CLOUDFLARE

ソリューション概説

クラウド環境およびオンプレミス環境のインフラへの特権アクセス

開発者の作業を妨げることのない、認証・認可・監査を簡素化した、インフラストラクチャへのスムーズなアクセスを提供します。

過剰な権限の問題

多くの企業がアプリやネットワークへの安全なアクセスを近代化するZero Trustイニシアチブを導入していますが、インフラセキュリティや特権アクセス管理（PAM）戦略は依然としてサイロ化されたままとなっており、これが複雑さ、または非効果化の要因となっています。

- **リスクが高すぎる：**有効期限が長い鍵や共有鍵は厄介な存在となり、過剰な権限やラテラルムーブメントに関連するリスクが増大
- **操作が煩雑すぎる：**手作業による認証情報のローテーション作業、可視性の低さにより、管理者の生産性が損なわれる

Zero Trust制御をインフラに拡張

レガシーであるPAMツールを採用したり、自社開発のサーバーアクセスや鍵の管理ソリューションを構築する代わりに、現在のチームの考え方をそのままZero Trustネットワークアクセス（ZTNA）および関連するVPNの代替案に流用することができます。

アプリと同じ方法でインフラへのアクセスを検証—既存のIDプロバイダーグループを活用し、SSO、MFA、デバイスコンテキストを使用してポリシーを構築し、適切なユーザーのみが適切なインフラストラクチャリソースにアクセスできるようにし、途中のすべてをログに記録します。

Cloudflareの統合型アプローチ

特権アクセスとZTNAの融合

Cloudflareは、現代のIAMツールと細かな文脈に基づく検証を、他のセキュアアクセスサービスエッジ（SASE）ベンダーよりもさらに広げる集約レイヤーとして機能します。これにより、以下のことが実現します。

- VPNの置き換えの範囲を、組織のアプリやネットワークだけでなく、最も機密性の高いインフラリソースにまで拡大
- 特権的な開発者用アクセス権と一般的な従業員/請負業者のアクセス権を統合することで総所有コストを削減

Cloudflareでインフラへの特権アクセスを近代化

リスクの軽減

セキュアシェル（SSH）鍵の漏洩を防止し、インフラが危険にさらされる可能性のある過剰権限のリスクを排除します。

業務を効率化

シンプルできめ細かいポリシーエディターと監査ロギングを内蔵し、従来のPAMやDIソリューションの複雑さを回避します。

開発者の作業をサポート

Zero Trust制御を導入し、開発者、DevOps、サイト・リライアビリティ・エンジニアリング（SRE）チームの本来の作業を妨げることのない環境を提供します。

アーキテクチャの概要

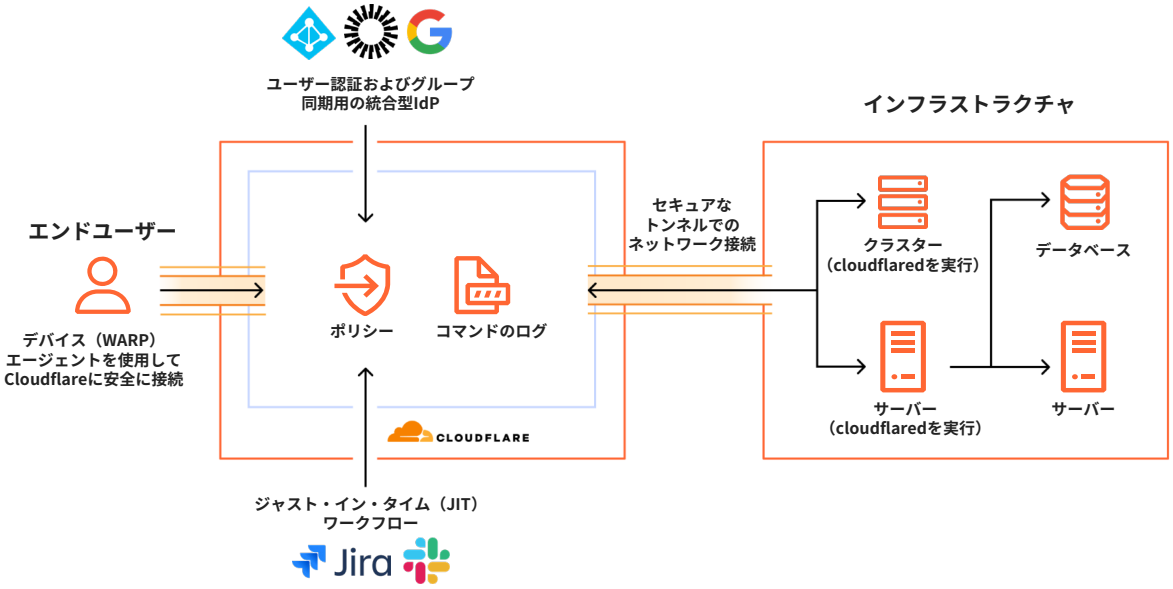

図1： BastionZeroから取得したテクノロジーがCloudflareのZTNAサービスにネイティブに再構築される様子を示しています。現在サポートされている機能の一覧については、Access for Infrastructureの技術文書を参照してください。

動作の仕組み

ネットワークではなく、ターゲットへの特権アクセスを認証、許可、監査

- 対象機器に対してZero Trustアクセスポリシーを作成し、利用するポート、プロトコル、ユーザー接続コンテキスト（*ルート*または*ec2-user*）を指定します。
- 特別なCLIやコマンドを使用せずに既存のワークフローに合わせるため、開発者が戸惑うことはありません。
- シングルサインオン（SSO）、多要素認証（MFA）、デバイスポスチャー、その他のコンテキストを使用して認証します。
- 明確な可視性とすべてのエンドユーザーコマンドをログに記録することで、コンプライアンス監査の要件をサポートします。

インフラアクセスにCloudflareを選ぶ理由

市場で最も包括的なZTNAソリューション

他のSSE/SASEベンダーは、これほどインフラアクセスに対してDevOpsフレンドリーなZero Trust制御を提供していません。さまざまなインフラアクセスの仕組みを提供するスタートアップ企業は、単に別のポイントソリューションを売り込むだけです。

CloudflareのZTNAサービスは、企業のレガシーPAMや自社製のサーバーアクセス機能から、より広範なVPNの置き換え、あるいはSASEアーキテクチャへの移行を支援します。これらすべてを世界最大級の規模、速度、信頼性を誇るネットワークの1つであるCloudflareのコネクティビティクラウドが実現します。

この機会に詳細をぜひご覧ください。ステップバイステップの技術文書をご覧いただくか、お問い合わせをご依頼ください。