



【Microsoft 365】 Copilot × Purview

2026年09月30日

改訂履歴

版数	発行日	改訂内容
第 1 版	2026年09月30日	初版発行

本書の内容は 2026/09/30 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ある旨、ご了承ください。

Agenda

1. 前提情報
 1. 本書の目的
 2. 用語集
2. Copilot 導入で顕在化するリスク
 1. Copilot が回答を生成するまでの流れを理解する
 2. Copilot 導入で見えてくる情報管理の課題
 3. Copilot 導入時に考慮すべきリスク
3. Purview の全体像と役割
 1. Purview 製品ポートフォリオ
 2. Purview が担う役割
 3. Purview 管理ポータル画面構成
4. 導入手順① DSPM で Copilot 利用開始前のリスク診断
 1. DSPM とは
 2. DSPM 設定手順
5. 導入手順② 秘密度ラベルで Copilot 参照データを管理
 1. Microsoft Information Protection とは
 2. ラベル設計手順
6. 導入手順③ DLP for Microsoft 365 Copilot で利用データを制御
 1. DLP for Microsoft 365 Copilot とは
 2. DLP ポリシー作成手順
7. 導入手順④ 監査で Copilot 利用状況を可視化
 1. 監査の役割
 2. 監査検索手順
8. 導入手順⑤ 電子情報開示で Copilot の調査対応
 1. 電子情報開示とは
 2. ケース作成手順
9. 導入手順⑥ インサイダーリスク管理・コミュニケーションコンプライアンスでリスクを検知
 1. インサイダー リスク管理でリスク行動を検知
 2. コミュニケーション コンプライアンスでやり取りを検知
10. Copilot ・ Purview のライセンス
 1. Copilot 関連ライセンス全体像
11. 運用・管理ベストプラクティス
 1. 推奨導入順序
 2. よくある失敗例と対処



1. 前提情報

1.1. 本書の目的

目的

Microsoft 365 Copilot 活用時に考慮すべき Microsoft Purview（以降、Purview）の機能、設定手順、ライセンス要件を理解し、AI ガバナンス実現のための推奨構成を検討できるようにする。

1.2. 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	Microsoft 365 Copilot	Word や Teams などの Microsoft 365 アプリに組み込まれた生成 AI アシスタント。
2	Copilot Chat	アプリ横断で社内データを参照しながら対話できる Copilot のチャット画面。
3	Microsoft Graph	Microsoft 365 上のデータや操作履歴へ統一的にアクセスするための基盤 API。
4	LLM（大規模言語モデル）	大量の文章で学習し、自然文の指示に対して文章を生成する AI モデル。
5	プロンプト	ユーザーが AI に与える自然文の指示や質問のこと。
6	応答	プロンプトに対して AI が生成した回答。
7	テナント	組織ごとに割り当てられる Microsoft 365 の管理単位。
8	過剰共有	業務上必要な範囲を超えて広くアクセス権が付与されている状態。
9	匿名リンク	サインインなしで誰でも閲覧できる共有リンク。過剰共有の主な原因。
10	AI ガバナンス	AI の利用状況とデータリスクを可視化し、方針に沿って統制する取り組み。
11	秘密度ラベル	データの機密度を表す分類タグ。暗号化やアクセス制御と連動する。
12	ラベルポリシー	作成した秘密度ラベルを対象ユーザーへ発行・適用するための設定。

1.2. 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	コンテンツ マーキング	ラベルに応じて文書へ透かし・ヘッダー・フッターを自動付与する機能。
14	自動分類	内容の判定結果に基づき、ラベルを自動で付与する仕組み。
15	監査ログ	誰がいつ何を操作したかを記録した証跡。Copilot の利用履歴も含む。
16	ロールグループ	管理者へ権限をまとめて割り当てる単位。表示される機能が変化する。
17	証跡保全	調査や法務対応のため、対象データを変更・削除させず保持する措置。
18	Microsoft Agent 365	AI エージェントの利用を管理・統制するための追加サービス。
19	Purview	データの保護・ガバナンス・コンプライアンスを担う Microsoft の統合サービス群。
20	DSPM	AI 利用に伴うデータリスクを診断し、改善の推奨事項を提示する機能。
21	DLP（データ損失防止）	機密情報の送信・共有・入力を条件に応じて検知し、警告やブロックを行う仕組み。
22	Information Protection	秘密度ラベルによる分類と暗号化など、データ保護を担う Purview の機能群。
23	Data Lifecycle Management	データの保持期間と削除を管理し、不要データを残さないための機能。
24	Data Map	社内外のデータ資産をスキャンし、所在とメタデータを台帳化する機能。

1.2. 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
25	監査（Standard ・ Premium）	操作ログを記録・検索する機能。Premium は保持期間や高度な検索に対応。
26	電子情報開示	調査や訴訟対応のため、対象データを検索・収集・保全・提出する機能。
27	インサイダー リスク管理	大量ダウンロードなど、内部不正につながるリスク行動を検知する機能。
28	コミュニケーション コンプライアンス	メールやチャットのやり取りから、ハラスメントや規程違反を検知する機能。
29	ポリシー	検知や制御の条件・対象範囲・動作をまとめた設定単位。
30	ポリシーモード	テスト・警告・適用など、ポリシーの動作段階を示す設定。
31	アラート	ポリシーに合致した操作を検知した際に管理者へ通知される警告。
32	リスクスコア	検知したユーザー行動の危険度を数値化し、対応の優先度を示す指標。
33	ケース	調査対象・担当者・収集データをひとまとめに管理する調査の単位。
34	レビュー担当者	検知されたやり取りを確認し、対応要否を判断する権限を持つ担当者。
35	保持設定（保持ポリシー）	対象データを一定期間、削除・改変させずに保持する設定。
36	機微情報（センシティブ情報）	マイナンバーやクレジットカード番号など、検知対象となる重要情報。

1.2. 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
37	CopilotInteraction	Copilot の操作が記録される監査ログのレコード種別。
38	エージェント	特定業務向けに構成された Copilot の拡張。独自データや処理を組み込める。
39	プラグイン	Copilot に外部サービスの機能やデータを接続する拡張部品。
40	会話 ID ・ メッセージ ID	やり取りを一意に識別する番号。会話単位での追跡に利用する。
41	Exchange Online	メールとメールボックスを提供するクラウドサービス。Copilot の対話履歴も保存される。
42	SharePoint ・ OneDrive	ファイルを保管・共有するサービス。Copilot の主な参照元。
43	Microsoft Teams	チャットと会議のサービス。やり取りが検知と参照の対象。
44	Microsoft Entra ID	ユーザー認証とアクセス権を管理する ID 基盤。



2. Copilot 導入で顕在化するリスク

2.1. Copilot が回答を生成するまでの流れを理解する

Copilot は利用者のアクセス権に基づき、Microsoft Graph 経由で必要な情報を取得して回答を生成します。そのため、ユーザーのアクセス権や共有設定が回答内容に影響します。

STEP

Copilot が回答を生成するまでの流れ

① プロンプト入力



プロンプト指示

Word・Excel・Teams・Copilot Chat などから、ユーザーが指示（プロンプト）を入力

② 利用者の権限で情報を検索



Graph による検索

- Copilot が関連する情報を探す
- SharePoint・OneDrive・Exchange・Teams から情報を取得
- ユーザーがアクセス権を持つ情報を参照
- 必要に応じて Web 検索も利用

