ホワイトペーパー

CLOUDFLARE

SASEの利用を開始する：ネットワークインフラストラクチャの安全性と合理化のためのガイド

セキュアアクセスサービスエッジ（SASE）により、旧来のネットワークアーキテクチャがシンプルになります。ネットワークサービスとセキュリティサービスを1つのグローバルネットワークで統合するのです。このホワイトペーパーでは、SASE誕生までのネットワークセキュリティの進化について説明し、SASEソリューションに含まれる幅広いサービスの概要とその採用に向けた実践的な手順について説明します。

03-4510-1893 | enterprise@cloudflare.com | www.cloudflare.com/ja-jp/

はじめに

2019年にGartner社が生み出したセキュアアクセスサービスエッジ（SASE）は当初、デジタルトランスフォーメーションを実現するプロセスの中枢をなす進化として認知されていました。SASEとは、高度なカスタマイズが可能なネットワークとセキュリティサービスが、グローバルクラウドプラットフォームにシームレスに統合されているモデルのことを指します。2023年までに20%の導入率が見込まれることから、Gartner社は、SASE機能の需要が「エンタープライズネットワークとネットワークセキュリティアーキテクチャを再定義し、競合情勢を変える」と主張しました。[1]

それ以来、SASEという用語は急激にITと企業のセキュリティ分野に広がっています。ネットワークセキュリティプロバイダーやSD-WANベンダーが、早急に自らをSASEリーダーと名乗るようになり、企業にはSASEフレームワークに似せた、急ごしらえでネットワークとセキュリティサービスを寄せ集めた、SASEフレームワークとはいえない不完全なものが残りました。

真のSASEの採用とは、既存のシングルポイントソリューションを組み合わせるだけのことではありません。企業ネットワークインフラストラクチャを完全に再考することが必要です。オンプレミスの堅牢なネットワーク境界を維持するだけでは、分散型のモバイルワーク環境はもはや完全には保護できません。その一方、ハイブリッドインフラストラクチャを保護するために複数のセキュリティサービスを連携させるには、費用がかかります。デプロイと管理はITチームの負担となり、結果として大規模なセキュリティギャップが生じてしまいます。

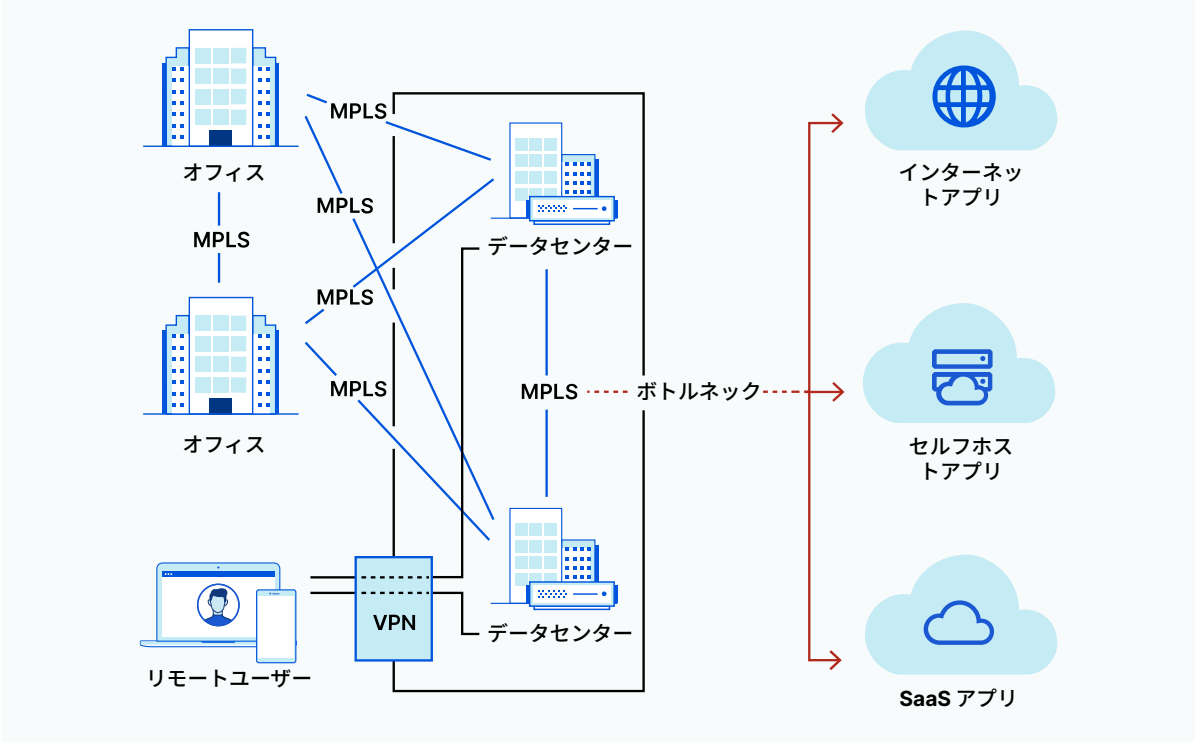
SASEは、ネットワーク境界を、一元化されたデータセンターからユーザー側に移行することにより、これらの課題を克服します。そして、ネットワークとネットワークセキュリティサービスを統合し、Zero Trustの原則をベースにした、単一のクラウドネイティブのプラットフォームからそうしたサービスを提供することで、サービス間のセキュリティギャップを排除します。ITチームはネットワークアクティビティをより詳細に可視化でき、クラウド移行プロセスもシンプルになります。

