mstep

Microsoft 365 Enterprise セキュリティ基礎と応用

（EMS - Microsoft Intune、Azure Information Protection、Microsoft Cloud App Security）

レベル 200 - 300

2021.04.08
Ver 4.4m

3-1

3 章：Azure Information Protection（AIP）

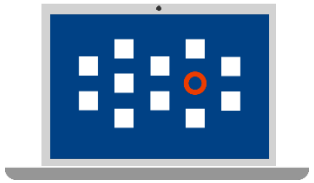
- Microsoft Information Protection の概要
- データの分類
- データの保護
- データの監視と追跡

Azure Information Protection（AIP）

3 章

ID とアクセスの管理

Azure Active Directory Premium



オンプレミス の ID 保護

Microsoft Defender for Identity (Azure ATP)

エンドポイントの管理

Microsoft Intune + Configuration Manager

情報の保護

Azure Information Protection (AIP)

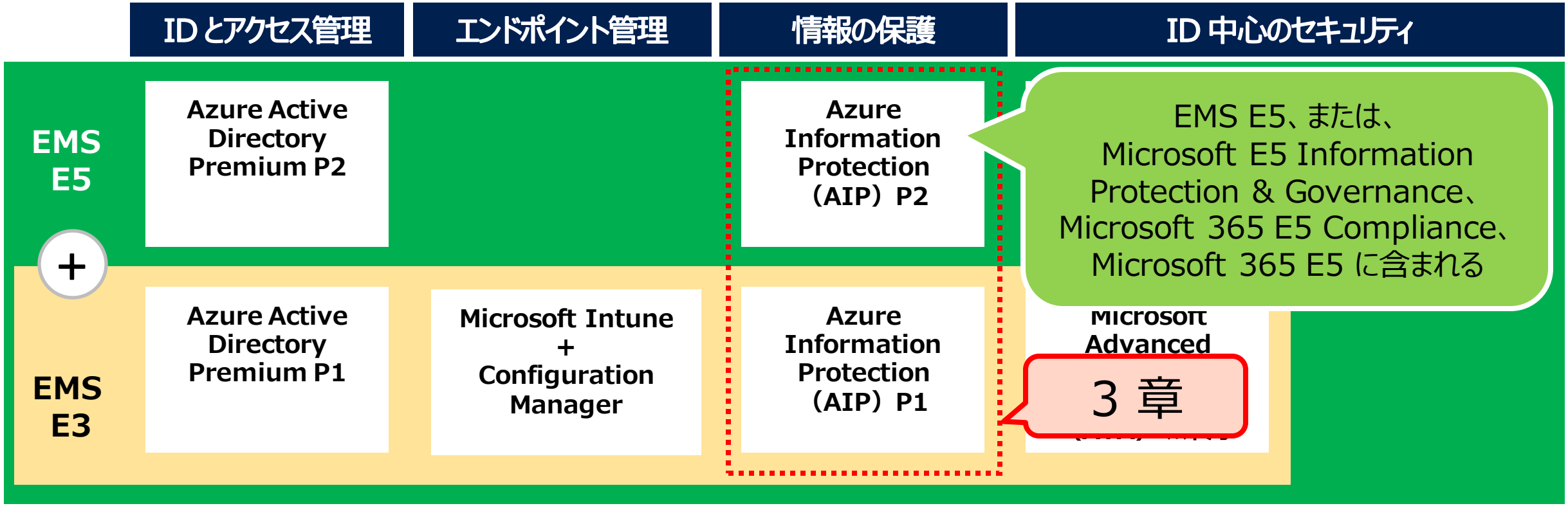
クラウド アプリのセキュリティ

Microsoft Cloud App Security (MCAS)

Enterprise Mobility + Security（EMS）E5

EMS と Azure Information Protection（AIP）

- EMS E5 に、AIP P2 のライセンスが含まれる



「Enterprise Mobility + Security 価格オプション」
https://www.microsoft.com/ja-jp/microsoft-365/enterprise-mobility-security/compare-plans-and-pricing

みなさんの組織では、徹底して実行できていますか？

すべての電子データ
を分類

＋

重要度に応じて保護
（暗号化、アクセス制御）

経済産業省の情報セキュリティ管理基準

※ 国際規格（ISO27001、27002）に準拠した、情報セキュリティ監査のための管理基準

出典：経済産業省「情報セキュリティ管理基準（平成２８年改正版）」から一部抜粋

8.2　情報分類

目的：組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。

8.2.1　情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類する。

8.2.1.1　情報の分類及び関連する保護管理策には、情報を共有又は制限する業務上の要求、及び法的要求事項を含める。

8.2.1.2　情報資産の管理責任者は、その情報の分類に対して責任を負う。

8.2.1.3　分類体系には、分類の規則及びその分類を時間が経ってからレビューするための基準を含める。

8.2.1.4　分類体系における保護レベルは、対象とする情報についての機密性、完全性、可用性及びその他の特性を分析することによって評価する。

8.2.1.5　分類体系は、アクセス制御方針と整合させる。

8.2.1.6　それぞれのレベルには、分類体系の適用において意味をなすような名称を付ける。

8.2.1.7　分類体系は、組織[21]し、保護に関にする。

分類

保護

8.2.3　資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施する。

8.2.3.1　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順を作成する。

8.2.3.2　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、各レベルの分類に応じた保護の要求事項に対応するアクセス制限に関する手順を含める。

8.2.3.3　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、資産の認可された受領者について、正式な記録を維持するための手順を含める。

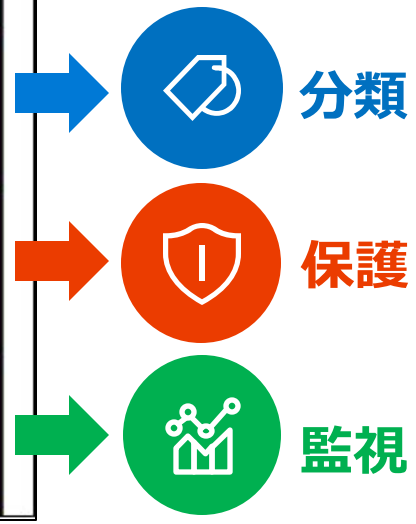
監視

経済産業省の営業秘密管理指針

- 企業が営業秘密の不正な流出等による被害に遭った場合、不正競争防止法により、法的保護を受けるために必要となる最低限の水準の対策を示している

表 4.4-1 営業秘密管理・保護システムに必要なセキュリティ対策

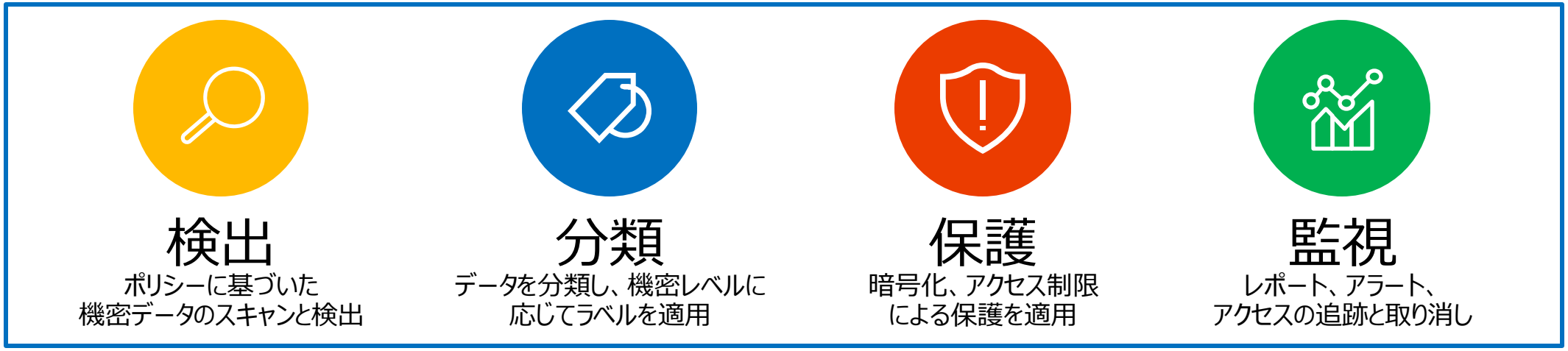
No	脅威	主な対策	PP での扱い
1	重要情報が営業秘密と認識されず、不正持出・不正利用される。	秘密情報の表示	技術対策（必須）
2	重要情報が誰にでもアクセスされ、不正持出・不正利用される。	アクセス制御	技術対策（必須）
3	重要情報へのアクセス記録が不明で、いつ不正持出・不正利用されたのかわからない。	監査・ログ記録	技術対策（必須）

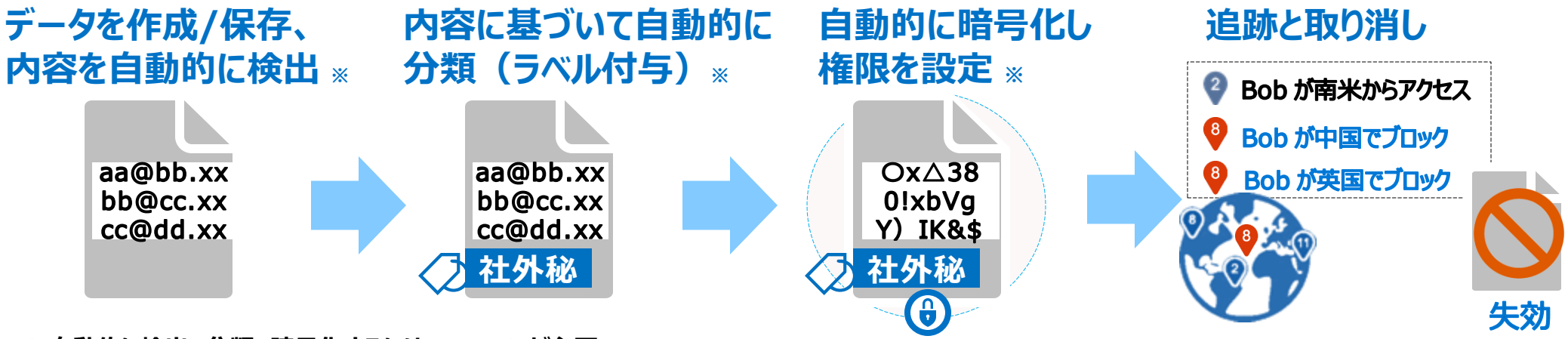


出典： IPA「営業秘密管理・保護システムに関するセキュリティ要件調査」から一部抜粋
https://www.ipa.go.jp/security/fy27/reports/eigyopp/20160304

Microsoft Information Protection

- 組織の機密情報を保護するための、情報保護ソリューション
  （購入できるサブスクリプションや製品のことではない）





※2 自動的に検出、分類、暗号化するには AIP P2 が必要

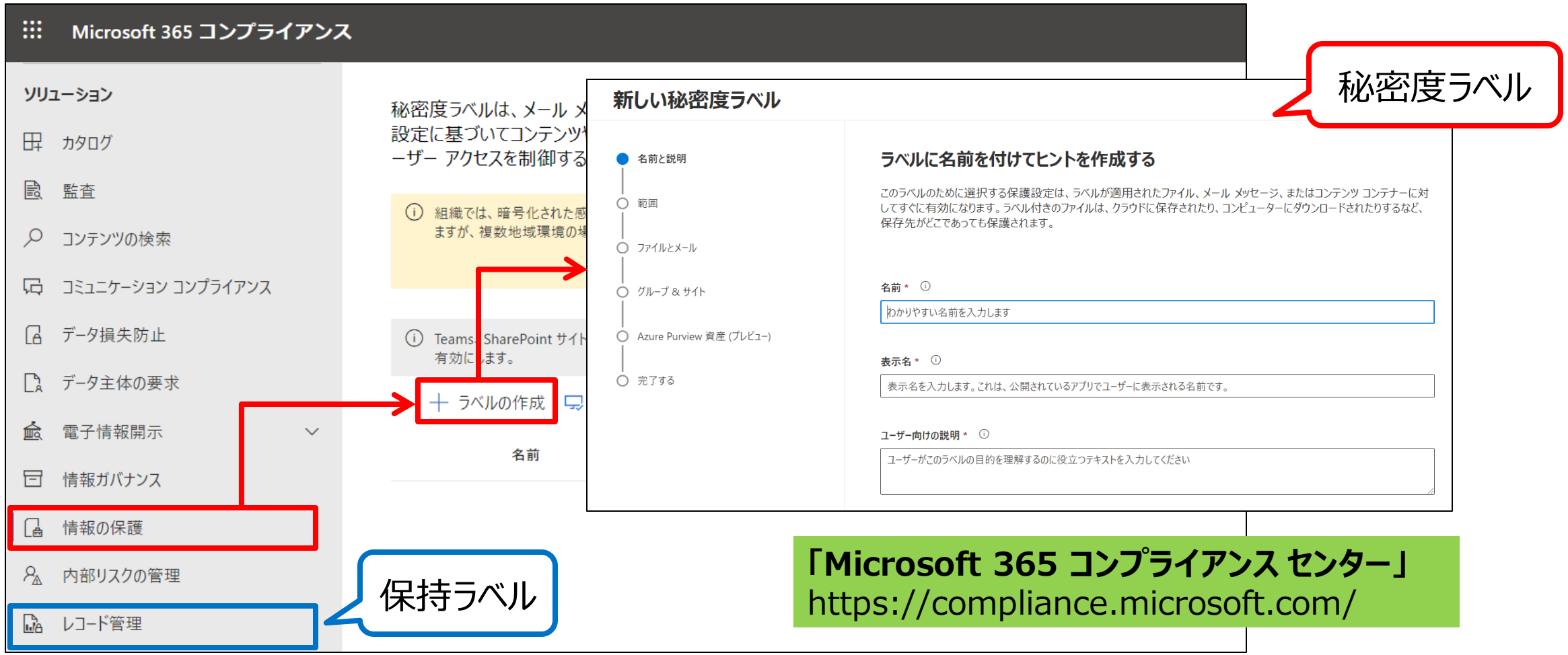
Microsoft Information Protection の主な機能

- **統一されたラベルの管理**
  - **秘密度ラベル ・・・ 分類と保護**
  - 保持ラベル ・・・ 分類と保持

- Office アプリに組み込まれている
  エンドユーザーのラベル付けエクスペリエンス
- Windows が統合ラベルを理解し、データに保護を適用する機能
- Microsoft Information Protection SDK
- ラベル付きで保護された Pdf を表示するための
  Adobe Acrobat Reader の機能

「Microsoft 365 コンプライアンス センター」でラベルを管理

- [情報保護] – [+ ラベルの作成] から、統合された「秘密度」ラベルを作成できる
- [レコード管理] – [ファイル計画] – [+ ラベルの作成] から、統合された「保持」 ラベルを作成できる



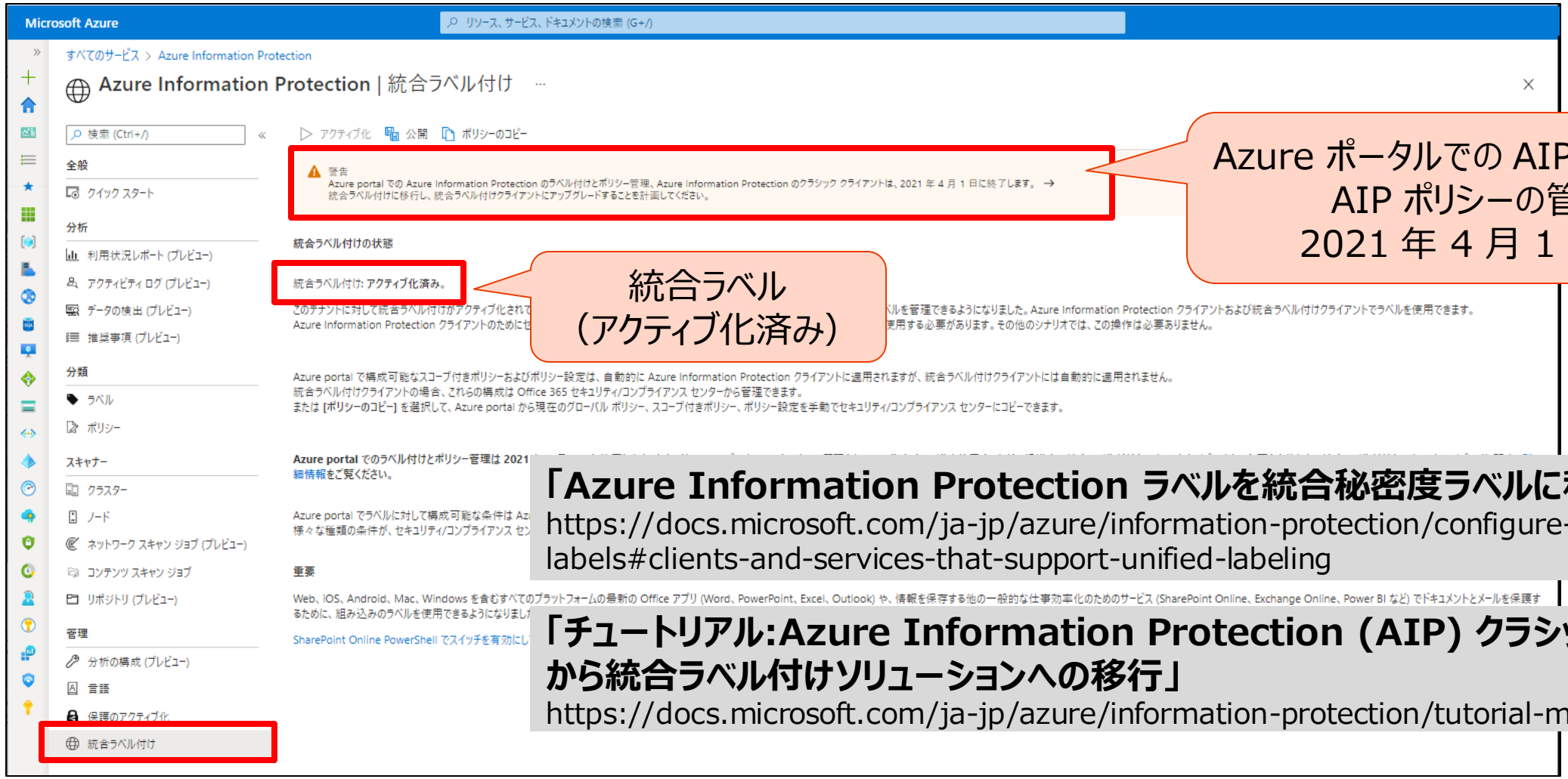
[参考] 従来のラベルから「統合ラベル」へ進化

- 少し前まで、2 パターンのラベルが存在していました・・・
  - Microsoft 365 のラベル
    - Microsoft 365 コンプライアンス センターで構成/管理
    - もともとは、保持ラベル ⇒ 保持ラベルと秘密度ラベルに進化
  - 従来の AIP のラベル（現在は、クラシック ラベル と呼んでいる）
    - Azure ポータルで構成/管理
    - もともと、秘密度ラベルと保持ラベル

