Microsoft

hypothesis

データ セキュリティ インデックス

トレンド、インサイト、戦略を活用してデータをセキュア化する

はじめに

データ急増の時代において、組織が保有するデータは組織の生命線であるという認識が急速に広まっています。組織が作成し、使用する豊富なデータは、重要な業務を強化し、戦略的かつグローバルな意思決定に情報を提供し、組織の未来の可能性を形成します。データは単なるリソースではなく、現代企業の心臓部であると言ってもよいでしょう。

しかし、データへの依存度が高まるにつれ、デジタルの影に潜む脆弱性が現実味を帯び、急速に拡大しているという厳しい現実が待っています。サイバー脅威、データ漏えい、インサイダー脅威に関する事故はもはや珍しくありません。これらは広範囲に及んで勢いを増しており、データに依存する組織にリスクをもたらしています。先日実施した調査では、意思決定者の 89% が自社のデータ セキュリティ態勢が成功に不可欠であると回答しています。

このホワイトペーパーでは、組織のデータの保護という基本的な必須要件について探っていきます。今回、この調査結果を皆さんにご紹介できることを、私もチームのメンバーも大変光栄に思っております。データ セキュリティを卓越したものへと前進させ続ける方法について、対話が始まるきっかけになれば幸いです。私たちが学んだことは、データ セキュリティがいかに重要な岐路に立たされているかを例証するものでした。セキュリティの意思決定者は、データの安全性確保が不可欠であることを認識しており、自分たちの取り組みに自信を持っていると回答する一方で、データ セキュリティのインシデントや課題を数多く経験しています。また、調査に回答したリーダーの 80% は、ベスト イン スイートで統合されたアプローチがポイント ソリューションよりも優れていることを認識していますが、ほとんどの企業ではに断片的なマルチ ツール システムを使用してデータを保護しているのが現状です。その結果、セキュリティ インシデントは減るどころか、ますます増えているのです。

この最新レポートをぜひお読みいただき、共有してください。ぜひ、私たちのチームにもご意見やご要望をお聞かせください。共に私たちの未来を守る最善の方法を考えていきましょう。

Rudra Mitra
マイクロソフト データ セキュリティとコンプライアンス部門担当
副社長

イントロダクション

データ漏えいやその他のセキュリティ インシデントの防止は、セキュリティおよびリスク部門の意思決定者にとっては常に懸念事項であり、サイバーセキュリティ プログラムの要でもあります。たった一度のインシデントが、風評被害や経済的損失を深刻化する可能性があります。組織は、従業員やお客様の情報、知的財産、財務予測、業務データなど、さまざまな機密データを保護する使命を負っています。

現在のデータセキュリティの慣行と傾向を理解し、組織にとっての機会を見極めるにあたり、マイクロソフトは独立調査機関である Hypothesis Group に依頼し、800人以上のデータセキュリティ専門家を対象に多国籍調査を実施しました。このレポートでは、データを保護するための傾向、インサイト、戦略など、調査から得られた 5 つの主要な知見を紹介しています。

主な調査結果

1

意思決定者は、自社の保護態勢が万全であると思っていますが、実際はそうではありません。

ほとんどの意思決定者は、自社のデータ セキュリティ ソリューションに満足し、自信があると回答していますが、それでも年間平均 59 件のデータ セキュリティ インシデントが発生しており、その影響は甚大です。

2

ツールの数が多ければ多いほど、データの安全性や効率が高まるわけではありません。その逆の場合もあります。

意思決定者の 80% は、包括的な統合ソリューションが、手作業によるベスト オブ ブリードのソリューションよりも優れていることを認識しています。しかし、企業のツールに対するアプローチは断片的で、平均で 10 個以上のデータセキュリティ ツールを使用していることがわかっています。しかし、非常に多くのツールを導入している企業では、データ セキュリティ インシデントも多く発生しているため、ツールが多くなればなるほど、セキュリティが弱くなることを示唆しています。

3

組織は、外部および内部のデータ セキュリティ インシデントのストレスに悩まされ続けており、これは特にビジネス データに顕著です。

今回調査した組織の 50% が、過去 1 年間にランサムウェアやマルウェアによる攻撃を経験しており、多くの意思決定者は、自社組織が将来の攻撃を防止し、対処する準備が十分に整っているとは考えていないことがわかっています。内部的には、悪意のある内部関係者が最大の懸念事項です。さらに、企業はビジネスデータの脆弱性を強く懸念しています。これによって、リスクに包括的に対処するセキュリティ プラットフォームの必要性が改めて浮き彫りになりました。

主な調査結果

4

組織はデジタル トランスフォーメーションを推進するクラウドと AI を必要としていますが、この両者は最も脆弱なデータ ロケーションでもあります。

クラウド アプリケーションと AI テクノロジーは、組織のコラボレーションと生産性を促進するには不可欠なものとなっています。しかし、この進化は、より動的で多面的なリスクも生み出しています。組織が AI を採用するようになると、責任ある安全な利用を実現するデータ セキュリティの強化が重要になります。

5

自動化と AI を利用することで、より優れた保護機能を実現できます。

組織は、担当チームが検知に費やす時間を削減し、予防にさらに多くの時間を費やすことを望んでいます。自動化によって、チームはよりプロアクティブ (事前対応的) な対策に集中できるようになる一方、データ セキュリティに AI を活用することで、組織はより戦略的になり、将来の脅威に対してよりスマートな態勢をとることができます。

