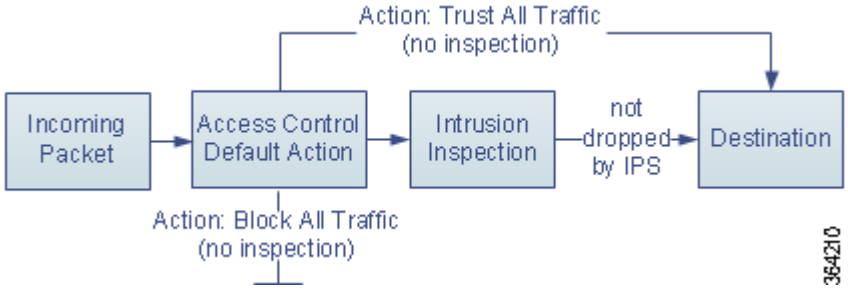
アクセス コントロール ポリシーの準備

*アクセス コントロール ポリシー*は、システムがネットワーク上のトラフィックを処理する方法を決定します。各 ASA FirePOWER モジュールに同時に適用できるポリシーは 1 つだけです。

最も単純なアクセス コントロール ポリシーは、その*デフォルト アクション*を使用してすべてのトラフィックを処理します。このデフォルト アクションは、すべてのトラフィックをさらなるインスペクションを行わずにブロックまたは信頼するように設定するか、あるいは、侵入がないかトラフィックをインスペクションするように設定することができます。



トラフィックのフローに影響を与えることができるのは、インライン展開された ASA FirePOWER モジュールだけであることに注意してください。トラフィックをブロックまたは変更するように設定されたアクセス コントロール ポリシーを、パッシブに展開されたデバイスに適用すると、予期しない結果になることがあります。場合によっては、パッシブに展開された ASA FirePOWER モジュールへのインライン設定の適用がシステムにより拒否されることもあります。

この章では、単純なアクセス コントロール ポリシーを作成して適用する方法について説明します。また、この章には、アクセス コントロール ポリシーの管理に関する基本情報（編集、更新、比較など）も含まれています。詳細については、以下を参照してください。

より複雑なアクセス コントロール ポリシーは、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することができます。さらに、*アクセス コントロール ルール*を使用して、ネットワーク トラフィックのロギングおよび処理を細かく制御することができます。これらのルールは単純でも複雑でもかまいません。複数の基準を使用してトラフィックを照合および検査できます。アクセス コントロール ポリシーの詳細設定オプションでは、復号、前処理、パフォーマンス、およびその他の一般設定を制御できます。

基本的なアクセス コントロール ポリシーを作成した後に、固有の展開環境に合わせて調整する方法については、次の章を参照してください。

- セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録（5-1 ページ）では、最新のレピュテーション インテリジェンスに基づいて接続を即座にブラックリスト登録（ブロック）する方法について説明します。
- ネットワーク分析ポリシーおよび侵入ポリシーについて（18-1 ページ）では、システムの侵入検知および防止機能の一部として、ネットワーク分析および侵入ポリシーがパケットを前処理し確認する方法について説明します。
- 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（6-1 ページ）では、アクセス コントロール ルールによって複数の ASA FirePOWER モジュール間のネットワーク トラフィックをきめ細かく処理する方法について説明しています。
- 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）では、最後の防衛ラインを侵入ポリシーおよびファイル ポリシーが提供する方法について説明します。この防衛ラインは、トラフィックがその宛先に到達する前に、侵入、禁止されたファイル、およびマルウェアを検出してブロックする（オプション）ことによって実現します。

アクセス コントロールのライセンスおよびロール要件

アクセス コントロール ポリシーは、ASA FirePOWER モジュールのどのライセンスでも作成できますが、多くの機能では、ポリシーを適用する前に適切なライセンスを有効にする必要があります。

詳細については、アクセス コントロールのライセンス要件（4-2 ページ）を参照してください。

アクセス コントロールのライセンス要件

アクセス コントロール ポリシーは、ASA FirePOWER モジュールのどのライセンスでも作成できますが、アクセス コントロールの一部の操作を行うには、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ります。

展開環境でサポートされていない機能は、警告アイコンおよび確認ダイアログ ボックスに示されます。詳細は、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（4-16 ページ）を参照してください。

次の表に、アクセス コントロール ポリシーを適用するためのライセンス要件を記載します。

表 4-1　　アクセス コントロールのライセンス要件

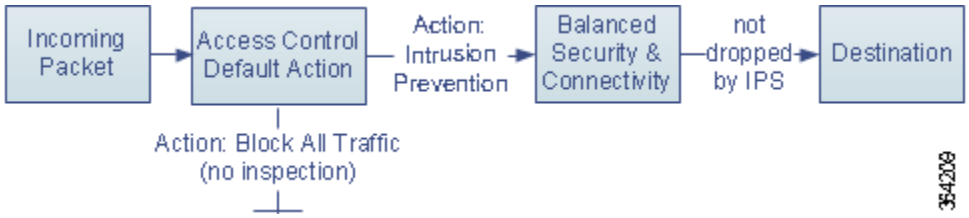
以下を実行するアクセス コントロール ポリシーを適用する場合	ライセンス
ゾーン、ネットワーク、またはポートに基づいてアクセス コントロールを実行する リテラル URL および URL オブジェクトを使用して URL フィルタリングを実行する	任意（Any）
位置情報データ（発信元または宛先の国/大陸）に基づいてアクセス コントロールを実行する	任意（Any）
侵入検知および侵入防御、ファイル制御、またはセキュリティ インテリジェンス フィルタリングを実行する	Protection
高度なマルウェア防御としてネットワークベースのマルウェア検出およびブロッキングを実行する	Malware
ユーザ制御またはアプリケーション制御を実行する	Control
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	URL Filtering

