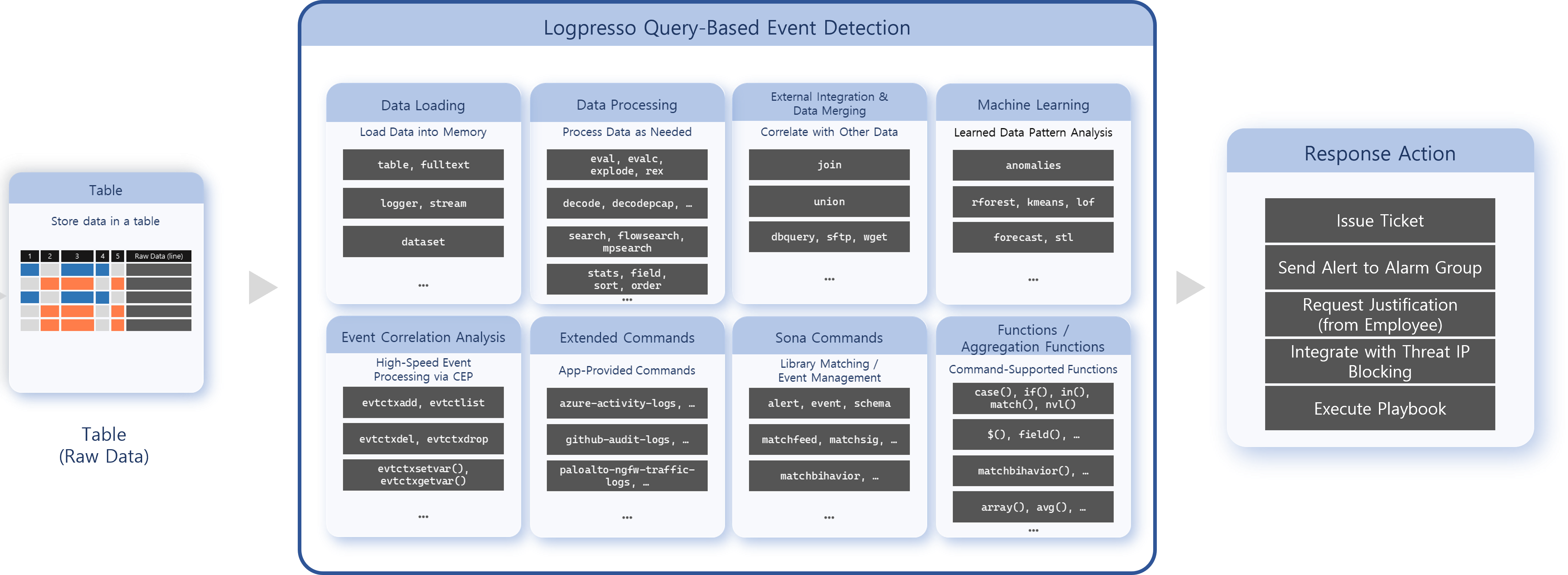
### バッチルール

#### 概要

バッチルールは、[ログプレッソクエリ](https://docs.logpresso.comnull)を定期的またはスケジュールに従って実行し、さまざまなシステムから収集されたデータ間の相関分析やイベント検出を行います。これにより、イベントの関連性や活動、パターンの詳細な分析が可能となります。バッチルールは通常、テーブルに保存されたデータに適用されます。以下の図は、バッチルールの動作イメージを示しています。

