【Microsoft Purview】
データ損失防止（DLP）設定手順

2026年2月27日

改訂履歴

版数	発行日	改訂内容
第1版	2026年2月27日	初版発行

本資料の内容は 2026/2/27 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. 本書の目的とゴール
    2. 用語集
2. 設定作業の全体概要
    1. 全体構成の概要
    2. 設定における各要素の役割
3. 作成するDLPポリシーの前提
    1. シナリオ概要
    2. DLPの動作
    3. 作成するDLPポリシー概要
4. DLPポリシー設定手順
    1. 設定手順概要
    2. 前提条件・事前準備
    3. 手順1：DLPポリシー作成の開始
    4. 手順2：基本情報・適用範囲の設定
    5. 手順3：検出条件の設定
    6. 手順4：制御の設定
    7. 手順5：設定内容の確認
    8. 手順6：運用開始
    9. 手順7：本番公開
5. DLP設定のトラブルシューティング
    1. DLP設定のトラブルシューティング
    2. シミュレーション結果が 0 件のまま
    3. ブロックされず送信できてしまう

1. 前提情報

1.1. 本書の目的とゴール

目的

本資料では、Microsoft Purview を利用して データ損失防止（DLP）ポリシーを作成・設定・公開するための実践的な手順を理解することを目的とします。
必要な事前準備、実際の設定手順を通じて設定作業の流れや確認ポイントを習得し、業務影響を抑えた初期導入ができることを目指します。

ゴール

本資料を学ぶことで、 Microsoft Purview DLP の設定作業を正しく理解し、設定時に発生するトラブルへの対応にも活かせる知識を身につけることを目指します。

1. **設定作業に必要な事前準備や前提条件の整理**
2. **Microsoft Purview ポータルを用いた DLP ポリシー作成の実践**
3. **本番適用前にシミュレーション結果を確認し設定内容を調整するための観点把握**

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	Outlook	Microsoft 365 に含まれるメール／予定表／連絡先管理のアプリケーション。 Exchange Online と連携してメールを送受信し、DLP ポリシーでは メール送信時の検出・制御対象となる。
2	Exchange Online	Microsoft 365 のクラウド型メールサービス。 DLP ポリシーではメール本文・添付ファイルの送信時を対象に、個人情報や機密情報の検出・制御を行う。
3	SharePoint / OneDrive / Teams	Microsoft 365 の情報共有・コラボレーションサービス。 SharePoint：チームや組織内でのファイル・サイト共有 OneDrive：個人用のクラウドストレージ Teams：チャット、会議、ファイル共有を統合したコラボレーションツール DLP ポリシーでは、ファイルの保存・共有・外部共有などが検出・制御対象となる。
4	ポリシー ヒント	DLP ポリシーに一致した操作を行おうとした際に、ユーザーに表示される注意喚起メッセージ。 誤送信防止やユーザー教育を目的として利用され、表示文言はカスタマイズできる。
5	エンドポイント DLP	PC（Windows、macOS など）のデバイス上の操作を対象とする DLP 機能。ローカルファイルのコピー、USB への保存、印刷など、Microsoft 365 以外の操作も含めて情報漏えい対策を行う。
6	Exact Data Match（EDM）	事前に登録した実在するデータ（顧客番号、社員番号など）と完全一致した場合に検出する仕組み。 通常のパターン検出よりも誤検知を大幅に減らせるため、高精度な DLP ポリシーが必要な場合に利用される。
7	Edge for Business ブラウザー	組織管理向けに最適化された Microsoft Edge。DLP ポリシーと連携し、管理されていないクラウド アプリへのデータ送信など、Web 経由の情報漏えいを制御できる。
8	個人情報（PII）	特定の個人を識別できる情報（Personally Identifiable Information）の総称。 例：氏名、住所、電話番号、メールアドレス、銀行口座番号など。

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
9	個人情報保護法	日本における個人情報の取扱いを定めた法律。Microsoft Purview の DLP テンプレートでは、この法律を考慮した個人情報・要配慮個人情報・特定個人情報などの検出ルールが提供される。
10	Microsoft Entra ID	Microsoft のクラウド型 ID・アクセス管理サービス。ユーザー、グループ、アプリケーションの管理を行い、DLP ポリシーでは適用対象ユーザーやグループの判定基盤として利用される。
11	グローバル管理者権限	Microsoft 365における最上位の管理者権限。ユーザー管理、ライセンス管理、セキュリティ、コンプライアンスなど、Microsoft 365 テナント全体のすべての管理機能にアクセスできる。
12	機密ラベル	ファイルやメールに「社外秘」「極秘」といったタグを付与する機能。DLP ポリシーと組み合わせることで、「社外秘ラベルが付いたファイルの送信をブロックする」といった制御が可能になる。
13	分類	特定のパターン（マイナンバー、クレジットカード番号、特定のキーワードなど）を自動で検知する仕組み。DLP は、この分類ルールに基づいて「機密情報が含まれているかどうか」を判断する。

2. 設定作業の全体概要

2.1. 全体構成の概要

本資料では、Microsoft Purview ポータルを用いた **データ損失防止（DLP）の設定手順**を説明します。
本章では、DLP 設定の全体構成および各構成要素の役割について整理します。

DLP 設定の全体構成

DLP 設定は以下4つの工程で構成されます。本書では、全体の流れを踏まえつつ、実際の設定作業にあたる②～④の工程を中心に解説します。

1. 設計内容の整理	2. ポリシー作成	3. シミュレーション	4. 本番公開
DLP ポリシーの目的を明確にし、保護対象となるデータや適用範囲を定義します。 ポリシー設計の前提条件を整理する工程です。	設計内容に基づき、検出条件を設定し、ブロックや通知などの制御内容を構成します。 監視・レポート設定を含め、実効性のあるポリシーを作成します。	作成したポリシーを本番適用前にシミュレーションします。誤検知や業務影響を確認したうえで、本番適用へ切り替えることが推奨されます。	シミュレーション結果を踏まえて設定内容を確定し、ポリシーを本番適用します。 公開後も監視・レポートを通じて運用状況を継続的に確認し、必要に応じて改善を行います。

設計のポイント

・目的を明確化することが重要
　→ 「何を守るのか」「なぜ守る必要があるのか」を定義しないまま設計すると、検出条件や制御アクションが過剰・複雑になりやすい。
・通知と監視を必ず有効化する
　→ ユーザーへの注意喚起と管理者による状況把握のため、ポリシーヒントによるユーザー通知と管理者向けアラートの設定は有効化が推奨される。

2.2. 設定における各要素の役割

このスライドでは、DLP ポリシー設定に関わる主な構成要素とその役割について整理します。

設定作業の構成要素と役割

カテゴリ	構成要素	役割
管理基盤	**Microsoft Purview ポータル**	Microsoft Purview の各種機能を一元管理する管理画面。DLP ポリシーの作成、編集、テスト、有効化を行う操作起点となる。
ポリシー構造	**DLP ポリシー**	DLP の適用範囲やルールを包括的に管理するための最上位オブジェクト。
	ワークロード設定	DLP を適用するサービスを指定する要素。Exchange Online、SharePoint、OneDrive、Teams など「どこで DLP を効かせるか」を定義する。
	ルール	DLP ポリシー内で実際の検出条件・制御アクションを定義する単位。どの条件で検知し、検知時に何を行うかを具体的に決定する。
	検出条件	DLP ルールを発動させるための判定条件。機密情報タイプ、機密ラベルなどを組み合わせて検知対象を絞り込む。
	機密情報タイプ	DLP で検出する機密情報の種類を定義するもの（例：クレジットカード番号、銀行口座番号など）。
	制御アクション	検出条件に一致した場合に実行される制御内容。ブロック、警告、オーバーライドなどの挙動を定義する。
運用・評価	**ユーザー通知（ポリシーヒント）**	DLP による検知や制御をユーザーに通知する仕組み。操作画面上に警告やガイダンスを表示し、適切な行動を促す。
	インシデント レポート	DLP による検知・制御結果を記録・可視化するための仕組み。違反内容や発生状況を管理者が確認し、監査や運用改善に利用する。
	ポリシーモード	DLP ポリシーの動作状態を制御する要素。テスト、本番有効などのモードを切り替えることで適用影響を調整する。

3. 作成するDLPポリシーの前提

3.1. シナリオ概要

Microsoft Purview DLP の利用シナリオとして「住所や銀行口座情報を含むメールや添付ファイルの外部送信抑止」を例に挙げます。
次章から設定手順をご説明するため、本章では上記利用シナリオにおける DLP ポリシーの概要を整理します。

シナリオ概要

利用者が Outlook（Exchange Online）からメールを作成し、社内宛てに送信するつもりが誤って外部宛（社外ドメイン）に送信しようとします。
そのメール本文または添付ファイルに住所・銀行口座番号などの個人情報が含まれているという、業務で発生しやすいメール誤送信による情報漏えいリスクを対象としたケースを想定します。

メール本文・添付ファイル内容の例

お疲れ様です。
新規取引先の登録にあたり、以下情報を共有します。

【所在地】
東京都〇〇区〇〇 1-2-3
【振込口座】
〇〇銀行 〇〇支店 普通 1234567

以上、登録をお願いいたします。

DLP 利用目的

- 送信前の警告・抑止による、誤送信の未然防止
- 運用改善に必要な情報の取得（検知状況・オーバーライド理由の蓄積）
  → DLP の検知結果を確認し、実際にどのような場面でポリシーが発動しているかを把握します。
  また、オーバーライド（ポリシーに一致しても利用者が理由を入力すれば送信を継続できる仕組み）の理由を蓄積することで、誤検知調整や制御強化（オーバーライド不可への変更等）の判断に活用します。

