CLOUDFLARE

製品概要

Cloudflare Zero Trust

最速のZero Trustブラウジング・
アプリケーションアクセスプラットフォーム

境界を越えるリスク

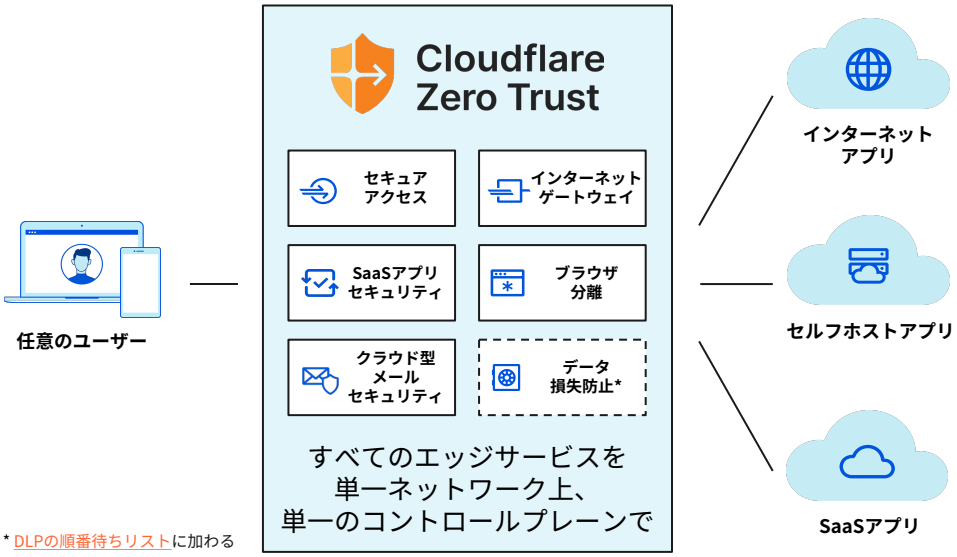
アプリケーションやユーザーが企業境界の壁から離れると、セキュリティチームはデータを安全に保つ方法について妥協しなければなりませんでした。VPN、ファイアウォール、Webプロキシなど、トラフィック保護のためのロケーション中心の対策は、重圧に耐えかねて破綻し、組織は、制限された可視性、設定の矛盾、過剰なリスクに悩まされています。

リスクはあらゆるところに存在するため、組織はクラウドで提供されるZero Trustに目を向け、適応しようとしています。

インターネットネイティブなZero Trustを採用

Cloudflare Zero Trustは、リモートユーザーやオフィスユーザーがアプリケーションやインターネットに接続する際の可視性を高め、複雑さを排除し、リスクを軽減するセキュリティプラットフォームです。シングルパスアーキテクチャで、トラフィックの検証、フィルタリング、検査を行い、脅威から分離します。

100か国以上、275以上の都市にまたがる世界最速のエニーキャストネットワークの1つで動作し、他のプロバイダーよりも高速にデプロイして優れたパフォーマンスを発揮します。



* DLPの順番待ちリストに加わる

VPNの代替
あらゆるユーザーをあらゆるリソースへ、シンプルかつセキュアに接続します

インターネットの保護
あらゆるポートとプロトコルにわたり、脅威からデータを安全に保護します

SaaSセキュリティ
メールを含むアプリケーションを可視化し制御します

セキュリティの最新化
生産性を向上、運用を簡素化、攻撃領域を縮小します

ビジネス上のメリット

過剰な信頼を抑制

アイデンティティとコンテキストベースのZero Trustルールで、アプリを保護します。ランサムウェア、フィッシング、その他のオンラインの脅威をブロックします。信頼できないWebコードをデバイスから遠く離れた場所で実行することで、エンドポイントをリスクから分離します。

複雑さを排除

レガシーポイント製品への依存を減らし、接続の開始方法やネットワークスタックの場所を問わず、すべてのトラフィックに標準的なセキュリティ管理を適用できます。

可視性の回復

DNS、HTTP、SSH、ネットワーク、シャドーITのアクティビティを包括的にログ収集します。すべてのアプリケーションのユーザーアクティビティを監視します。ご希望のクラウドストレージや分析ツールの複数に、ログを送信できます。

