AI活用型DSPMによる環境全体のデータの保護

単一の統合データ セキュリティ プラットフォームであらゆる場所のデータを保護

データシート

AI時代の多様なデータ環境の保護における課題

488万ドル

データ侵害1件あたりの
世界平均被害額

40倍

組織における
AI導入の急増

258日

データ侵害を
特定するまでの平均期間

(「COST OF A DATA BREACH 2024 REPORT」IBM SECURITY、2024年)
(ZSCALER THREATLABZ AIレポート)

「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

多様な環境でのデータ保護は本質的に複雑で、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やAIサービス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、データの状況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。多様な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以下の4つです。

01

アジャイルかつ複雑な環境

データ量の増加、クラウドの導入、AIを活用したオペレーションによって、複雑な環境で機密データを効果的に監視、保護することが難しくなっています。

02

データ ガバナンス

進化し続ける厳格な規制(GDPR、HIPAAなど)により、機密データ、顧客データ、AIの使用に関する強力なセキュリティが求められています。

03

データ漏洩のリスク

複雑なデータ環境では、設定ミス、過剰なアクセス権限、サービスの急速な拡張などによってリスクが生じやすくなります。

04

不十分なデータ コンテキスト

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、過剰なアラートが発生すれば、リソースのさらなる疲弊やセキュリティ侵害につながります。

包括的なDSPMの必要性が高まっている理由

従来のデータ保護ソリューションは、動的なデータ環境に対応した設計にはなっていません。そして、多くのDSPMベンダーが提供するアプローチは、ポイント製品によるサイロ化されたものであり、既存のデータ保護プログラムにシームレスに統合することはできません。クラウド データの保護には、一元的な新しいアプローチが求められているのです。

DSPM戦略の再定義

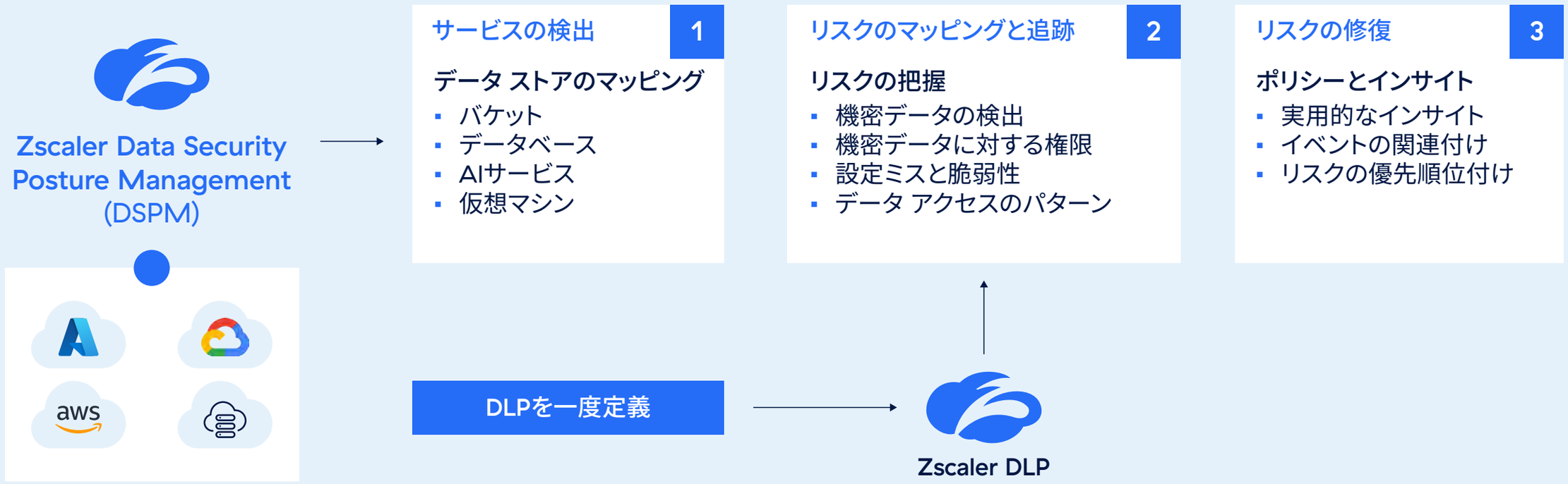
AIを活用したZscaler DSPMの仕組み

Zscaler AI Data Securityは、世界で最も包括的な完全統合型データ セキュリティ プラットフォームであり、Web、SaaS、パブリック クラウド、オンプレミス、メール、エンドポイント、プライベート アプリ、AIなど、あらゆるチャネルに存在するすべてのデータに対して詳細な制御とクラス最高のセキュリティを提供します。

このプラットフォームの一部であるZscaler DSPMは、堅牢なセキュリティをオンプレミスとパブリック クラウドのデータに拡張します。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。

