

# クラウド データを保護し 侵害を阻止する Zscaler DSPM

最も包括的な完全統合型データ保護  
プラットフォーム。一度定義すれば、  
あらゆる場所に適用可能です。

## 新たなターゲットとなったクラウド データ

82%

クラウドに保存されたデータに  
関係している侵害の割合

227日

データ侵害を特定するまでの  
平均期間

445万ドル

データ侵害の  
世界平均被害額

ESG.STATE OF DATA GOVERNANCE AND EMPOWERMENT REPORT,2022年  
IBM SECURITY,COST OF A DATA BREACH 2023 REPORT,2023年

「従来認識されていなかったデータ リポジトリー  
の特定と発見、関連するセキュリティ リスクやプ  
ライバシー リスクの軽減は喫緊の課題となっ  
ており、2026年までに20%以上の組織がDSPM  
テクノロジーを導入すると見られます」

- Gartner

GARTNERは、GARTNERリサーチの発行物に掲載された特定のベンダー、製品またはサービスを  
推奨するものではありません。また、最高のレーティング又はその他の評価を得たベンダーのみ  
を選択するようにテクノロジーユーザーに助言するものではありません。GARTNER・リサーチの  
発行物は、GARTNER・リサーチの見解を表したものであり、事実を表現したものではありません。  
GARTNERは、明示または黙示を問わず、本リサーチの商品性や特定目的への適合性を含め、  
一切の責任を負うものではありません。

## クラウド中心の環境におけるデータ保護の課題

マルチクラウド環境は本質的に複雑で、多くのリソースを消費します。膨大な量のデータがクラウドに送信されていることに加え、多数のユーザーがさまざまなクラウド プラットフォーム、アカウント、サービスにアクセスしていることから、クラウドで起こっていることを組織が理解および制御することは困難になっています。

マルチクラウド環境のデータ保護にあたってセキュリティの専門家が直面する課題は主に次の4つです。

### 01 クラウドのアジリティ

現代のアジャイルなクラウド テクノロジーやクラウド サービスによって、開発者が柔軟に共同作業を行い、データを共有しやすくなる一方、結果的に機密データに関する可視性や制御は失われる可能性があります。

### 02 クラウドの複雑さ

クラウド データの総量は、現在の33 ZBから、2025年までに175 ZBへと増加すると予測されています。複数のクラウド プラットフォーム、アカウント、サービスにデータが拡散しているため、どのクラウド サービス、リージョン、アカウントがデータを消費し、保存しているかを把握しにくくなっています。

残念ながら、従来のデータ保護ソリューションは動的なマルチクラウド環境に適した設計になっていないことがわかっています。DSPMのポイント製品を扱うベンダーが長年にわたり提供しているサイロ化されたアプローチは、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せん。クラウド データの保護において、一元的な新しいアプローチが求められていることは疑いようもありません。

### 03 過剰な権限

セキュリティ部門は、データの検出と分類という課題に加え、データへのアクセスを把握しながらデータ主権要件に準拠し、それを維持するという難題も抱えており、結果として大きなセキュリティ ギャップが生じています。

### 04 データに関するコンテキストの欠如

機密データのコンテキストに基づく優先順位付けを行わず、設定ミスや脆弱性に関するアラートが過剰な状態になれば、担当者の疲弊の深刻化やセキュリティ侵害につながります。

## 包括的なDSPMが重要な理由

## Zscaler Data Security Posture Management (DSPM)とは

Zscaler AI Data Protectionは、Web、SaaSベースのサービス、パブリック クラウド環境(AWS、Azure、GCP)、プライベート アプリケーション、メール、エンドポイントの構造化データおよび非構造化データを保護する、最も包括的な完全統合型データ保護プラットフォームです。

このZscalerのプラットフォームの一部として、Zscaler Data Security Posture Management (DSPM)は、クラス最高の堅牢なデータ セキュリティをパブリック クラウドに拡張します。クラウド データを詳細に可視化するとともに、データとアクセスを特定して分類し、公開状況とセキュリティ態勢をコンテキスト化します。セキュリティ部門はこれらの情報を活用することで、大規模なクラウド データ侵害から組織を守り、修復できるようになります。

また、統合された単一のDLPエンジンにより、すべてのチャンネルで一貫したデータ保護を実現します。あらゆる場所のあらゆるユーザーを追跡し、使用中のデータと保存データを管理することで、機密データをシームレスに保護しながら、コンプライアンスを確保します。