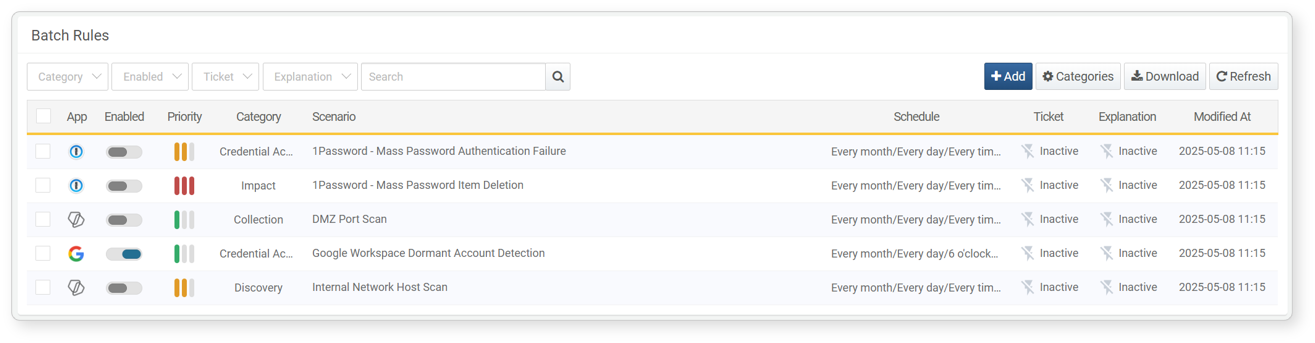


バッチルールは[ログプレッソクエリ](https://docs.logpresso.comnull)のコマンドや関数を活用し、柔軟なシナリオ作成が可能です。たとえば、特定ユーザーの行動を分析して潜在的な脅威を予測したり、不審な行動を検出したりできます。

多くの場合、バッチルールはイベント検出時にチケットを発行したり、アクターに弁明を要求します。アナリストやセキュリティチームのアラート疲労を防ぐため、ログプレッソ・ソナーは重複チケットの発生を抑制する仕組みを提供しています。同一内容のイベントは、アラームメッセージや定義された重複判定フィールドに基づき、1件のチケットとして処理できます。

#### バッチルールの検索

**ポリシー** > **バッチルール** で、バッチルールの一覧を閲覧・検索できます。



* **アプリ**: 関連アプリを示すアイコン。デフォルトルールやユーザー追加ルールはログプレッソアイコン、インストール済みアプリのルールは各アプリアイコンで表示されます。
* **有効化**: ルールの有効/無効を切り替えるトグルボタン (: 有効, : 無効)
* **状態**: **有効化**設定に応じたルールの状態（**緑**: 有効、**グレー**: 無効）
* **優先度**: ルールの重要度（高・中・低）
* **カテゴリ**: カテゴリ情報
* **ルール**: バッチルール名
* **タイプ**: ルールに設定された[ログスキーマ](https://docs.logpresso.comnull)
* **最終変更日**: バッチルールの最終変更日（または作成日）

特定のバッチルールを検索するには、ツールバーの検索ツールを利用します。検索ツールは、入力したキーワードがルールの**名前**、**説明**、**クエリ**フィールドに含まれるものを検索します。大文字・小文字は区別されません。

