CHAPTER 15

Attack Response Controller でのブロッキングとレート制限の設定

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。他の Cisco IPS センサーは、いずれも現在 IPS 7.1 をサポートしていません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降でサポートされています。ASA 8.3(*x*) ではサポートされていません。

（注） ARC は、以前は Network Access Controller と呼ばれていました。名前は変更されましたが、IME および CLI では、Network Access Controller、**nac**、および **network-access** という名前で呼ばれています。

この章では、センサー上でブロッキングを設定する方法について説明します。内容は次のとおりです。

ARC のコンポーネント

ここでは、ARC の各種コンポーネントについて説明します。内容は次のとおりです。

- 「サポートされるデバイス数」（P.15-6）

ブロッキングについて

（注）　ARC は、以前は Network Access Controller と呼ばれていました。名前は変更されましたが、IME および CLI では、Network Access Controller、**nac**、および **network-access** という名前で呼ばれています。

ARC は、攻撃側のホストおよびネットワークからのアクセスをブロックすることにより、疑わしいイベントに対応し、ネットワーク デバイスを管理します。ARC は、管理しているデバイスの IP アドレスをブロックします。他のマスター ブロッキング センサーを含め、管理しているすべてのデバイスに同じブロックを送信します。ARC は、ブロックの時間をモニタし、時間の経過後にブロックを削除します。

ARC は、7 秒以内に新しいブロックのアクション応答を完了します。ほとんどの場合は、より短い時間でアクション応答を完了します。このパフォーマンス目標を達成するために、センサーでのブロックの実行レートが高すぎたり、管理するブロッキング デバイスおよびインターフェイスが多すぎたりしないように設定してください。最大ブロック数は 250 以下にし、最大ブロッキング項目数は 10 以下にすることを推奨します。ブロッキング項目の最大数を計算するために、セキュリティ アプライアンスはブロッキング コンテキストあたり 1 つのブロッキング項目としてカウントします。ルータは、ブロッキング インターフェイス / 方向あたり 1 つのブロッキング項目としてカウントします。Catalyst ソフトウェアを実行しているスイッチは、ブロッキング VLAN あたり 1 つのブロッキング項目としてカウントします。推奨される制限を超えた場合、ARC はブロックをタイミングよく適用しなかったり、ブロックをまったく適用できなかったりすることがあります。

注意　ブロッキングは、マルチ モード管理コンテキストの FWSM ではサポートされません。

マルチモードで設定されているセキュリティ アプライアンスでは、Cisco IPS はブロック要求に VLAN 情報を含めません。したがって、ブロックされる IP アドレスが各セキュリティ アプライアンスに対して正しいことを確認する必要があります。たとえば、センサーは、VLAN A に対して設定されているセキュリティ アプライアンス カスタマー コンテキストでパケットをモニタし、VLAN B に対して設定されている別のセキュリティ アプライアンス カスタマー コンテキストでブロッキングしている場合があります。VLAN A でブロックをトリガーするアドレスは、VLAN B 上の別のホストを指している可能性があります。

ブロックには次の 3 種類があります。

- ホスト ブロック：特定の IP アドレスからのすべてのトラフィックをブロックします。
- 接続ブロック：特定の送信元 IP アドレスから特定の宛先 IP アドレスおよび宛先ポートへのトラフィックをブロックします。同じ送信元 IP アドレスから異なる宛先 IP アドレスまたは宛先ポートへの複数の接続ブロックによって、接続ブロックからホスト ブロックにブロックが自動的に切り替えられます。
- ネットワーク ブロック：特定のネットワークからのトラフィックをすべてブロックします。ホスト ブロックと接続ブロックは、手動で開始するか、シグニチャがトリガーされたときに自動的に開始できます。ネットワーク ブロックは手動でだけ開始できます。

（注） 接続ブロックとネットワーク ブロックは、適応型セキュリティ アプライアンスではサポートされていません。適応型セキュリティ アプライアンスは、追加の接続情報があるホスト ブロックだけをサポートします。

注意 ブロッキングとセンサーのパケット ドロップ機能を混同しないでください。センサーでは、インライン モードのセンサーに対してパケットのインライン拒否、接続のインライン拒否、および攻撃者のインライン拒否のアクションが設定されている場合にパケットをドロップできます。

自動ブロックの場合は、特定のシグニチャのイベント アクションとして [Request Block Host] チェックボックスまたは [Request Block Connection] チェックボックスをオンにし、そのアクションをすべての設定済みイベント アクション オーバーライドに追加する必要があります。これにより、SensorApp はそのシグニチャがトリガーされたときに ARC にブロック要求を送信することができます。ARC は、SensorApp からブロック要求を受信すると、ホストまたは接続をブロックするようにデバイス設定を更新します。

Cisco ルータおよび Catalyst 6500 シリーズ スイッチでは、ARC は ACL または VACL を適用してブロックを作成します。ACL および VACL は、インターフェイス方向または VLAN 上のデータ パケットの経路を許可または拒否します。各 ACL または VACL には、IP アドレスに適用される許可条件と拒否条件が含まれます。セキュリティ アプライアンスでは、ACL または VACL は使用されません。組み込みの **shun** および **no shun** コマンドが使用されます。

注意 ARC が作成する ACL が、ユーザやその他のシステムによって変更されることがあってはなりません。これらの ACL は一時的なものであり、新しい ACL がセンサーによって常に作成されています。Pre-Block ACL および Post-Block ACL に対してのみ、変更を加えることができます。

ARC がデバイスを管理するためには、次の情報が必要です。

- ログイン ユーザ ID（デバイスに AAA が設定されている場合）
- ログイン パスワード
- イネーブル パスワード（イネーブル特権のあるユーザは不要）
- 管理対象のインターフェイス（ethernet0 や vlan100 など）
- 作成される ACL または VACL で、最初に適用する任意の既存 ACL または VACL 情報（Pre-Block ACL または Pre-Block VACL）、または最後に適用する ACL または VACL 情報（Post-Block ACL または Post-Block VACL）これは、セキュリティ アプライアンスには該当しません。セキュリティ アプライアンスはブロックに ACL を使用しないためです。
- デバイスとの通信に Telnet と SSH のどちらを使用しているか
- ブロックしない IP アドレス（ホストまたはホストの範囲）
- ブロックの継続時間

ヒント ARC のステータスを表示するには、IME で [Configuration] > *sensor_name* > [Sensor Monitoring] > [Support Information] > [Statistics] を選択します。

（注）　レート制限およびブロッキングは、IPv6 トラフィックではサポートされていません。ブロック アクションまたはレート制限アクションが設定されているシグニチャが IPv6 トラフィックによってトリガーされると、アラートが生成されますが、アクションは実行されません。

詳細情報

- シグニチャに Request Block Host または Request Block Connection イベント アクションを追加する手順については、「シグニチャへのアクションの割り当て」（P.9-19）を参照してください。
- 特定の RR のアラートに Request Block Host または Request Block Connection イベント アクションを追加するオーバーライドを設定する手順については、「イベント アクション オーバーライドの追加、編集、削除、イネーブル化、ディセーブル化」（P.11-15）を参照してください。
- Pre-Block ACL および Post-Block ACL の詳細については、「センサーによるデバイスの管理方法」（P.15-19）を参照してください。

レート制限について

ARC は、保護されているネットワーク内のトラフィックのレート制限を行います。レート制限により、センサーはネットワーク デバイス上の指定したトラフィック クラスのレートを制限できます。レート制限応答は、ホスト フラッド エンジンとネット フラッド エンジン、および TCP ハーフオープン SYN シグニチャに対してサポートされます。ARC では、Cisco IOS 12.3 以降を実行しているネットワーク デバイスにレート制限を設定できます。マスター ブロッキング センサーは、レート制限要求をブロッキング転送センサーに転送することもできます。

