EBOOK

# WFA (Work From Anywhere) 環境におけるデータの保護

Zscaler Data Protection で重要な情報を安全に管理



© 2024 Zscaler, Inc. All rights reserved.

# 目次


| | |
|---|---|
| 主な課題 | 03 |
| Zscaler のソリューション | 04 |
| アウトオブバンド CASB | 05 |
| インライン CASB | 06 |
| エンドポイント DLP | 07 |
| メール DLP | 08 |
| AI を活用した自動データ検出 | 09 |
| 高度な分類 | 10 |
| 生成 AI セキュリティ | 11 |
| 統合型 SaaS セキュリティ | 12 |
| データ セキュリティ ポスチャー管理 (DSPM) | 13 |
| ブラウザー分離 | 14 |
| ワークフロー自動化 | 15 |
| まとめ | 16 |


© 2024 Zscaler, Inc. All rights reserved.

主な課題

# かつてないほど困難なデータ保護

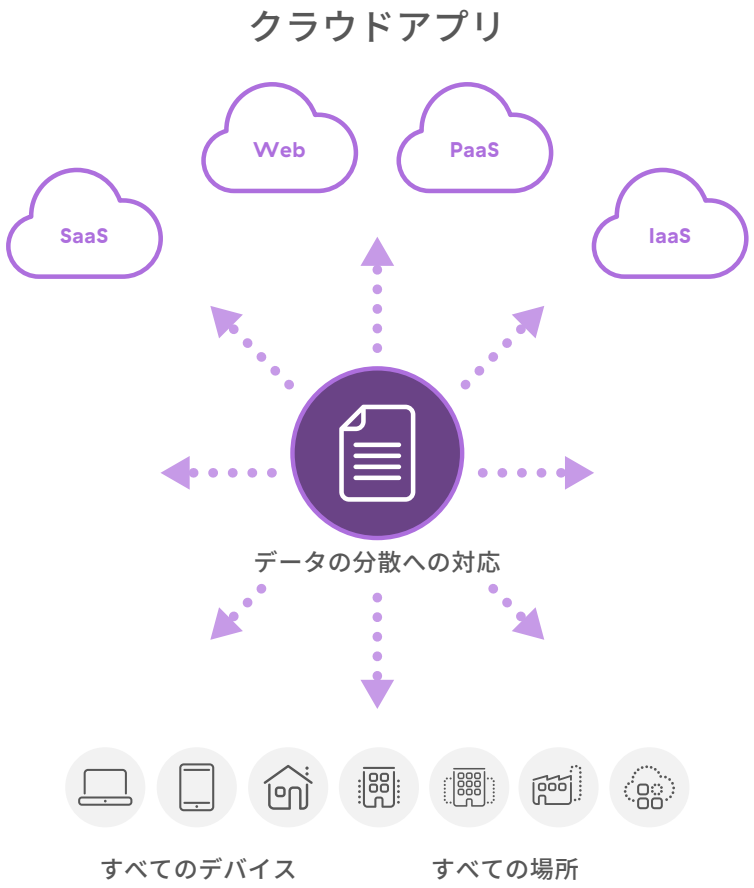
クラウド アプリの登場によってデータがさまざまな場所に分散され、従業員はあらゆる場所から接続するようになっています。従来型のデータ保護アプローチでは、データを十分に管理することはできません。その理由は、次のとおりです。

**ユーザーを追跡できない**
クラウド アプリがインターネット経由でアクセスされ、ネットワークやデータの制御が及ばないため、適切にデータを保護できません。

**コンプライアンスの状態を把握できない**
クラウド アプリが複数の場所やグループに分散しているため、コンプライアンスの状態を理解することが困難になっています。

**TLS/SSLインスペクションが限定的である**
ほとんどのトラフィックが暗号化されるようになった今、従来型のデータ保護アプローチでは大規模なTSL/SSLトラフィック検査ができず、潜在的なリスクを把握できません。

**全体像を可視化できない**
単一のソリューションのみを提供する製品や後付けのアプローチは、複雑性を招くだけでなく、脆弱性などをすべて確認できません。




© 2024 Zscaler, Inc. All rights reserved.

