CHAPTER 13

アクセス コントロール ポリシーの使用

*アクセス コントロール ポリシー*は、ネットワーク上の非高速パスを通るトラフィックを、システムでどのように処理するかを決定します。ユーザは 1 つ以上のアクセス コントロール ポリシーを設定して、設定したポリシーを 1 つ以上の管理対象デバイスに適用できます。各デバイスに同時に適用できるポリシーは 1 つだけです。

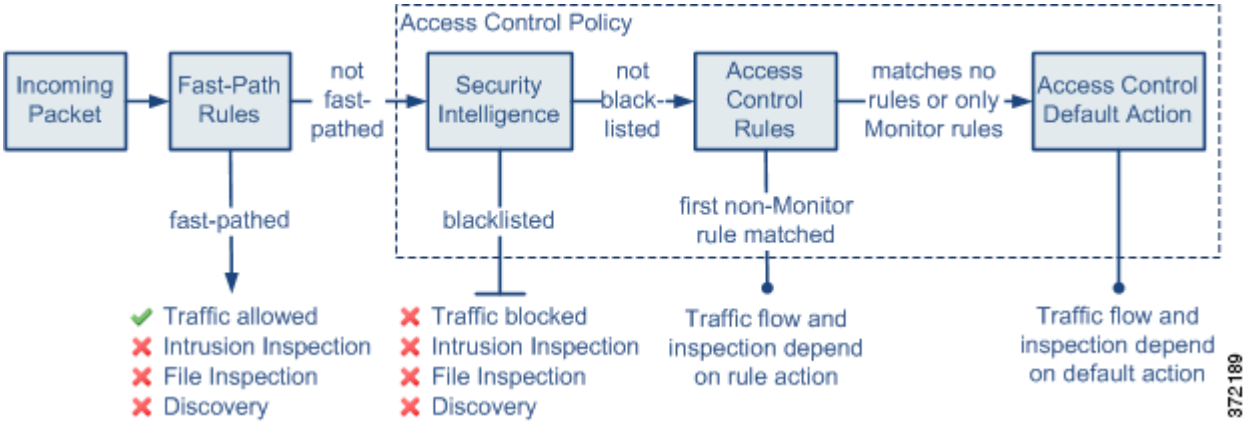
単純なアクセス コントロール ポリシーで、セキュリティ インテリジェンス データに基づいてトラフィックをフィルタリング（ブラックリスト登録またはモニタ）してから、ポリシーの*デフォルト アクション*を使用して、ブラックリスト登録されていないトラフィックを次のいずれかの方法で処理できます。

- すべてのトラフィックをネットワークからブロックする
- ネットワークに入ってくるすべてのトラフィックを信頼し、それ以降のインスペクションを行わない
- すべてのトラフィックがネットワークに入ることを許可し、ネットワーク検出ポリシーのみを使用してトラフィックのインスペクションを行う
- すべてのトラフィックがネットワークに入ることを許可し、侵入ポリシーおよびネットワーク検出 ポリシーを使用してトラフィックのインスペクションを行う

オプションで、ポリシーに*アクセス コントロール ルール*を追加して、ネットワーク トラフィックを処理してログに記録する方法を詳細に制御することができます。ルールごとに、ルールの*アクション*を指定します。つまり、トラフィックを信頼するか、モニタするか、ブロックするか、あるいは侵入ポリシーまたはファイル ポリシーを使用して、一致するトラフィックのインスペクションを行うかを指定します。各ルールには、制御する特定のトラフィックを識別するための一連の条件を含めます。ルールは単純なものにすることも、セキュリティ ゾーン、ネットワーク、VLAN、送信元または宛先の国/大陸、Active Directory LDAP ユーザ/グループ、アプリケーション、トランスポート プロトコル ポート、または URL の任意の組み合わせでトラフィックを照合する複雑なものにすることもできます。

システムはトラフィックをアクセス コントロール ルールと順番に照合し、最初に一致したルールでトラフィックを処理します。(モニタ ルールの場合は例外です。この場合は、トラフィックが引き続き評価されます)。

次の図に、FireSIGHT システムでのトラフィック フローを示し、それぞれのトラフィックに対して実行されるインスペクションのタイプを明記します。システムは、高速パスを通るトラフィックやブラックリスト登録されたトラフィックには、インスペクションを行わないことに注意してください。アクセス コントロール ルールまたはデフォルト アクションによって処理されるトラフィックの場合、使用されるルールのによって、フローとインスペクションが変わってきます。簡潔にするために、この図にはルールのアクションを示していませんが、信頼またはブロックされたトラフィックに対しては、システムはいかなる種類のインスペクションも行いません。さらに、デフォルト アクションでファイル インスペクションを行うことはできません。



この章では、基本的なアクセス コントロール ポリシー（セキュリティ インテリジェンスによるフィルタリングを含む）を作成し、そのポリシーにルールを追加する方法を説明します。FireSIGHT システムの関連コンポーネントの詳細については、次のマニュアルを参照してください。

- 「Fast-Path ルールの設定」（P.6-54）
- 「アクセス コントロール ルールの概要と作成」（P.14-1）
- 「ファイル ポリシーの概要と作成」（P.33-10）
- 「侵入ポリシーの設定」（P.20-1）
- 「ネットワーク検出の概要」（P.35-1）

アクセス コントロール ポリシーは、防御センターでのライセンスに関係なく作成できます。ただし、アクセス コントロールのある側面では、ポリシーを適用する前にターゲット デバイスで特定のライセンス交付対象の機能を有効化する必要があります。また、一部の機能は、特定のアプライアンス モデルでのみ使用できます。防御センターでは、ご使用の展開環境でサポートされない機能を示すために、警告アイコン（⚠）および確認ダイアログ ボックスを使用します。警告アイコンの上にポインタを置くと詳細が表示されます。

次の表に、アクセス コントロール ポリシーを適用する際のライセンスおよびアプライアンス モデル要件を記載します。シリーズ 2 デバイスは、ほとんどのProtection機能を自動的に有効にするため、デバイスで明示的にProtectionを有効にする必要はありません。

表 13-1　アクセス コントロールのためのライセンスおよびアプライアンスの要件

適用するポリシー	追加する必要のあるライセンス	追加先となる防御センター	それを以下のデバイスで有効にする
ゾーン、ネットワーク、VLAN、またはポートに基づいてアクセス コントロールを実行するポリシー、またはリテラル URL と URL オブジェクトを使用して URL フィルタリングを実行するポリシー	任意	任意	任意：例外として、シリーズ 2 デバイスではリテラル URL と URL オブジェクトを使用した URL フィルタリングを実行できません。また、ASA FirePOWER デバイスでは、VLAN タグ条件を使用してトラフィックを識別することはできません。
侵入検知および侵入防御、ファイル コントロール、またはセキュリティ インテリジェンス フィルタリングを実行するポリシー	Protection	任意	任意：例外として、シリーズ 2 デバイスではセキュリティ インテリジェンス フィルタリングを実行できません。
高度なマルウェア対策としてネットワークベースのマルウェア検出およびブロッキングを実行するポリシー	Malware	任意 DC500 を除く	シリーズ 3、仮想、X シリーズ、ASA FirePOWER
ユーザ制御またはアプリケーション制御を実行するポリシー	Control	任意：例外として、DC500 ではユーザ制御を実行できません。	シリーズ 3、仮想、X シリーズ、ASA FirePOWER
ジオロケーション データ（発信元または宛先の国/大陸）に基づいてアクセス コントロールを実行するポリシー	FireSIGHT	任意 DC500 を除く	シリーズ 3、仮想、ASA FirePOWER
カテゴリとレピュテーション データを使用して URL フィルタリングを実行するポリシー	URL Filtering	任意 DC500 を除く	シリーズ 3、仮想、X シリーズ、ASA FirePOWER

アクセス コントロール ポリシーの作成および管理の詳細については、次の項を参照してください。

- 「ポリシーの設定」（P.13-4）
- 「ポリシー内でのルールの編成」（P.13-25）
- 「アクセス コントロール ポリシーの管理」（P.13-31）

ポリシーの設定

ライセンス：任意

アクセス コントロール ポリシーを設定するには、ポリシーに一意の名前を付け、デフォルト アクションを指定し、ポリシーを適用するデバイス（つまり、*ターゲット*）を識別する必要があります。

次のことも実行できます。

- トラフィックに任意のアクセス コントロール ルールによるインスペクションを行う前に、セキュリティ インテリジェンス データに基づいてトラフィックをブラックリスト登録（それ以上のインスペクションをせずに拒否すること）し、またオプションで、同じデータに基づいてトラフィックをモニタする
- アクセス コントロール ルールを追加、編集、削除、有効化/無効化する
- アクセス コントロール ルールによって HTTP 要求がブロックされたときにユーザに表示される、HTTP ページ（*HTTP 応答*ページと呼ばれます）を設定する
- 詳細設定（接続イベントに格納する URL の文字数、ファイルおよびマルウェアのインスペクションの詳細度や期間、インタラクティブにブロックされたセッションのバイパス期間など）を行う
- デフォルト アクションによって処理されたトラフィックのログを記録する

アクセス コントロール ポリシーを作成または変更した後、そのポリシーをターゲット デバイスのすべて、または一部に適用できます。カスタム ユーザ プロファイルを作成して、ユーザーごとに、ポリシーの設定、編成、適用のための異なる権限を割り当てることもできます。

次の表に、ポリシーの [編集] ページで実行できる設定操作を要約します。

表 13-2　アクセス コントロール ポリシーの設定操作

目的	操作
ポリシーの名前または説明を変更する	[Name] フィールドまたは [Description] フィールドをクリックして、必要に応じて文字を削除し、新しい名前または説明を入力します。
デフォルト アクションを設定する	詳細については、「デフォルト アクションの設定」（P.13-5）を参照してください。
デフォルト アクションの接続をログに記録する	詳細については、「デフォルト アクションの接続のロギング」（P.13-8）を参照してください。
ユーザごとに異なる権限を割り当てる	詳細については、「アクセス コントロール ポリシーでのカスタム ユーザ ロールの使用」（P.13-9）を参照してください。
ポリシーの適用対象を管理する	詳細については、「ポリシー ターゲットの管理」（P.13-10）を参照してください。
ポリシーの変更を保存する	[Save] をクリックします。
ポリシーを保存し、適用する	[Save and Apply] をクリックします。詳細については、「アクセス コントロール ポリシーの適用」（P.13-39）を参照してください。 **ヒント**　[Access Control] ページで、ポリシーの横にある編集アイコン（）をクリックするという方法もあります。
ポリシーの変更をキャンセルする	[Cancel] をクリックします。変更を行った場合は、次に [OK] をクリックします。

表 13-2　アクセス コントロール ポリシーの設定操作（続き）

目的	操作
ポリシーにルールを追加する	[Add Rule] をクリックします。詳細については、「アクセス コントロール ルールの概要と作成」（P.14-1）を参照してください。 **ヒント**　ルールの行の空白部分を右クリックし、[Insert new rule] を選択するという方法もあります。
既存のルールを編集する	ルールの横にある編集アイコン（  ）をクリックします。詳細については、「アクセス コントロール ルールの作成と編集」（P.14-3）を参照してください。 **ヒント**　ルールを右クリックして、[Edit] を選択することもできます。
ルールを削除する	ルールの横にある削除アイコン（  ）をクリックし、[OK] をクリックします。 **ヒント**　選択したルールの行の空白部分を右クリックして [Delete] を選択した後、[OK] をクリックして、選択した 1 つ以上のルールを削除するという方法もあります。
既存のルールを有効または無効にする	選択したルールを右クリックして [State] を選択した後、[Disable] または [Enable] を選択します。無効なルールはグレーで表示され、ルール名の下に [(disabled)] というマークが付きます。
特定のルール属性の設定ページを表示する	ルールの行で、該当する条件のカラムに示されている名前、値、またはアイコンをクリックします。たとえば、[Source Networks] カラムに示されている名前または値をクリックすると、選択したルールの [Networks] ページが表示されます。詳細については、「さまざまな条件タイプを使用する」（P.14-17）を参照してください。
ブロックされた HTTP 要求に対する応答ページを設定する	詳細については、「HTTP 応答ページの追加」（P.13-12）を参照してください。
セキュリティ インテリジェンス データに基づいてトラフィックをフィルタリングする	詳細については、「セキュリティ インテリジェンス データに基づくトラフィックのフィルタリング」（P.13-13）を参照してください。
詳細設定を行う	詳細については、「アクセス コントロール ポリシーの詳細設定」（P.13-21）を参照してください。

デフォルト アクションの設定

ライセンス：任意

アクセス コントロール ポリシーのデフォルト アクションは、次のトラフィックをシステムで処理する方法を決定します。

- セキュリティ インテリジェンスによってブラックリスト登録されていないトラフィック
- ポリシーに含まれる非モニタ ルールのいずれにも一致しないトラフィック

アクセス コントロール ルールまたはセキュリティ インテリジェンス設定がまったく含まれていないアクセス コントロール ポリシーを適用する場合、デフォルト アクションが、ネットワーク上のすべてのトラフィックの処理方法を決定します。

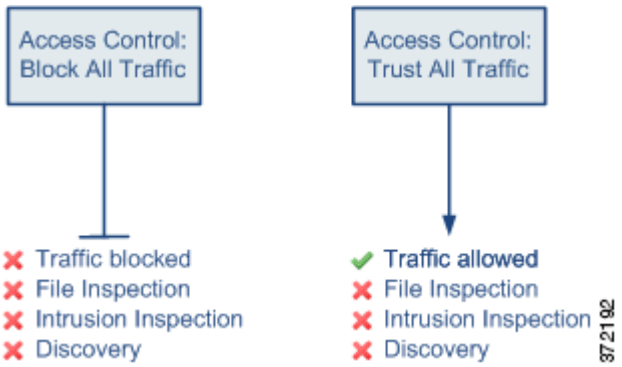
次の表に、選択可能なデフォルト アクションとそれがトラフィックに対して行う処理、および各オプションで処理されたトラフィックに実行されるインスペクションのタイプをリストします。

:

