

CISO向けガイド：AIを活用したDSPMで未来に備えたデータセキュリティを構築

2025

©2025 Zscaler, Inc. All rights reserved.

目次



現代のデータ セキュリティ環境の概要 3

CISOの新たな使命：AI時代に求められるデータ セキュリティの確立 4

DSPMの活用：AI時代のデータ セキュリティに求められる最新の必須要素 6

統合DSPMでデータ セキュリティ態勢を向上させる方法 7

- シャドーAI、シャドー データ、放棄されたデータへの対応 7
- AIを活用したデータ分類 8
- 予防的なリスク管理 9
- リアルタイムのガバナンスによるコンプライアンスの合理化 10
- 最小特権アクセスの適用 11
- ストレージと使用にかかるコストの最適化 12
- すべてのデータ環境での統一されたポリシーの施行 12
- インシデントへの迅速な対応 13
- AIセキュリティの強化 14

DSPMを活用した多様なデータ環境の保護 15

Zscaler DSPM 16

©2025 Zscaler, Inc. All rights reserved.

現代のデータ セキュリティ環境の概要

データが急激に増加し、多くのプラットフォームに分散することで、複雑さとコスト、そしてリスクが組織全体で増大しています。セキュリティ リーダーは現在、重要なデータを正確に把握して管理するという大きな課題に直面しています。さらに、その課題を一層難しくしているのが、AIの急速な普及です。これによりデータがさらに分散し、組織はデータ リスクやコンプライアンス違反のリスクに対してより脆弱になっています。

データ セキュリティ部門がセキュリティ リスクを効果的に軽減し、堅牢なコンプライアンスを確保するためには、自社全体のデータ環境をリアルタイムかつ包括的に把握できる先進的なツールが必要です。近年注目されているデータ セキュリティ ポスチャー マネジメント(DSPM)はAIと自動化を駆使して、データ セキュリティ リーダーがデータを継続的に可視化して把握するための強力な手段を提供します。

このeBookは、DSPMの変革力を深掘りしており、セキュリティ リーダーとセキュリティ部門がデータを事前予防的に保護することを後押しするものです。セキュリティとリスクの上級の専門家に特別に合わせた構成で、複雑なデータ セキュリティ環境に取り組むための実用的なインサイトを提供します。組織のデータ セキュリティ態勢を強化するための包括的なガイドとして、主な傾向の調査結果、喫緊の課題への対処方法、革新的な戦略を紹介し、変化を続けるAI時代においてデータ資産を保護する際にDSPMが果たす重要な役割を明らかにします。



©2025 Zscaler, Inc. All rights reserved.

CISOの新たな使命：AI時代に求められるデータ セキュリティの確立

AIとクラウド テクノロジーの急速な普及は、最高情報セキュリティ責任者(CISO)に新たな課題をもたらしています。これらの技術は、コスト削減やビジネス成果の拡大、そして大幅な生産性向上といった前例のない可能性を開く一方で、複雑なデータ セキュリティの課題も招いています。

急速に拡大するデータ環境

この課題の核心は、企業データの急増にあります。価値が高い機密情報は、もはや1か所に保管されるものではなくなりました。細分化が進み、AIエコシステム、SaaS、PaaS、マルチクラウドの展開環境、ハイブリッド クラウド アーキテクチャー、従来のオンプレミス インフラなど、多様な環境に分散しています。この急増は驚異的です。IDCは、データの年間増加率が21.2%となり、2026年までに22万1,000エクサバイトを超えると予測しています。

複雑さとリスクへの対応

こうした計り知れない複雑さのなか、CISOは、拡大し続ける一時的なデータ環境全体でデータ セキュリティを管理することを余儀なくされています。データは企業全体の数百もの多様なシステムやアプリケーションで絶えず作成、共有、保存されているため、包括的なデータ保護は極めて困難になっています。

AI時代における主要なデータ セキュリティ リスクとして、以下が挙げられます。

- **脆弱性とコンプライアンス リスク：**データが分散し断片化されると、データ侵害や規制違反のリスクが著しく高まります。データ ガバナンスとプライバシーに関する進化する規制(GDPR、CCPAなど)を確実に順守することは、非常に困難です。
- **ROTデータの脅威：**シャドー データ(未確認または不正なデータのコピー)や放棄データ(古くなったデータや忘れられたデータ)が制御なく拡散すると、深刻な脆弱性が生まれます。これがしばしば重大なセキュリティ上の見落としにつながり、攻撃対象領域を飛躍的に拡大します。
- **生成AIとLLMセキュリティの課題：**生成AIと大規模言語モデル(LLM)の急速な普及により、新たなリスクが浮上しています。これには、シャドーAI、データ漏洩(機密情報の意図しない流出)、AIシステム内の権限の問題、さらには新たな規制違反の可能性が含まれます。このため、AIセキュリティとLLMデータ ガバナンスを徹底することが不可欠です。

こうした多面的なデータ セキュリティの課題に対処するため、CISOには戦略的かつ積極的なアプローチを取ることが求められます。変化の激しい現代において機密情報を保護するためには、堅牢なデータ ガバナンス、高度なデータ保護ソリューション、包括的なAIセキュリティ フレームワークに重点を置く必要があります。

貴重なデータを失うリスク

標的型攻撃がますます増加し、規制要件も頻繁に変わるため、こうしたデジタル環境のセキュリティを優先することがCISOの重要課題となっています。過去12か月間にクラウド環境でデータ侵害を受けた組織は約44%にも上ります。[1]データ侵害は、情報漏洩、評判の低下、財務損失など、深刻な被害をもたらす可能性があります。AIとクラウド関連の攻撃の脅威環境が危険になるほど、CISOの役割はこれまで以上に重要になります。

444万米ドル

2025年に発生したデータ侵害の世界平均被害額[2]

1. Infosecurity Magazine、**Cloud Breaches Impact Nearly Half of Organizations**、2024 年 6 月 25 日。
2. **IBM、2025 年データ侵害のコストに関する調査**

©2025 Zscaler, Inc. All rights reserved.