レート制限を追加するには、次の項目を指定します。

- レート制限のための送信元アドレスまたは宛先アドレス（あるいはその両方）
- TCP または UDP プロトコルを使用したレート制限のための送信元ポートまたは宛先ポート（あるいはその両方）

レート制限シグニチャを調整することもできます。また、アクションを [Request Rate Limit] に設定し、これらのシグニチャのパーセンテージを設定する必要があります。

（注）　レート制限およびブロッキングは、IPv6 トラフィックではサポートされていません。ブロック アクションまたはレート制限アクションが設定されているシグニチャが IPv6 トラフィックによってトリガーされると、アラートが生成されますが、アクションは実行されません。

表 15-1 に、サポートされているレート制限シグニチャとパラメータを示します。

表 15-1　レート制限シグニチャ

シグニチャ ID	シグニチャ名	プロトコル	許可される宛先 IP アドレス	データ
2152	ICMP Flood Host	ICMP	Yes	echo-request
2153	ICMP Smurf Attack	ICMP	Yes	echo-reply
4002	UDP Flood Host	UDP	Yes	なし
6901	Net Flood ICMP Reply	ICMP	No	echo-reply
6902	Net Flood ICMP Request	ICMP	No	echo-request
6903	Net Flood ICMP Any	ICMP	No	なし

表 15-1　レート制限シグニチャ（続き）

シグニチャ ID	シグニチャ名	プロトコル	許可される宛先 IP アドレス	データ
6910	Net Flood UDP	UDP	No	なし
6920	Net Flood TCP	TCP	No	なし
3050	TCP HalfOpenSyn	TCP	No	halfOpenSyn

ヒント　ARC のステータスを表示するには、IME で [Configuration] > *sensor_name* > [Sensor Monitoring] > [Support Information] > [Statistics] を選択します。

詳細情報

- ルータにレート制限を設定する手順については、「ルータ ブロッキング デバイスおよびレート制限デバイスのインターフェイスの設定」（P.15-21）を参照してください。
- センサーをマスター ブロッキング センサーとして設定する手順については、「マスター ブロッキング センサーの設定」（P.15-28）を参照してください。

レート制限でのサービス ポリシーについて

レート制限が設定されているインターフェイス/方向にサービス ポリシーを適用しないでください。適用した場合は、レート制限アクションが失敗します。レート制限を設定する前に、インターフェイス/方向にサービス ポリシーがないことを確認し、存在する場合には削除します。ARC では、ARC が以前に追加したものでないかぎり、既存のレート制限は削除されません。

レート制限では ACL が使用されますが、ブロックと同じ方法では使用されません。レート制限では、**ACL** および**クラス マップ** エントリを使用してトラフィックを識別し、**ポリシー マップ**および**サービス ポリシー** エントリを使用してトラフィックをポリシングします。

ARC を設定する前に

注意　2 つのセンサーが同じデバイスでブロッキングまたはレート制限を制御することはできません。この状況が必要な場合は、一方のセンサーをマスター ブロッキング センサーとして設定してデバイスを管理し、もう一方のセンサーでマスター ブロッキング センサーに要求を転送できます。

（注）　マスター ブロッキング センサーを追加する場合は、センサーあたりのブロッキング デバイス数を減らします。たとえば、それぞれ 1 つのブロッキング インターフェイス/方向を持つ 10 個のセキュリティ アプライアンスと 10 台のルータでブロックする場合は、センサーに 10 個を割り当て、マスター ブロッキング センサーに残りの 10 個を割り当てることができます。

ブロッキングやレート制限を実行するように ARC を設定する前に、必ず次の作業を行ってください。

- ネットワーク トポロジを分析し、どのデバイスをどのセンサーによってブロックしなければならないか、またブロックしてはならないのはどのアドレスかを確認します。

- 各デバイスにログインするために必要なユーザ名、デバイスのパスワード、イネーブル パスワード、および接続タイプ（Telnet または SSH）の情報を収集します。
- デバイス上のインターフェイスの名前を確認します。
- 必要に応じて、Pre-Block ACL または Pre-Block VACL、および Post-Block ACL または Post-Block VACL の名前を確認します。
- ブロックするインターフェイスとブロックしないインターフェイス、およびその方向（インかアウトか）を確認します。誤ってネットワーク全体をシャットダウンすることは避けなければなりません。

サポートされるデバイス数

注意　推奨される制限を超えた場合、ARC はブロックをタイミングよく適用しなかったり、ブロックをまったく適用できなかったりすることがあります。

デフォルトでは、ARC サービスは任意の組み合わせで 250 個までのデバイスをサポートします。ARC によるブロッキングがサポートされるデバイスは、次のとおりです。

- Cisco IOS 11.2 以降（ACL）を使用する Cisco シリーズ ルータ
  - Cisco 1600 シリーズ ルータ
  - Cisco 1700 シリーズ ルータ
  - Cisco 2500 シリーズ ルータ
  - Cisco 2600 シリーズ ルータ
  - Cisco 2800 シリーズ ルータ
  - Cisco 3600 シリーズ ルータ
  - Cisco 3800 シリーズ ルータ
  - Cisco 7200 シリーズ ルータ
  - Cisco 7500 シリーズ ルータ
- Catalyst 5000 スイッチ、RSM 搭載、IOS 11.2(9)P 以降（ACL）
- Catalyst 6500 スイッチおよび 7600 ルータ、IOS 12.1(13)E 以降（ACL）
- Catalyst 6500 スイッチ 7600 ルータ、Catalyst ソフトウェア バージョン 7.5(1) 以降（VACL）
  - Supervisor Engine 1A（PFC 搭載）
  - Supervisor Engine 1A（MSFC1 搭載）
  - Supervisor Engine 1A（MFSC2 搭載）
  - Supervisor Engine 2（MSFC2 搭載）
  - Supervisor Engine 720（MSFC3 搭載）

  （注）　Supervisor Engine での VACL ブロッキングと MSFC での ACL ブロッキングがサポートされます。
- PIX Firewall、バージョン 6.0 以降（**shun** コマンド）
  - 501

  - 506E
  - 515E
  - 525
  - 535
- ASA、バージョン 7.0 以降（**shun** コマンド）
  - ASA-5510
  - ASA-5520
  - ASA-5540
- FWSM 1.1 以降（**shun** コマンド）

ブロッキングを設定するには、ACL、VACLS、または **shun** コマンドのいずれかを使用します。すべてのファイアウォールおよび ASA モデルは **shun** コマンドをサポートします。

ARC によるレート制限がサポートされるデバイスは、次のとおりです。

- Cisco IOS 12.3 以降を使用する Cisco シリーズ ルータ
  - Cisco 1700 シリーズ ルータ
  - Cisco 2500 シリーズ ルータ
  - Cisco 2600 シリーズ ルータ
  - Cisco 2800 シリーズ ルータ
  - Cisco 3600 シリーズ ルータ
  - Cisco 3800 シリーズ ルータ
  - Cisco 7200 シリーズ ルータ
  - Cisco 7500 シリーズ ルータ

注意　ARC は、VIP を使用する 7500 ルータ上でレート制限を実行することはできません。ARC はエラーを報告しますが、レート制限は実行できません。

ブロッキング プロパティの設定

ここでは、センサーのブロッキング プロパティを設定する方法について説明します。内容は次のとおりです。

[Blocking Properties] ペイン

（注）　ブロッキングの対象としない IP アドレスを追加、編集、削除するには、管理者またはオペレータであることが必要です。

ブロッキングとレート制限をイネーブルにするために必要な基本的な設定を行うには、[Blocking Properties] ペインを使用します。

ブロッキング プロパティについて

ARC は、管理対象デバイス上のブロッキング アクションおよびレート制限アクションを制御します。手動であってもブロックされてはならないホストおよびネットワークを識別できるように、センサーを調整する必要があります。これは、信頼されたネットワーク デバイスの通常の動作が攻撃として扱われる可能性があるためです。そのようなデバイスは絶対にブロックしてはなりません。また、信頼できる内部のネットワークも絶対にブロックしてはなりません。シグニチャを適切にチューニングすることにより、偽陽性の数を減らし、ネットワークが正しく動作することを保証できます。シグニチャのチューニングとフィルタリングによって、アラームの生成を防止します。アラームが生成されない場合、それに関連付けられたブロックも実行されません。

