### 脅威インテリジェンスフィード

#### 概要

ログプレッソは、Logpresso CTIを通じてサイバー脅威インテリジェンス（CTI）サービスを提供し、組織が最新および既知の脅威に効果的に対応できるよう支援します。これらのサービスは、多様かつ最新の脅威情報を収集・分析・共有し、組織がサイバー脅威を迅速に特定・対応できるようにします。

Logpresso CTI

ログプレッソ・ソナーをインストールすると、Logpresso CTIフィードの一覧が提供されます。

|  |  |  |  |
| --- | --- | --- | --- |
| 名前 | STR\_FEED\* | 種別 | 説明 |
| Logpresso CTI IP | logpresso\_cti\_ip | IP | サイバー攻撃に関連する悪意のあるIPアドレス |
| Logpresso CTI Domain | logpresso\_cti\_domain | DOMAIN | マルウェア配布サイトやC&Cサーバーなどの悪意のあるドメイン |
| Logpresso CTI URL | logpresso\_cti\_url | URL | 悪意のあるURLに関するインジケーター（IoC） |
| Logpresso CTI MD5 | logpresso\_cti\_md5 | MD5 | MD5ハッシュベースのインジケーター |
| Logpresso CTI SHA1 | logpresso\_cti\_sha1 | SHA1 | SHA1ハッシュベースのインジケーター |
| Logpresso CTI SHA256 | logpresso\_cti\_sha256 | SHA256 | SHA256ハッシュベースのインジケーター |

\* **STR\_FEED**については、[matchfeed](https://docs.logpresso.comnull)コマンドのname=STR\_FEEDオプションを参照してください。

Logpresso CTIを利用するには、以下の手順が必要です。

サブスクリプションが必要です。有料契約者はリアルタイムフィードを、無料契約者は90日遅延したフィードを利用できます。

ログプレッソ・ソナーが[Logpresso CTIサービス](https://cti.logpresso.com)に接続できるよう、ネットワークセキュリティポリシーを設定してください。CTIサービスを提供するアプリも、それぞれのサービスプロバイダーへのネットワークアクセスが必要です。

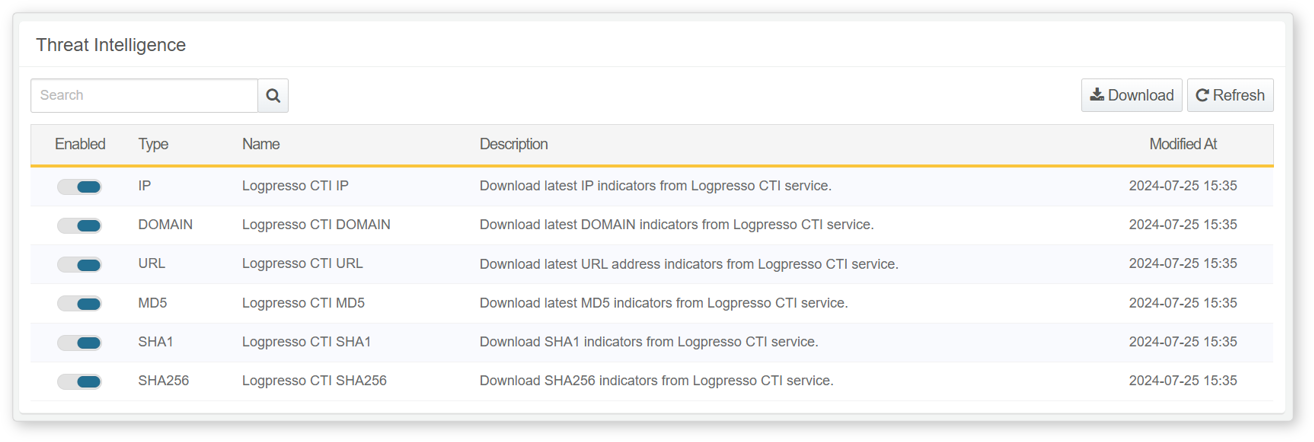
ログプレッソプラットフォーム内でLogpresso CTIサーバーの接続プロファイルを設定します。詳細は[接続プロファイル](https://docs.logpresso.comnull)を参照してください。

