機密データを保護

優れたネットワークアーキテクチャで、有効性と効率性が高く俊敏なデータ保護を実現します。

全環境のデータを一元的に保護

データ保護は新たな任務ではないものの、ハイブリッドクラウドアーキテクチャへの移行とAIの急速な導入により、新たな課題が生じています：

- **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[1]。
- **79%の国**がデータプライバシー法を制定しています[2]。

Cloudflareは、お客様のデータのライフサイクル全体にわたって一貫した制御を適用します：

- **全環境を保護：**Web、SaaS、メール、クラウドのトラフィックに一貫した制御を強制適用します。
- **AIによる持ち出しをブロック：**生成AIプロンプトを分析して機密データの流出をブロックし、AIの利用を管理します。
- **データリスクを管理：**シャドーIT/AIを検出して管理し、CASBでSaaS/クラウドアプリをスキャンします。

「未承認のAIツールが増えて、セキュリティのアプローチを見直さざるを得なくなり、現在SASEを検討中です。」 - *情報セキュリティ部門責任者、**AllSaints***

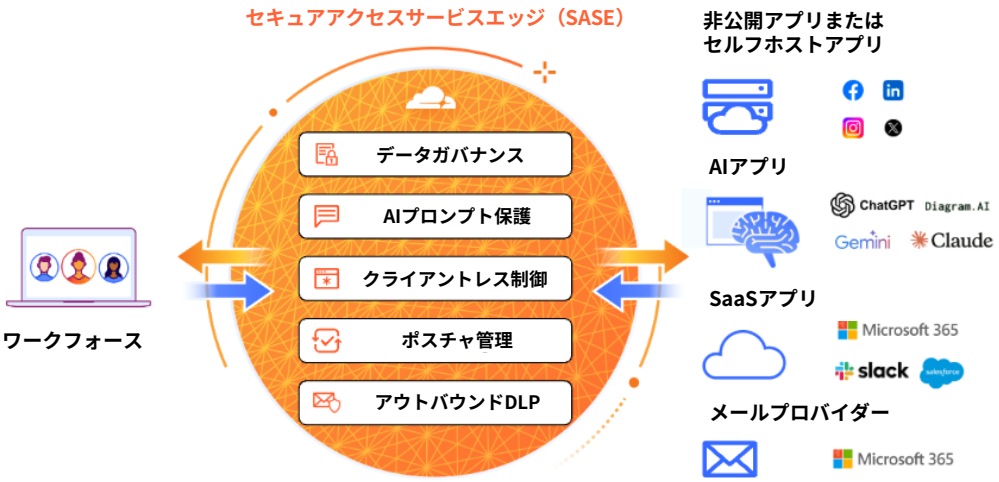
エンタープライズDLPよりもSASEを選ぶ理由？

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、あらゆるアプリケーションおよびデータソースとワークフォースとの間に位置するように構築されています。このためSASEは、データを安全に保護する上で理想的な出発点である場合が多いのです。