③ 回答を生成



Copilot からの回答

- 取得した情報をもとに回答を生成
- 回答とあわせて参照元を提示
- 応答は元データの権限とラベルを継承

※プロンプトと回答は基盤モデルの学習に利用されません

2.2. Copilot 導入で変わる情報活用

Copilot により必要な情報へ素早く到達できるようになり、これまで以上に情報を活用しやすくなります。

変化

Copilot 活用時に把握しておくべき情報管理の観点



情報へ到達しやすくなる

Copilot は**社内データを横断して回答を作成するため、利用者が複数の資料や過去のやり取りを探し回ることなく、必要な情報を取得できる**ようになります。

ポイント

- 検索スキルに依存せず必要な情報に届く
- 埋もれていた過去資料も活用しやすい
- 部門を越えた情報活用が進む
- 業務の立ち上がりが速くなる



過剰共有が顕在化する

利用者がアクセスできる情報を横断して参照できるため、**不要に広いアクセス権が設定されている場合、その影響を受けやすくなります。**

ポイント

- 意図しない資料が引用されうる
- 匿名リンク・全社サイトが要因になりやすい
- 権限の棚卸しが事実上の前提条件になる



情報活用が定着する

Copilot の利用が組織全体に広がることで、**情報検索や文書作成の効率化が進み、生産性向上が期待できます。**

ポイント

- 日常業務での利用機会が増える
- 部門ごとに独自の活用方法が広がる
- 業務プロセスへの定着が進む
- 組織全体の生産性向上につながる

2.3. Copilot 導入時に考慮すべきリスク

Copilot により情報活用の幅が広がる一方で、情報管理や運用面で考慮すべきリスクも存在します。

リスク

Copilot 利用で想定されるリスクと対策の全体像

機密情報の露出



- 権限過多のデータが回答に混入する
- 引用元から二次拡散する恐れがある
- 回答内容から機密情報が漏えいする恐れがある

機密情報の入力・転記



- プロンプトへ機密情報を入力してしまう
- 生成物を外部資料に記載してしまう
- 生成物の取り扱い基準が曖昧になる

不適切利用の検知不足



- ポリシー違反の利用を検知できない
- 再発防止策につなげられない
- 注意喚起の根拠を示せない

利用状況の可視化不足



- 利用履歴を取得できず実態が不明になる
- 監査要求に応えられない
- 部門別の傾向を把握できない

調査体制の不足



- 情報の漏えい時に証跡を追えない
- 影響範囲の特定に時間がかかる
- 証跡の保全措置を取れない

リスク状況の把握不足



- AI 利用実態やデータリスクを把握できない
- 対策の優先順位を判断できない
- 改善効果を確認できない



3. Purview の全体像と役割

3.1. Purview 製品ポートフォリオ

Microsoft 365 には Microsoft Purview が用意されており、セキュリティ・コンプライアンス・ガバナンスを支援する 3 領域で構成されています。



セキュリティ

データを保護し、漏えいを防止

守る対象

- ◆Microsoft 365 全体
- ◆エンドポイント
- ◆AI 利用時のデータ

主要機能

- ◆Information Protection
- ◆DLP
- ◆Data Lifecycle Management
- ◆DSPM

提供価値

- ◆機密情報の分類と保護
- ◆誤共有・持ち出しの抑制
- ◆データの暗号化・利用制御



コンプライアンス

リスク検知とコンプライアンスの確保

守る対象

- ◆ユーザーの操作履歴
- ◆チャットなどのコミュニケーション
- ◆規制・法令対応

主要機能

- ◆監査
- ◆電子情報開示
- ◆インサイダー リスク管理
- ◆コミュニケーション コンプライアンス

提供価値

- ◆利用状況の可視化
- ◆内部不正・リスクの早期検知
- ◆監査・法令対応の証跡確保



ガバナンス

利用を可視化し、品質を担保

守る対象

- ◆Microsoft 365 全体
- ◆エンドポイント
- ◆AI 利用時のデータ

主要機能

- ◆利用状況の分析
- ◆AI 利用ポリシーの管理
- ◆Data Map

提供価値

- ◆AI リスクの可視化
- ◆データ資産の可視化と検索性向上
- ◆ポリシー準拠の徹底

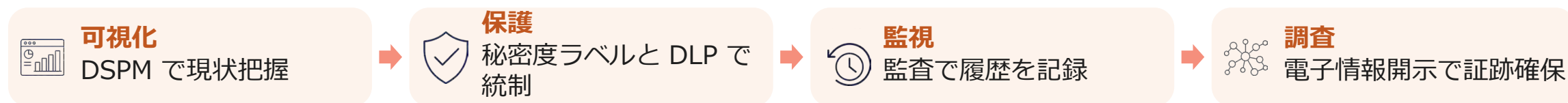
詳細はこちら→ [【Purview】サービス概要](#)

3.2. Purview が担う役割

P.13 にて紹介した各リスクには対応する Purview 機能があり、組み合わせて多層的に統制します。

リスク	Purview 機能	担う役割
機密情報の露出	秘密度ラベル	データを秘密度で分類し、暗号化と利用権限を付与する
機密情報の入力・転記	DLP	機密情報を含むデータの Copilot での入力・参照を制限する
	コミュニケーション コンプライアンス	不適切なプロンプトやポリシー違反を検知する
利用状況の可視化不足	監査	プロンプトと応答を含む操作ログを記録し検索する
調査体制の不足	電子情報開示	インシデント・法務対応に必要な証拠を保全し収集する
不適切利用への対応	インサイダー リスク管理	大量取得など、リスクの高いユーザー操作を検知する
リスク状況の把握不足	DSPM	AI 利用状況とデータリスクを可視化し推奨対応を提示する

上記機能の一部を利用した導入順序の例



※提供範囲は、ご利用のライセンスに応じて異なります。

詳細は、P.56 [Copilot と Purview のライセンス体系](#)をご参照ください。

3.3. Purview 管理ポータル画面構成

DSPM、DLP、監査などの各機能は、Microsoft Purview ポータルから管理します。本ページでは基本的な画面構成を紹介します。



1 上部バー

検索、Copilot、各種設定へアクセスできます。

2 左ナビゲーション

ホームや各ソリューション、設定画面へ移動できます。

3 ソリューションカード

利用する機能を選択して設定画面へ移動します。

4 すべてのソリューション

Purview の全機能を一覧で確認できます。

Purview ポータル ホーム画面 (<https://purview.microsoft.com>)

補足

各機能の利用には対応する Purview ロールが必要です。
詳細は、[Microsoft Purview ポータルでの Microsoft Entra ロール](#)を参照ください。



4. 導入手順① DSPM で Copilot 利用開始前のリスク診断

全体の導入の流れは[11.1. 推奨導入順序](#)を参照

4.1. DSPM とは

Purview DSPM は、Copilot 活用に向けてデータリスクを可視化し、優先的に対応すべき課題を把握するための機能です。

DSPM で把握できる 3 つの観点

1 AI 利用状況の可視化

どの AI アプリがどれだけ使われているかを把握



- Microsoft 365 Copilot
- Copilot in Teams
- Copilot in Outlook
- その他の AI アプリ

- ・ 部門別の傾向を把握
- ・ 件数と利用者数を集計
- ・ Copilot 以外の AI も対象

2 リスク評価

推奨アセスメントで対処すべき項目を提示

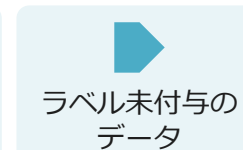


- 高リスク 28 件
- 中リスク 64 件
- 低リスク 153 件

- ・ 要確認項目を自動抽出
- ・ レポートとして提示
- ・ 改善の優先度を明確化

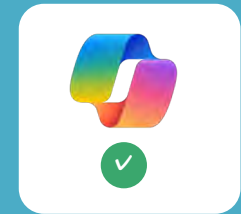
3 過剰共有分析

広範囲に共有されたデータを事前に検出



- ・ 共有サイトを特定
- ・ 広範囲共有を把握
- ・ ラベル未付与を検出

4 Copilot 展開へ



データリスクを把握・改善し
リスクを低減した状態で
Copilot を展開

- ・ リスクを最小化
- ・ 安全な環境を構築
- ・ 信頼性を確保

DSPM の価値

1 利用状況を把握

2 リスクを特定

3 改善対象を洗い出し

4 安全に Copilot 活用

4.2. DSPM 設定手順

DSPM を使い始めるためのセットアップ タスクの確認手順を説明します。

セットアップ タスクを完了

AI 利用状況を確認

過剰共有分析を確認

レポートでリスク評価し改善

STEP 1 セットアップ タスクを完了する

1. Purview ポータルにサインインする
2. 画面左部もしくは [ソリューション] から [DSPM] を開く
3. [タスクとアクション] > [セットアップ タスク] に表示されるタスクを確認する
4. 監査の有効化やユーザー範囲の設定など、セットアップ タスクに従って必要な初期設定を完了する