SASEの始まり — 旧モデル

SASEがもたらした重要な変化を理解するためは、ネットワークインフラストラクチャとセキュリティの漸進的な進化をよく知ることが重要です。

かつて、クラウドコンピューティングが広く採用される前は、オンプレミスの施設内に、企業リソース、データ、アプリケーションがあり、ハードウェアのファイアウォールとDDoS対策アプライアンスがこれらを保護していました。企業の従業員は、ネットワークファイアウォールでフィルタリングされたプライベート接続を介して内部リソースにアクセスしていました。リモートのロケーションから接続するユーザーは通常、VPN経由で接続していましたが、過密の回避や脆弱性へのパッチ対応のために遅延、高額な費用が生じ、モバイル体験にもマイナスの影響がありました。

オープンインターネットへの恐怖が、このセットアップが広く用いられる理由となりました。このオープンインターネットとは、エンタープライズクラスのパフォーマンスとセキュリティのニーズをほとんど考慮せずに、なによりも耐障害性を重視して構築されたツールなのです。インターネットは本質的に攻撃に対して脆弱であることが証明されているため、企業は独自のプライベートネットワークを確立し、データ、アプリケーション、企業リソースを（失敗することも多かったのですが）守ろうとしました。 物理的なファイアウォールボックスとDDoS対策アプライアンス、および一元化されたデータセンターを介して、すべての着信トラフィックをトロンボーン（再ルーティング）し、データセンターで検査とフィルタリングを行ったのです。