VPNの代替・強化 (ZTNA)

リモートユーザーとアプリケーションをより高速、簡単、安全に接続する方法

課題：低速、複雑、危険なVPN

従来のVPNは、ますます大きな負担となっています。そしてパフォーマンスの低下が、エンドユーザーの生産性を低下させます。管理者は扱いにくい設定に苦労しているのです。さらに、VPNを利用すると、マルウェアがネットワーク上で横方向に拡散しやすくなります。

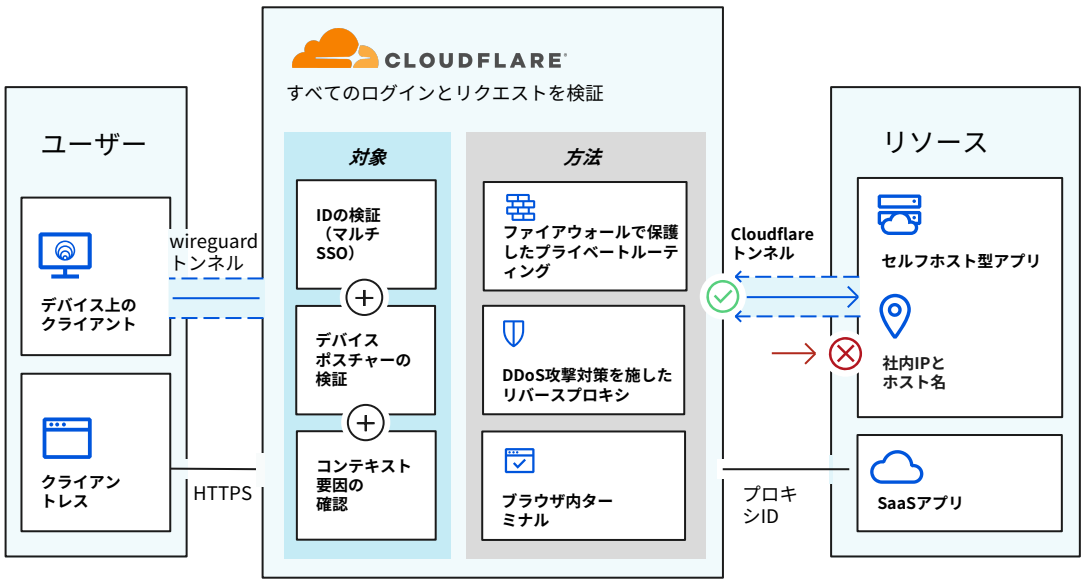
クラウドの導入やハイブリッドワークの加速により、これらの欠陥がさらに露呈し、VPNはより脆弱なものとなっています。

Zero Trust Network Access (ZTNA)

ZTNAサービスであるCloudflare Accessは、オンプレミスネットワーク、パブリッククラウド、SaaS環境において、あらゆるアプリケーションを保護し、VPNクライアントを強化または代替するものです。

Accessは、お客様のIDプロバイダーやエンドポイント保護プラットフォームと連携して、拒否をデフォルト設定とするゼロトラストルールを適用し、企業アプリケーション、プライベートIPスペース、ホスト名へのアクセスを制限します。

仕組み



クライアントレスデプロイメント
ブラウザからアクセス可能なWeb、SSH、VNCベースのセルフホスト型アプリのためのものです。

Cloudflareのデバイスクライアントを使用したデプロイ
社内IP、ホスト名、非ウェブアプリに接続します。

主なユースケース

リモートワークやBYODの取り組みを支援

ID、デバイスポスチャー、認証方法、およびその他のコンテキスト要因に基づいて、どこにいるかにかかわらず、すべてのユーザーのアクセスを検証します。

これらのZero Trustポリシーを、ハイブリッド従業員に適用します。管理対象デバイスと非管理対象デバイスの両方を保護することで、BYOD (Bring-Your-Own-Device) イニシアチブをサポートします。