以上のリスクに対処し、規制を確実に順守するために、セキュリティ リーダーはデータ環境を徹底的に理解する必要がありますが、データの量や種類、速度などの要因によってセキュリティの確保が難しくなっています。以下を把握しているリーダーは少ないというのが現状です。

- データの場所はどこか？
- どのデータ ストアに貴重なデータや機密データが含まれているのか？
- そのデータ ストアにアクセスできるのは誰/何で、どのAIツールか？
- データにはどのようにアクセスでき、どのようにAIツールと共有されるのか？
- データの価値はどれほどなのか？
- データはどのように処理されていて、コンプライアンス態勢にはどのように影響するか？

限界を超える必要性：従来のデータ セキュリティではAI時代に対応できない理由

データ セキュリティ環境は根本的な変化を遂げています。多くのCISOとセキュリティ部門は増え続ける脅威に対応するために、さまざまな種類のセキュリティ ツールを導入してきました。しかし、こうした従来のデータ セキュリティ ツールでは、現代の動的な環境に必要とされる重要なインサイトと保護を十分に提供できないことが次第に明らかになりつつあります。

AIセキュリティにおける未解決の課題

従来のソリューションには、新たに登場する技術特有の挙動や障害パターン、高度なデータ ガバナンス要件に対応できないという大きな欠点があります。特に、LLMや生成AIエージェント、その他の基盤モデルに対する十分な保護を提供できません。このような新しいAIリスクには、根本的に異なるアプローチが必要です。

新時代のセキュリティに必要な発想の転換

現在の新しい脅威環境では、単なる新しいソリューションでは不十分であり、AI時代に対応したデータ ガバナンスとセキュリティのための包括的かつ統合的なアプローチが求められます。AIセキュリティを後付け的要素として扱うのではなく、サイバーセキュリティ戦略の中核に据える新しい発想への転換が必要です。

予算が厳しくなる中での投資の最適化

これらの課題にさらに拍車をかけるのが、セキュリティ予算の厳しさであり、セキュリティ リーダーは投資を批判的に評価し、最適化する必要に迫られています。運用複雑性の軽減、コストの最小化、サイバーセキュリティ防御の強化、セキュリティ上の重大ギャップの解消といった領域が最も注目を集めています。逆説的ですが、この戦略的投資には多くの場合、セキュリティ部門自らがAIによる高度なセキュリティ ソリューションを活用することが含まれます。問題となる側面を持つ高度なAIツールですが、一方で、可視性の向上、リスク検出の加速、効率を高めたインシデント対応を提供し、最終的にはAI時代の脅威に対抗できるようセキュリティ態勢全体の強化を実現する、強力な支援ツールでもあります。

3. IBM、2025 年データ侵害のコストに関する調査

97%

AI関連の侵害を報告した組織のうち、AIに対する適切なアクセス制御が欠けていた組織の割合[3]



©2025 Zscaler, Inc. All rights reserved.

DSPMの活用：AI時代のデータ セキュリティに求められる最新の必須要素

前例のないAIリスクと従来のサイバーセキュリティ ツールが抱える限界が明らかになるなかで、現代のデータ セキュリティ アプローチは単に有益なだけでなく、不可欠なものとなっています。データ セキュリティ ポスチャー マネジメント(DSPM)は、重要な役割を担う欠かせないソリューションとして登場しました。

DSPMは、現代の複雑なデータ環境に対処するために必要なコンテキストと自動化を提供します。将来を見据えたアプローチを採用することで、CISOはデータをより深く理解し、規制を確実に順守しつつ、AI活用によるリスクを最小限に抑えることができます。

4. 同上

190万米ドル

セキュリティにAIと自動化を活用する組織の平均コスト削減額[4]



©2025 Zscaler, Inc. All rights reserved.