（注）　[Never Block Address] はレート制限には適用されません。このオプションは、Request Block Host または Request Block Connection イベント アクションにのみ適用されます。このオプションは、Deny Attacker Inline、Deny Connection Inline、または Deny Packet Inline イベント アクションには適用されません。ブロック、拒否、またはドロップの対象から外すホストをフィルタ処理によって除外するには、イベント アクション規則を使用します。

ネットマスクを指定すると、それがブロックされないネットワークのネットマスクになります。ネットマスクを指定しないと、指定した IP アドレスだけがブロックされません。

注意　センサーがそれ自体をブロックすることを許可すると、ブロッキング デバイスとの通信ができなくなる可能性があるため、お勧めしません。センサーでそれ自体の IP アドレスをブロックするルールが作成されても、センサーからブロッキング デバイスへのアクセスが妨げられないことが確認された場合は、このオプションを設定できます。

デフォルトでは、センサーのブロッキングはイネーブルになっています。デバイスが ARC によって管理されていて、手動で何かを設定する必要があるときは、まずブロッキングをディセーブルにする必要があります。ユーザと ARC の両方が同じデバイスで同時に変更を加える状況を回避する必要があります。この状況が発生すると、デバイスまたは ARC でエラーが発生します。

デフォルトでは、Cisco IOS デバイスではブロッキングのみサポートされます。レート制限またはブロッキングとレート制限を選択することにより、ブロッキングのデフォルトをオーバーライドできます。

[Blocking Properties] ペインのフィールド定義

[Blocking Properties] ペインには次のフィールドがあります。

- [Enable blocking] : ホストのブロッキングをイネーブルにするかどうか。デフォルトはイネーブルです。[Enable blocking] がディセーブルであり、他のフィールドにデフォルト以外の値がある場合は、エラー メッセージが表示されます。

（注） ブロッキングをイネーブルにする場合は、レート制限もイネーブルにします。ブロッキングをディセーブルにする場合は、レート制限もディセーブルにします。これは、ARC が新しいブロックまたはレート制限の追加や既存のブロックまたはレート制限の削除を行えないことを意味します。

（注） ブロッキングをイネーブルにしない場合でも、他のすべてのブロッキング設定を指定できます。

- [Allow sensor IP address to be blocked] : センサーの IP アドレスのブロッキングを許可するかどうか。デフォルトはディセーブルです。
- [Log all block events and errors] : ブロックの開始から終了までのイベントと発生したエラー メッセージをログに記録するようにセンサーを設定します。ブロックがデバイスに追加されるかデバイスから削除されると、イベントがログに記録されます。これらすべてのイベントおよびエラーをログに記録する必要はない可能性があります。このオプションをディセーブルにすると、新しいイベントとエラーが抑止されます。デフォルトはイネーブルです。

（注） すべてのブロック イベントとエラーの記録はレート制限にも適用されます。

- [Enable NVRAM write] : ARC の最初の接続時にルータが NVRAM への書き込みを実行するようにセンサーを設定します。イネーブルになっている場合は、ACL が更新されるたびに NVRAM が書き込まれます。デフォルトはディセーブルです。

（注） NVRAM の書き込みをイネーブルにすると、ブロッキングとレート制限に対するすべての変更が NVRAM に必ず書き込まれます。ルータが再起動された場合でも、適切なブロックとレート制限がアクティブになります。NVRAM の書き込みがディセーブルになっている場合、ルータの再起動後にブロッキングまたはレート制限が行われない期間が短時間発生します。NVRAM 書き込みをイネーブルにしない場合、NVRAM の寿命が延び、新しいブロックとレート制限の設定にかかる時間が短縮されます。

- [Enable ACL Logging] : ACL または VACL のブロック エントリにログ パラメータを追加するように ARC を設定します。これにより、デバイスはパケットがフィルタ処理されるときに syslog イベントを生成します。このオプションは、ルータとスイッチだけに適用されます。デフォルトはディセーブルです。
- [Maximum Block Entries] : ブロックするエントリの最大数。値は 1 ～ 65535 です。デフォルトは 250 です。
- [Maximum Interfaces] : ブロックを実行するためのインターフェイスの最大数を設定します。

  たとえば、PIX 500 シリーズ セキュリティ アプライアンスは 1 つのインターフェイスとカウントされます。1 つのインターフェイスを持つルータは 1 つとしてカウントされますが、2 つのインターフェイスを持つルータは 2 つとしてカウントされます。インターフェイスの最大数はデバイスあたり 250 です。デフォルトは 250 です。

（注） [Maximum Interfaces] を使用して、ARC が管理できるデバイスおよびインターフェイスの最大数を設定します。ブロッキング デバイスの合計数（マスター ブロッキング センサーを含まない）がこの値を超えることはできません。ブロッキング項目の合計数もこの値を超えることはできません。ブロッキング項目は 1 つのセキュリティ アプライアンス コンテキスト、1 つのルータ ブロッキング インターフェイス / 方向、または VLAN をブロッキングしている 1 つの Catalyst ソフトウェア スイッチです。

（注） また、デバイスあたり 250 個のインターフェイス、250 台のセキュリティ アプライアンス、250 台のルータ、250 台の Catalyst ソフトウェア スイッチ、および 100 台のマスター ブロッキング センサーは、固定の最大数であり、変更できません。

- [Maximum Rate Limit Entries] : レート制限エントリの最大数。レート制限エントリの最大数は、ブロッキング エントリの最大数以下である必要があります。ブロッキング エントリより多いレート制限エントリを設定すると、エラーが発生します。値は 1 ～ 32767 です。デフォルトは 250 です。
- [Never Block Addresses] : センサーによるブロッキングの対象外とする IP アドレスを設定します。

（注） [Never Block Address] はレート制限には適用されません。このオプションは、Request Block Host および Request Block Connection イベント アクションにのみ適用されます。このオプションは、Deny Attacker Inline、Deny Connection Inline、または Deny Packet Inline イベント アクションには適用されません。ブロック、拒否、またはドロップの対象から外すホストをフィルタ処理によって除外するには、イベント アクション規則を使用します。

  - [IP Address] : ブロックしない IP アドレス。
  - [Mask] : ブロックしない IP アドレスに対応するマスク。

ブロッキング プロパティの設定

ブロッキング プロパティを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Management] > [Blocking] > [Blocking Properties] を選択します。

ステップ 3　[Enable blocking] チェックボックスをオンにして、ブロッキングとレート制限をイネーブルにします。

（注） ブロッキングまたはレート制限が機能するためには、ブロッキングまたはレート制限を実行するようにデバイスを設定する必要があります。

ステップ 4　必要な場合以外は、[Allow the sensor IP address to be blocked] チェックボックスをオンにしないでください。

注意　センサーがそれ自体をブロックすることを許可すると、ブロッキング デバイスとの通信ができなくなる可能性があるため、お勧めしません。このオプションは、センサーが自分の IP アドレスをブロックする規則を作成した場合に、そのためにセンサーがブロックしている装置にアクセスできなくなることはないと保証されている場合にだけ選択します。

ステップ 5　ブロッキング イベントとエラーをログに記録する場合は、[Log all block events and errors] チェックボックスをオンにします。