# Zscaler が提供する適切なデータ管理

## Zscaler Data Protection は、以下の基本原則を遵守することで、比類のないデータ保護を実現することができます。

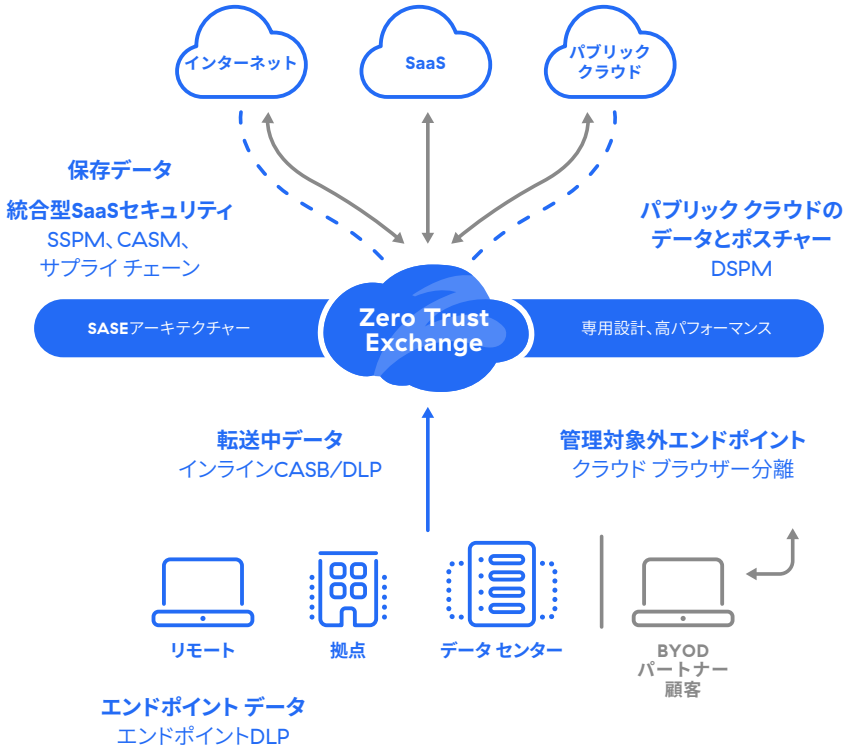
### 目的に特化した SASE アーキテクチャー
世界 150 か所のデータ センターに分散した高性能なインライン クラウドから、すべてのユーザーにリアルタイムの保護を提供します。

### 大規模な SSL インスペクション
すべての SSL トラフィックを検査し、データの漏洩を防ぎます。ユーザー単位の容量制限はありません。

### コンプライアンスの可視化
SaaS、Microsoft 365、パブリック クラウドの違反や設定ミスを検査することで、コンプライアンスを簡単に維持できます。

### 1 つのプラットフォームとポリシーで完全な可視化
一元的なプラットフォームで、すべてのクラウド データ チャネル（転送中データ、保存データ、エンドポイントおよびクラウドのデータ）を安全に保護します。

**Zscaler Data Protection:** ソリューションの概要




© 2024 Zscaler, Inc. All rights reserved.

# アウトオブバンド CASB で承認されたアプリを安全に管理

リモート ワークの従業員が多い場合、クラウド アプリは効率的なコラボレーションを可能にしますが、データが外部に流出してしまう問題も伴います。従業員がこれらのアプリを意図せずに使用する場合も多く、悪意のある活動につながる可能性があります。

## Zscaler のアウトオブバンド CASB によるクラウド アプリとデータの保護

- **公開された保存データの保護**
  クラウド アプリ、メール、ファイル共有サービス内の重要なデータを特定し、DLPポリシーを適用してアクセスや外部への公開を管理します。
- **不適切なデータ共有の防止**
  保存されている機密データに対してきめ細かなポリシーを適用し、組織外で共有されないようにします。




- **脅威の修復**
  OneDriveやBoxなどのファイル ホスティング サービスのデータ リポジトリーをスキャンして、悪意のあるコンテンツを迅速に検知、隔離します。
- **データ保護の簡素化**
  転送中データおよび保存データすべてに対して同一のデータと脅威ポリシーを提供する統一プラットフォームにより、単一のソリューションのみを提供する製品の複雑さを解消します。

© 2024 Zscaler, Inc. All rights reserved.

# インライン CASB で リアルタイムに可視化および制御

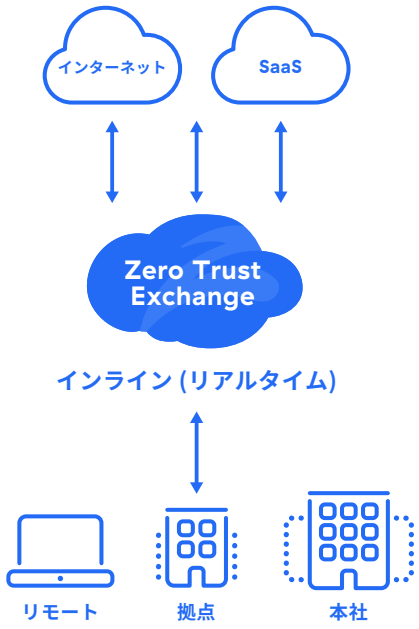
アウトオブバンド CASB は、保存データを保護しますが、クラウド アプリに対するリアルタイム コントロールも必要です。インライン CASB は、以下の方法でクラウドへの安全な移行を実現します。

