CHAPTER 6

アクセス コントロール ルールを使用したトラフィック フローの調整

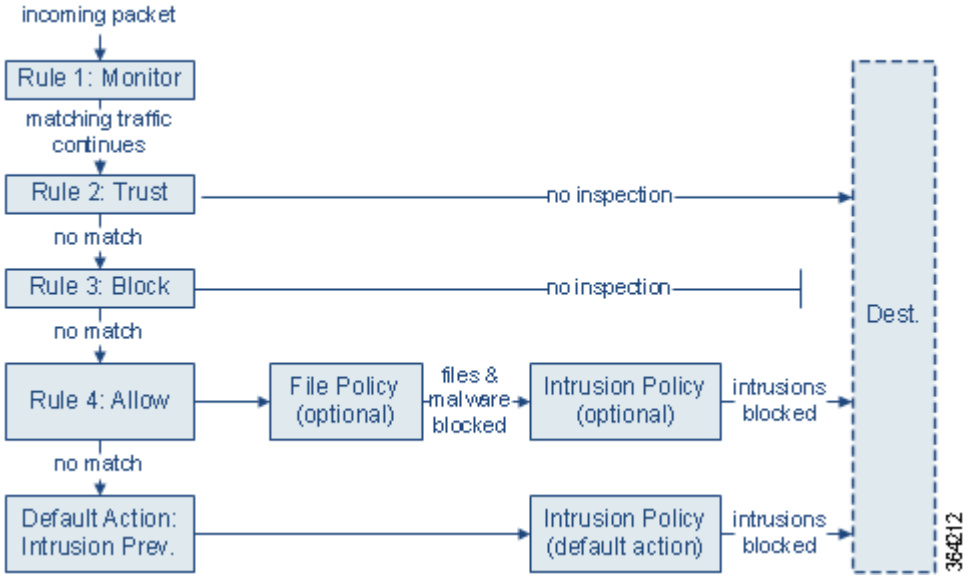
アクセス コントロール ポリシー内では、*アクセス コントロール ルール*によってネットワーク トラフィックを処理する詳細な方法が提供されます。

(注) セキュリティ インテリジェンス ベースのトラフィック フィルタリングと、一部の復号化および前処理は、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。また、*SSL インスペクション*機能を設定し、暗号化されたトラフィックをアクセス コントロール ルールが評価する前にブロックまたは復号することができます。

システムは、指定した順にアクセス コントロール ルールをトラフィックと照合します。ほとんどの場合、システムは、*すべて*のルールの条件がトラフィックに一致する場合、*最初*のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。条件は、単純にも複雑にも設定できます。セキュリティ ゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求された URL、およびユーザごとにトラフィックを制御することができます。

また、各ルールには*アクション*があり、これによって一致するトラフィックをモニタ、信頼、ブロック、または許可するかを決定します。トラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。ただし、システムはトラフィックを信頼またはブロックした後は、追加のインスペクションを実行**しません**。

次のシナリオでは、インラインの侵入防御展開環境で、アクセス コントロール ルールによってトラフィックを評価できる方法を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **ルール 1:モニタ**はトラフィックを最初に評価します。モニタ ルールはネットワーク トラフィックを追跡してログに記録しますが、トラフィック フローには影響しません。システムは引き続きトラフィックを追加のルールと照合し、許可するか拒否するかを決定します。
- **ルール 2:信頼**はトラフィックを 2 番目に評価します。一致するトラフィックは、追加のインスペクションなしでその宛先への通過を許可されます。一致しないトラフィックは、引き続き次のルールと照合されます。
- **ルール 3:ブロック**はトラフィックを 3 番目に評価します。一致するトラフィックは、追加のインスペクションなしでブロックされます。一致しないトラフィックは、引き続き最後のルールと照合されます。
- **ルール 4:許可**は最後のルールです。このルールの場合、一致したトラフィックは許可されますが、トラフィック内の禁止ファイル、マルウェア、侵入、エクスプロイトは検出されてブロックされます。残りの禁止されていない悪意のないトラフィックは宛先に向かうことを許可されます。ファイル インスペクションのみを実行する、または侵入インスペクションのみを実行する、もしくは両方とも実行しない追加の許可ルールを割り当てることができることに留意してください。
- **デフォルト アクション**は、いずれのルールにも一致しないすべてのトラフィックを処理します。このシナリオでは、デフォルト アクションは、悪意のないトラフィックの通過を許可する前に侵入防御を実行します。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルト アクションを割り当てることもあります。(デフォルト アクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません。)

