

IT 資格 道 場

Microsoft Information Security Administrator (SC-401) 学習用テキスト

予備知識ゼロから合格ラインへ —— 読んで理解する1冊目

無料サンプル(第1章まで)

SC-401 出題範囲(Study guide・Skills measured as of October 28, 2026)準拠
2026年10月版

ご利用にあたって

- このテキストは「IT資格道場」(www.shikaku-doujou.com)の購入者限定テキストのうち、学習用テキストの第1章までを収録した**無料サンプル**です。どなたでもご覧いただけます。
- 無料サンプルも著作物です。転載・改変しての再配布・二次販売はできません。
- AI モデルの学習データとしてのご利用(学習目的の入力・データセット化を含む)はできません。
- 製品版(学習用テキスト・頻出度別ノート・暗記用ノートの3点)は、ご購入者を識別できる透かし入りのPDFとして提供されます。
- 本PDFはスマートフォン・タブレットでの閲覧に合わせたA5版面・文字サイズで組版しています。

目次

この試験の範囲 [overview]

第1章 Implement information protection [1.1/1.2/1.3]

データ分類の実装と管理 [1.1]

Microsoft Purview で秘密度ラベルを実装および管理する [1.2]

Windows、ファイル共有、Exchange の情報保護を実装する [1.3]

サンプルはここまでです

3冊の使い方は、ダウンロード欄の案内を参照してください。

SAMPLE

この試験の範囲 [overview]

SC-401（Administering Information Security in Microsoft 365）は、Microsoft Purview を中心に、Microsoft 365 の情報を守る設定と運用を問う試験です。合格すると Microsoft Certified: Information Security Administrator Associate になります。

- レベル:Intermediate
- 試験時間:100 分
- 合格:1000 点満点の 700 点以上
- 言語:日本語で受験可能

出題範囲は 3 つの分野で、配点はどれも 30～35% です。この教材も同じ順に章を立てます。

分野	配点	内容
1 Implement information protection	30～35%	機密情報の種類、秘密度レベル、Windows・ファイル共有・Exchange の情報保護
2 Implement data loss prevention and retention	30～35%	DLP ポリシー、エンドポイント DLP、保持とレコード管理
3 Manage risks, alerts, and activities	30～35%	インサイダーリスク管理、監査とアラート対応、AI を使う環境のデータ保護

- 準拠する版:2026 年 10 月 28 日時点で測定されるスキルの学習ガイド
- 細目の番号:節の見出しの後ろにある [1.1] のような印
- 注意:製品の画面と名前は変わりやすい点

第1章 Implement information protection

[1.1/1.2/1.3]

この章は、組織のデータを見つけて、分類して、守るまでの道具を扱います。3つの細目に分かれます。

- **1.1:** 分類の道具 (SIT、フィンガープリント、EDM、分類子、OCR)。
- **1.2:** 守りの本体である秘密度ラベル。
- **1.3:** Windows、ファイル サーバー、メールへ広げる仕組み。

SIT (sensitive information type、機密情報の種類) と EDM (exact data match、完全なデータ一致) は、「何がそのデータか」を見分ける道具です。「どう守るか」を決めるのが秘密度ラベルで、暗号化と権限の実体は Azure Rights Management が担います。

データ分類の実装と管理 [1.1]

組織の機密情報の要件を特定し、分類の手段を選ぶ

Microsoft Purview がデータを分類する方法は、次の 3 つです。[^c1-1]

- **手動:** ユーザーが手で付ける。
- **パターン認識:** SIT のように、決まった形を自動で見つける。
- **機械学習:** トレーニング可能な分類子が、例から学習して見つける。

ドキュメントフィンガープリントと EDM は、どちらも最後は SIT の形で DLP ポリシーや自動ラベル付けから使われます。

要件の聞き取りは、次の 3 点で整えます。

- **何を:** データの種類 (カード番号、社員番号、契約書)。
- **どこで:** 場所 (Exchange、SharePoint、OneDrive、Teams、デバイス)。
- **何から:** 漏えいの経路 (外部への送信、共有、持ち出し)。

この 3 点が決まると、手段がほぼ 1 つに絞れます。

データの特徴	選ぶ手段	理由
国や業界で形が決まった番号 (カード番号、口座番号、各国の ID)	組み込みの SIT	定義済みで、そのまま使える
社内独自の形の番号 (社員番号 AB12345 など)	カスタム SIT (正規表現)	組み込みに無い形
申請書、特許テンプレートなど定型の書式	ドキュメントフィンガープリント	書式の文言そのものが目印
顧客台帳、患者台帳など実在する値の一覧	EDM	台帳の値と一致した時だけ検出する
契約書、財務報告など、形ではなく内容の種類	トレーニング可能な分類子	例を学習して判定する
画像やスキャン PDF の中の文字	OCR (SIT や分類子に加える)	画像から文字を取り出す

分類の結果が使われる先は、次の 7 つです。[^c1-1]

- DLP ポリシー
- 秘密度ラベル
- 保持ラベル
- 自動ラベル付けポリシー
- Insider risk management

- Communication compliance
- Microsoft Priva

間違えやすいのは EDM と通常のカスタム SIT の使い分けです。「9桁の数字」のように形だけで検出したいなら、カスタム SIT で足ります。「顧客台帳に実在する番号だけ」を拾って誤検知を減らしたいなら EDM です。「契約書らしさ」のように形が定まらないものには、どちらも向きません。トレーニング可能な分類子を選びます。

組み込みの SIT の構成 (パターン・主要要素・補強証拠・近接性・信頼度)

SIT は Name、Description、Pattern の 3 項目でできています。Pattern が検出の中身で、4 つの部品から成ります。[^c1-2]

- **主要要素** (primary element): 探したい本体。正規表現 (チェックサムの検証つきも可)、キーワードリスト、キーワード辞書、事前定義の関数のどれか。
- **補強要素** (supporting element): 主要要素が本物らしいことを裏づける証拠。主要要素の近くで見つかるほど、信頼度が上がる。
- **信頼度** (confidence level): 補強証拠がどれだけ見つかったかを表す。低、中、高の 3 段階。
- **近接性** (proximity): 主要要素と補強要素の間に許す文字数。

近接性の読み方は、例で見ると分かります。9桁の番号を主要要素に、「社員番号」というキーワードを補強要素にして、近接性を 250 文字とします。番号の前後 250 文字の窓の中にキーワードが丸ごと入っていれば一致です。窓の端にキーワードが半分かかっているだけでは一致しません。窓が主要要素を中心に左右へ広がることと、キーワードが全体として窓に収まる必要があることが、判断の分かれ目です。[^c1-2]

信頼度の数値は、低が 65、中が 75、高が 85 です。[^c1-3] 高信頼度ほど補強証拠を多く要求するので、誤検知（偽陽性）は最も少なく、見逃し（偽陰性）は最も多くなります。低信頼度はその逆です。低信頼度を指定すると、低・中・高のすべての一致が返ります（中は中と高、高は高だけです）。目安として、高信頼度は件数の少ない条件（5～10 件）に、低信頼度は件数の多い条件（20 件以上）に使います。[^c1-3]

ポリシーが SIT に求める件数は、インスタンス数 (instance count) で指定します。1 つの項目に含まれる重複のない一致数が、Min 以上 Max 以下なら条件を満たします。Min は 1～500、Max は 1～500 か Any で、Any なら Min を満たせば足ります。500 件以上を拾うなら、Min を 500、Max を Any にします。[^c1-6]

場面	調整
誤検知が多すぎて業務が止まる	信頼度を高に上げる、または件数条件を増やす
高信頼度にしたら見逃しが出る	信頼度を中に戻し、誤検知は件数条件を増やして抑える
見逃しを減らしたい調査用の検出	信頼度を低に下げる
少数でも漏れたら困る（1～2 件）	高信頼度と件数 1 を組み合わせる

組み込みの例としてクレジットカード番号の SIT を見ます。形式は 14～19 桁で、Luhn チェックサムを通る必要があり、近接性は 300 文字です。高信頼度（85）は、カード番号の関数に加えて、検証キーワード (cvv2 や security code など)、ブランド名 (visa など)、有効期限の形式のいずれかが近くにあるときです。低信頼度（65）は、関数とチェックサムが通るだけで成立します。[^c1-4] Luhn の検算は、右端の桁を 1 番目として偶数番目の桁を 2 倍し（2 桁になったら 9 を引く）、全部の桁を足し、和が 10 で割り切れなければ通りません。次

の例では、上の番号の和は 80 で通り、最後の桁を 8 にした下の番号の和は 81 で通りません。

4539148803436467 → Luhn を通る（カード番号の形として有効）

4539148803436468 → Luhn を通らない（最後の 1 桁が違っただけで無効）

Luhn を通る番号でも、金融機関がテストに使う予約番号は検出の対象外です。[^c1-4]

名前付きエンティティ (named entity) の SIT も組み込みです。人名、住所、医療用語を検出します。編集もコピーもできません。範囲の狭い un-bundled（単一の国や用語クラス）と、All physical addresses のように一括で拾う bundled があります。bundled の SIT をエンドポイント DLP のポリシーで使うには、Advanced classification scanning and protection を有効にします。[^c1-2]

要件を組み込みか、カスタムの SIT に置き換える

組み込みの SIT は編集できません。ただし複製して編集できるので、「ほぼ合うが少し違う」要件は、複製から始めるのが最短です。要件が組み込みに無い形なら、カスタム SIT をゼロから作ります。[^c1-5]

要件	手段
国の ID 番号の検出 (形は組み込みと同じ)	組み込みの SIT をそのまま使う
組み込みと同じ形だが、キーワードを自社用語にしたい	組み込みを複製して、補強要素を編集する
自社独自の形 (社員番号、案件番号)	カスタム SIT をゼロから作る

要件	手段
決まった語の一覧に一致したい(製品コード名の一覧)	キーワードリストかキーワード辞書
名前付きエンティティで検出したい	編集もコピーもできない。そのまま使う

複製できない SIT は次の 9 つです。[^c1-5]

- Canada driver's license number
- EU driver's license number
- EU national identification number
- EU passport number
- EU social security number or equivalent identification
- EU tax identification number
- International classification of diseases (ICD-10-CM)
- International classification of diseases (ICD-9-CM)
- U.S. driver's license number

