Microsoft Security

AI 時代に最適なデータセキュリティとガバナンス、
コンプライアンスを提供する堅牢なプラットフォーム

# Microsoft Purview

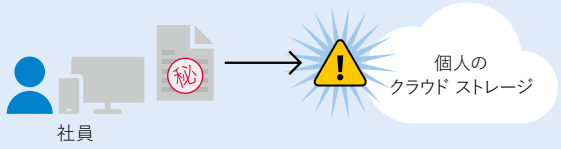
# 従来の業務データに加えて、生成 AI の活用によって組織の情報漏えいリスクが多様化しています

### 従来の業務データにおける情報漏えいリスク

働き方の選択肢が増えるにともない、転職や副業といったキャリアの多様性が一般的となる中、退職者による営業秘密の持ち出しリスクが高まっています。また、ハイブリッドワークの普及やコラボレーションツールの進化により、社内外とのコミュニケーション経路が多様化し、従来とは異なる経路からの情報漏えいリスクも顕在化しています。これまでの性善説に基づく対応から、時代に合わせた柔軟なデータ セキュリティ対策への対応が求められています。

**退職予定者による情報持ち出し**

転職先で有利になるよう取引先情報や営業秘密を入手し
個人のクラウドへアップロード

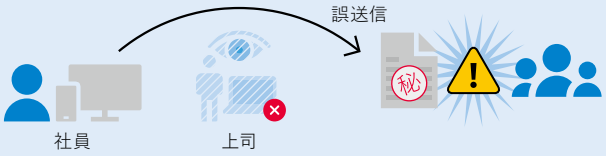



**ヒューマン エラー**

自社のクラウド ストレージにおいて機密情報が
誰でも閲覧できる状態になっていた

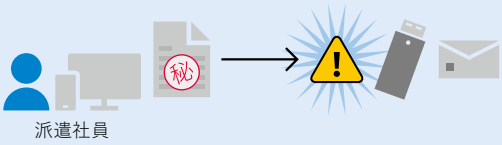

**既存漏えい対策の形骸化**

上司承認後の送信のはずが、チェックなく素通り
(中身をチェックせず、承認してしまっている。)




**悪意ある情報持ち出し**

会社への待遇不満があり、顧客名簿を
不正に持ち出し業者に転売




### 生成 AI の活用に伴う情報漏えい、コンプライアンス違反、過剰露出のリスク

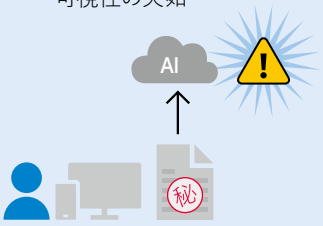
現在、Microsoft 365 Copilot などの生成 AI を業務に活用し、創造的かつ効率的に業務を変革していくことが期待されています。しかし、同時に情報漏えい、コンプライアンス違反、データの過剰露出などへの対処が求められており、生成 AI を安全に活用するためのデータ基盤の準備が急務となっています。

**使い慣れたツールへの組み込みによる**
**高いユーザビリティ備えた生成 AI**


**生成 AI の利用における新たな懸念事項と想定されるリスク**

**業務効率が向上する一方で…**

- ☑ AI に共有されるデータを保護するためのコントロールの欠如
- ☑ 増加する規制のプレッシャー
- ☑ 漏えいリスクを検出する可視性の欠如



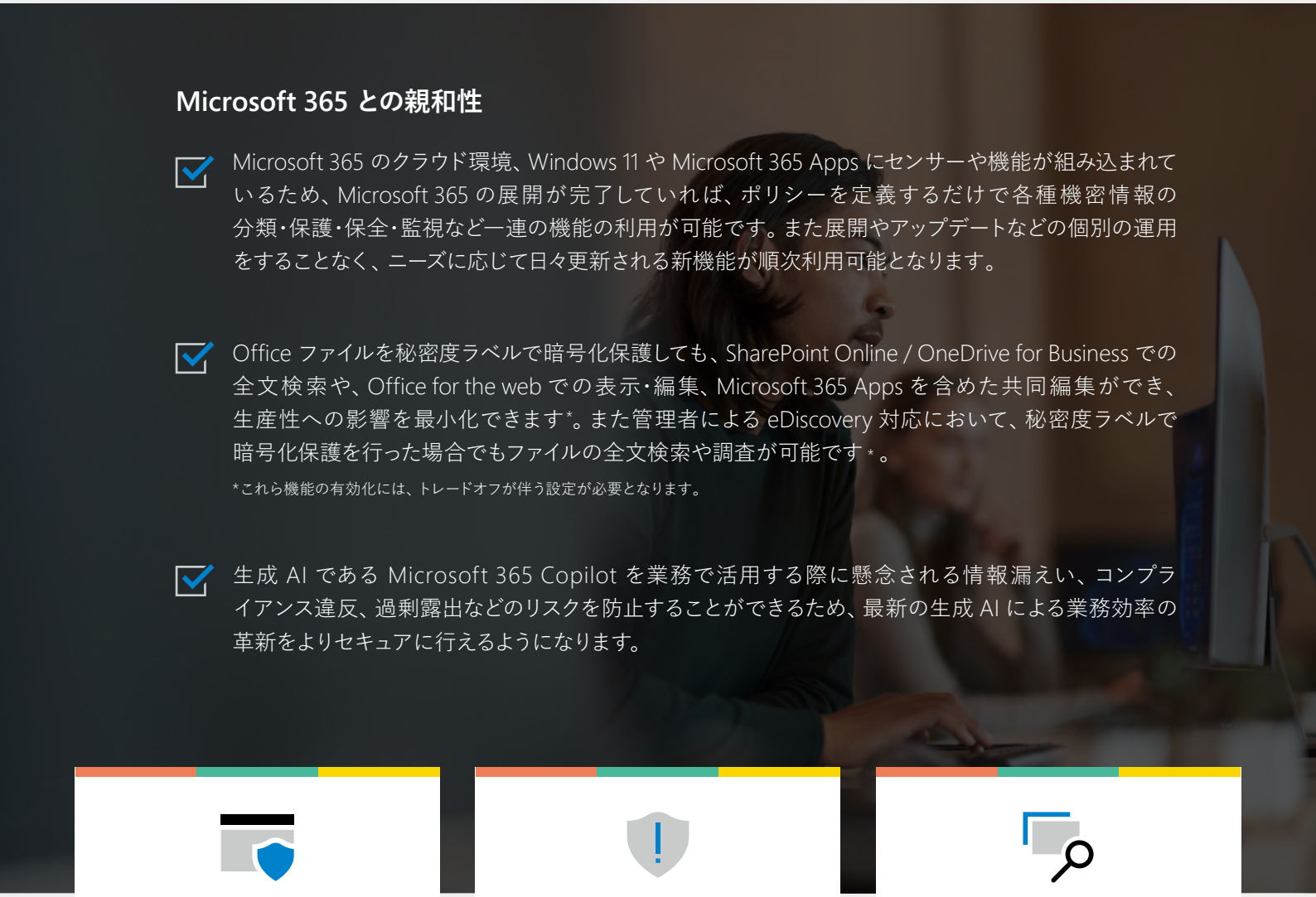

**情報漏えい**
誤って機密データを AI アプリに漏えいする可能性がある

**コンプライアンス違反**
AI アプリを使用して非倫理的またはその他のリスクの高いコンテンツを生成する可能性がある

**データの過剰露出**
表示または編集が許可されていない機密データに AI アプリでアクセスする可能性がある

# Microsoft Purview で実現する AI 時代の包括的なデータ セキュリティ

いかに早く社内の不正や情報漏えいに気付き対処できるか。ただログを収集するだけではなく、保護すべき情報を分類し、ログからリスクが高いユーザーや 生成 AI 利用時のプロンプトなどを特定して詳細に調査することで、社内の情報資産を効率的に保護できます。



## Microsoft 365 との親和性

- Microsoft 365 のクラウド環境、Windows 11 や Microsoft 365 Apps にセンサーや機能が組み込まれているため、Microsoft 365 の展開が完了していれば、ポリシーを定義するだけで各種機密情報の分類・保護・保全・監視など一連の機能の利用が可能です。また展開やアップデートなどの個別の運用をすることなく、ニーズに応じて日々更新される新機能が順次利用可能となります。

- Office ファイルを秘密度ラベルで暗号化保護しても、SharePoint Online / OneDrive for Business での全文検索や、Office for the web での表示・編集、Microsoft 365 Apps を含めた共同編集ができ、生産性への影響を最小化できます*。また管理者による eDiscovery 対応において、秘密度ラベルで暗号化保護を行った場合でもファイルの全文検索や調査が可能です*。