1

意思決定者は、自社の保護態勢が万全であると思っていますが、実際はそうではありません。

意思決定者は、自社の保護態勢が万全であると思っていますが、実際はそうではありません。

意思決定者は、表面的には自社のデータ セキュリティ ソリューションに高いレベルの信頼と満足度を示しており、大多数の組織では自社のデータ セキュリティの管理態勢がデータ侵害を防御に十分であること認識しています。つまり、データの大半がどこにあるのかを把握しており、データにまつわるリスクの大部分を検出できると感じています。

その一方で、企業は依然として大量のデータ セキュリティ インシデントを経験しており、過去 12 カ月で平均 59 件、そのうち 5 分の 1 が「深刻」なレベルのインシデントと見なされるものでした。このようなインシデントの影響は広範囲に及び、最も深刻なデータ セキュリティ インシデントの総費用は平均して約 24 万 4,000 ドルと推定されています。年間で考えると、インシデントのコストは 1,500 万ドルに達する可能性があります。これらのコストに加え、意思決定者の 10 人に 4 人が、データ セキュリティ インシデントの復旧にかかる運用コストや、風評被害によるビジネスの損失も高い関心事であると回答しています。

さらに、92%が、主にコスト、統合、導入に要する時間などの分野で、データ セキュリティに対する追加投資を阻害する課題に直面していることがわかっており。予算に見合った、労働効率の高いソリューションの必要性が浮き彫りになっています。

データ セキュリティ態勢に対して自覚している自信は、実際に組織が経験しているインシデントの現実とは異なります。組織がデータの所在を把握し、リスクを検出することはもちろん重要ですが、これらの対策を個別に、あるいは切り離して講じるだけでは、データ セキュリティおよびリスク部門の意思決定者の安心を確保できるようなインシデント対策としては不十分です。

金融サービスを提供する企業のある CISO (最高情報セキュリティ責任者) は次のようにコメントしています。「『データのセキュア化はしていましたが、保護はできませんでした』と取締役会で報告するわけにはいきません。ウォール ストリート ジャーナルの一面を飾るような、銀行の失態は誰も見たくないでしょう。」

59

過去 12 か月間に発生したデータ セキュリティ インシデントの平均数

最大で

1,500 万ドル

重大なセキュリティ インシデントの年間コスト

2

ツールの数が多ければ多いほど、データの安全性や効率が高まるわけではありません。その逆の場合もあります。

ツールの数が多ければ多いほど、データの安全性や効率が高まるわけではありません。その逆の場合もあります。

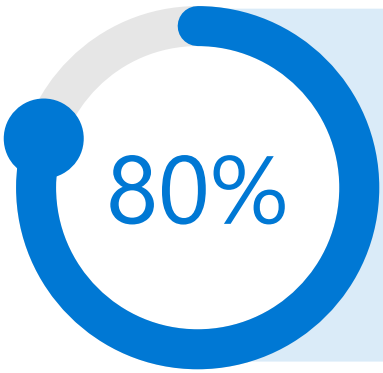
企業は、長年にわたるポイント ソリューションのアプローチが、可視性と効率性にギャップを生じさせたこと、そしてその原因がサイロ化したデータ セキュリティ ツールであることに気づき始めています。現在ではデータ セキュリティの統合ソリューションを求める傾向へと転換しつつあります。80% が、手作業による統合と管理が必要となる複数のベスト オブ ブリードのソリューションを使用するよりも、統合ソリューションを備えた包括的なデータ セキュリティ プラットフォームが優れていることを認識しています。

しかし、大多数が統合ソリューションが優れていると考えているにもかかわらず、データ セキュリティ ツールを多く使用しており、断片的な運用を続けています。

その結果、企業はデータ セキュリティ リスクに対処するために、データ損失防止、情報保護、インサイダー リスク管理、セキュリティ情報とイベント管理 (SIEM)、クラウド アクセス セキュリティ ブローカーなど、平均10個のデータ セキュリティ ツールを使用していると報告しています。従業員数が 5,000 人を超える組織では、平均ツール数はさらに多くなります。

より多くのツールを使用している企業 (16 個以上) は、ツールの数が少ない企業 (61% 対 56%) に比べて、データセキュリティ態勢に自信を持っている傾向が高いことから、より多くのツールを使用することで、誤った安心感を生み出している可能性があります。

調査結果によると、この安心感とは逆の結果が浮き彫りになっています。16 個またはそれ以上のツールを使用している組織では、過去 1 年間に発生したデータ セキュリティ インシデントが平均 133 件と多いのに対し、ツールの数が少ない組織では 48 件であることがわかっています。



の組織は、統合ソリューションを備えた包括的なセキュリティ プラットフォームが、手動の統合と管理が必要となる複数のベスト オブ ブリードのソリューションよりも優れていることを認識しています。

2.8倍

過去 1 年間で発生したデータ セキュリティ インシデント

ツールを 16 個以上使用している組織 (ツールが少ない組織と比較して)

ベスト オブ ブリードのソリューションや、より多くのツールの運用を好む企業の感情や取り組みを見てみると、今後は高度に統合されたソリューションや、厳選された少数のツールによるデータ セキュリティの強化が強く望まれるであろうことがわかります。

