CLOUDFLARE®

請負業者のアプリケーションアクセスを保護するためのゼロトラストガイド

+81 3 4510 1893 | enterprise@cloudflare.com | www.cloudflare.com/ja-jp/

CLOUDFLARE

I. エグゼクティブサマリー

契約社員、代理店、提携企業など、会社の外の共同作業者にアプリケーションアクセスを提供することは、セキュリティリスクと物流上の深刻な問題となる可能性があります。最新型のアプリケーションの多くは、旧式のIDやアクセス管理の（IAM）プラットフォームとの互換性がありません。
このため、間に合わせのシステムに頼ることを余儀なくされていますが、これは管理が大変です。

ゼロトラストネットワークアクセスは、これらの課題を克服するために、ビジネスに必須のアプリケーションに最小権限の原則を適用する方法です。最小権限の原則を各アプリケーションに適用することで、暗号化された接続トンネルの後ろにアプリケーションを隠し、すべてのリクエストを記録します。これにより、企業はIAMに関わるプロセスをシンプル化することができ、貴重な開発のための時間を増加させ、さらにデータ損失の可能性を大幅に削減できます。

PART 1

最小権限の原則：目標と課題

アクセス制御は、エンタープライズセキュリティプログラムの最も基本的な目的の1つです。独自のデータ、重要なシステム、製品品質を保護するために、セキュリティリーダーは最小権限 (POLP) の原則を実装させるべく尽力しています。POLP（最小権限）では、ユーザーは自分の仕事を実行するために必要なリソースにのみアクセスでき、そのアクセスは、それが必要な期間に限定されます。

この目標は、請負業者、ベンダー、提携企業、およびその他の信頼できる第三者の場合に特に重要です。これらのユーザーは、多くの場合、特定のタスクやプロジェクトの完遂を目的として召集されるため、特に慎重なアクセス管理が必要です。

理論的には、IAMプラットフォームは、次のような状況でPOLPを実装する企業を支援します。

- 既知のユーザーリストを定義する (ディレクトリ)
- 定義された基準（認証）に基づいてアクセスを円滑に進める
- 権限をアクセス可能なものに制限する（認可）
- 特定のリソースへのアクセスの定期的な調整 (ライフサイクル)

残念ながら、IAMの実態は異なるように見えることが多々あります。以下では、これらの目標を達成するための課題をいくつか説明します。

課題1：多様なアプリケーションを1つのIAMシステムに統合する

多くの大企業では、複雑で異種混合のアプリケーションおよびインフラストラクチャ環境を運用しています。
一部のサービスとしてのソフトウェア（SaaS）およびオンプレミスのアプリケーションは、IAMプラットフォームの標準ベースの認証方法に適していますが、アプリケーションの多くは、これらのプラットフォームとの統合が困難、または不可能です。Gartnerは、現在、シングルサインオントランザクションのわずか30%のみが最新のアイデンティティプロトコルを使用していると見積もっています。例としてSAML、OAUTH2、OIDC 1が挙げられます。その他の非標準トランザクションの70%では、従来の IAMプラットフォームとの統合が簡単ではないレガシープロトコルやカスタムフレームワークが含まれており、セキュリティを確保するためには余計な時間と開発作業が必要です。後者のカテゴリに分類される一般的なアプリケーションは次のとおりです。

- **社内でホストされるアプリケーション** (社内で開発されたプライベートアプリとプライベートでホストされるクラウドアプリを含む)
  - Atlassian アプリ
  - Drupal
  - Grafana
  - JIRA
  - Splunk
  - DataDog
  - Gitlab
  - Bitbucket
- **インフラストラクチャ**
  - Amazon Web サービス (AWS)
  - Google Cloud Platform (GCP)
  - Microsoft Azure