- **シャドー IT に伴うリスクを軽減**
  使用されているクラウド アプリの安全性を組織全体にわたり迅速に把握できます。

**例：**オンライン PDF 変換ツールやファイル共有サイトなど、内部データにアクセスするリスクのあるアプリの活動をブロックします。

- **公式に承認されたアプリに限定**
  ユーザーのアクティビティーを IT 部門や組織が承認したクラウド アプリに限定します。

**例：**OneDrive のみを許可し、Box をブロックすることで、Microsoft 365 の共有機能と生産性を向上させます。




- **ファイル タイプの管理で情報漏洩を防止**
  条件付きブロックとアラートで、ファイル タイプ別にデータ転送を制限します。

**例：**Word、Excel、PowerPoint のファイルのアップロードやダウンロードをユーザー単位やグループ単位で制限します。

- **テナント制限の適用**
  クラウド アプリの特定のインスタンスのみを許可することで、データ フローを管理します。

**例：**Microsoft 365 for Business へのアクセスのみを許可することで、個人用 Microsoft 365 インスタンスへのデータ流出を防止します。

© 2024 Zscaler, Inc. All rights reserved.

エンドポイント DLP

# エンドポイント DLP で デバイス データの制御を簡素化

優れたデータ保護にはエンドポイント戦略が必要です。エンドポイント DLP により、従来のアプローチの複雑性を排除して、デバイスを完全に保護できます。

- **一元的なポリシーと可視性**
  一元化された DLP エンジンにより、エンドポイント、インライン、クラウド全体で一貫したアラートを取得できます。
- **軽量のシングル エージェント**
  Zscaler のエージェントに組み込まれているため、エンドポイントに必要なエージェントの数を減らし、ユーザー エクスペリエンスを改善できます。
- **迅速な導入**
  既存の Zscaler DLP ポリシーを活用して、すぐに稼働させることができます。
- **より迅速なインシデント管理**
  ワークフロー自動化、詳細なダッシュボードとフォレンジックにより、インシデントにすばやく対応できます。

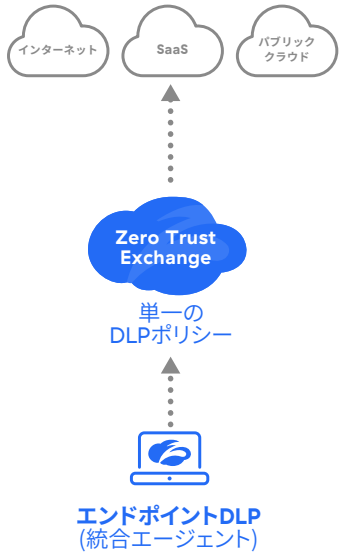
## エンドポイント DLP の 主なユース ケース

**データ カバレッジの向上**
あらゆる場所の重要なデータを隙なく適切に追跡および保護

**従業員の離職時のデータ保護**
離職する従業員によるデバイス データのコピーと転職先へのデータの持ち込みを阻止

**従来型のエンドポイント DLP の廃止**
複雑なポイント製品を排除し、統合プラットフォームを提供

**コンプライアンスの改善**
ファイルやデバイス全体でコンプライアンスを維持




### 保護されるチャネル

- リムーバブル メディア
- 個人用クラウド ストレージの同期
- ネットワーク共有
- 印刷

© 2024 Zscaler, Inc. All rights reserved.

リアルタイムのメール DLP

# 統一されたアプローチの リアルタイム メール DLP で複雑性を軽減

メールはデータに関する最大のリスク要因の 1 つです。Zscaler のメール DLP は、メール データに対する完全な DLP 制御を実現する強力なアプローチとなります。

従来のメール データ保護のアプローチは、手間のかかる複雑なものである場合があります。SSE の導入に伴い、IT 部門は複雑さを軽減しながらメール チャネル全体のデータを保護するための統一されたアプローチを求めています。

スマートホストを活用した Zscaler のメール DLP により、データ保護をメールにリアルタイムで簡単に拡張できます。Zscaler は SMTP リレーを利用することで、既存のメール アーキテクチャーへの簡単な統合を可能にし、メール データと添付ファイルに対する完全な制御を実現します。

