

 Microsoft 365 Compliance

Insider Risk Management



自己紹介



五戸 禎人 (gonoway)

Yoshihito Gonohe

Cloud Native Inc.

Cloud Security Architect

経歴

セキュリティ製品のデプロイ（前職）->MDM（Intune、Jamf）->育児（1年→CISSP取得）->IdP（Okta、Azure AD）・IGA

今やっていること

情報システム部門へのコンサルティング業務

新製品の調査・検証

その他言いたいこと

JPEMSUGも好きだし、JOUGも好きだし、JMUGも好きです！！

このセッションで話すこと

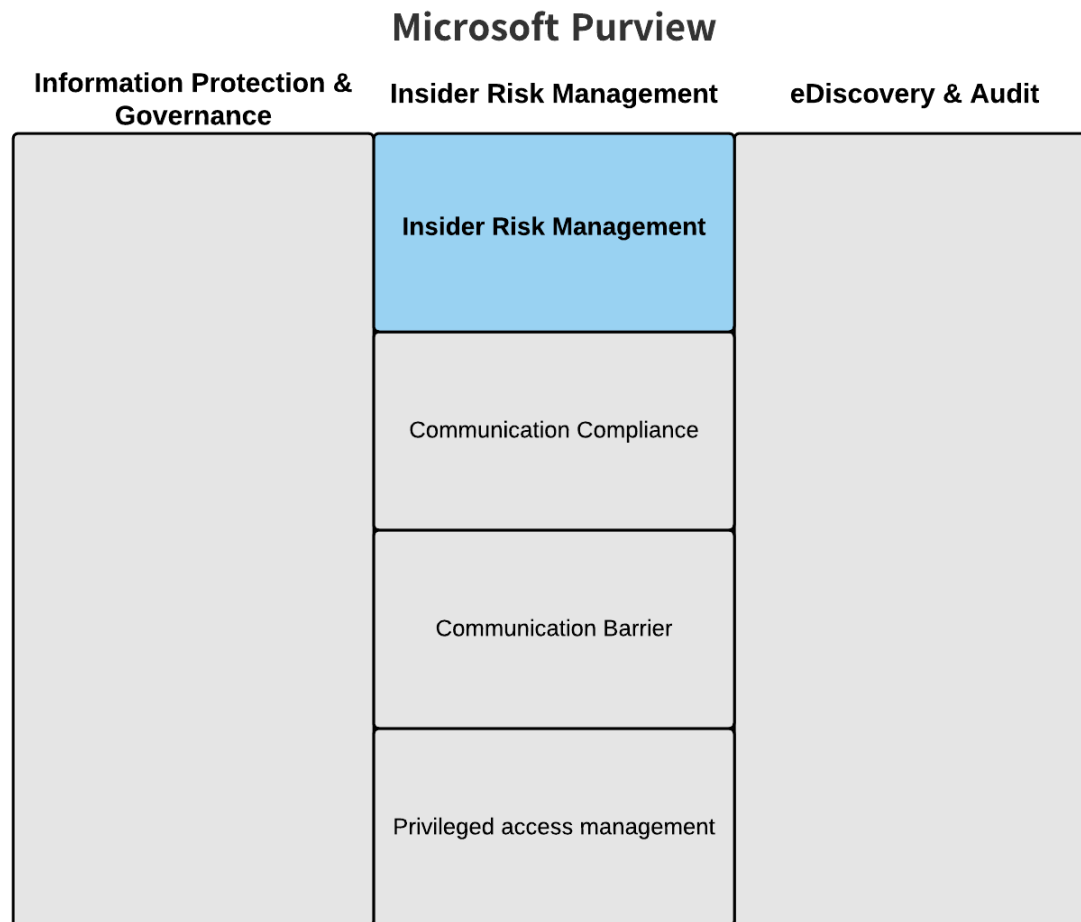
1. 概要・利用できるライセンス
2. 始め方
3. 今後の展望

このセッションで話すこと

1. 概要・利用できるライセンス
2. 始め方
3. 今後の展望

Insider Risk Managementとは

- 組織内の悪意のあるもしくは不注意な行動を検出・調査・対処するための機能
- Microsoft Purview リスクおよびコンプライアンスソリューションの1つの機能



Insider Risk Managementが使えるライセンス

- Microsoft 365 E5
- Microsoft 365 E5 Compliance Add-on
 - Microsoft365 E3 もしくは Office 365 E3 + EMS E3の利用が前提
- Microsoft 365 E5 Insider Risk Management Add-on
 - Microsoft365 E3 の利用が前提