※初期設定完了後、データの収集・分析が開始されます

Microsoft Purview

ソリューション、ユーザー、記事などを検索します

セットアップ タスク

データセキュリティ態勢管理 (クラシック) と AI 用データ セキュリティ態勢管理 (クラシック) は、2026 年 9 月 30 日に廃止されます。クラシック ソリューション になりました。

これらのセットアップ タスクは、リスクやセキュリティ制御を含む機密データを可視化し、それらのリスクを軽減し、機密データを保護します。

開始前 | 消去済み | 完了済み

9 | 0 | 1

最新の情報に更新

セットアップ タスク ↑ ↓	種類 ↓	期間 ↓
AI アプリの相互作用で機密データに分析情報を拡張する ブラウザー、アプリケーション、API の中で AI アプリと共有されている機密情報を検出します。	推奨	約 5 分
Microsoft Copilot エクスペリエンスでの安全なやり取り サポートされている Copilot およびエージェントから、データ セキュリティ態勢に関するプロンプトと応答をキャプチャします。	推奨	約 5 分
Microsoft Purview にデバイスをオンボードする 機密データが他の AI アプリに漏洩しないよう保護します。	推奨	約 1 時間
Microsoft Purview ブラウザー拡張機能のインストール 危険なユーザー アクティビティを検出し、他の AI アプリとのユーザーの対話に関する分析情報を取得します。	推奨	約 1 時間
Microsoft Purview 監査をアクティブにする Microsoft Copilot エクスペリエンスおよびエージェントを使用してユーザーとの対話に関する分析情報を取得します。	必須	約 7 分

4.2. DSPM 設定手順

DSPM の概要画面で Copilot の利用状況を確認する手順を説明します。

セットアップ タスクを完了

AI 利用状況を確認

過剰共有分析を確認

レポートでリスク評価し改善

※ STEP 1 完了後、データの収集・分析が開始されます。分析結果はデータの蓄積後に確認できます。

STEP 2 AI 利用状況を確認する

1. 画面左部メニューから [AI 観察可能性] を開き、[AI アプリ] を選択する
2. M365 Copilot – Apps などの該当のアプリを選択する
3. アプリリスクレベルや機密性の高いアクティビティの傾向を確認する
4. 気になる項目を選択し、詳細な分析結果を確認する



4.2. DSPM 設定手順

DSPM の過剰共有分析で、Copilot から参照され得るデータの共有状況を確認する手順を説明します。

セットアップ タスクを完了

AI 利用状況を確認

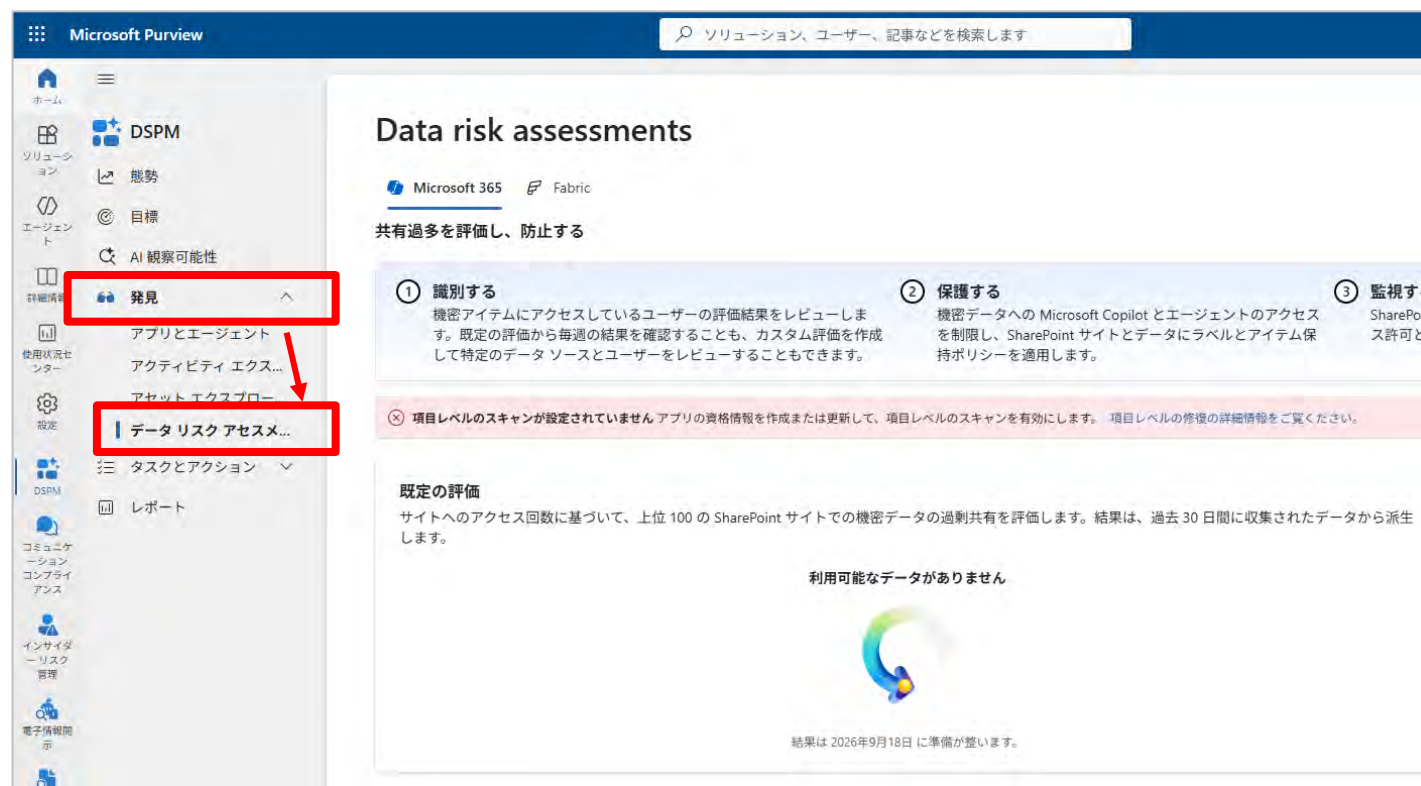
過剰共有分析を確認

レポートでリスク評価し改善

STEP 3 過剰共有分析を確認する

1. 画面左部メニューから [発見] を開き、
[データリスク アセスメント] を選択する
2. サイトやファイル単位の共有状況と対象
件数を確認する
3. 必要に応じて [カスタム評価] を実施し、
改善対象を洗い出す

※2026年9月30日時点では、プレビュー機能となります



4.2. DSPM 設定手順

DSPM のレポートを使ってデータリスクを評価する手順を説明します。

セットアップ タスクを完了

AI 利用状況を確認

過剰共有分析を確認

レポートでリスク評価し改善

STEP 4 レポートでリスクを評価する

1. 画面左部メニューから [レポート] を開く
2. Copilot からアクセスされたデータのレポートを確認する
3. 過剰共有の可能性のあるサイトやファイルを特定する
4. 表示された推奨事項をもとに改善対象を特定する

