



## セキュリティ インテリジェンス

以下のトピックでは、セキュリティインテリジェンスの概要（トラフィックのブロックリストと許可リストの使用、基本設定など）を示します。

- セキュリティインテリジェンスについて (1 ページ)
- セキュリティインテリジェンスのベストプラクティス (2 ページ)
- 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 (3 ページ)
- セキュリティインテリジェンスの要件と前提条件 (3 ページ)
- セキュリティインテリジェンス送信元 (4 ページ)
- セキュリティインテリジェンスの設定 (5 ページ)
- セキュリティインテリジェンス モニタリング (13 ページ)
- セキュリティインテリジェンス ブロッキングのオーバーライド (14 ページ)
- セキュリティインテリジェンスのトラブルシューティング (15 ページ)
- セキュリティインテリジェンス ブロックリストへの登録の履歴 (16 ページ)

### セキュリティ インテリジェンスについて

悪意のあるインターネットコンテンツに対する防御の前線として、セキュリティインテリジェンスは疑わしいIPアドレス、URL、ドメイン名が関連する接続をレピュテーションインテリジェンスを使用して迅速にブロックします。これは、セキュリティインテリジェンス ブロックリストと呼ばれます。

セキュリティインテリジェンスはアクセス制御の初期のフェーズであり、大量のリソースを消費する評価をシステムが実行する前に行われます。ブロックリストにより、インスペクションの必要がないトラフィックを迅速に除外できるため、パフォーマンスが向上します。



(注) ブロックリストを使用して、高速パストラフィックをブロックすることはできません。プレフィルタ評価の実行は、セキュリティインテリジェンスによるフィルタリングの前に行われます。FastPathが適用されたトラフィックは、セキュリティインテリジェンスを含め、以降のすべての評価をバイパスします。

## セキュリティ インテリジェンスのベストプラクティス

カスタムのブロックリストを設定できますが、シスコでは定期的に更新されるインテリジェンスフィードへのアクセスを提供しています。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。

ロックしないリストとモニター専用ブロックリストを使用して、セキュリティ インテリジェンス ブロックリスト機能の精度を上げることができます。これらのメカニズムは、ブロックリストによりトラフィックがロックされないようにしますが、一致するトラフィックを自動的に信頼したり FastPath を適用したりすることはしません。ロックしないリストに追加されたトラフィックや、セキュリティ インテリジェンス の段階でモニターされるトラフィックは、意図的に残りのアクセスコントロールによる分析が適用されます。



(注) 検出シグニチャまたはマルウェア URL を含むセキュリティ インテリジェンス 設定により、Firewall Threat Defense トラブルシューティングファイルがスキャンされたときに、誤った脅威アラートが発生する可能性があります。

### 関連トピック

[セキュリティ インテリジェンス](#)

## セキュリティ インテリジェンスのベストプラクティス

- システムが提供するセキュリティ インテリジェンス フィードによって検出されたすべての脅威をブロックするようにアクセス コントロール ポリシーを設定します。設定例：セキュリティ インテリジェンス ブロック（12 ページ）を参照してください。
- シスコが提供するセキュリティ インテリジェンス フィードをカスタム脅威データで補足する場合、または新しい脅威を手動でブロックする場合は、次のようにします。
  - IP アドレスの場合は、カスタムのセキュリティ インテリジェンス のリストおよびフィードか、ネットワークオブジェクトまたはグループを使用します。これらを作成するには、セキュリティ インテリジェンス および ネットワーク とそのサブトピックを参照してください。これらをセキュリティ インテリジェンス に使用するには、セキュリティ インテリジェンス の設定（5 ページ）を参照してください。セキュリティ インテリジェンス ポリシーで使用されるネットワークオブジェクトには、IPS ライセンスが必要です。
  - IP とドメインの場合は、カスタムのセキュリティ インテリジェンス のリストおよびフィードを使用し、オブジェクトまたはグループは使用しません。詳細については、手動 URL フィルタリング オプションを参照してください。
  - イベントからブロックリストにエントリを追加することもできます。グローバルおよび ドメイン のセキュリティ インテリジェンス リストを参照してください。