「たくさんあるシステムから、データをどのように収集し、集計し、利用すればよいのでしょうか？。この運用をうまく機能させるには、多くの異なるデータポイントをひとつのエコシステムにまとめる必要があります。これができなければ、穴だらけのデータ セキュリティになってしまいます。」

製造/生産担当
IT 部門長

第一に、複数の異なるデータ セキュリティ ツールを使用すると、可視性にギャップが生じ、シャドウ データが増加える可能性があります。実際、シャドウデータを懸念する人々は、最善のソリューションを好む傾向があります。 これは、ベスト オブ ブリードのアプローチを採用している組織では、データ セキュリティ態勢を包括的に可視化するにあたって、より多くの労力が必要になるからであると考えられます。

第二に、サイロ化されたソリューション管理は、データ セキュリティ チームにさらなる複雑性を課すことになります。別個のソリューションを運用することで、専任のスタッフ、エンドポイント エージェントのインストールとメンテナンス、さまざまな新しいプロセスが必要になるためです。ここでは、アラートのレビューとトリアージを例にとりましょう。これらは人員とリソースを必要とする代表的な作業です。アラート件数が増えると、独立したソリューションを管理するデータ セキュリティ チームにさらなる労力が求められることになります。運用するツールが多い組織では、1 日あたり平均 96 件のデータ セキュリティ アラートを受信しているのに対し、ツールが少ないチームではその半分以下の 44 件にとどまっています。その上、これらのアラートのすべてを確認できるわけではありません。アラートの確認率は、ツールの多い組織が 61% であるのに対し、ツールの少ない組織では 68% であることがわかっています。これはまた、多くのツールを使用する組織は、少ない量のツールを使用する組織と比較して、より「リアクティブ (事後対応的)」であるという結果を示しています。

最後に、たくさんのツールを運用する場合、組織はインサイトと改善計画の統合に多大な努力を払う必要があります。つまり、情報が翻訳中に失われる可能性があることを示しています。データ セキュリティに関する一番の課題について尋ねたところ、「データ セキュリティ ソリューションの導入や維持にかかるコスト」と「データ セキュリティ ソリューションの統合に関する課題」が上位 2 位に挙げられました。

これは、処理に時間がかかること、プロセスが遅いことを意味しています。16 以上のツールを運用している企業の 37% が「データ セキュリティの調査完了までに 1 カ月以上かかる」と回答しており、少数のツールを運用している企業ではこれがわずか 21% に留まっています。

「迅速な対応とはほど遠い状態です。私たちが使用している複数のシステムはどれも、独自のポータル、独自のツールを備え、独自の対応が必要となります。そのため、メンバーそれぞれの知識やノウハウが熟達していても属人化しています。問題が発生した際には、全員が集まって何が起こっているのかを判断し、そこから対処を始めます。この部分でどうしてもちょっとした手作業が必要になってしまうのです。」製造および生産担当、インフラストラクチャ&オペレーション部門のディレクター談

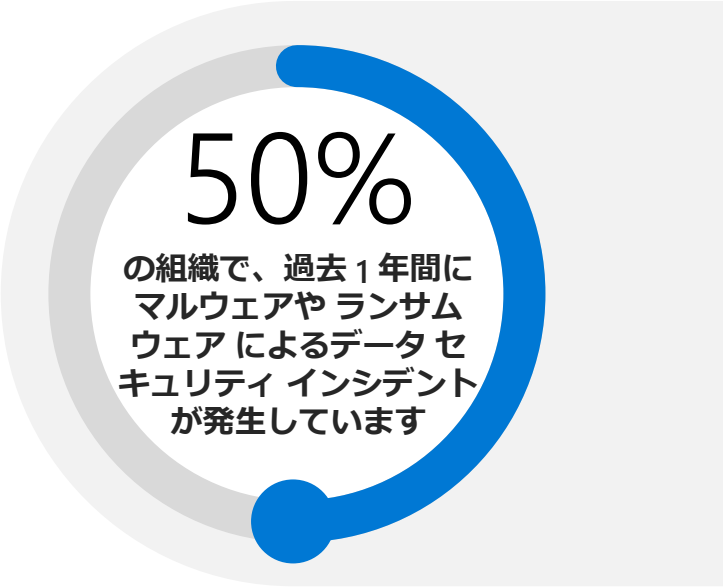
統合ソリューションの方が優れていることを理解していても、複数ソリューションによる運用を継続することで、結局逆の方向に進むことになってしまいます。そしてコストも時間も浪費するのです。

データ セキュリティ ツールの使用数が少ない (16個未満) 場合と多い (16個以上) 場合の結果の比較	**ツールが少ない組織**	**ツールが多い組織**
過去 12 ヶ月間の**データ セキュリティ** インシデント発生件数	**48**	**133**
重大なデータ セキュリティインシデントの割合	**19%**	**26%**
現在のデータ セキュリティ戦略は比較的**リアクティブ(事後対応的)**である	**31%**	**40%**
ソリューションの**統合** に関する課題がある	**24%**	**39%**
データ セキュリティ チームが最も時間を費やしている のは**対応**である	**19%**	**26%**
データ セキュリティの態勢に**自信を持っている**	**56%**	**61%**
1 日あたりの平均**受信**アラート件数	**44**	**96**
1 日あたりで**内容確認できる**アラートの割合	**68%**	**61%**
データセキュリティ調査の完了に 1 か月以上を要している	**21%**	**37%**