表 13-3　アクセス コントロール ポリシーのデフォルト アクション

デフォルト アクション	トラフィックに対して行う処理	インスペクション
Access Control: Block All Traffic	それ以上のインスペクションは行わずにブロックする。	なし
Access Control: Trust All Traffic	信頼する（それ以上のインスペクションを行わずに許可する）	なし
Network Discovery Only	許可	ネットワーク検出
Intrusion Prevention	ユーザが指定した侵入ポリシーに合格する限り、許可する	侵入およびネットワーク検出

次の図は、アクセス コントロールのブロックおよび信頼のデフォルト アクションを説明しています。デフォルト アクションでブロックまたは信頼されたトラフィックに対しては、システムはいかなる種類のインスペクションも行わないことに注意してください。

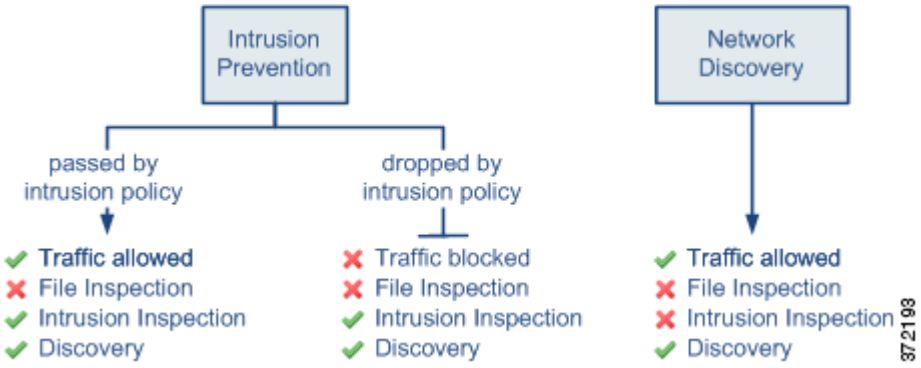


デフォルト アクションで処理されるトラフィックに対して、ネットワーク検出または侵入ポリシー、あるいはその両方でインスペクションを行うようにデフォルト アクションを設定することもできます。侵入検知もアクセス コントロールも実行しない場合、デフォルト アクションとして [Network Discovery Only] 選択すると、防御センターのパフォーマンスが向上します。このパフォーマンス向上を生かすには、アクセス コントロール ルールで、アプリケーション、ユーザ、または URL の条件や、ファイル インスペクションまたは侵入インスペクションのオプションが使用されないようにする必要があります。

注　[Network Discovery Only] をデフォルト アクションとして選択しても、検出インスペクションが自動的に保証されるわけではありません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。詳細については、「ネットワーク検出の概要」（P.35-1）を参照してください。

デフォルト アクションで処理されるトラフィックに、侵入ポリシーでのインスペクションを行う場合、ネットワーク検出ポリシーの設定によっては、システムによってさらにネットワーク検出を使用したインスペクションも行われる場合があります。侵入ポリシーとアクセス コントロール ルールの関連付けについては、「侵入ポリシーとアクセス コントロール ルール」（P.14-37）を参照してください。

次の図は、[Intrusion Prevention] および [Network Discovery Only] のデフォルト アクションを説明しています。ファイル インスペクションはアクセス コントロール ルールでサポートされていますが、デフォルト アクションで処理されるトラフィックに対してファイル インスペクションを実行することはできません。



次の手順で、ポリシーの編集の際にアクセス コントロール ポリシーのデフォルト アクションを設定する方法を説明します。アクセス コントロール ポリシーを編集する詳細な手順については、「アクセス コントロール ポリシーの編集」（P.13-34）を参照してください。

アクセス コントロール ポリシーのデフォルト アクションを設定する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

ポリシーの [Edit] ページが表示されます。

ステップ 3　[Default Action] を選択します。

- すべてのトラフィックをブロックする場合は、[Access Control: Block All Traffic] を選択します。
- すべてのトラフィックを信頼する場合は、[Access Control: Trust All Traffic] を選択します。
- すべてのトラフィックを許可し、ネットワーク検出を使用してインスペクションする場合は、[Network Discovery Only] を選択します。
- すべてのトラフィックをネットワーク検出と侵入ポリシーの両方を使用してインスペクションする場合は、侵入ポリシーを選択します。侵入ポリシーは、いずれもIntrusion Prevention というラベルで始まります。侵入ポリシーによってトラフィックがブロックされる可能性があることに注意してください。

  デフォルトでは、侵入ポリシーはデフォルトの変数セットを使用します。侵入ポリシーで使用する変数セットを変更する方法については、「アクセス コントロール ポリシーの詳細設定」（P.13-21）の「**デフォルト アクションの変数セット**」を参照してください。

注意　シスコの担当者から指示された場合を除き、`Experimental Policy 1` は使用**しないで**ください。シスコでは、試験用にこのポリシーを使用します。

ステップ 4　次の項「デフォルト アクションの接続のロギング」の説明に従って、デフォルト アクションのロギング オプションを設定します。

デフォルト アクションの接続のロギング

ライセンス：任意

デフォルト アクションによって処理されたトラフィックの接続データをログに記録するかどうかを決定する必要があります。ポリシーのデフォルト アクションによって処理された接続のロギング オプションは、個々のアクセス コントロール ルールによって処理された接続のロギング オプションとほとんど同じです。ただし、次の違いがあります。

- デフォルト アクションにはファイル ロギング オプションがありません。デフォルト アクションを使用してファイル制御やマルウェア保護を実行することはできないためです。
- アクセス コントロールのデフォルト アクションに関連付けられた侵入ポリシーによって侵入イベントが生成された場合、システムは、そのイベントに関連する接続の終了を自動的にログに記録**しません**。このことは、接続データをログに記録する必要がない、侵入検知および侵入防御専用の展開環境に役立ちます。

  ただし例外として、デフォルト アクションの接続開始ロギングを有効にした場合はその限りではありません。この場合、関連付けられた侵入ポリシーがトリガーされると、システムは接続の開始だけでなく、接続の終了もログに記録**します**。

接続のロギングの詳細については、「接続、ファイル、マルウェアに関する情報のロギング」（P.14-39）を参照してください。

一般に、接続データに関する何らかの詳細な分析を実行する場合は、接続の終了をログに記録する必要があります。カスタム ワークフローに接続の要約を表示する場合、接続データをグラフ形式で表示する場合、またはトラフィック プロファイルを作成して使用する場合は、接続終了時の接続イベントをログに記録することが**必須**となります。Block All Traffic がデフォルト アクションの場合、トラフィックが拒否されて、それ以上のインスペクションは行われないため、接続開始イベントだけをログに記録するので構いません。

接続イベントを防御センターデータベースに記録すると、FireSIGHT システムでの分析、レポート作成、および相関の機能を活用できます。また、syslog または SNMP トラップ サーバにほとんどの接続イベントを送信できます。

次の手順で、接続をログに記録するようにアクセス コントロール ポリシーを設定する方法を説明します。アクセス コントロール ポリシーを編集する詳細な手順については、「アクセス コントロール ポリシーの編集」（P.13-34）を参照してください。

デフォルト アクションによって処理されたトラフィックの接続をログに記録する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（  ）をクリックします。

ポリシーの [Edit] ページが表示されます。

ステップ 3　[Default Action] ドロップダウン リストの横にあるロギング アイコン（  ）をクリックします。

[Logging] ポップアップ ウィンドウが表示されます。

ステップ 4　接続の開始/終了時点でのロギングを示す [Log at Beginning of Connection] または [Log at End of Connection] を選択します。

ブロックされたトラフィックの接続終了イベントをログに記録することはできません。

ステップ 5　接続イベントの送信先を指定します。次の選択肢があります。

- 接続イベントを防御センターに送信する場合は、[防御センター] を選択します。
- 接続イベントを Syslog に送信するには、[Syslog] を選択して、ドロップダウン リストから Syslog アラート応答を 1 つ選択します。オプションで、追加アイコン（  ）をクリックすることで、syslog アラート応答を設定できます。「Syslog アラート応答の作成」（P.15-5）を参照してください。
- 接続イベントを SNMP トラップ サーバに送信する場合は、[SNMP Trap] を選択し、ドロップダウン リストから SNMP アラート応答を選択します。オプションで、追加アイコン（  ）をクリックすることで、SNMP アラート応答を設定できます。「SNMP アラート応答の作成」（P.15-4）を参照してください。

ステップ 6　変更を保存します。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（「アクセス コントロール ポリシーの適用」（P.13-39）を参照してください）。

アクセス コントロール ポリシーでのカスタム ユーザ ロールの使用

ライセンス：任意

「カスタム ユーザ ロールの管理」（P.48-55）で説明しているように、カスタム ユーザ ロールを作成して専用のカスタム特権を割り当てることができます。カスタム ユーザ ロールには、メニュー ベースのシステム権限の任意のセットを割り当てることができます。また、カスタム ユーザ ロールは、完全にオリジナルなものを作成することも、事前定義されたユーザー ロールを基に作成することもできます。アクセス コントロール関連の機能に対するカスタム ロールにより、ユーザがアクセス コントロール ポリシー、侵入ポリシー、ファイル ポリシーを表示、変更、適用できるかどうか、また、管理者ルール カテゴリまたは root ルール カテゴリのルールを挿入または変更できるかどうかが決まります。

次の表に、FireSIGHT システム ユーザが操作できるアクセス コントロール関連の機能を決定する、5 つのカスタム ロールの例を記載します。この表には、各カスタム ロールに必要な権限が、カスタム ユーザ ロール を作成するときに表示される順でリストされています。

表 13-4　　アクセス コントロールのカスタム ロールの例

カスタム ロールの権限	アクセス コントロールの編集	侵入の編集	ファイル ポリシーの編集	ポリシーの適用（すべて）	侵入ポリシーの適用
アクセス コントロール	はい	いいえ	いいえ	はい	はい
アクセス コントロール リスト	はい	いいえ	いいえ	はい	はい
アクセス コントロール ポリシーの変更	はい	いいえ	いいえ	いいえ	いいえ
侵入ポリシーの適用	いいえ	いいえ	いいえ	はい	はい
アクセス コントロール ポリシーの適用	いいえ	いいえ	いいえ	はい	いいえ
侵入	いいえ	はい	いいえ	いいえ	いいえ
侵入ポリシー	いいえ	はい	いいえ	いいえ	いいえ
侵入ポリシーの変更	いいえ	はい	いいえ	いいえ	いいえ
ファイル ポリシー	いいえ	いいえ	はい	いいえ	いいえ
ファイル ポリシーの変更	いいえ	いいえ	はい	いいえ	いいえ

システムがレンダリングする Web インターフェイスは、ユーザーがアクセス コントロール ポリシーと侵入ポリシーの両方を適用できるのか、侵入ポリシーだけを適用できるのか、あるいはいずれも適用できないのかによって、異なることに注意してください。たとえば、上記の表の「侵入ポリシーの適用」が可能なユーザには、アクセス コントロール ポリシーの表示と侵入ポリシーの適用が許可されますが、アクセス コントロール ポリシー /侵入ポリシーの編集、アクセス コントロール ポリシーの適用、ファイル ポリシーの表示は許可されません。Web インターフェイスは、次のようになります。

- [Access Control] ページで、編集アイコン（）が非表示になる
- [Access Control] ページで、削除アイコン（）が非表示になる
- クイック適用のポップアップ ウィンドウが、侵入ポリシーだけに適用される
- 詳細適用ポップアップ ウィンドウで、アクセス コントロール ポリシーのチェック ボックスが無効になる

ポリシー ターゲットの管理

ライセンス：任意

アクセス コントロール ポリシーを適用するには、その前に、ポリシーを適用する管理対象デバイス（デバイス グループを含む）を特定する必要があります。ポリシーを適用する管理対象デバイスは、ポリシーを作成または編集する際に特定できます。使用可能なデバイスのリストを検索し、選択済みデバイスのリストにデバイスを追加できます。選択済みデバイスをドラッグ アンド ドロップしたり、2 つのリストの間にあるボタンを使用してデバイスを追加したりできます。

異なるバージョンの FireSIGHT システムを実行中のスタック デバイスをターゲットにすることはできません（たとえば、デバイスのいずれかでのアップグレードが失敗します）。デバイス スタックをターゲットにすることはできますが、スタック内の個々のデバイスをターゲットにすることはできません。詳細については、「スタックに含まれるデバイスの管理」（P.6-40）を参照してください。

次の表では、対象のデバイスを管理する場合に実行可能な操作の概要を説明しています。

表 13-5　対象のデバイス管理アクション

目的	操作
使用可能なデバイスのリストを検索する	検索フィールド内をクリックし、検索文字列を入力します。検索文字列を入力すると、デバイスのリストが更新されて、検索文字列に一致するデバイス名が表示されます。
使用可能なデバイスの検索をクリアする	検索フィールドのクリア アイコン（）をクリックします。
使用可能なデバイスを選択し、選択済みターゲットのリストに追加する	デバイス名をクリックします。複数のデバイスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。 ヒント　使用可能なデバイスを右クリックして、[Select All] をクリックするという方法もあります。

表 13-5　対象のデバイス管理アクション（続き）

目的	操作
選択したデバイスを追加する	[Add to Policy] をクリックします。 **ヒント**　選択済みデバイスのリストにドラッグ アンド ドロップするという方法もあります。
選択済みデバイスのリストから単一のデバイスを削除する	デバイスの横にある削除アイコン（）をクリックします。 **ヒント**　デバイスを右クリックして、[Delete] を選択するという方法もあります。
選択済みデバイスのリストから複数のデバイスを削除する	Ctrl キーまたは Shift キーを押しながらクリックして複数のデバイスを選択し、選択したデバイスの行を右クリックで強調表示してから、[Delete Selected] をクリックします。
設定を保存する	[OK] をクリックします。
変更を保存せずに設定を廃棄する	[Cancel] をクリックします。

次の手順で、アクセス コントロール ポリシーを設定してターゲット デバイスを管理する方法を説明します。アクセス コントロール ポリシーを編集する詳細な手順については、「アクセス コントロール ポリシーの編集」（P.13-34）を参照してください。

