

プライベートルーティングでゼロトラストネットワークアクセス

ラテラルムーブメントを防ぎ、VPN への依存を減らす

アプリケーションにアクセスするために VPN や IP ロケーション制限など、ネットワークベースの制御を信頼することで、攻撃領域が広がり、可視性が制限され、エンドユーザーの満足度が損なわれる可能性があります。Cloudflare の Zero Trust ネットワークアクセスは、ご利用の ID プロバイダーおよびエンドポイント保護プラットフォームと機能します。それにより、デフォルトでアクセスを拒否し、自社アプリケーション、社内の IP スペース、ホスト名へのアクセスを制限する、Zero Trust ルールを強制的に実行します。Cloudflare の広大で効率的なエニーキャスト ネットワークにより、ユーザー接続を VPN の利用時より高速化できます。

Zero Trust ネットワークアクセスをデプロイして以来、Cloudflare で見られたメリットをご紹介します。

- 攻撃領域を 91% 縮小¹
- IT の対応業務が減り、コスト削減が倍増
- VPN 関連のチケット対応業務時間を最大 80% 短縮
- チケット量が 70% 減少
- 新入社員のオンボーディングでの能率向上により、300 時間以上を削減

Access を利用するメリット



すべてのアプリケーションを保護

Cloudflare は ID とアプリケーションのどちらにも依存せず、お好みの ID プロバイダーを使って、SaaS、クラウド、オンプレミスのあらゆるアプリケーションを保護できます。



社内リソース間でのラテラルムーブメントを阻止

レガシーアプリにさえ、IP ファイアウォールと Zero Trust のルールを設定した強力で一貫性のある認証方法を適用します。



クライアントの有無を問わず、ユーザーを柔軟に接続

クライアントソフトウェアやエンドユーザー側の設定は不要で、Web アプリケーションの接続や SSH 接続が容易になります。Web 以外のアプリケーションや RDP 接続、プライベートルーティングでは、インターネットやアプリケーションアクセスのユースケースすべてに 1 つの包括的クライアントを使います。



デバイス認識型のアクセスを適用

リソースにアクセスを許可する前に、ゲートウェイクライアントやシリアル番号、mTLS 証明書が存在など、デバイスポスチャースIGNAL を評価し、お客様のリソースにアクセスできるデバイスを安全で既知のデバイスだけに限定します。CrowdStrike、Carbon Black、Sentinel One、Tanium などの Endpoint Protection Platform (EPP) プロバイダーから提供されるデバイスポスチャーを統合します。



複数の ID プロバイダーを連合アイデンティティに

ご利用の企業 ID プロバイダー (Okta、Azure AD など) をすべて統合して、移行、調達、サードパーティのユーザーアクセスをより安全にします。一時的なアクセス用にワンタイム PIN を有効化、または、LinkedIn や GitHub といったソーシャル ID ソースを統合します。



すべてのアプリでユーザーアクティビティをログに記録

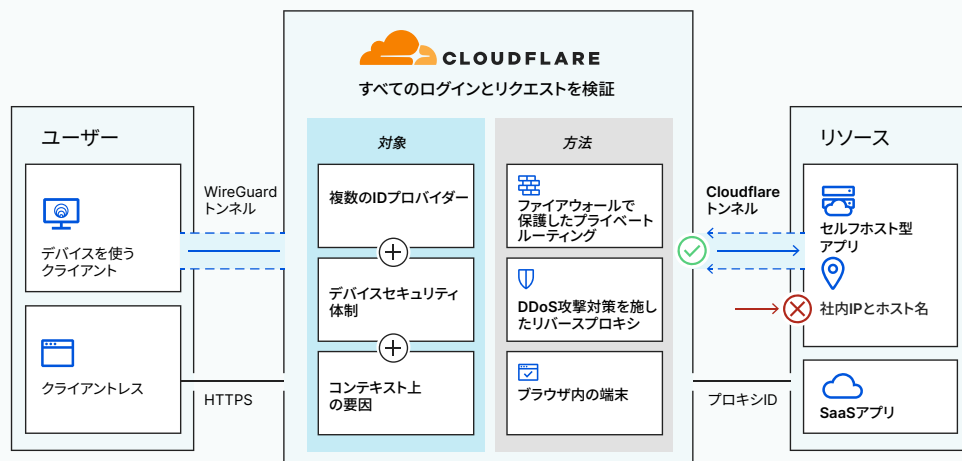
保護されたアプリケーションで行われたリクエストをすべて記録します。ログインとログアウトだけではなく。Cloudflare のアクティビティログを集約するか、SIEM プロバイダーにエクスポートします。