- 新しいフィードをテストする場合、またはパッシブ展開の場合は、アクションをブロックからモニターのみに設定します。セキュリティインテリジェンスマニタリング（13ページ）を参照してください。
- 特定のサイトまたはアドレスをセキュリティインテリジェンスのブロッキングから除外する必要がある場合は、セキュリティインテリジェンスブロッキングのオーバーライド（14ページ）を参照してください。
- Firepower 展開が Cisco XDR と統合されていて、カスタムのセキュリティインテリジェンスのリストおよびフィードを使用している場合は、そのリストとフィードで Security Services Exchange を必ず更新します。詳細については、Security Services Exchange のオンラインヘルプでイベントの自動プロモーションを設定するための手順を参照してください。この統合に関する一般的な情報については、Cisco Secure Firewall Management Center アドミニストレーションガイドの「SecureX 統合の有効化」を参照してください。
- システムで提供されるセキュリティインテリジェンスのカテゴリは、時間の経過とともに通知なしに変更される場合があります。定期的に変更を確認し、それに応じてポリシーを変更することを計画する必要があります。
- また、悪意のあるサイトからの保護を強化するために、URL フィルタリング（個別のライセンス要件がある個別の機能）を設定する必要があります。「URL フィルタリング」を参照してください。

## 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

### Threat Defense ライセンス

IPS

### 従来のライセンス

保護

## セキュリティインテリジェンスの要件と前提条件

### モデルのサポート

任意

### サポートされるドメイン

任意

### ユーザの役割

- 管理者

- ・アクセス管理者
- ・ネットワーク管理者

**重要**

SIポリシーを正常に適用するには、デバイスにネットワーク検出ポリシーを適用する必要があります。

## セキュリティ インテリジェンス送信元

- ・システムが提供するフィード

シスコは、ドメイン、URL、およびIPアドレスについて定期的に更新されるインテリジェンスフィードへのアクセスを提供します。詳細については、[セキュリティ インテリジェンス](#)を参照してください。

名前に「TID」が含まれるフィードがある場合、このフィードはセキュリティ インテリジェンスによって使用されません。代わりに、このフィードは、[Secure Firewall Threat Intelligence Director](#)で説明されている機能によって使用されます。

- ・サードパーティフィード

オプションで、Cisco 提供のフィードをサードパーティのフィードで補完できます。これらのフィードは、Secure Firewall Management Center が定期的にインターネットからダウンロードする動的リストです。[カスタム セキュリティ インテリジェンス フィード](#)を参照してください。

- ・カスタムブロックリストまたはフィード（またはオブジェクトまたはグループ）

手動で作成したリストまたはフィードを使用して、特定の IP アドレス、URL、またはドメイン名をブロックします（IPアドレスの場合、ネットワークオブジェクトまたはグループを使用することもできます）。

たとえば、フィードによってまだブロックされていない悪意のあるサイトまたはアドレスに気付いた場合は、これらのサイトをカスタム セキュリティ インテリジェンス リストに追加し、このカスタムリストをアクセスコントロールポリシーの[セキュリティ インテリジェンス (Security Intelligence) ]タブでブロックリストに追加します。[カスタム セキュリティ インテリジェンス リスト](#)および[セキュリティ インテリジェンス の設定 \(5 ページ\)](#)を参照してください。

IPアドレスの場合、リストやフィードではなく、オプションでネットワークオブジェクトをこの目的に使用できます。詳細については、[ネットワーク](#)を参照してください（URLの場合、他の方法よりもリストとフィードを使用することを強くお勧めします）。

- ・カスタムのブロックしないリストまたはフィード

特定のサイトまたはアドレスのセキュリティインテリジェンスブロックを無効にします。  
[セキュリティインテリジェンスプロッキングのオーバーライド（14ページ）](#) を参照してください。

- グローバルブロックリスト（ネットワーク、URL、DNS ごとに 1 つ）

イベントの確認中に、セキュリティインテリジェンスがそのソースからの今後のトラフィックを処理する場合は、イベントの IP アドレス、URL、またはドメインを該当するグローバルブロックリストにすぐに追加できます。[グローバルおよびドメインのセキュリティインテリジェンスリスト](#) を参照してください。