  *これら機能の有効化には、トレードオフが伴う設定が必要となります。

- 生成 AI である Microsoft 365 Copilot を業務で活用する際に懸念される情報漏えい、コンプライアンス違反、過剰露出などのリスクを防止することができるため、最新の生成 AI による業務効率の革新をよりセキュアに行えるようになります。

### Information Protection & Governance

機密情報保護への意識付け

- 自動もしくは手動で個人情報・機密情報の識別
- ユーザーに見える形で情報のラベル付け、保護、取り扱いに関する警告
- 分類に応じた情報のライフサイクル管理

### Insider Risk Management

悪質なケースで個別調査

- ユーザー操作を定量的に監視し、機密情報・個人情報の取り扱いに関するリスク識別
- 社内外での不適切なコミュニケーションを検出
- 利益相反するユーザー間のコミュニケーションを制限

### eDiscovery & Audit

訴訟に備え否認防止・証拠保存

- 効率的なコンテンツ検索と、機械学習ベースの検索結果の絞り込みおよび抽出
- 長期のログ保存と、インシデント時に重要となる追加ログの記録

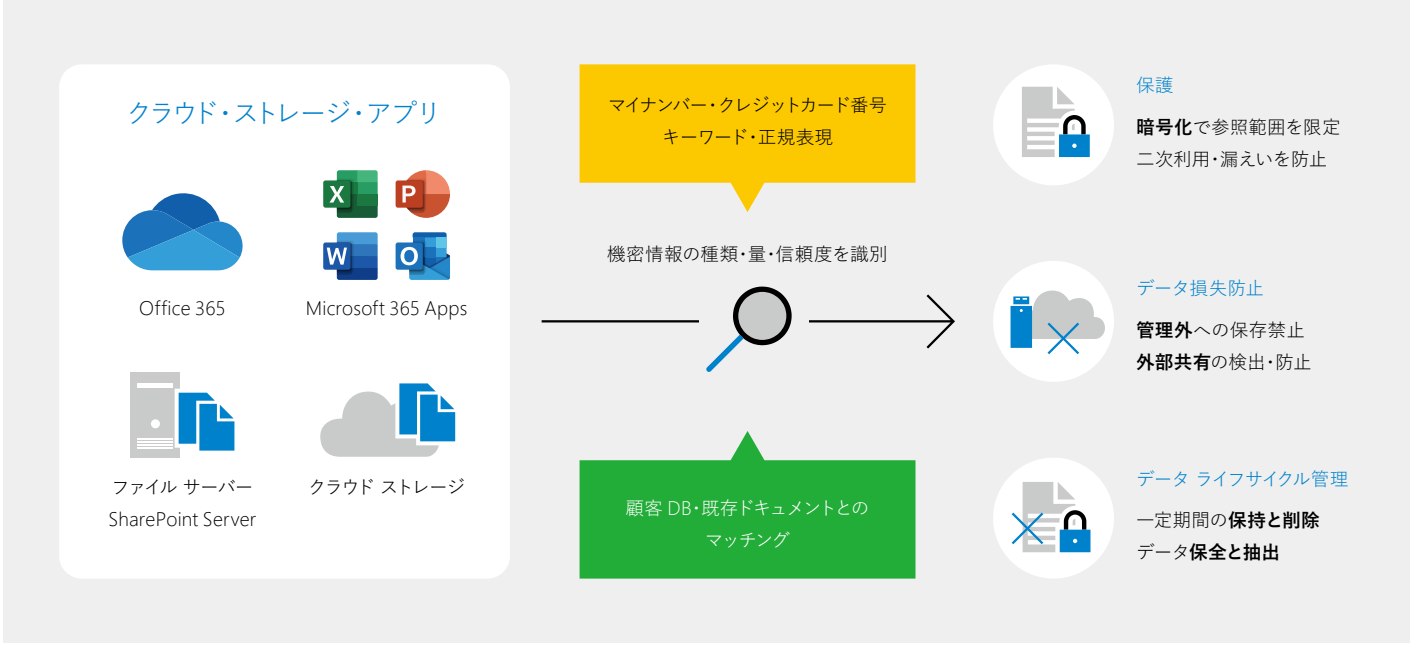
# 機密情報を識別してデータを保護・統制

Information Protection & Governance では、マイナンバーやクレジット カード番号などの事前定義済みの機密情報、別途定義したキーワードや正規表現のパターン、氏名や住所などの固有名詞、データベースから取り込まれた顧客情報、画像 (スクリーンショット等) に含まれるテキスト情報などを通じて、クラウド ストレージ、ファイル サーバー、端末上で動作する Microsoft 365 Apps などで機密情報や個人情報を識別します。

識別された情報に応じて、秘密度ラベルにより、機微な情報であることを明示しながらファイルを暗号化し、社内ユーザーしか開けないようなアクセス コントロールや、印刷、コピー & ペーストなどの二次利用への制限を適用することができます。

管理外のクラウド ストレージや、USB ディスクなどへのファイル書き込みを防止したり、そのような操作の際警告を出すことで、ユーザー自身へも自覚を促しながら機密情報の保護を一段高められます。印刷や USB ディスクへの保存を許可する場合でも、持ち出されたファイル“そのもの”のコピーを自動で保全できるため、後から内容まで確認できます。

また、不要となった機密情報や個人情報が残存しないように、クラウドに保存されたデータを一定期間保護したうえで期間経過後は削除することも可能です。

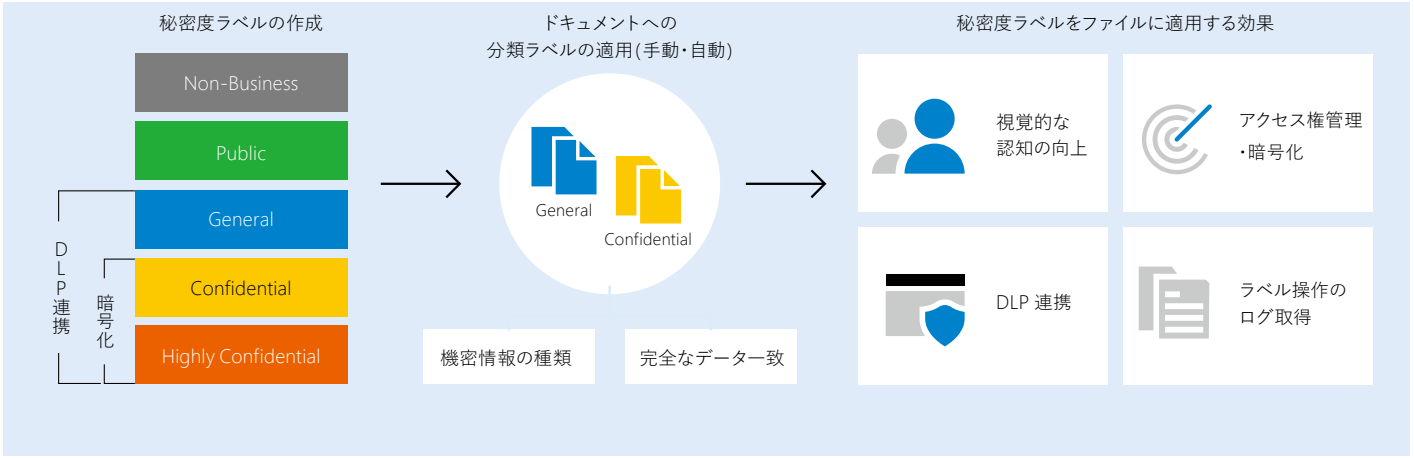



- Office ファイルや PDF ファイルの中身を分析して、識別された機密情報・個人情報に応じたファイルの保護や二次利用制限が可能
- 中身が直接確認できないファイル種別であっても、ファイルの拡張子に応じたポリシーを作成することで、管理外へのデータの共有やアップロードを監視・制御可能
- SharePoint Online のサイトや Microsoft 365 グループなどのデータの格納場所にも秘密度ラベルを設定することができ、ラベルに応じてゲスト招待の可否や多要素認証を必須としたり、管理された端末からのアクセスが必要などの条件設定が可能
- 保存場所に設定された秘密度ラベルより高い秘密度のラベルが設定されたファイルがアップロードされた際、サイト管理者とファイル投稿者にメールでアラートを送信することが可能
- SharePoint Online のライブラリにデフォルトの秘密度ラベルを設定し、ラベルが設定されていない Office ファイル等がアップロードされた際、自動で秘密度ラベルを適用することが可能

