CLOUDFLARE

ソリューション概説

Cloudflare AI Security Suite

AIライフサイクル全体にわたるデータ制御とリスク管理によって、
AIとのインタラクションを保護

安心してAIを拡張

AIリスク対策には最新のセキュリティが必要

イノベーションの加速にAIが活用されていますが、これには重大なセキュリティリスクが伴います。AIをブロックしたり、複雑なポイントソリューションを追加したりする旧来のやり方は、イノベーションを阻害し、以下の現実を無視しているため、うまくいきません：

- **従業員の85%**が、IT部門による審査を受ける前にAIツールを使用している[1]
- **93%が、承認を得ずに企業データをAIに入力**している[2]
- **侵害された組織の63%**は、AIガバナンスポリシーを整備していない[1]

チームに力を与え、AIのメリットである生産性向上効果を享受しつつ、ビジネスに必要なセキュリティとコントロールを維持できるようにしましょう。

エージェンティックAIや生成AIを保護する統合プラットフォーム

Cloudflareは、AIを安心して導入していただける単一のプラットフォームを提供しており、セキュリティリーダーがリスクを管理し、テクノロジーチームが生産性を上げ、プラットフォームエンジニアが安全に構築できるようにすることで、誰もが安全に、協力してイノベーションを起こせるようにしています。

Cloudflare AI Security Suiteの利用を始めましょう

Cloudflare AI Security Suiteは統合プラットフォームで提供され、AIツールの業務利用と外部公開アプリケーションを保護します。シャドーAIを検出し、モデルを不正利用から保護し、エージェントのアクセスを保護し、プロンプト入力でのデータ露出を防ぎ、高い可視性と強力な制御によって、企業がより安全かつ効率的にイノベーションを進められるようにします。

可視性を拡張

AIアプリ、APIエンドポイント、AIエージェント接続をすべて可視化します。

リスクを低減

ガードレール、ポスチャ管理、リアルタイムの脅威軽減によって低減します。

データを保護

従業員とAIエージェントについて、迅速な保護と利用制御を行います。

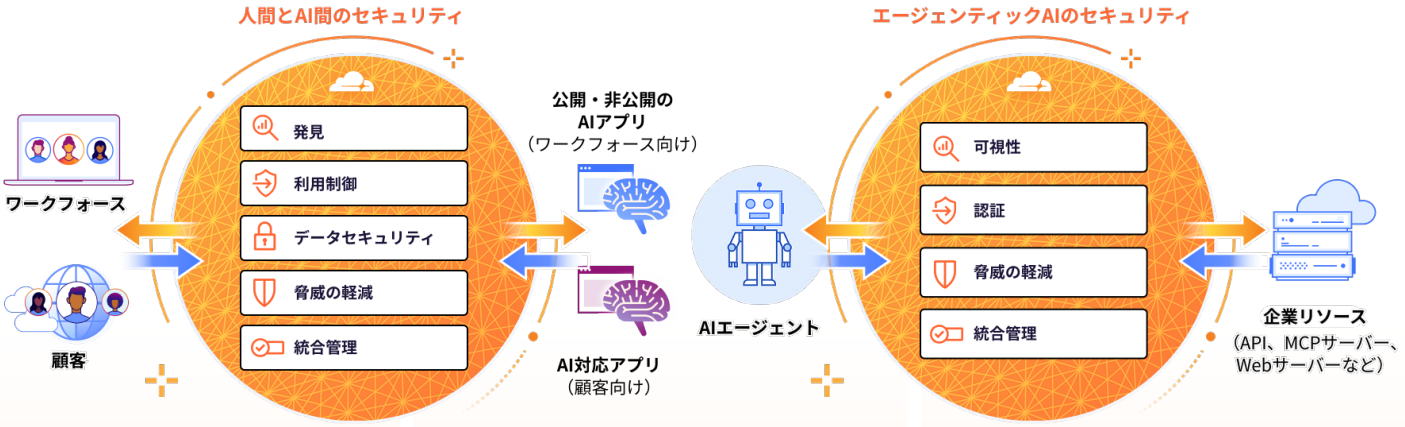
CloudflareでAIを開発すると、
セキュリティ機能が組み込まれます。

 | 050-1791-1110 | enterprise@cloudflare.com | Cloudflare.com/ja-jp/

REV:PMM-OCT2025

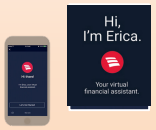
Cloudflare AI Security Suiteで 生成AIやエージェンティックAIとのコミュニケーションを保護

ワークフォースが生成AIで使用するデータを制御し、自律エージェントがもたらすセキュリティリスクを管理することによって、すべてのAIコミュニケーションを保護しましょう。