アクセス コントロール ポリシーのターゲット デバイスを管理する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

ポリシーの [Edit] ページが表示されます。

ステップ 3　デバイス ターゲットのリンクをクリックし、[Manage Targets] をクリックします。

[Manage Device Targets] ポップアップ ウィンドウが表示されます。

ステップ 4　オプションで、[Available Devices] リストの上にある [Search] プロンプトをクリックして、名前を入力します。

検索文字列を入力すると、リストが更新されて、検索文字列に一致するデバイスが表示されます。クリア アイコン（）をクリックすることで、リストをクリアできます。

ステップ 5　追加するデバイスまたはデバイス グループをクリックします。複数のデバイスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。

ヒント　使用可能なデバイスを右クリックして、[Select All] をクリックするという方法もあります。

ステップ 6　[Add to Policy] をクリックします。

選択したデバイスが追加されます。

ヒント　ドラッグ アンド ドロップを使用することもできます。

ステップ 7　オプションで、削除アイコン（ ）をクリックして、選択済みデバイスのリストからデバイスを削除します。または、Ctrl キーまたは Shift キーを押しながらクリックして複数のデバイスを選択し、選択したデバイスを右クリックして [Delete Selected] を選択します。

ステップ 8　設定を保存するには [OK] をクリックし、設定を破棄するには [Cancel] をクリックします。

[OK] をクリックすると、設定がポリシーに追加され、ポリシーの [Edit] ページが表示されます。

HTTP 応答ページの追加

ライセンス：FireSIGHT

アクセス コントロール ルールによってユーザの HTTP 要求がブロックされたときに、ユーザの Web ブラウザに表示される内容は、セッションをどのようにブロックするかによって異なります。ルール アクションを選択する際には、次の選択肢があります。

- 接続を拒否する場合は、[Block] または [Block with reset] を選択します。ブロックされたセッションがタイムアウトになると、[Block with reset] の場合は、システムが接続をリセットします。ただし、いずれのブロック アクションの場合でも、デフォルトのブラウザまたはサーバのページを、接続が拒否されたことを説明するカスタム ページでオーバーライドすることができます。システムではこのカスタム ページを*HTTP 応答ページ*と呼んでいます。
- ユーザーに警告する HTTP 応答ページを表示する一方、ユーザがボタンをクリックすることで、処理を続行あるいはページを最新表示して、要求された元のサイトをロードできるようにする場合は、[Interactive Block] または [Interactive Block with reset] を選択します。応答ページをバイパスした後、ロードされなかったページの要素をロードするために、ページを最新表示しなければならない場合があります。

シスコで提供している汎用の応答ページを表示するか、カスタム HTML を入力するかのいずれかを選択できます。カスタム テキストを入力する際には、使用した文字数がカウンタで示されます。ブロックされたセッションのカスタム ページには、最大 1353 文字を使用できます。クリックして続行する場合のカスタム ページは、1273 文字に制限されます。

セキュリティ インテリジェンスによるブラックリスト登録や Secure Sockets Layer（SSL）証明書に基づくアプリケーション条件の検出によってトラフィックがブロックされた場合には、HTTP 応答ページは表示されないことに注意してください。

ヒント　アクセス コントロール ポリシーのすべてのルールに対してインタラクティブ ブロックを素早く無効にできるようにするには、シスコ提供のページもカスタム ページも表示しないでください。

各アクセス コントロール ポリシーで、ブロック ルールおよびインタラクティブ ブロック ルールに対応する応答ページを個別に設定します。ユーザに表示されるページは、ルール アクションによって決まります。たとえば、セッションがブロックされたユーザにはシスコ提供のページを表示する一方、クリックして続行できるユーザに対しては、カスタム ページを表示するなどです。ルール アクションの詳細については、「ルール アクションについて」（P.14-6）を参照してください。

まれに、アプリケーション条件が含まれる別のルールがブロック ルールに先行する場合、システムが正常にトラフィックをブロックしたとしても、HTTP 応答ページが表示されないことがあります。

HTTP 応答ページの設定方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

ポリシーの [Edit] ページが表示されます。

ステップ 3　[HTTP Responses] タブを選択します。

アクセス コントロール ポリシーの HTTP 応答ページ設定が表示されます。

ステップ 4　[Block Response Page] および [Interactive Block Response Page] の場合、ドロップダウン リストから応答を選択します。各ページには、次の選択肢があります。

- 汎用の応答を使用する場合は、[Cisco-provided] を選択します。表示アイコン（）をクリックすると、このページの HTML コードが表示されます。
- カスタム応答を作成する場合は、[Custom] を選択します。

  ポップアップ ウィンドウが表示されます。このウィンドウに事前入力されているシスコ提供のコードを置換または変更できます。完了したら、変更を保存します。カスタム ページは、編集アイコン（）をクリックすると編集できます。
- システムに HTTP 応答ページを表示させない場合は、[None] を選択します。インタラクティブにブロックされるセッションに対してこのオプションを選択すると、ユーザはクリックして続行することができなくなります。

ステップ 5　[Save] をクリックして設定を保存します。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。詳細については、「アクセス コントロール ポリシーの適用」（P.13-39）を参照してください。

セキュリティ インテリジェンス データに基づくトラフィックのフィルタリング

ライセンス：Protection

サポート対象デバイス：シリーズ 3、仮想、X シリーズ、ASA FirePOWER

サポート対象防御センター：任意（DC500 以外の）

セキュリティ インテリジェンス機能を使用すると、送信元または宛先 IP アドレスに基づいてネットワークへの出入りを許可するトラフィックを、アクセス コントロール ポリシーごとに指定できます。この機能が特に役立つのは、アクセス コントロール ルールによる分析をトラフィックに適用する前に、特定の IP アドレスをブラックリスト登録する（つまり、その IP アドレスを宛先または送信元とするトラフィックを拒否する）必要がある場合です。

セキュリティ インテリジェンス フィルタリングと同様の機能を実行するアクセス コントロール ルールを作成することもできます。ただし、アクセス コントロール ルールは対象範囲が広く、設定の難易度が高いだけでなく、動的フィードを使用した自動更新に対応できません。これに対し、セキュリティ インテリジェンス フィルタリングでは、最新のインテリジェンスに基づいて即時に接続をブラックリスト登録できるため、多くのリソースを必要とする詳細な分析を行う必要がなくなります。

オプションで、セキュリティ インテリジェンス フィルタリングには「モニタ専用」設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブラックリスト登録されるはずの接続をシステムが分析できるだけでなく、ブラックリストと一致する接続をログに記録することもできます。

ブラックリストを作成するのに役立つように、シスコでは、シスコ インテリジェンス フィードを提供しています。このフィードは VRT によってレピュテーションに欠けると判断された IP アドレスのコレクションからなり、これらのコレクションは定期的に更新されます。インテリジェンス フィードを補完するには、グローバル ブラックリストを含めた、サードパーティによる IP アドレスのフィードやカスタム リストを利用できます。また、ネットワーク オブジェクトおよびグループを使用して IP アドレスをブラックリスト登録することもできます。これらの設定は、*セキュリティ インテリジェンス オブジェクト*と総称されます。

注　グローバル ブラックリスト（またはグローバル ホワイトリスト。以下を参照）のフィードの更新および追加では、展開環境全体にわたって自動的にその変更が実装されますが、セキュリティ インテリジェンス オブジェクトに対するその他すべての変更には、アクセス コントロール ポリシーの再適用が必要になります。詳細については、「セキュリティ インテリジェンス オブジェクトの機能」の表を参照してください。

ブラックリスト登録する IP アドレスの選択

ブラックリストを作成する最も簡単な方法は、オープン リレーとなることが分かっている IP アドレス、既知の攻撃者、不正な IP アドレス（bogon）などを追跡する、シスコ インテリジェンス フィードを使用することです。インテリジェンス フィードは定期的に更新されるため、このフィードを使用することで、システムは最新の情報を使用してネットワーク トラフィックをフィルタリングできます。ただし、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）を表す不正な IP アドレスが現れては消えるペースが早すぎて、新しいポリシーを更新して適用するには間に合わないこともあります。

したがって、インテリジェンス フィードを補完するために、サードパーティの IP アドレスのリストとフィードを使用してセキュリティ インテリジェンス フィルタリングを実行できるようになっています。

- *リスト*とは、防御センターにアップロードする IP アドレスの静的リストのことです。
- *フィード*とは、防御センターが定期的にインターネットからダウンロードする、IP アドレスの動的リストのことです。シスコ インテリジェンス フィードは、特殊なタイプのフィードです。

高可用性およびインターネット アクセス要件を含め、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する方法の詳細については、「セキュリティ インテリジェンス リストとフィードの操作」（P.5-4）を参照してください。

また、分析の過程で、イベント ビュー、Context Explorer、またはダッシュボードで任意の IP アドレスを選択して*グローバル ブラックリスト*を作成することもできます。たとえば、エクスプロイトの試みに関連する侵入イベントで、一連のルーティング可能 IP アドレスに気付いた場合、これらの IP アドレスを直ちにブラックリスト登録することができます。防御センターではすべてのアクセス コントロール ポリシーで、このグローバル ブラックリスト（および関連する*ホワイトリスト*）を使用してセキュリティ インテリジェンス フィルタリングを行います。これらのグローバル リストを管理する方法の詳細については、「グローバル ホワイトリストおよびブラックリストの操作」（P.5-7）を参照してください。

さらに、ブラックリストを作成するもう 1 つの簡単な方法として、IP アドレス、IP アドレス ブロック、あるいは IP アドレスのコレクションを表す*ネットワーク オブジェクト*または*ネットワーク オブジェクト グループ*を使用することもできます。ネットワーク オブジェクトの作成および変更の詳細については、「ネットワーク オブジェクトの操作」（P.5-4）を参照してください。

注　シリーズ 2デバイスはデフォルトで、その他すべてのProtection機能を使用できるものの、セキュリティ インテリジェンス フィルタリングを行うことはできません。入力したグローバル ホワイトリストまたはブラックリストを使用するアクセス コントロール ポリシーをシリーズ 2 デバイス（またはライセンスなしのシリーズ 3 デバイス）に適用することはできません。いずれかのグローバル リストに IP アドレスを追加した場合は、ポリシーのセキュリティ インテリジェンス設定から空でないリストを削除してからでないと、ポリシーを適用できません。

セキュリティ インテリジェンスのホワイトリスト

ブラックリストに加え、各アクセス コントロール ポリシーにはホワイトリストが関連付けられます。ホワイトリストにも、セキュリティ インテリジェンス オブジェクトを取り込むことができます。ポリシーでは、ホワイトリストがブラックリストをオーバーライドします。つまり、システムは、送信元または宛先の IP アドレスがホワイトリストに登録されているトラフィックは、たとえそれらの IP アドレスがブラックリストにも登録されているとしても、そのトラフィックをアクセス コントロール ルールを使用して評価します。通常、ブラックリストがまだ有用であっても、その適用範囲があまりにも広く、インスペクション対象のトラフィックを誤ってブロックする場合には、ホワイトリストを使用してください。

たとえば、信頼できるフィードにより、重要なリソースへのアクセスが不適切にブロックされたが、そのフィードが全体としては組織にとって有用である場合は、そのフィード全体をブラックリストから削除するのではなく、不適切に分類された IP アドレスだけをホワイトリストに登録するという方法を取ることができます。

セキュリティ ゾーンを基準としたセキュリティ インテリジェンス フィルタリングの適用

さらに細かく制御するには、接続の送信元または宛先 IP アドレスが特定のセキュリティ ゾーン内にあるかどうかに基づいて、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ことができます。

上述のホワイトリストの例を拡張するとしたら、不適切に分類された IP アドレスをホワイトリストに登録した後、組織でそれらの IP アドレスにアクセスする必要があるユーザが使用しているセキュリティ ゾーンを使用して、ホワイト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だけが、ホワイトリストに登録された IP アドレスにアクセスできます。別の例として、サードパーティのスパム フィードを使用して、電子メール サーバのセキュリティ ゾーンのトラフィックをブラックリスト登録することも考えられます。

接続のモニタリング（ブラックリスト登録の代替手段）

特定の IP アドレスまたはアドレス一式をブラックリスト登録する必要があるかどうかわからない場合は、「モニタ専用」設定を使用できます。この設定では、システムが一致する接続をアクセス コントロール ルールに渡せるだけでなく、ブラックリストと一致する接続をログに記録することもできます。注意する点として、グローバル ブラックリストをモニタ専用に設定することはできません。

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。

パッシブ展開環境では、パフォーマンスを最適化するために、シスコでは常にモニタ専用の設定を使用することを推奨しています。その理由は、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ないためです。

ブラックリスト登録された接続のロギング

ブラックリスト登録された接続をログに記録すると、ブラックリスト登録された IP アドレスを宛先または送信元とするネットワーク トラフィックが検出されたときに接続イベントを生成することができます。セキュリティ インテリジェンス フィルタリングによって生成されるイベントは、システムによる接続拒否（ブラックリストの場合）または接続のインスペクション（モニタ専用に設定されたブラックリストの場合）のいずれかの決定を表します。このロギング設定は、アクセス コントロール ルールやデフォルト アクションのロギング設定とは独立しています。

ブラックリスト登録されたオブジェクトをモニタ専用に設定する場合は、セキュリティ インテリジェンスのロギングを有効にする必要があります。アクセス コントロール ルールによるインスペクションが適用される、一致する接続については、後続の処理に使用されるアクセス コントロール ルールまたはデフォルト アクションのロギング設定に応じて、追加の接続イベントが生成される場合があります。

ヘルス モニタリング

デフォルトのヘルス ポリシーには、セキュリティ インテリジェンス モジュール（「セキュリティ インテリジェンス モニタリングの設定」（P.55-27）を参照）が組み込まれます。このモジュールは、次の場合に警告を出します。

- 防御センターがフィードを更新できない場合、またはフィードのデータが壊れているか、データに認識可能な IP アドレスが含まれていない場合
- 管理対象デバイスが、更新されたセキュリティ インテリジェンスのデータを防御センターから受信できない場合
- 管理対象デバイスが、メモリの問題により、防御センターから提供されたセキュリティ インテリジェンス データの一部をロードできない場合