3

組織は、外部および内部のデータ セキュリティ インシデントのストレスに悩まされ続けており、これは特にビジネス データに顕著です。

組織は、外部および内部のデータ セキュリティ インシデントのストレスに悩まされ続けており、これは特にビジネス データに顕著です。



データに関わる人々、データにまつわる活動、データ処理に使用されるデバイスやアプリなど、データを取り巻く要因は常に進化しているため、データ セキュリティ インシデントやデータ侵害はいつでもどこでも発生する可能性があります。そして、これらの脅威は、外部の攻撃者だけでなく、従業員、契約社員、パートナーなどの信任を得ている人物からも発生します。悪意があろうとなかろうと、これらすべての要素がデータ セキュリティ インシデントを引き起こす可能性があります。そのため、常にさまざまな分野にわたる保護が必要となるのです。

ある金融サービスのIT部門長は次のように語っています。「インシデントの発生源は常に変動しています。標的が動いているようなものです。常に進化、変化しており、柔軟です。保護の対象となるものとその所在地は、より多様化していくでしょう。」

データ セキュリティ インシデントの発生源は多岐にわたる可能性があります。マルウェアやランサムウェアなどの外部からの脅威 (悪意のあるソフトウェアがシステムに侵入し、攻撃者がシステムやネットワークに不正にアクセスするケース) は圧倒的に多く、調査対象となった組織の 50% が過去 1 年間に少なくとも 1 度は経験しています。

さらに、これらの攻撃は組織が最も脆弱性を感じている箇所を狙われる傾向が高く、41% が今後 1 年間のマルウェアやランサムウェア攻撃に対処する準備ができていないと回答しています。この脆弱性を感じている割合は、ベスト オブ ブリードのアプローチを好むユーザーの間ではさらに高くなります。44% がこの種の攻撃に対する備えがないと感じているのに対し、統合ソリューションを好むユーザーでは 36% に留まっています。

また、インサイダー リスクからの保護と防止も、意思決定者にとって最重要課題です。35% が悪意のあるインサイダーや漏えいしたアカウントに対する防御を強化する必要があると回答しており、3 分の 1 が不注意によるインサイダー インシデントを懸念しています。悪意のある内部関係者によるインシデントは、2 番目に多いタイプのインシデントです。これは必ずしもデータ セキュリティ侵害の主要原因ではないかもしれませんが、意思決定者が最も予防不足を感じている部分です。

「月に一度は必ず、パニックに陥った管理者から電話がかかってきます...『インシデントが発生した』、『インシデントを発見した』、『脅威担当チームがインシデントを発見した』などさまざまです。これらは偶発的なエラーであることもあれば、場合によっては自分たちが何をできるのかさえ認識していないこともあります。」

米国の政府機関 CISO

インサイダーとは一般的に、外部の人間に公開されていない会社のリソース、データ、シス テムへのアクセスを許可された、または知識のある信任を得た個人を指します。その結果、内部の関係者に関連するデータ セキュリティ リスクは、よりとらえどころがなく、検出が困難になる傾向があります。マイクロソフトの CISO、Bret Arsenault 氏は次のように指摘しています。「最終的には、違反が故意か偶発的かは問題ではありません。すべての企業のセキュリティ戦略に、インサイダー リスク プログラムを含める必要があるでしょう。」

データ セキュリティ インシデントの概要

データ セキュリティ インシデントの原因	過去 12 か月間で最も多かったインシデント	今後 12 か月間での予防対策が不十分だと自覚している
マルウェア / ランサムウェア	50%	41%
アカウントの侵害	38%	35%
サービス拒否 (DoS) 攻撃	35%	33% は
インサイダー (過失)	32%	29%
インサイダー (不注意)	31%	32%
悪意のあるインサイダー	31%	35%
物理的特性	29%	29%

組織が選択するデータセキュリティ ソリューションは、価値の高いビジネス データ、業務データ、個人データなど、さまざまな機密データにも対応する必要があります。過去 12 か月間のデータ セキュリティ インシデントでは、74% の組織でビジネス データの漏えい、65% で業務データの侵害、58% で個人データが危険にさらされた経験があります。さまざまな種類のデータの中でも、知的財産、ITおよびネットワーク設計、個人情報 (PII) の漏えいや流出が最も多いことがわかっています。

将来を見据えると、77% の組織が、知的財産やソース コードなどのビジネス データを最も脆弱なものであると認識しています。これは主に、ビジネスデータが競争上の優位性を確立し、収益を生み出す上で重要な役割を果たしているためです。しかし、従来のパターン認識、正規表現、機能マッチ技術では、特定の文字列形式やキーワードを持たないコンテンツを効果的に識別できない場合があるため、このようなデータの識別と分類は困難な場合があります。そのため、組織は脆弱な機密データを検出し、保護するための、より高度な技術を必要としています。

今後 12 カ月で最もリスクの高いデータの種類

77% ビジネス データ		64% 業務データ		63% 個人データ	
知的財産	30%	IT およびネットワーク設計	29%	個人を特定できる情報 (PII)	31%
ソース コード	28%	決算書類	18%	人事情報(給与、履歴書など)	21%
事業計画	27%	売上および収益レポート	15%	ペイメント カード インダストリー (PCI) データ	18%
企業秘密	24%	調達と請求書	12%	保護対象保健情報 (PHI)	18%
合併と買収に関するファイル	20%	法的文書/契約文書	12%	資格情報	17%
工事仕様書	18%	製造プロセス/バッチ ファイル	11%		