¹Zero Trust ネットワークアクセスがインターネットのブラウジングに導入された場合

Cloudflare の違い

- **すべてを卓越したパフォーマンス**により、リクエストをより高速にルーティングします。さらに、Cloudflare のエニーキャストネットワーク全体で、最適化された、インテリジェンス主導型のルーティングが適用されます。平均で Web アプリのアクセス速度が 30% 高速化、TCP 接続ではラウンドトリップタイムが 17% 減少しています。Cloudflare のインテリジェンスは、1 秒あたり 2500 万件の HTTP リクエストと、1 秒あたり 3 万 9000 件の新規 TCP 接続のネットワークデータ分析がもとになっています。
- **よりシンプルな管理**で Zero Trust ネットワーク、Secure Web Gateway、リモートのブラウザ分析、その他の機能を 1 つのコントロールプレーンへと統合。また、管理機能は複数のベンダーから取得して継ぎ合わせたものではなく、一から構築されています。
- **単一パスの検査**がトラフィックを世界中でスピーディに検証、フィルター、検査します。これを可能にしているのが、世界 250 都市以上のロケーションに広がる全データセンターにデプロイされた Cloudflare サービスです。

仕組み



ユーザーは、VPN ではなくクライアントまたは Web ブラウザを介して企業リソースに接続します。リクエストは、Cloudflare のエッジ経由でルーティングされ高速処理される際に、ID プロバイダーやデバイス、その他のコンテキストからの信号を組み入れた Zero Trust ルールに照らして評価されます。かつては、RDP ソフトウェアや SMB ファイルビューア、その他のシッククライアントプログラムをプライベートネットワークに接続するには VPN が必要でしたが、今では Cloudflare のネットワークを介してあらゆる TCP トラフィックをプライベートにルーティングすることができます。トラフィックは、Cloudflare ネットワーク上で高速化、検証され、シングルパスでフィルタリングされるため、パフォーマンス向上とセキュリティ強化につながります。

「Cloudflare Access によって、当社独自の IAM (Identity and Access Management) システムを開発する必要がなくなりました。Access で保護されるアプリにユーザー許可機能を構築する必要もありません。私たちは「オールイン」を選びました。社内の全員に「座席」を設けたのです。」

Jim Tyrrell 氏
Canva、インフラストラクチャ責任者



「Delivery Hero では、常にお客様に素晴らしい体験をお届けできるように努めています。Cloudflare Access は、社内チームも同様に支援してくれます。安全な労働環境を提供し、世界中の当社のすべてのアプリケーションにアクセスするために、VPN も必要ありません。」

William Carminato 氏
Delivery Hero、エンジニアリング、シニアディレクター

Delivery Hero

IAM（ID とアクセスの管理）の統合

 Active Directory
  okta
  Google Workspace
  Ping Identity
  citrix
  Centrify
  onelogin
  SAML OIDC

エンドポイント保護プラットフォーム（EPP）の統合

 CROWDSTRIKE
  vmWare Carbon Black
  SentinelOne
  TANIUM

主な機能

📋 一貫したポリシー	
カスタムアプリケーション、プライベートネットワーク、インターネットアクセスポリシー	無制限
企業 IdP とソーシャル IdP による認証	✓
サードパーティ統合と Cloudflare を使用したデバイスポスター	✓
自社デバイスのシリアル番号リスト用に CSV ベースのバルクインポート	✓

👁️ 可視性を高める	
アクティビティログの保持	6 か月間
ID ベースの国、州、デバイスの詳細ビュー	✓
ログをクラウドストレージまたは SIEM ヘブッシュ	✓

🔒 セキュアな接続	
インターネットへのクライアントベースの暗号化接続（WARP クライアント）	Win、Mac、iOS、Android
セルフホストアプリケーションや SaaS アプリケーションへのクライアントレスでセキュアなアクセス	✓
セルフホスト型アプリケーション、社内 IP、ホスト名のプライベート接続（Cloudflare Tunnel）	✓

🔗 シンプルな相互運用性	
エンドポイントとモビリティの統合管理	✓
ローカル接続または VPN 接続用のスプリットトンネリング	✓
管理対象外デバイスのクライアント自己登録機能	✓
カスタマイズ可能なアプリランチャー	✓
認証は複数 ID プロバイダーを同時にサポート	✓
SAML と OIDC に対応した汎用コネクタとカスタムコネクタ	✓
自動サービスのためのトークンベースの認証	✓
IoT およびその他の mTLS ユースケースの証明書ベースの認証	✓

🚀 パフォーマンス上の妥協は一切なし	
稼働率を保証する SLA	100%
最速級のネットワーク（250 超の PoP から 50ms 以内の距離）	✓
最速、プライバシー優先の DNS リゾルバ（250 超の PoP で 7 ~ 31ms）	✓
超高速のポリシー更新（250 超の PoP へ 500ms 以内）	✓
超高速のリモートブラウザ（ピクセルプッシュなし、サードパーティクラウドではなく独自のネットワークで稼働）	アドオン

さらに詳しい情報をご希望ですか？

こちら www.cloudflare.com/ja-JP/products/zero-trust/access/ にアクセスして、アカウントを作成してください。50 ユーザーまで無料でご利用いただけます。