このセッションで話すこと

1. 概要・利用できるライセンス

2. 始め方

3. 今後の展望

Insider Risk Managementの始め方

到達点：自社がどんな状態なのかを把握できる。

設定所要時間：2~3分！

※ Microsoft Purviewのページへのアクセス権を保持している前提

- Microsoft Purviewのページにアクセスする
- 画面左の内部リスクの管理を開く
- 潜在的な内部リスクをスキャンする
- おわり！

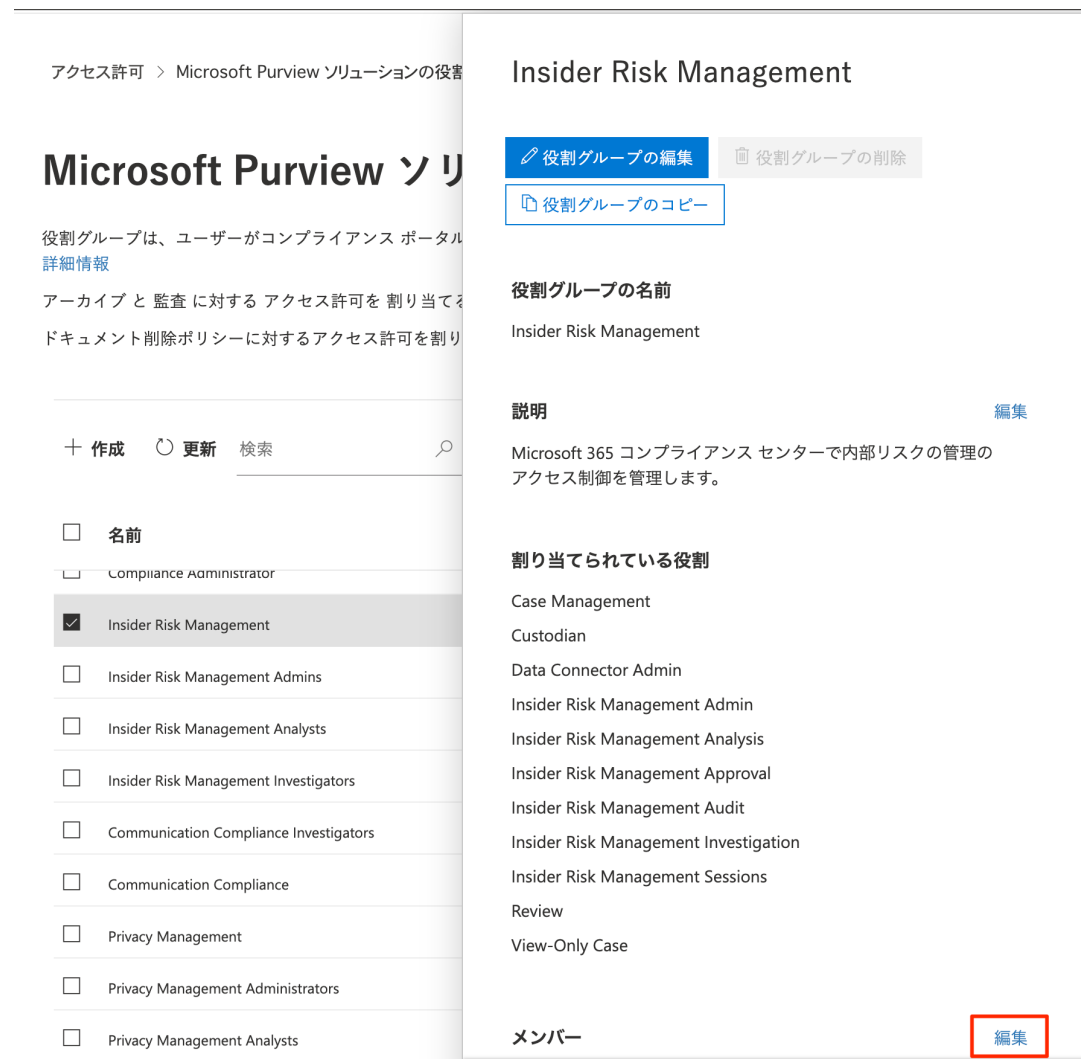
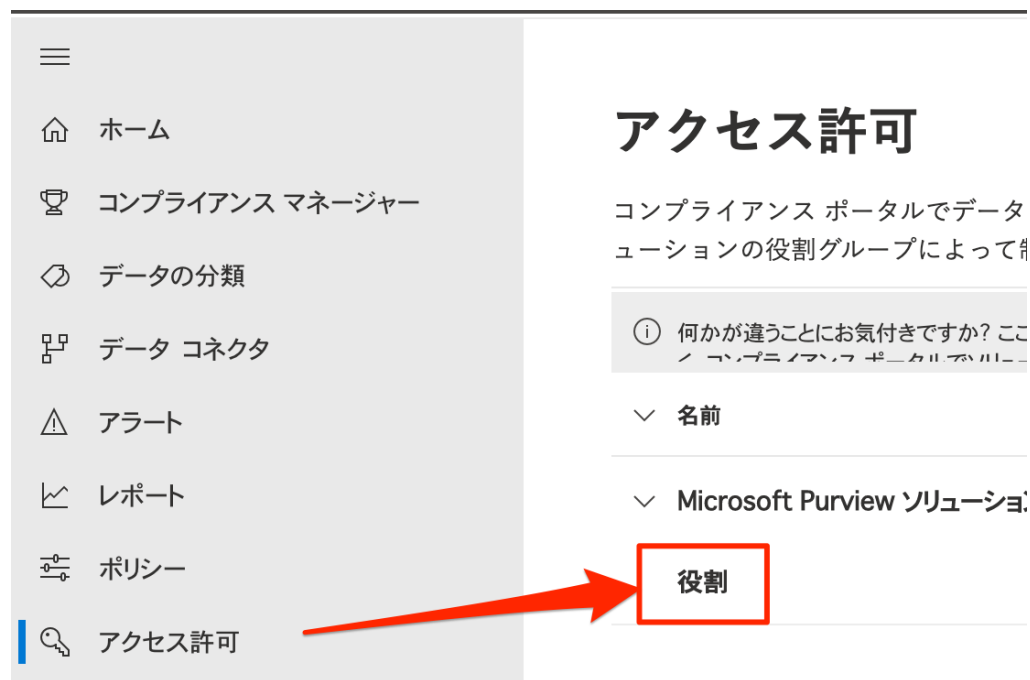
Microsoft Purviewのページにアクセス

