CHAPTER 14

アクセス コントロール ルールの概要と作成

一連の *アクセス コントロール ルール*は、アクセス コントロール ポリシーの主要なコンポーネントです。これらなしでも基本的なアクセス コントロール ポリシーを作成できますが、アクセス コントロール ルールを使用すると、どのトラフィックがネットワークに入ることができるか、出て行くことができるか、または出ずに内部を通過できるかをきめ細かく管理できます。たとえば、一部またはすべてのソーシャル ネットワーキング トラフィックをブロックしたり、社内の営業部門が会計レコードにアクセスできないようにしたり、どのユーザがどのサイトやネットワークにアクセスするかをモニタしたりすることができます。

注 ハードウェアベースの Fast-Path ルールおよびセキュリティ インテリジェンスベースのトラフィック フィルタリング（ブラックリスト機能）は、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**行われます。

アクセス コントロール ポリシー内では、システムによってルール番号の上位から下位の順序で、トラフィックがルールに照合されます。ルールの順序などの基本属性に加えて、各ルールには次に示す主要なコンポーネントがあります。

- 一連の*ルール条件*：制御の対象となる特定のトラフィックを識別します
- *ルール アクション*：ルールの条件を満たすトラフィックがシステムによってどのように処理されるかを決定します
- ファイル、マルウェア、および侵入に対する*インスペクション*オプション：このオプションがない場合には許可されるトラフィックに対して一致を検査し、任意選択でブロックできます
- *ロギング*オプション：該当するトラフィックと、それがルールによってどのように処理されたかの記録を保持できます

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、セキュリティ インテリジェンスのブラックリストに含まれず、しかもポリシー内のモニタ ルール以外のどの条件も満たさないトラフィックを処理します。アクセス コントロール ポリシーおよびデフォルト アクションの詳細については、「アクセス コントロール ポリシーの使用」（P.13-1）を参照してください。

ヒント 侵入検知および防御を実行するために FireSIGHT システムを使用する場合、ディスカバリ データを活用する必要がなければ、新しいディスカバリを無効化することでパフォーマンスを最適化できます。まず、適用されるアクセス コントロール ポリシーに、ユーザ、アプリケーション、または URL の条件を扱うルールが含まれないことを確認してください。その後、ネットワーク検出ポリシーからすべてのルールを削除し、それを管理対象デバイスに適用します。ディスカバリの設定の詳細については、「ネットワーク検出の概要」（P.35-1）を参照してください。

任意のライセンスを使ってアクセス コントロール ルールを作成できますが、ルール条件とインスペクション オプションをによっては、アクセス コントロール ポリシーのターゲット デバイスで特定のライセンス機能を有効化する必要があります。ライセンスが必要な機能を使用するポリシーを、ライセンス供与されていないデバイスに適用することはできません。防御センターでは、ライセンス供与されてい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が使用されます。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 ルールを使用するために必要なライセンスを示します。

表 14-1　アクセス コントロール ルールのライセンス要件

以下のルールを含むアクセス コントロール ポリシーを適用する場合	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、またはポートの条件を使用するルール、あるいはリテラル URL および URL オブジェクトのみを使用する URL 条件を使用するルール	任意	任意	任意：例外として、シリーズ 2 デバイスはリテラル URL および URL オブジェクトを使って URL フィルタリングを実行できず、ASA FirePOWER モジュールは VLAN タグ条件を使ってトラフィックを照合できません
侵入ポリシー、またはマルウェア検出/ブロックを実行しないファイル ポリシーに関連付けられているルール	Protection	任意	任意：例外として、シリーズ 2 デバイスはセキュリティ インテリジェンス フィルタリングを実行できません
マルウェア検出/ブロックを実行するファイル ポリシーに関連付けられているルール	Malware	任意（DC500 を除く）	シリーズ 3、仮想、X シリーズ、ASA FirePOWER
アプリケーション条件またはユーザ条件を使用するルール	Control	任意：例外として、DC500 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
位置情報条件を使用するルール	FireSIGHT	任意（DC500 を除く）	シリーズ 3、仮想、ASA FirePOWER
URL カテゴリおよびレピュテーション データを使用する URL 条件を含むルール	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 ルールの詳細については、次の項を参照してください。

- 「アクセス コントロール ルールの作成と編集」（P.14-3）
- 「ルール アクションについて」（P.14-6）
- 「ルール条件とそのメカニズムについて」（P.14-10）
- 「さまざまな条件タイプを使用する」（P.14-17）
- 「許可されたトラフィックに対するファイル インスペクションと侵入インスペクションの実行」（P.14-35）
- 「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）
- 「ルールにコメントを追加する」（P.14-45）

アクセス コントロール ルールの作成と編集

ライセンス：任意

アクセス コントロール ルールは設定や条件からなる単純なセットであり、次のような機能を持ちます。

- ネットワーク トラフィックを限定する
- その限定条件に一致するトラフィックをさらに検査/ロギングするかどうか、またその方法を指定する
- 最終的なトラフィックのフローを決定する

アクセス コントロール ルールは、既存のアクセス コントロール ポリシーの中に作成し、編集します。各ルールは 1 つのポリシーにのみ属します。

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、防御センターは、ポリシーで定義された各ルールを展開されたルール セットとしてデバイスに送信します。このセットの各ルールは、ルール内のさまざまな条件を組み合わせた 1 つの可能な組を表します。たとえば、送信元ゾーンとして内部セキュリティ ゾーン、さらに送信元ポート LDAP と HTTPS を含む 1 つのルールは、2 つのルールとしてデバイスに送信されます。1 つは LDAP 送信元ポートを介した内部送信元ゾーンのトラフィックに一致し、もう 1 つは HTTPS 送信元ポートを介した内部送信元ゾーンのトラフィックに一致します。

ただし、アクセス コントロール ポリシーに複雑なルールが多数含まれる場合、展開されたルールの数がそのデバイスでの許容数を超えると、そのポリシーが管理対象デバイスに適用されない可能性があることに注意してください。このような状況が生じた場合、ルールの条件を分析して、不要な設定を除去できるかどうか確認してください。

ルールの追加と編集は同様の Web インターフェイスで行います。ページ上部でルール名、状態、アクション、位置を指定します。ページの左側のタブを使用して、条件を構築します。条件タイプごとに独自のタブがあります。ページの右側のタブを使用して、インスペクションとロギングのオプションを設定し、ルールにコメントを追加します。

次のリストは、アクセス コントロール ルールの設定可能なコンポーネントを示しています。

Name

各ルールに一意の名前を付けます。30 文字までの印刷可能文字を使用できます。スペースや特殊文字を含めることができますが、コロン（:）は使用できません。

Rule State

デフォルトでは、ルールが有効状態になります。ルールを無効状態にすると、システムはネットワーク トラフィックの評価にそのルールを使用しません。アクセス コントロール ポリシーでルールのリストを表示するとき、無効状態のルールはグレーで表示されますが、変更は可能です。

Action

ルールのアクションは、ルールの条件に一致するトラフィックがシステムによってどのように処理されるかを決定します。一致するトラフィックに対するアクションとして、信頼、モニタ、ブロック、または許可（追加のインスペクションあり/なし）が可能です。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、モニタ アクセス コントロール ルール以外のどの条件にも一致しないトラフィックを処理します。

注　アクセス コントロール ルールのアクションとポリシーのデフォルト アクションが一緒に機能して、侵入、ファイル、またはネットワーク検出のいずれかのポリシーを使って検査可能なネットワーク トラフィックを決定します。システムは、信頼されたトラフィックとブロックされたトラフィックに対してインスペクションを実行**しません**。

ルール アクションの詳細、およびルール アクションがインスペクションとトラフィック フローに与える影響の詳細については、「ルール アクションについて」（P.14-6）を参照してください。

現在のインスペクションとロギングの設定

IPS、**Files**、および Logging の各オプションは、ルールで現在選択されている侵入ポリシー、ファイル ポリシー、および ロギング の各オプションを示します。[IPS] または [Files] 設定をクリックして [Inspection] タブを開くか、[Logging] 設定をクリックして [Logging] タブを開きます。

位置（順序とカテゴリ）

アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で先頭から順にアクセス コントロール ルールをトラフィックと照合します。オプションで、カテゴリ別にルールをグループ化できます。デフォルトで、システムには 3 つのカテゴリ（管理者、標準、ルート）があります。独自のカスタム カテゴリを任意の位置に追加できますが、シスコ提供のカテゴリを削除したり、それらの順序を変更したりすることはできません。

ルールをポリシーに追加するときには、2 つの方法のいずれかに従ってルールの位置を指定します。最初の方法は、カテゴリの中にそれを**挿入**する方法で、そのカテゴリの（数値順で）最後の位置になります。別の方法は、ルール番号を参照ポイントとして使用する方法で、特定のルールの**上**または**下**にそれを配置できます。既存のルールを編集するときには、同様の方法でルールを**移動**できます。詳細については、「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。

条件

ルール条件は、制御の対象となる特定のトラフィックを識別します。条件では、複数の属性を任意に組み合わせてトラフィックを照合できます。属性にはセキュリティ ゾーン、ネットワーク、VLAN、Active Directory LDAP ユーザまたはグループ、アプリケーション、トランスポート プロトコル ポート、送信元/宛先の国または大陸、URL 情報などがあります。単純な条件または複雑な条件が可能で、場合によってはアクセス コントロール ポリシーの対象デバイスにライセンスを適用する必要もあります。

条件の追加の詳細については、「ルール条件とそのメカニズムについて」（P.14-10）および「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。

ファイルおよび侵入に関するインスペクション オプション

ルールのインスペクション オプションの適用対象となるのは、通常であればそのまま許可されるトラフィックです。追加のインスペクションを実行するようシステムを設定するには、侵入ポリシーまたはファイル ポリシー（またはその両方）をルールに関連付けて、変数セットを侵入ポリシーにリンクします。

ファイル ポリシーは*ファイル制御*を実行します。つまり、ユーザが特定のアプリケーション プロトコルを介して特定の種類のファイルをアップロード（送信）またはダウンロード（受信）しようとすると、それを検出してブロックすることができます。また、ファイル

ポリシーでシスコの高度なマルウェア対策機能を使用して、伝送された特定のファイルが組織にとって脅威となるかどうかを判別し、ブロックすることができます。侵入ポリシーは、侵入検知および防御を実行し、有害なパケットをドロップする機能があります。

両方のタイプのインスペクションには、Protection ライセンスが必要です。AMP には、Malware ライセンスが必要です。ルールと侵入ポリシーまたはファイル ポリシーとの関連付けの詳細については、「許可されたトラフィックに対するファイル インスペクションと侵入インスペクションの実行」（P.14-35）を参照してください。

ロギング オプション

アクセス コントロール ルールのロギング オプションを使用すると、一致するトラフィックのレコードを保持するかどうか、およびそれを保持する方法を指定し、そのトラフィック内でのファイルやマルウェアの検出をログに記録することができます。

一般に、接続の開始時または終了時（またはその両方）で接続イベントをログに記録できます。ただし、ブロックされたトラフィックに関しては、一致するトラフィックが追加のインスペクションはされずに拒否されるため、ログに記録できるのはトラフィックの接続開始イベントだけです。さらに、システムはモニタ対象トラフィックの接続終了イベントを自動的にロギングしますが、モニタ対象トラフィックの接続開始ロギングがされるかどうかは、デフォルト アクション、またはトラフィックによりトリガーされるモニタ ルール以外の最初のルールによって決定されます。

接続終了でログに記録することを選んだ場合には、システムが接続終了を検出したとき、一定時間後に接続終了が検出されない場合、またはメモリ制約のためセッションをトラックできなくなった場合にイベントが生成されます。

接続のログは、防御センター データベースの他に、システム ログ（Syslog）または SNMP トラップ サーバに記録できます。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。

コメント

アクセス コントロール ルールで変更を保存するたびに、コメントを追加できます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更日と変更理由を記したりすることができます。あるルールの全コメントのリストを表示し、各コメントを追加したユーザやコメント追加日を確認することができます。詳細については、「ルールにコメントを追加する」（P.14-45）を参照してください。

アクセス コントロール ルールを作成または編集する方法：

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　ルールの追加先にするアクセス 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　次のように新しいルールを追加するか、既存のルールを編集します。

- 新しいルールを追加するには、[Add Rule] をクリックします。
- 既存のルールを編集するには、そのルールの横にある編集アイコン（  ）をクリックします。

[Add Rule] ページまたは [Editing Rule] ページが表示されます。

ヒント　右クリック コンテキスト メニューを使用して、さまざまなルール作成/管理操作を実行することができます（「コンテキスト メニューの使用」（P.2-6）を参照）。また、ルールをドラッグ アンド ドロップして順序を変更することもできます。

ステップ 4　前述の方法で、ルールのコンポーネントを設定します。次の設定をするか、デフォルト設定をそのまま使用することができます。

- ルールに一意の名前 [Name] を付ける必要があります。
- ルールを有効にするかどうか [Enabled] を指定します。
- ルールの [Action] を選択します。
- ルールの位置を指定します。
- ルールの条件を設定します。
- ルールの [Inspection] オプションを設定します。
- [Logging] オプションを指定します。
- [Comment] を追加します。

ステップ 5　[Add] または [Save] をクリックします。

変更が保存されます。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）。

ルール アクションについて

ライセンス：任意

各アクセス コントロール ルールに関連付けられるアクションは、次の事柄を決定します。

- ルールの条件に一致するトラフィックに対して、システムで信頼、モニタリング、ブロック、許可（追加のインスペクションあり/なし）のどのアクションを実行するか
- いくつかのルール アクションの場合、一致するトラフィックの通過を許可する前に、システムで侵入ポリシー、ファイル ポリシー、ネットワーク検出ポリシーを使ってトラフィックに対する追加のインスペクションを行うかどうか
- 一致するトラフィックの詳細をいつ、どのようにログに記録するか

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、モニタ以外のどのアクセス コントロール ルールの条件にも一致しないトラフィックを処理します（「デフォルト アクションの設定」（P.13-5）を参照）。ルール アクションの詳細と、接続ロギングに与える影響については、以下の項および「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。

許可

許可アクションにより、一致するトラフィックの通過が許可されます。オプションで、許可ルールに侵入ポリシーまたはファイル ポリシー（またはその両方）を関連付けることもできます。この 2 種類のポリシーは、次のように追加のインスペクションを行い、独自の設定に従ってネットワーク トラフィックをブロックすることができます。