統合DSPMでデータ セキュリティ態勢を向上させる方法

ここでは、CISOがAI、ML、リスクの関連付けを効果的に使用してデータ セキュリティ態勢を改善できる方法をいくつか紹介します。

シャドーAI、シャドーデータ、放棄されたデータへの対応

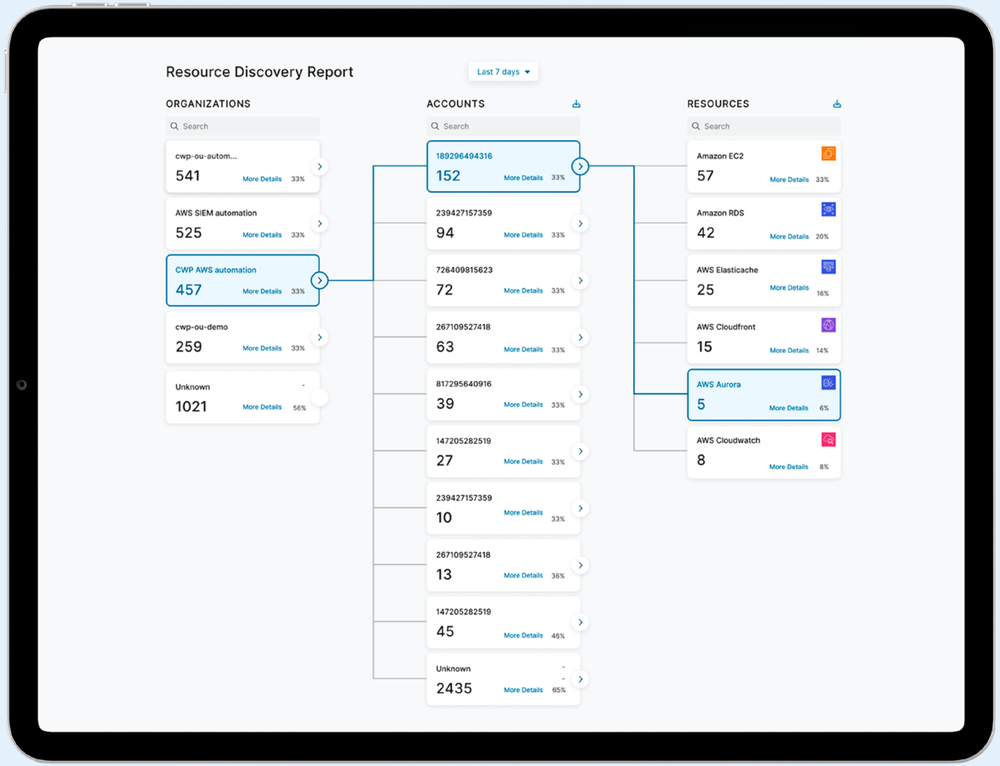
シャドー データ
シャドー データや活用されないまま放棄されたデータは、ITセキュリティ プロトコルやデータ ガバナンス フレームワークの範囲を超えて機能することが多いため、セキュリティに大きなリスクをもたらします。IBMによると、データ侵害の35%はシャドー データに関連しており、その侵害にかかる費用は平均で16%高くなっています。さらに、シャドー データ関連の侵害は、特定に26.2%、封じ込めに20.2%長く時間がかかっています[5]。シャドー データは適切な監視がされていない状態で、非構造化ファイルや構造化データベース、クラウド ストレージ、個人用デバイスに存在する可能性があります。一方、放棄されたデータはライフサイクル管理がされず、リスクになる可能性があります。DSPMは、AIを活用してデータ ストアを継続的に検出し、データ環境の全体的な可視性を向上させます。AIによってダーク データやシャドー データのカタログが自動生成されるため、組織はこれまで見落とされていたデータを明確に把握できるようになります。また、潜在的なリスクについてセキュリティ部門に警告し、侵害リスクを最小限に抑えます。DSPMは、データへのアクセスで見られる異常やパターンを監視して検出することで、潜在的なセキュリティ侵害を予測します。

シャドーAI
シャドーAIは、シャドーITと同様に、主に許可されていないAIツールを使用して企業の機密データにアクセスすることを指します。これは、データ セキュリティとコンプライアンスに広範な影響を及ぼす可能性があります。使いやすく、生産性を向上させるAIツールの普及により、従業員はIT部門の監督なしにこれらのツールを利用するケースが増えています。一見無害に思えるかもしれませんが、従来のセキュリティ フレームワークで単にAIツールを禁止するだけでは対処できない、連鎖的な問題を生む恐れがあります。

DSPMを使用すると、組織はAIの恩恵を受けることができます。AIツールをブロックしたり禁止したりするのではなく、DSPMを使用してシャドーAIのリスクを管理しながら、AIのメリットを活用できます。DSPMに組み込まれたAIセキュリティ機能により、データとAIモデルをエンドツーエンドで可視化し制御することで、AIに関連するリスクを未然に防ぎます。DSPMは以下を実現するのに役立ちます。

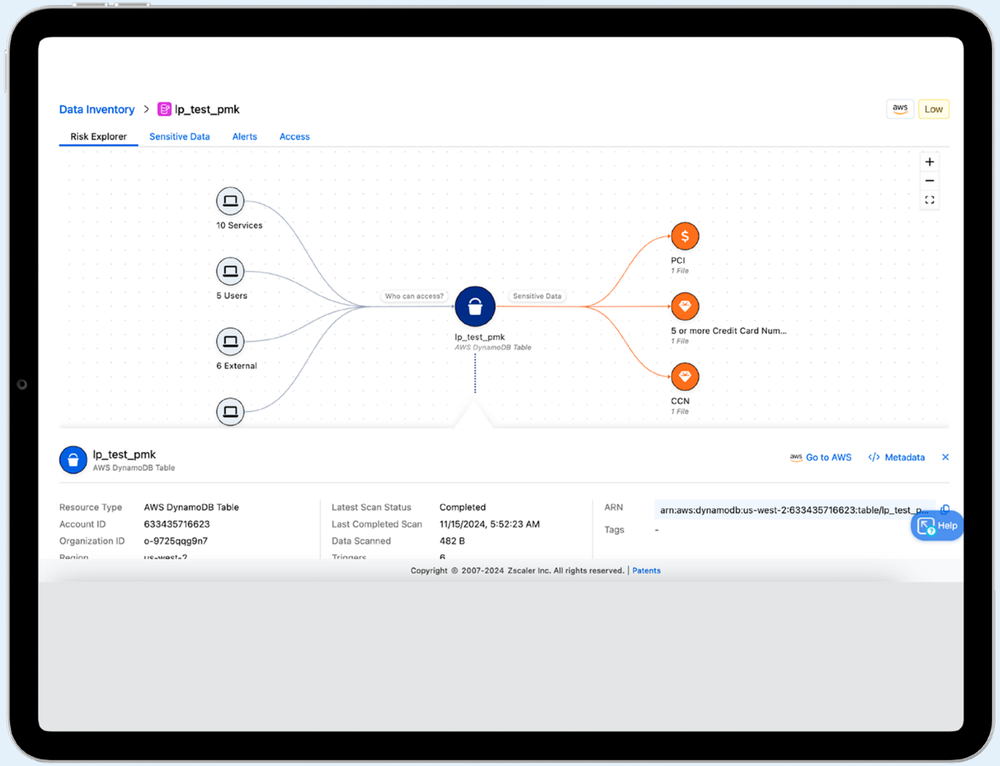
- AIモデル、エージェント、サービスを包括的に把握
- AIトレーニング データを特定し、データ ポイズニング、設定ミス、漏洩から保護
- 新たなAIコンプライアンス フレームワークに対応

