【Microsoft Purview】サービス概要

2025年10月31日

改訂履歴

版数	発行日	改訂内容
第1版	2025年10月31日	初版発行
第2版	2025年12月9日	スライド49：EnterpriseライセンスにTeamsを含むライセンスが復活したため、Teamsが含むのと含まれないプランが用意されている旨とその場合アドオンが必要な旨を補足説明

本資料の内容は 2025/12/9 時点のものです。製品のアップデートにより変更となる場合がございます旨ご了承ください。

Agenda

1. 前提情報
    1. 用語集
2. Microsoft Purview とは
    1. データ管理・活用における課題
    2. Microsoft Purviewの概要
3. データセキュリティ
    1. データセキュリティの概要
    2. 機能①情報保護
    3. 機能②DLP
    4. 機能③インサイダーリスク
    5. まとめ
4. データガバナンス
    1. データガバナンスの概要
    2. 機能①データマップ機能
    3. 機能②データカタログ機能
    4. まとめ
5. リスクとコンプライアンス
    1. リスクとコンプライアンスの概要
    2. 機能①監査
    3. 機能②電子情報開示（eDiscovery）
    4. まとめ
6. ユースケース
    1. ユースケース①退職予定者による機密情報持ち出し防止
    2. ユースケース②全社的な機密データ棚卸しと継続保護
    3. Copilot活用イメージ
7. ライセンス
    1. ライセンスと課金形態の概要
    2. 機能別ライセンス対応表
    3. アドオン機能

1. 前提情報

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
1	オンプレミス	企業が情報システムを自社内で保有・管理する形態。サーバーやソフトウェアを自社設備内に設置・運用します。
2	SaaS	クラウド経由でベンダーが提供するソフトウェアを、インターネット経由で利用する形態。 例：Gmail、Slackなど。
3	機密データ	漏洩、改ざん、紛失などが発生した場合に、事業や個人に重大な損害を与える可能性のある、厳重な管理が必要な情報。
4	GDPR	GDPR（(General Data Protection Regulation)）は、欧州経済領域 (EEA) における個人データ保護の法令。域外へのデータ移転規制や、違反時の高額な制裁金などで知られている。
5	シナジー	複数の要素（事業、組織、技術など）が組み合わされることによって、単独では得られない相乗効果が生じること。
6	エンドポイント	ネットワークに接続されている末端のデバイス（PC、スマートフォン、サーバーなど）。セキュリティ対策の対象となります。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
7	AWS	Amazon社が提供する世界最大のクラウドコンピューティングサービス。サーバー、ストレージ、データベースなど多様なITインフラ機能を提供します。
8	SQL Server	Microsoft社が開発・提供するリレーショナルデータベース管理システム (RDBMS) の一つ。
9	Azure Data Lake	Microsoft Azure上で提供される、ビッグデータ解析のために設計された、ペタバイト級のデータを格納できるスケーラブルなストレージサービス。
10	SQL	データベースの操作や管理に使われる標準的な言語。データの検索、挿入、更新、削除などを行う際に使用されます。
11	Sentinel	Microsoft Azure上で提供される、クラウドネイティブなSIEM (Security Information and Event Management) ソリューション。セキュリティログを集約・分析し、脅威を検出します。
12	Power BI	Microsoft社が提供するビジネスインテリジェンス (BI) ツール。データの可視化や分析を行い、意思決定を支援します。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
13	エージェント	PCや端末にインストールして動作するソフトウェアで、クラウド環境だけでは取得できない操作ログやファイル操作の情報を収集するために使用されます。
14	Compliance Manager	Mictrosoft Compliance Managerは、組織のマルチクラウド コンプライアンス要件をより簡単かつ便利に管理するのに役立つ Microsoft Purview コンプライアンス ポータルの機能です。データ保護リスクのインベントリの作成から、複雑な制御の実装の管理、規制や認証の最新情報の入手、監査人への報告まで、コンプライアンスの過程全体を支援します。
15	営業秘密	企業が事業上の競争力を保つために秘密として管理している重要な情報のこと。 技術情報（設計図、製造方法など）や営業情報（顧客リスト、価格情報など）が含まれます。 「秘密として管理されている」「事業に有用」「一般に知られていない」の3要件を満たすと、法律で保護されます。Purviewでは、営業秘密に該当する情報を分類・保護することが可能です。
16	Google Cloud	Google が提供するクラウドプラットフォームの総称。インフラ（仮想マシン、ストレージ、ネットワーク）から、AI・データ分析・開発ツールまで幅広いサービスを提供しています。 Microsoft AzureやAmazon Web Services（AWS）と同様に、企業がシステムやデータをクラウド上で運用するための基盤となります。
17	プレディクティブコーディング	電子情報開示（eDiscovery）などの分野で使われる、機械学習（AI）を利用した文書の選別・分類技術です。膨大な電子データの中から、裁判や調査で必要となる「関連性の高い文書」を効率的かつ正確に見つけ出すために使用されます。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
18	フォレンジック調査	「フォレンジック調査」は、IT分野では主に「デジタルフォレンジック（Digital Forensics）」を指します。サイバー攻撃や企業内不正、訴訟などのインシデントが発生した際に、コンピューターやネットワーク、スマートフォンなどのデジタル機器に残された電磁的記録を、法的な証拠として利用できる形で収集・分析する科学的な調査手法です。
19	メタデータ	データそのものの内容ではなく、そのデータを説明するための情報のことです。 例：ファイル名・作成者・作成日・保存場所・サイズなどがメタデータにあたります。
20	API	アプリケーション同士がデータや機能をやり取りするための仕組み。 Purviewでは、監査ログや分類情報を外部システムに自動取得したり、他のツールと連携する際に利用。 APIを使うことで、人手を介さずに処理の自動化やデータ統合が可能になります。
21	アクセス帯域	一定時間内に送受信できるデータ量の上限を示す指標。 Purviewでは、監査ログの取得や分類処理の速度に影響し、大量データを扱う場合は帯域が重要。 Premiumではより高い帯域が利用可能で、大規模組織でも高速に処理できる。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
22	スキャンルール	Purviewのデータマップで使用される設定項目です。データソースをスキャンする際に、どの範囲・頻度・方法でメタデータを収集するかを定義します。スキャンルールを設定することで、特定のフォルダーやファイル形式のみを対象にしたり、スケジュール実行を自動化したりできます。これにより、効率的かつ一貫したデータ資産の可視化・分類が可能になります。
23	AIP（Azure Information Protection）	Microsoft が提供する情報保護ソリューションで、機密度ラベルを使ってファイルやメールに分類・保護を適用できます。暗号化やアクセス制御を行い、組織外への情報漏えいを防止します。現在は Microsoft Purview 情報保護に統合されています。
24	統合ラベル付けクライアント（Unified Labeling Client）	Microsoft の情報保護ラベルをローカル環境で適用・表示するためのクライアントツールです。AIP クライアントの後継で、Microsoft 365 コンプライアンスセンターと統合され、統一されたラベルポリシーを利用できます。現在は Purview への統合が進んでいます。
25	セルフホステッド統合ランタイム（SHIR）	オンプレミス環境とクラウドサービス（Microsoft Purview、Azure Data Factory など）の間で安全にデータやメタデータを転送するためのコンポーネントです。社内ネットワーク上にインストールして、オンプレミスのデータソースをクラウドからスキャン・接続可能にします。

2. Microsoft Purviewとは

2.1. データ管理・活用における課題

近年、企業が扱うデータ量は急速に増加し、オンプレミス環境・クラウド環境・SaaSなど多様な場所にデータが分散しています。
これにより、「どこに・どのようなデータが存在しているのか」「誰がアクセスできるのか」「適切に保護されているのか」といった全体像の把握が難しくなっています。
一方で、データは単なる保管対象ではなく、業務改善や新たな価値創出のための重要な資産としての活用が求められています。
しかし、多くの企業では以下のような課題が見られます。