アクセス コントロール ルールの詳細については、以下を参照してください。

- アクセス コントロール ルールの作成および編集(6-3 ページ)
- ポリシー内のアクセス コントロール ルールの管理(6-12 ページ)
- アクセス コントロール ポリシーとルールのトラブルシューティング(4-14 ページ)

アクセス コントロール ルールの作成および編集

ライセンス:任意（Any）

アクセス コントロール ポリシー内では、アクセス コントロール ルールによってネットワーク トラフィックを処理する詳細な方法が提供されます。一意の名前に加え、各アクセス コントロール ルールには次の基本コンポーネントがあります。

状態（State）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、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せず、そのルールに対する警告とエラーの生成を停止します。

位置（Position）

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上から順に、ルールをトラフィックと照合します。モニタ ルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

条件（Conditions）

条件は、ルールが処理する特定のトラフィックを指定します。条件により、セキュリティ ゾーン、ネットワークもしくは地理的位置、ポート、アプリケーション、要求された URL、またはユーザごとにトラフィックを照合することができます。条件は、単純にも複雑にも設定できます。条件の使用には、多くの場合、ライセンスが必要です。

アクション（Action）

ルールのアクションによって、一致したトラフィックの処理方法が決まります。一致したトラフィックをモニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。システムは信頼されたトラフィックまたは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**しない**ことに注意してください。

インスペクション（Inspection）

アクセス コントロール ルールのインスペクション オプションは、ユーザが許可してしまう可能性がある悪意のあるトラフィックをシステムで検査してブロックする方法を制御します。ルールを使用してトラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出たりする前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

ログ

ルールのロギング設定によって、システムが記録する処理済みトラフィックのレコードを管理します。1 つのルールに一致するトラフィックのレコードを 1 つ保持できます。一般に、接続の開始時および終了時にセッションをログに記録できます。接続のログは、ASA FirePOWER モジュールの他に、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。

説明

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。

アクセス コントロール ルールを追加および編集するには、アクセス コントロール ルール エディタを使用します。アクセス コントロール ポリシー エディタの [ルール（Rules）] タブからルール エディタにアクセスします。ルール エディタで、次の操作を実行します。

- エディタの上部で、ルールの名前、状態、位置、アクションなどの基本的なプロパティを設定します。
- エディタの左下にあるタブを使用して、条件を追加します。
- インスペクションおよびロギングのオプションを設定し、さらにルールにコメントを追加するには、右下にあるタブを使用します。便宜上、どのタブを表示しているかに関係なく、エディタにはルールのインスペクションおよびロギングのオプションがリストされます。

（注） アクセス コントロール ルールの適切な作成と順序付けは複雑なタスクですが、効果的な展開を構築するためには不可欠です。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、追加のライセンスが必要となったり、ルールに無効な設定が含まれる場合があります。システムが想定どおりにトラフィックを確実に処理できるように、アクセス コントロール ポリシー インターフェイスにはルールに対する強力な警告およびエラーのフィードバック システムがあります。詳細については、アクセス コントロール ポリシーとルールのトラブルシューティング（4-14 ページ）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変更するには、次の手順を実行します。

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アクセス コントロール ポリシー（Access Control Policy）] の順に選択します。

手順 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。

手順 3　次の選択肢があります。

- 新しいルールを追加するには、[ルールの追加（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。

手順 4　ルールの**名前**を入力します。

各ルールには固有の名前が必要です。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。

手順 5　上記に要約されるようにルール 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。

- ルールを**有効**にするかどうかを指定します。
- ルールの位置を指定します。ルールの評価順序の指定（6-5 ページ）を参照してください。
- ルールの**アクション**を指定します。ルール アクションを使用したトラフィックの処理とインスペクションの決定（6-8 ページ）を参照してください。
- ルールの条件を設定します。ルールが処理するトラフィックを指定するための条件の使用（6-6 ページ）を参照してください。
- 許可ルールおよびインタラクティブ ブロック ルールの場合は、ルールの [インスペクション（Inspection）] オプションを設定します。侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（11-1 ページ）を参照してください。
- [アプリケーション（Applications）] タブでセーフサーチ（）アイコンまたは YouTube EDU（）アイコンをクリックして、コンテンツ制限設定を行います。アイコンが淡色表示の場合、そのルールに対してコンテンツ制限は無効になっています。詳細については、アクセス コントロール ルールを使用したコンテンツ制限の実施（13-2 ページ）を参照してください。