DSPMを導入することで、セキュリティ リーダーは混乱したセキュリティ状況を管理されたイノベーションへと変革できます。これにより、統合的なデータ探索、コンテキストに基づくリスク評価、そしてAIのあらゆるやり取りに対応する自動ガバナンスが可能になります。



5. 同上

©2025 Zscaler, Inc. All rights reserved.



AIを活用したデータ分類

効果的なデータ分類は、堅牢なデータ セキュリティの基盤です。設定ミスや安全でない慣行によって引き起こされうる漏洩を回避するには、機密データを関連するリスクに予防的にマッピングすることが不可欠です。従来のアプローチの多くは手作業や単純なパターン認識に依存しているため、誤検知が増加したり、セキュリティ リソースの割り当てが非効率になったりする傾向があります。多くの場合、組織は正規表現ベースのソリューションに大きく依存していますが、これは柔軟性に欠け、誤検知による負担が大きいアプローチで、脆弱で非効率的であることが証明されています。現在のポイント製品を使ったアプローチも、分類を中央集約型の統合プラットフォームに組み込めないため、特に組織内でデータが移動する際に、アラートの一貫性が欠けたり、可視性が分断されたりする問題が生じています。

AIを活用したLLM分類機能を備えたDSPMにより、セキュリティ リーダーは従来の正規表現ベースのワークフローを強化できます。これにより、可視性と柔軟性が飛躍的に向上し、既知および未知の機密データを効果的に保護できるようになります。キーワード依存の手法とは異なり、LLM分類ではより深いコンテンツ識別が可能になります。高度な言語処理を使用してデータを分類し、事前定義されたパターンやキーワードを必要とせずに、コンテンツの意図とコンテキストを理解します。この仕組みを活用すれば、組織は既存のデータ保護の取り組みをさらに強化できます。また、これまで見落とされていた、あるいは検出できなかった新しいタイプの機密データを発見して保護することも可能になります。

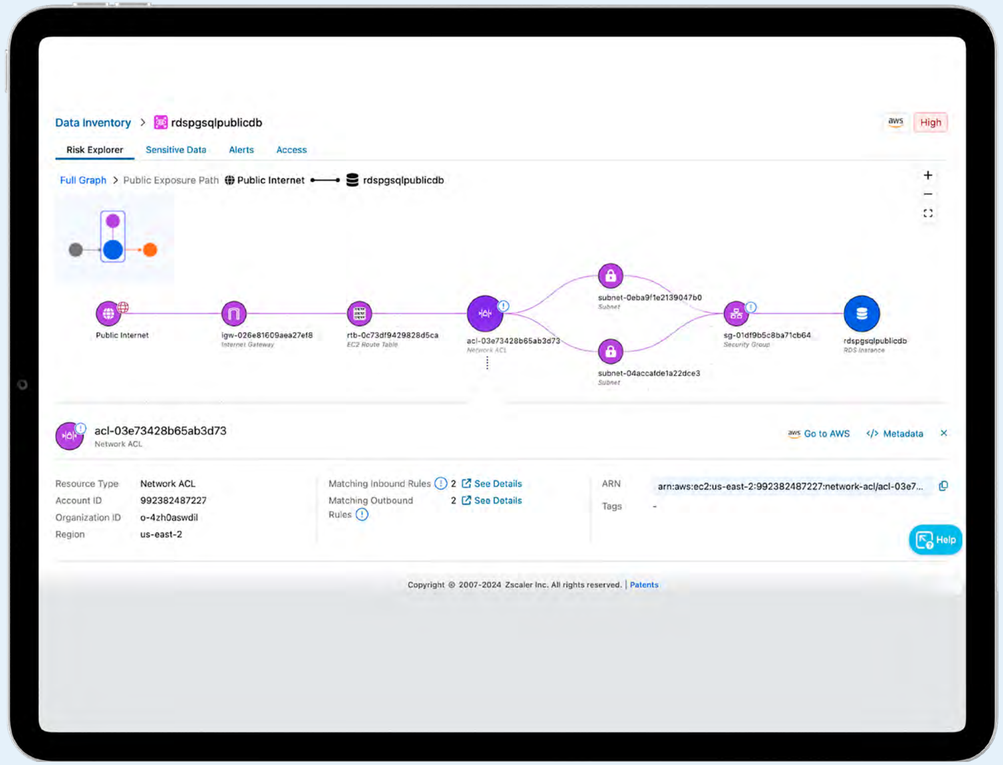
©2025 Zscaler, Inc. All rights reserved.