データの所在や構造が把握できない
データが部門・システムごとに散在し、統一的なカタログや可視化が行われていない。

ガバナンス・セキュリティの不備
アクセス権限や機密データの管理が属人的であり、情報漏洩リスクを抱えている。

コンプライアンス対応の複雑化
法規制（例：個人情報保護法、GDPRなど）に沿ったデータ分類・監査が困難。

データ活用の非効率
必要なデータを見つけるのに時間がかかり、データ分析やAI活用のスピードが低下。

Microsoft Purview は、こうした背景のもとで生まれた **統合的なデータガバナンスおよびコンプライアンスプラットフォーム** です。
データの発見・分類・カタログ化から、アクセス権限の管理、リスク・コンプライアンス対応までを包括的に支援し、組織全体での **安全なデータ利活用の基盤** を提供します。

2.2. Microsoft Purviewの概要

Microsoft Purview（以下、Purview） は、組織全体のデータを 安全に管理・活用するための統合プラットフォームです。
クラウド、オンプレミス、SaaS など多様な環境に散在するデータ資産を可視化・分類・制御し、データガバナンス、セキュリティ、コンプライアンスを一元的に実現します。Purviewは主に以下の3つの領域で構成されています。

Microsoft Purview

データセキュリティ

組織のデータを「誰が・どのように」利用できるかを制御し、**機密情報を保護する領域**です。
Microsoft 365 や Azure などのサービスと連携し、機密データの自動検出・分類、暗号化、アクセス制御、データ損失防止（DLP）などを通じて、データ漏えいリスクを低減します。

データガバナンス

組織全体の**データ資産を可視化・整理し、信頼性あるデータ活用を促進する領域**です。
データカタログ機能により、データの所在・構造・利用状況を一元管理し、ユーザーが必要なデータを迅速に発見・活用できる環境を提供します。また、データのリネージ（流れ）や所有者情報の把握にも役立ちます。

リスクとコンプライアンス

法令・規制・社内ポリシーに準拠したデータ管理を実現する領域です。
個人情報や機密データの検出、コンプライアンスポリシーの評価、監査レポートの自動化などを通じて、組織のコンプライアンス対応を効率化します。
Microsoft 365 の Compliance Manager と連携することで、規制準拠状況を可視化することも可能です。

Purview はこれらの領域を横断的にカバーすることで、**「データを守りながら最大限に活用する」ための統合的基盤** を提供します。
次の章から、上記のPurviewを構成する主な領域である「データセキュリティ」、「データガバナンス」、「リスクとコンプライアンス」 の3つの観点に分けて、その機能と特徴を詳しく説明します。

2.2. Microsoft Purviewの概要

Purview活用の基本的な流れ

Purviewは、組織のデータを保護・管理・活用するための統合プラットフォームです。
しかし、Purviewは自動で全てを判断するツールではなく、**人が定めたルールや社内統制方針に基づき動作するサポートツール**です。一般的に「社内ルール策定 ＞ データの可視化　＞　分析 ＞ 分類・ラベル付与 ＞ 対応・改善」という流れで、組織の意思決定や運用を支援します。
この流れを理解することで、Purviewの役割と、組織における人の判断との関係を明確に把握することができます。

ポイント

・Purviewを導入する前に、データの分類ルールやラベル運用方針、アクセス権限など社内ルールをあらかじめ整備しておかないと、管理が煩雑になり運用負荷が高くなる可能性があります。

2.2. Microsoft Purviewの概要

Purviewの各機能で扱えるデータ範囲

ここではPurviewの主要な機能のそれぞれが組織のデータ全体をどこまでカバーし、特にオンプレミス環境にどのように対応しているかを一覧で整理します。

■データセキュリティ

	主な対象データ	オンプレ対応	説明
情報保護	主にMicrosoft 365内データ（Exchange、SharePoint、Teams、OneDrive）などのクラウドデータ及びエンドポイント	△	一部の機能で対応。AIPスキャナーや統合ラベル付けクライアントを使用することで、オンプレミスのファイルサーバーやSharePoint Server 上のファイルにも秘密度ラベルを適用可能。ただし、クラウド環境に比べて設定や運用に追加の構成が必要です。
DLP	Microsoft 365 サービス内、エンドポイント、Teams、オンプレミスのSharePoint/Exchange/ファイル共有、非Microsoft クラウドアプリ	△	DLPオンプレミス統合を構成することで、オンプレミスのSharePoint ServerやExchange Serverを限定的に対象化可能。また、Endpoint DLPによりオンプレミスPC上の操作（コピー、印刷、USB転送など）を監視・制御可能。
インサイダーリスク	Microsoft 365上の操作ログ	△	Endpoint DLPの活動ログをシグナルとして統合することで、オンプレPC上の一部操作（USB転送、印刷など）を検知可能。ただし、インサイダーリスク管理自体はクラウドサービスの操作を主に対象。

2.2. Microsoft Purviewの概要

■データガバナンス

	主な対象データ	オンプレ対応	説明
データマップ	Azure、Microsoft 365、オンプレミスのデータベース（SQL Server、Oracleなど）、SaaSなど、広範なデータソース。	△	一部の環境で対応。セルフホステッド統合ランタイム（SHIR）や各種データコネクタを使用することで、オンプレミスのファイル共有やデータベースからメタデータをスキャンし、Purviewのデータマップに取り込むことが可能。ただし、構成には追加のセットアップが必要で、対応データソースも限定されます
データカタログ	データマップで収集された全データ資産	○	データカタログ機能自体はクラウドサービス上で提供されますが、データマップがオンプレミス環境を含むデータ資産を統合的に管理しているため、カタログからもオンプレミスのデータ資産を検索・発見できます。

2.2. Microsoft Purviewの概要

■リスクとコンプライアンス

	主な対象データ	オンプレ対応	説明
監査	ほぼすべての Microsoft 365 サービス (Exchange Online, SharePoint Online, Teams, Entra IDなど) での操作ログ	✕	監査ログ機能は Microsoft 365 のクラウドサービスにおけるユーザーおよび管理者のアクティビティを対象としています。オンプレミス環境での操作やアクティビティは収集対象外です。
電子情報開示（eDiscovery）	Microsoft 365 サービス内のすべてのデータ（Exchange Online、SharePoint Online、OneDrive for Business、Teams、など）	△	部分的に対応。ハイブリッド構成を利用することで、オンプレミスの Exchange Serverおよび SharePoint Serverのコンテンツを電子情報開示の検索・収集対象に含めることが可能です。ただし、クラウドベースの 電子情報開示機能に比べ、構成や機能には一部制限があります。

2.2. Microsoft Purviewの概要

Purviewを導入する際のメリットとポイントについて紹介いたします。

メリット

■ データ管理の効率化
データマップやカタログ機能により、社内の膨大なデータを一元管理します。
クラウド・オンプレミス問わず「どこに・どんなデータがあるか」を可視化し、管理者の負担を軽減します。

■ データ利活用の促進
用語集や分類情報で、必要なデータをスピーディに検索可能です。
業務や開発でのデータ探索時間を短縮し、生産性向上につなげます。

■ 自動分類によるリスク低減
機密情報を自動検出・分類し、重要データを確実に保護します。
ラベル付けや暗号化を自動化することで、情報漏洩リスクを軽減します。

■ アクセス管理の統合と可視化
クラウドやオンプレミスを含むハイブリッド環境でも、Purviewを通じてデータ全体に一貫した分類・ポリシーを適用可能です。
Entra IDなどの認証基盤と連携し、アクセス権限の統一的な管理や不正行為・外部流出の検知を行えます。

ポイント

・データの 「検出 → 分類 → 保護 → 監査」 を一気通貫で管理し、セキュリティと利活用を両立します。
・Purviewを導入する前に、データの分類ルールやラベル運用方針、アクセス権限など社内ルールをあらかじめ整備しておかないと、管理が煩雑になり運用負荷が高くなる可能性があります。

3.データセキュリティ

3.1. データセキュリティの概要

「データセキュリティ」は、組織のデータを保護し、情報漏洩や不正アクセスなどのリスクを最小限に抑えるための包括的なソリューションです。
組織の情報セキュリティを確保するために、**予防・発見・防止**の3つの管理手段を提供しています。