## Zscaler のメール DLP の特長

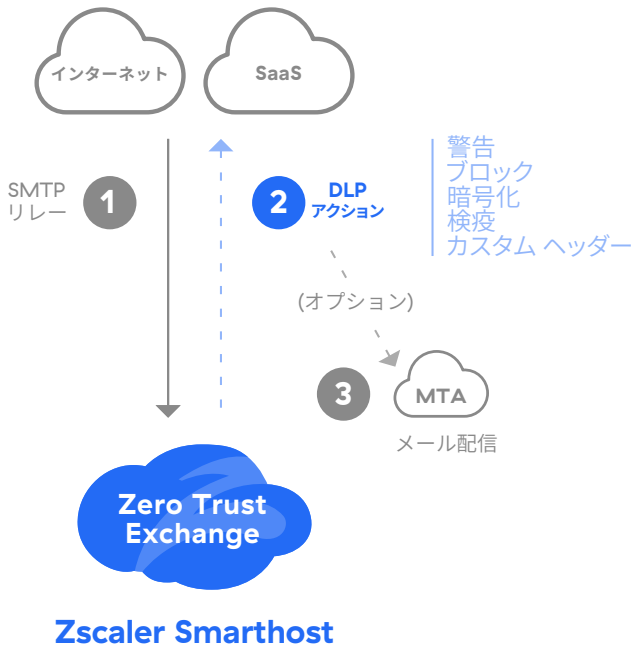
**プロトコルに依存しない**
管理対象デバイスおよび管理対象外デバイス、モバイルでも有効

**導入が簡単**
MX レコードの変更は不要

**柔軟なポリシー**
調整可能なポリシー定義ときめ細かいポリシー評価

**一元化と統合**
すべてのチャネルにわたって統一された UI と DLP エンジン

## リアルタイムのメールDLP



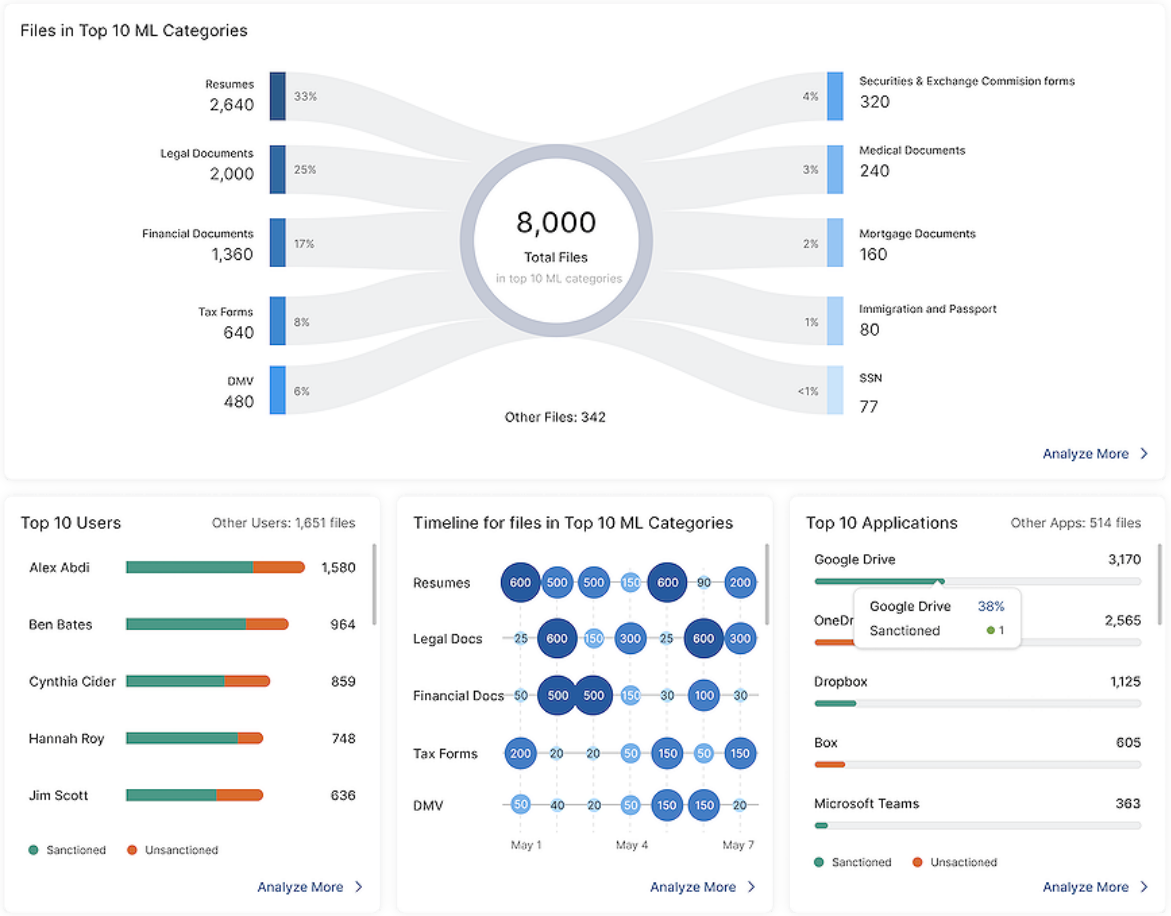

© 2024 Zscaler, Inc. All rights reserved.