柔軟性のあるサードパーティーアクセスを合理化

請負業者、サプライヤー、代理店、協力業者などのアクセス設定を迅速化します。

複数のIDプロバイダー (IDP) を一度に搭載することができます。そしてすでに使用しているIDPに基づいて、最小権限ルールを設定します。

SSOライセンスのプロビジョニング、VPNの導入、一度限りの権限の作成は不要です。

管理設定とサポートを簡素化

新しいユーザー、IDプロバイダー、Zero Trustルールを数分で追加できます。

従業員のオンボーディング時間を短縮し (eTeacher Group)、IPベースのアクセス設定から脱却することで、新たな生産性を引き出します (BlockFi)。VPNを管理するための専任スタッフを採用する必要はありません (ezCater)。

インターネット上の脅威とデータ保護 (SWG & RBI)

インターネット向けトラフィックをフィルター、検査、分離します

課題：進化する脅威の状況

ユーザーの生産性を維持しながら、セキュリティをレベルアップさせることは、決して難しいことではありません。リモートワークとは、管理されていないデバイスがより増え、機密データがより多くローカルに保存されることを意味します。一方、ランサムウェア、フィッシング、シャドーITなど、インターネットを介した脅威は爆発的に増加し、その巧妙さも増しています。

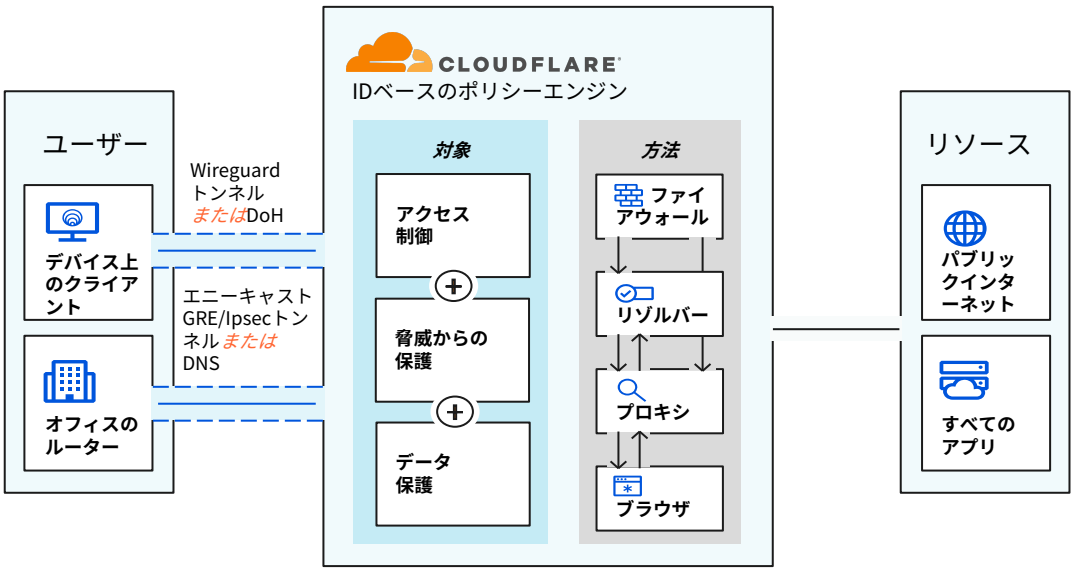
従来のポイントソリューションやデータバックアップに依存することは、次のランサムウェアの脅威から身を守るためにはリスクの高い戦略です。

SWGによるZero Trustブラウジング

セキュアWebゲートウェイ (SWG) であるCloudflare Gatewayは、IDベースのWebフィルタリングとネイティブに統合されたリモートブラウザ分離 (RBI) でユーザーを保護します。

DNSフィルタリングから始めることで、リモートユーザーやオフィスユーザーの価値実現までの時間を短縮することができます。次に、より包括的なHTTPS検査を適用し、最後にRBI制御を拡張して、すべてのインターネットアクティビティにZero Trustを採用します。