3.2. DLPの動作

判定するポイント

DLP は宛先や添付ファイルの有無だけで制御せず、メールや添付ファイルの中身（コンテンツ）を評価して判定します。
また、本シナリオでは誤検知を抑えるために単一要素ではなく複数要素の組み合わせで検出します。
・例：住所 “だけ” → 検出の対象外
・例：住所＋銀行口座番号 → 違反として検出

さらに、業務影響を抑えるために外部宛送信時のみ制御対象とします。
・社内宛メールはポリシーの適用対象外

制御方針

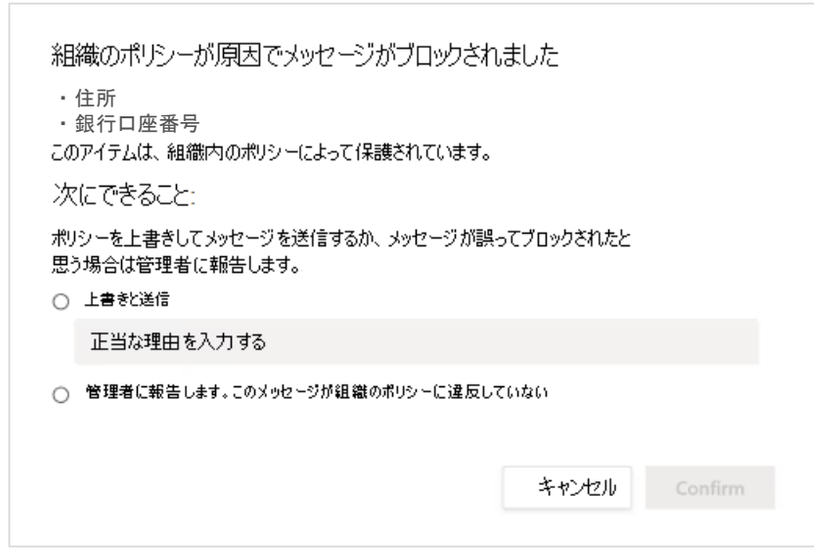
初期導入フェーズでは、初めから最も強い制御であるブロックのみを行うのではなく、弱い制御であるユーザー通知（ポリシーヒント）を中心に、誤送信を抑止します。
本手順で作成する DLP ポリシーは、以下の制御を組み合わせます。

・ユーザー通知（ポリシーヒント）：
メール送信時（送信ボタン押下後）にユーザーへ警告を表示し、送信内容の確認を促す。

・ブロック＋オーバーライド：
送信をブロックするが、必要時は理由入力によりブロックを回避できる。
回避により送信を許可することができ、業務継続が可能。（オーバーライド）

制御によるユーザー体験

ユーザーへは以下の様な画面が表示されます。
・警告が表示され、送信がブロックされる。
・「理由を入力して送信」か「ポリシー違反ではないと報告して送信」のどちらかを選択し実行する。
・または、「キャンセル」より送信を中止する。

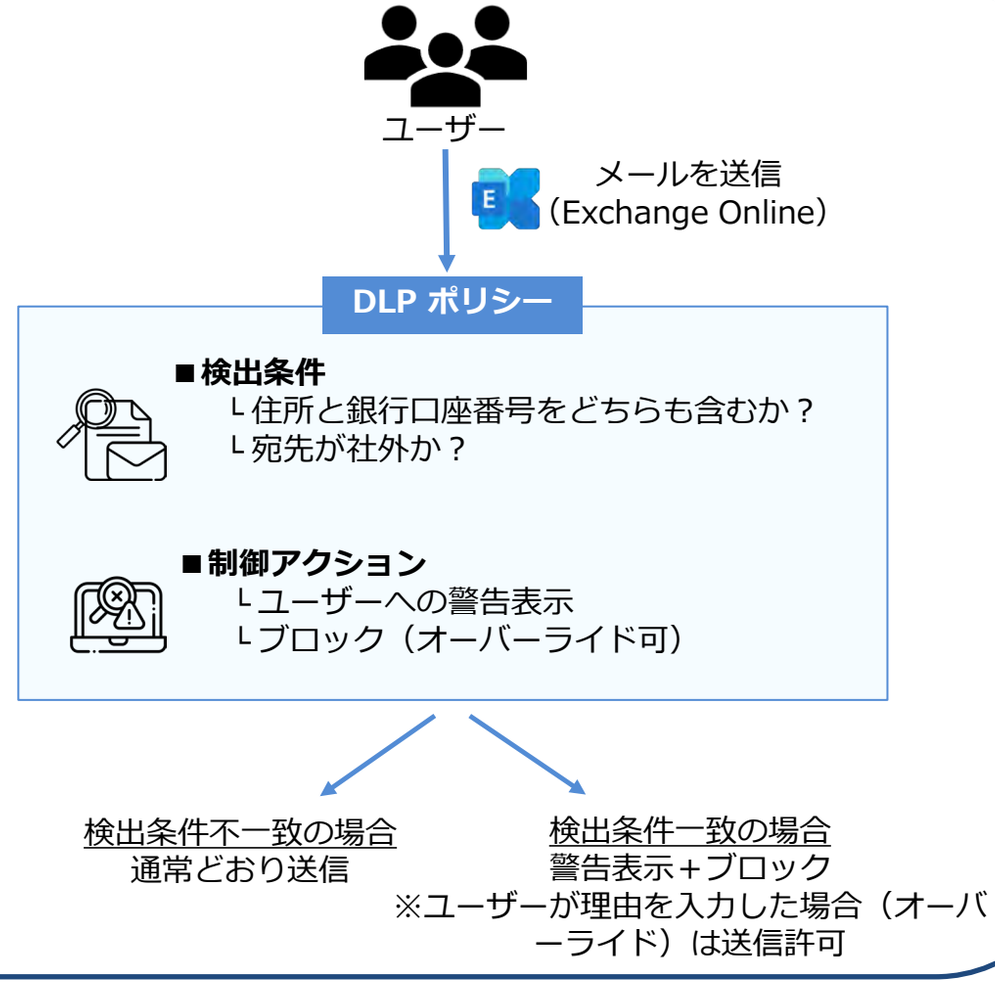


3.3. 作成するDLPポリシー概要

DLP ポリシーの対象や検出・制御内容の概要を整理します。

作成する DLP ポリシー

- **目的**
  住所と銀行口座番号を含むメールの外部送信を抑止する
- **ポリシー名**
  例：住所・銀行口座番号の外部送信抑止（メール）
- **対象サービス（ワークロード）**
  Exchange Online
- **検出条件**
  住所と銀行口座番号の両方を含む場合に検出
  社内宛は対象外とし、外部宛送信時のみ評価・制御
- **制御アクション**
  ユーザー通知（ポリシーヒント）表示＋ブロック（オーバーライド可）



4. DLPポリシー設定手順

4.1. 設定手順概要

以下の図は、設定作業全体の流れを示したものです。
それぞれのステップで必要となる設定内容について、次のスライド以降で詳しくご説明します。

0. 前提条件・事前準備	1. DLP ポリシー作成の開始	2. 基本情報・適用範囲の設定	3. 検出条件の設定	4. 制御の設定	5. 設定内容の確認	6. 運用開始	7. 本番公開
DLP ポリシー作成に必要なライセンスや、権限の準備を行います。	Microsoft Purview ポータルで DLP ポリシーのテンプレートを選択し、ポリシーの作成を開始します。	運用時に判別しやすい名称・目的を明記します。 どの範囲にポリシーを適用するかを確定します。	住所・銀行口座番号などの情報を検出できるよう、検出条件を設定します。	違反を検出した場合に行う制御の内容を設定します。 利用者への警告表示とあわせてブロックやオーバーライドなどの制御を設定し、ポリシーモードを選択します。	検出条件や制御内容が想定どおりに設定できているか、内容を最終確認します。	選択したポリシーモードで運用を開始します。 設定した検出条件や制御内容が想定どおりに機能するかを確認し、必要に応じてポリシー設定を調整します。	その後、本番公開し対象ユーザーに DLP ポリシーを適用します。

DLP ポリシー設定のポイント

- **段階導入が基本**：導入初期は検証用グループ＋シミュレーションモードで影響を最小化
- **単一要素ではなく組み合わせで検出**：住所などの汎用的な個人情報は誤検知が出やすいため、検出要素を組み合わせて設計
- **止めすぎない制御**：ユーザー通知（ポリシーヒント）＋必要時のオーバーライドで業務継続性を確保
- **ポリシー設定を見直し運用改善につなげる**：検知結果やオーバーライド理由を分析し、検出条件調整や制御強化に反映

4.2. 前提条件・事前準備

本手順書の前提条件

- 本手順は、Microsoft Purview ポータルを利用した データ損失防止（DLP）ポリシーの作成を対象とします。
- 対象ワークロードは Exchange Online（メール） とします。
- 本手順は「個人情報（住所・銀行口座番号）」を題材にしますが、機密情報タイプや条件は組織の要件に応じて調整してください。（機密情報タイプの定義一覧はMicrosoft公式サイトを参照ください。）
- 本手順には、以下の内容は含まれません。
    - Exchange Online 以外のワークロード（SharePoint、OneDrive、Teamsなど）を対象とした DLP
    - エンドポイント DLP（USB コピー、印刷、ブラウザアップロードなど）
    - Exact Data Match（EDM）など高度な検出方式