4

組織はデジタル トランスフォーメーションを推進するクラウドと AI を必要としていますが、この両者は最も脆弱なデータ ロケーションでもあります。

組織はデジタル トランスフォーメーションを推進するクラウドと AI を必要としていますが、この両者は最も脆弱なデータ ロケーションでもあります。

クラウド アプリケーションとプラットフォームを介したコラボレーションは、新しい AI テクノロジーと組み合わせることで、従業員の生産性を大幅に向上させ、柔軟な勤務形態を実現します。そのため、クラウド アプリケーションと AI テクノロジーは組織にとって不可欠なものとなっています。現在、企業は平均して SaaS、PaaS、IaaS にまたがる 147 のパブリック クラウドサービスを利用しています。[1] また、66% の組織が AI 戦略を策定しており、36% がすでにこれを導入しています。[2] しかし、この進化によって、さまざまな環境にまたがるデータの境界を明確に定義することが難しくなるため、より動的で多面的なリスクが生み出されています。

1. リスクとリスクガバナンスの測定、クラウド セキュリティ アライアンス (CSA)、2022年
2. マイクロソフト データ セキュリティ AI 研究による仮説、2023 年 3 月

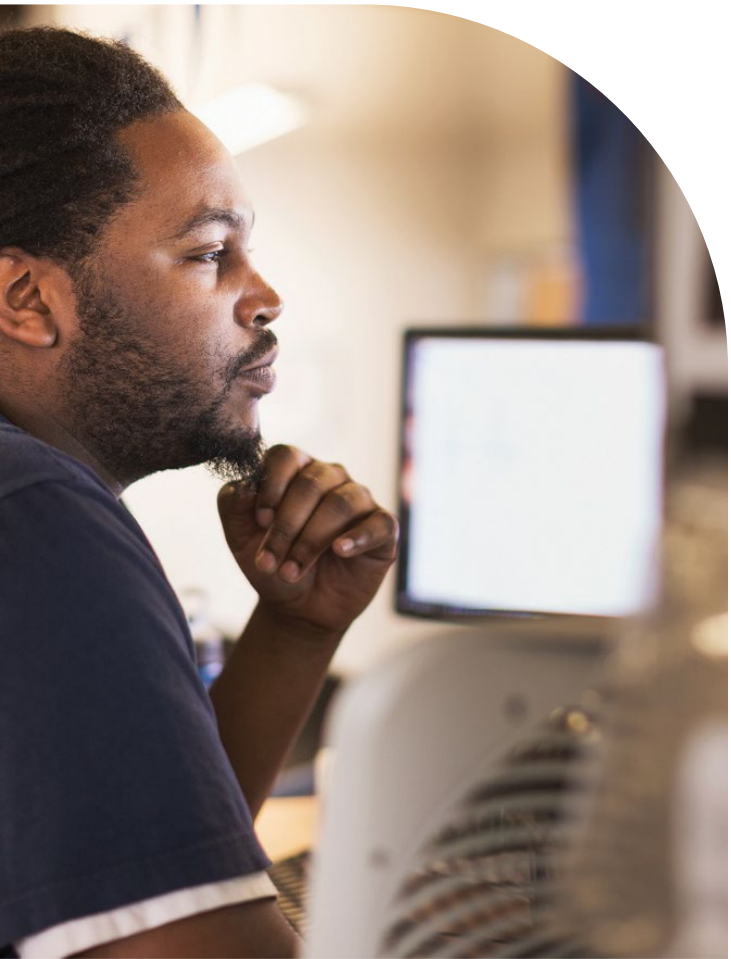
このような生産性の高いデータ拠点に適切なデータ セキュリティ ソリューションを導入することは、今ではさらに重要になっています。過去 12 カ月間に発生したセキュリティ インシデントは、42% がクラウド ストレージ、31% が電子メール、インスタント メッセージ、オンライン会議ツールで発生していることがわかっています。インシデントは、生産性が高く、コラボレーションが最も活発な場所で発生する傾向が高くなっています。

この種のインシデントの管理にはリソースが不可欠です。79% の組織で、データ セキュリティ チームが重要なデータ セキュリティの責任を効果的に管理するには、より多くの人材が必要であると報告しています。しかし、より多くの人材を必要としている組織では、過半数 (57%) がベスト イン ブリードのアプローチを好んでいます。この傾向は、より多くのソリューションを使用している組織ほど、無数のユーザー アクティビティの中から真のリスクを見極めるのが困難であることを示唆しています。

データの主な所在地

データの場所	過去 12 か月間で侵害を受けた	最もリスクが高い
クラウド ストレージ (Box、OneDrive、Google ドライブなど)	42%	54%
メール/インスタント メッセージ/オンライン会議ツール	31%	39%
サービスとしてのプラットフォーム (PaaS)	29%	34%
サービスとしてのインフラ (IaaS)	28%	36%
AI (ChatGPT、Bard など)	27%	38%
SaaS ベースのデータベース/データ レイク	27%	41%
エンドポイント / デバイス	25%	36%
オンプレミスのリポジトリ / ファイル共有 / データベース	24%	28%
シャドウ データ	21%	23%
基幹業務アプリケーション	17%	25%
開発者 ツール	16%	23%