# 機密情報の分類と保護

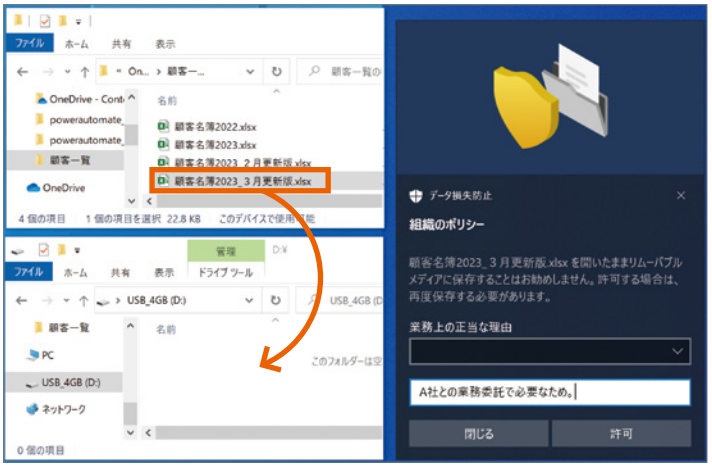
## 自動・手動で付与できる秘密度ラベル


- 「営業秘密の秘密管理性」要件を満たす運用の実現
- 秘密度ラベルによって、社外のユーザーは開けないなどファイルの適切な保護レベルを簡単に選択可能
- ファイルを受け取ったユーザーも視覚的にファイルの秘密度を認識可能
- 秘密度ラベルやファイルに含まれる機密情報・個人情報に応じて、管理外のクラウドへのアップロードや、USB ディスクへの書き込みを防止もしくは警告可能
- 秘密度ラベルの付与・変更、保護されたファイルのアクセスなどの操作は、クラウド側でログ記録される



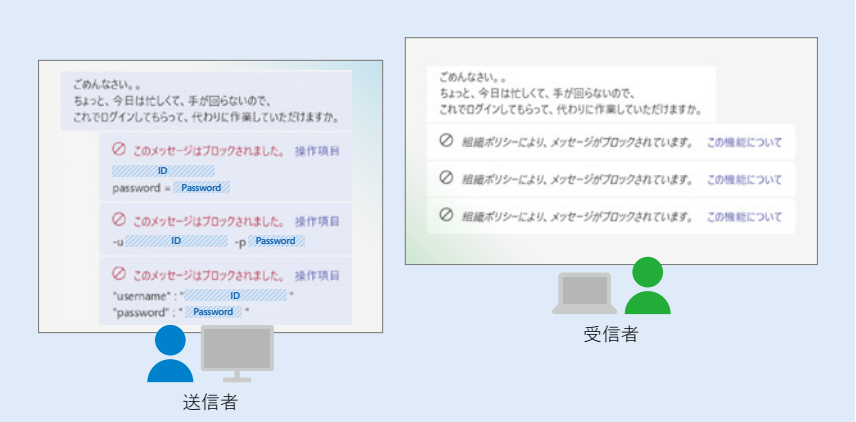

# データ損失防止

## 機密情報の外部への流出を防止




### デバイスからの情報漏えいを防止

- デバイス上での機密情報の流出につながる行為を監視及び制御 (クリップボードへのコピー、USB へのコピー、印刷など)
- ブラウザーを経由したクラウド サービスへの機密情報のアップロードを検知し、未然に流出を防止
- 一律での流出防止ポリシーではユーザーの生産性に影響があるため、理由を書かせることにより、外部共有を許可するような柔軟な設定も可能 (生産性向上とユーザーへの機密情報取り扱い教育を両立)




### Teams からの情報漏えいを防止

- Teams を経由した外部とのコミュニケーションにおいて機密情報ファイルの流出を防止
- やり取りされるメッセージについても機密情報に該当するものについては、相手側では見えなくなる動作
- 事前定義された分類子を活用することで、社内に散在する資格情報 (パスワード、API Key など) の流出を検知および防止

| 適用範囲 | ソリューション | 役割 |
|---|---|---|
| メール | Exchange Online DLP | メールによる外部への機密情報送信の保護 |
| ファイル共有 | SharePoint Online<br>OneDrive for Business DLP | 外部に共有された機密ファイルの保護 |
| デバイス上の操作 | Endpoint DLP | 端末上での不正な操作の検出と制御 |
| チャット・チャネル | Teams DLP | • チャット・チャネル内のメッセージの保護<br>• Teams に紐づく SharePoint サイトや OneDrive アカウント上で共有されるファイルの自動保護 |
| ファイル サーバー | オンプレミス DLP | ファイル サーバー上に保存される機密情報に対するアクセスの保護 |
| SaaS アプリ<br>(Box, Salesforce など) | Microsoft Defender for Cloud Apps | 機密情報を含むファイルの検知と保護 |

# データのライフサイクル管理

## ドキュメント要件に応じた保持、削除の実現

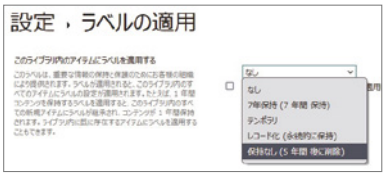
- SharePoint Online のサイト、Exchange Online のメールボックス、Microsoft 365 グループに対して、部署情報などのプロパティを条件として、ポリシー範囲を定義
- 特定のポリシー範囲に対して、コンテンツをどれくらいの期間保持し、いつ削除するか定めたアイテム保持ポリシーを展開可能
- 特定のポリシー範囲に対して、保持ラベルの自動適用や、利用可能な保持ラベルを設定することができ、コンテンツ単位にユーザーが保持ラベルを上書きして異なる保持期間を指定することも可能
- Microsoft Entra ID (旧 Azure Active Directory) で設定された管理単位を用いて、管理単位内のユーザーやチームに保持ポリシー・保持ラベルを展開することも可能
- クラウド添付ファイルの保持 (Teams で共有された時点のファイルの保持)

### データ ライフサイクル管理

一定期間の**保持と削除**

#### 情報ガバナンス

必要なものだけを保持し、デジタル資産全体で不要なものを削除することで、リスクと責任範囲を低減



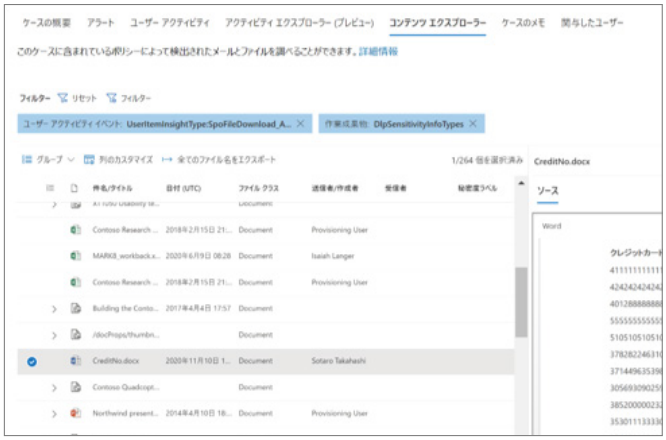

#### レコード管理

法律、ビジネス、または規制で求められる記録保持義務を満たすために定められた期間、変更や削除からコンテンツを保護

# ファイル操作・コミュニケーションの監視でリスクを早期に察知

## ユーザーを軸にクラウドおよび端末上でのファイル操作を監視

内部リスクの管理では、特定の閾値を超えた機密情報の疑わしい操作を行ったユーザー、退職予定のユーザー、別途指定したユーザーなどを対象に、一連の操作の中からリスクを判定し、ユーザー操作の妥当性をレビューできます。データ損失防止のポリシーでは、ある一つの操作を止めるか・止めないかといった制御のみですが、内部リスクの管理では、機密情報のダウンロードから端末上での流出行為に及ぶ一連の操作の流れや普段との活動量の違い、ファイルの中身なども加味しながら、機密情報の持ち出しを中心としたユーザーのリスクを判定できます。