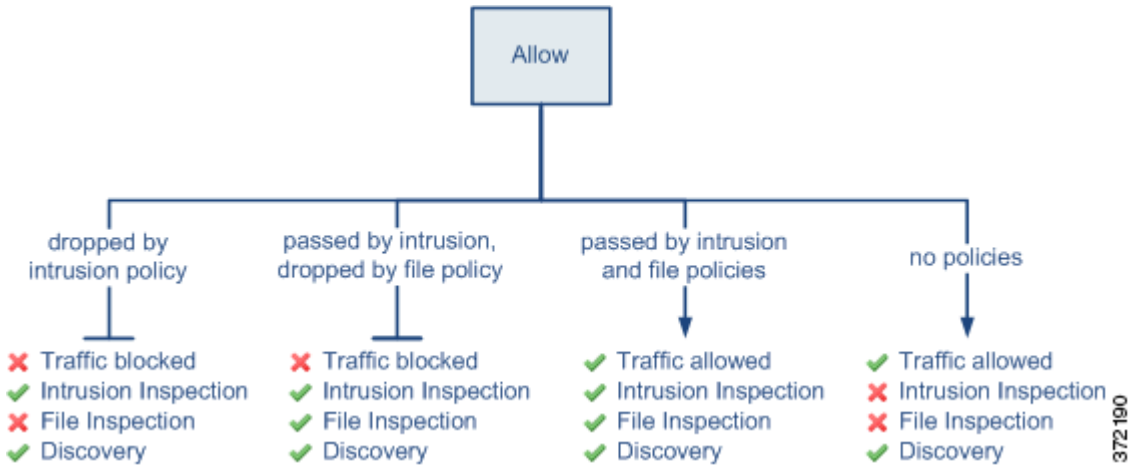
- ファイル ポリシーを関連付けて使用すると、ファイル制御を実行できます。つまり、ユーザが特定のアプリケーション プロトコルを介して特定の種類のファイルをアップロード（送信）またはダウンロード（受信）しようとすると、それを検出してブロックすることができます。また、ファイル ポリシーを使用すると、そのようなファイルの限定セットに対してマルウェア検査を実行し、オプションで、検出されたマルウェアをブロックできます。
- 侵入ポリシーを関連付けて使用すると、侵入検知および防御の設定に従ってネットワーク トラフィックを分析し、オプションで、有害なパケットをドロップできます。

侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付ける方法については、「許可されたトラフィックに対するファイル インスペクションと侵入インスペクションの実行」（P.14-35）を参照してください。

下の図に、許可ルールの条件（またはユーザによりバイパスされるインタラクティブ ブロック ルール（「インタラクティブ ブロックおよびリセット付きインタラクティブ ブロック」（P.14-9）を参照）の条件）を満たすトラフィックに対して実行されるインスペクションの種類を示します。侵入インスペクションの前にファイル インスペクションが行われることに注意してください。そこでブロックされたファイルに対しては、侵入関連の exploit は検査されません。

単純化のために、侵入ポリシーとファイル ポリシーの両方がアクセス コントロール ルールに関連付けられている状態（またはどちらも関連付けられていない状態）のトラフィック フローを図に示しています。ただし、いずれか一方を設定して他方は設定なしにすることもできます。ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーが決定します。侵入ポリシーがない場合、トラフィック フローはファイル ポリシーが決定します。

トラフィックが侵入ポリシーとファイル ポリシーのどちらかによって検査またはドロップされるかどうかに関わらず、システムはネットワーク検出を使ってトラフィックを検査できます。



注　**許可**ルール アクションを選択しても、ディスカバリ インスペクションが必ず行わ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。

許可されたネットワーク トラフィックは、接続の開始および終了の両方でログに記録することができます。

信頼

信頼アクションでは、トラフィックは追加のインスペクションなしで通過を許可されます。信頼されたトラフィックを、ファイル ポリシー、侵入ポリシー、またはネットワーク検出ポリシーで検査することはできません。

信頼されたネットワーク トラフィックは、接続の開始および終了の両方でログに記録できます。信頼ルールで検出された TCP 接続は、次のようにアプライアンスに応じて異なる方法でログに記録されることに注意してください。

- シリーズ 2、仮想アプライアンス、および FireSIGHT Software for X-Series では、信頼ルールによって最初のパケットで検出された TCP 接続だけが接続終了イベントを発生させます。システムは、最後のセッション パケットの 1 時間後にイベントを生成します。
- シリーズ 3 アプライアンスでは、信頼ルールによって最初のパケットで検出された TCP 接続は、モニタ ルールの有無に応じて異なるイベントを発生させます。モニタ ルールがアクティブな場合、システムはパケットを評価し、接続の開始および終了イベントを生成します。アクティブなモニタ ルールがない場合、システムは接続終了イベントだけを生成します。

モニタ

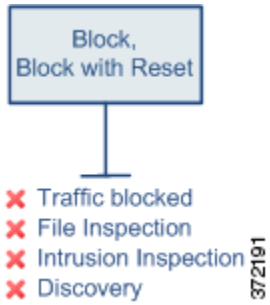
モニタ アクションはトラフィック フローに影響を与えません。つまり、一致するトラフィックが直ちに許可または拒否されることはありません。その代わり、追加のルールが存在する場合はそのルールに照らしてトラフィックが照合され、許可/拒否が決定されます。モニタ ルール以外の一致する最初のルールが、トラフィック フローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、システムはデフォルト アクションを使用します。

モニタ ルールの主な目的はネットワーク トラフィックのトラッキングなので、システムはモニタ対象トラフィックの接続終了イベントを自動的にログに記録します。つまり、トラフィックが他のルールに一致せず、デフォルト アクションでロギングが有効になっていない場合でも、接続はログに記録されます。ログに記録される接続に関連付けられるアクションは、接続によってトリガーされるモニタ ルール以外の最初のアクション、またはデフォルト アクションのいずれかです。

ローカル内トラフィックがレイヤ 3 展開のモニタ ルールに一致する場合、そのトラフィックはインスペクションをバイパスすることがあります。トラフィックのインスペクションを確実に実行するには、トラフィックをルーティングしている管理対象デバイスの詳細設定で [Inspect Local Router Traffic] を有効にします。

ブロックおよびリセット付きブロック

ブロック アクションおよび**リセット付きブロック** アクションはトラフィックを拒否し、追加のインスペクションは行われません。リセット付きブロック ルールでは接続のリセットも行います。ブロックされたトラフィックを、ファイル ポリシー、侵入ポリシー、またはネットワーク検出ポリシーで検査することはできません。

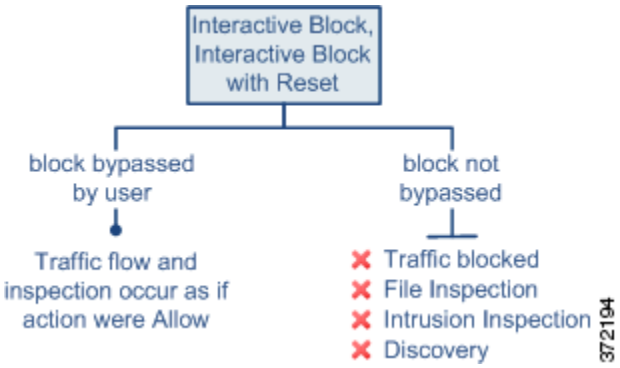


ブロックされたネットワーク トラフィックは、接続の開始時にのみログに記録できます。

インタラクティブ ブロックおよびリセット付きインタラクティブ ブロック

HTTP トラフィックの場合、**インタラクティブ ブロック** アクションおよび**リセット付きインタラクティブ ブロック** アクションを使用すると、ユーザは警告ページをクリックスルーすることで、Web サイトのブロックをバイパスできます。ユーザがブロックをバイパスしない場合、一致するトラフィックは拒否され、追加のインスペクションは行われません。リセット付きインタラクティブ ブロック ルールでは接続のリセットも行います。警告ページの設定については、「HTTP 応答ページの追加」（P.13-12）を参照してください。

一方、ユーザがブロックをバイパスすると、一致するネットワーク トラフィックは、許可されたトラフィックと同じ方法で扱われます（「許可」（P.14-6）を参照）。システムがインタラクティブ ブロック ルールを使ってユーザの HTTP 要求を最初にブロックすると、接続開始イベントにインタラクティブ ブロック アクション（またはリセット付きインタラクティブ ブロック アクション）のマークが付きます。システムにより表示される警告ページでユーザがクリックスルーすると、そのセッションでログに記録されるその後の接続イベントすべてに許可アクションが付きます。したがって、許可ルールの場合と同様に、両方の種類のインタラクティブ ブロック ルールにファイルポリシーと侵入ポリシーを関連付けることができます。また、システムはネットワーク検出を使用して、ユーザ許可されたこのトラフィックを検査できます。



インタラクティブ ブロックされるトラフィックに関するロギング オプションは、許可されたトラフィックに関するオプションと同じですが、ユーザがインタラクティブ ブロックをバイパスしない場合、システムがログに記録できるのは接続開始イベントだけであることに注意してください。

ルール条件とそのメカニズムについて

ライセンス：任意

ルールに一致するトラフィックのタイプを識別するために、アクセス コントロール ルールに条件を追加できます。さまざまな種類の条件を単独で、または任意に組み合わせてルールに追加することができます。

それぞれの条件タイプごとに、使用可能条件リストから、ルールに追加する条件を選択します。条件フィルタを適用できる場合は、条件フィルタを使って使用可能な条件を限定できます。使用可能な条件リスト、および選択した条件リストは、1 つの条件だけを含む場合も、数ページに及ぶ場合もあります。使用可能な条件は検索することができ、名前や値を入力するとそれに一致する条件だけが表示され、入力していくにつれてそのリストが更新されます。

条件のタイプに応じて、使用可能条件リストには、シスコから直接提供された条件と、他の FireSIGHT システム機能を使って設定された条件が一緒に含まれることがあります。その中には、オブジェクト マネージャ （[Objects] > [Object Management]）を使って作成されたオブジェクト、個別の条件ページから直接作成されたオブジェクト、およびリテラル条件が含まれます。

ルール条件の指定については、次の項を参照してください。

- 「ルール条件について」（P.14-10）に、さまざまなタイプのルール条件の定義を示します。
- 「ルール条件の追加」（P.14-13）に、ルール条件を選択および追加するためのコントロールを示しています。
- 「条件リストの検索」（P.14-15）では、使用可能な条件の検索方法を説明します。入力した名前や値に一致する条件だけが表示され、入力していくにつれてそのリストが更新されます。
- 「リテラル条件の追加」（P.14-16）に、リテラル条件をルールに追加する方法の説明を示します。
- 「条件でのオブジェクトの使用」（P.14-17）では、該当する条件タイプの設定ページから個別のオブジェクトをシステムに追加する方法について説明します。

ルール条件について

ライセンス：任意

次の表で説明されている任意の条件を満たすトラフィックと照合するアクセス コントロール ルールを設定できます。

表 14-2　アクセス コントロール ルール条件のタイプ

条件	説明	サポートされる防御センター	サポートされるデバイス
ゾーン	ポリシーの適用場所として可能な 1 つ以上のインターフェイスの設定。ゾーンは、送信元インターフェイスと宛先インターフェイスでトラフィックを分類するメカニズムであり、ルールに送信元のゾーン条件と宛先のゾーン条件を追加することができます。オブジェクト マネージャを使ってゾーンを作成する方法については、「セキュリティ ゾーンの操作」（P.5-43）を参照してください。これらの条件の追加の詳細については、「ゾーン条件の追加」（P.14-18）を参照してください。	任意	任意
ネットワーク	明示的に指定された、またはネットワーク オブジェクトとグループ（「ネットワーク オブジェクトの操作」（P.5-4）を参照）を使って指定された、個別の IP アドレス、CIDR ブロック、およびプレフィクス長からなる任意の組み合わせ。送信元と宛先のネットワーク条件をルールに追加できます。これらの条件の追加の詳細については、「ネットワーク条件の追加」（P.14-19）を参照してください。	任意	任意
位置情報	明示的に指定された、または位置情報オブジェクト（「位置情報オブジェクトの操作」（P.5-44）を参照）を使って指定された、モニタ対象トラフィックの送信元または宛先として識別される個々の国と大陸からなる任意の組み合わせ。送信元と宛先の位置情報条件をルールに追加できます。これらの条件の追加の詳細については、「位置情報条件の追加」（P.14-21）を参照してください。	任意（DC500 を除く）	シリーズ 3、仮想、ASA FirePOWER
VLAN タグ	VLAN によるネットワーク上のトラフィックの識別に使われる 0 ～ 4094 の数値。オブジェクト マネージャを使用して個別の VLAN タグ オブジェクトとグループ VLAN タグ オブジェクトを作成する方法については、「VLAN タグ オブジェクトの操作」（P.5-14）を参照してください。これらの条件の追加の詳細については、「VLAN タグ条件の追加」（P.14-22）を参照してください。	任意	任意（ASA FirePOWER を除く）
ユーザ	Microsoft Active Directory サーバから取得される個々の LDAP ユーザとユーザ グループ。ユーザ制御に使用するユーザとグループを指定および取得する方法については、「LDAP 認証について」（P.48-6）を参照してください。これらの条件の追加の詳細については、「ユーザ条件の追加」（P.14-24）を参照してください。	任意（DC500 を除く）	シリーズ 3、仮想、X シリーズ、ASA FirePOWER
アプリケーション	シスコ提供のアプリケーション、ユーザ定義アプリケーション、およびオブジェクト マネージャを使って作成したアプリケーション フィルタ 詳細については、「アプリケーション ディテクタの使用」（P.42-18）および「アプリケーション フィルタの操作」（P.5-16）を参照してください。これらの条件の追加の詳細については、「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。	任意	シリーズ 3、仮想、X シリーズ、ASA FirePOWER