- [ログ（Logging）] オプションを指定します。ネットワーク トラフィックの接続のロギング（36-1 ページ）を参照してください。
- コメント を追加します。ルールへのコメントの追加（6-11 ページ）を参照してください。

手順 6　[FirePOWER の変更の保存（Store FirePOWER Changes）] をクリックしてルールを保存します。

ルールが保存されます。削除アイコン（ ）をクリックすると、ルールを削除できます。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。設定変更の展開（4-13 ページ）を参照してください。

ルールの評価順序の指定

ライセンス：任意（Any）

最初にアクセス コントロール ルールを作成するときに、ルール エディタで [挿入（Insert）] ドロップダウンリストを使用してその位置を指定します。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上から順に、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。

ほとんどの場合、システムは、*すべて*のルールの条件がトラフィックに一致する場合、*最初の*アクセス コントロール ルールに従ってネットワーク トラフィックを処理します。モニタ ルール（トラフィックをログに記録するがトラフィック フローには影響しないルール）の場合を除き、システムは、そのトラフィックがルールに一致した後、追加の優先順位の低いルールに対してトラフィックを評価し続けることは**ありません**。

ヒント　アクセス コントロール ルールの順序を適切に設定することで、ネットワーク トラフィック処理に必要なリソースを削減して、ルールのプリエンプションを回避できます。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。詳細については、パフォーマンスを向上させプリエンプションを回避するためのルールの順序付け（4-17 ページ）を参照してください。

番号ごとのルールの順序付けに加えて、カテゴリ別にルールをグループ化できます。デフォルトでは、3 つのカテゴリ（管理者、標準、ルート）があります。カスタム カテゴリを追加できますが、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。既存のルールの位置またはカテゴリの変更の詳細については、ルールの位置またはカテゴリの変更（6-14 ページ）を参照してください。

ルールの編集または作成時にルールをカテゴリに追加するには、次の手順を実行します。

手順 1　アクセス コントロール ルール エディタで、[挿入（Insert）] ドロップダウンリストから、[カテゴリ（Into Category）] を選択し、使用するカテゴリを選択します。

ルールを保存すると、そのカテゴリの最後に配置されます。

ルールの編集または作成時にルールを番号別に配置するには、次の手順を実行します。

手順 1　アクセス コントロール ルール エディタで、[挿入（Insert）] ドロップダウンリストから、[ルールの上（above rule）] または [ルールの下（below rule）] を選択し、適切なルール番号を入力します。

ルールを保存すると、指定した場所に配置されます。

ルールが処理するトラフィックを指定するための条件の使用

ライセンス：機能に応じて異なる

アクセス コントロール ルールの条件によって、ルールが処理するトラフィックのタイプが識別されます。条件は、単純にも複雑にも設定できます。セキュリティ ゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求された URL、およびユーザごとにトラフィックを制御することができます。

条件をアクセス コントロール ルールに追加する場合は、次の点に注意してください。

- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールの**すべての**条件に一致する必要があります。たとえば、特定のホストの URL フィルタリング（URL 条件）を実行する単一のルールを使用できます（ゾーンまたはネットワーク条件）。
- ルールの条件ごとに、最大 50 の条件を追加できます。条件の基準の**いずれかに**一致するトラフィックはその条件を満たします。たとえば、最大 50 のユーザおよびグループのユーザ制御を実行する単一のルールを使用できます。

  最大 50 の送信元基準と最大 50 の宛先基準を使用して、送信元と宛先ごとにゾーンおよびネットワークの条件を制約できます。送信元基準と宛先基準の両方をゾーンまたはネットワークの条件に追加する場合、一致するトラフィックは、指定した送信元ゾーン/ネットワークの 1 つから発信され、**かつ**宛先ゾーン/ネットワークの 1 つから出力されるものでなければなりません。つまり、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、複数の条件タイプを 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、

```
Source Networks: 10.0.0.0/8, 192.168.0.0/16
Application Category: peer to peer
```