ステップ 6　ARC の最初の接続時にルータが NVRAM への書き込みを実行するようにセンサーを設定する場合は、[Enable NVRAM write] チェックボックスをオンにします。

ステップ 7　ACL または VACL のブロック エントリにログ パラメータを追加するように ARC を設定する場合は、[Enable ACL logging] チェックボックスをオンにします。

ステップ 8　[Maximum Block Entries] フィールドには、同時に維持されるブロックの数を入力します（1 ～ 65535）。

（注）　最大ブロック エントリ数を 250 より大きな値に設定することは推奨しません。

（注）　ブロック数が最大ブロック エントリ数を超えることはありません。最大数に達すると、既存のブロックがタイムアウトするか削除されるまで新しいブロックは発生しません。

ステップ 9　ブロックを実行するインターフェイスの数を [Maximum Interfaces] フィールドに入力します。

ステップ 10　レート制限エントリの数（1 ～ 32767）を [Maximum Rate Limit Entries] フィールドに入力します。

注意　レート制限エントリの最大数は、ブロッキング エントリの最大数以下である必要があります。ブロッキング エントリより多いレート制限エントリを設定すると、エラーが発生します。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 11　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

[Add Never Block Address] および [Edit Never Block Address] ダイアログボックスのフィールド定義

[Add Never Block Address] および [Edit Never Block Address] ダイアログボックスには次のフィールドがあります。

- [IP Address]：ブロックしない IP アドレス。
- [Mask]：ブロックしない IP アドレスに対応するマスク。

ブロックしない IP アドレスの追加、編集、削除

ブロックしない IP アドレスを追加、編集、削除するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Management] > [Blocking] > [Blocking Properties] を選択し、[Add] をクリックして、ブロックしないアドレスのリストにホストまたはネットワークを追加します。

ステップ 3　[IP Address] フィールドに、ホストまたはネットワークの IP アドレスを入力します。

ステップ 4　[Network Mask] フィールドで、ホストまたはネットワークのネットワーク マスクを入力するか、リストからネットワーク マスクを選択します。

ヒント　変更内容を破棄して [Add Never Block Address] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 5　[OK] をクリックします。エントリが同一である場合は、エラー メッセージが表示されます。新しいホストまたはネットワークが [Blocking Properties] ペインの [Never Block Addresses] リストに表示されます。

ステップ 6　[Never Block Addresses] リスト内の既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 7　[IP Address] フィールドで、ホストまたはネットワークの IP アドレスを編集します。

ステップ 8　[Network Mask] フィールドで、ホストまたはネットワークのネットワーク マスクを編集します。

ヒント　変更内容を破棄して [Edit Never Block Address] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 9　[OK] をクリックします。編集したホストまたはネットワークが [Allowed Hosts] ペインの [Never Block Addresses] リストに表示されます。

ステップ 10　リストからホストまたはネットワークを削除するには、そのホストまたはネットワークを選択し、[Delete] をクリックします。そのホストは、[Blocking Properties] ペインの [Never Block Addresses] リストに表示されなくなります。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 11　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

デバイス ログイン プロファイルの設定

ここでは、デバイス ログイン プロファイルの設定方法について説明します。内容は次のとおりです。

- 「[Add Device Login Profile] および [Edit Device Login Profile] ダイアログボックスのフィールド定義」（P.15-13）
- 「デバイス ログイン プロファイルの設定」（P.15-14）

[Device Login Profiles] ペイン

（注）　デバイス ログイン プロファイルを追加または編集するには、管理者またはオペレータであることが必要です。

センサーがブロッキング デバイスにログインするときに使用するプロファイルを設定するには、[Device Login Profiles] ペインを使用します。センサーが管理する他のハードウェアのデバイス ログイン プロファイルを設定する必要があります。デバイス ログイン プロファイルには、作成した名前の下に、ユーザ名、ログイン パスワード、およびイネーブル パスワードの情報が含まれます。たとえば、同じパスワードとユーザ名を共有するすべてのルータを 1 つのデバイス ログイン プロファイル名にまとめることができます。

（注）　ブロッキング デバイスを設定する前にデバイス ログイン プロファイルを作成する必要があります。

[Device Login Profiles] ペインのフィールド定義

[Device Login Profiles] ペインには次のフィールドがあります。

- [Profile Name]：プロファイルの名前。
- [Username]：ブロッキング デバイスへのログインに使用するユーザ名。
- [Login Password]：ブロッキング デバイスへのログインに使用するログイン パスワード。

  （注）　パスワードが存在する場合は、固定数のアスタリスクで表示されます。

- [Enable Password]：ブロッキング デバイスで使用されるイネーブル パスワード。

  （注）　パスワードが存在する場合は、固定数のアスタリスクで表示されます。

[Add Device Login Profile] および [Edit Device Login Profile] ダイアログボックスのフィールド定義

[Add Device Login Profile] および [Edit Device Login Profile] ダイアログボックスには次のフィールドがあります。

- [Profile Name]：プロファイルの名前。
- [Username]：ブロッキング デバイスへのログインに使用するユーザ名。
- [Login Password]：ブロッキング デバイスへのログインに使用するログイン パスワード。

（注）　パスワードが存在する場合は、固定数のアスタリスクで表示されます。

- [Enable Password] : ブロッキング デバイスで使用されるイネーブル パスワード。

（注）　パスワードが存在する場合は、固定数のアスタリスクで表示されます。

デバイス ログイン プロファイルの設定

デバイス ログイン プロファイルを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Management] > [Blocking] > [Device Login Profiles] を選択し、[Add] をクリックして、プロファイルを追加します。

ステップ 3　[Profile Name] フィールドにプロファイル名を入力します。

ステップ 4　（任意）[Username] フィールドに、ブロッキング デバイスへのログインに使用するユーザ名を入力します。

ステップ 5　（任意）[New Password] フィールドにログイン パスワードを入力します。

ステップ 6　（任意）確認のために [Confirm New Password] フィールドにもう一度ログイン パスワードを入力します。

ステップ 7　（任意）[New Password] フィールドにイネーブル パスワードを入力します。

ステップ 8　（任意）確認のために [Confirm New Password] フィールドにもう一度イネーブル パスワードを入力します。

ヒント　変更を破棄して [Add Device Login Profile] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 9　[OK] をクリックします。すでに存在するプロファイル名を入力すると、エラー メッセージが表示されます。新しいデバイス ログイン プロファイルが [Device Login Profile] ペインのリストに表示されます。

ステップ 10　デバイス ログイン プロファイル リストの既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 11　[Username] フィールドで、ブロッキング デバイスへのログインに使用するユーザ名を編集します。

ステップ 12　ログイン パスワードを変更するには、[Change the login password] チェックボックスをオンにします。

ステップ 13　[New Password] フィールドに新しいログイン パスワードを入力します。

ステップ 14　確認のために [Confirm New Password] フィールドに新しいログイン パスワードをもう一度入力します。

ステップ 15　イネーブル パスワードを変更するには、[Change the enable password] チェックボックスをオンにします。

ステップ 16　[New Password] フィールドに新しいイネーブル パスワードを入力します。

ステップ 17　確認のために [Confirm New Password] フィールドにもう一度イネーブル パスワードを入力します。

ヒント　変更を破棄して [Edit Device Login Profile] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 18　[OK] をクリックします。編集したデバイス ログイン プロファイルが、[Device Login Profile] ペインのリストに表示されます。

ステップ 19　リストからデバイス ログイン プロファイルを削除するには、そのプロファイルを選択し、[Delete] をクリックします。そのデバイス ログイン プロファイルは、[Device Login Profile] ペインのリストに表示されなくなります。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 20　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