セキュリティ インテリジェンス フィルタリングを実行するようにアクセス コントロール ポリシーを設定する方法の詳細については、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ホワイトリストおよびブラックリストの作成」（P.13-16）
- 「ホワイトリストまたはブラックリストに追加するオブジェクトの検索」（P.13-19）
- 「ホワイトリストまたブラックリストに追加するオブジェクトの作成」（P.13-19）
- 「ブラックリスト登録された接続のロギング」（P.13-20）

セキュリティ インテリジェンスのホワイトリストおよびブラックリストの作成

ライセンス：Protection

サポート対象デバイス：シリーズ 3、仮想、X シリーズ、ASA FirePOWER

サポート対象防御センター：任意（DC500 以外）

ホワイトリストとブラックリストを作成するには、ネットワーク オブジェクトとグループの任意の組み合わせに加え、セキュリティ ゾーン別に制約することができる、セキュリティ インテリジェンスのフィードとリストを入力します。

デフォルトでは、アクセス コントロール ポリシーは、任意のゾーンに適用される、防御センターのグローバル ホワイトリストおよびブラックリストを使用します。これらのリストはアナリストによって入力されます。アナリストは、コンテキスト メニューを使用して、簡単に個々の IP アドレスを追加できます。ポリシーのそれぞれについて、これらのグローバル リストを使用しないように選択することができます。詳細については、「グローバル ホワイトリストおよびブラックリストの操作」（P.5-7）を参照してください。

ホワイトリストとブラックリストを作成した後は、ブラックリスト登録された接続のロギングが可能になります。フィードとリストを含め、ブラックリスト登録された個々のオブジェクトをモニタ専用に設定することもできます。この設定では、システムがブラックリスト登録された IP アドレスを使用する接続をアクセス コントロールによって処理できるだけでなく、ブラックリストと一致する接続をログに記録することもできます。

ホワイトリスト、ブラックリスト、およびロギング オプションを設定するには、アクセス コントロール ポリシーの [Security Intelligence] タブを使用します。このページには、ホワイトリストまたはブラックリストのいずれかで使用できるオブジェクトのリスト（[Available Objects]）と、ホワイトリスト登録およびブラックリスト登録されたオブジェクトを制約するために使用できるゾーンのリスト（[Available Zones]）が表示されます。オブジェクトまたはゾーンのタイプは、異なるアイコンによって見分けられるようになっています。シスコ アイコン（）でマークされたオブジェクトは、シスコ インテリジェンス フィードの各種カテゴリを表します。

ブラックリストでは、ブロックするように設定されたオブジェクトはブロック アイコン（）でマークされ、モニタ専用オブジェクトはモニタ アイコン（）でマークされます。ホワイトリストがブラックリストをオーバーライドするため、両方のリストに同じオブジェクトを追加すると、ブラックリスト登録されたオブジェクトに取り消し線が表示されます。

ホワイトリストとブラックリストには、最大 255 個のオブジェクトを追加できます。つまり、ホワイトリストのオブジェクトとブラックリストのオブジェクトを合計した数は 255 以下でなければなりません。

ホワイトリストまたはブラックリストに、ネットマスクが /0 のネットワーク オブジェクトを追加することはできますが、そのようなオブジェクトのネットマスク /0 を使用するアドレス ブロックは無視され、ホワイトリストおよびブラックリストのフィルタリングでは、これらのアドレスは基準にされないことに注意してください。セキュリティ インテリジェンス フィードに含まれるネットマスク /0 のアドレス ブロックも同じく無視されます。ポリシーの適用対象となるすべてのトラフィックをモニタまたはブロックする場合は、セキュリティ インテリジェンス フィルタリングの代わりに、それぞれ [Monitor] または [Block] ルール アクションを指定し、[Source Networks] および [Destination Networks] にデフォルト値の **any** を使用したアクセス コントロール ルールを使用してください。

ヒント　セキュリティ インテリジェンスの ホワイトリストおよびブラックリストの通常の作成方法は、アクセス コントロール ルールの通常の作成方法と同じです。詳細については、「ルール条件とそのメカニズムについて」（P.14-10）を参照してください。

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 ホワイトリストおよびブラックリストを作成する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

ポリシーの [Edit] ページが表示されます。

ステップ 3　[Security Intelligence] タブを選択します。

アクセス コントロール ポリシーのセキュリティ インテリジェンス設定が表示されます。

ステップ 4　オプションで、ブラックリスト登録された接続をログに記録するには、ロギング アイコン（  ）をクリックします。

ロギングを有効にしてからでないと、ブラックリスト登録されたオブジェクトをモニタ専用に設定することはできません。詳細については、「ブラックリスト登録された接続のロギング」（P.13-20）を参照してください。

ステップ 5　1 つ以上の使用可能なオブジェクトを選択して、ホワイトリストおよびブラックリストの作成を開始します。

Ctrl キーまたは Shift キーを押しながらクリックして複数のオブジェクトを選択し、右クリックして [Select All] を選択します。

ヒント　リストに含める既存のオブジェクトを検索できます。組織のニーズを満たす既存のオブジェクトがない場合は、その場でオブジェクトを作成することもできます。詳細については、「ホワイトリストまたはブラックリストに追加するオブジェクトの検索」（P.13-19）および「ホワイトリストまたブラックリストに追加するオブジェクトの作成」（P.13-19）を参照してください。

ステップ 6　オプションで、使用可能なゾーンを選択して、選択したオブジェクトをゾーンを基準に制約します。

デフォルトでは、オブジェクトは制約されません。つまり、オブジェクトのゾーンは [Any] に設定されます。[Any] を使用しない場合、制約の基準にできるゾーンは 1 つだけです。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、オブジェクトをホワイトリストまたはブラックリストに追加する必要があります。また、グローバル ホワイトリストまたはブラックリストをゾーンによって制約することはできません。

ステップ 7　[Add to Whitelist] または [Add to Blacklist] をクリックします。

また、オブジェクトをクリックして選択し、いずれかのリストにドラッグすることもできます。

ヒント　オブジェクトを削除するには、そのオブジェクトの削除アイコン（  ）をクリックします。Ctrl キーまたは Shift キーを押しながらクリックして複数のオブジェクトを選択するか、または右クリックして [Select All]]を選択した後、右クリックして [Delete Selected] を選択します。グローバル リストを削除する場合は、選択した操作を確認する必要があります。ホワイトリストまたはブラックリストからオブジェクトを排除しても、そのオブジェクトは防御センターから削除されません。

ステップ 8　オブジェクトをホワイトリストまたはブラックリストに追加し終わるまで、ステップ 5 ～ 7 を繰り返します。

ステップ 9　オプションで、ブラックリスト登録されたオブジェクトをモニタ専用に設定するには、[Blacklist] 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、[Monitor-only (do not block)] を選択します。

パッシブ展開環境の場合、シスコではすべてのブラックリスト登録されたオブジェクトをモニタ専用に設定することを推奨します。ただし、グローバル ブラックリストをモニタ専用に設定することはできません。

ステップ 10　[Save] をクリックします。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。詳細については、「アクセス コントロール ポリシーの適用」（P.13-39）を参照してください。

ホワイトリストまたはブラックリストに追加するオブジェクトの検索

ライセンス：Protection

サポート対象デバイス：シリーズ 3、仮想、X シリーズ、ASA FirePOWER

サポート対象防御センター：任意（DC500 以外）

複数のネットワーク オブジェクト、グループ、フィード、およびリストを使用する場合は、検索機能を使用して、ブラックリストまたはホワイトリストに追加するオブジェクトを絞り込むことができます。

ブラックリストまたはホワイトリストに追加するオブジェクトを検索する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Search by name or value] フィールドに入力します。

検索文字列を入力すると、[Available Objects] リストが更新されて、検索文字列と一致する項目が表示されます。検索ストリングをクリアするには、検索フィールドの上にあるの再ロード アイコン（  ）をクリックするか、検索フィールド内のクリア アイコン（）をクリックします。

ネットワーク オブジェクトの名前、またはネットワーク オブジェクトに設定されている値を基準に検索できます。たとえば、`Texas Office` という名前で `192.168.3.0/24` という設定値を持つ個別ネットワーク オブジェクトがあり、そのオブジェクトが `US Offices` というグループ オブジェクトに含まれている場合、検索文字列の一部または全部（たとえば `Tex`）を入力するか、値（たとえば `3`）を入力することで、両方のオブジェクトを表示できます。

ホワイトリストまたブラックリストに追加するオブジェクトの作成

ライセンス：Protection

サポート対象デバイス：シリーズ 3、仮想、X シリーズ、ASA FirePOWER

サポート対象防御センター：任意（DC500 以外）

アクセス コントロール ポリシーの編集中に、ホワイトリストやブラックリストで使用するオブジェクト（ネットワーク オブジェクトや、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）をその場で作成できます。ネットワーク オブジェクトをグループ化する場合、またはネットワーク オブジェクト グループを作成する場合は、オブジェクト マネージャーを使用する必要があります。

ホワイトリストまたはブラックリストに追加するオブジェクトを作成する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　追加アイコン（  ）をクリックして、作成するオブジェクトのタイプを選択します。

- 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する場合は、[Add IP List]] を選択します。「セキュリティ インテリジェンス リストとフィードの操作」（P.5-4）を参照してください。
- ネットワーク オブジェクトを追加する場合は、[Add Network Object] を選択します。「ネットワーク オブジェクトの操作」（P.5-4）を参照してください。

ブラックリスト登録された接続のロギング

ライセンス：Protection

サポート対象デバイス：シリーズ 3、仮想、X シリーズ、ASA FirePOWER

サポート対象防御センター：任意（DC500 以外）

ブラックリスト化された接続のロギングを使用すると、ブラックリストに含まれる IP アドレスとの間のネットワーク トラフィックがシステムで検出されたときに接続イベントを生成できます。これらの接続イベントは、防御センター データベースに保存できます。さらに、アラート応答を使用して、イベントを syslog または SNMP トラップ サーバに記録することもできます。アラート応答の設定方法については、「アラート応答の使用」（P.15-2）を参照ください。

注　ブラックリスト登録されたオブジェクトをモニタ専用に設定する場合、またはセキュリティ インテリジェンス フィルタリングによって生成された接続イベントで他の防御センター ベースの分析を行う場合は、イベントを防御センターに送信することが**必須**となります。

アクセス コントロール ルールやデフォルト アクションのロギング オプションとは異なり、接続開始イベントまたは接続終了イベントを生成するかどうかを選択することはできません。セキュリティ インテリジェンス フィルタリングによって生成されるイベントは常に、接続が開始されたこと、そしてシステムによって以下のいずれかの決定が行われたことを表します。

- それ以上のインスペクションを行わずにトラフィックを拒否する（ブラックリストの場合）
- 接続に対してさらに分析を行う（モニタ専用に設定されたブラックリストの場合）

この決定は、接続イベントの理由を示す `IP Block` または `IP Monitor` のいずれかとして記録されます。この決定は接続イベントのアクションにも反映され、ブラックリスト登録された接続に対するアクションは `Block` となります。一方、モニタされる接続に対するアクションは、接続によってトリガーされた最初の非モニタ アクセス コントロール ルールのアクションか、またはデフォルト アクションとなります。

システムは、セキュリティ インテリジェンスのカテゴリもログに記録します。接続がブラックリスト登録された理由は、カテゴリによって特定されます。セキュリティ インテリジェンス接続データを容易に分析できるように、セキュリティ インテリジェンス イベント ビュー（[Analysis] > [Connections] > [Security Intelligence Events]）には、接続イベントとそのイベントに関連付けられたセキュリティ インテリジェンス カテゴリが併せて表示されます。接続イベントおよびセキュリティ インテリジェンス イベントの詳細については、「接続およびセキュリティ インテリジェンス のデータの使用」（P.16-1）を参照してください。

イベント ビューアでは、接続でブラックリスト登録された IP アドレスを特定できるように、IP アドレスの横にあるホスト アイコンは、ブラックリスト登録された IP アドレスとモニタされた IP アドレスでは少々異なる表示になっています。

ネットワーク トラフィックがアクセス コントロール ルールによって評価される前に、接続をブラックリスト登録するかどうかの決定が行われます。したがって、セキュリティ インテリジェンス フィルタリングによって生成される接続イベントには、セッション期間にわたるトラフィックの検査によって判断しなければならない情報や、アプリケーション データは含まれません。接続イベントに含まれる情報の詳細については、「接続およびセキュリティ インテリジェンスのイベントで利用可能な情報」（P.16-11）を参照してください。

`IP Block` 接続イベントのしきい値は、開始側と応答側の固有のペアあたり 15 秒です。つまり、システムは接続をブロックしてイベントを生成した時点から 15 秒の間、この 2 つのホスト間で接続がブロックされたとしても、ポートやプロトコルの違いに関わらず、別の接続イベントを生成しません。

ただし、モニタされる接続の場合、以降に接続を処理するアクセス コントロール ルールやデフォルト アクションでのロギング設定によっては、追加のイベントが生成されることもあります。同様の理由により、システムはホワイトリストに登録された IP アドレスを宛先または送信元とする接続を検出した場合、特に接続イベントを生成しません。つまり、ホワイトリスト登録された接続のイベントの生成は、その後システムがその接続をどのように処理するかに応じます。

ブラックリスト登録された接続をログに記録する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　アクセス コントロール ポリシーの [Security Intelligence] タブで、ロギング アイコン（  ）をクリックします。

[Blacklist Options] ダイアログボックスが表示されます。

ステップ 2　トラフィックがセキュリティ インテリジェンスの条件に一致した場合に接続開始イベントをログに記録するには、[Log Connections] チェック ボックスをオンにします。