- 進化して「統合ラベル」に！
  - 「Microsoft 365 コンプライアンス センター」で構成/管理
  - 秘密度ラベルと保持ラベル

[参考] Azure ポータルでのポリシー管理の終了

- Azure ポータルの [Azure Information Protection] の [統合ラベル付け]



Azure ポータルでの AIP のラベル付けと
AIP ポリシーの管理は、
2021 年 4 月 1 日に終了

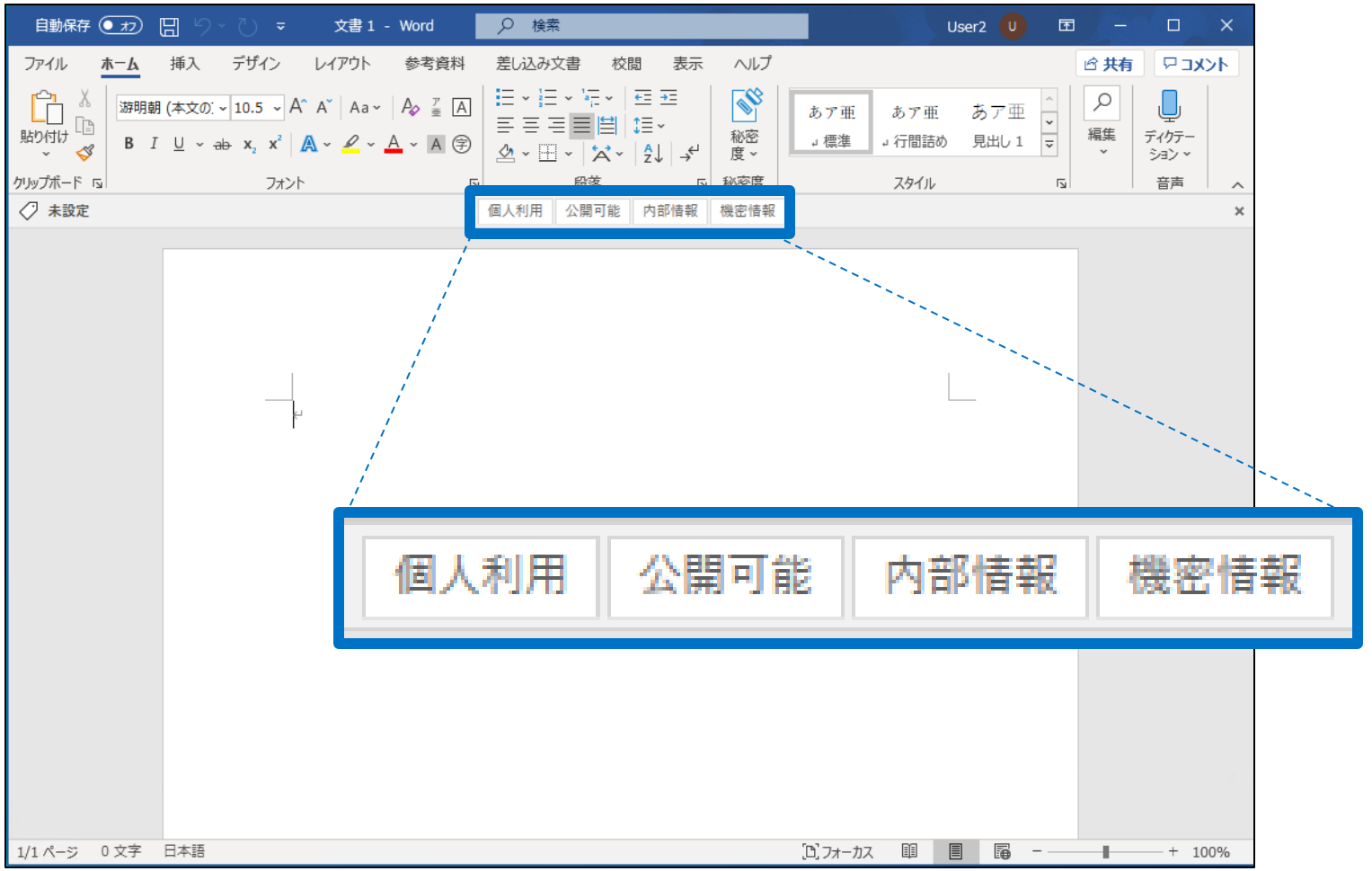
統合ラベル
（アクティブ化済み）

「Azure Information Protection ラベルを統合秘密度ラベルに移行する方法」
https://docs.microsoft.com/ja-jp/azure/information-protection/configure-policy-migrate-labels#clients-and-services-that-support-unified-labeling

「チュートリアル:Azure Information Protection (AIP) クラシック クライアントから統合ラベル付けソリューションへの移行」
https://docs.microsoft.com/ja-jp/azure/information-protection/tutorial-migrating-to-ul

秘密度ラベル

- 秘密度ラベルには、次の要素が含まれる
  - 視覚的なマーキング
    - 透かし文字
    - ヘッダー
    - フッター
  - 保護
    - 暗号化
    - アクセス許可
    - コンテンツ期限　など



秘密度ラベルの活用

- コンテンツの分類・・・ 単純にラベルによる分類（保護なし）
- コンテンツの暗号化およびコンテンツのマーキング（ヘッダーや透かし文字など）
- さまざまなプラットフォームをサポート（**Windows、macOS、iOS/iPadOS、Android**）
- **Office on the Web アプリと Office デスクトップ アプリでサポート（Word、Excel、Outlook、PowerPoint）**
- 外部ユーザーとの共有を行える Teams、Microsoft 365 グループ、SharePoint サイト、OneDrive for Business、OneDrive などのコンテンツを保護
- **Microsoft Cloud App Security** と連携すると、サード パーティーのアプリやサービス（Salesforce、Box、Dropbox など）のコンテンツを検出、分類、ラベル適用、保護できる
- **Power BI** にラベルを適用して表示し、サービスの外部に保存するときにデータを保護できる
- **Azure Purview** を使用して、Azure SQL Database や Azure BLOB ストレージのフォイルなどに秘密度ラベルを適用できる **Preview**
- **Microsoft Information Protection SDK** を使用して、サードパーティー アプリに対して、秘密度ラベルの読み取りと保護を適用

「秘密度ラベルの詳細」
https://docs.microsoft.com/ja-jp/microsoft-365/compliance/sensitivity-labels

Office アプリの秘密度ラベルの 2 つのソリューション

Microsoft 365 Apps for enterprise アプリとスタンドアロンの Office アプリ

- Microsoft 365 Apps for enterprise アプリの “組み込み” のラベル付けソリューション
  - Microsoft 365 Apps for enterprise は、Microsoft 365 サブスクリプションで使用できる Office のバージョン
  - Windows および macOS 用のデスクトップ Office のほか、Office iOS/iPadOS や Android Office にネイティブに組み込まれている
  - 個別のインストール不要

「企業内の Microsoft 365 アプリについて」
https://docs.microsoft.com/ja-jp/deployoffice/about-microsoft-365-apps

「Office アプリで秘密度ラベルを管理する」
https://docs.microsoft.com/ja-jp/microsoft-365/compliance/sensitivity-labels-office-apps

- AIP 統合ラベル付け “クライアント” ソリューション
  - **スタンドアロンの Office アプリ**で使用する “ラベル” 機能
  - 組み込みのラベル付けソリューションの代替手段
  - スタンドアロンの Office アプリを使用するデバイスに **“AIP 統合ラベル付けクライアント”** の **インストールが必要**
  - Windows コンピューターをサポート

「Azure Information Protection (AIP) の統合ラベルクライアントでサポートされるファイルの種類」
https://docs.microsoft.com/ja-jp/azure/information-protection/rms-client/clientv2-admin-guide-file-types

※ AIP クライアントがインストールされている場合、組み込みのラベル付けソリューションは Office アプリで無効になる（グループ ポリシーの設定で、組み込みのラベル付けを使用するように構成できる）

AIP 統合ラベル付けクライアント
Windows 10/8.1/8、Windows Server 2019/2016/2012 R2/2012

AIP P1

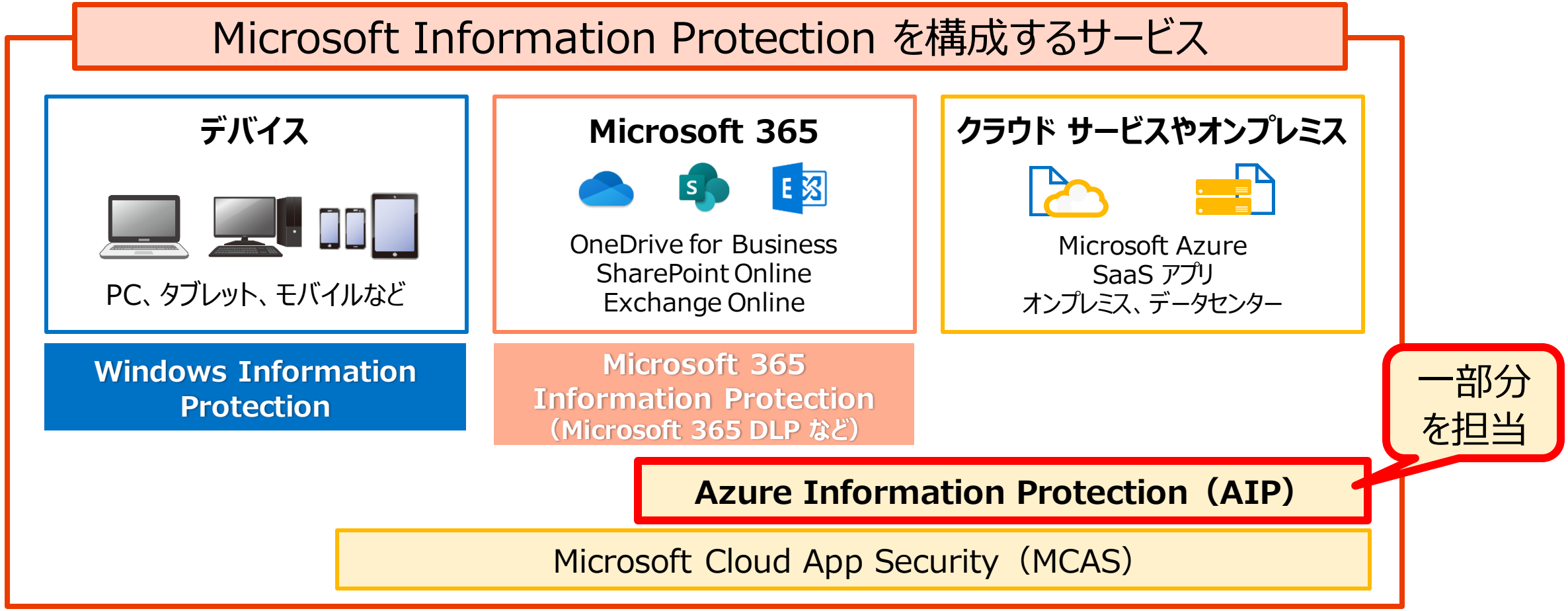
- ユーザーの Windows デバイス上のスタンドアロンの Office アプリで、統合ラベルの機能（ラベル付けや自動分類）を使用するには、**AIP 統合ラベル付けクライアント** のインストールが必要（無料）
  - https://www.microsoft.com/en-us/download/details.aspx?id=53018
  - .msi ファイルを Intune で展開することも、ユーザーが自分でインストールすることも可能

「管理者ガイド: Azure Information Protection 統合されたユーザー用ラベル付けクライアントのインストール」
https://docs.microsoft.com/ja-jp/azure/information-protection/rms-client/clientv2-admin-guide-install

「ユーザーガイド: Azure Information Protection 統合されたラベル付けクライアントをダウンロードしてインストールする」
https://docs.microsoft.com/ja-jp/azure/information-protection/rms-client/install-unifiedlabelingclient-app

Microsoft Information Protection を構成するサービス

- 複数のサービスで構成されている

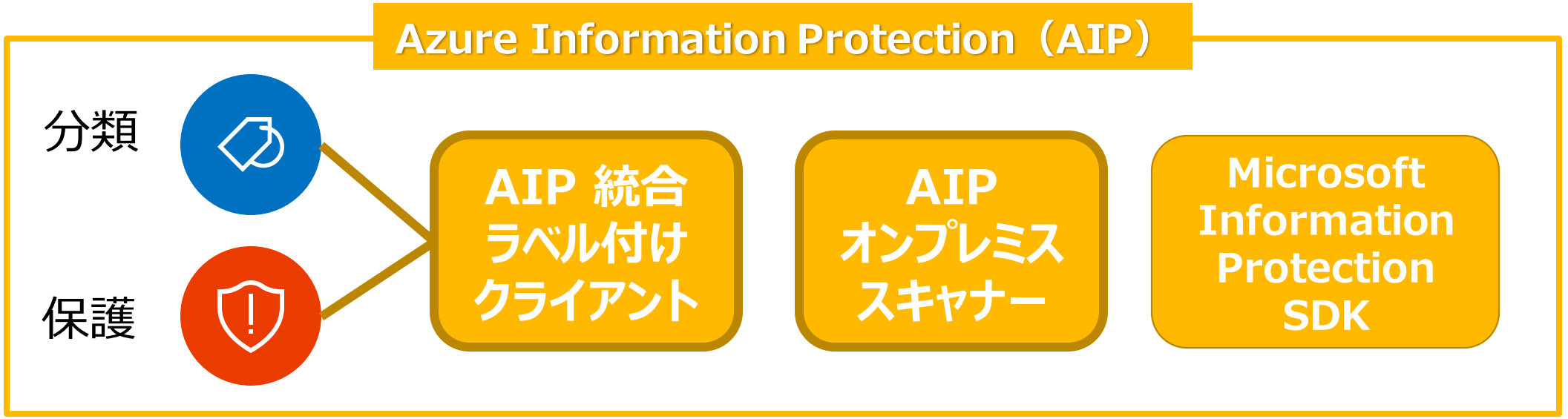


「機密情報の保護」
https://www.microsoft.com/ja-jp/security/technology/information-protection

