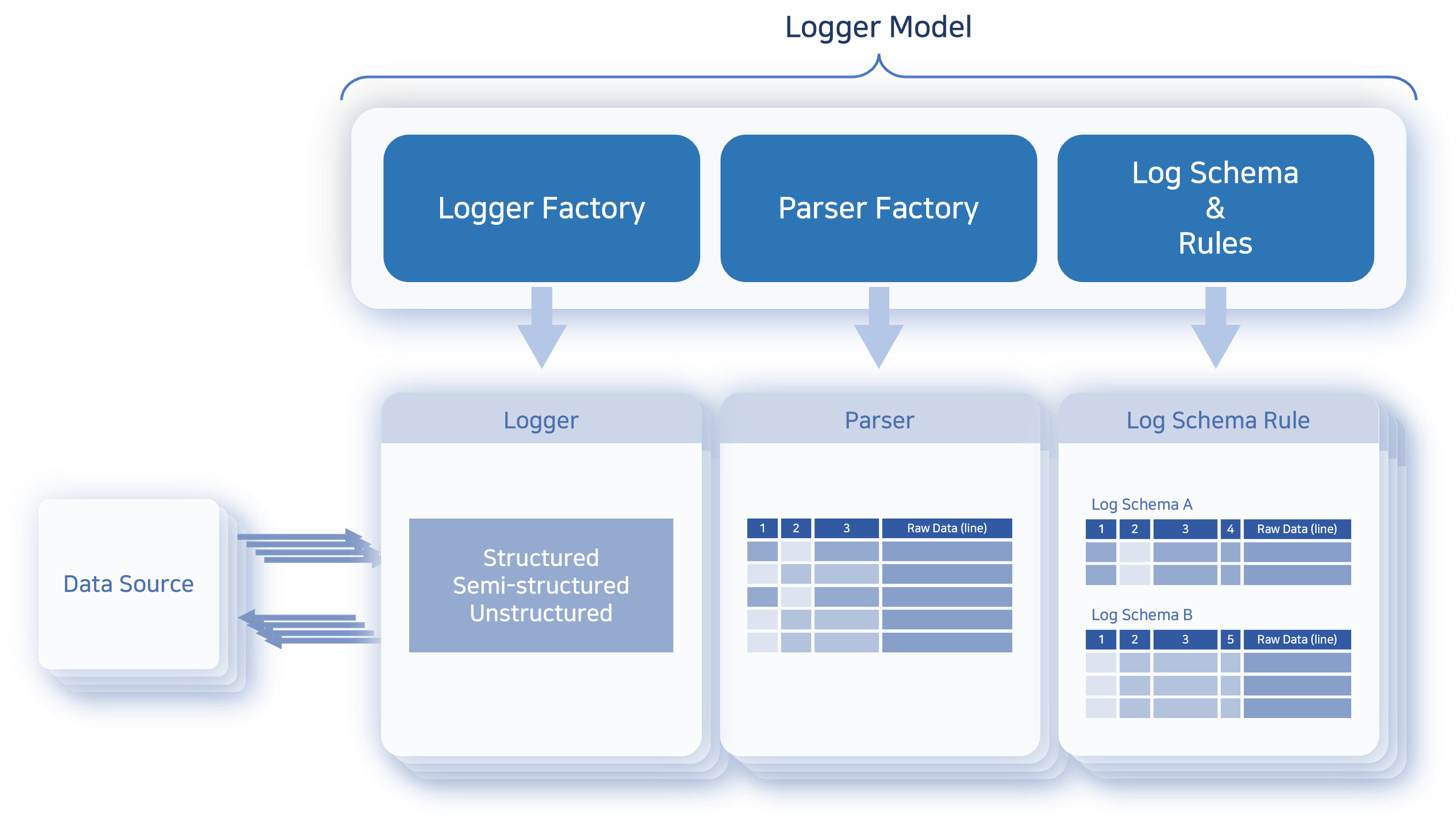
### ロガーモデル

#### 概要

ロガーモデルは、データ収集から正規化までの全データ処理パイプラインを定義するロードマップです。ロガーによる元データの収集方法、収集データのパース方法、パース後データの正規化方法を指定します。



一部のロガーモデルでは、パーサーが不要な場合があります。これは、ログデータがすでに構造化されており追加のパース処理が不要な場合に該当します。例えば、データベースに保存されたデータはフィールドごとに分割されているため、別途パース処理を行う必要がありません。

