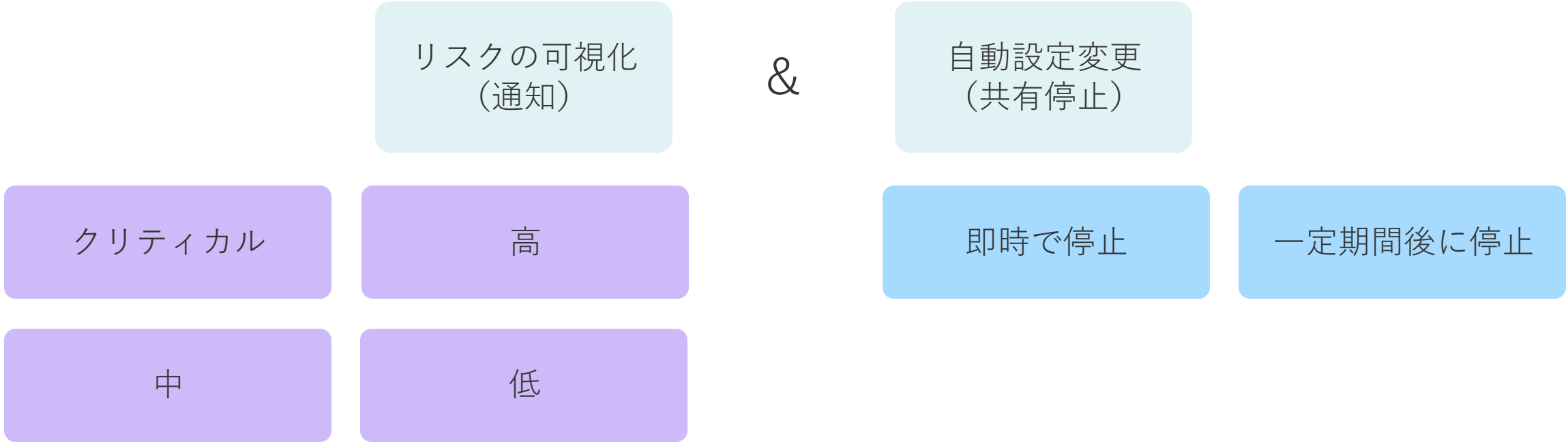
セキュリティリスクの検出ポリシー設定に関する活用例

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

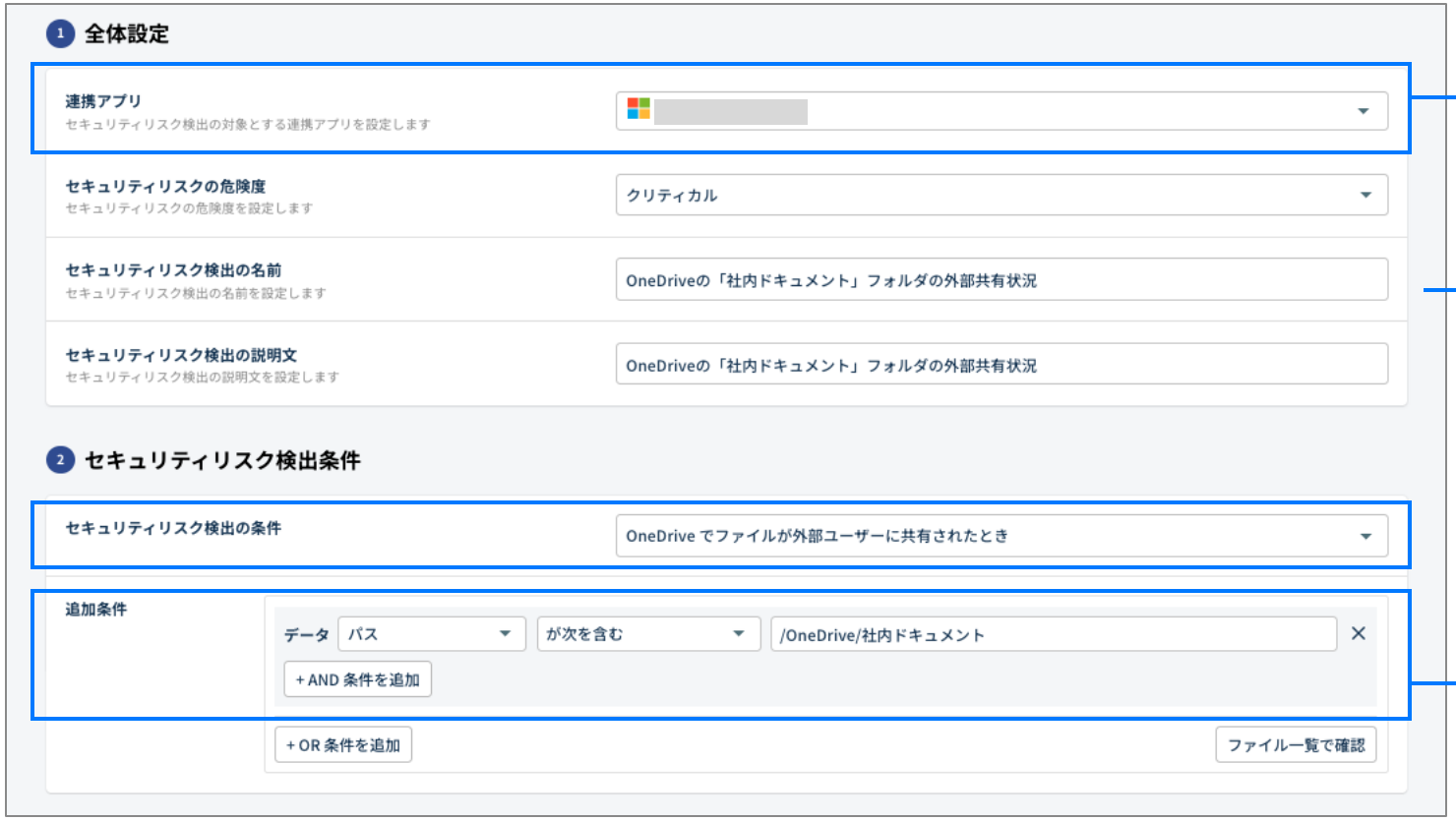
- インターネット公開
  - ファイルに紐づくURLを発行し共有する方式
  - リンクを知っている特定ドメイン（特に社内）の人に限定する場合と誰でもアクセス可能な一般公開のパターンが存在する