ステップ 3　接続イベントの送信先を指定します。次の選択肢があります。

- 接続イベントを防御センターに送信する場合は、[Defense Center] を選択します。
- 接続イベントを Syslog に送信するには、[Syslog] を選択して、ドロップダウン リストから Syslog アラート応答を 1 つ選択します。オプションで、syslog アラート応答を追加するには、追加アイコン（  ）をクリックします。「Syslog アラート応答の作成」（P.15-5）を参照してください。
- 接続イベントを SNMP トラップ サーバに送信する場合は、[SNMP Trap] を選択し、ドロップダウン リストから SNMP アラート応答を選択します。オプションで、SNMP アラート応答を追加するには、追加アイコン（  ）をクリックします。「SNMP アラート応答の作成」（P.15-4）を参照してください。

ステップ 4　[OK] をクリックしてロギング オプションを設定します。

[Security Intelligence] タブが再表示されます。

ステップ 5　[Save] をクリックします。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。詳細については、「アクセス コントロール ポリシーの適用」（P.13-39）を参照してください。

アクセス コントロール ポリシーの詳細設定

ライセンス：任意

通常、アクセス コントロール ポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。ほとんどの展開環境には、デフォルト設定が適切です。

一般的な詳細設定オプション

アクセス コントロール ポリシーを設定する際の一般的なオプションには、以下があります。

- HTTP トラフィックで、接続終了イベントのログを防御センター データベースに記録する場合（「接続、ファイル、マルウェアに関する情報のロギング」（P.14-39）を参照）、システムはセッション中にモニタ対象のホストが要求した URL を記録します。

デフォルトでは、システムは URL の最初の 1024 文字を接続ログに保管します。モニタ対象のホストが要求する完全な URL が取り込まれるようにするには、[Maximum URL characters to store in connection events] を使用して、URL ごとに最大 4096 文字を保管するようにシステムを設定できます。または、アクセスされた個々の URL を知る必要がない場合は、保管する文字数をゼロに設定して、URL の保管を無効にすることもできます。ネットワーク トラフィックによっては、URL の保管を無効にするか、あるいは保管する URL の文字数を制限すると、システム パフォーマンスが向上する可能性があります。

URL のロギングを無効にしても、URL フィルタリングには影響しません。アクセス コントロール ルールにより、要求された URL、そのカテゴリ、およびレピュテーションに基づいて、トラフィックが適切にフィルタリングされます。システムが、これらのルールによって処理されたトラフィックで要求された個々の URL を記録しないだけです。詳細については、「URL 条件の追加」（P.14-31）を参照してください。

- トラフィックが、[Interactive Block] または [Interactive Block with Reset] がアクションとして設定されたアクセス コントロール ルールと一致した場合、ユーザは応答ページでのクリック操作によって、ブロックをバイパスできます。[Allow an Interactive Block to bypass blocking for (seconds)] を使用することで、システムが応答ページを表示せずにユーザにブロックのバイパスを許可する期間を設定できます。デフォルト設定は 600 秒（10 分に相当）です。この期間は最長 31536000 秒（365 日に相当）に設定できます。毎回ユーザにブロックをバイパスさせるには、このオプションをゼロに設定します。
- 侵入ポリシーをアクセス コントロール ポリシーのデフォルト アクションに関連付ける場合、[Default Action Variable Set] によって、その侵入ポリシーで使用する変数セットが特定されます。侵入ポリシーの侵入ルールが変数セットの変数を使用する際にネットワーク トラフィックの送信元および宛先の IP アドレスとポートをどのように識別するかは、選択されている変数セットによって決まります。デフォルトでは、アクセス コントロール ポリシーはデフォルトの変数セットを使用します。ただし、カスタム セットを作成してある場合は、ドロップダウン リストから、作成済みカスタム セットのいずれかを選択することもできます。オプションで、選択されている変数セットの横にある編集アイコン（  ）をクリックして、その変数セットを新しいブラウザ タブで変更できます。アクセス コントロール ポリシーごとに異なる変数セットを選択して、ネットワーク上のさまざまな種類のトラフィックに合わせて侵入ポリシーをカスタマイズすることが可能です。

  詳細については、「デフォルト アクションの設定」（P.13-5）および「変数セットの操作」（P.5-19）を参照してください。

ファイルおよびマルウェアの検出オプション

ファイル コントロール、ファイル ストレージ、動的分析、あるいはマルウェアの検出またはブロッキングを行うためにファイル ポリシーを使用する場合は、次の表にリストするオプションを設定できます。

表 13-6　アクセス コントロール ファイルおよびマルウェア検出の詳細設定オプション

フィールド	説明	デフォルト値	範囲	注意
Limit the number of bytes inspected when doing file type detection	ファイル タイプを検出するときに検査するバイト数を指定します。	1460 バイト、または TCP パケットの最大セグメント サイズ	0 ～ 4294967295（4GB）	制限を完全に取り除くには、この値を 0 に設定します。 ほとんどの場合、システムは最初のパケットによって、一般的なファイル タイプを特定できます。
Do not calculate SHA-256 hash values for files larger than (in bytes)	システムが特定のサイズを超えるファイルを保管すること、ファイルでCollective Security Intelligence クラウド ルックアップを実行すること、またはカスタム検出リストに追加されたファイルをブロックすることを防止します。	10485760（10MB）	0 ～ 4294967295（4GB）	制限を完全に取り除くには、この値を 0 に設定します。 この値は、[Maximum file size to store (bytes)] および [Maximum file size for dynamic analysis testing (bytes)] の値以上に設定する必要があります。
Allow file if cloud lookup for Block Malware takes longer than (seconds)	マルウェア クラウド ルックアップの実行中に、システムが [Block Malware] ルールに一致し、性質がキャッシュに入れられていないファイルを保持する期間を指定します。システムが性質を取得する前にこの期間が満了すると、ファイルが渡されます。	2 秒	0 ～ 30 秒	「使用不可」の性質はキャッシュに入れられません。 このオプションは最大 30 秒に設定できますが、シスコではデフォルト値を使用して、接続失敗によってトラフィックがブロックされないようにすることを推奨します。このオプションの値を 0 に設定する場合は、**必ず** 事前にサポートに連絡してください。
Minimum file size to store (bytes)	システムがファイル ルールを使用して保管できるファイルの最小サイズを指定します。	6144（6KB）	0 ～ 10485760（10MB）	ファイル ストレージを無効にするには、この値を 0 に設定します。 このフィールドは、[Maximum file size to store (bytes)] および [Maximum file size to store (bytes)] の値以下に設定する必要があります。
Maximum file size to store (bytes)	システムがファイル ルールを使用して保管できるファイルの最大サイズを指定します。	1048576（1MB）	0 ～ 10485760（10MB）	ファイル ストレージを無効にするには、この値を 0 に設定します。 このフィールドは、[Minimum file size to store (bytes)] の値以上、および [Do not calculate SHA-256 hash values for files larger than (in bytes)] の値以下に設定する必要があります。

表 13-6　アクセス コントロール ファイルおよびマルウェア検出の詳細設定オプション（続き）

フィールド	説明	デフォルト値	範囲	注意
Minimum file size for dynamic analysis testing (bytes)	システムがクラウドに動的分析対象として送信できるファイルの最小サイズを指定します。	6144（6KB）	6144（6KB）～ 2097152（2MB）	このフィールドは、[Maximum file size for dynamic analysis testing (bytes)] および [Do not calculate SHA-256 hash values for files larger than (in bytes)] の値以下に設定する必要があります。 システムはクラウドをチェックして、送信可能なファイルの最小サイズが更新されているかどうかを調べます（最大で 1 日 1 回）。新しい最小サイズが現在の値より大きい場合、現在の値が新しい最小サイズに更新され、ポリシーは古いポリシーとしてマークされます。
Maximum file size for dynamic analysis testing (bytes)	システムがクラウドに動的分析対象として送信できるファイルの最大サイズを指定します。	1048576（1MB）	6144（6KB）～ 2097152（2MB）	このフィールドは、[Minimum file size for dynamic analysis testing (bytes)] の値以上、[Do not calculate SHA-256 hash values for files larger than (in bytes)] の値以下に設定する必要があります。 システムはクラウドをチェックして、送信可能なファイルの最大サイズが更新されているかどうかを調べます（最大で 1 日 1 回）。新しい最大サイズが現在の値より小さい場合、現在の値が新しい最大サイズに更新され、ポリシーは古いポリシーとしてマークされます。

ファイル サイズを増やすと、システムのパフォーマンスに影響を与える可能性があることに注意してください。

アクセス コントロール ポリシーの詳細設定オプションの設定方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（ ）をクリックします。

ポリシーの [Edit] ページが表示されます。

ステップ 3　[Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 4　前述のように詳細設定オプションを設定します。

ステップ 5　[Save] をクリックします。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。詳細については、「アクセス コントロール ポリシーの適用」（P.13-39）を参照してください。

ポリシー内でのルールの編成

ライセンス：任意

アクセス コントロール ポリシーの [Edit] ページには、アクセス コントロール ルールが番号順にリストされます。ページの左側には、各ルールの横にその数値位置が示されます。ルールを移動または挿入したり、ルールの順序を変更したりできます。たとえば、ルール 10 をルール 3 の下に移動すると、ルール 10 はルール 4 になり、それに合わせて後続のルールの番号が増分されます。

システムは、ポリシーの [編集] ページで配列されているルールの数値位置の順に、パケットをルールに照らし合わせるため、ルールの位置は重要です。パケットが特定のルールのすべての条件を満たすと、システムはパケットにそのルールの条件を適用し、後続のルールはそのパケットですべて無視されます。

ルールを追加または編集する際に、オプションでルールの数値位置を指定できます。また、新しいルールを追加する前に、特定のルールを強調表示すると、新しいルールのデフォルト位置が、その強調表示されたルールの下に設定されます。「アクセス コントロール ルールの作成と編集」（P.14-3）を参照してください。

特定のルールを見つけるには、検索文字列として、ルール名、あるいは設定済みのルール条件の名前や値の一部または全体を使用できます。また、ポリシーの適用対象デバイスを選択し、そのデバイスのルールだけが表示されるようにルールをフィルタリングすることもできます。

ルールの行の空白スペースをクリックすることで、1 つまたは複数のルールを選択できます。選択したルールを新しい位置にドラッグ アンド ドロップすると、そのルールの位置を変更できます。この場合、移動したルールの後続のすべてのルールの位置が変更されます。選択したルールを既存のルールの上または下にカット アンド ペーストできます。また、選択したルールを削除したり、既存のルール リスト内の任意の位置に新しいルールを挿入することもできます。

さらにルールを編成するには、管理カテゴリおよび root カテゴリの間にカスタム カテゴリを追加するという方法があります。追加したカスタム カテゴリは、削除したり、名前を変更したりすることができます。

先行ルールが優先して適用されるために決して一致することがないルールを示す、説明的な警告メッセージを表示することもできます。

次の表に、ルールを編成するために実行できる操作を要約します。

表 13-7　　アクセス コントロール ルールの編成操作

目的	操作
ポリシーにカテゴリを追加する	[Add Category] をクリックします。詳細については、「ルール カテゴリの処理」（P.13-26）を参照してください。 **ヒント**　ルールの行の空白部分を右クリックして、[Insert new category] を選択するという方法もあります。
検索文字列と一致するルール名と条件を検索する	[Search Rules] プロンプトをクリックし、名前または値を入力してから Enter キーを押します。詳細については、「ルールの検索」（P.13-28）を参照してください。
ルールの検索をクリアする	検索フィールドのクリア アイコン（ ✖ ）をクリックします。
選択したデバイスのルールを表示する	詳細については、「デバイスを基準としたルールのフィルタリング」（P.13-29）を参照してください。

表 13-7　アクセス コントロール ルールの編成操作（続き）

目的	操作
ルールを選択する	ルールの行の空白部分をクリックします。複数のルールを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。選択したルールが強調表示されます。 複数のカテゴリのルールを選択できることに注意してください。
ルールの選択をクリアする	ページの右下にある再ロード アイコン（）をクリックします。
選択したルールを切り取る、またはコピーする	選択したルールの行の空白部分を右クリックし、[Cut] または [Copy] を選択します。
切り取ったルールまたはコピーしたルールをルール リストに貼り付ける	選択したルールを貼り付けるルールの行の空白部分を右クリックし、[Paste above] または [Paste below] を選択します。
アクティブでないルールを有効にする	ルールを右クリックし、[State] > [Enable] を選択します。
アクティブなルールを無効にする	ルールを右クリックし、[State] > [Disable] を選択します。
選択したルールを移動する	選択したルールを新しい位置の下にドラッグ アンド ドロップします。この移動先の位置は、ドラッグ時にポインタの上に表示される青い横線で示されます。
ルールを削除する	ルールの横にある削除アイコン（）をクリックし、[OK] をクリックします。 ヒント　選択したルールの行の空白部分を右クリックして [Delete] を選択した後、[OK] をクリックして、選択した 1 つ以上のルールを削除するという方法もあります。
警告またはエラーを読む	警告またはエラー テキストを読むには、警告アイコン（）またはエラー アイコン（）の上にカーソルを移動します。詳細については、「警告およびエラーの処理」（P.13-30）を参照してください。
ルールに対して侵入ポリシーまたはファイル ポリシーが選択されているかどうかを判別する	侵入ポリシー アイコン（）またはファイル ポリシー アイコン（）を確認します。ポリシーのアイコンがアクティブ（黄色）の場合、ポリシーは選択されています。アクティブでない（白）場合、そのタイプのポリシーはルールに選択されていません。
ルールに選択されている侵入ポリシーまたはファイル ポリシーを表示する	侵入ポリシー アイコン（）またはファイル ポリシー アイコン（）をクリックします。

ルール カテゴリの処理

ライセンス：任意

ポリシーの [Edit] ページでアクセス コントロール ルールに事前定義されている次の 3 つのカテゴリを利用して、ルールを編成できます。

- Administrator Rules（管理者ルール）
- Standard Rules（標準ルール）
- Root Rules（root ルール）

定義済みカテゴリを移動、削除、名前変更することはできません。デフォルトでは、アクセス コントロール ポリシーの変更を許可する定義済みユーザ ロールはすべて、上記のすべてのカテゴリのルールの（カテゴリ内外への）移動および変更を許可します。これらの定義済みカテゴリのルールの移動および変更を制限するには、カスタム ユーザ ロールを作成します。詳細については、「カスタム ユーザ ロールの管理」（P.48-55）および「[Policies]メニュー」（P.48-64）を参照してください。