ロガーモデル：ベースモデルとアプリモデル

ロガーモデルは、ベースロガーモデルとアプリロガーモデルに分類されます。パーサーと同様に、管理者がロガーモデルを手動で設定する必要はほとんどありません。

**ベースロガーモデル**

ベースロガーモデルは、アプリをインストールしなくてもログプレッソ・ソナーで利用可能です。初期状態では、以下の2つのベースロガーモデルが提供されます。

|  |  |
| --- | --- |
| 名前 | 説明 |
| WTMP | wtmpログファイルの収集および正規化方法を定義します。 |
| Windows XML Event Log | Windowsのイベントログの収集および正規化方法を定義します。 |

Windows XMLイベントログ収集モデルは、Windowsセントリーを利用する環境でのみ対応しています。

以下は、ログプレッソ・ソナーで利用可能なベースロガーモデルタイプの一覧です。[ロガー固有の設定](https://docs.logpresso.comnull)は、ロガータイプによって異なります。

|  |  |
| --- | --- |
| タイプ | 説明 |
| CEPイベント | CEP（Complex Event Processing）イベントデータを収集します。 |
| 設定ファイルウォッチャー | ローカルホスト上で特定のパターンや名前に一致するファイルの変更を収集します。 |
| DNSスニファー | PCAPデバイスを通じてミラーリングされたDNS通信パケットをキャプチャします。 |
| 日次ローテーションディレクトリウォッチャー | ローカルホスト上で日次で作成されるディレクトリから一致するテキストログファイルを収集します。 |
| ディレクトリウォッチャー | ローカルホスト上の特定ディレクトリから定期的にテキストログファイルを収集します。 |
| ディスク使用量ロガー | ログプレッソ・ソナーのノードまたはセントリーのディスク使用量を定期的に監視・収集します。 |
| 外部プログラム | ローカルホスト上で実行されるコマンドやスクリプトの標準出力を収集します。 |
| FTP日次ディレクトリウォッチャー | リモートホスト上でFTP経由で日次作成されるディレクトリから一致するテキストログファイルを収集します。 |
| FTPディレクトリウォッチャー | リモートホスト上の特定ディレクトリからFTP経由でテキストログファイルを収集します。 |
| FTPローテーションログファイル | リモートホスト上でFTP経由で単一のローテーションテキストログファイルを収集します。 |
| フォワーダーパフォーマンス | ログプレッソ・ソナークラスター内のフォワーダーノードのパフォーマンスログを収集します。 |
| GZIPディレクトリウォッチャー | ローカルホスト上でGZIP形式で圧縮されたテキストログファイルを収集します。 |
| GZIP再帰ディレクトリウォッチャー | ローカルホスト上の特定ディレクトリから、特定パターンや名前に一致するGZIPログファイルを収集します。 |
| HTTPモニター | リモートホストからWebサービスのレスポンスコードや統計情報を収集します。 |
| HTTP POST | リモートホストからHTTP POSTメソッドで送信されたデータを収集します。 |
| HTTPスニファー | PCAPデバイスを利用してHTTPパケットを収集します。 |
| JDBCロガー | JDBCを利用してデータベースからデータを収集します。 |
| Linuxアカウントウォッチャー | ローカルホスト上のアカウントリストファイル（passwd）の変更を収集します。 |
| マルチローテーションログファイル | 異なるパスにバックアップされ、定期的に削除・再作成されるログファイルを収集します。 |
| NetFlow | NetFlow v5/v9パケットを収集します。 |
| PCAPディレクトリウォッチャー | ローカルディレクトリからPCAPファイルを収集します。 |
| PCAPパケット | PCAPデバイスを利用してすべてのパケットを収集します。 |
| RSS | 指定したURLのRSSフィードからデータを収集します。 |
| 再帰ディレクトリウォッチャー | ローカルホスト上の指定ディレクトリから、特定パターンや名前に一致するテキストログファイルを収集します。 |
| ローテーションログファイル | ローカルホスト上で単一のローテーションテキストログファイルを収集します。 |
| SFTP日次ローテーションディレクトリウォッチャー | SFTP経由で日次作成されるディレクトリを巡回し、一致するテキストログファイルを収集します。 |
| SFTPディレクトリウォッチャー | リモートホスト上の特定ディレクトリからSFTP経由でテキストログファイルを収集します。 |
| SFTPローテーションログファイル | リモートホスト上でSFTP経由で単一のローテーションテキストログファイルを収集します。 |
| SFTP WTMPファイル | リモートホスト上でSFTP経由でWTMPログを収集します。 |
| SNMP GET | SNMPエージェントからデータを収集します。 |
| SNMP Trap | SNMPトラップで受信したSNMPメッセージを収集します。 |
| SNMPv3 GET | SNMPv3エージェントからデータを収集します。 |
| SNMPv3ネットワーク使用量ロガー | SNMPv3エージェントからネットワークインターフェースのトラフィック統計を収集します。 |
| SSH実行 | SSHセッションで実行されたコマンドの標準出力を収集します。 |
| セントリーパフォーマンス | ログプレッソ・ソナーからセントリーのパフォーマンスログをバッチ収集します。 |
| ストリームクエリアウトプット | ログプレッソ・ソナーのストリームクエリから出力データを収集します。 |
| Syslog | リモートホストから送信されたSyslogメッセージを収集します。 |
| sFlow | sFlow v5パケットを収集します。 |
| TCPポートチェッカー | ローカル/リモートホストのTCPポート可用性を確認し、結果を収集します。 |
| WTMP | ローカルホスト上でWTMPログを収集します。 |
| WebKeeper（レガシーバージョン） | MSSQLを利用した旧バージョンのWebKeeperからデータを収集します。 |