予防的なリスク管理

セキュリティ リスクを効果的に制御し、コンプライアンスを確保するためには、データ セキュリティ態勢を予防的に管理する方法が必要です。データ保護でAIを活用するユース ケースとして挙げられるのが、セキュリティに対する予防的アプローチと予測分析です。AIアルゴリズムはデータを分析して関連付けることで、潜在的なセキュリティ リスクを予測します。この予防的なアプローチにより、組織は脅威と重大リスクの一歩先を行くことができます。

AIと高度な関連付け技術を活用するDSPMでは、潜在的なセキュリティ インシデントにつながる可能性のあるデータのパターンと傾向を特定できます。また、データ ストアの価値(リスクの重大度)に基づいてデータ ストアに優先順位が付けられるため、最も重要な資産のセキュリティ対策に取り組むことも可能です。さらに、AIは多数のセキュリティ プロセスを自動化することで、セキュリティ専門家の作業負荷を軽減します。これにより、予防的なセキュリティ アプローチが可能になり、全体的な運用効率が向上します。

Zscaler DSPMの高度な関連付けは、点と点を予防的に結び付けて隠れたリスクを検出するため、最も重要なデータに対するセキュリティ対策を優先できます。



6. IBM、2025 年データ侵害のコストに関する調査

49%

侵害後のセキュリティに投資する組織の割合[6]

©2025 Zscaler, Inc. All rights reserved.

リアルタイムのガバナンスによるコンプライアンスの合理化

GDPRからSECまでにわたる進化し続ける規制と内部のセキュリティ プロトコルの順守は、AIとデータ セキュリティの基礎といえます。今日、組織はGDPRやHIPAAなどの既存の規制だけでなく、EU AI法やNIST AI600などのAIに特化した新しいフレームワークにも対応する必要があります。セキュリティとコンプライアンス リスクは切り離せない関係にあり、互いに大きな影響を及ぼし、組織の前途を左右することもあります。データ侵害は規制違反につながり、高額の罰金が課せられたり、企業イメージが低下したりするなどの深刻な影響をもたらす可能性があります。反対に、規制に従うことは組織を守り、脆弱性や脅威に対するAIとデータのセキュリティを強化することにつながります。

多くの規制は、AIと機密データの把握、データにアクセスできるユーザーの制限、リスクの継続的な監視の3つに重点を置いています。これは簡単に聞こえるかもしれませんが、AIとデータ環境の複雑さを考えると非常に困難です。また、規制は新しいテクノロジー、プライバシーに関する懸念の変化、世界経済の相互接続性の高まりなどにより、絶えず進化しています。こうした規制環境でコンプライアンスを維持するには、常に警戒して適応する必要があります。従来のコンプライアンス アプローチの断片的なビュー、手動評価、事後対応では、明確さや効率性を提供することは困難です。

DSPMは、リアルタイムのデータ コンプライアンスとガバナンス機能でコンプライアンス プロセスを合理化します。DSPMソリューションはデータ コンプライアンスの状態を一元的に可視化し、包括的な分析、ベンチマーク、修復、レポート生成の機能を提供するため、コンプライアンスのギャップにすばやく対応できます。これらの機能は、データの状態を明確に把握してリスクを軽減することが欠かせない規制の厳しい業界では特に重要です。ガイド付きの修復手順や自動化されたワークフローなどがコンプライアンス ダッシュボードに示されるため、セキュリティ部門は迅速かつ効果的に行動できます。また、AIをガバナンスに適用すれば、堅牢なセキュリティ対策を維持しながら、規制要件を満たすことができます。

63%

AIガバナンス ポリシーを整備していない組織の割合[7]



7. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls

©2025 Zscaler, Inc. All rights reserved.

最小特権アクセスの適用

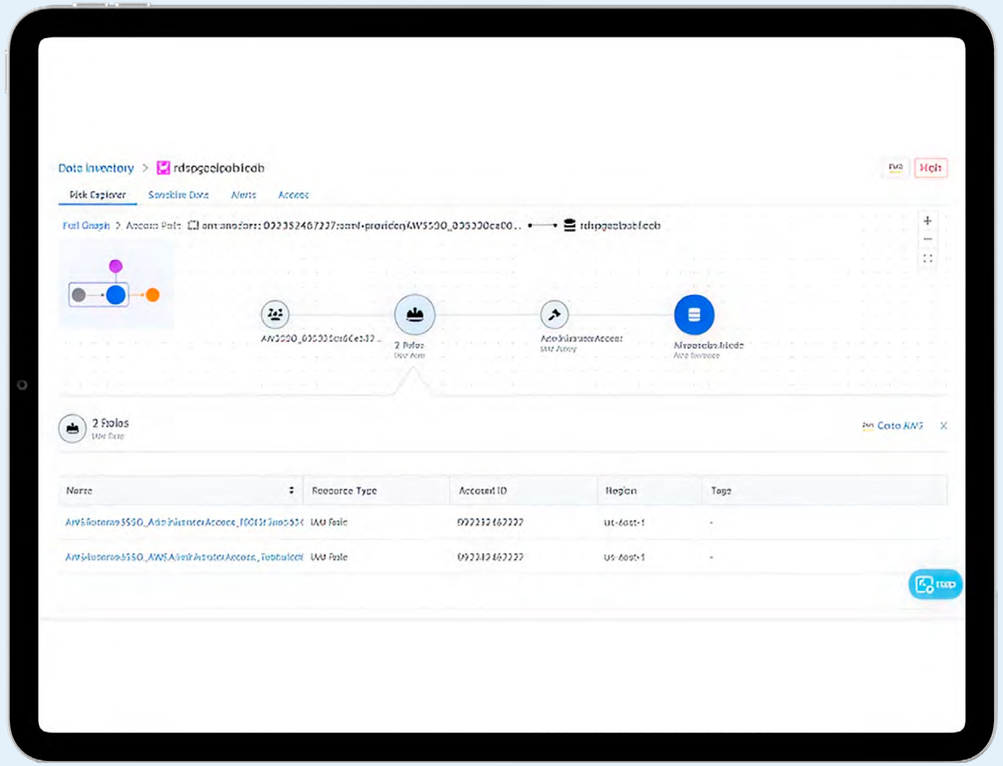
膨大な量のユーザー、アプリケーション、リソースが存在するクラウド データ環境には、不適切なアクセス制御、アイデンティティーの無秩序な増加、孤立したデータ ストアといった大きなリスクがあります。約90%の組織がアイデンティティー関連の侵害を受け、高コストなセキュリティ インシデントが発生しています。

