを自動化し、データ漏洩や攻撃、手動による設定やメンテナンスに悩まされることなく、戦略的イニシアチブに集中できるようになります。

SaaSセキュリティへのZero Trustアプローチの適用

SaaSセキュリティの正しいアプローチを開発するには、最新のSaaSとクラウドベースの脅威を俯瞰する必要がありますが、既存のソリューションを組織のニーズに合わせて調整することは、ITおよびセキュリティチームにとって負担の大きい作業となります。組織には、個別の脅威に対処したり、サイロ化したツールのパッチワークに頼るのではなく、簡素化され、管理が容易な、現代の脅威を予測し軽減することができるセキュリティプラットフォームが必要です。

SaaSセキュリティ戦略にとって不可欠な要素であるCASBとクラウドメールセキュリティの両機能が、すべての技術が単独ではなく連携して機能するZero Trustアーキテクチャの中で最適に機能するよう設計されています。この階層化は、正しく実装されれば、セキュリティギャップを排除し、セキュリティチームにかかる労力を減らし、脅威の監視を自動化するなど、隣接する問題を軽減することができます。



CloudflareがSaaSアプリケーションを保護する方法

Cloudflareは、SaaS環境全体を保護する最も簡単な方法を提供します。企業は、ユーザーが重要なリソースにアクセスする方法、外部または内部の攻撃からリソースを保護する方法、リアルタイムにリスクを監視して軽減する方法を制御できます。

* DLPの順番待ちリストに加わる

Cloudflare Zero Trustを使用したSaaSアプリケーションの保護

Cloudflare Zero Trustでは、転送中のデータを保護するために、アクセス（ZTNA）、ゲートウェイ（SWG）、ブラウザ分離（RBI）の制御をクラウドやSaaSアプリケーションの前に配置して、インラインに展開されたCASBアーキテクチャとしてサポート・運用します。

SaaSアプリケーション内の保存データの安全を守るために、簡単に設定できるAPI駆動型の統合機能により、使用頻度の高いアプリケーションの脆弱性や潜在的な脅威を継続的にスキャンします。

Cloudflare Area 1のメールセキュリティとCloudflare Zero Trustの組み合わせ

Cloudflare Area 1メールセキュリティは、ICESを代表するベンダーであり、メールセキュリティのニーズに応じてより柔軟に対応することが可能です。これは、APIを介して統合し、MXレコードの変更することでインラインでメールトラフィックを検証、フィルタリング、検査、分離するゲートウェイとして機能することによって実現しています。

Area 1は、インターネットを事前にクロールして攻撃インフラストラクチャやフィッシング活動を発見し、受信箱に届くよりも数日早くフィッシング攻撃からお客様を保護します。

CloudflareがSaaSアプリケーションのセキュリティ保護する方法の詳細については、https://www.cloudflare.com/ja-jp/products/zero-trustをご覧ください。

ソース

1. ガートナー社、「予測分析：世界規模での情報セキュリティおよびリスクマネジメント。」アナリスト：Shailendra Upadhyay、Mark Driver、Christian Canales、Ruggero Contu、Lawrence Pingree、Elizabeth Kim、John A. Wheeler、Nat Smith、Rahul Yadav、Swati Rakheja、Dave Messett、Mark Wah、Shawn Eftink。2021年8月12日ガートナー社。

2. ガートナー社、「2022年予測：これからは統合セキュリティプラットフォームの時代。」アナリスト：Charlie Winckless、Joerg Fritsch、Peter Firstbrook、Neil MacDonald、Brian Lowans。2021年12月1日ガートナー社。

4. ガートナー社、「クラウド・セキュリティのハイプ・サイクル：2021年。」アナリスト：Tom Croll、Jay Heiser。2021年7月27日ガートナー社。

6. ガートナー社、「マーケットガイド（Eメールセキュリティ）。」アナリスト：Mark Harris、Peter Firstbrook、Ravisha Chugh、Mario de Boer。2021年10月7日ガートナー社。

7. ガートナー社、「マーケットガイド（Eメールセキュリティ）。」アナリスト：Mark Harris、Peter Firstbrook、Ravisha Chugh、Mario de Boer。2021年10月7日ガートナー社。

8. ガートナー社、「マーケットガイド（Eメールセキュリティ）。」アナリスト：Mark Harris、Peter Firstbrook、Ravisha Chugh、Mario de Boer。2021年10月7日ガートナー社。

03-4510-1893 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3303.2022JUN24