**アプリロガーモデル**

ほとんどのロガーモデルはアプリのインストール時に提供されます。アプリロガーモデルは、対象システムから収集したデータからフィールドを抽出するために必要なすべての設定が事前に構成されています。

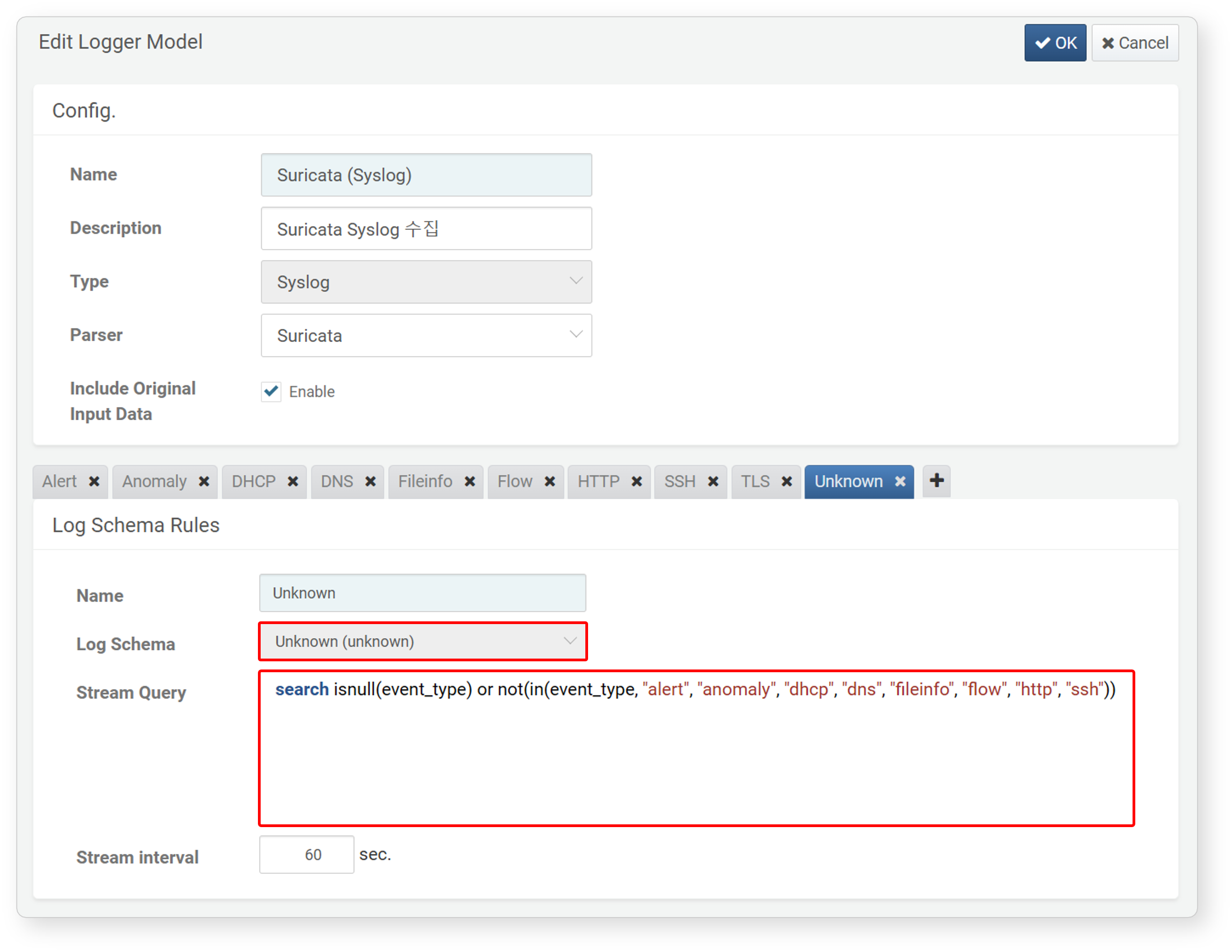
アプリロガーモデルを修正または削除しないでください。関連アプリの動作に支障をきたす恐れがあります。