バッチルールの有効化・無効化

バッチルールを有効または無効にするには、該当ルールの**有効化**列のトグルボタン (: 有効, : 無効) をクリックします。

バッチルール一覧のダウンロード

バッチルール一覧をローカルPCに保存するには、ツールバーの**ダウンロード**をクリックし、希望するファイル形式を選択してください。

バッチルール一覧の更新

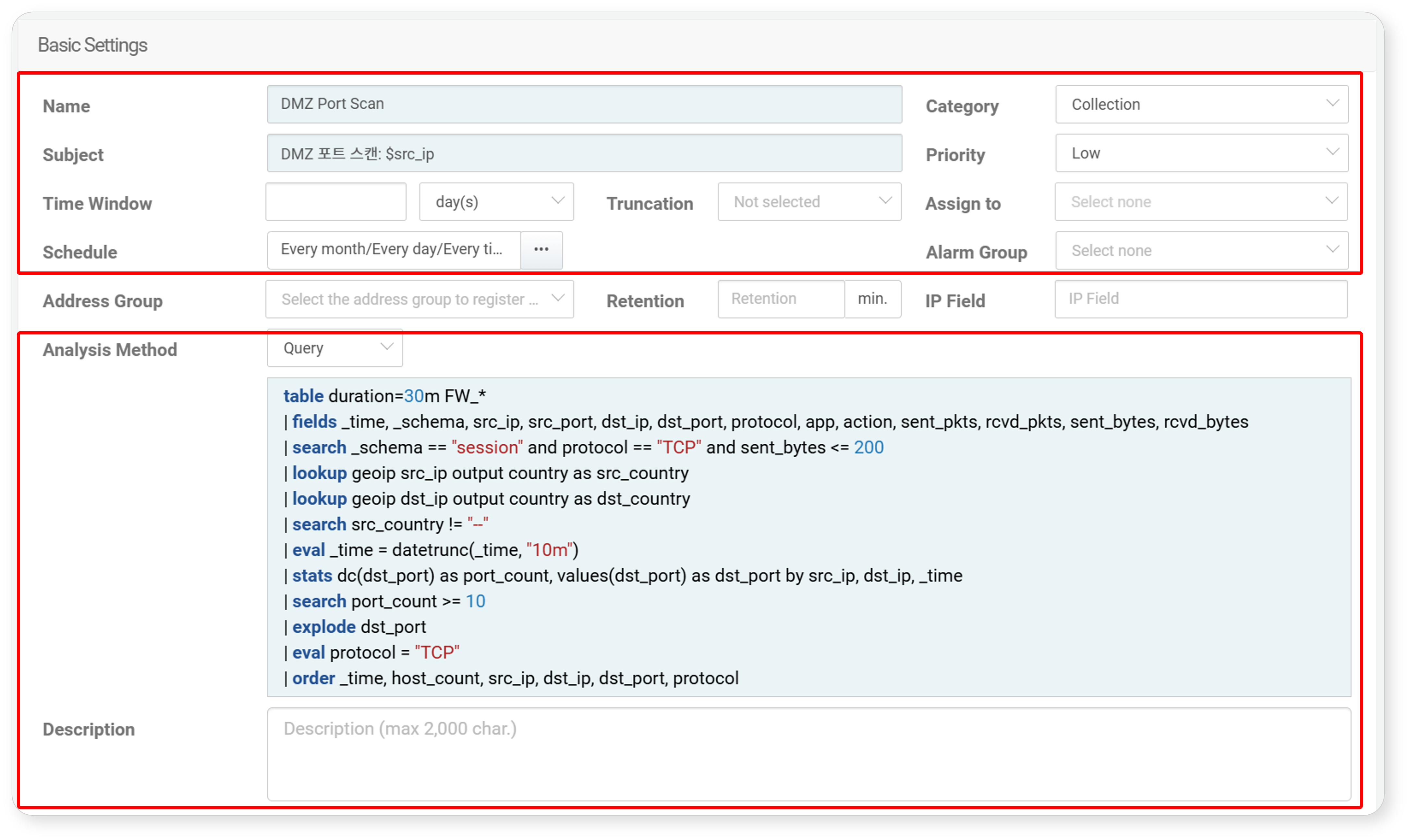
最新のバッチルール一覧を表示するには、ツールバーの**更新**をクリックします。

