Cisco ASA with FirePOWER Services ローカル管理設定ガイド

バージョン 6.0.0
2015 年 11 月 9 日

Cisco Systems, Inc.
www.cisco.com
シスコは世界各国 200 箇所にオフィスを開設しています。
所在地、電話番号、FAX 番号は以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

シスコ ASA FirePOWER モジュールの概要

シスコ ASA FirePOWER モジュール® は、Cisco ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X、ASA5545-X、ASA5555-X、ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40、ASA5585-X-SSP-60、および ISA3000 の各デバイスに展開できるモジュールです。モジュールは、ユーザの組織のセキュリティ ポリシー（ネットワークを保護するためのガイドライン）に準拠した方法でネットワーク トラフィックを処理するように設計されています。セキュリティ ポリシーにはアクセプタブル ユース ポリシー（AUP）も含まれていることがあります。AUP は、組織のシステムの使用方法に関するガイドラインを従業員に提供します。

このガイドでは、ASDM 経由でアクセス可能な、ASA FirePOWER モジュールの機能の Onbox 設定に関する情報を提供します。各章の説明、図、および手順では、ユーザ インターフェイスのナビゲート、システム パフォーマンスの最大化、問題のトラブルシューティングに役に立つ詳細な情報を記載しています。

（注） ASA FirePOWER モジュールをホストしている ASA でコマンドの権限を有効にする場合は、特権レベル 15 を持つユーザ名でログインして、ASA FirePOWER のホーム、設定、およびモニタリングのページを参照できるようにする必要があります。ステータス ページ以外の ASA FirePOWER のページに対する読み取り専用またはモニタ専用のアクセス権限は、サポートされていません。

続く各トピックでは、ASA FirePOWER モジュールの概要、主要なコンポーネント、およびこのマニュアルの使用方法について説明しています。

ASA FirePOWER モジュールの概要

ASA FirePOWER モジュールは、ネットワーク セグメントにインストールされている ASA デバイスで動作し、分析用のトラフィックをモニタします。

インラインで展開されたシステムは、アクセス コントロールを使用してトラフィックのフローに影響を与えることができ、これによって、ネットワークを出入りしたり通過したりするトラフィックを処理する方法を詳細に指定できます。ネットワーク トラフィックについて収集したデータおよびそのデータから収集したすべての情報は、次に基づいてそのトラフィックのフィルタ処理や制御ができます。

- シンプルで容易に決定されるトランスポート層およびネットワーク層の特性（送信元と宛先、ポート、プロトコルなど）
- レピュテーション、リスク、ビジネスとの関連性、使用されたアプリケーション、または訪問した URL などの特性を含む、トラフィックに関する最新のコンテキスト情報
- 組織内の Microsoft Active Directory LDAP ユーザ

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。たとえば、レピュテーション ベースのブラックリスト登録は、単純な送信元と宛先のデータを使用するため、禁止されたトラフィックをプロセスの初期段階でブロックできます。その一方、侵入およびエクスプロイトの検出とブロックは、プロセスの最後の防衛ラインとして実行されます。

ASA FirePOWER モジュール コンポーネント

続く各トピックでは、組織のセキュリティ、適用可能な使用ポリシー、およびトラフィック管理の戦略に対して有用な、ASA FirePOWER モジュールの主な機能について説明します。

- アクセス コントロール（1-2 ページ）
- 侵入検知および侵入防御（1-3 ページ）
- 高度なマルウェア防御とファイル制御（1-3 ページ）
- アプリケーション プログラミング インターフェイス（1-3 ページ）

アクセス コントロール

アクセス コントロールはポリシーベースの機能で、ユーザはこれを使用してネットワークを横断できるトラフィックを指定、検査、および記録できます。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。

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、詳細な検査を行わずにすべてのトラフィックをブロックまたは信頼するように設定することも、侵入についてトラフィックを検査するように設定することもできます。

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にすることも複雑にすることもでき、複数の基準を使用してトラフィックを照合および検査します。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、およびユーザ別にトラフィックを制御できます。アクセス コントロールの詳細オプションには、前処理およびパフォーマンスが含まれます。

各アクセス コントロール ルールにはアクションも含まれており、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。

侵入検知および侵入防御

侵入検知および侵入防御は、トラフィックが宛先に許可される前のシステムの最後の防御ラインです。侵入ポリシーは、アクセス コントロール ポリシーによって呼び出される侵入検知および侵入防御の設定の定義済みセットです。侵入ルールおよびその他の設定を使用して、これらのポリシーはセキュリティ違反がないかトラフィックを検査し、インライン展開では、悪意のあるトラフィックをブロックまたは変更できます。

システムが提供するポリシーが組織のセキュリティのニーズに十分に対応していない場合は、カスタム ポリシーを作成することで、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。設定できるカスタム ポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

高度なマルウェア防御とファイル制御

マルウェアの影響を特定して軽減しやすくするため、ASA FirePOWER モジュールのファイル制御および高度なマルウェア防御の各コンポーネントによって、ネットワーク トラフィック内のファイル（アーカイブ ファイルの内のマルウェア ファイルとネストされたファイルを含む）の伝送を検出、追跡、キャプチャ、分析、および必要に応じてブロックできます。

ファイル制御

ファイル制御により、デバイスは、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。ファイル制御は、全体的なアクセス コントロール設定の一部として設定します。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 ポリシーによって、ルールの条件を満たすネットワーク トラフィックが検査されます。

ネットワークベースの高度なマルウェア防御（**AMP**）

ネットワークベースの高度なマルウェア防御（AMP）によって、複数のファイル タイプのマルウェアに関してネットワーク トラフィックを検査できます。

検出されたファイルは、保存済みかどうかに関係なく、ファイルの SHA-256 ハッシュ値を使用して単純な既知の性質の検索を行うために Collective Security Intelligence クラウド に送信できます。このコンテキスト情報を使用して、特定のファイルをブロックまたは許可するようにシステムを設定できます。

マルウェア防御は、総合的なアクセス コントロール設定の一部として設定することができます。アクセス コントロール ルールに関連付けられているファイル ポリシーは、ルール条件に一致するネットワーク トラフィックを検査します。

アプリケーション プログラミング インターフェイス

アプリケーション プログラミング インターフェイス（API）を使用してシステムと対話する方法がいくつか用意されています。詳細については、次のいずれかのサポート サイトから追加資料をダウンロードできます。

- シスコ：（http://www.cisco.com/cisco/web/support/index.html）

ライセンスの表記規則

項の先頭に記載されているライセンス文は、その項に記載されている機能を使用するのに必要なライセンスを示しています。具体的なライセンスは次のとおりです。

保護

保護 ライセンスでは、デバイスで侵入検知および侵入防御、ファイル制御、セキュリティ インテリジェンスのフィルタリングを実行することができます。

Control

Control ライセンスでは、デバイスでユーザおよびアプリケーションの制御を実行することができます。Control ライセンスには 保護 ライセンスが必要です。

URL フィルタリング（**URL Filtering**）

URL フィルタリング（URL Filtering）ライセンスでは、デバイスが定期的に更新されるクラウドベースのカテゴリおよびレピュテーション データを使用して、モニタ対象ホストが要求する URL に基づいて、ネットワークを通過できるトラフィックを決定できます。URL フィルタリング（URL Filtering）ライセンスには 保護 ライセンスが必要です。

マルウェア

マルウェア ライセンスでは、デバイスが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。つまり、ネットワーク上で転送されるファイルに含まれるマルウェアの検出、キャプチャ、およびブロックができます。また、ネットワーク上で転送されるファイルを追跡するトラジェクトリを表示することもできます。マルウェア ライセンスには 保護 ライセンスが必要です。

ライセンス付きの機能の多くは追加的であるため、このドキュメントでは、各機能で最も必要なライセンスについてのみ記載しています。たとえば、ある機能で 、保護 および Control のライセンスが必要な場合、Control のみが記載されています。ただし、追加的でないライセンスを機能が必要とする場合、マニュアルではそのライセンスをプラス（+）文字で示しています。

ライセンス文の「または」という語は、その項に記載されている機能を使用するには特定のライセンスが必要であるが、追加のライセンスで機能を追加できることを示しています。たとえば、あるファイル ポリシー内で、一部のファイル ルール アクションには 保護 ライセンスが必要であり、他のファイル ルール アクションには マルウェア ライセンスが必要であるとします。この場合、そのファイル ルールの説明のライセンス文には、「保護 または マルウェア」と示されます。

IP アドレスの表記規則

IPv4 Classless Inter-Domain Routing（CIDR）の表記、および IPv6 の類似のプレフィックス長の表記を使用して、ASA FirePOWER モジュールの多数の場所でアドレス ブロックを定義することができます。

CIDR 表記は、ネットワーク IP アドレスとビット マスクを組み合わせて使用し、指定されたアドレス ブロック内の IP アドレスを定義します。たとえば次の表に、プライベート IPv4 アドレス空間を CIDR 表記で示します。

表 1-1　CIDR 表記の構文例

CIDR ブロック	CIDR ブロックの IP アドレス	サブネット マスク	IP アドレスの数
10.0.0.0/8	10.0.0.0 ～ 10.255.255.255	255.0.0.0	16,777,216
172.16.0.0/12	172.16.0.0 ～ 172.31.255.255	255.240.0.0	1,048,576
192.168.0.0/16	192.168.0.0 ～ 192.168.255.255	255.255.0.0	65,536

同様に、IPv6 はネットワーク IP アドレスとプレフィックス長を組み合わせて使用し、指定されたブロック内の IP アドレスを定義します。たとえば 2001:db8::/32 は、プレフィックス長が 32 ビットの 2001:db8:: ネットワーク内の IPv6 アドレスを表します。つまり、2001:db8:: ～ 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff を表します。

CIDR またはプレフィックス長の表記を使用して IP アドレスのブロックを指定する場合、ASA FirePOWER モジュール は、マスクまたはプレフィックス長で指定されたネットワーク IP アドレスの部分のみを使用します。たとえば、10.1.2.3/8 と入力した場合、ASA FirePOWER モジュール では 10.0.0.0/8 が使用されます。

つまり シスコ は、CIDR またはプレフィックス長の表記を使用する場合に、ビット境界上でネットワーク IP アドレスを使用する標準の方法を推奨していますが、ASA FirePOWER モジュールではこれは必要ありません。

再利用可能なオブジェクトの管理

柔軟性を高めて、使用しやすくするために、ASA FirePOWER モジュール では、名前付きオブジェクトを作成できます。これは、名前を値と関連付ける再使用可能な設定であり、その値を使用したい場合に、代わりに名前付きオブジェクトを使用できるようにします。

次のタイプのオブジェクトを作成できます。

- IP アドレスおよびネットワーク、ポート/プロトコルのペア、セキュリティ ゾーン、および送信側/宛先の国（位置情報）を表す、ネットワークベースのオブジェクト
- セキュリティ インテリジェンス フィードおよびリスト、アプリケーション フィルタ、URL、ファイル リスト、および侵入ポリシーの変数セットを含む、トラフィックを処理するためのオブジェクト

アクセス コントロール 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侵入ルール、レポート、ダッシュボードなど、ASA FirePOWER モジュール のさまざまな場所でこれらのオブジェクトを使用できます。

オブジェクトをグループ化すると、複数のオブジェクトを 1 つの設定で参照できます。ネットワーク、ポート、および URL オブジェクトをグループ化できます。

（注） ほとんどの場合、ポリシーで使用されるオブジェクトを編集するには、変更を反映するためにポリシーの再適用が必要になります。セキュリティ ゾーンを編集する場合にも、適切なデバイスの設定を再適用する必要があります。

詳細については、次の項を参照してください。

- オブジェクト マネージャの使用（2-2 ページ）
- ネットワーク オブジェクトの操作（2-4 ページ）
- セキュリティ インテリジェンス リストとフィードの操作（2-4 ページ）
- ポート オブジェクトの操作（2-11 ページ）
- URL オブジェクトの操作（2-12 ページ）
- アプリケーション フィルタの操作（2-13 ページ）
- 変数セットの使用（2-15 ページ）
- シンクホール オブジェクトの使用（2-32 ページ）
- ファイル リストの操作（2-32 ページ）
- セキュリティ ゾーンの操作（2-37 ページ）
- 暗号スイート リストの操作（2-38 ページ）

- 識別名オブジェクトの操作（2-39 ページ）
- PKI オブジェクトの操作（2-41 ページ）
- 位置情報オブジェクトの操作（2-50 ページ）

オブジェクト マネージャの使用

ライセンス：任意

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、アプリケーション フィルタ、変数セット、およびセキュリティ ゾーンなどのオブジェクトを作成および管理します。ネットワーク、ポート、および URL オブジェクトをグループ化できます。さらに、オブジェクトおよびオブジェクト グループのリストをソート、フィルタ、および参照することもできます。

詳細については、以下を参照してください。

- オブジェクトのグループ化（2-2 ページ）
- オブジェクトの参照、ソート、およびフィルタ（2-3 ページ）

オブジェクトのグループ化

ライセンス：任意

ネットワーク、ポート、および URL のオブジェクトをグループ化できます。システムでは、オブジェクトおよびオブジェクト グループを交互に使用することができます。たとえば、ポート オブジェクトを使用する場合はいつでも、ポート オブジェクト グループも使用できます。同じタイプのオブジェクトおよびオブジェクト グループには、同じ名前を付けることはできません。

ポリシーで使用されるオブジェクト グループ（たとえば、アクセス コントロール ポリシーで使用されるネットワーク オブジェクト グループ）を編集する場合、変更を有効にするためにポリシーを再適用する必要があります。

グループを削除しても、グループ内のオブジェクトは削除されず、相互の関連性だけが削除されます。さらに、使用中のグループは削除できません。たとえば、保存されたアクセス コントロール ポリシーの URL 条件で使用している URL グループは削除できません。

再利用可能なオブジェクトをグループ化するには、次の手順を実行します。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ 2　グループ化するオブジェクト タイプ [ネットワーク（Network）]、[ポート（Port）]、または [URL] で、[オブジェクト グループ（Object Groups）] を選択します。

グループ化するオブジェクト タイプのページが表示されます。

ステップ 3　グループ化するオブジェクトに対応する [追加（Add）] ボタンをクリックします。

グループを作成するためのポップアップ ウィンドウが表示されます。

ステップ 4　グループの名前を入力します。中カッコ（{}）を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　1 つ以上のオブジェクトを選択し、[追加（Add）] をクリックします。

- 複数のオブジェクトを選択するには、Shift キーまたは Ctrl キーを使用するか、右クリックして [すべて選択（Select All）] を選択します。
- 含める既存のオブジェクトを検索するには、フィルタ フィールド（  ）を使用します。これは入力に従って更新され、一致する項目を表示します。検索ストリングをクリアするには、検索フィールドの上にある再ロード アイコン（  ）をクリックするか、検索フィールド内のクリア アイコン（  ）をクリックします。
- 既存のオブジェクトがニーズを満たさない場合、すぐにオブジェクトを作成するには、追加アイコン（  ）をクリックします。

ステップ 6　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

グループが作成されます。

オブジェクトの参照、ソート、およびフィルタ

ライセンス：任意

オブジェクト マネージャには、ページあたり 20 のオブジェクトまたはグループが表示されます。オブジェクトまたはグループのタイプが 20 を超える場合は、ページ下部のナビゲーション リンクを使用して追加ページを表示します。特定のページにアクセスしたり、更新アイコン（  ）にアクセスしてビューを更新したりすることもできます。

デフォルトでは、オブジェクトとグループはページで、アルファベット順に名前でリストされます。ただし、表示されている任意の列でオブジェクトまたはグループの各タイプをソートできます。列見出しの横にある上（  ）または下（）矢印は、ページがその列でその方向にソートされていることを示します。ページのオブジェクトは、名前または値でフィルタすることもできます。

オブジェクトまたはグループをソートする方法：

ステップ 1　列の見出しをクリックします。反対方向でソートするには、見出しを再度クリックします。

オブジェクトまたはグループをフィルタする方法：

ステップ 1　[フィルタ（Filter）] フィールドのフィルタ条件を入力します。

ページは入力に従って更新され、一致する項目が表示されます。フィールドは、ワイルドカードとして 1 つ以上のアスタリスク（*）を受け入れます。

ネットワーク オブジェクトの操作

ライセンス:任意

ネットワーク オブジェクトは、個別に、またはアドレス ブロックとして指定できる 1 つ以上の IP アドレスを表します。ネットワーク オブジェクトおよびグループ（オブジェクトのグループ化 (2-2 ページ) を参照）を、アクセス コントロール ポリシー、ネットワークの変数、侵入ルール、レポートなど、ASA FirePOWER モジュール のさまざまな場所で使用できます。

また、使用中のネットワーク オブジェクトは削除できません。さらに、アクセス コントロールまたは侵入ポリシーで使用されるネットワーク オブジェクトを編集した場合は、変更を有効にするためにポリシーを再適用する必要があります。

ネットワーク オブジェクトを作成する方法:

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ 2　[ネットワーク（Network）] で、[個々のオブジェクト（Individual Objects）] を選択します。

ステップ 3　[ネットワークの追加（Add Network）] をクリックします。

[ネットワーク オブジェクト（Network Objects）] ポップアップ ウィンドウが表示されます。

ステップ 4　[名前（Name）] にネットワーク オブジェクトの名前を入力します。中カッコ（{}）を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　ネットワーク オブジェクトに追加する IP アドレスまたはアドレス ブロックごとに、値を入力して [追加（Add）] をクリックします。

ステップ 6　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

ネットワーク オブジェクトが追加されます。

セキュリティ インテリジェンス リストとフィードの操作

ライセンス:Protection

セキュリティ インテリジェンス機能を使用すると、アクセス コントロール ポリシーごとに、送信元または宛先 IP アドレスに基づいてネットワークをトラバースできるトラフィックを指定できます。これは、トラフィックがアクセス コントロール ルールによって分析される前に、特定の IP アドレスをブラックリストに入れる（トラフィックの送受信を拒否する）場合に特に役立ちます。同様に、IP アドレスをホワイトリストに追加して、アクセス コントロールを使用してシステムに接続を強制的に処理させることができます。

特定の IP アドレスをブラックリストに入れるかどうか決めていない場合は、「モニタのみ」設定を使用できます。この場合、システムはアクセス コントロールを使用して接続を処理できますが、接続の一致はブラックリストに記録されます。

グローバル ホワイトリストおよびグローバル ブラックリストは、デフォルトですべてのアクセス コントロール ポリシーに含まれており、すべてのゾーンに適用されます。また、各アクセス コントロール ポリシー内で、ネットワーク オブジェクトとグループの組み合わせを使用して個別のホワイトリストおよびブラックリストや、セキュリティ インテリジェンスのリストとフィードを作成できます。ユーザはこれらすべてをセキュリティ ゾーン別に抑制することができます。

フィードとリストの比較

セキュリティ インテリジェンス フィードは、ユーザが設定した間隔でシステムが HTTP または HTTPS サーバからダウンロードする IP アドレスの動的コレクションです。フィードは定期的に更新されるため、システムは最新の情報を使用してネットワーク トラフィックをフィルタできます。ユーザがブラックリストを作成できるように、ASA FirePOWER モジュールは、悪いレピュテーションがあると VRT が判断した IP アドレスを表すインテリジェンス フィードを提供します。

フィードの更新が反映されるまで数分かかる場合がありますが、フィードの作成または変更後、またはスケジュールされたフィードの更新後に、アクセス コントロール ポリシーを再適用する必要はありません。

(注)　システムがインターネットからフィードをダウンロードするタイミングを厳密に制御する場合は、そのフィードの自動更新を無効にすることができます。ただし、シスコは自動更新の許可を推奨します。手動でオンデマンド更新を行うことはできますが、システムで定期的にフィードをダウンロードできるようにすれば、最新の関連データを入手できます。

フィードとは対照的に、セキュリティ インテリジェンスのリストはシステムに手動でアップロードする IP アドレスの簡単な静的リストです。フィードおよびグローバル ホワイトリストやブラックリストを増加および微調整するには、カスタム リストを使用します。カスタム リストの編集（ネットワーク オブジェクトの編集およびグローバル ホワイトリストまたはブラックリストからの IP アドレスの削除）を行う場合、変更を反映させるためにアクセス コントロール ポリシーを適用する必要があることに注意してください。

フィード データの書式設定や破損

フィードとリストのソースは、1 行につき 1 つの IP アドレスまたはアドレス ブロックを持つ、最大 500 MB の単純なテキスト ファイルでなければなりません。コメント行は # 文字で始める必要があります。リストのソース ファイルは .txt 拡張子を使用する必要があります。