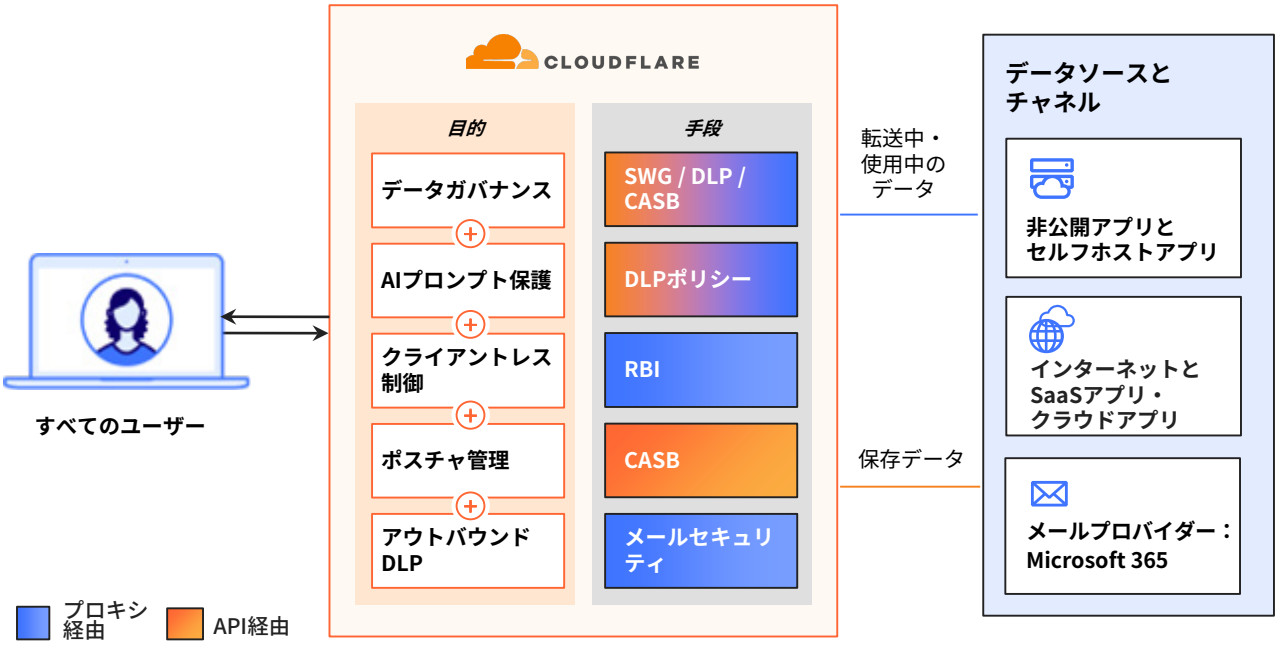
従業員がSaaSアプリのデータにアクセスする場合も、機密ファイルをダウンロードする場合も、生成AIツールとチャットする場合も、CloudflareのSASEプラットフォームは、すべてのデータインタラクションに一貫したセキュリティ制御を適用します。

仕組み

CloudflareのSASEプラットフォームは、ワークフォースとリソースの間に位置し、可視性と制御を一元化します。



CloudflareのSASEプラットフォームでAIを活用したデータ保護
Web、SaaS、メール、クラウドのトラフィックに適用されます



リアルタイムのインラインデータ保護

- **きめ細かなDLP：**PII、ソースコード、顧客データなどのコンテキストアウェアな検出により、機密データの露出を阻止します。
- **アウトバウンドメールDLP：**送信メールに含まれる機密データに自動的にフラグを立て、偶発的なデータ漏洩を防ぎます。
- **プロンプト保護：**AIによるリスキーなプロンプトやレスポンスを、意図（ジェイルブレイク試行、コードの不正使用、PIIリクエストなど）に基づいて検出し、ブロックします。

セキュアなアクセスとクライアント制御

- **セキュアなアプリアクセス：**すべての企業アプリケーションについて、エージェントAI接続の詳細DLPスキャンなど、ゼロトラストネットワークアクセス（ZTNA）のルールを適用します。
- **デバイスポスチャチェック：**詳細なデバイスポスチャチェック（ディスク暗号化や有効エンドポイントのDLPなど）に基づいてアクセスを制御します。
- **クライアントレス制御：**ブラウザベースのデータ制御を適用して、サードパーティのアクセスと従業員のBYODポリシーを保護します。

シャドーITとポスチャリスク

- **シャドーITやシャドーAIの発見：**環境全体にわたってシャドーITやシャドーAIを発見し、管理します。アプリ信頼度スコアとデータ転送メトリクスでリスクを定量化し、露出を迅速に軽減します。
- **ポスチャ管理：**SaaSアプリとクラウド環境をスキャンして、ポスチャリスクを検出します。見つかったセキュリティ脆弱性を、規定の対策で修正します。
- **テナント制御：**SaaSアプリの個人テナントをブロックし、データの流出を防ぎます。