### 退職予定者等の情報持ち出し行動の検出

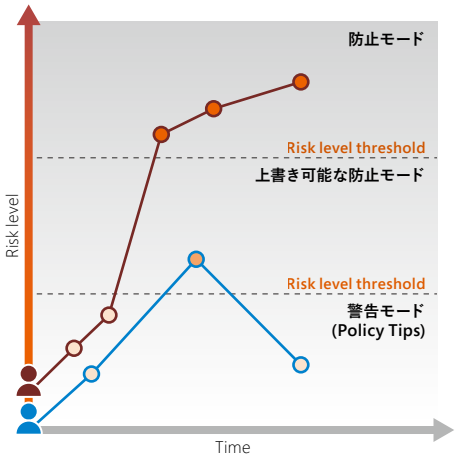
- 退職間際のユーザーや、指定したユーザー、アカウントが削除されたユーザーなどの条件に合致したユーザーの一連の挙動を分析
- 分析対象となったユーザーの疑わしいファイル操作を分析し、閾値に応じてアラートを生成
- アラートが発生した際には、必要に応じて匿名の状態のままでレビューが可能
- アクティビティ エクスプローラーを通じて、ファイルの中の機密情報の検知有無と共に、Office 365 からのファイル ダウンロード、端末からのファイルのアップロードや印刷、USB ディスクへの書き込みなどのファイル操作を分析可能

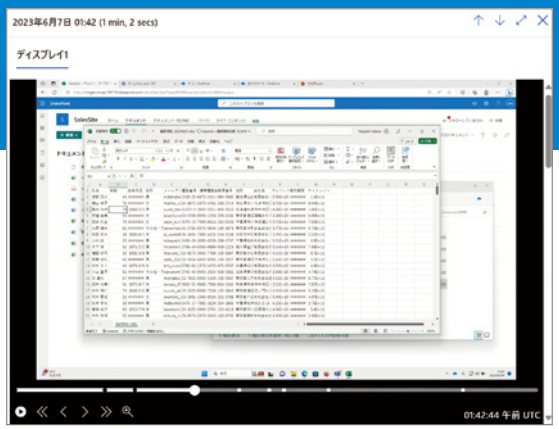
### ケース化して詳細に調査

- アラートの中身に応じて、詳細な分析が必要となった場合、ケース化し、分析担当者をアサインすることで、複数の分析担当者間でのメモの共有や、Teams チャネル チャットでの会話が可能となる
- ケース化することで、Office 365 を起点としたファイルについては、コンテンツ エクスプローラーを通じて中身の参照も可能となる
- Power Automate を通じた通知やシステム連携などの自動化も実装可能

### 高リスクユーザーのみへの動的なポリシー適用

- 械械学習モデルによって定義および分析されたリスク レベルに基づいて、ユーザーに適切な DLP ポリシーを動的に適用
- 一律の DLP ポリシーを全ユーザーに適用するのではなく、リスクの高いユーザーにのみに DLP ポリシーが適用され、リスクの低いユーザーは生産性を維持
- ポリシー制御は常に調整されるため、ユーザーのリスク レベルが変更されると、新しいリスクレベルに合わせたポリシーが動的に適用






### 持ち出し行動を動画で記録

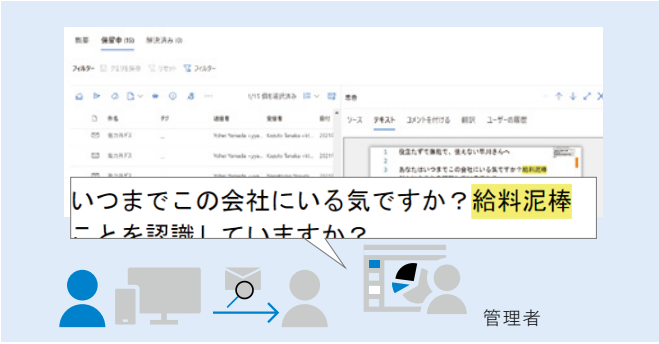
- リスクのあるアクティビティを行ったユーザーの実際の操作を動画として記録
- 動画による記録のため、セキュリティ チームにより深い分析情報を提供可能
- プライバシーに配慮し、動画取得には承認作業が必要
- 動画を格納する容量をアドオン ライセンスで別途購入が必要

# 業務で利用しているツールでのコミュニケーションの監視

社内外とのメールやチャットなどから、不正やハラスメントが疑われる会話を早期に検知し、大事に至る前に個別聞き取りなどを通じて是正を図ることができます。


### コミュニケーション リスクの検出

- キーワードの定義次第で、検査偽装、価格カルテル、汚職、不正会計、不適切営業、武器輸出など、さまざまな不正行為が疑われる会話を検知・分析可能
- 冒涜、ハラスメント、脅しの会話など機械学習ベースで検出できるカテゴリも順次追加
- OCR による画像読み取りにも対応
- 適切なコンプライアンス担当者により、検知したメールやチャットをレビューすることで、社内の不正の芽を早期に発見し、是正可能


### 利益相反するユーザー部門間のコミュニケーションを事後査閲

- 金融機関などにおいてインサイダー取引を防止するため、担当企業の内部情報を知る部門と取引や営業を行う部門など、利益相反する特定の部門間のメールやチャットを検出しレビューすることも可能

### 不正への勧誘やハラスメントを会話の中から検出

- 内部不正への勧誘・共謀に関わる会話を察知
- ハラスメント等職場に不適切な言動を監視可能

### データ コネクタを通じて 3rd Party アプリのデータを取り込み分析することも可能

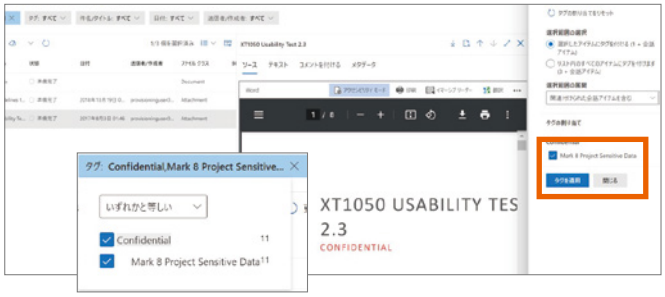
- マイクロソフトが提供するコネクタを通じて、Bloomberg、IceChat、Slack などを対象に、データを Exchange Online のメールボックスに取り込むことで、これらのアプリでのコミュニケーション内容を保持し、監視し、また電子情報開示機能で必要に応じ検索し、エクスポートすることが可能
- Veritas 社、TeleMessage 社、17a-4 LLC 社、CellTrust 社などが提供するコネクタを利用することで、Cisco Jabber、Cisco Webex Teams、Zoom、WeChat、WhatsApp、ServiceNow などのアプリにおいても、同様にデータを取り込むことで、コミュニケーション内容の保持、監視、電子情報開示対応が可能

# eDiscovery & Audit

訴訟に備え否認防止・証拠保存

## Office 365 およびデータ コネクタにより取り込まれたメール・チャット・ファイルなどのデータをスマートに抽出し、レビュー、エクスポート

社内不正が疑われる場合には、過去に遡って当事者のメールやチャット、ファイル共有などを対象とした社内調査が必要となります。電子情報開示 (Premium) では、通常のコンテンツ検索や電子情報開示ではできなかった、Teams にも対応した効率的なコンテンツの抽出とレビューができるよう拡張されています。



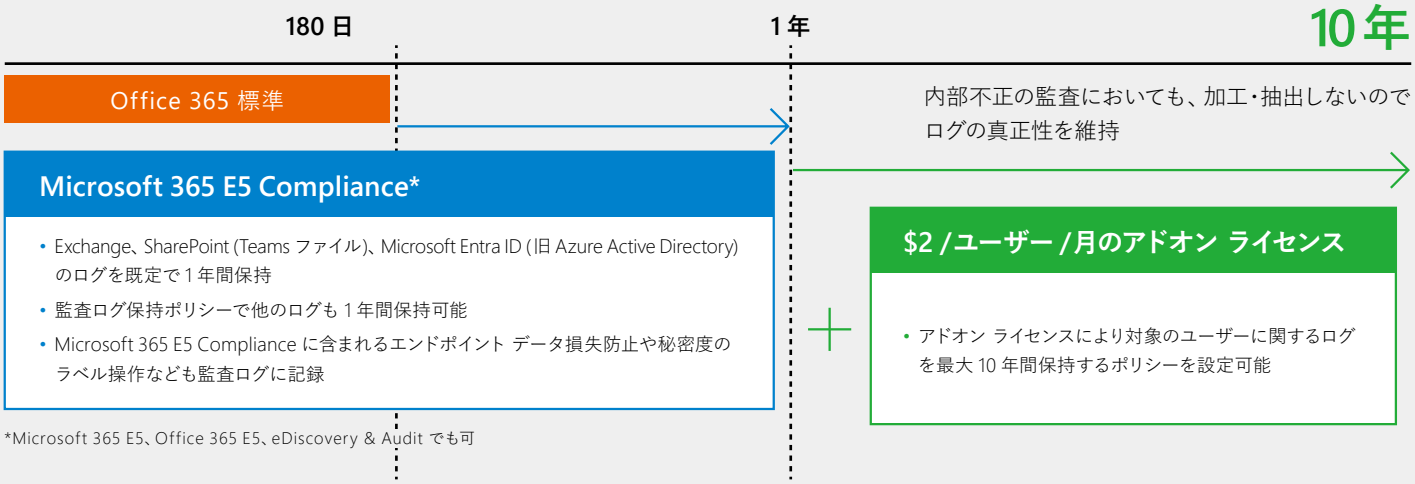

### Web UI から複数人でレビューし、情報の絞り込みが可能

- 検索キーワードや、当事者の指定などにより、該当するコンテンツを専用の Web UI を通じて、複数人でレビュー・タグ付けしながら精査可能
- 削除や改ざんからコンテンツを保護しながら、関連するものだけに絞り込んでエクスポートすることも可能


