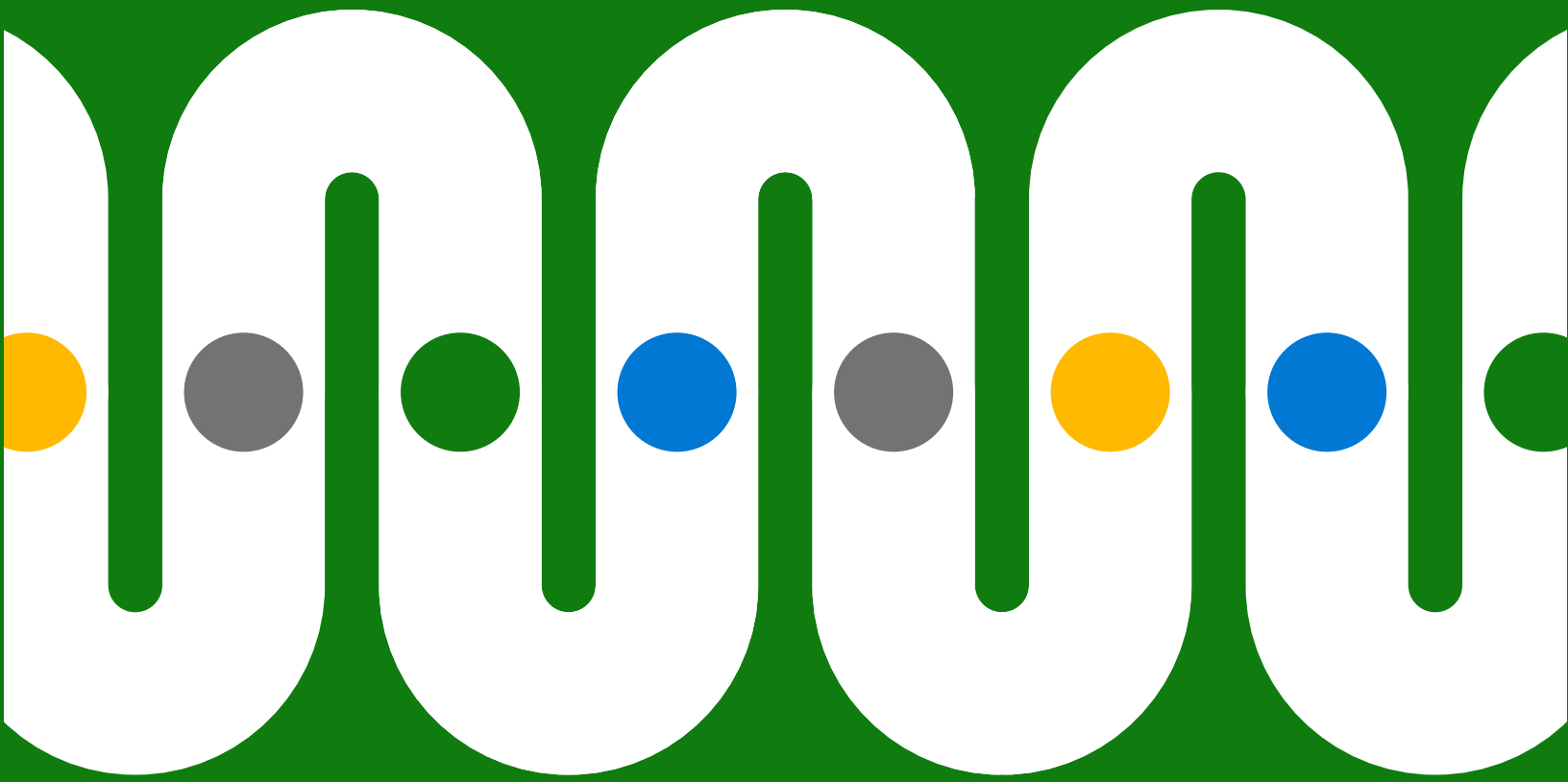
Microsoft Security

エンドツーエンドのデータ保護を実現する 3 つのステップ



目次

コンプライアンス意思決定者を対象とした調査によると、95% がデータ保護の課題を懸念しています。[2]

はじめに

組織のデジタル フットプリントはハイブリッド ワークにともなって急増してきました。これは従来の職場環境を大幅に超えています。

そして、データの断片化と流出がさらに進み、アプリケーション、デバイス、所在地の数が急速に拡大したことで、すべてが複雑化しています。さらに、多くの従業員の役割が、より大きな充実感や柔軟性を求めて変化しています。これにより増え続けるデータ資産全体に盲点が生じ、新たな課題になっています。[1]

こうしたすべての要因にともなって、CIO と CISO は情報保護の取り組みを再創造しています。実際、500 人を超える米国のコンプライアンス意思決定者を対象とした追跡調査によると、ほぼ全員 (95%) がデータ保護の課題を懸念しています。[2]

[1] " マイクロソフトが大改造中のインサイダー リスクの軽減にどのように役立つか 、Alym Rayani"、Microsoft Security。2022 年 2 月 28 日