企業の 3 分の 1 以上が AI 戦略を導入しており、さらに多くの企業が AI の導入を計画しています。AI はかつてないスピードで導入されており、過去のクラウドや電子メールの導入よりもはるかに速いスピードで導入されています。組織の AI 導入には、データ セキュリティを強化し、データの責任ある利用とリスク防止を実現することが不可欠です。AI は他の場所と比較して、データ セキュリティ インシデントのリスクが高い場所と見なされており、27% の組織が AI のデータ セキュリティ侵害を経験しています。AI を使用するリスクに関する組織の懸念は、AI と共有されるデータの管理不足、AI の危険な使用を検出し軽減する管理体制の欠如、AI 生成モデルの学習方法に関する透明性の欠如、AI による機密情報の漏えいなどが中心となっています。



「AI は生産性と効率性に優れていますが、潜在的なセキュリティとデータのリスクがあります。」
ある企業のセキュリティ部門の意思決定者

AI をめぐる懸念が存在する一方で、市場ではさまざまなベンダーが責任ある AI の利用を通じてビジネスを強化するイノベーションを開発しています。このことから、意思決定者はこの新しいテクノロジーに可能性を見出すこともできます。しかし、組織が AI をさらに活用するためには、AI に含まれる悪意のあるコンテンツやリスクのあるコンテンツの検出、AI にアップロードされる前のデータの暗号化、マスク、匿名化、AI が生成する機密データの識別が必要であるという声も上がっています。

AI に求められるデータ セキュリティ統制トップ 5

1	AI で**悪意のあるコンテンツや危険なコンテンツ を検出する**
2	データを AI にアップロードする前に**暗号化、マスキング、または匿名化する**
3	AI が生成する**機密データを見極める**
4	**機密データの** AI への**アップロードを防止する**
5	AI での**モデルまたはデータの操作を検出する**

5

自動化と AI を利用することで、より優れた保護機能を実現できます。

自動化と AI を利用することで、より優れた保護機能を実現できます。

組織の優先順位や予算の制約がないと仮定した場合、半数の組織がデータ セキュリティ管理にプロアクティブ (事前対応的) に取り組み、機密データやそれに関するリスクの発見、データ セキュリティ インシデントの防止などに多くの時間を費やしたいと考えていると回答しています。しかし現状では、半数以上の組織が、インシデントの検出、対応、調査といったリアクティブ (事後対応的) な対策に最も多くの時間を費やしています。データ セキュリティ インシデントの検出と対応には時間がかかります。データ セキュリティ インシデントの解決には、ほとんどの組織で約 1 カ月を要しており、解決に 6 カ月かかる組織もあります。

プロアクティブな対策を採用することのメリットは明白です。調査によると、プロアクティブな対策を採用している組織では、データ セキュリティ インシデントの発生に対するコストを抑え、インシデントを 1 カ月以内に調査できる可能性が高く、データ侵害の防止に自社の防御策が十分であると考えている傾向が高いことがわかっています。

しかし、プロアクティブなデータ セキュリティ対策がデータ セキュリティ リスクの低減に役立つことを認識していても、その対策の実施は進んでいません。たとえば、「プロアクティブ」に行動することで予防に多くの時間を割きたいと考えている組織は、ベスト オブ ブリードのソリューションを選ぶ傾向が高いことがわかっています。この運用では、検出信号と応答制御を同時に対処する際に、より多くのリソースを「リアクティブ」な対応に割かれることになってしまいます。

プロアクティブ / リアクティブな対策を採用している組織における結果の差異

	プロアクティブ	リアクティブ
過去 12 か月間で発生したデータ セキュリティ インシデントの平均コスト	207,000 ドル	330,000 ドル
データセキュリティ調査を平均 1 カ月以内に完了する	80%	68%
データ漏えい防止対策で、自社の防衛管理は十分である	77%	68%

リソースやスタッフには制約があり、アクティビティ間の労力配分も理想的とは言えないため、組織はプロアクティブな活動に多くの時間を確保できるようなテクノロジーを求めています。自動化は、組織がデータ セキュリティにプロアクティブに取り組む時間を作る一つの方法です。調査対象となった組織の 74% は、半自動化または完全自動化されたリスク軽減策を求めています。この軽減策では手作業による確認作業がなくなるため、セキュリティチームは潜在的なデータ セキュリティ インシデントの影響を事前に最小限に抑えることができます。さらに、データ セキュリティ レポートの作成、インシデント管理ワークフローの自動化、インシデントへの対応と調査など、自動化の恩恵を受けられるその他多くのタスクを認識しています。セキュリティ チームが自動化を望むタスクのほとんどは、リアクティブな対策です。これらのタスクを自動化することで、組織はデータ セキュリティ チームの負担を軽減し、よりプロアクティブな態勢をとることができます。

