CLOUDFLARE

ソリューション概要

# ワークフォースによる生成AIやエージェンティックAIの利用を保護

Cloudflare SASEプラットフォームの保護機能によりどんなAIツールでも安全に利用可能


## コントロールの回復と生産性の向上

AI導入を急ぐことが、データ漏洩、規制違反、攻撃対象領域の拡大といったリスク増大の要因となっています。AIの全面禁止は競争力を損うだけですし、ポイントソリューションを試しても複雑さが増すだけです。

Cloudflareは、AI環境全体にわたる可視性の拡張、リスクの軽減、データの包括的な保護を通じて、お客様の組織におけるAIの利用を保護します：

- **シャドーAIを検出**し、認可および未認可のすべてのAIツールに関するポリシーを管理します。
- IDベースのアクセス制御とポスチャ管理により、**AIガバナンスを強化**します。
- ユーザープロンプト内の機密情報をブロックし、トピックガードレールを適用し、スキャンでAIツールの設定ミスを検知することによって、**データ損失を阻止**します。

利用を特定のアプリケーションに限定するか、多様なツールを広く試すか、いずれのAI戦略をとる場合も、Cloudflareを拡張してAIを安全に導入できます。

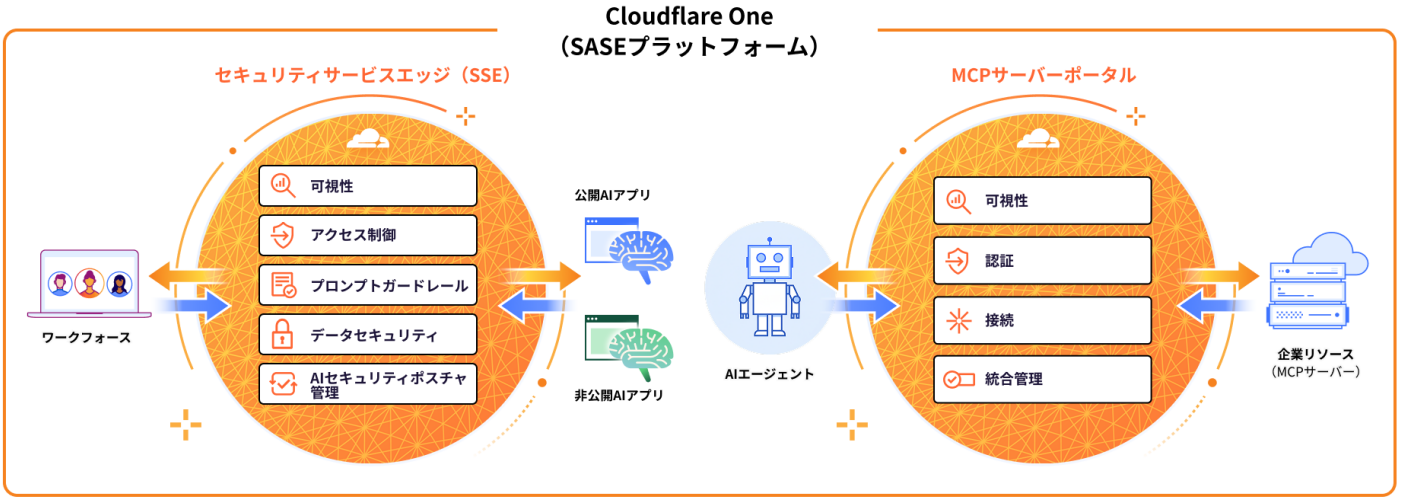
### ワークフォースのAI利用をSASEで保護する理由

Cloudflareのセキュアアクセスサービスエッジ（SASE）プラットフォームは、ワークフォースとAIツールの間に位置します。このため、SASEは多くの人にとって、AIを安全に使い始めるための理想的な出発点となります。

従業員がChatGPTとチャットする場合も、AIエージェントが企業リソースから情報を収集する場合も、CloudflareのSASEプラットフォームは一貫したセキュリティ制御を適用します。