基本的なアクセス コントロール ポリシーの作成

ライセンス: 任意（Any）

新しいアクセス コントロール ポリシーを作成する際には、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必要があります。この時点で、デフォルト アクションにより、ASA FirePOWER モジュールはすべての暗号化されていないトラフィックをどのように処理するかが決定されます。トラフィック フローに影響するその他の設定は、後で追加します。

新しいポリシーを作成するときには、次の図に示すように、さらなるインスペクションなしですべてのトラフィックをブロックするか、あるいは、侵入がないかトラフィックをインスペクションするようにデフォルト アクションを設定できます。



ヒント　初めてアクセス コントロール ポリシーを作成する場合は、トラフィックを信頼することをデフォルト アクションとして選択できません。デフォルトですべてのトラフィックを信頼する場合は、ポリシーを作成した後にデフォルト アクションを変更します。

新規のアクセス コントロール ポリシーを作成したり、既存のアクセス コントロール ポリシーを管理したりするには、[アクセス コントロール ポリシー（Access Control Policy）] ページ（[ポリシー（Policies）] > [アクセス コントロール（Access Control）]）を使用します。

必要に応じて、当初からシステムに付属している Default Trust All Traffic という名前のポリシーを使用したり変更したりできます。

アクセス コントロール ポリシーの作成方法:

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。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

ヒント　この ASA FirePOWER モジュールから既存のポリシーをコピーするか、または他の ASA FirePOWER モジュールからポリシーをインポートすることもできます。ポリシーをコピーするには、コピー アイコン（  ）をクリックします。ポリシーをインポートするには、設定のインポートおよびエクスポート（B-1 ページ）を参照してください。

手順 2　[新しいポリシー（New Policy）] をクリックします。

[新しいアクセス コントロール ポリシー（New Access Control Policy）] ポップアップ ウィンドウが表示されます。

手順 3　[名前（Name）] に一意のポリシー名を入力し、オプションで [説明（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。

手順 4　初期デフォルトアクションを指定します。

- [すべてのトラフィックをブロック（Block All Traffic）] を選択すると、[アクセス コントロール:すべてのトラフィックをブロック（Access Control: Block All Traffic）] をデフォルト アクションとするポリシーが作成されます。
- [侵入防御（Intrusion Prevention）] を選択すると、[侵入防御:バランスの取れたセキュリティと接続（Intrusion Prevention: Balanced Security and Connectivity）] をデフォルト アクションとするポリシーが作成されます。

初期デフォルト アクションを選択する手順、および後でそれを変更する手順については、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（4-5 ページ）を参照してください。

手順 5　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

アクセス コントロール ポリシー エディタが表示されます。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（4-9 ページ）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。設定変更の展開（4-15 ページ）を参照してください。

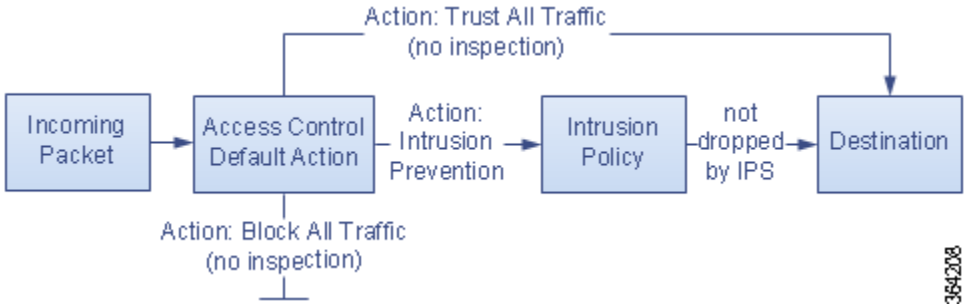
ネットワーク トラフィックに対するデフォルトの処理とインスペクションの設定

ライセンス:任意（Any）

アクセス コントロール ポリシーを作成する場合は、デフォルト アクションを選択する必要があります。アクセス コントロール ポリシーのデフォルト アクションにより、次に該当する復号化されたトラフィックまたは暗号化されていないトラフィックを、システムはどのように処理するかが決定されます。

- 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
- ポリシー内のどのルールにも一致しないトラフィック（トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く）

したがって、アクセス コントロール ルールまたはセキュリティ インテリジェンスの設定が含まれておらず、暗号化されたトラフィックの処理に SSL ポリシーを呼び出さないアクセス コントロール ポリシーを適用する場合、デフォルト アクションにより、ネットワーク上のすべてのトラフィックがどのように処理されるかが決まります。さらなるインスペクションなしですべてのトラフィックをブロックまたは信頼するか、あるいは、侵入がないかトラフィックをインスペクションすることができます。オプションを次の図に示します。



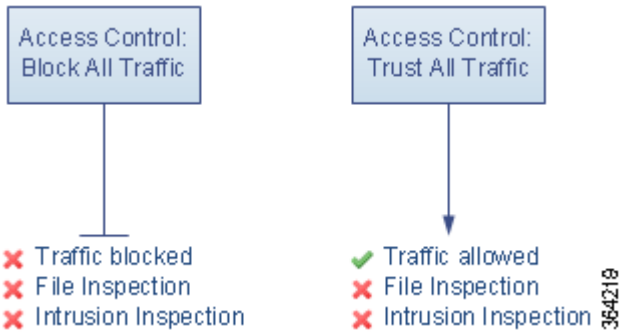
次の表に、さまざまなデフォルト アクションがトラフィックを処理する方法を示し、各デフォルト アクションで処理されるトラフィックで実行できるインスペクションのタイプを示します。デフォルト アクションで処理されるトラフィックに対しては、ファイルやマルウェアのインスペクションを実行**できない**ので注意してください。詳細については、侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（11-1 ページ）を参照してください。

:

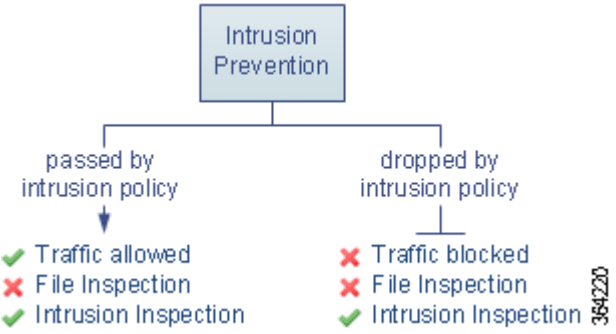
表 4-2　アクセス コントロール ポリシーのデフォルト アクション

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 タイプとポリシー
アクセス コントロール:すべてのトラフィックをブロック	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
アクセス コントロール:すべてのトラフィックを信頼	信頼(追加のインスペクションなしで最終宛先に許可)	なし
侵入防御	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(Protection ライセンスが必要)	侵入、指定した侵入ポリシーおよび関連する変数セットを使用

次の図は、**すべてのトラフィックをブロック**および**すべてのトラフィックを信頼**デフォルト アクションを示しています。



以下の図は、**侵入防御**のデフォルト アクションを示しています。



初めてアクセス コントロール ポリシーを作成する際には、デフォルト アクションで処理される接続のロギングはデフォルトで無効になります。侵入インスペクションを実行するデフォルト アクションを選択すると、デフォルトの侵入変数セットが選択した侵入ポリシーに自動的に関連付けられます。ポリシーを作成した後に、これらのオプションのどちらか、およびデフォルト アクション自体を変更できます。

アクセス コントロール ポリシーのデフォルト アクションと関連オプションを変更するには、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。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 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。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[デフォルト アクション（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、[アクセス コントロール：すべてのトラフィックをブロック（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、[アクセス コントロール：すべてのトラフィックを信頼（Access Control: Trust All Traffic）] を選択します。
- すべてのトラフィックを侵入ポリシー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 [侵入防御（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。

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。

手順 4　**侵入防御**のデフォルト アクションを選択した場合は、変数アイコン（）をクリックし、選択した侵入ポリシーに関連付けられている変数セットを変更します。

表示されるポップアップ ウィンドウで、新しい変数セットを選択して [OK] をクリックします。編集アイコン（）をクリックして、設定されている変数セットを新しいウィンドウで編集することもできます。変数セットを変更しない場合、システムはデフォルトのセットを使用します。詳細については、変数セットの操作（2-15 ページ）を参照してください。

手順 5　ロギング アイコン（）をクリックして、デフォルト アクションによって処理される接続のロギング オプションを変更します。

一致する接続は、その開始時と終了時にログに記録できます。ただし、システムはブロックされたトラフィックの終了時点をロギングできません。接続のログは、ASA FirePOWER モジュール イベント ビューア、外部のシステム 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、アクセス コントロールのデフォルト アクションによって処理される接続のロギング（36-13 ページ）を参照してください。

アクセス コントロール ポリシーの管理

ライセンス:任意（Any）

[アクセス コントロール ポリシー（Access Control Policy）] ページ（[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（Access Control）]）では、現在のカスタム アクセス コントロール ポリシーを、各ポリシーの適用状況に関する情報とともに確認できます。

ユーザが作成したカスタム ポリシーに加えて、カスタム ポリシー Default Allow All Traffic がシステムによって提供され、それを編集して使用することができます。

[アクセス コントロール ポリシー（Access Control Policy）] ページ上のオプションを使用して、次の表にあるアクションを実行できます。

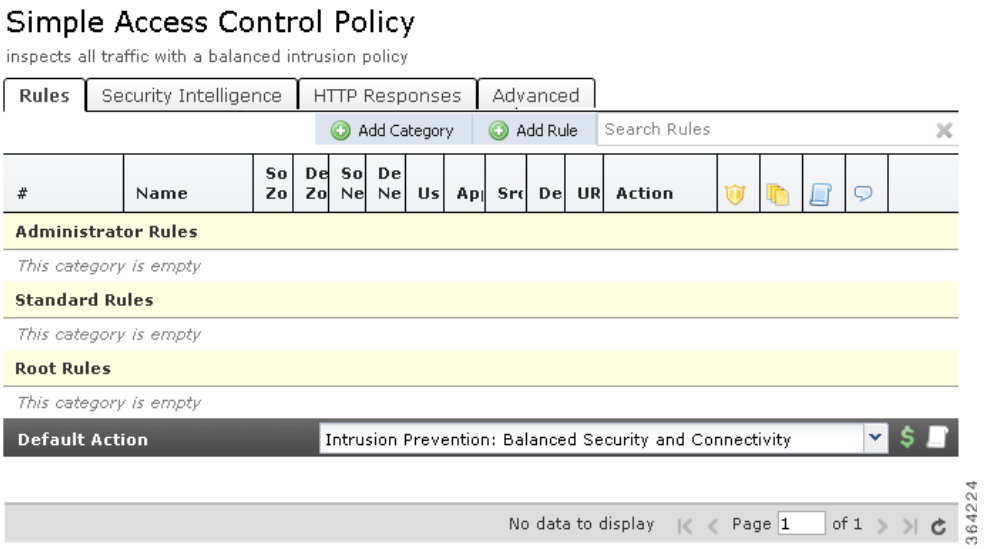
表 4-3　アクセス コントロール ポリシーの管理操作

目的	操作	参照先
新しいアクセス コントロール ポリシーを作成する	[新しいポリシー（New Policy）] をクリックします。	基本的なアクセス コントロール ポリシーの作成（4-3 ページ）
既存のアクセス コントロール ポリシーを編集する	編集アイコン（ ）をクリックします。	アクセス コントロール ポリシーの編集（4-9 ページ）
アクセス コントロール ポリシーを再適用する	適用アイコン（ ）をクリックします。	設定変更の展開（4-15 ページ）
アクセス コントロール ポリシーをエクスポートして別の ASA FirePOWER モジュールにインポートする	エクスポート アイコン（ ）をクリックします。	設定のエクスポート（B-1 ページ）
アクセス コントロール ポリシーの現行の構成設定をリストする PDF を表示する	レポート アイコン（ ）をクリックします。	現在のアクセス コントロール設定のレポートの生成（4-20 ページ）
アクセス コントロール ポリシーを比較する	[ポリシーの比較（Compare Policies）] をクリックします。	アクセス コントロール ポリシーの比較（4-21 ページ）
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、ポリシーを削除することを確認します。適用されたアクセス コントロール ポリシーまたは現在適用しているアクセス コントロール ポリシーは削除できません。	