# AI によるデータ検出で データを即座に検出して保護

データ保護プログラムの導入と運用化には、数か月単位の時間を要する場合があります。Zscaler の革新的なデータ検出を利用することで、データに関連するリスクや動作の迅速な把握が可能です。

## AI によるデータ検出

- エンドポイント、インライン、パブリック クラウド全体でデータを検出
- ユーザーやアプリによる漏洩リスクを迅速に把握
- 数クリックでポリシー作成に移行




© 2024 Zscaler, Inc. All rights reserved.

高度な分類 (EDM、IDM、OCR)

# カスタム データ、フォーム、画像を分類し、漏洩から保護

優れた DLP プログラムの中核となるのがデータ分類です。高度なデータ分類により、特殊なタイプの機密データを漏洩から保護できます。

## 完全データー致(EDM)

組織のカスタム データのフィンガープリントを生成し、保護できます。例：すべてのクレジット カード番号(Amazonでの購入処理に使用しているものなど)ではなく、顧客のクレジット カード番号でトリガーします。

## インデックス文書一致(IDM)

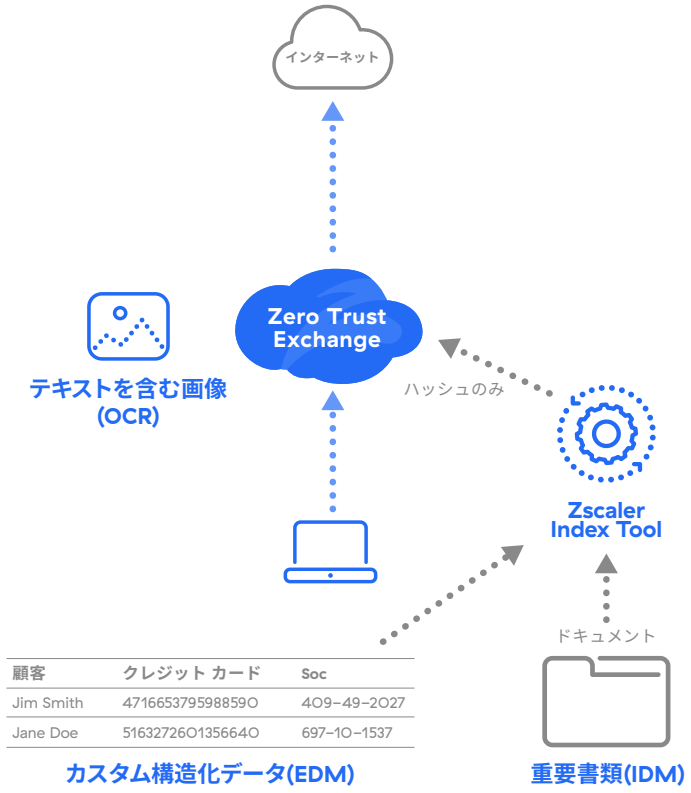
カスタム文書やフォームのフィンガープリントを生成し、保護します。例：税金や抵当関連の未記入のフォームのフィンガープリントを生成し、記入済みのフォームのデータをブロックします。

## 光学文字認識(OCR)

画像内のテキストを識別することで、情報漏洩を検出して防止します。例：機密性の高いコンテンツを含む可能性のあるスクリーンショットがないか監視します。

### Zscaler Index Tool

EDM と IDM 用のフィンガープリント補助ツールです。EDM と IDM のデータのハッシュを作成し、Zscaler クラウドに読み込んでポリシーの作成に活用します。




© 2024 Zscaler, Inc. All rights reserved.

生成 AI セキュリティ

# 生成 AI アプリを最大限に可視化して制御

生産性を高めるシャドー アプリを利用できるようにするには、生成 AI アプリへの機密データの漏洩を制御することが重要です。Zsclaer は、革新的なアプローチによって、すべての保護機能と可視化機能を 1 か所で提供します。

生成 AI アプリは、組織全体の生産性を向上させる可能性を持っています。しかし、ブロックについてより適切な判断を行うには、こうしたアプリを完全に可視化し、制御する必要があります。

Zscaler の革新的な生成 AI セキュリティは、組織全体のすべての生成 AI アプリを検出して、プロンプト レベルの入力を含む優れた可視性を提供し、IT 部門がより適切な判断を下せるよう支援します。

## 主なメリット

- ユーザーから AI アプリに送信されたプロンプトを表示し、コンテキストを含む完全な可視性を提供
- DLP 検査とクラウド アプリ制御にわたる柔軟なポリシー制御を実現
- Zscaler Cloud Browser でアクセスを分離し、データを保護