- **ワークフォース：**従業員、請負業者、開発者など
- **顧客：**Webサイト訪問者やアプリユーザー

- **生成AIアプリ：**スタンドアロンまたは組み込み
  Gemini Claude ChatGPT Copilot
- **AI対応アプリ**
  例：Bank of AmericaのAIチャットボット「Erica」



- あらゆるアプリに対応する汎用の**APIと**MCPサーバー
  Google Workspace
- 推論と検索拡張生成（RAG）のための**Webサーバー**

AIライフサイクルにわたる「セキュリティ・バイ・デザイン」でAI導入を加速

ワークフォースのAI利用を保護

AI利用制御とAIセキュリティポスチャ管理（AI-SPM）を実装して、リスクを軽減し、データを保護しましょう。

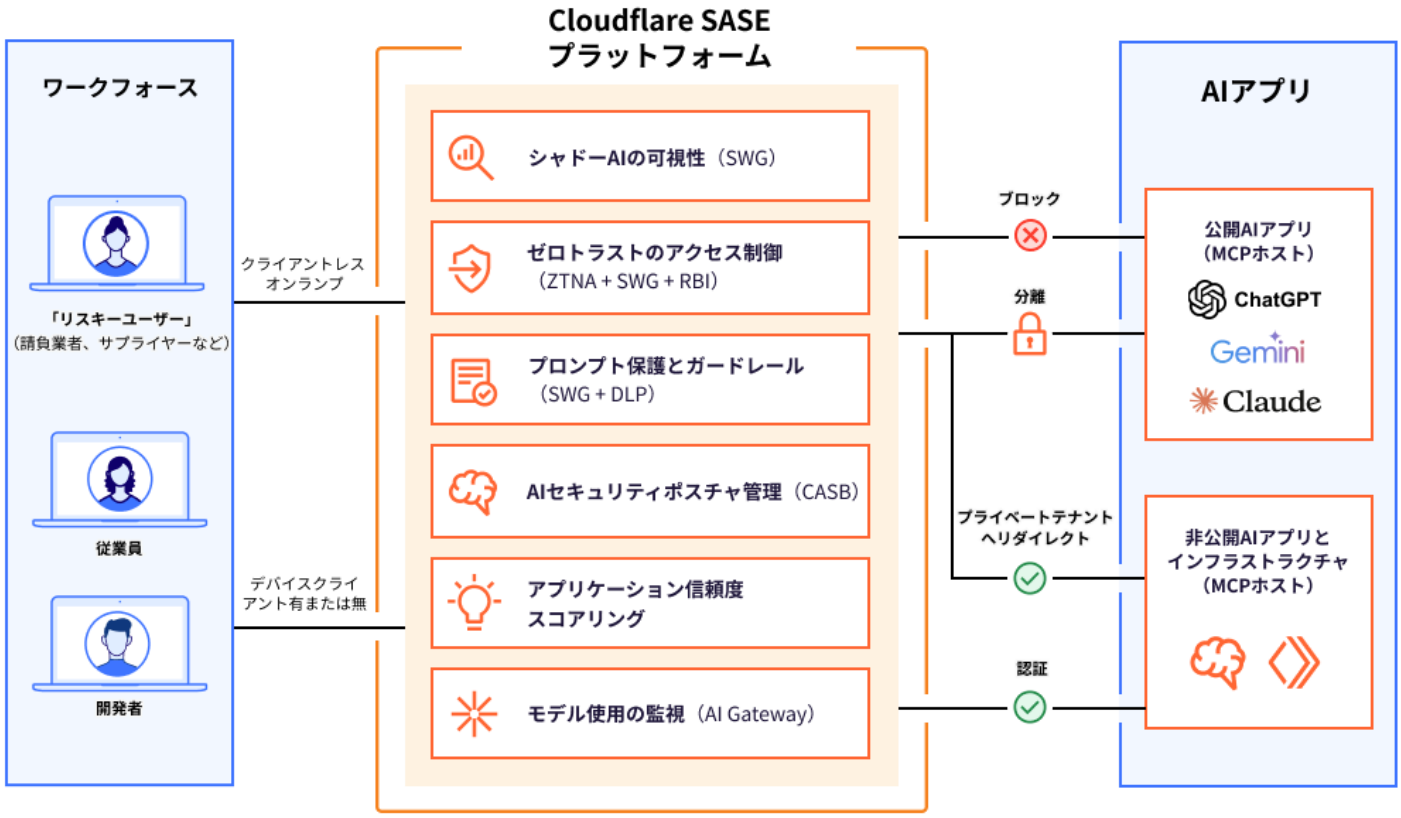
AI搭載アプリケーションを保護

AIアプリとAPIを、プロンプトインジェクションとデータ漏洩からリアルタイムで保護しましょう。

AIを安全に構築

可観測性、レート制限、インラインAIガードレールが統合されたプラットフォームで、開発者が安全にAIアプリを開発できるようにしましょう。