ログスキーマルール（正規化ルール）

ロガーモデルは、ログスキーマに基づいてログを正規化するための正規化ルールを提供します。正規化ルールは、ログスキーマ、入力ログデータを変換するためのクエリ、およびリフレッシュ間隔で構成されます。

1つのストリームログデータに複数タイプのログレコードが含まれる場合、正規化ルールは**MECE**（Mutually Exclusive, Collectively Exhaustive：相互排他かつ網羅的）原則に従い、重複なく全てのレコードを分類できるよう設計する必要があります。例えば、ログソースにA、B、Cの3種類のレコードが含まれる場合、ロガーモデルにはそれぞれに対応する3つの正規化ルールを含める必要があります。Palo Alto Networksファイアウォールのログには、セッションログと侵入検知ログが含まれており、それぞれの構造に適したスキーマで正規化する必要があります。

ログフォーマットの変化やパースエラーに対応するため、他のいずれのルールにも一致しない、または正規化できないレコードを捕捉するための正規化ルールも用意することが重要です。

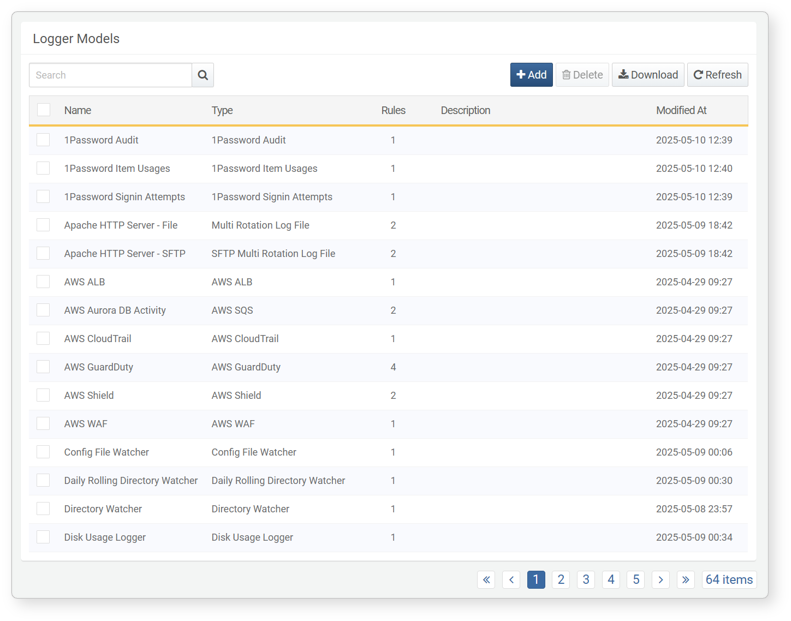


上図は[Suricata](https://logpresso.store/ja/apps/suricata)アプリのロガーモデル画面です。**Alert**、**Anomaly**、**DHCP**、**DNS**、**Fileinfo**、**Flow**、**HTTP**、**SSH**、**TLS**などのログスキーマルールに加え、**Unknown**ルールも定義されています。

**Unknown**ルールの**ストリームクエリ**は、入力データ内でevent\_typeフィールドに値がない、または正規化ルールで定義された値（alert、anomaly、dhcp、dns、fileinfo、flow、http、ssh、tls）に一致しないレコードを特定します。これらの一致しないレコードは**Unknown**として分類されます。

