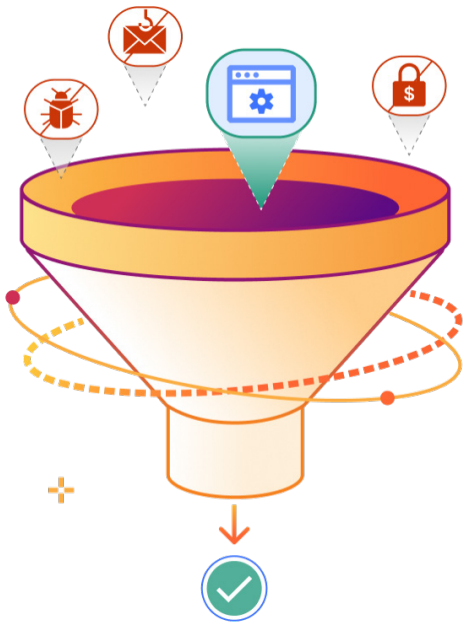
セキュアWebゲートウェイ（SWG）

Cloudflare Oneに含まれるコンポーザブルなサービスCloudflare Gatewayは、ID認識型のインターネットフィルタリングにより、サイバー脅威からユーザーとデータを保護します。



シンプルな最新脅威防御

複雑なレガシーWebセキュリティの代替

サイバー脅威はあらゆるところに存在し、拡大する攻撃対象領域のギャップを悪用し続けています。複数のポイントソリューション（DNSリゾルバ、Webゲートウェイ、ネットワークファイアウォールなど）を併用すれば、コスト、複雑さ、リスクが増すだけです。

Cloudflare Gatewayはセキュリティを簡素化し、インターネットや内部リソースへのアクセスに一貫した保護と可視性をもたらします。以下に役立つID認識型ポリシーでサイバーリスクを低減します。

- **インターネットに潜む脅威の阻止**　ランサムウェア、フィッシング、コマンド＆コントロールなどを阻止
- **L4-L7トラフィックの制御と監視**　DNS、HTTP、ネットワーク、ブラウザ分離のルールを適用
- **利用規定の適用**　すべてのリモートワーカーとオフィスワーカーに適用

シングルパスアーキテクチャでは、全トラフィックは検証、フィルタリング、検査され、脅威から分離されます。

今はSWG、将来はセキュリティサービスエッジ（SSE）

SWG制御の最新化は、セキュリティをSSEアーキテクチャに統合してゼロトラストのベストプラクティスを実践するための一般的ステップです。

Cloudflareを使った**ゼロトラスト導入の流れ**をご覧ください。

Cloudflareを選ぶ理由

統合セキュリティ

1つのネットワーク

セキュリティサービスエッジ（SSE）、Webアプリケーションとapiの保護（WAAP）、メールセキュリティ、その他の分野の全サービスを、単一のネットワークとコントロールプレーンで提供します。

大規模な脅威インテリジェンス

2兆

1日あたり2兆件のDNSクエリを処理します。新規、初照会、高リスクのドメインをリアルタイムで可視化することにより、AIとMLを活用した脅威ハンティングモデルを強化します。

拡張を想定して構築されたサービス

310以上

120か国以上に配された310か所以上のネットワークロケーション。全ロケーションでSWGとゼロトラストやSSEの機能をすべて実行できるため、常に高速で一貫性のある適用が可能です。

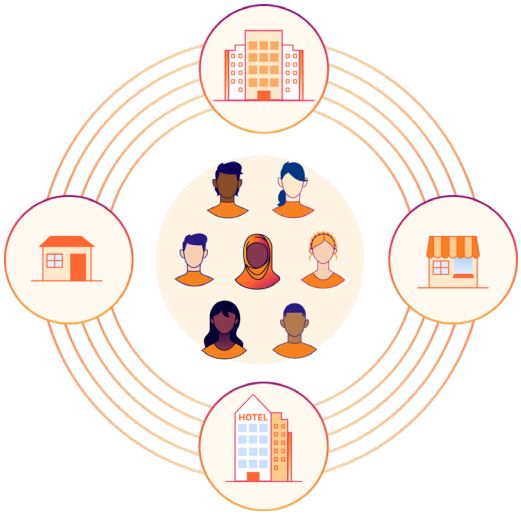
ユースケース：リモートワーカーとオフィスを脅威から防御

問題

ハイブリッドワークの導入で攻撃対象領域が拡大し、個別ツールを管理する際にセキュリティギャップが生じて、ランサムウェアやフィッシングなど、コスト増大やブランドの評判低下を招くサイバー脅威に狙われやすくなっています。