CloudflareのSASEプラットフォームで、ワークフォースによるAIアプリとワークロードの利用を保護



SSEが人とAIのコミュニケーションを保護

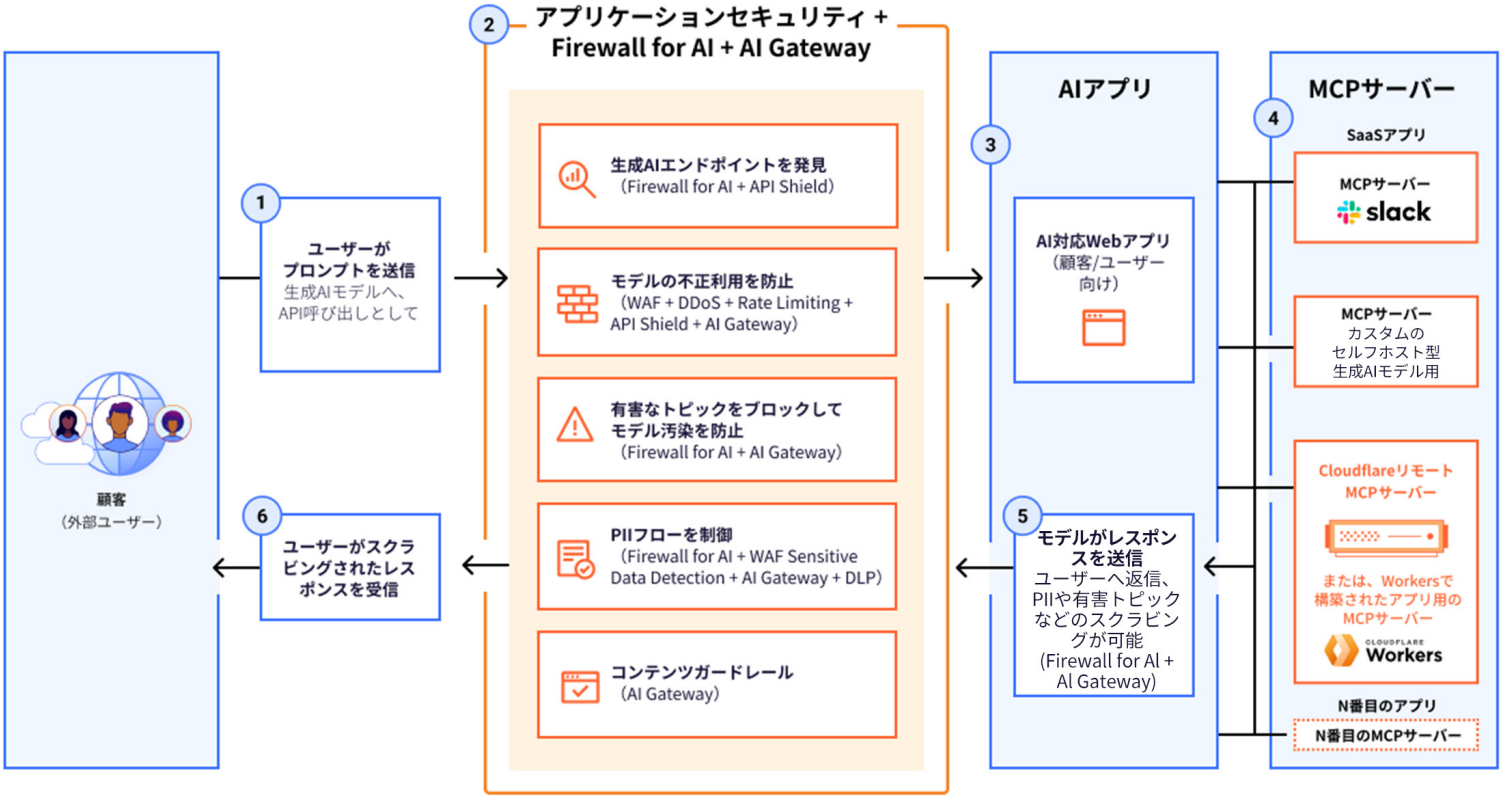
- **可視性：**インライントラフィック検査でシャドーAIの利用を検出して分析します。透明性の高いスコアリングで、AIアプリがもたらすリスクを評価します。
- **アクセス制御：**ユーザー接続をブロック、分離、リダイレクト、または許可します。アプリごとに、IDベースのゼロトラストルールを適用します。
- **プロンプト保護とガードレール：**ユーザープロンプトを検出し、意図（ジェイルブレイク試行、コードの不正使用、PIIの引き出しなど）に基づいてブロックします。
- **データセキュリティ：**AI駆動のデータ損失防止（DLP）検出機能により、PII、ソースコードなどの機密データの露出を阻止します。
- **AIセキュリティポスチャ管理：**生成AIツールとAPI連携し、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。現在、ChatGPT、Claude、Google Geminiに対応しています。