個人情報・営業秘密の保護対策

予防

機微情報の可視化と保護

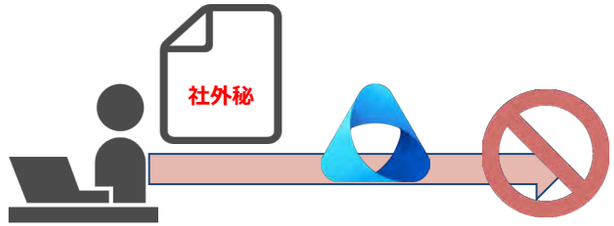
識別・分類　　**ラベル適用（暗号化/保護）**

営業秘密を社外に出さない仕組み」を整える

情報保護

防止

DLPによる情報漏洩のブロック



誤共有、誤送信などを防ぐ

データ損失防止（DLP）

発見

操作ログを清算して効率的に内部不正リスクを検知、対処

不正を見逃さず、早い段階で対処

インサイダーリスク管理

3.2. 機能①情報保護

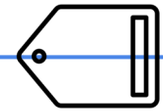
Microsoft Purview 情報保護は、クラウド、オンプレミス、エンドポイントなど、**あらゆる場所に存在する企業の機密情報を発見**し、**自動で分類・ラベリングを行い**、その情報がどこにあっても、誰と共有されても、**適切なアクセス制限と暗号化で情報漏洩のリスクを最小化するソリューションです**。Microsoft 365 のサービス全体で一貫したデータ保護を実現し、データがどこに保存・共有されても安全に管理できる点が大きな特徴です。

主な特徴

■自動検出によるリスク可視化

・個人情報（氏名、住所、クレジットカード番号情報など）や、機密データをAIで自動検出します。

・リスクを早期に可視化し、誤送信や共有ミスを防止します。



■柔軟な分類・ラベリング機能

・機密度に応じてデータに「公開」「社外秘」「機密」などのラベルを自動・手動で付与します。

・分類ルールをカスタマイズすることも可能です。

■ラベルに基づく暗号化とアクセス制御

・秘密度ラベルに基づき、ファイルやメールに暗号化とアクセス権限を自動的に付与します。

・共有相手のユーザーやドメインを指定し、安全に外部とコラボレーション可能です。ファイルを社外に送っても、暗号化と権限制御が維持され、情報漏洩を防ぎます。

■シームレスなユーザー体験

・Microsoft 365の各アプリ（Outlook、Word、Teamsなど）に情報保護機能が標準で組み込まれており、ユーザーは特別な操作を意識せずにラベル付与や暗号化を実施可能です。普段の業務フローの中で、セキュリティと利便性を両立します。

Microsoft Purview 情報保護は、従来の“守る”仕組みではなく、“データがどこにあっても自動で守られる”仕組みを提供します。

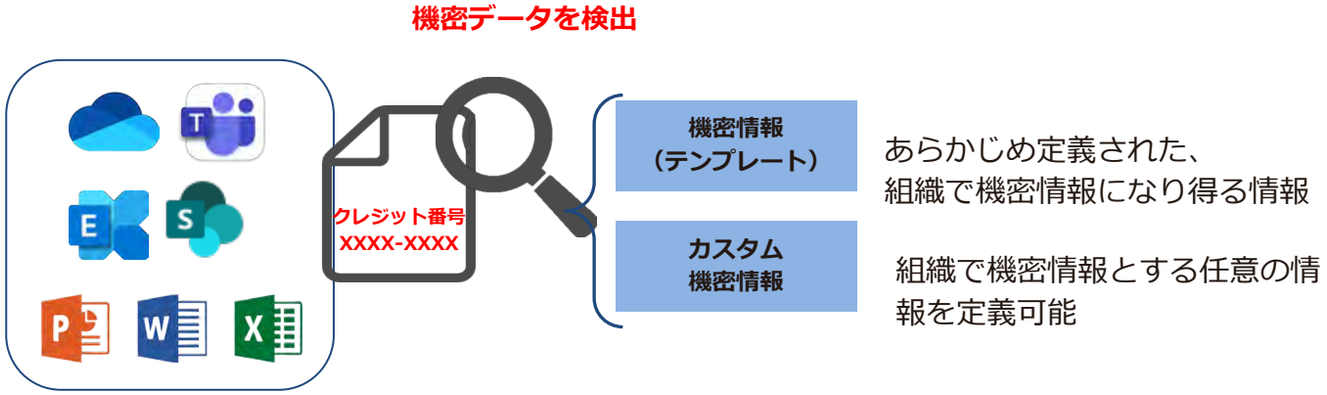
3.2. 機能①情報保護

「予防」の役割を担う情報保護（Information Protection）では、**データの検出から分類・保護までを一貫して行うことが可能です**。手動・自動のラベル付けに対応しており、機密データの管理を自動化できます。
Purview では、組織内外のデータを自動的にスキャンし、個人情報や財務情報などの機密データを検出します。
この「検出」によって、保護すべきデータを可視化し、次のステップである分類・ラベリング、暗号化へとつなげていくことができます。

検出

機密情報の定義と検出で守るべき情報を特定

・Purview では、あらかじめ定義された250種類以上の**標準テンプレート（マイナンバー、クレジットカード番号、医療情報など）**や、**組織独自のカスタムルール（キーワード・正規表現・辞書など）を使用**して、**ファイルやメールに含まれる個人情報・財務情報・機密文書などを自動的に検出します。**
・検出されたデータは「機密情報を含む」と判定され、**分類・ラベル付与・保護の対象となります。**



検出/保護対象範囲

・Exchange（メール）、SharePoint、OneDrive、Teams、Officeファイルなど、Microsoft 365全体のデータに加え、オンプレミスやクラウド（AWS、Google Cloud等）にあるデータソースも対象に含めることが可能です。

メリット

・広範囲なデータの自動検出で、リスクを早期に可視化することが可能です。
・人手では難しいデータ量にも対応し、誤検知や見落としを削減できます。
・検出結果をもとに自動でラベル付与・保護を実施でき、運用を効率化できます

3.2. 機能①情報保護

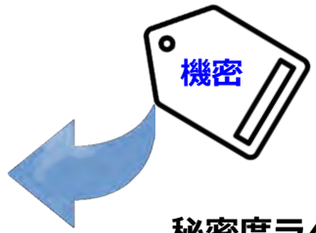
分類・ラベル化

機密情報の暗号化で、参照範囲を限定し、二次利用・漏洩を防止

・検出された機密データに対して、自動または手動でラベルを付与することで、データの重要度に応じた保護ポリシーを適用できます。
・データに「一般」、「機密」、「社外秘」など、データの重要度に応じて秘密度ラベルを付与し、ラベルごとに暗号化・アクセス制御・透かし表示などの保護を自動/手動で適用します。
・ラベル付けにより、誰がどこまでデータにアクセスできるかを明確化し、情報漏洩や二次利用を防止します。

保護・暗号化

検出・分類・ラベル付与の結果に応じて、Purview はデータに対して**暗号化やアクセス制御、透かし表示などの保護を適用**します。これにより、社内外を問わず安全な共有とコラボレーションが可能になります。



秘密度ラベル

分類

データの重要度を明示・管理するための秘密度ラベルを付与
・ファイルやメールに「一般」「機密」「社外秘」などのラベルを設定し、機密度を分類
・ラベル情報はファイル自体に埋め込まれ、他環境でも保持

＋

保護

不正アクセスや誤送信を防ぐ
・ファイルを暗号化
・アクセス可能なユーザーや操作権限を制限

マーキング

視覚的に機密情報であることを示す
・ヘッダー、フッター、透かしに機密度やファイル情報を表示

3.2. 機能①情報保護

ラベルに基づく主な保護設定

検出されたデータにラベルを付与すると、そのラベルに応じて**適切な保護が自動的に適用**されます。
つまり、「このデータは機密」「社外秘」などのラベルが付くと、誰がどのように扱えるかを自動で制御できるのです。

保護種類	内容	具体例
暗号化	特定のユーザーやグループのみアクセス可能にする	「社外秘」ラベルが付いたファイルを社外に送信しても、社内ユーザー以外は開けない
アクセス制御	印刷・コピー・転送などの操作を制限	「機密」ラベルのドキュメントはコピーや印刷を禁止し、情報漏洩を防止
透かし表示（マーキング）	ファイル上に「社外秘」などの透かしを自動付与し、視覚的に機密情報であることを示す	「社外秘」ラベルが付いたWordやPDFに自動で透かしを表示