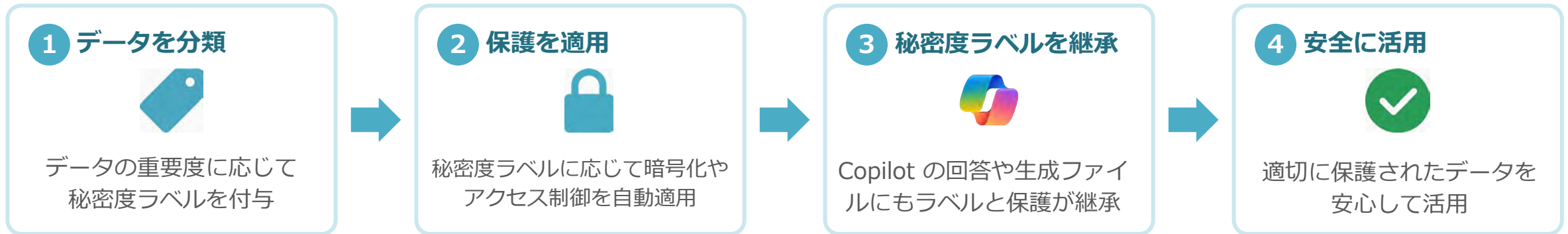




5. 導入手順② 秘密度ラベルで Copilot 参照データを管理

5.1. Microsoft Information Protection とは

Microsoft Information Protection は、データを分類・保護し、Copilot 活用時にもその保護を継承する機能群です。



分類（ラベルの種類）

データの重要度や取り扱い区分を秘密度ラベルで表現

 Public (公開)	社外公開可能な情報
 Internal (社内向け)	社内での共有を想定した情報
 Confidential (機密)	特定のユーザーのみアクセス可能な情報

自動分類・手動分類の両方に対応

保護（ポリシーの適用）

秘密度ラベルに基づき、データを自動で保護

 暗号化	ファイルやメールを暗号化し、不正なアクセスから保護
 アクセス制御	閲覧・編集・印刷・転送などの操作を制限

透明性の確保と、手動適用・自動適用の両方に対応

Copilot への効果

秘密度ラベルは Microsoft 365 全体で継承

 アクセス制御の継承	Copilot はユーザーの権限に基づきアクセスを制御
 保護の継承	出力ファイルや回答にも秘密度ラベルと保護が継承

データの機密性を維持したまま、AI の力を活用

5.2. ラベル設計手順

Purview ポータルで秘密度ラベルの作成を開始する手順を説明します。

作成開始

名前説明

適用範囲

保護種類

アクセス

マーク

サイト

確認作成

STEP 1 ラベルの作成を開始する

1. 画面左部メニューから [Microsoft Information Protection] を開く
2. [秘密度ラベル] を選択する
3. 既存のラベル一覧を確認する
4. [ラベルの作成] を選択する



5.2. ラベル設計手順

秘密度ラベルを作成し、利用者がデータの取り扱い区分を判断できる説明文の設定手順を説明します。

作成開始

名前説明

適用範囲

保護種類

アクセス

マーク

サイト

確認作成

STEP 2 名前と説明を設定する

1. ラベルの名前を入力する
2. ユーザーに表示される表示名を設定する
3. ラベルの優先度を設定する
4. ユーザー向けの説明を入力する
5. 管理者向けの説明を入力する
6. [次へ] で保護設定に進む

新しい秘密度ラベル

ラベルの詳細

- 範囲
- アイテム
- グループ & サイト
- 完了する

このラベルの基本的な詳細を指定します

このラベルのために選択する保護設定は、ラベルが適用されたアイテム、またはコンテンツ コンテナーに対してすぐに有効になります。ラベル付きのファイルは、クラウドに保存されたり、コンピューターにダウンロードされたりするなど、保存先がどこであっても保護されます。

名前 

わかりやすい名前を入力します。

表示名 

表示名を入力します。これは、公開されているアプリでユーザーに表示される名前です。

ラベルの優先度 

☒ 既定では、このラベルに保護設定の優先度が割り当てられますが、作成後に変更できます。

既定

ユーザー向けの説明 

ユーザーがこのラベルの目的を理解するために役立つテキストを入力してください。

管理者向けの説明 

このラベルを管理する管理者は役立つ説明を入力してください。

ラベルの色 



次へ

5.2. ラベル設計手順

秘密度ラベルを適用する対象範囲を定義し、Copilot の参照データを漏れなく分類する設定を説明します。

作成開始

名前説明

適用範囲

保護種類

アクセス

マーク

サイト

確認作成

STEP 3 ラベルの適用範囲を定義する

1. [ファイルと他のデータ資産] を選択し、Copilot が引用する文書を対象にする
2. [メール]を選択し、メールを対象にする
3. [会議] を選択し、 Copilot が引用する Teams の会議や予定表の情報も対象に含める
4. [グループとサイト] を選択し、Copilot が引用する SharePoint ・ Teams のコンテナを対象にする

新しい秘密度ラベル

- ラベルの詳細
- 範囲
- アイテム
- グループ & サイト
- 完了する

このラベルの範囲を定義する

ラベルは、データ資産とコンテナ (SharePoint サイトや Teams など) に適用できます。関連する保護設定を表示できるように、このラベルを使用する場所をお知らせください。 [ラベルの範囲に関する詳細情報](#)

☒ ファイルと他のデータ資産

Microsoft 365、Fabric (Power BI を含む)、Viva Engage (プレビュー)、および Azure のファイルとデータ資産にラベルを付けます。

☒ メール

すべてのバージョンの Outlook から送信されたメッセージをラベルを付けます。

☒ 会議

Outlook と Teams でスケジュールされた予定表のイベントと会議をラベルを付けます。

① 親ラベルは、サブラベルから会議スコープを自動的に継承します

☐ グループ & サイト

プライバシー、アクセスの制御、その他の設定を構成して、ラベル付き Teams、Microsoft 365 グループ、Entra セキュリティ グループ、SharePoint サイト、Viva Engage コンテンツ (プレビュー)、Loop ワークスペースを保護します。

① 秘密度ラベルを Teams、SharePoint サイト、Microsoft 365 グループに適用するには、最初に [次の手順を実行して](#) 機能を有効にします。

① スキーマ化されたデータ資産オプションがどこに行ったのか気になりますか? このラベルを Azure のデータ資産に適用するには、上で [ファイルとその他のデータ資産] を選択し、Azure ストレージと Azure SQL を対象とする自動ラベル付けポリシーにこのラベルを追加します。 [詳細情報](#)

5.2. ラベル設計手順

ラベル付きデータを Copilot が参照した場合にも保護を維持できるよう、適用する保護設定の選択手順を説明します。

作成開始

名前説明

適用範囲

保護種類

アクセス

マーク

サイト

確認作成

STEP 4 保護設定の種類を選択する

1. [アクセスの制御] を選択し、権限のないユーザーによる閲覧や編集を制限する
2. [コンテンツ マーキングを適用する] を選択し、透かしやヘッダーなどを設定する
3. Copilot の入力元となる Teams 会議やチャットの保護設定を必要に応じて選択する

※アクセス制御やコンテンツ マーキングは、Copilot が参照するデータや生成されるファイルにも継承されます

新しい秘密度ラベル

- ☒ ラベルの詳細
- ☒ 範囲
- ☒ アイテム
- ☐ グループ & サイト
- ☐ 完了する

選択した項目の種類の保護設定を選択します

Microsoft 365 内の項目にラベルが適用されるときに、構成する保護設定が適用されます。

- ☒ **アクセスの制御**
ラベル付きアイテムにアクセスして表示できるユーザーを制御します。
- ☒ **コンテンツ マーキングを適用する**
ラベル付けされた項目にカスタム ヘッダー、フッター、透かしを追加します。
- ☐ **Teams の会議とチャットを保護する**
Teams 会議とチャットの保護設定を構成します。

① Teams の会議とチャットを保護するには、組織に Teams Premium ライセンスが必要です。 [Teams Premium に関する詳細情報](#)

5.2. ラベル設計手順

暗号化とアクセス許可を設定し、ラベル付きデータの利用範囲を制御する手順を説明します。

作成開始

名前説明

適用範囲

保護種類

アクセス

マーク

サイト

確認作成

STEP 5 アクセスの制限を設定する

1. [アクセス許可を今すぐに割り当てる] を選択し、対象ユーザーを指定する
2. コンテンツへのアクセス有効期限とオフラインアクセスを設定する
※端末に残ったコピーは Copilot の制御が及ばないため短めに設定します
3. ユーザーやグループごとに閲覧・編集などの利用権限を割り当てる

新しい秘密度ラベル

ラベルの詳細
範囲
アイテム
アクセスの制御
コンテンツのマーキング
ファイルとメールの自動ラベル付け
グループ & サイト
完了する

アクセスの制御

暗号化機能を使用して、ラベル付けされた項目にアクセスできるユーザーを制御します。指定した範囲に応じて、項目にはメール、Office、Fabric および Power BI ファイル、会議出席依頼を含めることができます。 [アクセス制御設定に関する詳細情報](#)