表 14-2　アクセス コントロール ルール条件のタイプ（続き）

条件	説明	サポートされる防御センター	サポートされるデバイス
ポート	トランスポート プロトコルに基づいて作成される、個別のポート オブジェクトとグループ ポート オブジェクトを含むトランスポート プロトコル ポート。オブジェクト マネージャを使用して個別のトランスポート プロトコル オブジェクトとグループ トランスポート プロトコル オブジェクトを作成する方法については、「ポート オブジェクトの操作」（P.5-13）を参照してください。これらの条件の追加の詳細については、「ポート条件の追加」（P.14-29）を参照してください。	任意	任意
URL	カテゴリとレピュテーションでグループ化されたシスコ提供の URL、リテラル URL、およびオブジェクト マネージャを使って作成された個別の URL オブジェクトとグループ URL オブジェクト。詳細については、「クラウド通信の有効化」（P.51-27）および「URL オブジェクトの操作」（P.5-15）を参照してください。これらの条件の追加の詳細については、「URL 条件の追加」（P.14-31）を参照してください。	任意（DC500 を除く：ただし DC500 ではリテラル URL、URL オブジェクト、URL オブジェクト グループがサポートされます）	シリーズ 3、仮想、X シリーズ、ASA FirePOWER

1 つ以上のタイプのアクセス コントロール ルール条件を任意に組み合わせて、それに一致するトラフィックをフィルタ処理できます。システムは、同じタイプの複数の条件を OR 演算でリンクし、異なる条件タイプを AND 演算でリンクします。たとえば、次のようなルール条件の場合、

```
宛先ネットワーク：10.4.0.0/16、10.5.0.0/16
VLAN タグ：11
```

このルールは VLAN 11 上で 10.4.0.0/16 または 10.5.0.0/16 にあるホストに向かうトラフィックに一致します。たとえば、

```
10.1.1.1 から 10.4.12.1、VLAN 11
```

または

```
192.168.2.1 から 10.5.15.23、VLAN 11
```

ルールで複数の条件を指定した場合、ルールのすべての条件に一致するトラフィックがルールに一致します。特定のタイプの条件を 1 つもルールに追加しない場合、システムはそのタイプの任意のトラフィックをデフォルト設定として使用します。つまり、システムはその条件タイプに基づいてトラフィックをフィルタ処理しません。

送信元と宛先のゾーン条件、および送信元と宛先のネットワーク条件を追加できることに注意してください。それ以外の条件では送信元も宛先も指定しないため、すべてのトラフィックをルールと比較して、一致するトラフィックを識別します。

ルール条件の追加

ライセンス：任意

アクセス コントロール ルールに条件を追加する方法は、基本的にすべての条件タイプで同じです。左側にある 1 つまたは 2 つの使用可能条件リストから条件を選択し、右側にある 1 つまたは 2 つの選択済み条件リストに、選択したそれらの条件を追加します。

すべての条件タイプで、使用可能な個々の条件を 1 つまたは複数クリックすると、それが強調表示され、選択状態になります。また、アプリケーション条件では、チェック ボックスを選択または選択解除し、シスコ提供のフィルタまたはユーザ定義のフィルタを介して使用可能なアプリケーションのリストを制限することもできます。

すべての場合に、2 つのタイプのリスト間にあるボタンをクリックすると、選択した条件を選択済み条件リストに追加できます。または、条件をドラッグ アンド ドロップして、選択した条件のリストに入れることもできます。

ゾーン、（位置情報を含む）ネットワーク、ポートなどのいくつかのページには、左側に 1 つの使用可能条件リストがあり、その条件を右側の 2 つの選択済み条件リストのいずれかに追加できます。他のページ（アプリケーション、URL など）には、左側に 2 つの使用可能条件リストがあり、この両方を使って条件を選択し、それを右側の 1 つの選択済み条件リストに追加できます。さらに他のページ（VLAN タグとユーザ）には、左側に 1 つの使用可能条件リストがあり、それを右側の 1 つの選択済み条件リストに追加できます。

選択済み条件リストには、タイプごとに最大 50 個までの条件を追加できます。たとえば、アプライアンスの上限に達するまで、最大 50 個の送信元ゾーン条件、最大 50 個の宛先ゾーン フィルタ、最大 50 個のユーザ条件などを追加できます。

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、防御センターは、ポリシーで定義された各ルールを展開されたルール セットとしてデバイスに送信することに注意してください。このセット内の各ルールは、ルール内のさまざまな条件を組み合わせた 1 つの可能な組を表します。たとえば、送信元ゾーンとして内部セキュリティ ゾーン、さらに送信元ポート LDAP と HTTPS を含む 1 つのルールは、2 つのルールとしてデバイスに送信されます。1 つは LDAP 送信元ポートを介した内部送信元ゾーンのトラフィックに一致し、もう 1 つは HTTPS 送信元ポートを介した内部送信元ゾーンのトラフィックに一致します。

アクセス コントロール ポリシーに複雑なルールが多数含まれる場合、展開されたルールの数がそのデバイスでの許容数を超えると、そのポリシーが管理対象デバイスに適用されない可能性があります。このような状況が生じた場合、ルールの条件を分析して、不要な設定を除去できるかどうか確認してください。

使用可能条件リストに、1 ページに表示可能な数を超える条件が含まれる場合は、リスト下のナビゲーション リンクを使ってページ間を切り替えることができます。

次の表に、条件を選択してルールに追加する際に実行できる操作の説明を示します。

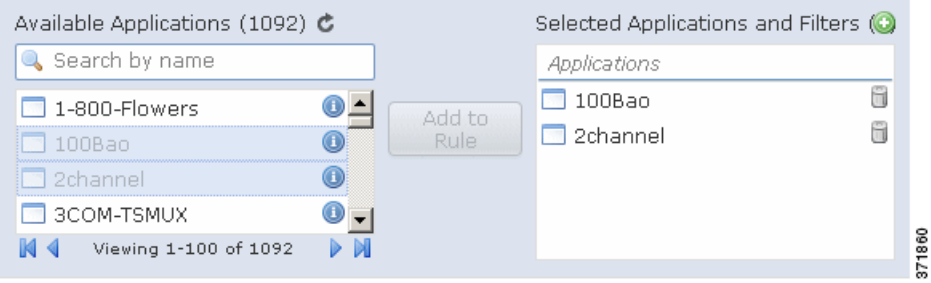
表 14-3　条件の追加

目的	操作
使用可能な条件を選択して、選択済み条件のリストに追加する	使用可能な条件をクリックします。複数の条件を選択するには Ctrl キーと Shift キーを使用します。
リストされたすべての使用可能な条件を選択する	いずれかの使用可能な条件の行を右クリックし、[Select All] をクリックします。
使用可能な条件またはフィルタ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。詳細については、「条件リストの検索」（P.14-15）を参照してください。

表 14-3　条件の追加（続き）

目的	操作
使用可能な条件やフィルタを検索しているときに検索内容をクリアする	検索フィールドの上のリロード アイコン（）、または検索フィールド内のクリア アイコン（）をクリックします。
選択した条件を、使用可能条件リストから選択済み送信元条件リスト、または宛先条件リストに追加する	[Add to Source] または [Add to Destination] をクリックします。ゾーン、ネットワーク、位置情報、およびポートの条件は、送信元と宛先の条件リストに追加できます。詳細については、「ゾーン条件の追加」（P.14-18）、「ネットワーク条件の追加」（P.14-19）、「位置情報条件の追加」（P.14-21）、および「ポート条件の追加」（P.14-29）を参照してください。
選択した条件を、使用可能条件リストから 1 つの選択済み条件リストに追加する	[Add to Rule] をクリックします。VLAN タグ、ユーザ、アプリケーション、および URL の条件では、1 つの選択済み条件リストが使用されます。
選択した使用可能な条件を、選択済み条件リストにドラッグ アンド ドロップする	選択した条件を右クリックして、選択済み条件リストにドラッグ アンド ドロップします。
リテラル フィールドを使用して、選択済み条件リストにリテラル条件を追加する	クリックしてリテラル フィールドからプロンプトを除去し、リテラル条件を入力して、[Add] をクリックします。ネットワーク、VLAN タグ、および URL の条件には、リテラル条件を追加するためのフィールドがあります。
ドロップダウン リストを使用して、選択済み条件リストにリテラル条件を追加する	ドロップダウン リストから条件を選択して、[Add] をクリックします。ポート条件には、リテラル条件を追加するためのドロップダウン リストがあります。詳細については、「ポート条件の追加」（P.14-29）を参照してください。
個々のオブジェクトまたは条件フィルタを追加して、使用可能条件リストからそれを選択できるようにする	追加アイコン（）をクリックします。オブジェクト マネージャを使ってオブジェクトを追加する方法については、「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。
選択済み条件リストから 1 つの条件を削除する	条件の横にある削除アイコン（）をクリックします。
選択済み条件リストから 1 つの条件を削除する	1 つの選択済み条件の行を右クリックして強調表示し、[Delete] をクリックします。
選択済み条件リストから複数の条件を削除する	Shift キーと Ctrl キーを使って複数の条件を選択するか、右クリックして [Select All] を選択します。次に、いずれかの選択済み条件の行を右クリックして強調表示し、[Delete Selected] をクリックします。

すでに選択した条件はグレー表示され、同じ選択済み条件リストには追加できなくなります。すでに追加した条件を選択すると、追加ボタンもグレー表示されます。まだ追加していない条件を選択すると、追加ボタンがアクティブになり、それを使用できます。次の例では 100Bao および 2channel アプリケーションがすでに追加され、現在選択されています。選択済みアプリケーションと [Add to Rule] ボタンがどちらもグレー表示されています。



同様に、複数の条件を組み合わせて使用できない場合（たとえば送信元ポートと宛先ポートのトランスポート プロトコルが異なっている場合など）、先に選択した内容に基づいて無効な条件がグレー表示されます。

該当する条件ページとポリシー編集ページで、ポインタを 1 つの個別オブジェクトの上に置くとそのオブジェクトの内容が表示され、グループ オブジェクトの上に置くと、グループ内の個々のオブジェクトの数が表示されます。

新しいルールに条件を追加する基本的な手順を次に示します。ルールの追加と変更に関する詳しい説明は、「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。

使用可能な条件を選択済み条件リストに追加する方法：

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　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　[Add Rule] をクリックします。

[Add Rule] ページが表示されます。

ステップ 4　ルールに追加する条件のタイプを示すタブをクリックします。

選択した条件のタイプに対応する条件ページが表示されます。

ステップ 5　「条件の追加」表に含まれているいずれかのアクションを実行します。

ステップ 6　設定を保存するには、[Add] をクリックします。

ルールが追加され、ポリシー編集ページが表示されます。

条件リストの検索

ライセンス：任意

使用可能なアクセス コントロール ルール条件および条件カテゴリのリストをフィルタ処理して、リストに表示される項目数を制限できます。入力していくと、リストが更新されて一致する項目が表示されます。

オプションで、オブジェクト名およびオブジェクトに設定されている値を検索対象にすることができます。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。

新しいルールでリストをフィルタ処理する基本的な手順を次に示します。ルールの追加と変更に関する詳しい説明は、「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。

使用可能な条件または条件カテゴリのリストを検索する方法：

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　[Add Rule] をクリックします。

[Add Rule] ページが表示されます。

ステップ 4　リストを検索するには、検索フィールド内部をクリックしてプロンプトをクリアした後、検索文字列を入力します。

入力していくとリストが更新され、一致する項目とクリア アイコン（  ）が検索フィールドに表示されます。検索文字列に一致する項目がない場合、リストが更新されて、リストには何も表示されません。

ステップ 5　オプションで、検索フィールドの上のリロード 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（）をクリックして検索文字列を消去します。

完全なリストが表示されます。

ステップ 6　設定を保存するには、[Add] をクリックします。

ルールが追加され、ポリシー編集ページが表示されます。

リテラル条件の追加

ライセンス：任意

次の条件タイプでは、選択済み条件リストにリテラル値を追加できます。

- ネットワーク
- VLAN タグ
- ポート
- URL

ポート条件を除くすべての条件では、選択済み条件リストの下にある設定フィールドでリテラル値を入力します。

ポート条件では、ドロップダウン リストからプロトコルを選択します。（宛先ポートの）プロトコルが [All] である場合、およびオプションで、プロトコルが TCP または UDP である場合は、設定フィールドにポート番号を入力します。プロトコルが ICMP または IPv6-ICMP である場合は、タイプおよび（該当する場合は）関連するコードを選択します。送信元ポートを追加するとき、プロトコルのデフォルトとして TCP が設定されます。リテラル ポートを設定するときには、プロトコルを指定する必要があります。

該当するそれぞれの条件ページには、リテラル値を追加するために必要なコントロールがあります。設定フィールドに入力した値が無効である場合や、まだ有効と認識されていない場合は、赤いテキストとして表示されます。入力した値が有効と認識された時点で、黒いテキストに変化します。有効な値が認識されると、グレー表示の [Add] ボタンがアクティブになります。追加したリテラル値は、選択済み条件リストにただちに表示されます。

それぞれのタイプのリテラル値を追加する詳しい方法については、次を参照してください。

- 「ネットワーク条件の追加」（P.14-19）
- 「VLAN タグ条件の追加」（P.14-22）
- 「ポート条件の追加」（P.14-29）
- 「URL 条件の追加」（P.14-31）

条件でのオブジェクトの使用

ライセンス：任意

オブジェクト マネージャ（[Objects] > [Management]）で作成したアプリケーション フィルタとオブジェクトは、該当する使用可能なアクセス コントロール ルール条件リストでただちに選択可能になります。詳細については、「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。

また、アクセス コントロール ポリシーから多数のオブジェクトを即座に作成できます。該当する条件ページ上のコントロールでは、オブジェクト マネージャでの設定コントロールと同じ機能を利用できます。

即座に作成された個別のオブジェクトは、使用可能なオブジェクトのリストにただちに表示され、それを現在のルールや他の既存のルール、さらに今後のルールに追加することができます。該当する条件ページとポリシー編集ページで、ポインタを 1 つの個別オブジェクトの上に置くとそのオブジェクトの内容が表示され、グループ オブジェクトの上に置くと、グループ内の個々のオブジェクトの数が表示されます。

さまざまな条件タイプを使用する

ライセンス：任意

1 つ以上のタイプのルール条件を任意に組み合わせて、トラフィックをフィルタ処理することができます。詳細については、次の項を参照してください。

- 「ゾーン条件の追加」（P.14-18）では、オブジェクト マネージャを使って作成したセキュリティ ゾーンを基準にトラフィックをフィルタ処理する方法について説明します。
- 「ネットワーク条件の追加」（P.14-19）では、IP アドレスまたはアドレス ブロックを基準にトラフィックをフィルタ処理する方法について説明します。
- 「位置情報条件の追加」（P.14-21）では、国または大陸を基準にトラフィックをフィルタ処理する方法について説明します。