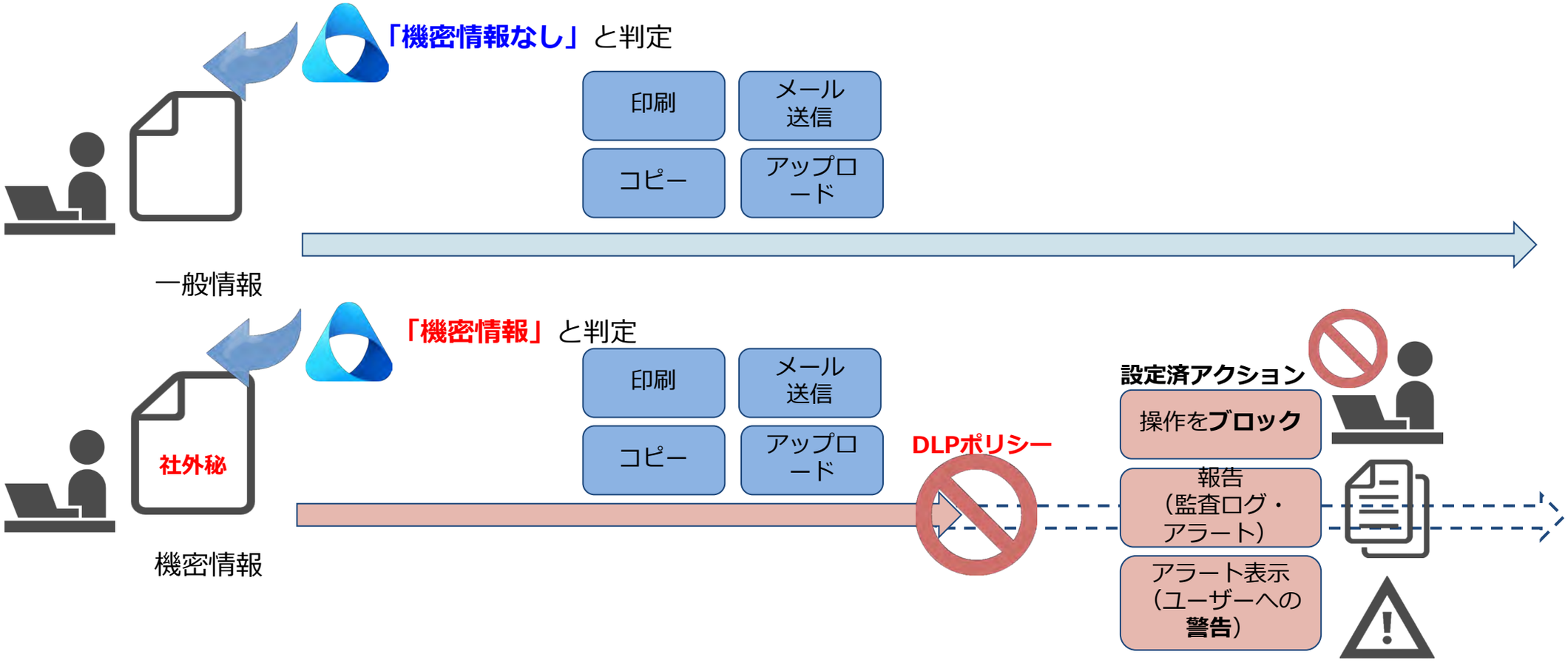
メリット

自動化で運用負荷を軽減：ルールに基づいたラベル付与や保護の適用を自動または推奨（管理者に通知し、ラベル付与の最終判断実施）で可能（リスク度合いに応じた柔軟な運用に対応）
情報漏洩リスクの低減：データに応じた保護を一元管理
社内外での安全なコラボレーション：ラベルに基づきアクセス権限を統一

3.3. 機能②DLP

情報保護の「防止」の役割とされるDLP（Data Loss Prevention：データ損失防止）は、**組織の機密情報が意図せず社外へ送信・共有されることを防ぐ**ための機能です。

Exchange（メール）、Teams、SharePoint、OneDriveなどの通信・保存データを常時監視し、あらかじめ設定した**ポリシーに基づいて「検出」「警告」「ブロック」を自動で実行します。これにより、人為的な誤送信や不正持ち出しによる情報漏洩リスクを未然に防止します。**



3.3. 機能②DLP

DLPと従来の情報漏えい対策とでは、情報漏洩を防ぐ情報の範囲が異なります。いい換えれば、従来の情報漏洩対策ではすべての情報を対象とするのに対し、DLPは特定された機密情報のみが対象となります。

主な特徴

■機密データを自動的に検出・保護

・重要データ（マイナンバー、クレジットカード番号、社員IDなど）を自動検出

・カスタム定義で独自データも検出可能

・検出したデータに基づき、送信ブロックや暗号化、通知などのポリシーを自動適用

■リアルタイム検出とユーザー通知

・データが送信・共有されるタイミングでポリシーを自動評価

・リアルタイム警告により、ユーザーにその場で注意喚起

・監査ログ・アラート によって管理者が即時に違反を把握可能

■Microsoft 365 全体に統一ポリシーを適用

・Exchange Online、SharePoint、OneDrive、Teams、エンドポイントなどに同一ポリシーを展開可能

・Purviewポータルから一元管理できるため、運用負荷を軽減

■レポート・監査機能による可視化

・検出状況・違反傾向・ポリシー効果をレポートで可視化

・Microsoft 365 Defender や Sentinel との連携でセキュリティ監視を強化

・検出データをもとにリスク分析・改善策立案が可能

3.3. 機能②DLP

DLPポリシーの仕組みと設定イメージ

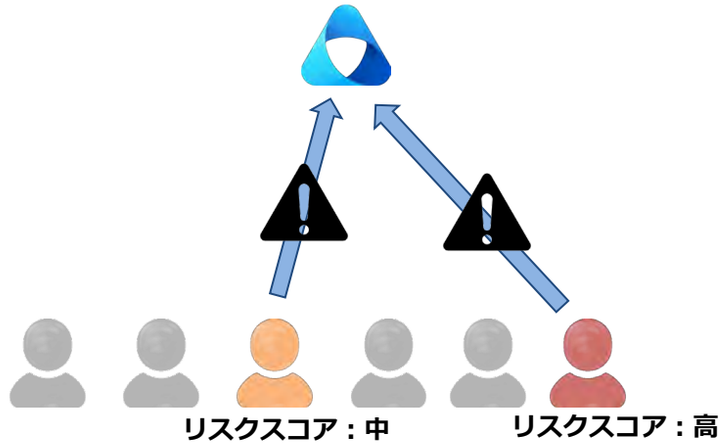
DLPポリシーは、「どのようなデータを」「どのような条件で」「どう保護するか」を定義するルールです。
Purviewでは、テンプレートを活用して短時間でポリシーを作成・適用できます。

ポリシー設定	設定内容	設定例
スコープ	対象とするサービス範囲を指定。 Exchange online（メール）, SharePoint, OneDrive, Teamsなどから選択可能。	Teams ＋ OneDrive
検出条件	DLPが違反を検知するためのルールを設定。 ・機密情報タイプ（例：「マイナンバー」「クレジットカード番号」など） ・分類・ラベル付けされたデータ ・ファイル拡張子や種類 ・コンテンツの共有条件	”マイナンバー” ＋”外部共有時”
アクション	ユーザーの操作に対してシステムが直接行う制御を定義。 （例：送信ブロック、暗号化、自動ラベル付与、警告表示（ポリシーチップ）など）	警告表示／送信ブロック／報告通知
通知/報告	アクションとは別に、情報を伝える仕組みを定義。 （例：ユーザーへのポップアップ警告、管理者へのメール通知、違反レポート生成、監査ログ記録など）	ポリシーチップ通知／管理者アラート

3.4. 機能③インサイダーリスク管理

最後にPurview 情報保護の「発見、検知」の役割である「インサイダーリスク管理」についてです。社内からの情報漏洩や不適切なデータ利用を防ぐため、**ユーザーの意図的・非意図的なリスク行動を監視・分析し、潜在的リスクを早期に検出し対応を支援します。**

ポリシー設定により、リスク管理が可能で、**リスクのある行動をスコア化することができます。**



主な特徴

■リスクの自動検出
・従業員のファイル操作、メール送信、Teams/SharePoint の利用状況などを監視
・異常な行動パターンや機密情報の不適切利用を自動で検出