新しいカスタム カテゴリは、事前定義された標準カテゴリと root カテゴリの間に追加できます。カスタム カテゴリを追加すると、追加のポリシーを作成しなくても、ルールをさらに細かく編成できます。追加したカスタム カテゴリは、名前を変更したり、削除したりすることができます。カスタム カテゴリを移動することはできませんが、カスタム カテゴリのルールは、（カテゴリ内外への）移動が可能です。アクセス コントロール ポリシーの変更権限が割り当てられているユーザーは、制限なく、これらのカテゴリにルールを追加したり、カテゴリ内のルールを変更したりできます。

次の手順は、アクセス コントロール ポリシーに新しいカテゴリを追加する方法を示しています。アクセス コントロール ポリシーを編集する詳細な手順については、「アクセス コントロール ポリシーの編集」（P.13-34）を参照してください。

新しいカテゴリを追加する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（  ）をクリックします。

ポリシーの [Edit] ページが表示されます。

ステップ 3　オプションで、既存のルールの行の空白部分をクリックして、新しいカテゴリのデフォルトの位置を設定します。

ステップ 4　[Add Category] をクリックします。

または、ポリシーにルールを追加してある場合、既存のルールを右クリックし、[Insert new category] をクリックします。

[Add Category] ポップアップ ウィンドウが表示されます。

ステップ 5　[Name] に、一意のカテゴリ名を入力します。

最大 30 文字の英数字の名前を入力できます。名前には、スペース、および印刷可能な特殊文字を含めることができます。

ステップ 6　次の選択肢があります。

- 既存のカテゴリのすぐ上に新しいカテゴリを配置する場合は、最初の [Insert] ドロップダウン リストから [above Category] を選択した後、2 番目のドロップダウン リストからカテゴリを選択します。ここで選択したカテゴリの上にルールが配置されます。
- 既存のルールの下に新しいカテゴリを配置する場合は、ドロップダウン リストから [below rule] を選択した後、既存のルール番号を入力します。

  このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。
- 既存のルールの上にルールを配置する場合は、ドロップダウン リストから[above rule]を選択した後、既存のルール番号を入力します。

  このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

ステップ 7　カテゴリを追加するには [OK] をクリックし、変更を破棄するには [キャンセル] をクリックします。

[OK] をクリックすると、カテゴリがポリシーに追加されます。

カテゴリ名を編集するには、追加したカテゴリの横にある編集アイコン（）をクリックします。カテゴリを削除するには、削除アイコン（  ）をクリックします。削除するカテゴリに含まれるルールは、その上にあるカテゴリに追加されます。

ルールの検索

ライセンス：任意

スペースおよび印刷可能な特殊文字を含む英数字文字列を使用して、アクセス コンロトール ルールのリストで一致する値を検索できます。この検索では、ルール名およびルールに追加したルール条件が検査されます。ルール条件の場合は、条件タイプ（ゾーン、ネットワーク、アプリケーションなど）ごとに追加できる任意の名前または値が検索照合されます。これには、個々のオブジェクト名または値、グループ オブジェクト名、グループ内の個々のオブジェクト名または値、およびリテラル値が含まれます。

検索文字列のすべてまたは一部を使用できます。照合ルールごとに、一致する値のカラムが強調表示されます。たとえば、`100Bao` という文字列のすべてまたは一部を基準に検索すると、少なくとも、100Bao アプリケーションを追加した各ルールの [Applications] カラムが強調表示されます。100Bao という名前のルールもある場合は、[Name] カラムと [Applications] カラムの両方が強調表示されます。

1 つ前または次の照合ルールに移動することができます。ステータス メッセージには、現行の一致および合計一致数が表示されます。

複数ページのルール リストでは、どのページでも一致が検出される可能性があります。最初の一致が検出されたのが最初のページではない場合は、最初の一致が検出されたページが表示されます。最後の一致が現行の一致となっている場合、次の一致を選択すると、最初の一致が表示されます。また、最初の一致が現行の一致となっている場合、前の一致を選択すると、最後の一致が表示されます。

次の手順で、アクセス コントロール ポリシー ルールの検索方法を説明します。アクセス コントロール ポリシーを編集する詳細な手順については、「アクセス コントロール ポリシーの編集」（P.13-34）を参照してください。

ルールの検索方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　検索するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

ポリシーの [Edit] ページが表示されます。

ステップ 3　[Search Rules] プロンプトをクリックし、検索文字列を入力してから Enter キーを押します。

一致する値を含むルールのカラムが強調表示されます。表示されている（最初の）一致は、他とは区別できるように強調表示されます。

ヒント　検索を開始するには、Tab キーを使用するか、ページの空白部分をクリックします。

ステップ 4　次の選択肢があります。

- 照合ルールの間を移動する場合は、次の一致アイコン（ ▼ ）または前の一致アイコン（ ▲ ）をクリックします。
- 検索文字列をクリアする場合は、クリア アイコン（ ✖ ）をクリックします。

  ページが最新表示されて、強調表示がクリアされます。

デバイスを基準としたルールのフィルタリング

ライセンス：任意

1 つ以上のデバイスまたはデバイス グループを指定してアクセス コントロール ポリシーにリストされたアクセス コントロールをフィルタリングし、該当するデバイスまたはデバイス グループのルールのみを表示することができます。システムは、アクセス コントロール ルールのゾーン条件を使用して、デバイスをネットワーク上のデバイスと関連付けます。詳細については、「セキュリティ ゾーンの操作」（P.5-43）および「ゾーン条件の追加」（P.14-18）を参照してください。

指定されていないデバイスおよびグループのルールは表示されません。ルールにゾーンを追加しないと、そのようなルールはすべてのゾーンに適用され、したがって、すべてのデバイスに適用されることになるので、非表示にはなりません。

次の手順で、デバイスまたはデバイス グループを基準にルールをフィルタリングする方法を説明します。アクセス コントロール ポリシーを編集する詳細な手順については、「アクセス コントロール ポリシーの編集」（P.13-34）を参照してください。

デバイスまたはデバイス グループを基準にルールをフィルタリングする方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　変更するアクセス コントロール ポリシーの横にある編集アイコン（  ）をクリックします。

ポリシーの [Edit] ページが表示されます。

ステップ 3　ルールのリストの上にある [Filter by Device] をクリックします。

[Filter by Device] ポップアップ ウィンドウが表示されます。ポリシーにデバイスまたはデバイス グループを追加してある場合は、ターゲットのデバイスおよびデバイス グループのリストが表示されます。

ステップ 4　1 つまたは複数のチェック ボックスをオンにして、これらのデバイスまたはグループに適用されるルールだけを表示します。リセットしてすべてのルールを表示するには、[All] チェック ボックスを選択します。

ステップ 5　[OK] ボタンをクリックして、ルールのリストを更新します。

ページが更新されて、選択したデバイスおよびデバイス グループのルールが表示され、選択しなかったデバイスおよびデバイス グループのルールが非表示になります。

ヒント　これらのフィルタは、新しいルールを追加したり、既存のルールを編集して保存したりすると、クリアされます。

警告およびエラーの処理

ライセンス：任意

アクセス コントロール ポリシーの設定可能な要素の多さから、ポリシーは非常に複雑なものになることがあります。ルールは、別のルールによって回避される場合があります。アクセス コントロール ポリシー外部の設定に依存する機能が設定されている場合もあります。ユーザが設定するポリシーによって期待した結果が導き出されるようにするために、アクセス コントロール ポリシー インターフェイスには、強力な警告およびエラーのフィードバック システムが備わっています。ポリシー内のルールやその他の要素に対して警告が出された場合、そのポリシーを適用することはできますが、エラーに該当する設定部分は有効になりません。要素にエラーがある場合は、エラーのある設定が修正されるまで、ポリシーを適用できません。

ポリシーに含まれるオブジェクトに対する警告テキストを表示するには、その横にある警告アイコン（  ）の上にマウスのポインタを移動します。オブジェクトに対するエラー テキストを表示するには、その横にあるエラー アイコン（  ）の上にマウスのポインタを移動します。

警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。警告が出されているルールを無効にしても、エラー アイコンは消えません。この場合、ルールが無効にされていても、ポリシーは適用されないことに注意してください。

無効な設定について

アクセス コントロール ポリシーが依存する外部の設定は変更される可能性があるため、有効であったアクセス コントロール ポリシー設定が無効になる場合があります。

たとえば、ルールに URL 条件が含まれる場合、URL Filtering ライセンスが有効になっていないデバイスをターゲットに選択すると、そのルールは無効になります。その時点で、ルールの横にエラー アイコンが表示され、ポリシーをそのデバイスに適用できなくなります。適用可能にするには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、または適切なライセンスを有効にする必要があります。

別の例として、ルールの送信元ポートにポート グループを追加した後、そのポート グループを変更して ICMP ポートを含めると、ルールは無効になり、その横に警告アイコンが表示されます。それでもポリシーを適用することはできますが、そのルールが実際にターゲット デバイスに適用されることはありません。

同様に、ルールにユーザを追加した後、LDAP ユーザ認識設定を変更してそのユーザを除外すると、ユーザはアクセス コントロールの対象ユーザではなくなるため、そのルールは適用されなくなります。

以上のいずれの場合にしても、問題についてのアラートのために、アクセス コントロール ポリシーまたはアクセス コントロール ポリシー リストに警告またはエラーが表示されます。

ルールの優先適用について

アクセス コントロール ルールの条件が後続のルールよりも優先して適用され、後続のルールによるトラフィックの照合が回避される場合があります。次に例を示します。

ルール 1：管理者ユーザを許可
ルール 2：管理者ユーザをブロック

上記の 2 番目のルールによってトラフィックがブロックされることはありません。なぜなら、最初のルールによってトラフィックは既に許可されるためです。

どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。次の例では、最初のルールでの VLAN 範囲に 2 番目のルールでの VLAN が含まれるため、最初のルールが 2 番目のルールよりも優先して適用されることになります。

ルール 1：VLAN 22 ～ 33 を許可
ルール 2：VLAN 27 をブロック

次の例では、VLAN が設定されていないルール 1 はあらゆる VLAN と一致します。そのため、ルール 1 が優先して適用され、ルール 2 での VLAN 2 の照合は行われません。

ルール 1：送信元ネットワーク 10.4.0.0/16 を許可
ルール 2：送信元ネットワーク 10.4.0.0/16 の VLAN 2 を許可

あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールは回避されます。次に例を示します。

ルール 1：VLAN 1 URL www.example.com を許可
ルール 2：VLAN 1 URL www.example.com を許可

条件が 1 つでも異なる場合は、後続のルールが回避されることはありません。次に例を示します。

ルール 1：VLAN 1 URL www.example.com を許可
ルール 2: VLAN 2 URL www.example.com を許可

アクセス コントロール ポリシーの管理

ライセンス：任意

[Access Control] ポリシー ページ（[Policies] > [Access Control]）では、現行のアクセス コントロール ポリシーの名前とオプションの説明、および次のステータス情報を確認できます。

- ターゲット デバイスに対してポリシーが最新の状態になっている（緑のテキスト）
- ターゲット デバイスに対してポリシーが失効している（赤のテキスト）

このページのオプションを使用して、さまざまな操作を行うことができます。具体的には、ポリシーの比較、新規ポリシーの作成、ターゲット デバイスへのポリシーの適用、ポリシーのコピー、各ポリシーに最近保存された設定をすべてリストするレポートの表示、ポリシーの編集、ポリシーの削除などです。

ヒント　展開環境の他の防御センターに対して、アクセス コントロール ポリシーをエクスポート/インポートすることもできます。詳細については、「設定のインポートおよびエクスポート」（P.A-1）を参照してください。

デバイスを追加するときの選択内容によっては、次の 2 つのデフォルト アクセス コントロール ポリシーのいずれかが表示され、既にデバイスに適用されていることがあります。

- デフォルト アクセス コントロール ポリシー。すべてのトラフィックをネットワークからブロックします。
- デフォルト侵入ポリシー。すべてのトラフィックを許可し、Balanced Security および Connectivity の侵入ポリシーをネットワーク上のトラフィックに適用します。「侵入ポリシーの設定」（P.20-1）を参照してください。

これらのポリシーはいずれも、独自に作成するポリシーと同じように使用できます。

次の表で、[Access Control] ポリシー ページでポリシーを管理するために実行できる操作を説明します。

表 13-8　アクセス コントロール ポリシーの管理操作

目的	操作
新しいアクセス コントロール ポリシーを作成する	[Create Policy] をクリックします。詳細については、「アクセス コントロール ポリシーの作成」（P.13-33）を参照してください。
既存のアクセス コントロール ポリシーの設定を変更する	編集アイコン（）をクリックします。詳細については、「アクセス コントロール ポリシーの編集」（P.13-34）を参照してください。
アクセス コントロール ポリシーを、そのポリシーのすべてのターゲット デバイスに適用する	ポリシー適用アイコン（）をクリックします。詳細については、「アクセス コントロール ポリシーの適用」（P.13-39）を参照してください。
ポリシーがデバイスに対して失効する原因となった変更内容を判別する	赤いステータス メッセージをクリックして詳細適用ビューを表示した後、変更内容を表示するポリシーおよびデバイスに対して [Out-of-date] をクリックします。詳細については、「選択したポリシー設定の適用」（P.13-42）および「2 つのアクセス コントロール ポリシーの比較」（P.13-37）を参照してください。
アクセス コントロール ポリシーをコピーする	コピー アイコン（）をクリックします。詳細については、「アクセス コントロール ポリシーのコピー」（P.13-35）を参照してください。
アクセス コントロール ポリシーの現行の設定をリストする PDF を表示する	レポート アイコン（）をクリックします。詳細については、「アクセス コントロール ポリシー レポートの表示」（P.13-35）を参照してください。
アクセス コントロール ポリシーを比較する	[Compare Policies] をクリックします。詳細については、「2 つのアクセス コントロール ポリシーの比較」（P.13-37）を参照してください。
アクセス コントロール ポリシーを削除する	削除アイコン（）をクリックして、[OK] をクリックします。ポリシーの削除をキャンセルする場合は、[Cancel] をクリックします。操作を続行するかどうかを確認するプロンプトには、そのポリシーで別のユーザーがまだ保存していない変更があるかどうかも通知されます。