キーワードリスト、正規表現、辞書、関数が合計 10 個以上ある SIT も、ポータルからは複製できません。その場合は PowerShell で複製します。

キーワードの持ち方は、量で選びます。

- **キーワード リスト:** 1 語 50 文字まで、最大 2,048 語。
- **キーワード辞書:** それを超える語数や長い語に使う。全辞書の合計の上限は文書によって値が違う(上限一覧のページは 1 MB、PowerShell の作成ページはテナントで 480 KB。どちらも圧縮後)。[^c1-6][^c1-8]

日本語など2バイト文字の言語は、語の間に区切りが無いため、Purview が語の間に空白を補います。日本語と英数字が混ざる語（「東京オリンピック2020」）は、空白あり・なしの2通りを登録します。リストの一致方式は、単語一致 (word) より文字列一致 (string) が推奨されています。[^c1-2][^c1-5]

カスタムの SIT を作成し、管理する

ポータルでの作成は、Information Protection > Classifiers > Sensitive info types で Create sensitive info type を選んで始めます。手順は次の順です。[^c1-5]

1. Name と Description を入れる。
2. Create pattern で、パターンごとに既定の信頼度 (Low、Medium、High) を選ぶ。
3. 主要素を定義する。正規表現 (検証子つきも可)、キーワードリスト、キーワード辞書、事前定義の関数から選ぶ。
4. 近接性 (Character proximity) を入れる。
5. 補強要素と、追加チェック (additional checks) を必要なだけ足す。
6. 推奨の信頼度 (recommended confidence) を選んで保存する。

カスタム SIT は 1 つ の ルール パッケージ (Microsoft.SCCManaged.CustomRulePack) に入ります。SharePoint と OneDrive の既存の内容に効かせるには、サイトやライブラリの再クロールを要求します。[^c1-5]

正規表現には決まりがあります。エンジンは Boost.RegEx 5.1.3 です。先頭と末尾を示す位置アンカー (^ と \$) は使えません。キャプチャグループは主要なもの 1 つだけで、前後の文脈は非キャプチャグループ (?:...) で書きます。分岐は、その 1 つのキャプチャグループの内側に | で入れます。[^c1-5][^c1-7]

誤: (?:[\s,;])([A-Z]{2}[0-9]{3})(?:[\s,;])|(?:[\s,;])([A-Z]{2}[0-9]{5})(?:[\s,;])

正: (?:[\s,;])([A-Z]{2}[0-9]{3}|[A-Z]{2}[0-9]{5})(?:[\s,;])

正の式は、キャプチャグループが1つです。誤の式は、トップレベルのキャプチャグループが2つ以上あるので、検証で止まります。

上限は表で覚えます。[^c1-6]

項目	上限
ポータルで作るカスタム SIT の数	500(それ以上は申請)
正規表現 1 つの長さ	1,024 文字
1 つの SIT の別個の正規表現	20
キーワードリストの 1 語	50 文字
キーワードリストの語数	2,048
キーワード辞書の合計 (圧縮後)	1 MB (PowerShell の作成ページは 480 KB。文書によって値が違う)
ルール パッケージの数	10
1 パッケージの SIT の数	50
ルール パッケージの大きさ	150 KB

検証子 (validator) は、正規表現の一致が本物かを計算で確かめる部品です。チェックサム検証子には、重み (Weights)、法 (Mod)、チェック桁の位置 (CheckDigit) を指定します。8 桁の免許番号で最後の桁が mod 9 のチェック桁なら、正規表現は \d{8}、重みは 8,7,6,5,4,3,2,0 です。チェック桁自身は合計に加えないので、その位置の重みは 0 です。先頭 7 桁が 1234567 なら合計

は 112、112 を 9 で割った余りは 4 なので、12345674 は有効で、12345675 は有効ではありません。[^c1-7]

追加チェック (additional checks) は、一致の後で誤検知を落とす条件です。テスト用のカード番号などの除外、始まりと終わりの文字、全桁が同じ数字 (111111) の除外、直前の語 (prefix) と直後の語 (suffix) で絞る指定があります。[^c1-7]

PowerShell では、XML のルール パッケージを作ってアップロードします。Entity とパッケージには、別々の GUID を振ります。Entity には patternsProximity と recommendedConfidence が必須で、recommendedConfidence が無いと、その SIT を使うポリシーを保存できません。Version は、再アップロードのたびに上げないと展開されません。キーワードの matchStyle は word と string があり、アジアの言語には string を使います。[^c1-8]

```
New-DlpSensitiveInformationTypeRulePackage -FileData
([System.IO.File]::ReadAllBytes('C:\My Documents\MyNewRulePack.xml'))
Get-DlpSensitiveInformationTypeRulePackage
```

XML の中では、Pattern 中の複数の Match は暗黙の AND で結ばれ、1 つでも欠けると一致しません。OR にしたいときは Any 要素を使い、minMatches="1" なら「どれか 1 つ」になります。minMatches="0" と maxMatches="0" を両方指定すると、「その証拠が無いこと」を条件にできます。[^c1-8]

作った SIT は、サンプル ファイルをアップロードして試せます。結果は信頼度ごとの一致数で出ます。この機能は、テナントに Exchange Online のライセンスが 1 つ以上ないと選べません。[^c1-2]

社員番号が「EM」と 6 桁の数字 (EM123456) で、前後は空白、カンマ、セミコロンのどれかの場面を考えます。組み込みに無い形なので、カスタム SIT をゼロから作ります。主要素は正規表現 `(?:[\s,;])(EM[0-9]{6})(?:[\s,;])`、補強要素は「社員番号」「Employee ID」のキーワード リスト、近接性は 300 文字です。位置アンカーは使えないので、前後の区切りは非キャプチャグループで書かなければなりません。この式では、前後に区切りのある "EM123456" は一致し、区切りの無い "EM123456"、5 桁、7 桁の番号は一致しません。

ドキュメントフィンガープリント

ドキュメントフィンガープリント (document fingerprinting) は、定型の書式 (空の申請書、特許テンプレート) を渡すと、その書式の語のパターンから SIT を作る機能です。元の文書は保存されません。語のパターンを表すハッシュ値だけが保存され、元の文書は復元できません。[^c1-9]

フィンガープリント SIT は、Exchange、SharePoint、OneDrive、Teams、デバイスを対象にした DLP ポリシーで使えます。日本語、中国語、韓国語のような 2 バイト文字の言語の書式も対象です。自動ラベル付けでは Exchange、SharePoint、OneDrive で使えます。デバイスで使うときは Advanced classification scanning and protection を有効にします。[^c1-9]

一致の方式は 2 つです。部分一致は、信頼度 (低、中、高) ごとに、文書の語がテンプレートとどれだけ重なれば検出するかを 30%~90% の割合で指定します。完全一致は、高信頼度を Exact に設定します。その場合は、テンプレートと完全に同じ文字列の文書しか検出しません。[^c1-9]

PowerShell は Security & Compliance PowerShell を使います。New-DlpFingerprint でなく、New-DlpSensitiveInformationType に - FileData を渡して作り、割合は ThresholdConfig で指定します。

```
$Patent_Form = ([System.IO.File]::ReadAllBytes('C:\My  
Documents\patent.docx'))  
  
New-DlpSensitiveInformationType -Name "Patent SIT" -FileData  
$Patent_Form -ThresholdConfig @{low=40;medium=60;high=80} -IsExact  
$false -Description "Contoso Patent Template"
```

この設定では、書式の語の 40% 以上が重なれば低、60% 以上で中、80% 以上で高の一致になります。割合ごとに判定すると、45% なら低だけ、65% なら低と中、85% なら 3 段階すべてに当たり、35% ではどの信頼度にも当たりません。更新は Set-DlpSensitiveInformationType を使います。[^c1-9]

検出できない場合と上限は、次のとおりです。

- **対象外の文書:** パスワード保護のファイル、画像だけのファイル、元の書式の語を全部は含まない文書、4 MB を超えるファイル。
- **テンプレートの条件:** 抽出テキストが 256～204,800 文字。埋め込み文書の文字は無視される。
- **テナントの上限:** フィンガープリントは専用のルール パックに入り、上限は 300 KB。およそ 100 個。

すでにフィンガープリントがあるテンプレートで、もう 1 つ作ることはできません。[^c1-9]

完全なデータ一致 (EDM) の SIT

EDM は、機密情報の実際の値を入れた表 (機密情報ソース テーブル) と照合して検出する方法です。パターンでなく実在の値で一致するので誤検知が少なく、表は毎日更新できます。表は最大 1 億行です。構造化データを扱い、機密の値は Microsoft を含め誰にも渡りません。[^c1-10]

仕組みの要は、一方向のハッシュです。表の値はソルトつきでハッシュ化し、ハッシュだけをサービスへアップロードします。平文はアップロードしません。検出側も、内容の文字列をハッシュにして照らします。[^c1-10]

作業は次の順です。

1. 機密情報ソース テーブルを CSV、TSV、パイプ区切りのいずれかで用意する。
2. スキーマ(XML)を作る。
3. EDM Upload Agent でハッシュ化し、アップロードする。
4. EDM の SIT (ルール パッケージ)を作る。
5. DLP ポリシーや自動ラベル付けから使う。

スキーマは XML ファイルです。スキーマ名 (DataStore)、列名、検索対象の列 (searchable)、列ごとの設定を定義します。列ごとの設定は、大文字小文字を区別しない caseInsensitive と、無視する区切り文字の ignoredDelimiters です。列名は表の見出しと 1 対 1 で、英字で始まる 3 文字以上の英数字だけにします。1 テナントに 11 個以上のスキーマは作れません。[^c1-11]

```
<DataStore name="PatientRecords" description="Schema for patient
records" version="1">
  <Field name="PatientID" searchable="true" caseInsensitive="true"
ignoredDelimiters="-,/,*,#,^" />
  <Field name="FirstName" />
</DataStore>
```

caseInsensitive と ignoredDelimiters を併用した PatientID では、FOO-1234 と fOo#1234 が同じ値として扱われます。ただし ignoredDelimiters

は、主要素に対応づけた SIT の検出には影響しません。その SIT が、記号ありでもなしでも文字列を拾える形である必要があります。[^c1-11]