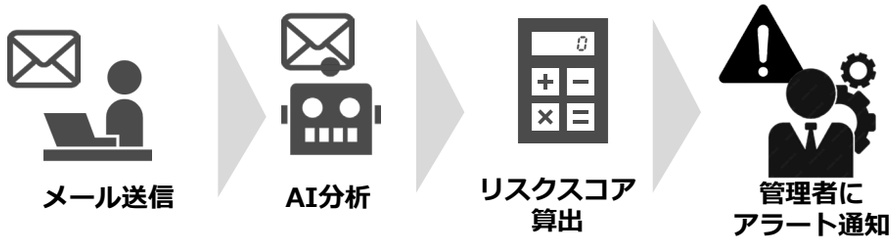
■AIによる行動分析
・過去の行動パターンや類似ケースをもとに**リスクスコアを算出。**リスク度合を0～100で評価し、高スコアのユーザーや行動を優先的に管理者が確認できる
・潜在的な情報漏洩や不正行為を事前に可視化

■リスク管理ポリシーの設定
・機密データの外部送信、異常なダウンロード、ポリシー違反など、どのような行動をリスクとみなして検知・監視するかルールをあらかじめ設定

■対応・調査の支援
・リスクの高い行動を検出すると自動でアラートを管理者に通知
・調査用のログや詳細レポートを提供し、迅速な対応を支援

3.4. 機能③インサイダーリスク管理

インサイダーリスク管理では、社員の行動を単に監視するのではなく、AIが行動パターンを分析して潜在的なリスクを自動評価します。
ファイル操作やメール送信、チャットでのやり取りなど、組織内のデータ利用状況を幅広くチェックし、リスクスコアを算出して優先度の高い案件を可視化します。この仕組みにより、管理者は膨大なログを個別に確認することなく、早期にリスクを把握して対応できます。



リスクとされる行動

種類	内容	例
機密情報の持ち出し	社外への不正持ち出しやUSBへのコピーなど	ファイルを個人クラウドに保存、メールで転送
異常なデータアクセス	通常の業務範囲を超えた大量ダウンロードや閲覧	大量の顧客情報を短時間でダウンロード
誤送信・誤共有	本来アクセスすべきでない相手に情報を送信・共有	社外メールへの送信、誤ったTeamsチャネルで共有
退職者や異動者によるリスク	権限変更前後の不適切なデータ利用	退職予定者が重要データを個人メールに送信

メリット

・社内外への情報漏洩リスクを早期に把握できる
・自動化・AI分析により運用負荷を軽減
・法規制・コンプライアンスへの対応が容易
・従業員の行動を可視化し、リスク管理の透明性向上

3.5. まとめ

データセキュリティについてのポイントと、できないことをまとめています。

ポイント

◆機密データの自動検出と分類
・組織内外に存在する機密情報を自動的に検出・分類し、秘密度ラベルによる一貫した保護を実現します。
◆DLPによる漏洩対策
・メール送信やクラウド共有時など、機密データの不適切な共有・転送をリアルタイムで検知・制御します。
◆インサイダーリスク管理による内部リスクの低減
・異常な行動や情報持ち出しの兆候を検出し、早期にリスク対応を行うことで内部不正を未然に防止します。
◆統合ポリシーによる一元管理
・情報保護・DLP・リスク管理が共通の分類・ラベルを利用し、Microsoft 365全体で統一されたポリシー運用が可能です。

できないこと/注意点

◆ データ保護（Information Protection）
・外部ツールや古いOfficeではラベル自動適用できない場合がある
・ファイルコピーやスクリーンショットの完全防止は不可
・PDFなど一部形式の透かし自動付与は制限あり

◆DLP
・Microsoft以外のクラウドサービスには適用不可

◆インサイダーリスク管理
・ローカルPC上のすべての操作ログは取得不可（Microsoft Endpoint DLPエージェントが必要）
・すべてのメール添付やチャット内容のリアルタイム監視は不可

4. データガバナンス

4.1. データガバナンスの主な機能

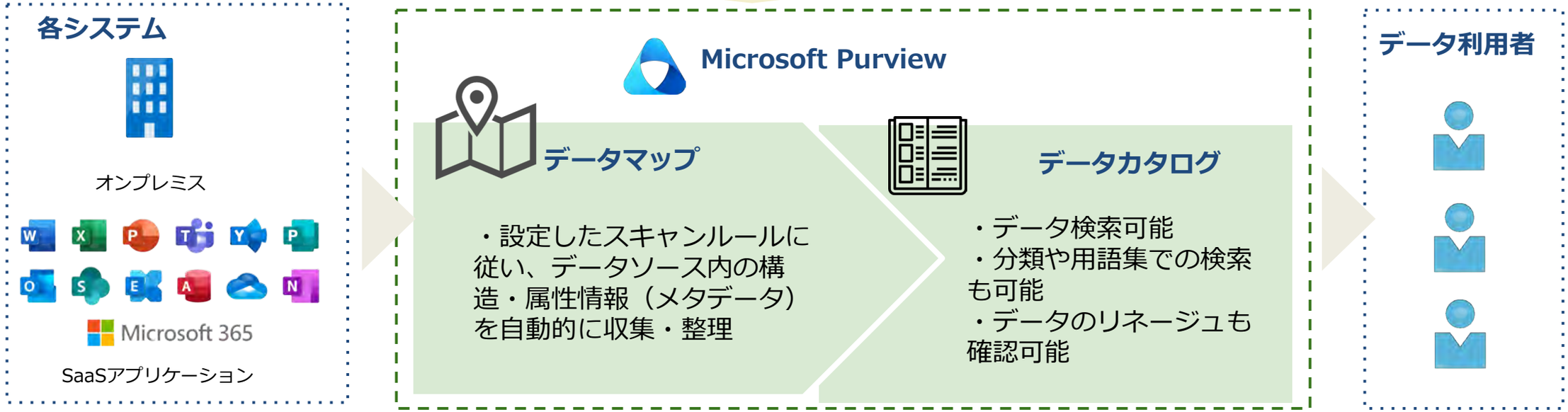
「データガバナンス」は、**社内に分散するデータを一元管理し、整理・可視化することで、業務効率化とデータ活用を促進する機能**です。
企業内でデータが部門ごと・システムごとに散在すると、以下のような課題が生じます。

データの信頼性が低い
（どこにどのデータがあるかわからない）

必要な情報を見つけにくい
（最新版が不明、重複データが多い

管理統制が難しい
（権限や利用状況の把握が困難）

データの自動的な検出・見える化を行う「地図」のような役割である **データマップ** 、
ユーザーが**データを検索・理解・共有するための「図書館」の役割**、 **データカタログ**にて
データ資産の全体像を把握し、ビジネスにおける適切な利用を促進し、可視化・統制することが可能です。



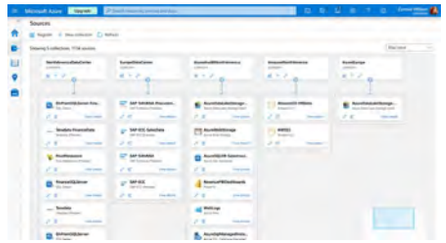
4.2. 機能①データマップ

Microsoft Purview の 「データマップ」機能 は、**クラウド、オンプレミス、SaaS などに分散するデータ資産を自動でスキャンし、**
「どこに・どんなデータがあるか」「どのようにつながっているか」 を**一元的に可視化する機能です**。
データ資産を“地図”のように把握することで、データ管理や分析、ガバナンスの効率を大幅に向上させることができます。

主な特徴

機能	内容	補足
データの可視化	依存関係の可視化：分散するデータの所在や構造を把握。テーブルやファイル、レポート間の参照・加工関係を把握し、変更の影響範囲を事前に確認可能	SQL Server、Azure Data Lake、SharePoint、Salesforce などのデータソースを可視化
自動スキャン・分類	接続先のデータをスキャンし、種類や属性を自動分類	個人情報、財務データ、顧客データ、機密情報など
データリネージュ	データがどこから来て、どのように変換され、どこで使われているかを追跡し可視化する機能	Excel → SQL → Power BI など、データの利用経路を可視化し影響範囲を分析
メタデータ管理	ファイル名、作成者、更新日時、保存場所などを一元管理	ポリシー適用や検索、レポート作成に活用可能