☐ 項目に既に適用されている場合は、アクセス制御の設定を削除する

☒ アクセス制御設定の構成

☐ Office デスクトップ アプリの共同編集を有効にすると、複数のユーザーが、アクセス制御の設定が適用されているラベル付きドキュメントを同時に編集できるようになります。
[この設定に関する詳細情報](#)

[共同編集設定に移動](#)

アクセス許可を今すぐ割り当てますが、それともユーザーが決定するようにしますか？

ラベルがメールや Office ファイルに適用されると、選択した設定が自動的に適用されます。

コンテンツに対するユーザーのアクセス許可の期限

オフライン アクセスを許可する

5.2. ラベル設計手順

ラベル付きデータに透かしやヘッダーを設定し、必要に応じてファイルとメールの自動ラベル付けを構成する手順を説明します。

作成開始

名前説明

適用範囲

保護種類

アクセス

マーク

サイト

確認作成

STEP 6 コンテンツのマーキングを設定する

1. [コンテンツのマーキング] を選択し、ラベル付きの文書とメールを対象にする
2. 透かし・ヘッダー・フッターから、付与するマークの種類を選択する
3. [テキストのカスタマイズ] より表示するテキストやフォント、配置をカスタマイズする
4. [ファイルとメールの自動ラベル付け] を選択する

The screenshot shows the '新しい秘密度ラベル' (New Security Label) configuration page. The left sidebar has a navigation menu with 'ラベルの詳細' (Label Details), '範囲' (Scope), 'アイテム' (Items), 'アクセスの制御' (Access Control), 'コンテンツのマーキング' (Content Marking), 'ファイルとメールの自動ラベル付け' (Automatic Labeling of Files and Emails), 'グループ & サイト' (Groups & Sites), and '完了する' (Finish). The 'コンテンツのマーキング' section is active. It contains a heading 'コンテンツのマーキング' and a sub-heading 'このラベルが適用されているコンテンツにカスタム ヘッダー、フッター、透かしを追加します。' (Add custom headers, footers, and watermarks to the content to which this label is applied). Below this is a note about document watermarking. A toggle switch 'コンテンツのマーキング' is turned on. There are three checkboxes: '透かしの追加' (Add watermark) with a link to 'テキストのカスタマイズ' (Customize text), 'ヘッダーの追加' (Add header) with a link to 'テキストのカスタマイズ' (Customize text), and 'フッターの追加' (Add footer) with a link to 'テキストのカスタマイズ' (Customize text). The 'フッターの追加' checkbox is checked. At the bottom are '戻る' (Back) and '次へ' (Next) buttons.

The screenshot shows the '新しい秘密度ラベル' (New Security Label) configuration page. The left sidebar is the same as the previous screenshot. The 'ファイルとメールの自動ラベル付け' (Automatic Labeling of Files and Emails) section is active. It contains a heading 'ファイルとメールの自動ラベル付け' and a sub-heading 'ユーザーが Office ファイルを編集したり、ここで選択した条件に一致するコンテンツを含む Outlook からのメールを作成、返信、または転送したりする場合は、このラベルを自動的に適用するか、ユーザー自身で適用することをお勧めします。' (If a user edits Office files or creates, replies to, or forwards email from Outlook containing content that matches the conditions you selected here, we recommend that you automatically apply this label or let the user apply it themselves). Below this is a note about automatic labeling. A toggle switch 'ファイルとメールの自動ラベル付け' is turned on. There is a section 'これらの条件に一致するコンテンツを抽出する' (Extract content that matches these conditions) with a '+ 条件の追加' (Add condition) button. Below this is a section 'コンテンツが次の条件に一致する場合' (If content matches the following conditions) with a dropdown menu set to '自動的にラベルを適用する' (Automatically apply label). Below this is a section 'ラベルを適用するときに、このメッセージをユーザーに表示する' (When applying the label, display this message to the user) with a text input field. At the bottom are '戻る' (Back) and '次へ' (Next) buttons.

5.2. ラベル設計手順

グループとサイトの保護範囲を定義し、過剰共有された場所から Copilot が情報を取得しないようにする手順を説明します。

作成開始

名前説明

適用範囲

保護種類

アクセス

マーク

サイト

確認作成

STEP 7 グループとサイトの保護を定義する

1. [プライバシーと外部ユーザーアクセス]にて[プライバシー] と [外部ユーザーのアクセス] 設定を構成する

※公開範囲が広いサイトは、多くのユーザーの Copilot から参照される可能性があります

2. [外部共有および条件付きアクセス] にて外部ユーザーのアクセス可否を設定する
3. [プライベート チームの検出可能性と共有チャネルの設定] にて管理されていない端末からのアクセス条件を設定し、持ち出しを抑止する

新しい秘密度ラベル

- ラベルの詳細
- 範囲
- アイテム
- グループ & サイト
- 完了する

グループとサイトの保護設定を定義

保護設定

これらの設定は、このラベルが適用されているチーム、グループ、およびサイトに適用されます。これらのコンテナーに格納されているファイルには直接適用されません。 [これらの設定についての詳細情報](#)

- ☐ プライバシーと外部ユーザー アクセス
内部および外部のユーザーがラベル付けされたチームと Microsoft 365 グループにアクセスするレベルを制御します。
- ☐ 外部共有および条件付きアクセス
外部共有を制御し、条件付きアクセスを構成して、ラベル付き SharePoint サイトを保護します。
- ☐ プライベート チームの検出可能性と共有チャネルの設定
プライベート チームを検索で検出可能にするかどうかを決定し、共有チャネルに招待できるチームの種類を制御します。

5.2. ラベル設計手順

設定内容を確認し、秘密度ラベルの作成を完了する手順を説明します。

作成開始

名前説明

適用範囲

保護種類

アクセス

マーク

サイト

確認作成

STEP 8 内容を確認して作成する

1. 設定した項目を一覧で確認する
2. 修正が必要な項目は [編集] から戻る
3. [ラベルを作成] をクリックする
4. ラベルポリシーで発行し、Microsoft 365 や Copilot で利用できるようにする

新しい秘密度ラベル

- ラベルの詳細
- 範囲
- アイテム
- グループ & サイト
- 完了する

あ
編集

表示名
あ
編集

ユーザー向けの説明
あ
編集

説明
あ
編集

範囲
ファイルと他のデータ資産、メール、会議
編集

アクセスの制御
アクセスの制御
編集

コンテンツのマーキング
なし
編集

ファイルとメールの自動ラベル付け
なし
編集

ミーティングの設定
編集



6. 導入手順③ DLP for Microsoft 365 Copilot で 利用データを制御

6.1. DLP for Microsoft 365 Copilot とは

DLP for Microsoft 365 Copilot は、機密情報の入力や参照を保護し、ポリシー違反を検知・対応する機能です。

① 入力を保護

プロンプトへの機密情報の入力を制限し、違反時はユーザーに警告

ユーザーのプロンプト
この顧客の売上データ
は**1,000 万円**です



ブロック

機密情報を含む

主な制御

- 機密情報の入力を検知・ブロック
- 違反時にユーザーへ警告を表示
- 例外申請の運用をサポート

② 機密情報の参照を制御

ラベルやポリシーに基づき、機密データの参照を制限し、回答に使用させない



Copilot

組織のデータ



機密



機密



参照対象
から除外

主な制御

- 指定ラベルのデータを参照から除外
- 高機密データを回答に使用しない
- ラベルとポリシーで柔軟に制御

③ 違反を検知

違反アクティビティを記録・通知し、管理者が迅速に対応

DLP
ダッシュボード



アラート通知



監査ログ



確認と対応

主な機能

- 違反アクティビティを記録・通知
- レポートで傾向を確認し対応を支援
- 監査ログと連携して統制を強化

機密情報の入力・参照・利用をポリシーで制御

機密情報の漏えいを防止

コンプライアンスを強化

安心して Copilot を活用

6.2. DLP ポリシー作成手順

DLP ポリシーの作成を開始するまでの手順を説明します。

作成開始

カテゴリ

名前設定

適用先

ルール

確認完了

STEP 1 ポリシーの作成を開始する

1. [データ損失防止] から [ポリシー] を開く
2. [ポリシーの作成] をクリックする
3. 保護先を [エンタープライズ アプリケーションとデバイス] に指定する