さらに、AIモデルとLLMを利用したツールにより、不正なデータ アクセスに関する別のリスクも生じています。主なリスクとして、意図しないまたは許可されていない機密データの開示、データの持ち出し(AIの出力を介した機密データの窃取)、侵害されたアイデンティティーがAIシステムを悪用して不正アクセスを取得する高度な攻撃などが挙げられます。

そのため、データ ストアへの最小特権アクセスを確保することが、データ セキュリティの基本原則となります。データや権限の無秩序な増加、複雑なAIやマルチクラウド アーキテクチャーといった要因により、データ アクセス ガバナンスはますます困難になっています。しかし、機密データの漏洩は通常、高度なサイバー攻撃の起点であるため、データ アクセス ガバナンスはデータ セキュリティの重要な要素であることに変わりはありません。

DSPMはデータ アクセス ガバナンスに対する統合的なアプローチを提供し、データ セキュリティ態勢やユーザー行動を継続的に監視します。アイデンティティーやデータ アクセス管理におけるロールや権限、関連する属性を精査し、データ ストアへの危険なアクセス経路を迅速に特定します。また、構造化データ、非構造化データ、オンプレミス、マルチクラウド、SaaS環境にわたるさまざまなデータをサポートし、異なるデータ資産やAIエコシステム全体に対してリスクの特定、対応を可能にします。これにより、一貫したアクセス ポリシーの施行が実現します。AIによってアクセス パターンと潜在的な脆弱性に関する詳細なインサイトが提供されるため、データ セキュリティ部門は最小特権アクセスをより効果的に施行できます。このアプローチにより、不正アクセスのリスクが軽減され、データ環境の全体的なセキュリティが強化されます。

8. Security Today、Study: **90 Percent of Organizations Experienced an Identity-Related Incident in Last Year**、2024 年 6 月 5 日。



90%

アイデンティティー関連のインシデントが発生した組織の割合[8]

©2025 Zscaler, Inc. All rights reserved.

ストレージと使用にかかるコストの最適化

データ部門は、重複するまたは放置されたデータ リポジトリーを特定し、それらを排除したり、より費用対効果の高いストレージ ソリューションへ移動させたりすることで、ストレージと使用にかかるコストを最適化する必要があります。従来の方法ではこうしたデータを適切に特定、管理できない場合が多く、結果として余分なストレージ費用が発生します。

DSPMは、重複するまたは放置されたデータ ストアに関するインサイトを提供することでこの問題に対処し、組織が適切な対策を講じられるようにします。Zscaler DSPMのような製品は、重複するまたは放置されたデータ ストアを包括的に表示し、安全に削除または移行できるデータを特定します。

AIによるインサイトにより、過剰なストレージ費用を削減し、機密データの適切な管理と保護を確保できます。

すべてのデータ環境での統一されたポリシーの施行

従来の方法でさまざまな環境にわたって一貫したデータ セキュリティ ポリシーを維持するのは簡単ではありません。DSPMソリューションは、マルチクラウド環境に統一されたアプローチを提供することで、データ セキュリティの課題を解消します。このソリューションにより、すべてのデータ環境で一貫したポリシーを施行できるようになります。

Zscaler DSPMは、データ セキュリティのための統一された戦略を提供します。この戦略により、すべてのデータ環境で統一されたポリシーを確立し、クラウド データの包括的な監視を徹底しながら、リスクの特定と解決のプロセスを合理化できます。AI/MLによるインサイトを活用することで、データ侵害のリスクを軽減し、データ保護のルールをより適切に順守できます。



©2025 Zscaler, Inc. All rights reserved.