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。

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。



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。

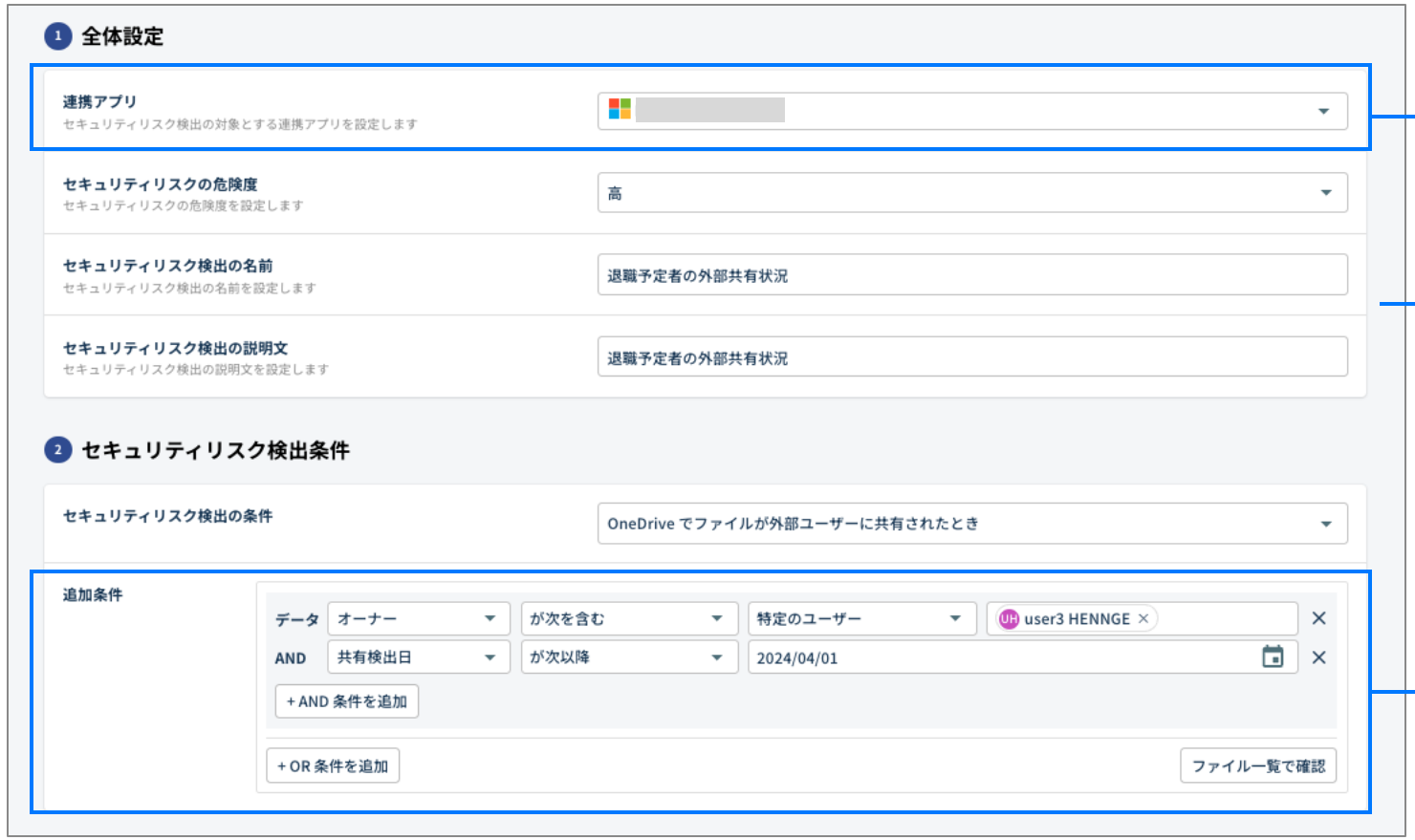
任意の値を入力します。

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。



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。

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。