ソリューション

CloudflareのSWGは、リモートワーカーとオフィスワーカーに一貫したWebセキュリティを提供します。 ほとんどの組織は、まずDNSフィルタリングから始めて価値実現までの時間を短縮し、その後すべてのインターネットアクティビティのより包括的な検査と制御を重ねていきます。



利用開始

Cloudflareネットワークへトラフィックを送信 まずDNS解決のために（後に網羅的なHTTP検査のために）

DNSフィルタリングを適用 リモートワーカーの場合はID/デバイスごと、オフィスの場合は場所ごとに

きめ細かな制御を重ね掛け HTTP、ネットワーク、ブラウザ分離のルールなど

クラウドメールセキュリティを展開 インライン方式（MXとして）、API経由、または両方（マルチモード）で

まず、ネットワーク接続オン・オフ状態でのWebブラウジングを保護

次に、メールセキュリティを重ね掛け

リスク低減とチームの生産性向上を同時に実現

シンプルで柔軟性の高い展開

DNS解決にネットワークルーターを使用。 GRE/IPsecトンネル、WANコネクタ、または既存のSD-WAN経由でL3トラフィックを送信します。

あるいは、当社のデバイスクライアントをフォワードプロキシにしてトラフィックを転送します。

高速で一貫性のある保護

当社ネットワーク全体のシングルパス検査で、全環境に高速で一貫性のあるポリシーを適用します。

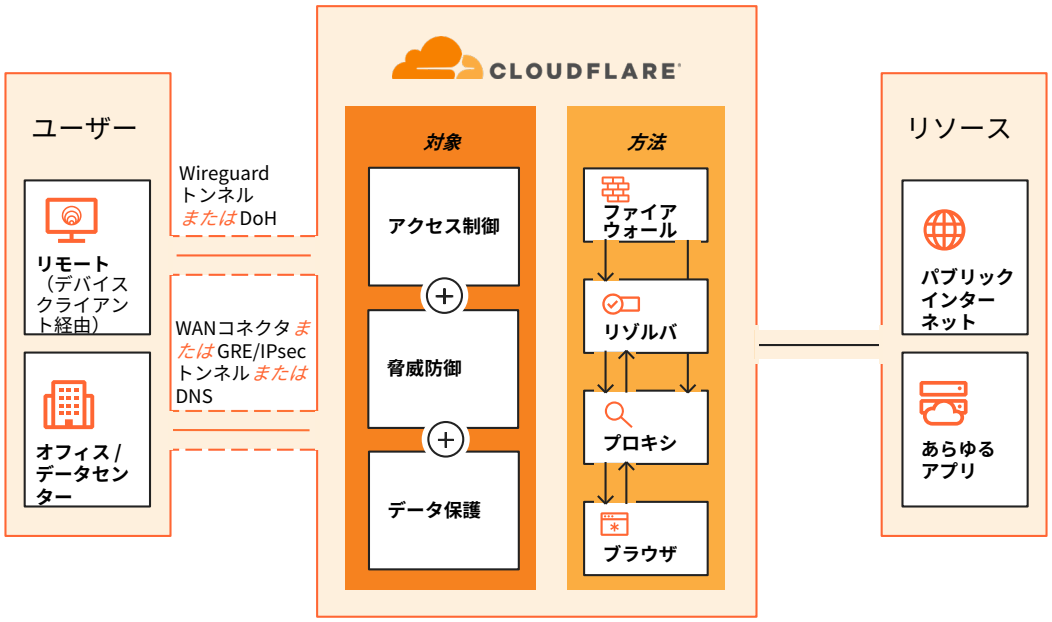
Zscaler、Netskope、Palo Alto Networksといったベンダーとの比較テストで高速保護は実証済みです。

ゼロトラストの導入を加速

単一の統合コントロールプレーンと単一のポリシーマネジャーで、コンポーザブルなSSE/SASEサービスをすべて管理します。

Webとメールのセキュリティから始め、その他のゼロトラスト制御を自分のペースで重ねていくことができます。

SWGの仕組み



セキュリティをシンプルに

ファイアウォール、リゾルバ、プロキシ、ブラウザ制御を、インターネットへのトラフィックと内部リソースへのトラフィックの両方に適用します。

単一のポリシーマネージャーでポリシーを作成します。

SWGの基盤上にSSE制御をレイヤー化

CloudflareのSWGをフォワードプロキシにしてトラフィックを経由させることにより、ネイティブ統合されコンポーザブルな当社SSEサービスの機能を使って、セキュリティ制御と可視性をさらに拡張することができます。

