Microsoft Security

データ セキュリティ インデックス

データを安全に保ち、
生成 AI をナビゲートするための
トレンド、インサイト、戦略

2024 年レポート

まえがき

進化するデータ セキュリティの状況に関する調査を始めて 2 年目を迎えるにあたり、目の前にある課題と機会はかつてないほど深刻になっています。昨年、データ セキュリティ インシデントの深刻さが増しました。このデータ中心の時代において、データの保護を維持するために使用される戦略とツールは急速なペースで進化しています。

今年は、新たなフロンティア、データ セキュリティ戦略における生成 AI (AI) の役割と影響について探ります。

AI は、これまでにないほどのイノベーションと効率化を実現することで、世界中で波を起こしています。しかし、この大きな可能性を活用することで、組織は、データ セキュリティ リスクと、それがデータ セキュリティ チームの責任をどのように形作るかにも関心を寄せています。AI は、組織が基本的なデータ セキュリティ対策を強化して、データの過剰共有や漏えいの影響を最小限に抑える準備をし、AI を安全に導入するためのプロセスを構築するための促進剤であると考えています。一方、AI は、保護における隠れたリスクやギャップを特定し、保護ポリシーを推奨して、より速いセキュリティ インシデントの調査と修復を支援することにより、組織がデータ セキュリティ対策を強化するのにも役立ちます。

マイクロソフトの調査の目的は、データ セキュリティのリーダーに実用的なインサイトとガイダンスを提供して、チームがデータ セキュリティ戦略を自信を持って適応させ、AI の使用を効果的に保護し、データ セキュリティ戦略に AI を組み込めるようにすることです。AI の広がりと可能性は目覚ましいものですが、AI はハイブリッド ワーク、クラウド、モビリティなど、企業を席巻する最新の変革の波に過ぎません。近年、リスクを軽減して効果を最大化するために AI の使用を可視化することに対して、時代を超越した必要性が浮き彫りになりました。これらの知見から得た情報をもとに、AI で使用されるデータを適切に保護し、AI を使用してデータのセキュリティ対策を強化することで、チームが将来の課題に対処する際の生産性、レジリエンス、アジリティを向上させることができます。

ぜひ最新の調査結果をご覧いただき、このインサイトを皆様のデータ セキュリティ体制の強化にお役立てください。また、皆様が AI を活用して包括的なデータ セキュリティ戦略を構築し、さらなるイノベーションを解き放ち、私たち全員にとってより安全な未来を確保するきっかけとなることを願っています。

Rudra Mitra
コーポレート バイス プレジデント
マイクロソフト データ セキュリティおよび
コンプライアンス担当

はじめに

組織では年間平均 156 件のデータ セキュリティ インシデントが発生しており、これらのインシデントの影響はデータ セキュリティの意思決定者にとって常に懸念事項となっています。それには正当な理由があります。攻撃者があらゆる脆弱性を悪用し、常に進化し続ける脅威状況では、1 つのインシデントが財務上、社会上の大きな損害を与える可能性があります。これは、AI の急速な導入によって誇張されるだけであり、適切な保護とセキュリティ対策をしなければ、ユーザーが誤ってまたは悪意を持って機密性の高いビジネス クリティカルなデータ (従業員や顧客の情報、知的財産、財務予測、運用データなど) を危険にさらす可能性があります。組織がこの幅広い機密データを保護する新しい方法を模索する中、多くの意思決定者は AI の劇的な台頭に注目しています。

AI の課題は 2 つあります。組織の 3 分の 2 が、従業員の許可されていない AI ツールの使用を認めていることを考えると、従業員が AI ツールを安全に使用していることを保証することが重要です。同時に、高度なデータ セキュリティ戦略において、AI を効果的なツールとして活用するチャンスでもあります。

AI を活用したデータ セキュリティ ソリューションは、脅威をリアルタイムで特定して対応し、データ セキュリティ プログラムの全体的な速度と精度を向上させ、データ セキュリティ インシデントを発生前に防止するのに役立つインサイトを提供する上で、すでに重要な役割を果たしています。組織は、AI がもたらすリスクを管理するだけでなく、AI の能力を活用して、人間による処理が困難なパターンを特定して分析し、最終的にはますます巧妙化するサイバー攻撃を撃退する必要があります。

2023 年、マイクロソフトは独立した研究機関である Hypothesis に委託して、800 人以上のデータ セキュリティ担当者を対象に多国籍調査を実施し、パートナーと顧客により良いサービスを提供して、ビジネス リーダーが独自のデータ セキュリティ戦略を策定するのを支援するためのデータ セキュリティ インデックス イニシアチブに着手しました。

2024 年のこのレポートは、以前の調査に基づき、1,300 人を超えるデータ セキュリティ担当者を対象として拡大された多国籍調査からの新しいインサイトを用いて作成し直しています。調査した市場全体で一貫したインサイトとトレンドが明らかになる一方で、世界中の最新のデータ セキュリティと、AI プラクティスおよびトレンドに関する新たな知見が得られました。

hypothesis Microsoft Security

主な調査結果

1

データ セキュリティを取り巻く状況は依然として分裂しており、AI の使用に関連する従来のリスクと新しいリスクの両方にわたって、まとまりのあるデータ セキュリティ戦略の必要性が高まっています