## 生成AIの可視性

**シャドーAIの検出**
利用者の多いAIアプリケーションを網羅するアプリ カタログ

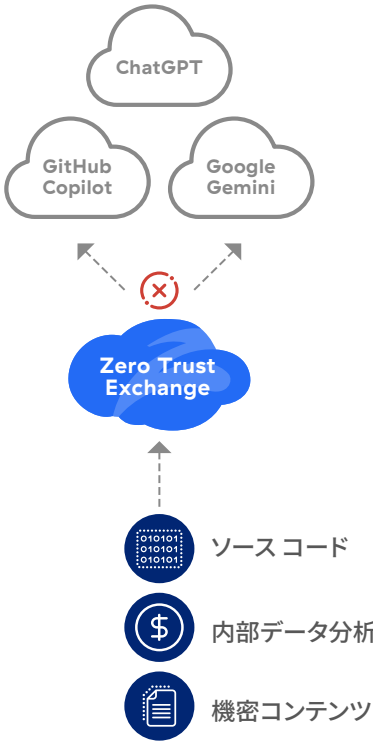
**入力されたプロンプトの可視化**
ユーザーがAIアプリに送信している実際のプロンプトを確認

## 生成AIアプリの制御

**DLP検査**
AIアプリに送信される機密データとコンテンツをブロック

**クラウド アプリの制御**
すべてのユーザー、部門、ロケーションにわたりAIアプリのアクセスを制御

**ブラウザー分離**
安全なクラウド ブラウザーでデータとアプリの使用を制限



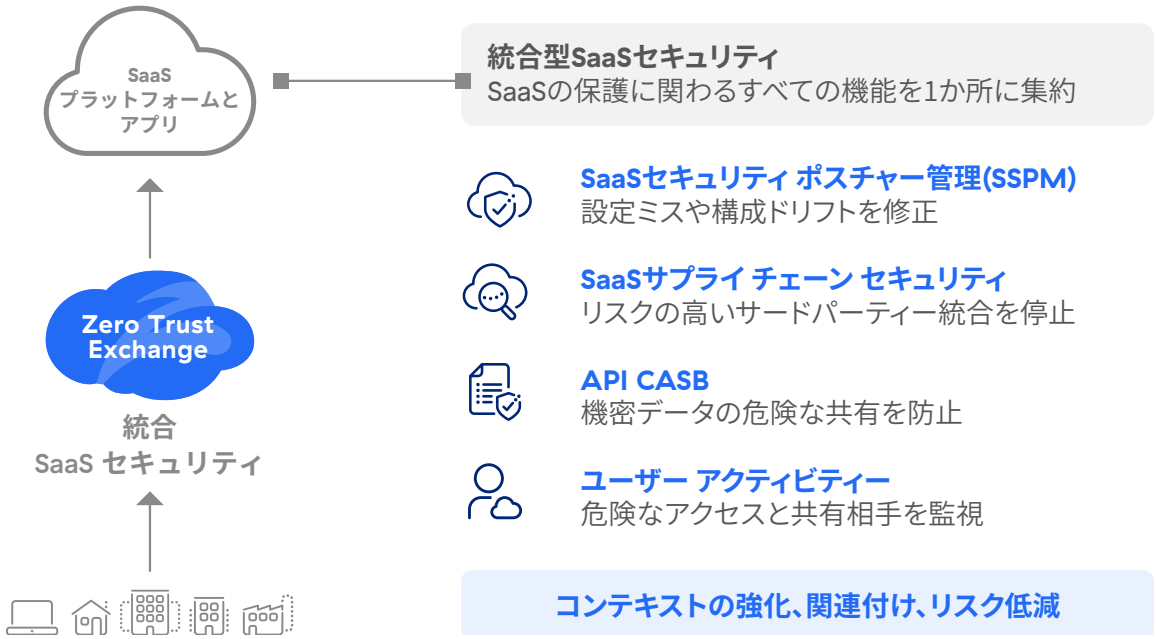

© 2024 Zscaler, Inc. All rights reserved.

# 完全統合型のアプローチで SaaS プラットフォームを保護

SaaS のクラウドとデータを保護するには、多くのツールが必要です。SSPM を他の主要な SaaS セキュリティ アプローチと統合することで、IT 部門による SaaS のデータ保護およびポスチャー管理を大幅に簡素化できます。

多くのクラウド侵害は、危険な設定ミスや SaaS プラットフォームに接続されたサードパーティー アプリによって発生します。クラウド内にある膨大な量の機密データを保護するには、SaaS のポスチャーの把握と管理が重要です。

Zscaler SaaS Security Posture Management の SaaS セキュリティ ポスチャー管理 (SSPM) を利用することで、統合的なアプローチで Office 365 や Google などの SaaS プラットフォームをスキャンおよび保護できるようになります。危険な設定ミスやアプリの統合に関する詳細な可視性を得られるほか、自動修復、ガイダンスの取得、危険な接続アプリの無効化に関する制御が可能です。




© 2024 Zscaler, Inc. All rights reserved.