これらの問題点を克服するために、企業は通常、次のアプローチに頼っています。

メソッド	課題とリスク
一元型IAMプラットフォームで機能しないアプリケーションの場合、管理者はユーザーネームとパスワードを分けています。	企業には、管理、オンボード、およびオフボードを行わなければならない別のユーザーIDセットを持つことになります。
バーチャルプライベートネットワークを介してアプリケーションを配信します（VPN）。	ユーザーにVPNを使用したアクセスやリモートVPNエージェントを使用したアクセスを提供するには、ネットワークファイアウォールに穴を開けなければなりません。
シングルサインオン (SSO) を有効にするために、プライベートアプリケーションサーバーでカスタムソフトウェアを構築し、保守します。	開発者の継続的な努力が必要で、企業はそれを割り当てなければなりません。

課題2：サードパーティユーザーが独自の複雑さをもたらす

外部ユーザーは、さらなる課題をもたらします。これらのユーザーはリモートまたは一時的な作業を行うことが多いため、セキュリティリーダーは、通常、次のアプローチに頼らざるを得ません。どちらのアプローチも実装が難しく、安全でない可能性があります。

メソッド	課題とリスク
一元型IAMプラットフォームで機能しないアプリケーションの場合、管理者はユーザーネームとパスワードを分けています。	• 企業には、管理、オンボード、およびオフボードを行わなければならない別のユーザーIDセットを持つことになります。
バーチャルプライベートネットワークを介してアプリケーションを配信します（VPN）。	• ユーザーにVPNを使用したアクセスやリモートVPNエージェントを使用したアクセスを提供するには、ネットワークファイアウォールに穴を開けなければなりません。
シングルサインオン (SSO) を有効にするために、プライベートアプリケーションサーバーでカスタムソフトウェアを構築し、保守します。	• 開発者の継続的な努力が必要で、企業はそれを割り当てなければなりません。

課題2：サードパーティユーザーが独自の複雑さをもたらす

外部ユーザーは、さらなる課題をもたらします。これらのユーザーはリモートまたは一時的な作業を行うことが多いため、セキュリティリーダーは、通常、次のアプローチに頼らざるを得ません。どちらのアプローチも実装が難しく、安全でない可能性があります。

メソッド	課題とリスク
サードパーティユーザーへのVPNの貸与	• 新規ユーザーの支援にはコストと時間がかかります。請負業者への物理的な機械の発行が必要な場合は特にこの傾向があります。 • ユーザーが接続してから、ラテラルムーブメント（lateral movement）を起こす リスクがあります。 • データ流出のリスクがあります。ユーザーが個人を特定できる情報（PII）をパソコンに保存できるためです。
サードパーティユーザーのための企業ユーザーIDの作成	• ユーザーアカウントを適切なリソースにプロビジョニングするのは手動による作業で時間もかかります。 • 企業は、アカウントのオンボーディング、オフボーディング、権限の管理を担当しなければならなくなり、ID管理プラットフォームを担当する人員も確保しなければなりません。 • 人事部門やIT部門などの部門間のやり取りが増える。
IAMプラットフォームを、サードパーティによって管理される既存のプラットフォームに接続する	• プラットフォームを統合し、一度限りの許可ルールを作成するプロセスは時間がかかる。 • プラットフォーム間の潜在的な非互換性。 • 個人のサードパーティーにとっては、実現が難しい。

PART 2

ゼロトラストネットワークアクセスの利点

ゼロトラストネットワークアクセス（ZTNA）は、これらの課題を克服するためのフレームワークです。これは次のような考えの下で運営されています。 企業は、その境界の内側または外側にかかわらず、あらゆるユーザーまたはデバイスを、片時も信頼してはいけません。 サードパーティのアクセスに関するセキュリティ上の懸念を軽減するには、社内リソースへのアクセスは、全般的な許可ではなく、特定のものに限定されるべきです。

ゼロトラストネットワークアクセスは、次の方法でこれを達成します。

- 社内アプリケーションをバーチャルプライベートネットワークから切り離し、それぞれの周囲にロジカルなアクセス境界を作り出します
- アプリケーションを暗号化された接続トンネルの背後に隠します
- 可視性の向上のために、社内リソースに対して行われたすべてのリクエスト（認証要求とアプリケーション自体へのリクエスト）を記録します