検索対象の列 (searchable) には、主要素として探す列を指定します。主要素は既存の SIT で検出できる必要があり、たとえば SSN を主要素にするなら SSN の SIT に対応づけます。主要素が見つからなければ、補強要素だけでも一致しません。主要素が見つかった後で、補強要素 (名前、生年月日、住所など) を近接性の範囲内で探します。補強要素は単独でも組み合わせでも照合されるので、名前と生年月日が両方一致すれば、より強い証拠になります。[^c1-10]

スキーマを XML で作って PowerShell から登録するときは New-DlpEdmSchema を使い、反映に 10〜60 分かかります。searchable の数は、作成ページが 1〜10 個、PowerShell 手順の説明が最大 5 個までと書いており、食い違っています (1 つ以上が必須である点は同じです)。

アップロードは EDM Upload Agent (EdmUploadAgent.exe) で行います。

コマンド	役割
/Authorize	資格情報でサインインして認可する
/SaveSchema、/ValidateData	スキーマの保存、表がスキーマに合うかの検証
/CreateHash	ハッシュとソルトのファイルを作る (2 台方式の 1 台目)
/UploadHash	ハッシュを送る (2 台方式の 2 台目)
/UploadData	ハッシュ化とアップロードを 1 台で行う
/GetDataStore、/GetSession	アップロードの結果と履歴の確認

実行するユーザーは、EDM_DataUploaders セキュリティ グループのメンバーにします。ハッシュ化とアップロードを別の PC で行う 2 台方式が、平文の表をインターネットに接続した PC に置かないためのベスト プラクティスです。2 台方式で両方の PC に入れる Upload Agent は、同じバージョンでなければなりません。ソルトは既定で自動付与されます。/Salt で自分のソルトを指定できますが、一度使うと、標準版の Upload Agent には戻れません。[^c1-12]

EDM の SIT を作る方法には、新しい体験とクラシックがあります。新しい体験はスキーマと SIT を 1 つの流れで作ります。スキーマ名は SIT 名に schema を足した名前でも自動に決まり、高と中の信頼度のルールも自動で作られます。1 つのスキーマに複数の SIT は対応づけられず、SIT は最大 10 個までで、11 個目はエラーになって作れません。クラシックを使うのは、次の場合です。[^c1-13]

- 複数の SIT を 1 つのスキーマに対応づけたい。
- スキーマ名を自分で決めたい。
- 10 個を超えて SIT を管理したい。

必要な役割は、どちらの体験でも Global Admin、Compliance Admin、Exchange Admin のいずれかです。

EDM の SIT は、DLP、自動ラベル付け、Insider risk management、eDiscovery、Defender for Cloud Apps で使えます。DLP ポリシーでは、EDM の SIT を高信頼度の条件に、元になった組み込みの SIT を低信頼度の条件に並べると、少数でも確実に拾い、件数が多いときは広く拾う組み立てになります。[^c1-10][^c1-13] 秘密度ラベルの自動適用に EDM を使うときは、EDM でない SIT を少なくとも 1 つ、同じ条件に入れないと動きません。EDM だけの条件にすると、ラベルの自動適用の設定は自動でオフになります。

申請書の様式が毎年同じで、記入前の様式のファイルがあるなら、ドキュメントフィンガープリントです。誰が何を書いても様式の語は残るからです。契約者番号の台帳 (CSV) があり、台帳にある番号だけを拾いたいなら、EDM です。前者は書式の一致、後者は値の一致で、見ているものが同じではありません。台帳の平文をインターネットに接続した PC に置きたくなければ、隔離した PC で /CreateHash を実行し、別の PC で /UploadHash を実行します。

トレーニング可能な分類子

トレーニング可能な分類子は、「形」でなく「内容の種類」を例から学習して判定する道具です。契約書、履歴書、財務報告のように、パターンでは言い表せない文書に向きます。[^c1-14]

種類は 2 つです。Microsoft が事前学習させた分類子 (Ready to use と表示される) と、自分で学習させるカスタムの分類子です。カスタムは英語にしか対応しません。暗号化された項目には効きません。[^c1-14]

カスタムの分類子を作る手順は次のとおりです。[^c1-15]

1. 分類したい内容の例 (陽性) を 50～500 件集める。
2. 該当しない内容の例 (陰性) を 150～1,500 件集める。
3. 陽性と陰性を、SharePoint の別々のフォルダーに入れる。
4. Purview ポータルで Create trainable classifier を選び、両方のフォルダーの URL を指定する。
5. 24 時間以内に処理が終わり、状態が In progress から Training is complete に変わる。
6. 予測を確かめ、Publish for use で公開する。

処理されるのは、作成日時が新しい順の最大 2,000 件です。テスト用には、陽性 50 件以上と陰性 150 件以上を含む 200 件以上が推奨されます。例のフォルダーは、通信サイトなどの SharePoint サイトに置きます。Teams のフォルダーや OneDrive は使えません。新しいサイトを作ったときは、インデックスが済むまで少なくとも 1 時間待ちます。テキストの形式のファイルだけが使え、画像や画像だけの PDF は使えません。[^c1-15]

公開した分類子は、Office の自動ラベル付け (秘密度ラベル)、保持ラベルの自動適用、Communication compliance、DLP の条件として使えます。ただし Communication compliance は、Microsoft が提供する分類子だけに対応し、カスタムは使えません。[^c1-14][^c1-15] 公開した後の再学習はできません。精度を上げたいときは、分類子を削除し、より大きなサンプルでやり直します。公開前なら、結果を確かめてデータを足し、学習をやり直せます。既定では、作成した本人だけが学習と予測の確認をできます。[^c1-14][^c1-15]

使い道ごとの役割は、次のとおりです。[^c1-15]

- **保持ラベル ポリシー:** Records Management か Retention Management。
- **秘密度ラベル ポリシー:** Security Administrator、Compliance Administrator、Compliance Data Administrator のいずれか。
- **Communication compliance:** Insider Risk Management Administrator か Supervisory Review Administrator。

Data explorer と Content explorer で分類とラベルの使用状況を見る

どちらも、テナントの項目のうち、秘密度ラベル、保持ラベル、SIT で分類されたもの、トレーニング可能な分類子に一致したものの現況を、ラベルや SIT 別に見る画面です。場所 (Exchange、SharePoint、OneDrive、Teams) を掘り下

げてフォルダーから項目まで進め、結果は .csv に書き出せます。件数の反映には時間がかかり、最大 7 日、SharePoint のファイルは最大 14 日です。最近の動きを見たいときは、Activity explorer を使います。[^c1-16][^c1-17]

見える内容に応じて、アクセス権は 2 段あります。1 段目は、タブそのものを開くための役割です。次のいずれかを持つアカウントが開けます。

- Compliance administrator
- Security administrator
- Compliance data administrator
- Global administrator (Data explorer のみ)
- Purview の役割グループ Information Protection、Information Protection Admins、Analysts、Investigators、Readers (細かく絞るとき)

この役割だけでは、項目の一覧も中身も見えません。2 段目は、項目の閲覧のための役割グループです。[^c1-16][^c1-17]

役割グループ (Content explorer と Data explorer に同名が各 1 組)	見えるもの
List viewer	項目の一覧と、その場所
Content viewer	項目の中身。一覧で項目名を見るのにも必要 (名前に機密が含まれるため)

この 2 つは独立で、累積しません。一覧だけ見せたいなら List viewer、中身まで見せるなら Content viewer も付けます。Information Protection のルールグループ (Information Protection と、その Admins、Analysts、Investigators、Readers) でも調整できます。管理単位 (administrative unit) による範囲の制限にも対応しています。この権限は、項目に個別に付いた権限より優先されます。[^c1-16][^c1-17]

暗号化された文書は、プレビューもダウンロードもできません。暗号化された秘密度ラベルの項目は、SharePoint と OneDrive では Content explorer に出ません。SharePoint と OneDrive のファイルのラベルを出すには、事前に Office ファイル向けの秘密度ラベルを有効にしておきます。[^c1-16]

SIT の光学式文字認識 (OCR) の構成

OCR は、画像の中の文字を取り出して、SIT やトレーニング可能な分類子で検査できるようにする機能です。既存の DLP、records management、Insider risk management のポリシーが、画像にもそのまま効きます。使うには、課金の準備が先です。[^c1-18]

1. Azure の従量課金サブスクリプションを用意する (Global admin)。
2. OCR のコストを見積もり、Microsoft Syntex の従量課金を Azure に設定する (Global admin か SharePoint admin)。Syntex 自体のセットアップは不要。
3. Purview ポータルの Settings > Optical character recognition (OCR) で構成する (Compliance admin)。

構成では、画像を検査する場所と、対象にするグループ (含めるか除くか) を選びます。場所は Exchange、SharePoint、OneDrive、Teams、Windows と macOS のデバイスです。設定は有効にして約 1 時間後に効き、有効にした後でアップロードされた画像だけが検査されます。構成できるのは、Compliance administrator、Compliance data administrator、Global administrator などの役割グループです。[^c1-18]

課金は、画像 1 枚を 1 トランザクション、PDF は 1 ページを 1 トランザクションと数えます。5 枚の PNG、10 ページの PDF、3 ページの PDF を検査すると、 $5 + 10 + 3 = 18$ トランザクションです。課金を減らすキャッシュがあり、メール

の小さな画像(ロゴや署名)は、テナント全体でユニークな画像ごとに 5 日の窓で 1 回だけ数えます。エンドポイントのキャッシュは 30 日で、SharePoint と OneDrive の単独の画像にはありません。[^c1-18]

場所	画像の種類と制約
Exchange、Teams	1 つ 20 MB まで
SharePoint、OneDrive、Windows と macOS の端末	1 つ 50 MB まで
全場所の解像度	50 × 50 px 以上、16,000 × 16,000 px 以下
Exchange の埋め込み画像	1 ファイルあたり 20 枚まで

画像の形式は、Exchange では JPEG、JPG、PNG、BMP、TIFF とスキャンした PDF、Teams と端末では同じ画像形式と画像だけの PDF です。SharePoint と OneDrive は、HEIC、GIF、RAW 系など、さらに多くの形式に対応します。OCR が取り出すのは先頭の 200 万文字までです。Exchange では、DLP のポリシー ヒントは画像に対応しません。[^c1-18]

Microsoft Purview で秘密度ラベルを実装および管理する [1.2]