事前準備

1. ライセンスと環境の確認

対象ユーザーに Microsoft 365 E3以上のライセンスが割り当てられ、Exchange Online のメール送受信が利用可能な状態であることを確認します。

※本手順は DLP の初期導入を想定しており、 Exchange Online を対象とした基本的な DLP 設定（Microsoft 365 E3 ライセンスで実施可能な範囲）について記載しています。設定する制御内容やポリシー適用対象（例：Teams、エンドポイント、クラウドアプリ連携、高度な検出方式など）によっては、上位ライセンス（E5 または E5 Compliance 相当）が必要となる場合があるため、要件および対象範囲に応じたライセンスの確認を実施してください。

4.2. 前提条件・事前準備

事前準備

2.管理者権限の確認

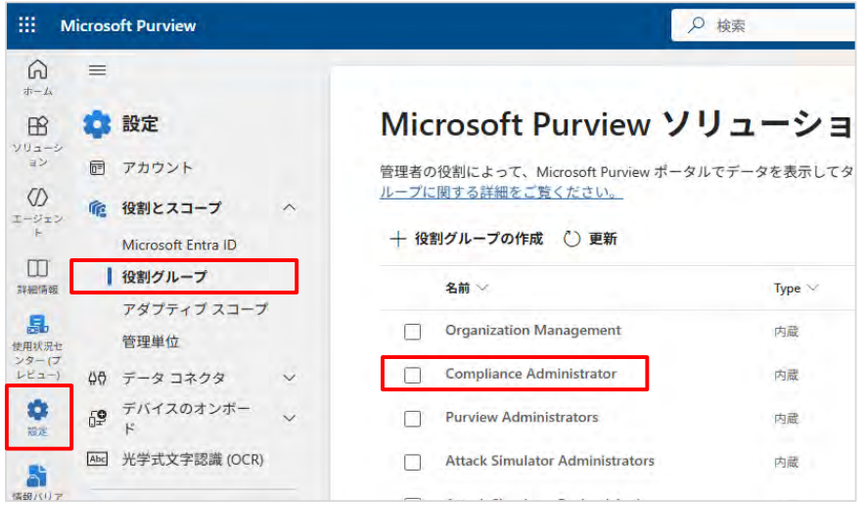
以下のいずれかの条件を満たすアカウントであることを確認します。
権限不足の場合、作成途中でポリシーの保存や公開ができず手戻りになるため、作業前の確認を推奨します。

- グローバル管理者権限を持つアカウント
- Purview 固有の以下のいずれかの役割グループに所属しているアカウント

■Purview 側の役割グループ（一例）

- Compliance Administrator（コンプライアンス管理者）
  → Purview ポータル内で、DLP 設定に必要な権限を含み各ガバナンス機能を広く管理できる役割グループ
- Information Protection Admins（情報保護管理者）
  → Purview ポータル内で、DLP ポリシー、機密ラベルや分類など、情報保護に関連する一部の操作を実行するためのロールを束ねた役割グループ

※ Microsoft Purview ポータルでの権限について詳しくは[Microsoft公式サイト]をご確認ください。



役割グループの確認は、「Purview ポータルの設定 → 役割とスコープ → 役割グループ」から実施します。
役割グループに未所属の場合は、以下手順で割り当てを実施します。

手順

1. Microsoft Purview ポータルにアクセスします。
2. 左側メニューから「設定」を選択し「役割グループ」をクリックします。
3. 役割グループの一覧画面で割り当てたい役割グループを選択します。
   （例：Compliance Administrator）

4.2. 前提条件・事前準備

手順

4. 選択した役割グループの「編集」をクリックします。
5. 「ユーザーの選択」をクリックし、役割グループに割り当てたいユーザーにチェックを入れ「選択」をクリックします。
6. ユーザーが追加されていることを確認し、「次へ」をクリックします。

4.2. 前提条件・事前準備

手順

7. 選択したユーザーが表示されていることを確認し、「保存」をクリックします。
8. 「役割グループを正常に更新しました」の表示を確認し、「完了」をクリックします。

4.2. 前提条件・事前準備

事前準備

3. 適用対象（ユーザー／グループ）の整理

- ポリシーを適用する対象を、全社にするか、特定のユーザー／グループにするかを決めます。
- 特定のグループから小規模で開始する場合は、対象グループをあらかじめ用意しておくと、適用範囲の設定がスムーズになります。

4. 運用方針（制御レベル）の整理

- 送信抑止の強さ（警告／ブロック／オーバーライド可否）を決めます。
- 利用者向けのユーザー通知（ポリシーヒント）に記載する文言方針（注意喚起のトーンや、取るべき行動の案内）を整理しておきます。

4.3. 手順1：DLPポリシー作成の開始

0. 前提条件・事前準備 | **1. DLP ポリシー作成の開始** | 2. 基本情報・適用範囲の設定 | 3. 検出条件の設定 | 4. 制御の設定 | 5. 設定内容の確認 | 6. 運用開始 | 7. 本番公開

Microsoft Purview ポータルにアクセスし、DLP ポリシーの管理画面を開きます。以降の作業はすべて Purview ポータル上で実施します。

手順

1. DLP ポリシーの作成／編集／公開が可能な管理者アカウントで、Microsoft Purview ポータルにアクセスします。
2. 左側メニューから「データ損失防止」を選択し「ポリシー」をクリックします。
3. ポリシー画面で「ポリシーの作成」を選択します。

4.3. 手順1：DLPポリシー作成の開始

手順

4. DLP ポリシーで保護するデータの種類を選択する画面で、「エンタープライズ アプリケーションとデバイス」 を選択します。

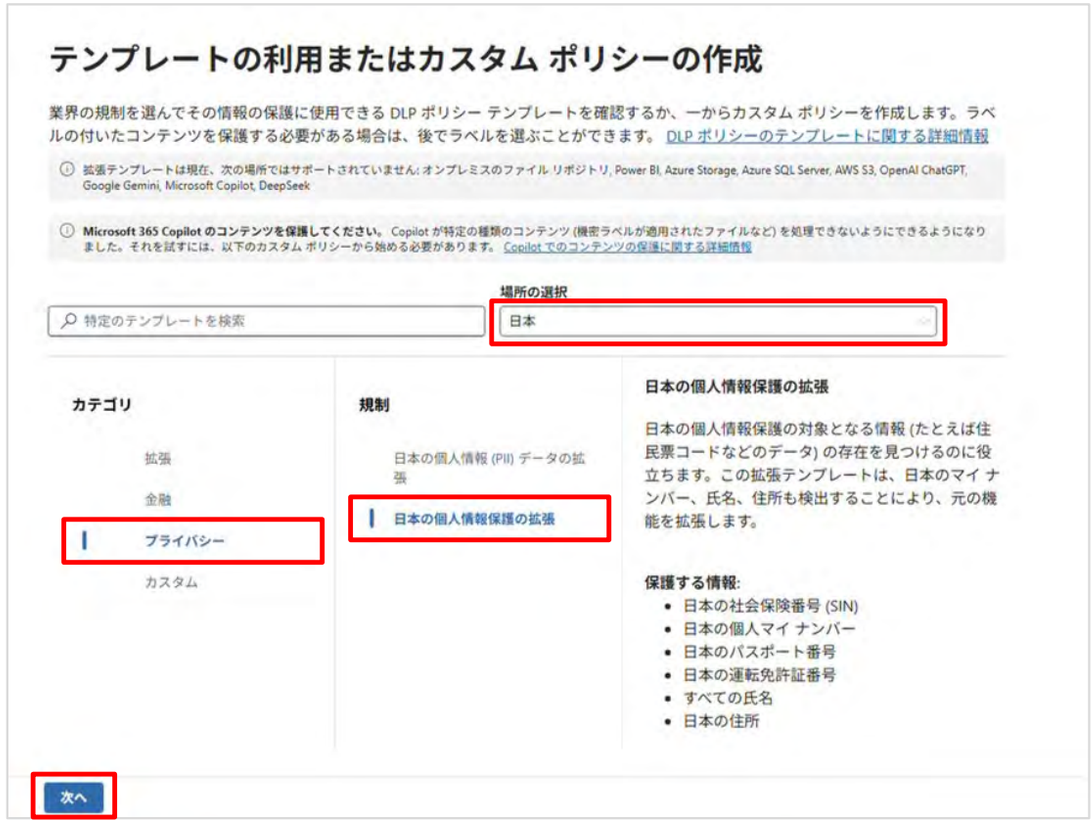
エンタープライズ アプリケーションとデバイス：

Microsoft 365（Exchange、SharePoint、OneDrive、Teams など）のデータに加え、組織内の接続されたソース全体を対象とする DLP ポリシーの種類

インライン Web トラフィック：

Edge for Business ブラウザーやネットワークを経由して送信されるデータ（Microsoft 365 の管理下にないクラウド アプリケーションへの送信など）を対象とする DLP ポリシーの種類

4.3. 手順1：DLPポリシー作成の開始



手順

テンプレートの利用またはカスタムポリシーの作成画面が表示されます。

5. 場所の選択で「日本」を選択します。
6. カテゴリで「プライバシー」を選択し、規制で「日本の個人情報保護の拡張」を選択します。

※テンプレートの名称は、テナントの設定や提供時期により表記が異なる場合があります。一覧に表示されない場合は、テンプレート検索で「個人情報」「プライバシー」などのキーワードを入力して検索してください。