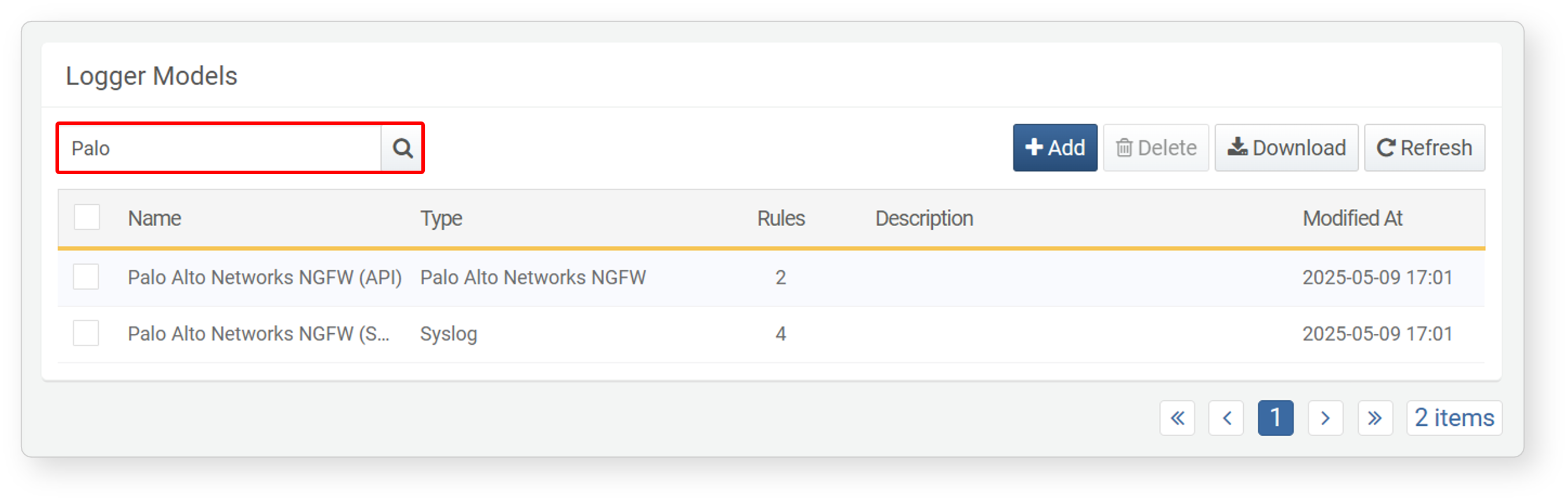
#### ロガーモデルの検索

**ロガー** > **ロガーモデル**でロガーモデルの一覧を確認できます。



* **名前**：ロガーモデルを識別するための名称
* **タイプ**：実行するロガーのタイプ
* **ルール数**：ロガーモデルに定義されたログスキーマルールの数
* **説明**：ロガーモデルに関する追加情報
* **最終更新日**：ロガーモデルの作成または最終更新日時

特定のロガーモデルを検索する場合は、ツールバーの検索ツールを利用します。検索ツールは、**名前**に入力したキーワードを含むロガーモデルを検索します。大文字・小文字は区別されません。