組織は、データ セキュリティ対策に高いレベルの満足度と自信を持っていると報告しています。ただし、特に組織が現在のデータ セキュリティ ポリシーと AI アプリケーションの使用 / 導入の増加との間にギャップを見つけているため、データ セキュリティ インシデントの重大度は上昇し続けています。多くの組織はこれらの利害と義務に直面し、依然として複数のデータ セキュリティ ツールに依存しているため、全体的な脆弱性とリスクを高める可能性があります。

2

エンド ユーザーが AI アプリを採用する機会が増えるにつれ、組織の最も機密性の高いデータの整合性に対するリスクが増大し、より高い可視性と新しい保護制御が必要になります

AI ツールが日常業務に不可欠になるにつれ、組織はデータ セキュリティのリスクを懸念しています。彼らは防御を強化する必要性を認識し、AI によって引き起こされるデータ セキュリティ インシデントの防止に取り組んでいますが、これらのツールの不正使用は、より堅牢な可視性の必要性を浮き彫りにします。

3

意思決定者は、データ セキュリティの取り組みを後押しする AI の可能性を楽観視しています

組織は、検出と対応の機能を向上させるために AI を組み込んだデータ セキュリティ ツールに積極的に投資しています。AI は、保護されていないデータの検出、保護ポリシーの推奨、データ セキュリティ インシデントの迅速な調査と修復に役立つため、最終的にデータ セキュリティ チームは戦略的な作業により多くの時間と注意を集中させることができます。また、AI の使用は、組織の全体的なデータ セキュリティ戦略 (特にインシデントに迅速かつ正確に対応する能力) に対する自信と満足度を高めます。

1

データ セキュリティを取り巻く状況は依然として分裂しており、AI の使用に関連する従来のリスクと新しいリスクの両方にわたって、まとまりのあるデータ セキュリティ戦略の必要性が高まっています

データ セキュリティ対策に対する意思決定者の自信と、データの真の保護レベルとの間には乖離があります

2023 年に報告されたように、意思決定者の大多数はデータ セキュリティ戦略に自信を持っており、74% が 2024 年に現在のソリューションに満足していると報告しています。また、機密データの追跡と管理に安心感を持っており、88% が自分の重要な情報の所在場所をほとんど知っていると考え、85% が、データが適切に分類され、ラベル付けされていると述べています。また、ほとんどの意思決定者は自分の防御対策を信頼しており、79% がデータ流出を防止できると確信しており、76% が対策ではなく事前対応と回答しています。

ただし、インシデントの重大度が増し続けるにつれて、彼らの自信はテストされています。**年間データ セキュリティ インシデントの平均数は、2023 年の 166 件、2024 年の 156 件と高いままであり、これらのインシデントの重大度は、深刻なインシデントの割合が 20% から 2024 年の 27% に増加しています。**

156
データ セキュリティ インシデントの数

27%
重大と見なされるインシデントの割合 (2023 年の 20% から増加)

63%
確認される 1 日あたりのアラートの割合

「ソフトウェア プラットフォームが確立された場所、そのデータが保存される場所、そのデータにアクセスするユーザーにより、AI ツールとベンダーのデータ セキュリティと管理が複雑になりました。当社には 100 年分を超えるデータがあり、事業を展開するすべての管轄で法的要件に従って保護および管理する必要があります」と、重機メーカーの情報ガバナンス担当シニア マネージャーは述べています。

データ セキュリティ インシデントの重大度が増すと、結果的にアラートの量は増加しています。**組織は 1 日平均 66 件のアラートに直面しており、2023 年の 52 件から増加しています。**その数は組織の規模によって大きく異なり、中規模企業 (従業員 500 ～ 999 人) と大企業 (従業員 1,000 ～ 4,999 人) は平均 56 アラートを受信し、超大企業 (従業員 5,000 人以上) は平均 80 アラートを受信します。

膨大な量のデータ セキュリティ アラートを考えると、ほとんどの組織が追いつかないのは当然のことです。データ セキュリティ チームは、平均して、日々のアラートの 63% を確認しています。これらのアラートの 35% は誤検知であることが判明しています。この制御感と運用実態の不一致により、データ セキュリティ チームは、適切な保護が実施されているかどうかや、それらを微調整する方法を評価しようとする一方で、潜在的に深刻なインシデントが見落とされる可能性があることを懸念して、圧倒されます。