6.2. DLP ポリシー作成手順

DLP ポリシーのカテゴリとテンプレートを指定する手順を説明します。

作成開始

カテゴリ

名前設定

適用先

ルール

確認完了

STEP 2 カテゴリを指定する

1. [カスタム] から [カスタムポリシー] を選択する

Copilot が特定の種類のコンテンツを処理できないようにするための設定です

2. [次へ] に進む

データ損失防止 > ポリシーの作成

テンプレートまたはテンプレートに関する詳細情報

- 名前
- 管理単位
- 場所
- ポリシーの設定
- ポリシー モード
- 完了

テンプレートの利用またはカスタム ポリシーの作成

業界の規制を選んでその情報の保護に使用できる DLP ポリシー テンプレートを確認するか、一からカスタム ポリシーを作成します。ラベルの付いたコンテンツを保護する必要がある場合は、後でラベルを選ぶことができます。DLP ポリシーのテンプレートに関する詳細情報

① Microsoft 365 Copilot のコンテンツを保護してください。Copilot が特定の種類のコンテンツ (機密ラベルが適用されたファイルなど) を処理できないようにできるようになりました。それを試すには、以下のカスタム ポリシーから始める必要があります。Copilot でのコンテンツの保護に関する詳細情報

テンプレートを検索してください

特定のテンプレートを検索

場所の選択

すべての国または地域

カテゴリ	規制	カスタム ポリシー
拡張		
金融		
医療と保健		
プライバシー		
カスタム	カスタム ポリシー	一からカスタム ポリシーを作成します。保護するコンテンツの種類とそれを保護する方法を選択します。

6.2. DLP ポリシー作成手順

DLP ポリシーの名前と説明を設定する手順を説明します。

作成開始

カテゴリ

名前設定

適用先

ルール

確認完了

STEP 3 名前と説明を設定する

1. [名前] を設定し [次へ] に進む
2. 管理単位は何も追加せず [次へ] に進む

※ Microsoft 365 Copilot を対象とする場合は、**管理単位**を追加しません

データ損失防止 > ポリシーの作成

☒ テンプレートまたはテンプレートに関する詳細情報

☒ 名前

☒ 管理単位

☐ 場所

☐ ポリシーの設定

☐ ポリシー モード

☐ 完了

管理単位を割り当てる

このポリシーを割り当てる管理単位を選択します。管理単位は Microsoft Entra ID に作成され、ポリシーを特定のユーザーまたはグループのセットに制限します。選択内容は、次の手順で利用できる場所のオプションに影響します。

このポリシーをすべてのユーザーとグループに割り当てる場合は、[次へ] を選択して続行します。 [管理単位に関する詳細情報](#)

① 管理単位は、すべての場所でサポートされているわけではありません。管理単位は、Fabric や Microsoft 365 Copilot、Copilot Chat など、一部の場所には適用されません。そのため、ここで管理単位を選択すると、このポリシーのスコープを、次の手順でそれらの場所にスコープできなくなります。

+ 管理単位の追加または削除

管理単位

完全なディレクトリ

6.2. DLP ポリシー作成手順

Copilot を対象とした DLP ポリシーを作成する手順を説明します。

作成開始

カテゴリ

名前設定

適用先

ルール

確認完了

STEP 4 適用先を選択する

1. ポリシーの適用先の一覧を確認する
2. [Microsoft 365 Copilot および Copilot Chat] を有効にする
3. [編集] から対象のユーザーとグループを指定する
4. 必要に応じて他の場所も併せて選択する
5. [次へ] に進む

データ損失防止 > ポリシーの作成

- テンプレートまたはテンプレートに関する詳細情報
- 名前
- 管理単位
- 場所
- ポリシーの設定
- ポリシー モード
- 完了

このポリシーの適用先を選択します

デバイス	スコープに対する位置情報を有効にする
インスタンス	スコープに対する位置情報を有効にする
オンプレミスのリポジトリ	スコープに対する位置情報を有効にする
Fabric ワークスペースと Power BI ワークスペース	スコープに対する位置情報を有効にする
☒ Microsoft 365 Copilot および Copilot Chat	すべてのユーザーとグループ 編集
マネージド クラウド アプリ	スコープに対する位置情報を有効にする
Microsoft Foundry	スコープに対する位置情報を有効にする
ボックス	スコープに対する位置情報を有効にする
Google Workspace	スコープに対する位置情報を有効にする
Dropbox	スコープに対する位置情報を有効にする

戻る 次へ

6.2. DLP ポリシー作成手順

Copilot がナレッジソースを参照する動作をルールで制御する DLP ルールを作成する手順を説明します。

作成開始

カテゴリ

名前設定

適用先

ルール

確認完了

STEP 5 ルールを作成する

1. ポリシー設定の定義で[詳細な DLP ルールを作成またはカスタマイズ]を選択する
2. [ルールを作成]よりルール名を入力し、[条件の追加]で対象とする機密情報や条件を指定する
3. [操作]の[処理の追加]で[Copilot によるコンテンツの処理を制限する]を選択する
4. [ナレッジソースにアクセスしています]を選択し、参照を制限する
5. [インシデント レポート]をオンにし、[メールアラートの送信先]を設定して[保存]する

The screenshot displays the 'ポリシーの設定の定義' (Policy Definition) and 'ルールの作成' (Rule Creation) sections. In the 'ポリシーの設定の定義' section, the option '詳細な DLP ルールを作成またはカスタマイズします' (Create or customize a detailed DLP rule) is selected. A red arrow points from this option to the 'ルール名' (Rule Name) field in the 'ルールの作成' section. In the 'ルールの作成' section, the '条件' (Condition) is set to 'ナレッジソースにアクセスしています' (Accessing knowledge source). The '操作' (Action) is set to 'Copilot によるコンテンツの処理を制限する' (Restrict content processing by Copilot). The 'インシデント レポート' (Incident Report) is turned on, and the 'メール アラートの送信先 (オプション)' (Email alert destination (optional)) is set to '管理者' (Administrator). The '保存' (Save) button is visible at the bottom.

6.2. DLP ポリシー作成手順

設定内容を確認して DLP ポリシーを作成する手順を説明します。

作成開始

カテゴリ

名前設定

適用先

ルール

確認完了

STEP 6 確認と完了

1. 運用目的に応じてポリシーモードを選択する
※テスト運用の場合は [シミュレーション]、本番適用の場合は [強制適用] を選択します
2. [次へ] に進む
3. 設定内容を確認する
4. [送信] してポリシーを作成する

The screenshot shows the '確認と完了' (Review and Complete) step in the Microsoft Purview DLP Policy creation process. On the left, a progress bar indicates the following steps: 'テンプレートまたはテンプレートに関する詳細情報' (selected), '名前', '管理単位', '場所', 'ポリシーの設定', 'ポリシーモード', and '完了'. The main content area is titled '確認と完了' and contains a summary of the policy configuration with '編集' (Edit) buttons for each section:

- 基本設定**
 - 保護対象の情報: カスタム ポリシー (編集)
- 名前**
 - カスタム ポリシー (編集)
- 説明**
 - 一からカスタム ポリシーを作成します。保護するコンテンツの種類とそれを保護する方法を選択します。 (編集)
- 場所**
 - Microsoft 365 Copilot および Copilot Chat (編集)
- モード**
 - シミュレーション モードでポリシーを実行する (編集)
- ルール**
 - 既定 (編集)

At the bottom, there are '戻る' (Back) and '送信' (Send) buttons.