ブロッキング デバイスの設定

ここでは、ブロッキング デバイスの設定方法について説明します。内容は次のとおりです。

[Blocking Device] ペイン

（注）　ブロッキング デバイスを設定するには、管理者またはオペレータであることが必要です。

センサーがブロッキングとレート制限を実行するために使用するデバイスを設定するには、[Blocking Device] ペインを使用します。Cisco IOS ルータまたは Catalyst 6500 スイッチに配置する ACL 規則を生成するか、またはセキュリティ アプライアンス上に排除規則を生成することによって攻撃をブロックするようにセンサーを設定できます。このようなルータ、スイッチ、ファイアウォールは、ブロッキング デバイスと呼ばれます。

レート制限では ACL が使用されますが、ブロックと同じ方法では使用されません。レート制限では、ACL およびクラス マップ エントリを使用してトラフィックを識別し、ポリシー マップおよびサービス ポリシー エントリを使用してトラフィックをポリシングします。

注意　1 つのセンサーで複数のデバイスを管理できますが、1 つのデバイスに対して複数のセンサーは使用できません。そのような目的には、マスター ブロッキング センサーを使用する必要があります。

[Blocking Devices] ペインでデバイスを設定するためには、まずセンサーが管理する各デバイスにデバイス ログイン プロファイルを指定する必要があります。

[Blocking Devices] ペインのフィールド定義

[Blocking Devices] ペインには次のフィールドがあります。

- [IP Address] : ブロッキング デバイスの IP アドレス。
- [Sensor's NAT Address] : センサーの NAT アドレス。
- [Device Login Profile] : ブロッキング デバイスへのログインに使用するデバイス ログイン プロファイル。
- [Device Type] : デバイスのタイプ（[Cisco Router]、[Cat 6K]、[PIX/ASA]）。デフォルトは [Cisco Router] です。
- [Response Capabilities] : デバイスが、ブロッキング、レート制限、またはその両方を使用するかどうかを示します。
- [Communication] : ブロッキング デバイスへのログインに使用する通信メカニズム（[SSH 3DES] および [Telnet]）を示します。デフォルトは [SSH 3DES] です。

[Add Blocking Device] および [Edit Blocking Device] ダイアログボックスのフィールド定義

[Add Blocking Device] および [Edit Blocking Device] ダイアログボックスには次のフィールドがあります。

- [IP Address] : ブロッキング デバイスの IP アドレス。
- [Sensor's NAT Address] : センサーの NAT アドレス。
- [Device Login Profile] : ブロッキング デバイスへのログインに使用するデバイス ログイン プロファイル。
- [Device Type] : デバイスのタイプ（[Cisco Router]、[Cat 6K]、[PIX/ASA]）。デフォルトは [Cisco Router] です。
- [Response Capabilities] : デバイスが、ブロッキング、レート制限、またはその両方を使用するかどうかを示します。
- [Communication] : ブロッキング デバイスへのログインに使用する通信メカニズム（[SSH 3DES] および [Telnet]）を示します。デフォルトは [SSH 3DES] です。

ブロッキング デバイスおよびレート制限デバイスの追加、編集、削除

ブロッキング デバイスおよびレート制限デバイスを追加、編集、または削除するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Blocking] > [Blocking Devices] を選択し、[Add] をクリックして、ブロッキング デバイスを追加します。デバイス ログイン プロファイルを設定していない場合は、エラー メッセージが表示されます。

ステップ 3　[IP Address] フィールドには、ブロッキング デバイスの IP アドレスを入力します。

ステップ 4　（任意）[Sensor's NAT Address] フィールドにセンサーの NAT アドレスを入力します。

ステップ 5　[Device Login Profile] ドロップダウン リストからデバイス ログイン プロファイルを選択します。

ステップ 6　[Device Type] ドロップダウン リストからデバイス タイプを選択します。

ステップ 7　[Response Capabilities] フィールドで、[Block] チェックボックスまたは [Rate Limit] チェックボックス（あるいは両方）をオンにし、デバイスがブロッキングとレート制限のどちらを実行するか、または両方を実行するかを指定します。

（注）　シグニチャがトリガーされたときに SensorApp がブロック要求またはレート制限要求を ARC に送信するように、特定のシグニチャに対してブロッキング アクションとレート制限アクションを選択する必要があります。

ステップ 8　[Communication] ドロップダウン リストから、次のいずれかの通信タイプを選択します。[SSH 3DES] を選択した場合は、ステップ 11 に進んでください。

ヒント　変更内容を破棄して [Add Blocking Device] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 9　[OK] をクリックします。IP アドレスがすでに追加されている場合は、エラー メッセージが表示されます。新しいデバイスが [Blocking Devices] ペインのリストに表示されます。

ステップ 10　[SSH 3DES] を選択した場合は、デバイスを既知のホスト リストに追加する必要があります。

（注）　[SSH 3DES] を選択する場合は、ブロッキング デバイスが 3DES 暗号化をサポートする機能セットまたはライセンスを備えている必要があります。

（注）　[Configuration] > *sensor_name* > [Sensor Management] > [SSH] > [Known Host Keys] > [Add Known Host Key] を選択して、デバイスを既知のホスト リストに追加することもできます。

a.　センサーに Telnet 接続し、CLI にログインします。

b.　グローバル コンフィギュレーション モードを開始します。

```
sensor# configure terminal
```

c.　公開キーを入手します。

```
sensor(config)# ssh host-key blocking_device_ip_address
```

d.　公開キーを既知のホストのリストに追加することを確認するように求めるメッセージが表示されます。

```
Would you like to add this to the trusted certificate table for this host?[yes]:
```

e.　**yes** と入力します。

f.　グローバル コンフィギュレーション モードと CLI を終了します。

```
sensor(config)# exit
sensor# exit
```

ステップ 11　ブロッキング デバイス リストの既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 12　必要に応じて、センサーの NAT アドレスを編集します。

ステップ 13　必要に応じて、デバイス ログイン プロファイルを変更します。

ステップ 14　必要に応じて、デバイス タイプを変更します。

ステップ 15　必要に応じて、デバイスがブロッキングとレート制限のどちらを実行するかの設定を変更します。

ステップ 16　必要に応じて、通信タイプを変更します。

ヒント　変更内容を破棄して [Edit Blocking Device] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 17　[OK] をクリックします。編集したブロッキング デバイスが [Blocking Device] ペインのリストに表示されます。

ステップ 18　リストからブロッキング デバイスを削除するには、そのデバイスを選択し、[Delete] をクリックします。そのデバイスは、[Blocking Device] ペインのリストに表示されなくなります。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 19　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

Router Blocking Device Interfaces の設定

ここでは、ルータ ブロッキング デバイス インターフェイスの設定方法について説明します。内容は次のとおりです。

[Router Blocking Device Interfaces] ペイン

（注）　ルータ ブロッキング デバイス インターフェイスを設定するには、管理者またはオペレータであることが必要です。

[Router Blocking Device Interfaces] ペインで、ルータにブロッキング インターフェイスまたはレート制限インターフェイスを設定し、ブロッキングまたはレート制限の対象とするトラフィックの方向を指定する必要があります。

ルータ ブロッキング デバイス インターフェイスの概要

（注）　Pre-Block ACL および Post-Block ACL はレート制限には適用されません。

Pre-Block ACL と Post-Block ACL は、ルータのコンフィギュレーション内に作成し、保存します。これらの ACL は名前付きまたは番号付きの拡張 IP ACL にする必要があります。ACL の作成の詳細については、ルータのマニュアルを参照してください。[Pre-Block ACL] と [Post-Block ACL] の各フィールドに、ルータにすでに設定されている ACL の名前を入力します。

Pre-Block ACL は、主にブロック対象外のものを許可するために使用されます。この ACL を使用してパケットがチェックされるとき、最初に一致する行によってアクションが決まります。最初に一致する行が Pre-Block ACL の許可の行である場合、ACL の後の方に（自動ブロックの）拒否の行があっても、そのパケットは許可されます。Pre-Block ACL は、ブロックによって生じる拒否の行よりも優先されます。