アクセス コントロール ポリシーの作成

ライセンス：任意

新しいアクセス コントロール ポリシーを作成するために最低限必要な操作は、そのポリシーに一意の名前を付けて、デフォルト アクションを指定することです。ポリシーの作成時にポリシー ターゲットを特定する必要はありませんが、このステップを実行してからでないと、ポリシーを

適用することはできません。「ポリシー ターゲットの管理」（P.13-10）を参照してください。

新しいポリシーのデフォルト アクションを選択する際には、次のオプションがあります。

- [Block all traffic] を選択して、[Access Control: Block All Traffic] をデフォルト アクションとして使用するポリシーを作成する
- [Intrusion Prevention] を選択して、[Intrusion Prevention: Balanced Security and Connectivity] をデフォルト アクションとして使用するポリシーを作成する
- [Network Discovery] を選択して、[Network Discovery Only] をデフォルト アクションとして使用するポリシーを作成する

アクセス コントロール ポリシーを作成した後、デフォルト アクションを変更できます。デフォルト アクションの選択に関するガイダンスについては、「デフォルト アクションの設定」（P.13-5）を参照してください。

アクセス コントロール ポリシーの作成方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　[New Policy] をクリックします。

[New Access Control Policy] ポップアップ ウィンドウが表示されます。

ステップ 3　[Name] に一意のポリシー名を入力し、オプションで [Description] にポリシーの説明を入力します。

印刷可能なすべての文字を使用できます。これにはスペースと特殊文字も含まれますが、番号記号（#）、セミコロン（;）、または波カッコ（{}）は使用できません。名前には少なくとも 1 つのスペース以外の文字が含まれている必要があります。

ステップ 4　[Default Action] で、デフォルト アクションを指定します。

ステップ 5　[Available Devices] から、ポリシーを適用するデバイスを選択します。

複数のデバイスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックするか、右クリックをして [Select All] を選択します。表示されるデバイスを絞り込むには、[Search] フィールドに検索文字列を入力します。検索をクリアするには、クリア アイコン（ ）をクリックします。

ステップ 6　[Selected Devices] に、選択したデバイスを追加します。それには、クリックしてドラッグするか、[Add to Policy] をクリックします。

ステップ 7　[Save] をクリックします。

アクセス コントロール ポリシーの [Edit] ページが表示されます。ルールの追加を含め、新しいポリシーの設定方法については、「アクセス コントロール ポリシーの編集」（P.13-34）を参照してください。ポリシーを有効にするには適用する必要があることに注意してください。「アクセス コントロール ポリシーの適用」（P.13-39）を参照してください。

アクセス コントロール ポリシーの編集

ライセンス：任意

ポリシーの [Edit] ページで、ポリシーを設定し、アクセス コントロール ルールを編成できます。詳細については、「ポリシーの設定」（P.13-4）および「ポリシー内でのルールの編成」（P.13-25）を参照してください。

設定を変更すると、変更がまだ保存されていないことを通知するメッセージが表示されます。変更を維持するには、ポリシーの [Edit] ページを終了する前に、ポリシーを保存する必要があります。変更を保存しないでポリシーの [Edit] ページを終了しようとすると、変更がまだ保存されていないことを警告するメッセージが表示されます。この場合、変更を破棄してポリシーを終了するか、ポリシーの [Edit] ページに戻るかを選択できます。

セッションのプライバシーを保護するために、ポリシーの [Edit] ページで 60 分間操作が行われないと、ポリシーの変更が破棄されて、[Access Control] ページに戻されます。30 分間操作が行われなかった時点で、変更が破棄されるまでの分数を示すメッセージが表示されます。以降、このメッセージは定期的に更新されて残りの分数を示します。ページで何らかの操作を行うと、タイマーがキャンセルされます。

2 つのブラウザ ウィンドウで同じポリシーを編集しようとすると、新しいウィンドウで編集を再開するか、元のウィンドウでの変更を破棄して新しいウィンドウで編集を続けるか、または 2 番目のウィンドウをキャンセルしてポリシーの [Edit] ページに戻るかを選択するよう求めるプロンプトが出されます。

複数のユーザが同じポリシーを同時に編集する際、各ユーザに対し、ポリシーの [Edit] ページに変更を保存していない他のユーザを特定するメッセージが表示されます。いずれかのユーザが変更を保存しようとすると、その変更によって他のユーザの変更が上書きされることを警告するメッセージが表示されます。同一のポリシーを複数のユーザが保存する場合、最後に保存された変更が維持されます。

アクセス コントロール ポリシーの編集方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（  ）をクリックします。

ポリシーの [Edit] ページが表示されます。

ステップ 3　次の選択肢があります。

- ポリシーを設定する場合は、「ポリシーの設定」（P.13-4）と「アクセス コントロール ポリシーの設定操作」の表で説明されているすべての操作を使用できます。
- ポリシー ルールを編成する場合は、「ポリシー内でのルールの編成」（P.13-25）と「アクセス コントロール ルールの編成操作」の表で説明されているすべての操作を使用できます。

ステップ 4　設定を保存または廃棄します。次の選択肢があります。

- 変更を保存し、編集を続行する場合は、[Save] をクリックします。
- 変更を保存し、ポリシーを適用する場合は、[Save and Apply] をクリックします。「アクセス コントロール ポリシーの適用」（P.13-39）を参照してください。

  変更を有効にするには、ポリシーを適用する必要があります。
- 変更を破棄する場合は、[Cancel] をクリックし、プロンプトが出されたら [OK] をクリックします。

  変更が廃棄されて、[Access Control] ページが表示されます。

アクセス コントロール ポリシーのコピー

ライセンス：任意

アクセス コントロール ポリシーをコピーして、名前を変更できます。ポリシーをコピーすると、そのポリシーのすべてのルールと設定がコピーされます。

アクセス コントロール ポリシーをコピーする方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にあるコピー アイコン（  ）をクリックします。

[Copy Access Control Policy] ポップアップ ウィンドウが表示されます。

ステップ 3　[Name] に一意のポリシー名を入力します。

印刷可能なすべての文字を使用できます。これにはスペースと特殊文字も含まれますが、番号記号（#）、セミコロン（;）、または波カッコ（{}）は使用できません。名前には少なくとも 1 つのスペース以外の文字が含まれている必要があります。

ステップ 4　[OK] をクリックします。

[Access Control] ページに、コピーしたアクセス コントロール ポリシーが名前のアルファベット順で表示されます。

アクセス コントロール ポリシー レポートの表示

ライセンス：任意

アクセス コントロール ポリシー レポートとは、特定の時点でのポリシーおよびルールの設定を記録したものです。このレポートは、監査目的や、現行の設定を調べるために使用できます。

ヒント　また、ポリシーを現在適用されているポリシーや別のポリシーと比較する、アクセス コントロール比較レポートを生成することもできます。詳細については、「2 つのアクセス コントロール ポリシーの比較」（P.13-37）を参照してください。

アクセス コントロール ポリシー レポートは、次の表に記載するセクションからなります。

表 13-9　アクセス コントロール ポリシー レポートのセクション

セクション	説明
Title Page	ポリシー レポートの名前、ポリシーが最後に変更された日時、その変更を行ったユーザの名前が記載されます。
Table of Contents	レポートの内容が記載されます。
Policy Information	ポリシーの名前と説明、ポリシーを最後に変更したユーザの名前、ポリシーが最後に変更された日時が記載されます。「アクセス コントロール ポリシーの編集」（P.13-34）を参照してください。
Device Targets	ポリシーがターゲットとする管理対象デバイスがリストされます。「ポリシー ターゲットの管理」（P.13-10）を参照してください。
HTTP Block Response HTTP Interactive Block Response	ポリシーに関連付けられている HTTP ブロック応答ページの詳細が記載されます。「HTTP 応答ページの追加」（P.13-12）を参照してください。
Security Intelligence	セキュリティ インテリジェンスのホワイトリストおよびブラックリストの詳細が記載されます。「セキュリティ インテリジェンス データに基づくトラフィックのフィルタリング」（P.13-13）を参照してください。
Default Action	デフォルト アクションが記載されます。「デフォルト アクションの設定」（P.13-5）を参照してください。
Rules	ルール カテゴリ別に、ポリシーに含まれる各ルールのルール アクションおよび条件が記載されます。「アクセス コントロール ルールの概要と作成」（P.14-1）および「ルール カテゴリの処理」（P.13-26）を参照してください。
Referenced Objects	ポリシーで使用されている個々のすべてのオブジェクトおよびグループ オブジェクトの名前と設定が、各オブジェクトが設定されている条件タイプ別（ネットワーク、VLAN、タグなど）に記載されます。「ルール条件について」（P.14-10）および「再利用可能なオブジェクトの管理」（P.5-1）を参照してください。
Variable Sets	変数セットがリストされます。変数セットがルールまたはアクセス コントロール ポリシーのデフォルト アクションにリンクされている場合は、その変数セットに含まれる変数もリストされます。「変数セットの操作」（P.5-19）を参照してください。

アクセス コントロール ポリシー レポートの表示方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　レポートの生成対象とするポリシーの横にあるレポート アイコン（  ）をクリックします。アクセス コントロール ポリシー レポートを生成する前に、必ずすべての変更を保存してください。レポートには、保存された変更のみが表示されます。

システムによってレポートが生成されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウに表示される場合や、レポートをコンピュータに保存するよう求めるプロンプトが出される場合があります。

2 つのアクセス コントロール ポリシーの比較

ライセンス：任意

組織の標準に準拠しているかを確認する目的や、システム パフォーマンスを最適化する目的でポリシーの変更を検討するために、2 つのアクセス コントロール ポリシーの差異を調べることができます。任意の 2 つのポリシーを比較することも、現在適用されているポリシーを別のポリシーと比較することもできます。オプションで、比較した後に PDF レポートを生成することで、2 つのポリシーの間の差異を記録できます。

ポリシーを比較するために使用できるツールは 2 つあります。

- 比較ビューは、2 つのポリシーを左右に並べて表示し、その差異のみを示します。比較ビューの左右のタイトル バーに、それぞれのポリシーの名前が示されます。ただし、[Running Configuration] を選択した場合、現在アクションなポリシーは空白のバーで表されます。

  このツールを使用すると、Web インターフェイスで 2 つのポリシーを表示してそれらに移動するときに、差異を強調表示することができます。

- 比較レポートは、ポリシー レポートと同様の形式ですが、2 つのポリシーの間の差異だけが、PDF 形式で記録されます。

  これを使用して、ポリシーの比較の保存、コピー、出力、共有を行って、さらに検証することができます。

ポリシー比較ツールの概要と使用法の詳細については、次の項を参照してください。

- 「アクセス コントロール ポリシー比較ビューの使用」（P.13-37）
- 「アクセス コントロール ポリシー比較レポートの使用」（P.13-38）

アクセス コントロール ポリシー比較ビューの使用

ライセンス：任意

比較ビューには、両方のポリシーが左右に並べて表示されます。それぞれのポリシーは、比較ビューの左右のタイトル バーに示される名前で特定されます。現在実行されている設定ではない 2 つのポリシーを比較する場合、最後に変更された日時とその変更を行ったユーザがポリシー名と共に表示されます。

2 つのポリシーの間の差異は、次のように強調表示されます。

- 2 つのポリシーの間で異なっている設定は、青色で強調表示され、その差異が赤いテキストで示されます。
- 一方のポリシーにはあり、他方のポリシーにはない設定は、緑色で強調表示されます。

次の表に、実行できる操作を記載します。

表 13-10　アクセス コントロール ポリシー比較ビューの操作

目的	操作
個々の変更の間を移動する	またはタイトル バーの上にある [Previous] または [Nex] をクリックします。 左側と右側の間で移動するには、中央の二重矢印アイコン（  ）をクリックします。表示する差異を変更するには、[Difference] 番号で調整します。
新しいポリシー比較ビューを生成する	[New Comparison] をクリックします。 [Select Comparison] ウィンドウが表示されます。詳細については、「アクセス コントロール ポリシー比較レポートの使用」（P.13-38）を参照してください。
ポリシー比較レポートを生成する	[Comparison Report] をクリックします。 ポリシー比較レポートは、2 つのポリシーの間の差異だけをリストした PDF ドキュメントです。

アクセス コントロール ポリシー比較レポートの使用

ライセンス：任意

アクセス コントロール ポリシー比較レポートとは、ポリシー比較ビューで識別された、2 つのアクセス コントロール ポリシーの間、またはポリシーと現在適用中のポリシーの間にあるすべての差異を、PDF 形式で記録したものです。このレポートを使用することで、2 つのポリシー設定の間の違いをさらに調べ、調査結果を保存して共有できます。

ユーザは、アクセス権限が与えられている任意のポリシーの比較ビューから、アクセス コントロール ポリシー比較レポートを生成できます。ポリシー レポートを生成する前に、必ずすべての変更を保存してください。レポートには、保存されている変更だけが表示されます。

ポリシー比較レポートの形式は、ポリシー レポートと同様です。唯一異なる点は、ポリシー レポートにはポリシーのすべての設定が記載される一方、ポリシー比較レポートにはポリシー間で異なる設定だけがリストされることです。アクセス コントロール ポリシー比較レポートは、「アクセス コントロール ポリシー レポートのセクション」の表に記載されているセクションからなります。

ヒント　同様の手順を使用して、侵入ポリシー、ファイル ポリシー、システム ポリシー、またはヘルス ポリシーを比較できます。

2 つのアクセス コントロール ポリシーを比較する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　[Compare Policies] をクリックします。

[Select Comparison] ウィンドウが表示されます。

ステップ 3　[Compare Against] ドロップダウン リストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[Other Policy] を選択します。

  ページが更新されて、[Policy A] と [Policy B] という 2 つのドロップダウン リストが表示されます。
- 現在適用されているポリシーを別のポリシーと比較する場合は、[Running Configuration] を選択します。