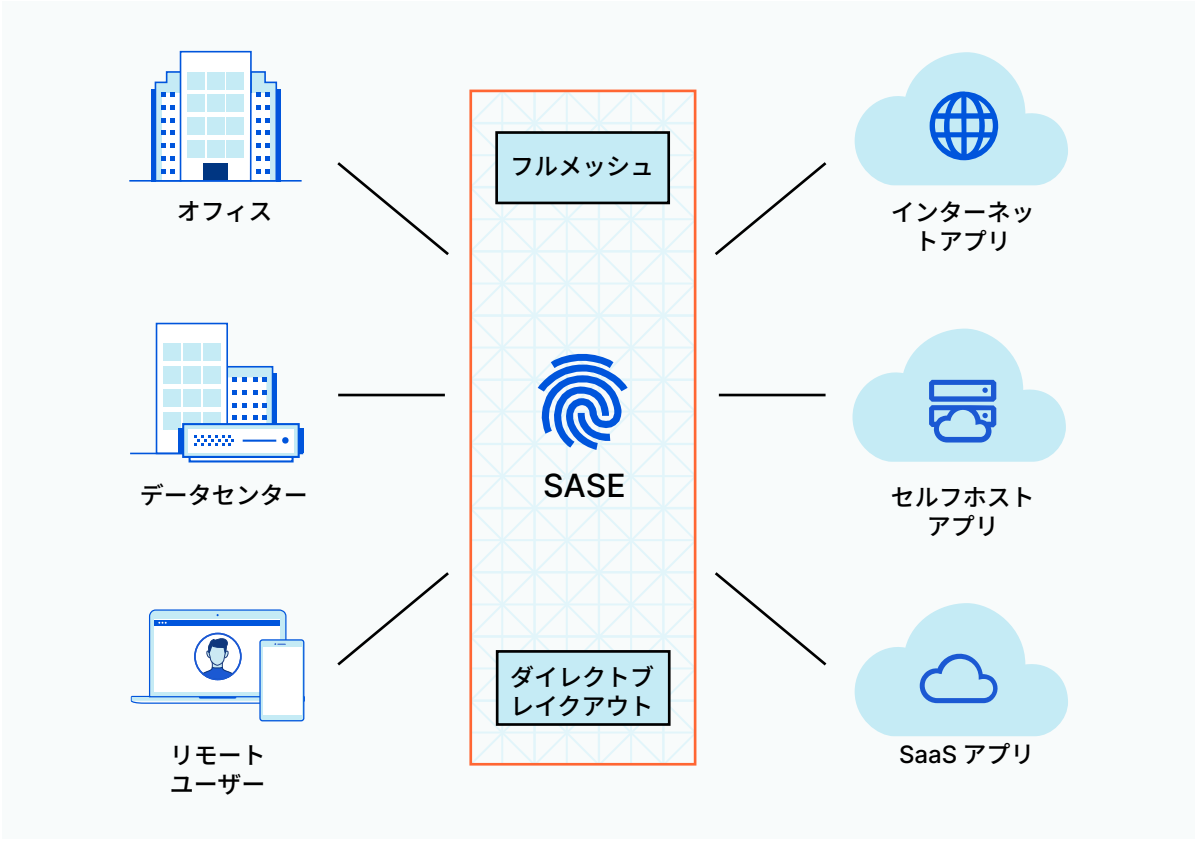
このネットワークセキュリティモデルは高価かつ複雑で、このモデルを導入してもなお、企業はデータ漏えいや内部の脅威に対して脆弱でした。サイバー攻撃者によりネットワークの境界が侵害されると、攻撃者はランサムウェアを拡散させ、ユーザーアカウントの乗っ取り[2]、貴重な顧客データの窃盗など 3、企業内で重大な損害をもたらしました。

クラウドとSaaSサービスの登場により、企業にネットワークインフラストラクチャについて再考する機会があたえられ、自由度と柔軟性が高まりました。アプリケーション、データ、従業員はオンプレミス施設内に常駐する必要がないためです。

SASEの始まり — 新モデル

しかし、その自由度は新たなセキュリティ上の課題を招きます。ITチームでは、オンプレミスサービスとクラウドベースのサービスが混在したものを保護するタスクに加えて、モバイル環境とリモートワーク環境の保護に関する仕事が増えています。[4] これを成功させるには、多くの場合、高価なハードウェアを維持し、複数のベンダーの単一ポイントセキュリティサービスを組み合わせる必要があります。そのため、実装に時間がかかり、管理も困難になります。

ネットワークセキュリティの次なる進化は、従来の「ハブアンドスポーク」インフラストラクチャを保護していたハードウェアや、ハイブリッドクラウドアーキテクチャに必要となる複雑な解決策とは異なる形のものになっていくでしょう。むしろ、SASEフレームワークのように、ネットワークサービスとセキュリティサービスをまとめ、一つの統合サービスとして提供する形になっていくはずです。



効果のないハードウェアアプライアンスに依存したり、サイロ化されたセキュリティサービスにパッチを適用するのではなく、SASEは、ネットワークセキュリティに対する合理的なアプローチを提供します。そして、複雑なバックホールをインターネットエッジに置き換え、企業は単一のパスでトラフィックのルーティング、迅速化、検証、フィルター、分離、検査などを実行できるようになります。フルメッシュのWAN接続、ゼロトラストアクセスポリシー、ネットワークレベルの脅威保護などを組み合わせることで、SASEはレガシーVPN、ハードウェアファイアウォール、プロキシ、DDoS対策アプライアンスの必要性を排除し、企業はネットワークセキュリティ構成をより詳細に可視化し、制御できるようになります。

SASEの範囲を定義 — 中心となる機能

SASE は、ソフトウェア定義のワイドエリアネットワーキングとコアネットワークセキュリティサービスを組み合わせて、クラウドエッジで提供する、クラウドベースのセキュリティモデルです。ほとんどのSASE製品は、その特徴として次の5つの主な機能を備えています。