システムが破損したフィードまたは認識不能な IP アドレスを持つフィードをダウンロードした場合、システムは古いフィード データを引き続き使用します（これが初回のダウンロードである場合を除く）。ただし、システムがフィード内の IP アドレスを 1 つでも認識できる場合、システムは認識できるアドレスで更新します。

インターネット アクセスとハイ アベイラビリティ

システムは、ポート 443/HTTPS を使用してインテリジェンス フィードをダウンロードし、443/HTTP または 80/HTTP を使用してカスタムまたはサードパーティのフィードをダウンロードします。フィードを更新するには、デバイスでインバウンドとアウトバウンドの両方の適切なポートを開く必要があります。フィード サイトに直接アクセスできない場合、システムはプロキシ サーバを使用できます。

(注)　システムはカスタム フィードのダウンロード時にピア SSL 証明書の検証を実行しません。また、システムは、証明書のバンドルまたは自己署名証明書を使用したリモート ピアの検証もサポートしていません。

フィードとリストの管理

セキュリティ インテリジェンスのリストとフィード（総称してセキュリティ インテリジェンス オブジェクトと呼ばれる）は、オブジェクト マネージャのセキュリティ インテリジェンス ページを使用して作成および管理します。（ネットワーク オブジェクトおよびグループの作成および管理の詳細については、ネットワーク オブジェクトの操作（2-4 ページ）を参照してください）。

保存または適用されているアクセス コントロール ポリシーで現在使用されているカスタム リストまたはフィードは削除できないことに注意してください。さらに、個別の IP アドレスは削除できますが、グローバル リストは削除できません。同様に、インテリジェンス フィードは削除できませんが、編集することによって更新の頻度を無効にしたり、変更したりできます。

セキュリティ インテリジェンス オブジェクトのクイック リファレンス

次の表に、セキュリティ インテリジェンスのフィルタリングを実行する場合に使用できるオブジェクトのクイック リファレンスを示します。

表 **2-1**　セキュリティ インテリジェンス オブジェクトの機能

機能	グローバル ホワイトリストまたはブラックリスト	インテリジェンス フィード	カスタム フィード	カスタム リスト	ネットワーク オブジェクト
使用方法	デフォルトで、アクセス コントロール ポリシーで	ホワイトリストまたはブラックリスト オブジェクトとして任意のアクセス コントロール ポリシーで			
セキュリティ ゾーンで制約することができるか	いいえ	はい	はい	はい	はい
削除できるか	いいえ	いいえ	はい（保存または適用されているアクセス コントロール ポリシーで現在使用されている場合を除く）		
オブジェクト マネージャの編集機能	IP アドレスのみを削除する	更新の頻度を無効にするか、変更する	完全に変更する	変更されたリストのみをアップロードする	完全に変更する
変更時にアクセス ポリシー コントロールの再適用が必要か	削除する場合は、はい（IP アドレスを追加する場合は、再適用する必要はありません）	いいえ	いいえ	はい	はい

セキュリティ インテリジェンスのリストおよびフィードの作成、管理、および使用の詳細については、以下を参照してください。

- グローバル ホワイトリストおよびブラックリストの操作（2-7 ページ）
- インテリジェンス フィードの操作（2-7 ページ）
- カスタム セキュリティ インテリジェンス フィードの操作（2-8 ページ）
- 手動によるセキュリティ インテリジェンス フィードの更新（2-9 ページ）
- カスタム セキュリティ インテリジェンスのリストの操作（2-9 ページ）
- 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）

グローバル ホワイトリストおよびブラックリストの操作

ライセンス：Protection

システムのグローバル ホワイトリストおよびブラックリストは、デフォルトですべてのアクセス コントロール ポリシーに含まれており、すべてのゾーンに適用されます。ポリシーのそれぞれについて、これらのグローバル リストを使用しないように選択することができます。

グローバル リストに IP アドレスを追加した後は、アクセス コントロール ポリシーを再適用する必要はありません。逆に、グローバル ホワイトリストまたはブラックリストから IP アドレスを削除した後は、変更を反映するためにアクセス コントロール ポリシーを適用する必要があります。

ネットマスク /0 のネットワーク オブジェクトはホワイトリストまたはブラックリストに追加できますが、ネットマスク `/0` を使用したアドレス ブロックは無視され、これらのアドレスに基づいたホワイトリストおよびブラックリスト フィルタリングは行われないことに注意してください。セキュリティ インテリジェンス フィードからのネットマスク `/0` のアドレス ブロックも無視されます。すべてのトラフィックをモニタまたはブロックする場合は、セキュリティ インテリジェンス フィルタリングの代わりに、[モニタ（Monitor）] または [ブロック（Block）] ルール アクションでアクセス コントロール ルールを使用し、[送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] のデフォルト値 **any** をそれぞれ使用します。

IP アドレスをグローバル ホワイトリストまたはブラックリストから削除する方法：

ステップ **1**　オブジェクト マネージャのセキュリティ インテリジェンス ページで、グローバル ホワイトリストまたはブラックリストの横にある編集アイコン（ ）をクリックします。

[グローバル ホワイトリスト（Global Whitelist）] または [グローバル ブラックリスト（Global Blacklist）] ポップアップ ウィンドウが表示されます。

ステップ **2**　リストから削除する IP アドレスの横にある削除アイコン（ ）をクリックします。

複数の IP アドレスを同時に削除するには、Shift キーおよび Ctrl キーを使用してそれらを選択し、右クリックして [削除（Delete）] を選択します。

ステップ **3**　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

変更は保存されますが、それを有効にするにはアクセス コントロール ポリシーを適用する必要があります。

インテリジェンス フィードの操作

ライセンス：Protection

ブラックリストを作成するのに役立つように、ASA FirePOWER モジュール は、悪いレピュテーションがあると VRT が判断した IP アドレスの定期的に更新されるいくつかのリストから成るインテリジェンス フィードを提供します。フィードの各リストは特定のカテゴリ（オープン リレー、既知の攻撃者、偽の IP アドレス（bogon）など）を表します。アクセス コントロール ポリシーでは、カテゴリのいずれかまたはすべてをブラックリストに登録できます。

インテリジェンス フィードは定期的に更新されるため、システムは最新の情報を使用してネットワーク トラフィックをフィルタできます。ただし、セキュリティに対する脅威（マルウェア、スパム、ボットネット、フィッシングなど）を表す不正な IP アドレスが現れては消えるペースが速すぎて、新しいポリシーを更新して適用するには間に合わないこともあります。

インテリジェンス フィードは削除できませんが、編集することによって更新の頻度を変更できます。デフォルトで、フィードは 2 時間ごとに更新されます。

インテリジェンス フィードの更新頻度を変更する方法:

ステップ 1　オブジェクト マネージャの [セキュリティ インテリジェンス（Security Intelligence）] ページで、インテリジェンス フィードの横にある編集アイコン（ ）をクリックします。

[セキュリティ インテリジェンス（Security Intelligence）] ポップアップ ウィンドウが表示されます。

ステップ 2　[更新頻度（Update Frequency）] を編集します。

2 時間から 1 週間までの範囲で、さまざまな間隔から選択できます。フィードの更新を無効にすることもできます。

ステップ 3　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

変更が保存されます。

カスタム セキュリティ インテリジェンス フィードの操作

ライセンス：Protection

カスタムまたはサードパーティのセキュリティ インテリジェンス フィードを使用すると、インターネット上で定期的に更新される他の信頼できるホワイトリストおよびブラックリストによって、インテリジェンス フィードを拡大することができます。内部フィードをセットアップすることもできます。

フィードを設定する場合は、URL を使用して場所を指定します。この URL は Punycode エンコードすることができません。デフォルトで、システムは、設定した間隔でフィード ソース全体をダウンロードします。

オプションで、md5 チェックサムを使用して、更新フィードをダウンロードするかどうか判断するようにシステムを設定できます。モジュールが最後にフィードをダウンロードした後にチェックサムが変更されていない場合、システムで再ダウンロードを行う必要はありません。特に内部フィードが大きい場合には、md5 チェックサムを使用することができます。md5 チェックサムは、チェックサムのみを含む単純なテキスト ファイルに保存する必要があります。コメントはサポートされていません。

セキュリティ インテリジェンス フィードを設定する方法:

ステップ 1　オブジェクト マネージャの [セキュリティ インテリジェンス（Security Intelligence）] ページで、[セキュリティ インテリジェンスの追加（Add Security Intelligence）] をクリックします。

[セキュリティ インテリジェンス（Security Intelligence）] ポップアップ ウィンドウが表示されます。

ステップ 2　[名前（Name）] にフィードの名前を入力します。中カッコ（{}）を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 3　[タイプ（Type）] ドロップダウン リストから、[フィード（Feed）] を設定することを指定します。

ポップアップ ウィンドウが新しいオプションで更新されます。

ステップ 4　[フィード URL（Feed URL）] を指定し、オプションで [MD5 URL] を指定します。

ステップ 5　[更新頻度（Update Frequency）] を選択します。

2 時間から 1 週間までの範囲で、さまざまな間隔から選択できます。フィードの更新を無効にすることもできます。

ステップ 6　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

セキュリティ インテリジェンス フィードのオブジェクトが作成されます。フィードの更新を無効にした場合を除き、システムはフィードをダウンロードして検証しようとします。これで、アクセス コントロール ポリシーでフィード オブジェクトを使用できるようになりました。

手動によるセキュリティ インテリジェンス フィードの更新

ライセンス：Protection

手動でセキュリティ インテリジェンス フィードを更新すると、インテリジェンス フィードを含め、すべてのフィードが更新されます。

すべてのセキュリティ インテリジェンス フィードを更新する方法：

ステップ 1　オブジェクト マネージャの [セキュリティ インテリジェンス（Security Intelligence）] ページで、[フィードの更新（Update Feeds）] をクリックします。

ステップ 2　すべてのフィードを更新することを確認します。

更新が有効になるまで数分かかる場合があることを警告する確認ダイアログが表示されます。

ステップ 3　[OK] をクリックします。

フィードの更新をダウンロードして検証した後、システムは更新されたフィードを使用してトラフィックのフィルタリングを開始します。

カスタム セキュリティ インテリジェンスのリストの操作

ライセンス：Protection

セキュリティ インテリジェンスのリストは、手動でアップロードする IP アドレスおよびアドレス ブロックのシンプルな静的リストです。カスタム リストは、フィードやグローバル リストの 1 つを増やしたり、微調整したりする場合に役立ちます。

アドレス ブロックのネットマスクは、IPv4 および IPv6 の場合、それぞれ 0 から 32、または 0 から 128 までの整数になることに注意してください。

たとえば、信頼できるフィードが重要なリソースへのアクセスを誤ってブロックしているものの、このフィードが全体的に組織にとって有用である場合、セキュリティ インテリジェンス フィード オブジェクトをアクセス コントロール ポリシーのブラックリストから削除する代わりに、誤って分類された IP アドレスだけが含まれるカスタム ホワイトリストを作成できます。

セキュリティ インテリジェンスのリストを変更するには、ソース ファイルを変更して、新しいコピーをアップロードする必要があることに注意してください。詳細については、セキュリティ インテリジェンス リストの更新（2-10 ページ）を参照してください。

新しいセキュリティ インテリジェンス リストをアップロードするには、次の手順を実行します。

ステップ 1　オブジェクト マネージャの [セキュリティ インテリジェンス（Security Intelligence）] ページで、[セキュリティ インテリジェンスの追加（Add Security Intelligence）] をクリックします。

[セキュリティ インテリジェンス（Security Intelligence）] ポップアップ ウィンドウが表示されます。

ステップ 2　[名前(Name)] にリストの名前を入力します。中カッコ({})を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 3　[タイプ(Type)] ドロップダウンリストから、[リスト(List)] をアップロードすることを指定します。

ポップアップ ウィンドウが新しいオプションで更新されます。

ステップ 4　[参照(Browse)] をクリックしてリストの .txt ファイルを位置指定し、[アップロード(Upload)] をクリックします。

リストがアップロードされます。ポップアップ ウィンドウに、システムがリスト内で検出した IP アドレスとアドレス ブロックの総数が表示されます。

番号が予期したものでない場合は、ファイルの書式設定を調べ、再試行してください。

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

セキュリティ インテリジェンス リストのオブジェクトが保存されます。これで、アクセス コントロール ポリシーでリスト オブジェクトを使用できるようになりました。

セキュリティ インテリジェンス リストの更新

ライセンス:Protection

セキュリティ インテリジェンス リストを編集するには、ソース ファイルを変更して、新しいコピーをアップロードする必要があります。ASDM を使用してファイルの内容を変更することはできません。ソース ファイルへのアクセス権がない場合は、ASDM インターフェイスを使用してコピーをダウンロードできます。

セキュリティ インテリジェンス リストを変更する方法:

ステップ 1　オブジェクト マネージャの [セキュリティ インテリジェンス(Security Intelligence)] ページで、更新するリストの横にある編集アイコン( )をクリックします。

[セキュリティ インテリジェンス(Security Intelligence)] ポップアップ ウィンドウが表示されます。

ステップ 2　編集するリストのコピーが必要な場合は、[ダウンロード(Download)] をクリックして、プロンプトに従ってリストをテキスト ファイルとして保存します。

ステップ 3　必要に応じてリストを変更します。

ステップ 4　[セキュリティ インテリジェンス(Security Intelligence)] ポップアップ ウィンドウで、[参照(Browse)] をクリックして、変更されたリストを参照し、[アップロード(Upload)] をクリックします。

リストがアップロードされます。

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

変更が保存されます。アクティブなアクセス コントロール ポリシーでリストが使用されている場合、変更を有効にするにはポリシーを適用する必要があります。

ポート オブジェクトの操作

ライセンス:任意

ポート オブジェクトは、異なるプロトコルをそれぞれ少し異なる方法で表します。

- TCP および UDP の場合、ポート オブジェクトは、カッコ内にプロトコル番号が記載されたトランスポート層プロトコルと、オプションの関連ポートまたはポート範囲を表します。例:`TCP(6)/22`。
- ICMP および ICMPv6(IPv6 ICMP)の場合、ポート オブジェクトは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を表します。例:`ICMP(1):3:3`
- ポート オブジェクトは、ポートを使用しない他のプロトコルを表すこともできます。

システムが既知のポート用にデフォルトのポート オブジェクトを提供することに注意してください。これらのオブジェクトは変更または削除できますが、シスコは代わりにカスタム ポート オブジェクトを作成することを推奨します。

ポート オブジェクトおよびグループ(オブジェクトのグループ化(2-2 ページ)を参照)を、アクセス コントロール ポリシーおよびポート変数、およびイベント検索など、ASA FirePOWER モジュール のさまざまな場所で使用できます。

使用中のポート オブジェクトは削除できません。さらに、アクセス コントロール ポリシーで使用されるポート オブジェクトを編集した場合は、変更を有効にするために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 ルールの送信元ポートの条件には TCP/UDP 以外のプロトコルを追加できないことに注意してください。さらに、送信元ポートと宛先ポートの両方のポート条件をルールで設定する場合、トランスポート プロトコルを混在させることはできません。

送信元ポートの条件で使用されるポート オブジェクト グループにサポート対象外のプロトコルを追加した場合、使用されるルールはポリシー適用時に適用されません。さらに、TCP と UDP の両方のポートを含むポート オブジェクトを作成してから、ルールの送信元ポートの条件としてそのポート オブジェクトを追加した場合、宛先ポートを追加することはできません。その逆もまた同様です。

ポート オブジェクトを作成する方法:

ステップ **1**　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [オブジェクト管理(Object Management)] の順に選択します。

[オブジェクト管理(Object Management)] ページが表示されます。

ステップ **2**　[ポート(Port)] で、[個々のオブジェクト(Individual Objects)] を選択します。

ステップ **3**　[ポートの追加(Add Port)] をクリックします。

[ポート オブジェクト(Port Objects)] ポップアップ ウィンドウが表示されます。

ステップ **4**　[名前(Name)] にポート オブジェクトの名前を入力します。中カッコ({})を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ **5**　[プロトコル(Protocol)] を選択します。

[TCP]、[UDP]、[IP]、[ICMP]、または [IPv6-ICMP] から選択するか、[その他(Other)] ドロップダウンリストを使用して別のプロトコルまたは [すべて(All)] プロトコルを選択できます。

ステップ **6**　オプションで、[ポート(Port)] またはポート範囲を使用して TCP または UDP ポート オブジェクトを制限します。

1 ～ 65535 までの任意のポートを指定するか、すべてのポートと一致するように `any` を指定できます。ポートの範囲を指定するには、ハイフンを使用します。

ステップ 7　オプションで、[タイプ（Type）] および、該当する場合は関連する [コード（Code）] を使用して、ICMP または IPV6-ICMP ポート オブジェクトを制限します。

ICMP または IPv6-ICMP オブジェクトを作成する場合、タイプ、および該当する場合はコードを指定できます。ICMP の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 [英語] および http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml [英語] を参照してください。任意のタイプと一致するようにタイプに any を設定するか、指定したタイプの任意のコードと一致するようにコードに any を設定できます。

ステップ 8　オプションで、[その他（Other）] を選択し、ドロップダウン リストからプロトコルを選択します。[すべて（All）] プロトコルを選択した場合は、[ポート（Port）] フィールドにポート番号を入力します。

ステップ 9　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

ポート オブジェクトが追加されます。

URL オブジェクトの操作

ライセンス：任意

設定した各 URL オブジェクトは、単一の URL または IP アドレスを表します。URL オブジェクトおよびグループ（オブジェクトのグループ化（2-2 ページ） を参照）を、アクセス コントロール ポリシーで使用できます。たとえば、特定の URL をブロックするアクセス コントロール ルールを作成することもできます。

HTTPS トラフィックをブロックするには、トラフィックの Secure Sockets Layer（SSL）証明書から URL を入力できることに注意してください。証明書から URL を入力する場合は、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` の代わりに `example.com` と入力します。）証明書の URL に基づいてトラフィックをブロックする場合、その Web サイトへの HTTP トラフィックと HTTPS トラフィックの両方がブロックされます。

使用中の URL オブジェクトは削除できません。さらに、アクセス コントロール ポリシーで使用される URL オブジェクトを編集した場合は、変更を有効にするためにポリシーを再適用する必要があります。

URL オブジェクトを追加する方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ 2　[URL] で、[個々のオブジェクト（Individual Objects）] を選択します。

ステップ 3　[URL の追加（Add URL）] をクリックします。

[URL オブジェクト（URL Objects）] ポップアップ ウィンドウが表示されます。

ステップ 4　[名前（Name）] に URL オブジェクトの名前を入力します。中カッコ（{}）を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　URL オブジェクトの [URL] または IP アドレスを入力します。

ステップ 6　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

URL オブジェクトが追加されます。

アプリケーション フィルタの操作

ライセンス:任意

ASA FirePOWER モジュールは IP トラフィックを分析するときに、ネットワーク上でよく使用されているアプリケーションを特定しようとします。アプリケーション認識は、アプリケーション ベースのアクセス コントロールを行うために不可欠です。システムは多くのアプリケーションに対応するディテクタとともに配布されており、シスコは頻繁に更新を提供し、システムおよび脆弱性データベース(VDB)の更新を通じてディテクタをさらに追加します。

アプリケーション フィルタは、アプリケーションのリスク、ビジネスとの関連性、タイプ、カテゴリ、およびタグに関連付けられている条件に従ってアプリケーションをグループ化します。アプリケーション フィルタを使用すると、アプリケーションを個別に検索および追加する必要がないため、アクセス コントロール ルール用のアプリケーション条件を素早く作成できます。詳細については、トラフィックとアプリケーション フィルタの一致(8-3 ページ)を参照してください。

アプリケーション フィルタを使用する別の利点は、新しいアプリケーションを変更または追加する場合にフィルタを使用するアクセス コントロール ルールを更新する必要がないことです。たとえば、すべてのソーシャル ネットワーキング アプリケーションをブロックするようにアクセス コントロール ポリシーを設定し、VDB の更新に新しいソーシャル ネットワーキング アプリケーション ディテクタが含まれる場合、ポリシーは VDB の更新時に更新されます。システムが新しいアプリケーションをブロックする前にポリシーを再適用する必要がありますが、アプリケーションをブロックするアクセス コントロール ルールを更新する必要はありません。