  ページが更新されて、[Target/Running Configuration A] と [Policy B] という 2 つのドロップダウン リストが表示されます。

ステップ 4　選択した比較タイプによって、次の選択項目があります。

- 2 つの異なるポリシーを比較することを選択した場合は、[Policy A] および [Policy B] ドロップダウン リストのそれぞれから、比較するポリシーを選択します。
- 現在実行されている設定を別のポリシーと比較する場合は、[Policy B] ドロップダウン リストから 2 つ目のポリシーを選択します。

ステップ 5　ポリシー比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ 6　オプションで、[Comparison Report] をクリックして、アクセス コントロール ポリシー比較レポートを生成します。

アクセス コントロール ポリシー比較レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウに表示される場合や、レポートをコンピュータに保存するよう求めるプロンプトが出される場合があります。

アクセス コントロール ポリシーの適用

ライセンス：任意

アクセス コントロール ポリシーに変更を加えた後、そのポリシーを 1 つ以上のデバイスに適用することで、デバイスがモニタ対象とするネットワークに設定の変更を実装できます。ポリシーを適用するには、その前に、ポリシーを適用するターゲット デバイスを指定する必要があります。「ポリシー ターゲットの管理」（P.13-10）を参照してください。

アクセス コントロール ポリシーを適用する際には、次の点に注意してください。

- 特殊なケースとして、アクセス コントロール ポリシーを適用すると、トラフィック フローと処理が一時的に中断されたり、いくつかのパケットが検査されないまま通過したりすることがあります。このような事態は、Snort® プロセスが再起動すると発生します。このプロセスが再起動するのは、たとえば、防御センター アップグレードに続いて新しいバージョンの Snort を管理対象デバイスにプッシュするアクセス コントロール ポリシーを適用する場合や、共有オブジェクト ルールが含まれるルールのインポートを行った後に初めてポリシーを適用する場合です。さらに場合によっては、VDB アップデートを更新すると、Snort プロセスが再起動することもあります。インラインで FireSIGHT Software for X-Series を配置していて、ロード バランシングおよび冗長性のために複数の VAP-VAP グループを設定している場合、デバイスが再起動するまで影響を受ける VAP をロード バランス リストから削除し、再起動した後に再インストールすることで、処理の中断を防ぐことができます。詳細については、「ソフトウェア更新の実行」（P.53-3）、「脆弱性データベースの更新」（P.53-14）、「ルールの更新とローカル ルール ファイルのインポート」（P.53-16）、および『*FireSIGHT Software for X-Series Installation Guide*』を参照してください。

- 3D7010、3D7020、および 3D7030 管理対象デバイスでは、アクセス コントロール ポリシーを適用するまでに最大 5 分の時間がかかります。なるべく不都合が生じないように、アクセス コントロール ポリシーは変更時間帯に適用してください。
- 多数の FireSIGHT 機能（セキュリティ インテリジェンス、ファイル キャプチャ、多くのルールが設定された侵入ポリシー、URL フィルタリングなど）を有効にしたアクセス コントロール ポリシーを適用すると、一部のローエンド ASA FirePOWER デバイスでは、デバイスのメモリー割り当てが最大限まで使用された状態になってメモリー使用量の警告が断続的に出されることがあります。
- アクセス コントロール ポリシーに、最近適用されたデバイス設定によって有効になるライセンスが必要な場合、システムはそのデバイス設定の適用が完了するまで、アクセス コントロール ポリシー適用タスクをキューに入れます。
- [Drop and Generate Events] に設定された侵入ルールが、[Drop when Inline] が選択されている侵入ポリシーに関連付けられている場合、この侵入ポリシーを、パッシブ インターフェイス セットまたはタップ モードのインライン インターフェイス セットを使用するデバイスに適用しても、これらの侵入ルールはイベントを生成するものの、パケットをドロップすることも、攻撃をブロックすることも**ありません**。詳細については、「インライン展開での破棄動作の設定」（P.20-15）および「タップ モード」（P.7-8）を参照してください。
- 異なるバージョンの FireSIGHT システムを実行しているスタック デバイスに、アクセス コントロール ポリシーを適用することはできません （たとえば、それらのデバイスの 1 つでアップグレードが失敗した場合などにバージョンが異なることがあります）。詳細については、「スタックに含まれるデバイスの管理」（P.6-40）を参照してください。
- 一部の機能には、最小バージョンの FireSIGHT システム、または特定のデバイス モデルが必要です。ジオロケーション データに基づくアクセス コントロールを実行するには、管理対象デバイスがバージョン 5.3 以降を実行している必要があります。シリーズ 2 アプライアンスでサポートされていない機能の概要については、「管理対象デバイスの各モデルでサポートされる機能」（P.1-9）を参照してください。
- クイック適用ポップアップ ウィンドウの適用ボタンのラベルは、アクセス コントロール ポリシー、侵入ポリシー、またはその両方の適用を許可されているかによって異なります。「アクセス コントロール ポリシーでのカスタム ユーザ ロールの使用」（P.13-9）を参照してください。
- ポリシーのアプリケーション ルール条件ごとに、少なくとも 1 つのディテクタが有効にされている必要があります。あるアプリケーションのディテクタが 1 つも有効になっていない場合、システムは、アプリケーションに関するシスコ提供の全ディテクタを自動的に有効化します。それが 1 つも存在しない場合は、アプリケーション用に最後に変更されたユーザ定義ディテクタが有効化されます。詳細については、「アプリケーション条件を使用する」（P.14-25）を参照してください。
- アクセス コントロール ポリシーに追加できる固有の侵入ポリシーの数に制限はありません。ただし、アクセス コントロール ポリシーをデバイスに適用するときに、デバイスでサポートされる侵入ポリシーの最大数を超えていることを警告するポップアップ ウィンドウが表示される場合があります。この最大値は、デバイスの物理メモリやプロセッサ数をはじめ、さまざまな要因によって左右されます。侵入ポリシーと変数セットの固有のペアは、1 つのポリシーとしてカウントされることに注意してください。

ヒント　デバイスでサポートされる侵入ポリシーの数を超えた場合、アクセス コントロール ポリシーを再評価してください。いくつかの侵入ポリシーを統合すると、複数のアクセス コントロール ルールに 1 つの侵入ポリシーを関連付けることができます。

- 適用されたポリシー、または現在適用されているポリシーを削除することはできません。
- アクセス コントロール ポリシーおよび関連する侵入ポリシーは任意の組み合わせで適用することができますが、アクセス コントロール ポリシーを適用すると、そのポリシーに関連付けられたすべてのファイル ポリシーが自動的に適用されます。ファイル ポリシーを個別に適用することはできません。

詳細については、次の項を参照してください。

- 「完全なポリシーの適用」（P.13-41）で、クイック適用オプションを使用して、アクセス コントロール ポリシーを関連する侵入ポリシーおよびファイル ポリシーと併せて適用する方法について説明しています。
- 「選択したポリシー設定の適用」（P.13-42）で、アクセス コントロール ポリシー、関連する侵入ポリシー、またはその両方の組み合わせを選択して適用する方法について説明しています。

完全なポリシーの適用

ライセンス：任意

アクセス コントロール ポリシーは、任意の時点で適用することができます。アクセス コントロール ポリシーを適用すると、そのポリシーがターゲットとするデバイスで現在実行されているものとは異なる侵入ポリシーおよびファイル ポリシーも、ポリシーに関連付けられたポリシーとして適用されます。単一のクイック適用操作として、ポップアップ ウィンドウを使用してすべてのポリシーを適用することができます。クイック適用オプションを使用する場合、変更されていない侵入ポリシーやファイル ポリシーは適用されません。

クイック適用ポップアップ ウィンドウの適用ボタンのラベルは、アクセス コントロール ポリシー、侵入ポリシー、またはその両方の適用を許可されているかによって異なります。「アクセス コントロール ポリシーでのカスタム ユーザ ロールの使用」（P.13-9）を参照してください。

完全なアクセス コントロール ポリシーのクイック適用を実行する方法：

アクセス：Admin/Security Approver

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　適用するポリシーの横にある適用アイコン（  ）をクリックします。

[Apply Access Control Rules] ポップアップ ウィンドウが表示されます。

または、ポリシーの [Edit] ページで [Save and Apply] をクリックするという方法もあります。「アクセス コントロール ポリシーの編集」（P.13-34）を参照してください。

ステップ 3　[Apply All] をクリックします。

ポリシー適用タスクがキューに入れられます。[OK] をクリックして [Access Control] ページに戻ります。

ヒント　ポリシー適用タスクの進行状況は、[Task Status] ページ（[System] > [Monitoring] > [Task Status]）でモニタできます。

選択したポリシー設定の適用

ライセンス：任意

ポリシー適用の詳細ページを使用して、アクセス コントロール ポリシーや関連する侵入ポリシーに変更を適用できます。詳細ページには、ポリシーがターゲットとするデバイスがリストされ、デバイス別のアクセス コントロール ポリシーおよびそれに関連付けられた侵入ポリシーの各カラムが表示されます。ターゲット デバイスごとに、変更をアクセス コントロール ポリシー、個々の侵入ポリシーまたはその組み合わせ、あるいはその両方に適用するかどうかを指定できます。

次の場合には、アクセス コントロール ポリシーとそれに関連付けられた侵入ポリシーの両方を適用する必要があります。

- アクセス コントロール ポリシーが初めてデバイスに適用される場合
- アクセス コントロール ポリシーに新しく侵入ポリシーが追加される場合

いずれの場合も、アクセス コントロール ポリシーの状態と侵入ポリシーの状態はリンクされます。つまり、両方とも適用するか、どちらも適用しないかのいずれかを選択する必要があります。

どの侵入ポリシーを適用するかに関わらず、アクセス コントロール ポリシーを適用すると、そのポリシーがターゲットとするデバイスで現在実行されているものとは別のファイル ポリシーが、ポリシーに関連付けられたファイル ポリシーとして自動的に適用されます。ファイル ポリシーを個別に適用することはできません。

[Access Control Policy] カラム

[Access Control Policy] カラムには、アクセス コントロール ポリシーを適用するかどうかを指定するチェック ボックスがあります。

ヒント　タスク キューにまだ入っているポリシー、つまり適用タスクがまだ完了していないポリシーを再び適用することもできますが、それには何の利点もありません。

ステータス メッセージには、ポリシーが現在最新の状態であるか、失効しているかどうかが示されます。ポリシーが失効している場合は、新しいブラウザ ウィンドウで、そのポリシーと現在実行中のポリシーとの比較結果を表示できます。この比較には、アクセス コントロール ポリシーに関連付けられている侵入ポリシーでの差異は含まれません。

[Intrusion Policies] カラム

[Intrusion Policies] カラムには、アクセス コントロール ポリシーに関連付けられている侵入ポリシーをデバイスに適用するかどうかを指定する 1 つ以上のチェック ボックスがあります。単一のグレー表示されたチェック ボックスは、関連付けられているすべての侵入ポリシーが、現在実行されているポリシーと同じであることを意味します。この場合、チェック ボックスはクリアされていて、選択することはできません。変更されていない侵入ポリシーを適用することはできません。このカラムには、変更されている侵入ポリシーだけがリストされ、個別に選択できるようになっています。ポリシーに含まれる複数のルールに同じ侵入 ポリシーが関連付けられている場合、その侵入ポリシーはデバイスごとに一度だけリストされます。

前述したようにアクセス コントロール ポリシーと侵入ポリシーを一緒に適用しなければならない場合、侵入ポリシーのチェック ボックスは選択された状態でグレー表示され、変更することができません。これに該当するのは次のような場合です。

- アクセス コントロール ポリシーが初めてデバイスに適用される場合
- アクセス コントロール ポリシーに新しく侵入ポリシーが追加される場合

ステータス メッセージには、侵入ポリシーが現在最新の状態であるか、失効しているかどうかが示されます。侵入ポリシーが、リストされたデバイスで現在実行されている侵入ポリシーと同じでない場合、その侵入ポリシーは失効していることになります。侵入ポリシーがデバイス上の侵入ポリシーとまったく同じであれば、その侵入ポリシーは最新の状態です。ポリシーが失効している場合は、新しいブラウザ ウィンドウで、そのポリシーと現在実行中のポリシーとの比較結果を表示できます。

選択したアクセス コントロール ポリシー設定を適用する方法：

アクセス：Admin/Security Approver

ステップ 1　[Policies] > [Access Control] を選択します。

[Access Control] ページが表示されます。

ステップ 2　適用するポリシーの横にある適用アイコン（）をクリックします。

[Apply Access Control Rules] ポップアップ ウィンドウが表示されます。

または、ポリシーの [Edit] ページで [Save and Apply] をクリックするという方法もあります。「アクセス コントロール ポリシーの編集」（P.13-34）を参照してください。

ステップ 3　[Details] をクリックします。

詳細な [Apply Access Control Rules] ポップアップ ウィンドウが表示されます。

ヒント　このポップアップ ウィンドウは、[Access Control] ページ（[Policies] > [Access Control]）から開くこともできます。それには、ポリシーの [Status] カラムに示されている失効メッセージをクリックします。

ステップ 4　デバイス名の横にあるアクセス コントロール ポリシーのチェック ボックスを選択するかクリアにして、アクセス コントロール ポリシーをターゲット デバイスに適用するかどうかを指定します。

ステップ 5　デバイス名の横にある侵入ポリシーのチェック ボックスを選択するかクリアして、侵入ポリシーをターゲット デバイスに適用するかどうかを指定します。

ステップ 6　[Apply Selected Configurations] をクリックします。

ポリシー適用タスクがキューに入れられます。[OK] をクリックして [Access Control] ページに戻ります。

ヒント　ポリシー適用タスクの進行状況は、[Task Status] ページ（[System] > [Monitoring] > [Task Status]）でモニタできます。

注　デバイスでサポートされる侵入ポリシーの最大数を超えていることを警告するポップアップ ウィンドウが表示される場合があります。アクセス コントロール ポリシーを正常に適用するには、適用する（デフォルト アクションを含む）侵入ポリシーの数が最大数に収まるまで、アクセス コントロール ポリシーから侵入ポリシーを削除します。