- 「VLAN タグ条件の追加」（P.14-22）では、VLAN タグを基準にトラフィックをフィルタ処理する方法について説明します。
- 「ユーザ条件の追加」（P.14-24）では、Microsoft Active Directory サーバから取得されるユーザおよびユーザ グループを基準にトラフィックをフィルタ処理する方法について説明します。
- 「アプリケーション条件を使用する」（P.14-25）では、シスコ提供のアプリケーションを含む定義済みリスト、カスタム アプリケーション、およびオブジェクト マネージャを使って作成したアプリケーション フィルタに基づいてトラフィックをフィルタ処理する方法を説明します。
- 「ポート条件の追加」（P.14-29）では、指定したトランスポート プロトコル ポートを基準にトラフィックをフィルタ処理する方法について説明します。
- 「URL 条件の追加」（P.14-31）では、URL（レピュテーションやカテゴリなどの統計情報を含む）を基準にトラフィックをフィルタ処理する方法について説明します。

ゾーン条件の追加

ライセンス：任意

システムのセキュリティ ゾーンは、管理対象デバイス上のインターフェイスで構成されます。アクセス コントロール ルールに追加されるゾーンは、ネットワークにおける、これらのゾーンのインターフェイスを持つデバイスに対するルールを対象としています。アクセス コントロール ルールの条件として、セキュリティ ゾーンを追加できます。オブジェクト マネージャを使ってセキュリティ ゾーンを作成する方法については、「セキュリティ ゾーンの操作」（P.5-43）を参照してください。

ゾーンによってトラフィックをフィルタ処理する際には、次の重要事項に注意してください。

- ルール内のすべてのゾーンは同じタイプ（スイッチド、ルーテッドなど）である必要があります。
- 送信元ゾーンとしてのみ、パッシブ ゾーンを追加できます。
- 使用可能なゾーン リスト内のゾーンの横にある警告アイコン（⚠）は、ゾーンにインターフェイスが含まれないことを示しています。アイコンの上にポインタを置くと、メッセージが表示されて、ルールを有効にするには少なくとも 1 つのインターフェイスがゾーンに含まれる必要があることを示します。「セキュリティ ゾーンの操作」（P.5-43）を参照してください。

注　レイヤ 2 展開では、宛先ネットワークや宛先セキュリティ ゾーンに基づいて出トラフィックをブロックすることはできません。代わりに、ブロッキング送信元ネットワークまたは送信元セキュリティ ゾーンに基づいて入力トラフィックをブロックするアクセス コントロール ルールを作成する必要があります。レイヤ 2 展開の詳細については、「仮想スイッチのセットアップ」（P.8-1）を参照してください。

次の手順は、アクセス コントロール ルールの追加時または編集時に送信元と宛先のゾーン条件を追加する方法を示しています。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 ルールにゾーン条件を追加する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　ルール編集ページの [Zones] タブを選択します。

[Zones] ページが表示されます。

ステップ 2　必要に応じて、[Available Zones] リストの上にある [Search by name] プロンプトをクリックして、名前か値を入力します。

入力していくと、リストが更新されて一致する条件が表示されます。詳細については、「条件リストの検索」（P.14-15）を参照してください。

ステップ 3　[Available Zones] リスト内の条件をクリックします。複数の条件を選択するには、Shift キーと Ctrl キーを使用するか、右クリックして [Select All] をクリックします。

選択した条件が強調表示されます。

ゾーンの横にある警告アイコン（⚠）は、ゾーンにインターフェイスが含まれないためルールが有効にならないことを示します。「セキュリティ ゾーンの操作」（P.5-43）を参照してください。

ステップ 4　次のいずれかの操作をします。

- 送信元ゾーンによってトラフィックをフィルタ処理するには、[Add to Source] をクリックします。
- 宛先ゾーンによってトラフィックをフィルタ処理するには、[Add to Destination] をクリックします。

オプションで、選択した条件を [Source Zones] リストまたは [Destination Zones] リストにドラッグ アンド ドロップすることもできます。

選択した条件が追加されます。同じ条件を送信元ゾーンと宛先ゾーンの両方に追加できることに注意してください。

ステップ 5　ルールを保存するか、編集を続けます。

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）。

ネットワーク条件の追加

ライセンス：任意

次に示す任意の種類のネットワーク条件をアクセス コントロール ルールに追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのネットワーク オブジェクト

  オブジェクト マネージャを使用して個別のネットワーク オブジェクトとグループ ネットワーク オブジェクトを作成する方法については、「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。
- ネットワーク条件ページから追加した個々のネットワーク オブジェクト（独自のルールや、他の既存のルール、さらに今後のルールにこれらを追加できます）

  詳細については、「条件でのオブジェクトの使用」（P.14-17）を参照してください。
- リテラルの単一 IP アドレスまたはアドレス ブロック

  詳細については、「リテラル条件の追加」（P.14-16）を参照してください。

注　レイヤ 2 展開では、宛先ネットワークや宛先セキュリティ ゾーンに基づいて出トラフィックをブロックすることはできません。代わりに、送信元ネットワークまたは送信元セキュリティ ゾーンに基づいて入力トラフィックをブロックするアクセス コントロール ルールを作成する必要があります。レイヤ 2 展開の詳細については、「仮想スイッチのセットアップ」（P.8-1）を参照してください。

送信元または宛先の IPv6 トラフィックに一致する条件を含むルールをアクセス コントロール ポリシーに追加する場合、それらのルールの前に、IPv6 ネイバー探索プロトコル（ICMPv6 タイプ 135 および 136）を使用するトラフィックを指定するポート条件で許可ルールを追加してください。ポート条件の詳細については、「ポート条件の追加」（P.14-29）を参照してください。

位置情報ルール条件は [Networks] タブの下に表示されますが、FireSIGHT ライセンスが必要であり、異なるオブジェクトを使用します。位置情報条件の追加については、「位置情報条件の追加」（P.14-21）を参照してください。

次の手順は、アクセス コントロール ルールの追加時または編集時に送信元と宛先のネットワーク条件を追加する方法を示しています。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 ルールにネットワーク条件を追加する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　ルール編集ページの [Networks] タブを選択します。

[Networks] ページが表示されます。

ステップ 2　必要に応じて、[Available Networks] リストの上にある [Search by name or value] プロンプトをクリックして、名前か値を入力します。

入力していくと、リストが更新されて一致する条件が表示されます。詳細については、「条件リストの検索」（P.14-15）を参照してください。

ステップ 3　[Available Networks] リスト内の条件をクリックします。複数の条件を選択するには、Shift キーと Ctrl キーを使用するか、右クリックして [Select All] をクリックします。

選択した条件が強調表示されます。

ステップ 4　次のいずれかの操作をします。

- 送信元ネットワークによってトラフィックをフィルタ処理するには、[Add to Source] をクリックします。
- 宛先ネットワークによってトラフィックをフィルタ処理するには、[Add to Destination] をクリックします。

代わりに、選択した条件を [Source Networks] リストまたは [Destination Networks] リストにドラッグ アンド ドロップすることもできます。

選択した条件が追加されます。同じ条件を送信元ネットワークと宛先ネットワークの両方に追加できることに注意してください。

ステップ 5　オプションで、[Available Networks] リストの上にある追加アイコン（ ）をクリックして、個別のネットワーク オブジェクトを追加します。

各ネットワーク オブジェクトに複数の IP アドレス、CIDR ブロック、およびプレフィクス長を追加できます。その後、オプションで、追加済みのオブジェクトを選択できます。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）および「条件でのオブジェクトの使用」（P.14-17）を参照してください。

ステップ 6　オプションで、[Source Networks] リストまたは [Destination Networks] リストの下にある [Enter an IP address] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [Add] をクリックします。

リストが更新されて、それらのエントリが表示されます。詳細については、「リテラル条件の追加」（P.14-16）を参照してください。

ステップ 7　ルールを保存するか、編集を続けます。

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）。

位置情報条件の追加

ライセンス：FireSIGHT

サポート対象デバイス：シリーズ 3、仮想、ASA FirePOWER

サポート対象防御センター：任意（DC500 を除く）

FireSIGHT システムの位置情報機能は、モニタ対象ネットワークにおけるトラフィックの送信元と宛先の地理的な場所（国と大陸）を識別します。確実に最新の位置情報データを使用してトラフィックをフィルタ処理するために、シスコ防御センターで位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。GeoDB の更新については、「地理情報データベースについて」（P.53-30）を参照してください。位置情報機能の詳細については、「地理情報の使用」（P.47-24）を参照してください。

注　位置情報条件を含むアクセス コントロール ポリシーを適用するには、対象となる管理対象デバイスで FireSIGHT システム バージョン 5.3 以降が実行されている必要があります。

次に示す任意の種類の位置情報条件をアクセス コントロール ルールに追加できます。

- [Available Networks] リストの [Geolocation] タブから直接選択した大陸と国
- オブジェクト マネージャを使って作成した位置情報オブジェクト（国と大陸を独自に組み合わせたカスタマイズ オブジェクトを表す）

  オブジェクト マネージャを使って位置情報オブジェクトを作成する方法については、「位置情報オブジェクトの操作」（P.5-44）を参照してください。

次の手順は、アクセス コントロール ルールの追加時または編集時に送信元と宛先の位置情報条件を追加する方法を示しています。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 ルールに位置情報条件を追加する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　ルール編集ページの [Networks] タブを選択します。

[Networks] ページが表示されます。

ステップ 2　[Available Networks] で、[Geolocation] タブを選択します。

[Geolocation] ページが表示されます。

ステップ 3　オプションで、[Available Networks] リストの上にある [Search by name or value] プロンプトをクリックして、国、大陸、オブジェクトの名前か、国の ISO コード（たとえば USA、CHN）を入力します。

入力していくと、リストが更新されて一致する条件が表示されます。詳細については、「条件リストの検索」（P.14-15）を参照してください。

ステップ 4　[Available Networks] リスト内の条件（国または大陸）をクリックします。複数の条件を選択するには、Shift キーと Ctrl キーを使用するか、右クリックして [Select All] をクリックします。

大陸を選択した場合、その大陸に関連付けられているすべての国と、GeoDB 更新によってその大陸に今後追加されるすべての国が自動的に選択されます。ある大陸に属するいずれかの国を選択解除すると、その大陸全体が選択解除され、今後もそこに国が自動追加されなくなります。国と大陸を任意に組み合わせて選択できます。

選択した条件が強調表示されます。

ステップ 5　次のいずれかの操作をします。

- 送信元の国または大陸によってトラフィックをフィルタ処理するには、[Add to Source] をクリックします。
- 宛先の国または大陸によってトラフィックをフィルタ処理するには、[Add to Destination] をクリックします。

代わりに、選択した条件を [Source Networks] リストまたは [Destination Networks] リストにドラッグ アンド ドロップすることもできます。

選択した条件が追加されます。同じ条件を送信元の国/大陸および宛先の国/大陸の両方に追加できることに注意してください。

ステップ 6　ルールを保存するか、編集を続けます。

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）。

VLAN タグ条件の追加

ライセンス：任意

サポート対象デバイス：任意（ASA FirePOWER を除く）

次に示す任意の種類の VLAN タグ条件をアクセス コントロール ルールに追加できます。

- オブジェクト マネージャを使って作成した個別およびグループの VLAN タグ オブジェクト

  オブジェクト マネージャを使って個別の VLAN タグ オブジェクトとグループ VLAN タグ オブジェクトを作成する方法については、「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。

- VLAN タグ条件ページから追加した個別の VLAN タグ オブジェクト（独自のルールや、他の既存のルール、さらに今後のルールにこれらを追加できます）

  詳細については、「条件でのオブジェクトの使用」（P.14-17）を参照してください。

- リテラル VLAN タグ条件

  詳細については、「リテラル条件の追加」（P.14-16）を参照してください。

システムは、ネットワークのすべてのトラフィックを検査して指定の VLAN タグを探し、最も内側の VLAN タグを使用して VLAN を基準にパケットを識別します。

次の手順は、アクセス コントロール ルールの追加時または編集時に VLAN 条件を追加する方法を示しています。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 ルールに VLAN タグ条件を追加する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　ルール編集ページの [VLAN Tags] タブを選択します。

[VLAN Tags] ページが表示されます。

ステップ 2　必要に応じて、[Available VLAN Tags] リストの上にある [Search by name or value] プロンプトをクリックして、名前または値を入力します。

入力していくと、リストが更新されて一致する条件が表示されます。詳細については、「条件リストの検索」（P.14-15）を参照してください。

ステップ 3　[Available VLAN Tags] リスト内の条件をクリックします。複数の条件を選択するには Shift キーと Ctrl キーを使用するか、右クリックして [Select All] をクリックします。

選択した条件が強調表示されます。

ステップ 4　次のいずれかの操作をします。

- [Add to Rule] をクリックします。
- 選択した条件を [Selected VLAN Tags] リストにドラッグ アンド ドロップします。

選択した条件が追加されます。

ステップ 5　オプションで、[Available VLAN Tags] リストの上にある追加アイコン（  ）をクリックして、VLAN タグ オブジェクトを追加します。

追加するそれぞれの VLAN タグ オブジェクトで、1 から 4094 までの任意の VLAN タグを指定できます。VLAN タグからなる範囲を指定するにはハイフンを使用してください。その後、追加済みのオブジェクトを選択できます。詳細については、「VLAN タグ オブジェクトの操作」（P.5-14）および「条件でのオブジェクトの使用」（P.14-17）を参照してください。

ステップ 6　オプションで、[Selected VLAN Tags] リストの下にある [Enter a VLAN Tag] プロンプトをクリックし、VLAN タグまたは範囲を入力して、[Add] をクリックします。

1 ～ 4094 の任意の VLAN タグを指定できます。VLAN タグの範囲を指定するには、ハイフンを使用します。

リストが更新されて、それらのエントリが表示されます。詳細については、「リテラル条件の追加」（P.14-16）を参照してください。

ステップ 7　ルールを保存するか、編集を続けます。

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）。

ユーザ条件の追加

ライセンス：Control

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 を除く）

Microsoft Active Directory サーバから取得されるユーザおよびユーザ グループに関してトラフィックを照合するようアクセス コントロール ルールを設定できます。

ユーザ条件を含むアクセス コントロール ルールを作成するには、その前に、組織内の少なくとも 1 つの Microsoft Active Directory サーバと防御センターとの間の接続を設定しておく必要があります。この設定は認証オブジェクトと呼ばれ、サーバの接続設定と認証フィルタ設定が含まれています。また、ユーザ条件で使用できるユーザとグループも指定されます。詳細については、「防御センターとの LDAP 接続の構築」（P.35-44）を参照してください。

