# セキュリティ インテリジェンス

セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。ここでは、セキュリティ インテリジェンスの実装方法について説明します。



## セキュリティ インテリジェンスについて

セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。システムは、この望ましくないトラフィックをアクセス制御ポリシーで評価する前にドロップすることにより、使用されるシステムリソースの量を減らします。

次のものに基づいてトラフィックをブロックできます。

- Cisco Talos Intelligence Group（Talos） フィード：Talos は、定期的に更新されるセキュリティ インテリジェンス フィードへのアクセスを提供します。セキュリティに対する脅威（マルウェア、スパム、ボットネット、スパム、フィッシングなど）を表すサイトが現れては消えるペースが早すぎて、カスタム設定を更新して導入するのが間に合わないことがあります。システムはフィードの更新を定期的にダウンロードするため、設定を再導入する必要なく新しい脅威インテリジェンスを利用できます。

（注） Talos フィードはデフォルトで1時間ごとに更新されます。**[デバイス（Device）] > [更新（Updates）]** ページからは、更新頻度を変更するだけでなく、オンデマンドでフィードを更新することもできます。

- ネットワークおよびURL オブジェクト：ブロック対象の IP アドレスまたは URL が既知の場合は、それらのオブジェクトを作成し、それらをブロックリストまたは例外リストに追加することができます。FQDN または範囲指定によりネットワーク オブジェクトを使用できないことに注意してください。

IP アドレス（ネットワーク）と URL で別のリストを作成します。

（注） HTTP/HTTPS リクエストの宛先が、ホスト名ではなく IP アドレスを使用する URL の場合は、ネットワークアドレスリストにある IP アドレスのレピュテーションが検索されます。ネットワークおよび URL リストで IP アドレスを重複させる必要はありません。

# ブロックリストの例外の作成

ブロックリストごとに、関連する例外リスト（ブロック禁止リストとも呼ばれる）を作成できます。例外リストの唯一の目的は、ブロックリストに表示される IP アドレスまたは URL を除外することです。つまり、使用する必要があり、安全であることがわかっているアドレスや URLが、ブロックリストに設定されているフィードにある場合、ブロックリストから完全にカテゴリを削除せずに、そのネットワーク/URL を除外できます。

除外されたトラフィックは、以後アクセス制御ポリシーによって評価されます。接続が許可またはドロップされたかどうかの最終決定は、接続に一致するアクセス制御ルールに基づきます。アクセスルールはまた、接続に侵入やマルウェア検査を適用するかどうかも判断します。

# セキュリティ インテリジェンス フィード カテゴリ

次の表では、Cisco Talos Intelligence Group（Talos） フィードで使用可能なカテゴリについて説明します。これらのカテゴリは、ネットワークブロッキングと URL ブロッキングの両方で使用できます。

これらのカテゴリは時間とともに変化する可能性があるため、新しくダウンロードしたフィードのカテゴリが変更される場合があります。セキュリティインテリジェンスを設定する際は、カテゴリ名の横にある情報アイコンをクリックして説明を表示できます。

**表 *1 : Cisco Talos Intelligence Group（Talos） フィードカテゴリ***

| セキュリティインテリジェンス カテゴリ | 説明 |
|---|---|
| 攻撃者 | 悪意のある発信アクティビティが知られているアクティブスキャナやホスト |
| Banking_fraud | 電子バンキングに関連する詐欺行為を行うサイト |
| Bogon | Bogon ネットワークおよび割り当てられていない IP アドレス |
| Bots | バイナリ マルウェア ドロッパをホストするサイト |

| セキュリティインテリジェンス カテゴリ | 説明 |
|---|---|
| CnC | botnets 用のホスト C & C サーバを有するサイト |
| 仮想通貨マイニング | プールと財布へのリモートアクセスを提供するホスト (cryptocurrency のマイニングのため) |
| Dga | C & C サーバのランデブー ポイントとして機能するさまざまなドメイン名を生成するために使用されるマルウェア アルゴリズム |
| Exploitkit | クライアントのソフトウェアの脆弱性を特定するために設計されたソフトウェア キット |
| High_risk | セキュリティグラフからの OpenDNS 予測セキュリティアルゴリズムと一致するドメインとホスト名 |
| Ioc | 侵害の兆候（IOC）に関与していることが観察されているホスト |
| Link_sharing | 権限のないファイルを共有する web サイト |
| 悪意のある（Malicious） | 他のより詳細な脅威カテゴリに必ずしも適合しているわけではない、悪意のある動作を示しているサイト |
| Malware | マルウェアバイナリまたはエクスプロイト キットを有するサイト |
| Newly_seen | 最近登録されたドメイン、またはテレメトリでまだ認識されていないドメイン<br>**注目**<br>現在、このカテゴリにはアクティブなフィードがなく、将来の使用のために予約されています。 |
| Open_proxy | 匿名 Web ブラウジングを許可するオープン プロキシ |
| Open_relay | スパム用に使用されることが既知のオープン メール リレー |
| Phishing | フィッシング ページを有するサイト |
| 応答 | 悪意があるか疑わしいアクティブに積極的に参加している IP アドレスと URL |
| Spam | スパムを送信することが知られているメール ホスト |
| スパイウェア | スパイウェアおよびアドウェアのアクティビティを含む、提供する、またはサポートすることが知られているサイト |
| Suspicious | 疑いがあり、既知のマルウェアと同様の特性を持つようなファイル |
| Tor_exit_node | Tor アノニマイザー ネットワークの出口ノード サービスを提供することが知られているホスト |