7. 「次へ」をクリックします。

<u>補足：テンプレートの選択について</u>

カテゴリ「プライバシー」には以下2種類のテンプレートが存在します。

・日本の個人情報（PII）データの拡張

氏名や住所などの一般的な個人識別情報（PII）の検出を主な目的としたテンプレートです。

・日本の個人情報保護の拡張

日本の個人情報保護法を考慮し、個人情報に加えてマイナンバーや要配慮個人情報なども対象とした、より包括的なテンプレートです。

本シナリオのルール（住所と銀行口座番号を検出条件として設定する場合）はどちらのテンプレートでも設定可能ですが、将来的な拡張や法令対応を考慮し「日本の個人情報保護の拡張」テンプレートを使用しています。

4.4. 手順2：基本情報・適用範囲の設定

運用時にポリシーを識別しやすいようポリシー名と説明を設定し、DLP の適用範囲を設定します。
説明には、ポリシーの目的・対象（メール）・制御の範囲（外部送信のみ）などの情報を入力すると、運用時や見直しの際にどのようなポリシーかを把握しやすくなります。

手順

1. 名前に、作成する DLP ポリシーの名称を入力します。
   例：住所・銀行口座番号の外部送信抑止（メール）
2. 説明を入力します。
   例：Exchange Online（メール）を対象に、住所・口座番号を含む外部宛送信を抑止する。
3. 「次へ」 をクリックします。

4.4. 手順2：基本情報・適用範囲の設定

手順

管理単位の割り当て画面が表示されます。
このステップでは、DLP ポリシーをどの組織範囲に適用するか（管理単位）を設定します。

4. 管理単位として「完全なディレクトリ」が選択されていることを確認します。

※ 管理単位を利用していない場合や、全社を対象とした DLP ポリシーを作成する場合は、既定のまま変更する必要はありません。

5. 「次へ」をクリックします。

補足：管理単位について

管理単位は Microsoft Entra ID の機能で、DLP ポリシーを特定の組織単位（部署や拠点など）に限定して適用したり、管理者が作成・管理できる範囲やアラート・イベントの可視範囲を組織単位ごとに分割する目的で利用します。
本手順では全社での運用を想定するため、管理単位は既定の「完全なディレクトリ」のまま進め、後続の手順で適用対象を特定のグループに絞り込みます。

4.4. 手順2：基本情報・適用範囲の設定

手順

適用対象ワークロードの選択画面が表示されます。

6. 「Exchange メール」にチェックが入っていることを確認します。
7. Exchange メールの「編集」をクリックします。

他のワークロード（SharePoint、OneDrive、Teams 等）が選択されている場合は、今回の手順ではメールのみを対象とするためチェックを外します。

8. exchange メールのスコープで、適用範囲として「特定のグループ」を選択します。

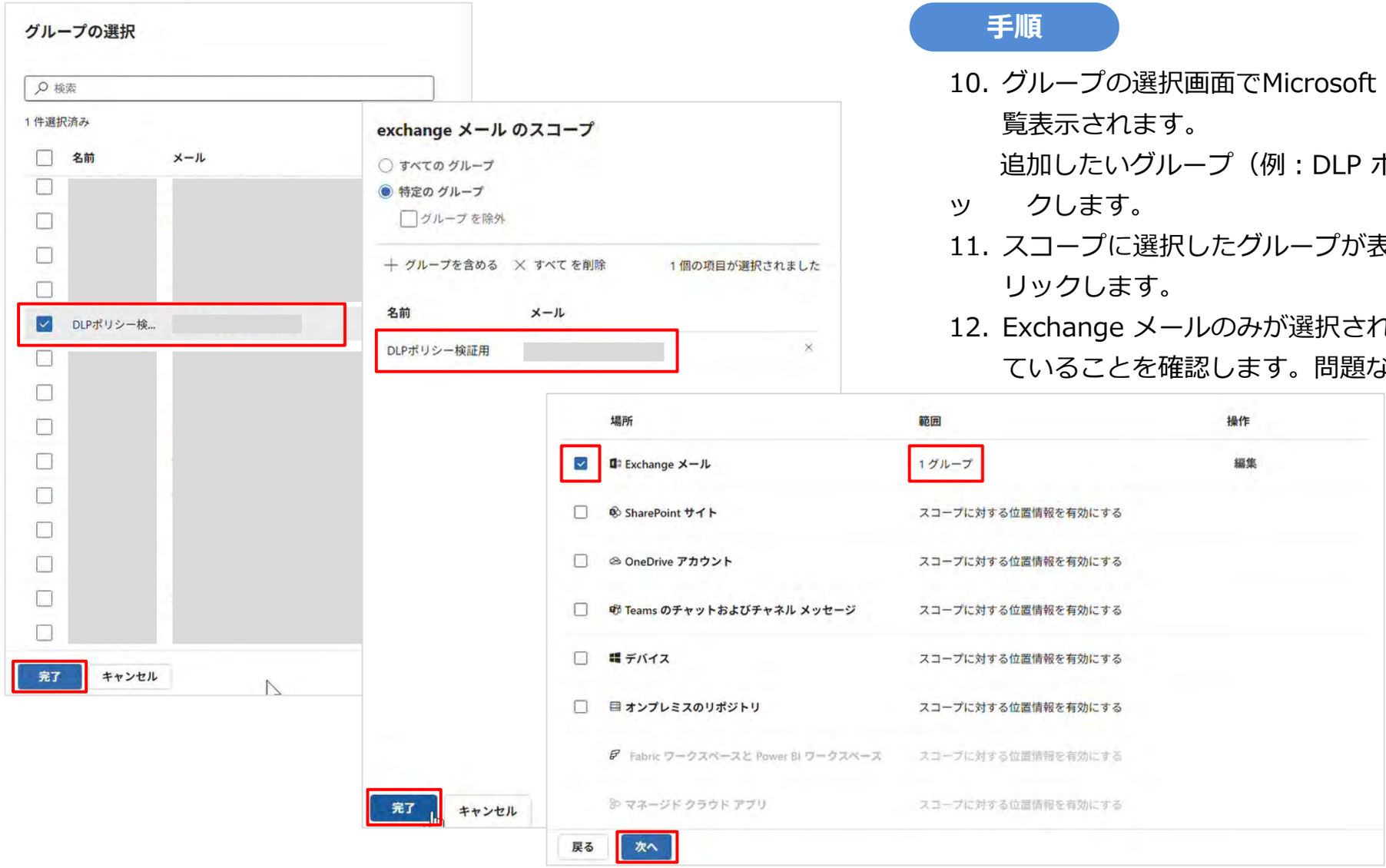
すべてのグループ：管理単位の中で全体を対象に適用する場合に選択
特定のグループ：管理単位の中で特定のグループに所属するユーザーのみに適用する場合に選択

9. 「+グループを含める」 をクリックします。

<u>補足：「グループを除外」オプションについて</u>

「すべてのグループ」を適用対象とした場合に、特定のグループを適用対象から除外するためのオプションです。
今回は「特定のグループ」を適用対象としているため、「グループを除外」は選択できずグレーアウトされます。

4.4. 手順2：基本情報・適用範囲の設定



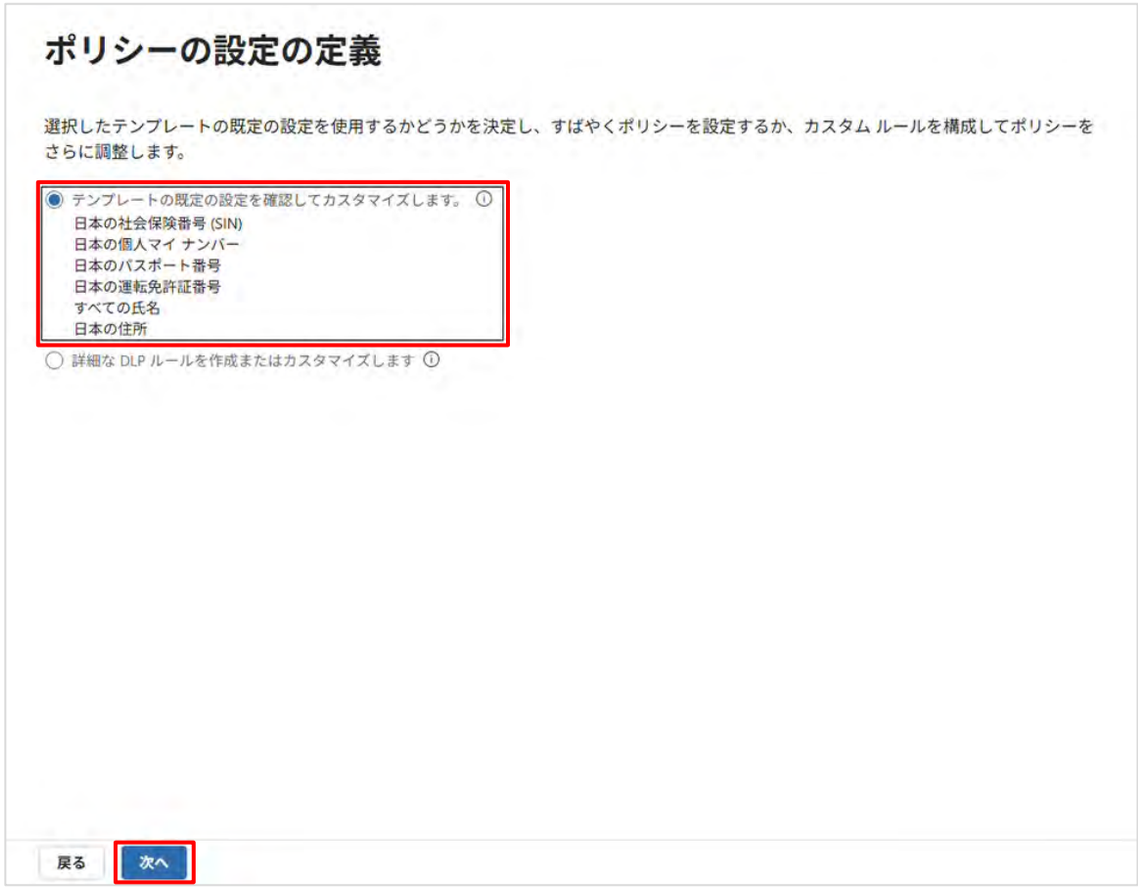
手順

10. グループの選択画面でMicrosoft Entra ID 上で管理されているグループが一覧表示されます。
    追加したいグループ（例：DLP ポリシー検証用）を選択し、「完了」をクリッ　クします。
11. スコープに選択したグループが表示されていることを確認し、「完了」をクリックします。
12. Exchange メールのみが選択され、かつ適用範囲が特定のグループに絞られていることを確認します。問題なければ「次へ」をクリックします。