[2] "2021 年 9 月 、マイクロソフトが Vital Findings から委託した米国のコンプライアンス意思決定者 512 人を対象とした調査 "

IT チームとセキュリティ チームは、マルチクラウド、ハイブリッド クラウド、オンプレミス環境全体でデータ ライフサイクル全体を管理する、より優れた方法を模索しています。このエンドツーエンドの取り組みを構成する 3 つの重要なステップを次に示します。

ステップ 1: データを識別する

データの保存場所、種類、使用方法や共有方法を特定します

ステップ 2: データを分類する

データを分類してラベル付けを行い、適用するべき適切なポリシーとリスク軽減策を把握します

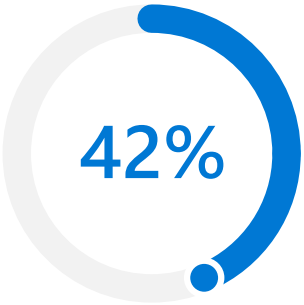
ステップ 3: データ損失を防止する

インテリジェントな検出と制御で、従業員に対するリスク軽減策と柔軟性のバランスを取ります

この取り組みの最終目標は、高い生産性を損なうことなく隙間を埋め、リスクを最小化することです。

ステップ 1

データを識別する



全体に占める "詳細不明" なデータの割合について、組織の 42% が少なくとも半分であると回答しました。[3]

こうした "識別できない" データの形式は、メールの添付ファイルや顧客との通話記録から、機器のログや監視カメラ映像に至るまで、多岐にわたります。

適切なポリシーや保護をデータに適用するためには、データの保存場所、種類、使用方法や共有方法などの特定が不可欠です。

現代の組織は膨大なデータを常に生成しています。それはドキュメント、メール、メッセージだけでなく、監視カメラの映像や位置情報も含みます。この状況は、オンプレミスとクラウドでのアプリ、デバイス、ストレージの急増にともない、すべてが悪化しています。

こうしたデータをすべて識別することは困難であり、実際、組織の 42% が自社のデータの少なくとも半分が "詳細不明" であると回答しています。[3] これはつまり、収集したものの、ビジネス上の目的が不明で活用していない情報です。作成した従業員のプロジェクトや役割が変更されることで、データの詳細がわからなくなることがありますが、多くの場合、作成や変更の時点でデータを識別する仕組みが整っていません。

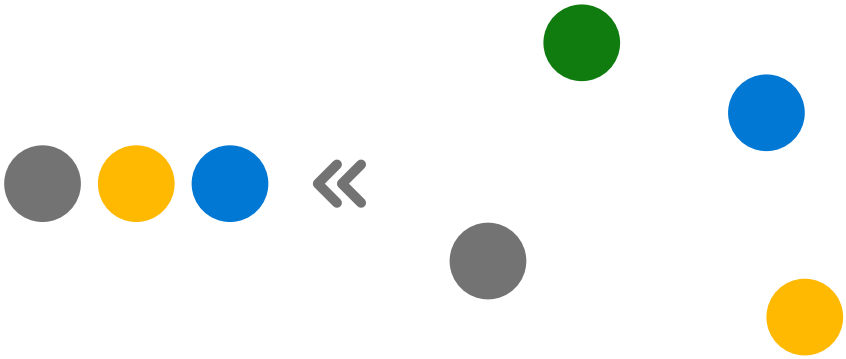
[3] "2022 State of Data Governance and Empowerment Report", Enterprise Strategy Group. 2022 年 7 月

プラットフォームを一元化して、エンドツーエンドの検出ワークフローを構築できます。

Microsoft.com で Microsoft Purview のデータ検出についてご確認ください。

この課題は今後も拡大する一方です。作成、キャプチャ、複製、利用される新しいデータの量は、2026 年までに倍増すると予想されており、企業が生み出すデータは、消費者データの 2 倍を超えるスピードで増加しています。[4]

人工知能 (AI) と機械学習 (ML) を活用すれば、メール アドレス、医療データ、クレジット カード番号、知的財産など、機密データを識別して自動で分類できます。さらに AI と ML は分類の正確性を高め、過去にさかのぼったデータの検証も実現させます。こうした識別プロセスはデータ資産全体に適用できるため、コンテンツの保存、収集、分析、レビュー、エクスポートを、保存場所やクラウドの種類によらずに実施できます。



[4] "Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", John Rydning, IDC. 2022 年 5 月

ステップ 2

データを分類する

適切なデータ分類により、適切なポリシーとリスク軽減策を決定することで、さまざまな種類のデータが誤ってまたは意図的に悪用されたり、認証を経ずにアクセスされる事態を防止できます。さらに暗号化や電子透かしを導入すれば、保存中、転送中、使用中に、データの保護を強化できます。

ただし分類とポリシーを導入する際は、組織内を移動するデータの追跡が必要です。さらにラベル付けと保護ポリシーは個別のドキュメントに限定できず、オンプレミスからクラウドベースのリポジトリ、さらにサービスとしてのソフトウェア (SaaS) から OS ネイティブ アプリに至るまで、デジタル資産全体を対象にする必要があります。