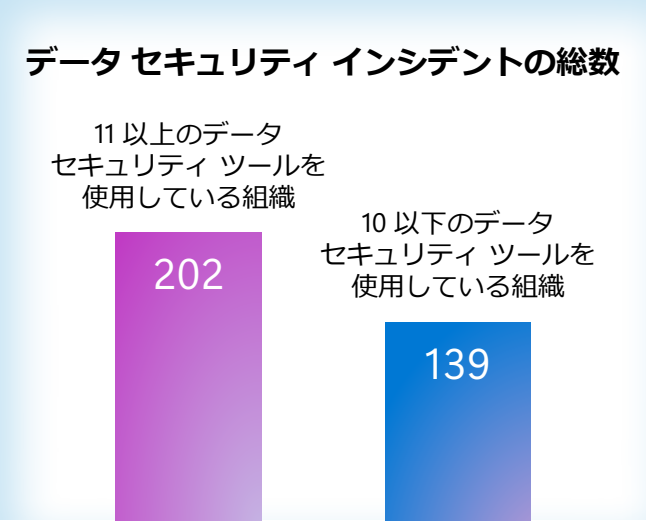
AI ツールの使用に関連する従来のデータ リスクと新たなデータ リスクに対処するために、より堅牢でまとまりのあるデータ セキュリティ戦略の必要性が高まっています

自由に使えるツールの数は増加していますが、多くの意思決定者は多ければ良いとは限らないことを認識し続けています。実際、21% が、最大の課題 / リスクとして、異なるツールによってもたらされる統合的かつ包括的な可視性 (およびリスクに対する理解の共有) の欠如を挙げています。[1]

ほとんどの意思決定者 (82%) が、包括的で完全に統合されたプラットフォームが複数の孤立したツールを管理するよりも優れていることに同意しています。**平均して 12 種類ものデータ セキュリティ ソリューションをこなしているため、複雑化が進み脆弱性も増しています。**これは特に大規模な組織に当てはまります。平均して、中規模企業は 9 ツール、大企業は 11 ツール、超大規模企業は 14 ツールを使用しています。

データは、使用されているデータ セキュリティ ツールの数とデータ セキュリティ インシデントの頻度の間に強い相関関係があることを示しています。中規模および大規模企業では年間平均 89 件のインシデントが報告されていますが、超大規模企業では年間 248 件という驚異的なインシデントが発生しています。この明確な違いは、大規模な組織がデータ セキュリティ対策にかなりの自信を持っているにもかかわらず、直面するリスクが高いことを浮き彫りにしています。

2024 年には、データ セキュリティ ツールの使用数が多い (11 以上) 組織では、平均 202 件のデータ セキュリティ インシデントが発生しましたが、ツールが 10 以下の組織では 139 件でした。



断片化されたソリューションでは、データが孤立し、ワークフローがばらばらになっているため、潜在的なリスクに対する包括的な可視性が制限される可能性があるため、データ セキュリティ体制を把握するのが難しくなります。ツールが統合されていない場合、データ セキュリティ チームは、データを関連付け、まとまりのあるリスク ビューを確立するためのプロセスを構築する必要があります。これが盲点となり、リスクの効果的な検出と軽減が困難になる可能性があります。

懸念事項が高まっているのは、AI アプリケーションの使用によるデータ セキュリティ インシデントの増加です。このインシデントは、2023 年の 27% から 2024 年には 40% へとほぼ倍増しました。このインシデントの増加は、マルウェアとランサムウェア攻撃の急増によって促進されており、2023 年の 50% から最大 59% に増加しています。AI アプリの使用による攻撃は、機密データを公開するだけでなく、AI システム自体の機能を危険にさらし、すでに分裂しているデータ セキュリティ環境をさらに複雑にします。つまり、AI ツールの使用に関連する従来のリスクと新たなリスクの両方に対処できる、より強力でまとまりのあるデータ セキュリティ戦略がますます緊急に必要とされています。

1. マイクロソフトの委託により MDC Research が実施した、データ セキュリティ、ガバナンス、コンプライアンス、およびプライバシーの意思決定に関する 2024 年 9 月の調査

次のステップ

データ セキュリティ インシデントの重大度が増している中、AI が役立つ好機が浮き彫りになっています。最先端の組織は、AI を活用したデータ セキュリティを実装して、インシデントの優先順位付け、データ分類の自動化、現在の保護ポリシーの微調整方法の特定に役立てています。AI はインシデント アラートの潜在的な重大度を自動的に統合し、データ セキュリティ チームに迅速な対応のための実用的なインサイトを提供して、誤検知に費やす時間を削減します。これにより、ワークフローが合理化され、データ セキュリティ チームはより戦略的なデータ セキュリティの改善と事前対策に集中できます。

2

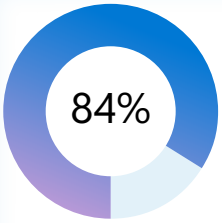
エンド ユーザーが AI アプリを採用する機会が増えるにつれ、組織の最も機密性の高いデータの整合性に対するリスクが増大し、より高い可視性と新しい保護制御が必要になります