ネットワークの構築と管理

ソフトウェア定義のワイドエリアネットワーク (SD-WAN) により、企業は、ハードウェアルーターまたはマルチプロトコルラベルスイッチング（MPLS）回線を使うことなく、プライベートコーポレートネットワークを構築できます。この仮想ソフトウェアベースアーキテクチャなら、ネットワークインフラストラクチャの作成や保守時に柔軟度は増しますが、どうしてもセキュリティ上の脆弱性が出てきてしまいます。

トラフィックのフィルタリング

セキュアWebゲートウェイ（SWG）は、Webトラフィックからの不必要なコンテンツをフィルタリングした上で不正なユーザー行為をブロックし、さらに企業のセキュリティポリシーを適用することで、サイバー脅威やデータ漏えいを防止します。これには通常、URLフィルタリング、マルウェア対策検出とブロック、アプリケーション制御などの機能が含まれます。

データを保護する

クラウドアクセスセキュリティブローカー（CASB）は、クラウドでホストされるサービスに向けて、いくつかのセキュリティ機能を実行します（例：SaaS、IaaS、PaaSアプリケーション）。Standard CASBの機能には、アクセス制御と情報漏えい防止対策（DLP）による機密性の高いデータの保護、シャドーIT（承認されていない企業システム）の特定、データプライバシー規制の確実な順守などがあります。

ユーザーとアプリケーションを結びつける

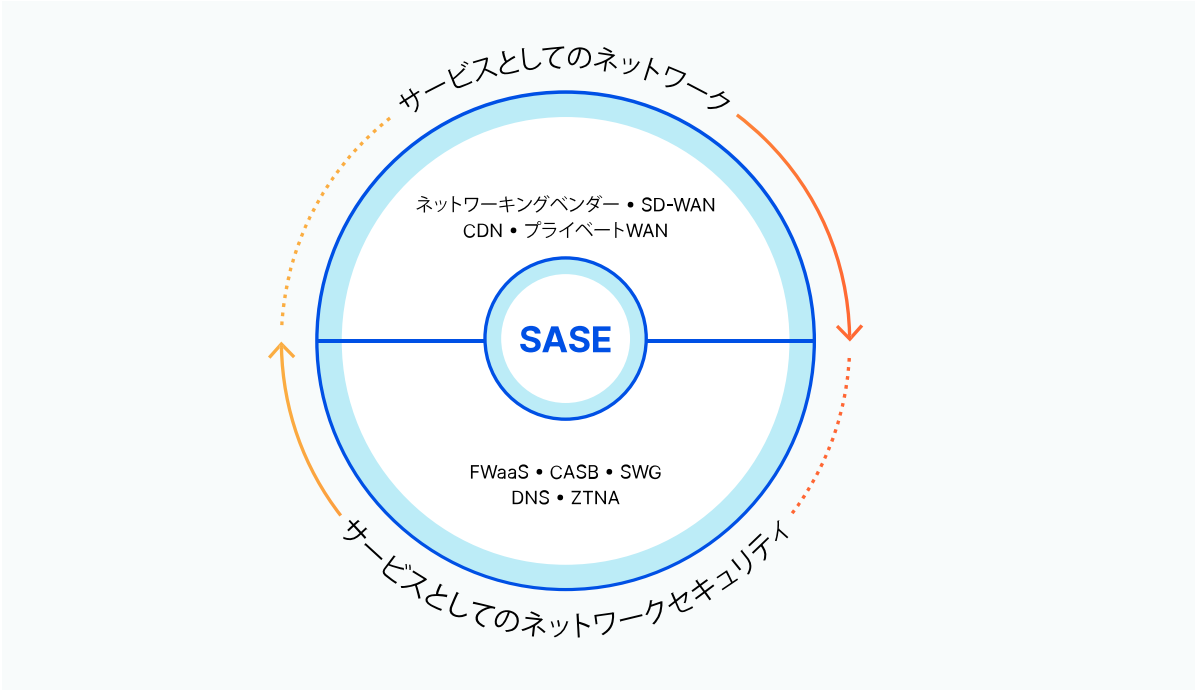
ゼロトラストネットワークアクセス (ZTNA) では、内部リソースを保護し、潜在的なデータ漏えいを防ぐため、保護対象となるすべてのアプリケーションにおいて、全ユーザーのリアルタイム検証が必要となります。「ゼロトラスト」アプローチでは、ユーザーの身元が明らかになるまで、どのエンティティも自動的には信頼されません。 ユーザーがプライベートネットワーク境界内にいたとしてもです。

