

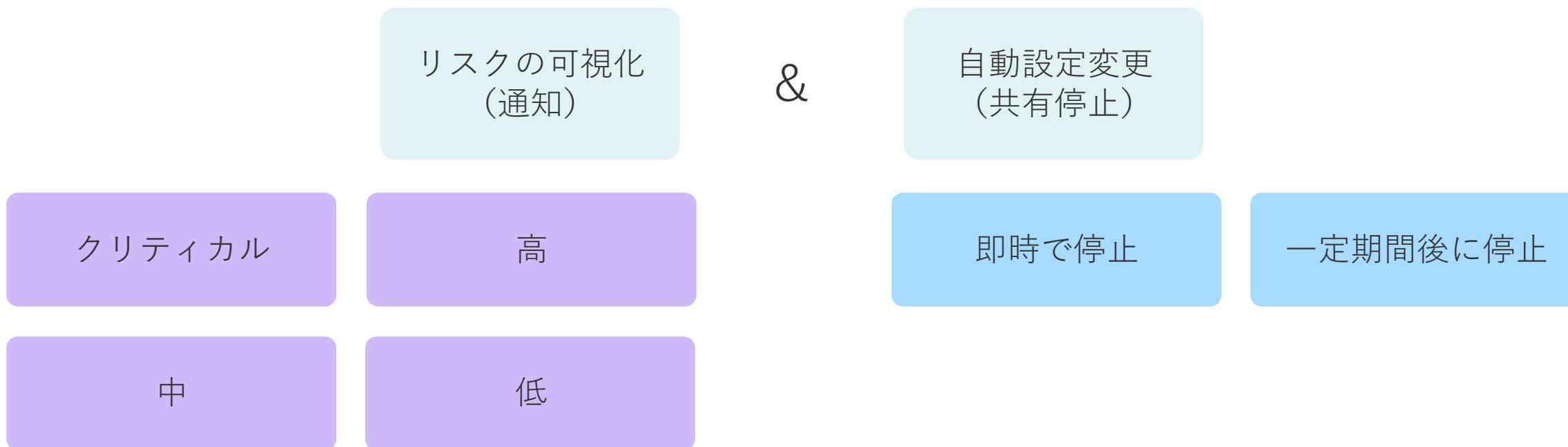


セキュリティリスクの検出ポリシー設定 に関する活用例

セキュリティリスクの検出ルールとしてご活用いただける設定集を紹介します。

基本的なフィルター（ポリシー）の考え方

- 可視化（通知）と共有停止の2つの観点でフィルターを組みます。
- 可視化（通知）はリスク度を「クリティカル」「高」「中」「低」の4つのレベルで表現可能です。
- 共有停止は「即時停止」か「一定の日数が経過後に停止」から選択可能です。



外部共有の基本的な考え方

- ファイル転送
 - 大容量ファイル送信ツールを用いてファイルを転送する方式
 - HENNGE Secure Transferなどのリンクを生成して取引先にダウンロードしてもらうものが一般的
- 外部共有 / コラボレーション
 - ファイルやフォルダに対するアクセス権限、編集権限を外部のユーザに与える方式
 - 自由にアップロード・ダウンロード、共同編集が可能
- インターネット公開
 - ファイルに紐づくURLを発行し共有する方式
 - リンクを知っている特定ドメイン（特に社内）の人に限定する場合と誰でもアクセス可能な一般公開のパターンが存在する

設定例について

- 次頁以降にて、検出するセキュリティリスクのポリシー設定例をご紹介します。
設定時は以下の画面右上 [検出するセキュリティリスクを追加] から追加が可能です。
- 同条件にてファイル共有自動停止のポリシーを作成することも可能です。

リスク管理

- ダッシュボード
- セキュリティリスク一覧**
- ファイル
 - ファイル一覧
 - ファイル共有自動停止
- テナント管理
 - アプリ連携
 - ユーザー
 - バックグラウンド処理
 - 監査ログ