AI はますます日々の業務に不可欠な存在となっています。組織はこの新しい現実を受け入れ、積極的に適応する必要があります

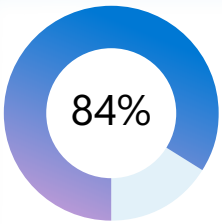
従業員による AI ツールの急速な導入は、データ セキュリティに対する組織のアプローチに大きな変化を促しました。AI は生産性とワークフローを変革していますが、他の新しいテクノロジと同様に、既存のリスクを増幅させたり、機密情報を保護するための別のアプローチを必要とする新しいリスクを発生させる可能性もあります。その結果、企業は依然として急速に変化する状況の中に足場を見出しています。運輸業のエンジニアリング兼アナリティクス担当ディレクターは、次のように主張しています。「私たちは AI 側でデータをより注意深く監視しています。生産性とセキュリティ、正確性、プライバシーの間には対立がありました。」

従業員による AI の使用を保護する自信はまだまちまちです。大多数 (84%) は、データ入力の管理と検出についてより自信を持ちたいと考えています。組織の 22% がデータのセキュリティを維持する能力に非常に自信を持っていると回答していますが、ほとんどの組織 (59%) は「非常に自信がある」とのみ回答しており、改善の余地があることを示しています。ほとんどの企業 (86%) は、AI ツールによって生成されたデータの管理と検出について、より強気になりたいと考えていることを認めています。

AI が日々の生産性に不可欠になるにつれて、AI アプリの使用により、データ セキュリティ インシデントに対する懸念も高まっています。**組織のほぼ 3 分の 1 (31%) は、従業員の AI の使用によるデータ セキュリティ インシデントの増加を予測しており、84% がこれらのリスクから保護するためにさらに対策を講じる必要があることを認めています。**このような不安は、最大規模の組織の間で特に高くなっています。中規模企業の 26% が AI 関連のデータ セキュリティ インシデントの増加を予想し、大企業の 29% が増加を予測し、さらに超大規模企業の 36% を占めるかなり上位のグループが増加を予測しています。



AI アプリやツールへのデータ入力の管理や検出に対する自信を深めたい



従業員による AI アプリや AI ツールの使用リスクから保護するために、より多くの対応を行う必要があると回答

AI の不正利用が蔓延している割合

40% は、自社の AI アプリがすでにデータ セキュリティ インシデントで侵害または侵害されていると報告しています。繰り返しになりますが、この数字は大規模な組織ほど高くなっています。中規模企業ではインシデント発生率が 36%、大企業では 38%、さらに超大規模企業では 44% と最も高くなっています。

AI の不正使用は、多くの場合、従業員が個人の資格情報でログインしたり、個人のデバイスを使用して業務関連のタスクを行ったりすることで発生します。**平均して、組織の 65% が、従業員の許可されていない AI ツールの使用を認めています。**従業員は、次のようにして許可されていない AI ツールを使用しています。

- 53% が仕事目的で個人の資格情報でログインする
- 48% が仕事で AI を使用する場合に個人のデバイスを使用する
- 47% が個人的な目的で AI を使用する場合に仕事用の資格情報を使用する

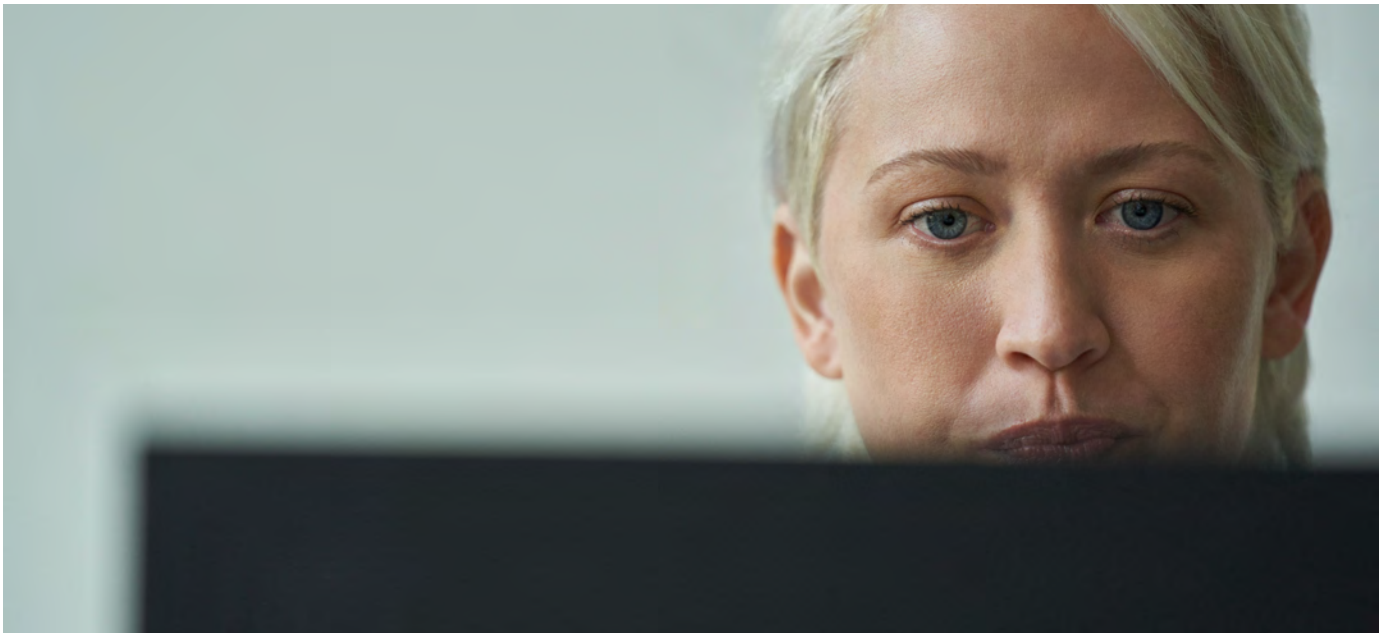
全組織の半数が、従業員が安全でない方法で AI アプリを使用した場合にリスクを検出して軽減するコントロールが欠如していることを懸念していると述べています。この数字は企業規模によって異なり、中規模企業の 43%、大企業の 50%、超大規模企業の 54% が、これらのリスクを管理する能力に懸念を表明しています。