- グローバルブロックしないリスト（ネットワーク、URL、DNS ごとに 1 つ）

イベントの確認中に、セキュリティインテリジェンスがそのソースからの今後のトラフィックをブロックしたくない場合は、イベントの IP アドレス、URL、またはドメインを該当するグローバルブロックしないリストにすぐに追加できます。[「グローバルおよびドメインのセキュリティインテリジェンスリスト」](#) 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

各アクセスコントロールポリシーには、セキュリティインテリジェンスオプションがあります。ネットワークオブジェクト、URL オブジェクトとリスト、およびセキュリティインテリジェンスフィードとリストをブロックリストまたはブロックしないリストに追加でき、これらはすべてセキュリティゾーンによって制約できます。アクセスコントロールポリシーに DNS ポリシーを関連付け、ドメイン名をブロックリストまたはブロックしないリストに追加することもできます。

ブロックしないリストに含まれるオブジェクトの数とブロックリストに含まれるオブジェクトの数の合計が、125 個のネットワークオブジェクトまたは 32767 個の URL オブジェクトとリストを超えることはできません。

### 始める前に

- ヒント：推奨される最小構成については、[設定例：セキュリティインテリジェンスプロック（12ページ）](#) も参照してください。
- すべてのオプションを選択できるようにするには、少なくとも 1 つの管理対象デバイスを Management Center に追加します。
- パッシブ展開の場合、またはモニター専用にセキュリティインテリジェンス フィルタリングを設定する場合は、ロギングを有効にします。『Cisco Secure Firewall Management Center アドミニストレーションガイド』の「Logging Connections with Security Intelligence」を参照してください。
- ドメインのセキュリティインテリジェンスアクションを実行する DNS ポリシーを設定します。詳細については、「[DNS ポリシー](#)」を参照してください。

## 手順

---

**ステップ1** アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス (Security Intelligence) ] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

**ステップ2** 次の選択肢があります。

- [ネットワーク (Networks) ] をクリックして、ネットワークオブジェクト (IP アドレス) を追加します。

(注)

セキュリティ インテリジェンス ポリシーで使用されるネットワークオブジェクトには、IPS ライセンスが必要です。

- [URL (URLs) ] をクリックして、URL オブジェクトを追加します。

**ステップ3** ブロックしないリストまたはブロックリストに追加する [Available Objects] を検索します。次の選択肢があります。

- [名前または値で検索 (Search by name or value) ] フィールドに入力して、利用可能なオブジェクトを検索します。リロード (C) または [クリア (Clear) ] (X) をクリックして、検索文字列をクリアします。

- 既存のリストまたはフィードがニーズを満たしていない場合は、[追加 (Add) ] (+) をクリックし、[新規ネットワークリスト (New Network List) ] または [新規 URL リスト (New URL List) ] を選択し、[セキュリティ インテリジェンス フィードの作成または新しいセキュリティ インテリジェンス リストの Secure Firewall Management Center へのアップロード](#) の説明に従って続行します。

- 既存のオブジェクトがニーズを満たしていない場合は、[追加 (Add) ] (+) をクリックし、[新規ネットワークオブジェクト (New Network Object) ] または [新規 URL オブジェクト (New URL Object) ] を選択し、[ネットワーク オブジェクトの作成](#) の説明に従って続行します。

セキュリティ インテリジェンスは、/0 ネットマスクを使用して、IP アドレス ブロックを無視します。

**ステップ4** 追加する 1 つ以上の利用可能なオブジェクトを選択します。

**ステップ5** (オプション) [利用可能なゾーン (Available Zone) ] を選択して、選択したオブジェクトをゾーンごとに制約します。

システムが提供するセキュリティ インテリジェンス リストをゾーンで制約することはできません。

## (注)

SIリストの[すべて (Any) ]ゾーンは、セキュリティゾーンの一部であるインターフェイスにのみ適用されます。ただし、例外として、セキュリティゾーンに関連付けられたインターフェイスがデバイスがない場合、[すべて (Any) ]ゾーンはどのインターフェイスにも一致します。