さらに、ユーザ エージェントをインストールする必要もあります。エージェントは、Active Directory 資格情報で認証するユーザをモニタし、このようなログインのレコードを防御センターに送信します。これらのレコードはユーザを IP アドレスに関連付け、これによってユーザ条件を含むアクセス コントロール ルールがトリガー可能になります。詳細については、「防御センターとユーザ エージェント間の接続の設定」（P.35-51）を参照してください。

アクセス コントロール ルールでグループを指定した場合、そのグループの全メンバー（サブグループのメンバーを含む）が自動的に含まれることに注意してください。ただし、個別に除外されたユーザと、除外されたサブグループのメンバーは含まれません。

ユーザ グループ条件を含むアクセス コントロール ルールを使ってシステムがトラフィックを処理し、関連するイベントを生成するためには、その前にそのグループの少なくとも 1 ユーザがネットワーク トラフィックで検出される必要があります。この最初の接続は、一致するアクセス コントロール ルール**ではなく**、アクセス コントロール ポリシーのデフォルト アクションによって処理されます。

注意　非常に多くのユーザ グループを含むユーザ認識パラメータを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、システムはメモリ制限のためにグループに基づいてユーザ マッピングをドロップすることがあります。その結果、ユーザ グループに基づくアクセス コントロール ルールが想定どおりに起動しない可能性があります。

次の手順は、アクセス コントロール ルールの追加時または編集時にユーザ条件を追加する方法を示しています。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 ルールにユーザ条件を追加する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　ルール編集ページの [Users] タブを選択します。

[Users] ページが表示されます。

ステップ 2　必要に応じて、[Available Users] リストの上にある [Search by name or value] プロンプトをクリックして、名前または値を入力します。

入力していくと、リストが更新されて一致する条件が表示されます。詳細については、「条件リストの検索」（P.14-15）を参照してください。

ステップ 3　[Available Users] リスト内の条件をクリックします。複数の条件を選択するには、Shift キーと Ctrl キーを使用するか、右クリックして [Select All] をクリックします。

選択した条件が強調表示されます。

ステップ 4　次のいずれかの操作をします。

- [Add to Rule] をクリックします。
- 選択した条件を [Selected Users] リストにドラッグ アンド ドロップします。

選択した条件が追加されます。

ステップ 5　ルールを保存するか、編集を続けます。

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）。

アプリケーション条件を使用する

ライセンス：Control

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

アプリケーション トラフィックを照合するアクセス コントロール ルールを設定できます。（シスコ提供あるいはユーザ定義の）個別のアプリケーションまたはアプリケーション フィルタを、アクセス コントロール ルールの条件として使用できます。項目の総数が 50 を超えない限り、アプリケーションとフィルタを任意に組み合わせて追加できます（1 つのフィルタを 1 項目として数えます）。既存のフィルタが最適でない場合は、アプリケーション条件の作成中にアプリケーション フィルタをその場で作成できます。その後、新しいフィルタをそのルールや他の既存のルール、さらに今後のルールで使用することができます。詳細については、次の項を参照してください。

- シスコ提供のアプリケーションおよびユーザ定義アプリケーションについては、「アプリケーション検出について」（P.35-12）および「アプリケーション ディテクタの使用」（P.42-18）を参照してください。
- シスコ提供のアプリケーション フィルタおよびユーザ定義アプリケーション フィルタについては、「アプリケーション フィルタの操作」（P.5-16）を参照してください。
- アプリケーション フィルタをその場で追加する方法については、「条件でのオブジェクトの使用」（P.14-17）を参照してください。

アプリケーションを追加するときには、次の点に注意してください。

- システムは、アプリケーションが識別される接続内ペイロードがないパケットに対してデフォルト ポリシー アクションを適用します。たとえば TCP 接続が確立されているときに、これが当てはまる可能性があります。
- クライアントとサーバの間で接続が確立される前に、アプリケーションを識別したり URL をフィルタ処理したりすることはできません。したがって、アプリケーションまたは URL を含むルール内の他のすべての条件にパケットが一致する場合、アプリケーション識別が未完了であると、パケットは通過を許可されます。この動作により接続が確立され、こうしてアプリケーションの識別が可能になります。

アプリケーション条件を含むアクセス コントロール ルールをシステムが処理するとき、セッション内でアプリケーションが識別される時点までは、他の点でそのルールに一致するパケットがデフォルト侵入ポリシーを使って許可され、検査されます。アプリケーションがルール内の条件に一致した場合、システムはルール アクションを適用します。そうでない場合は、ポリシー内の残りのアクセス コントロール ルールが評価されます。アプリケーション識別は、通常、3 ～ 5 個のパケットの範囲内で完了するはずです。完了しない場合、ネットワーク検出ポリシーが最新のものであること、すべてのデバイスに適用されること、およびアクセス コントロール ルールで設定されたネットワークとポートが 1 つも除外されないことを確認してください。

- Web サーバによって参照されるトラフィック（たとえばアドバタイズメント トラフィック）を処理するルールを作成するには、参照元アプリケーションではなく、参照されるアプリケーションに関する条件を追加します。詳細については、「特記事項：照会先 Web アプリケーション」（P.35-17）を参照してください。
- ポリシー内のアプリケーション ルール条件ごとに、少なくとも 1 つのディテクタを有効にする必要があります（「ディテクタのアクティブ化と非アクティブ化」（P.42-30）を参照）。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。「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。

詳細については、次の項を参照してください。

- 「アプリケーション条件リストについて」（P.14-26）
- 「アプリケーション条件の追加」（P.14-28）

アプリケーション条件リストについて

ライセンス：Control

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

アプリケーション条件ページには、次の 3 つのリストが表示されます。

- 左側の [Application Filters] リストに表示されるフィルタを選択すると、[Available Applications] リストに示されるアプリケーションを限定できます。
- 中央の [Available Applications] にはアプリケーションのリストが表示され、条件としてルールに追加されるアプリケーションをこの中から選択できます。
- 右側の [Selected Applications] リストには、すでにルールに追加されたアプリケーションが表示されます。

[Available Applications] リストにアプリケーションを表示させるために [Application Filters] リストからフィルタを選択するときには、次の点に注意してください。

- シスコ提供のフィルタ タイプを任意に組み合わせて、[Application Filters] リストで複数のフィルタを選択することができます。

  システムは、OR 演算を使用して同じフィルタ タイプの複数のフィルタをリンクします。たとえば、Risks（リスク）タイプの下の Medium（中）および High（高）フィルタを選択すると、結果として次のようなフィルタになります。

  ```
  Risk: Medium OR High
  ```

  たとえば Medium フィルタに 110 個のアプリケーション、High フィルタに 82 個のアプリケーションが含まれる場合、システムはこれら 192 個のアプリケーションすべてを [Available Applications] リストに表示します。

システムは AND 演算を使用して、異なるタイプのフィルタをリンクします。たとえば Risks タイプで Medium および High フィルタを選択し、Business Relevance（業務との関連性）タイプで Medium および High フィルタを選択した場合、結果として次のようなフィルタになります。

```
Risk: Medium OR High
AND
Business Relevance: Medium OR High
```

この場合、システムは Risk タイプ Medium または High、および Business Relevance タイプ Medium または High の両方に含まれるアプリケーションだけを表示します。

- [Available Applications] リストで、カスタム フィルタを別のフィルタ（他のカスタム フィルタを含む）と組み合わせて選択することはできません。これは、カスタム フィルタにフィルタを追加できないためです。
- [Application Filters] リストで 1 つ以上のフィルタを選択すると、[All apps matching the filter]（フィルタに一致する全アプリ）条件が [Available Applications] リストに追加されます。同様に、[Application Filters] リストでフィルタが未選択であるときに [Available Applications] リストを検索した場合も、[All apps matching the filter] 条件が [Available Applications] リストに追加されます。[Application Filters] リストで 1 つ以上のフィルタを選択し、しかも [Available Applications] リストを検索した場合、選択内容と検索フィルタ適用後の [Available Applications] リストが AND 演算を使って結合されます。つまり [All apps matching the filter] 条件には、[Available Applications] リストに現在表示されている個々のすべての条件と、[Available Applications] リストの上で入力された検索文字列が含まれます。

  [All apps matching the filter] 条件が [Selected Applications and Filters] リストに追加されると、（それを構成する個々の条件の数にかかわらず）最大 50 個の条件のうち 1 条件としてカウントされます。

  [All apps matching the filter] を追加すると、追加されたフィルタの名前は「フィルタ タイプ + 各タイプの最大 3 フィルタの名前」を連結させたものとなります。同じタイプのフィルタが 3 個を超える場合は、その後に省略記号（...）が表示されます。たとえば次のフィルタ名には、Risks タイプの 2 つのフィルタと Business Relevance タイプの 4 つのフィルタが含まれています。

  ```
  Risks: Medium, High Business Relevance: Low, Medium, High,...
  ```

  [All apps matching the filter] を使って追加したフィルタで表されないフィルタ タイプは、追加されたフィルタの名前に含まれません。[Selected Applications and Filters] リスト内のフィルタ名の上にポインタを置いたときに表示される説明テキストは、これらのフィルタ タイプが [any]（オプション）に設定されていることを示します。つまり、これらのフィルタ タイプはフィルタを課さないため任意の値が許容されます。

  [All apps matching the filter] の複数のインスタンスを追加することができます。例として、最初のフィルタ（たとえば Risks、High）用に [All apps matching the filter] を追加し、すべての項目を選択解除して、別のフィルタ タイプ（たとえば Business Relevance、High）用に新しく選択した後、[All apps matching the filter] を再び追加できます。
- アクセス コントロール ポリシーを適用するとき、[Selected Applications] リストに追加済みの固有のアプリケーションからなる 1 つのリストがシステムによって生成されます。これにより、アプリケーション条件が重複して追加されるのを防ぎます。

アプリケーション条件の追加

ライセンス：Control

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

次の手順は、アクセス コントロール ルールの追加時または編集時にアプリケーション条件を追加する方法を示しています。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 ルールにアプリケーション条件を追加する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[Applications] タブを選択します。

[Applications] ページが表示されます。

ステップ 2　オプションで、[Applications Filters] リストまたは [Available Applications] リストの上にある [Search by name] プロンプトをクリックして、名前を入力します。

入力していくと、リストが更新されて一致する条件が表示されます。詳細については、「条件リストの検索」（P.14-15）を参照してください。

カスタム アプリケーション フィルタを選択すると検索フィールドが無効になることに注意してください。これは、選択したカスタム フィルタにフィルタを追加できないためです。

ステップ 3　オプションで、[Available Applications] リストに表示されるアプリケーション リストを限定します。次のいずれかの操作をします。

- フィルタ タイプの横にある矢印をクリックしてそれを展開し、アプリケーションを表示/非表示にする各フィルタの横のチェック ボックスを選択/選択解除します。

  なお、各フィルタの横の数値は、フィルタに含まれるアプリケーションの数を示します。

- シスコ提供のフィルタ タイプ（[Risks]、[Business Relevance]、[Types]、[Categories]、または [Tags]）を右クリックして、[Check All] または [Uncheck All] をクリックします。シスコ提供のフィルタ タイプの詳細については、「アプリケーションの特徴」の表を参照してください。

[Available Applications] リストが次のように更新されます。

- リストには、現在選択されているフィルタに含まれるアプリケーションが表示されます。
- [All apps matching the filter] 選択項目が表示されます。この条件には、[Available Applications] リストに現在表示されているすべてのアプリケーションおよびフィルタが含まれます。

  [All apps matching the filter] と組み合わせて個々のアプリケーションを選択したり追加したりできないことに注意してください。さらに、それぞれを個別に追加することは可能ですが、それによってルール条件が重複することに注意してください。アクセス コントロール ポリシーを適用するとき、システムは重複した条件をまとめて 1 つの条件にします。

- [Available Applications] リストの上の数値は、現在表示されているリスト内のアプリケーションの数を示します。

ステップ 4　オプションで、[Available Applications] リスト内のアプリケーションの横にある情報アイコン（  ）をクリックします。

ポップアップ ウィンドウが表示され、アプリケーションについての要約情報が示されます。次のいずれかの操作をします。

- 追加の情報を表示するには、いずれかのインターネット検索リンクをクリックします。
- ポップアップ ウィンドウを終了して [Applications] ページに戻るには、クローズ アイコン（  ）をクリックするか、[Available Applications] リスト内の別の場所をクリックします。

ステップ 5　[Available Applications] リスト内のアプリケーションを 1 つクリックします。複数のアプリケーションを選択するには、Shift キーと Ctrl キーを使用するか、右クリックして現在表示されているすべてのアプリケーションを選択します。なお、最大で 50 個の条件を追加できます。

ステップ 6　次のいずれかの操作をします。

- [Add to Rule] をクリックします。
- 選択した条件を [Selected Applications and Filters] リストにドラッグ アンド ドロップします。

選択した条件が追加されます。フィルタは [Filters] という見出しの下に表示され、アプリケーションは [Applications] という見出しの下に表示されます。

ステップ 7　必要に応じて、[Selected Applications and Filters] リストの上にある追加アイコン（  ）をクリックすると、[Selected Applications and Filters] リストに現在含まれている個々のすべてのアプリケーションおよびフィルタからなる 1 つのカスタム フィルタを追加できます。

アプリケーション条件ページまたはオブジェクト マネージャを使って作成したカスタム フィルタは、[Application Filters] リストの [User-Created Filters] という見出しの下に表示されます。

オブジェクト マネージャを使ってアプリケーション フィルタを追加する方法については、「アプリケーション フィルタの操作」（P.5-16）を参照してください。条件ページからフィルタを追加する方法については、「条件でのオブジェクトの使用」（P.14-17）を参照してください。

ステップ 8　ルールを保存するか、編集を続けます。

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）。

ポート条件の追加

ライセンス：任意

送信元ポートと宛先ポート、およびトランスポート プロトコルに基づいてネットワーク トラフィックを照合するために、ポート条件をルールに追加します。次に示す任意の種類のポート条件をアクセス コントロール ルールに追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのポート オブジェクト

  オブジェクト マネージャを使用して個別のポート オブジェクトとグループ ポート オブジェクトを作成する方法については、「ポート オブジェクトの操作」（P.5-13）を参照してください。
- ポート条件ページから追加した個別のポート オブジェクト（独自のルールや、他の既存のルール、さらに今後のルールにこれらを追加できます）