AI の利用が増えていることを考えると、より多くのデータ セキュリティ制御が必要です

日常業務にますます AI が組み込まれるにつれて、組織はより強力な保護の必要性を認識しています。**企業の 96% が従業員によるツールの使用に懸念を抱いていますが、ほぼ同数の企業に、懸念を克服するためのソリューションに投資する意思があります。**

「注目すべきは、どのようにして AI の先を行くかです。セキュリティの焦点は、データ サイズを縮小し、データをより注意深く監視することです。AI 側では、バイアスを特定するためにモデルをより典型的にするために、より多くのデータが必要です。では、どのようにして調整すればよいのでしょうか？」と、運輸業のエンジニアリング、アーキテクチャー、アナリティクス担当ディレクターは言います。意思決定者の大多数 (87%) は、AI ツールを使用するための安全なプラクティスにおける従業員のトレーニングに時間とお金の両方を費やす準備ができています。**これは、85% が、従業員が競争力を維持するためにそれらのツールの使用が重要であると述べているためです。**

ほぼすべての組織 (93%) は、AI の使用に関する統制を開発または実装する段階にありますが、多くはまだ初期段階にあります。AI のデータ セキュリティ制御を完全に実装している企業は 39% のみで、24% はポリシーを策定していますが、まだ実行に移していません。ホスピタリティにおけるデータ セキュリティのバイス プレジデントは、「AI の制御を調整する必要がありますが、その間は AI の使用を受け入れています。AI によって生活はより良くなり、私たちの効率は改善されます。」と断言しています。



組織は機密データが AI アプリで悪用されないように保護するための対策を講じていますが、より包括的な管理が求められていることは明らかです。現在、企業の 43% は機密データが AI アプリにアップロードされるのを防止することに重点を置いており、別の 42% は潜在的な調査やインシデント対応のためにそれらのアプリ内のすべてのアクティビティとコンテンツをログに記録しています。同様に、42% が許可されていないツールへのユーザー アクセスをブロックしており、同割合が AI の安全な使用に関する従業員のトレーニングに投資しています。

許可されていない AI を使用する従業員がいる企業では、特定の種類の制御の必要性が高くなります。**許可されていない AI を使用している企業では、42% が AI クエリに基づいてリスクの高いユーザーを特定する制御を必要としています。一方、不正使用がない企業では 30% となっています。さらに、許可されていない AI の使用に対処している組織の 40% が、データのライフサイクルを管理するための制御 (保持プロトコルや削除プロトコルなど) を必要としていますが、この問題がない企業では 27% です。**

必要な AI 制御のトップ 5

機密データの AI へのアップロードを防止する	43%
潜在的な調査やインシデント対応のために、すべてのアクティビティとコンテンツのログを AI ツールで記録する	42%
許可されていない AI ツールへのユーザー アクセスをブロックする	42%
AI ツールの安全な使用方法について従業員へのトレーニングを行う	42%
AI に対するクエリに基づいてリスクの高いユーザーを特定する	41%

次のステップ

強力なデータ セキュリティ体制を維持するには、チームに AI アプリでデータを検出、保護、管理するための完全な制御セットが必要です。チームが使用できる 3 つの重要な戦略を次に示します。

AI アプリの使用状況とアプリを流れるデータの可視性を高める : AI アプリを検出して使用できるデータ セキュリティ ツールを活用します。これらのツールは、サポートされているデータ セキュリティ管理や規制への準拠などの詳細を含む、使用されている AI アプリの包括的なリストとそのリスク プロファイルに関するインサイトを提供します。AI とのやり取りの中で機密データを一貫して分類できるツールを使用し、AI アプリにおけるデータの流れの傾向を示します。