アクセス コントロール ポリシーの編集

ライセンス:任意（Any）

新しいアクセス コントロール ポリシーを初めて作成する場合は、アクセス コントロール ポリシー エディタが表示され、[ルール（Rules）] タブがフォーカスされます。次の図は、新たに作成されたポリシーを示しています。新しいポリシーにはルールやその他の設定がまだ存在しないため、デフォルト アクションによってすべての暗号化されていないすべてのトラフィックが処理されます。この場合、デフォルト アクションは、最終宛先に許可する前に、システムによって提供される [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] 侵入ポリシーを使用してトラフィックを検査します。



ルールの追加や編成などを行うには、アクセス コントロール ポリシー エディタを使用します。次のリストには、変更可能なポリシー設定に関する情報を記載しています。

名前（Name）と説明（Description）

ポリシーの名前と説明を変更するには、該当するフィールドをクリックし、新しい名前または説明を入力します。

セキュリティ インテリジェンス（Security Intelligence）

セキュリティ インテリジェンスは、悪意のあるインターネット コンテンツに対する最初の防御ラインです。この機能を使用すると、最新のレピュテーション インテリジェンスに基づいて、接続を即座にブラックリスト登録（ブロック）することができます。重要なリソースへの継続的なアクセスを確保するために、ブラックリストはカスタム ホワイトリストで上書きできます。このトラフィック フィルタリングは、ルールやデフォルト アクションを含めて、他のどのポリシー ベースのインスペクション、分析、トラフィック処理よりも**先に**行われます。詳細については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録（5-1 ページ）を参照してください。

ルール（Rule）

ルールによって、ネットワーク トラフィックをきめ細かく処理することができます。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。これらの条件には、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、またはユーザが含まれます。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、特定のライセンスが必要です。

ルールを追加、分類、有効化、無効化、フィルタリング、または管理するには、[ルール（Rules）] タブを使用します。詳細については、アクセス コントロール ルールを使用したトラフィック フローの調整（6-1 ページ）を参照してください。

デフォルト アクション（Default Action）

デフォルト アクションは、セキュリティ インテリジェンスによってブラックリスト登録されず、いずれのアクセス コントロール ルールにも一致しないトラフィックをシステムが処理する方法を決定します。デフォルト アクションを使用すると、すべてのトラフィックをさらなるインスペクションなしでブロックまたは信頼するか、あるいは、侵入がないかトラフィックをインスペクションすることができます。デフォルト アクションによって処理される接続のロギングを有効または無効にできます。

詳細については、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（4-5 ページ）およびアクセス コントロールの処理に基づく接続のロギング（36-11 ページ）を参照してください。

HTTP 応答（HTTP Responses）

ユーザの Web サイト要求がシステムによってブロックされた場合にブラウザに表示するものを指定できます。システム付属の一般的な応答ページを表示するか、カスタム HTML を入力するかを指定できます。ユーザに警告するページを表示することもできますが、続行するかページを更新して最初に要求したサイトをロードするかを、ボタンをクリックして選択させることもできます。詳細については、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。

アクセス コントロールの詳細オプション

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。デフォルト設定は、ほとんどの展開環境に適しています。変更できる詳細設定には次のものがあります。

全般設定：

接続イベントで保存する URL の最大文字数（Maximum URL characters to store in connection events）：ユーザによって要求された URL それぞれについて、ASA FirePOWER モジュール データベースに保存する文字数。接続で検出された URL のロギング（36-15 ページ）を参照してください。

ブロックをバイパスするためのインタラクティブ ブロックを許可する期間（秒）（Allow an Interactive Block to bypass blocking for (seconds)）：ユーザが最初のブロックをバイパスした後に Web サイトを再ブロックするまでの時間。ブロックされた Web サイトのユーザ バイパス タイムアウトの設定（8-16 ページ）を参照してください。

URL キャッシュ ミス ルックアップの再試行（Retry URL cache miss lookup）：無効化されていると、システムは、カテゴリがキャッシュされていない場合でもトラフィックをクラウド ルックアップなしで即座に URL に渡すことができます。クラウド ルックアップを要求する URL は、他のカテゴリのクラウド ルックアップが完了するまで、システムによって [未分類（Uncategorized）] として扱われます。

ポリシー適用時にトラフィックのインスペクションを実施（Inspect traffic during policy apply）：有効化されている場合（デフォルト）、特定の設定によって Snort プロセスの再起動が要求されていない限り、設定変更の展開時にトラフィックのインスペクションを行います。有効化されている場合、リソース需要のため、いくつかのパケットがインスペクションなしでドロップされることがあります。

アイデンティティ/SSL ポリシーの設定

サブポリシー（SSL、アイデンティティ）をアクセス コントロールに関連付けるには、次の詳細設定を使用します。

ネットワーク分析ポリシーと侵入ポリシー

アクセス コントロール ポリシーのデフォルトの侵入ポリシーと、関連する変数セットを変更します。これらは、システムがトラフィックのインスペクション方法を確定できるようになる前に、トラフィックに当初のインスペクションをするために使用されます。また、アクセス コントロール ポリシーのデフォルトのネットワーク分析ポリシーを変更します。これは、前処理のオプションを制御します。