ルールは、いずれかのプライベート IPv4 ネットワーク上のホストからのピアツーピア アプリケーション トラフィックを照合します。パケットは一方**または**もう一方の送信元ネットワークから発信され、**かつ**ピアツーピア アプリケーション トラフィックを表している必要があります。次の接続の両方がルールをトリガーします。

```
10.42.0.105 to anywhere, using LimeWire
192.168.42.105 to anywhere, using Kazaa
```

ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。たとえば、ネットワーク条件を持つがアプリケーション条件を持たないルールは、セッションで使用されるアプリケーションに関係なく、送信元または宛先に基づいてトラフィックを評価します。

（注）　アクセス コントロール ポリシーを適用すると、システムは、そのポリシーのすべてのルールを評価し、ASA FirePOWER モジュールがネットワーク トラフィックを評価するために使用する条件の拡張セットを作成します。複雑なアクセス コントロール ポリシーやルールは、重要なリソースを消費する可能性があります。アクセス コントロール ルールを簡素化するヒントと、パフォーマンスを改善する他の方法については、アクセス コントロール ポリシーとルールのトラブルシューティング（4-14 ページ）を参照してください。

アクセス コントロール ルールを追加または編集するときは、ルール エディタの左下にあるタブを使用してルール条件を追加したり編集したりします。次の表に、追加できる条件のタイプを示します。

表 6-1　アクセス コントロール ルール条件のタイプ

条件	トラフィックの照合	詳細（Details）
ゾーン	特定のセキュリティ ゾーンでインターフェイスを介したデバイスへの着信またはデバイスからの発信	セキュリティ ゾーンは、ご使用の導入ポリシーおよびセキュリティ ポリシーに準じた 1 つ以上のインターフェイスの論理グループです。ゾーン条件を作成するには、セキュリティ ゾーンによるトラフィックの制御（7-2 ページ）を参照してください。
ネットワーク	その送信元または宛先 IP アドレス、国、または大陸による	明示的に IP アドレスまたはアドレス ブロックを指定できます。位置情報機能を使用して、その送信元または宛先の国または大陸に基づいてトラフィックを制御できます。ネットワーク条件を作成するには、ネットワークまたは地理的位置によるトラフィックの制御（7-3 ページ）を参照してください。
ポート	その送信元または宛先ポートによる	TCP および UDP の場合、トランスポート層プロトコルに基づいてトラフィックを制御できます。ICMP および ICMPv6（IPv6 ICMP）の場合、インターネット層プロトコルと、オプションのタイプおよびコードに基づいてトラフィックを制御できます。ポート条件を使用して、ポートを使用しない他のプロトコルでトラフィックを制御することもできます。ポート条件を作成するには、ポートおよび ICMP コードによるトラフィックの制御（7-6 ページ）を参照してください。
アプリケーション	セッションで検出されたアプリケーションによる	基本的な特性であるタイプ、リスク、ビジネス関連性、カテゴリ、タグに応じて、個々のアプリケーションへのアクセスやフィルタ アクセスを制御できます。アプリケーション条件の作成については、アプリケーション トラフィックの制御（8-2 ページ）を参照してください。
URL	セッションで要求された URL による	ネットワーク上のユーザがアクセスできる Web サイトを、個別にまたは URL の一般的分類とリスク レベルに基づいて制限できます。URL 条件の作成については、URL のブロッキング（8-8 ページ）を参照してください。
Users	セッションに関与するユーザによる	モニタ対象セッションに関与するホストにログインした LDAP ユーザに基づいてトラフィックを制御できます。Microsoft Active Directory サーバから取得された個別ユーザまたはグループに基づいてトラフィックを制御できます。ユーザ条件を作成するには、アクセス コントロール ルール：レルムとユーザ（9-1 ページ）を参照してください。

アクセス コントロール ルールはどのライセンスでも作成可能ですが、ルール条件によっては、ポリシーを適用する前に、ライセンスが提供する特定の機能を有効にする必要があることに注意が必要です。詳細については、アクセス コントロールのライセンス要件（4-2 ページ）を参照してください。

ルール アクションを使用したトラフィックの処理とインスペクションの決定

ライセンス:任意（Any）

すべてのアクセス コントロール ルールには、一致するトラフィックについて次のことを決定する *アクション*があります。

- 処理:第一に、ルール アクションは、システムがルールの条件に一致するトラフィックをモニタ、信頼、ブロック、または許可するかどうかを制御します。
- インスペクション:特定のルール アクションでは、適切にライセンス付与されている場合、通過を許可する前に一致するトラフィックをさらに検査することができます。
- ロギング:ルール アクションによって、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できるかが決まります。