  詳細については、「条件でのオブジェクトの使用」（P.14-17）を参照してください。
- トランスポート プロトコル、ポート、またはその両方からなるリテラル ポート値（特定のトランスポート プロトコル選択用）

  詳細については、「リテラル条件の追加」（P.14-16）を参照してください。

次の手順は、アクセス コントロール ルールの追加時または編集時にポート条件を追加する方法を示しています。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。

タイプ 0 が設定された宛先 ICMP ポート、またはタイプ 129 が設定された宛先 ICMPv6 ポートを追加した場合には、要求されていないエコー応答だけがアクセス コントロール ルールで照合されることに注意してください。ICMP エコー要求への応答として送信される ICMP エコー応答は無視されます。ルールですべての ICMP エコーに一致させるには、ICMP タイプ 8 または ICMPv6 タイプ 128 を使用してください。

ポートに ICMP または ICMPv6 タイプを選択した場合、ポートに関連するコードだけを選択できます。ICMP タイプとコードの詳細については、
http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml および
http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml を参照してください。

送信元ポートと宛先ポートの両方をルールに追加する場合、ルール内のすべてのポート用に 1 つのトランスポート プロトコル（TCP または UDP）を共有するポート オブジェクトまたはポート リテラルだけを追加できます。[Selected Source Ports] リストにポートを追加すると、その後いずれかのポート リストに追加できるのは同じプロトコル（TCP または UDP）を使用するポートだけです。同様に、宛先ポートを追加した後、さらに追加する送信元ポートまたは宛先ポートは、同じプロトコルでなければなりません。たとえば、送信元ポートとして DNS over TCP を追加した後、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat （UDP）は追加できません。

送信元ポートだけをルールに追加する場合は、異なるトランスポート プロトコルを使用するポートを追加できます。たとえば、ルールに宛先ポートが存在しない場合は、DNS over TCP および DNS over UDP の両方をルールに追加できます。同様に、宛先ポートだけを追加した場合、異なるトランスポート プロトコルを使用する宛先ポート リテラルまたはポート オブジェクトを追加できます。両方のプロトコルを使用するポートを [Selected Source Ports] リストに追加した後、[Selected Destination Ports] リストにはポートを追加できません（その逆の操作もできません）。

コンテキストに照らして無効なプロトコルのポートを含むポート オブジェクトやポート オブジェクト グループを追加できないことに注意してください。たとえば、送信元ポートとして ICMP ポート オブジェクトを追加することはできません。ルールにすでに含まれるポート オブジェクト グループに、無効なプロトコルを持つポートを追加すると、ルールの横に警告が表示されます。送信元ポートと宛先ポートの両方を追加した場合、ルール エディタでは、すべてのポート オブジェクトとグループが、ルール内で最初に作成されたリテラル ポートで指定されるプロトコルに一致する必要があります。ターゲット デバイスに適用されるアクセス コントロール ポリシーから、無効な設定がシステムによって除去される方法については、「警告およびエラーの処理」（P.13-30）を参照してください。

アクセス コントロール ルールにポート条件を追加する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　ルール編集ページの [Ports] タブを選択します。

[Ports] ページが表示されます。

ステップ 2　必要に応じて、[Available Ports] リストの上にある [Search by name or value] プロンプトをクリックして、名前または値を入力します。

入力していくと、リストが更新されて一致する条件が表示されます。詳細については、「条件リストの検索」（P.14-15）を参照してください。

ステップ 3　[Available Ports] リスト内の条件をクリックします。複数の条件を選択するには、Shift キーと Ctrl キーを使用するか、右クリックしてすべての条件を選択します。なお、最大で 50 個の条件を追加できます。

選択した条件が強調表示されます。

ステップ 4　次のいずれかの操作をします。

- [Add to Source] をクリックして、選択されたポートを [Source Ports] リストに追加します。
- [Add to Destination] をクリックして、選択されたポートを [Destination Ports] リストに追加します。
- 使用可能なポートをリストにドラッグ アンド ドロップします。

ステップ 5　オプションで、個別のポート オブジェクトを作成して追加するには、[Available Ports] リストの上にある追加アイコン（  ）をクリックします。

追加する各ポート オブジェクトでは、1 つのポートを識別できます。その後、追加済みのオブジェクトをルールの条件として選択できます。詳細については、「ポート オブジェクトの操作」（P.5-13）および「条件でのオブジェクトの使用」（P.14-17）を参照してください。

ステップ 6　オプションで、リテラル ポートを追加するには、[Selected Source Ports] または [Selected Destination Ports] リストの下にある [Protocol] ドロップダウン リストからエントリを選択します。

[TCP]、[UDP]、または宛先ポートで [All] を選択した場合、必要に応じてポートを入力してから [Add] をクリックします。宛先ポートで [ICMP] または [IPv6-ICMP] を選択した場合、ポップアップ ウィンドウが表示され、必要に応じてそこでタイプおよび関連するコードを選択します。その後、[Add] をクリックします。0 ～ 65535 の値を持つ 1 つのポートを指定できます。

選択した条件が追加されます（ただし、追加されるポートのプロトコルが、すでに追加済みのポートと競合しない場合）。

ステップ 7　ルールを保存するか、編集を続けます。

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）。

URL 条件の追加

ライセンス：URL Filtering

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：機能に応じて異なる

FireSIGHT システムでは、モニタ対象ホストから要求される URL に基づきネットワーク内を移動できるトラフィックを決定するアクセス コントロール ルールを作成できます。その際、防御センターによって Collective Security Intelligence クラウドから得られるこのような URL についての情報が関連付けられます。この機能は、*URL フィルタリング*と呼ばれます。

URL Filteringのライセンスがない場合でも、許可またはブロックの対象となる個々の URL または URL グループを指定できます。一方、カテゴリやレピュテーションに基づく URL を実行するには、その前に、対象デバイスで URL Filtering ライセンスを有効にし、さらに防御センターとシスコ クラウドとの通信を明示的に許可する必要もあります。DC500 防御センターおよびシリーズ 2 デバイスでは、カテゴリとレピュテーション データを使った URL フィルタリングがサポートされないことに注意してください。また、シリーズ 2 デバイスでは個々の URL や URL グループを指定できません。URL フィルタリングの前提条件については、「クラウド通信の有効化」（P.51-27）を参照してください。

URL カテゴリおよびレピュテーション データの使用

防御センターはシスコ クラウドと通信することで、よくアクセスされる多数の URL に関するデータを取得し、アプライアンス上のローカル データベースにそのデータを保存します。これらの各 URL には、次のようなカテゴリとレピュテーションが関連付けられています。

- URL *カテゴリ*とは、URL の一般的な分類です。たとえば ebay.com は**オークション** カテゴリ、monster.com は**求職**カテゴリに属します。1 つの URL は複数のカテゴリに属することができます。
- URL *レピュテーション*は、組織のセキュリティ ポリシーに反する目的でその URL が使用される可能性を表します。各 URL のリスクは、**ハイ リスク**（レベル 1）から**有名**（レベル 5）の範囲に及びます。

URL カテゴリとレピュテーションを使用すると、アクセス コントロール ルール用の URL 条件を素早く作成できます。これらのルールでは、URL カテゴリとリスクをグループ化して結合できます。たとえば、**薬物乱用**カテゴリ内の**ハイ リスク** URL をすべてブロックする URL 条件を作成できます。その後、モニタ対象ネットワークでだれかがそのカテゴリ/レピュテーションの URL を閲覧しようとすると、セッションがブロックされます。

注　接続ログ、侵入イベント、およびアプリケーション詳細の URL に URL カテゴリおよびレピュテーション データを表示するには、URL 条件を含む少なくとも 1 つのアクセス コントロール ルールを作成する必要があります。

なお、URL のカテゴリやレピュテーションがクラウドで不明な場合、または防御センターがクラウドと通信できない場合には、カテゴリやレピュテーションに基づく URL 条件を含むアクセス コントロール ルールが URL によってトリガー**されない**ことに注意してください。URL にカテゴリやレピュテーションを手動で割り当てることはできません。

URL 検出とブロッキングの制約事項

クライアントとサーバの間で接続が確立される前は、システムは URL をフィルタ処理できません。したがって、URL 条件を含むルール内の他のすべての条件にパケットが一致する場合、URL 識別が未完了であると、パケットは通過を許可されます。この動作により接続が確立され、こうして URL の識別が可能になります。

URL 条件を含むアクセス コントロール ルールをシステムが処理するとき、セッション内で HTTP アプリケーションが識別される時点までは、他の点でそのルールに一致するパケットがデフォルト侵入ポリシーを使って許可され、検査されます。HTTP アプリケーションが識別された後、システムは、URL 条件に一致する残りのセッション トラフィックに対してルールのアクションを適用します。HTTP 識別は、通常、3 ～ 5 個のパケットの範囲内で完了するはずです。完了しない場合、ネットワーク検出ポリシーが最新のものであること、すべてのデバイスに適用されること、およびアクセス コントロール ルールで設定されたネットワークとポートが 1 つも除外されないことを確認してください。

URL 条件の作成時にレピュテーション レベルを選択すると、ルール アクションに応じて次のように動作が異なります。

- ルールによってトラフィックをブロックする場合（ルール アクションは**ブロック**、**リセット付きブロック**、**インタラクティブ ブロック**、または**リセット付きインタラクティブ ブロック**）、1 つのレピュテーション レベルを選択すると、そのレベルよりも厳しいすべてのレピュテーションが一緒に選択されます。たとえば**疑わしいサイト**（レベル 2）をブロックするようルールを設定した場合、**ハイ リスク**（レベル 1）のサイトも自動的にブロックされます。
- ルールによってトラフィックを許可する場合（ルール アクションは**許可**、**信頼**または**モニタ**）、1 つのレピュテーション レベルを選択すると、そのレベルよりも良いすべてのレピュテーションが一緒に選択されます。たとえば**無害なサイト**（レベル 4）を許可するようルールを設定した場合、**有名**（レベル 5）サイトもまた自動的に許可されます。

ルールのアクションを変更した場合、システムは、上記の点に従って URL 条件のレピュテーション レベルを自動的に変更します。レピュテーション レベルを指定しない場合、システムはデフォルトとして**任意**（つまりすべてのレベル）を設定します。たとえば、レピュテーションとは無関係に、すべてのマルウェア サイトをブロックすることができます。また、**任意**を使用して任意のカテゴリを表すこともできます。たとえば、**任意**カテゴリおよび**ハイ リスク** レピュテーションに一致するすべての URL をブロックできます。

リテラル URL、URL オブジェクト、および URL グループの使用

カテゴリとレピュテーションを使って URL 条件を作成することに加えて、個別の URL または URL グループを指定すると、より細かなカスタマイズされた方法で許可/ブロック対象 URL を管理できます。また、これは特別なライセンスなしで実行できる唯一の URL フィルタリング機能です。次に示す任意の種類の URL 条件をアクセス コントロール ルールに追加できます。

- 個別の URL オブジェクトおよび URL オブジェクト グループ。それぞれ個々の URL と複数 URL からなるグループを表します（「URL オブジェクトの操作」（P.5-15）を参照）

  URL カテゴリの場合とは異なり、レピュテーションを使って URL オブジェクトとグループを限定することはできません。既存の URL オブジェクトが適切でない場合は、URL 条件の作成時に URL オブジェクトをその場で作成できます。その後、新しいオブジェクトをそのルールや他の既存のルール、さらに今後のルールで使用することができます。詳細については、「条件でのオブジェクトの使用」（P.14-17）を参照してください。

- リテラル URL（詳細については「リテラル条件の追加」（P.14-16）を参照）

  URL オブジェクトをその場で作成する場合とは異なり、リテラル URL をアクセス コントロール ルールに追加した場合、他のルールでその URL を再利用することはできません。

ネットワーク トラフィックが URL 条件に一致するかどうか判別するために、システムは単純な部分文字列マッチングを実行します。URL オブジェクトまたはリテラル URL の値が、モニタ対象ホストから要求された URL の一部分に一致する場合、アクセス コントロール ルールの URL 条件が満たされます。たとえば example.com へのすべてのトラフィックを許可する場合、ユーザは次の URL を含むサイトを参照できます。

- http://example.com/
- http://example.com/newexample
- http://www.example.com/

つまり、URL 条件で個別の URL を指定するときには、影響を受ける可能性のある他のトラフィックについて慎重に考慮する必要があります。たとえば、ign.com （ゲーム サイト）を明示的にブロックする場合を考えてください。部分文字列マッチングにより *ign.com* 自体だけでなく veris*ign.com* もブロックされることになり、意図しない動作が生じる可能性があります。

なお、HTTPS トラフィックをブロックするため、トラフィックに関する Secure Sockets Layer（SSL）証明書のコモンネームを入力できます。証明書からの URL を入力するときには、ドメイン名を入力し、サブドメイン情報を省略します。たとえば `www.example.com` ではなく `example.com` と入力します。証明書 URL に基づいてトラフィックをブロックする場合、その Web サイトに向かう HTTP と HTTPS の両方のトラフィックがブロックされます。

URL フィルタリング方針の選択

URL 条件の作成方法を決定するときに考慮すべき点として、URL リテラル、オブジェクト、およびグループを使用すると許可/ブロック対象の URL を正確に制御できますが、作成したルールによって意図しない結果が生じないよう注意深く確認する必要があります。

別の方法として、シスコ クラウドのカテゴリおよびレピュテーション データを使用すると制御の正確性はやや低下しますが、ポリシーの作成と管理はより簡単になります。この方法では、システムが URL を適切にフィルタ処理しているという信頼度も増します。さらに重要な点として、クラウドは常に更新されて新しい URL が追加され、既存の URL も新しいカテゴリとリスクに更新されるため、システムでクラウドを使用すると常に最新情報を使って対象の URL をフィルタ処理できます。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表す悪意のあるサイトは、組織でポリシーを更新したり新規ポリシーを適用したりするペースを上回って次々と現れては消える可能性があります。