たとえば、デバイスに5つのインターフェイスがあり、それらのどれもセキュリティゾーンに関連付けられていない場合、[すべて (Any) ]ゾーンに割り当てられたSIリストは、デバイスのすべてのインターフェイスのトラフィックに対して検査されます。そのデバイスのセキュリティゾーンに1つのインターフェイスを追加すると、ゾーンがSIリストに対して[すべて (Any) ]に設定されている他の4つのインターフェイスのSI検査が効果的に削除されます。他の4つのインターフェイスをセキュリティゾーンに追加すると、それらは[すべて (Any) ]ゾーンにアタッチされているSIリストによって評価されます。

**ステップ6** [Add to Do Not Block list] または [Add to Block list] をクリックするか、選択したオブジェクトをクリックしていずれかのリストにドラッグします。

ロックしないリストまたはロックリストからオブジェクトを削除するには、[削除 (Delete) ] (trash bin icon) をクリックします。複数のオブジェクトを削除するには、オブジェクトを選択し、右クリックして [Delete Selected] を選択します。

**ステップ7** (オプション) ブロックリストのオブジェクトをモニター専用に設定するには、[ブロックリスト (BlockList) ]にリストされている該当するオブジェクトを右クリックし、[モニター専用 (ロックしない) (Monitor-only (do not block)) ]を選択します。

システムが提供するグローバルセキュリティインテリジェンスリストをモニター専用に設定することはできません。

**ステップ8** [DNS ポリシー (DNS Policy) ] ドロップダウンリストから DNS ポリシーを選択します。

**ステップ9** [保存 (Save) ] をクリックします。

---

### 次のタスク

- 設定変更を展開します[設定変更の展開](#)を参照してください。

#### 関連トピック

[セキュリティインテリジェンス](#)

[Snort 再起動のシナリオ](#)

## セキュリティインテリジェンス オプション

アクセス制御ポリシーエディタの[セキュリティインテリジェンス (Security Intelligence) ]タブを使用して、ネットワーク (IP アドレス) と URL セキュリティインテリジェンスを構成し、ドメインにセキュリティインテリジェンスを設定した DNS ポリシーにアクセス制御ポリシーを関連付けます。

## 使用可能なオブジェクト

使用可能なオブジェクトは次のとおりです。

- システム提供のフィードによって入力されたセキュリティ インテリジェンス のカテゴリ。  
詳細については、[セキュリティ インテリジェンス カテゴリ（9 ページ）](#) を参照してください。
- システム提供のグローバルのロックリストとロックしないリスト。  
説明については、[セキュリティ インテリジェンス 送信元（4 ページ）](#) を参照してください。
- [オブジェクト（Object）]>[オブジェクト管理（Object Management）]>[セキュリティ インテリジェンス（Security Intelligence）]で作成するセキュリティ インテリジェンス のリストとフィード。  
説明については、[セキュリティ インテリジェンス 送信元（4 ページ）](#) を参照してください。
- [オブジェクト（Object）]>[オブジェクト管理（Object Management）]の各ページで設定されている、ネットワークと URL のオブジェクトとグループ。これらは、前の箇条書きのセキュリティ インテリジェンス オブジェクトとは異なります。  
ネットワークオブジェクトの詳細については、[ネットワーク](#) を参照してください。（URL には、オブジェクトやグループではなく、セキュリティ インテリジェンス のリストまたはフィードを使用します。）

## 使用可能なゾーン

システムが提供するグローバルリストを除いて、ゾーンごとにセキュリティ インテリジェンス フィルタリングを制約できます。

例：パフォーマンスを向上させるために、ターゲットの適用が必要になる場合があります。より具体的な例として、電子メールトラフィックを処理するセキュリティ ゾーンでのみ、スパムをブロックできます。

複数のゾーンでオブジェクトのセキュリティ インテリジェンス フィルタリングを適用するには、ゾーンのそれぞれについて、オブジェクトをロックリストまたはロックしないリストに追加する必要があります。

## DNS ポリシー

セキュリティ インテリジェンス を使用して DNS トラフィックを照合するには、セキュリティ インテリジェンス 設定の DNS ポリシーを選択する必要があります。