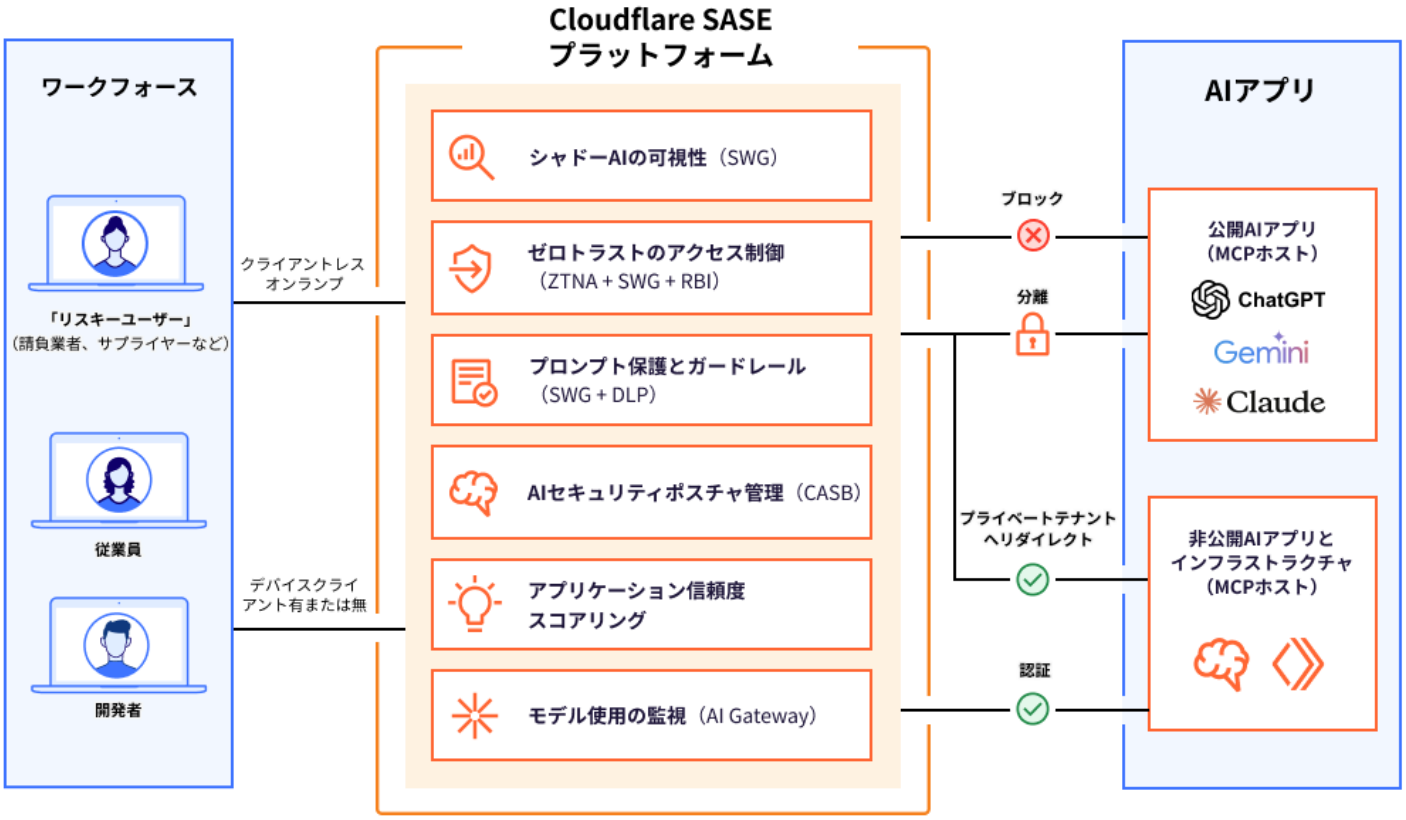
## 生成AIやエージェンティックAIとの通信を保護

CloudflareのSASEプラットフォームなら、単一の統合ダッシュボードとコントロールプレーンで、組織全体における人間とAI、マシンとマシンの両方のやり取りを管理できます。




Cloudflareは他のSASEベンダーと異なり、外部公開されたAI対応のアプリやワークロード（WebサイトのAIチャットボットやレコメンドエンジンなど）への接続と保護もサポートします。

# Cloudflare SASEプラットフォームのAI利用制御で、**ユーザーと生成AIアプリの通信を保護**




- **可視性：**インライントラフィック検査で、シャドーAIの利用を検知し、分析します。透明性の高いスコアリングで、AIアプリがもたらすリスクを評価します。
- **アクセス制御：**ユーザー接続をブロック、分離、リダイレクト、または許可します。アプリごとに、IDベースのゼロトラストルールを適用します。
- **プロンプト保護とガードレール：**ユーザープロンプトを検出し、意図（ジェイルブレイク試行、コードの不正使用、PIIの引き出しなど）に基づいてブロックします。
- **データセキュリティ：**AIを活用したデータ損失防止（DLP）によってPII、ソースコードなどを検出し、機密データの露出を阻止します。
- **AIセキュリティポスチャ管理：**生成AIツールとAPI連携し（現在、ChatGPT、Claude、Google Geminiと可能）、当社のクラウドアクセスセキュリティブローカー (CASB)でスキャンして設定ミスを検出します。