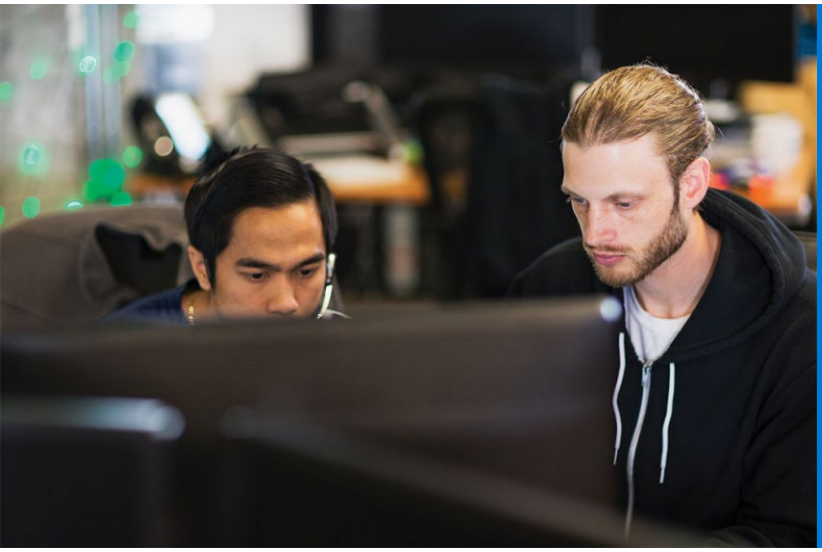
データ セキュリティ チームが自動化/軽減したい分野トップ 5

リアクティブ

1. インシデント管理と対応に向けた自動化されたワークフローの作成
2. データ セキュリティ レポートの作成

リアクティブ

3. データ セキュリティ インシデントへの対応と抑制
4. 調査中にインシデントを適切なチーム (SOC、法務、人事など) に引き渡す
5. データ セキュリティ インシデントの調査



「高リスクのデータで、手作業で評価をしているものは多く存在します。AI は、リソース不足の状況下でチームの応答時間を短縮すると同時に、データ保護に貢献します。」

英国セキュリティ企業 意思決定者

データ セキュリティに AI を活用することで、組織がより戦略的になり、将来の脅威についてもよりスマートになります。テクノロジーによって、検出されたインシデントへの対応を迅速化し、データ セキュリティの専門家がさらに調査する時間を確保できます。自動化と同様に、組織は AI が役立つさまざまなシナリオを挙げています。これによると、さらに強固なセキュリティを実現できるため、**チームの時間を節約できます。**AI の主な利用シナリオには、不適切なデータ共有の自動ブロック、重大なデータ セキュリティ リスクや異常なデータ活動の検出、潜在的なデータ セキュリティ インシデントの調査などが含まれています。

AI と自動化の利点を活用し、さらに統合されたソリューションに移行することで、組織はよりプロアクティブなデータ セキュリティ戦略を採用し、より安全な未来に向けて備えることができます。

AI を使用する上位のシナリオ

不適切なデータ共有を**自動的にブロックする**

重要なデータ セキュリティ リスク / 異常なデータ アクティビティを**検出する**

データ環境のセキュリティを強化する**推奨事項**

潜在的なデータセキュリティ インシデントの**調査**

データ セキュリティ ポリシーの**適切な調整**

調査結果に基づく推奨事項

- 統合プラットフォームを採用してデータ セキュリティ態勢を強化する
- 綿密な防御アプローチにより、外部と内部の両方からデータ セキュリティ インシデントを防御する
- AI と自動化でデータ セキュリティ戦略をアップグレードする

統合プラットフォームを採用してデータ セキュリティ態勢を強化する

この調査結果によると、運用するソリューションを少数に抑えることで、より高度なセキュリティを実現できることがわかっています。一見矛盾しているように思えるかもしれませんが、独立した多数のソリューションを運用することで生じる安心感は、いわば錯覚であり、組織はこれを打破する必要があります。ベンダーを絞り込むことで、戦略的アプローチを得られるため、コスト削減とセキュリティ強化を実現できます。

この変革に着手するにあたって、データ セキュリティの意思決定者は、チームに権限を与えることで、新しいセキュリティ管理の調査や計画、セキュリティ ポリシーの最適化などの戦略的作業により多くの時間を割けるようになります。調査では、実際に意思決定者の 84% がそうしたいと考えています。このプロセスでは、これまでのサイロ化されたソリューションを置き換える必要があります。これらソリューションは「ベスト オブ ブリード」と見なされることもありますが、他のツールとの効果的な統合が望めるものではありません。

意思決定者は、チームとの緊密なコラボレーションを促進することで、データ セキュリティ プログラムの目標と主要業績評価指標 (KPI) を設定できます。それらの要素によって、ソリューションの要件を定義し、絶対的に必要な機能を見極められるため、対策を前進させられるようになります。このアプローチにより、包括的な目的に沿ったツールを提供してくれるベンダーをピンポイントで見つけることができます。重要なのは、将来を考慮した考え方を促進し、チームが既存の慣行やサイロ化した使用用途に過度に固執することを避けることで、より統合的なアプローチに向けて必要な変革を実施できるようにすることです。

統合データ セキュリティ プラットフォームを導入することで、セキュリティ チームを強化し、以下すべての重要なタスクをシームレスに実行できるようになります。

1. デジタル環境内の機密データを検出して保護する。

2. このデータに関連する重大なリスクを検出する。

3. 通常の事業活動に影響を与えることなく、機密データの不正使用を防止する。

統合されたデータ セキュリティ戦略を導入することで、組織はより高いレベルの保護を実現すると同時に、セキュリティ インフラを簡素化できます。

綿密な防御アプローチにより、外部と内部の両方からデータ セキュリティ インシデントを防御する

一般的にデータ セキュリティ インシデントは、外部の攻撃者、悪意のある内部関係者、または内部関係者の不注意が引き起こすものです。組織はデータの保護対策を講じることで、外部からの脅威による不正アクセスを防止し、内部関係者による盗難や偶発的なデータ流出のリスクを軽減する必要があります。