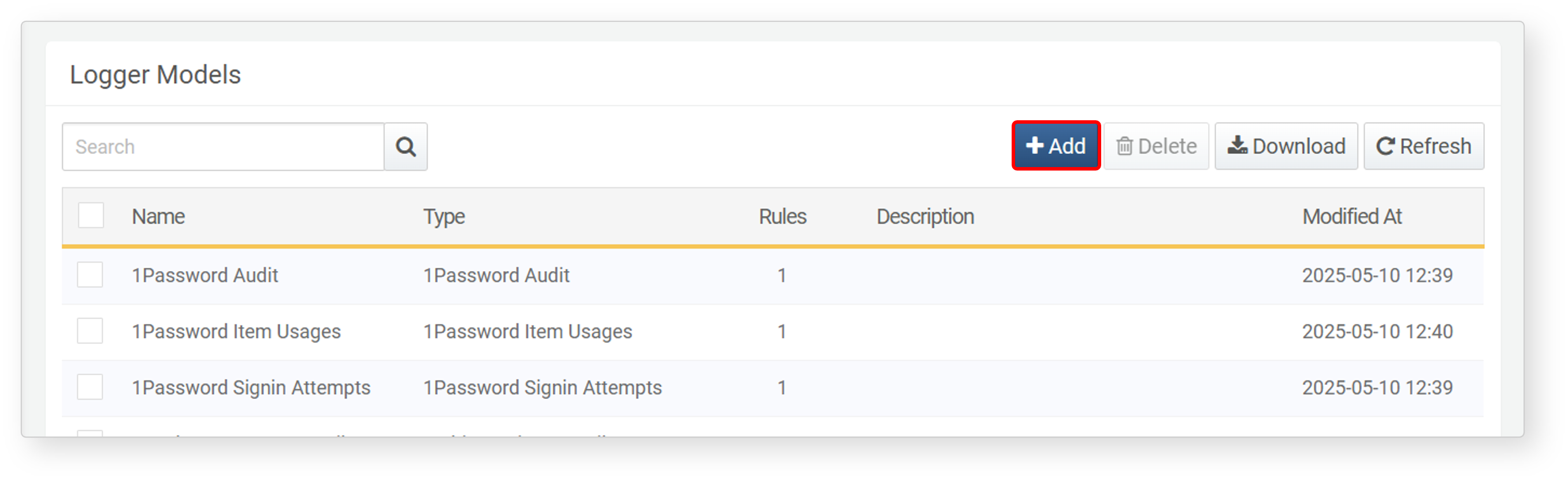


#### ロガーモデルの追加

多くの環境ではアプリロガーモデルで十分ですが、カスタムロガーモデルが必要な場合は新規作成が可能です。

ロガーモデルを追加するには：

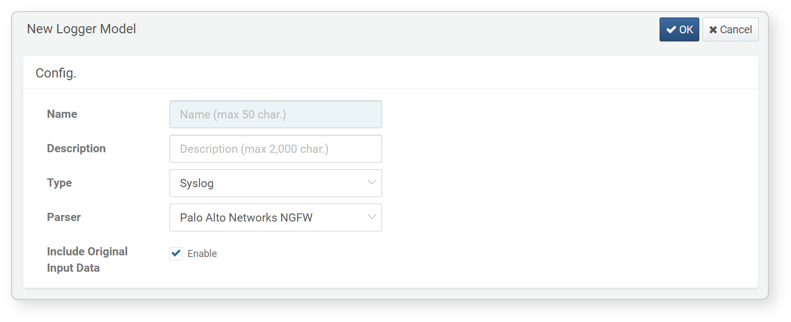
**ロガー** > **ロガーモデル**に移動し、ツールバーの**追加**をクリックします。



[設定](https://docs.logpresso.comnull)および[ログスキーマルール](https://docs.logpresso.comnull)の必要項目を入力または選択し、右上の**OK**をクリックします。

設定

ロガーモデルの**名前**、**説明**、**タイプ**、**パーサー**を入力または選択します。

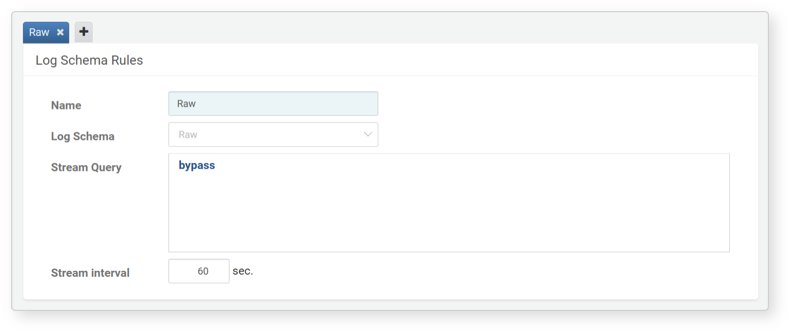


* **名前**：Webコンソール上でロガーモデルを識別するための名称
* **説明**：ロガーモデルの説明。詳細情報を記載できます。
* **タイプ**：実行するロガーのタイプ
* **パーサー**：ロガーからのデータを処理するパーサー名。入力データがすでに構造化されている場合（例：JDBCロガーの場合）は、パーサーを選択する必要はありません。