Azure Information Protection の構成要素

AIP P1
AIP P2

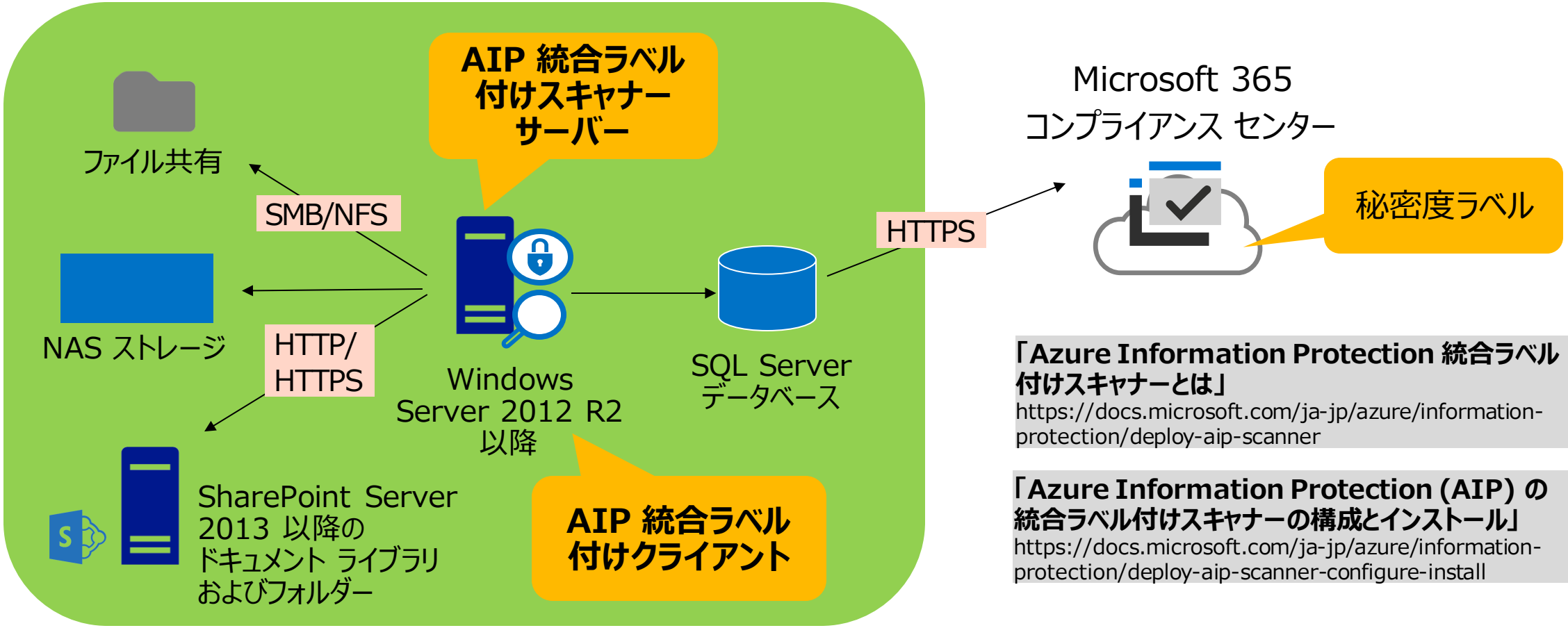
- 組織のコンテンツにラベルを適用してドキュメントや電子メールの検出、分類、および保護を行う、クラウド ソリューション
- Microsoft Information Protection（MIP）の一部



「Azure Information Protection とは」
https://docs.microsoft.com/ja-jp/azure/information-protection/what-is-information-protection

AIP 統合ラベル付けスキャナー（検出）

- Windows Server に Azure Information Protection 統合ラベル付けスキャナーを構成し、オンプレミスのデータ ストアに格納されているファイル内にある機密情報を検索
  - スキャナーはインストールされている IFilters を使い、ファイルにラベルを付ける必要があるかどうかを判断

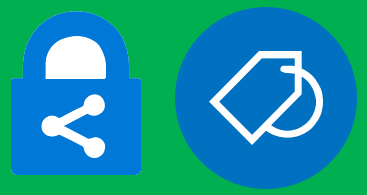


「Azure Information Protection 統合ラベル付けスキャナーとは」
https://docs.microsoft.com/ja-jp/azure/information-protection/deploy-aip-scanner

「Azure Information Protection (AIP) の統合ラベル付けスキャナーの構成とインストール」
https://docs.microsoft.com/ja-jp/azure/information-protection/deploy-aip-scanner-configure-install

3-2

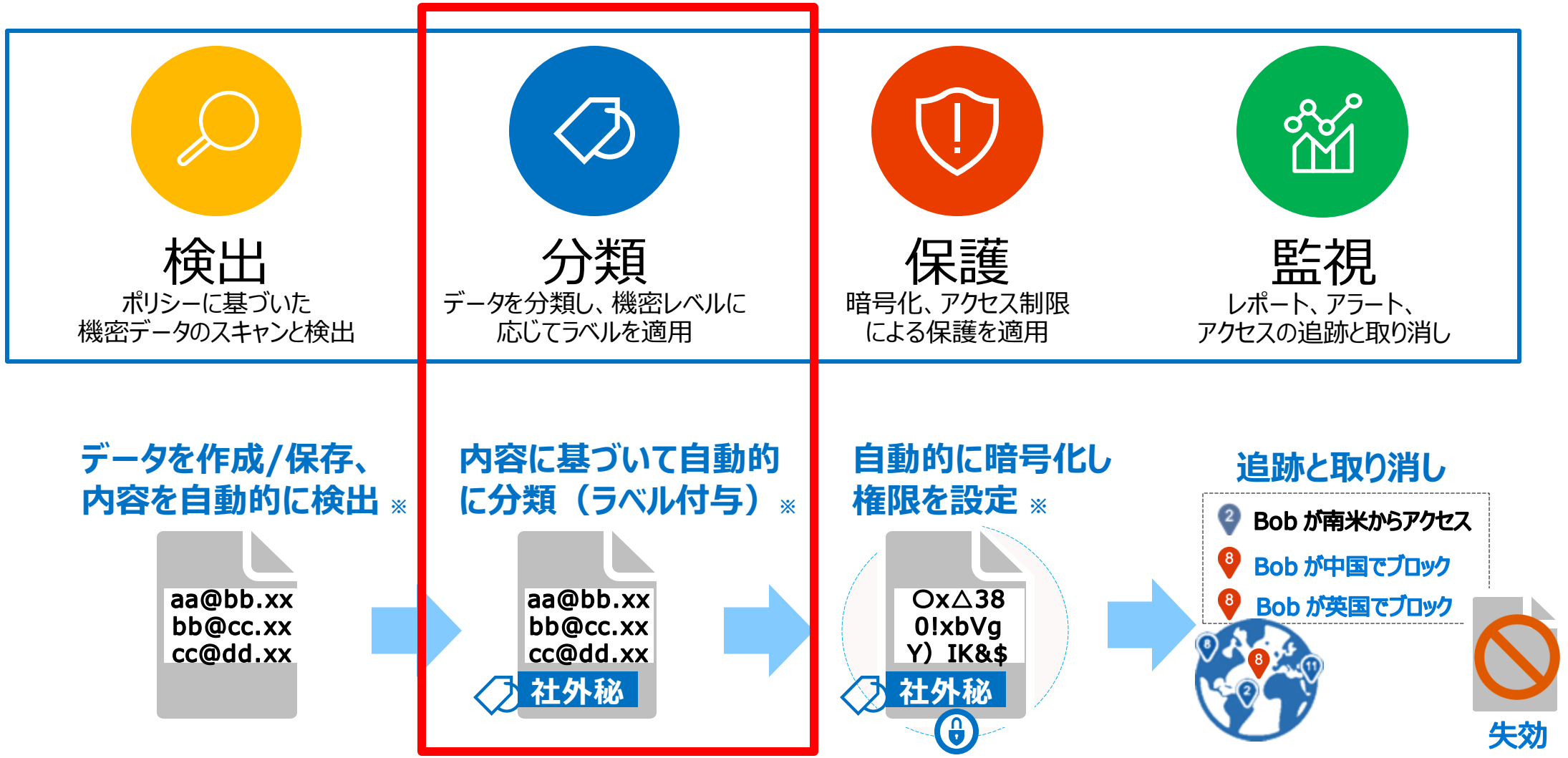
3 章：Azure Information Protection（AIP）



- Microsoft Information Protection の概要
- データの分類
- データの保護
- データの監視と追跡

Microsoft Information Protection のアプローチ

AIP P1
AIP P2



※ 自動的に検出、分類、暗号化するには AIP P2 が必要

統合 秘密度ラベルの管理

- Microsoft 365 コンプライアンス センターの [情報の保護]

- 手順
  - 手順 1：秘密度ラベルの作成
    - 視覚的マーキング
    - 保護
  - 手順 2：ラベル ポリシーの作成
    - ラベルの発行
    - ラベルの割り当て