シスコ 提供のアプリケーション フィルタがユーザのニーズに応じてアプリケーションをグループ化しない場合、独自のフィルタを作成することができます。ユーザ定義フィルタでは、ASA FirePOWER モジュール 提供のフィルタをグループ化して結合できます。たとえば、非常にリスクが高く、ビジネス関連性が低いアプリケーションをすべてブロックするフィルタを作成することができます。個々のアプリケーションを手動で指定することによってもフィルタを作成できますが、これらのフィルタは、モジュール ソフトウェアまたは VDB を更新しても自動的に更新されないことを覚えておいてください。

ASA FirePOWER モジュール 提供のアプリケーション フィルタと同様、ユーザ定義のアプリケーション フィルタもアクセス コントロール ルールで使用できます。

アプリケーション フィルタを作成および管理する場合は、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)])を使用します。アプリケーションの条件をアクセス コントロール ルールに追加しながら、アプリケーション フィルタをすぐに作成できることに注意してください。

[アプリケーション フィルタ(Application Filters)] リストには、独自のフィルタを作成するために選択できる ASA FirePOWER モジュール 提供のアプリケーション フィルタが含まれています。表示されるフィルタは検索文字列を使用することによって抑制できます。これは、カテゴリとタグの場合に特に役立ちます。

[使用可能なアプリケーション(Available Applications)] リストには、選択したフィルタ内の個別のアプリケーションが含まれます。また、検索ストリングを使用して、表示されるアプリケーションを抑制することもできます。

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。中リスク フィルタに 100 のアプリケーションが含まれており、高リスク フィルタに 50 のアプリケーションが含まれているシナリオについて考えてみてください。両方のフィルタを選択すると、システムは使用可能な 150 のアプリケーションを表示します。

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、中リスクおよび高リスクのフィルタと中レベルおよび高レベルのビジネス関連性のフィルタを選択した場合、システムは、中リスクまたは高リスクで、かつ中レベルおよび高レベルのビジネス関連性があるアプリケーションを表示します。

ヒント　関連するアプリケーションについての詳細は情報アイコン( )をクリックします。詳細情報を表示するには、表示されるポップアップでインターネット検索リンクのいずれかをクリックします。

フィルタに追加するアプリケーションを決定したら、それらを個別に追加するか、アプリケーション フィルタを選択した場合は、[フィルタに一致するすべてのアプリケーション(All apps matching the filter)] を追加することができます。[選択済みのアプリケーションとフィルタ(Selected Applications and Filters)] リストにあるアイテムの合計数が 50 を超えない限り、複数のフィルタおよび複数のアプリケーションを任意の組み合わせで追加できます。

アプリケーション フィルタを作成すると、オブジェクト マネージャの [アプリケーション フィルタ(Application Filters)] ページにリストされます。このページには、各フィルタを構成する条件の合計数が表示されます。

表示されるアプリケーション フィルタのソートとフィルタの詳細については、オブジェクト マネージャの使用(2-2 ページ)を参照してください。使用中のアプリケーション フィルタは削除できないことに注意してください。さらに、アクセス コントロール ポリシーで使用されるアプリケーション フィルタを編集した場合は、変更を有効にするためにポリシーを再適用する必要があります。

アプリケーション フィルタを作成する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [オブジェクト管理(Object Management)] の順に選択します。

[オブジェクト管理(Object Management)] ページが表示されます。

ステップ 2　[アプリケーション フィルタ(Application Filters)] をクリックします。

[アプリケーション フィルタ(Application Filters)] セクションが表示されます。

ステップ 3　[アプリケーション フィルタの追加(Add Application Filter)] をクリックします。

[アプリケーション フィルタ(Application Filter)] ポップアップ ウィンドウが表示されます。

ステップ 4　[名前(Name)] にフィルタの名前を指定します。中カッコ({})を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　オプションで、[アプリケーション フィルタ(Application Filters)] リストにある ASA FirePOWER モジュール 提供のフィルタを使用して、フィルタに追加するアプリケーションのリストを絞り込みます。

- リストを展開および縮小するには、各フィルタ タイプの横にある矢印をクリックします。
- フィルタ タイプを右クリックし、[すべて選択(Check All)] または [すべて選択解除(Uncheck All)] をクリックします。このリストには、各タイプで選択したフィルタ数が示されることに注意してください。
- 表示されるフィルタを絞り込むには、[名前で検索(Search by name)] フィールドに検索文字列を入力します。これは、カテゴリとタグの場合に特に有効です。検索をクリアするには、クリア アイコン( )をクリックします。
- フィルタのリストを更新し、選択したフィルタをすべてクリアするには、リロード アイコン( )をクリックします。
- すべてのフィルタと検索フィールドをクリアするには、[すべてのフィルタをクリア(Clear All Filters)] をクリックします。

選択したフィルタに一致するアプリケーションが [使用可能なアプリケーション(Available Applications)] リストに表示されます。リストには一度に 100 のアプリケーションが表示されます。

ステップ 6　[使用可能なアプリケーション（Available Applications）] リストから、フィルタに追加するアプリケーションを選択します。

- 前の手順で指定した制約を満たすすべてのアプリケーションを追加するには、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] を選択します。
- 表示される個別のアプリケーションを絞り込むには、[名前で検索（Search by name）] フィールドに検索文字列を入力します。検索をクリアするには、クリア アイコン（ ）をクリックします。
- 使用可能な個別のアプリケーションのリストを参照するには、リストの下部にあるページング アイコンを使用します。
- 複数の個別オブジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。現在表示されている個別のアプリケーションを選択するには、右クリックして [すべて選択（Select All）] を選択します。
- アプリケーションのリストを更新し、選択したアプリケーションをすべてクリアするには、リロード アイコン（ ）をクリックします。

個別のアプリケーションと [フィルタに一致するすべてのアプリケーション（All apps matching the filter）] は同時に選択できません。

ステップ 7　選択したアプリケーションをフィルタに追加します。クリックしてドラッグするか、[ルールに追加（Add to Rule）] をクリックできます。

結果は次のもので構成されています。

- 選択したアプリケーション フィルタ
- 選択した個別の使用可能なアプリケーション、または [フィルタに一致するすべてのアプリケーション（All apps matching the filter）]

フィルタには最大 50 のアプリケーションおよびフィルタを追加できます。選択したアプリケーションからアプリケーションまたはフィルタを削除するには、該当する削除アイコン（ ）をクリックします。1 つ以上のアプリケーションおよびフィルタを選択するか、または右クリックして [すべて選択（Select All）] を選択してから、右クリックして [選択対象を削除（Delete Selected）] を選択することもできます。

ステップ 8　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

アプリケーション フィルタが保存されます。

変数セットの使用

ライセンス：Protection

変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制、適応プロファイル、および動的ルール状態にある IP アドレスを表すこともできます。

ヒント　プリプロセッサ ルールは、侵入ルールで使用されるネットワーク変数で定義されたホストにかかわらず、イベントをトリガーできます。

変数セットを使用して、変数を管理、カスタマイズ、およびグループ化します。ASA FirePOWER モジュール 提供のデフォルトの変数セットを使用するか、独自のカスタム セットを作成することができます。どのセットでも、定義済みのデフォルトの変数を変更し、ユーザ定義の変数を追加および変更することができます。

ほとんどの 共有オブジェクトのルール、および ASA FirePOWER モジュールが提供する 標準テキスト ルール は、定義済みのデフォルト変数を使用して、ネットワークおよびポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 $HOME_NET を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 $EXTERNAL_NET を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Web サーバに対するエクスプロイトを検出するルールは、$HTTP_SERVERS 変数および $HTTP_PORTS 変数を使用します。

ルールがより効率的なのは、変数がユーザのネットワーク環境をより正確に反映する場合です。少なくとも、定義済みのデフォルトの変数の最適化（2-16 ページ）で説明されているように、デフォルトのセットにあるデフォルトの変数を変更する必要があります。$HOME_NET などの変数がネットワークを正しく定義し、$HTTP_SERVERS にネットワーク上のすべての Web サーバが含まれていれば、処理は最適化され、疑わしいアクティビティがないかどうかすべての関連システムがモニタされます。

変数を使用するには、変数セットをアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに関連付けられている侵入ポリシーにリンクします。デフォルトでは、デフォルトの変数セットは、アクセス コントロール ポリシーによって使用されるすべての侵入ポリシーにリンクされています。

詳細については、次の各項を参照してください。

- 定義済みのデフォルトの変数の最適化（2-16 ページ）
- 変数セットについて（2-19 ページ）
- 変数セットの管理（2-20 ページ）
- 変数の管理（2-22 ページ）
- 変数の追加および編集（2-23 ページ）
- 変数のリセット（2-30 ページ）
- 変数セットを侵入ポリシーにリンクさせる（2-31 ページ）
- 拡張変数について（2-31 ページ）

定義済みのデフォルトの変数の最適化

ライセンス：Protection

ASA FirePOWER モジュールはデフォルトで、定義済みのデフォルト変数で構成される単一のデフォルトの変数セットを提供します。脆弱性調査チーム（VRT）はルールの更新を使用して、デフォルト変数を含む、新規および更新された侵入ルール、および他の侵入ポリシー要素を提供します。詳細については、ルールの更新とローカル ルール ファイルのインポート（43-10 ページ）を参照してください。

ASA FirePOWER モジュール で提供される多くの侵入ルールは定義済みのデフォルト変数を使用するため、これらの変数に対して適切な値を設定する必要があります。変数セットを使用してネットワーク上のトラフィックを特定する方法によっては、任意またはすべての変数セットにあるこれらのデフォルト変数の値を変更することができます。詳細については、変数の追加および編集（2-23 ページ）を参照してください。

注意　アクセス コントロールまたは侵入ポリシーをインポートすると、デフォルトの変数セットにある既存のデフォルト変数が、インポートされたデフォルト変数でオーバーライドされます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。詳細については、設定のインポート（B-3 ページ）を参照してください。

以下の表は、ASA FirePOWER モジュール で提供される変数について説明し、ユーザが通常変更する変数を示します。変数をご使用のネットワークに合わせて調整する方法を決定するには、プロフェッショナル サービスまたはサポートに問い合わせてください。

表 **2-2**　***ASA FirePower*** モジュールによって提供される変数

変数名	説明	変更しますか
$AIM_SERVERS	既知の AOL Instant Messenger（AIM）サーバを定義し、チャットベースのルールおよび AIM エクスプロイトを検索するルールで使用されます。	不要。
$DNS_SERVERS	ドメイン ネーム サービス（DNS）サーバを定義します。DNS サーバに特に影響するルールを作成する場合、$DNS_SERVERS 変数を宛先または送信元 IP アドレスとして使用できます。	現在のルール セットでは不要です。
$EXTERNAL_NET	保護されていないネットワークとして ASA FirePOWER モジュールが表示するネットワークを定義し、外部ネットワークを定義するために多くのルールで使用されます。	はい。$HOME_NET を適切に定義してから、$EXTERNAL_NET の値として $HOME_NET を除外する必要があります。
$FILE_DATA_PORTS	ネットワーク ストリームでファイルを検出する侵入ルールで使用される、暗号化されていないポートを定義します。	不要。
$FTP_PORTS	ネットワーク上の FTP サーバのポートを定義し、FTP サーバのエクスプロイト ルールに使用されます。	FTP サーバがデフォルト ポート以外のポートを使用する場合は変更します（モジュール インターフェイスでデフォルト ポートを確認できます）。
$GTP_PORTS	パケット デコーダが GTP（General Packet Radio Service（GPRS）トンネリング プロトコル）PDU 内部でペイロードを取得するデータ チャネル ポートを定義します。	不要。
$HOME_NET	関連した侵入ポリシーがモニタするネットワークを定義し、内部ネットワークを定義するために多くのルールで使用されます。	内部ネットワークの IP アドレスを指定する場合は変更します。
$HTTP_PORTS	ネットワーク上の Web サーバのポートを定義し、Web サーバのエクスプロイト ルールに使用されます。	Web サーバがデフォルト ポート以外のポートを使用する場合は変更します（モジュール インターフェイスでデフォルト ポートを確認できます）。
$HTTP_SERVERS	ネットワーク上の Web サーバを定義します。Web サーバのエクスプロイト ルールで使用されます。	HTTP サーバを実行する場合は変更します。
$ORACLE_PORTS	ネットワーク上で Oracle データベース サーバのポートを定義し、Oracle データベースでの攻撃をスキャンするルールで使用されます。	Oracle サーバを実行する場合は変更します。

表 2-2　*ASA FirePower* モジュールによって提供される変数（続き）

変数名	説明	変更しますか
$SHELLCODE_PORTS	システムにシェル コードのエクスプロイトをスキャンさせるポートを定義し、シェル コードを使用するエクスプロイトを検出するルールで使用されます。	不要。
$SIP_PORTS	ネットワーク上の SIP サーバのポートを定義し、SIP のエクスプロイト ルールに使用されます。	不要。
$SIP_SERVERS	ネットワーク上で SIP サーバを定義し、SIP をターゲットとしたエクスプロイトを解決するルールで使用されます。	はい。SIP サーバを実行している場合は、$HOME_NET を適切に定義してから、$SIP_SERVERS の値として $HOME_NET を含める必要があります。
$SMTP_SERVERS	ネットワーク上で SMTP サーバを定義し、メール サーバをターゲットとするエクスプロイトを解決するルールで使用されます。	SMTP サーバを実行する場合は変更します。
$SNMP_SERVERS	ネットワーク上で SNMP サーバを定義し、SNMP サーバでの攻撃をスキャンするルールで使用されます。	SNMP サーバを実行する場合は変更します。
$SNORT_BPF	システム上のバージョン 5.3.0 より前の ASA FirePOWER モジュール ソフトウェア リリースに存在し、その後バージョン 5.3.0 以上にアップグレードされた場合にのみ表示されるレガシー拡張変数を識別します。拡張変数について（2-31 ページ）を参照してください。	変更しません。この変数は表示または削除のみが可能です。削除後に、編集または復元することはできません。
$SQL_SERVERS	ネットワーク上でデータベース サーバを定義し、データベースをターゲットとしたエクスプロイトを解決するルールで使用されます。	SQL サーバを実行する場合は変更します。
$SSH_PORTS	ネットワーク上の SSH サーバのポートを定義し、SSH サーバのエクスプロイト ルールに使用されます。	SSH サーバがデフォルト ポート以外のポートを使用する場合は変更します（モジュール インターフェイスでデフォルト ポートを確認できます）。
$SSH_SERVERS	ネットワーク上で SSH サーバを定義し、SSH をターゲットとしたエクスプロイトを解決するルールで使用されます。	はい。SSH サーバを実行している場合は、$HOME_NET を適切に定義してから、$SSH_SERVERS の値として $HOME_NET を含める必要があります。
$TELNET_SERVERS	ネットワーク上で既知の Telnet サーバを定義し、Telnet サーバをターゲットとしたエクスプロイトを解決するルールで使用されます。	Telnet サーバを実行する場合は変更します。
$USER_CONF	本来はモジュール インターフェイスを介して使用できない 1 つ以上の機能を設定できる一般ツールを提供します。拡張変数について（2-31 ページ）を参照してください。 ⚠ 注意　$USER_CONF の設定が競合または重複していると、システムは停止します。拡張変数について（2-31 ページ）を参照してください。	機能の説明で指示されている場合や、サポートによる指示があった場合を除き、変更しません。

変数セットについて

ライセンス:Protection

変数を任意のセットに追加すると、それはすべてのセットに追加されます。つまり、各変数セットは、システムで現在設定されているすべての変数のコレクションになります。どの変数セットでも、ユーザ定義の変数を追加し、任意の変数の値をカスタマイズすることができます。

ASA FirePOWER モジュールは初めに、定義済みのデフォルト値で構成される単一のデフォルトの変数セットを提供します。デフォルト設定では、各変数は最初にはそのデフォルト値に設定されています。定義済みの変数の場合、このデフォルト値は VRT によって設定され、ルール更新で提供される値です。

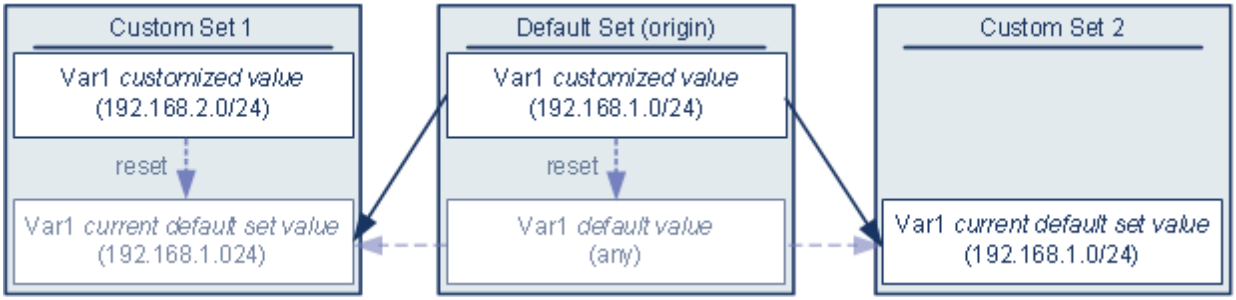
定義済みのデフォルト変数は、デフォルト値のままにすることもできますが、シスコは定義済みのデフォルトの変数の最適化（2-16 ページ）で説明されているように、定義済みの変数のサブセットを変更することを推奨します。

変数はデフォルト セットでのみ使用できますが、多くの場合、1 つ以上のカスタム設定を追加し、異なるセットで異なる変数の値を設定し、場合によっては新しい変数を追加することによって、最大限に活用できます。

複数のセットを使用する場合は、デフォルトのセットにある任意の変数の現在値によって、他のすべてのセットの変数のデフォルト値が決まることに注意してください。

例:デフォルト セットにユーザ定義変数を追加する

次の図は、値が `192.168.1.0/24` のデフォルト セットにユーザ定義の変数 `Var1` を追加した場合のセットのインタラクションを示しています。



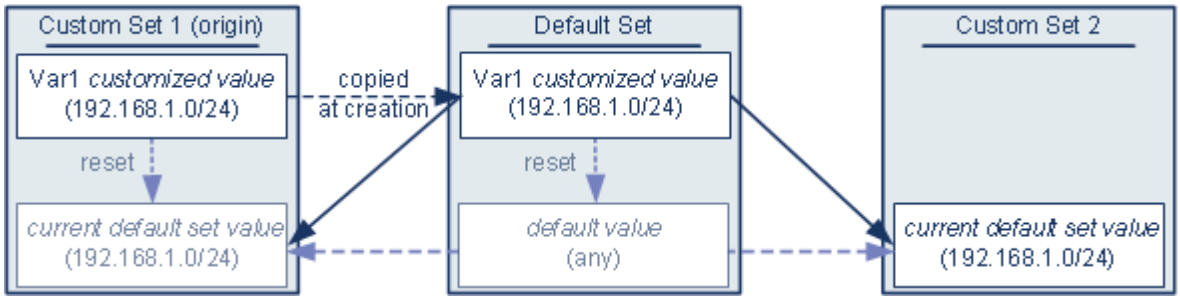
オプションで、任意のセットの `Var1` 値をカスタマイズできます。`Var1` がカスタマイズされていない Custom Set 2 では、この値は `192.168.1.0/24` です。Custom Set 1 では、`Var1` のカスタマイズ値 `192.168.2.0/24` はデフォルト値をオーバーライドします。デフォルト設定では、ユーザ定義変数をリセットすると、すべてのセットのデフォルト値が `any` にリセットされます。

この例では、Custom Set 2 で `Var1` を更新しなかった場合、デフォルト セットで `Var1` をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 `Var1` が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

この例では示されていませんが、セット間のインタラクションは、デフォルトのセットのデフォルト変数をリセットすると現在のルールの更新でシステムによって設定された値にリセットされること以外は、ユーザ定義変数およびデフォルト変数で同じであることに注意してください。