# セキュリティ インテリジェンスのためのライセンス要件

セキュリティ インテリジェンスを使用するには、**IPS** ライセンスを有効にする必要があります。「オプション ライセンスのイネーブル化とディセーブル化」を参照してください。

# セキュリティ インテリジェンスの設定

セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。許可された接続もすべてアクセス コントロール ポリシーによって引き続き評価され、最終的にドロップされる可能性があります。セキュリティ インテリジェンスを使用するには、IPS ライセンスを有効にする必要があります。

## 手順

**ステップ 1** **[ポリシー（Policies）]** > **[セキュリティインテリジェンス（Security Intelligence）]** の順に選択します。

**ステップ 2** ポリシーが有効になっていない場合は、[セキュリティインテリジェンスの有効化（Enable Security Intelligence）] ボタンをクリックします。

[セキュリティインテリジェンス（Security Intelligence）] をクリックして [オフ（Off）] にすることで、いつでもポリシーを無効にできます。設定は維持されるため、ポリシーを再度有効にするときに再設定する必要はありません。

**ステップ 3** セキュリティ インテリジェンスを設定します。

ネットワーク（IP アドレス）と URL には別々のブロックリストがあります。

a) [ネットワーク（Network）] または [URL] タブをクリックして、設定するリストを表示します。

b) ブロック/ドロップリストで、[+] をクリックして、接続をすぐにドロップするオブジェクトまたはフィードを選択します。

オブジェクトセレクタは、種類によってオブジェクトおよびフィードを別々のタブに整理します。希望するオブジェクトがまだ存在しない場合、リストの下部にある [新しいオブジェクトの作成（Create New Object）] リンクをクリックして作成します。Cisco Talos Intelligence Group（Talos） フィードの説明については、フィードの横にある [i] ボタンをクリックします。セキュリティ インテリジェンス フィード カテゴリ （2 ページ） も参照してください。

（注）
セキュリティ インテリジェンスでは、ネットマスク /0 を使用する IP アドレスのブロックを無視します。これには、any-ipv4 と any-ipv6 のネットワーク オブジェクトが含まれます。ネットワークのブロックのためにこれらのオブジェクトを選択しないでください。

c) 非ブロックリストで、[+] をクリックし、ブロックリストの例外をすべて選択します。

このリストを設定する唯一の理由は、ブロックリストにある IP アドレスまたは URL を例外にすることです。適用除外された接続は、その後アクセス制御ポリシーによって評価され、いずれにしても破棄される可能性があります。

d) 他のブロックリストを設定するには上記の手順を繰り返します。

**ステップ 4** （オプション）[ログ設定の編集（Edit Logging Settings）] ボタン（⚙）をクリックしてログを設定します。

ロギングを有効にした場合は、ブロックリストのエントリに一致するものが記録されます。ロギングを有効にして、除外された接続がアクセス制御ルールに一致した場合、ログ メッセージは取得しますが例外エントリに一致するものは記録されません。

次の設定を行います。

- [接続イベント ロギング（Connection Events Logging）]：クリックしてロギングを有効または無効に切り替えます。
- [syslog]：外部の syslog サーバにイベントのコピーを送信するには、このオプションを選択して、syslog サーバを定義するサーバ オブジェクトを選択します。必要なオブジェクトが存在しない場合は、[新しい Syslog サーバの追加（Add Syslog Server）] をクリックして作成します。

  デバイスのイベント ストレージは限られているため、外部の syslog サーバにイベントを送信することにより、長期間ストレージが利用できるようになり、イベントの分析を向上できます。

# セキュリティ インテリジェンスのモニタリング

セキュリティ インテリジェンス ポリシーのログ記録を有効にすると、システムは、ブロックリストの項目に一致する接続ごとにセキュリティ インテリジェンス イベントを生成します。これらの接続に一致する接続イベントがあります。

ドロップされた接続の統計情報は、[モニタリング（Monitoring）] ページの、使用可能なさまざまなダッシュボードに表示されます。

**[モニタリング（Monitoring）] > [アクセスおよびSIルール（Access and SI Rules）]** ダッシュボードに、トラフィックと一致する、上位のアクセス ルールとセキュリティ インテリジェンスに相当するルールが表示されます。

さらに、**[モニタリング（Monitoring）] > [イベント（Events）]**、次に [セキュリティインテリジェンス（Security Intelligence）] を選択して、セキュリティ インテリジェンス イベントと、関連する接続イベントを [接続（Connection）] タブに表示することができます。

- イベントの [SIカテゴリID（SI Category ID）] フィールドは、ネットワークまたは URL オブジェクトあるいはフィードなど、ブロックリストに一致するオブジェクトを示します。

- 接続イベントの[理由（Reason）]フィールドは、イベントに表示されたアクションが適用された理由について説明します。たとえば、ブロックアクションは、IP ブロックまたは URL ブロックなどの理由と組み合わされて、接続がセキュリティインテリジェンスによってドロップされたことを示します。

# セキュリティ インテリジェンスの例

使用例の章には、セキュリティ インテリジェンス ポリシーの実装例が含まれています。脅威のブロック方法を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。