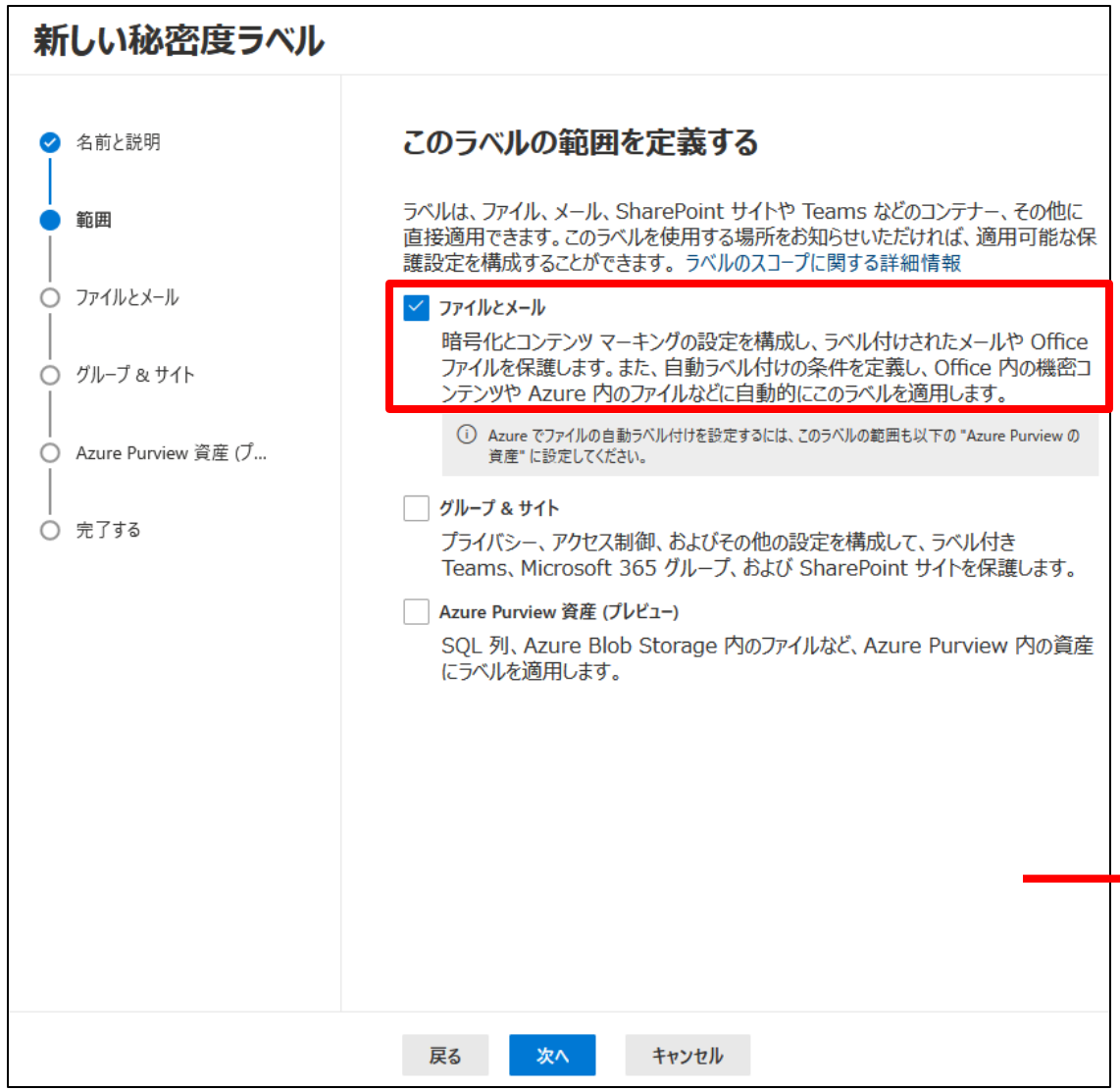
手順 1：秘密度ラベルの作成

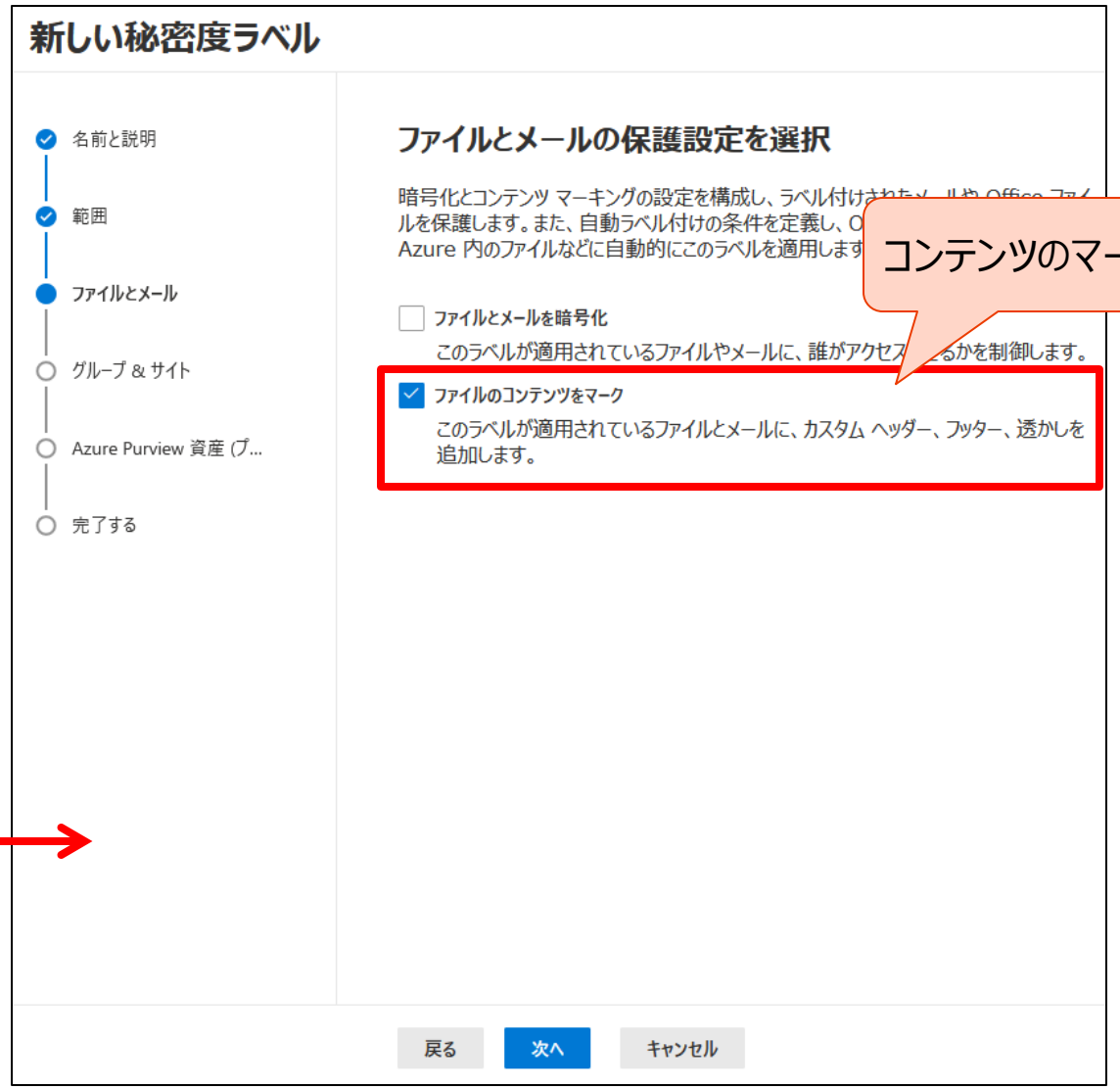
例）視覚的マーキング

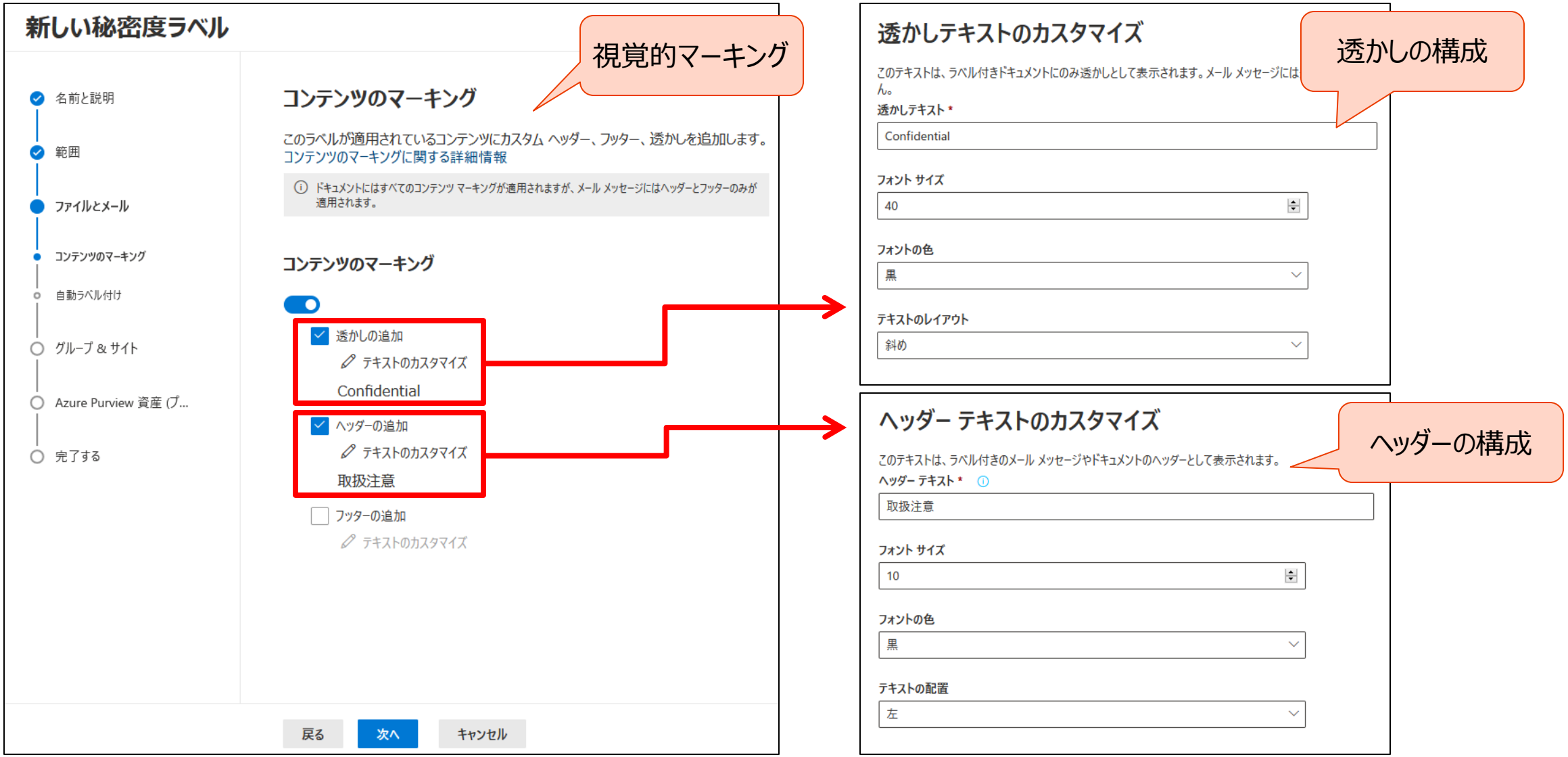
- [情報保護] – [+ ラベルの作成] で、秘密度ラベルを作成

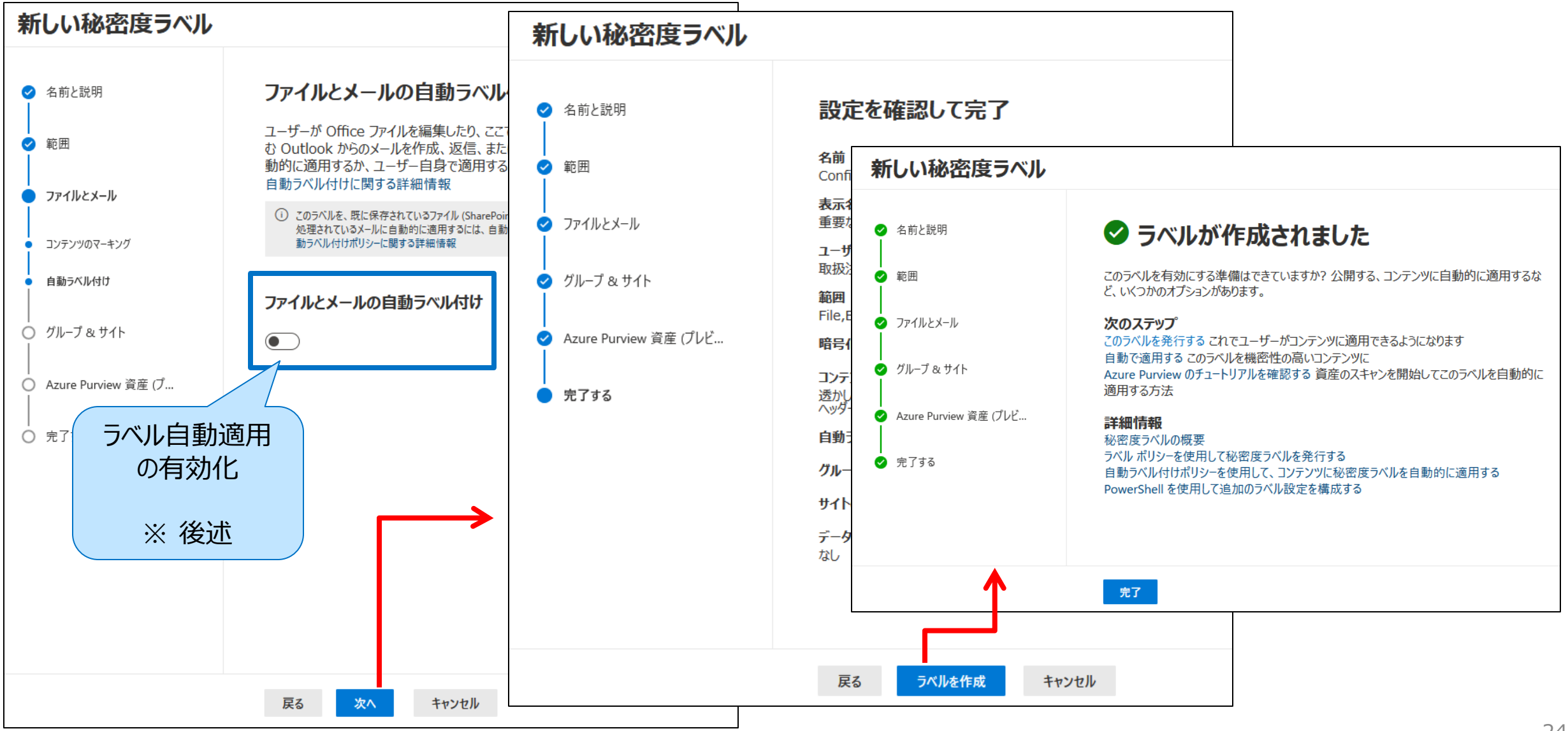
「Microsoft 365 コンプライアンス センター」
https://compliance.microsoft.com/

例）コンテンツをマーキングするラベルの作成



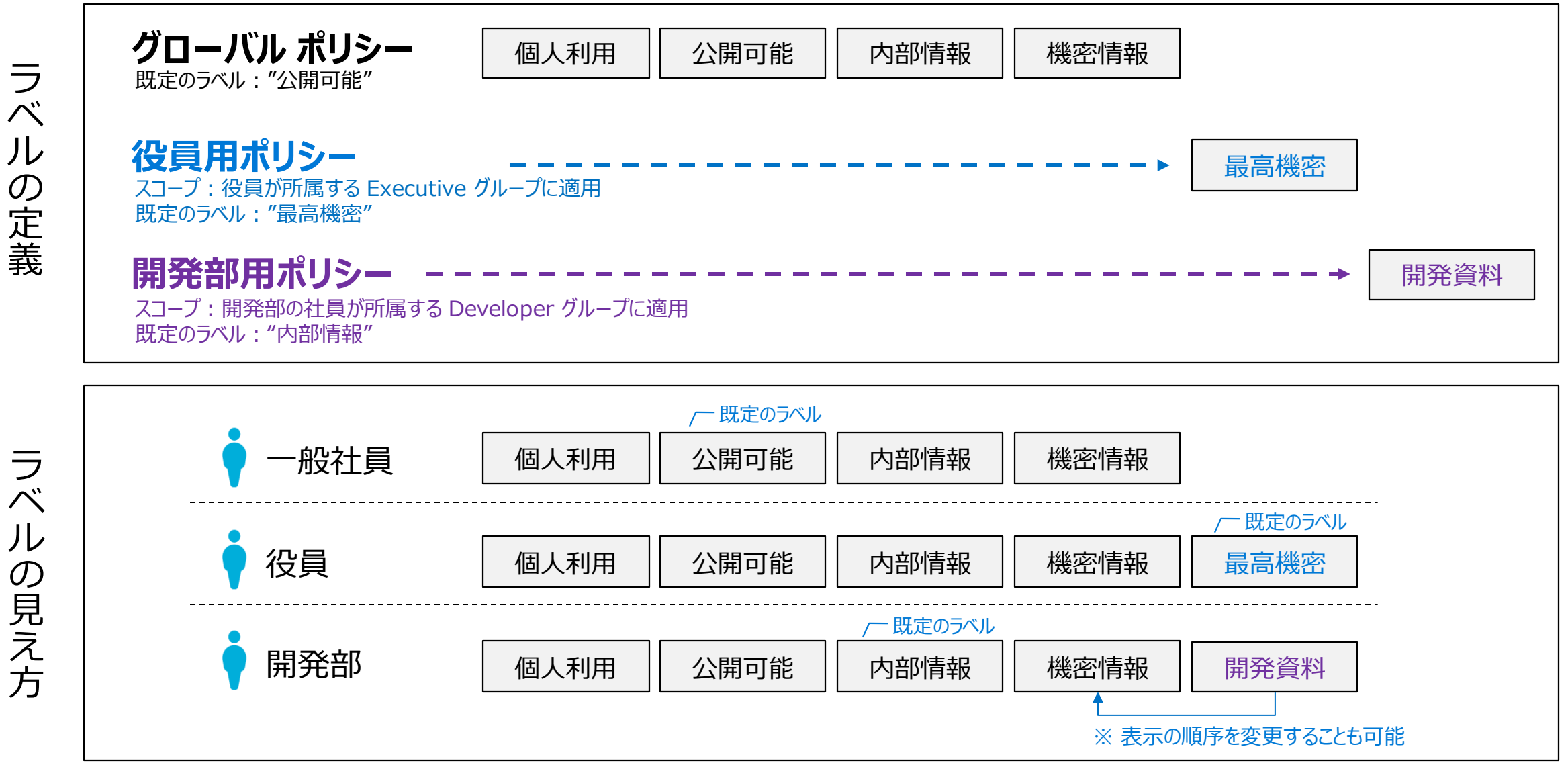



新しい秘密度ラベル
名前と説明
範囲
ファイルとメール
コンテンツのマーキング
自動ラベル付け
グループ & サイト
Azure Purview 資産 (プ...
完了する
コンテンツのマーキング
このラベルが適用されているコンテンツにカスタム ヘッダー、フッター、透かしを追加します。
コンテンツのマーキングに関する詳細情報
ドキュメントにはすべてのコンテンツ マーキングが適用されますが、メール メッセージにはヘッダーとフッターのみが適用されます。
コンテンツのマーキング
透かしの追加
テキストのカスタマイズ
Confidential
ヘッダーの追加
テキストのカスタマイズ
取扱注意
フッターの追加
テキストのカスタマイズ
戻る
次へ
キャンセル
視覚的マーキング
透かしテキストのカスタマイズ
このテキストは、ラベル付きドキュメントにのみ透かしとして表示されます。メール メッセージには
ん。
透かしテキスト *
Confidential
フォント サイズ
40
フォントの色
黒
テキストのレイアウト
斜め
透かしの構成
ヘッダー テキストのカスタマイズ
このテキストは、ラベル付きのメール メッセージやドキュメントのヘッダーとして表示されます。
ヘッダー テキスト *
取扱注意
フォント サイズ
10
フォントの色
黒
テキストの配置
左
ヘッダーの構成


新しい秘密度ラベル
名前と説明
範囲
ファイルとメール
コンテンツのマーキング
自動ラベル付け
グループ & サイト
Azure Purview 資産 (プ...
完了
ファイルとメールの自動ラベル
ユーザーが Office ファイルを編集したり、ここ
む Outlook からのメールを作成、返信、また
動的に適用するか、ユーザー自身で適用する
自動ラベル付けに関する詳細情報
このラベルを、既に保存されているファイル (SharePoi
処理されているメールに自動的に適用するには、自動
動ラベル付けポリシーに関する詳細情報
ファイルとメールの自動ラベル付け
ラベル自動適用
の有効化
※ 後述
戻る
次へ
キャンセル
新しい秘密度ラベル
名前と説明
範囲
ファイルとメール
グループ & サイト
Azure Purview 資産 (プレビ...
完了する
設定を確認して完了
名前
Confi
表示名
重要な
ユーザ
取扱注
範囲
File,E
暗号化
コンテ
透かし
ヘッダー
自動注
グルー
サイト
データ
なし
戻る
ラベルを作成
キャンセル
新しい秘密度ラベル
名前と説明
範囲
ファイルとメール
グループ & サイト
Azure Purview 資産 (プレビ...
完了する
ラベルが作成されました
このラベルを有効にする準備はできていますか? 公開する、コンテンツに自動的に適用するなど、いくつかのオプションがあります。
次のステップ
このラベルを発行する これでユーザーがコンテンツに適用できるようになります
自動で適用する このラベルを機密性の高いコンテンツに
Azure Purview のチュートリアルを確認する 資産のスキャンを開始してこのラベルを自動的に適用する方法
詳細情報
秘密度ラベルの概要
ラベル ポリシーを使用して秘密度ラベルを発行する
自動ラベル付けポリシーを使用して、コンテンツに秘密度ラベルを自動的に適用する
PowerShell を使用して追加のラベル設定を構成する
完了