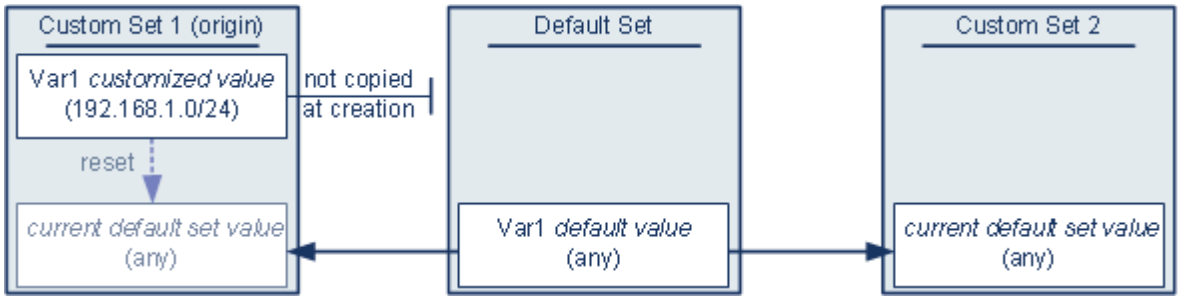
例：カスタム セットにユーザ定義変数を追加する

次の 2 つの例は、カスタム セットにユーザ定義変数を追加した場合の変数セットのインタラクションについて示しています。新しい変数を保存すると、設定値を他のセットのデフォルト値として使用するかどうかを尋ねるプロンプトが出されます。次の例では、設定値を使用するという選択がなされています。



Custom Set 1 からの Var1 の発信元を除き、この例は Var1 をデフォルト セットに追加した上述の例と同じであることに注意してください。Var1 のカスタマイズ値 192.168.1.0/24 を Custom Set 1 に追加すると、値はデフォルト値 any を持つカスタマイズ値としてデフォルト セットにコピーされます。その後、Var1 の値とインタラクションは、Var1 をデフォルト セットに追加した場合と同じになります。前述の例と同様、デフォルト セットで Var1 をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 Var1 が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

次の例では、前述の例にあるように値が 192.168.1.0/24 の Var1 を Custom Set 1 に追加しますが、Var1 の設定値を他のセットのデフォルト値として使用しないことを選択します。



このアプローチでは、Var1 をデフォルト値 any を持つすべてのセットに追加します。Var1 を追加したら、任意のセットでその値をカスタマイズできます。このアプローチの利点は、デフォルト セットで Var1 を最初にカスタマイズしないことによって、デフォルト セットの値をカスタマイズし、Var1 をカスタマイズしていない Custom Set 2 などのセット内の現在の値を意図せずに変更してしまうリスクが軽減されます。

変数セットの管理

ライセンス：Protection

[オブジェクト マネージャ（Object Manager）] ページ（[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）]）で [変数セット（Variable Sets）] を選択した場合、オブジェクト マネージャは、デフォルトの変数セットとユーザが作成したカスタム セットをリストします。

新しくインストールされたシステムで、デフォルトの変数セットは、ASA FirePOWER モジュールで定義済みのデフォルト変数だけで構成されます。

各変数セットには、シスコによって提供されるデフォルト変数と、任意の変数セットから追加したすべてのカスタム変数が含まれます。デフォルト設定は編集できますが、デフォルト セットの名前を変更したり、削除したりすることはできないことに注意してください。

次の表に、変数セットを管理するために実行できるアクションを要約します。

表 **2-3**　変数セットの管理アクション

目的	操作
変数セットを表示する	[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] を選択し、[変数セット（Variable Set）] を選択します。
変数セットを名前でフィルタする	名前の入力を開始します。入力するにつれて、ページが更新され、一致する名前が表示されます。
名前のフィルタリングをクリアする	フィルタ フィールドのクリア アイコン（ ）をクリックします。
カスタム変数セットを追加する	[変数セットの追加（Add Variable Set）] をクリックします。 便宜を図るため、新しい変数セットには、現在定義されているすべてのデフォルト変数とカスタマイズ変数が含まれます。
変数セットを編集する	編集する変数セットの横にある編集アイコン（ ）をクリックします。 ヒント　変数セットの行内で右クリックし、[編集（Edit）] を選択することもできます。
カスタム変数セットを削除する	変数セットの横にある削除アイコン（ ）をクリックしてから、[はい（Yes）] をクリックします。デフォルトの変数セットは削除できません。削除する変数セットで作成された変数は、他のセットで削除されたり他の方法で影響を受けたりしないことに注意してください。 ヒント　変数セットの行内で右クリックし、[削除（Delete）] を選択してから、[はい（Yes）] をクリックすることもできます。複数のセットを選択するには、Ctrl キーと Shift キーを使用します。

変数セットを設定した後、それらを侵入ポリシーにリンクできます。

変数セットを編集または作成する方法:

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ **2**　[変数セット（Variable Set）] を選択します。

ステップ **3**　変数セットを追加したり、既存のセットを編集したりするには、次の手順に従います。

- 変数セットを追加するには、[変数セットの追加（Add Variable Set）] をクリックします。
- 変数セットを編集するには、変数セットの横にある編集アイコン（ ）をクリックします。

新規の変数セット ページ、または変数セットの編集ページが表示されます。変数セット内の変数を追加および編集する方法の詳細については、変数の追加および編集（2-23 ページ）を参照してください。

変数の管理

ライセンス：Protection

変数セット内の新規の変数セット ページ、または変数セットの編集ページで変数を管理します。すべての変数セットの変数ページでは、変数は [カスタマイズされた変数（Customized Variables）] ページ領域と [デフォルトの変数（Default Variables）] ページ領域に分かれています。

デフォルトの変数は、ASA FirePOWER モジュール によって提供される変数です。デフォルト変数の値をカスタマイズすることができます。デフォルト変数の名前変更または削除はできません。また、デフォルト値を変更することもできません。

カスタマイズされた変数は、次のいずれかになります。

- カスタマイズされたデフォルト変数

  デフォルト変数の値を編集すると、システムはその変数を [デフォルトの変数（Default Variables）] 領域から [カスタマイズされた変数（Customized Variables）] 領域に移動します。デフォルト セットの変数値によってカスタム セットの変数のデフォルト値が決まるため、デフォルト セットのデフォルト変数をカスタマイズすると、他のすべてのセットの変数のデフォルト値が変更されます。

- ユーザ定義変数

  独自の変数を追加および削除したり、異なる変数セット内の値をカスタマイズしたり、カスタマイズされた変数をそのデフォルト値にリセットしたりできます。ユーザ定義変数をリセットすると、それは [カスタマイズされた変数（Customized Variables）] 領域に残ります。

次の表に、変数を作成または編集するために実行できるアクションを要約します。

表 *2-4*　変数の管理アクション

目的	操作
変数のページを表示する	変数セット ページで、[変数セットの追加（Add Variable Set）] をクリックして新しい変数セットを作成するか、編集する変数セットの横にある編集アイコン（ ）をクリックします。
変数セットに名前を付け、オプションで説明を加える	[名前（Name）] および [説明（Description）] フィールドに、スペースや特殊文字を含む、英数字文字列を入力します。
変数を追加する	[追加（Add）] をクリックします。 詳細については、変数の追加および編集（2-23 ページ）を参照してください。
変数を編集する	編集する変数の横にある編集アイコン（ ）をクリックします。 詳細については、変数の追加および編集（2-23 ページ）を参照してください。
変更された変数をデフォルト値にリセットする	ヒント　変更された変数の横にあるリセット アイコン（ ）をクリックします。影付きリセット アイコンは、現在の値がすでにデフォルト値であることを示します。
ユーザ定義のカスタマイズされた変数を削除する	変数セットの横にある削除アイコン（ ）をクリックします。変数の追加後に変数セットを保存した場合は、[はい（Yes）] をクリックして変数を削除することを確認します。 デフォルト変数は削除できません。また、侵入ルールまたは他の変数によって使用されているユーザ定義変数は削除できません。
変数セットへの変更を保存する	変数セットがアクセス コントロール ポリシーで使用されている場合は [ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックしてから、[はい（Yes）] をクリックして変更を保存することを確認します。 デフォルト セットの現在の値によって他のすべてのセットのデフォルト値が決まるため、デフォルト セットの変数を変更またはリセットすると、デフォルト値がカスタマイズされていない他のセットの現在の値が変更されます。

変数セットの変数を表示する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [オブジェクト管理(Object Management)] の順に選択します。

[オブジェクト管理(Object Management)] ページが表示されます。

ステップ 2　[変数セット(Variable Set)] を選択します。

ステップ 3　変数セットを追加したり、既存のセットを編集したりするには、次の手順に従います。

- 変数セットを追加するには、[変数セットの追加(Add Variable Set)] をクリックします。
- 変数セットを編集するには、変数セットの横にある編集アイコン( )をクリックします。

新規の変数セット ページ、または変数セットの編集ページが表示されます。

ステップ 4　変数を追加したり、既存の変数を編集したりするには、次の手順に従います。

- 変数を追加するには、[追加(Add)] をクリックします。
- 変数を編集するには、変数の横にある編集アイコン( )をクリックします。

新規の変数ページ、または変数の編集ページが表示されます。

変数セット内の変数を追加および編集する方法の詳細については、変数の追加および編集 (2-23 ページ)を参照してください。

変数の追加および編集

ライセンス:Protection

任意のカスタム セットで変数を変更できます。

カスタム 標準テキスト ルール を作成する場合、独自のユーザ定義変数を追加して、トラフィックをより正確に反映したり、ショートカットとしてルール作成プロセスを単純化したりできます。たとえば、「緩衝地帯」(つまり DMZ) でのみトラフィックを検査するルールを作成する場合、公開されているサーバの IP アドレスが値にリストされる変数 `$DMZ` を作成できます。こうして、この地帯で作成された任意のルールで `$DMZ` 変数を使用できます。

変数セットに変数を追加すると、他のすべてのセットにもその変数が追加されます。以下に説明されている 1 つの例外を除き、変数はデフォルト値として他のセットに追加され、その後ユーザはそれをカスタマイズできます。

カスタム セットから変数を追加すると、設定値をデフォルト セットのカスタマイズ値として使用するかどうかを決定する必要があります。

- 設定値(たとえば、192.168.0.0/16) を使用する場合、変数は、デフォルト値 `any` を持つカスタマイズ値として設定値を使用するデフォルト セットに追加されます。デフォルト セットの現在の値によって他のセットのデフォルト値が決まるため、他のカスタム セットの初期のデフォルト値は設定値(この例では 192.168.0.0/16)になります。
- 設定値を使用しない場合、変数はデフォルト値 `any` のみを使用してデフォルト セットに追加され、こうして、他のカスタム セットの初期のデフォルト値は `any` になります。

詳細については、変数セットについて(2-19 ページ)を参照してください。

変数セット内の変数の追加は [新規変数(New Variable)] ページで行い、既存の変数の編集は [変数の編集(Edit Variable)] ページで行います。これら 2 つのページは、既存の変数を編集する場合に、変数名または変数タイプを変更できないこと以外は、同じように使用します。

各ページは主に次の 3 つのウィンドウで構成されます。

- 既存のネットワークまたはポート変数、オブジェクト、およびネットワーク オブジェクト グループを含む、使用可能な項目
- 変数定義に包含するネットワークまたはポート
- 変数定義から除外するネットワークまたはポート

次の 2 種類の変数を作成または編集できます。

- ネットワーク変数は、ネットワーク トラフィックのホストの IP アドレスを指定します。ネットワーク変数の操作（2-27 ページ）を参照してください。
- ポート 変数は、ネットワーク トラフィックの TCP または UDP ポートを指定するもので、いずれかのタイプを意味する値 `any` を指定することもできます。ポート変数の操作（2-29 ページ）を参照してください。

ネットワーク変数タイプを追加するのか、ポート変数タイプを追加するのかを指定すると、ページが更新され、使用可能な項目がリストされます。リストの上部にある検索フィールドを使用してリストを制約できます。これは、入力するにつれて更新されます。

項目のリストから使用可能な項目を選択してドラッグし、包含または除外することができます。また、項目を選択し、[包含（Include）] または [除外（Exclude）] ボタンをクリックすることもできます。複数の項目を選択するには、Ctrl キーと Shift キーを使用します。包含または除外された項目のリストの下にある設定フィールドを使用して、ネットワーク変数にリテラル IP アドレスおよびアドレス ブロック、およびポート変数にポートおよびポート範囲を指定できます。

ネットワーク変数の場合、包含または除外する項目のリストは、リテラル文字列や既存の変数、オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせで構成できます。

次の表に、変数を作成または編集するために実行できるアクションを要約します。

表 *2-5*　変数の編集アクション

目的	操作
変数のページを表示する	変数セットのページで、[追加（Add）] をクリックして新しい変数を追加するか、既存の変数の横にある編集アイコン（  ）をクリックします。
変数に名前を付ける	[名前（Name）] フィールドに、下線文字（_）以外の特殊文字が含まれない、大文字と小文字が区別される一意の英数字文字列を入力します。 変数名は大文字と小文字を区別することに注意してください。たとえば、`var` と `Var` はそれぞれ一意です。
ネットワーク変数またはポート変数を指定する	[タイプ（Type）] ドロップダウンリストから [ネットワーク（Network）] または [ポート（Port）] を選択します。 ネットワーク変数およびポート変数を使用して設定する方法の詳細については、ネットワーク変数の操作（2-27 ページ）およびポート変数の操作（2-29 ページ）を参照してください。
利用可能なネットワークのリストから選択できるように、個別のネットワーク オブジェクトを追加する	[タイプ（Type）] ドロップダウンリストから [ネットワーク（Network）] を選択し、追加アイコン（  ）をクリックします。オブジェクト マネージャを使用してネットワーク オブジェクトを追加する方法の詳細については、ネットワーク オブジェクトの操作（2-4 ページ）を参照してください。

表 2-5　変数の編集アクション（続き）

目的	操作
利用可能なポートのリストから選択できるように、個別のポート オブジェクトを追加する	[タイプ（Type）] ドロップダウンリストから [ポート（Port）] を選択し、追加アイコン（ ）をクリックします。 任意のポート タイプを追加できますが、いずれかのタイプを意味する値 any を含め、TCP および UDP ポートだけが有効な変数値であり、使用可能なポートのリストにはこれらの値タイプを使用する変数のみが表示されます。オブジェクト マネージャを使用してポート オブジェクトを追加する方法の詳細については、ポート オブジェクトの操作（2-11 ページ）を参照してください。
使用可能なポート項目またはネットワーク項目を名前で検索する	使用可能な項目のリストの上にある検索フィールドで名前を入力していきます。入力するに従ってページが更新され、一致する名前が表示されます。
名前の検索をクリアする	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。
使用可能な項目を区別する	変数アイコン（ ）、ネットワーク オブジェクト アイコン（ ）、ポート アイコン（ ）、およびオブジェクト グループ アイコン（ ）の横にある項目を探します。 ポート グループではなく、ネットワーク グループだけが使用可能であることに注意してください。
変数定義に含める（または除外する）オブジェクトを選択する	使用可能なネットワークまたはポートのリストにあるオブジェクトをクリックします。複数のオブジェクトを選択するには、Ctrl キーと Shift キーを使用します。
含まれる（または除外される）ネットワークまたはポートのリストに、選択した項目を追加する	選択した項目をドラッグ アンド ドロップします。あるいは、[包含（Include）] または [除外（Exclude）] をクリックします。 使用可能な項目のリストから、ネットワークやポートの変数とオブジェクトを追加できます。また、ネットワーク オブジェクト グループを追加することもできます。
リテラル ネットワークまたはポートを含める（または除外する）ために、ネットワークまたはポートのリストに追加する	クリックしてリテラル [ネットワーク（Network）] または [ポート（Port）] フィールドからプロンプトを削除し、ネットワーク変数の場合はリテラル IP アドレスまたはアドレス ブロック、ポート変数の場合はリテラル ポートまたはポート範囲をそれぞれ入力して、[追加（Add）] をクリックします。 ドメイン名やリストを入力できないことに注意してください。複数の項目を追加するには、それぞれを個別に追加します。
値が any の変数を追加する	変数に名前を付け、変数タイプを選択してから、値を設定せずに [ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。
包含/除外リストから変数またはオブジェクトを削除する	変数の横にある削除アイコン（ ）をクリックします。
新規または変更された変数を保存する	[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。カスタム セットから変数を追加している場合は、[はい（Yes）] をクリックすると設定値が他のセットのデフォルト値として使用され、[いいえ（No）] をクリックするとデフォルト値 any が使用されます。

詳細については、次の各項を参照してください。

- ネットワーク変数の操作（2-27 ページ）
- ポート変数の操作（2-29 ページ）

変数を追加または編集する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [オブジェクト管理(Object Management)] の順に選択します。

[オブジェクト管理(Object Management)] ページが表示されます。

ステップ 2　[変数セット(Variable Set)] を選択します。

ステップ 3　変数セットを追加したり、既存のセットを編集したりするには、次の手順に従います。

- 変数セットを追加するには、[変数セットの追加(Add Variable Set)] をクリックします。
- 既存の変数セットを編集するには、変数セットの横にある編集アイコン( )をクリックします。

新規の変数セット ページ、または変数セットの編集ページが表示されます。

ステップ 4　新しい変数を追加したり、既存の変数を編集したりするには、次の手順に従います。

- 新しい変数を追加するには、[追加(Add)] をクリックします。
- 既存の変数を編集するには、変数の横にある編集アイコン( )をクリックします。

新規の変数ページ、または変数の編集ページが表示されます。

ステップ 5　新しい変数を追加している場合は:

- [名前(Name)] に一意の変数名を入力します。

  英数字およびアンダースコア(_)文字を使用できます。
- ドロップダウンリストから、変数の [タイプ(Type)] として [ネットワーク(Network)] または [ポート(Port)] を選択します。

ステップ 6　オプションで、使用可能なネットワークまたはポートのリストから、包含または除外項目リストに項目を移動します。

1 つ以上の項目を選択してから、ドラッグ アンド ドロップするか、[包含(Include)] または [除外(Exclude)] をクリックできます。複数の項目を選択するには、Ctrl キーと Shift キーを使用します。

ヒント　ネットワーク変数またはポート変数の包含リストと除外リストにあるアドレスやポートが重複している場合、除外されているアドレスまたはポートが優先されます。

ステップ 7　オプションで、1 つのリテラル値を入力し、[追加(Add)] をクリックします。

ネットワーク変数の場合、単一の IP アドレスまたはアドレス ブロックを入力できます。ポート変数の場合、単一ポートまたはポート範囲を追加できます。ポート範囲は上限値と下限値をハイフン(-)で区切ります。

複数のリテラル値を入力する場合は、必要に応じてこの手順を繰り返します。

ステップ 8　[ASA FirePOWER の変更の保存(Store ASA FirePOWER Changes)] をクリックして変数を保存します。カスタム セットから新しい変数を追加する場合、次のオプションがあります。

- [はい(Yes)] をクリックすると、設定値を使用する変数がデフォルト セットのカスタマイズ値として追加され、結果として他のカスタム セットのデフォルト値として追加されます。
- [いいえ(No)] をクリックすると、変数はデフォルト セットのデフォルト値 `any` として追加され、結果として他のカスタム セットのデフォルト値として追加されます。

ステップ 9　変更を終えたら、変数セットを保存するために [ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックして、[はい（Yes）] をクリックします。

変更内容が保存され、変数セットにリンクされているアクセス コントロール ポリシーに失効ステータスが表示されます。変更を反映させるには、変数セットが侵入ポリシーに関連付けられているアクセス 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（4-12 ページ）を参照してください）。

ネットワーク変数の操作

ライセンス：Protection

ネットワーク変数で表される IP アドレスを、侵入ポリシーで有効になった侵入ルール、侵入ポリシー ルール抑制、動的ルール状態、および適応型プロファイルで使用することができます。ネットワーク変数とネットワーク オブジェクトおよびネットワーク オブジェクト グループとの相違点として、ネットワーク変数は侵入ポリシーおよび侵入ルールに固有のものです。一方、ネットワーク オブジェクトおよびグループを使用すると、アクセス コントロール ポリシー、ネットワーク変数、侵入ルール、レポートなど、ASA FirePOWER モジュール のさまざまな場所で IP アドレスを表すことができます。詳細については、ネットワーク オブジェクトの操作（2-4 ページ）を参照してください。

次の設定でネットワーク変数を使用して、ネットワーク上のホストの IP アドレスを指定できます。

- 侵入ルール

  侵入ルールの [送信元 IP（Source IPs）] および [宛先 IP（Destination IPs）] 見出しフィールドを使用すると、パケット インスペクションを、特定の送信元または宛先 IP アドレスを持つパケットに制限することができます。侵入ルールでの IP アドレスの指定（27-5 ページ）を参照してください。

- 抑制

  送信元または宛先の侵入ルール抑制の [ネットワーク（Network）] フィールドを使用すると、特定の 1 つの IP アドレスまたは IP アドレス範囲が侵入ルールやプリプロセッサをトリガーした場合の侵入イベント通知を抑制できます。侵入ポリシー単位の抑制の設定（24-28 ページ）を参照してください。