4.5. 手順3：検出条件の設定

0. 前提条件・事前準備 | 1. DLP ポリシー作成の開始 | 2. 基本情報・適用範囲の設定 | **3. 検出条件の設定** | 4. 制御の設定 | 5. 設定内容の確認 | 6. 運用開始 | 7. 本番公開

住所・銀行口座番号などの情報を検出できるよう、検出条件を設定します。



手順

1. ポリシーの設定の定義画面で「テンプレートの既定の設定を確認してカスタマイズします。」を選択します。

※「詳細な DLP ルールを作成またはカスタマイズします」は、検出条件や制御アクションを一から詳細に設定したい場合に使用する選択肢です。本手順では一般的なシナリオとしてテンプレートの既定設定をベースにカスタマイズするため、「テンプレートの既定の設定を確認してカスタマイズします。」を選択します。

2. 「次へ」をクリックします。

4.5. 手順3：検出条件の設定

手順

保護対象の情報画面が表示されます。

3. 「編集」をクリックします。

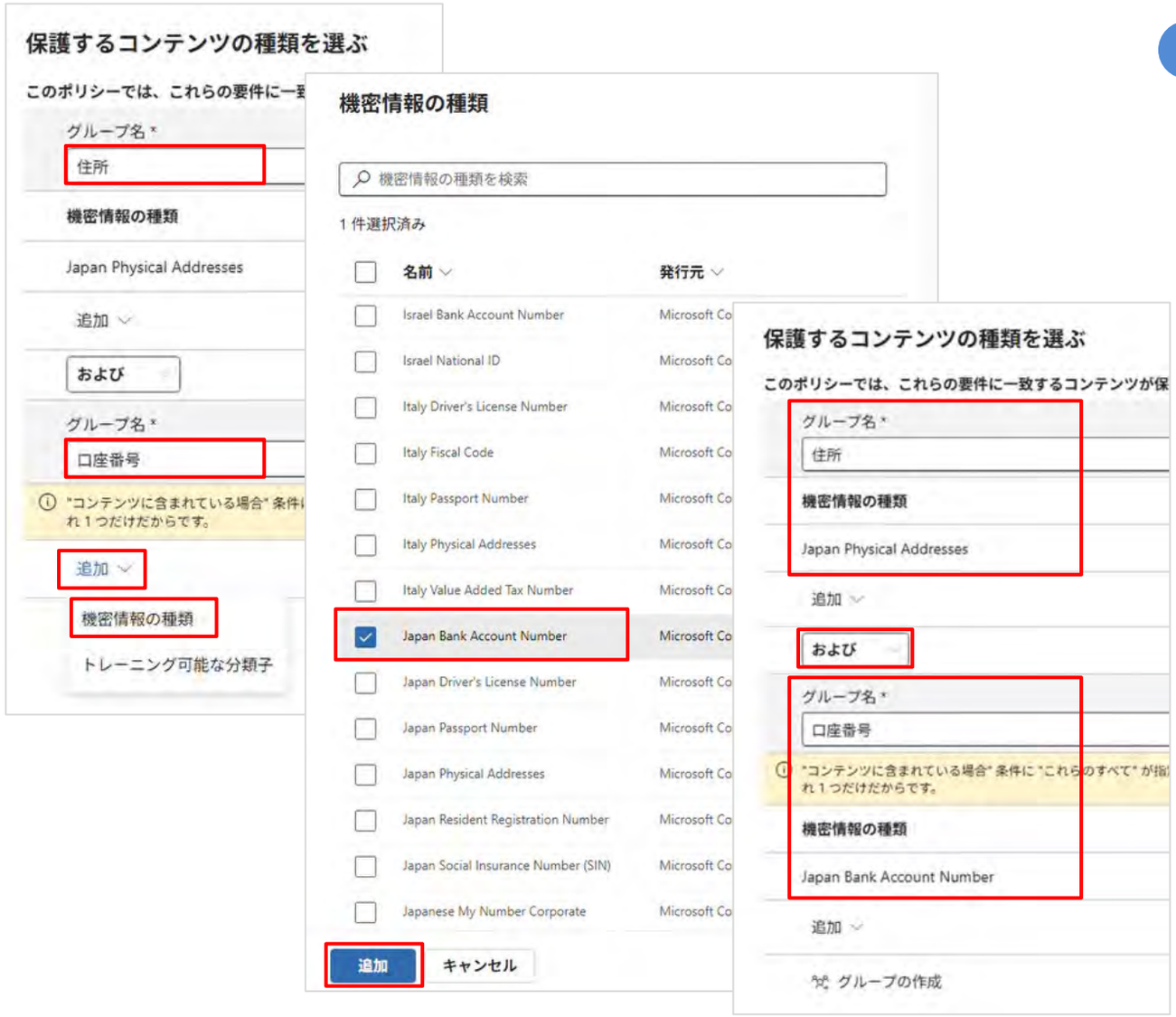
DLP の検出条件は、「グループ」という単位で構成されます。

4. グループの中に既定で複数の機密情報の種類が設定されているため、項目を編集します。

   一覧から「Japan Physical Addresses（住所）」を残し、それ以外の不要な機密情報の種類（社会保険番号、マイナンバー、パスポート番号、運転免許証番号、氏名）を削除（ゴミ箱）アイコンをクリックして削除します。

（後続の手順で銀行口座番号を追加し、住所と組み合わせて検出条件を作成します。）

4.5. 手順3：検出条件の設定



手順

5. グループ名に任意の名称（例：住所、口座番号）を入力します。
6. グループ名「口座番号」に銀行口座番号の機密情報の種類を追加するため、「追加」をクリックして「機密情報の種類」を選択します。
7. 機密情報の種類の一覧から「Japan Bank Account Number（銀行口座番号）」を選択して「追加」をクリックします。
8. 設定した「住所」と「口座番号」がそれぞれのグループで表示されていること、組み合わせの選択肢で「および」を選択できていることを確認します。
   これにより、住所と銀行口座番号の両方を含む場合のみ検出されます。

<u>組み合わせの選択肢</u>

および（AND）：複数の条件をすべて満たす場合に検出されます。
または（OR）：いずれか一方を満たす場合に検出されます。
検出する機密情報の種類を「および」で組み合わせることで、単一要素ではなく複数要素を組み合わせた検出が可能になります。

4.5. 手順3：検出条件の設定

補足：検出条件の設計の考え方

DLP の検出条件は、「グループ」という単位で構成されます。
各グループの中に機密情報の種類を設定し、その組み合わせによって検出ロジックが決まります。

■ ルール判定の基本

1. グループ内の関係：OR ⇒ グループ内のいずれか1つの条件に一致すれば検出されます。
2. グループ間の関係：および（AND）／または（OR）⇒ グループ同士の組み合わせ方を選択できます。

■ 設定例

① 「住所」「銀行口座番号」を同じグループに設定する場合
→ 住所 ”OR” 銀行口座番号（どちらか1つでも含まれていれば検出）

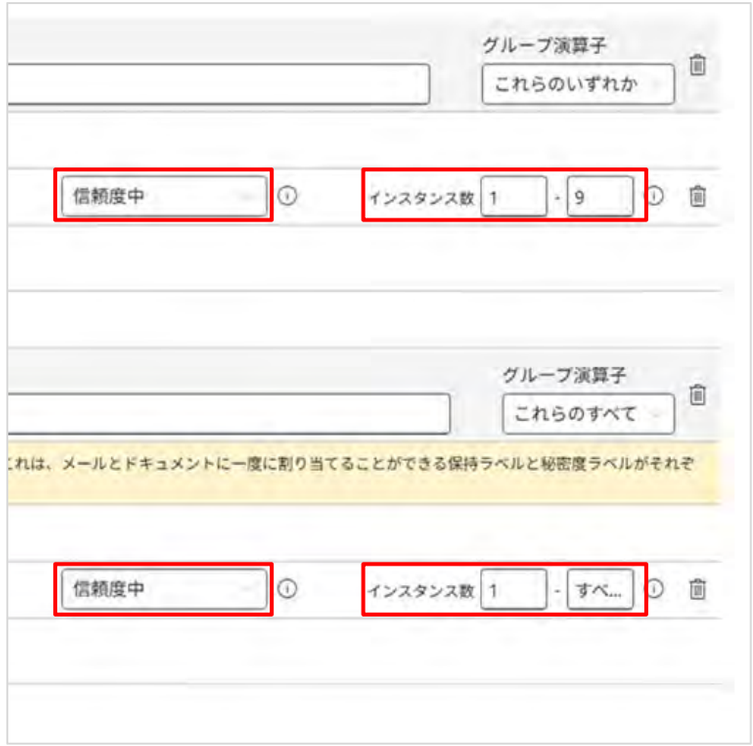
② グループを分けて設定する場合
→ および（AND） を選択：住所 “AND” 銀行口座番号（両方が含まれている場合のみ検出）
→ または（OR） を選択：住所 ”OR” 銀行口座番号（どちらか1つでも含まれていれば検出）