データ セキュリティ ポスチャー管理 (DSPM)

# 完全に統合されたデータ保護アプローチで パブリック クラウドとデータを保護

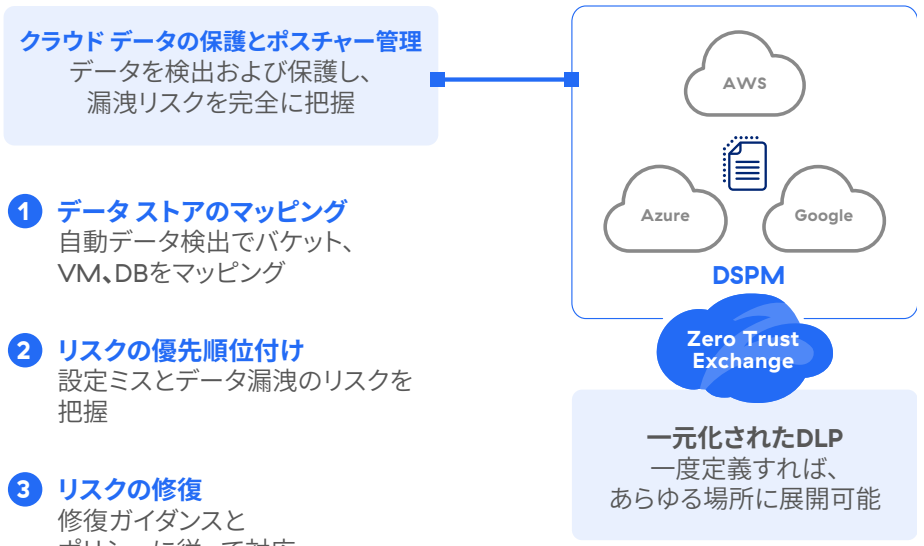
## データ保護を担当するチームには、パブリック クラウド データを保護するための統一されたアプローチが必要です。Zscaler DSPM は、既存のデータ保護プログラムにシームレスに統合できます。

AWSやAzureなどのパブリック クラウドに保存された機密データは、きわめて動的なものになる場合があります。過剰な権限、脆弱性、シャドー データといった問題に対処するために、IT部門にはパブリック クラウド データの検出、分類、保護のためのより優れた方法が必要です。

Zscaler DSPMでは、機密データの検出、リスクの把握、アクセスとポスチャーの制御を迅速に行えます。さらに、Zscalerの統合DSPMは他のすべてのチャネル(エンドポイント、ネットワーク、SaaS)と同じDLPエンジンを活用しているため、データの移動先にかかわらず一貫したアラートを提供することが可能です。

### 主なメリット

- AIを活用した自動検出で機密データを迅速に検出
- 設定ミス、公開状況、脆弱性を関連付け、クラウド データのリスクをより詳細に把握
- 既存のDLP辞書をパブリック クラウド データに拡張し、可視性とコンテキストを強化
- 修復に関する実用的なガイダンスでリスクを迅速に解決




© 2024 Zscaler, Inc. All rights reserved.

ブラウザー分離

# BYOD デバイスからの Web アプリ データの利用とアクセスを保護

パートナー、請負業者、従業員は、個人デバイスの利用時に組織のデータへのアクセスを必要とする場合があります。こうしたデバイスが管理対象外の場合、このデータに対する制御を維持するにはどうすればよいのでしょうか。

Zscaler User Portal 2.0 とクラウド ブラウザーを利用することで、管理対象外デバイスを安全にサポートすることが可能です。その仕組みは以下のとおりです。

## User Portal 2.0 によってアクセスとデータを保護する仕組み

- ユーザーが認証を行いポータルにログインすると、許可された Web アプリ (SaaS またはプライベート アプリ) のダッシュボードが表示されます。エンドポイント エージェントは必要ありません。
- 分離されたブラウザーでアプリにアクセスすると、データはピクセルとしてエンドポイントに安全にストリーミングされます。
- アプリは完全にインタラクティブに使用できるものの、切り取り、貼り付け、ダウンロード、印刷はブロックされ、スクリーンショットには透かしが入ります。




## BYODのメリット

### 脅威対策とデータ保護

すべてのトラフィックのインライン検査により、管理対象デバイスと同一水準のセキュリティが確保されます。

### データとファイルの分離

ドキュメントの表示や(アプリ間での)ファイルの共有を可能にしながら、エンドポイントのダウンロード機能やクリップボード機能を無効にできます。

### 統一されたDLPポリシー

ビジネス ポリシーを活用し、機密データに対する一貫した保護とアラートを実現します。

© 2024 Zscaler, Inc. All rights reserved.