MCPサーバーポータルがAIとリソースのコミュニケーションを保護

- **可視性：**監査・分析用に、すべてのMCP（モデルコンテキストプロトコル）リクエストのログを集計します。ポータルに追加する前に、各MCPサーバーのレビューと承認を行います。
- **認証：**ユーザーのポータルへのアクセスを、IDに基づいて認証します。最小権限の原則に基づき、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。

注：MCPサーバーポータルは、お客様がCloudflareで構築または展開するリモート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。

Cloudflareのモデル非依存インラインセキュリティで AI対応のアプリとワークロードを保護



外部公開されたAIをアプリケーションセキュリティとFirewall for AIで保護

- **生成AIエンドポイントを検出：**お客様の全Webプロパティの AIモデルとAPIを、すべて自動的に検出します。
- **AIモデルを不正利用から保護：**専用のFirewall for AIで、プロンプトインジェクション、モデル汚染、過剰使用など、従来のセキュリティ保護を回避する可能性のある脅威をブロックします。
- **PIIフローの制御：**ユーザーのプロンプトとモデルのレスポンスをスキャンして、機密データの露出をブロックし、コンプライアンスの維持に役立ちます。
- **コンテンツガードレール：**Llama Guardなどの統合モデルを使用して、安全でないプロンプトや有害なプロンプトをブロックします。カスタムWAFルールの作成により、不審なAIインタラクションのブロックやログ記録が簡単にできます。

開発者プラットフォームとAI Gatewayで構築したAIを保護

- **統合AIコントロールプレーン：**すべてのAIアプリを単一のダッシュボードで管理します。リクエストのルーティング、レスポンスのキャッシュ、コストの制御、パフォーマンスの監視を行います。
- **エッジで認証情報を保護：**APIキーとシークレットをエッジで安全に保管し、クライアントサイドでの露出を防止し、複数プロバイダー間のキーローテーションを簡素化します。
- **コンテンツの安全を確保するガードレールを適用：**プロンプトやレスポンスに含まれる有害コンテンツや個人情報（PII）を自動的に識別し、ブロックまたは除去します。

Cloudflareは公開と非公開の両方のAI環境を保護する唯一のベンダー

安心してAIを導入できるように適切なガードレールを実装し、セキュリティがイノベーションを妨げず、加速するようにしましょう。

- **統合型のAIエコシステム保護：**複雑なセキュリティスタックはリスクを高めます。単一プラットフォームでデータを保護し、AIライフサイクル全体のコンプライアンスを確保しましょう。
- **将来を見据えたグローバルアーキテクチャ：**スケーリングしてあらゆるトラフィック量に対応し、新たな脅威に常に適応し、新たなユースケースに合わせてプログラム可能な、耐量子安全性を備えたネットワークで、将来の課題を今日のうちに解決しましょう。
- **AI駆動のセキュリティ：**当社のAI駆動防御システムは、プロンプトとレスポンスを検査し、リアルタイムで脅威を検出します。
- **実績あるAIリーダーシップ：**生成AI企業上位50社の80%が信頼するプラットフォームで、安心してイノベーションを進めましょう。
- **モデル非依存の展開：**セキュリティコントロールは、お客様の環境内のすべてのAIモデルに対応しており、AIの展開を管理するための統合的アプローチを提供します。

お客様の声

indeed

世界No.1の求人Webサイト
導入事例を読む

シャドーAIを識別して制御

VPN置き換えプロジェクトと並行して実施

APPLIED

保険テクノロジー
導入事例を読む

ChatGPTのような公開生成AIツールを隔離

機密データのコピー・アンド・ペーストをブロック

AI対応SaaS企業

PIIを保護

公開された生成AIエンドポイントへ顧客が機密情報を送信するのを防止

Cyndx

AI主導のフィンテック

推論コストを95%削減

Cloudflareで、AIモデルプロバイダーからのレスポンスをキャッシュして実行

貴社のAIセキュリティのニーズについてお聞かせください

専門担当者と話す

1. 2025年 Manage Engine調査：出典
2. 2025年 IBM、「Cost of a Data Breach」レポート：出典