Post-Block ACL は、同じインターフェイスまたは方向に対して、追加的にブロッキングまたは許可を行う場合に最適です。センサーが管理するインターフェイスまたは方向に既存の ACL がある場合、その ACL を Post-Block ACL として使用できます。Post-Block ACL がない場合、センサーは新しい ACL の最後に **permit ip any any** を挿入します。

センサーが起動すると、2 つの ACL の内容が読み込まれます。そして、次のエントリを持った 3 つ目の ACL が作成されます。

- センサーの IP アドレスに対する **permit** 行
- Pre-Block ACL のすべての設定行のコピー
- センサーによってブロックされている各アドレスの **deny** 行
- Post-Block ACL のすべての設定行のコピー

センサーは新しい ACL を、指定したインターフェイスと方向に適用します。

（注）　新しい ACL がルータのインターフェイスまたは方向に適用されると、そのインターフェイスまたは方向に対する他の ACL が適用されなくなります。

センサーによるデバイスの管理方法

（注）　ACL はレート制限デバイスには適用されません。

ARC は、Cisco のルータやスイッチを管理する場合、それらのデバイス上の ACL を使用します。ACL は、次のように作成されます。

1. センサー IP アドレス、またはセンサーの NAT アドレス（指定されている場合）がある **permit** 行

   （注）　センサーのブロックを許可している場合、この行は ACL に含まれません。

2. Pre-Block ACL（指定されている場合）

   この ACL は、すでにデバイスに存在している必要があります。

（注）　ARC は、この ACL の行を読み取り、その行を ACL の先頭にコピーします。

3. アクティブなブロックがある場合、そのブロック
4. 次のいずれか
   - Post-Block ACL（指定されている場合）

     この ACL は、すでにデバイスに存在している必要があります。

     （注）　ARC は、この ACL の行を読み取り、その行を ACL の末尾にコピーします。

     （注）　一致しなかったすべてのパケットを許可する場合は、ACL の最後の行を必ず **permit ip any any** にしてください。

   - **permit ip any any**（Post-Block ACL を指定した場合は使用されません）

ARC は、デバイスの管理に 2 つの ACL を使用します。アクティブな ACL は一度に 1 つだけです。オフラインの ACL 名を使用して新しい ACL が作成され、それがインターフェイスに適用されます。次に、ARC は次のサイクルで逆のプロセスを実行します。

注意　ARC が作成する ACL が、ユーザやその他のシステムによって変更されることがあってはなりません。これらの ACL は一時的なものであり、新しい ACL がセンサーによって常に作成されています。Pre-Block ACL および Post-Block ACL に対してのみ、変更を加えることができます。

Pre-Block ACL または Post-Block ACL を修正する必要がある場合は、次の手順を実行します。

1. センサーでブロッキングをディセーブルにします。
2. デバイスの設定に変更を加えます。
3. センサーでブロッキングを再びイネーブルにします。

ブロッキングが再度イネーブルになると、センサーは新しいデバイス設定を読み取ります。

注意　1 つのセンサーで複数のデバイスを管理できますが、1 つのデバイスに対して複数のセンサーは使用できません。その場合は、マスター ブロッキング センサーを使用してください。

詳細情報

- ブロッキングをイネーブルにする手順については、「ブロッキング プロパティの設定」（P.15-10）を参照してください。
- センサーをマスター ブロッキング センサーとして設定する手順については、「マスター ブロッキング センサーの設定」（P.15-28）を参照してください。

[Router Blocking Device Interfaces] ペインのフィールド定義

[Router Blocking Device Interfaces] ペインには次のフィールドがあります。

- [Router Blocking Device]：ルータ ブロッキング デバイスまたはレート制限デバイスの IP アドレス。

- [Blocking Interface]：ルータ ブロッキング デバイスまたはレート制限デバイス上で使用するインターフェイス。有効な値は、a ～ z、A ～ Z、0 ～ 9、特殊文字の "." および "/" で構成される 1 ～ 64 文字の文字列です。
- [Direction]：ブロッキング ACL を適用する方向。有効な値は、[In] または [Out] です。
- [Pre-Block ACL]：ブロッキング ACL の前に適用する ACL。有効な値は 0 ～ 64 文字です。このフィールドはレート制限には適用されません。
- [Post-Block ACL]：ブロッキング ACL の後に適用する ACL。有効な値は 0 ～ 64 文字です。このフィールドはレート制限には適用されません。

（注）　Post-Block ACL を Pre-Block ACL と同じものにすることはできません。

[Add Router Blocking Device Interface] および [Edit Router Blocking Device Interface] ダイアログボックスのフィールド定義

[Add Router Blocking Device Interface] および [Edit Router Blocking Device Interface] ダイアログボックスには次のフィールドがあります。

- [Router Blocking Device]：ルータ ブロッキング デバイスまたはレート制限デバイスの IP アドレス。
- [Blocking Interface]：ルータ ブロッキング デバイスまたはレート制限デバイス上で使用するインターフェイス。有効な値は、a ～ z、A ～ Z、0 ～ 9、特殊文字の "." および "/" で構成される 1 ～ 64 文字の文字列です。
- [Direction]：ブロッキング ACL を適用する方向。有効な値は、[In] または [Out] です。
- [Pre-Block ACL]：ブロッキング ACL の前に適用する ACL。有効な値は 0 ～ 64 文字です。このフィールドはレート制限には適用されません。
- [Post-Block ACL]：ブロッキング ACL の後に適用する ACL。有効な値は 0 ～ 64 文字です。このフィールドはレート制限には適用されません。

（注）　Post-Block ACL を Pre-Block ACL と同じものにすることはできません。

ルータ ブロッキング デバイスおよびレート制限デバイスのインターフェイスの設定

ルータ ブロッキング デバイスおよびレート制限デバイスのインターフェイスを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Management] > [Blocking] > [Router Blocking Device Interfaces] を選択し、[Add] をクリックして、ルータ ブロッキング デバイスまたはレート制限デバイスのインターフェイスを追加します。

ステップ 3　[Router Blocking Device] ドロップダウン リストから、ルータ ブロッキング デバイスまたはレート制限デバイスの IP アドレスを選択します。

ステップ 4　[Blocking Interface] フィールドにブロッキング インターフェイスまたはレート制限インターフェイスの名前を入力します。

ステップ 5　[Direction] ドロップダウン リストから方向（[In] または [Out]）を選択します。

ステップ 6　（任意）[Pre-Block ACL] フィールドに Pre-Block ACL の名前を入力します。

（注）　この手順はレート制限デバイスには適用されません。

ステップ 7　（任意）[Post-Block ACL] フィールドに Post-Block ACL の名前を入力します。

（注）　この手順はレート制限デバイスには適用されません。

ヒント　変更を破棄して [Add Router Blocking Device Interface] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 8　[OK] をクリックします。IP アドレス、インターフェイス、方向の組み合わせがすでに存在する場合は、エラー メッセージが表示されます。新しいインターフェイスが [Router Blocking Device Interfaces] ペインのリストに表示されます。

ステップ 9　ルータ ブロッキング デバイス インターフェイス リスト内の既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 10　必要に応じて、ブロッキング インターフェイスまたはレート制限インターフェイスの名前を編集します。

ステップ 11　必要に応じて、方向を変更します。

ステップ 12　必要に応じて、Pre-Block ACL の名前を編集します。

ステップ 13　必要に応じて、Post-Block ACL の名前を編集します。

ヒント　変更を破棄して [Edit Router Blocking Device Interface] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 14　[OK] をクリックします。編集したブロッキング デバイス インターフェイスまたはレート制限デバイス インターフェイスは、[Router Blocking Device Interfaces] ペインのリストに表示されなくなります。