アクセス コントロール ルールが決定される前に使用される侵入ポリシー（Intrusion Policy used before Access Control rule is determined）：アクセス コントロールのデフォルト侵入ポリシーの設定（20-1 ページ）を参照してください。

侵入ポリシーの変数セット（Intrusion Policy Variable Set）：変数セットの操作（2-15 ページ）を参照してください。

デフォルトのネットワーク分析ポリシー（Default Network Analysis Policy）：アクセス コントロールのデフォルト ネットワーク分析ポリシーの設定（20-4 ページ）を参照してください。

前処理オプションを特定のセキュリティ ゾーン、ネットワーク、および VLAN に合わせてカスタマイズするには、カスタムのネットワーク分析ルールおよびネットワーク分析ポリシーを使用します。

カスタム ルール/ポリシー（Custom Rules/Policies）：ネットワーク分析ポリシーによる前処理のカスタマイズ（20-3 ページ）を参照してください。

ファイルおよびマルウェアの設定

ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整（11-20 ページ）では、FirePOWER のファイル制御および AMP のパフォーマンス オプションに関する情報を提供しています。

インテリジェント アプリケーション バイパスの設定

インテリジェント アプリケーション バイパス（IAB）は、トラフィックがインスペクション パフォーマンスとフローしきい値の組み合わせを超過したときにバイパスするアプリケーションを指定する、または、バイパスに関するテストを行うための、エキスパート レベルの設定です。詳細については、インテリジェント アプリケーション バイパス（12-1 ページ）を参照してください。

トランスポート層とネットワーク層のプリプロセッサの設定

トランスポートおよびネットワークのプリプロセッサの詳細設定は、アクセス コントロール ポリシーを展開するすべてのネットワーク、ゾーン、および VLAN にグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。詳細については、トランスポート/ネットワークの詳細設定の構成（24-2 ページ）を参照してください。

検出拡張の設定

検出拡張の詳細設定を行うことで、適応型プロファイルを使用して、ホストのオペレーティング システムに応じて、パッシブ展開におけるパケット フラグメントと TCP ストリームの再構成を向上させることができます。詳細については、パッシブ展開における前処理の調整（25-1 ページ）を参照してください。

パフォーマンス設定

侵入防御パフォーマンスの調整（11-7 ページ）では、侵入行為についてトラフィックを分析する際にシステムのパフォーマンスを向上させるための情報を提供しています。

遅延ベースのパフォーマンス設定

遅延ベースのパフォーマンス設定に関する情報については、パケットおよび侵入ルール遅延しきい値の設定（11-11 ページ）を参照してください。

アクセス コントロール ポリシーを編集すると、変更がまだ保存されていないことを示す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 エディタ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 エディタ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 エディタ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 エディタで 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、[アクセス コントロール ポリシー（Access Control Policy）] ページに戻ります。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。

アクセス コントロール ポリシーの編集方法:

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。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 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。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　ポリシーを編集します。上に概要を示したいずれかのアクションを実行します。

手順 4　設定を保存または廃棄します。

- 変更を保存し、編集を続行する場合は、[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] 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、[ASA FirePOWER 変更の適用（Apply ASA FirePOWER Changes）] をクリックします。設定変更の展開（4-15 ページ）を参照してください。
- 変更を廃棄する場合は、[キャンセル（Cancel）] をクリックし、プロンプトが出たら [OK] をクリックします。

他のポリシーとアクセス コントロールとの関連付け

ライセンス:任意（Any）

次のサブポリシーのいずれかをアクセス コントロール ポリシーに関連付けるには、アクセス コントロール ポリシーの拡張設定を使用します。

- SSL ポリシー:セキュア ソケット レイヤ（SSL）または Transport Layer Security（TLS）で暗号化されたアプリケーション層プロトコル トラフィックに対し、モニタ、復号化、ブロック、または許可を行います。
- アイデンティティ ポリシー:トラフィックに関連付けられているレルムと認証方式に基づいて、ユーザ認証を実行します。

注意　SSL ポリシーまたはアイデンティティ ポリシーの関連付けを行ったり、その後で [なし（None）] を選択してポリシー関連付けの解除を行ったりすると、設定変更の展開時に Snort プロセスが再開し、トラフィックのインスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。

他のポリシーをアクセス コントロール ポリシーに関連付ける方法:

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　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。

手順 3　[詳細設定（Advanced）] タブをクリックします。

手順 4　適切な [ポリシー設定（Policy Settings）] 領域で、編集アイコン（  ）をクリックします。

手順 5　ドロップダウン リストからポリシーを選択します。

ユーザ作成ポリシーを選択した場合、編集アイコンをクリックすると、ポリシーを編集できます。

手順 6　[OK] をクリックします。

手順 7　設定を保存または廃棄します。

- 変更を保存し、編集を続行する場合は、[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] 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、[ASA FirePOWER 変更の適用（Apply ASA FirePOWER Changes）] をクリックします。設定変更の展開（4-15 ページ）を参照してください。
- 変更を廃棄する場合は、[キャンセル（Cancel）] をクリックし、プロンプトが出たら [OK] をクリックします。

失効したポリシーの警告について

ライセンス:任意（Any）

[アクセス コントロール ポリシー（Access Control Policy）] ページ（[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（Access Control）]）では、有効期限が切れたポリシーは、赤色のステータス テキストで表示されます。

ほとんどの場合、アクセス コントロール ポリシーを変更したときは、変更を有効にするためにそのポリシーを再適用する必要があります。アクセス コントロール ポリシーが他のポリシーを呼び出したり、または他の設定に依存したりする場合、それらを変更すると、アクセス コントロール ポリシーを再度適用する必要があります（または、侵入ポリシーの変更の場合は、侵入ポリシーだけを再度適用できます）。