# ワークフローの自動化で情報漏洩インシデントの管理を強化

## データ保護プログラムを次のレベルに引き上げるには、運用の効率化とユーザーへの教育を可能にする強力なインシデント管理ツールが必要です。

インシデント情報やツールが集約されていないために、多くの保護プログラムが課題を抱えています。さらに、ユーザーは、不適切なデータの扱いをした際にどのような行動にリスクがあったのかを知ることができません。

Zscaler Workflow Automation は、DLP 管理者がインシデント管理を強化するための専用ツールを提供します。

すべてのフォレンジックが 1 か所に集約されているため、管理者は危険な行動を迅速に把握して、ユーザーにインシデントを割り当てて妥当性を確認し、インシデントを解決するためのポリシー アクションをすばやく実装できます。

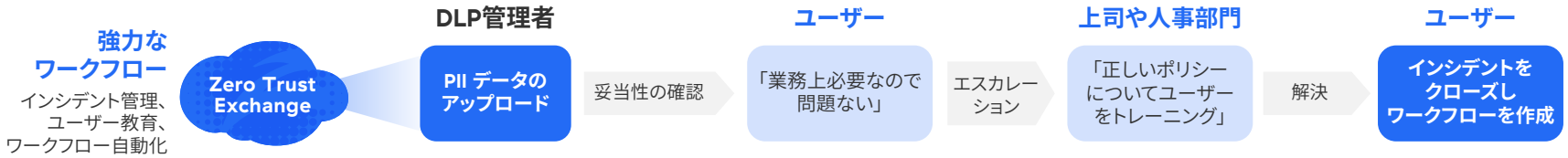
### ワークフロー自動化によるデータ保護プログラム強化の仕組み

**インシデント管理の迅速化**
情報漏洩インシデント管理専用のプラットフォームで時間を節約

**ルーチンの自動化**
ワークフローを使用して反復的なタスクとエスカレーションを自動化することで日常業務を合理化

**ユーザーへの教育**
Slack、Teams、メールを通じてユーザーとインシデントに関わる行動の妥当性を確認し、データ保護のベスト プラクティスを教育

**完全な統合**
包括的なインシデント処理システムにより、保護プログラムに起こりがちな機能不全を回避




© 2024 Zscaler, Inc. All rights reserved.

まとめ

# 最大限の保護を最小限の作業で

Zscaler Data Protection は、ユーザーとそのユーザーがアクセスするアプリケーションを追跡することで、クラウドとモバイル環境のデータを保護します。Zscaler Zero Trust Exchange™ は、コンプライアンスを簡素化し、データ保護を容易にするために必要な保護と可視性を実現する専用プラットフォームです。

Zero Trust Exchangeは、以下を実現します。

**同一水準の保護の提供**
接続方法や場所に関係なく、すべてのユーザーに一貫したデータ保護ポリシーを適用します。

**すべての TLS/SSL トラフィックを検査**
SSL の盲点を排除し、業界最高の SLA で保障します。

**コンプライアンスの簡素化**
PCI、PII、PHI データの検索と管理が容易になり、コンプライアンス要件を確実に遵守します。

**複雑性の解消**
すべてのクラウドチャネル ( 転送中データ、保存データ、エンドポイントやクラウドのデータ ) の保護を可能にする一元的なプラットフォームで、複雑性を解消します。

© 2024 Zscaler, Inc. All rights reserved.

# クラウドファーストのモバイル環境向けに設計されたデータ保護

データはもはやデータ センターには存在しません。あらゆる場所に存在し、どこからでもアクセスできる時代です。クラウドとモバイル環境で、既存のセキュリティ アプローチでデータを十分に保護することはほぼ不可能です。Zscaler Data Protectionを利用すれば、ユーザーが接続する場所やアプリケーションがホストされる場所に関係なく、重要なデータに対して同一水準の保護を提供することができます。

**Zscaler Data Protection の導入事例はこちら ›**

eBookを入手する

**Zscaler Data Protection プラットフォームの詳細はこちら ›**

Webページを見る

zscaler™ | Experience your world, secured.™

**Zscaler について**
Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SSE ベースの Zero Trust Exchange は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.jp** をご覧いただくか、Twitter で **@zscaler** をフォローしてください。

© 2024 Zscaler, Inc. All rights reserved. Zscaler™、Zero Trust Exchange™、**zscaler.jp/legal/trademarks** に記載されたその他の商標は、米国および / または各国の Zscaler, Inc. における (i) 登録商標またはサービス マーク、(ii) 商標またはサービス マークです。その他の商標はすべて、それぞれの所有者に帰属します。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.jp