6.2. DLP ポリシー作成手順

作成した DLP ポリシーによって検知されたアラートは、必要に応じて以下の手順で確認します。

作成開始

カテゴリ

名前設定

適用先

ルール

確認完了

補足 アラートの確認場所

1. [アラート] を選択し、ポリシーに一致した検知の一覧を表示する
2. 時間範囲・状態・重要度で絞り込み、確認したいアラートを特定する
3. アラートを開き、対象ユーザーと一致したコンテンツを確認する
4. 内容を確認し、必要に応じて対応したうえで状態を [解決済み] に更新する





7. 導入手順④ 監査で Copilot 利用状況を可視化

7.1. 監査の役割

監査は Copilot の利用履歴を記録し、「誰が・いつ・どのアプリで・何を参照したか」を可視化します。

概要

Copilot の利用履歴から確認できる主な情報

項目	記録される内容	何がわかるか
ユーザー・日時	Copilot を実行したユーザーと操作日時	利用実態の把握、調査の起点
利用アプリ	Teams ・ Word ・ Outlook など操作元のアプリ	どの業務で使われているか
参照リソース	応答に参照したファイル・サイトと秘密度ラベル	機密情報へのアクセスや過剰共有の検知
会話・メッセージ情報	メッセージ ID、会話 ID、プロンプト種別などのフラグ	会話単位での操作の追跡
エージェント・プラグイン	利用したエージェントや接続プラグインの情報	拡張機能の利用状況の統制



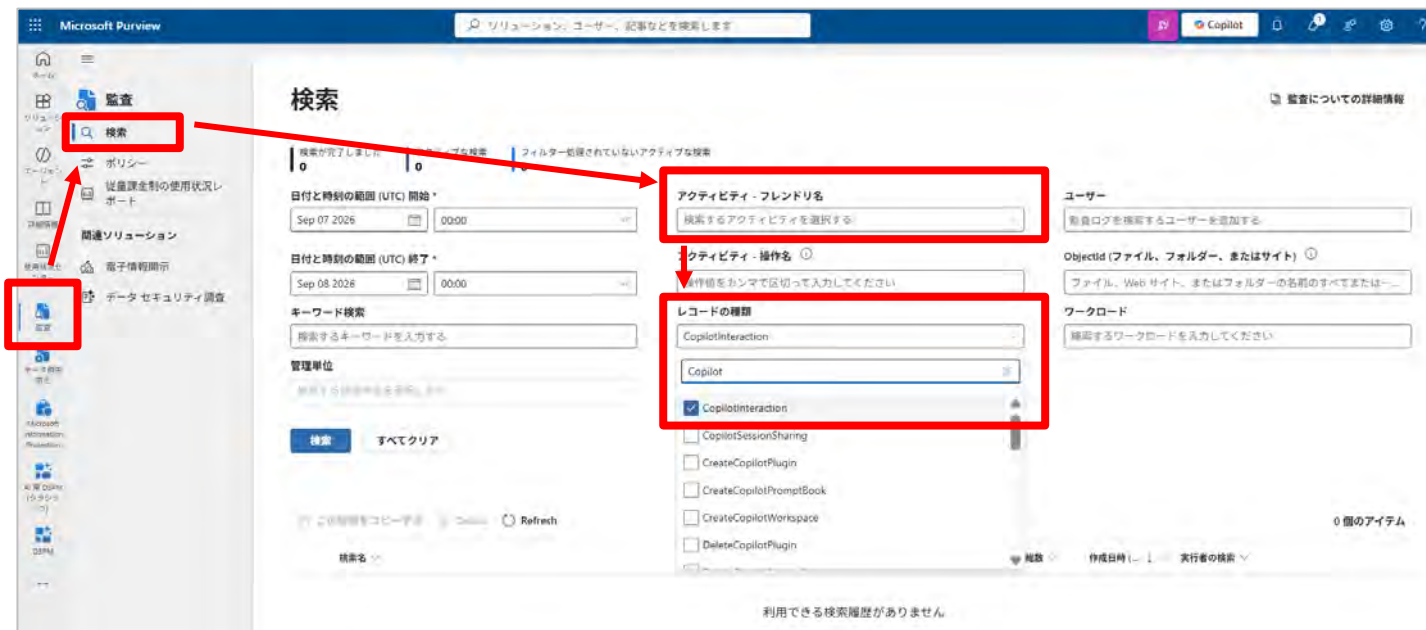
監査ログでは利用履歴を確認できますが、プロンプトや応答本文の確認には電子情報開示が必要です。
※保存状況や保持設定によって取得可能な範囲は異なります

7.2. 監査検索手順

このページでは、監査の検索画面で Copilot 関連イベントを絞り込む手順を説明します。

手順 検索条件を指定して検索

1. [監査] から [検索] を開く
2. 検索する期間を指定する
3. アクティビティから Copilot 関連イベントを選択する
4. 対象のユーザーやレコードの種類で絞り込む
5. [検索] を実行して結果を確認する





8. 導入手順⑤ 電子情報開示で Copilot の調査対応

8.1. 電子情報開示とは

監査ログでは確認できないプロンプトや応答本文も、電子情報開示を利用することで検索・収集・レビュー・保全できます。

① 検索・収集

Copilot の対話履歴を検索し、関連データを収集します。



ポイント

- プロンプトと応答を検索
- ユーザー・期間で絞り込み
- 参照ファイルも収集

主な機能

-  **対話履歴の検索**
条件を指定して検索
-  **コンテンツ収集**
メールやファイルを収集
-  **証跡の収集**
参照元もまとめて収集

② レビュー・法務対応

ケース単位で管理し、レビューと分析を行います。



ポイント

- ケース単位で管理
- 注釈・タグ付けで分析
- 法務対応を支援

主な機能

-  **ケース管理**
対象範囲と権限を設定
-  **レビュー・分析**
注釈やタグ付け
-  **エクスポート**
証拠として出力

③ 証拠保全

メールボックスに保全設定を適用し、証拠を保持します。



ポイント

- Legal Hold で保全
- 削除・改変を防止
- 調査完了まで保持

主な機能

-  **Legal Hold**
保全設定を適用
-  **削除・改変の防止**
操作変更を防止
-  **保全期間の管理**
調査完了まで保持

8.2. ケース作成手順

電子情報開示のケース一覧から作成を開始する手順を説明します。

ケース一覧を開く

ケースを作成

ソースを追加

クエリを実行

STEP 1 ケースの作成を開始する

1. [電子情報開示] から [ケース] を開く
2. 既存のケース一覧を確認する
3. [ケースを作成] に進む



8.2. ケース作成手順

電子情報開示のケースを作成するために、ケース名と詳細設定を行う手順を説明します。

ケース一覧を開く

ケースを作成

ソースを追加

クエリを実行

STEP 2 新しいケースを作成する

1. ケース名を入力する
2. ケースの説明を入力する
3. [詳細設定] のオプションを確認する
※ 電子情報開示 (Premium) を有効にすると、高度な検索・分析機能を利用できます
4. [作成] をクリックする
5. 作成後にメンバーとアクセス権を設定する

ケース

● セキュリティリスクを調査したり、危険な...