次に例を示します。

- ルールですべてのゲーム サイトをブロックする場合、新しいドメインが登録されて**ゲーム**に分類されると、これらのサイトをシステムで自動的にブロックできます。
- ルールですべてのマルウェアをブロックする場合、あるブログ ページがマルウェアに感染すると、クラウドはその URL のカテゴリを**ブログ**から**マルウェア**に変更することができ、システムはそのサイトをブロックできます。
- リスクの高いソーシャル ネットワーキング サイトをブロックするルールを使用している場合、ある参加者がプロファイル ページに悪意のあるペイロードへのリンクを掲載すると、クラウドはそのページのレピュテーションを**無害なサイト**から**ハイ リスク**に変更でき、システムでそれをブロックできます。

URL での検索クエリ パラメータ

システムでは、URL 条件の照合に URL 内の検索クエリ パラメータを使用しないことに注意してください。たとえば、すべてのショッピング トラフィックをブロックする場合を考えます。amazon.com を探すために Web 検索を使用してもブロックされませんが、amazon.com を閲覧しようとするとブロックされます。

次の手順は、ルールの追加時または編集時に URL 条件をアクセス コントロール ルールに追加する方法を示しています。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 ルールに URL 条件を追加する方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[URLs] タブを選択します。

[URLs] ページが表示されます。

ステップ 2　必要に応じて、[Available Users] リストの上にある [Search by name or value] プロンプトをクリックして、名前または値を入力します。

入力していくと、リストが更新されて一致する条件が表示されます。詳細については、「条件リストの検索」（P.14-15）を参照してください。

ステップ 3　[Categories and URLs] リストで条件をクリックして、それを選択します。複数の条件を選択するには Shift キーと Ctrl キーを使用します。選択した条件を解除するには、リスト内の任意の条件をクリックします。

[Categories and URLs] リストですべての条件を選択すると、[Selected URLs] リストに追加可能な最大数（50 項目）を超えることに注意してください。

選択した条件が強調表示されます。

ステップ 4　オプションで、[Reputations] ウィンドウでレピュテーション レベルを 1 つクリックします。右クリックして [Select All] をクリックすることで 任意を選択できますが、選択できるのはただ 1 つのレピュテーション レベルだけであることに注意してください。

選択したレベルが強調表示されます。

ステップ 5　次のいずれかの操作をします。

- [Add to Rule] をクリックします。
- 選択した条件を [Selected URLs] リストにドラッグ アンド ドロップします。

選択した条件が追加され、選択したレピュテーション レベルがそれに付加されます。

ステップ 6　オプションで、[Categories and URLs] リストの上にある追加アイコン（ ）をクリックして、個別の URL オブジェクトを追加します。

追加するそれぞれの個別 URL オブジェクトでは、1 つの URL を指定できます。その後、追加済みのオブジェクトをルールの条件として選択できます。詳細については、「URL オブジェクトの操作」（P.5-15）および「条件でのオブジェクトの使用」（P.14-17）を参照してください。

ステップ 7　オプションで、[Selected URLs] リストの下にある [Enter URL] プロンプトをクリックし、リテラル URL を入力して、[Add] をクリックします。

リストが更新されて、それらのエントリが表示されます。詳細については、「リテラル条件の追加」（P.14-16）を参照してください。

リテラル URL にはレピュテーション レベルを指定できないことに注意してください。

ステップ 8　ルールを保存するか、編集を続けます。

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）。

許可されたトラフィックに対するファイル インスペクションと侵入インスペクションの実行

ライセンス：Protection または Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

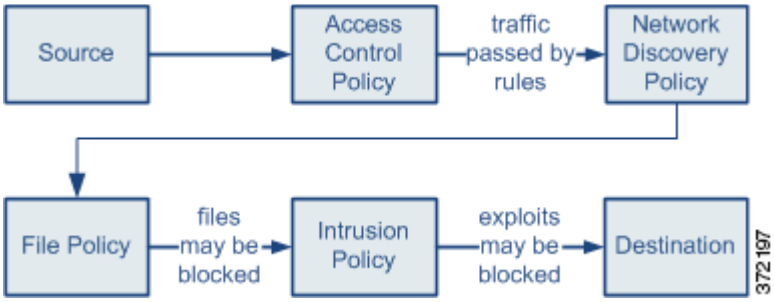
アクセス コントロール ルールの条件に一致するトラフィックを処理することに加えて、侵入ポリシーまたはファイル ポリシーをルールに関連付けることにより、許可されたトラフィックに対する追加のインスペクションを実行できます。

このような関連付けを行うと、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイル ポリシー（またはその両方）を使ってトラフィックを検査するよう、システムに指示できます。実際の展開とポリシー設定に応じて、侵入ポリシーとファイル ポリシーはどちらも、ネットワーク トラフィックが目的の宛先に到達することを防止できます。

下の図に示すように、許可ルール、またはユーザによってバイパスされたインタラクティブ ブロック ルールに一致するトラフィックに対して、次のことが実行されます。

- システムは、現在適用されているネットワーク検出ポリシーのリストに含まれるネットワークを対象にディスカバリを自動的に実行します。
- オプションのファイル ポリシーがファイル制御と AMP を実行します。さらに、
- オプションの侵入ポリシーが検出および防止を実行します。

ファイル インスペクションは侵入ポリシー インスペクションの前に行われるため、そこでブロックされたファイル（マルウェアを含む）に対しては、侵入関連の exploit は検査されません。



許可ルールとインタラクティブ ブロック ルール、およびこれらのアクションを含むアクセス コントロール ルールでのみ追加のインスペクションがトリガーされる理由の詳細については、「ルール アクションについて」（P.14-6）を参照してください。また、アクセス コントロールのデフォルト アクションに、ファイル ポリシーではなく侵入ポリシーを関連付けることができる点にも注意してください。

ヒント　システムは、信頼されたトラフィックに対してはどんなインスペクションも実行しません。侵入ポリシーもファイル ポリシーも含めずに許可ルールを設定すると、信頼ルールの場合と同様にトラフィックが通過しますが、許可ルールでは一致するトラフィックに対してディスカバリを実行できます。

ファイルポリシーと侵入ポリシーに関連付けられた複数のアクセス コントロール ルールを 1 つのアクセス コントロール ポリシーに含めることができます。これにより、さまざまなインスペクション ポリシーを、ネットワーク上のさまざまな種類のトラフィックに対して照合できます。

なお、1 つのアクセス コントロール ポリシーで使用可能な固有の侵入ポリシーの数は、ターゲット デバイスのモデルによって異なることに注意してください。より強力なデバイスは、より多数のポリシーを処理できます。さらに、システムでは、1 つの侵入ポリシーおよびそれにリンクされた変数セットの固有の組み合わせごとに、単一の侵入ポリシーとして数えられることにも注意してください。インスペクションを実行するためのリソースがターゲット デバイスで不足している場合、システムでアクセス コントロール ポリシーを適用することはできません。デバイスでサポート可能な数よりも多い侵入ポリシーを含むアクセス コントロール ポリシーを適用しようとすると、ポップアップ ウィンドウに警告が表示され、デバイスでサポートされる侵入ポリシー最大数を超えたことを示します。

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。

ファイル ポリシーとアクセス コントロール ルール

*ファイル ポリシー*は、ファイル制御を行うためにシステムで使用される設定のセットです。ユーザが特定のアプリケーション プロトコルを介して特定の種類のファイルをアップロード（送信）またはダウンロード（受信）しようとすると、それを検出してブロックすることができます。また、Malware ライセンスとともにファイル ポリシーを使用すると、そのようなファイルの限定セットに対してマルウェア検査を実行し、オプションで、検出されたマルウェアをブロックできます。ファイル ポリシーの詳細については、「ファイル ポリシーの概要と作成」（P.33-10）を参照してください。

ファイル ポリシーをアクセス コントロール ルールに関連付けると、防御センターはそのファイル ポリシーに関してファイルとマルウェアのイベント ロギングを自動的に有効化します。シスコは、このロギング設定を有効のままにしておくことを推奨します。

また、ファイル ポリシーによってイベントが生成されると、システムは（起動元のアクセス コントロール ルールにおける他のロギング設定とは無関係に）関連する接続の終了を防御センターのデータベースに自動的にロギングします。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。

DC500 では Malware ライセンスを使用できないため、マルウェア ブロックまたはマルウェア クラウド ルックアップ アクションを行うルールを含むファイル ポリシーを適用する目的でこのアプライアンスを使用できないことに注意してください。同様に、シリーズ 2 デバイスでは Malware ライセンスを有効にできないため、これらのアクションを行うルールを含むファイル ポリシーをこのアプライアンスに適用することはできません。

侵入ポリシーとアクセス コントロール ルール

*侵入ポリシー*は、侵入検知および防御の設定からなるセットです。システムでこれを使用すると、ネットワーク トラフィックを分析して、オプションで有害なパケットをドロップできます。システムは、侵入ポリシー違反を侵入イベントとしてログに記録します。

侵入ポリシー内で有効化される侵入ルールでは、リテラル設定の代わりに変数を使用して、ネットワーク トラフィックにおける送信元と宛先の IP アドレスとポートをより効率的に識別できます。変数セットの中でこれらの変数を管理します。カスタム値を持つさまざまな変数セットをさまざまな侵入ポリシーにリンクすると、ネットワーク トラフィックをより正確に照合できます。デフォルトでは、アクセス コントロール ルールに関連付けられた侵入ポリシーは、デフォルト変数セット内の変数値を使用します。オプションで、カスタム変数セットを侵入ポリシーにリンクすることもできます。

カスタム ポリシーの作成方法や変数セットの使用法など、侵入ポリシーの詳細については、「侵入防御の概要」（P.17-1）、「侵入ポリシーの設定」（P.20-1）、および「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 ルールに関連付けられた侵入ポリシーがイベントを生成すると、システムは（ルールにおける他のロギング設定とは無関係に）関連する接続の終了を防御センター データベースに自動的にロギングします。シリーズ 3 または仮想アプライアンスでこの接続ロギングを無効にするには、CLI を使用します。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。

一方、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ている侵入ポリシーで侵入イベントが生成されたときには、システムは関連する接続の終了を自動的にロギング**しません**。これは、接続データをログに記録する必要のない、侵入検知および防御のみを行う展開で役立ちます。

ただし、デフォルト アクションで接続開始ロギングを有効にした場合、接続開始のロギングに加えて、関連する侵入ポリシーがトリガーしたときにシステムによって接続終了がログに記録**される**ことに注意してください。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。

次に示す任意の侵入ポリシーをアクセス コントロール ルールに関連付けることができます。

シスコ作成のポリシー

これらは変更不能な*デフォルト*侵入ポリシーであり、セキュリティと接続性のバランスを詳細に考慮して調整されています。デフォルト ポリシーをそのまま使用したり、これに基づいてカスタム ポリシーを作成したりすることで、シスコ脆弱性調査チーム（VRT）の経験を活用できます。詳細については、「デフォルト侵入ポリシーの使用」（P.20-18）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。

ユーザ作成のポリシー

ネットワーク内を移動するトラフィックを検査して環境のパフォーマンスを改善させるために調整された*カスタム*侵入ポリシーを選択することができます。

お客様が独自に作成するカスタム ポリシーに加えて、シスコは初期インライン ポリシーと初期パッシブ ポリシーの 2 つのカスタム ポリシーを提供しています。これらの 2 つのポリシーは、基本ポリシーとして「セキュリティと接続性のバランス」デフォルト ポリシーを使用しています。両者の唯一の相違点は、**インライン時のドロップ**設定がインライン ポリシーでは有効化され、パッシブ ポリシーでは無効化されていることです。詳細については、「カスタム基本ポリシーの使用」（P.20-19）を参照してください。

次の手順は、侵入ポリシーまたはファイル ポリシーを新しいアクセス コントロール ルールに関連付ける基本的な方法を示しています。ルールの追加と変更に関する詳しい説明は、「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。

侵入ポリシーまたはファイル ポリシーを新しいアクセス コントロール ルールに関連付けるには：

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　[Add Rule] をクリックします。

[Add Rule] ページが表示されます。

ステップ 4　[Action] が [Allow]、[Interactive Block]、または [Interactive Block with reset] のいずれかに設定されていることを確認します。

ステップ 5　[Inspection] タブを選択します。

[Inspection] ページが表示されます。

ヒント　関連するファイル ポリシー、ユーザ作成の侵入ポリシー、または変数セットを編集するための新しいブラウザ タブを開くには、該当するドロップダウン リストの横にある編集アイコン（）をクリックします。

ステップ 6　[Intrusion Policy] で侵入ポリシーを選択します。ユーザ作成の侵入ポリシーを選択した場合は、オプションで [Variable Set] を侵入ポリシーにリンクさせることができます。詳細については、「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 ルールに一致するトラフィックに対する侵入インスペクションを無効化するには、[None] を選択します。

注意　シスコの担当者から指示された場合を除き、Experimental Policy 1 を選択**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 7　[File Policy] を 1 つ選択します。

アクセス コントロール ルールに一致するトラフィックに対するファイル インスペクションを無効にするには、[None] を選択します。

ステップ 8　[Add] をクリックして変更を保存します。

ルールが追加され、ポリシー編集ページが表示されます。

接続、ファイル、マルウェアに関する情報のロギング

ライセンス：任意

ポリシー内のアクセス コントロール ルールごとに、ルールの条件に一致するトラフィックに関する接続データをログに記録するかどうか決定する必要があります。接続のロギングを個々のルールに結び付けることで、ログ対象となる接続をきめ細かく制御できます。また、アクセス コントロール ルールのロギング設定では、接続に関連するファイル イベントとマルウェア イベントをログに記録するかどうかも決定します。

ヒント　アクセス コントロール ルールの外側で、他の 2 種類の接続データをロギングできます。まず、デフォルト アクションによって処理された接続をログに記録できます。さらに、セキュリティ インテリジェンス データに基づいて接続を拒否（ブラックリスト化）するか、検査（モニタのみに設定されたブラックリスト化）するかについてシステムが下した判断をログに記録することもできます。

どの接続をログに記録するかの決定

組織のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。目標は、生成されるイベントの数を抑え、分析のために重要な意味を持つルールのロギングだけを有効化することです。ただし、ネットワーク トラフィックの広範な確認が必要な場合は、追加のアクセス コントロール ルールに関するロギングやデフォルト アクションに関するロギングを有効にできます。

パフォーマンスを最適化するため、シスコは、接続の開始と終了の両方ではなく、どちらか一方をロギングすることをお勧めします。1 つの接続に関して、接続終了イベントには、接続開始イベントに含まれるすべての情報に加えて、セッション期間中に収集された情報も含まれることに注意してください。