秘密度ラベルの管理の役割とアクセス許可

ラベルを作って設定する人には、Microsoft Purview ポータルの権限が要ります。使えるのは次のどれかです。[^c1-19]

- Information Protection の役割グループ (Information Protection、Information Protection Admins、Analysts、Investigators、Readers)
- 新しい役割グループに追加した Sensitivity Label Administrator ロール (読み取り専用は Sensitivity Label Reader)

- Compliance Data Administrator、Compliance Administrator、Security Administrator の役割グループ

この権限は、ラベルとラベル ポリシーを作って設定するときだけ要ります。アプリでラベルを付けるユーザーには要りません。

管理単位 (administrative unit) も使えます。役割グループのメンバーに管理単位を割り当てると、その管理者が管理できるのは、管理単位の中のユーザーだけになります。ラベル ポリシーと自動ラベル付けポリシーも、管理単位で初期の対象を絞れます。Exchange と OneDrive では選んだ管理単位のユーザーだけが、SharePoint では選んだ管理単位のサイトだけが対象です。保護ポリシーは管理単位に対応しません。[^c1-19]

手動のラベル付けは Microsoft 365 の多くのプランで使えます。自動ラベル付け (クライアント側もサービス側も) には、E5 系の上位プランが要ります。具体的には E5、E5 Compliance、E5 Information Protection & Governance、Azure Information Protection Premium P2 です。E3 と Business Premium には含まれません。[^c1-26]

項目とコンテナのラベルを定義する

ラベルを作るとき最初に決めるのが範囲 (scope) です。範囲は、設定できる項目と、ラベルがどのアプリやサービスで選べるかを決めます。[^c1-20]

範囲	対象	注意
Files & other data assets	Office、Loop、Power BI のファイルなど	新しいラベルでは既定で選ばれている
Emails	メール	ファイルと同時に選ぶのが普通

範囲	対象	注意
Meetings	カレンダーの予定、Teams 会議のオプション、チャット	Files と Emails の両方を選ばないと選べない
Groups & sites	Teams、Microsoft 365 グループ、SharePoint サイト、Viva Engage、Loop ワークスペース	コンテナのラベルを有効にして同期した後に選べる

Groups & sites だけを選んだラベルは、Office アプリには出ず、ファイルやメールには付けられません。逆に、Files と Emails だけのラベルは、グループやサイトには付けられません。[^c1-20]

1 つの項目に付けられる秘密度ラベルは 1 つだけです。文書とメールには、秘密度ラベルと保持ラベルを 1 つずつ付けられます。同じ組織のユーザーには、付いたラベルがアプリの中でタグのように見えます。ほかの組織のユーザーやゲストには、自組織のラベルは見えません。[^c1-20]

ラベル一覧の並び順が優先度です。いちばん制限の強いラベル (Highly Confidential) を一番下に、弱いラベル (Personal や Public) を上に置きます。優先度は、次の場面で使われます。[^c1-21]

- 低い優先度のラベルに替えるとき、理由の入力を求める判定。
- 自動ラベル付けで複数のラベルが一致したとき、どれを選ぶかの判定。
- メールの添付ファイルからラベルを引き継ぐときの判定。

ラベルを 2 階層にまとめる方法には、旧来の親ラベルとサブラベル、そして置き換え先のラベル グループがあります。ユーザーには、たとえば「Confidential \ All Employees」のように見えます。2 階層目のラベルは、1 階層目から色だけを引き継ぎ、ほかの設定は引き継ぎません。[^c1-22]

親ラベルは、それ自体をコンテンツに付けられません。既定のラベルにしたり、自動適用や推奨に設定したりしても適用されません。ラベル グループは、名前、説明、色、優先度だけを設定できる枠で、発行できるのは中のラベルだけです。サブラベルは親(またはラベル グループ)と優先度を共有するので、サブラベル同士の入れ替えは、ラベルを下げる操作と見なされません。[^c1-21]
[^c1-22]

数の目安もあります。主ラベルは 5 個まで、1 つの主ラベルのサブラベルも 5 個までが目安で、超えると効果が下がり、アプリが全部のラベルを表示できないことがあります。暗号化でユーザーと権限を指定するラベルは、テナントで最大 500 個です。それ以外のラベルは 1,000 個以上でも持てます。[^c1-21]

ラベルを削除しても、付いているコンテンツからラベルは外れず、保護も保たれます。ラベルを編集した場合、コンテンツには、付けた時点の版のラベルが効きます。ただし、Assign permissions now の暗号化で利用者や権限を変えた場合は、既存のコンテンツにも、利用者が暗号化サービスと認証するときに新しい設定が効き、多くの場合はラベルを付け直す必要がありません。ラベルポリシーから外す操作は、ラベルの削除とは別です。ポリシーから外すと、そのポリシーのユーザーはラベルを選べなくなりますが、ラベルとラベルが付いたコンテンツは残ります。[^c1-21]

Teams のチームにだけ付けるラベルは、範囲を Groups & sites だけにします。この場合、そのラベルは Word や Outlook に出ません。会議の保護も同じラベルに足したいなら、Meetings を選ぶために Files & other data assets と Emails も選ぶ必要があり、ラベルは Office アプリにも出るようになります。Highly Confidential を一覧の上に置くと、Public への変更が「ラベルを下げる操作」と判定されず、理由の入力が求められません。

ラベルの暗号化の設定

暗号化を設定するには、ラベルの範囲に Files & other data assets を含め、保護の設定のページで Control access を選びます。選べる設定は 2 つです。
[^c1-23]

- **Remove access control settings if already applied to items:** 既存の暗号化を、ラベルとは無関係に付いたものも含めて外す。
- **Configure access control settings:** ラベルで暗号化を設定する。

Configure の中で、権限の決め方を 2 つから選びます。

方式	決める人	向く場面
Assign permissions now (今すぐ権限を割り当てる)	管理者。誰がどの権限かをラベルで固定する	最高機密のように、権限をあらかじめ決められる内容
Let users assign permissions (ユーザーに任せる)	ラベルを付けるユーザー	契約書のように、共同作業の相手が案件ごとに変わる内容

ユーザーに任せる方式は、Outlook では Do Not Forward か Encrypt-Only を選びます。Do Not Forward では、受信者は転送、印刷、コピーができません。Outlook の転送ボタンや「名前を付けて保存」、印刷のメニューが使えなくなり、宛先の追加や変更もできません。Encrypt-Only では、受信者は Save As、Export、Full Control 以外のすべての使用権限を持ちます。コピー、印刷、転送ができ、できないのは保護を外すことだけです。Word、Excel、PowerPoint では、ラベルを付けるときに、ユーザーが権限を与える相手を選ぶ画面が出ます。
[^c1-23]

Assign permissions now では、次の項目を決めます。
[^c1-23]

- **User access to content expires:** アクセスの期限。特定の日付か、ラベルを付けてからの日数。日付は、現在のタイムゾーンの午前 0 時から効く。
- **Allow offline access:** オフラインでの使用。Never、Always、または日数。期限が来ると、ユーザーは再認証され、アクセスが記録される。
- **Assign permissions to specific users and groups:** 誰にどの権限を与えるか。

権限を与える相手には、次の種類を選べます。

- 組織のすべてのメンバー (ゲストは含まれない)
- Any authenticated users (認証できる誰でも)
- 特定のユーザーと、メールが有効なセキュリティグループ、配布グループ、Microsoft 365 グループ
- 任意のメール アドレスまたはドメイン

メールが有効でないセキュリティグループと、Exchange の動的配布グループは使えません。ドメインを指定すると、その組織の検証済みドメインすべてが対象になり、特定のドメインには絞れません。ユーザーを 1 人ずつ指定するより、グループが推奨です。[^c1-23]

Any authenticated users は、誰が開けるかを制限しません。暗号化と使い方の制限 (コピーや印刷の禁止、期限、オフライン) だけをかけたい場面で使います。Google などのソーシャル ログインとワンタイム パスコードは、Exchange Online のメールと会議の招待でだけ使えます。[^c1-23]

権限は、定義済みのレベル (Editor、Restricted Editor など) か、使用権限を個別に選ぶカスタムで与え、ユーザーごとに変えられます。ラベルを付けたユーザーは Rights Management issuer になり、常に Full Control を持ちま

す。期限が過ぎても、オフラインでも、文書が取り消された (revoke された) 後でも、開けます。[^c1-23]

オフラインアクセスの推奨は、内容の機密度で分かります。

- **漏れると事業に損害が出る内容** (契約書、セキュリティ レポート): 7 日。
- **従業員と顧客の情報、パスワード、ソースコード**、および動的透かしを使うラベル: Never。
- **機密性が低い内容** (権限を外した後に最大 30 日ほど開けても構わない): Always。

User access to content expires は、時間の制約が無い限り Never が推奨です。オフラインの値を変えられるのは Assign permissions now のラベルだけで、ユーザーに任せる方式では変えられません。ユーザーに任せる方式は、テナントの Rights Management 使用ライセンス (use license) の有効期間を使います。対象は Do Not Forward、Encrypt-Only、ユーザー定義の権限で、既定は 30 日です。ユーザーがコンテンツを開くと使用ライセンスが発行され、有効な間は再認証されません。期限が切れた後の最初のアクセスで、再認証され、暗号化の設定とグループのメンバーシップが再評価されます。[^c1-23]

暗号化には前提があります。Azure Rights Management が有効である必要があります (新しいテナントでは既定で有効です)。Exchange を Azure Rights Management 向けに構成していないと、次の制限が出ます。モバイルと Outlook on the web で、暗号化メールを見られません。暗号化メールを検索できません。Exchange Online の DLP で、Rights Management の保護を設定できません。Microsoft Entra の条件付きアクセスとクロステナントのアクセス設定が、許可されたユーザーのアクセスを妨げることもあります。[^c1-23]

ラベルの変更が既存のコンテンツにどう効くかは、場面で変わります。

- **SharePoint と OneDrive のファイル(ラベルの有効化済み)**: 次にアクセスされたとき (Office for the web で開く、ダウンロードするなど) に、暗号化の状態が自動で変わる。
- **それ以外のラベル済みの項目**: ラベルを外して付け直すまで、以前の暗号化の状態のまま。
- **権限の変更 (Assign permissions now)**: サービスと認証するときに効く。すでに開いたユーザーは、使用ライセンスが切れるまで変わらない。
- **ユーザーに任せる方式との切り替え**: 変更後に付けた項目にだけ効く。

