

「セキュリティ・バイ・デザイン」でAIの導入加速

AI普及一方で、従来のセキュリティは取り残されています

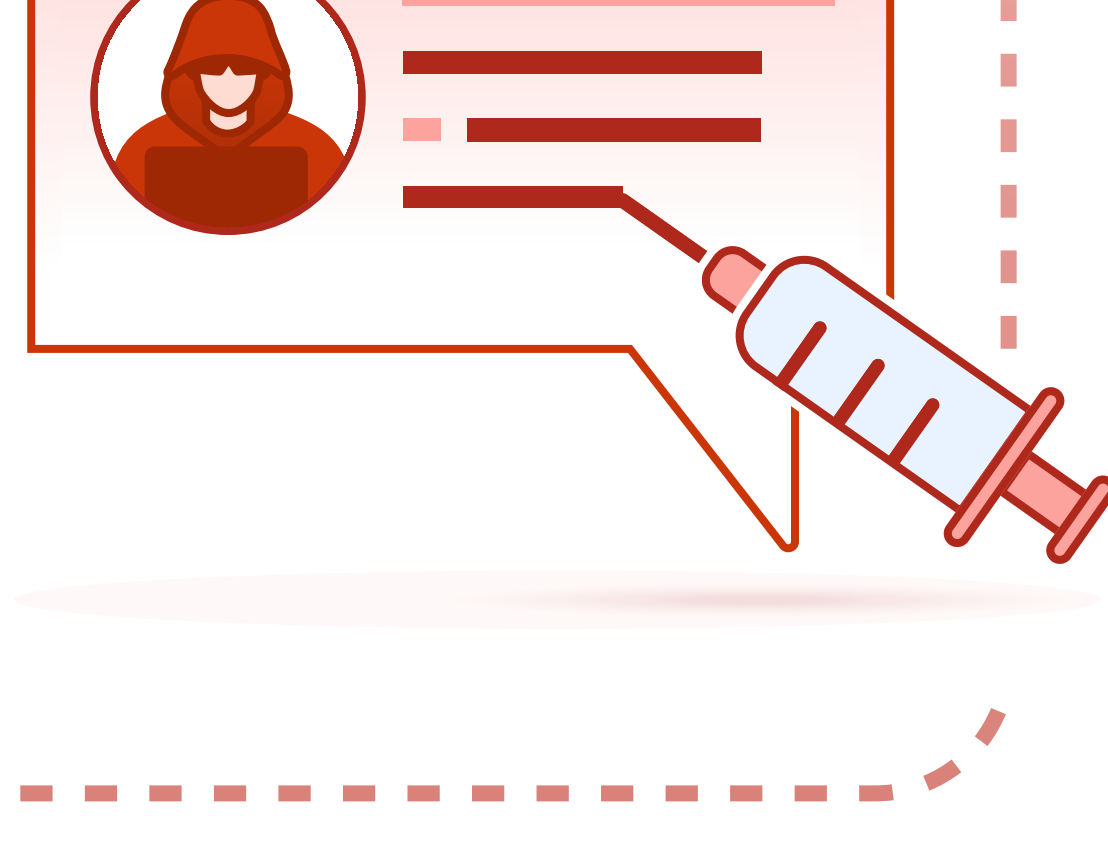


98%

企業の98%がシャドーAIを含む非承認アプリを使用しています。この盲点は、データ漏洩やコンプライアンス違反のリスクにつながります。¹

50%