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、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（ネットワーク トラフィックに対するデフォルトの処理とインスペクションの設定（4-4 ページ）を参照）。

インライン展開されたデバイスのみがトラフィックをブロックまたは変更できることに留意してください。パッシブ展開されたデバイスは、トラフィックの分析およびロギングはできますが、トラフィックに影響を与えることはできません。ルール アクションの詳細と、ルール アクションがトラフィックの処理、インスペクション、およびロギングにどのように影響するかについては、次の項を参照してください。

- [モニタ（Monitor）] アクション:アクションの遅延とログの確保（6-8 ページ）
- 信頼アクション:インスペクションなしでのトラフィックの通過（6-9 ページ）
- ブロッキング アクション:インスペクションなしでトラフィックをブロック（6-9 ページ）
- インタラクティブ ブロッキング アクション:ユーザが Web サイト ブロックをバイパスすることを許可する（6-10 ページ）
- 許可アクション:トラフィックの許可および検査（6-10 ページ）
- 侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（11-1 ページ）
- アクセス コントロールの処理に基づく接続のロギング（36-10 ページ）

[モニタ（Monitor）] アクション:アクションの遅延とログの確保

ライセンス:任意（Any）

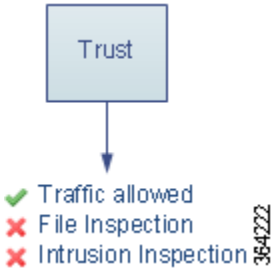
モニタ アクションはトラフィック フローに影響を与えません。つまり、一致するトラフィックがただちに許可または拒否されることはありません。その代わり、追加のルールに照らしてトラフィックが照合され、許可/拒否が決定されます。モニタ ルール以外の一致する最初のルールが、トラフィック フローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、システムはデフォルト アクションを使用します。

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。詳細については、モニタされる接続のロギングについて（36-5 ページ）を参照してください。

信頼アクション:インスペクションなしでのトラフィックの通過

ライセンス:任意(Any)

信頼アクションでは、トラフィックはいかなる種類の追加のインスペクションもなく通過を許可されます。

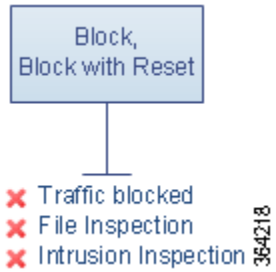


信頼されたネットワーク トラフィックは、接続の開始および終了の両方でログに記録できます。詳細については、信頼されている接続のロギングについて(36-5 ページ)を参照してください。

ブロッキング アクション:インスペクションなしでトラフィックをブロック

ライセンス:任意(Any)

ブロック アクションおよび**リセットしてブロック** アクションはトラフィックを拒否し、いかなる追加のインスペクションも行われません。リセットしてブロック ルールでは接続のリセットも行います。



復号化された HTTP トラフィックの場合、システムが Web 要求をブロックした際に、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。URL ブロック時のカスタム Web ページの表示(8-17 ページ)を参照してください。

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。インライインで展開されたデバイスのみがトラフィックをブロックできることに注意してください。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。詳細については、ブロックされた接続およびインタラクティブにブロックされた接続のロギングについて(36-6 ページ)を参照してください。

注意　サービス妨害(DoS)攻撃中にブロックされた TCP 接続をロギングすると、多数の類似のイベントによってシステム パフォーマンスが影響を受ける可能性があります。ブロック ルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニタするかどうかを検討します。

インタラクティブ ブロッキング アクション:ユーザが Web サイト ブロックをバイパスすることを許可する

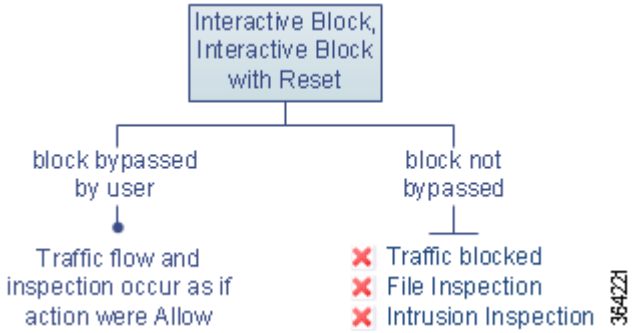
ライセンス:任意(Any)