- 動的ルール状態

  送信元または宛先の動的ルール状態の [ネットワーク（Network）] フィールドを使用すると、指定時間内に発生した侵入ルールやプリプロセッサ ルールの一致数が多すぎる場合に、それを検出できます。動的ルール状態の追加（24-31 ページ）を参照してください。

- 適応型プロファイル

  適応型プロファイルの [ネットワーク（Networks）] フィールドは、パッシブ展開でのパケット フラグメントと TCP ストリームの再構築リアセンブリを改善させる必要があるネットワーク内のホストを特定します。パッシブ展開における前処理の調整（22-1 ページ）を参照してください。

このセクションで示されるフィールドで変数を使用する場合、侵入ポリシーにリンクされた変数セットは、侵入ポリシーを使用するアクセス コントロール ポリシーで処理されるネットワーク トラフィックでの変数値を決定します。

次のネットワーク設定を任意に組み合わせて変数に追加できます。

- 使用可能なネットワーク リストから選択したネットワーク変数、ネットワーク オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせ

  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（2-4 ページ）を参照してください。

- [新規変数（New Variable）] または [変数の編集（Edit Variable）] ページから追加した個々のネットワーク オブジェクト（独自の変数や、他の既存の変数、さらに今後の変数にこれらを追加できます）

- リテラルの単一 IP アドレスまたはアドレス ブロック

  それぞれを個別に追加することにより、複数のリテラル IP アドレスとアドレス ブロックをリストできます。IPv4 および IPv6 アドレスとアドレス ブロックを単独で、または任意に組み合わせてリストできます。IPv6 アドレスを指定するときには、RFC 4291 で定義された任意のアドレス指定規則を使用できます。

追加する変数での包含ネットワークのデフォルト値は `any` で、これは任意の IPv4 または IPv6 アドレスを示します。除外ネットワークのデフォルト値は none で、これは「ネットワークなし」を示します。また、リテラル値の中でアドレス `::` を指定すると、包含ネットワーク リストで任意の IPv6 アドレスを指定でき、除外リストでは IPv6 アドレスなしを指定できます。

除外リストにネットワークを追加すると、指定されたアドレスおよびアドレス ブロックが拒否されます。つまり、除外された IP アドレスやアドレス ブロックを除き、任意の IP アドレスに一致させることができます。

たとえば、リテラル アドレス `192.168.1.1` を除外すると 192.168.1.1 以外の任意の IP アドレスが指定され、`2001:db8:ca2e::fa4c` を除外すると 2001:db8:ca2e::fa4c 以外の任意の IP アドレスが指定されます。

リテラル ネットワークまたは使用可能なネットワークを任意に組み合わせて、除外で使用できます。たとえば、リテラル値 `192.168.1.1` および `192.168.1.5` を除外すると、192.168.1.1 と 192.168.1.5 以外の任意の IP アドレスが含まれます。つまり、システムはこの構文を「192.168.1.1 でなく、しかも 192.168.1.5 でない」と解釈し、大カッコ内に列挙されたものを除くすべての IP アドレスに一致させます。

ネットワーク変数を追加または編集するときには、次の点に注意してください。

- 論理的に言って、値 `any` を除外することはできません。any を除外すると「アドレスなし」を意味することになります。たとえば、除外ネットワーク リストに、値 `any` を持つ変数を追加することはできません。
- ネットワーク変数は、指定された侵入ルールおよび侵入ポリシー機能に関するトラフィックを識別します。プリプロセッサ ルールは、侵入ルールで使われているネットワーク変数で定義されたホストとは無関係に、イベントをトリガーできることに注意してください。
- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、アドレス ブロック 192.168.5.0/24 を包含し、192.168.6.0/24 を除外することはできません。エラー メッセージが表示され、問題となっている変数が明示されます。包含される値の範囲外となる値を除外した場合は、変数セットを保存できません。

ネットワーク変数の追加および編集の詳細については、変数の追加および編集（2-23 ページ）を参照してください。

ポート変数の操作

ライセンス：Protection

ポート変数は、侵入ポリシーで有効になった侵入ルールの [送信元ポート（Source Port）] および [宛先ポート（Destination Port）] 見出しフィールドで使用できる TCP ポートと UDP ポートを表します。ポート変数とポート オブジェクトおよびポート オブジェクト グループとの相違点は、ポート変数が侵入ルール固有のものであることです。TCP や UDP 以外のプロトコル用にポート オブジェクトを作成し、ポート変数およびアクセス コントロール ポリシーでポート オブジェクトを使用できます。詳細については、ポート オブジェクトの操作（2-11 ページ）を参照してください。

侵入ルールの [送信元ポート（Source Port）] および [宛先ポート（Destination Port）] 見出しフィールドでポート変数を使用すると、パケット インスペクションを、特定の送信元または宛先 TCP/UDP ポートを持つパケットに制限することができます。

これらのフィールドで変数を使用した場合、アクセス コントロール ルールまたはポリシーに関連付けられた侵入ポリシーにリンクされる変数セットは、アクセス コントロール ポリシーが適用されるネットワーク トラフィックでのこれらの変数の値を決定します。

次のポート設定を任意に組み合わせて変数に追加できます。

- 使用可能なポート リストから選択したポート変数およびポート オブジェクトの任意の組み合わせ

  使用可能なポート リストには、ポート オブジェクト グループが表示されず、したがってこれらを変数に追加できないことに注意してください。オブジェクト マネージャを使用してポート 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（2-11 ページ）を参照してください。

- [新規変数（New Variable）] または [変数の編集（Edit Variable）] ページから追加した個々のポート オブジェクト（独自の変数や、他の既存の変数、さらに今後の変数にこれらを追加できます）

  有効な変数値は TCP および UDP ポートのみです（どちらのタイプでも値 `any` を含む）。新しい変数のページまたは変数の編集ページを使用して、有効な変数値ではない有効なポート オブジェクトを追加した場合、オブジェクトはシステムに追加されますが、使用可能なオブジェクト リストには表示されません。オブジェクト マネージャを使用して、変数で使われるポート オブジェクトを編集する場合、有効な変数値にのみ値を変更できます。

- 単一のリテラル ポート値とポート範囲

  ポート範囲はダッシュ（-）を使って区切る必要があります。下位互換性のために、コロンで指定されるポート範囲もサポートされていますが、作成するポート変数ではコロンを使用できません。

  複数のリテラル ポートの値および範囲をリストするには、それぞれを個別に追加して任意に組み合わせることができます。

ポート変数を追加または編集するときには、次の点に注意してください。

- 追加する変数での包含ポートのデフォルト値は `any` で、これは任意のポートまたはポート範囲を示します。除外ポートのデフォルト値は `none` で、これは「ポートなし」を示します。

ヒント　値 `any` を持つ変数を作成するには、特定の値を追加せずに変数に名前を付けて保存します。

- 論理的に言って、値 `any` を除外することはできません。any を除外すると「ポートなし」を意味することになります。たとえば、値 `any` を持つ変数を除外ポート リストに追加した場合、変数セットを保存することはできません。

- 除外リストにポートを追加すると、指定されたポートおよびポート範囲が拒否されます。つまり、除外されたポートまたはポート範囲を除き、任意のポートに一致させることができます。
- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、ポート範囲 10 から 50 を包含し、ポート 60 を除外することはできません。エラー メッセージが表示され、問題となっている変数が明示されます。包含される値の範囲外となる値を除外した場合は、変数セットを保存できません。

ポート変数の追加および編集の詳細については、変数の追加および編集（2-23 ページ）を参照してください。

変数のリセット

ライセンス：Protection

変数セットの新しい変数ページまたは変数の編集ページで、変数をデフォルト値にリセットできます。次の表に、変数をリセットするときの基本原則を要約します。

表 ***2-6***　変数のリセット値

リセットする変数のタイプ	それが含まれるセットタイプ	リセット後の値
デフォルト	デフォルト	ルール更新値
ユーザ定義	デフォルト	任意
デフォルトまたはユーザ定義	カスタム	現在のデフォルト セット値（変更/未変更にかかわらず）

カスタム セットの変数をリセットすると、単にデフォルト セット内のその変数の現在値にリセットされます。

逆に、デフォルト セットの変数の値をリセットまたは変更すると、すべてのカスタム セット内のその変数のデフォルト値が常に更新されます。リセット アイコンがグレー表示され、その変数をリセットできないことを示している場合、そのセットでは変数のカスタマイズ値が存在しないことを意味します。カスタム セット内の変数の値をすでにカスタマイズした場合を除き、デフォルト セットの変数を変更すると、変数セットがリンクされた侵入ポリシーで使われている値が更新されます。

（注）　デフォルト セット内の変数を変更するときには、その変更により、リンクされたカスタム セットの変数を使用する侵入ポリシーがどのような影響を受けるか評価するのが適切です（特に、カスタム セット内の変数値をカスタマイズしていない場合）。

カスタマイズされた値とリセット値が同じである場合は、次のいずれかを示しています。

- カスタム セットまたはデフォルト セットの中で、値 `any` を持つ変数を追加した
- カスタム セットの中で、明示的な値を持つ変数を追加し、設定した値をデフォルト値として使用することを選択した

変数セットを侵入ポリシーにリンクさせる

ライセンス：Control

デフォルトは、ASA FirePOWER モジュールは、アクセス コントロール ポリシーで使用されるすべての侵入ポリシーにデフォルト変数セットをリンクします。侵入ポリシーを使用するアクセス コントロール ポリシーを適用すると、その侵入ポリシー内で有効になった侵入ルールは、リンクされた変数セットの変数値を使用します。

アクセス コントロール ポリシー内の侵入ポリシーで使われるカスタム変数セットを変更すると、システムの [アクセス コントロール（Access Control）] ページで、そのポリシーのステータスが「失効」と示されます。変数セットの変更内容を反映させるには、アクセス コントロール ポリシーを再適用する必要があります。デフォルト セットを変更すると、侵入ポリシーを使用するすべてのアクセス コントロール ポリシーのステータスが「失効」と示され、変更内容を反映させるにはすべてのアクセス コントロール ポリシーを再適用する必要があります。

情報については、次の各項を参照してください。

- デフォルト セット以外の変数セットをアクセス コントロール ルールにリンクさせるには、侵入防御を実行するアクセス コントロール ルールの設定（10-5 ページ）の手順を参照してください。
- デフォルト セット以外の変数セットをアクセス コントロール ポリシーのデフォルト アクションにリンクさせるには、デフォルト処理の設定およびネットワーク トラフィックのインスペクション（4-5 ページ）を参照してください。
- 変数セットを侵入ポリシーにリンクさせるポリシーを含むアクセス コントロール ポリシーを適用するには、設定変更の展開（4-12 ページ）を参照してください。

拡張変数について

ライセンス：Protection

拡張変数を使用すると、他の方法ではモジュール インターフェイスで設定できない機能を設定することができます。現在、ASA FirePOWER モジュールには 2 つの拡張変数だけが備わっており、そのうち USER_CONF 拡張変数のみを編集できます。

USER_CONF

USER_CONF は、本来はモジュール インターフェイスを介して使用できない 1 つ以上の機能を設定できる一般ツールを提供します。

注意　機能の説明またはサポート担当の指示に従う場合を除き、拡張変数 USER_CONF を使用して侵入ポリシー機能を設定しないでください。競合または重複する設定が存在すると、システムが停止します。

USER_CONF を編集するときには、1 行に合計 4096 文字まで入力できます。行は自動的に折り返します。変数の最大長 8192 文字、またはディスク スペースなどの物理制限に達するまで、任意の数の有効な指示または行数を含めることができます。コマンド ディレクティブでは、完全な引数の後にバックスラッシュ（\）行連結文字を使用します。

USER_CONF をリセットすると、空になります。

シンクホール オブジェクトの使用

ライセンス:Protection

シンクホール オブジェクトとは、シンクホール内のすべてのドメイン名のルーティング不可アドレスか、またはサーバに解決されない IP アドレスのいずれかを付与する DNS サーバを表します。DNS ポリシー ルール内のシンクホール オブジェクトを参照して、一致するトラフィックをシンクホールにリダイレクトすることができます。オブジェクトには、IPv4 アドレスと IPv6 アドレスの両方を割り当てる必要があります。

使用中のシンクホール オブジェクトは削除できません。さらに、DNS ポリシーで使用されるシンクホール オブジェクトを編集した後、変更内容を有効にするには、設定を再適用する必要があります。

シンクホール オブジェクトを作成する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [オブジェクト管理(Object Management)] の順に選択します。

[オブジェクト管理(Object Management)] ページが表示されます。

ステップ 2　オブジェクト タイプのリストから [シンクホール(Sinkhole)] を選択します。

ステップ 3　[シンクホールの追加(Add Sinkhole)] をクリックします。

ステップ 4　名前を入力します。

ステップ 5　シンクホールの [IPv4 アドレス(IPv4 Address)] と [IPv6 アドレス(IPv6 Address)] を入力します。

ステップ 6　次の選択肢があります。

- シンクホール サーバにトラフィックをリダイレクトする場合は、[シンクホールへの接続のログ(Log Connections to Sinkhole)] を選択します。
- 非解決 IP アドレスにトラフィックをリダイレクトする場合は、[シンクホールへの接続をブロックしてログ(Block and Log Connections to Sinkhole)] を選択します。

ステップ 7　侵入の痕跡(IoC)のタイプをシンクホールに割り当てるには、[タイプ(Type)] ドロップダウンからいずれかのタイプを選択します。

ステップ 8　[ASA FirePOWER の変更の保存(Store ASA FirePOWER Changes)] をクリックします。

ステップ 9　シンクホール オブジェクトを使用する DNS ポリシーを含んでいるすべてのアクセス コントロール ポリシーを再適用します。

ファイル リストの操作

ライセンス:マルウェア

ネットワークベースの高度なマルウェア防御(AMP)を使用している場合、Collective Security Intelligence クラウドによってファイルの性質が誤って認識されたときに、SHA-256 ハッシュ値を使ってそのファイルをファイル リストに追加すると、その後、ファイルがより適切に検出されるようになります。ファイル リストのタイプに応じて、次の操作を実行できます。

- クラウドがクリーンの性質を割り当てた場合と同じ方法でファイルを扱うには、クリーンリストにファイルを追加します。
- クラウドがマルウェアの性質を割り当てた場合と同じ方法でファイルを扱うには、カスタム検出リストにファイルを追加します。

これらのファイルのブロッキング動作は手動で指定されるため、そのファイルがクラウドによってマルウェアと識別されるような場合でも、システムはマルウェア クラウド ルックアップを実行しません。ファイルの SHA 値を計算するには、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）] アクションと [マルウェア ブロック（Block Malware）] アクションのどちらか、および一致するファイル タイプを使用して、ファイル ポリシー内のルールを設定する必要があることに注意してください。詳細については、ファイル ルールの操作（32-11 ページ）を参照してください。

システムのクリーン リストとカスタム検出リストは、デフォルトですべてのファイル ポリシーに含まれています。ポリシーごとに、いずれかまたは両方のリストを使用しないことを選択できます。

注意　実際にマルウェアであるファイルをこのリストに含めないでください。クラウドがそのファイルのマルウェアの性質を割り当てた場合、またはファイルをカスタム検出リストに追加した場合でも、システムはそれをブロックしません。

各ファイル リストには、一意の SHA-256 値を最大 10000 個まで含めることができます。ファイルをファイル リストに追加するには、次の操作を実行できます。

- ファイルをアップロードする。これにより、システムはそのファイルの SHA-256 値を計算してそれを追加します。
- ファイルの SHA-256 値を直接入力する。
- 複数の SHA-256 値を含むコンマ区切り値（CSV）ソース ファイルを作成してアップロードする。重複しないすべての SHA-256 値がこのファイル リストに追加されます。

ファイル リストにファイルを追加したり、ファイル リスト内の SHA-256 値を編集したり、ファイル リストから SHA-256 値を削除したりした場合、変更を有効にするには、そのリストを使用するファイル ポリシーを含むアクセス コントロール ポリシーをすべて再適用する必要があります。

ファイル リストの使用の詳細については、次のトピックを参照してください。

- ファイル リストに複数の SHA-256 値をアップロードする（2-33 ページ）
- 個別のファイルをファイル リストにアップロードする（2-35 ページ）
- ファイル リストに SHA-256 値を追加する（2-35 ページ）
- ファイル リスト上のファイルの変更（2-36 ページ）
- ファイル リストからソース ファイルをダウンロードする（2-37 ページ）

ファイル リストに複数の SHA-256 値をアップロードする

ライセンス：マルウェア

SHA-256 値のリストと説明を含むコンマ区切り値（CSV）ソース ファイルをアップロードすることによって、複数の SHA-256 値をファイル リストに追加できます。システムはその内容を検証し、有効な SHA-256 値をファイル リストに入れます。

ソース ファイルは、ファイル名拡張子 .csv の単純なテキスト ファイルである必要があります。見出しはポンド記号（#）で始まる必要があります。これはコメントとして処理され、アップロードされません。各エントリには、1 つの SHA-256 値の後に（最大 256 個の英文字または特殊文字からなる）説明が含まれる必要があり、LF または CR+LF 改行文字で終わる必要があります。システムはエントリ内のこれ以外の情報をすべて無視します。

次の点に注意してください。

- ファイル リストからソース ファイルを削除すると、それに関連付けられているすべての SHA-256 ハッシュもファイル リストから削除されます。

- ソース ファイルのアップロードに成功した結果、10000 個を超える個別の SHA-256 値がファイル リストに含まれる場合は、複数のファイルをファイル リストにアップロードすることはできません。
- システムは、アップロード時に 256 文字を超える説明を最初の 256 文字で切り捨てます。説明にコンマを含める場合は、エスケープ文字（\）を使用する必要があります。説明が含まれていない場合、代わりにソース ファイル名が使用されます。
- すでにファイル リストに存在する SHA-256 値を含むソース ファイルをアップロードした場合、新しくアップロードされた値によって既存の SHA-256 値が変更されることはありません。SHA-256 値に関連するキャプチャ済みファイル、ファイル イベント、またはマルウェア イベントを表示するとき、個々の SHA-256 値から脅威名または説明が得られます。
- システムはソース ファイル内の無効な SHA-256 値をアップロードしません。
- アップロードされた複数のソース ファイル内に同じ SHA-256 値に関するエントリが含まれる場合、システムは最も新しい値を使用します。
- 1 つのソース ファイル内に同じ SHA-256 値のエントリが複数含まれる場合、システムは最後のものを使用します。
- オブジェクト マネージャ内でソース ファイルを直接編集することはできません。変更を行うには、最初にソース ファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。詳細については、ファイル リストからソース ファイルをダウンロードする（2-37 ページ）を参照してください。

ソース ファイルをファイル リストにアップロードする方法:

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ 2　[ファイル リスト（File List）] をクリックします。

[ファイル リスト（File List）] セクションが表示されます。

ステップ 3　ソース ファイルからの値の追加先となるファイル リストの横にある編集アイコン（  ）をクリックします。

[ファイル リスト（File List）] ポップアップ ウィンドウが表示されます。

ステップ 4　[追加方法（Add by）] フィールドから [SHA のリスト（List of SHAs）] を選択します。

ポップアップ ウィンドウが更新され、新しいフィールドが含まれます。

ステップ 5　オプションで、[説明（Description）] フィールドにソース ファイルの説明を入力します。

説明を入力しない場合、システムはファイル名を使用します。

ステップ 6　[参照（Browse）] をクリックしてソース ファイルを参照してから、[リストのアップロードと追加（Upload and Add List）] をクリックしてリストを追加します。

ソース ファイルがファイル リストに追加されます。SHA-256 カラムには、ファイルに含まれる SHA-256 値の数がリストされます。

ステップ 7　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

ステップ 8　ファイル リストを使用するファイル ポリシーを含んでいるすべてのアクセス コントロール ポリシーを再適用します。

ポリシーが適用されると、システムはファイル リスト内のファイルに対してマルウェア クラウド ルックアップを実行しなくなります。

個別のファイルをファイル リストにアップロードする

ライセンス:マルウェア

ファイル リストに追加するファイルのコピーがある場合、分析用にファイルをシステムにアップロードできます。システムはファイルの SHA-256 値を計算し、ファイルをリストに追加します。SHA-256 を計算するとき、システムはファイル サイズを制限しません。