すでに暗号化されているコンテンツに別のラベルを付けるには、付ける人に Export または Full Control の使用権限が要ります。Rights Management issuer、owner、スーパーユーザーの役割でも構いません。どれも無ければ、ラベルは付けられません。暗号化されたメールに添付された、暗号化されていない Office 文書は、メールの暗号化の設定を自動で引き継ぎます。引き継ぐのは暗号化だけで、ラベルは引き継ぎません。[^c1-23]

このほか、暗号化のオプションに Double Key Encryption があります。サービスの構成が済んでいる場合にだけ選び、保存した後はそのラベルを編集できません。Outlook では、暗号化の代わりに S/MIME の保護を適用するラベルも設定できます。[^c1-23]

取引先 A 社の全員に、契約書を限られた権限で見せ、30 日後には開けなくしたい場面を考えます。Assign permissions now を選び、A 社のドメインを指定し、権限は使用権限を絞った定義済みレベルかカスタムにして、User access to content expires を 30 日後にします。案件ごとに相手が変わる契約書なら、Let users assign permissions を選び、ラベルを付けるときに相手を選ばせます。SharePoint の自動ラベル付けポリシーで使う暗号化ラベル

は、Assign permissions now にして、期限を Never にします。この用途に Let users assign permissions は使えません。

コンテンツマーキング

コンテンツマーキングは、ラベルが付いたコンテンツに、ヘッダー、フッター、透かしを直接書き込む設定です。文字数の上限は表のとおりです。[^c1-20]

種類	上限
透かし	255 文字
ヘッダー、フッター	1,024 文字
Excel のヘッダーとフッター	合計 255 文字 (見えない書式コードも数える)

透かしは、文書と Loop のコンポーネントやページに付けられ、メールと会議の招待には付けられません。ヘッダーとフッターは、メールにも付けられます。[^c1-20]

文字列には変数を入れられます。構文は大文字と小文字を区別します。[^c1-24]

変数	展開される値
<code>\${Item.Label}</code>	付けたラベルの表示名
<code>\${Item.Name}</code>	ファイル名、またはメールの件名
<code>\${Item.Location}</code>	文書のパスとファイル名、またはメールの件名
<code>\${User.Name}</code>	ラベルを付けたユーザーの表示名
<code>\${User.PrincipalName}</code>	ラベルを付けたユーザーの UPN

変数	展開される値
<code>\${Event.DateTime}</code>	ラベルを付けた日時 (Microsoft 365 アプリではユーザーのローカル時刻、Office Online と自動ラベル付けポリシーでは UTC)

アプリごとに文字列を変えるには、`${If.App.<アプリ>}` と `${If.End}` で囲みます。アプリ名は Word、Excel、PowerPoint、Outlook で、W、X、P、O に略せ、複数なら `WXO` のようにまとめます。たとえば `${If.App.WP}This content is ${If.End}Confidential` と書きます。Word と PowerPoint の透かしは「This content is Confidential」、Excel の透かしは「Confidential」になり、Outlook には透かしが付きません。[^c1-24]

動的透かし (dynamic watermark) は、通常のマーキングと別物です。暗号化するラベルでしか使えません。ファイルを開いたユーザーのメール アドレス (UPN) が、そのたびに各ページへ表示されます。いったん付くと、ラベルを外すか (許可されていれば) エクスポートしない限り、変更も削除もできません。通常のマーキングは、暗号化しないラベルでも使え、付いた後にユーザーが変更も削除もできます。動的透かしに対応しないアプリでは、文書が開けません。ラベルを付けた本人 (Rights Management owner) と、Office for the web では開けます。オフラインアクセスは Never にするのが推奨です。[^c1-23][^c1-24]

ラベルの発行ポリシー

ラベルは、発行ポリシーで配って初めてユーザーに見えます。ラベルの発行先は、ユーザーとグループです (保持ラベルがメールボックスのような場所に発行されるのとは違います)。既定は組織の全ユーザーですが、ポリシーを分ければ、部署ごとに見えるラベルを変えられます。たとえば全員に Public、

General、Confidential を見せ、法務部門だけに Highly Confidential を見せます。反映には最大 24 時間かかります。[^c1-25]

発行ポリシーで決める設定は、次のとおりです。[^c1-25]

- **既定のラベル:** ファイルと Loop、メールと会議、新しいコンテナー、Power BI の 5 種類に、同じラベルまたは別々のラベルを指定できる。ユーザーは変更できる。
- **ラベルの必須化 (mandatory labeling):** ファイルの保存、メールや会議招待の送信、グループやサイトの作成、ラベルの無い Power BI コンテンツの利用の前に、ラベルを付けさせる。
- **ラベルを下げる、外すときの理由の要求:** ファイル、メール、会議で、既定で有効。

暗号化するラベルを文書の既定にするのは、普通は勧められません。社外の相手が、暗号化に対応したアプリや認証できるアカウントを持たないことがあるからです。サブラベルがあるときは、親ラベルを既定にしてはいけません。既定にするのはサブラベルです。必須化は、既定のラベルを併用しないと、頻繁な確認でユーザーが困ります。必須ラベルと Office の自動ラベル付けは、タイミングの問題で自動適用が動かないことがあります。[^c1-25][^c1-26]

理由の入力を求める判定は、優先度の順で決まります。たとえば Confidential (順序 3) の文書を Public (順序 1) に替えるときは、理由の入力を求められます。理由を求めるのは、ラベルを下げる、または外すときです。次の場合は対象外です。[^c1-21][^c1-25]

- サブラベル同士の入れ替え (親と同じ優先度を共有する)。
- グループとサイトのラベル。
- ラベル グループ内のサブラベル。

Office アプリでは、理由の入力はアプリのセッションごとに 1 回で、Microsoft Purview Information Protection クライアントではファイルごとに入力します。[^c1-25]

複数のポリシーの設定がぶつかったときの決め方も出ます。ユーザーが複数のポリシーに入っていれば、全部のポリシーのラベルを受け取り、設定が衝突したときは、順序番号が最大の（一覧で一番下の）ポリシーの設定が、設定ごとに優先されます。標準ポリシー（番号 0、既定ラベル General）と IT 部門のポリシー（番号 1、必須化あり）に入るユーザーは、既定ラベルが General、必須化ありです。法務部門のポリシー（番号 2、既定ラベル Confidential）も加わると、既定ラベルは Confidential に変わりますが、必須化は衝突しないので消えません。ポリシーの設定が期待どおり効かないときは、まずポリシーの順序を確認めます。[^c1-25]

自動ラベル付け

秘密度ラベルを自動で付ける方法は 2 つです。[^c1-26]

項目	クライアント側(ラベルの設定)	サービス側(自動ラベル付けポリシー)
動く場所	Word、Excel、PowerPoint、Outlook	SharePoint、OneDrive、Exchange (転送中のメール)
アプリのバージョン	影響する	影響しない
場所での絞り込み	できない	できる
例外、AND/OR/NOT の入れ子	できない	できる
推奨(ユーザーに確認)	できる	できない

項目	クライアント側(ラベルの設定)	サービス側(自動ラベル付けポリシー)
シミュレーション	できない	できる
PDF と画像	対象外	対象
受信メールのラベル付け	できない	できる
ラベルの設定場所	ラベルの Auto-labeling for files and emails	Information protection > Policies > Auto-labeling policies

クライアント側は、ユーザーが文書を編集したりメールを書いたりしている間に動きます。保存の前でもラベルを付けられるので、遅延が小さくなります。推奨の場合も自動の場合も、最終的に受け入れるか断るかはユーザーが決めます。サービス側は、保存済みのファイル (SharePoint、OneDrive) と送受信されるメール (Exchange Online) に動きます。ユーザーが関わらないので、推奨はできません。代わりに、有効にする前にシミュレーションで確かめます。
[^c1-26]

条件は、SIT かトレーニング可能な分類子です。EDM の SIT を使う場合は、EDM でない SIT を少なくとも 1 つ、同じ条件に入れます。トレーニング可能な分類子だけを条件にしたラベルでは、自動ラベル付けポリシーを自動作成するオプションが出ません。[^c1-26]

複数のラベルの条件に一致したときは、優先度が最も高い (順序番号が最大の) ラベルが選ばれ、サブラベルがあれば、さらに最後のサブラベルが選ばれます。クライアント側では、未ラベルのファイルに同じ親のサブラベルが複数一致すると、自動に設定したサブラベルが、推奨に設定したサブラベルより優先されます。すでに同じ親のサブラベルが付いているファイルには、何もしません。[^c1-26]

既存のラベルを置き換えるかどうかの規則は、表で覚えます。[^c1-26]

既存のラベル	クライアント側の設定	ポリシー
手動で付けた、優先度の低いラベル	置き換えない	既定は置き換えない(設定で可能)
手動で付けた、優先度の高いラベル	置き換えない	置き換えない
自動または既定で付いた、優先度の低いラベル	置き換える	置き換える
自動または既定で付いた、優先度の高いラベル	置き換えない	置き換えない

ポリシーは、ラベルを外して未ラベルに戻すことはしません。ただし SharePoint と OneDrive では、ラベルを自動で外す設定にしたポリシーが、手動で付けたラベルも外せます。[^c1-26]

サービス側のポリシーを作る前に、前提を確かめます。[^c1-26]

1. Microsoft 365 の監査ログを有効にする(シミュレーションに必須)。
2. SharePoint と OneDrive の Office ファイルで、秘密度ラベルを有効にする。
3. 適用するラベルが親ラベルでないこと(親ラベルは、ポリシーが動いても何も付かない)。
4. SharePoint または OneDrive のコンテンツを暗号化するラベルは、Assign permissions now にして、User access to content expires を Never にする。Exchange だけのポリシーなら、Let users assign permissions (Do Not Forward か Encrypt-Only) でもよい。S/MIME のラベルは自動適用できない。

5. PDF を処理するなら、テナントで PDF のラベル付けを有効にする。有効でなければ、PDF は評価されずに飛ばされる。

ポリシーを保存すると、既定でシミュレーションで実行されます。完了までは最大 12 時間ほどかかります。シミュレーションを 1 回も実行していないポリシーでは、ラベルを自動適用できません。結果を確かめ、必要なら条件を直して再実行し、問題が無ければ Turn on policy で有効にします。有効にするには、Compliance Administrator か Compliance Data Administrator が要ります。シミュレーションの後、7 日間編集しなければ自動で有効にする設定も選べます。シミュレーションでは、一致するファイルが 2,000 万を超えると、有効にできません。対象を絞って、やり直します。ファイルが開かれている間は、ラベルを付けられません。[^c1-26]