ロックリストまたはロックしないリストの使用、または DNS リストまたはフィードに基づくトラフィックのモニタリングには、以下の条件もあります。

- DNS セキュリティ インテリジェンス のリストとフィードを設定します。[セキュリティ インテリジェンス](#) を参照してください。

- DNS ポリシーを作成します。詳細については、[基本的な DNS ポリシーの作成](#)を参照してください。
- DNS リストまたはフィードを参照する DNS ルールを設定します。詳細については、[DNS ルールの作成と編集](#)を参照してください。
- DNS ポリシーはアクセス コントロール ポリシーの一部として展開するため、両方のポリシーを関連付ける必要があります。詳細については、[DNS ポリシーの導入](#)を参照してください。

### ブロックしないリスト

[セキュリティインテリジェンス ブロッキングのオーバーライド](#) (14 ページ) を参照してください。

リスト内のすべてのオブジェクトを選択するには、オブジェクトを右クリックします。

### ブロックリスト

[設定例：セキュリティインテリジェンス ブロック](#) (12 ページ) およびこの章の他のトピックを参照してください。

ブロックリストのビジュアルインジケータの説明については、[ブロックリストのアイコン](#) (11 ページ) を参照してください。

リスト内のすべてのオブジェクトを選択するには、オブジェクトを右クリックします。

### ログ

デフォルトで有効になっているセキュリティインテリジェンス ロギングは、アクセス制御ポリシー対象のデバイスが処理するブロックされ、監視対象である接続はすべてロギングされます。ただし、システムはブロックしないリストの一一致はロギングしません。ブロックしないリストの接続のロギングは、その接続の最終的な傾向によって異なります。ブロックリストの接続については、ブロックリストのオブジェクトをモニターのみに設定する前にロギングを有効にする必要があります。

ロギング設定を有効化、無効化、または表示するには、ブロックリストでオブジェクトを右クリックします。

### 関連トピック

[グローバルおよびドメインのセキュリティインテリジェンス リスト](#)

[セキュリティインテリジェンス リストとマルチテナンシー](#)

## セキュリティインテリジェンス カテゴリ

セキュリティインテリジェンスのカテゴリは、[セキュリティインテリジェンス](#)で説明されているシステム提供のフィードによって決定されます。

これらのカテゴリは、次の場所で使用されます。

- ・アクセス コントロール ポリシーの [Security Intelligence] タブの [Networks] サブタブ
- ・アクセス コントロール ポリシーの [Security Intelligence] タブの [Networks] タブの横にある [URLs] サブタブ
- ・[DNS rule configuration] ページの [DNS] タブの DNS ポリシー
- ・トラフィックが上記の場所のブロック設定またはモニター設定と一致する場合に生成されるイベント



(注) 組織で Secure Firewall Threat Intelligence Directorを使用している場合：イベントを表示すると、アクションが TID によって実行されたことを示すカテゴリ（TID URL ブロックなど）が表示されることがあります。

カテゴリはクラウドから Talos によって更新されます。このリストは、Firepower リリースとは無関係に変更される場合があります。

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  |
| 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   |

| セキュリティインテリジェンス カテゴリ  | 説明   |
|----------------------|--|
| 悪意のある<br>(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><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   |

## ブロックリストのアイコン

アクセスコントロールポリシーの[セキュリティインテリジェンス (Security Intelligence) ]タブの[ブロックリスト (Block list) ]に、次のビジュアルインジケータが表示される場合があります。

| アイコンまたはビジュアルインジケータ | 説明  |
|--------------------|---|
| Block (■)          | オブジェクトはブロックするように設定されています。   |
| モニター (⌚)           | オブジェクトは監視専用に設定されています。<br><a href="#">セキュリティインテリジェンス モニタリング (13 ページ)</a> を参照してください |

## ■ 設定例：セキュリティインテリジェンスブロック

| アイコンまたはビジュアルインジケータ        | 説明   |
|---------------------------|--|
| オブジェクトが取り消し線付きのテキストで表示される | 同じオブジェクトがブロックをオーバーライドする [ブロックしない (Do Not Block) ] リストにもあります。 |

## 設定例：セキュリティインテリジェンスブロック

システムにより定期的に更新されるセキュリティ インテリジェンス フィードによって検出可能なすべての脅威をブロックするようにアクセス コントロール ポリシーを設定します。

ブロックしないリストに含まれるオブジェクトの数とブロックリストに含まれるオブジェクトの数の合計が、125 個のネットワーク オブジェクトまたは 32767 個の URL オブジェクトとリストを超えることはできません。