- Microsoft Purview (<https://compliance.microsoft.com/homepage>) のページにアクセスする
 - アクセス権限がなければAzure ADグローバル管理者に権限付与のお願い

The screenshot shows the Microsoft Purview homepage. The left sidebar contains a navigation menu with the following items: ホーム (Home), コンプライアンス マネージャー (Compliance Manager), データの分類 (Data Classification), データ コネクタ (Data Connectors), アラート (Alerts), レポート (Reports), ポリシー (Policies), アクセス許可 (Access Reviews), and 試用版 (Trial). The main content area is titled 'ホーム' (Home) and features two primary cards. The first card, 'コミュニケーション コンプライアンス' (Communication Compliance), is titled 'コミュニケーション リスクを最小限に抑える' (Minimize communication risk) and includes a brief description and a link for more details. The second card, 'コンプライアンス マネージャー' (Compliance Manager), displays a 'コンプライアンス スコア: 74%' (Compliance Score: 74%) and includes a progress bar for 'Protect information' (27 / 434) and 'Govern information' (0 / 27). The top right of the interface shows settings, help, and a user profile icon labeled 'YG'.

権限付与のお願いの仕方

- Microsoft Purviewページの[アクセス許可] - [役割]の以下の権限を付与してもらう
 - Insider Risk Management



画面左の内部リスクの管理を開く

- アクセス権限がなければ (ry

The screenshot displays a web application interface. On the left is a sidebar menu with the following items: ホーム (Home), コンプライアンス マネージャー (Compliance Manager), データの分類 (Data Classification), データ コネクタ (Data Connector), レポート (Report), ポリシー (Policy), アクセス許可 (Access Permission), ソリューション (Solution), カタログ (Catalog), コンテンツの検索 (Content Search), コミュニケーション コンプライアンス (Communication Compliance), 電子情報開示 (Electronic Information Disclosure), 情報ガバナンス (Information Governance), 情報の保護 (Information Protection), and 内部リスクの管理 (Internal Risk Management). The '内部リスクの管理' item is highlighted with a red rectangular box. The main content area is titled 'ホーム' (Home) and features a 'コンプライアンス マネージャー' (Compliance Manager) card and a 'ソリューション カタログ' (Solution Catalog) card. The 'コンプライアンス マネージャー' card displays the message 'アクセスが拒否されました' (Access is denied) and a link to '詳細情報' (Detailed Information). The 'ソリューション カタログ' card displays the message 'コンプライアンスのニーズに対応するソリューションを見つける' (Find solutions that meet compliance needs) and a link to '詳細情報' (Detailed Information).