システムに **SHA-256** 値を計算させることによってファイルを追加するには、次の手順を実行します。

ステップ **1**　オブジェクト マネージャの [ファイル リスト(File List)] ページで、ファイルの追加場所となるクリーン リストまたはカスタム検出リストの横の編集アイコン( )をクリックします。

[ファイル リスト(File List)] ポップアップ ウィンドウが表示されます。

ステップ **2**　[追加方法(Add by)] フィールドから [SHA の計算(Calculate SHA)] を選択します。

ポップアップ ウィンドウが更新され、新しいフィールドが含まれます。

ステップ **3**　オプションで、[説明(Description)] フィールドにファイルの説明を入力します。

説明を入力しない場合、アップロード時にファイル名が説明として使用されます。

ステップ **4**　[参照(Browse)] をクリックしてソース ファイルを参照してから、[SHA を計算して追加(Calculate and Add SHA)] をクリックしてリストを追加します。

ファイルがファイル リストに追加されます。

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

ステップ **6**　ファイル リストを使用するファイル ポリシーを含んでいるすべてのアクセス コントロール ポリシーを再適用します。

ポリシーが適用されると、システムはファイル リスト内のファイルに対してマルウェア クラウド ルックアップを実行しなくなります。

ファイル リストに **SHA-256** 値を追加する

ライセンス:マルウェア

ファイルの SHA-256 値を送信して、それをファイル リストに追加できます。重複する SHA-256 値は追加できません。

ファイルの **SHA-256** 値を手動で入力することによってファイルを追加する方法:

ステップ **1**　オブジェクト マネージャの [ファイル リスト(File List)] ページで、ファイルの追加場所となるクリーン リストまたはカスタム検出リストの横の編集アイコン( )をクリックします。

[ファイル リスト(File List)] ポップアップ ウィンドウが表示されます。

ステップ **2**　[追加方法(Add by)] フィールドから [SHA 値の入力(Enter SHA Value)] を選択します。

ポップアップ ウィンドウが更新され、新しいフィールドが含まれます。

ステップ **3**　[説明(Description)] フィールドにソース ファイルの説明を入力します。

ステップ **4**　ファイルの SHA-256 値全体を入力するか、貼り付けます。システムでは値の部分的な一致はサポートされません。

ステップ 5　ファイルを追加するには、[追加(Add)] をクリックします。

ファイルがファイル リストに追加されます。

ステップ 6　[ASA FirePOWER の変更の保存(Store ASA FirePOWER Changes)] をクリックします。

ステップ 7　ファイル リストを使用するファイル ポリシーを含んでいるすべてのアクセス コントロール ポリシーを再適用します。

ポリシーが適用されると、システムはファイル リスト内のファイルに対してマルウェア クラウド ルックアップを実行しなくなります。

ファイル リスト上のファイルの変更

ライセンス:マルウェア

ファイル リストの個々の SHA-256 値を編集または削除することができます。オブジェクト マネージャ内でソース ファイルを直接編集できないことに注意してください。変更を行うには、最初にソース ファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。詳細については、ファイル リストからソース ファイルをダウンロードする (2-37 ページ)を参照してください。ファイル リスト上のファイルを編集する方法:

ステップ 1　オブジェクト マネージャの [ファイル リスト(File List)] ページで、変更するファイルが入っているクリーン リストまたはカスタム検出リストの横の編集アイコン( )をクリックします。

[ファイル リスト(File List)] ポップアップ ウィンドウが表示されます。

ステップ 2　編集する SHA-256 値の横にある編集アイコン( )をクリックします。

[SHA-256 の編集(Edit SHA-256)] ポップアップ ウィンドウが表示されます。

ヒント　リストからファイルを削除することもできます。削除するファイルの横にある削除アイコン( )をクリックしてください。

ステップ 3　[SHA-256] 値または [説明(Description)] を更新します。

ステップ 4　[保存(Save)] をクリックします。

[ファイル リスト(File List)] ポップアップ ウィンドウが表示されます。リスト内のファイル エントリが更新されます。

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

ステップ 6　ファイル リストを使用するファイル ポリシーを含んでいるすべてのアクセス コントロール ポリシーを再適用します。

ポリシーが適用されると、システムはファイル リスト内のファイルに対してマルウェア クラウド ルックアップを実行しなくなります。

ファイル リストからソース ファイルをダウンロードする

ライセンス:マルウェア

ファイル リスト上の既存のソース ファイル エントリを表示、ダウンロード、または削除できます。いったんアップロードされたソース ファイルを編集することはできません。まずファイル リストからソース ファイルを削除し、更新後のファイルをアップロードする必要があります。ソース ファイルをアップロードする方法については、ファイル リストに複数の SHA-256 値をアップロードする (2-33 ページ) を参照してください。

ソース ファイルに関連付けられたエントリ数とは、個別の SHA-256 値の数です。ファイル リストからソース ファイルを削除すると、ファイル リストに含まれる SHA-256 エントリの合計数は、ソース ファイル内の有効なエントリ数だけ減少します。

ソース ファイルをダウンロードする方法:

ステップ 1　オブジェクト マネージャの [ファイル リスト (File List)] ページで、ソースファイルのダウンロード対象となるクリーン リストまたはカスタム検出リストの横の編集アイコン( )をクリックします。

[ファイル リスト (File List)] ポップアップ ウィンドウが表示されます。

ステップ 2　ダウンロードするソース ファイルの横にある表示アイコン( )をクリックします。

[リストで SHA-256 を表示 (View SHA-256's in list)] ポップアップ ウィンドウが表示されます。

ステップ 3　[SHA リストのダウンロード (Download SHA List)] をクリックし、プロンプトに従ってソース ファイルを保存します。

ステップ 4　[閉じる (Close)] をクリックします。

[ファイル リスト (File List)] ポップアップ ウィンドウが表示されます。

セキュリティ ゾーンの操作

ライセンス:任意

サポートされるデバイス:任意

セキュリティ ゾーンは、1 つ以上の ASA インターフェイスからなるグループです。これを使用すると、さまざまなポリシーと設定でトラフィック フローを管理および分類できます。1 つのデバイスで複数のゾーンを設定できます。これにより、ネットワークを複数セグメントに分割して、さまざまなポリシーをそれらに適用できます。トラフィックをセキュリティ ゾーンと照合するには、少なくとも 1 つのインターフェイスをそのセキュリティ ゾーンに割り当てる必要があり、各インターフェイスは 1 つのゾーンのみに属することができます。

セキュリティ ゾーンを使用してインターフェイスをグループ化することに加えて、アクセス コントロール ポリシーでゾーンを使用できます。たとえば、特定の送信元または宛先ゾーンにのみ適用されるアクセス コントロール ルールを作成することができます。

オブジェクト マネージャの [セキュリティ ゾーン (Security Zones)] ページには、ASA FirePOWER モジュールで設定されたゾーンがリストされます。

使用中のセキュリティ ゾーンは削除できません。インターフェイスをゾーンで追加または削除した後は、デバイス設定を再適用する必要があります。また、ゾーンを使用するアクセス コントロール ポリシーを再適用する必要もあります。

セキュリティ ゾーンを追加する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [オブジェクト管理(Object Management)] の順に選択します。

[オブジェクト管理(Object Management)] ページが表示されます。

ステップ 2　[セキュリティ ゾーン(Security Zones)] を選択します。

ステップ 3　[セキュリティ ゾーンの追加(Add Security Zone)] をクリックします。

[セキュリティ ゾーン(Security Zones)] ポップアップ ウィンドウが表示されます。

ステップ 4　[名前(Name)] に、ゾーンの名前を入力します。中カッコ({})とポンド記号(#)を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　[タイプ(Type)] で、ゾーンのインターフェイスのタイプを選択します。

セキュリティ ゾーンの作成後に、タイプを変更することはできません。

ステップ 6　1 つ以上のインターフェイスを選択します。

複数のオブジェクトを選択するには、Ctrl キーと Shift キーを使用します。インターフェイスをまだ設定していない場合は、空のゾーンを作成し、後でそこにインターフェイスを追加できます。ステップ 9 に進みます。

ステップ 7　[追加(Add)] をクリックします。

選択したインターフェイスがゾーンに追加され、デバイス別にグループ化されます。

ステップ 8　他のデバイスのインターフェイスをゾーンに追加するには、ステップ 6 から 8 までを繰り返します。

ステップ 9　[ASA FirePOWER の変更の保存(Store ASA FirePOWER Changes)] をクリックします。

セキュリティ ゾーンが追加されます。

暗号スイート リストの操作

ライセンス:任意

暗号スイート リストは複数の暗号スイートからなるオブジェクトです。各定義済み暗号スイートの値は、SSL または TLS 暗号化セッションのネゴシエーションに使われる暗号スイートを表しています。暗号スイートおよび暗号スイート リストを SSL ルールで使用すると、クライアントとサーバが暗号スイートを使って SSL セッションをネゴシエートしたかどうかに基づいて暗号化トラフィックを制御できます。SSL ルールに暗号スイート リストを追加すると、リスト内のいずれかの暗号スイートでネゴシエートされた SSL セッションがルールに一致します。

(注)　ASDM インターフェイスでは暗号スイート リストと同じ場所で暗号スイートを使用できますが、暗号スイートを追加、変更、削除することはできません。

使用中の暗号スイート リストは削除できません。さらに、SSL ポリシーで使用される暗号スイート リストを編集した後、変更内容を有効にするには、関連するアクセス コントロール ポリシーを再適用する必要があります。

暗号スイート リストを作成する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [オブジェクト管理(Object Management)] の順に選択します。

[オブジェクト管理(Object Management)] ページが表示されます。

ステップ 2　[暗号スイート リスト(Cipher Suite List)] を選択します。

ステップ 3　[暗号スイートの追加(Add Cipher Suites)] をクリックします。

[暗号スイート リスト(Cipher Suite List)] ポップアップ ウィンドウが表示されます。

ステップ 4　[名前(Name)] に、暗号スイート リストの名前を入力します。縦線(|)と中カッコ({})を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　1 つ以上の暗号スイートを選択して、[追加(Add)] をクリックします。

- 複数の暗号スイートを選択するには、Ctrl キーまたは Shift キーを使用するか、右クリックして [すべて選択(Select All)] を選択します。
- リストに含める既存の暗号スイートを検索するにはフィルタ フィールド( )を使用できます。入力していくとフィールドが更新され、一致する項目が表示されます。検索ストリングをクリアするには、検索フィールドの上にある再ロード アイコン( )をクリックするか、検索フィールド内のクリア アイコン( )をクリックします。

ステップ 6　[ASA FirePOWER の変更の保存(Store ASA FirePOWER Changes)] をクリックします。

暗号スイート リストが作成されます。

識別名オブジェクトの操作

ライセンス:任意

それぞれの識別名オブジェクトは、公開鍵証明書のサブジェクトまたは発行元にリストされた識別名を表します。SSL ルールで識別名オブジェクトとグループ(オブジェクトのグループ化 (2-2 ページ)を参照)を使用すると、サブジェクトまたは発行元として識別名を含むサーバ証明書を使ってクライアントとサーバが SSL セッションをネゴシエートしたかどうかに基づき、暗号化トラフィックを制御できます。

識別名オブジェクトには、共通名属性(**CN**)を含めることができます。「CN=」なしで共通名を追加すると、システムはオブジェクトを保存する前に「CN=」を追加します。

さらに、次の表に示す属性を含む識別名を追加することもできます。属性はカンマで区切って使用します。

表 *2-7*　識別名の属性

属性(**Attribute**)	説明	使用可能な値
C	国コード(Country Code)	2 つの英字
CN	Common Name	最大 64 文字の英数字、バックスラッシュ (\)、ハイフン (-)、引用符 (")、アスタリスク (*)、スペース文字
O	Organization	
OU	組織	

ワイルドカードとして 1 つ以上のアスタリスク（*）を属性に定義できます。共通名属性では、ドメイン名ラベルごとに 1 つ以上のアスタリスクを定義できます。ワイルド カードはそのラベル内でのみ照合されますが、ワイルド カードを使用して複数のラベルを定義できます。例については、以下の表を参照してください。

表 *2-8*　共通名属性のワイルドカードの例

属性（**Attribute**）	一致	一致しない
CN=”*ample.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”exam*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*xamp*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*.example.com”	mail.example.com	example.com example.text.com ampleexam.com
CN=”*.com”	example.com ampleexam.com	mail.example.com example.text.com
CN=”*.*.com”	mail.example.com example.text.com	example.com ampleexam.com

使用中の識別名オブジェクトは削除できません。さらに、SSL ポリシーで使用される識別名オブジェクトを編集した後、変更内容を有効にするには、関連するアクセス コントロール ポリシーを再適用する必要があります。

識別名オブジェクトを追加する方法:

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ 2　[識別名（Distinguished Name）] の下で、[個々のオブジェクト（Individual Objects）] を選択します。

ステップ 3　[識別名の追加（Add Distinguished Name）] をクリックします。

[識別名（Distinguished Name）] ポップアップ ウィンドウが表示されます。

ステップ 4　[名前（Name）] に、識別名オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　[DN] フィールドに、識別名または共通名の値を入力します。次の選択肢があります。

- 識別名を追加する場合は、表 2-7（ 2-39 ページ）に示されている属性をカンマで区切って含めることができます。
- 共通名を追加する場合は、複数のラベルとワイルドカードを含めることができます。

ステップ 6　[ASA FirePOWER の変更の保存(Store ASA FirePOWER Changes)] をクリックします。

識別名オブジェクトが追加されます。

PKI オブジェクトの操作

ライセンス:任意

PKI オブジェクトは、SSL インスペクション展開をサポートするために必要な公開鍵証明書、およびペアになった秘密鍵を表します。内部 CA オブジェクトおよび信頼できる CA オブジェクトは、認証局(CA)証明書で構成されます。また、内部 CA オブジェクトには、証明書とペアになった秘密鍵も含まれます。内部証明書オブジェクトおよび外部証明書オブジェクトは、サーバ証明書で構成されます。また、内部証明書オブジェクトには、証明書とペアになった秘密鍵も含まれます。SSL のルールでこれらのオブジェクトを使用すると、次のものを復号できます。

- 発信トラフィック:内部 CA オブジェクトを使ってサーバ証明書を再署名することによって復号します
- 受信トラフィック:内部証明書オブジェクトにある既知の秘密鍵を使用して復号します

さらに、SSL ルールを作成して、次のものを使って暗号化されたトラフィックを照合することができます。

- 外部証明書オブジェクト内の証明書
- 信頼できる CA オブジェクトの CA によって署名された証明書、または信頼できる CA チェーン内で署名された証明書

証明書とキーの情報を手動で入力し、その情報を含むファイルをアップロードします。場合によっては、新しい CA 証明書や秘密キーを生成することができます。

オブジェクト マネージャで PKI オブジェクトのリストを表示すると、システムは証明書のサブジェクト識別名をオブジェクト値として表示します。証明書の完全なサブジェクト識別名を表示するには、値の上にポインタを移動してください。証明書に関する他の詳細を表示するには、PKI オブジェクトを編集します。

(注)　ASA FirePOWER モジュールは、内部 CA オブジェクトと内部証明書オブジェクトに保存されるすべての秘密鍵を、保存前にランダムに生成された鍵を使って暗号化します。パスワード保護されている秘密キーをアップロードすると、アプライアンスはユーザ提供のパスワードを使って秘密キーを復号し、ランダムに生成されたキーを使ってそれを再暗号化してから保存します。

詳細については、次の項を参照してください。

- 内部認証局オブジェクトの使用(2-42 ページ)
- 信頼できる認証局オブジェクトの使用(2-46 ページ)
- 外部証明書オブジェクトの使用(2-48 ページ)
- 内部証明書オブジェクトの使用(2-49 ページ)

内部認証局オブジェクトの使用

ライセンス：任意

設定されたそれぞれの内部認証局（CA）オブジェクトは、組織で制御される CA の CA 公開鍵証明書を表します。このオブジェクトは、オブジェクト名、CA 証明書、およびペアになった秘密鍵からなります。SSL ルールで内部 CA オブジェクトとグループ（オブジェクトのグループ化（2-2 ページ）を参照）を使用すると、内部 CA によってサーバ証明書に再署名することにより、発信する暗号化トラフィックを復号できます。

（注）　[復号 - 再署名（Decrypt - Resign）] SSL ルールで内部 CA オブジェクトを参照する場合、ルールが暗号化セッションに一致すると、SSL ハンドシェイクのネゴシエート中は証明書を信頼できないという警告がユーザのブラウザに表示されることがあります。これを回避するには、信頼できるルート証明書のクライアントまたはドメイン リストに内部 CA オブジェクト証明書を追加します。

次の方法で内部 CA オブジェクトを作成できます。

- RSA ベースまたは楕円曲線ベースの既存の CA 証明書と秘密キーをインポートする
- 新しい RSA ベースの自己署名 CA 証明書と秘密キーを生成する
- RSA ベースの未署名の CA 証明書と秘密キーを生成する。内部 CA オブジェクトを使用する前に、証明書に署名するために証明書署名要求（CSR）を別の CA に送信する必要があります。

署名付き証明書を含む内部 CA オブジェクトを作成した後で、CA 証明書と秘密鍵をダウンロードできるようになります。システムは、ダウンロードされた証明書と秘密キーをユーザ提供のパスワードで暗号化します。

システムで生成された場合でも、ユーザによって作成された場合でも、内部 CA オブジェクトの名前は変更できますが、他のオブジェクト プロパティは変更できません。

使用中の内部 CA オブジェクトは削除できません。さらに、SSL ポリシーで使用される内部 CA オブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を反映させるには、アクセス コントロール ポリシーを再適用する必要があります。

詳細については、次の項を参照してください。

- CA 証明書と秘密キーのインポート（2-42 ページ）
- 新しい CA 証明書と秘密キーの生成（2-43 ページ）
- 新しい署名付き証明書の取得およびアップロード（2-44 ページ）
- CA 証明書と秘密キーのダウンロード（2-45 ページ）

CA 証明書と秘密キーのインポート

ライセンス：任意

X.509 v3 CA 証明書と秘密キーをインポートすることによって、内部 CA オブジェクトを設定できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

秘密キー ファイルがパスワード保護されている場合は、復号パスワードを提供できます。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書またはキーの情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

（注）　ルールに [復号 - 再署名（Decrypt - Resign）] アクションを設定すると、そのルールでは、設定されているルール条件に加えて、参照される内部 CA 証明書の暗号化アルゴリズムのタイプに基づいてトラフィックが照合されます。たとえば、楕円曲線ベースのアルゴリズムで暗号化された発信トラフィックを復号するには、楕円曲線ベースの CA 証明書をアップロードする必要があります。詳細については、復号アクション: さらに検査するためにトラフィックを復号（13-11 ページ）を参照してください。

内部 **CA** 証明書と秘密鍵をインポートする方法:

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ **2**　[PKI] で、[内部 CA（Internal CAs）] を選択します。

ステップ **3**　[CA のインポート（Import CA）] をクリックします。

[内部認証局のインポート（Import Internal Certificate Authority）] ポップアップ ウィンドウが表示されます。

ステップ **4**　[名前（Name）] に、内部 CA オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ **5**　[証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ **6**　[キー（Key）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

ステップ **7**　アップロード ファイルがパスワード保護されている場合は、[暗号化済み、パスワード: （Encrypted, and the password is:）] チェック ボックスをオンにして、パスワードを入力します。

ステップ **8**　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

内部 CA オブジェクトが追加されます。

新しい **CA** 証明書と秘密キーの生成

ライセンス: 任意

識別情報を提供することにより、RSA ベースの自己署名 CA 証明書と秘密キーを生成するように内部 CA オブジェクトを設定できます。次の表に、証明書を生成するために提供する識別情報について説明します。

表 ***2-9***　生成される内部 ***CA*** の属性

フィールド	使用可能な値	必須
国名（Country Name）（2 文字コード）	2 つの英字	はい
都道府県（State or Province）	最大 64 文字の英数字、バックスラッシュ（\）、ハイフン（-）、引用符（"）、アスタリスク（*）、ピリオド（.）、スペース文字	いいえ
市区町村（Locality or City）		
組織（Organization）		
組織部門（Organizational Unit）		
共通名（Common Name）		

生成される CA 証明書の有効期間は 10 年です。[有効期間の開始（Valid From）] の日付は、生成の一週間前です。

自己署名 **CA** 証明書の生成方法:

ステップ **1** [設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ **2** [PKI] で、[内部 CA（Internal CAs）] を選択します。