インシデントへの迅速な対応

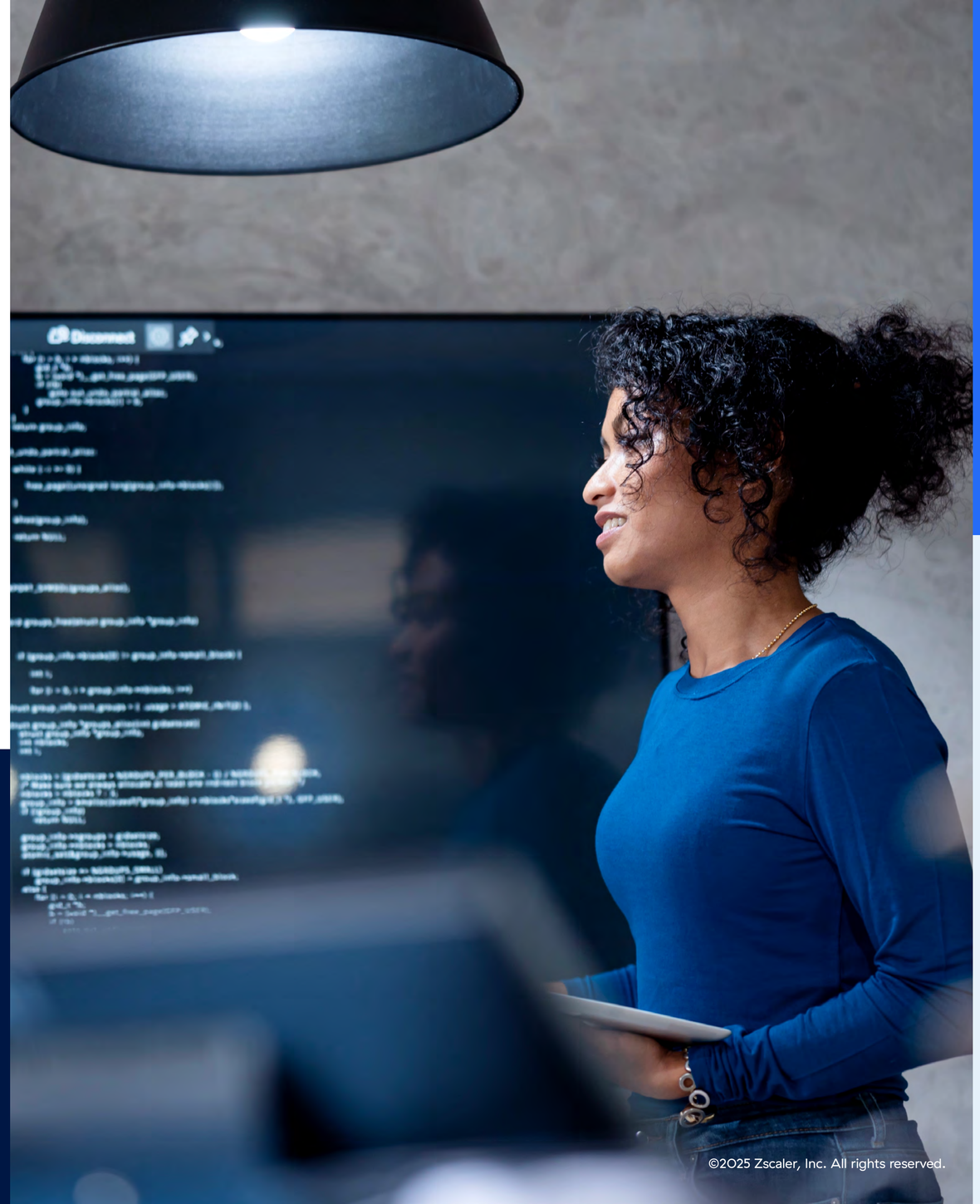
リスクの特定と軽減は、データ セキュリティ専門家の基本的な役割です。脅威が進化するスピードは速いため、リアルタイムの対応が求められますが、従来の方法では、AIが牽引する動的な脅威環境に対抗できず行き詰まる可能性があります。この課題を解消するのが、AIを活用したセキュリティの自動化です。

DSPMは、データを常に監視し、異常を検知することで、脅威への迅速な対応を支援します。DSPMソリューションは、高度なリスク関連付けと適応型のアクセス インテリジェンスを提供することで、リスク軽減を強化します。たとえば、Zscaler DSPMには、Zscaler ThreatLabzが提供する脅威インテリジェンス、綿密な修復ガイダンス、迅速なセキュリティの実装が組み込まれています。AI活用型の高度な脅威相関により、組織は潜在的なリスクや重要な攻撃ベクトルを特定し、最も重大なリスクに集中して取り組めるようになります。

9. Statista、**Mean time to identify and contain data breaches worldwide from 2017 to 2024**、2024 年 12 月 9 日閲覧。

194日間

データ侵害を特定するまでの平均期間[9]



©2025 Zscaler, Inc. All rights reserved.

AIセキュリティの強化

多くの組織がAIアプリケーションを急速に採用していますが、生成AI (GenAI)や大規模言語モデル(LLM)などのAIアプリケーションは、重大なデータ侵害やコンプライアンス違反のリスクをもたらします。最近の報告によると、13%の組織がAIモデルまたはアプリケーションの侵害を受けており[10]、AIが価値の高い標的となっていることがわかります。

生成AIを業務全体に統合している場合、これらのモデル内で機密データが誤用されないようにするための対策を講じる必要があります。セキュリティ部門は、データのフラグ付け、タグ付け、分類を優先し、さまざまな部門が責任を持って生成AIを活用できるようにしなければなりません。

DSPMは、統合されたAI-SPM機能により、生成AIの環境にあるデータの制御と保護を強化します。データを綿密に識別し分類することで、機密情報がLLMに取り込まれるのを防ぎ、データ侵害とコンプライアンス違反のリスクを軽減します。DSPMは「データファースト」のアプローチを採用し、インフラだけでなく、AIが利用する情報の保護に重点を置いています。データのライフサイクル全体を通じて継続的にデータを検出、分類、監視することで、データ ポイズニング、機密データの漏洩、モデルの盗用といったAI特有のセキュリティ リスクを軽減します。

AI-SPM機能が組み込まれたDSPMを採用すれば、AIアプリケーションへの信頼を強化できます。そうすることで、重要なデータを保護するだけでなく、AIアプリケーションの信頼性と安全性を高められます。



10. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls

©2025 Zscaler, Inc. All rights reserved.