アプリケーションとインフラストラクチャを保護する

クラウドベースのファイアウォール（FWaaS）は、URLフィルタリング、侵入防止、統一されたポリシー管理を含む一連のセキュリティ機能を通じて、クラウドインフラストラクチャとアプリケーションをサイバー攻撃から保護します。

SASEの範囲を定義 — クラス最高の機能

従来のSASEソリューションには、上記の5つのサービスが含まれていますが、このリストは厳格な要件というよりも出発点です。SASEは、「ソフトウェアベースのネットワークアーキテクチャ」と「クラウドベースのセキュリティサービス」という 2 つの基本的で個別の機能を統合したものです。さらに、ベンダーは必要に応じてサービスの追加／削除が可能です。



SD-WANは、お客様がネットワーク接続で自身に近い短距離を管理するのに役立つ一方で、ユーザーとアプリケーション間の中距離のセキュリティ、パフォーマンス、信頼性を直接確保することができません。せいぜい、複数のグローバルネットワークを信頼し、複数のセキュリティサービスをチェイニングすることで、エンドツーエンドの接続を最適化するぐらいですが、それは複雑で費用もかかります。SD-WANの有無に関係なく、ゼロからWAN-as-a-service（サービスとしてのWAN）を構築したSASEプロバイダーは、お客様がたった1つのグローバルネットワークを、デフォルトで構築されたセキュリティ、パフォーマンス、信頼性で保護できるようにします。SWG、CASB、ZTNAを連携することで、セキュリティリスクは大幅に減少しますが、これらの組み合わせでは依然として、あらゆる事例において脅威とデータ保護との間に多くの隔たりを残してしまいます。すべてのデータセンターで、SWG、CASB、ZTNAとネイティブに統合するために、ゼロからリモートのブラウザ分離を構築したSASEプロバイダーは、こうした隔たりを排除します。

SASEアプローチのメリット

SASEは進化し続けているため、その実装はベンダーや企業ごとに大幅に異なることもあります。ただ大抵のSASEソリューションは、オンプレミスおよびハイブリッドなネットワークセキュリティ構成よりも、以下のような点が優れていると言えるでしょう。

実装の効率化

ネットワークとセキュリティサービスを統合しているため、クラウドベースサービスのオンボードやオンプレミスアプライアンスのセットアップも必要なく、時間、費用、社内リソースを投じなくとも、ネットワークとセキュリティサービスを最新の脅威に対抗するようアップデートできます。

シンプルなポリシー管理

SASEを使うと、企業はロケーション、ユーザー、デバイス、アプリケーションのすべてに対して、アクセスポリシーを設定、監視、調整、適用できます。攻撃や忍び寄る脅威は、単一のポータルから特定、軽減が可能に。 ひとつしか機能を持たないセキュリティツールを複数使って個別に監視および管理する必要はありません。

IDベースのネットワークアクセス

SASEは、ゼロトラストセキュリティモデルに大きく依拠しており、ユーザーの身元とアクセスは、複数の要因を組み合わせて判断されます。ユーザーのロケーション、時刻、企業のセキュリティ基準、コンプライアンスポリシー、継続的なリスク/信頼の評価などの要因が考慮されます。このレベルのセキュリティは過度に寛容かつ本質的に脆弱なVPNからの格別な進化であり、外部と内部のデータ漏えいやその他の攻撃から保護します。

遅延の減少

SASEでは遅延が減り、パフォーマンスが向上します。それは、広大なエッジネットワーク全体で、トラフィックができるだけユーザーに近いところで処理できるように、ネットワークトラフィックをルーティングするためです。ルーティングの最適化は、ネットワークの輻輳と他の要因に基づいて、最速のネットワークパスを決定するのに役立ちます。

グローバルネットワーク

SASEフレームワークは、単一のグローバルネットワーク上に構築されるため、企業は、ネットワーク境界をリモートユーザー、支社、デバイス、またはアプリケーションを問わず、どこでも望むところに設置することができ、その上、ネットワークインフラストラクチャ全体の可視性と制御性も高まります。

SASEの利用を開始する

入り組んだオンプレミスセットアップに多大な時間、リソース、費用を投じた企業や、クラウドベースのセキュリティサービスの複雑なWebを管理する企業、今後のリモートワークに合わせてまだ調整を続けている企業にとってSASEの導入は難しいと思われがちですが、そうとは限りません。