※ OR条件の場合は、「同じグループにまとめる」方法と「グループを分けてORで結合する」方法のいずれでも設計が可能です。
ただし、将来的な拡張（条件の追加や一部条件のみ必須化するケースなど）を考慮すると、要素や目的ごとにグループを分けて設計する方が保守性が高く、推奨されます。

ポイント

・グループ内に複数の機密情報の種類を追加すると、OR条件（いずれか一致で検出）になる。
・複数の条件をすべて満たす場合のみ検出したい場合は、条件を別グループに分け「および（AND）」で組み合わせる必要がある。

4.5. 手順3：検出条件の設定



手順

機密情報の種類の追加が完了したら、画面右側の「信頼度」と「インスタンス数」を設定します。

9. 検出の厳しさ（低／中／高）を選択する信頼度で「信頼度中」を選択します。
10. インスタンス数で最小値を「1」に設定します。最大値は、運用方針に応じて次のいずれかを設定します。
    - 誤検知を抑えたい場合：任意の上限（例：9 など）
    - 上限を設けず1件以上でよい場合：「すべて（Any）」

補足：信頼度とは

・信頼度（低／中／高）は、機密情報が検出されたときに「どの程度確からしい一致か」を表す目安です。

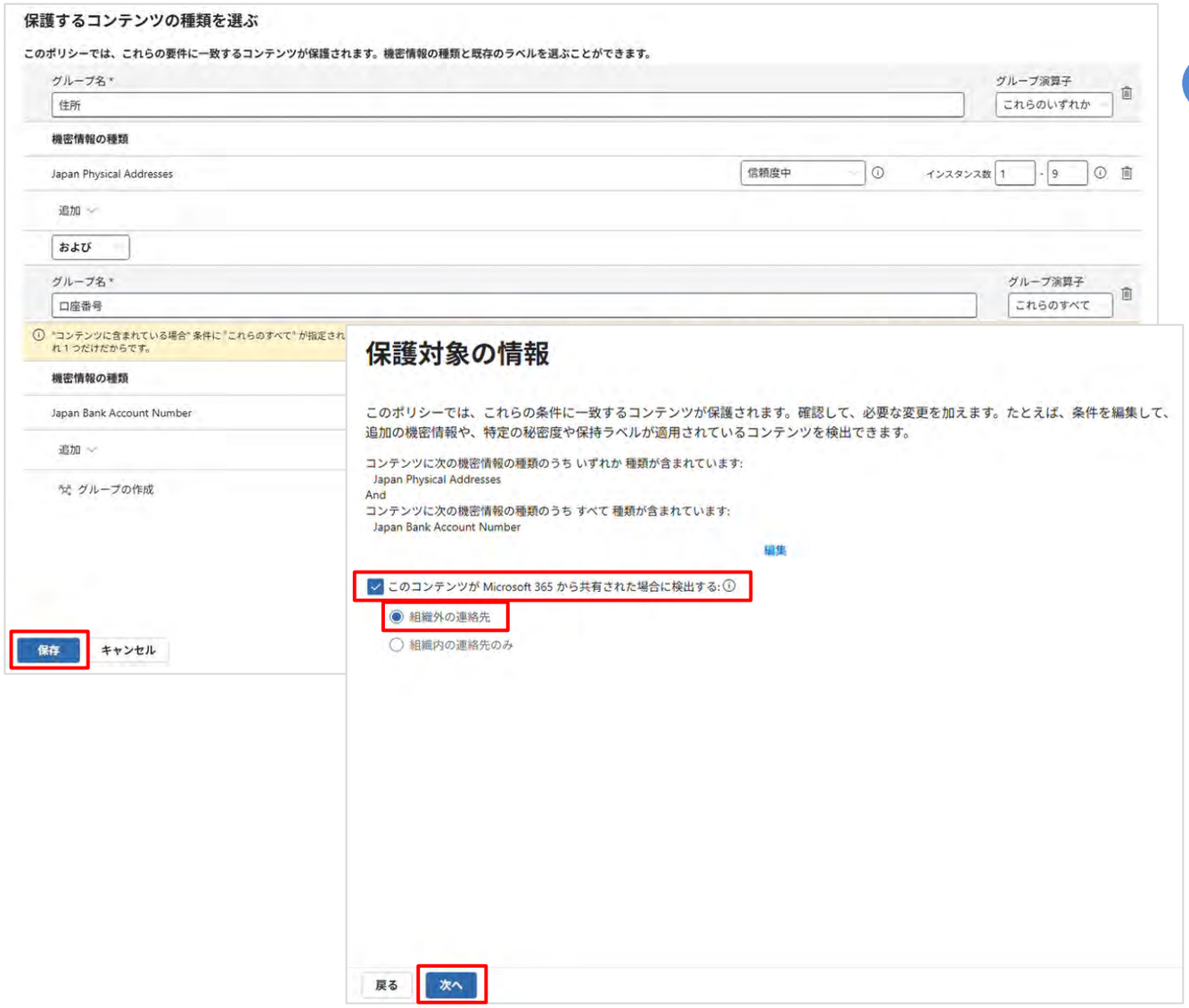
・基本的に信頼度を高くすると誤検知は減る傾向にありますが、検出条件が厳しくなるため、見逃しが増える可能性があります。まずは「中」で設定し、必要に応じて調整することが推奨されます。

補足：インスタンス数とは

・インスタンス数は、同一の機密情報の種類が1つのメール（または1つのファイル）内に何件含まれるかを条件として指定する数値です。

・最小値はルールが一致するために必要な最低件数（1～500）、最大値は許容する上限件数（1～500 または「すべて（Any）」を設定します。

4.5. 手順3：検出条件の設定



手順

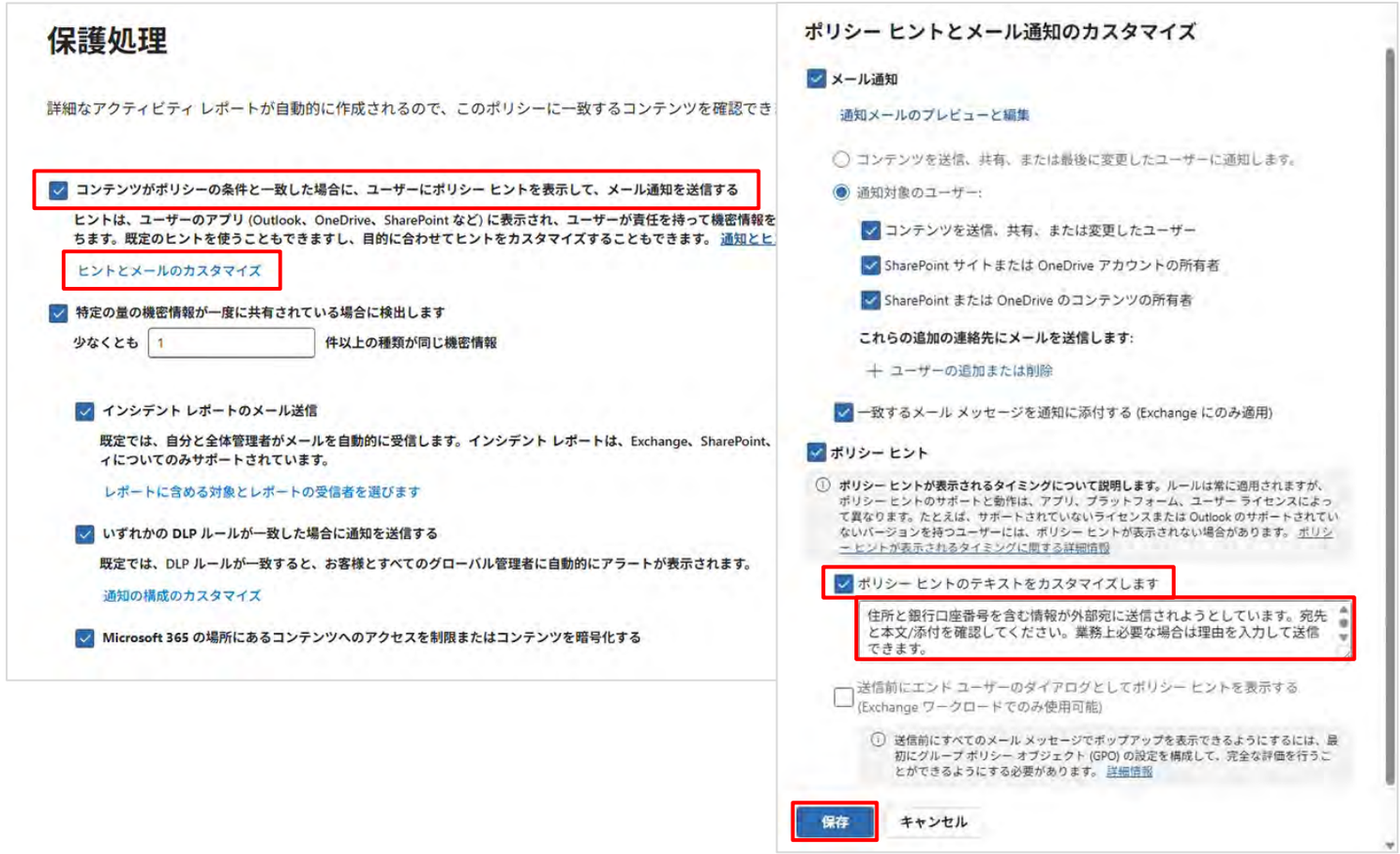
11. 検出条件の設定が問題ないことを確認し、「保存」をクリックして設定を確定します。
12. 「このコンテンツが Microsoft 365 から共有された場合に検出する」にチェックが入っていることを確認し、「組織外の連絡先」を選択します。