ポリシーの再適用が必要な設定変更には次のものがあります。

- アクセス コントロール ポリシー自体の変更:アクセス コントロール ルール、デフォルト アクション、セキュリティ インテリジェンス フィルタリング、NAP ルールなどの詳細オプションの変更。
- アクセス コントロール ポリシーが呼び出す侵入ポリシーおよびファイル ポリシーのいずれかの変更:SSL ポリシー、ネットワーク分析ポリシー、侵入ポリシー、およびファイル ポリシー。
- アクセス コントロール ポリシーで使用される再利用可能なオブジェクトまたは設定、あるいはアクセス コントロール ポリシーが呼び出すポリシーの変更:ネットワーク オブジェクト、ポート オブジェクト、URL オブジェクト、位置情報オブジェクト、セキュリティ インテリジェンスのリストとフィード、アプリケーション フィルタまたはディテクタ、侵入ポリシーの変数セット、ファイル リスト、復号化関連オブジェクト、セキュリティ ゾーンなど。
- システム ソフトウェア、侵入ルール、または脆弱性データベース（VDB）の更新。

これらの設定の一部は、ASA FirePOWER モジュールインターフェイスの複数の場所から変更できることに留意してください。たとえば、セキュリティ ゾーンは、オブジェクト マネージャ（[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）]）を使用して変更できます。

次の更新では、ポリシーの再適用は必要**ありません**。

- URL フィルタリング データへの自動更新
- スケジュールされた位置情報データベース（GeoDB）の更新

アクセス コントロールまたは侵入ポリシーが失効した理由を確認するには、比較ビューアを使用します。

アクセス コントロール ポリシーが失効した理由を確認するには、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。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。失効したポリシーには、ASA FirePOWER モジュールがポリシーの更新を必要としていることを示す赤色のステータス テキストが付いています。

手順 2　失効したポリシーのポリシー ステータスをクリックします。

詳細な [アクセス コントロール ポリシーの適用（Apply Access Control Policy）] ポップアップ ウィンドウが表示されます。

手順 3　該当する変更されたコンポーネントの横にある [失効（Out-of-date）] をクリックします。

ポリシーの比較レポートが新しいウィンドウに表示されます。詳細については、アクセス コントロール ポリシーの比較（4-21 ページ）および 2 つの侵入ポリシーまたはリビジョンの比較（26-11 ページ）を参照してください。

手順 4　オプションで、ポリシーを再度適用します。

設定変更の展開を参照してください。

設定変更の展開

ライセンス：任意（Any）

ASA FirePOWER モジュールを使用して展開環境の設定を行った後で、その設定に変更を加える場合は、その都度、新しい設定を展開する必要があります。

この導入アクションにより、次の設定コンポーネントが配布されます。

- アクセス コントロール ポリシーとすべての関連ポリシー：DNS、ファイル、ID、侵入、ネットワーク分析、SSL
- 導入されたポリシーに関連付けられているすべての関連ルール設定とオブジェクト
- 侵入ルール アップデート
- デバイスとインターフェイスの設定

注意　特殊なケースとして、設定変更を展開すると、トラフィック フローと処理が一時的に停止したり、いくつかのパケットが検査されないまま通過することがあります。利用できない時間を最小限にするために、導入は変更時間帯に実行します。

設定変更を展開するには、次のようにします。

手順 1　[展開（Deploy）] をクリックして、[FirePOWER 変更の展開（Deploy FirePOWER Changes）] を選択します。

手順 2　[展開（Deploy）] をクリックします。

手順 3　変更の展開時にエラーまたは警告が出された場合には、次の選択肢があります。

- [続行（Proceed）] をクリックして、エラーまたは警告条件を解決しないで導入を続行します。
- [キャンセル（Cancel）] をクリックして、展開を実行せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

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

ライセンス：任意（Any）

アクセス コントロール ポリシーを適切に設定すること、特に、アクセス コントロール ルールを作成して順序付けることは複雑なタスクです。しかし、これは効果的な展開を構築するために不可欠なタスクです。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、ルールに無効な設定が含まれてしまう可能性があります。ルールおよび他のポリシー設定にはどちらも追加ライセンスが必要な場合があります。

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強力なフィードバック システムがあります。アクセス コントロール ポリシーおよびルール エディタのアイコンは、アクセス コントロールのエラー アイコンの表に示すように、警告とエラーを示します。

ヒント　アクセス コントロール ポリシー エディタで、ポリシーのすべての警告を表示するポップアップ ウィンドウを表示するには [警告の表示（Show Warnings）] をクリックします。

また、トラフィックの分析およびフローに影響を与える可能性がある問題の適用時には、システムによって警告が表示されます。

表 4-4　アクセス コントロールのエラー アイコン

アイコン	説明	詳細
	エラー	ルールまたは設定にエラーがある場合、影響を受けるルールを無効にしても、問題を修正するまでポリシーを適用できません。
	警告	ルールまたはその他の警告を表示するアクセス コントロール ポリシーを適用できます。しかし、警告とマークされている誤った設定には影響を与えません。 たとえば、プリエンプション処理されたルールや、誤った設定（空のオブジェクト グループを使用した条件、一致するアプリケーションがないアプリケーション フィルタ、クラウド通信を有効にしないまま行った URL 条件の設定など）によってトラフィックと一致することがないルールを含むポリシーであっても、適用することができます。これらのルールは、トラフィックを評価しません。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。 別の例として、多くの機能では、特定のライセンスが必要です。アクセス コントロール ポリシーは、該当するデバイスのみに正常に適用されます。
	情報	情報アイコンは、トラフィックのフローに影響する可能性がある設定に関する有用な情報を表示します。これらの問題によってポリシーの適用が阻まれることはありません。 たとえば、ユーザがアプリケーション制御または URL フィルタリングを実行している場合、システムは接続においてアプリケーション トラフィックまたは Web トラフィックを識別するまで、その接続の最初の数パケットと一部のアクセス コントロール ルールとの照合をスキップすることがあります。これにより接続を確立することができ、アプリケーションと HTTP 要求を識別できるようになります。詳細については、アプリケーション制御の制約事項（8-7 ページ）およびURL の検出とブロッキングの制約事項（8-14 ページ）を参照してください。