SASEの使用を開始するには、次の5つの実用的なステップがあります。

1. リモートワーク中の社員を保護。

VPNへの依存を減らし、さらにはVPNの置き換えを可能にし、社内外の脅威から企業データとリソースを保護して、ユーザーエクスペリエンスを向上させるZTNAソリューションを実装します。セキュリティで保護されたWebゲートウェイ、ファイアウォール、デバイスのブラウザをエッジに置くことで、中央データセンター経由でバックホールすることなく、トラフィックのフィルタリング、分離、検査が可能になります。

2. クラウド境界の背後に支社を配置。

ゼロトラストアーキテクチャを支社に適用することで、オンプレミスのセキュリティアプライアンス（統合型脅威の管理など）は不要になります。オンプレミスのアプライアンスでは維持費用がかかり、急速に変化する脅威情勢に対しては効果がありません。

3. DDoS攻撃対策をエッジに移動。

リアルタイムで脅威を検出／軽減できるクラウドネイティブのネットワーク層DDoS攻撃対策により、DDoS対策アプライアンスを一掃し、企業ネットワークを攻撃から守ります。

4. アプリケーションをクラウドへ移行。

組織の規模拡大に合わせて、データセンターからクラウドにセルフホストアプリケーションを移行し、すべてのトラフィックに一貫したクラウドセキュリティポリシーを確実に適用します。

5. オンプレミスのセキュリティアプライアンスを、統合型クラウドネイティブポリシーの施行に置き換える。

ポリシーの施行場所をエッジへとシフトすることで、ネットワークのハードウェアアプライアンス管理の費用と複雑性を抑えます。そうすることで、トラフィック、攻撃パターン、セキュリティポリシーをすべて1つのパスで監視し、1つのウィンドウで管理できるようになります。

CLOUDFLAREのSASE、CLOUDFLARE ONE

CloudflareのSASE「Cloudflare One」は、ユーザーを企業のリソースへ動的につなぐゼロトラストの「サービスとしてのネットワーク（NaaS）」プラットフォーム。ユーザーがどこにいても、ユーザーの近くでIDベースのセキュリティ制御を提供します。

Cloudflare Oneのネットワークサービスの利点（インフラストラクチャチーム）	Cloudflare Oneのゼロトラストサービスの利点（ITセキュリティチーム）
• Cloudflareのグローバルネットワークを、WANとして利用する。 • クラウドネイティブのネットワークファイアウォールで、レガシーアプライアンスを置き換える。 • アプリケーションのパフォーマンスとエンドユーザーの遅延を改善する。	• VPNを使わずに、ユーザーとリソースを簡単かつ安全に接続し、 • ラテラルムーブメント、ランサムウェア、マルウェア、フィッシングを阻止します。 • エンドユーザーのエクスペリエンスと管理者の手間、特にオンボードの時間を改善する。

Cloudflareを選ぶ理由

シンプルなデプロイメントと管理

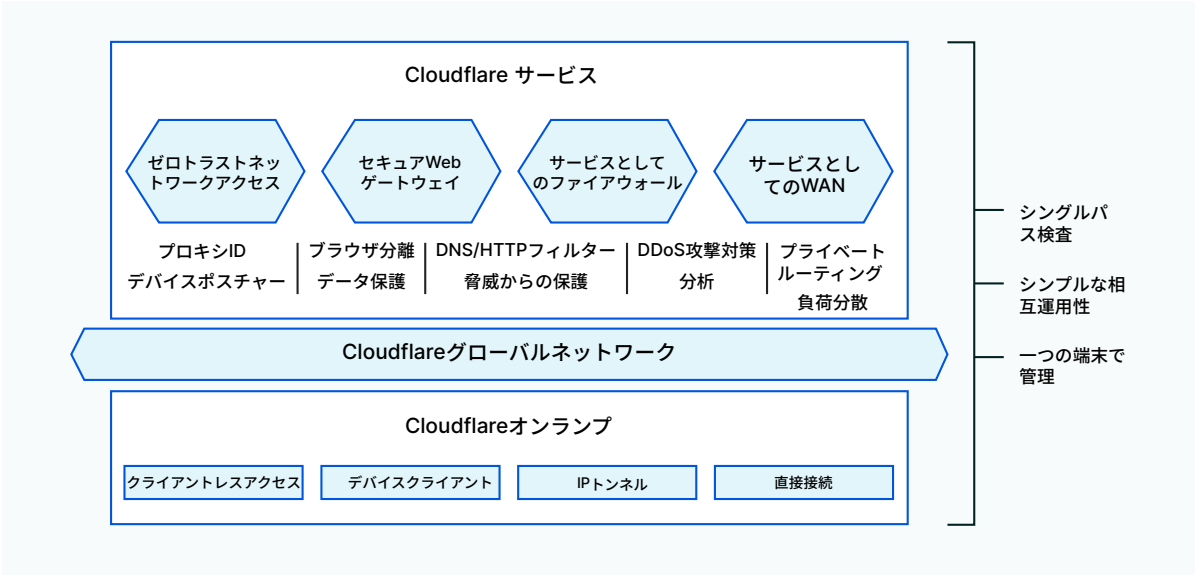
Cloudflare Oneのサービスはすべて、世界で250都市以上のすべてのお客様にご利用いただけます。SASEモデルに移行する際、複数の個別製品を手動で統合する必要はありません。