この設定により、社内から社外へ送信・共有される場合のみを検出対象とすることができます。

13. 「次へ」をクリックします。

4.6. 手順4：制御の設定

違反を検出した際の制御アクションを設定します。



手順

保護処理の画面が表示されます。

1. 「コンテンツがポリシーの条件と一致した場合に、ユーザーにポリシー ヒントを表示して、メール通知を送信する」にチェックが入っていることを確認します。
2. 「ヒントとメールのカスタマイズ」をクリックします。
3. ポリシーヒントの「ポリシーヒントのテキストをカスタマイズします」にチェックを入れ、ユーザー向けに表示する文言を設定します。

   例：住所と銀行口座番号を含む情報が外部宛に送信されようとしています。宛先と本文/添付を確認してください。業務上必要な場合は理由を入力して送信できます。

4. 「保存」をクリックして元の画面に戻ります。

<u>補足：メール通知について</u>

メール通知は既定で有効となっています。有効の場合、ポリシーに一致したイベント発生時にメール通知が送信されます。通知対象のユーザーを設定できるため、運用方針に合わせて確認・調整してください。

4.6. 手順4：制御の設定

手順

5.　「Microsoft 365 の場所にあるコンテンツへのアクセスを制限またはコンテンツを暗号化する」にチェックを入れ、「次へ」をクリックします。

補足：その他の設定項目について

・特定の量の機密情報が一度に共有されている場合に検出します

1通のメール（または1つのファイル）内に、同一の機密情報の種類が何件含まれるか（インスタンス数）を条件として設定します。

例：「少なくとも 10 件以上」など、目的に応じて件数条件を調整できます

・インシデント レポートのメール送信

ポリシー一致時に、管理者へメールでレポートを送る設定です。

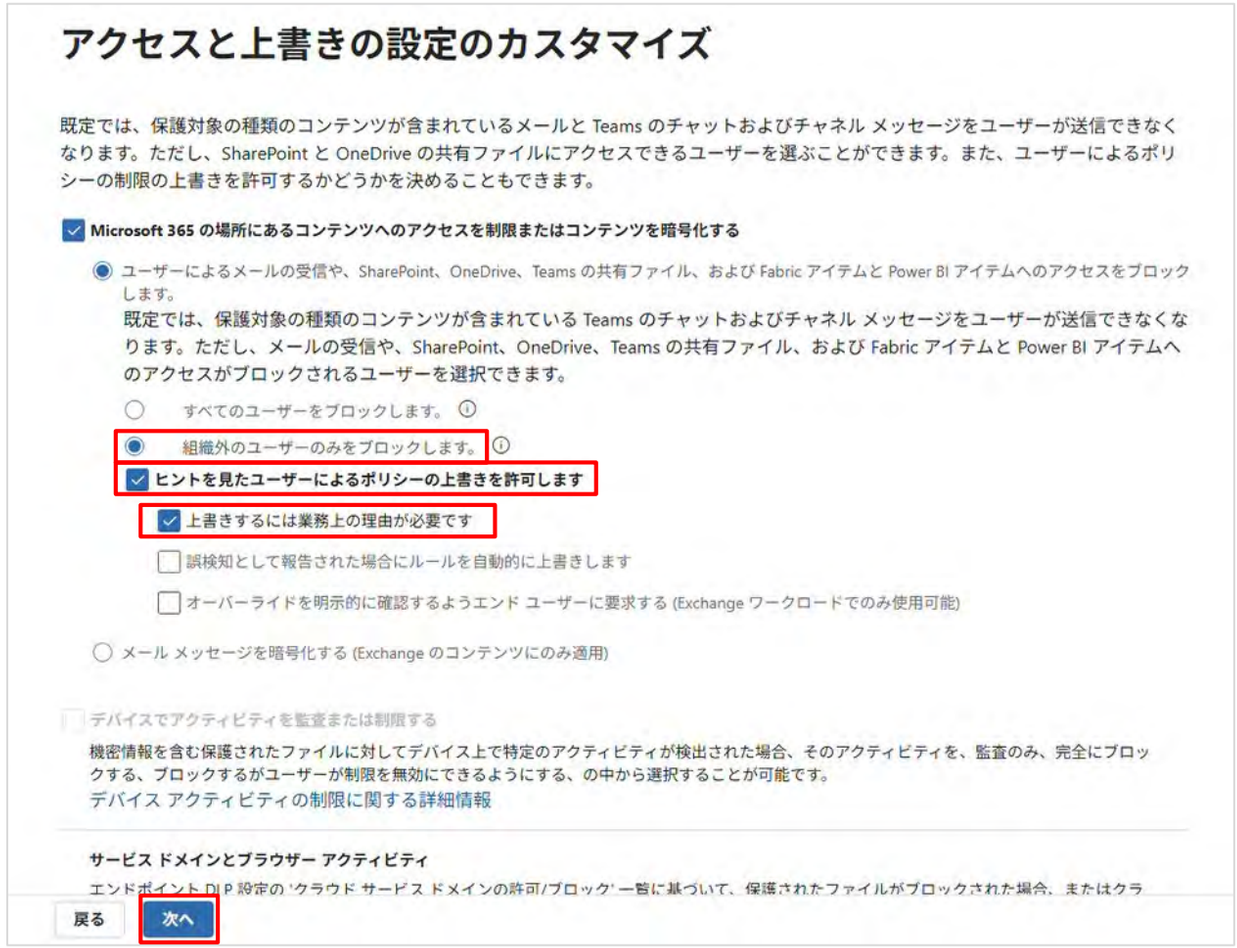
実際のポリシー違反や誤検知の発生状況を把握でき条件を調整しやすくなるため、導入初期は有効化が推奨されます。

・いずれかの DLP ルールが一致した場合に通知を送信する

ポリシー一致時に Microsoft Purview ポータル上で管理者へアラートが表示される設定です。

監視体制がある場合は有効にすると便利ですが、導入初期は誤検知も含めアラートが増える可能性があるため、重要度や頻度を調整しながら段階的に運用することを推奨します。

4.6. 手順4：制御の設定



手順

アクセスと上書きの設定のカスタマイズ画面が表示されます。

前の手順で有効化した「Microsoft 365 の場所にあるコンテンツへのアクセスを制限またはコンテンツを暗号化する」について詳細を設定します。

6. ブロック対象として「組織外のユーザーのみをブロックします。」を選択します。
7. 「ヒントを見たユーザーによるポリシーの上書きを許可します」にチェックを入れます。
8. 「上書きするには業務上の理由が必要です」にチェックを入れます。

上記設定で ブロック＋上書き（オーバーライド）の制御アクションが可能になります。

9. 「次へ」をクリックします。

4.6. 手順4：制御の設定

手順

ポリシーモードの画面が表示されます。

10. 運用方針に合わせてポリシーモードの状態を選択します。

・シミュレーションモードでポリシーを実行する（導入初期に推奨）

ポリシー条件に一致するかどうかを評価しますが、制御アクション（ユーザーへの警告やブロックなど）は実行されません。管理者はシミュレーション結果を確認し、影響範囲を把握できます。

・ポリシーをすぐに有効にする

作成したポリシーが有効になり、設定した制御アクション（ブロック、上書き（オーバーライド）など）がユーザー操作に適用されます。

・ポリシーをオフのままにする

ポリシーは無効の状態で、制御アクションは実行されません。設計中や関係者レビュー中などに使用します。

11. 「次へ」をクリックします。

4.7. 手順5：設定内容の確認

設定内容を最終確認し、ポリシーを作成します。

手順

1. 確認と完了画面で、表示されている設定内容のサマリーを確認します。各項目の「編集」をクリックすると、該当する設定画面に戻り、内容を修正することができます。

   検出条件（住所と銀行口座番号の AND 条件）や、制御内容（ブロック＋上書き（オーバーライド）許可）などが想定どおりになっていることを確認します。
2. 問題なければ 「送信」をクリックします。

   「送信」をクリックすると、DLP ポリシーが作成されます。

4.8. 手順6：運用開始

ポリシーが作成されます。作成後、選択したポリシーモード（シミュレーションモード）での運用を開始します。

手順

1. 「新しいポリシーが作成されました」の表示を確認し、「完了」をクリックします。
2. ポリシー一覧に画面遷移します。作成したポリシーが表示されていることを確認します。
   ポリシーのモード（シミュレーション）が想定どおりになっていることを確認します。

4.8. 手順6：運用開始

補足：シミュレーションモードの活用

シミュレーションモードは、ポリシーを適用した場合の影響を評価しながら、実際の制御アクションは実行しない状態です。
作成したポリシーを選択し「シミュレーションの表示」をクリックすると、シミュレーション結果をダッシュボードで確認できます。