これらの課題に取り組むにあたって、組織はデータ セキュリティに徹底的な防御のアプローチを採用することができます。この戦略は、美術館が貴重な美術品を保護するシステムに類似しています。脅威インテリジェンスを備えた最新鋭の監視カメラによる来館者の監視、チケット システムによる身元と入館の管理が徹底され、作品周辺には厳重なセキュリティ対策が施されています。皆さんの貴重なデータを保護するデータ セキュリティ管理もこれと同様です。これらの対策は、外部からの悪意ある人物に起因するものでも、組織内の人物に起因するものでも、その両方に対して潜在的なインシデントを阻止するものです。

進化するデータ セキュリティのリスクに対処するには、組織全体で協調して取り組むことで、「徹底的な防御」戦略を実施する必要があります。データ セキュリティ チームがセキュリティ オペレーション センター (SOC) などの他部門と連携することで、データ セキュリティへの投資を最適化できます。注目すべきは、プロアクティブな組織であることを自覚している組織の 66% が、SOCチームと連携しているという事実です。そのような自覚がない組織では 54% に留まっています。

セキュリティ チーム全体のチームワークと同様に、データ セキュリティ ソリューションも、他のシステム (Extended Detection and Response (XDR) や Identity and Access Management (IAM) など) とシームレスに統合することで、外部および内部からのデータ セキュリティ インシデントを効果的に防止する必要があります。これらの統合により、企業はセキュリティ インシデントに対する包括的な調査と対応を実施し、影響を受けたデータ、関係者、アクティビティを完全に理解し、複数の緩和制御で対応することができます。結果的に、情報に基づいた的確かつ迅速な対応ができるようになるため、潜在的なセキュリティ インシデントの影響を最小限に抑えることができます。

AI と自動化でデータ セキュリティ戦略をアップグレードする

自動化と AI により、組織はデータ セキュリティにさらにプロアクティブに取り組めるようになります。組織が自動化と AI への取り組みに着手するにあたっての推奨事項を以下に紹介します。

- 機密データの検出: AI を活用して機密データを識別し、暗号化や権限管理などの保護ポリシーの適用を支援しましょう。これは特に、従来のパターン認識テクノロジーでは検出が困難なビジネスデータにとって重要です。組織は、機械学習や AI を搭載した分類システムなどの分類テクノロジーを活用できます。分類システムは、そのインテリジェンスと、データのコンテキストやビジネスカテゴリに基づいて機密コンテンツを迅速に特定する能力を備えています。あるいは、組織は正確なデータ マッチング技術を導入することで、業務データや個人データを検出できます。

  さらに、業界の規制が進化し (GDPR、HIPAA、PCI DSS など)、データのランドスケープがより動的になるにつれ、新しい機密データのカテゴリーを識別する必要性があるでしょう。そこで、カスタマイズ可能で容易に適応できる高度な分類技術を所有しておくことが重要になります。

- 重要なデータ セキュリティ リスクを検出する: AI の力を活用して、機密データに関連する重大なリスクをピンポイントで特定し、戦略的にリソースを割り当てることで、潜在的な高リスクのインシデントに対処します。AI テクノロジーは忠実度の高いアラートを生成できるため、セキュリティ チームは大量の誤検知アラートの選別に費やしていた貴重な時間を節約できます。さらに AI は、捉えどころのないリスクの特定にも効果を発揮できるため、特に悪意ある行為者が検知を逃れようとする場合に有用です。こうした脅威を凌駕するには、マシンの速度を利用することが不可欠です。

- データ セキュリティ インシデントを動的に防止する: AI と自動化を利用して、評価されたリスクに基づいて予防策と緩和策を自動的に調整し、より適応性の高いプロアクティブなデータセキュリティ戦略を実現します。AI を搭載したソリューションがリスクを検出し評価すると、自動化された予防コントロールが迅速に作動し、リスクの高い部分に的確に緩和コントロールを適用してデータを保護します。たとえば、高リスクのユーザーによるデータ流出の意図を早い段階で検出した場合、組織はより厳格なデータ損失防止 (DLP) ポリシーを適用し、潜在的なデータ セキュリティ インシデントに先手を打つことができます。

このレポートでご紹介したインサイトと推奨事項が、皆様のデータ セキュリティ態勢を強化し、進化するリスクから組織を強化するお役に立てば幸いです。

マイクロソフト データ セキュリティの詳細情報については、次をご参照ください: https://aka.ms/DataSecurityNews

詳細な調査目標、方法論、対象者の募集について

調査の目的は以下のとおりです。

1. 優先事項、考え方、課題など、データ セキュリティの現状を理解する
2. データ セキュリティ インシデントの原因と結果をマッピングすることで、データ セキュリティ チームが取るべき行動を特定し、データ セキュリティの態勢を強化する。
3. データ セキュリティに AI を活用した新たな戦略やイノベーションなど、データセキュリティの未来を探る

方法:

データ セキュリティの意思決定者 822 人を対象に、2023 年 7 月 28 日から 8 月 9 日まで、15 分間の多国籍オンライン調査を実施しました。

質問は主にデータ セキュリティの状況を中心にまとめており、データ セキュリティ チームのリソース配分、データ セキュリティ インシデント、データ セキュリティに 人工知能 (AI) を使用することについての考え方をお聞きしました。

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)

企業組織で働いている (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 822 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	329
英国	322
オーストラリア	171