#### バッチルールの追加

バッチ検出ルールを追加するには、以下の手順に従います。

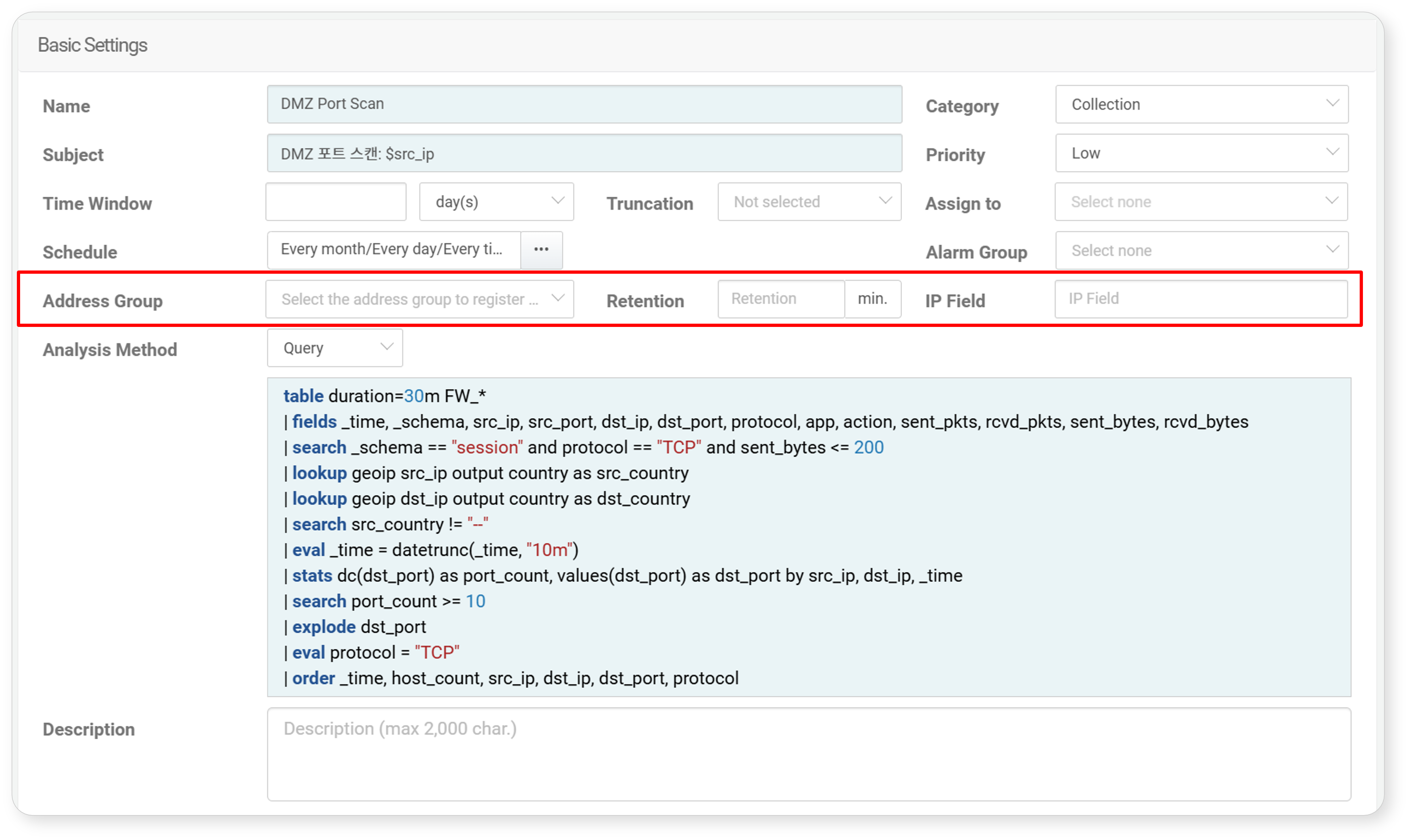
**ポリシー** > **バッチルール** に移動し、ツールバーの**追加**をクリックします。