主な上限は次のとおりです。[^c1-26]

項目	上限
テナントで 1 日に自動ラベルを付けるファイル	50 万
テナントの自動ラベル付けポリシー	100
ポータルで明示的に指定できる SharePoint サイト (ポリシーごと)	1,000
アダプティブ スコープ (PowerShell) で指定できるサイト	50,000
シミュレーションで一致できるファイル	2,000 万

Exchange では、PDF と Office の添付も条件の検査に使われ、一致するとラベルが付くのはメールで、添付には付きません。受信メールにラベルを付けるには、Exchange の場所を「すべて含める・除外なし」にします。社外の送信者

のメールに暗号化を効かせるには、追加設定で Rights Management owner を指定します。[^c1-26]

コンテナのラベル(Teams・Microsoft 365 グループ・SharePoint サイト)

コンテナのラベルは、ファイルでなく、Teams、Microsoft 365 グループ、SharePoint サイト、Viva Engage コミュニティ、Loop ワークスペースを守ります。使える設定は、プライバシー、外部ユーザーのアクセス、外部共有、管理されていないデバイスからのアクセス、認証コンテキスト、プライベート チームの検出可否、共有チャネルの招待の制御です。[^c1-27]

コンテナのラベルは、中のファイルやメールにはラベルを引き継ぎません。暗号化やマーキングのようなアイテム単位の設定も効きません。サイトの中の文書をラベル付けしたいなら、ユーザーが文書に付けられるよう、SharePoint と OneDrive でラベルを有効にしておきます。[^c1-27]

最初に一度だけ、次の手順で有効化と同期をします。[^c1-27]

1. Microsoft Entra ID 側で、Microsoft 365 グループのラベル対応を有効にする。
2. Security & Compliance PowerShell で `Execute-AzureAdLabelSync` を実行し、ラベルを Microsoft Entra ID に同期する。

これで、ラベルの範囲に Groups & sites を選べるようになります。

設定ごとの動きは、次のとおりです。[^c1-27]

- **プライバシー**: Public か Private を選ぶと、ラベルを付けたときにプライバシーを設定して固定する。ラベルを外さない限り、変更できない。None なら、ユーザーが決められる。

- **外部ユーザーのアクセスと外部共有:** 所有者がゲストを追加できるかどうかと、SharePoint の外部共有の範囲 (全員、新規と既存のゲスト、既存のゲストのみ、組織内のみ)。
- **管理されていないデバイスと認証コンテキスト:** Microsoft Entra の条件付きアクセスが前提。認証コンテキストは、公開済みのものを選び、MFA や利用規約の同意を求められる。
- **プライベート チームの検出可否:** チェックを外すと、ラベルが付いたプライベート チームは、検出を許可されたユーザーにも見えなくなる。
- **共有チャネルの招待の制御:** Internal only、Same label only、Private team only の 3 つ。すでに招待されたチームを外せるのは Private team only だけで、個々のユーザーへの招待には影響しない。

管理されていないデバイスの設定には、SharePoint の app-enforced restrictions を使う条件付きアクセス ポリシーが要り、構成していなければ何も効きません。テナント全体の設定より緩い値を選んでも効かないので、テナントが「Allow limited, web-only access」なら、ブロックか限定アクセスを選びます。認証コンテキストに対応しないアプリでは、アクセスが拒否されます。

外部共有や認証コンテキストをラベルに入れると、サイトの所有者が、ラベルを付け替えるだけで、管理者だけに許された設定を変えられます。所有者に変えさせたくない設定は、ラベルに入れません。付いたラベルを後で変えられるのは、グループに接続されたサイトでは Microsoft 365 グループの所有者、そうでないサイトでは SharePoint のサイト管理者です。Teams の共有チャネルは、親チームのラベルを自動で引き継ぎ、外すことも替えることもできません。^[^c1-27]

サイトの既定の共有リンクの種類は、PowerShell でしか設定できません。MembersCanShare (MemberShareAll 、 MemberShareFileAndFolder 、

MemberShareNone) も同じです。[^c1-27]

運用の注意があります。ラベルを作ったら、まず少人数のテスト ユーザーに発行し、反映を待ってからチームやサイトを作れるか確かめて、全員に発行します。待ち時間は、新しいラベルで 1 時間以上、既存のラベルの変更で 24 時間以上で、Teams の共有チャネルの設定を含むときは、新しいラベルでも 24 時間以上です。ラベルを付けた後で、コンテナの設定を変えるのは避けます。外部ユーザーのアクセスの設定をラベルで外しても、すでに入っているゲストのアクセスは取り消されません。ラベルを削除するときは、先にすべてのラベル ポリシーから外し、1 時間待ち、選択肢から消えたのを確かめてから削除します。順序を守らないと、新しいチーム、グループ、サイトの作成が失敗することがあります。[^c1-27]

高い優先度のラベルが付いた文書を低い優先度のラベルのサイトへアップロードすると、SharePoint が検出し、監査イベントとメールが自動で作られます。ラベルの並び順は、この判定にも使われます。[^c1-27]

既存のサイトにまとめて付けるには、SharePoint Online Management Shell の `Set-SPOTenant` に `-SensitivityLabel` を指定します。サイトごとに別のラベルを付けるなら `Set-SPOSite` を使います。ラベルは名前でなく GUID で指定します。GUID は、Security & Compliance PowerShell の `Get-Label | ft Name, Guid` で調べます。サイトは、どの SharePoint サイト コレクションでも、OneDrive でも構いません。[^c1-27]

Power BI の項目への秘密度ラベル

Power BI でも、Microsoft Purview の同じラベルを使います。Power BI サービスでは、セマンティック モデル、レポート、ダッシュボード、データフローに付けられ、Power BI Desktop では .pbix に付けられます。使えるようにするための条件は、次のとおりです。[^c1-28]

- Fabric 管理ポータルの Information protection の設定で、Allow users to apply sensitivity labels for content を有効にする。
- ラベルを付けるユーザーが、Azure Information Protection Premium P1 か P2 のライセンスを持つ。
- 同じユーザーが、Power BI Pro か Premium Per User のライセンスを持つ。
- 同じユーザーが、対象の項目の作成と編集の権限を持つ。

挙動の大事な違いは、サービスの中と外です。

- **Power BI サービスの中:** ラベルはアクセスを変えない。アクセスは Power BI の権限だけで決まる。ラベルの暗号化は適用されない。
- **サービスの外へ出るとき:** 対応するエクスポートの経路で、ラベルが自動で付き、暗号化も効く。
- **Power BI Desktop:** 暗号化つきのラベルは、.pbix を開けるかどうかに影響する。権限が足りないユーザーは、ファイルを開けない。

対応するエクスポートの経路は、次のとおりです。

- Excel、PDF、PowerPoint への書き出し (PowerPoint は Export as image のときだけ)
- Analyze in Excel
- Microsoft 365 E3 以上での、Excel のライブ接続ピボットテーブル
- サービスからの .pbix のダウンロード

非対応の経路では、ラベルも暗号化も付きません。Power BI の管理者は、非対応の経路からのエクスポートをブロックできます。レポートとセマンティック

モデルのラベルが異なる場合、.pbix のダウンロードでは、より制限の強い方が付きます。[^c1-28]

継承の仕組みが 4 つあります。[^c1-28]

- **作成時の継承:** 新しいレポートやダッシュボードは、親のラベルを引き継ぐ。
- **データソースからの継承:** ラベル付きの Azure Synapse Analytics と Azure SQL Database のデータから引き継ぐ。
- **ダウンストリーム継承:** 付けたラベルが、それから作られたコンテンツにも自動で付く。
- **エクスポート時の継承:** ファイルに書き出すとき、ラベルがファイルに付く。

既定のラベルのポリシーは、ラベルの無いコンテンツに既定のラベルを自動で付けます。必須ラベルのポリシーは、ラベルを付けさせますが、親ラベルが付いた項目は対象にならず、すり抜けます。マルチテナントと B2B のシナリオには対応しません。[^c1-28]

Microsoft Defender for Cloud Apps で秘密度ラベルを適用する

Microsoft Defender for Cloud Apps は、Purview の秘密度ラベルをファイルに適用できます。対象は Box、Google Workspace、SharePoint Online、OneDrive のファイルです。適用はファイルポリシーのガバナンス アクションとして行い、ラベルの設定によっては暗号化も付きます。[^c1-29]

前提は次のとおりです。[^c1-29]

- Defender for Cloud Apps と Microsoft Purview の両方のライセンスがある。
- Microsoft 365 のアプリ コネクタを有効にしている。

- 適用するラベルは、ラベル ポリシーで発行済みである。
- ラベルの範囲が、少なくとも Files と Emails を含む。
- ラベルの構成で、Defender for Cloud Apps がラベルの情報を読めるよう、権限が認証済みの任意のユーザーか組織の全ユーザーに与えられている。

対象のファイルは、Word、Excel、PowerPoint の Office ファイルと PDF で、PDF には統合ラベルが必要です。ラベルの一覧は 1 時間ごとに取得され、適用できるファイルは 30 MB までです。新しいファイルを自動でスキャンするオプションは、Microsoft Defender ポータルの Information Protection の設定で有効にします。このオプションだけでは、既存のファイルは、変更されるまでスキャンされません。既存のファイルを調べるには、コンテンツ検査を含むファイルポリシーが 1 つ要ります。[^c1-29]

適用の方法は 2 つです。

- **手動:** Files の画面で、ファイルの 3 点メニューから Apply sensitivity label を選ぶ。
- **自動:** ファイルポリシーの Governance actions で Apply sensitivity label を選ぶ。ポリシーに一致したファイルに自動で付く。

1 日の Apply label の実行は、アプリごと、テナントごとに 100 件が上限です。上限に達すると一時停止し、翌日の 12:00 UTC 以降に自動で再開します。ポリシーを無効にすると、そのポリシーの待機中のラベル付けは中断されます。[^c1-29]

動作の限界を表で覚えます。[^c1-29]