復号化された HTTP トラフィックの場合、[インタラクティブ ブロック(Interactive Block)] アクションおよび [リセットしてインタラクティブ ブロック(Interactive Block with reset)] アクションを使用すると、ユーザはカスタマイズ可能な警告ページ(*HTTP 応答*ページと呼ばれます)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。[リセットしてインタラクティブ ブロック(Interactive Block with reset)] ルールでは接続のリセットも行います。

Web トラフィックを復号化する SSL インスペクションを設定し、そのトラフィックがインタラクティブ ブロック ルールに一致する場合、システムは応答ページを暗号化し、再度暗号化された SSL 応答ストリームの最後にそのページを送信します。

インタラクティブにブロックされたすべてのトラフィックに対し、システムの処理、インスペクション、およびロギングは、ユーザがブロックをバイパスするかどうかによって異なります。

- ユーザがブロックをバイパスしない(できない)場合は、ルールはブロック ルールを模倣します。一致したトラフィックは追加のインスペクションなしで拒否され、接続の開始のみをロギングできます。これらの接続開始イベントには、インタラクティブ ブロックまたはリセットしてインタラクティブ ブロック アクションがあります。
- ユーザがブロックをバイパスする場合、ルールは許可ルールを模倣します。したがって、ユーザは、どちらかのタイプのインタラクティブ ブロック ルールをファイル ポリシーと侵入ポリシーに関連付け、このユーザ許可されたトラフィックを検査できます。さらにシステムは、接続イベントの開始と終了の両方をログに記録できます。これらの接続イベントには許可アクションがあります。



許可アクション:トラフィックの許可および検査

ライセンス:任意(Any)

許可アクションにより、一致したトラフィックの通過が許可されます。トラフィックを許可すると、関連付けられた侵入ポリシーまたはファイル ポリシー(あるいはその両方)を使用して、暗号化されていないまたは復号化されたネットワーク トラフィックをさらにインスペクションし、ブロックすることができます。

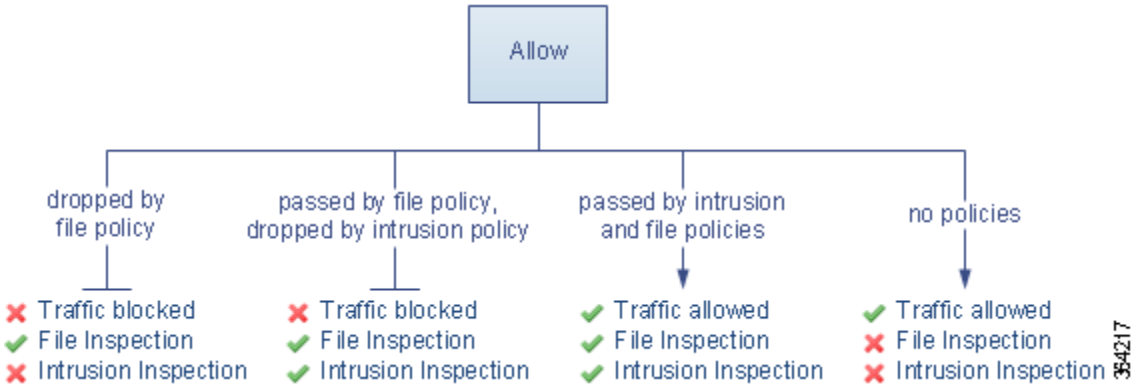
- Protection ライセンスを使用すると、侵入ポリシーを使用して、侵入検知および防御の設定に従ってネットワーク トラフィックを分析し、必要に応じて有害なパケットをドロップすることができます。

- また、Protection ライセンスを使用すると、ファイル ポリシーを使用してファイル制御を実行できます。ファイル制御により、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タイプ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）するのを検出およびブロックすることができます。
- Malware ライセンスを使用すると、この場合もファイル ポリシーを使用して、ネットワークベースの高度なマルウェア防御（AMP）を実行できます。ネットワークベースの AMP は、マルウェアの有無についてファイルを検査し、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、侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（11-1 ページ）を参照してください。

下の図は、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 ブロッキング アクション：ユーザが Web サイト ブロックをバイパスすることを許可する（6-10 ページ）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ています。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、侵入関連のエクスプロイトについては検査されません。