従来の分類手法は、多くの部分を手作業に頼っており、間違いや重要なデータの見落としが発生するリスクを抱えています。このプロセスはトレーニング可能な組み込み分類子によって自動化でき、さらに管理者は統合ソリューションを使用して、すべてのシステム全体に適用するポリシーを一元的に管理できます。

分類とポリシーはどちらも、移動するデータの追跡を必要とします。

たとえば、従業員がクレジット カード番号を Microsoft Word ドキュメントから Excel にコピーする場合は、分類とポリシーを両方のドキュメントに自動で適用するべきです。

環境全体の機密データを、より適切に管理し、保護できます。

Microsoft.com で Microsoft Purview のデータ分類と保護についてご確認ください。

ステップ 3

データ損失を防止する

データの特定と分類が完了したら、データ損失防止 (DLP) ソリューションによって保護ポリシーをエンド ツー エンドに適用し、詳細不明なデータやデータ流出などの脅威を軽減できます。これにより、従業員や退職者が、意図的または不注意にかかわらず、認証を回避して機密データの共有、公開、転送を実行できなくなります。

インテリジェントな DLP ソリューションはコンテキストを活用し、柔軟性の提供とバランスをとりながら、リスクの高い操作をブロックします。たとえばユーザーは、潜在的なリスクと適用されるポリシーを通知された上で、その操作を続行できる場合があります。これにより機密データを保護しながら、同時にリスクを適切に理解するためにユーザーをトレーニングできます。

DLP ソリューションは、知的財産やその他の重要なビジネス データを保護するだけでなく、一般データ保護規則 (GDPR)、医療保険の携行性と責任に関する法律 (HIPAA)、カリフォルニア州消費者プライバシー法 (CCPA) などの規制への準拠も改善します。

また、DLP に向けた包括的な取り組みで、組織全体に一貫してポリシーを適用し、データ ライフサイクルが抱える “弱点 “ を保護します。

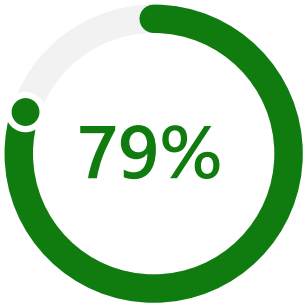
DLP ポリシーはコンプライアンスに違反したアクションを防止できます。

たとえば、従業員がクレジット カード番号を含むスプレッドシートをフラッシュ ドライブにダウンロードしたり、またはクラウド ストレージにアップロードを試みた場合、この活動を DLP ポリシーがコンプライアンス違反として識別し、阻止します。

機密情報のインテリジェントな検出と制御を実現します。

Microsoft.com で Microsoft Purview のデータ損失防止についてご確認ください。

データ保護を後から追加せずに、一部として組み込む。



コンプライアンス意思決定者を対象にした調査によると、79% がコンプライアンスとデータ保護製品を複数購入しており、

さらに過半数が 3 つ以上購入しています。[5]

多くの組織は、データ ライフサイクルの隙間を管理するために複数のソリューションを使用し、情報保護に ”後から追加する” アプローチを採用してきました。しかし、この方法では、セキュリティ、データ ガバナンス、コンプライアンス、法務の各チームが分断された状態で協力を余儀なくされるため、リソースの負担が増える上に、多くの場合、効果がありません。

その一方、“一部として組み込む” アプローチでは、データの識別、データの分類、DLP を統合して隙間を埋めることができ、統合ソリューションによってポリシーの一元的な管理と適用が容易になります。さらに、アプリケーション内にわかりやすい方法でポリシー通知を表示することで、ユーザーのトレーニング時間を削減します。

[5] "February 2022 survey of 200 US compliance decision-makers (n=100 従業員数 : 599-999 人、n=100 従業員数 : 1000 人以上) マイクロソフトの委託により MDC Research が実施。"

組み込まれた統合ソリューション : Microsoft Purview

Microsoft Purview を導入すると、データ資産全体の管理、保護、管理に役立つ包括的なソリューション セットによって、まとまりのないデータが溢れる現代の職場が抱える課題に対処できます。

ガバナンスの一歩先を目指しましょう。
Microsoft Purview によるデータ保護について詳細をご覧ください >

データ保護の各分野に特化した情報は、Microsoft Purview の活用方法に関する詳細でご確認ください :
データの探索 >

データの分類と保護 >

データ損失防止 >

Microsoft Security

©2022 Microsoft Corporation. All rights reserved. このドキュメントは現時点の情報に基づくものです。このドキュメントに記載されている情報 (URL や他のインターネット Web サイトに関する情報を含む) および見解は、将来予告なしに変更されることがあります。このドキュメントの使用に起因するリスクは、お客様が負うものとします。このドキュメントは、いかなるマイクロソフト製品の知的財産に関する法的権利もお客様に許諾するものではありません。お客様は、私的な参照目的に限り、ドキュメントを複製して使用することができます。