プロンプトインジェクション攻撃で、LLMアプリのOWASPトップ10でセキュリティ脅威の最上位にランクインしています。²



97%

AI関連のセキュリティインシデントに直面している企業の97%で、AIへの適切なアクセス制御が欠如していました。³



93%

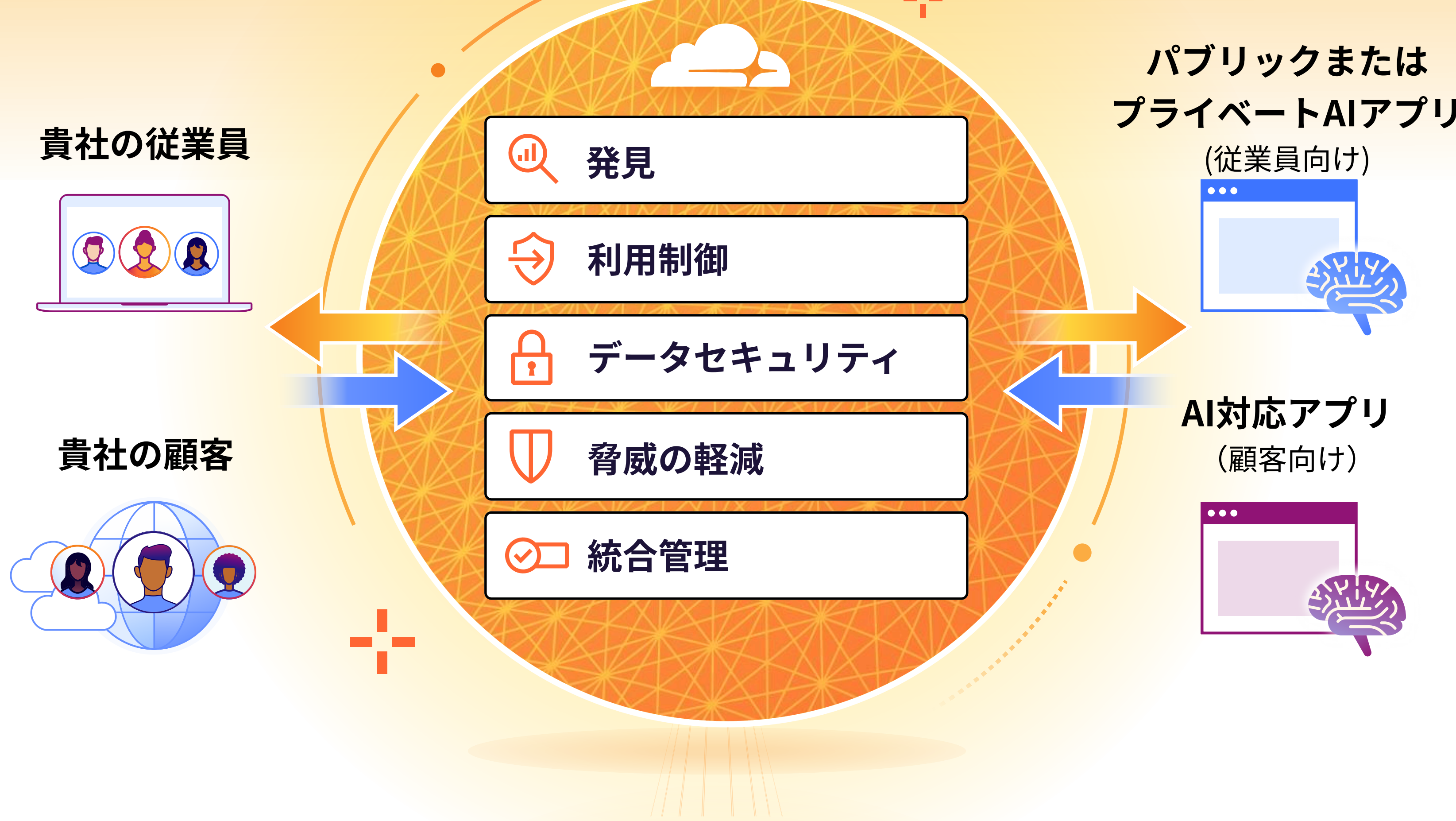
従業員の93%が、承認なしにAIツールに情報を入力していることを認めています。⁴