## Zscaler DSPMの特長

### 01 統合型データ セキュリティ プラットフォーム

Zscaler DSPMは、Zscaler AI Data Protectionプラットフォームとシームレスに統合されています。このプラットフォームは、一元的なDLPエンジンを中心に構築されており、セキュリティ部門はこれによってWeb、SaaS、オンプレミス アプリケーション、エンドポイント、BYODデバイス、パブリック クラウドに対応するクラス最高のデータ セキュリティを実現できます。

### 02 AIによる自動データ検出

Zscalerのエージェントレス アプローチによって、展開と運用を大幅に加速しながら、構成なしで自動的にデータを検出、分類、識別できます。

### 03 担当部門の支援と運用の簡素化

強力な脅威相関で隠れたリスクと重大な攻撃経路を明らかにすることにより、過剰なアラートを大幅に削減し、担当部門が最も重要なリスクに集中できるようになります。



## DSPMのユース ケース

機能	特長	メリット
データの検出と分類	<p>さまざまなクラウド プラットフォームとサービスの機密データをリアルタイムまたはほぼリアルタイムでスキャンし、検出できます。</p> <p>事前定義されたポリシーまたはカスタム ポリシーに基づいて、機密データの分類、ラベル付け、インベントリー化を正確に行えます。</p> <p>1日あたり数十億件のトランザクションを監視するZscalerプラットフォームによって強化されたAIベースの正確なデータ分類を利用できます。</p>	クラウド データの拡散を高いレベルで可視化し、機密データの存在を認識していなかった場所も含め、機密データを検出できます。
公開状況のマッピングと追跡	<p>マルチクラウド環境に存在する機密データのセキュリティ、インベントリー、コンプライアンスを一元的に可視化できます。</p> <p>ミッションクリティカルなデータ資産とその構成へのすべてのアクセス パスについて、ユーザー中心の視点からリスクベースのきめ細かい可視性を得られます。</p> <p>設定ミス、過剰な権限、脆弱性などの隠れたリスクを分析できます。</p>	侵害されたデータ資産、アクセス、隠れた攻撃経路、進行中の高度な脅威がデータに及ぼし得る影響の範囲を把握できます。
リスクの修復	<p>重大度に基づいてリスクの優先順位付けを行えます。</p> <p>コンテキストベースの修復ガイダンスを活用しながら、問題や違反の根本的な修正を簡単に行えます。</p>	データの漏洩や侵害のリスクを最小限に抑えられます。
一貫したポスチャーの維持	<p>エンドポイント、メール、SaaS、パブリック クラウドなど、あらゆる場所にクラス最高の一貫したデータセキュリティを適用できます。</p>	全体的なセキュリティ態勢を改善し、脅威に先回りに対応できます。
継続的なコンプライアンスの維持	<p>規制上の基準に照らしてポスチャーを継続的にマッピングし、コンプライアンス違反を特定して修正できます。</p> <p>包括的なコンプライアンス ダッシュボードを活用して、セキュリティに関する部門間のコラボレーションを簡素化できます。</p>	違反を制御し、監査を簡素化するとともに、財務的な損失や信用失墜を防止できます。
ワークフローの統合	<p>既存のセキュリティ エコシステム、サードパーティーのサービス、リスクの優先順位付けのためのネイティブ ツール、コラボレーション アプリケーションとシームレスに統合できます。</p>	機密データの保護にかかるコストと複雑さを最小限に抑えられます。

## Zscaler DSPMの主要コンポーネント

データ検出	構造化/非構造化データ ストアの特定	DSPMのSKUに含まれる
データ分類	デフォルトの検出とカスタム ルールによる機密データの自動的な検出と分類	DSPMのSKUに含まれる
データ アクセス制御	データ リソースへのアクセスのマッピングと追跡	DSPMのSKUに含まれる
リスク評価	AI、ML、高度な脅威相関を用いた重大度と影響に基づくリスクの検出と優先順位付け	DSPMのSKUに含まれる
リスク修復	完全なコンテキストを含む段階的な修復ガイダンスの提供	DSPMのSKUに含まれる
コンプライアンス管理	GDPR*、CIS、NIST、PCI DSS*などの業界基準やコンプライアンス標準に対するデータ セキュリティ態勢の自動マッピング	DSPMのSKUに含まれる

\*製品ロードマップ上の機能

## Zscaler DSPMを体験

## デモを予約する

ガイド付きのデモでZscaler DSPMプラットフォームをご体験ください。

[デモを依頼する](#)

## リリース イベントを見る

DSPMがどのように複雑さを解消しながら、最新の高度な攻撃や脅威に対するデータ保護を強化し、セキュリティ部門の効率を最大化するかをご紹介します。

[リリース イベントを見る](#)

詳細はこちら  
[www.zscaler.jp/dspm](http://www.zscaler.jp/dspm)