シンプルにするために、この図では、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 フローを示しています。ただし、どちらか 1 つだけを設定することも可能です。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によって決定されます。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 ポリシーによって決定されます。



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。

ルールへのコメントの追加

ライセンス：任意（Any）

アクセス コントロール ルールを作成または編集するときは、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、ルールの変更時期と変更理由を記載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。

ルールを保存すると、最後に保存してから追加されたすべてのコメントは読み取り専用になります。

コメントをルールに追加するには、次の手順を実行します。

手順 1　アクセス コントロール ルール エディタで、[コメント（Comments）] タブを選択します。
[コメント（Comments）] ページが表示されます。

手順 2　[新規コメント（New Comment）] をクリックします。
[新規コメント（New Comment）] ポップアップウィンドウが表示されます。

手順 3　コメントを入力し、[OK] をクリックします。
コメントが保存されます。ルールを保存するまでこのコメントを編集または削除できます。

手順 4　ルールを保存するか、編集を続けます。

ポリシー内のアクセス コントロール ルールの管理

ライセンス：任意（Any）

次の図に示すアクセス コントロール ポリシー エディタの [ルール（Rules）] タブでは、ポリシー内のアクセス コントロール ルールを追加、編集、検索、移動、有効化、無効化、削除、または管理できます。

ポリシー エディタでは、各ルールに対してルールの名前、条件の概要、ルール アクションが表示され、さらにルールのインスペクション オプションとロギング オプションを示すアイコンが表示されます。その他のアイコンは、次の表に示すように、コメント、警告、エラー、およびその他の重要な情報を表しています。無効なルールはグレーで表示され、ルール名の下に [(無効)((disabled))] というマークが付きます。

表 6-2　アクセス コントロール ポリシー エディタについて

アイコン	説明	操作
	侵入インスペクション	ルールのインスペクション オプションを編集するには、アクティブな（黄色の）インスペクション アイコンをクリックします（侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御 (11-1 ページ)を参照）。アイコンが非アクティブ（白）の場合、そのタイプのポリシーがルールに選択されていません。
	ファイルおよびマルウェア インスペクション	

表 6-2　アクセス コントロール ポリシー エディタについて（続き）

アイコン	説明	操作
	logging	ルールのロギング オプションを編集するには、アクティブな（青色の）ロギング アイコンをクリックします（アクセス コントロールの処理に基づく接続のロギング（36-10 ページ）を参照）。アイコンが非アクティブ（白）の場合、接続ロギングがそのルールで無効になっています。
	コメント	ルールにコメントを追加するには、コメント列の数字をクリックします（ルールへのコメントの追加（6-11 ページ）を参照）。数字は、ルールにすでに含まれているコメントの数を示します。
	警告	アクセス コントロール ポリシー エディタで [警告の表示（Show Warnings）] をクリックすると、ポリシーに関するすべての警告を列挙するポップアップ ウィンドウが表示されます。アクセス コントロール ポリシーとルールのトラブルシューティング（4-14 ページ）を参照してください。
	error	
	情報	

アクセス コントロール ルールの管理については、以下を参照してください。

- アクセス コントロール ルールの作成および編集（6-3 ページ）
- アクセス コントロール ルールの検索（6-13 ページ）
- ルールの有効化と無効化（6-14 ページ）
- ルールの位置またはカテゴリの変更（6-14 ページ）

アクセス コントロール ルールの検索

ライセンス：任意（Any）

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 アプリケーションが追加された各ルールの [アプリケーション（Applications）] 列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、[名前（Name）] カラムと [アプリケーション（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。

ルールを検索するには、次の手順を実行します。

手順 1　検索するポリシーのアクセス コントロール ポリシー エディタで、[検索ルール（Search Rules）] プロンプトをクリックし、検索文字列を入力して Enter を押します。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。

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。

手順 2　目的のルールを見つけます。

- 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。
- ページを更新し、検索文字列および強調表示をクリアするには、クリア アイコン（ ）をクリックします。

ルールの有効化と無効化

ライセンス：任意（Any）

アクセス コントロール ルールを作成すると、そのルールはデフォルトで有効になります。ルールを無効にすると、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せず、そのルールに対する警告とエラーの生成を停止します。アクセス コントロール ポリシーのルール リストを表示したときに、無効なルールはグレー表示されますが、変更は可能です。また、ルール エディタを使用してアクセス コントロール ルールを有効化または無効化することもできます。アクセス コントロール ルールの作成および編集（6-3 ページ）を参照してください。