ログスキーマルール（正規化ルール）

1つ以上の正規化ルールを設定できます。各正規化ルールは、入力レコードが重複なく分類され、漏れがないように設計する必要があります（MECE原則）。

* ログスキーマルールを追加するには、\*\*+\*\*タブをクリックします。
* ログスキーマルールを削除するには、タブの**X**をクリックします。



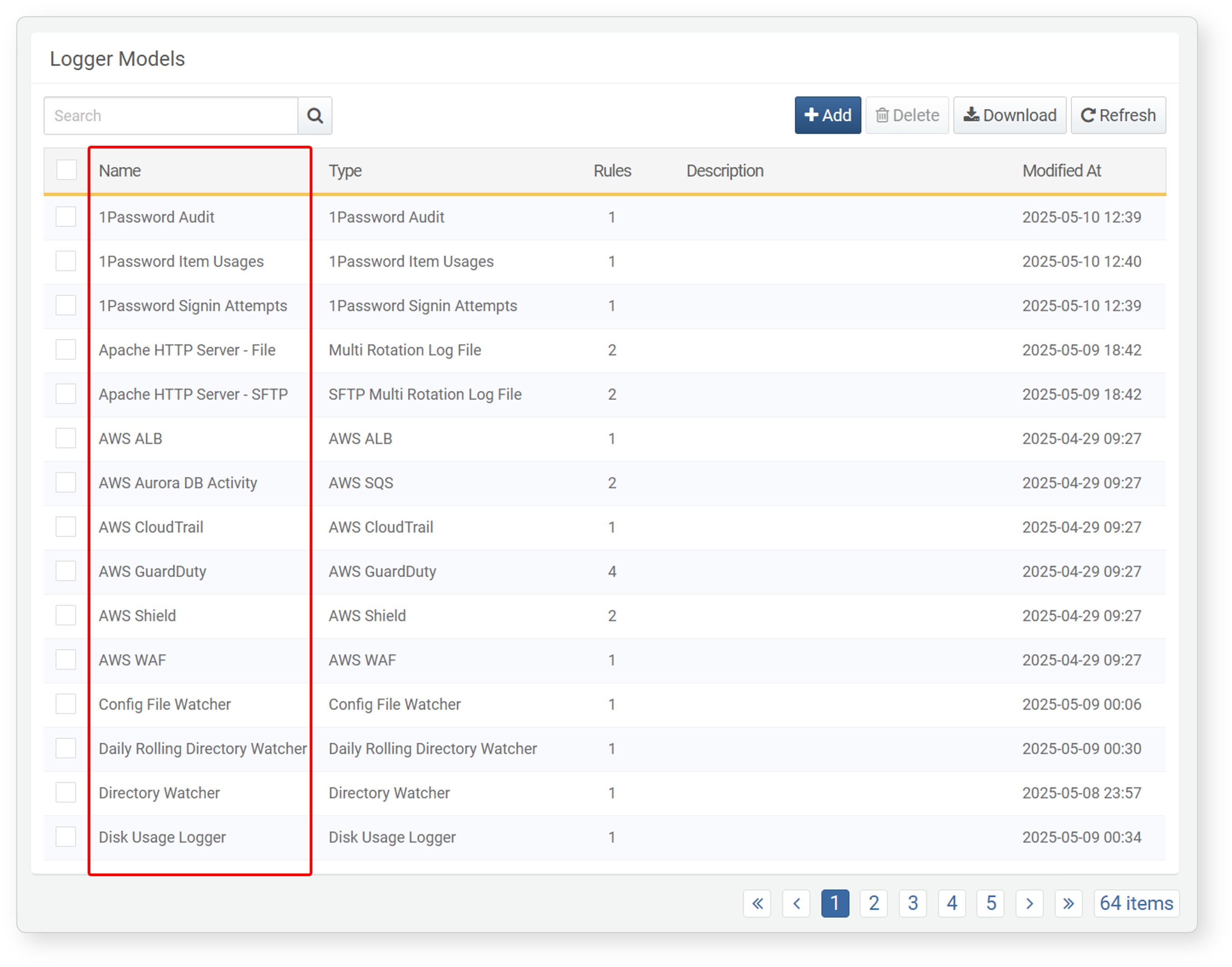
* **名前**：ログスキーマルールを識別する名称
* **ログスキーマ**：適用するログスキーマ
* **ストリームクエリ**：パース済みデータの一部または全体をログスキーマにマッピングするための前処理クエリ
* クエリ文は通常、[search](https://docs.logpresso.comnull)コマンドを利用して特定フィールド値で入力データをフィルタリングします。
* 入力フィールド名をログスキーマに合わせてリネームしたり、空フィールドに値を割り当てるクエリも記述できます。
* **ストリームインターバル**：ストリームクエリのリセット間隔（デフォルト：60秒、0に設定するとリアルタイムリセット）