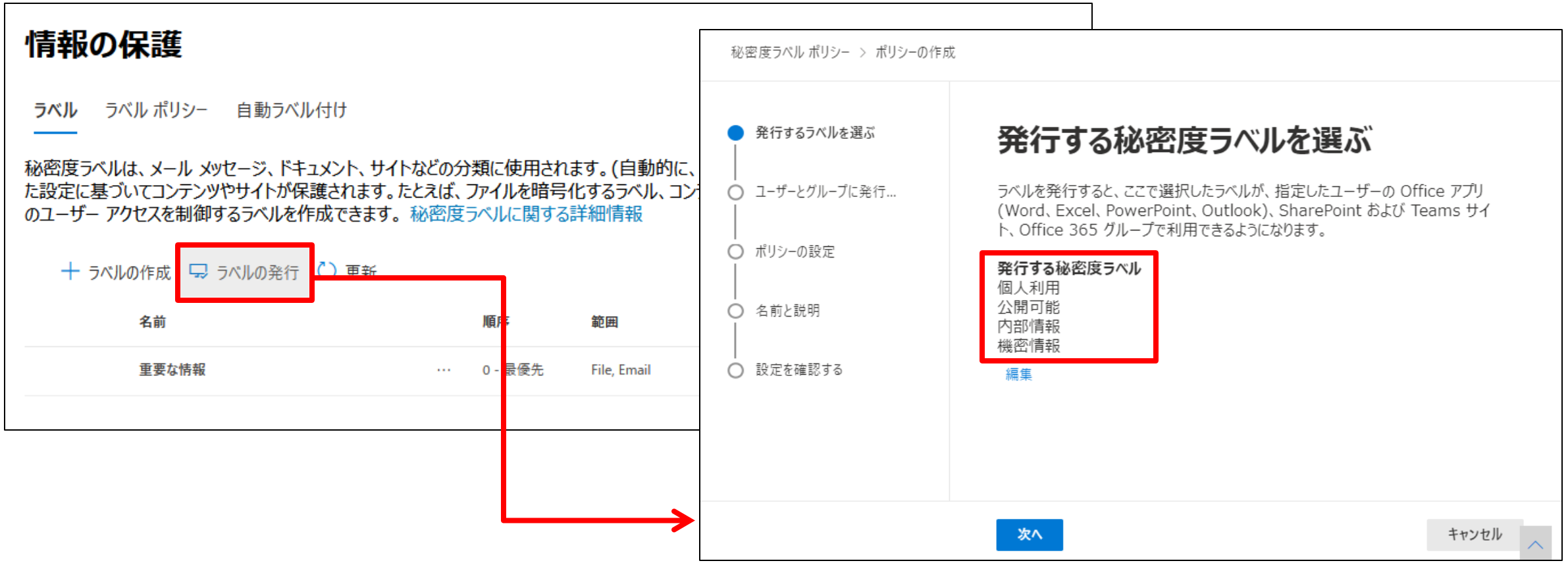
手順 2：ラベル ポリシーの作成（ラベルの発行）

特定のグループへのラベルの割り当て



例）コンテンツをマーキングするラベルの発行

- ラベルの発行（ポリシーの作成）

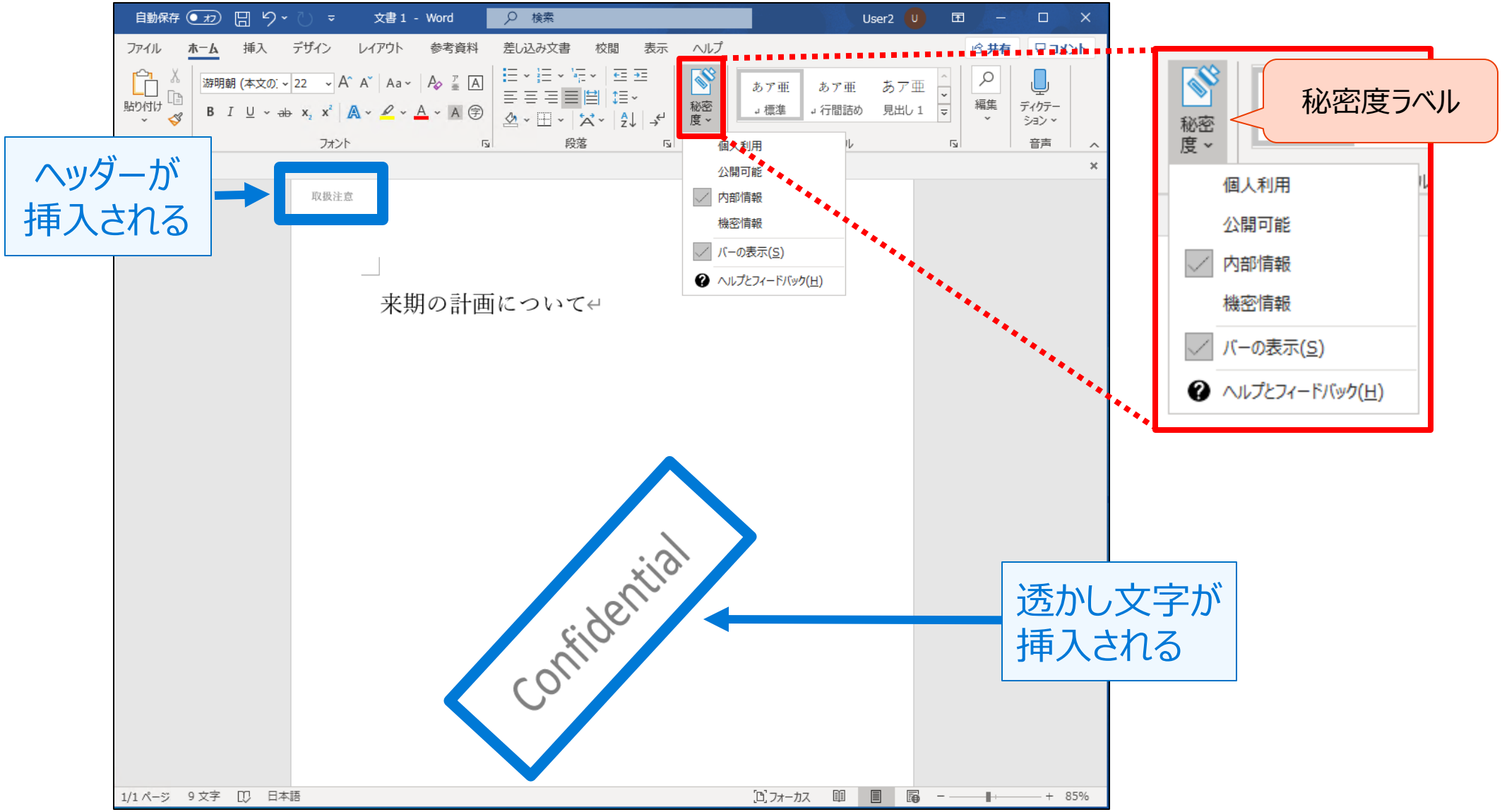


「Azure Information Protection向けのユーザーとグループの準備」
https://docs.microsoft.com/ja-jp/azure/information-protection/prepare


秘密度ラベル ポリシー > ポリシーの作成
発行するラベルを選ぶ
ユーザーとグループに発行する
ポリシーの設定
名前と説明
設定を確認する
ポリシーの設定
既定でドキュメントとメールにこのラベルを適用する
なし
ユーザーは、ラベルを削除したり、分類ラベルを下位のものにし
メールまたはドキュメントへのラベルの適用をユーザーに要求する
カスタム ヘルプ ページへのリンクをユーザーに提示します
戻る
次へ
キャンセル
秘密度ラベル ポリシー > ポリシーの作成
発行するラベルを選ぶ
ユーザーとグループに発行する
ポリシーの設定
名前と説明
設定を確認する
ポリシーの名前を設定する
カスタム ポリシーの設定を追加したので、ポリシーに名前を付けてください。
名前 *
エディフィスト ABC
秘密度ラベル ポリシーの説明を入力してください
説明
戻る
次へ
キャンセル


秘密度ラベル ポリシー > ポリシーの編集
発行するラベルを選ぶ
ユーザーとグループに発行する
ポリシーの設定
名前と説明
設定を確認する
確認と完了
入力した内容の要約を示します。
名前
エディフィスト ABC
説明
編集
これらのラベルを発行する
個人利用
公開可能
内部情報
機密情報
編集
ユーザーとグループに発行する
M365-work@edifistabc.net
編集
ポリシーの設定
必須のラベル
編集
戻る
送信
秘密度ラベル ポリシー > ポリシーの作成
発行するラベルを選ぶ
ユーザーとグループに発行する
ポリシーの設定
名前と説明
設定を確認する
新しいポリシーが作成されました
秘密度ラベル ポリシーが作成されました。
完了
ポリシーによって
ラベルが発行された！
情報の保護
ナビゲーションに表示
ラベル
ラベル ポリシー
自動ラベル付け
秘密度ラベル ポリシーを作成すると、ユーザーの Office アプリ (Outlook や Word など)、SharePoint サイト、Office 365 グループに 1 つ以上のラベルを発行できます。発行すると、ユーザーはコンテンツを保護するためにラベルを適用できます。秘密度ラベル ポリシーに関する詳細情報
ラベルを発行
更新
1 個のアイテム
名前
作成者
最終更新日
エディフィスト ABC
桂ゆうり
2021年3月12日 19:52

例）透かし文字とヘッダーを付けた「内部情報」ラベル

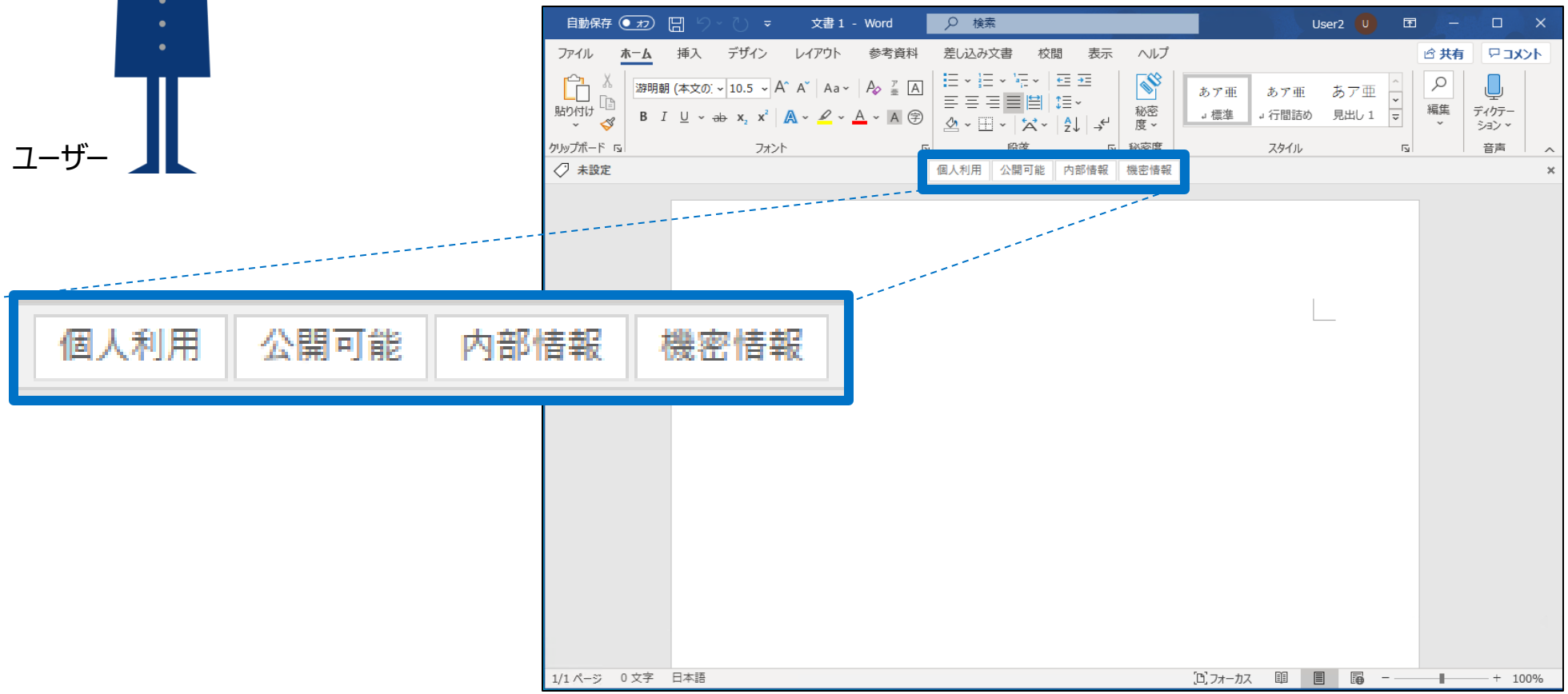


ラベルを付与するのは、誰？

どのラベルを
選べば
いいのかな‥

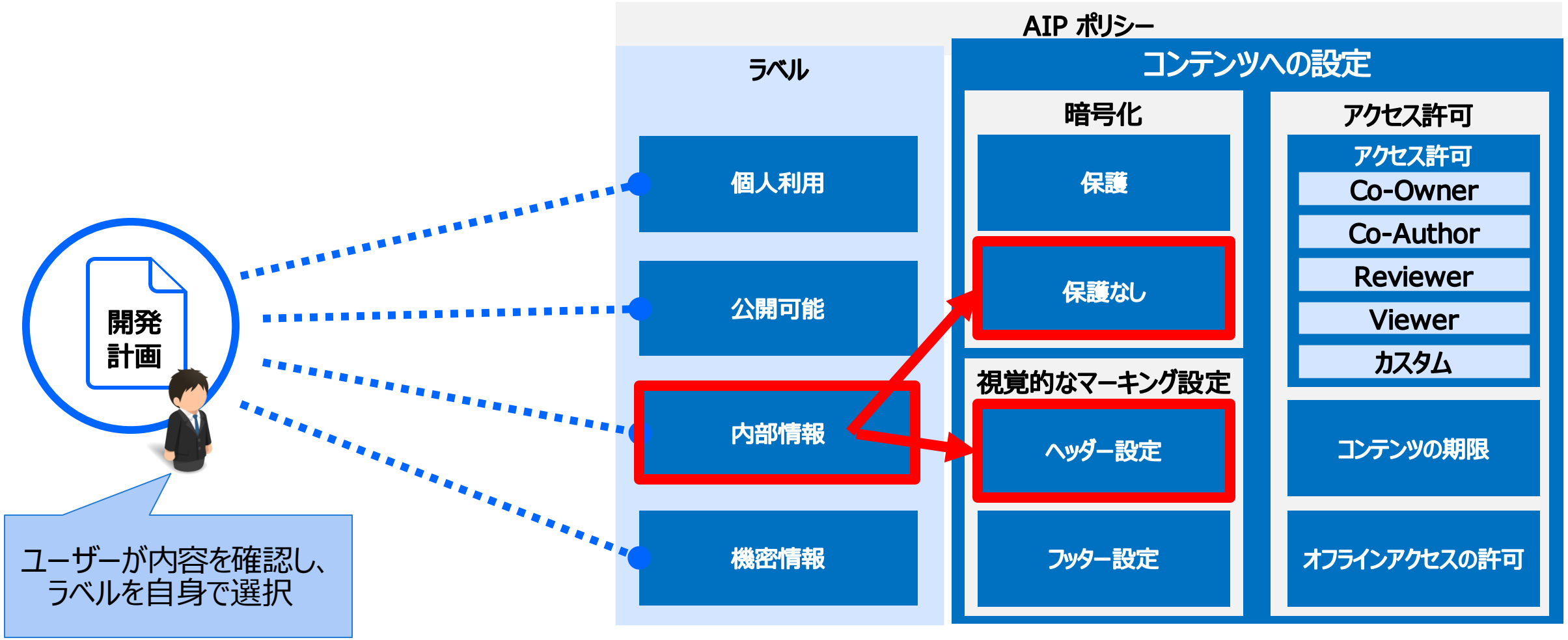
ユーザー

ラベルは、自分の判断で、自由に選んで良いですか？



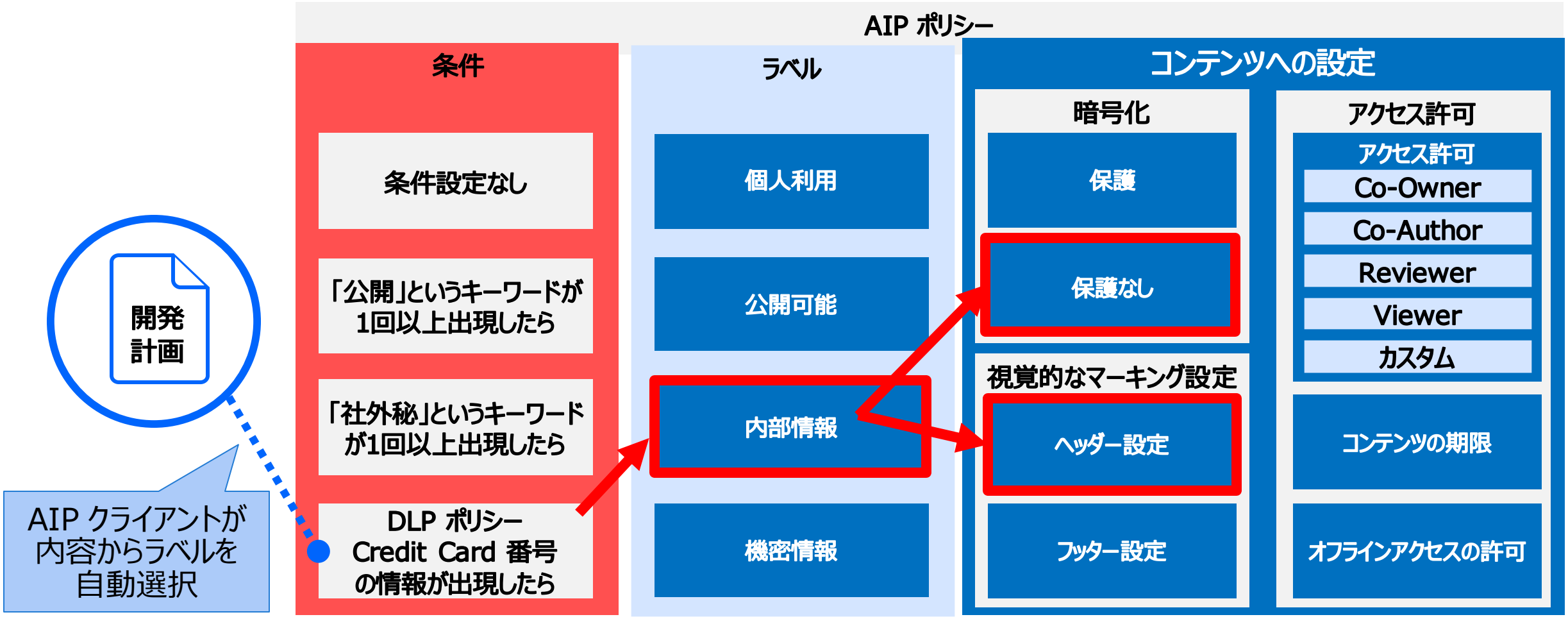
方法 1：マーキング ラベルの手動適用

- ユーザーが、コンテンツに対する “ラベル” を手動で選択し、コンテンツを分類する



方法 2：マーキング ラベルの自動適用

- コンテンツの内容から、AIP が自動的にラベルを判定して適用する



[比較] AIP プラン　1/2

今回はこれ！

機能	Free	OFFICE 365 用の AIP	AIP P1	AIP P2
Azure Information Protection ポリシー対応アプリおよびサービスから職場または学校アカウントを使用した、AIP コンテンツの使用	○	○	○	○
Microsoft Exchange Online、Microsoft SharePoint Online、Microsoft OneDrive for Business コンテンツの保護	-	○	○	○
ユーザー管理のキー プロビジョニング ライフ サイクル用の Bring Your Own Key (BYOK)	-	○	○	○
部門テンプレートを含む、カスタム テンプレート	-	○	○	○
Rights Management コネクタによるオンプレミスの Exchange および SharePoint コンテンツの保護	-	○	○	○
職場または学校アカウントの使用による Azure Information Protection コンテンツの作成	-	○	○	○
Office 365 Message Encryption	-	○	○	○
管理制御[3]	-	○	○	○
Windows から Windows Mobile、iOS、Mac OSX、Android まで、あらゆるプラットフォームの保護に役立つ Azure Information Protection ソフトウェア開発者キット	-	-	○	○
PTXT、PJPG、PFILE などの非 Microsoft Office ファイル形式の保護 (汎用保護)	-	-	○	○
手動、既定、必須のドキュメント分類	-	-	○	○