SaaSアプリ　オンプレミス



・データの可視化
・分類　・リネージュ管理

メリット

・従来、人の手によって行われていたデータの分類作業が、データの整理や管理が容易になり、どのデータと依存関係があるのか把握できます。
・不要なデータを整理してデータの最適化を図ることができます。
・ラベルを付けてデータを分類することで、データ管理が視覚化され、管理者の負荷が軽減します。

4.3. 機能②データカタログ

「データカタログ」は、企業内のデータを整理・分類し、ユーザーが必要なデータを辞書のように素早く検索できる機能です。
前スライドのデータマップで収集した情報をもとに、データの所在や内容を把握し、利活用を促進します。
例えば、社内のエンジニアやデータアナリスト、データ科学者が分析作業を行う際や利活用促進のために、必要なデータを提供できます。

主な特徴

機能	内容
検索性の向上	・データ名、説明、作成者、更新日時などを整理 ・キーワードやタグで迅速に検索可能
タグ付け・カテゴリー管理	・用途や部門ごとにカテゴリーを作成 ・関連データにタグを付けてグループ化 例：「顧客リスト」「売上データ」など
データの詳細情報を提供	・出所、所有者、利用履歴、所管部署、関連データを一覧表示 ・データの正確性・信頼性を保証

メリット

・必要なデータをすぐに見つけられる
キーワード検索やタグ・カテゴリーで、データ発見の時間を大幅に短縮。分析やレポート作成の効率が向上。
・データの信頼性・正確性を担保
出所や所有者、利用履歴、関連情報を確認でき、重複や誤用を防止。組織全体で安全にデータを活用。
・部門横断でデータを活用・再利用
アクセス権限を適切に管理しながら、必要なデータを共有。データ利活用の促進とガバナンス強化を両立。

4.4. まとめ

データガバナンスのポイントと、できないことをまとめています。

ポイント

◆データマップで全社データを可視化
・クラウド・オンプレミス問わず、組織内のデータ資産を自動で収集・分類
・データの所在や種類、利用状況を一目で把握可能

◆データカタログで検索・活用が容易に◎
・データの内容や意味、所有者情報を統合管理
・ユーザーは必要なデータを簡単に検索・理解・活用できる

◆分類・ラベリングとの連携でセキュリティ強化
・機密情報や個人情報などの分類を一元管理
・データ活用時に誤使用や漏洩リスクを低減

できないこと/注意点

◆ データマップ
・すべての社内外データソースを自動で収集・マッピングするわけではない
→ 対応コネクタが必要、非対応のシステムは手動登録が必要
・データの内容や意味までは自動理解できない
→ データの分類や重要度は管理者が設定したルールやラベル付与結果に依存
→データ保護でラベルを付与した後にデータマップで収集・分類することで、ラベル情報も含めてカタログ化される

◆データカタログ
・自動でデータの品質や正確性を保証するものではない
・全ユーザーの検索アクセス権を自動制御するわけではない
→ カタログのアクセス権は管理者が個別設定する必要あり
・データの構造的な関係は可視化できるが、業務的なつながりや計算処理の依存関係は管理者やユーザーが手動で補足する必要がある
・実際の分析やレポート作成は行えない
→データカタログはあくまでデータの参照先・発見を支援するツール。分析やレポート作成には別のツール（Power BI、Excelなど）を使用する必要がある

5.リスクとコンプライアンス

5.1. リスクとコンプライアンスの概要

Purview の「リスクとコンプライアンス」は、**組織内の情報の扱いを可視化し、内部不正・情報漏洩・法令違反などのリスクを早期に検知・防止するための統合ソリューションです**。データの取り扱い履歴を監査したり、法的対応のための証拠データを収集・管理したりすることで、信頼性の高いガバナンス体制の構築を支援します。主な機能として「監査」「電子情報開示（eDiscovery）」があります。

監査

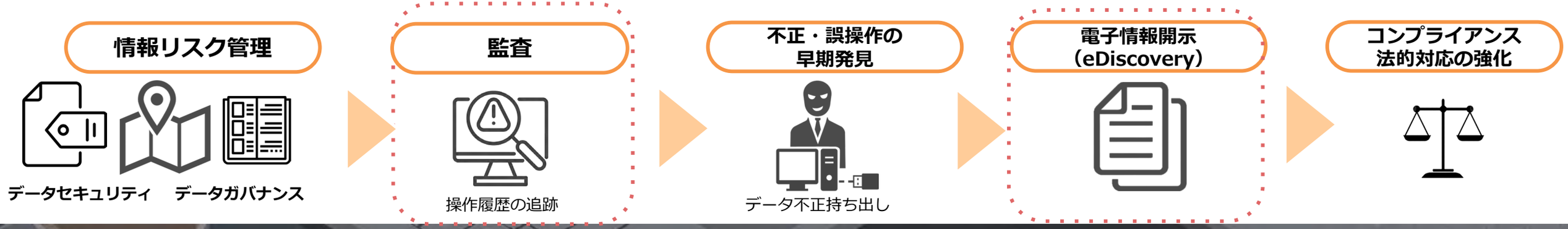
・ユーザーや管理者の操作履歴を記録・追跡
・不正操作や誤操作の早期発見、監査対応を支援

電子情報開示（eDiscovery）

・訴訟や調査のために必要な電子データを効率的に検索・保全・エクスポート
・コンプライアンスや法的対応を支援

コンプライアンス強化のプロセス

組織のリスク管理とコンプライアンス強化のために、どのような手順が行われるかを示す一連の流れです。
情報リスクの可視化から始まり、監査による操作履歴の追跡、不正や誤操作の早期検知、さらに eDiscovery による証拠データの保全・法的対応までのプロセスを示しています。この一連の流れによって、組織内での情報リスクを最小化し、コンプライアンスを確実に強化できます。



5.2. 機能①監査

監査機能は、Microsoft 365 環境内でのユーザーおよび管理者のアクティビティを詳細に記録する機能です。
本機能を利用することで、以下のような各種アクティビティログを収集することが可能です。

主な特徴

■操作履歴の記録
ユーザーや管理者の操作内容を自動で記録
例：ファイルの作成・編集・削除、メール送信、権限変更など
※Purviewポータル内の操作も一部記録可能（データマップやカタログのスキャン実行、ラベルポリシーの作成・変更など）

■検索・フィルタリング
・日付、ユーザー、対象データ種類などで操作履歴を簡単に検索
必要な証跡を素早く確認可能
例：特定ユーザーの過去30日間のOneDrive操作ログを抽出、Exchangeメール削除履歴を検索

■不正・誤操作の検知
・許可されていない操作やポリシー違反の操作を特定
→早期対応によりリスクを最小化
例：外部共有が禁止されたファイルを共有した操作を検知、機密ラベル付きのファイルダウンロード履歴を確認

■監査レポート作成
・操作履歴やイベントの集計・レポート作成
・内部監査やコンプライアンス報告に活用可能
例：特定期間のSharePointサイトへのアクセス数や削除操作数を自動集計して報告書に出力

5.2. 機能①監査

監査機能には **Standard（標準）** と **Premium（プレミアム）** の 2 つのエディションがあり、いずれも基本的なアクティビティ監査を提供しますが、Premium では保持期間の延長や高価値イベントの記録、フォレンジック調査向けの高度な分析が可能になります。
特に、セキュリティインシデント対応や長期的な証跡管理を求める環境では、Premium エディションの利用が推奨されます。

項目	Standard（標準）	Premium（プレミアム）
概要	多くのユーザー／管理者アクティビティの監査ログを検索可能。標準的なコンプライアンス／調査用途に対応。	Standardの機能を含みつつ、長期保持、カスタム保持ポリシー、高価値インサイト、API帯域強化などが追加。
ログ保持期間（デフォルト）	180日	主なサービス（例：Exchange, SharePoint, Entra ID）については 1年（さらに別ライセンスで最大10年まで）
カスタム監査ログポリシー	標準では “ポリシーによるカスタム保持” の柔軟性は限定的またはなし	サービス・ユーザー・活動別に「監査ログをどれだけ保持するか」をカスタマイズ可能。
API/アクセス帯域	監査ログ抽出・検索API利用可（標準帯域・性能は標準）	より高い帯域・パフォーマンスでAPI利用可能。大規模組織でのログ取得／分析に優位
レポート作成	・操作履歴の集計・CSV出力 ・内部監査向け集計（小～中規模組織向け） ・Exchange/SharePoint/OneDrive/Teamsの操作対象	・大量ログ対応の集計・カスタムレポート ・高性能ダッシュボード表示 ・長期保持ログやAPI経由での自動取得