ケースを作成 一覧のエクスポート

ケース名

新しいケース

ケース名 *

ケースの一意の名前を入力してください

ケースの説明

ケースの説明を入力

▼ 詳細設定 (オプション)

電子情報開示 (Premium)

検索可能なクエリ条件、ファイルによる検索、秘密度の種類などのプレミアム機能を使用するには、電子情報開示 (Premium) を有効にします。

作成

8.2. ケース作成手順

作成したケースに調査対象のソースを追加し、検索範囲を決める手順を説明します。

ケース一覧を開く

ケースを作成

ソースを追加

クエリを実行

STEP 3 検索対象のソースを追加する

1. [検索の作成] にて名前を入力し、[ソースの検索] を開く
2. 検索対象を選択する
※ 対象ユーザーを指定するか、ケース内のすべてのソースを選択できます。
3. [メールボックスとサイト(既定)] など、含める範囲の種類を選択する
4. [検索] で該当するソースを表示し、[追加] でケースに登録する



8.2. ケース作成手順

作成したケースに調査対象のソースを追加後、クエリを実行します。

ケース一覧を開く

ケースを作成

ソースを追加

クエリを実行

STEP 4 ソース追加後、クエリを実行する

1. [クエリの実行] を選択し、指定した条件で検索結果が取得できることを確認する





9. 導入手順⑥ インサイダーリスク管理・コミュニケーションコンプライアンスでリスクを検知

9.1. インサイダーリスク管理でリスク行動を検知

インサイダーリスク管理では、リスクの高いユーザー行動を検知し、優先度をつけて対応します。

検知対象

インサイダーリスク管理はユーザーの機密情報の大量取得と異常な AI 利用を検知する



機密情報の大量取得

短時間の大量ダウンロードなど、通常業務から外れた取得行動を検知できます。

ポイント

- 短時間の大量ダウンロードを検知
- ラベル付きデータの持ち出しを把握
- 退職予定などの条件と組み合わせ可能
- アラートは重要度別に振り分け



異常な Copilot 利用

普段と異なる Copilot の使われ方を検知し、リスクスコアで優先度を判断できます。

ポイント

- 通常と異なる Copilot 利用を検知
- リスクスコアで対応優先度を判断
- アラートから調査へ連携できる
- 対応状況はケースとして記録

確認手順



Purview ポータル

インサイダーリスク管理を開く



アラート

検知されたアラートを確認する



ユーザー

対象ユーザーのリスクを確認する

※確認するには、対象のアカウントに [インサイダー リスク管理] のロールグループ割り当てが必要です

9.2. コミュニケーションコンプライアンスでやり取りを検知

コミュニケーションコンプライアンスでは、やり取りの内容を対象に違反を検知します。

検知対象

コミュニケーションコンプライアンスが検知する違反の内容



不適切なプロンプト

ハラスメントや不適切な表現を検知し、Copilot への入力内容も対象にできます。

ポイント

- ハラスメントや不適切表現を検知する
- Copilot への入力内容も対象になる
- 検知条件はポリシーで定義する
- 対象ユーザーの範囲を指定できる



ポリシー違反

機密情報の共有や社内規程への違反を検知し、レビューと記録につなげます。

ポイント

- 機密情報の共有や規程違反を検知する
- レビュー担当者へ通知される
- 対応状況を記録として残せる
- 傾向はレポートで確認できる

確認手順



Purview ポータル

コミュニケーションコンプライアンスを開く



ポリシー

検知条件と対象範囲を設定



アラート

検知内容をレビューし対応

※確認するには、対象のアカウントに [コミュニケーション コンプライアンス] のロールグループ割り当てが必要です



10. Copilot ・ Purview の ライセンス

10.1. Copilot と Purview のライセンス体系

Copilot 活用に関連するライセンスの違いと、目的に応じた構成例を整理します。

1

基本構成

小規模・段階導入向け

Microsoft 365 E3
+
Microsoft 365 Copilot

利用可能な機能

- 秘密度ラベル（手動）
- データ損失防止（DLP）
- 監査

まずは基本的なガバナンスを確立したい
組織に適した構成です

2

標準構成

全社展開向け

Microsoft 365 E5
+
Microsoft 365 Copilot

E3 に加え、利用可能な機能

- 秘密度ラベル（自動）
- Teams の DLP
- 監査 Premium
- 電子情報開示 (Premium)
- DSPM（データリスクの可視化）

自動化や高度な検索により、
より強固なガバナンスを実現できます

3

AI ガバナンス構成

強固なガバナンス向け

Microsoft 365 E5
+
Microsoft 365 Copilot
+
Purview 追加ライセンス

追加ライセンスで利用可能な主な機能

- インサイダー リスク管理
- コミュニケーション コンプライアンス
- エージェント管理

AI エージェント利用時に必要な、
強固なガバナンス機能を利用できます

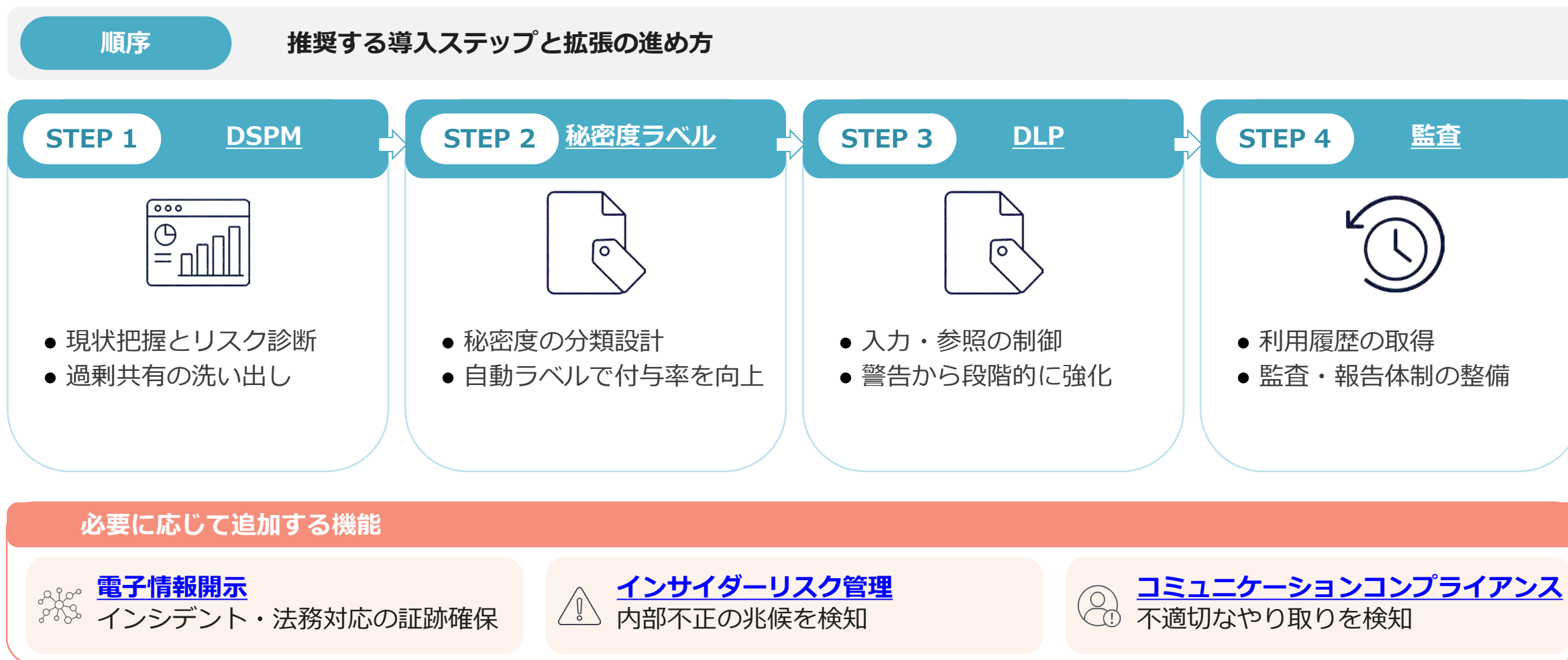
※本スライドは代表的な構成例です。実際のライセンス要件は機能ごとに異なるため、[最新のライセンスガイド](#)をご確認ください。



11. 運用・管理ベストプラクティス

11.1. 推奨導入順序

リスクの把握から着手し、段階的に統制範囲を広げる順序を推奨します。



11.2. よくある失敗例と対処

導入現場で繰り返し発生する失敗例と対処を、事前に押さえておきます。

注意点

導入現場で繰り返し発生する失敗例と対処

01 導入後に過剰共有へ気付く



- 展開前の診断を実施していないケース
- 対処①：DSPM で事前診断を行う
- 対処②：改善対象に優先順位をつける

02 ラベル未整備



- 分類基準が定義されていないケース
- 対処①：4 段階のラベル設計から着手
- 対処②：自動ラベルで付与率を上げる

03 DLP 未実装



- 入力制御がないまま利用を開始
- 対処①：警告モードから段階的に適用
- 対処②：例外運用も併せて設計する

04 監査未確認



- 調査時にログが残っていないケース
- 対処①：監査ログの有効化を初期に確認
- 対処②：保持期間を要件に合わせる