仕組み



バックホールはもう必要ありません。 L4-7トラフィックを従来のアプライアンスではなく、Cloudflare経由で送信します。

フィルター、検査、分離は、インターネット向けと内部リソース向けの両方のトラフィックに適用できます。

主なユースケース

ランサムウェアの防止

グローバルネットワークのインテリジェンスに基づき、ランサムウェアのサイトおよびドメインをブロックします。危険なサイトのブラウジングを分離し、保護を強化します。

SWGフィルタリングとRBIを、デフォルト拒否、ZTNAと組み合わせることで、ランサムウェアの感染が横方向に広がり、ネットワーク全体に権限が拡大するリスクを軽減できます。

フィッシングのブロック

既知のフィッシングドメインと、「新しい」または「新しく発見した」フィッシングドメインをフィルタリングします。ブラウジングを分離し、有害なペイロードがローカルで実行されないようにします。RBIのキーボード入力制御により、不審なフィッシングサイトへの機密情報の送信を阻止します。

さらに、近日中にArea 1を利用して、管理者がワンクリックでメールフィルタリングを有効にできるようにします。

情報漏えいの防止

ユーザーによるサイトへのファイルのアップロードを停止できる「ファイルタイプコントロール」を使用して、データ損失防止 (DLP) を実装します。

Zero Trustブラウジングをデプロイし、Webベースのアプリケーション内にあるデータを制御・保護します。そしてダウンロード、アップロード、コピーペースト、キーボード入力、印刷機能など、ブラウザ内のユーザーアクションを制御します。

SaaSセキュリティ (CASB)

SaaSセキュリティの効率化により、より少ないオーバーヘッドで可視化と制御を実現

課題：SaaSアプリの普及

現代の従業員は、かつてないほどSaaSアプリケーションに依存しています。しかし、SaaSアプリケーションはそれぞれ異なる構成で、異なるセキュリティ上の配慮を必要とし、従来ある境界の保護の外側で運用されています。

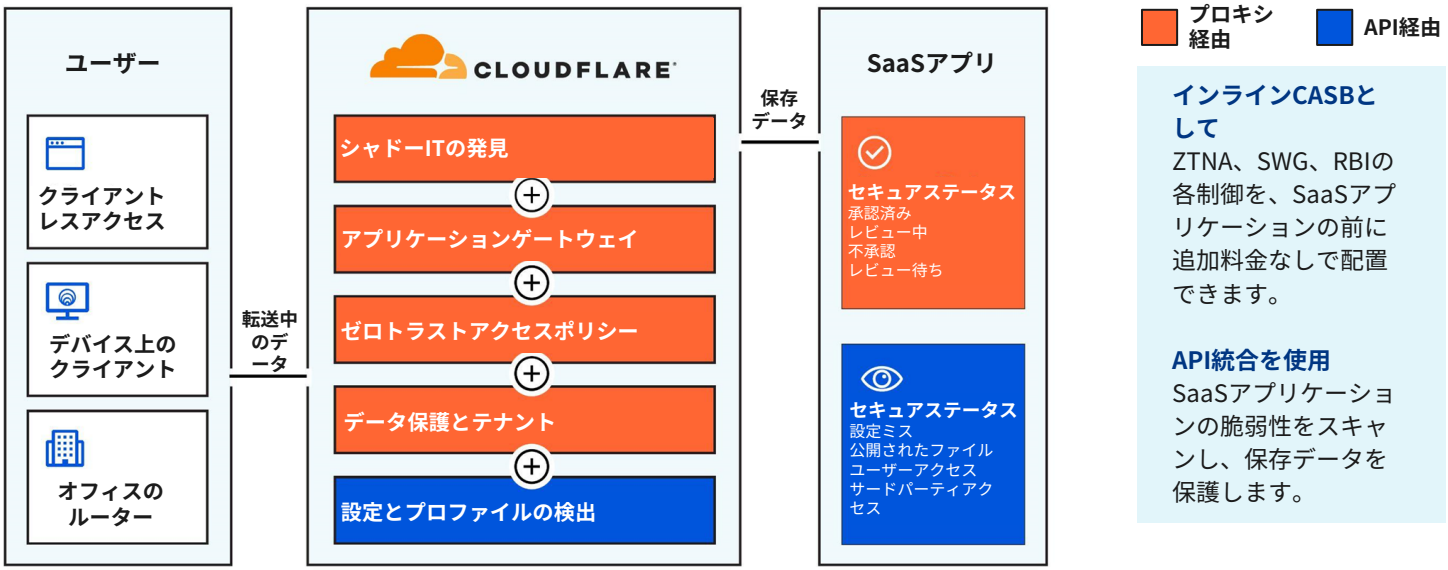
企業が何十、何百ものSaaSアプリケーションを採用するにつれ、一貫したセキュリティ、可視性、パフォーマンスを維持することがますます困難になってきています。