### 始める前に

- すべてのオプションを選択できるようにするには、少なくとも 1 つの管理対象デバイスを Management Center に追加します。
- ドメインのセキュリティ インテリジェンス の脅威カテゴリをすべてブロックするように DNS ポリシーを設定します。詳細については、[DNS ポリシー](#) を参照してください。
- ブロックするエンティティのカスタムリストがある場合、または設定する予定がある場合は、各タイプ (URL、DNS、ネットワーク) のセキュリティ インテリジェンス オブジェクトを作成します。「[セキュリティ インテリジェンス](#)」を参照してください。

### 手順

**ステップ1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)] をクリックします。

**ステップ2** 新しいアクセス コントロール ポリシーを作成するか、既存のポリシーを編集します。

**ステップ3** アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス (Security Intelligence)] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

**ステップ4** [Networks] をクリックして、IP アドレスのブロック条件を追加します。

- [Networks] リストを下にスクロールし、[Global] リストの下にリストされているすべての脅威カテゴリを選択します。
- これらの脅威をブロックするセキュリティゾーンを選択します（該当する場合）。
- [Add to Block List] をクリックします。

- d) ブロックするアドレスを含むカスタムリストまたはフィードを作成している場合は、上記と同じ手順を使用してブロックリストに追加します。

**ステップ5** [URL]をクリックしてURLのブロック条件を追加し、[Networks]で実行した手順を繰り返します。

**ステップ6** [DNSポリシー (DNS Policy)]ドロップダウンリストからDNSポリシーを選択します。DNSポリシーの概要を参照してください。

**ステップ7** [保存 (Save)]をクリックします。

#### 次のタスク

- これらの接続のロギングを有効にします。『Cisco Secure Firewall Management Centerアドミニストレーションガイド』の「Logging Connections with Security Intelligence」を参照してください。
- 設定変更を展開します設定変更の展開を参照してください。
- 保護を強化するには、悪意のあるURLをブロックするようにURLフィルタリングを設定します。「URLフィルタリング」を参照してください。

## セキュリティインテリジェンスマニタリング

モニタリングでは、セキュリティインテリジェンスによってブロックされるはずのトラフィックの接続イベントをログに記録しますが、トラフィックをブロックすることはありません。モニタリングは、特に次の場合に役立ちます。

- 実装する前のフィードテスト。

たとえば、サードパーティのフィードを使用したブロッキングを実装する前に、そのフィードをテストする必要があるとします。フィードをモニター専用に設定すると、ブロックされるはずの接続をシステムで詳細に分析できるだけでなく、そのような接続のそれぞれをログに記録して、評価することもできます。

- パフォーマンスを最適化するためのパッシブ展開。

パッシブに展開された管理対象デバイスはトラフィックフローに影響を与えることができないため、トラフィックをブロックするようにシステムを構成しても何のメリットもありません。また、ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。



(注)

構成されている場合、Secure Firewall Threat Intelligence Directorは実行されるアクション（モニターまたはブロック）に影響を与える可能性があります。詳細については、Threat Intelligence Director-Firewall Management Centerのアクションの優先順位付けを参照してください。

## セキュリティ インテリジェンス ブロッキングのオーバーライド

セキュリティ インテリジェンス モニタリングを設定するには：

**設定例：セキュリティインテリジェンスブロック（12ページ）** の手順に従ってセキュリティ インテリジェンス ブロックを設定したら、ブロックリストで該当する各オブジェクトを右クリックし、[モニターのみ（Monitor-only）] を選択します。システムが提供するセキュリティ インテリジェンス リストをモニター専用に設定することはできません。

# セキュリティ インテリジェンス ブロッキングのオーバーライド

必要に応じて、ブロックしないリストを使用して、特定のドメイン、URL、またはIP アドレスが、セキュリティ インテリジェンスのリストまたはフィードによってブロックされないようにすることができます。

たとえば、以下を行うことができます。

- 信頼できるセキュリティ インテリジェンス フィードで時折発生する誤検出ブロックをオーバーライドする
- レピュテーションに基づいて早期にブロックするのではなく、特定のトラフィックを詳細に検査する
- セキュリティ インテリジェンス ブロッキングからのゾーンに基づいて、該当しなければ制限されたトランザクションを免除する