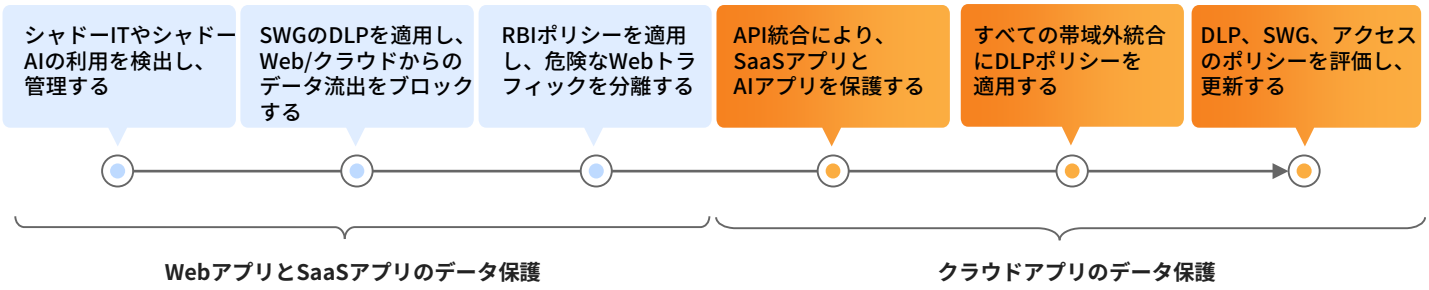
統合とレポート作成

- **CASBの統合：**主要なSaaSプラットフォームやAIプラットフォーム（Microsoft 365、Google Workspace、ChatGPTなど）とシームレスに統合し、APIベースのCASBスキャンを実行します。
- **Microsoft MIPの統合：**Microsoft Information Protection（MIP）の秘密度ラベルと継続的に同期し、DLPポリシー適用の一貫性を確保します。
- **可観測性とフォレンジック：**監査のため好みのSIEMにデータをセキュアにログ記録したり、ダッシュボードまたはAPIを介して即座にログを分析します。

データ保護の導入プロセス例

まず、シャドーITやシャドーAIの使用を発見して、攻撃対象領域の可視性を確保します。SWGで基本的なDLPポリシーを設定して、管理されていないクラウドアプリからの高リスクデータ漏洩をブロックし、RBIをデプロイして未承認Webトラフィックを分離します。

次にCASBをデプロイして、設定ミスを修正し、内部共有ポリシーを適用することで、認可されたSaaSアプリやAIアプリを保護します。SWG、メール、CASBの詳細DLPとアクセスのポリシーを洗練・統合し、すべての主要データベクトルについて、自動化され統合された損失防止を実現します。



導入開始のサンプルユースケース

- すべての未承認通信・保存経路で、**個人識別情報（PII）と保護対象保健情報（PHI）の流出をリアルタイムでブロック**します。
- インサイダーによる窃取や不正配布から**ソースコードと知的財産（IP）を保護**します。
- 生成AIアプリ用の**プロンプト保護ポリシーを適用**し、機密データの露出とモデル汚染を防ぎます。
- すべてのSaaSアプリとAIアプリの**設定ミスを防止**し、きめ細かいアクセス制御を適用します。

お客様の導入成果

EESTI RAUDTEE

インフラプロバイダー
導入事例を読む

データ損失とSaaSの脆弱性を軽減

データ漏洩と設定ミスの検出によって

APPLIED

保険テクノロジー
導入事例を読む

ChatGPTなどの公開生成AIツールを隔離

機密データのコピー＆ペーストをブロック

Flo

世界有数の健康管理アプリ
導入事例を読む

患者データを保護

メールセキュリティとゼロトラストでコンプライアンスを実現

CREDIT SAISON INDIA

ノンバンク金融会社
導入事例を読む

PIIを保護し、コンプライアンスを実現

不要なデータエグレスを防止

データ保護のニーズについて話しませんか？

ワークショップを依頼する

1. 2025年 Manage Engine調査：情報源
2. 2025年 国連貿易開発会議：情報源