セキュリティリスク一覧

検出するセキュリティリスクを追加

66% 合計スコア 9 セキュリティリスク 3 リスク対象あり 1 アプリ

セキュリティリスク名	カテゴリ	アプリ	危険度	リスク対象数
OneDriveの「社内ドキュメント」フォルダの外部共有状況	データ漏洩対策	Henнге M365 example	クリティカル	0
OneDrive: ファイルがインターネット上に公開されている	データ漏洩対策	Henнге M365 example	クリティカル	17
SharePoint: ファイルがインターネット上に公開されている	データ漏洩対策	Henнге M365 example	クリティカル	0
退職予定者の外部共有状況	データ漏洩対策	Henнге M365 example	高	0
SharePoint: ファイルが外部に共有されている	データ漏洩対策	Henнге M365 example	高	0
OneDrive: ファイルが外部に共有されている	データ漏洩対策	Henнге M365 example	高	1
特定ドメイン以外へのファイル共有状況を確認	データ漏洩対策	Henнге M365 example	中	0
SharePoint のインターネットに公開されたファイル・フォルダ	データ漏洩対策	Henнге M365 example	中	0
OneDrive のインターネットに公開されたファイル・フォルダ	データ漏洩対策	Henнге M365 example	中	17

ページごとの行 50 ▼ 1~9/9 < >

Case 1. 外部共有禁止フォルダの外部共有状況を可視化する

- 社内共有と外部共有の用途でフォルダを明確に分けられている場合に用いられます。

1 全体設定

連携アプリ
セキュリティリスク検出の対象とする連携アプリを設定します

セキュリティリスクの危険度
セキュリティリスクの危険度を設定します

セキュリティリスク検出の名前
セキュリティリスク検出の名前を設定します

セキュリティリスク検出の説明文
セキュリティリスク検出の説明文を設定します

2 セキュリティリスク検出条件

セキュリティリスク検出の条件

追加条件

データ	パス	が次を含む
	パス	が次を含む

+ AND 条件を追加

+ OR 条件を追加

ファイル一覧で確認

対象の連携アプリを指定します。
ここではOne Driveの「社内ドキュメント」というフォルダで社外秘のファイルを保管しているイメージで設定します。

任意の値を入力します。

対象のフォルダパスを指定します。

※ 通知設定は任意でご利用ください。

Case 2. 退職予定者のファイル外部共有状況を可視化する

- 退職予定が決まった日などを起点に、退職予定者がオーナーとなっている外部共有ファイルの状況を確認します。

1 全体設定

連携アプリ
セキュリティリスク検出の対象とする連携アプリを設定します

セキュリティリスクの危険度
セキュリティリスクの危険度を設定します

セキュリティリスク検出の名前
セキュリティリスク検出の名前を設定します

セキュリティリスク検出の説明文
セキュリティリスク検出の説明文を設定します

2 セキュリティリスク検出条件

セキュリティリスク検出の条件

追加条件

データ	オーナー	が次を含む	特定のユーザー	user3 HENNGE	×
AND	共有検出日	が次以降	2024/04/01	📅	×

+ AND 条件を追加

+ OR 条件を追加

ファイル一覧で確認

対象の連携アプリを指定します。

任意の値を入力します。

対象のユーザと期間を指定します。
ここでは退職予定者と退職の話から1ヶ月遡った日付として指定しています。

Case 3. 特定ドメイン以外への外部共有状況を可視化する

- 事業会社や外部協力会社など特定のドメイン以外への共有状況を確認します。

セキュリティリスク検出ルールの新規作成

1 全体設定

連携アプリ
セキュリティリスク検出の対象とする連携アプリを設定します

Henнге osaka test

セキュリティリスクの危険度
セキュリティリスクの危険度を設定します

中

セキュリティリスク検出の名前
セキュリティリスク検出の名前を設定します

特定ドメイン以外へのファイル共有状況を確認

セキュリティリスク検出の説明文
セキュリティリスク検出の説明文を設定します

特定ドメイン以外へのファイル共有状況を確認

2 セキュリティリスク検出条件

セキュリティリスク検出の条件

OneDrive でファイルが外部ユーザーに共有されたとき

追加条件

データ	共有ドメイン	が次で終わらない	@hogehoge.co.jp	×
AND	共有ドメイン	が次で終わらない	@henнге.com	×

+ AND 条件を追加

+ OR 条件を追加

ファイル一覧で確認

対象の連携アプリを指定します。

任意の値を入力します。

対象のドメイン（事業会社や協力会社など）を指定します。
ここでは2つのドメインを「AND」で指定しています。

ここで指定したドメイン「以外」の共有状況を検出できます。