#### ロガーモデルの編集

アプリロガーモデルのログスキーマルールは編集しないでください。アプリの動作に支障をきたす恐れがあります。

ロガーモデルを編集するには：

編集したいロガーモデルの**名前**をクリックします。



**ロガーモデル編集**ページで必要な情報を更新し、**OK**をクリックします。

* 編集可能な項目については**ロガーモデルの追加**を参照してください。
* **タイプ**は変更できません。タイプを変更する場合は、既存モデルを削除し新規作成してください。

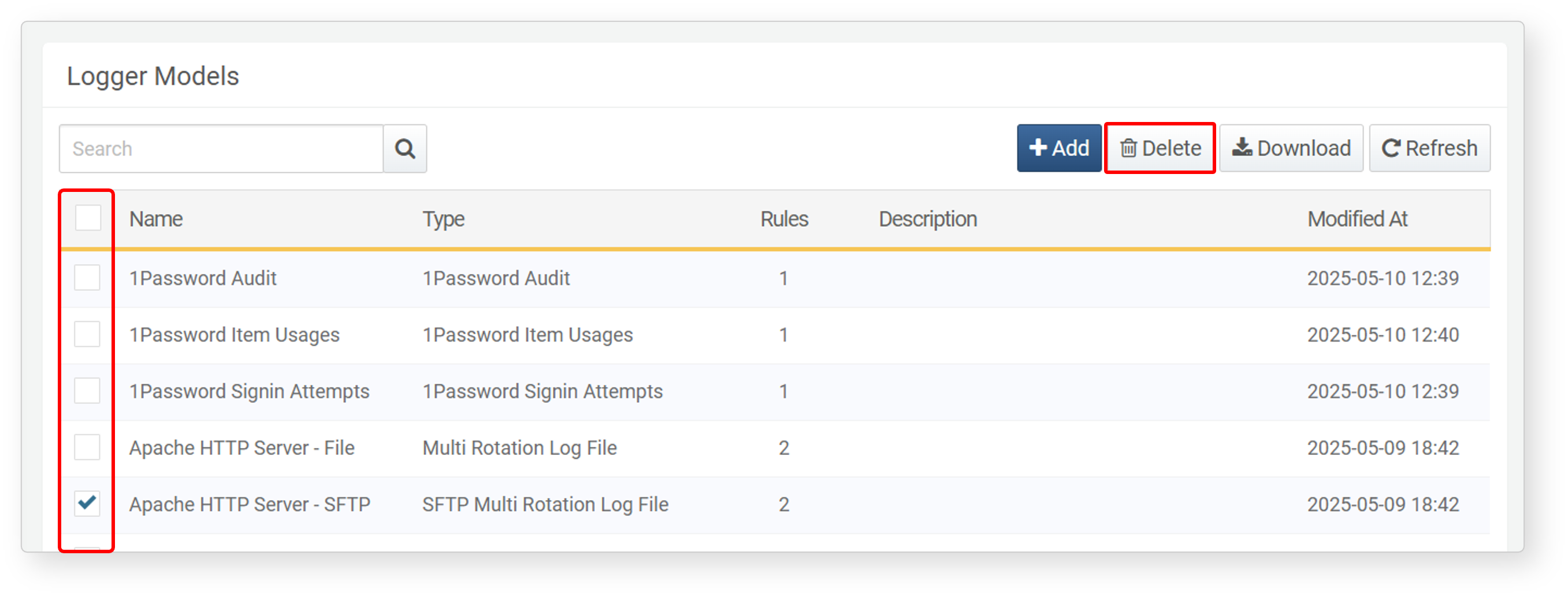
#### ロガーモデルの削除

ベースロガーモデルやアプリロガーモデルは削除しないでください。アプリの動作に支障をきたす恐れがあります。

ロガーモデルを削除するには：

削除したいロガーモデルの横にあるチェックボックスを選択します。

ツールバーの**削除**をクリックします。



**ロガーモデル削除**ダイアログで削除対象モデルの一覧を確認し、**削除**をクリックします。操作を中止する場合は**キャンセル**をクリックします。

削除に失敗した場合は、**ロガーモデル削除失敗**ダイアログに失敗理由が表示されます。