アプリによるCTI提供

ログプレッソストアの[S2W Quaxar](https://logpresso.store/ja/apps/quaxar)などのアプリも脅威インテリジェンスを提供します。アプリをインストール後、**脅威インテリジェンス**リストからそのCTIフィードにアクセスできます。サブスクリプションの要否については各CTIサービスプロバイダーにご確認ください。

#### 脅威インテリジェンスフィードの検索

**ポリシー > 脅威インテリジェンス**に移動すると、最新の脅威インテリジェンスフィードを閲覧・検索できます。



* **有効化**: 脅威インテリジェンスフィードの有効／無効を切り替えます（: オン、: オフ）
* **種別**: 提供される脅威インテリジェンスの種類
* **IP**: 攻撃元やC&Cサーバーの特定に用いられる悪意のあるIPアドレス
* **DOMAIN**: フィッシングサイトやマルウェア配布に関連する悪意のあるドメイン
* **MD5, SHA1, SHA256**: ファイルの整合性検証やマルウェア識別用のハッシュ値
* **URL**: マルウェア配布やフィッシングに利用される悪意のあるWeb URL
* **EMAIL**: 流出したメールアドレス
* **名前**: CTIフィードの名称
* **説明**: CTIフィードの説明
* **最終更新日**: 最終更新日時

ツールバーの検索機能を利用して、特定の脅威インテリジェンスフィードを検索できます。検索は**名前**フィールドに対して大文字・小文字を区別せずに一致します。

脅威インテリジェンスフィードリストのダウンロード

脅威インテリジェンスフィードの一覧をローカルPCにダウンロードするには、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。

脅威インテリジェンスフィードリストの更新

最新の脅威インテリジェンスデータを表示するには、ツールバーの**更新**をクリックしてください。

脅威インテリジェンスの活用

脅威インテリジェンスフィードは、以下の方法で活用できます。

シナリオビルダー

**ポリシー > ストリームルール**で検出ルールを追加・修正する際、**シナリオビルダー**を利用して脅威インテリジェンスを組み込むことができます。

以下は、入力フィールドタイプごとの脅威インテリジェンスフィード活用概要です。詳細は[フィールドタイプ別ルールとパラメータ](https://docs.logpresso.comnull)を参照してください。

**IP**

|  |  |  |  |
| --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 説明 |
| IPアドレスがレピュテーションDBに存在 | レピュテーションDB | CTIフィード選択 | 指定したレピュテーションDBに一致するフィールド値をフィルタ |
| IPアドレスがいずれかのレピュテーションDBに存在 | - | - | いずれかの脅威インテリジェンスフィードに存在する値をフィルタ |

**MD5/SHA1/SHA256**

|  |  |  |  |
| --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 説明 |
| 指定したハッシュ値に一致 | ハッシュ | 最大255文字 | 指定したハッシュ値に一致するフィールド値をフィルタ |
| いずれかのレピュテーションDBに存在 | - | - | いずれかの脅威インテリジェンスフィードに存在する値をフィルタ |
| 指定したレピュテーションDBに存在 | レピュテーションDB | CTIフィード選択 | 指定したレピュテーションDBに一致するフィールド値をフィルタ |

**URL**

|  |  |  |  |
| --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 説明 |
| いずれかのレピュテーションDBに存在 | - | - | いずれかのレピュテーションDBに存在する値をフィルタ |
| 指定したレピュテーションDBに存在 | レピュテーションDB | CTIフィード選択 | 指定したレピュテーションDBに一致するフィールド値をフィルタ |

**DOMAIN**

|  |  |  |  |
| --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 説明 |
| いずれかのレピュテーションDBに存在 | - | - | いずれかのレピュテーションDBに存在する値をフィルタ |
| 指定したレピュテーションDBに存在 | レピュテーションDB | CTIフィード選択 | 指定したレピュテーションDBに一致するフィールド値をフィルタ |

クエリ

**ポリシー > ストリームルール**または**ポリシー > バッチルール**で検出ルールを追加・修正する際、[matchfeed](https://docs.logpresso.comnull)コマンドや[matchfeed()](https://docs.logpresso.comnull)関数を利用して脅威インテリジェンスを組み込むことができます。脅威インテリジェンスフィードは、クエリ入力をサポートするあらゆる場所で活用可能です。