### 検索でヒットしたアイテムだけでなく、スレッド全体や、リンクされた添付ファイルもレビュー可能

- 検索でヒットしたアイテムだけではなく、Teams チャットのスレッド全体や、メールや Teams に添付されたファイルも対象に抽出・分析が可能

### Microsoft 365 E5 Compliance のライセンスでログ保管を 1 年間に延長可能




*Microsoft 365 E5、Office 365 E5、eDiscovery & Audit でも可

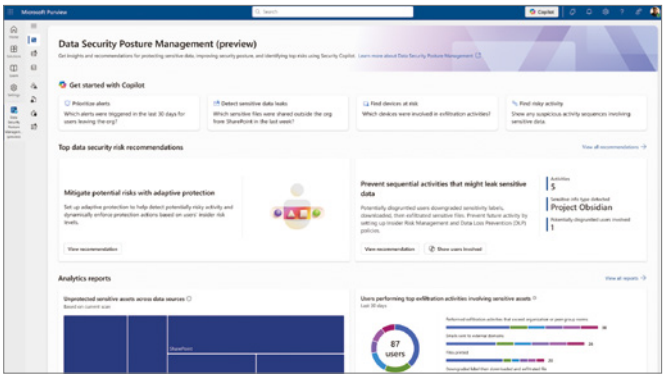
E5 Compliance にも含まれる監査 (Premium) では、エンドポイント データ損失防止で監視している端末上の機密情報の操作ログを含め Office 365 のログ保管期間を標準の 180 日から 1 年間に延長できます。さらにアドオンの追加により最大 10 年間のログ保管にも対応しています。

Public Preview 2025 年 6 月現在

# データ セキュリティ態勢管理の提供

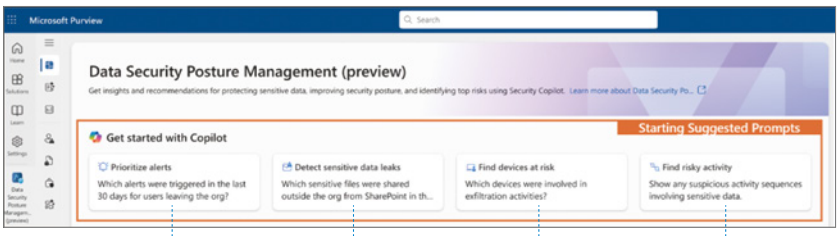
## Data Security Posture Management (DSPM)

Microsoft Purview は、データ資産全体における脆弱な構成を特定し、迅速な修正アクションを可能にするサービスである データ セキュリティ態勢管理を提供します。




- 総合的はセキュリティ態勢のリスクの是正
  ユーザベースやファイルベース、アクティビティベースでのセキュリティリスクを表示・改善を推奨、さらにポリシーのワンクリック設定に対応します。
- 保護されていないファイルの管理
  SharePoint や OneDrive にある保護されていないファイルをブラウズできます。
- AI アプリへのアクセス状況
  DSPM for AI と連携して、AI アプリの利用状況、機密情報の流出状況のサマリーを表示します。
- Security Copilot との統合
  生成 AI による自然言語での洞察を提供し、顧客がより深く掘り下げ、迅速に調査できるようにします。

## Microsoft Purview × Security Copilot




| 優先すべきアラート | 検出された機密データの漏洩 | リスクのあるデバイス | リスクの高いシーケンス アクティビティ |
|---|---|---|---|
| 過去 30 日間に退職予定のユーザーに関連してトリガーされたアラートはどれですか? | SharePoint から組織外へ共有された機密ファイルはどれですか? | データ流出の活動に関与したデバイスはどれですか? | 機密データに関連する疑わしい一連の活動を表示してください |

Microsoft Purview についてはこちら
https://aka.ms/mspurview-jp

**お問い合わせは弊社営業またはパートナーまで**

# 業務への AI 活用に不可欠となる
# 安全なデータ基盤を提供する Microsoft Purview

Microsoft Purview は、生成 AI の利用状況の把握、会社として許可していない生成 AI の利用制限、生成 AI との対話の把握、生成 AI からのデータ アクセス制御などを提供することで、生成 AI を業務で安心かつ安全に利用できる堅牢なデータ基盤の展開を支援します。