リモートブラウザ分離でWebとアプリのアクティビティを保護

- すべてのブラウザコードをCloudflareのグローバルネットワーク上で低遅延で実行することにより、ローカルデバイスをマルウェアから分離します。
- DLPスキャンとブラウザ制御（コピー＆ペーストのブロック、アップロード/ダウンロードや印刷の制限）によってアプリを隔離し、データを保護します。デバイスクライアントの有無は問いません。

マルチモードDLPとCASBでデータを保護

- 事前定義されたプロファイル（財務データや健康データなど）やカスタムプロファイル（完全なデーター致：EDMなど）で、HTTP(S)トラフィックやファイルに含まれる機密データを検出しブロックすることによって、データ漏えいを防止します。
- 統合DLP機密データ検出機能でSaaSスイートをスキャンし、設定ミスがあれば予め決められた修正処置を行います。

ZTNAでID認識型アクセスポリシーを拡張

- セルフホスト型企業アプリ、SaaSアプリ、プライベートネットワークのIPやホスト名へのアクセスを制限するゼロトラストルールを適用します。
- IDとエンドポイントの保護プロバイダーを一度統合し、同じルールビルダーを使ってインターネットとアプリのアクセスルール全体にポスチャチェックを適用します。

可視性を向上

- すべてのマネージドおよびアンマネージドデバイスについて、詳細な監査ログを保持します（契約プランの場合、DNSログは6か月間、HTTPログとネットワークログは30日間保存）。
- 相関と詳細分析のために、希望のSIEMへログプッシュします。