ホーム

コンプライアンス マネージャー

アクセスが拒否されました

コンプライアンス スコアにアクセスする権限がありません。適切なアクセス許可の付与について、グローバル管理者にお問い合わせください。

[詳細情報](#)

ソリューション カタログ

コンプライアンスのニーズに対応するソリューションを見つける

組織で利用できる新規および改善されたコンプライアンスおよびリスク管理ソリューションを見つけることができます

カタログを参照して、各ソリューションのメリットと、コンプライアンスのニーズを満たすために各ソリューションがどのようにインテリジェントに連携するかについて確認できます。

潜在的な内部リスクをスキャンする

● 推奨アクション部分のスキャンを実行する

内部リスクの管理

概要 アラート ケース ポリシー ユーザー フォレンジック レコーディング (

Yoshihito Gonohe、最初にこちらの対応を取ると、あなたの活動

<input type="radio"/> 潜在的な内部リスクをスキャンする	オプション
分析スキャンを実行して、組織内の潜在的なリスクを特定します。	
<input type="radio"/> 内部リスク管理について知識を得ましょう	オプション
ソリューションの詳細を知る... その内容、ベスト プラクティス、共通の専門用語、その他など。	
<input type="radio"/> 内部リスク設定の構成	必須
内部リスクのすべての機能とワークフローに適用される設定を定義します。	
<input checked="" type="checkbox"/> 最初のポリシーを作成	必須
事前定義済みのテンプレートを使用して、データの盗難などのリスクアクティビティを検出します。	
<input checked="" type="checkbox"/> あなたのチームが仕事を完了できることを確認する	必須
内部リスク管理の役割グループに他の管理者を追加して、アクセス許可を割り当てます。	

すべての推奨処理

潜在的な内部リスクをスキャンする

☐ 未開始 ⌚ 48 時間

分析スキャンを実行して、組織内の潜在的な内部リスクを検出します。結果を評価したら、推奨ポリシーを確認して設定します。[分析スキャンに関する詳細情報](#)

これから行うこと

- 内部リスク ポリシーによって検出された同じアクティビティに対して、組織内のソース (Microsoft 365 監査ログや Azure Active Directory など) をスキャンします。
- スキャンが完了すると、匿名化されたスキャン結果をレビューすることで、潜在的なリスクを特定し、どのポリシーを作成するかを決定できるようになります。