これらの手順により、企業は既存のIDプロバイダーに実装したきめ細かなアクセス制御を社内管理アプリケーションやインフラストラクチャに適用できます。企業は、また、サードパーティユーザーにアプリケーションレベルで社内リソースへのアクセスを許可したり、複数の組織のユーザーに社内IDで社内にホストされているリソースへのアクセスを許可したりできます。

以下に、このフレームワークを適用する際の例を示します。

ゼロトラストネットワークアクセスのサンプル事例

新しいアプリやサービスの開発は共同作業であり、多くの企業では、請負業者と正社員を組み合わせたチームで新しい製品を開発しています。企業の開発アプリケーションや環境の保護は、次のような場合に困難になります。

- 企業に、SSHアクセスが必要な業務上重要なインフラストラクチャ（バーチャルプライベートクラウドなど）やアプリケーション（BitBucket、Gitワークフローなど）がある場合。
- プロダクトチームが、他の国々を含めて部分的にリモートで働いている場合。
- リモート開発者は、VPN経由で開発環境やアプリケーションにアクセス権限を持つため、これが接続速度を低下させる原因や、追加のリスクを招く原因にもなります。

ゼロトラストネットワークアクセスは、次の方法でこれらの課題に対処できます。

1. 業務上極めて重要なインフラストラクチャへのリモートアクセスの保護インフラストラクチャ
2. 開発サイトとステージングサイトを本番環境に移行する前にロックダウン
3. 開発者にとって重要な他の社内アプリケーションを保護（例：GitHub、Jira）

PART 3

企業でのゼロトラストネットワークアクセスの実装

ゼロトラストネットワークアクセスは、信頼できるサードパーティユーザーが社内アプリやリソースにアクセスできるようにするためのプロセスを保護し、高速化します。一度実装すれば、サードパーティがアプリケーションにアクセスするためにVPNを使用する必要はありません。代わりに、企業が定義した認証プロセスを使用してログインできるようになります。

ログイン体験の変更は、ユーザーに大きな影響を与えます。これを正しく行うには、チーム間のコミュニケーションと計画が必要です。成功するプログラムでは、多くの場合、最初に小さな試験的なユーザーグループを設定して、1つのターゲットアプリケーションを決めることからはじめています。社内で管理されるアプリケーションのインデックスを作成し、請負業者やその他の外部当事者がアクセスする必要があるアプリケーションを特定しておくことをお勧めします。

このインデックスを使って、テストグループでZTNAで試験的に実施するアプリケーションを1つ特定します。
次の基準を満たすアプリケーションが優先されます。

- Webアプリケーション
- HTTPSを使用するアプリケーション
- 既存のSSOプロバイダーでは保護されないもの
- 会社全体の5〜10%で使用されているもの

このようなインデックスの例を次に示します。

アプリケーション/リソース	アクセスするユーザー	現在のオンボーディングプロセス	影響を受けるユーザー数	ZTNAパイロットへの適合性 (1-5)
Grafana	社内 - 経理部 社外 - コンサルタント	Azure AD + VPN	45	4
Drupal	社内 - マーケティング、サポート 社外 - 海外開発	Azure AD + VPN	1000	3
JIRA	社内 - 全部署 社外 - 複数の契約チーム	Azure AD + VPN	10,000	1

適切なパイロットアプリケーションおよび請負業者のユーザーグループを特定し、アプリケーションを適切なサイズでテストした後、請負業者のシステムへのアクセスを識別および確認する方法を検討します。ZTNAに強力なベンダーパートナーを選択した場合、パートナーへのアクセスを提供する方法について複数の選択肢があります。

オプション 1：請負業者がそれぞれの企業のSSOプロバイダーでログインできるようにする

貴社と協力関係にある外部企業がSSOでそれぞれの社内アプリケーションへのアクセスを管理している場合、請負業者のコーポレートアイデンティティをそのまま貴社のアプリケーションのログインに使用できるようにすることもできます。