ステップ **3** [CA の生成（Generate CA）] をクリックします。

[内部認証局の生成（Generate Internal Certificate Authority）] ポップアップ ウィンドウが表示されます。

ステップ **4** [名前（Name）] に、内部 CA オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ **5** 表 2-9（ 2-43 ページ）の説明に従って、識別属性を入力します。

ステップ **6** [自己署名 CA の生成（Generate self-signed CA）] をクリックします。

内部 CA オブジェクトが追加されます。

新しい署名付き証明書の取得およびアップロード

ライセンス:任意

署名付き証明書を CA から取得することによって、内部 CA オブジェクトを設定できます。これは、次の 2 段階からなります。

- 内部 CA オブジェクトを設定するための識別情報を指定します。これにより、未署名の証明書およびペアになった秘密鍵が生成され、指定した CA に対する証明書署名要求（CSR）が作成されます。
- CA により署名付き証明書が発行されたら、それを内部 CA オブジェクトにアップロードして、未署名の証明書と置き換えます。

署名付き証明書が含まれている場合にのみ、SSL ルールで内部 CA オブジェクトを参照できます。

未署名の **CA** 証明書と **CSR** を作成する方法:

ステップ **1** [設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ **2** [PKI] で、[内部 CA（Internal CAs）] を選択します。

ステップ **3** [CA の生成（Generate CA）] をクリックします。

[内部認証局の生成（Generate Internal Certificate Authority）] ポップアップ ウィンドウが表示されます。

ステップ **4** [名前（Name）] に、内部 CA オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ **5** 表 2-9（ 2-43 ページ）の説明に従って、識別属性を入力します。

ステップ **6** [CSR の作成（Generate CSR）] をクリックします。

[内部認証局の生成（Generate Internal Certificate Authority）] ポップアップ ウィンドウが表示されます。

ステップ 7　CA に送信するために CSR をコピーします。

ステップ 8　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

CA オブジェクトが作成されます。これを使用する前に、まず CA によって発行された署名付き証明書をアップロードする必要があることに注意してください。

CSR への応答として発行された署名付き証明書をアップロードする方法:

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ 2　[PKI] で、[内部 CA（Internal CAs）] を選択します。

ステップ 3　CSR を待機している未署名の証明書を含む CA オブジェクトの横の編集アイコン（ ）をクリックします。

[内部認証局の編集（Edit Internal Certificate Authority）] ポップアップ ウィンドウが表示されます。

ステップ 4　[証明書のインストール（Install Certificate）] をクリックします。

[内部認証局のインストール（Install Internal Certificate Authority）] ポップアップ ウィンドウが表示されます。

ステップ 5　[証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6　アップロードされるファイルがパスワード保護されている場合は、[暗号化済み、パスワード:（Encrypted, and the password is:）] チェック ボックスを選択し、パスワードを入力します。

ステップ 7　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

CA オブジェクトに署名付き証明書が含まれ、SSL ルールでこれを参照できます。

CA 証明書と秘密キーのダウンロード

ライセンス:任意

証明書および鍵の情報を含むファイルを内部 CA オブジェクトからダウンロードすることにより、CA 証明書およびペアになった秘密鍵をバックアップまたは転送できます。

注意　ダウンロードされた鍵情報は必ず安全な場所に保存してください。

システムは、内部 CA オブジェクトに保存されている秘密鍵をディスクに保存する前に、ランダムに生成された鍵を使って暗号化します。証明書および秘密鍵を内部 CA オブジェクトからダウンロードすると、システムはまず情報を復号してから、証明書および秘密鍵の情報を含むファイルを作成します。その後、ダウンロード ファイルを暗号化するためにシステムで使われるパスワードを提供する必要があります。

注意　システム バックアップの一部としてダウンロードされる秘密鍵は、復号されてから、非暗号化バックアップ ファイルに保存されます。詳細については、バックアップ ファイルの作成（45-1 ページ）を参照してください。

内部 **CA** 証明書と秘密鍵をダウンロードする方法:

ステップ **1** [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [オブジェクト管理(Object Management)] の順に選択します。

[オブジェクト管理(Object Management)] ページが表示されます。

ステップ **2** [PKI] で、[内部 CA(Internal CAs)] を選択します。

ステップ **3** 証明書および秘密鍵をダウンロードする対象となる内部 CA オブジェクトの横の編集アイコン( )をクリックします。

[内部認証局の編集(Edit Internal Certificate Authority)] ポップアップ ウィンドウが表示されます。

ステップ **4** [ダウンロード(Download)] をクリックします。

[ダウンロード ファイルの暗号化(Encrypt Download File)] ポップアップ ウィンドウが表示されます。

ステップ **5** [パスワード(Password)] および [パスワードの確認(Confirm Password)] フィールドに、暗号化パスワードを入力します。

ステップ **6** [ASA FirePOWER の変更の保存(Store ASA FirePOWER Changes)] をクリックします。

ファイルを保存するよう求められます。

信頼できる認証局オブジェクトの使用

ライセンス:任意

設定済みの、信頼できる認証局(CA)オブジェクトはそれぞれ、組織外の信頼できる CA に属する CA 公開鍵証明書を表します。このオブジェクトは、オブジェクト名と CA 公開鍵証明書からなります。SSL ポリシーで外部 CA オブジェクトとグループ(オブジェクトのグループ化(2-2 ページ)を参照)を使用すると、信頼できる CA またはトラスト チェーン内の任意の CA によって署名された証明書を使って暗号化されたトラフィックを制御できます。

信頼できる CA オブジェクトを作成した後で、その名前を変更したり、証明書失効リスト(CRL)を追加したりすることはできますが、他のオブジェクト プロパティを変更することはできません。オブジェクトに追加できる CRL の数には制限がありません。オブジェクトにアップロード済みの CRL を変更するには、オブジェクトをいったん削除して再作成する必要があります。

使用中の信頼できる CA オブジェクトを削除することはできません。さらに、SSL ポリシーで使用されている信頼できる CA オブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を反映させるには、アクセス コントロール ポリシーを再適用する必要があります。

詳細については、次の項を参照してください。

- 位置情報オブジェクトの操作(2-50 ページ)
- 信頼できる CA オブジェクトへの証明書失効リストの追加(2-47 ページ)

信頼できる **CA** オブジェクトの追加

ライセンス:任意

X.509 v3 CA 証明書をアップロードすることによって、外部 CA オブジェクトを設定できます。次のサポートされている形式のいずれかでエンコードしたファイルをアップロードできます。

- 識別符号化規則(DER)
- プライバシー強化電子メール(PEM)

ファイルがパスワード保護されている場合は、復号パスワードを提供する必要があります。証明書が PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

ファイルに適切な証明書情報が含まれる場合にのみ、CA 証明書をアップロードできます。システムはオブジェクトを保存する前に証明書を検証します。

信頼できる **CA** 証明書をインポートする方法:

ステップ **1** [設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ **2** [PKI] で、[信頼できる CA（Trusted CAs）] を選択します。

ステップ **3** [信頼できる CA の追加（Add Trusted CAs）] をクリックします。

[信頼できる認証局のインポート（Import Trusted Certificate Authority）] ポップアップ ウィンドウが表示されます。

ステップ **4** [名前（Name）] に、信頼できる CA オブジェクトの名前を入力します。縦線（|）と中カッコ（{ }）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ **5** [証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ **6** ファイルがパスワード保護されている場合は、[暗号化済み、パスワード:（Encrypted, and the password is:）] チェック ボックスをオンにして、パスワードを入力します。

ステップ **7** [ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

信頼できる CA オブジェクトが追加されます。

信頼できる **CA** オブジェクトへの証明書失効リストの追加

ライセンス:任意

信頼できる CA オブジェクトに CRL をアップロードできます。信頼できる CA オブジェクトを SSL ポリシーの中で参照すると、セッションの暗号化証明書を発行した CA がその後で証明書を取り消したかどうかに基づいて、暗号化されたトラフィックを制御できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

CRL を追加した後、失効した証明書のリストを表示することができます。オブジェクトにアップロード済みの CRL を変更するには、オブジェクトをいったん削除して再作成する必要があります。

適切な CRL を含んでいるファイルのみをアップロードできます。信頼できる CA オブジェクトに追加できる CRL の数には制限がありません。ただし、CRL をアップロードした場合、別の CRL を追加する前に、オブジェクトをその都度保存する必要があります。

CRL をアップロードする方法:

ステップ **1** [設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ 2　[PKI] で、[信頼できる CA（Trusted CAs）] を選択します。

ステップ 3　信頼できる CA オブジェクトの横にある編集アイコン（）をクリックします。

[信頼できる認証局の編集（Edit Trusted Certificate Authority）] ポップアップ ウィンドウが表示されます。

ステップ 4　[CRL の追加（Add CRL）] をクリックして、DER または PEM でエンコードされた CRL ファイルをアップロードします。

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

変更が保存されます。

外部証明書オブジェクトの使用

ライセンス：任意

設定済みのそれぞれの外部証明書オブジェクトは、組織に属さないサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名と証明書からなります。SSL ルールで外部証明書オブジェクトとグループ（オブジェクトのグループ化（2-2 ページ）を参照）を使用すると、サーバ証明書で暗号化されたトラフィックを制御できます。たとえば、信頼できる自己署名サーバ証明書をアップロードできますが、信頼できる CA 証明書を使って検証することはできません。

X.509 v3 サーバ証明書をアップロードすることによって、外部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

適切なサーバ証明書情報を含んでいるファイルだけをアップロードできます。システムはオブジェクトを保存する前にファイルを検証します。証明書が PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

外部証明書オブジェクトを作成した後、その名前を変更することはできますが、他のオブジェクト プロパティを変更することはできません。

使用中の外部証明書オブジェクトは削除できません。さらに、SSL ポリシーで使用されている外部証明書オブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を反映させるには、アクセス コントロール ポリシーを再適用する必要があります。

外部証明書オブジェクトを追加する方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ 2　[PKI] で、[外部証明書（External Certs）] を選択します。

ステップ 3　[外部証明書の追加（Add External Cert）] をクリックします。

[既知の外部証明書の追加（Add Known External Certificate）] ポップアップ ウィンドウが表示されます。

ステップ 4　[名前（Name）] に、外部証明書オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　[証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバ証明書ファイルをアップロードします。

ステップ 6　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

内部 CA オブジェクトが追加されます。

内部証明書オブジェクトの使用

ライセンス：任意

設定済みのそれぞれの内部証明書オブジェクトは、組織に属するサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名、公開鍵証明書、およびペアになった秘密鍵からなります。SSL ルールで内部証明書オブジェクトとグループ（オブジェクトのグループ化（2-2 ページ）を参照）を使用すると、既知の秘密鍵を使用して組織のいずれかのサーバに着信するトラフィックを復号することができます。

X.509 v3 RSA ベースまたは楕円曲線ベースのサーバ証明書およびペアの秘密キーをアップロードすることにより、内部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

ファイルがパスワード保護されている場合は、復号パスワードを提供する必要があります。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書またはキーの情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

内部証明書オブジェクトを作成した後、その名前を変更することはできますが、他のオブジェクト プロパティを変更することはできません。

使用中の内部証明書オブジェクトは削除できません。さらに、SSL ポリシーで使用されている内部証明書オブジェクトを編集すると、関連するアクセス コントロール ポリシーが失効します。変更を反映させるには、アクセス コントロール ポリシーを再適用する必要があります。

内部証明書オブジェクトを追加する方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ 2　[PKI] で、[内部証明書（Internal Certs）] を選択します。

ステップ 3　[内部証明書の追加（Add Internal Cert）] をクリックします。

[既知の内部証明書を追加（Add Known Internal Certificate）] ポップアップ ウィンドウが表示されます。

ステップ 4　[名前（Name）] に内部証明書オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　[証明書データ（Certificate Data）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバ証明書ファイルをアップロードします。

ステップ 6　[キー（Key）] フィールドの上部にある [参照（Browse）] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

ステップ 7　アップロードする秘密キー ファイルがパスワード保護されている場合は、[暗号化済み、パスワード：（Encrypted, and the password is:）] チェック ボックスをオンにして、パスワードを入力します。

ステップ 8　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

内部証明書オブジェクトが追加されます。

位置情報オブジェクトの操作

ライセンス：任意

設定済みの位置情報（ジオロケーション）オブジェクトは、モニタ対象ネットワーク上のトラフィックの送信元または宛先としてシステムで識別された 1 つ以上の国または大陸を表します。位置情報オブジェクトを、アクセス コントロール ポリシーで使用できます。たとえば、特定の国が送信元/宛先であるトラフィックをブロックするアクセス コントロール ルールを作成できます。地理的な場所によるトラフィックのフィルタリングについては、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。

常に最新の情報を使用してネットワーク トラフィックをフィルタ処理できるように、シスコ では、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 の更新をダウンロードおよびインストールする方法については、位置情報データベースの更新（43-21 ページ）を参照してください。

使用中の位置情報オブジェクトは削除できません。さらに、アクセス コントロール ポリシーで使用される位置情報オブジェクトを編集した後、変更内容を有効にするにはアクセス コントロール ポリシーを再適用する必要があります。

位置情報オブジェクトを追加する方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [オブジェクト管理（Object Management）] の順に選択します。

[オブジェクト管理（Object Management）] ページが表示されます。

ステップ 2　位置情報を示す [位置情報（Geolocation）] を選択します。

[位置情報オブジェクト（Geolocation Objects）] ページが表示されます。

ステップ 3　[位置情報の追加（Add Geolocation）] をクリックします。

[位置情報オブジェクト（Geolocation Object）] ポップアップ ウィンドウが表示されます。

ステップ 4　[名前（Name）] に、位置情報オブジェクトの名前を入力します。中カッコ（{}）を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5　位置情報オブジェクトに含める国および大陸のチェック ボックスを選択します。

大陸を選択すると、その大陸内のすべての国、および 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選択されます。大陸の下でいずれかの国を選択解除すると、その大陸が選択解除されます。国と大陸を任意に組み合わせて選択できます。

ステップ 6　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

位置情報オブジェクトが追加されます。

デバイス設定の管理

[デバイス管理(Device Management)] ページでは、ASA FirePOWER モジュールのデバイスおよびインターフェイスの設定を管理することができます。

注意 フェールオーバーのペアで ASA を設定した場合、ASA FirePOWER の設定は、セカンダリ デバイス上の ASA FirePOWER モジュール に自動的に同期されません。設定を変更するたびに、プライマリから ASA FirePOWER の設定を手動でエクスポートし、それをセカンダリへインポートする必要があります。

詳細については、次の項を参照してください。

- デバイス設定の編集(3-1 ページ)
- ASA FirePOWER モジュール インターフェイスの管理(3-4 ページ)
- デバイス設定への変更の適用(3-5 ページ)
- リモート管理の設定(3-6 ページ)
- eStreamer サーバでの eStreamer の設定(3-8 ページ)

デバイス設定の編集

[デバイス管理(Device Management)] ページの [デバイス(Device)] タブには、デバイスが ASA FirePOWER モジュール に適用されたときに詳細なデバイス設定と情報が表示されます。また、このページでは、デバイス設定の一部(表示されるモジュール名の変更および管理設定の変更など)を変更することもできます。

詳細については、次の各項を参照してください。

- 一般的なデバイス設定の編集(3-2 ページ)
- デバイス システム設定の表示(3-2 ページ)
- 高度なデバイス設定について(3-3 ページ)

一般的なデバイス設定の編集

ライセンス：任意

[デバイス（Device）] タブの [一般（General）] セクションに表示されるモジュール名は、変更できます。ここで、デバイスがパケットを ASA FirePOWER モジュール に転送できるかどうかを指定することもできます。

一般的なデバイス設定を編集するには、次の手順を実行します。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [デバイス（Device）] の順に選択します。

[デバイス（Device）] ページが表示されます。

ステップ 2　[一般（General）] セクションの横にある編集アイコン（）をクリックします。

[一般（General）] ポップアップ ウィンドウが表示されます。

ステップ 3　[名前（Name）] フィールドに、モジュールに割り当てる新しい名前を入力します。英数字と特殊文字を入力できます。ただし、+、(、)、{、}、#、&、\、<、>、?、‘、および “ の文字は無効です。

ステップ 4　パケット データをイベントと一緒に ASA FirePOWER モジュール に保存できるようにするには、[パケットの転送（Transfer Packets）] チェック ボックスをオンにします。デバイスがイベントと一緒にパケット データを送信できないようにするには、このチェック ボックスをオフにします。

ステップ 5　[保存（Save）] をクリックします。

これにより、変更内容が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイス設定への変更の適用（3-5 ページ）を参照してください）。

デバイス システム設定の表示

ライセンス：任意

[デバイス（Device）] タブの [システム（System）] セクションには、次の表に示すように、システム情報の読み取り専用テーブルが表示されます。

表 *3-1*　*[システム（System）]* セクション テーブルのフィールド

フィールド	説明
モデル	デバイスのモデル名と番号。
シリアル（Serial）	デバイスのシャーシのシリアル番号。
時刻（Time）	デバイスの現在のシステム時刻。
バージョン（Version）	ASA FirePOWER モジュール に現在インストールされているソフトウェアのバージョン。
ポリシー	ASA FirePOWER モジュール に現在適用されているシステム ポリシーへのリンク。

高度なデバイス設定について

[デバイス（Device）] タブの [詳細設定（Advanced）] セクションには、次の表に示すように、構成時の詳細設定が表示されます。

表 *3-2*　*[詳細設定（**Advanced**）]* セクション テーブルのフィールド

フィールド	説明
アプリケーション バイパス（Application Bypass）	モジュールでの自動アプリケーション バイパスの状態。
バイパスしきい値（Bypass Threshold）	自動アプリケーション バイパスのしきい値（ミリ秒）。

上記の設定は、いずれも [詳細設定（Advanced）] セクションを使用して編集できます。詳細については、次の各項を参照してください。

- 自動アプリケーション バイパス（3-3 ページ）
- 詳細なデバイス設定の編集（3-3 ページ）

自動アプリケーション バイパス

ライセンス：任意

自動アプリケーション バイパス（AAB）機能は、インターフェイスでのパケット処理時間に制限を設け、この時間を超過した場合、パケットに検出のバイパスを許可します。この機能は任意の展開で使用できますが、インライン展開ではとりわけ価値があります。

パケット処理の遅延は、ネットワークで許容できるパケット レイテンシとバランスを取って調整します。Snort 内での不具合やデバイスの誤った設定が原因で、トラフィックの処理時間が指定のしきい値を超えると、AAB により、その障害発生から 10 分以内に Snort が再起動され、トラブルシューティング データが生成されます。このデータを分析することで、過剰な処理時間の原因を調査できます。

このオプションが選択されている場合は、バイパスしきい値を変更できます。デフォルト設定は 3000 ミリ秒（ms）です。有効な範囲は 250 ms ～ 60,000 ms です。

（注）　AAB がアクティブ化されるのは、単一パケットに過剰な処理時間がかかっている場合のみです。AAB がアクティブになると、システムはすべての Snort プロセスをキルします。

自動アプリケーション バイパスを有効にしてバイパスしきい値を設定する方法の詳細については、詳細なデバイス設定の編集（3-3 ページ）を参照してください。

詳細なデバイス設定の編集

[デバイス（Devices）] タブの [詳細設定（Advanced）] セクションを使用して、自動アプリケーション バイパスを変更できます。

詳細なデバイス設定を変更するには、以下を行います。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [デバイス（Device）] の順に選択します。

[デバイス（Device）] ページが表示されます。

ステップ 2　[詳細設定（Advanced）] セクションの横にある編集アイコン（）をクリックします。

[詳細設定（Advanced）] ポップアップ ウィンドウが表示されます。

ステップ 3　ネットワークがレイテンシの影響を受けやすい場合は、必要に応じて、[自動アプリケーション バイパス（Automatic Application Bypass）] を選択します。自動アプリケーション バイパスは、インライン展開でとりわけ役立ちます。詳細については、自動アプリケーション バイパス（3-3 ページ）を参照してください。

ステップ 4　[自動アプリケーション バイパス（Automatic Application Bypass）] オプションを選択すると、[バイパスしきい値（Bypass Threshold）] にバイパスしきい値（ミリ秒）を入力できるようになります。デフォルト設定は 3000 ms です。有効な範囲は 250 ms ～ 60,000 ms です。

ステップ 5　[保存（Save）] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイス設定への変更の適用（3-5 ページ）を参照してください）。