アクセス コントロール ポリシーおよびルールを適切に設定することで、ネットワーク トラフィックの処理に必要なリソースも減らすことができます。複雑なルールの作成、多数のさまざまな侵入ポリシーの呼び出し、およびルールの誤った順序付けはすべて、パフォーマンスに影響を与える可能性があります。

詳細については、以下を参照してください。

- パフォーマンスを向上させるためのルールの簡素化（4-17 ページ）
- ルールのプリエンプションと無効な設定の警告について（4-18 ページ）
- 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（4-19 ページ）

パフォーマンスを向上させるためのルールの簡素化

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 ポリシーを適用すると、システムはすべてのルールをまとめて評価し、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。サポートされるアクセス コントロール ルールまたは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 ルールの簡素化

次のガイドラインは、アクセス コントロール ルールを簡素化し、パフォーマンスを向上させるのに役立ちます。

- ルールの作成時には、条件を構成する要素は可能な限り少なくします。たとえば、ネットワーク条件では、個々の IP アドレスではなく IP アドレス ブロックを使用します。ポート条件では、ポート範囲を使用します。アプリケーション制御および URL フィルタリングを実行する場合はアプリケーション フィルタと URL カテゴリおよびレピュテーションを使用し、ユーザ制御を実行する場合は LDAP ユーザ グループを使用します。

  ただし、アクセス コントロール ルールの条件で使用する要素をオブジェクトに組み合わせても、パフォーマンスは向上しません。たとえば、50 個の IP アドレスを 1 つのネットワーク オブジェクトに含めて使用することにパフォーマンス的なメリットはなく、条件にこれらの IP アドレスを個別に含めるよりも単に構成上のメリットがあるだけです。

- できる限り、セキュリティ ゾーンごとにルールを制限します。デバイスのインターフェイスがゾーン制限されたルールのゾーンの 1 つにない場合、ルールはそのデバイスのパフォーマンスに影響を与えません。

- ルールを過度に設定しないでください。処理するトラフィックの照合が 1 つの条件で十分な場合には、2 つの条件を使用しないでください。

侵入ポリシーと変数セットの急増の回避

アクセス コントロール ポリシーでトラフィックをインスペクションするために使用できる一意の侵入ポリシーの数は、ポリシーの複雑度によって異なります。許可ルールおよびインタラクティブ ブロック ルール、ならびにデフォルト アクションにはそれぞれ、1 つの侵入ポリシーを関連付けることができます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。アクセス コントロール ポリシー全体で、侵入ポリシーを 3 つしか選択できない場合があります。

侵入ポリシーの数がサポートされる数を超える場合は、アクセス コントロール ポリシーを再評価してください。複数の侵入ポリシーまたは変数セットを統合すると、複数のアクセス コントロール ルールに 1 つの侵入ポリシーと変数セットのペアを関連付けることができます。

アクセス コントロール ポリシーの次の場所のそれぞれで、選択したポリシーの数と、それらのポリシーが使用する変数セットの数を確認します。アクセス コントロール ポリシーの詳細設定の [アクセス コントロール ルールが決定される前に使用される侵入ポリシー（Intrusion Policy used before Access Control rule is determined）] オプション、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、およびポリシー内のアクセス コントロール ルールのインスペクション設定。

ルールのプリエンプションと無効な設定の警告について

ライセンス: 任意（Any）

アクセス コントロール ルール（および、高度な展開ではネットワーク分析ルール）の適切な設定と順序付けは、効果的な展開を構築するために不可欠です。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 ルールが他のルールをプリエンプション処理したり、ルールに無効な設定が含まれている場合があります。同様に、アクセス コントロール ポリシーの詳細設定を使用して設定するネットワーク分析ルールにも、これと同じ問題が生じる可能性があります。システムは、警告とエラーのアイコンを使用してこれらをマークします。

ルールのプリエンプションの警告について

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。

```
Rule 1: allow Admin users
Rule 2: block Admin users
```

上記の最初のルールによってトラフィックは事前に許可されているため、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。

次の点に注意してください。

- 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。
- 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。
- 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。

無効な設定の警告について

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。次の例について考えてみます。

- ルールの送信元ポートにポート グループを追加し、その後そのポート 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。ポリシーをまだ適用することはできますが、ルールはネットワーク トラフィックに影響を与えません。
- ルールにユーザを追加し、その後 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、そのルールは影響を与えなくなります。

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

ライセンス：任意（Any）

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。

アクセス コントロール ルールを適切に順序付けることで、ネットワーク トラフィックの処理に必要なリソースが減り、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。

重要性が最も高いルールから最も低いルールへの順序付け

最初に、組織のニーズに適するルールを順序付けする必要があります。すべてのトラフィックに適用する必要がある優先順位ルールをポリシーの先頭部分付近に配置します。たとえば、ある 1 人のユーザからのトラフィックに侵入がないかを検査する（許可ルールを使用）が、部門内の他のすべてのユーザは信頼する（信頼ルールを使用）場合は、その順序に 2 つのアクセス コントロール ルールを配置します。

特定のルールから一般的なルールへの順序付け

特定のルール、つまり処理するトラフィックの定義を絞り込むルールを先に設定することで、パフォーマンスを向上させることができます。これは、広範な条件を持つルールが多様なタイプのトラフィックを照合し、後でより多くの特定のルールをプリエンプション処理できるという理由からも重要です。

ほとんどのソーシャル ネットワーキング サイトをブロックする一方で、特定の他のサイトへのアクセスを許可するシナリオを想定してください。たとえば、グラフィック デザイナーに対して Creative Commons Flickr や deviantART コンテンツへのアクセスは許可したいが、Facebook や Google+ などの他のサイトへのアクセスは許可したくない場合があります。この場合はルールを次のように順序付けする必要があります。

```
Rule 1: Allow Flickr, deviantART for the "Design" LDAP user group
Rule 2: Block social networking
```