世界中どこでも均一なセキュリティとスピード

Cloudflareの各データセンターでは、シングルパスのトラフィック検査およびルーティングを行い、ユーザーが世界中どこにいようと同じ保護を提供します。遅延や「トロンボーン効果」による減速はありません。

既にお使いのものに接続

Cloudflareは世界で最もパワフルでピアリング先が多いネットワークを運営しており、Cloudflare Oneはお客様が既にお使いのID、エンドポイント、クラウドプロバイダーをサポートします。使い勝手が良く、統合が容易



CLOUDFLAREのSASE、CLOUDFLARE ONE

世界のどこからでも仕事ができる現代において、Cloudflare Oneは、お客様がユーザー、アプリケーション、支社オフィスを結ぶのに必要なセキュリティ対策機能と接続機能を提供します。

<table>
<tr><th colspan="2">Cloudflare One</th></tr>
<tr><td>ゼロトラストネットワークアクセス
アイデンティティとコンテキストに基づくルールを適用し、ラテラルムーブメントを制限することによって、あらゆるユーザーをあらゆるアプリケーション、プライベートネットワークに、VPNより速く安全につなぎます。

中心的なSASEの機能：
• ユーザーとアプリケーションを結びつける
• データを保護する</td><td>サービスとしてのWAN
お客様の従来型WANアーキテクチャに代えて当社のグローバルなプライベートバックボーンを導入することによって、高速パフォーマンス、内蔵セキュリティ、高耐障害性のエニーツーエニー接続を可能にします。

中心的なSASEの機能：
• ネットワークの構築と管理</td></tr>
<tr><td>セキュアWebゲートウェイ
DNS、HTTP、ネットワーク、ブラウザ分離のルール適用と無制限のSSL検査によって、既知・未知のインターネットの脅威をブロックし、データの流れを簡単に制御します。

中心的なSASEの機能：
• トラフィックのフィルタリングと検査：
• データを保護する</td><td>サービスとしてのファイアウォール
インバウンドとアウトバウンドのトラフィックすべてにステートフルインスペクションのルールを適用することによって、高速パフォーマンスを維持しながら、アクセスを制御しDDoS攻撃や他の脅威をブロックします。
中心的なSASEの機能：
• アプリケーションとインフラの保護</td></tr>
<tr><td colspan="2">Cloudflareグローバルネットワーク
インターネット人口の95%に50ミリ秒未満で到達する当社のネットワークは、250都市以上に広がり、容量は100Tbps以上、相互接続点は10,000か所以上。稼働率100%のSLAに基づいて運営されています。</td></tr>
<tr><td>クライアントレスアクセス
セルフホストアプリやSaaSアプリへ、単なるHTTPより安全なブラウザーベースでアクセスし、あらゆるユーザー、デバイス（第三者のものやBYODを含む）を数分でオンボードします。</td><td>IPトンネル
クラウドまたはオンプレミスの環境で、GREトンネルまたは当社独自のトンネルコネクターを使い、BGPエニーキャストでルートをアナウンスすることを通じて、パブリックとプライベートのIPサブネット全部をオンボードします。</td></tr>
<tr><td>デバイスクライアント
あらゆるアプリケーション、プライベートネットワーク、インターネット通信の宛先に対し、安全なクライアントベースのアクセスを可能にするため、Windows、macOS、iOS、Android、ChromeOS、Linux のデバイスをオンボードします。</td><td>直接接続
信頼性とセキュリティを確保するため、お客様のネットワークインフラストラクチャの物理的もしくはバーチャルなオンボーディングを、パブリックなインターネット上ではなく、1600余のコロケーション施設内で実施します。</td></tr>
</table>