ポリシーの策定と適用 : 分析から得られたインサイトに基づいてポリシーを作成します。これらのポリシーには、承認された AI アプリのガイドラインと、承認されていないアプリの従業員による使用をブロックまたは制限するための手順を含めることができます。使用が認められた AI アプリでも、機密データやビジネス クリティカル データの使用を制限しながら、機密性のないデータの流れを許可する詳細なポリシーを作成できます。これには、データ セキュリティを確保するために機密データをブラウザーベースの AI ツールに貼り付けるなど、特定のアクションのブロックが含まれます。

リスクを定期的に評価し、ポリシーを改善する : 使用されている AI アプリ、それらのアプリを流れている機密データの傾向、それらのアプリに関するユーザー アクティビティの、リスク レベルを示すレポートを定期的に生成します。これは、全体的なリスクの状況を評価し、最も関連性の高いデータ セキュリティ ポリシーについて情報に基づいた決定を下すのに役立ちます。

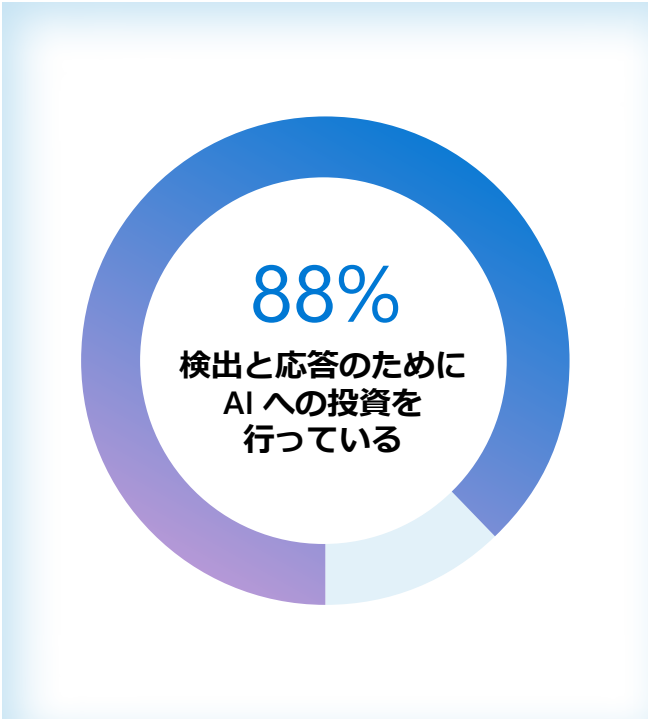
3

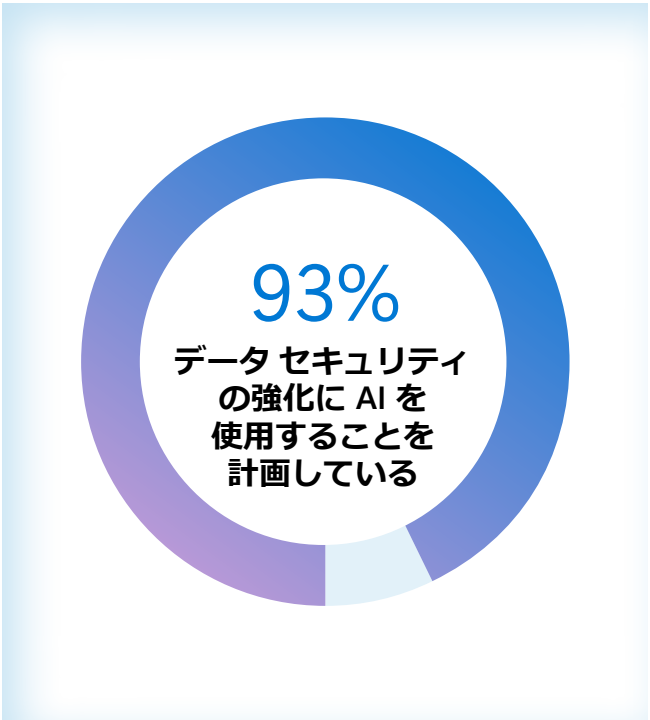
意思決定者は、データ セキュリティの取り組みを後押しする AI の可能性を楽観視しています

データ セキュリティ調査は AI に大きく依存しています

組織の大多数 (88%) は、機密データの検出、異常なアクティビティの検出、リスクのあるデータの自動的な保護など、検出と対応の取り組みを改善するためにすでに AI に投資しています。**組織の 77% が AI がこれらのプロセスを加速すると考えており、76% が AI によって検出と対応の戦略の精度が向上すると考えています。**

意思決定者の 73% がデータ セキュリティの強化に AI を使用することに懸念を表明していますが、50% はデータ セキュリティの強化に AI を使用することを使用を禁止していないと回答し、23% だけが AI の使用を控えていると回答しています。全体では、圧倒的に 93% が、懸念にもかかわらず、データ セキュリティの強化に AI を使用することを少なくとも計画しています。