状況	結果
Defender for Cloud Apps の外で保護なしのラベルが付いている	上書きはできるが、外せない
Defender for Cloud Apps の外で保護つきのラベルが付いている	外せない
Defender for Cloud Apps がすでにラベルを付けたファイル	上書きしない
パスワード保護のファイル	ラベルを読めない
空のファイル、チェックアウトが必須のライブラリのファイル	ラベルを付けない
1 つのファイルに 2 つのファイルポリシーが適用される	最初に起動したポリシーのガバナンス アクションだけが保証される

ファイルポリシーは、2027 年 1 月 6 日に廃止される予定です。ファイルに基づく保護を続けるには、Microsoft Purview の DLP か自動ラベル付けポリシーへ移行します。[^c1-29][^c1-30]

Windows、ファイル共有、Exchange の情報保護を実装する [1.3]

Microsoft Purview Information Protection クライアントの計画と配置

Microsoft Purview Information Protection クライアントは、Office に組み込まれたラベル付けの外側へ、秘密度ラベルを広げる Windows 用のソフトウェアです。Office 以外のファイルにも対応し、Azure Information Protection (AIP) 統一ラベル付けクライアントの後継です。構成部品は 4 つです。[^c1-31]

部品	役割
Information protection scanner	ネットワーク共有や SharePoint Server のライブラリで、ファイルを探して、ラベルを付けて、暗号化する
Information protection file labeler	ファイルエクスプローラーから、ラベルと暗号化を付ける
Information protection viewer	暗号化されたファイルを表示する
PowerShell モジュール	ファイルのラベルを調整し、スキャナーを導入して構成する

このクライアントは Windows でしか動きません。Office のラベル付けは Office 組み込みの機能が担うので、Office アドインはありません。入れるのは、ファイルエクスプローラーでラベルを付けたい PC、PowerShell でファイルを扱いたい PC、スキャナーのサーバーです。[^c1-31]

導入の前提は表のとおりです。[^c1-31]

項目	要件
OS	Windows 11 (Enterprise multi-session を含む)、Windows 10 (x64)、Windows Server 2019、Windows Server 2016
ARM64	viewer と file labeler だけ対応。スキャナーと PowerShell は非対応
.NET Framework	4.7.2 以上。なければインストーラーが入れ、再起動が要る
Windows PowerShell	4.0 以上。インストーラーは確認も導入もしない

項目	要件
契約と ID	ラベル付けに使えるクラウドの契約と Microsoft Entra ID。オンプレミスのアカウントを使うなら、ディレクトリの統合も要る
導入する人	クライアント PC のローカル管理者

インストーラーは `PurviewInfoProtection.exe` と `.msi` の 2 種類です。サイレントのインストールは、次のとおりです。[^c1-31]

```
PurviewInfoProtection.exe /quiet
PurviewInfoProtection.exe PowerShellOnly=true /quiet
```

2 行目は PowerShell のコマンドレットだけを入れますが、スキャナーのサーバーには完全なクライアントが要ります。インストール後は、File Explorer を再起動します。[^c1-31]

暗号化なしのラベルなら、Office 以外にも、PDF、Project (mpp)、Publisher (pub)、XPS、画像 (jpg、png、tif など)、dwfx、psd、dng などに付けられます。[^c1-31] 暗号化には 2 つの水準があります。

水準	対象	権限の強制
ネイティブ暗号化	テキストと画像、Office (Word、Excel、PowerPoint)、PDF など、Rights Management に対応するファイル	強制される
汎用 (generic) 暗号化	それ以外のファイル (vsd、rtf など)。pfile という形式に包む	強制されない。認証と、開いた記録 (監査ログ) だけ

汎用暗号化のファイルには、共同所有者 (co-owner) の権限を割り当てること
が推奨されています。ラベルの名前と説明は自動では翻訳されないので、ユ
ーザーの言語で見せるには、`Set-Label` の `LocaleSettings` で翻訳を設定しま
す。[^c1-31]

クライアントでファイルを管理する (PowerShell のコマンドレット)

クライアントの PowerShell モジュール (PurviewInformationProtection)
の、ファイル操作の中心は 3 つです。[^c1-32]

コマンドレット	役割
<code>Get-FileStatus</code>	ファイルのラベルと保護の状態を調べる
<code>Set-FileLabel</code>	ラベルと保護を付ける (手動、自動、カスタム権限)
<code>Remove-FileLabel</code>	ラベルや保護を外す

`Set-FileLabel` は、ラベルの ID (GUID) を `-LabelId` で渡して手動で付けます。
内容を検査して自動で付けるときは `-AutoLabel` を付けます。付けた時点で、
既存のラベルや保護は置き換えられます。主なパラメーターは次のとおりで
す。[^c1-32]

- **-AutoLabel:** 自動ラベル付けのモードで動かす。付けなければ手動モード。
- **-Force:** 条件が当てはまるとき、既存のラベルを置き換える。
- **-JustificationMessage:** ラベルを下げる、外す、保護を外すときの理由。
ポリシーが理由を求めるのに渡さないと、ラベルは付かず、状態が
Skipped、コメントが Justification required になる。
- **-Owner:** ラベルや保護を付ける対象の所有者。

- **-PreserveFileDetails:** 更新日時を変えない (SharePoint では更新日時と更新者を変えない)。
- **-WhatIf:** 実行せずに、結果を確認する。`-DiscoveryInfoTypes` で、探す SIT を ID で指定できる。

カスタム権限は、`New-CustomPermissions` で作ったオブジェクトを `-CustomPermissions` に渡します。実際の使い方は、パイプラインで絞ってから付ける形が基本です。ラベルが付いていないファイルだけに General を付ける例は、次のとおりです。[^c1-32]

```
Get-ChildItem C:\Projects\*.docx -File -Recurse |  
Get-FileStatus |  
Where-Object {$_.IsLabeled -eq $False} |  
Set-FileLabel -LabelId d9f23ae3-1234-1234-1234-f515f824c57b
```

`Remove-FileLabel` は、何を外すかをスイッチで選びます。[^c1-32]

- **-RemoveLabel:** ラベルを外す。保護をテンプレートで付けていたラベルなら、保護も一緒に外れる。カスタム権限で付けた保護は残る。
- **-RemoveProtection:** 保護だけを外す。
- **両方を指定:** ラベルと保護の両方を外す。

ラベルを外すのに理由が必要なポリシーなら、`-JustificationMessage` を渡します。

```
Remove-FileLabel C:\Projects\Analysis.docx -RemoveProtection -  
RemoveLabel -JustificationMessage 'The previous label no longer  
applies'
```

.zip 中のファイルを検査するには、スキャナーが `Set-FileLabel` を使います。[^c1-31]

情報保護スキャナーでオンプレミスのデータを一括分類する

スキャナーは、Windows Server で動くサービスで、オンプレミス (on-premises) のファイルを探して一括で分類 (bulk classification) し、保護します。対象は、SMB または NFS (プレビュー) の UNC パスのネットワーク共有と、SharePoint Server の文書ライブラリです。リアルタイムでは動きません。指定した場所を順番にクロールし、1 回だけ、または繰り返して実行します。実行ファイルとシステム ファイルは、自動で除外されます。ラベルは Microsoft Purview ポータルで構成したものを使います。[^c1-33]

検査では、Windows の IFilter でファイルの文字を取り出し、SIT やパターンで判定します。検査できない種類のファイルには、ポリシーの既定のラベルか、スキャナーに設定した既定のラベルが付きます。暗号化なしのラベルに対応しない種類 (.txt など) には、暗号化するラベルでその種類を保護の対象に加えない限り、ラベルを付けられません。スキャナーが既定で暗号化するのは、Office のファイルと PDF だけです。[^c1-33][^c1-35]

環境の前提は、次の表のとおりです。[^c1-34]

項目	要件
サーバー	4 コア、RAM 8 GB、空き 10 GB。64 ビットの Windows Server 2016、2019、2022、2025 (Server Core と Nano Server は非対応)
.zip の検査	Microsoft Office iFilter を入れる
SQL Server	2016 以上の Enterprise か Standard。Express はテスト環境向け。大文字小文字を区別しない照合順序

項目	要件
インストールする人	SQL Server の Sysadmin。構成データベースを自動で作り、サービス アカウントに db_owner を付ける
構成 DB の大きさ	100 KB + ファイル数 × (1000 + 4 × 平均ファイル名の長さ)
クライアント	完全版を入れる (PowerShell だけでは不可)
ラベル	少なくとも 1 つ (スキャナー アカウント用)

100 万ファイル、平均ファイル名 250 バイトなら、構成 DB は約 2.0 GB です。小規模でなければ、SQL Server はスキャナーと別のマシンに置くのが推奨です。[^c1-34]

サービス アカウントの条件は次のとおりです。[^c1-34]

- **種類:** Active Directory のアカウントで、Microsoft Entra ID に同期されている。
- **Log on locally と Log on as a service:** Log on locally はインストールと構成に必要で、動作を確認したら外してよい。Log on as a service はインストール中に自動で付与される。
- **リポジトリの権限:** ファイル共有は Read、Write、Modify (検出だけなら Read で足りる)。SharePoint は Full Control。
- **暗号化の再保護や解除をするラベルの場合:** Azure Rights Management のスーパーユーザーにして、スーパーユーザー機能を有効にする。

Log on locally を一時的にでも付けられない場合は、Set-Authentication の -OnBehalfOf を使います。[^c1-35]

導入は、次の順に進めます。[^c1-35]

- 1. Purview ポータルで、スキャナーのクラスター、コンテンツスキャンジョブ、ジョブのリポジトリ(UNC パスや SharePoint の URL)を作る。
- 2. PowerShell で Install-Scanner -SqlServerInstance <名前> -Cluster <クラスター名> を実行し、サービスをインストールする。
- 3. Microsoft Entra にアプリを登録し、Set-Authentication で認証を設定する。
- 4. 最初の検出スキャンを実行し、レポートを確認める。
- 5. ジョブを本番の設定に切り替え、Start-Scan でスキャンを開始する(止めるのは Stop-Scan)。

手順 3 のアプリには、Azure Rights Management Service の Content.DelegatedReader と Content.DelegatedWriter を付けます。Microsoft Information Protection Sync Service の UnifiedPolicy.Tenant.Read も付け、管理者の同意を与えます。[^c1-35]トークンの有効期間は、クライアントシークレットの設定(1 年、2 年、無期限)で決まり、切れたらやり直します。