ルールを入れ替える場合は次のようになります。

```
Rule 1: Block social networking
Rule 2: Allow Flickr, deviantART for the "Design" LDAP user group
```

最初のルールは、Flickr や deviantART を含む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ます。2 番目のルールに照合されるトラフィックがないため、利用可能にしようとしたコンテンツにグラフィック デザイナーはアクセスできません。

トラフィックを後で検査するルールの配置

侵入、ファイルおよびマルウェアのインスペクションには処理リソースが必要であるため、トラフィックをインスペクションしないルール（信頼、ブロック）をトラフィックのインスペクションを行うルール（許可、インタラクティブ ブロック）よりも前に配置することで、パフォーマンスを向上させることができます。信頼ルールやブロック ルールは、システムが別の方法で検査した可能性があるトラフィックを迂回させることができるからです。他の要素がすべて同等である、つまりルールのセットで、より重要というルールがなく、プリエンプションが問題ではない場合には、次の順序でルールを配置することを考慮してください。

- 一致する接続はロギングするが、トラフィックで他のアクションは実行しないモニタ ルール
- 追加のインスペクションなしでトラフィックを処理する信頼ルールおよびブロック ルール

- トラフィックの追加のインスペクションを行わない許可ルールおよびインタラクティブ ブロック ルール
- マルウェア、侵入、またはその両方がないか任意でトラフィックを検査する許可ルールおよびインタラクティブ ブロック ルール

現在のアクセス コントロール設定のレポートの生成

ライセンス:任意（Any）

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。このレポートには、次の情報が含まれており、監査目的や現在の設定の調査目的に使用できます。

表 4-5　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
ポリシー情報（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。
HTTP ブロック レスポンス（HTTP Block Response） HTTP インタラクティブ ブロック レスポンス（HTTP Interactive Block Response）	ポリシーを使用して Web サイトをブロックするときにユーザに表示されるページの詳細が示されます。
セキュリティ インテリジェンス（Security Intelligence）	ポリシーのセキュリティ 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示されます。
デフォルト アクション（Default Action）	デフォルト アクションと関連する変数セット（存在する場合）が示されます。
ルール（Rule）	ポリシーの各アクセス コントロール ルールが示され、その設定の詳細が示されます。
詳細設定（Advanced Settings）	次のようなポリシーの詳細設定の情報 • アクセス コントロール ポリシーのトラフィックを前処理するために使用されるネットワーク分析ポリシー、およびグローバル前処理オプション • パッシブ展開用の適応型プロファイル設定 • ファイル、マルウェアおよび侵入を検出するためのパフォーマンス設定 • 他のポリシー全体の設定
参照オブジェクト（Referenced Objects）	侵入ポリシーの変数セットや SSL ポリシーで使用されるオブジェクトなど、アクセス コントロール ポリシーによって参照される再利用可能なオブジェクトに関する詳細を提供します。

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、アクセス コントロール ポリシーの比較（4-21 ページ）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:

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。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 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。コンピュータにレポートを保存するように求められます。

アクセス コントロール ポリシーの比較

ライセンス:任意（Any）

組織の標準に準拠していることを確認するためや、システム パフォーマンスを最適化するために、ポリシーの変更を検討する際には、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、[実行中の設定（Running Configuration）] を選択した場合、現在アクティブなポリシーは空白のバーで表されます。

  これを使用すると、相違点を強調表示したまま、ユーザ インターフェイス上で両方のポリシーを表示し、そこへ移動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（4-22 ページ）
- アクセス コントロール ポリシー比較レポートの使用（4-22 ページ）

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（Any）

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 つのポリシー間の差異は、次のように強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーで異なることを示し、差異は赤色で示されます。
- 緑色は強調表示された設定が一方のポリシーには存在するが、他方には存在しないことを示します。

次の表に、実行できる操作を記載します。

表 4-6　　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
変更に個別にナビゲートする	タイトル バーの上にある [前へ（Previous）] または [次へ（Next）] をクリックします。 左側と右側の間にある二重矢印アイコン（ ）が移動し、表示している違いを示す [差異（Difference）] 番号が変わります。
新しいポリシー比較ビューを生成する	[新しい比較（New Comparison）] をクリックします。 [比較の選択（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（4-22 ページ）を参照してください。
ポリシー比較レポートを生成する	[比較レポート（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（Any）

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差異（2 つのアクセス コントロール ポリシーの差異、またはあるポリシーと現在適用中のポリシーとの差異）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、表 4-5（4-20 ページ）に記載されているセクションが含まれています。

ヒント　同様の手順を使用して、SSL ポリシー、ネットワーク分析ポリシー、侵入ポリシー、ファイル ポリシー、またはシステム 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:

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。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　[ポリシーの比較（Compare Policies）] をクリックします。

[比較の選択（Select Comparison）] ウィンドウが表示されます。

手順 3　[比較対象（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、[他のポリシー（Other Policy）] を選択します。

  ページが更新されて、[ポリシー A（Policy A）] と [ポリシー B（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。
- 現在のアクティブ ポリシーを他のポリシーに対して比較するには、[実行中の設定（Running Configuration）] を選択します。

  ページが更新されて、[ターゲット/実行中の設定 A（Target/Running Configuration A）] と [ポリシー B（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。

手順 4　選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較する場合は、[ポリシー A（Policy A）] と [ポリシー B（Policy B）] ドロップダウンリスト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、[ポリシー B（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。

手順 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。

手順 6　必要に応じて、アクセス コントロール ポリシー比較レポートを生成するには [比較レポート（Comparison Report）] をクリックします。

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。コンピュータにレポートを保存するように求められます。