クラウドアクセスセキュリティブローカー (CASB)

CloudflareのCASBサービスは、SaaSアプリケーションの包括的な可視化と制御を実現し、データ漏えいやコンプライアンス違反を容易に防止することができます。

インサイダーの脅威、危険なデータ共有、悪質なユーザーをブロックします。HTTPリクエストをすべてログに記録し、無許可のSaaSアプリケーションを明らかにします。SaaSアプリケーションをスキャンして、設定ミスや不審なアクティビティを検出します。

仕組み



インラインCASBとして

ZTNA、SWG、RBIの各制御を、SaaSアプリケーションの前に追加料金なしで配置できます。

API統合を使用

SaaSアプリケーションの脆弱性をスキャンし、保存データを保護します。

主なユースケース

テナント保護・データ保護の制御を適用

HTTPゲートウェイポリシーによるテナント制御を適用することで、ユーザーが不注意または悪意を持って、一般的なSaaSアプリケーションの誤ったバージョンにアクセスしたり、データ保存したりすることを防止します。

WebベースのSaaSアプリケーション内のユーザーのアクション（コピー＆ペースト、ダウンロード、印刷など）を制御することで、データ損失のリスクを最小限に抑えることができます。

シャドーITの抑制と制御

未承認のSaaSアプリケーションによってもたらされるリスクを最小限に抑えます。

Cloudflareは、アクティビティログ内のすべてのHTTPリクエストを集約し、アプリケーションの種類ごとに自動的に分類しています。
そして管理者は、組織全体で承認済みおよび未承認の両方のアプリのステータスを設定し、使用状況を追跡できます。

新たな脅威や設定ミスの発見

一般的なSaaSアプリ（Google Workspace、Microsoft 365など）にAPIで接続し、リスクをスキャンします。

データおよび従業員を危険にさらす可能性のある権限、設定ミス、不適切なアクセス、制御上の問題を可視化することで、ITおよびセキュリティチームを強化します。

Zero Trustで近日公開：クラウドメールセキュリティ (CES)

Zero Trustをメールに拡張する

CLOUDFLARE®
AREA 1 SECURITY

2022年4月1日、Cloudflareは、メール、Web、ネットワーク環境におけるフィッシング攻撃からユーザーを保護する、クラウドネイティブメールセキュリティのリーディングカンパニーである Area 1 Securityの買収を完了しました。発表を読む。

課題：メールは最大の脅威ベクトル

メールは、チームのコミュニケーション手段としては一番の方法ですが、同時に攻撃者が侵入する手段としても一番です。実際、最近の調査では、すべてのサイバー攻撃の91%がフィッシングメールで始まることが分かっています。

メールは、ベンダー、パートナー、顧客といった組織外の人々も含め、すべての人をインサイダーにします。

結論：メールには暗黙的な多くの信頼があり、攻撃者はこれを悪用して、一般的なビジネスワークフロー（パスワードリセット、ファイル共有通知など）、または信頼できる存在（CEO、請求書を送付するベンダーやパートナーなど）になりすまします。