**バッチルール追加**画面で、以下の基本設定を入力します。



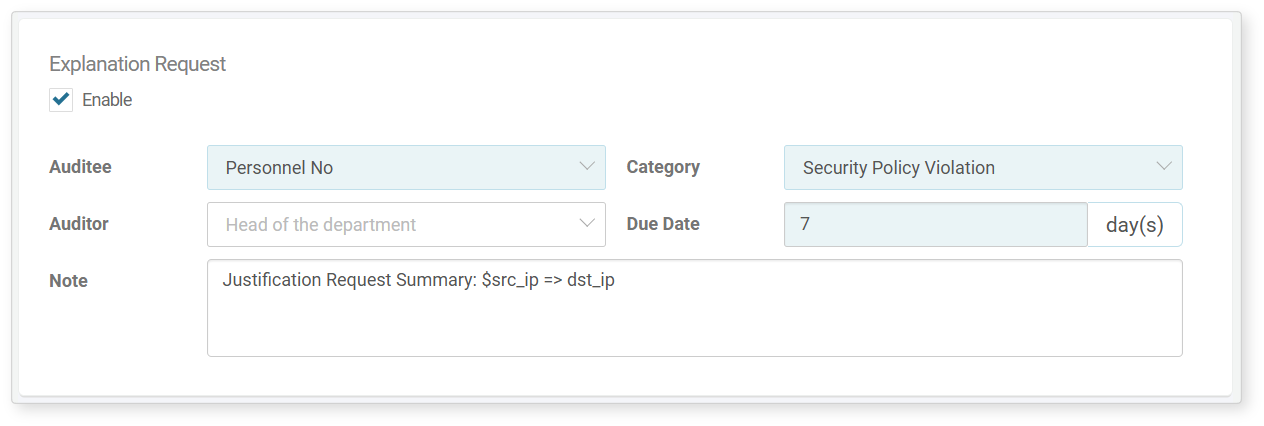
* **名前**: バッチルールの一意な名称（最大50文字）。重複不可。
* **カテゴリ**: バッチルールのカテゴリ。ツールバーの**カテゴリ**から新規追加も可能です。カテゴリ未設定の場合、チケットは発行されません。
* **メッセージ**: イベント検出時にチケットへ付与されるタイトル
* [ログスキーマ](https://docs.logpresso.comnull)で定義されたフィールド名を $field または $field$ 形式で使用できます。イベント検出の根拠となったログからフィールド値を取得してメッセージが生成されます（例: $src\_ip）。日本語フィールド名の場合は必ず $FieldName$ 形式を使用してください。
* **詳細設定**の**重複判定フィールド**が未設定の場合、生成されたメッセージ（最大2,000文字）が同一かどうかで重複チケットの発生を防ぎます。
* **優先度**: 検出イベントの重大度（高・中・低）。
* **タイムウィンドウ**: **分析方法**が**クエリ**の場合、データ分析対象期間を定義します。fromおよびtoパラメータの値を計算して分析範囲を指定します。数値＋単位（秒、分、時、日）で入力します。デフォルトは未設定です。
* この機能を利用するには、データ取得コマンド（例: table）内で from=$("from") to=$("to") を含める必要があります。
* 例：**タイムウィンドウ**を30日に設定した場合、table from=$("from") to=$("to") FW\_\* のようなクエリで、実行時点から過去30日間の\*\*"FW\_"\*\*で始まるテーブルのデータを取得します。（範囲: 1～3,153,600,000）
* **丸め単位**: 取得データに適用する時間精度。None、秒、分、時、日から選択可能。デフォルトは**None**。
* **タイムウィンドウ**が**5分**、**丸め単位**が**秒**の場合、ミリ秒は切り捨てられ、タイムスタンプは秒単位に丸められます。
* **担当者**: 発行されたチケットを割り当てる[ユーザー](https://docs.logpresso.comnull)アカウント。複数選択可能。未指定の場合は担当者なしでチケットが作成されます。
* **スケジュール**: 検出ルールの実行インターバル。[CRON構文](https://www.man7.org/linux/man-pages/man5/crontab.5.html)で設定可能です。
* **アラームグループ**: イベント検出時にアラームを受信する[アラームグループ](https://docs.logpresso.comnull)。
* アラーム受信設定は、選択したアラームグループ内で構成する必要があります。
* **分析方法**: スケジュールに従って実行されるデータ分析方法（デフォルト: クエリ）。
* **データセット**: [学習データセット](https://docs.logpresso.comnull)リストから選択。
* **クエリ**: クエリを入力（最大5,000文字）。
* **説明**: バッチルールの詳細説明（最大2,000文字）。

攻撃者IPや異常アクターのIPを個別管理したり、アドレスグループ情報をファイアウォールやIPSへ転送する場合は、以下の設定を行います。



* **アドレスグループ**: **IPフィールド**で指定した値（IPアドレス）を追加する[アドレスグループ](https://docs.logpresso.comnull)。
* **保持期間**: **アドレスグループ**内でIPアドレスを保持する期間（分単位）。指定期間経過後、自動的にアドレスグループから削除されます。未指定の場合は無期限（範囲: 1～100,000,000）。
* **IPフィールド**: イベント検出時に**アドレスグループ**へ追加するIPアドレスを含むフィールド名。[ログスキーマ](https://docs.logpresso.comnull)で定義されたIP関連フィールド名（例: src\_ip, dst\_ip）（最大50文字）。
* ブロック連携など外部セキュリティシステムとの連携については、「システム > レスポンスターゲット」を参照してください。