[比較] AIP プラン　2/2

今回はこれ！

機能	Free	OFFICE 365 用の AIP	AIP P1	AIP P2
Azure Information Protection スキャナーによる、オンプレミスにあって機密情報のタイプのいずれかに該当するファイルを対象としたコンテンツ検出	-	-	○	○
Azure Information Protection スキャナーによる、オンプレミスのファイル サーバーまたはリポジトリにあるファイルすべてを対象としたラベル付け	-	-	○	○
ファイル分類インフラストラクチャ (FCI) コネクタの使用による、オンプレミスの Windows Server ファイル共有との Rights Management コネクタ	-	-	○	○
ドキュメントの追跡と失効	-	-	○	○
Microsoft Information Protection ソフトウェア開発者キット (SDK) による、Windows、iOS、Mac OSX、Android、Linux を含むすべてのプラットフォームにあるメールとファイルを対象としたラベル付けと保護	-	-	○	○
自動および推奨の分類の条件構成	-	-	-	**○**
Outlook で事前に構成された S/MIME 保護を**自動**的に適用するためのラベルの設定	-	-	-	**○**
Outlook を使用しているときに情報の過度の共有を制御します（メールに対する警告、理由の入力、ブロック）	-	-	-	○
規制が厳しいシナリオ用の、Azure Information Protection と Active Directory (AD) Rights Management にまたがる Hold Your Own Key (HYOK)	-	-	-	○
サポートされているオンプレミスのファイルの**自動分類、ラベル付け、保護**のための Azure Information Protection スキャナー	-	-	-	**○**

「Azure Information Protection の価格」 https://azure.microsoft.com/ja-jp/pricing/details/information-protection/

組織のコンテンツを分類する方法

AIP P1
AIP P2

- 方法 1：ユーザーが手動でラベルを付ける “手動分類”
  - 管理者が分類用のラベルを作成し、
    ユーザーが手動でコンテンツに分類用のラベルを付ける

AIP P1

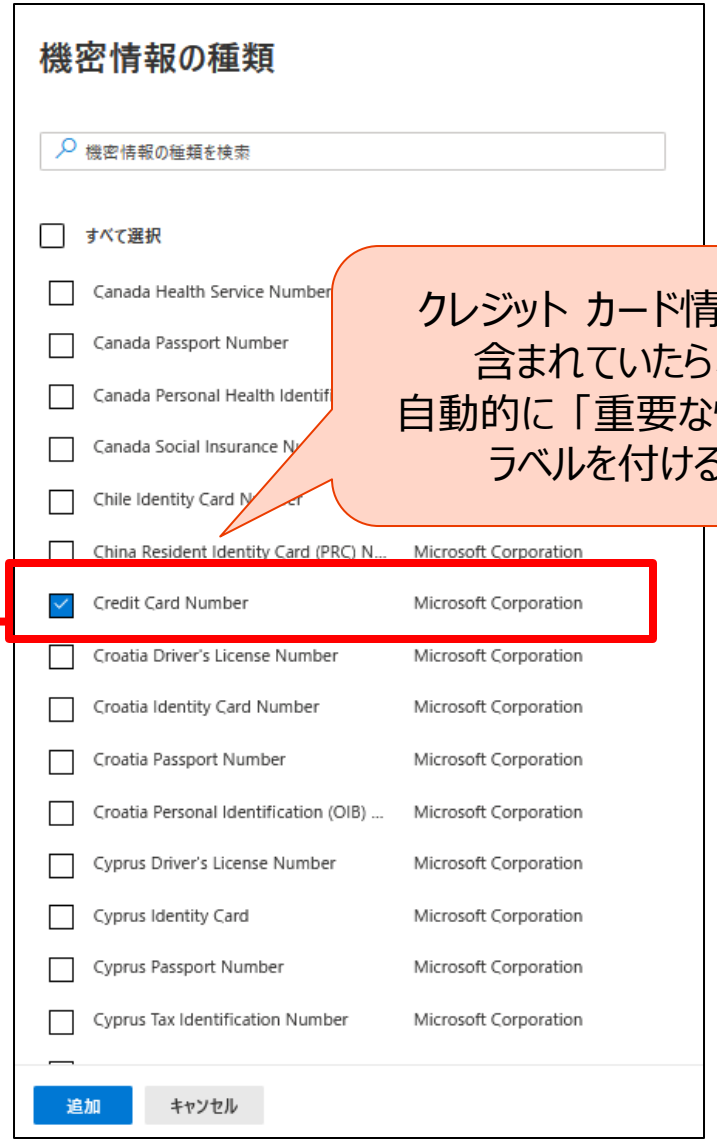
- **方法 2：ラベルの自動適用による “自動分類”**
  - 管理者が、自動適用の条件付きで分類用のラベルを作成する

AIP P2

例）ラベルの自動適用による“自動分類”

AIP P2

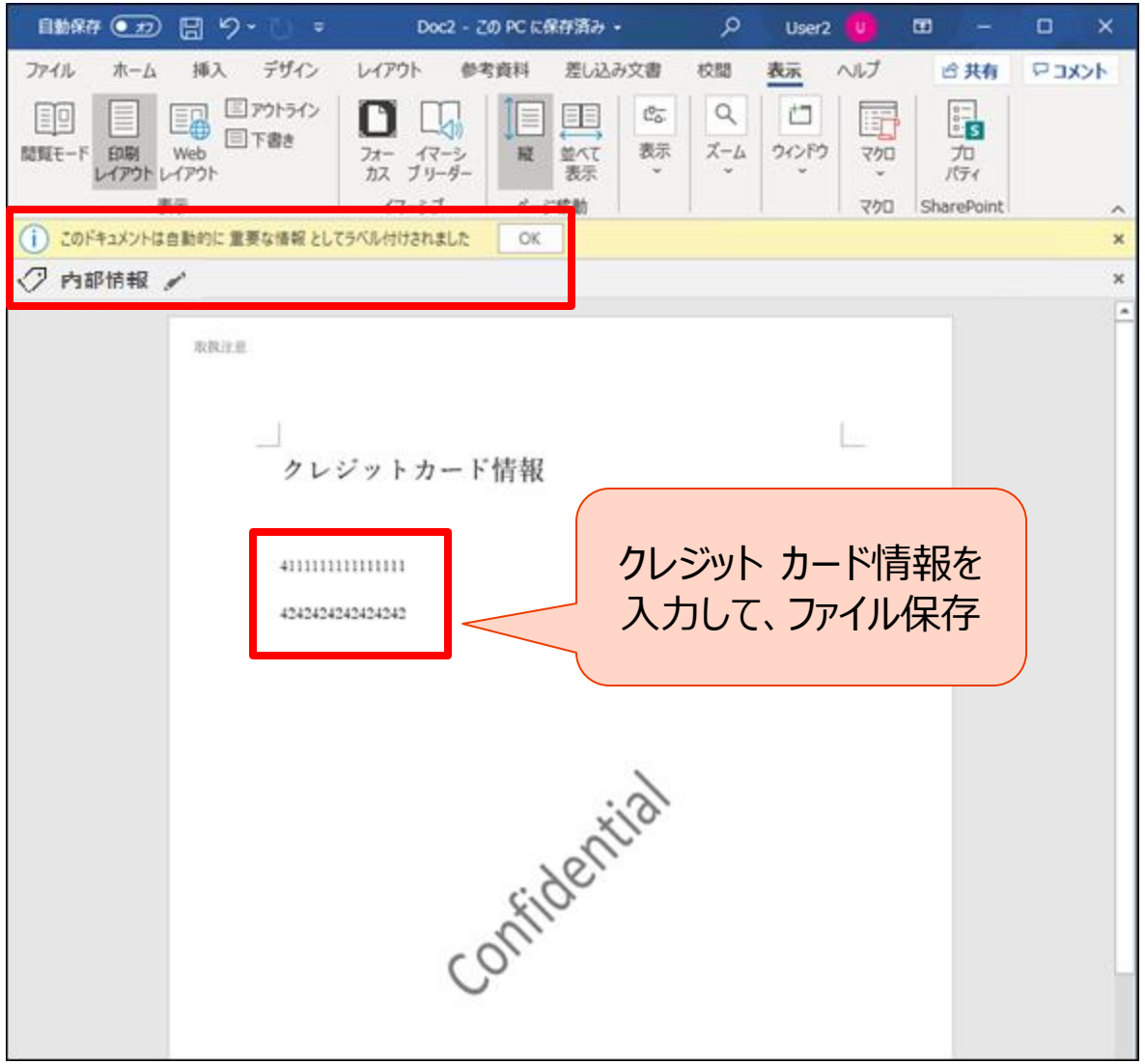
ラベルの適用方法
（勧める、自動）



クレジット カード情報が
含まれていたら、
自動的に「重要な情報」
ラベルを付ける

例）自動ラベル付けされた Word ファイル

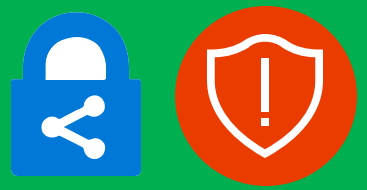
自動ラベル付け



クレジット カード情報を
入力して、ファイル保存

3-3

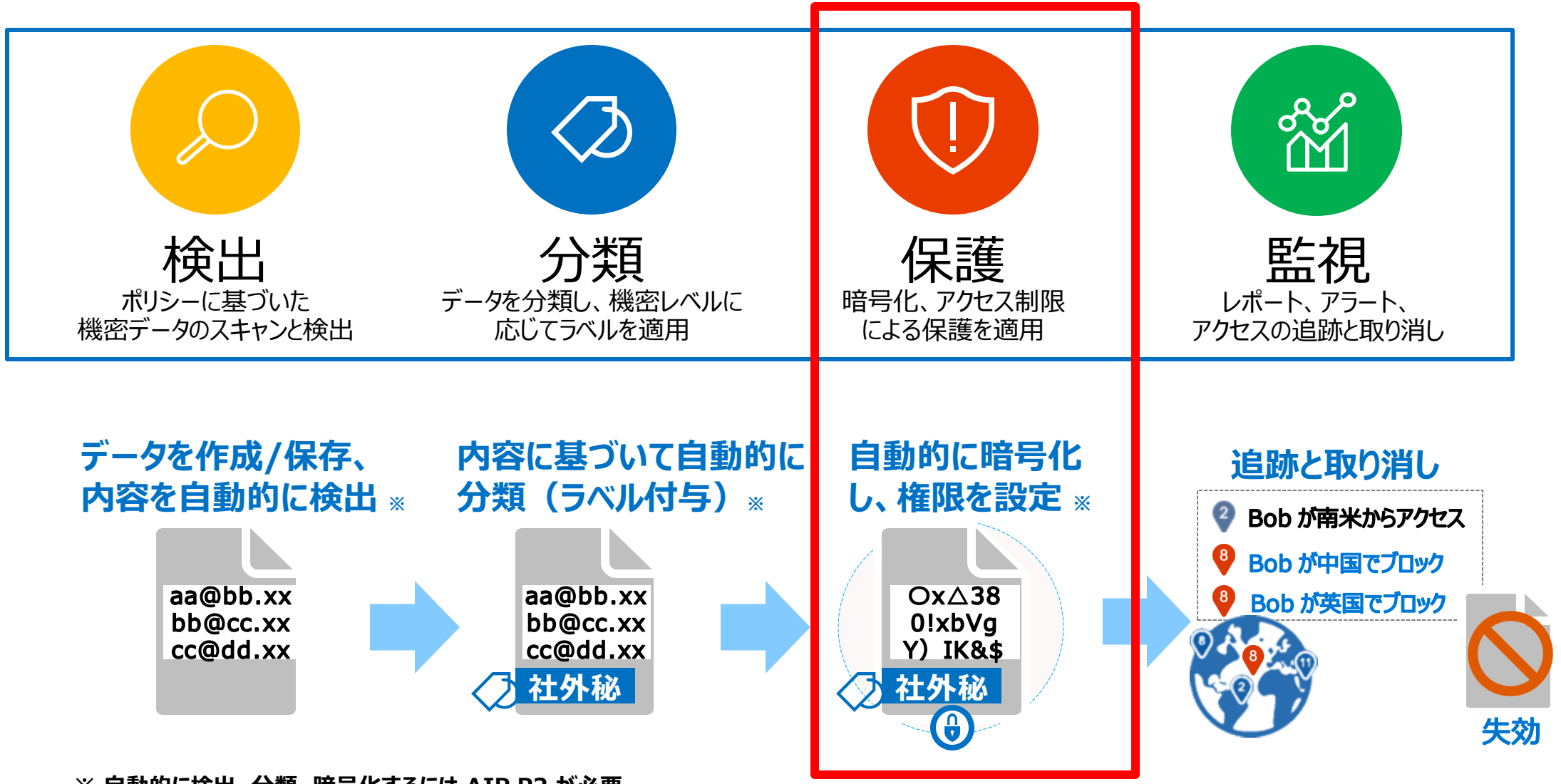
3 章：Azure Information Protection（AIP）



- Microsoft Information Protection の概要
- データの分類
- データの保護
- データの監視と追跡

Microsoft Information Protection のアプローチ

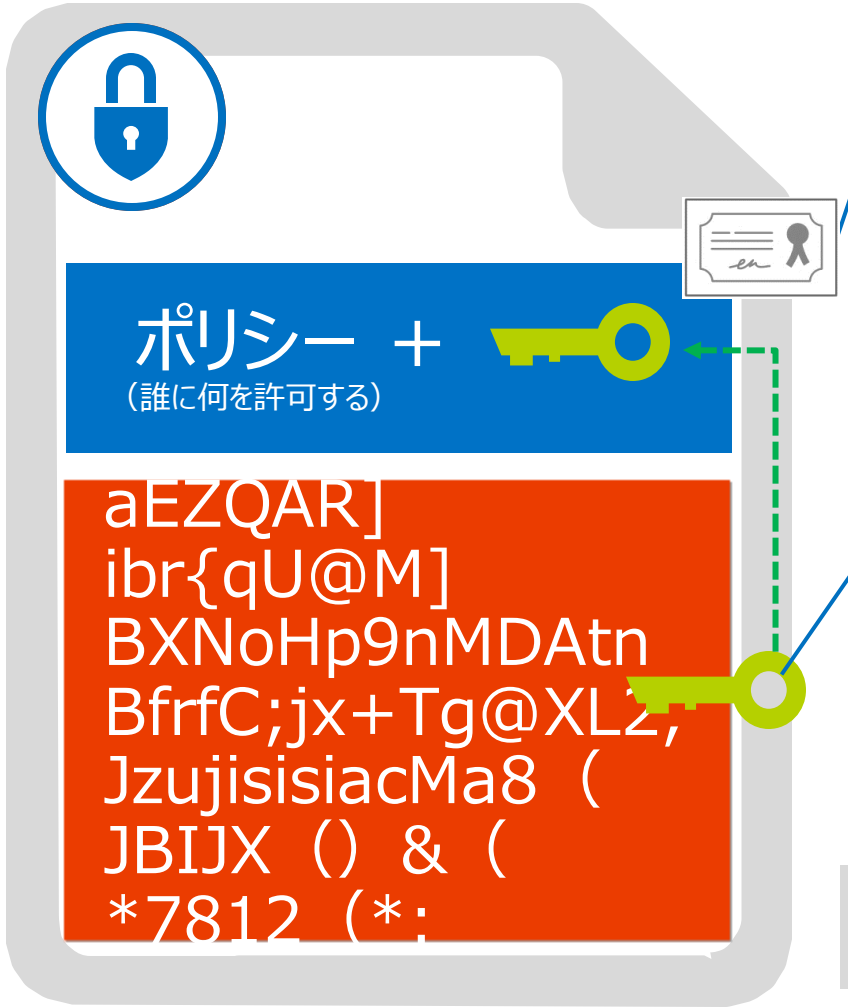
AIP P1
AIP P2



※ 自動的に検出、分類、暗号化するには AIP P2 が必要

秘密度ラベルで使用する暗号化アルゴリズム

- ポリシー（アクセス許可）とコンテンツ キー、および、データ部の暗号化で使用するアルゴリズム



ポリシー（アクセス許可）とコンテンツ キーを保護

- AIP のテナント キーを使用（または BYOK）
  暗号化アルゴリズム：RSA
  鍵長：2048 ビット（1024 ビットのオプション シナリオあり）
  証明書の署名：SHA-256