たとえば、不適切に分類された URL をブロックしないリストに追加した後、組織内でそれらの URL にアクセスする必要があるユーザーが使用しているセキュリティ ゾーンによりブロックしないリストのオブジェクトを制限するという方法が考えられます。この方法では、ビジネスニーズを持つユーザーだけが、ブロックしないリスト上の URL にアクセスできます。



(注)

Do Not Block リストのエントリは、ブロックリストから除外されるだけです。セキュリティ インテリジェンス ポリシーを通過する接続には、アクセスコントロールルールが適用されます。したがって、Do Not Block リストのエントリは、その後、アクセスコントロールルールまたは侵入ポリシーによってブロックされる可能性があります。Do Not Block エントリは、常にブロックリストから除外する必要があります。

## 手順

**ステップ1** オプション1：イベントのIP アドレス、URL、またはドメインを、グローバルのブロックしないリストに追加します。グローバルおよびドメインのセキュリティ インテリジェンス リストを参照してください。

**ステップ2 オプション2：カスタムのセキュリティインテリジェンスのリストまたはフィードを使用します。**

- a) カスタムのセキュリティインテリジェンスのリストまたはフィードを作成します。[カスタムセキュリティインテリジェンスリスト](#)または[セキュリティインテリジェンスフィードの作成](#)を参照してください。
- b) IP アドレス（ネットワーク）と URL の場合：アクセスコントロールポリシーを編集し、[セキュリティインテリジェンス（Security Intelligence）] タブをクリックしてから、[ネットワーク（Networks）] または [URL（URLs）] サブタブでカスタムのリストまたはフィードをクリックし、[ブロックしないリストに追加（Add to Do Not Block List）] をクリックします。
- c) 変更を保存します。
- d) ドメイン（DNS）の場合：[セキュリティインテリジェンスオプション（7ページ）](#) トピックの「DNS ポリシー」セクションを参照してください。
- e) 変更を展開します。

## セキュリティインテリジェンスのトラブルシューティング

セキュリティインテリジェンスのトラブルシューティングについては、次の項を参照してください。

### セキュリティインテリジェンスのカテゴリが使用可能なオプションのリストに表示されない

**症状：**アクセスコントロールポリシーの[セキュリティインテリジェンス（Security Intelligence）] タブで、[利用可能なオプション（Available Options）] の下にある [ネットワーク（Networks）] タブにセキュリティインテリジェンスカテゴリ（CnC や Exploitkit など）が表示されない。

**原因：**

- Management Center に少なくとも 1 つの管理対象デバイスが追加されるまで、これらのカテゴリは表示されません。すべての TALOS フィードを取得するには、デバイスを追加する必要があります。
- URL フィルタリング機能は、セキュリティインテリジェンス機能とは異なる一連のカテゴリを使用します。表示されると予想されるカテゴリは、URL フィルタリングカテゴリである可能性があります。URL フィルタリングカテゴリを表示するには、アクセスコントロールルールの [URL] タブを調べます。

セキュリティ インテリジェンス ブロック リストへの登録の履歴

## セキュリティ インテリジェンス ブロック リストへの登録の履歴

| 機能                      | 最小 Firewall Management Center | 最小 Firewall Threat Defense | 詳細  |
|-------------------------|-------------------------------|----------------------------|---|
| 新しいセキュリティ インテリジェンス カテゴリ | すべて                           | すべて                        | <p>Talos では、次の新しいセキュリティ インテリジェンス カテゴリを追加しました。</p> <ul style="list-style-type: none"> <li>• banking_fraud</li> <li>• ioc</li> <li>• high_risk</li> <li>• link_sharing</li> <li>• malicious</li> <li>• newly_seen</li> <li>• spyware</li> </ul> <p>新しいカテゴリに対応するようにアクセス制御と DNS ポリシーを更新し、定期的に将来の変更を確認する必要があります。</p> <p>新規/変更されたページ：[セキュリティ インテリジェンス (Security Intelligence) ] タブの [ネットワーク (Network) ] および [URL (URLs) ] サブタブ、[DNS ポリシー (DNS policies) ] の [DNS ルール (DNS rules) ] サポートされているプラットフォーム：Firewall Management Center</p> |

## 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。