検出イベントが自社従業員に関する場合、**弁明**を従業員に要求できます。



* **弁明要求**: 検出された脅威やイベントに関与した従業員または関係者に弁明を要求するかどうか（デフォルト: 無効）。
* **従業員**: 検出イベントの責任者となる従業員IDを含むフィールド。
* 脅威検出時、指定した従業員IDに紐づく従業員へ自動的に弁明要求メールが送信されます。この場合、**ポリシー** > **従業員**で従業員情報（従業員ID、アカウント、メール）が設定されている必要があります。
* **カテゴリ**: 弁明要求の分類。必要に応じて、**レスポンス** > **弁明** > **カテゴリ**で追加設定可能です。
* **監査者**: 提出された弁明の二次審査者（未設定時は「部門長」がデフォルト）。一次・二次審査者の詳細は[弁明](https://docs.logpresso.comnull)を参照してください。
* **期限**: 弁明提出の締切日（デフォルト: 7日）。期限を過ぎると弁明提出はできません。
* **備考**: 弁明要求メールに含める追加情報。入力内容はメール/SMSテンプレートの $user\_note マクロ部分に挿入されます。ログスキーマで定義されたフィールド名を $FieldName マクロ形式で挿入すると、値がメッセージ内で置換されます。**レスポンス** > **弁明**の詳細画面でも備考を確認できます（最大10,000文字）。

弁明要求には「emp\_key」フィールドが必要です。存在しない場合は、手順5の\*\*クエリ\*\*でユーザーアカウントやIPアドレスを従業員IDにマッピングするクエリを作成し、「emp\_key」フィールドを生成してください。

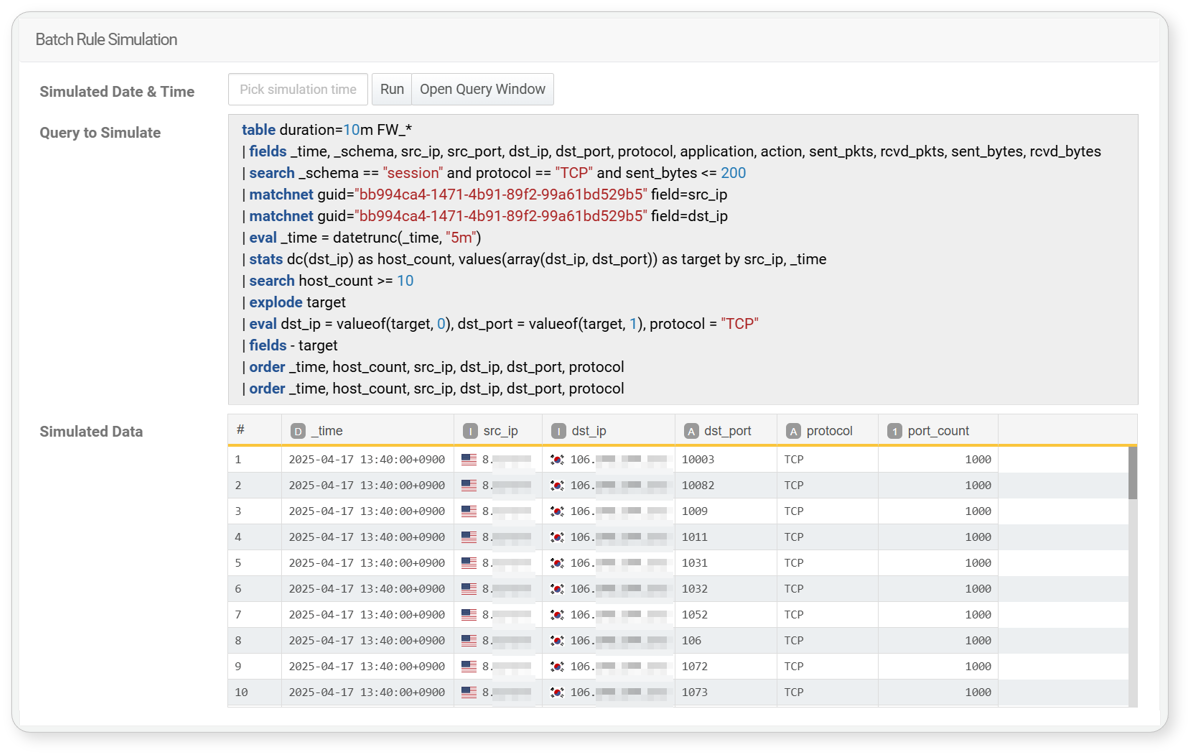
イベント検出時にチケットを発行する場合は、**詳細設定**を構成します。

* **チケット分類**: セキュリティ運用時にチケットを分類するための[チケット分類](https://docs.logpresso.comnull)（デフォルト: なし）
* イベント検出時に自動でチケットを発行するには、チケット分類の指定が必要です。