選定ポイント

・**標準（Standard）**は、通常の操作履歴の確認や短期的な監査目的に適しています。
・**プレミアム（Premium）** は、セキュリティインシデント調査 や 長期的な証跡保持 が必要な組織に最適です。

5.3. 機能②電子情報開示（eDiscovery）

電子情報開示（eDiscovery） は、訴訟、社内調査、コンプライアンス対応などの際に、関連する電子データを効率的に検索・保全・分析・エクスポートするための機能です。
Exchange、Teams、SharePoint、OneDrive などの Microsoft 365 データを対象に、証拠保全から提出までのプロセスを一貫して実施できる点が特徴です。これにより、法的リスクの低減や、内部統制・コンプライアンス体制の強化を支援します。

主な特徴

■対象データの広範な検索・保管
・Exchange メール、Teams チャット、SharePoint、OneDrive、Office ドキュメントなど、組織内の多様なデータを検索対象とする。
・必要に応じて、データを保持（ホールド）し、削除や改ざんを防止

■条件・キーワードによる高度な検索
・キーワード、送信者/受信者、日付範囲、特定のラベルや機密情報タイプなどで絞り込み可能
・法務・監査の目的に応じた柔軟な検索が可能

■証拠保全
・調査対象のメールやファイルを保持し、ユーザー操作や自動削除から保護
・訴訟・監査・内部調査に必要なデータの完全性を確保

■監査レポート作成
・検索・ホールドしたデータを安全にエクスポート
・法務担当者によるレビューやマークアップ、分析を支援

5.3. 機能②電子情報開示（eDiscovery）

電子情報開示機能には**Standard（標準）** と **Premium（プレミアム）** の ２つのエディションがあります。機能に違いがあります。
Premium ではより高度な調査・分析・エクスポートまでを一貫して実施できます。

項目	Standard（標準）	Premium（プレミアム）
主な目的	基本的なコンテンツ検索・保持	高度な調査・分析・レビュー・エクスポート
主な利用シナリオ	法的ホールド、訴訟初期対応、監査目的の検索	訴訟・内部調査の詳細分析、レビュー、法的提出
データソース	Exchange Online、SharePoint、OneDrive、Teams	Standard対象＋監査ログ・メールの添付ファイル・Teamsの会話データなど拡張
検索機能	キーワード検索、条件検索	高度なクエリ、近接検索、AIベースの関連性分析
保持（ホールド）機能	ケース（調査）単位でコンテンツ保持が可能 （調査・対応期間中の一時保持）	関係者単位での保持、ケース管理機能あり、長期保持・大規模管理対応
分析・レビュー機能	なし（検索まで）	組み込みのレビュー・タグ付け・重複排除・分析ビュー
エクスポート機能	検索結果のダウンロード	レビュー済みデータを法的形式でエクスポート

選定ポイント

・**Standard（標準）**は、基本的な検索や保持を行いたい場合に適しています。
→監査対応や必要なメール・ファイルをケース単位で一時的に保持可能。（監査対応や、必要なメール・ファイルを調査・対応期間中、確実に保持する用途に最適です。（ケースがクローズされるまでデータは保持されます。）
・**Premium（プレミアム）** は、詳細な調査や法的対応が必要な場合に適しています。
→訴訟・内部不正調査などで、データの分析・レビュー・提出まで一貫して行いたい場合に最適です。

5.3. 機能②電子情報開示（eDiscovery）

監査と電子情報開示(eDiscovery)は、どちらもMicrosoft 365 のセキュリティとコンプライアンスを支える重要な機能ですが、目的と使用方法には明確な違いがあります。

項目	監査	電子情報顔開示（eDiscovery）
目的	日常的なアクティビティの追跡とセキュリティ強化、内部統制の証跡提示。	法的調査やコンプライアンス調査のための証拠の収集、保全、分析。（訴訟対応、規制当局への報告など）
主な用途	・不正アクセスの検出・原因調査 ・ユーザーや管理者による不審な操作の監視（例：大量のファイルダウンロード） ・内部／外部監査時の操作履歴の証跡提示	・訴訟対応に必要なメール、チャット、ファイル等のデータの収集と保持（ホールド） ・内部調査における、特定の事象や人物に関連する情報の抽出とレビュー
データの種類	ユーザーや管理者による操作ログ（アクティビティ）	Microsoft 365内のコンテンツデータ（メール、ファイル、Teamsチャットなど）とその関連情報
主要機能	・リアルタイムに近いアクティビティ追跡 ・アラート設定（不審な操作の自動検知） ・詳細なログのエクスポート	・ケース管理（調査案件ごとのデータ一元管理） ・データの検索、収集、保持（ホールド） ・高度なフィルタリングと分析（会話のスレッド化、プレディクティブコーディングなど）

Point

多くの場合、監査の操作履歴の調査から、電子情報顔開示（eDiscovery）を使った本格的な調査に移行します。
例：「監査ログで不審なファイルアクセスを確認」→「eDiscoveryでそのファイルと関連するメール/チャットを収集し、ホールドして法的にレビューする」
このシームレスな連携こそが、Microsoft Purviewの統合ソリューションとしての強みであると言えます。

5.4. まとめ

リスクとコンプライアンスのポイントと、できないことをまとめています。

ポイント

◆監査（Audit）で操作履歴を可視化
・ユーザーや管理者の操作ログを自動記録
・不正操作やポリシー違反を早期に把握可能
◆法務・内部統制のサポート
・訴訟や監査対応に必要なデータを確実に収集・保全
・内部統制の証跡を自動化し、管理者負荷を軽減

◆電子情報開示（eDiscovery）で証拠保全・調査を効率化
・メール・Teams・SharePoint・OneDriveなど、組織内データを横断検索
・調査対象データの保持（Legal Hold）、レビュー、エクスポートまで一貫対応

できないこと/注意点

◆ 監査
・オンプレミス環境やクラウド外のすべての操作ログは自動収集できない
→ ローカルPC操作やUSB書き出し、印刷などは補完設定・エージェントが必要
・すべてのユーザー操作をリアルタイムで追跡するわけではない
→ オフライン作業や非対応アプリ（古いOffice、サードパーティサービスなど）の操作は即時追跡不可
・持ち出し防止（ブロック）はできない
→ DLPのように操作自体を制御する機能ではなく、あくまで操作の記録・証跡を残す機能

◆電子情報開示（eDiscovery）
・すべての端末・クラウドサービスを網羅して自動収集できるわけではない
→ 対応サービスのみ自動検索、非対応データは手動収集が必要
・法的手続きや裁判所命令などに必要な正式な証跡の全機能は、管理者が適切に操作・設定する必要あり
・大量データの高度な分析やAIによる自動判断は限定的

6.ユースケース

6.1. ユースケース①退職予定者による機密情報持ち出し防止

◆課題
・退職予定者・異動者による機密情報の持ち出しは大きなリスク
・複数クラウド・社内システムにデータが分散しており、手作業での監査は時間がかかる

◆Purviewの機能
監査：ユーザーや管理者の操作履歴を自動で記録・追跡。ファイルアクセスや編集、削除、メール送信などの操作を網羅的に把握。
DLP：機密情報の外部送信やコピー、持ち出しを制御し、ポリシー違反を検知。
情報保護：ファイルの暗号化やアクセス制御を適用し、不正利用を防止。

◆活用内容
・退職予定者や特定ユーザーの機密データアクセスを監視
・ポリシー違反を検知した場合、即座にアラートを発生
・監査ログを定期レポート化し、内部統制の証跡として保存