活用方法

シミュレーション結果の一致件数が、想定どおりの範囲かを確認します。

・一致件数が0件の場合

条件が厳しすぎるもしくは運用実態に合っていない可能性があるため、ポリシー設計の目的に合わせて、検出条件（信頼度・インスタンス数・AND/OR）や適用範囲を見直す必要があります。

・一致件数が多すぎる場合

誤検知や業務影響の可能性があるため、条件調整の判断材料として活用します。

ポイント

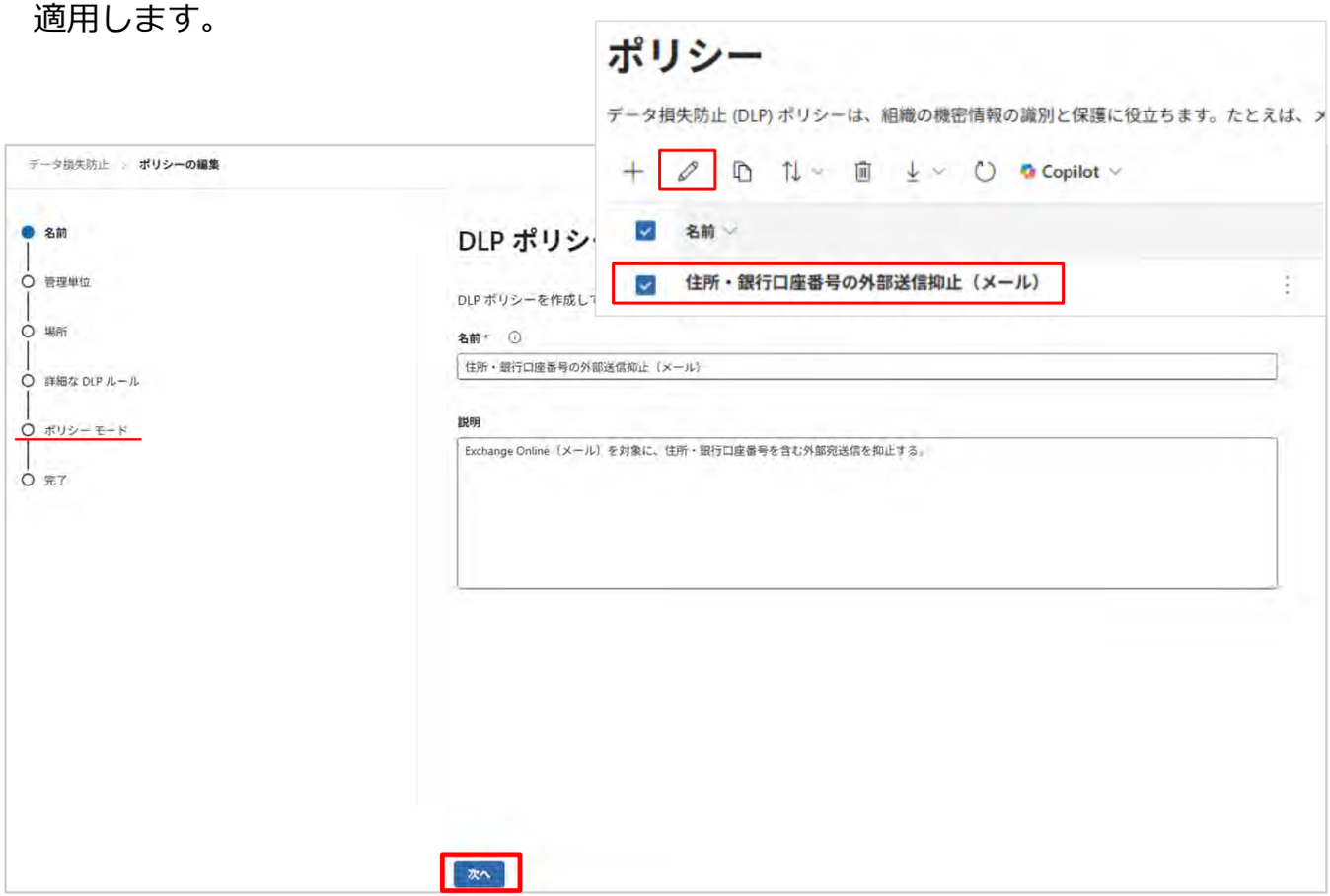
・シミュレーションは最大15日間実行され、結果は30日間保存されます。

・Exchange（メール）は シミュレーション開始後に新しく発生したメールが検出対象であるため、条件に合うメールが送られない場合はシミュレーションの一致件数が0件となります。

※シミュレーションモードについて詳細はMicrosoft公式サイトをご確認ください。

4.8. 手順7：本番公開

シミュレーションモードを経て、DLP ポリシーが想定どおりに機能するかの確認やポリシー設定の調整が完了したら、本番公開し実際にユーザーへポリシーを適用します。



手順

1. ポリシー一覧の画面で作成した DLP ポリシーを選択し、「編集（鉛筆マーク）」をクリックします。
2. 設定画面に遷移します。ポリシーモードをシミュレーションモードから有効に切り替える必要があるため、設定画面の「次へ」をクリックして「ポリシーモード」の設定画面まで進みます。

4.8. 手順7：本番公開

手順

3. ポリシーモードの画面で「ポリシーをすぐに有効にする」を選択し、「次へ」をクリックします。
4. 確認と完了の画面で、「作成後、ポリシーを有効にしますか？」が「はい」と表示されていることを確認します。
5. 問題なければ、「送信」をクリックします。

DLP ポリシーの編集が完了し、本番公開されポリシーがユーザーに適用されます。

5. DLP設定のトラブルシューティング

5.1. DLP設定のトラブルシューティング

DLP 設定では、設定ミスや仕様の誤解、反映タイミングなど、さまざまな要因でトラブルが発生する場合があります。
本スライドでは、代表的なトラブルとその初期対応方法を整理しています。
問題が発生した際の確認ポイントとしてご活用ください。

トラブル内容	初期対応方法	補足/参考情報
ポリシーが一致しない（検出されない）	検出条件の設定（機密情報タイプ、AND条件、信頼度、インスタンス数）が厳しすぎないか確認 *1 ポリシーモードで「ポリシーがオフ」になっていないか確認 *2	*1 手順3：検出条件の設定をご確認ください *2 手順4：制御の設定をご確認ください
シミュレーション結果が 0 件のまま	シミュレーション開始後にポリシーが一致するメールを送信しているか確認 組織外の連絡先を条件としている場合、メールの宛先が外部宛てか確認	–
ブロックされず送信できてしまう	ポリシーモードで「すぐに有効化」になっているか確認 制御したい適用範囲のユーザー（組織内/組織外）が正しく選択されているか確認	仕様によりシミュレーション中はブロックなどの制御アクションは発生しません
ユーザー通知が表示されない	保護処理でユーザー通知（ポリシーヒント）が有効になっているか確認 シミュレーション中の場合、シミュレーション中もヒントを表示する設定が有効か確認	–
誤検知が多い（想定外のメールが検出されてしまう）	信頼度を「中→高」に変更・インスタンス数の最小値を引き上げる・AND条件を見直すなどで、検出条件を見直し厳しくする	住所などの汎用的な情報は誤検知が出やすいため、単一要素ではなくAND条件での設定が推奨されます

5.2. シミュレーション結果が 0 件のまま

エラー概要

DLP ポリシーを シミュレーションモードで実行し、「シミュレーションの表示」を確認しても一致件数が 0 件のままで、想定した検出が確認できない。

↓「シミュレーションの概要」タブで
「0件の一致が見つかりました」と表示される。

原因

・検出条件に一致するメールが送信されていない。（Exchangeのシミュレーションは開始後に新しく発生したメール送信が評価対象のため、開始前に送信されたメールは検出対象外）
・条件の絞り込みで組織外の連絡先を指定しているが、実際の送信先が外部宛になっていない。
・検出条件が厳しすぎて一致しない。（例：信頼度「高」、件数条件が過大など）
・シミュレーション実行直後で、評価・集計がまだ反映されていない。

対処法

・［手順4：制御の設定］でポリシーがシミュレーションモードで実行中かを確認する。
・シミュレーション開始後に、条件に合致する操作（例：外部宛メール送信）を実施したかを確認する。
・［手順3：検出条件の設定］で条件が厳しすぎないかを確認し、必要に応じて緩和する。
・シミュレーション実行直後の場合は、少し時間を空けて再度シミュレーションの概要を確認する。（シミュレーションは最大15日間の期間で蓄積される）

5.3. ブロックされず送信できてしまう

エラー概要

DLP ポリシーで「組織外ユーザーのみブロック」を設定したが、
外部宛にメール送信できてしまいブロックが発生しない。

↓違反が検出されず、送信できてしまう。

原因

・ポリシーモードがシミュレーションモードになっている。
・アクセスと上書きの設定のカスタマイズでMicrosoft 365 の場所にあるコンテンツへのアクセスを制限する設定が有効化されておらず、ブロック設定が実際には適用されていない。
・条件設定が成立していない。（設定ミスにより検出条件に一致しない）

対処法

・シミュレーションモードではブロックは発生しないため、ポリシーモードで「すぐに有効化」になっているかを確認する。
・［手順4：制御の設定］で「Microsoft 365 の場所にあるコンテンツへのアクセスを制限またはコンテンツを暗号化する」にチェックが入っていること、「組織外ユーザーのみをブロック」が選択されているかを確認する。
・上記が正しく設定できていてもブロックが行われない場合は、［手順3：検出条件の設定］で組織の用途に合った検出条件を設定できているか、条件を見直す。