このアプローチは、次の場合に適しています。

- 貴社のSSOとパートナー企業のSSO間のフェデレーションの確立に時間を費やせる場合。
- 請負業者のSSOに実装されている多要素認証 (MFA) などのセキュアなアクセスポリシーを利用したい場合。
- 請負業者が貴社から離れた場合、請負業者のIDのライフサイクルを管理する必要はありません。IDはユーザーが請負業者の企業ディレクトリにある場合にのみ有効です。

使用事例

1. A社から来たホセは、SSOを使用して、A社のユーザー名とパスワードで、CRMプラットフォームにログインします。
2. 貴社のアプリケーションにログインしようとすると、会社Aのログインページにリダイレクトされ、会社の認証情報を使ってログインするよう求められます。
3. ホセがSSOによって検証され、ZTNAプラットフォームでアプリケーションアクセス権が与えられている場合、彼はアプリケーションにアクセスできます

オプション 2：Eメールのワンタイムpinを使用したパートナーログインを提供する

特定のアプリケーションへのアクセス権を請負業者に共有する必要があるが、別の組織のIDプロバイダー (IDP) とのフェデレーションを確立したくない場合は、メールのワンタイムPIN (OTP) がシンプルな認証方法です。このアプローチにより、企業は、メールアドレスのシンプルなリストを使用して請負業者グループへのアプリケーションアクセスを許可し、サービスにログインする必要があるたびに、ユーザーのメールアドレスに一意のログインコードを配信します。

このアプローチは、次の場合に適しています。

- 請負業者に法人IDPアカウントを発行したくない場合
- 請負業者の企業SSOとのフェデレーションを確立したくない場合
- メールアクセスが、アプリケーションアクセスにとって適切な信頼レベルであると考える場合
- 複数の企業の請負業者と共同作業している場合

フローの例：

1. B社から来たカレンは、貴社のマーケティングチームと協力して、新しいランディングページの制作に取り組んでいます。ステージングサイトは貴社のCMSでホストされています。
2. カレンがデザイン作業のためにCMSにアクセスする際、彼女はメールアドレスを入力するように求められます。
3. メールをチェックすると、アクセスに必要なログイン画面にコピー＆ペーストできるコードを取得できました。

オプション 3：合意されたソーシャルIDを使用する

場合によっては、GitHub や LinkedIn などのソーシャル IDプロバイダーを使用して、請負業者に貴社のアプリケーションへのアクセスを許可すること検討した方がいい場合もあります。

このアプローチは、次の場合に適しています。

- 社内ID管理システムを使用しない小規模な会社のユーザーとコラボレーションしている場合
- 請負業者が複数の会社に渡っていて、認証するには、共通のフレームワーク（GitHub、LinkedIn）が必要な場合

フローの例：

ロバートは、貴社の開発チームと協力して新しいモバイルアプリケーションの品質管理に取り組むベンダーです。彼が貴社のWebアプリケーションにログインしようとすると、LinkedIn のログイン画面にリダイレクトされました。LinkedIn のログインに成功すると、貴社のアプリケーションにアクセスできるようになります。

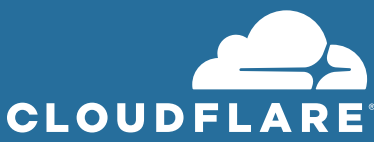
Cloudflareがゼロトラストネットワークアクセスの実装にどのように貢献するか

Cloudflare for Teamsは、企業のデバイス、ネットワーク、および社内アプリケーションの保護を支援するCloudflareの製品です。オープンなインターネット上の貴社のチームの接続を保護し、高速なアクセスを提供します。
また、アプリケーションへのユーザーアクセスを制御し、ゼロトラストアーキテクチャを採用することもできます。

詳細について、および当社のチームに連絡するには、teams.cloudflare.comをご覧ください。

巻末注

1. アクセス管理のためのMagic Quadrant 2019 Gartner、https://www.gartner.com/en/documents/3956209/magic-quadrant-for-access-management,2020年2月24日にアクセス



+81 3 4510 1893 | enterprise@cloudflare.com | www.cloudflare.com/ja-jp/

改訂版：200318