◆メリット
・内部情報漏洩リスクを未然に防止
・分散データを統合監視◎
・管理者の負荷軽減、内部統制証跡を自動化

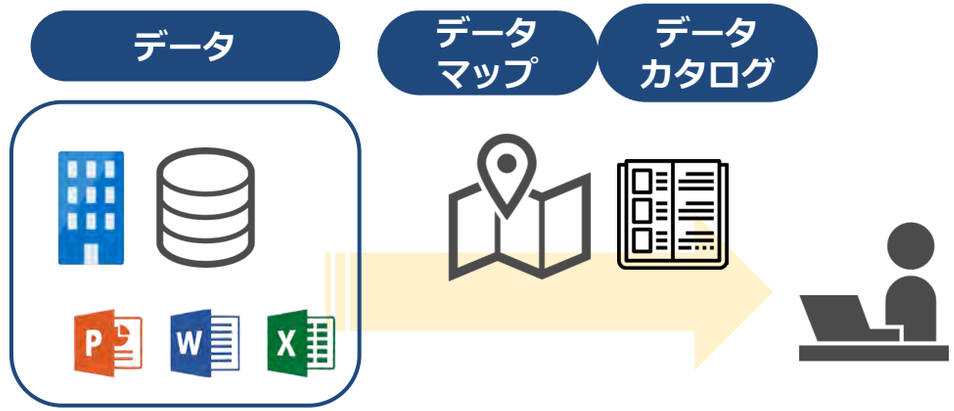
6.2. ユースケース②営業提案資料作成の効率化

◆課題
・提案資料作成時、顧客情報や売上データを複数システムから収集する必要がある
・更新漏れや取りこぼしが発生すると資料の正確性・信頼性に影響

◆Purviewの機能
データマップ：クラウド・オンプレミス・SaaSなど分散するデータ資産の所在や依存関係を一目で可視化。
データカタログ：データの種類や属性を整理・分類し、必要な情報を簡単に検索・取得可能。

◆活用内容
・整理されたデータを参照して自動収集・整理
・依存関係も可視化されるため漏れなく資料に反映
・データ検索・収集の手間を削減し営業活動に集中

◆メリット
・提案資料作成工数を大幅削減
・データ正確性・最新性を保証、提案内容の信頼性向上
・分散データの統合管理で情報探しの手間を削減



6.3. Copilot活用イメージ

Purview によって整理・分類された組織のデータやメタデータを、Copilot が活用することで、より効率的な情報活用・分析・意思決定支援 が可能になります。Purview が提供するデータガバナンスやセキュリティ情報を基に、Copilot が自然言語で質問に答えたり、レポート作成を支援します。

活用場面	機能	Purviewの役割	Copilotの役割	メリット
データ探索・検索	データマップ	データ所在や依存関係を可視化	自然言語で「最新売上データを出して」と指示可能	必要な情報を瞬時に把握
レポート作成＋分析	データカタログ/データマップ	データ分類やリネージュで正確なデータ特定	指定データから自動で表・グラフ作成	提案資料や社内レポート作成の工数削減
コンプライアンス確認	情報保護/DLP/監査	機密情報ラベルやポリシー適用・監査ログ管理	コンプライアンスに関わるデータの扱い方をガイドしたり、ルールに反しそうな操作を行う前に注意を促す支援	データ利用ミス防止
ナレッジ活用	データカタログ/メタデータ管理	データ所有者・更新履歴など整理	過去データや社内資料の要約・検索を支援	過去事例や顧客情報を簡単参照可能

データ管理

Purview

自然言語活用

Copilot

レポート/分析/提案

出力

まとめ

・Purview が「信頼できるデータ基盤」を提供
・Copilot が「自然言語での活用・分析・レポート作成」を支援
・両者を組み合わせることで、迅速かつ安全に意思決定が可能

7.ライセンス

7.1. ライセンスと課金形態の概要

Microsoft Purview の利用には、機能や対象データソースに応じて異なる課金モデルが用意されています。
ここでは、Microsoft 365 ライセンスに含まれる「ユーザーごとのライセンスモデル」と、利用量に応じて課金される「従量課金制モデル」の2種類について説明します。なお、両モデルは併用可能です。

ユーザーごとのライセンスモデル

■Purviewの適用対象
- Microsoft 365ユーザー
- Windows/macOS デバイス

■ライセンス種別
- Microsoft 365 E3/E5/A5/F5/G5 などの既存の Microsoft 365ライセンスに含まれる。

■主な機能
- 情報保護
- DLP
- 監査
- インサイダーリスク管理
- eDiscovery

★Microsoft 365環境内のユーザー・デバイスに対する保護が中心。

従量課金制モデル

■Purviewの適用対象
- Microsoft 365以外のデータソース
  （例：AWS、Azure SQL、Box、Google Driveなど）
- AIアプリケーション

■課金方法
- Azureベースの消費単位に応じて課金（vCore時間、GB/日など）

■利用条件
- Microsoft 365テナントにAzureサブスクリプションの関連付けが必要。

■主な機能
- データカタログ
- データマップ
- 情報保護（Microsoft 365以外のデータ）
- インサイダーリスク管理（Microsoft 365以外のデータ）
- eDiscovery（Microsoft 365 以外の AI アプリケーション データ）

★Microsoft 365外のクラウドやオンプレミス環境に対する保護が中心。

7.2. 機能別ライセンス対応表

Microsoft Purviewの機能は、Microsoft 365のライセンスによって利用範囲が異なります。Business Basic / Standardではほとんどの Purview機能が利用できず、情報保護やDLPなどの高度な機能は提供されません。そのため、Purviewを本格的に活用するには、Business Premium以上のライセンスが推奨されます。以下の表は、各ライセンスプランにおけるPurview機能の対応状況を整理したものです。

機能カテゴリ	機能名	Business Basic/Standard	Business Premium	Microsoft 365 E3	Microsoft 365 E5	補足
情報保護	秘密度ラベルの手動設定	×	○	○	○	
	秘密度ラベルの自動設定	×	×	×	○	
	基本的なメッセージの暗号化	×	○	○	○	
	高度なメッセージの暗号化	×	×	×	○	
DLP	Exchange Online	×	○	○	○	
	SharePoint Online / OneDrive	×	○	○	○	
	Microsoft Teams	×	×	×	○	E3/E5には Teams を含むプランと含まないプランがあり、Teams を含まない場合はアドオンの購入が必要
	エンドポイント（Windows/macOS）	×	×	×	○	
	Microsoft 365 Copilot	×	×	×	○	Copilotの利用には、別途ライセンスが必要

7.2. 機能別ライセンス対応表

機能カテゴリ	機能名	Business Basic/Standard	Business Premium	Microsoft 365 E3	Microsoft 365 E5	補足
インサイダーリスク管理	ー	×	×	×	○	
データマップ	ー	×	×	×	×	**従量課金制モデル**
データカタログ	ー	×	×	×	×	**従量課金制モデル**
監査	標準	○	○	○	○	
	プレミアム	×	×	×	○	
eDiscovery	標準	×	○	○	○	
	プレミアム	×	×	×	○	

補足

Purviewの一部機能は Microsoft 365 E5 のみに含まれますが、必要な機能のみを以下のアドオンで個別に導入することも可能です。

- Information Protection and Governance：情報保護・データ保持
- Insider Risk Management：内部リスクの検知と対応
- eDiscovery and Audit：電子情報開示と監査ログ管理

7.3. アドオン機能

Microsoft 365 E3 や Business Premium では基本的な情報保護やコンプライアンス機能を提供していますが、より高度な機能を必要とする場合には、**Microsoft Purview Suite アドオンを追加**することで、複数の機能をまとめて導入し、E5と同等の機能を利用できます。

Purview Suiteには、対象ライセンスに応じて以下2種類のアドオンと機能が提供されています。

■**Microsoft Purview Suite for Business Premium**
中小企業向けのBusiness Premiumライセンスに対応したアドオンで、最大300ユーザーまでの環境に適しています。

■**Microsoft Purview Suite**
Enterprise向けのE3ライセンスに対応したアドオンで、ユーザー数制限なく、より大規模な環境での導入に適しています。

主な機能には、DLP（Teams・エンドポイントなど）、高度な暗号化、インサイダーリスク管理、eDiscovery（プレミアム）、監査（プレミアム）などが両ライセンスに含まれており、E5と同等のPurview機能を利用できるようになります。

アドオン追加のメリット

✓ E5ライセンスを導入せずに、必要な情報保護・コンプライアンス機能をまとめて追加できる
コストを抑えながら、E5相当の機能を利用可能

✓ 複数の機能を一括で導入できるため、管理がシンプルで運用負荷を軽減できる
個別アドオンの選定・設定が不要