ステップ 15　リストからルータ ブロッキング デバイス インターフェイスまたはレート制限デバイス インターフェイスを削除するには、そのインターフェイスを選択し、[Delete] をクリックします。そのルータ ブロッキング デバイス インターフェイスまたはレート制限デバイス インターフェイスは、[Router Blocking Device Interfaces] ペインのリストに表示されなくなります。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 16　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

Cat 6K のブロッキング デバイス インターフェイスの設定

ここでは、Catalyst 6500 Series シリーズ インターフェイスの設定方法について説明します。内容は次のとおりです。

[Cat 6K Blocking Device Interfaces] ペイン

（注）　Catalyst 6500 シリーズ スイッチのブロッキング デバイス インターフェイスを設定するには、管理者またはオペレータであることが必要です。

[Cat 6K Blocking Device Interfaces] ペインで、ブロッキング Catalyst 6500 シリーズ スイッチの VLAN ID および VACL を指定します。

Cat 6K ブロッキング デバイス インターフェイスの概要

Cisco Catalyst ソフトウェアを実行している場合にはスイッチ自体にある VACL を使用し、Cisco IOS ソフトウェアを実行している場合には MSFC 上またはスイッチ自体にあるルータの ACL を使用して、ARC のブロッキングを設定できます。ここでは、VACL を使用したブロッキングについて説明します。VACL を使用するスイッチでレート制限を実行するように設定することはできません。Catalyst 6500 シリーズ スイッチ上でブロッキング インターフェイスを設定し、ブロックするトラフィックの VLAN を指定する必要があります。

Pre-Block VACL と Post-Block VACL は、スイッチ設定内に作成し、保存します。これらの VACL は名前付きまたは番号付きの拡張 IP VACL にする必要があります。VACL の作成の詳細については、スイッチのマニュアルを参照してください。[Pre-Block VACL] と [Post-Block VACL] の各フィールドに、スイッチにすでに設定されている VACL の名前を入力します。

Pre-Block VACL は、主としてセンサーによってブロックしない対象を許可する場合に使用します。パケットが VACL に対してチェックされると、最初に一致した行によってアクションが決定されます。最初の行が Pre-Block VACL の permit 行と一致する場合、VACL の後の方に（自動ブロックからの）deny 行がある場合でも、パケットは許可されます。Pre-Block VACL では、ブロックの結果の deny 行をオーバーライドできます。

Post-Block VACL は、同じ VACL に対して追加的にブロッキングまたは許可を行う場合に最適です。センサーが管理する VLAN に既存の VACL がある場合、その VACL を Post-Block VACL として使用できます。Post-Block V ACL がない場合、センサーは新しい VACL の最後に **permit ip any any** を挿入します。

（注）　IDSM-2 は新しい VACL の末尾に **permit ip any any capture** を挿入します。

センサーが起動すると、2 つの VACL の内容を読み取ります。センサーは次のエントリから成る 3 つ目の VACL を作成します。

- センサーの IP アドレスに対する **permit** 行
- Pre-Block VACL のすべての設定行のコピー
- センサーによってブロックされている各アドレスの **deny** 行
- Post-Block VACL のすべての設定行のコピー

センサーは新しい VACL を指定された VLAN に適用します。

（注）　新しい VACL がスイッチの VLAN に適用されると、その VLAN に対する他の VACL の適用は無効になります。

詳細情報

ルータ ACL を使用したブロッキングについては、「ルータ ブロッキング デバイスおよびレート制限デバイスのインターフェイスの設定」（P.15-21）を参照してください。

[Cat 6K Blocking Device Interfaces] ペインのフィールド定義

[Cat 6K Blocking Device Interfaces] ペインには次のフィールドがあります。

- [Cat 6K Blocking Device] : Catalyst 6500 シリーズ スイッチ ブロッキング デバイスの IP アドレス。
- [VLAN ID] : Catalyst 6500 シリーズ スイッチ ブロッキング デバイスで使用する VLAN ID。値は 1 ～ 4094 です。
- [Pre-Block VACL] : ブロッキング VACL の前に適用する VACL。値は 0 ～ 64 文字です。
- [Post-Block VACL] : ブロッキング VACL の後に適用する VACL。値は 0 ～ 64 文字です。

（注）　Post-Block VACL を Pre-Block VACL と同じものにすることはできません。

[Add Cat 6K Blocking Device Interface] および [Edit Cat 6K Blocking Device Interface] ダイアログボックスのフィールド定義

[Add Cat 6K Blocking Device Interface] および [Edit Cat 6K Blocking Device Interface] ダイアログボックスには次のフィールドがあります。

- [Cat 6K Blocking Device] : Catalyst 6500 シリーズ スイッチ ブロッキング デバイスの IP アドレス。
- [VLAN ID] : Catalyst 6500 シリーズ スイッチ ブロッキング デバイスで使用する VLAN ID。値は 1 ～ 4094 です。
- [Pre-Block VACL] : ブロッキング VACL の前に適用する VACL。値は 0 ～ 64 文字です。
- [Post-Block VACL] : ブロッキング VACL の後に適用する VACL。値は 0 ～ 64 文字です。

（注）　Post-Block VACL を Pre-Block VACL と同じものにすることはできません。

Cat 6K のブロッキング デバイス インターフェイスの設定

Catalyst 6500 シリーズ スイッチ ブロッキング デバイス インターフェイスを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Management] > [Blocking] > [Cat 6K Blocking Device Interfaces] を選択し、[Add] をクリックして、Catalyst 6500 シリーズ スイッチ ブロッキング デバイス インターフェイスを追加します。

ステップ 3　[Cat 6K Blocking Device] ドロップダウン リストから、Catalyst 6500 シリーズ スイッチの IP アドレスを選択します。

ステップ 4　[VLAN ID] フィールドに VLAN ID を入力します。

ステップ 5　（任意）[Pre-Block VACL] フィールドに Pre-Block VACL の名前を入力します。

ステップ 6　（任意）[Post-Block VACL] フィールドに Post-Block VACL の名前を入力します。

ヒント　変更を破棄して [Add Cat 6K Blocking Device Interface] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 7　[OK] をクリックします。IP アドレスと VLAN の組み合わせがすでに存在している場合は、エラー メッセージが表示されます。新しいインターフェイスが [Cat 6K Blocking Device Interfaces] ペインのリストに表示されます。

ステップ 8　Catalyst 6500 シリーズ スイッチ ブロッキング デバイス インターフェイス リストの既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 9　必要に応じて、VLAN ID を編集します。

ステップ 10　必要に応じて、Pre-Block VACL の名前を編集します。

ステップ 11　必要に応じて、Post-Block VACL の名前を編集します。

ヒント　変更を破棄して [Edit Cat 6K Blocking Device Interface] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 12　[OK] をクリックします。編集した Catalyst 6500 シリーズ スイッチ ブロッキング デバイス インターフェイスが [Cat 6K Blocking Device Interfaces] ペインのリストに表示されます。

ステップ 13　リストから Catalyst 6500 シリーズ スイッチ ブロッキング デバイス インターフェイスを削除するには、そのインターフェイスを選択し、[Delete] をクリックします。その Catalyst 6500 シリーズ スイッチ ブロッキング デバイス インターフェイスは、[Cat 6K Blocking Device Interfaces] ペインのリストに表示されなくなります。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 14　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

マスター ブロッキング センサーの設定

ここでは、マスター ブロッキング センサーの設定方法について説明します。内容は次のとおりです。

[Master Blocking Sensor] ペイン

（注）　マスター ブロッキング センサーを設定するには、管理者またはオペレータであることが必要です。

[Master Blocking Sensor] ペインで、ブロッキング デバイスの設定に使用するマスター ブロッキング センサーを指定します。

マスター ブロッキング センサーについて

複数のセンサー（ブロッキング転送センサー）が、1 つ以上のデバイスを制御する、指定したマスター ブロッキング センサーに、ブロッキング要求を転送できます。マスター ブロッキング センサーは、他の 1 つ以上のセンサーに代わって 1 つ以上のデバイスでブロッキングを制御するセンサーで実行されている ARC です。マスター ブロッキング センサー上の ARC は、他のセンサーで実行されている ARC の要求に応じて、デバイスのブロッキングを制御します。マスター ブロッキング センサーは、レート制限を転送することもできます。