## お客様の成果

**indeed**
世界No.1の求人Webサイト

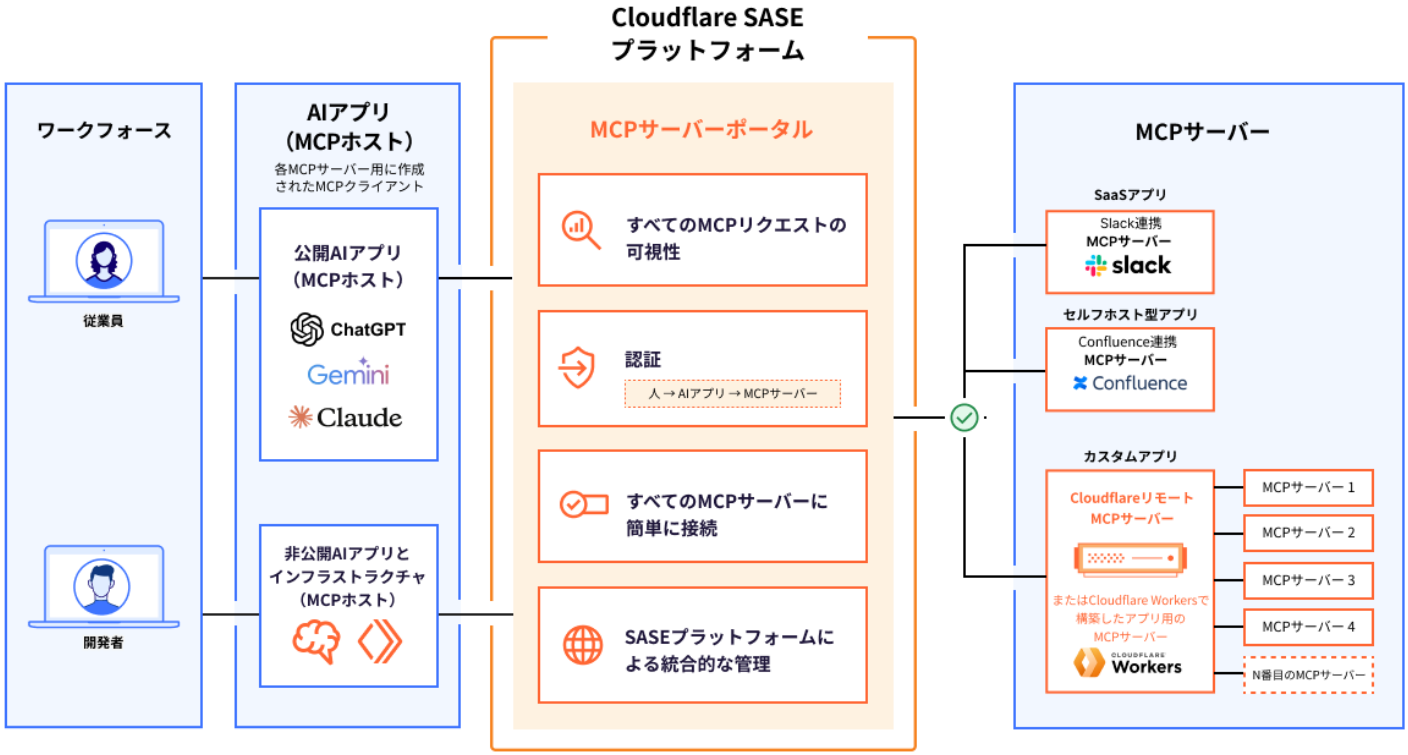
VPN代替プロジェクトと並行して**シャドーAIの特定と制御**を実施

**APPLIED**
保険テクノロジー

**ChatGPTのような公開生成AIツールを隔離し、**機密データのコピー＆ペーストをブロック

# Cloudflare SASEプラットフォーム上のMCPサーバーポータルで、**エージェンティックAIの通信（AIからリソースへ）を保護**




- **可視性：**監査・分析用に、すべてのMCPリクエストのログを集計します。MCPサーバーをポータルに追加する前に、レビューと承認を行います。
- **認証：**ポータルへのユーザーアクセスを、IDに基づいて認証します。最小特権の原則に基づき、MCPサーバーへのアクセスを制限します。
- **接続：**個々のMCPサーバーを設定するのではなく、アクセス可能なすべてのMCPサーバーを単一のURLに紐づけます。
- **統合管理：**AIとの接続にも、人間のユーザーと接続する時と同じきめ細かいアクセスポリシーを適用します。
- **ポータルごとにツールをカスタマイズ：**ユーザーごとに利用可能なツールとプロンプトテンプレートを選択できます。

**注：**Cloudflareの[MCPサーバーポータル]は、Cloudflare上に[構築または展開されたリモートMCPサーバー]を含め、すべてのMCPサーバーをサポートしています。この機能は、[ゼロトラストネットワークアクセス（ZTNA）]制御として利用可能です。

**[こちらのブログ]で、当社のビジョンについて詳しくご紹介しています。**

**Cloudflareがお客様のAI利用をどう保護できるか、ご確認ください。**

**ワークショップを依頼する**