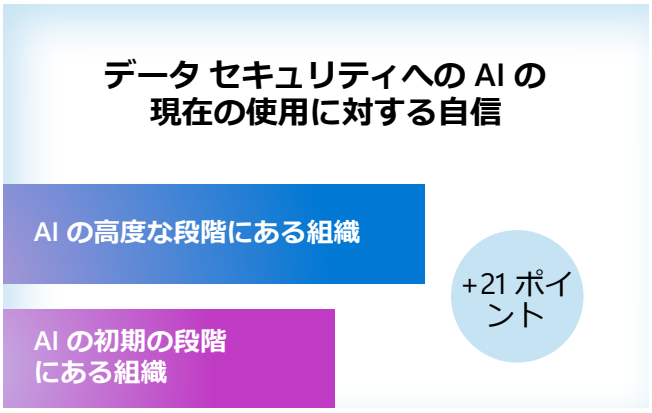


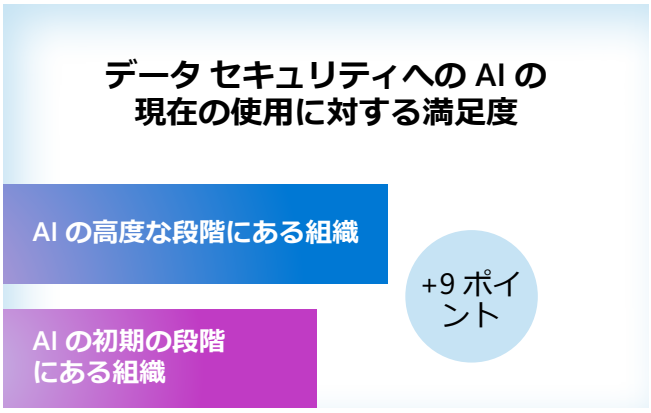
AI を使用してデータ セキュリティを強化することで、可視性、信頼性、満足度が向上します

データ セキュリティの強化に AI を使用する主な利点の 1 つは、システム全体の可視性が向上することです。これにより、意思決定者がデータの保存場所や分類方法を把握する際に抱える懸念を軽減できます (20%)。[1] 88% のデータ セキュリティの意思決定者は、データ セキュリティ ソリューションに AI を統合することでチームの可視性が高まり、組織が他の方法よりもはるかに多くのデータを処理および分析できるようになると考えています。中規模組織は、データ セキュリティ プロセスにおける人的ミスの最小化など、短期的なリスクの軽減に主に重点を置いています。実際、中規模企業の 43% がヒューマン エラーによるリスクの軽減を優先しているのに対し、超大規模企業では 37% にとどまっています。

対照的に、大企業はアプローチがより進んでおり、長期的なリスクと適応性の必要性を強調しています。このように高度なレベルが上がったため、データ セキュリティ チームは進化するリスクにより適切に適応することができます。これは、中規模組織の 43% と比較して、超大規模企業の 49% にとって最優先事項です。

全体として、データ セキュリティの強化に AI の使用が進んでいる組織では、データ セキュリティ戦略に対する自信と満足度がはるかに高いと報告されています。**AI 導入の高度な段階にある組織の 90% が、データ セキュリティの強化に AI を使用することについて、非常に自信がある、または非常に自信があると回答しています。それに対し、初期の段階の組織では 69% です。同様に、AI を高度に活用している組織の 76% が自社のデータ セキュリティ ソリューションに満足している一方で、初期の段階の組織で同じことを報告した組織ではわずか 67% です。**





1. マイクロソフトの委託により MDC Research が実施した、データ セキュリティ、ガバナンス、コンプライアンス、およびプライバシーの意思決定に関する 2024 年 9 月の調査

組織は、AI によってデータ セキュリティ インシデントの数を減らし、アラート管理を改善しています

データ セキュリティの運用を強化するために AI を活用している組織では、アラートが大幅に減少しています。**AI を活用したデータ セキュリティ ツールを導入している組織は、1 日平均 47 件のアラートを受信するのに対し、導入していない組織は 79 件のアラートを受信します。また、AI を使用している組織は毎日のアラートの 66% を確認できますが、AI を使用していない組織は 60% しか確認できません。**

さらに、データ セキュリティの強化に AI を使用している組織は、リスクの軽減にも AI を使用している傾向が高くなっています (56% 対 26%)。アラートの量の減少と、AI を活用してアラートを軽減する能力の向上が、データ セキュリティ インシデントの全体数に劇的な影響を与えたようです。データ セキュリティの強化に AI を導入した組織は、データ セキュリティの強化に AI を使用していない組織と比較して、データ セキュリティ インシデントが 65% 減少しています。

AI は対応に最大の影響を与えると予想されます

検出に関しては、意思決定者の 33% は AI が異常なアクティビティの検出に役立つことを期待しており、23% は AI が潜在的なデータ セキュリティ インシデントの調査に役立つと確信しています。さらに 22% は、データ環境のセキュリティ強化のために AI が提案を行う可能性を見出しています。

ただし、意思決定者が、AI が最も大きな影響を与えることを期待するのは対応です。34% は、AI が機密データの不適切な共有を自動的にブロックできると考えており、32% はリスクのあるデータを保護すると回答しています。別の 26% は、AI がデータ セキュリティ リスクの軽減と適切な制御の適用に役立つと考えていますが、同じ 26% が、AI が危険なユーザーの行動に対して自動的にフラグを立てることを期待しています。