影響

スキャンは毎日実行されます。スキャンを停止する場合は、内部リスク設定で分析をオフにしてください。

通知


☒ 分析スキャンで分析情報が初めて検出されたときにメールを送信する

スキャンの実行 後で保存

おわり！

- おわりです。数日間待ちます。

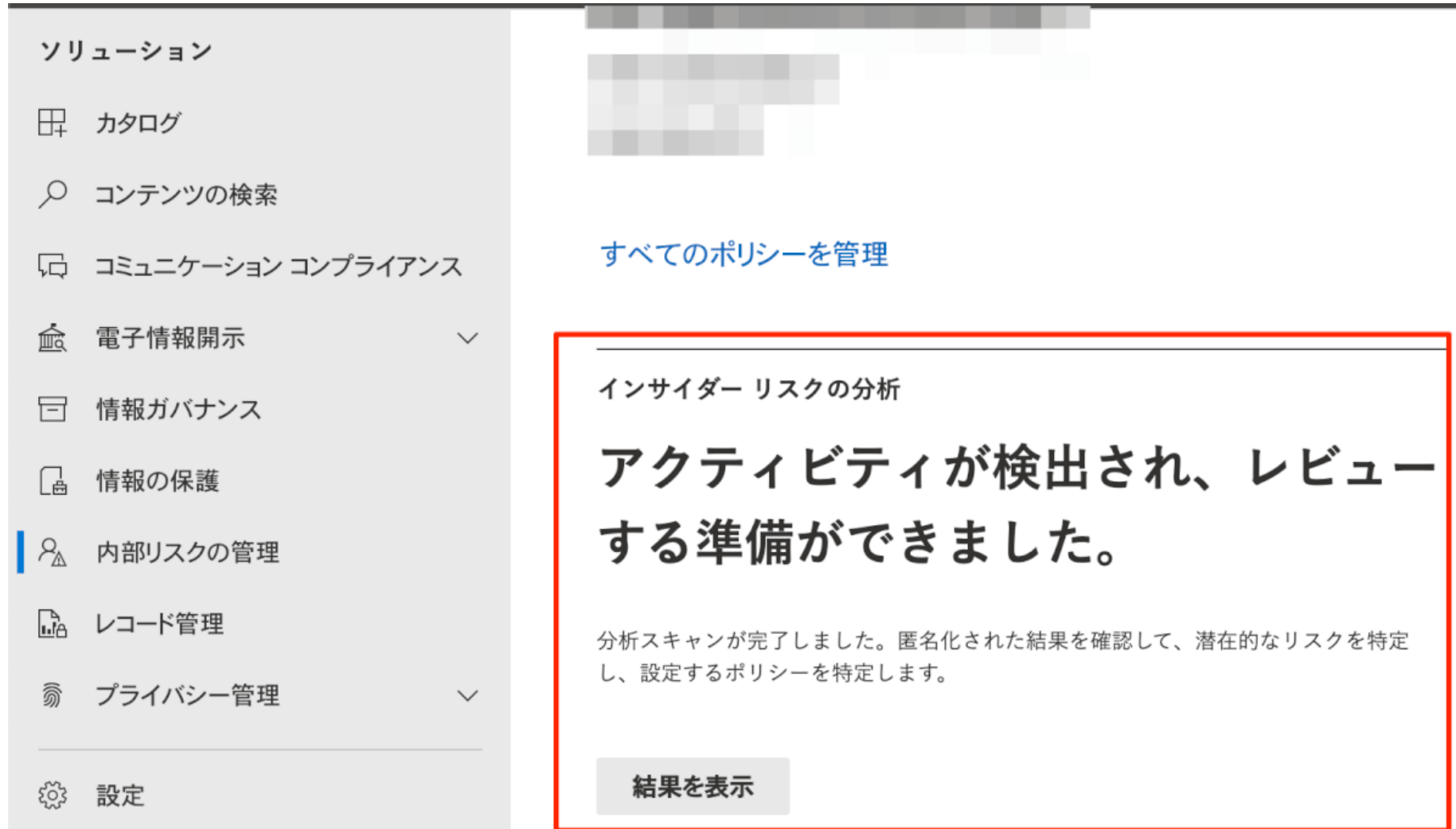


 スキャンが開始されました。結果報告をお待ちいただきありがとうございます。

お客様の環境にインサイダー リスクがないかスキャンするまでお待ちいただきありがとうございます。今後数日以内に、分析情報やポリシーに関する推奨事項がありましたら、メールでお知らせします。このソリューションでは、レポートを確認して [概要] ページで表示することもできます。

スキャン完了後

- 数日後に内部リスクの管理画面から、結果を表示できます。



結果の表示

- 検出された潜在的なリスクと、対処するための分析情報と推奨事項が表示されます。

データ漏洩の可能性のあるアクティビティ

0% のユーザー 流出処理を実行しました

スキャンされた 3 ユーザーからのアクティビティ

おすすめ: ユーザーの「一般的なデータ漏洩」ポリシーを設定する

組織外での情報の偶発的な共有から悪意のあるデータの盗難まで、潜在的なデータ漏洩を検出して警告します。

詳細を表示

上位の流出アクティビティ

おすすめ

ユーザーの「一般的なデータ漏洩」ポリシーを設定する

組織外での偶発的な情報共有から悪意のあるデータ盗難まで、潜在的なデータ漏洩を検出して警告するポリシーを作成します。

詳細を表示

組織外のユーザーにメールを送信する

スキャンされた 2 ユーザーからのアクティビティ

ユーザーの上位 1% が組織外のユーザーに 32 回以上メールを送信しました

ユーザーの上位 5% が組織外のユーザーに 32 回以上メールを送信しました

ユーザーの上位 10% が組織外のユーザーに 32 回以上メールを送信しました

SharePoint ファイルをダウンロードしています

スキャンされた 1 ユーザーからのアクティビティ

ユーザーの上位 1% が SharePoint ファイルを 2 回以上ダウンロードしました

ユーザーの上位 5% が SharePoint ファイルを 2 回以上ダウンロードしました

ユーザーの上位 10% が SharePoint ファイルを 2 回以上ダウンロードしました



このセッションで話すこと

1. 概要・利用できるライセンス
2. 始め方
3. 今後の展望

今後の展望

- ID領域でもHRを上流として、IdPやIGAに入退社情報や異動情報を流し込み、下流のシステムへのProvisioning/Deprovisioningやアクセス権変更を行う流れ。（HR Driven Provisioning）
- Insider Risk ManagementもHRコネクタがあり、退職日データを流し込むことで、退職日直前の人々の行動について絞りこむことができる。
- データ持ち出しの観点でもHR情報を活用する世界線に今後なるかも。

おしまい