Gatewayの機能

脅威防御とセキュアアクセス	
セキュリティとアプリケーションのカテゴリ	包括的な対策により、ランサムウェア、フィッシング、DGAドメイン、DNSトンネリング、新規および初照会のドメイン、C2とボットネット、その他のセキュリティリスクから保護します。25のアプリカテゴリ（AIを含む）をインラインCASBでカバーします。
再帰DNSフィルタリング	ドメインとIPアドレスの許可/ブロック/オーバーライドをセキュリティまたはコンテンツのカテゴリごとに行います。DNSフィルタリングは当社のテナントAPIを通じて管理でき、親子構成が可能です。
HTTP(S)フィルタリングと検査	トラフィックの制御を、送信元、送信先、ドメイン、HTTPメソッド、URLなどに基づいて行います。HTTP1/2/3インスペクションによって、アンチウィルススキャンとDLPスキャン、ファイル制御、デバイスポスチャ、テナント、リモートブラウザ分離などが可能です。
無制限のTLS1.3検査	デフォルトでTLS1.3検査が無制限。すべてのHTTPSトラフィックが復号化され、ポリシーが適用され、リクエストが当社の証明書またはお客様のカスタム証明書で再暗号化されます。いずれも市場最速の低遅延で実行されます。DNS over TLS（DoT）とDNS over HTTP（DoH）の規格に対応。FIPS 140-2に準拠した暗号スイートのみを有効にします。
L4 FWaaS	L4ネットワークポリシーはすべてのパブリック/プライベートTCP/UDPパケットに適用され、検出されたプロトコル、ジオロケーション、SNIドメインなどによって、非HTTPリソースへのアクセスを制御します。22番ポートでSSHトラフィックを監査します。（L3 FWaaS機能をWANネットワーキングサービスに組み込んでいます。）
アンチウイルス検査	スキャンにより、アップロードまたはダウンロードされたファイル（PDF、ZIP、RARなど全タイプ）に潜むウイルスを検出します。
IDとデバイスポスチャのチェック	すべての主要大手IDプロバイダー、ソーシャルID、SAMLおよびOIDC規格に基づいてポリシーを設定します。デバイスクライアントまたはサードパーティのエンドポイント保護プロバイダーを介して、デバイスポスチャを検証します。
脅威インテリジェンスの統合	脅威インテリジェンスは、当社独自のAI/MLモデルとサードパーティのフィードに基づきます。ファーストパーティインテリジェンスは、最大級の権威的かつ再帰的なDNSリゾルバ（1日あたり2兆以上のクエリを処理）が取得するグローバルテレメトリを基にしています。当社のWebクローラーは、新たなキャンペーンインフラストラクチャを発見するために、数週間ごとにWeb全体（80億ページ以上）のインデックスも作成しています。カスタムの脅威フィードや署名（IPS、URL、ドメインなど）もサポートしています。
オンランプとオフランプ	
デバイスクライアントあり	当社のデバイスクライアント（WARP）をフォワードプロキシにして、フルWireGuardトンネルまたはDoHサーバー経由でトラフィックを転送します。セルフエンロールまたはMDM経由でデプロイします。デバイスポスチャチェックを有効にします。デバイスがネットワークに接続している状態かどうかを検出します。
クライアントレスのオプション	お客様のロケーションからのDNSクエリネットワークルーティング、Anycast GRE/IPsecトンネル、WANコネクタ、PACファイルを使ったプロキシエンドポイント、URL書き換えによるクライアントレスWeb分離などがあります。
IPv4とIPv6に対応	すべての機能が、IPv4接続とIPv6接続（IP6のみかデュアルスタックかは問わず）で利用可能です。
トラフィックのルーティング	
専用エグレスIPとエグレスポリシー	送信元IPに基づいてトラフィックを許可リストに追加する際に使える静的IP（IPv4またはIPv6）の専用範囲です。エグレスポリシーで、ID、ジオロケーション、デバイスポスチャなどの属性に基づいて、使用するエグレスIPを選択します。各エグレスIPは個々のアカウントに固有のものであり、他のお客様は使用しません。
リゾルバポリシー	DNSリクエストをカスタムDNSリゾルバにルーティングし、プライベートネットワークサービスや社内アプリなどのパブリックにルーティングできないドメインに到達します。（デフォルトでは、 DNSリクエストは、Cloudflare独自のパブリックDNSリゾルバ1.1.1.1を使用します。1.1.1.1は世界最速で最も信頼性の高いリゾルバの1つです。）
スプリットトンネリング	プライベートネットワーキングやVPN併用のためのIPアドレスやドメインを、除外または包含します。
可視化と拡張性	
ログ	網羅的なロギングを、すべてのポートで検査されるすべてのDNSクエリ、L4ネットワークパケット、HTTPリクエストについて実施します。ログプッシュまたはAPIで、既存のSIEMツール、オーケストレーションツール、および分析ツールと統合します。管理者は全ユーザーの個人特定情報（PII）について、収集除外や墨消しを選択できます。
シャドーITの発見	エンドユーザーがインラインCASB経由でアクセスするSaaSやプライベートネットワークのオリジンを追跡、レビュー、承認します。
ページのカスタマイズ	カスタムHTTPブロックページをアップロードして、お客様のブランディングに合わせたり、より良いユーザーエクスペリエンスのための指示を伝えたりします。
自動化	直感的なAPIとTerraformプロバイダーを使って、SSE/ゼロトラスト実装のあらゆる側面をプログラム的に管理できます。さらに、ユーザーレスサービストークンで自動化サービスをサポートします。

Cloudflare SWGの導入事例

CloudflareとAccentureが、米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）のインターネットアクセスを保護

100以上 **の米国連邦政府文民省庁**
のオフィス拠点をCloudflareのDNSフィルタリングで保護
詳細を見る

スカンジナビアのIT・デジタルコミュニケーションコンサルティング会社

「私たちはCloudflareを利用して、ポートの保護、脅威のフィルタリング、トラフィックのクリーンアップを行い、攻撃対象領域を小さくしています」

— Victor Persson氏、セキュリティオペレーションリード
導入事例を読む

日本のクラウドインテグレーター兼コンサルティング会社

4,000 **週間リクエストブロック数**
有害で好ましくないインターネットコンテンツへのリクエストをブロック
導入事例を読む

競合サービスZscalerとの比較（一部項目）

評価ポイント	Cloudflare Gateway	Zscaler Internet Access
アーキテクチャ	✓ 1つのクラウドプラットフォーム、1つのコントロールプレーン	✗ 多くの断片化されたクラウド、多くのコントロールプレーン
管理インターフェース	✓ 1つのインターフェースで全SSEサービスを管理	✗ 別々のインターフェースでSWGとZTNAを管理
シングルパス検査	✓ あり 全SSEサービスが対象	✗ なし
IPv6のみのサポート	✓ あり	✗ なし
稼働率を保証するSLA	✓ 全サービスで100%	✗ たいていのサービスで99.999% DNSリゾルバでは99.9%