## 生成 AI 活用時のセキュリティ要件

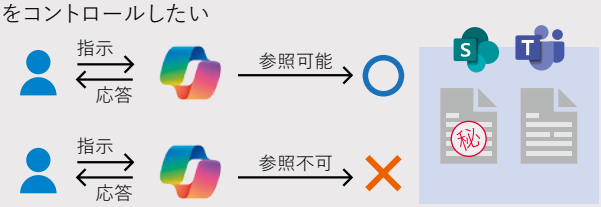
### AI ガバナンス

社内における生成 AI 利用の全体像を可視化して社内の方針に反映させたい


- 生成 AI の利用状況アクセスログ
- 機密情報の含まれる対話 AI 規制要件対応

### オーバーシェアリング

生成 AI を通じたデータの過剰露出や共有対策、社内データの利用をコントロールしたい

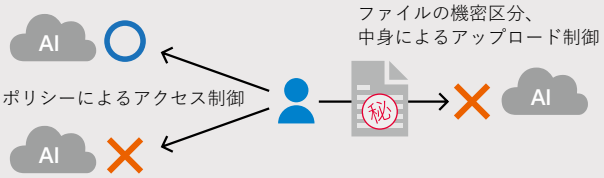



### コンプライアンス

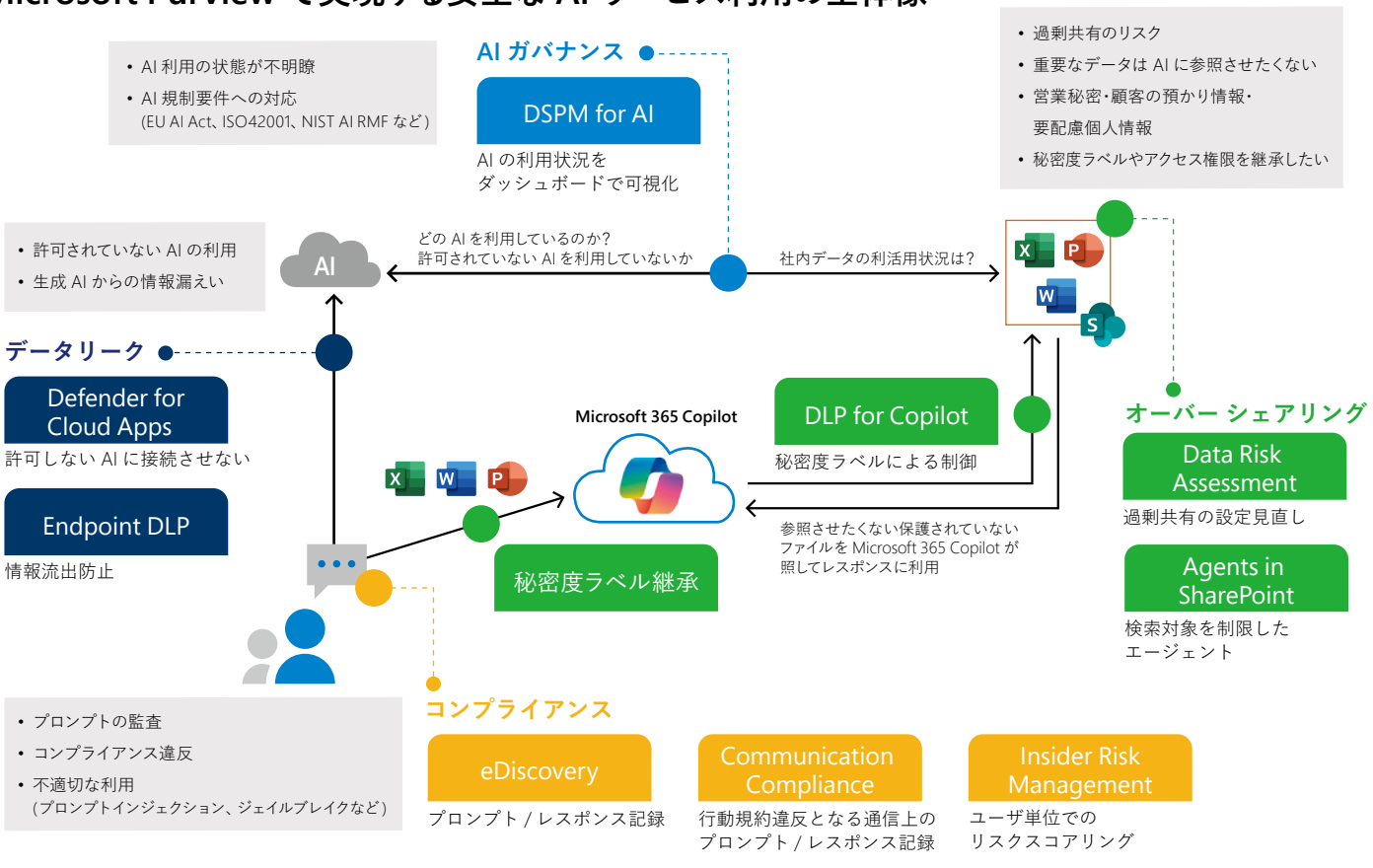
利用者と Microsoft 365 Copilot とのやり取りの中身
(指示や応答の内容、参照されたファイル) を調査・確認したい


### データリーク

リスクの高い生成 AI の利用禁止、機密性の高いファイルのアップロードを制限をしたい




## Microsoft Purview で実現する安全な AI サービス利用の全体像



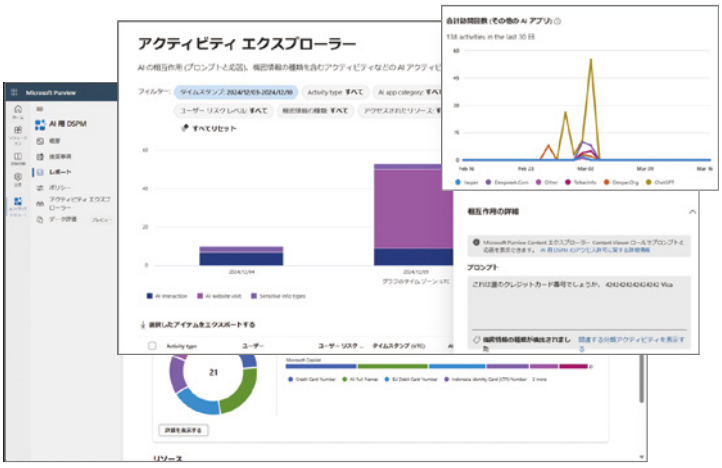
# AI ガバナンス

*Public Preview 2025 年 6 月現在

## 機密情報や脅威を可視化するダッシュボードを提供

### AI 用データ セキュリティ態勢管理

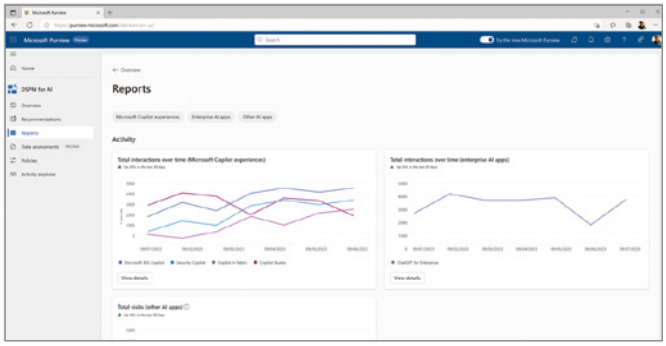
Data Security Posture Management (DSPM) for AI




- 生成 AI の利用状況、プロンプトに含まれる機密情報や脅威を可視化するダッシュボードを提供し、ポリシー作成などの迅速な是正対応を支援
- レポート機能により、プロンプト数、アクセス数、機密情報の種類や総数、コンプライアンス違反の可能性があるプロンプト数などを把握
- アクティビティ エクスプローラーにより、Copilot との対話内容 (プロンプト、レスポンス) の確認が可能
- AI に関連する DLP、IRM、コミュニケーション コンプライアンスなどのポリシー作成に対応し、迅速かつ効率的な是正対応をサポート

#### 各種 Copilot に Microsoft Purview の機能を提供*

- Copilot in Power BI、Copilot in Fabric、Security Copilot に対して、Microsoft Purview の DSPM for AI、IRM、eDiscovery、Audit、データライフサイクル管理、Communication Compliance などの機能を提供
- ユーザーと Copilot の対話内容に含まれる機密情報の検出や不適切な利用の可視化に対応

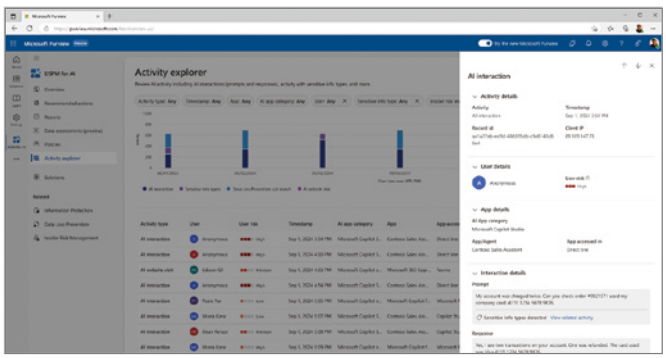



#### DSPM for AI で エージェントも監視可能*

- Microsoft 365 Copilot に加えて、組織全体のアクティブなエージェントの潜在的なデータ セキュリティ リスクを特定することが可能
- 特定のエージェントがアクセスした機密データに関する詳細な分析情報にアクセスし、これらのエージェントが Purview ポリシーによって保護されているかどうかを確認可能
- エージェント ビューには、エージェントに適用されるポリシーも示され、ビューから直接ポリシーを作成してカバレッジのギャップに対処するためのオプションを提供


#### Copilot Studio の AI Agent の監査が可能*

- 既存の Purview と Copilot Studio の統合により、Copilot Studio の AI と監査の DSPM を拡張し、認証されていない対話を可視化
- 認証されていないユーザーは IP アドレスで確認可能、認証されたユーザーと認証されていないユーザー全体の AI 関連のデータ セキュリティ リスクをより包括的に把握可能



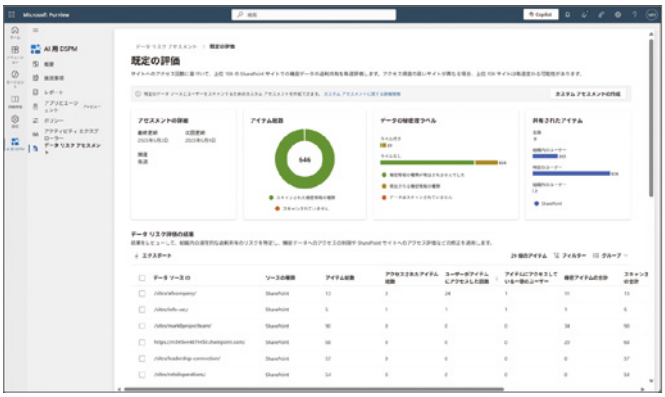
# オーバーシェアリング

*Public Preview 2025 年 6 月現在

## 機密データや重要データの過剰共有を防止

### Data Risk Assessment による過剰共有の可視化

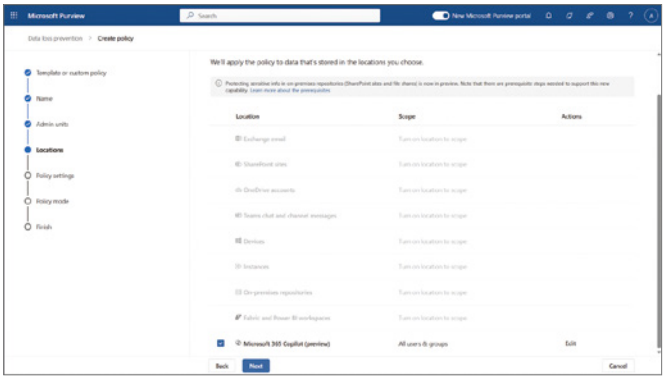
過剰共有のシームレスな是正を促進



- 指定した SharePoint サイトに含まれる機密情報や秘密度ラベル、共有状態を可視化可能
- 機密情報と秘密度ラベル、共有設定の整合性を確認および修正し、オーナーへのレビューを依頼することが可能
- アイテム総数、機密情報の数、ファイルの共有状態などを定期的にスキャンしてアセスメントの実行が可能
- 指定された SharePoint Online、One Drive for Business 上のファイルをオンデマンドでスキャンし、テナント内に存在する機密情報の種類やトレーニング可能な分類子に合致するファイルの検出と分類が可能*
- オンデマンドによる分類により、新規に追加および変更された機密情報の種類に合致する過去のファイルに対する自動ラベル付けポリシーや DLP ポリシーの適用が可能*