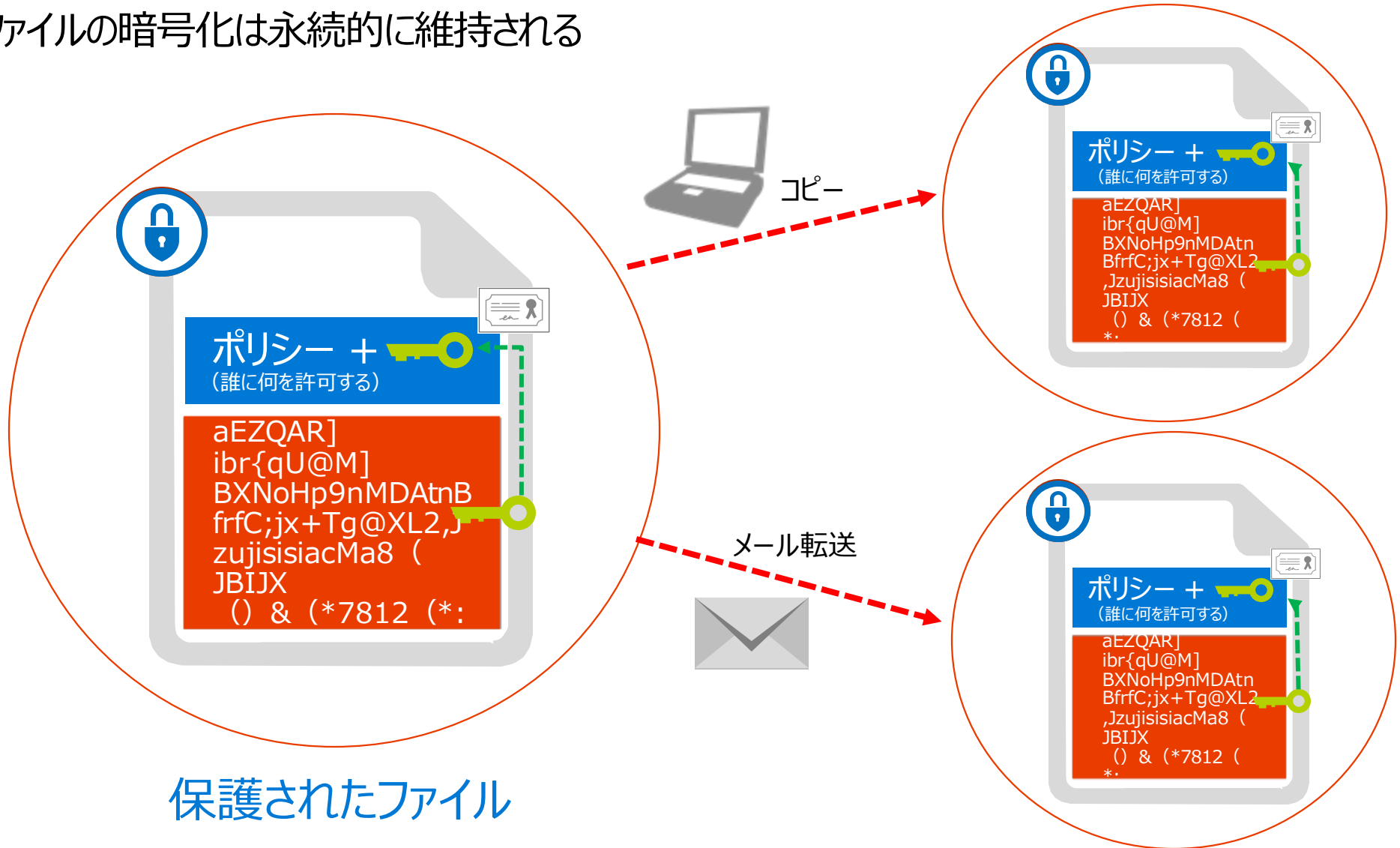
コンテンツの保護

- コンテンツ キーを生成（ドキュメントごとに固有）
  暗号化アルゴリズム：AES
  鍵長：128 ビットと 256 ビット（保護方法による）

「Azure RMS が動作する しくみ」
https://docs.microsoft.com/ja-jp/azure/information-protection/how-does-it-work

コンテンツの場所に依存しない、永続的な暗号化

- ファイル自体が保護されるため、ファイルが別の場所にコピーされたとしても、ファイルの暗号化は永続的に維持される



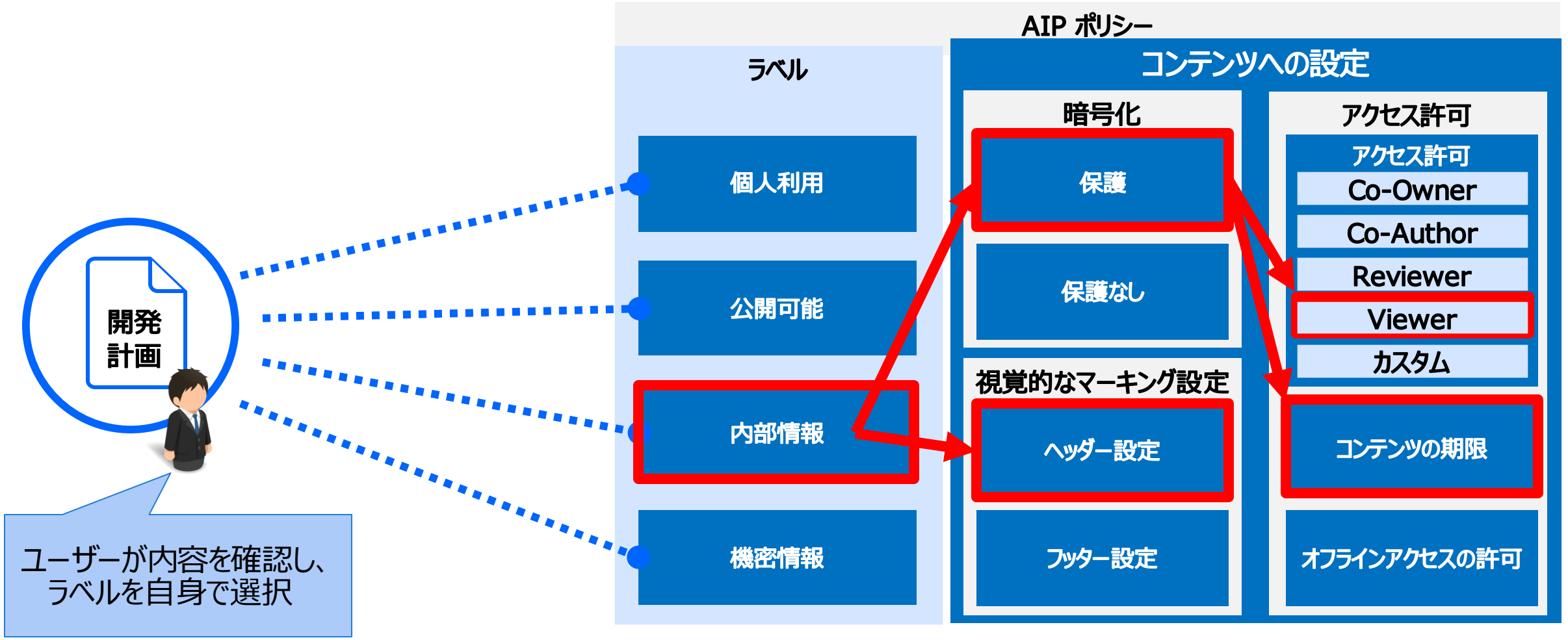
保護されたファイル

暗号化が
維持される！

許可された
アクセスのみ
行える！

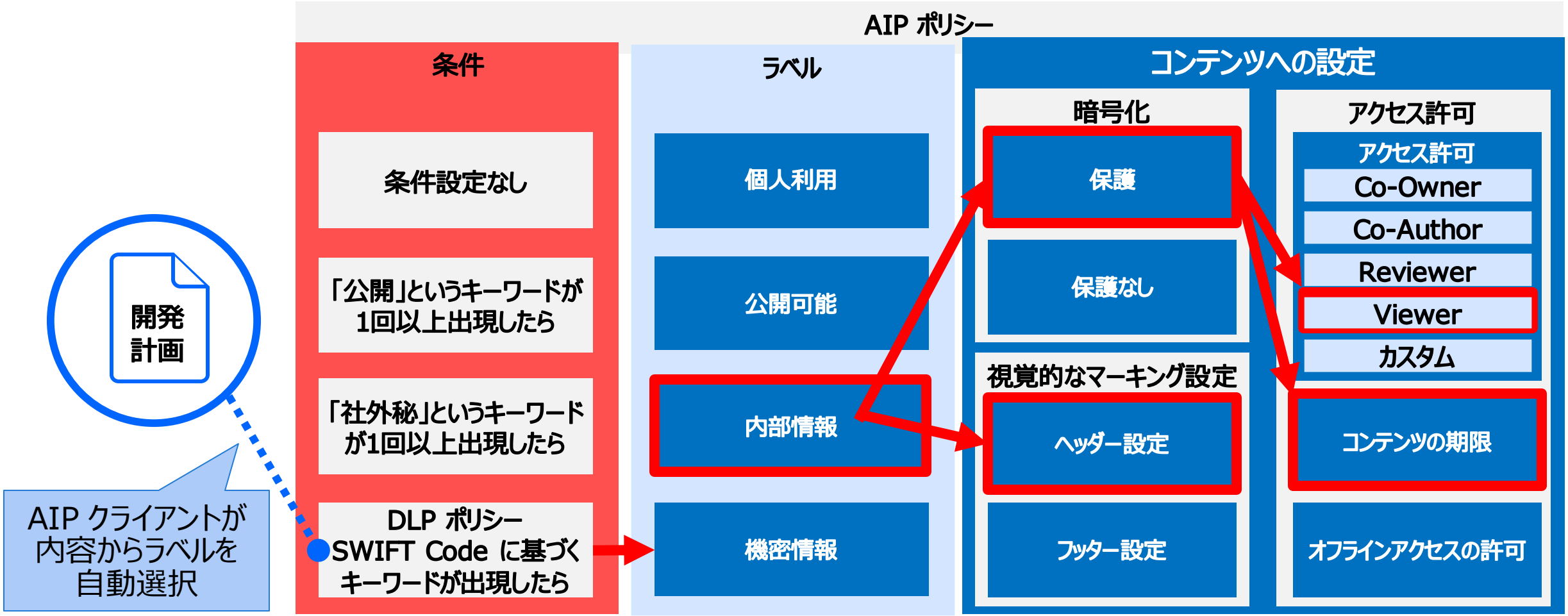
方法 1：マーキング & 保護ラベルの手動適用

- ユーザーが、コンテンツに対する “ラベル” を手動で選択し、コンテンツを分類する



方法 2 :マーキング & 保護ラベルの自動適用

- コンテンツの内容から、AIP が自動的にラベルを判定して適用する



組織のコンテンツを保護（暗号化）する方法

AIP P1
AIP P2

- 方法 1：ユーザーが手動で保護ラベルを付ける “手動保護”
  - 管理者がコンテンツを保護するラベルを作成し、ユーザーが手動でコンテンツに保護ラベルを付ける

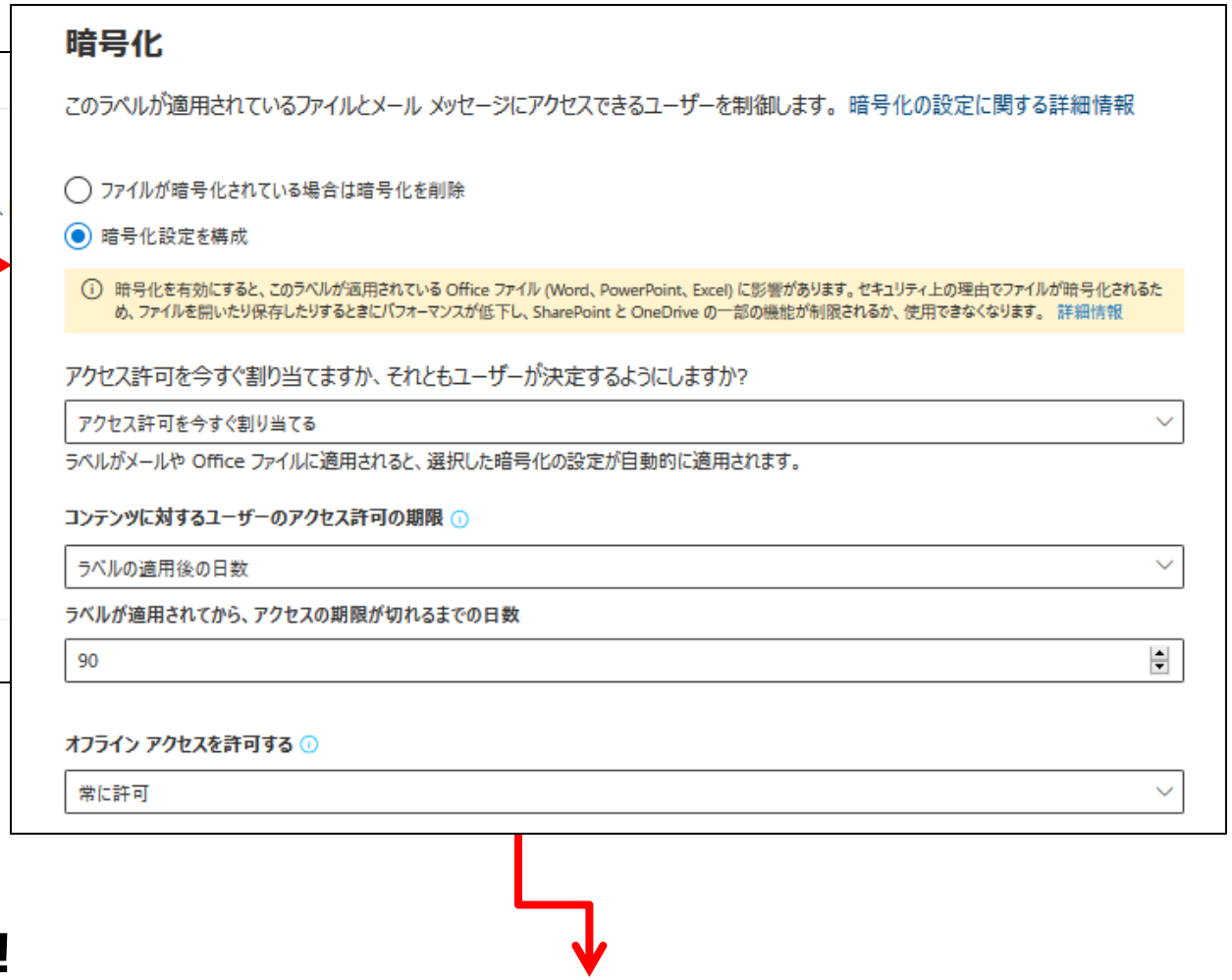
AIP P1

- **方法 2：ラベルの自動適用による “自動保護”**
  - 管理者が、自動適用の条件付きで、コンテンツを保護するラベルを作成する

AIP P2

例）秘密度ラベルの暗号化設定

- 秘密度ラベルに対して、暗号化を設定



・この秘密度ラベルには、
すでに自動適用の条件が構成されている
・このラベルに暗号化の構成を追加するだけで、
ドキュメントを自動暗号化する秘密度ラベルが完成！

暗号化

このラベルが適用されているファイルとメール メッセージにアクセスできるユーザーを制御します。暗号化の設定に関する詳細情報

- ○ ファイルが暗号化されている場合は暗号化を削除
- ◉ 暗号化設定を構成

ⓘ 暗号化を有効にすると、このラベルが適用されている Office ファイル (Word、PowerPoint、Excel) に影響があります。セキュリティ上の理由でファイルが暗号化されるため、ファイルを開いたり保存したりするときにパフォーマンスが低下し、SharePoint と OneDrive の一部の機能が制限されるか、使用できなくなります。 詳細情報

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

アクセス許可を今すぐ割り当てる

ラベルがメールや Office ファイルに適用されると、選択した暗号化の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 ⓘ

ラベルの適用後の日数

ラベルが適用されてから、アクセスの期限が切れるまでの日数

90

有効期限

オフライン アクセスを許可する ⓘ

常に許可

特定のユーザーとグループにアクセス許可を付与する * ⓘ

アクセス許可の割り当て

1 個のアイテム

ユーザーとグループ	アクセス許可
M365-work@edifistabc.net	Viewer

☐ 二重キー暗号化を使う ⓘ

戻る　次へ　キャンセル

アクセス許可の割り当て

このラベルが適用されたコンテンツを使用するアクセス許可が、選択したユーザーまたはグループにだけ割り当てられます。既存のアクセス許可 (共同所有者、共同作成者、レビュー担当者など) から選択することもできますし、必要に応じてそれらをカスタマイズすることもできます。

- ＋ 組織内のすべてのユーザーとグループを追加する
- ＋ 任意の認証済みユーザーを追加 ⓘ
- ＋ ユーザーまたはグループを追加する
- ＋ 特定のメールアドレスまたはドメインを追加する ⓘ