その他の項目におけるCloudflareとZscalerの比較

迅速な保護

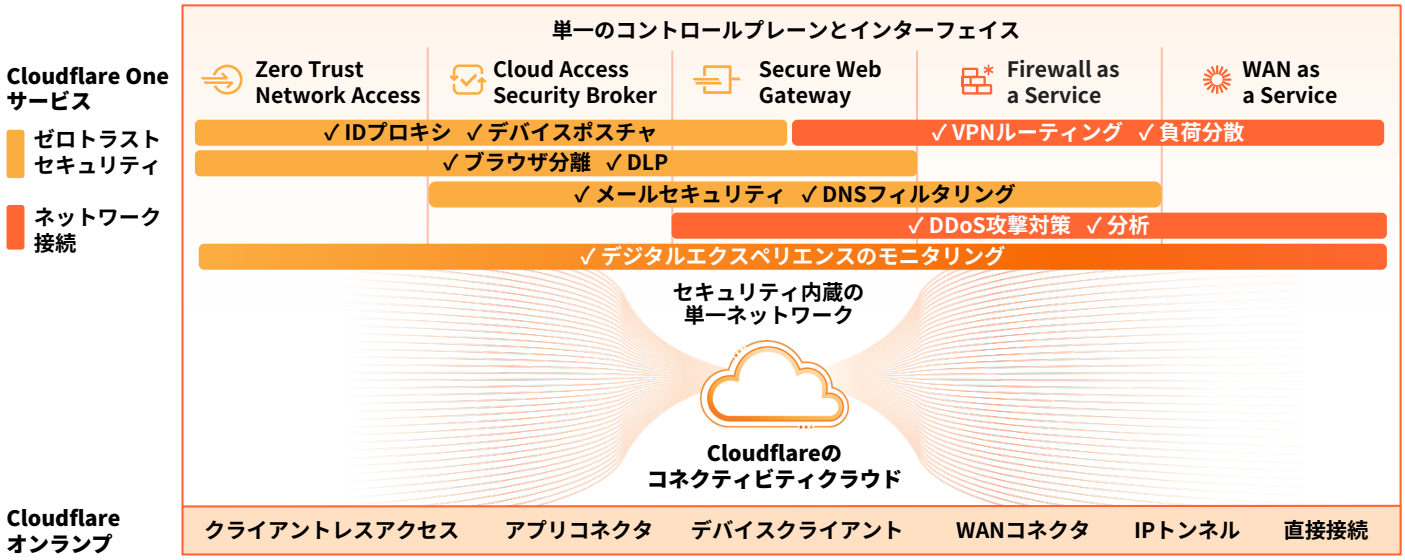
13-58%
より高速なセキュアWebゲートウェイ（SWG）

45-64%
より高速なリモートブラウザ分離（RBI）

ソース：ファーストパーティテストおよびサードパーティテスト

CloudflareのSSEプラットフォームでセキュリティを最新化

Cloudflare Gatewayは、当社のSSEプラットフォームCloudflare Oneに含まれるコンポーザブルなサービスです。Web、SaaS、非公開アプリの環境で相互運用可能なCloudflare Oneのセキュリティ機能を使って、お客様がお使いのSWGを基盤として構築し、可視性と制御を拡張します。



1つの統合プラットフォーム

- **セキュアアクセス** あらゆるリソースにアクセスするあらゆるユーザーを検証し、セグメント化
- **脅威防御** 広大なネットワークを活用したAI/MLと脅威インテリジェンスで全チャネルを保護
- **データ保護** 転送中、保存中、使用中のデータの可視性と制御を強化

1つのプログラム可能なネットワーク

- **有効性向上** 接続とポリシー管理の簡素化により実現
- **生産性向上** 環境を問わず高速で信頼性が高く一貫したUXを提供することで実現
- **俊敏性向上** 迅速なイノベーションでセキュリティ要件の変化に対応

インターネットセキュリティのアプローチを考えましょう

ワークショップを依頼する

CLOUDFLARE

担当者へのご相談前にさらに詳しい情報をご希望の場合は、

当社のSASEレファレンスアーキテクチャで詳細をご確認ください。
また、その仕組みはゼロトラストプラットフォームを説明するインタラクティブツアーでもご覧いただけます。