コンテンツスキャンジョブの最初の構成は、検出だけで終わる安全な設定にします。[^c1-35]

設定	最初の検出(初期構成)	本番の運用
Schedule	Manual	Always
Info types to be discovered	Policy only(初期構成で変更)	必要なら All

設定	最初の検出 (初期構成)	本番の運用
Enforce sensitivity labeling policy	Off (レポートのみ)	On
Label files based on content	On	On
Default label	Policy default	用途で選ぶ
Relabel files	Off	必要なら On
Preserve "Date modified" など	On	On
Default owner	Scanner Account	用途で選ぶ

本番にするには、ジョブの Schedule を Always に、Enforce sensitivity labeling policy を On に変えます。PowerShell なら、`Set-ScannerContentScan -Schedule Always -Enforce On` です。最初の周回はすべてのファイルを検査するので時間がかかり、2 周目以降は既定で新しいファイルと変更されたファイルだけを検査します。ただし、条件や自動ラベル付けの設定を変えると、すべてのファイルを再スキャンします。[^c1-35]

目的別の設定は、次のとおりです。[^c1-35]

- **未ラベルのファイルすべてに既定のラベルを付ける:** Label files based on content を Off、Default label を Custom (使うラベル) にする。ラベル済みのファイルにも付けるなら、Relabel files と Enforce default label も On にする。
- **ラベルをすべて外す:** Label files based on content を Off、Default label を None、Relabel files と Enforce default label を On にする。保護も外れるが、ラベルとは別に付けた保護は残る。

スキャナーのライセンスは、機能で分かります。スキャナーによる探索（検出）は Microsoft 365 E3 で使えます。ラベル付け（自動やポリシーによるものを含む）は、Microsoft 365 E5 か Information Protection and Governance が必要です。[^c1-36]

Microsoft Purview Message Encryption の設計と実装

Microsoft Purview Message Encryption は、組織の内外の相手と暗号化したメールをやり取りする仕組みです。Azure Rights Management の上で動き、暗号化の方法は 3 つあります。Rights Management テンプレート、Do Not Forward、Encrypt-only です。管理者は、Exchange のメールフロールール（トランスポート ルール）で、条件に合うメールを自動で暗号化できます。Office 365 Message Encryption (OME) という旧称の仕組みは、2023 年 7 月 1 日に非推奨になりました。[^c1-37][^c1-39]

受信者の体験は、相手によって変わります。[^c1-37][^c1-43]

受信者	体験
Microsoft 365 の組織のユーザー、Microsoft アカウント (outlook.com など)	対応する Outlook で、そのまま読める（インライン）
Gmail、Yahoo	ラッパー メールが届き、暗号化メッセージポータルで認証して読む（リンク型）
Outlook 以外のメール クライアント	暗号化メッセージ ポータルで読む

Do Not Forward（転送不可）は、受信者が転送、印刷、コピーをできません。Encrypt-only は、受信者が転送、印刷、コピーをできますが、保護を外せません。Rights Management テンプレートは、管理者が作った権限の組を使います。[^c1-23]

導入の流れは、次のとおりです。[^c1-38]

1. Azure Rights Management が有効かを確かめる (有効なら、Message Encryption は自動で有効になる)。
2. Exchange Online PowerShell で `Get-IRMConfiguration` を実行し、`AzureRMSLicensingEnabled` が `$True` を確かめる。`$False` なら `Set-IRMConfiguration` で `$True` にする。
3. `Test-IRMConfiguration -Sender <送信者> -Recipient <受信者>` で全体を確かめる。結果が OVERALL RESULT: PASS ならよい。
4. メールフロールールを作る、または既存のルールを更新する。

Azure Rights Management に対応する前の AD RMS は、Message Encryption と互換性がありません。AD RMS を使っている場合は、先に Azure Rights Management に移行します。既存のメールフロールールを更新しないと、ユーザーには古い HTML 添付の形式の暗号化メールが届き続け、新しい体験になりません。ハイブリッド構成のオンプレミス ユーザーは、メールが Exchange Online を経由するときだけ、暗号化メールを送受信できます。[^c1-38][^c1-39]

メールフロールールは、Exchange 管理センターの Mail flow > Rules で作ります。暗号化するルールは、次の順に設定します。[^c1-39]

1. Apply this rule if で条件を選ぶ (受信者が特定のアドレス、受信者が組織外、件名やメッセージに特定の語を含む、など)。
2. Do the following で、Modify the message security を選ぶ。
3. Apply Office 365 Message Encryption and rights protection を選ぶ。
4. RMS テンプレート (Encrypt、Do Not Forward など) を選んで保存する。

暗号化を外すルールでは、Modify the message security の中の Remove Office 365 Message Encryption and rights protection を選びます。添付の

保護も外すなら、Remove attachment rights protection も選びます。

注意があります。組織外の送信者から届く受信メールは、メールフロールールでは暗号化できません。ルールを組んでも、暗号化されずに配信されます。

[^c1-39]

ライセンスは、Office 365 と Microsoft 365 の E3 と E5、Microsoft 365 Business Premium、Office 365 の A1、A3、A5 などに含まれ、追加は要りません。Office 365 E1 や Exchange Plan 1、Plan 2、Microsoft 365 Business Basic などには、Azure Information Protection Plan 1 を足すと使えます。

[^c1-40]

Microsoft Purview Advanced Message Encryption

Advanced Message Encryption は、Message Encryption に、外部の受信者向けの管理を足す上位の機能です。足されるのは、複数のブランドテンプレート、メールの有効期限、メールの失効(revoke)、暗号化メッセージ ポータルのアクティビティ ログです。SIT やキーワードに一致したメールを自動で対象にするポリシーも組めます。[^c1-41]

ライセンスは、次のいずれかで使えます。[^c1-36]

- Microsoft 365 E5、A5、G5
- Microsoft Purview Suite
- Information Protection and Governance
- Office 365 E5、A5、G5

有効期限と失効は、どちらも次の 2 つの条件を同時に満たす場合にだけ効きます。[^c1-41][^c1-42][^c1-43]

- メール宛先が、組織の外の受信者であること。

- 受信者が、暗号化メッセージ ポータル(リンク型の体験)で読むこと。

ポータルで読ませるには、カスタムのブランドテンプレートを作り、メールフロー ルールでそのテンプレートを適用します。テンプレートを使うと、ラッパー メールが付き、受信者は通知メールのリンクからポータルに入ります。Microsoft 365 のユーザーや Microsoft アカウントのユーザーが対応する Outlook で読むインライン表示のメールは、有効期限を付けられず、失効もできません。^{[^c1-41][^c1-43]}

有効期限は、テンプレートを作るときに `-ExternalMailExpiryInDays` で日数を指定します。値は 1~730 です。期限が切れたメールを開こうとすると、ポータルにエラーが出ます。受信者には、ラッパー メールで期限が見えます。^[^c1-42]

```
New-OMEConfiguration -Identity "Expire in 7 days" -  
ExternalMailExpiryInDays 7
```

失効の手順は次のとおりです。^[^c1-43]

1. メッセージの ID (Message ID) を調べる (メッセージトレースか、暗号化レポート)。
2. `Get-OMEMessageStatus -MessageId "<id>"` で、失効できるか (IsRevocable) を確かめる。
3. `Set-OMEMessageRevocation -Revoke $true -MessageId "<id>"` で失効させる。ポータルの暗号化レポートの Revoke message でもよい。

送信者は、Outlook on the web の送信済みフォルダーで、メールの上の Remove external access を選んで失効させます。これは、ソーシャル アカウント (gmail.com や yahoo.com) の受信者 1 人に送ったメールのように、リン

ク型で届いたメールに限られます。失効したメールを受信者がポータルで開くと、「The message has been revoked by the sender」というエラーが出て、読めません。Encrypt-Only のように Outlook on the web から直接暗号化したメールも、失効の対象です。管理者の実行には、Compliance Administrator か Exchange Administrator の権限が要ります。[^c1-43]

ブランドテンプレートの操作は、コマンドレットで分かります。[^c1-44]

コマンドレット	役割	必要なライセンス
Get-OMEConfiguration	テンプレートの設定を見る	Message Encryption で可
Set-OMEConfiguration	既定のテンプレート、または作ったカスタム テンプレートを変更する (既定は削除できない)	Message Encryption で可
New-OMEConfiguration	カスタム テンプレートを作る	Advanced Message Encryption のみ
Remove-OMEConfiguration	カスタム テンプレートを削除する	Advanced Message Encryption のみ

Message Encryption だけでは、既定のテンプレート 1 つだけを編集できません。変えられる要素は、ロゴ、背景色、導入文や免責文などの文言、プライバシー文書の URL です。ワンタイム パスコードの可否 (-OTPEnabled) と、ソーシャル ID でのサインインの可否 (-SocialIdSignIn) も変えられます。[^c1-44]

複数のテンプレートで部署ごとに外観や認証の方法を変えたいときは、Advanced Message Encryption が要ります。必要な権限は Compliance Administrator などです。

サンプルはここまでです

続き(第2章～巻末)は、SC-401 問題集のご購入で、頻出度別ノート・暗記用ノートと合わせて3点すべてダウンロードできます。

SAMPLE

Microsoft Information Security Administrator (SC-401) 学習用テキスト(無料サンプル)

版

2026年10月版(SC-401 出題範囲(Study guide・Skills measured as of October 28, 2026)準拠)

発行

IT資格道場(<https://www.shikaku-doujou.com>)

お問い合わせ

info@shikaku-doujou.com

Microsoft、Microsoft 365、Microsoft Purview、Microsoft Defender、Microsoft Teams、Microsoft Entra、Microsoft Copilot、Azure、Exchange、SharePoint、OneDrive および Microsoft の製品名・サービス名は、Microsoft Corporation の米国およびその他の国における商標または登録商標です。記載されているその他の会社名・製品名・サービス名は、各社の商標または登録商標です。

本教材は公式シラバスの内容を基に作成したもので、Microsoft Corporation との提携・承認関係はありません。

本文・図表・設問はすべてオリジナルの著作物です。無断での転載・複製・再配布・二次販売はできません。お気づきの点は info@shikaku-doujou.com までご連絡ください。