CloudflareでAIライフサイクル保護

生成AIとエージェンティックAI

人間対AIのセキュリティ

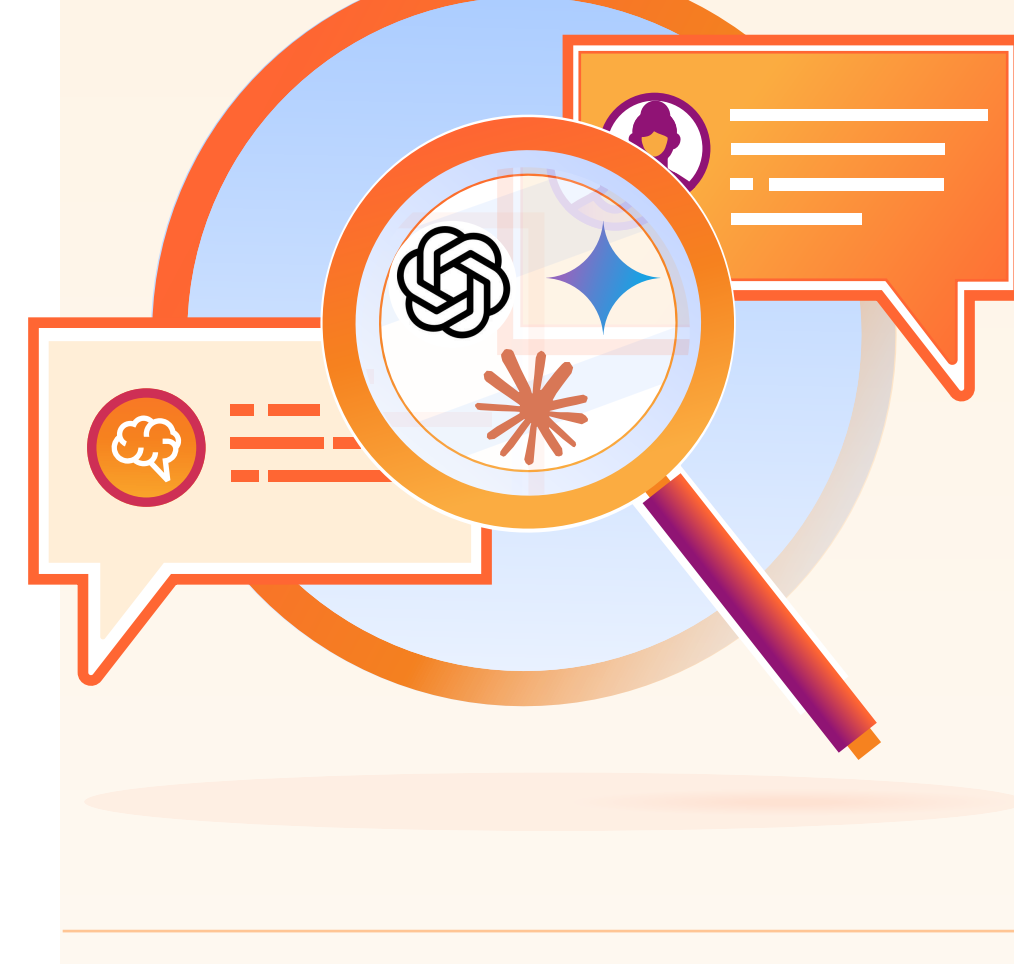


エージェンティックAIセキュリティ



セキュリティは内蔵型

CloudflareでのAI開発の場合



従業員による生成AIの利用を保護

- シャドーAIの発見
- AIアプリのリスク評価
- AIアプリのポスチャを管理
- 秘密データの入力制限
- プロンプトと応答にガードレールを適用

AI対応アプリとワークロードを保護

- Shadow AIのエンドポイントを検出
- AIモデルとトレーニングデータを悪用から保護
- プロンプトや応答に個人を特定できる情報露出を防止
- コンテンツのモデレーションを適用



お客様が構築するものを保護する

- 認証/認可を組み込んだMCPサーバーを構築
- AIモデルのリクエスト/応答、トークンの使用、コストの記録と制限
- モデルのフォールバックとレート制限でサービスの中断を防止

Cloudflareと他社の違い

AIライフサイクルの包括的な保護

開発からデプロイまで、人間とAIおよびAIとリソースの通信を保護する単一のプラットフォーム。



リアルタイムのインラインAIセキュリティ

パブリックとプライベートのAI環境をカバーする制御により、AIのプロンプトと応答をリアルタイムで保護。



将来を見据えたグローバルAIアーキテクチャ

当社のグローバルネットワークを活用して、AIの要求するスケールとパフォーマンスに一貫したエッジ適用を実現しましょう。



モデル非依存のデプロイ

セキュリティコントロールは、環境内のすべてのAIモデルに対して機能し、AIの展開を管理するための1つの統合されたアプローチを提供。



お客様の導入事例

indeed

世界No.1の求人Webサイト

シャドーAIの特定と管理
リモートアクセス最新プロジェクトと並行



AI対応のSaaS企業

PIIを保護
顧客による秘密情報のパブリック生成AIエンドポイントへの送信防止

Cyndx

AI主導のフィンテック企業

推論コストを95%削減
Cloudflareを採用してAIモデルプロバイダーからの応答をキャッシュし、実行

CloudflareがAI導入を保護する方法をご紹介します

導入事例を詳しく見る

1. Varonis, 2025年データセキュリティの現状
2. Liu, S., Wang, Z., Chen, Y., Deng, G., Liu, Y., 及びLiu, Y. (2024年)。大規模言語モデルに対する自動およびユニバーサルプロンプトインジェクション攻撃。
3. IBM, 2025年データ侵害のコストに関する調査
4. 企業におけるシャドーAIの管理、ManageEngine