注意　2 つのセンサーが同じデバイスでブロッキングまたはレート制限を制御することはできません。この状況が必要な場合は、一方のセンサーをマスター ブロッキング センサーとして設定してデバイスを管理し、もう一方のセンサーでマスター ブロッキング センサーに要求を転送できます。

マスター ブロッキング センサーを追加する場合は、センサーあたりのブロッキング デバイス数を減らします。たとえば、それぞれ 1 つのブロッキング インターフェイス/方向を持つ 10 個のファイア ウォールと 10 台のルータでブロックする場合は、センサーに 10 個を割り当て、マスター ブロッキング センサーに残りの 10 個を割り当てることができます。

ブロッキング転送センサーで、マスター ブロッキング センサーとして機能するリモート ホストを識別します。マスター ブロッキング センサーでは、ブロッキング転送センサーをアクセス リストに追加する必要があります。

マスター ブロッキング センサーが Web 接続に TLS を必要とする場合は、マスター ブロッキング センサー リモート ホストの X.509 証明書を受け入れるようにブロッキング転送センサーの ARC を設定する必要があります。センサーでは TLS がデフォルトでイネーブルになりますが、このオプションは変更できます。

（注）　通常、マスター ブロッキング センサーはネットワーク デバイスを管理するように設定します。ブロッキング転送センサーは、通常は他のネットワーク デバイスを管理するようには設定されていませんが、これを行うことは可能です。

ブロッキングやレート制限用に設定されたデバイスが存在しない場合でも、ブロッキングまたはレート制限を実行するように設定されたセンサーは、ブロッキング要求またはレート制限要求をマスター ブロッキング センサーに転送できます。ブロッキングまたはレート制限要求がイベント アクションとして設定されているシグニチャが起動した場合、センサーはブロック要求またはレート制限要求をマスター ブロッキング センサーに転送し、そのセンサーがブロックまたはレート制限を実行します。

注意　1 つのセンサーだけがデバイス上のすべてのブロッキング インターフェイスを制御する必要があります。

[Master Blocking Sensor] ペインのフィールド定義

[Master Blocking Sensor] ペインには次のフィールドがあります。

- [IP Address] : マスター ブロッキング センサーの IP アドレス。
- [Port] : マスター ブロッキング センサーへの接続に使用するポート。デフォルトは 443 です。
- [Username] : マスター ブロッキング センサーへのログインに使用するユーザ名。ユーザ名は、^[A-Za-z0-9()+:,_/-]+$ の形式で入力します。ユーザ名は、文字または数字で始まり、A ～ Z（大文字または小文字）、0 ～ 9 の数字、「-」および「_」を含み、長さが 1 ～ 64 文字であることが必要です。
- [TLS Used] : TLS を使用するかどうか。

[Add Master Blocking Sensor] および [Edit Master Blocking Sensor] ダイアログボックスのフィールド定義

[Add Master Blocking Sensor] および [Edit Master Blocking Sensor] ダイアログボックスには次のフィールドがあります。

- [IP Address] : マスター ブロッキング センサーの IP アドレス。すでに存在する IP アドレスを入力すると、警告が表示されます。
- [Port (optional)] : マスター ブロッキング センサーへの接続に使用するポート。デフォルトは 443 です。
- [Username] : マスター ブロッキング センサーへのログインに使用するユーザ名。ユーザ名は、^[A-Za-z0-9()+:,_/-]+$ の形式で入力します。ユーザ名は、文字または数字で始まり、A ～ Z（大文字または小文字）、0 ～ 9 の数字、「-」および「_」を含み、長さが 1 ～ 64 文字であることが必要です。
- [Change the password] : パスワードを変更するかどうか。
- [New Password] : マスター ブロッキング センサーへのログインに使用するログイン パスワード。
- [Confirm Password] : 確認のためにログイン パスワードを再入力します。
- [Use TLS] : TLS を使用するかどうか。

マスター ブロッキング センサーの設定

マスター ブロッキング センサーを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Management] > [Blocking] > [Master Blocking Sensor] を選択し、[Add] をクリックして、マスター ブロッキング センサーを追加します。

ステップ 3　[IP Address] フィールドには、マスター ブロッキング センサーの IP アドレスを入力します。

ステップ 4　（任意）[Port] フィールドにポート番号を入力します。デフォルトは 443 です。

ステップ 5　[Username] フィールドにユーザ名を入力します。

ステップ 6　[New Password] フィールドに、ユーザのパスワードを入力します。

ステップ 7　確認のために [Confirm New Password] フィールドにもう一度パスワードを入力します。

ステップ 8　[TLS] チェックボックスをオンにします。

ヒント　変更内容を破棄して [Add Master Blocking Sensor] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 9　[OK] をクリックします。IP アドレスがすでに追加されている場合は、エラー メッセージが表示されます。新しいマスター ブロッキング センサーが [Master Blocking Sensor] ペインのリストに表示されます。

ステップ 10　TLS を選択した場合は、マスター ブロッキング センサー リモート ホストの TLS/SSL X.509 証明書を受け入れるようにブロッキング転送センサーの ARC を設定する必要があります。

（注）　[Configuration] > *sensor_name* > [Sensor Management] > [Certificates] > [Trusted Hosts] > [Add Trusted Host] を選択して、X.509 証明書を受け入れるようにブロッキング転送センサーを設定することもできます。

a.　管理者権限を持つアカウントを使用してブロッキング転送センサーの CLI にログインします。

b.　グローバル コンフィギュレーション モードを開始します。

```
sensor# configure terminal
```

c.　信頼できるホストを追加します。

```
sensor(config)# tls trusted-host ip-address master_blocking_sensor_ip_address
```

信頼できるホストの追加を確認するように求めるメッセージが表示されます。

```
Would you like to add this to the trusted certificate table for this host?[yes]:
```

d.　**yes** と入力してホストを追加します。

e.　グローバル コンフィギュレーション モードと CLI を終了します。

```
sensor(config)# exit
sensor# exit
```

（注） 証明書のフィンガープリントに基づいて証明書を受け入れるように要求されます。センサーが提供するのは、自己署名証明書（認識された認証局の署名がある証明書ではなく）だけです。ホスト センサーにログインし、**show tls fingerprint** コマンドを入力して、ホスト証明書のフィンガープリントが一致することを確認することによって、マスター ブロッキング センサーのホスト センサー証明書を検証できます。

ステップ 11　マスター ブロッキング センサー リストの既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 12　（任意）ポートを編集します。

ステップ 13　必要に応じて、ユーザ名を編集します。

ステップ 14　このユーザのパスワードを変更するには、[Change the password] チェックボックスをオンにします。

a.　[New Password] フィールドに新しいパスワードを入力します。

b.　確認のために [Confirm New Password] フィールドに新しいパスワードをもう一度入力します。

ステップ 15　必要に応じて、[TLS] チェックボックスをオンまたはオフにします。

ヒント　変更内容を破棄して [Edit Master Blocking Sensor] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 16　[OK] をクリックします。編集したマスター ブロッキング センサーが [Master Blocking Sensor] ペインのリストに表示されます。

ステップ 17　リストからマスター ブロッキング センサーを削除するには、そのマスター ブロッキング センサーを選択し、[Delete] をクリックします。そのマスター ブロッキング センサーは、[Master Blocking Sensor] ペインのリストに表示されなくなります。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 18　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。