さらに、FireSIGHT システムでは接続データを使用して、[Connection Summary] ダッシュボードの表示、トラフィック プロファイルの作成、接続データやトラフィック プロファイルの変更に基づく相関ルールのトリガー、および相関ルールへの接続トラッカーの追加を行います。防御センター データベースにロギングされない接続に関しては、これらの機能を利用できません。

接続イベントのログは、防御センター データベースの他に、システム ログ（Syslog）または SNMP トラップ サーバに記録できます。どの時点で、どんな方法で接続をログに記録できるかは、ルール アクション（「ルール アクションについて」（P.14-6）を参照）に応じて異なります。次の表にそれを要約します。

表 14-4

ルール アクションまたはロギング オプション	ロギングされる時点		送信先	
	開始	終了	防御センター	Syslog、SNMP
信頼 デフォルト アクション：信頼	はい	はい	はい	はい
許可 デフォルト アクション：侵入 デフォルト アクション：ディスカバリ	はい	はい	はい	はい
モニタ	いいえ	はい（必須）	はい（必須）	はい
ブロック リセット付きブロック デフォルト アクション：ブロック	はい	いいえ	はい	はい
インタラクティブ ブロック リセット付きインタラクティブ ブロック	はい	はい（バイパスされた場合、イベントは許可アクションを示します）	はい	はい
セキュリティ インテリジェンス	はい	いいえ	はい	はい

アクセス コントロール ルールのロギング設定とは無関係に、ファイル イベントまたは侵入イベントを含む接続がシステムによって自動的にログに記録されることがあることに注意してください（「ファイル イベントとマルウェア イベントに関連付けられた接続のロギング」（P.14-42）および「侵入に関連付けられた接続のロギング」（P.14-42）を参照）。

接続イベントをログに記録する場所または送信先の決定

接続イベントをログに記録するとき、防御センター データベースにそれを保存できます。FireSIGHT システムでは接続データを使用して、[Connection Summary] ダッシュボードの表示、トラフィック プロファイルの作成、接続データやトラフィック プロファイルの変更に基づく相関ルールのトリガー、および相関ルールへの接続トラッカーの追加を行います。これらの機能を利用するには、防御センター データベースに接続をロギングする**必要があります**。データベースの制限については、「データベース イベント制限の設定」（P.50-15）を参照してください。

また、アラート応答を使用して Syslog や SNMP トラップ サーバに接続イベントをロギングすることもできます。アラート応答の設定については、「アラート応答の使用」（P.15-2）を参照してください。

接続の開始または終了のロギング

ルール アクションに応じて、接続の開始または終了（またはその両方）で接続イベントをログに記録できます。一致するトラフィックは拒否されて、追加のインスペクションは行われないため、ブロックされたトラフィックまたはセキュリティ インテリジェンスでブラックリスト化されたトラフィックに関してロギングできるのは接続開始イベントだけです。

一般に、何らかの形で接続データを詳しく分析する必要がある場合は、接続終了時のイベントをログに記録するのが適切です。その理由は、接続開始イベントには、セッション期間を通してトラフィックを検査して判別された情報（たとえば伝送されたデータ総量、接続の最後のパケットのタイムスタンプなど）が含まれないためです。

このため、システムは接続終了データだけを使用して接続の概要データを設定します（「接続サマリーについて」（P.16-3）を参照）。その後、システムはこれを使用して接続グラフとトラフィック プロファイルを作成します。したがって、カスタム ワークフローで接続の概要の表示を使用したり、グラフィカル形式で接続データ表示したり、トラフィック プロファイルを作成/使用したりするためには、接続終了時点の接続イベントをログに記録する**必要があります**。

ただし、単にシステムで新しい接続が検出されるたびにイベントをロギングするだけでよい場合は、接続開始イベントで十分です。接続の開始イベントまたは終了イベントのどちらかに基づいて相関ルールをトリガーとして使用することもできます。

ブロック ルールのロギング

一致するトラフィックは拒否されて、追加のインスペクションは行われないため、ブロッキング ルールでは接続開始イベントだけをログに記録できます ただし、インタラクティブ ブロック ルールでは接続終了のロギングを設定できます。その理由は、システムにより表示される警告ページをユーザがクリックスルーすると（「HTTP 応答ページの追加」（P.13-12）を参照）、その接続は新規の、許可された接続と見なされ、それが終了する時点までシステムによってモニタできるためです。

したがって、インタラクティブ ブロック ルールまたはリセット付きインタラクティブ ブロック ルールにパケットが一致する場合、システムは以下の接続イベントを生成できます。

- ユーザの HTTP 要求が最初にブロックされたときの接続開始イベント（接続ログ内で、このイベントには `Interactive Block` アクションまたは `Interactive Block with reset` アクションが関連付けられます）
- 複数の接続開始または終了イベント（ユーザが警告ページをクリックスルーし、要求した最初のページをロードした場合。これらのイベントには `Allow` アクションおよび理由 `User Bypass` が関連付けられます）

モニタ ルールのロギング

パケットがモニタ ルールに一致する場合、ルールのロギング設定や、後で接続を処理するデフォルト アクションとは無関係に、システムは常に接続終了における接続イベントを生成します。言い換えると、パケットが他のルールに一致せず、デフォルト アクションでロギングが有効になっていない場合でも、パケットがモニタ ルールに一致すれば必ず接続がロギングされます。

モニタ ルールに一致するトラフィックは、必ず後で別の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ため、モニタ ルールが原因でロギングされる接続に関連するアクションは、決して `Monitor` にはなりません。代わりに、次のいずれかになります。

- 接続によってトリガーされたモニタ ルール以外の最初のアクション、または
- デフォルト アクション

システムは、1 つの接続が 1 つのモニタ ルールに一致するたびに 1 つの別個のイベントを生成するわけでは**ありません**。1 つの接続が複数のモニタ ルールに一致する可能性があるため、防御センター データベースにロギングされる各接続イベントには、最大で 8 つの一致するモニタ ルール（接続に一致する最初の 8 つのモニタ ルール）の情報が含まれることがあります。

同様に、Syslog または SNMP トラップ サーバに接続イベントを送る場合、システムは 1 つの接続が 1 つのモニタ ルールに一致するたびに 1 つの別個のアラートを送信するわけではありません。代わりに、接続の終了時にシステムから送られるアラートに、接続に一致した最初の 8 つのモニタ ルールの情報が含まれます。

ヒント　接続ログ内のルール アクションは決して Monitor になりませんが、モニタ ルールに一致する接続に対する相関ポリシー違反をトリガーすることはできます。詳細については、「相関ルール トリガー条件の指定」（P.39-6）を参照してください。

ファイル イベントおよびマルウェア イベントのロギング

アクセス コントロール ルールに関連付けられたファイル ポリシーでファイル イベントまたはマルウェア イベントが生成されたとき、そのイベントがデータベースにロギングされるかどうかは、ルールのロギング設定によって決まります。この設定は自動的に有効になりますが、無効にすることもできます。

ファイル ポリシーでは次の種類のイベントが生成されることがあります。

- *ファイル イベント*：検出またはブロックされたファイル（マルウェア ファイルを含む）を表します
- *マルウェア イベント*：マルウェア クラウド ルックアップまたはマルウェア ブロック ルールによって評価されたファイル内のマルウェアの検出またはブロックを表します
- *レトロスペクティブ マルウェア イベント*：以前に検出されたファイルでのマルウェア処理が変化した場合に生成されます

ファイル イベントまたはマルウェア イベントがファイル ポリシーで生成されると、システムは（起動元のアクセス コントロール ルールにおけるロギング設定とは無関係に）関連する接続の終了を防御センター データベースに自動的にロギングします。

ファイル インスペクションの実行の詳細については、「ファイル ポリシーの概要と作成」（P.33-10）および「許可されたトラフィックに対するファイル インスペクションと侵入インスペクションの実行」（P.14-35）を参照してください。

ファイル イベントとマルウェア イベントに関連付けられた接続のロギング

防御センター データベースにロギングされるそれぞれの接続イベントには、接続で検出またはブロックされたファイルの情報が含まれることがあります。ファイル イベントまたはマルウェア イベントがファイル ポリシーで生成されると、システムは（起動元のアクセス コントロール ルールにおけるロギング設定とは無関係に）関連する接続の終了を防御センター データベースに自動的にロギングします。この接続ロギングを無効にすることはできません。

注　NetBIOS-ssn（SMB）トラフィックのインスペクションによって生成されたファイル イベントでは、クライアントとサーバは永続的接続を確立しているので、その時点では接続イベントを生成しません。システムはクライアントまたはサーバがセッションを終了した後に接続イベントを生成します。

接続でファイルがブロックされた場合、接続ログ内で関連付けられるアクションは Block です。ファイル ポリシーを許可ルールに関連付けたとしてもそうなります。接続の原因は、File Monitor（ファイル タイプまたはマルウェアが検出された）、あるいは Malware Block または File Block（ファイルがブロックされた）です。

侵入に関連付けられた接続のロギング

防御センター データベースにロギングされるそれぞれの接続イベントには、接続で検出またはブロックされた侵入についての情報が含まれることがあります。アクセス コントロール ルールに関連付けられた侵入ポリシーが侵入イベントを生成すると、システムは（ルールにおけるロギング設定とは無関係に）関連する接続の終了を防御センター データベースに自動的にロギングします。

ヒント　仮想アプライアンスでこの接続ロギングを無効にするには、CLI を使用します（「log-ips-connections」（P.D-30）を参照）。

接続で侵入がブロックされた場合、接続ログ内で関連付けられるアクションは `Block`、理由は `Intrusion Block` です（侵入ポリシーを許可ルールに関連付けたとしても）。

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ている侵入ポリシーで侵入イベントが生成されたときには、システムは関連する接続の終了を自動的にロギング**しない**ことに注意してください。これは、接続データをログに記録する必要のない、侵入検知および防御のみを行う展開で役立ちます。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。

デフォルト アクションのロギング

ポリシーのデフォルト アクションによって処理されるトラフィックをロギングする際のオプションは、個々のアクセス コントロール ルールによって処理されるトラフィックをロギングするオプションとよく似ています。たとえば、デフォルト アクションですべてのトラフィックをブロックする場合、デフォルト アクションに関する接続終了イベントをロギングすることはできません。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。

セキュリティ インテリジェンスによるフィルタ処理判断のロギング

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。

セキュリティ インテリジェンスのフィルタ処理機能によって生成されたイベントは、接続の開始、およびシステムによる判断を表します。つまり接続を拒否するか（ブラックリスト化）、それとも検査するか（モニタのみに設定されたブラックリスト化）の決定です。このような検査対象となる接続に関して、接続をさらに処理するアクセス コントロール ルールまたはデフォルト アクションでのロギング設定に応じて、追加の接続イベントがシステムによって生成されることがあります。

セキュリティ インテリジェンスによるフィルタ処理判断をロギングする際のオプションは、個々のアクセス コントロール ルールによって処理されるトラフィックをロギングするオプションと似ています。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。

接続ログについて

個々の接続イベントで入手可能な情報は、接続ロギング オプションの設定内容など、いくつかの要因によって決まります。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。

次の手順では、アクセス コントロール ルールの条件に一致するトラフィック内の接続をログに記録する新しいルールの設定方法を示します。ルールの追加と変更に関する詳しい説明は、「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。

接続、ファイル、およびマルウェア情報をログに記録するアクセス コントロール ルールを設定する方法：

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　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　[Add Rule] をクリックします。

[Add Rule] ページが表示されます。

ステップ 4　[Logging] タブを選択します。

[Logging] タブが表示されます。以下の図は、ファイル ポリシーに関連付けられているルールの [Logging] ページを示しています。

ステップ 5　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に関しては、接続終了イベントをロギングできません。

ステップ 6　接続に関連しているファイル イベントとマルウェア イベントをすべてログに記録するかどうか指定するには、[Log Files] チェック ボックスを使用します。

ファイル ポリシーをルールに関連付けると、このチェック ボックスが自動的に有効になります。シスコは、この設定を有効のままにしておくことを推奨します。

ステップ 7　接続イベントの送信先を指定します。次のいずれかの操作をします。

- 接続イベントを防御センターに送信するには、[Defense Center] を選択します。ルール アクションが [Monitor] である場合は、接続を防御センターにロギングする必要があります。
- 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（）をクリックして Syslog アラート応答を追加することもできます（「Syslog アラート応答の作成」（P.15-5）を参照）。
- 接続イベントを SNMP トラップ サーバに送信するには、[SNMP Trap] を選択して、ドロップダウン リストから SNMP 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（）をクリックして SNMP アラート応答を追加することもできます（「SNMP アラート応答の作成」（P.15-4）を参照）。

ステップ 8　[Add] をクリックして変更を保存します。

ルールが追加され、ポリシー編集ページが表示されます。

ルールにコメントを追加する

ライセンス：任意

アクセス コントロール ルールにコメントを追加することができます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更日と変更理由を記したりすることができます。

ルールを保存する前に、コメントを編集または削除できます。保存後は、コメントの編集も削除もできなくなります。

あるルールの全コメントのリストを表示し、各コメントを追加したユーザやコメント追加日を確認することができます。ルールを作成または編集するときにコメントを表示できます。

ルールの変更内容を保存するとき、コメントの追加が任意選択または必須の操作である場合には、現在の編集セッションでコメントが未追加であればコメントを追加するよう求められることに注意してください。詳細については、「アクセス コントロール ポリシー設定の構成」（P.50-8）を参照してください。

新しいルールにコメントを追加する基本的な手順を次に示します。ルールの追加と変更に関する詳しい説明は、「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。

コメントをルールに追加する方法：

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　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　[Add Rule] をクリックします。

[Add Rule] ページが表示されます。

ステップ 4　[Comments] タブを選択します。

[Comments] ページが表示されます。

ステップ 5　必要に応じて、コメントを追加するには [New Comment] をクリックします。

[New Comment] ポップアップ ウィンドウが表示されます。

ステップ 6　コメントを入力し、[OK] をクリックするとコメントが追加されます。[Cancel] をクリックするとコメントが破棄され、[Comments] ページに戻ります。

ルールの変更内容を保存するとき、コメントの追加が任意選択または必須の操作である場合には、現在の編集セッションでコメントが未追加であればコメントを追加するよう求められることに注意してください。詳細については、「アクセス コントロール ポリシー設定の構成」（P.50-8）を参照してください。

ステップ 7　[Add] をクリックして変更を保存します。

ルールが追加され、ポリシー編集ページが表示されます。