クラウドネイティブのメールセキュリティの統合

Cloudflare Zero TrustにArea 1メールセキュリティを追加することで、メールから暗黙的な信頼を取り除き、フィッシングやビジネスメール詐欺 (BEC) 攻撃を先制して阻止します。さらに、メール脅威ポリシーの作成と調整にかかる時間を短縮します。

送信者を決して信用しないことで、メールを含むすべてのユーザートラフィックを検証、フィルタリング、検査し、インターネットの脅威から分離します。Area 1は、高度な脅威を阻止し、プロアクティブなセキュリティ体制を採用して、フィッシングインシデントの対応時間を90%削減します。

メールセキュリティは、RBIやCASBなどと強力に組み合わせることで、当社のZero Trustサービス全体に統合されます。例えば、メールに記載されているリンクを疑わしく思うが、完全にブロックしたくないという場合はありませんか？万が一に備えて、分離されたブラウザでレンダリングし、テキスト入力をブロックします。

その仕組みとは：すべての内部ネットワーク、外部ネットワーク、Webトラフィック、メールトラフィックへのZero Trust

セキュリティの最新化：Cloudflareがもたらす違い

セキュリティ最新化のための強固な基盤

シンプルなデプロイ

Cloudflareは、組み立て可能な統一プラットフォームを提供し、容易なセットアップと運用を実現します。ソフトウェアのみのコネクタと1回限りの統合により、Cloudflareのオンランプとエッジサービスがすべて連動します。

これは、IT担当者とエンドユーザーにとって、より良いエクスペリエンスにつながります。

ネットワークの耐障害性

当社のエンドツーエンドのトラフィック自動化により、どのロケーションからでも信頼性の高いスケーラブルなネットワーク接続と一貫した保護を実現します。

Cloudflareでは、他のセキュリティプロバイダーとは異なり、すべてのエッジサービスがあらゆるネットワークロケーションで実行でき、すべてのお客様にご利用いただけるように構築されています。

イノベーションの速度

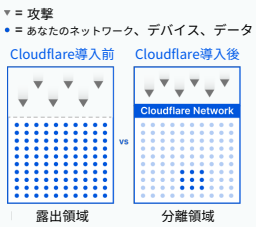
当社では将来性のあるアーキテクチャを採用しているため、新しいセキュリティやネットワーク機能を非常に迅速に構築し、出荷することができます。

新しいインターネット標準やセキュリティ標準を迅速に採用し、お客様主導のユースケースを構築するなど、当社の技術力の高さはその歴史が物語っており、当社の基盤は極めて高いオプション性を備えています。

Zero Trustがあなたのビジネスの時間とコストを削減する5つの方法

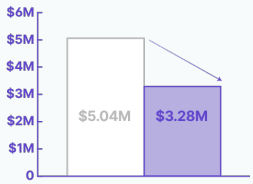
攻撃領域を縮小

91% ↓



漏えいのコストを削減

35% ↓



従業員のオンボーディングを加速

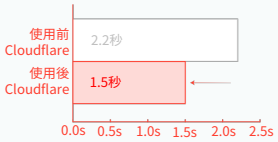
60% ↑

ITチケットの負担を軽減

80% ↓

ユーザー遅延の減少

39% ↓



ユーザビリティのための最適化

一括管理用インターフェイス

アプリケーションとインターネットアクセスの両方のポリシーに対応したダッシュボードをネイティブに構築し、設定を簡素化します。

1つのダッシュボードで、IDプロバイダー、エンドポイント保護、ネットワークオンランプと統合することができます。

単一の統合プラットフォーム

寄せ集められたVPNクライアント、オンプレミスファイアウォール、その他のポイントセキュリティソリューションを、1つのプラットフォームと1つのコントロールプレーンに置き換えます。

セキュリティをエッジに移行することで、コストと複雑さを削減します。

比類ないユーザーエクスペリエンス

Cloudflareは、あなたのユーザーやサービスの近くに位置しています。世界100か国以上、275以上の拠点からなる広大なエニーキャストネットワークで、最適化されたインテリジェンス駆動型のルーティングを利用して、リクエストを高速にルーティングします。

Zero Trust体制を加速させる

今すぐお試しください！

お問い合わせ