CLOUDFLARE ONEで得られるビジネスの結果

↓91%

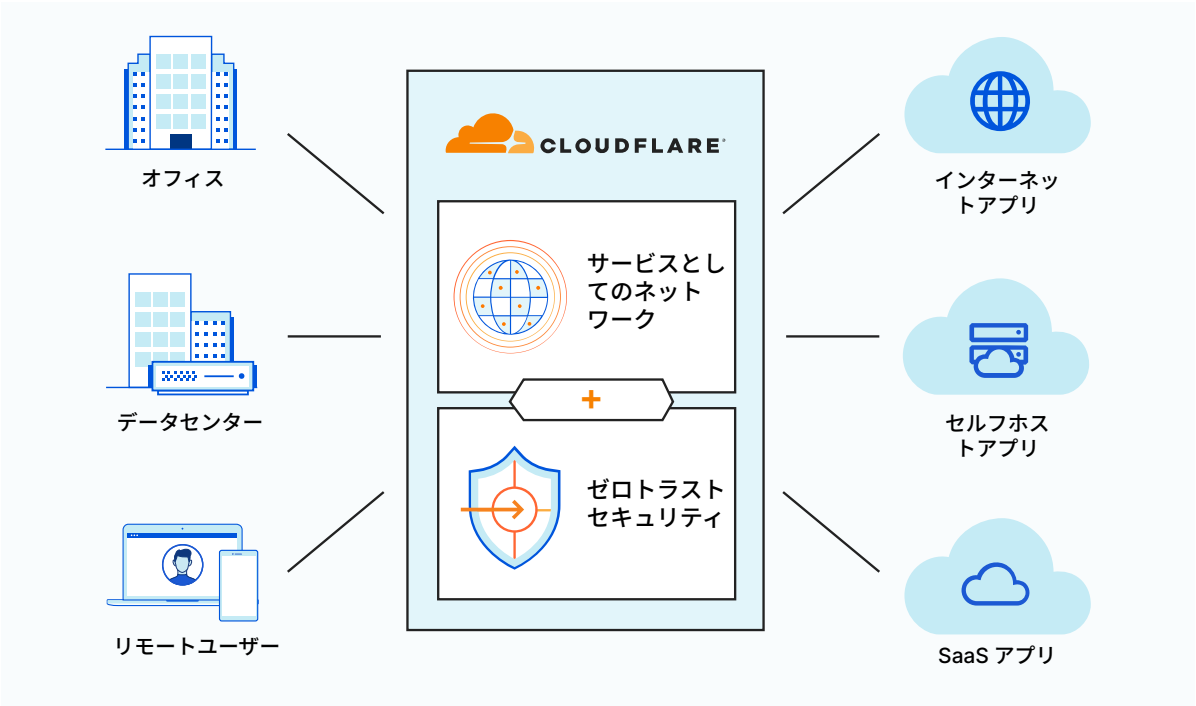
高リスクのブラウジングをエンドユーザーのシステムから分離し、アプリケーションアクセスをネットワークから分離することで、攻撃対象領域を最大91%縮小します。

10 → 1

最大10の個別製品を1つのプラットフォームに統合することで、総保有コスト（TCO）を低減し、ビジネス運営を迅速化します。

↑60%

VPNではなくCloudflareでユーザーをリソースに接続すれば、新入社員や契約社員のオンボーディングにかかる時間が最大60%短縮できます。



Cloudflare Oneの詳細については、こちらをご覧ください。

こちらをクリック

参考文献

1. Gartner、『The Future of Network Security Is in the Cloud（ネットワークセキュリティの未来はクラウドにある）』アナリスト：Neil MacDonald、Lawrence Orans、 Joe Skorupa. 2019年8月30日. Gartner.

2. Twitter Inc. 『An update on our security incident（セキュリティインシデントの最新情報）』 Twitter. 2020年10月27日にアクセス

3. Marriott International News Center. 『Marriott International Notifies Guests of Property System Incident（マリオットインターナショナルからお客様へ、資産システムに関する事件についてのお知らせ）』 Marriott. 2020年10月27日にアクセス

4. Jessica Bursztynsky著『Dropbox is the latest San Francisco tech company to make remote work permanent.（サンフランシスコの最新テクノロジー企業Dropbox社、リモートワークを恒久化）』 CNBC. CNBC. 2020年10月27日にアクセス