統合された単一のDLPエンジンにより、すべてのチャ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。

複雑な環境全体にわたるAIおよびデータの保護と侵害の阻止



パブリック クラウドの構造化データと非構造化データを保護する統合DLP

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

包括的なZscaler AI Data Securityプラットフォームとのシームレスな統合により、Web、SaaS、オンプレミス アプリ、エンドポイント、BYOD、パブリック クラウドにわたって最高水準のデータ セキュリティを実現します。

02

AIによる自動データ検出および自動分類

構成なしでデータを自動的に検出、分類、特定できるため、展開と運用を大幅に加速できます。

03

安全なAIイノベーション

生成AIツールの安全な導入と活用のために、AIセキュリティ ポスチャー管理(AI-SPM)を自動化し、きめ細かな管理を実現します。

04

ガバナンスとコンプライアンス

厳格なセキュリティおよびプライバシー規制(例：GDPR、NIST)への準拠を徹底するために、ベスト プラクティスの自動化、ポリシーの施行、監査証跡の管理を行います。

05

部門の強化と運用の簡素化

強力な脅威相関によって隠れたリスクや重大な攻撃経路を特定し、アラートの過多を最小化することで、担当部門が最重要リスクへの対応に集中できるようにします。

Zscaler DSPMのメリット

単一の革新的なプラットフォームでDSPMとデータ セキュリティを統合

環境全体のデータの把握

すべてのデータとアプリの検出
継続的な検出とカタログ化

包括的なカバレッジ
あらゆる場所のデータの可視化

SaaS　IaaS
エンドポイント　オンプレミス*

インテリジェントなLLM分類
予期しない新たなデータの検出

統合ダッシュボード*
完全なコンテキストと関連付け

* 新たなイノベーション：2025年第3四半期(CY)

環境全体のデータの制御

クラウド データの保護
リスクと設定ミスの防止
(CASB、SSPM、DSPM)

転送中データの制御
アウトバウンド データと生成AIなどのクラウド アプリの制御
(シャドーIT/AI、Web、メールのDLP)

デバイス データの保護
持ち出しの阻止とBYODの保護
(エンドポイントDLP、ブラウザー分離)

リスクと運用の管理
インシデント対応ワークフローの自動化とユーザー コーチング

特長	特長	メリット
データの検出と分類	• 多様なデータ環境全体の機密データをスキャン、検出します。 • 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。 • 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。	データの拡散を高いレベルで可視化し、機密データの存在すら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。
情報漏洩のマッピングと追跡	• 環境内の機密データとAIサービスのセキュリティ、インベントリー、コンプライアンスを一元的に把握できます。 • ミッションクリティカルなデータ アセットと構成へのすべてのアクセス経路をリスクとユーザーに基づいて詳細に表示します。 • 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。	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。

特長	特長	メリット
リスクの修復	• 重大度に基づいてリスクの優先順位付けを行えます。 • 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。	データの漏洩や侵害のリスクを最小限に抑えられます。
AIサービスの保護	• AIサービスとモデルをあらゆる側面から可視化し、制御します。 • AIデータ セットを検出、分類、微調整します。 • データの露出や過剰共有、データ ポイズニングなどの隠れたリスクを特定、修復します。	AIの安全な導入を加速させます。
一貫したポスチャーの維持	• エンドポイント、メール、SaaS、オンプレミス、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。	全体的なセキュリティ態勢を改善し、脅威に先回りで対応できます。
継続的なコンプライアンスの維持	• データとAI関連の規制上の基準に照らしてセキュリティ態勢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。 • 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。	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	• 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 アプリケーションをシームレスに統合できます。	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のAI活用型DSPM:主要コンポーネント

特長		DSPMに含まれる
データ検出	構造化/非構造化データ ストアの自動的な特定	✓
データの分類	すぐに使えるAIを活用型の検出とカスタム ルールによる機密データの自動的な検出と分類	✓
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	✓
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	✓
リスクの修復	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	✓
コンプライアンスの管理	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	✓
AI-SPM	AIとデータの使用状況の検出、インベントリー化、保護	✓

Zscaler DSPMのさらなる詳細

デモを依頼

ガイド付きのデモでZscaler DSPMをご体験ください。

デモを依頼

DSPMのウェビナーを見る(英語)

DSPMが複雑さを解消し、最新の高度な攻撃や脅威に対する優れたデータ セキュリティを提供しながら、セキュリティ部門の効率を最大化する仕組みをご確認ください。

オンデマンドで見る(英語)

詳細はこちら：www.zscaler.jp/dp/dspm

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™プラットフォームは、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.com/jp**をご覧いただくか、Twitterで**@zscaler**をフォローしてください。

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

zscaler™

Zero Trust Everywhere