チケット発行は、イベントトリガーで起動するプレイブック内でも制御可能です。プレイブック内で制御する場合は、ここでの設定は不要です。```

* **重複判定フィールド**: 重複チケット検出に使用するフィールドをマクロ形式（例: $field\_name）でカンマ区切りで指定（最大2,000文字）。未指定時は**メッセージ**文字列が基準となります。
* **重複無視期間**: チケット発行後、重複イベントを無視する期間（デフォルト: 0、範囲: 0～86,400秒）。
* 「0」設定時：**チケット再割当期間**の設定に従います。
* 非0設定時：指定期間中は重複イベントを無視し、チケットの根拠データには含まれません。
* **チケット再割当期間**: 同一イベント発生時に新規チケットを作成せず、既存チケットに根拠データや発生回数を追加する期間（デフォルト: 3,600秒、範囲: 0～86,400秒）- 「0」設定時：イベント発生ごとに同一タイトルの新規チケットが作成されます。- 非0設定時：指定期間中は既存チケットに根拠データや発生回数が追加されます。
* **フィールド順序**: チケットの根拠データに表示するログデータフィールドの順序。カンマ区切りでフィールド名を入力（最大2,000文字）。特殊文字やパイプ（|）は使用不可。
* **チケットクローズ時の処理**: **チケット再割当期間**有効時、チケットクローズ後の処理方法（デフォルト: タイマーリセット）。- **タイマー維持**: チケットクローズ後も、マージタイマー有効期間内に同一脅威イベントが発生した場合、根拠データや発生回数がクローズ済みチケットに追加されます。- **タイマーリセット**: チケットクローズ時にマージタイマーも終了し、以降の同一脅威イベントには新規チケットが作成されます。

バッチルールのシミュレーションを、過去または未来の特定時点で実行できます。バッチルールシミュレーション欄で実行時刻を設定し、**実行**をクリックします。



クエリに無効な構文や存在しないデータテーブルの参照、その他実行上の問題がある場合、バッチルールシミュレーションは実行できません。

#### バッチルールの複製

既存のバッチルールを複製するには：

バッチルール一覧で複製したいルールのチェックボックスを選択します。

ツールバーにアクションメニューが表示されるので、**複製**をクリックします。

**バッチルール複製**ダイアログで選択内容を確認し、**複製**をクリックします。キャンセルする場合は**キャンセル**をクリックします。

* 複製されたルールは「元のルール名のコピー」という名称で無効状態で追加されます。

#### バッチルールの編集

バッチルールを編集するには：

バッチルール一覧で編集したいルール名をクリックします。

**バッチルール編集**画面で情報を更新し、**OK**をクリックします。編集可能な項目の説明は[バッチルールの追加](https://docs.logpresso.comnull)を参照してください。

#### バッチルールの手動実行

バッチルールを手動で実行するには：

バッチルール一覧で実行したいルール名をクリックします。

ツールバーにアクションメニューが表示されるので、**今すぐ実行**をクリックします。

ルールがイベントを検出した場合、**レスポンス** > **チケット**または**分析** > **検出サマリー**で検出結果を確認できます。

無効状態のバッチルールを実行しても、正常に実行されますがチケットは発行されません。

#### バッチルールの削除

バッチルールを削除するには：

バッチルール一覧で削除したいルールのチェックボックスを選択します。

ツールバーにアクションメニューが表示されるので、**削除**をクリックします。

**バッチルール削除**ダイアログで選択内容を確認し、**削除**をクリックします。キャンセルする場合は**キャンセル**をクリックします。

#### ルールカテゴリ

ルールカテゴリの追加・編集・削除が可能です。詳細は[ストリームルール – ルールカテゴリ](https://docs.logpresso.comnull)を参照してください。