1 個のアイテム

M365-work@edifistabc.net

アクセス許可の選択

Viewer
VIEW,VIEWRIGHTSDATA,OBJMODEL

アクセス許可

アクセス許可の選択

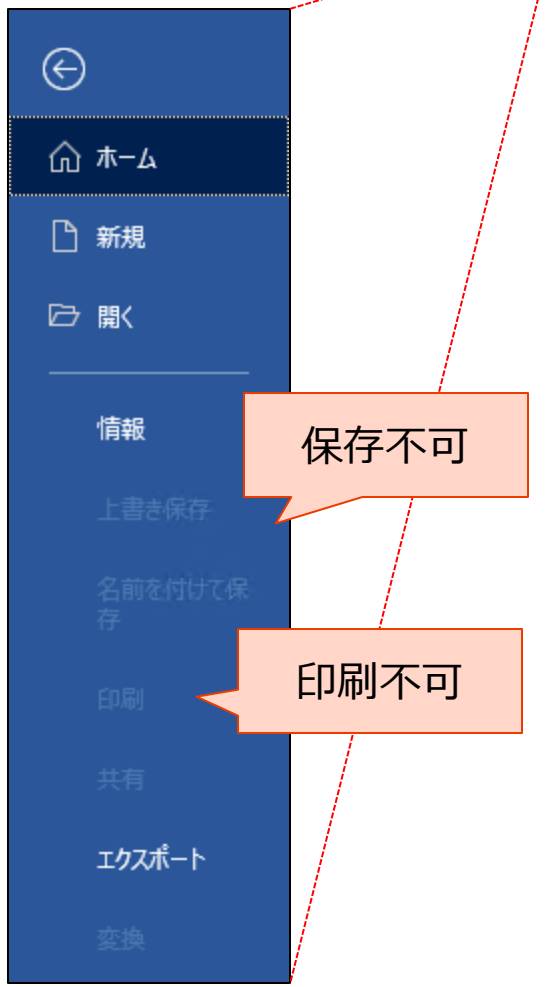
このユーザー/グループに対して許可する操作を選びます

閲覧者

- 共同所有者
- 共同作成者
- レビュー担当者
- 閲覧者
- カスタム

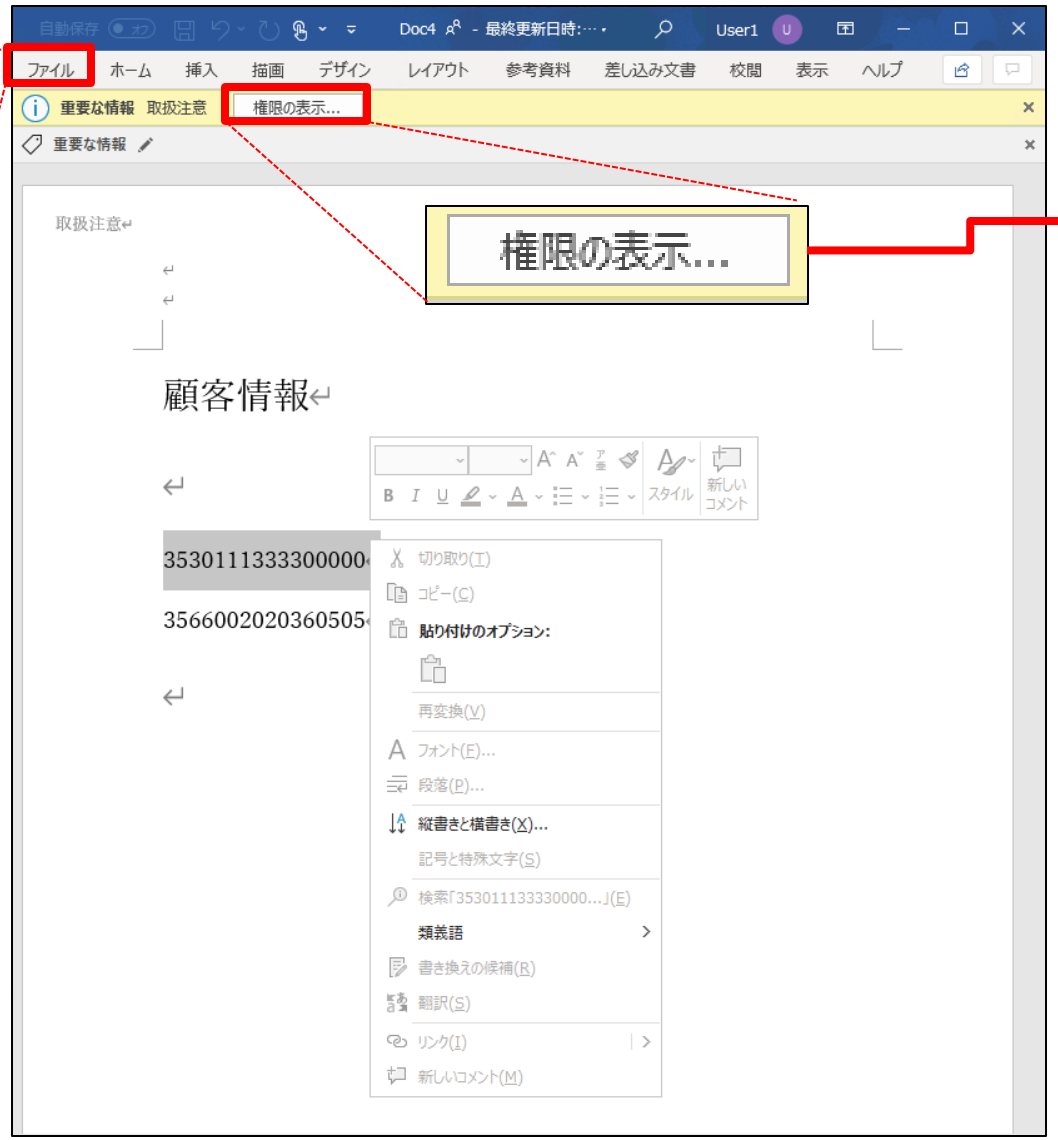
例）保護された Word ファイル

[ファイル] メニュー

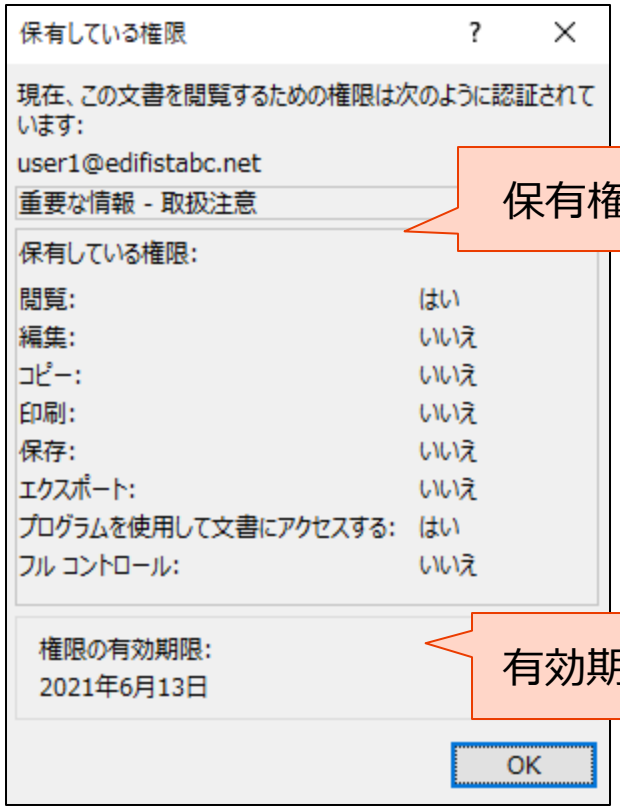


保存不可

印刷不可



権限の表示...



保有権限

有効期限

[参考] 技術資料

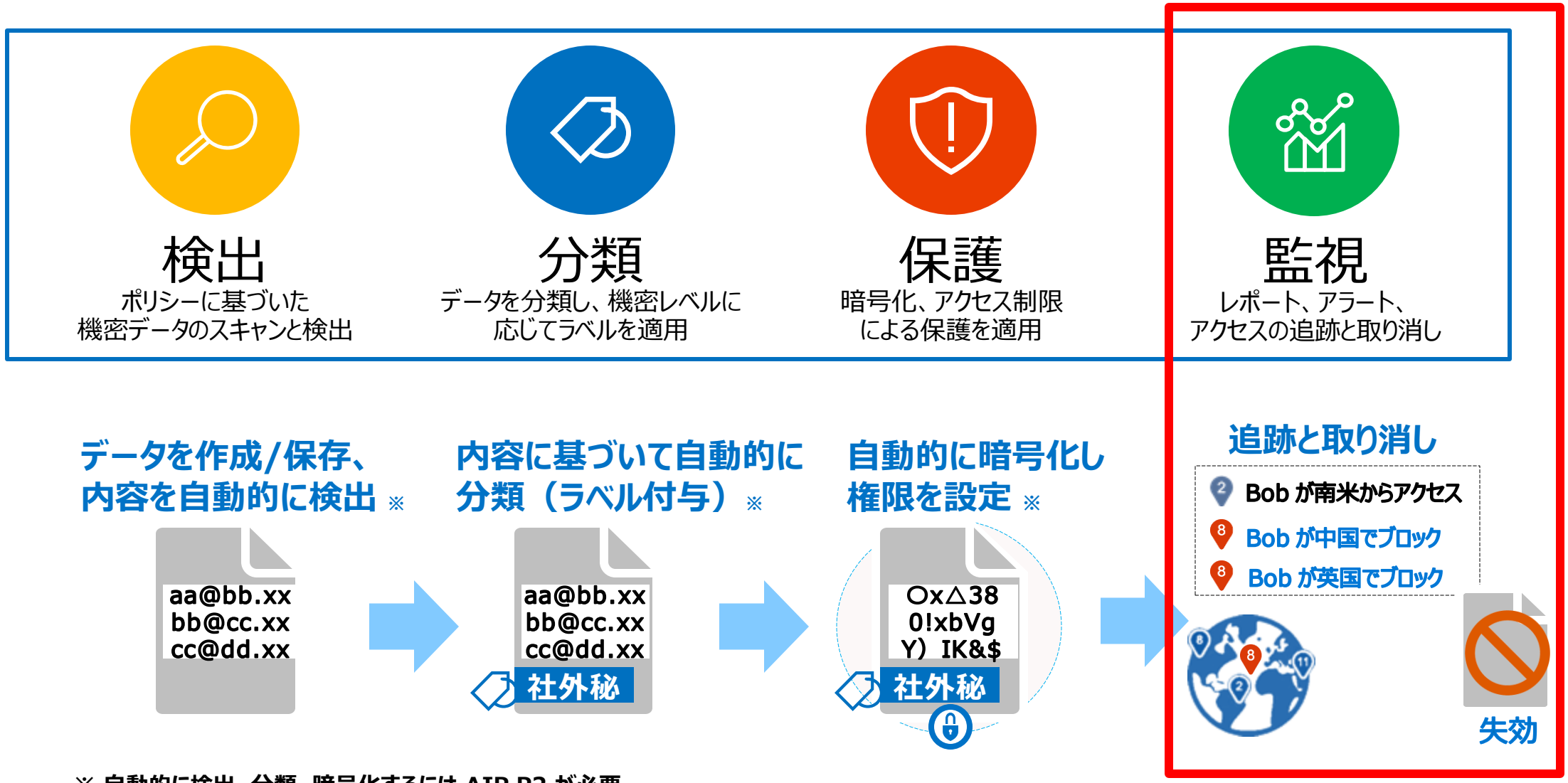
- **「Microsoft 365 の二重キー暗号化」** Microsoft 365 E5
  - https://docs.microsoft.com/ja-jp/microsoft-365/compliance/double-key-encryption?view=o365-worldwide

3-4

3 章：Azure Information Protection（AIP）

- Microsoft Information Protection の概要
- コンテンツの分類
- コンテンツの保護
- コンテンツの監視と追跡

Microsoft Information Protection のアプローチ



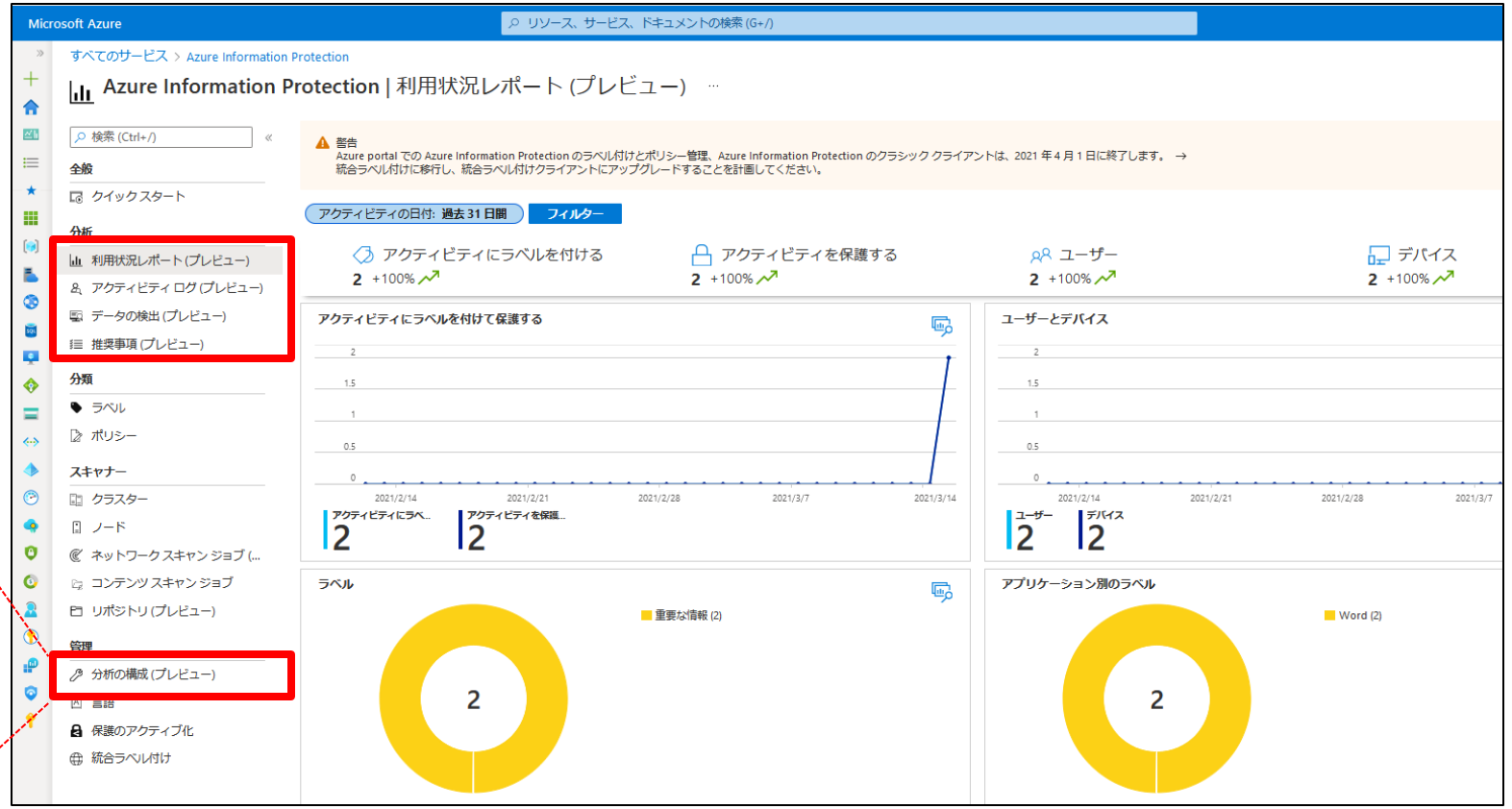
※ 自動的に検出、分類、暗号化するには AIP P2 が必要

AIP P1

使用状況のログ分析（AIP Analytics レポート）

- Azure ポータルの [Azure Information Protection] の分析メニュー
  - Azure Log Analytics にログを収集し分析

統一されたラベル付けクライアントは、
ユーザー アクティビティをローカルの
Windows イベント ログには記録しない



AIP P1

ドキュメント アクセスの追跡と取り消し（プレビュー）

- AIP 統合ラベルクライアントのみサポート

- ドキュメントを追跡対象として登録すると、Microsoft 365 のグローバル管理者は、成功したアクセス イベントと拒否された試行を含むアクセスの詳細を追跡し、必要に応じてアクセス権を取り消すことができる

「管理者ガイド: Azure Information Protection を使用したドキュメントアクセスの追跡と取り消し (パブリックプレビュー)」
https://docs.microsoft.com/ja-jp/azure/information-protection/rms-client/track-and-revoke-admin

[参考] 技術資料

- **「Azure Information Protection の分析と中央レポート (パブリックプレビュー)」**
  - https://docs.microsoft.com/ja-jp/azure/information-protection/reports-aip
- **「Azure Information Protection からの保護の使用状況のログと分析」**
  - https://docs.microsoft.com/ja-jp/azure/information-protection/log-analyze-usage
- **「管理者ガイド: Azure Information Protection クライアントファイルと クライアント使用状況ログの統合」**
  - https://docs.microsoft.com/ja-jp/azure/information-protection/rms-client/clientv2-admin-guide-files-and-logging
- **「Azure Information Protection 監査ログの参照 (パブリックプレビュー)」**
  - https://docs.microsoft.com/ja-jp/azure/information-protection/audit-logs
- **「Azure Information Protection からデータを接続する」（Azure Sentinel との統合）**
  - https://docs.microsoft.com/ja-jp/azure/sentinel/connect-azure-information-protection