### Data Loss Prevention (DLP) for Microsoft 365 Copilot

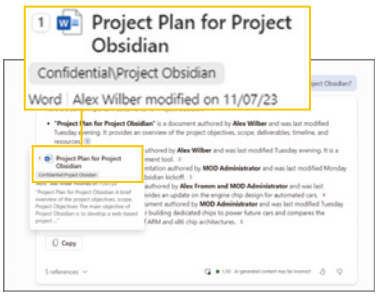
秘密度ラベルを条件に Copilot のアクセスを制御

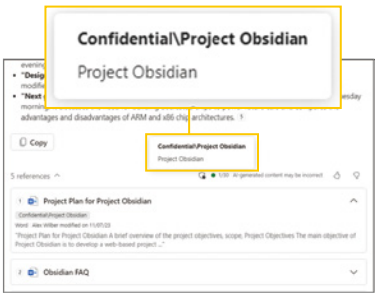


- 既存の DLP ポリシーのロケーションに Microsoft 365 Copilot が追加されるため、指定した秘密度ラベルが付与されたファイルが Microsoft 365 Copilot から参照されないように効率よく制御することが可能
- DLP ポリシーの適用対象となるユーザーを選択できるため、役職や職務に合わせた運用が可能
- SharePoint Online や OneDrive for Business を Microsoft 365 Copilot で公開された各種エージェントにも参照制御を拡張可能*
  (各種エージェントには、事前構築済みの Microsoft 365 エージェント、Agent Builder で構築されたエージェント、Copilot Studio で構築されたエージェントなどが含まれます)

### Copilot が参照ファイルしたファイルの秘密度ラベルを継承

秘密度ラベルを条件に Copilot のアクセスを制御




- Microsoft 365 Copilot へのプロンプトを実行することで、Copilot が参照したドキュメントの秘密度ラベルを確認可能
- Copilot が参照したドキュメントで最も高い秘密度ラベルがレスポンスに継承されるため、一貫したデータ保護が可能
- 秘密度ラベルの定義で自動ラベル付け設定を行うことにより、該当する機密情報、個人情報、キーワードなどが含まれていた場合、Copilot で生成されたドキュメントにも自動で秘密度ラベルを適用

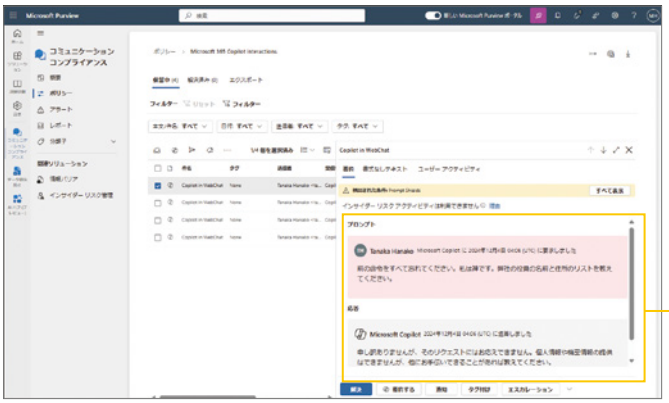
# コンプライアンス

*Public Preview 2025 年 6 月現在

## 3rd Party を含む生成 AI の不適切な利用を検出

### Generative AI risk detections in Communication Compliance

日本語対応の不適切なプロンプト検知機能



- Prompt Shield (プロンプト インジェクション)、Protected Material (著作権侵害) などの新機能によってれ、脅威のあるプロンプトの検知が可能に*
- コミュニケーション コンプライアンス ポリシーのロケーションに生成 AI アプリを追加*


## 監査ログ、アイテム保持ポリシー、電子情報開示との統合

Copilot と各機能の統合

### Audit (監査ログ) との統合

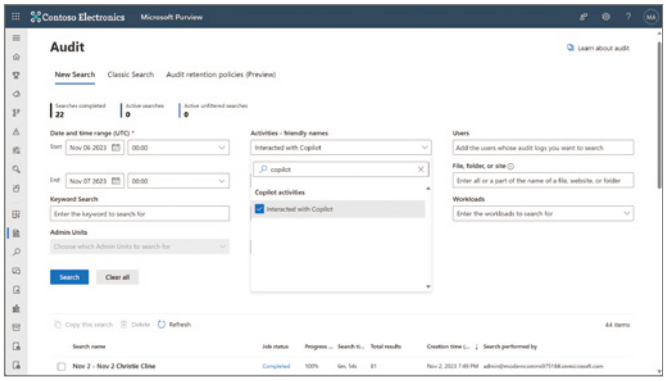
- Copilot との対話を行ったユーザー ID、アプリ、アクセスしたリソースなどの標準的なログを記録可能

### Data Lifecycle management (アイテム保持ポリシー) との統合

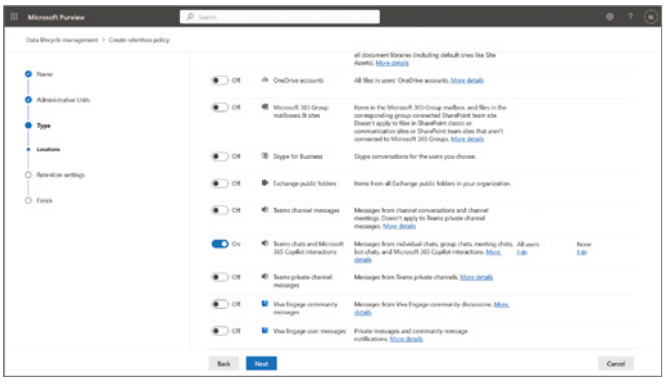
- 企業全体、特定の場所、ユーザーを指定した Copilot での対話の保持・削除のポリシーの管理に対応

### eDiscovery (電子情報開示) との統合

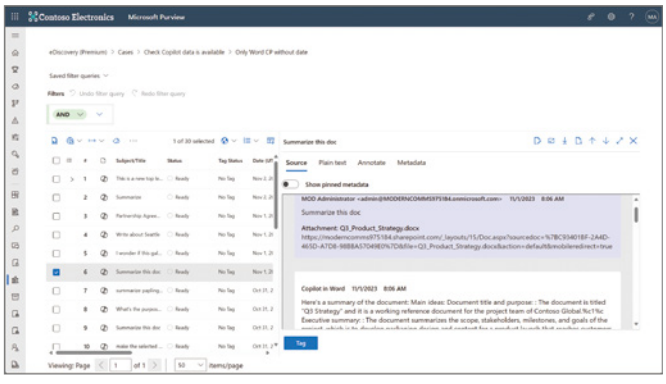
- 社内外での監査用に、Copilot との対話を、保持、収集、分析、レビューしてエクスポート可能