アクセス コントロール ルールの状態を変更するには、次の手順を実行します。

手順 1　有効化または無効化するルールを含むポリシーのアクセス コントロール ポリシー エディタで、ルールを右クリックして、ルールの状態を選択します。

- 非アクティブなルールを有効にするには、[状態（State）] > [有効化（Enable）] を選択します。
- アクティブなルールを無効にするには、[状態（State）] > [無効（Disable）] の順に選択します。

手順 2　[FirePOWER の変更の保存（Store FirePOWER Changes）] をクリックしてポリシーを保存します。

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。設定変更の展開（4-13 ページ）を参照してください。

ルールの位置またはカテゴリの変更

ライセンス：任意（Any）

アクセス コントロール ルールを整理しやすくするために、すべてのアクセス コントロール ポリシーにはシステムによって提供される 3 つのルール カテゴリ（管理者ルール、標準ルール、ルート ルール）があります。これらのカテゴリは移動、削除、名前変更することはできませんが、カスタム カテゴリを作成することができます。

詳細については、以下を参照してください。

- ルールの移動（6-15 ページ）
- 新しいルール カテゴリの追加（6-15 ページ）

ルールの移動

ライセンス：任意（Any）

アクセス コントロール ルールの順序を適切に設定することで、ネットワーク トラフィック処理に必要なリソースを削減して、ルールのプリエンプションを回避できます。

次の手順は、アクセス コントロール ポリシー エディタを使用して 1 つ以上のルールを同時に移動する方法を示しています。また、ルール エディタを使用して個々のアクセス コントロール ルールを移動することもできます。アクセス コントロール ルールの作成および編集（6-3 ページ）を参照してください。

ルールを移動するには、次の手順を実行します。

手順 1　移動するルールを含むポリシーのアクセス コントロール ポリシー エディタで、各ルールの空白領域をクリックしてルールを選択します。複数のルールを選択するには、Ctrl キーと Shift キーを使用します。

選択したルールが強調表示されます。

手順 2　ルールを移動します。カット アンド ペーストやドラッグ アンド ドロップを使用することもできます。

新しい場所にルールをカット アンド ペーストするには、選択したルールを右クリックし、[カット（Cut）] を選択します。次に、貼り付けたい位置に隣接するルールの空白部分を右クリックし、[上に貼り付け（Paste above）] または [下に貼り付け（Paste below）] を選択します。2 つの異なるアクセス コントロール ポリシー間ではアクセス コントロール ルールをコピー アンド ペーストできないことに注意してください。

手順 3　[FirePOWER の変更の保存（Store FirePOWER Changes）] をクリックしてポリシーを保存します。

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。設定変更の展開（4-13 ページ）を参照してください。

新しいルール カテゴリの追加

ライセンス：任意（Any）

アクセス コントロール ルールを整理しやすくするために、すべてのアクセス コントロール ポリシーにはシステムによって提供される 3 つのルール カテゴリ（管理者ルール、標準ルール、ルート ルール）があります。これらのカテゴリは移動、削除、名前変更することはできませんが、標準ルールとルート ルール間でカスタム カテゴリを作成することができます。

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。追加したカテゴリは、名前変更と削除ができます。これらのカテゴリの移動はできませんが、ルールのカテゴリ間およびカテゴリ内外への移動は可能です。

新しいカテゴリを追加するには、次の手順を実行します。

手順 1　ルール カテゴリを追加するポリシーのアクセス コントロール ポリシー エディタで、[カテゴリの追加（Add Category）] をクリックします。

ヒント　ポリシーにルールがすでに含まれている場合は、既存のルールの行の空白部分をクリックして、新しいカテゴリを追加する前にその位置を設定できます。既存のルールを右クリックし、[新規カテゴリの挿入（Insert new category）] を選択することもできます。

[カテゴリの追加（Add Category）] ポップアップ ウィンドウが表示されます。

手順 2　[名前（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。

手順 3　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 [挿入（Insert）] ドロップダウン リストから [カテゴリの上（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 [ルールの下（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 [ルールの上（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。

手順 4　[OK] をクリックします。

カテゴリが追加されます。カテゴリ名を編集するには、カスタム 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。

手順 5　[FirePOWER の変更の保存（Store FirePOWER Changes）] をクリックしてポリシーを保存します。