DSPMを活用した多様なデータ環境の保護

DSPMの戦略的な使用は、より堅牢なデータ セキュリティを追求するうえで最も重要です。これらのテクノロジーは、最新のデータ環境の複雑さを効果的に管理するために必要なコンテキストと自動化を提供します。セキュリティ リーダーは予防的な対策をとることで、機密データをより効果的に保護し、コンプライアンスを確保しながら、生成AIのような進歩的なテクノロジーに関連するリスクを軽減できます。

「これまで認識されていなかったデータ リポジトリーを特定し、関連するセキュリティ リスクやプライバシー リスクを軽減することが組織の喫緊の課題となっているため、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、Innovation Insight: Data Security Posture Management、
Brian Lowans, Joerg Fritsch, Andrew Bales、
2023年3月28日

Gartnerは、Gartner Inc.または関連会社の米国およびその他の国における登録商標およびサービスマークであり、同社の許可に基づいて使用しています。All rights reserved.



©2025 Zscaler, Inc. All rights reserved.

Zscaler DSPM

Zscaler DSPMは、SaaS環境、AWS、Azure、GCPなどのパブリック クラウド環境、オンプレミス、エンドポイントに対応し、構造化データと非構造化データを保護する、最も包括的な統合型データ保護プラットフォームです。

また、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。

Zscaler DSPMは、AIを活用した統合アプローチにより、IaaS、SaaS、オンプレミス、エンドポイントなど、すべてのデータ ストアにわたる強力なデータ保護を確保します。Zscaler Data Securityプラットフォームとネイティブに統合されており、すべてのデータの完全な把握と制御を、単一のプラットフォームで行えます。

Zscaler Data Securityプラットフォームは、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クラス最高の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、転送中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。

ソリューションの詳細：zscaler.com/jp/dspm

デモ： DSPMのインタラクティブな製品ツアー

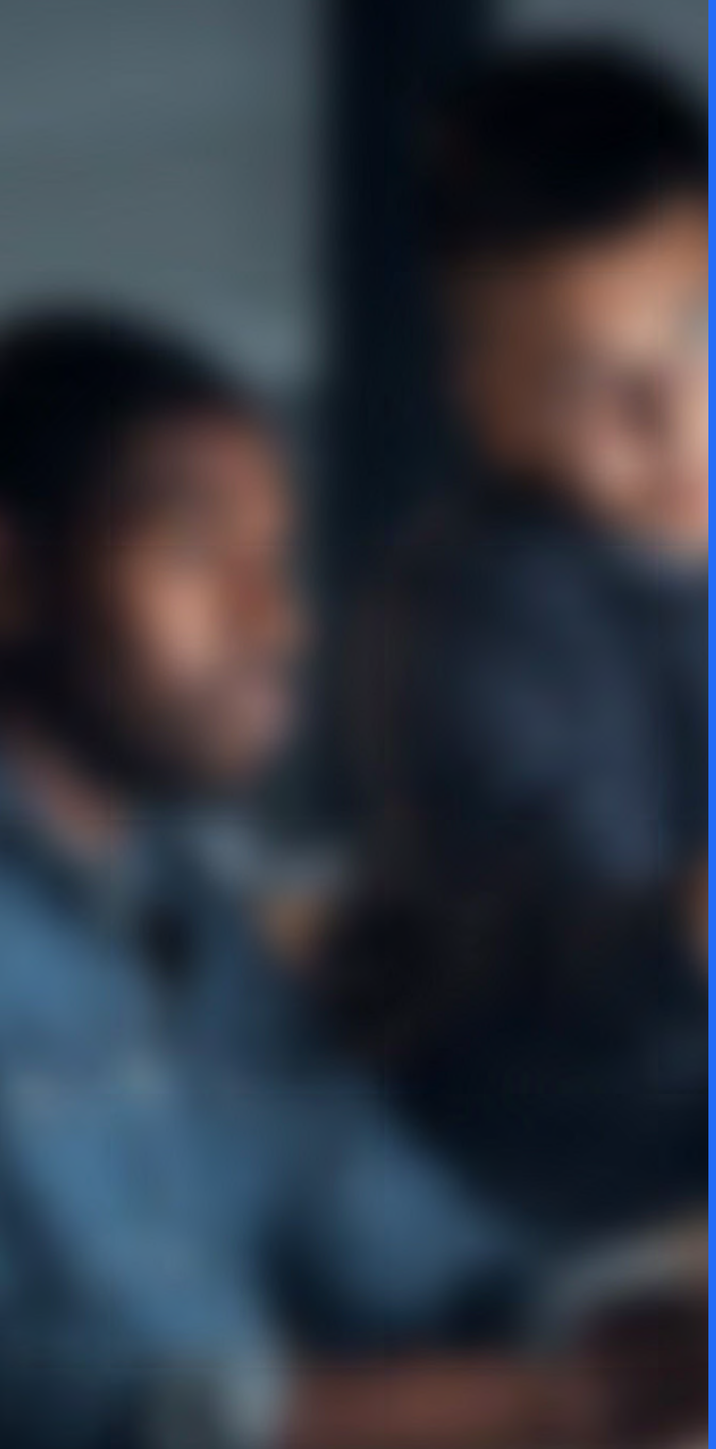


データ保護戦略にDSPMを取り入れるべき理由

オンデマンド ウェビナーを見る(英語) ⟶

DSPM関連のリソースはこちらのQRコードからご確認いただけます。

©2025 Zscaler, Inc. All rights reserved.





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™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。

© 2025 Zscaler, Inc. All rights reserved. Zscaler™および**zscaler.com/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、または(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.com/jp**