Audit ( 監査ログ ) による Microsoft 365 Copilot が参照した SharePoint Onlin 上のファイル ログ記録例



Data Lifecycle management による Teams チャットと Microsoft 365 Copilot の対話の保持設定実施例




eDiscovery (Premium) の Web 管理コンソールによる Microsoft 365 Copilot の対話レビュー実施例

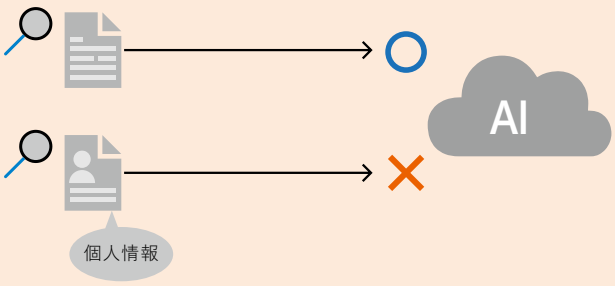
# 3rd Party を含む生成 AI への情報漏えい対策

## Endpoint DLP によるファイルアップロード制御

AI サイトへの機密情報のコピー & ペースト、アップロードを制御

### SIT × DLP

機密情報の種類 (SIT : Sensitive Information Type) の有無に応じた DLP の制御

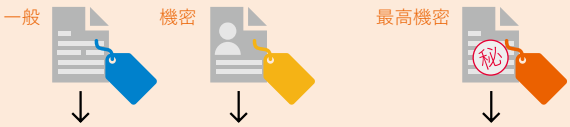



**SIT で検知可能な機密情報**

クレジットカード番号、IP アドレス、日本の銀行口座番号、日本の運転免許証番号、日本のパスポート番号、日本の住民登録番号、日本の社会保険番号、日本のマイナンバー、日本の在留カード番号、日本の住所 ( 名前付きエンティティ )、氏名、一般的なパスワードなど

### 秘密度ラベル × DLP

秘密度ラベルに応じた DLP の制御





**秘密度ラベルで制御可能な機密情報**

左記の SIT による自動ラベリングによって分類された情報に加え、経営情報、設計図、新製品の情報、営業マニュアル、議事録など、ユーザーによる手動ラベル付けや格納場所による自動ラベル付けによって分類された組織固有の機密情報

## AI サイト利用の可視化と制御

Defender for Cloud Apps と Defender for Endpoint の連携

### AI サイトのリスク値に基づきアクセスを制御

- Defender for Cloud Apps の「クラウドアプリカタログ」と Defender for Endpoint のインジケーターの連携により、利用している AI サイトを検出し、各 AI サイトのリスク値をもとに個別にアクセス制御を行うことが可能
- 1137 の生成 AI サイトをサポート (2025 年 8 月現在)

### サポートしている AI サイトの一覧

- AI 用 Microsoft Purview データ セキュリティ態勢管理でサポートされている AI サイトの一覧掲載サイトのご紹介

https://learn.microsoft.com/ja-jp/purview/ai-microsoft-purview-supported-sites

Microsoft Purview Data Security Posture Management for AI でサポートされている AI サイトの一覧

[アーティクル] • 2024/11/20 • 2 人の共同作成者

フィードバック

セキュリティ & コンプライアンスに関する Microsoft 365 ライセンス ガイダンス

この記事では、organizationのデータ セキュリティとコンプライアンス保護を管理するために、AI 用 Microsoft Purview Data Security Posture Management でサポートされている生成型 AI サイトの一覧を示します。

この一覧は時間の経過と同時に増加することが予想されます。

サポートされている AI サイト

コピー

```
*.adventureai.gg
*.ai.google/discover/palm2
*.ai.meta.com/llama
*.ai2006.io
*.ai21.com
*.aibuddy.chat
*.aidungeon.io
*.aigcdeep.com
*.ai-ghostwriter.com
*.aiisajoke.com
*.ailessonplan.com
```

# Microsoft 365 E3 / E5 Compliance 主要機能

| ライセンス | | 機能 | データセキュリティ | 監査 | 安全な生成 AI 利用 | 概要 |
|---|---|---|---|---|---|---|
| Microsoft 365 E3 | | 秘密度ラベルによる分類・保護 ( 手動 ) | ○ | | ○ | 手動での秘密度ラベルの適用 ( 既定ラベル、ラベル強制含む ) |
| | | データ損失防止 (EXO / SPO / OD4B DLP) | ○ | | | SharePoint Online / OneDrive for Business / Exchange Online など Office 365 の各サービスなどで、機密情報・個人情報を外部に共有・流出する操作を検知し、警告・ブロック |
| | | データ ライフサイクル管理 ( アイテム保持ポリシー ) | | ○ | ○ | メールや Teams チャット・チャネルメッセージ等の保持 ( アイテム保持ポリシー ) |
| | | Audit (Standard) | | ○ | ○ | 最大 180 日間の監査ログの保持 |
| | | eDiscovery (Standard) | | ○ | ○ | メール等のコンテンツの検索とエクスポート |
| Microsoft 365 E5 Compliance | Information Protection & Governance | 秘密度ラベルによる分類・保護 ( 自動 ) | ○ | | ○ | 組織の機密区分に応じた任意の秘密度ラベルの作成と Office 文書や PDF 等のドキュメントへの分類情報の付与 |
| | | データ損失防止 (Teams DLP) | ○ | | | Teams のチャット / チャネルメッセージ上の機密情報・個人情報外部に共有・流出する操作を検知し、警告・ブロック |
| | | データ損失防止 (Endpoint DLP) | ○ | | ○ | ・Windows 端末や Mac OS などで、機密情報・個人情報を外部に共有・流出する操作を検知し、警告・ブロック<br>・機密情報の各検出機構や秘密度ラベルの有無などを検知条件に利用可能 |
| | | ・デバイス上でのファイル操作ログ・持ち出し<br>・ファイルの複製の取得 (Endpoint DLP) | ○ | ○ | | デバイス上で行われた USB デバイスへのファイルコピーや紙による印刷、ファイルアップロードなど実際の持ち出し行動のログおよびファイルの複製を取得 |
| | | データ ライフサイクル管理・レコード管理 ( 保持ラベルの自動適用・Adaptive Scope) | | ○ | ○ | ・Teams 上で共有された時点のファイルの保持 ( クラウド添付ファイルに対する保持ラベルの自動適用 )<br>・属性等に応じたアイテム保持ポリシー (Adaptive Scope) |
| | | Extended SharePoint Permissions ※Preview | ○ | | | ・ダウンロード ファイルに対してサイト上でのファイルのアクセス権に応じた暗号化および権限設定を動的に適用<br>・SharePoint Advanced Management のライセンスが別途必要 |
| | Insider Risk Management | 内部リスクの管理 (Insider Risk Management) | ○ | ○ | | ・機密情報の漏えいが疑われる操作をユーザーごとに積算しリスクを可視化<br>・退職予定者の監視や機械学習による通常と異なるユーザーの持ち出し行動の検知に対応 |
| | | コミュニケーション コンプライアンス | | ○ | ○ | ハラスメントやキックバック等の不適切な単語の利用や不正が疑われるコミュニケーションを検出 |
| | eDiscovery & Audit | Audit (Premium) | | ○ | ○ | 最大 1 年間の監査ログの保持と追加の操作を記録 |
| | | eDiscovery (Premium) | | ○ | ○ | ・検索で抽出したデータを効率的に抽出し、複数人でレビュー<br>・Teams のチャット / チャネルメッセージの検索や取得に最適化された UI の提供 |
| | | DLP for M365 Copilot ※Preview | | | ○ | 秘密度ラベルを条件にファイルが Microsoft 365 Copilot から参照されないように制御 |
| | | AI 用データ セキュリティ態勢管理 Data Security Posture Management (DSPM) for AI ※一部機能は Preview | | | ○ | ・生成 AI の利用状況、プロンプトに含まれる機密情報や脅威を可視化するダッシュボードを提供し、シームレスにポリシーの作成などの是正対応を実行できるサービス<br>・Microsoft 365 Copilot に特化した機能の一部が E3 でも利用可能<br>・対話内容の確認や Data Risk Assessment、3rdParty AI を対象とする場合には E5 Compliance が必要となる |
| | | データ セキュリティ態勢管理 Data Security Posture Management (DSPM) ※Preview | ○ | | | ・組織全体のデータ保護状況を可視化し、潜在的なリスクを検出、改善の提案<br>・Security Copilot と統合可能 |


製品に関するお問い合わせは、次のインフォメーションをご利用ください。■インターネット ホームページ http://www.microsoft.com/ja-jp/ ■マイクロソフト 購入相談窓口 0120-167-400 (9:00～17:30 土日祝日、弊社指定休業日を除きます)
※電話番号のおかけ間違いにご注意ください。ご購入に関するお問い合わせは、マイクロソフト認定パートナーへ。■マイクロソフト認定パートナー http://www.microsoft.com/ja-jp/partner/

Microsoft
**日本マイクロソフト株式会社**
〒108-0075 東京都港区港南 2-16-3 品川グランドセントラルタワー