次のステップ

データ セキュリティ ソリューションに AI を統合すると、リアルタイムのガイダンス、要約機能、自然言語サポートをチームに提供して、見落としていた可能性のある領域にスポットライトを当てることができます。これにより、調査を加速し、データ セキュリティ チーム全体の専門知識を強化することもできます。これらの機能がどのように影響を与えることができるかを次に示します。

アラートの要約 : 分析するソースの量と多様なポリシー ルールのために、調査が困難になる場合があります。データ損失防止 (DLP) とインサイダー リスク管理 (IRM) に AI を組み込むことで、チームはソース、ポリシー ルール、ユーザー リスクの分析情報を含むアラートの概要をすばやく受け取り、侵害された機密データとそれに関連するユーザー リスクを把握できます。

コンテキスト コミュニケーション : 組織は、ビジネス コミュニケーションに関する規制要件を遵守する必要があり、多くの場合、広範な違反のレビューを必要とします。AI を活用すると、データ セキュリティ チームは規制や企業ポリシーに照らしてコンテンツを評価して、データ セキュリティ インシデントにつながるリスクの高い通信を明らかにすることができます。

自然言語によるキーワード クエリ : 検索は調査時の複雑で時間のかかるワークフローであり、通常はキーワード クエリ言語を使用する必要があります。AI により、データ セキュリティ チームは検索プロンプトを自然言語で入力できるため、検索の開始を合理化し、より高度な調査を行うことができます。

調査結果に基づく推奨事項

1 統合プラットフォームの導入によりデータ セキュリティ インシデントを回避する

完全に統合されたデータ セキュリティ プラットフォームを導入することで、ますます進化する環境においてより安全で合理化された戦略が提供されます。また、複雑さの軽減、可視性の向上、保護の向上が実現します。統合アプローチにより、組織は、データ セキュリティ制御を一元化し、データ、ユーザー、アクティビティ全体にわたる統一された可視性を提供することで、データ セキュリティ体制の管理を改善して、データ リスクに関する検出と保護を強化および合理化できます。82% の組織が、統合プラットフォームが優れていると回答しており、統合に向けた取り組みは単に有益であるだけでなく、不可欠です。

2 AI の内部利用に対する可視性を高め、従業員による、生産性に影響を与えない AI の使用のために必要な制御を評価する

AI が職場で一般的になるにつれて、既存のリスクが増幅され、新たなリスクが発生する可能性があります。組織は、安全でない AI の使用から保護するために、より多くのことを行う必要があることを認めています。AI アプリに搭載されたコントロールと可視性を活用することは、生産性を損なわずにデータのセキュリティを維持するために不可欠です。AI の安全な使用について従業員にトレーニングを行うことで、組織はリスクの高い行動を最小限に抑えながら、それらの強力なツールをチームが引き続き活用できるようにします。

3 AI を活用してデータ セキュリティ戦略のレベルを高める

AI により、データ セキュリティ チームは、絶え間ない脅威や大量のアラートに対応するのではなく、より戦略的なイニシアチブに集中できます。AI 導入の高度な段階にある企業は、データ セキュリティ ソリューションを使い始めたばかりの企業よりも自信があり、満足しています。包括的なデータ セキュリティ戦略の一環として AI を導入することで、組織は可視性を高め、リスクを検出して対応する能力を強化し、最終的には全体的なデータ セキュリティ体制を強化できます。

調査の目的

調査目的 :

1. データ セキュリティ インシデントにおける優先事項と考え方、課題、原因と結果などの、データ セキュリティを取り巻く状況を理解する。
2. 新たな戦略やイノベーション、組織が将来に向けてどのような投資をするつもりかなど、データ セキュリティの未来を探る。
3. データ セキュリティにおける AI の役割とデータ保護における AI の役割を明らかにする。

調査の手法

データ セキュリティの意思決定者 1,376 人を対象に、2024 年 8 月 5 日から 23 日にかけて、20 分の多国籍オンライン調査を実施しました。

質問は、2023 年と比較したデータ セキュリティの状況とデータ セキュリティ インシデントに集中していました。さらに、今年の調査では、従業員による AI の使用の確保とデータ セキュリティの強化のための AI の使用に関する質問が含まれていました。

対象者の募集

調査の基準として、以下に該当するデータ セキュリティの意思決定者を対象としました。

- データ セキュリティの権限を持つ CISO およびそれに相当する意思決定者 (C-2 以上)
- 企業組織に所属 (従業員数 500 人以上)
- 規制産業と非規制産業の両方を含める (教育、政府機関、非営利団体を除く)

調査対象となった 1,376 人のデータ セキュリティ意思決定者を国で分けると以下の通りです。

- 米国 : 302
- 英国 : 305
- インド : 301
- ブラジル : 158
- フランス : 156
- オーストラリア : 154

hypothesis Microsoft Security