ASA FirePOWER モジュール インターフェイスの管理

ライセンス：Control、防御

ASA FirePOWER インターフェイスを編集する際に、ASA FirePOWER モジュール から設定できるのは、インターフェイスのセキュリティ ゾーンのみです。詳細については、セキュリティ ゾーンの操作（2-37 ページ）を参照してください。

ASDM および CLI を使用してインターフェイスを設定します。

ASA FirePOWER インターフェイスを編集するには、以下を行います。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] の順に選択します。

[インターフェイス（Interfaces）] ページが表示されます。

ステップ 2　編集するインターフェイスの横にある編集アイコン（）をクリックします。

[インターフェイスの編集（Edit Interface）] ポップアップ ウィンドウが表示されます。

ステップ 3　[セキュリティ ゾーン（Security Zone）] ドロップダウンリストから、既存のセキュリティ ゾーンを選択するか、または [新規（New）] を選択して、新しいセキュリティ ゾーンを追加します。

ステップ 4　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

セキュリティ ゾーンが設定されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイス設定への変更の適用（3-5 ページ）を参照してください）。

デバイス設定への変更の適用

ライセンス:任意

デバイスの ASA FirePOWER 設定に変更を加えた後、それらの変更を適用するまでは、モジュール全体に変更が反映されません。デバイスが変更適用前の状態でなければ、このオプションは無効になります。

インターフェイスを編集してデバイス ポリシーを再適用すると、編集したインターフェイス インスタンスだけでなく、デバイス上のすべてのインターフェイス インスタンスで Snort が再起動することに注意してください。

変更をデバイスに適用するには、以下を行います。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [デバイス（Device）] または [設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] の順に選択します。

[デバイス管理（Device Management）] ページが表示されます。

ステップ 2　[ASA FirePOWER 変更の適用（Apply ASA FirePOWER Changes）] をクリックします。

ステップ 3　プロンプトが出されたら、[適用（Apply）] をクリックします。

デバイスの変更が適用されます。

ヒント　必要に応じて、[デバイス変更の適用（Apply Device Changes）] ダイアログ ボックスで [変更の表示（View Changes）] をクリックします。新しいウィンドウに [デバイス管理のレビジョン比較レポート（Device Management Revision Comparison Report）] ページが表示されます。詳細については、デバイス管理のリビジョン比較レポートの使用（3-5 ページ）を参照してください。

ステップ 4　[OK] をクリックします。

[デバイス管理（Device Management）] ページに戻ります。

デバイス管理のリビジョン比較レポートの使用

ライセンス:任意

デバイス管理の比較レポートを使用して、変更を確認してから、アプライアンスに適用できます。このレポートには、現在のアプライアンスの設定と、変更適用後のアプライアンスの設定との間の差異がすべて表示されます。これにより、設定の潜在的なエラーを検出することができます。

変更適用前と適用後のアプライアンスを比較するには、以下を行います。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [デバイス（Device）] または [設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] の順に選択します。

[デバイス管理（Device Management）] ページが表示されます。

ステップ 2　[変更を適用（Apply Changes）] をクリックします。

[デバイス変更の適用（Apply Device Changes）] ポップアップ ウィンドウが表示されます。アプライアンスが変更適用前の状態でなければ、[変更を適用（Apply Changes）] ボタンは無効のままになります。

ステップ 3　[変更の表示（View Changes）] をクリックします。

新しいウィンドウに [デバイス管理のレビジョン比較レポート（Device Management Revision Comparison Report）] ページが表示されます。

ステップ 4　[前へ（Previous）] と [次へ（Next）] をクリックして、現在のアプライアンスの設定と変更適用後のアプライアンスの設定との間のすべての差異を確認します。

ステップ 5　必要に応じて、レポートの PDF バージョンを生成するには、[比較レポート（Comparison Report）] をクリックします。

リモート管理の設定

ライセンス：任意

ある FireSIGHT システム アプライアンスと別のアプライアンスを相互に管理できるようにするには、その前に、2 つのアプライアンスの間に双方向の SSL 暗号化通信チャネルをセットアップする必要があります。このチャネルを使用して、両方のアプライアンスが設定とイベント情報を共有します。ハイ アベイラビリティ ピアも、このチャネルを使用します。このチャネルは、デフォルトではポート 8305/tcp に位置します。

管理対象のアプライアンス、つまり防御センターで管理するデバイス上には、リモート管理を設定する必要があります。リモート管理を設定した後、管理側アプライアンスの Web インターフェイスを使用して、管理対象アプライアンスを展開環境に追加できます。

（注）　リモート管理を確立して、防御センター に Cisco ASA with FirePOWER Services を登録した後、ASDM の代わりに 防御センター から ASA FirePOWER モジュール を管理する必要があります。

2 つのアプライアンス間の通信を可能にするためには、アプライアンスが互いを認識する手段を提供しなければなりません。通信を許可するために、FireSIGHT システムでは 3 つの基準を使用します。

- 通信を確立する対象のアプライアンスのホスト名または IP アドレス

  NAT 環境では、ルーティング可能なアドレスがもう一方のアプライアンスにないとしても、リモート管理を設定する際、または管理対象アプライアンスを追加する際には、ホスト名または IP アドレスのいずれかを指定する必要があります。

- 接続を識別するために自己生成される、最大 37 文字の英数字による登録キー
- FireSIGHT システムが NAT 環境で通信を確立するために利用できる、オプションの一意の英数字による NAT ID

  NAT ID は、管理対象アプライアンスを登録するために使用されているすべての NAT ID の間で一意でなければなりません。

管理対象デバイスを防御センターに登録すると、ユーザが選択したアクセス コントロール ポリシーがデバイスに適用されます。ただし、選択したアクセス コントロール ポリシーで使用される機能に必要なライセンスがデバイスで有効になっていなければ、アクセス コントロール ポリシーの適用は失敗します。

ローカル アプライアンスのリモート管理を設定するには、以下を行います。

アクセス：Admin

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ローカル（Local）] > [設定（Configuration）] > [登録（Registration）] の順に選択します。

[リモート管理（Remote Management）] ページが表示されます。

ステップ 2　[マネージャの追加（Add Manager）] をクリックします。

[リモート管理の追加（Add Remote Management）] ページが表示されます。

ステップ 3　[管理ホスト（Management Host）] に、このアプライアンスを管理するために使用するアプライアンスの IP アドレスまたはホスト名を入力します。

ホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。

NAT 環境では、管理対象アプライアンスを追加する際に IP アドレスまたはホスト名を指定する予定の場合、ここで IP アドレスまたはホスト名を指定する必要はありません。その場合、FireSIGHT システム は後で指定される NAT ID を使用して、管理対象 ASA FirePOWER モジュール インターフェイス上のリモート マネージャを識別します。

注意　ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

ステップ 4　[登録キー（Registration Key）] フィールドに、アプライアンス間の通信をセットアップするために使用する登録キーを入力します。

ステップ 5　NAT 環境の場合は、[固有 NAT ID（Unique NAT ID）] フィールドに、アプライアンス間の通信をセットアップするために使用する、英数字による一意の NAT ID を入力します。

ステップ 6　[保存（Save）] をクリックします。

アプライアンスが相互に通信できることを確認すると、ステータスとして [登録保留（Pending Registration）] が表示されます。

ステップ 7　管理側アプライアンスの Web ユーザ インターフェイスを使用して、このアプライアンスを展開環境に追加します。

（注）　NAT を使用する一部のハイ アベイラビリティ展開では、デバイスのリモート管理を有効にする際に、セカンダリ防御センターをマネージャとして追加しなければならない場合もあります。詳細については、サポートにお問い合わせください。

リモート管理の編集

ライセンス：任意

管理側アプライアンスのホスト名または IP アドレスを編集するには、以下の手順を使用します。また、管理側アプライアンスの表示名を変更することもできます。表示名は、FireSIGHT システムのコンテキスト内でのみ使用されます。ホスト名をアプライアンスの表示名として使用することもできますが、別の表示名を入力してもホスト名は変更されません。

リモート管理を編集するには、以下を行います。

アクセス：Admin

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ローカル（Local）] > [設定（Configuration）] > [登録（Registration）] の順に選択します。

[リモート管理（Remote Management）] ページが表示されます。

ステップ 2　リモート管理設定を編集するマネージャの横にある編集アイコン（）をクリックします。

[リモート管理の編集（Edit Remote Management）] ページが表示されます。

ステップ 3　[名前（Name）] フィールドで、管理側アプライアンスの表示名を変更します。

ステップ 4　[ホスト（Host）] フィールドで、管理側アプライアンスの IP アドレスまたはホスト名を変更します。

ホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。

ステップ 5　[保存（Save）] をクリックします。

変更が保存されます。

eStreamer サーバでの eStreamer の設定

ライセンス：FireSIGHT + Protection

eStreamer サーバとして使用するアプライアンスで eStreamer イベントの外部クライアントへのストリームを開始するには、その前に、イベントをクライアントに送信するように eStreamer サーバを設定し、クライアントに関する情報を指定して、通信を確立するときに使用する認証クレデンシャルを生成する必要があります。

eStreamer イベント タイプの設定

要求したクライアントに eStreamer サーバが送信できるイベント タイプを制御できます。

管理対象デバイスまたは防御センターのいずれかで使用可能なイベント タイプは、以下のとおりです。

- 侵入イベント
- 侵入イベント パケット データ
- 侵入イベント追加データ

eStreamer によって送信されるイベントのタイプを設定する方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ローカル（Local）] > [設定（Configuration）] > [登録（Registration）] の順に選択します。

[登録（Registration）] ページが表示されます。

ステップ 2　[eStreamer] タブを選択します。

[eStreamer] ページが表示されます。

ステップ 3　[eStreamer イベント構成（eStreamer Event Configuration）] の下で、eStreamer から要求元のクライアントに転送するイベントのタイプの横にあるチェック ボックスをオンにします。

管理対象デバイスまたは防御センターで、次のいずれかまたはすべてを選択できます。

- [侵入イベント（Intrusion Events）]：侵入イベントを送信します。
- [侵入イベント パケット データ（Intrusion Event Packet Data）]：侵入イベントに関連付けられたパケットを送信します。
- [侵入イベント追加データ（Intrusion Event Extra Data）]：HTTP プロキシまたはロード バランサ経由で Web サーバに接続しているクライアントの発信元 IP アドレスのような侵入イベントに関連付けられた追加データを送信します。

（注）　これは、eStreamer サーバが送信できるイベントを制御することに注意してください。クライアントは、eStreamer サーバに送信する要求メッセージで受信するイベント タイプを具体的に要求する必要があります。詳細については、『*FireSIGHT* システム *eStreamer Integration Guide*』を参照してください。

ステップ **4**　[保存（Save）] をクリックします。

設定が保存され、選択したイベントが、要求時に、eStreamer クライアントに転送されます。

eStreamer クライアントの認証の追加

eStreamer がクライアントに eStreamer イベントを送信するには、その前に、eStreamer ページから eStreamer サーバのピア データベースにクライアントを追加しておく必要があります。また、eStreamer サーバによって生成された認証証明書をクライアントにコピーする必要もあります。

eStreamer クライアントを追加する方法：

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ローカル（Local）] > [設定（Configuration）] > [登録（Registration）] の順に選択します。

[登録（Registration）] ページが表示されます。

ステップ **2**　[eStreamer] タブを選択します。

[eStreamer] ページが表示されます。

ステップ **3**　[クライアントの作成（Create Client）] をクリックします。

[クライアントの作成（Create Client）] ページが表示されます。

ステップ **4**　[ホスト名（Hostname）] フィールドに、eStreamer クライアントを実行しているホストのホスト名または IP アドレスを入力します。

（注）　ホスト名を使用する場合、eStreamer サーバはホストを IP アドレスに解決できる必要があります。DNS 解決を設定していない場合、最初に設定するか、IP アドレスを使用する必要があります。

ステップ **5**　証明書ファイルを暗号化するには、[パスワード（Password）] フィールドにパスワードを入力します。

ステップ **6**　[保存（Save）] をクリックします。

これで、eStreamer サーバは、ホストが eStreamer サーバ上のポート 8302 にアクセスすることを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。新しいクライアントが [ホスト名（Hostname）] の下に表示された状態で、[eStreamer] ページが再表示されます。

ステップ 7　クライアントのホスト名の横にあるダウンロード アイコン( )をクリックして、証明書ファイルをダウンロードします。

ステップ 8　SSL 認証のためにクライアントが使用する適切なディレクトリに証明書ファイルを保存します。

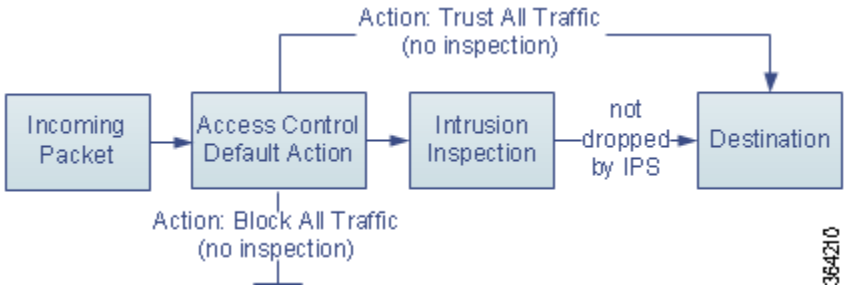
これで、クライアントは eStreamer に接続できるようになりました。eStreamer サービスを再起動する必要はありません。

ヒント　クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン( )をクリックします。eStreamer サービスを再起動する必要はありません。アクセスはただちに取り消されます。

アクセス コントロール ポリシーの開始

アクセス コントロール ポリシーは、ネットワーク上のトラフィックを、システムでどのように処理するかを決定します。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、詳細な検査を行わずにすべてのトラフィックをブロックまたは信頼するように設定することも、侵入についてトラフィックを検査するように設定することもできます。



インライン展開されたASA FirePOWER モジュール だけがトラフィックのフローに影響を与える可能性が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、前処理、パフォーマンス、および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（15-1 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できるしくみについて説明します。
- 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（10-1 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 でのライセンスに関係なく作成できますが、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の要件（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の要件

アクセス コントロール ポリシーは ASA FirePOWER モジュール でのライセンスに関係なく作成できます。ただし、アクセス コントロールの一部として、ポリシーを適用する前に特定のライセンス交付対象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。詳細については、警告アイコンの上にポインタを置き、アクセス コントロール ポリシーおよびルールのトラブルシューティング（4-13 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際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の要件

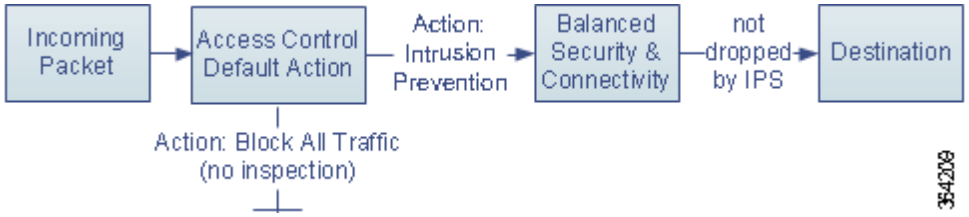
以下を実行するアクセス コントロール ポリシーを適用する場合	ライセンス
ゾーン、ネットワーク、またはポートに基づいてアクセス コントロールを実行する リテラル URL および URL オブジェクトを使用して URL フィルタリングを実行する	任意
位置情報データ（発信元または宛先の国/大陸）に基づいてアクセス コントロールを実行する	任意
侵入検知および侵入防御、ファイル制御、またはセキュリティ インテリジェンス フィルタリングを実行する	Protection
高度なマルウェア防御としてネットワークベースのマルウェア検出およびブロッキングを実行する	マルウェア
ユーザ制御またはアプリケーショ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

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 アクションによって、ASA FirePOWER モジュール がすべてのトラフィックを処理する方法が決定されます。トラフィック フローに影響する他の設定は後から追加します。

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、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ブロックするか、トラフィックを検査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:

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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、デフォルト処理の設定およびネットワーク トラフィックのインスペクション（4-5 ページ）を参照してください。

ステップ 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（4-8 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（4-12 ページ）を参照してください。

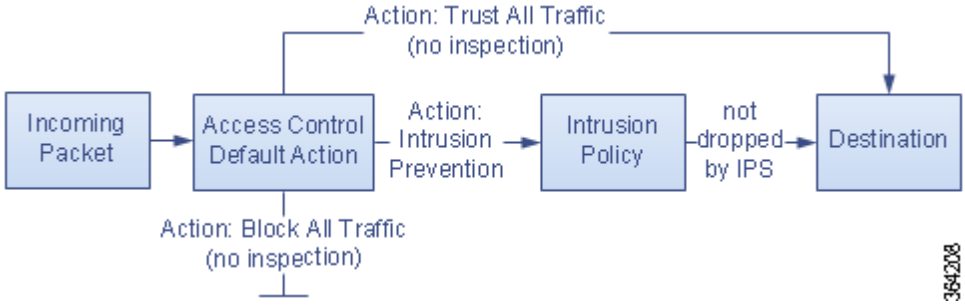
デフォルト処理の設定およびネットワーク トラフィックのインスペクション

ライセンス:任意

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 アクションは、次のトラフィックをシステムで処理する方法を決定します。

- セキュリティ インテリジェンスによってブラックリスト登録されていないトラフィック
- ポリシー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いないアクセス コントロール ポリシーを適用すると、デフォルト アクションによって、ネットワーク上のすべてのトラフィックの処理方法が決定されます。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ブロックまたは信頼するか、あるいは侵入の有無についてトラフィックを検査できます。オプションを次の図に示します。

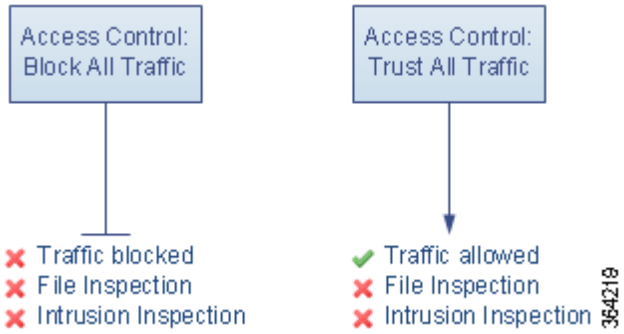


次の表に、さまざまなデフォルト アクションがトラフィックを処理する方法を示し、各デフォルト アクションで処理されるトラフィックで実行できるインスペクションのタイプを示します。デフォルト アクションで処理されるトラフィックに対しては、ファイルやマルウェアのインスペクションを実行できないので注意してください。詳細については、侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（10-1 ページ）を参照してください。

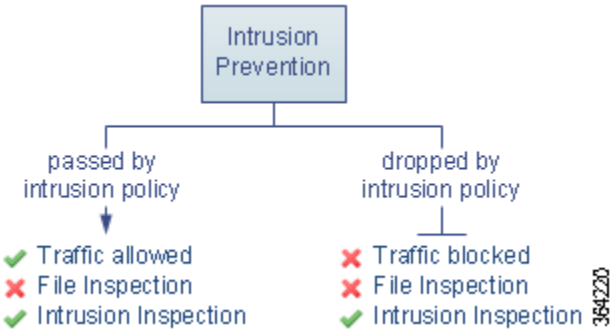
表 **4-2**　　アクセス コントロール ポリシーのデフォルト アクション

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（Access Control: Block All Traffic）	それ以上のインスペクションは行わずにブロックする	なし
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）	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（Intrusion Prevention）	ユーザが指定した侵入ポリシーに合格する限り、許可する（Protection ライセンスが必要）	侵入（intrusion）、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（Block All Traffic）] および [すべてのトラフィックを信頼（Trust All Traffic）] デフォルト アクションを示しています。



次の図は、[侵入防御（Intrusion Prevention）] のデフォルト アクションを説明しています。



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。

ステップ 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。

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

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。

ステップ 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。
- 侵入ポリシーを使用してすべてのトラフィックを検査するには、侵入ポリシーを選択します。いずれの侵入ポリシーも **Intrusion Prevention** というラベルから始まっています。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。

ステップ 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、変数セットの使用（2-15 ページ）を参照してください。

ステップ 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。

接続の開始時点と終了時点で一致する接続をロギングできます。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。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 サーバに接続をロギングできます。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た接続のロギング（33-12 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

[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、現在のカスタム アクセス コントロール ポリシーをポリシー適用の有無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（4-8 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（4-12 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場所にインポートする ASA FirePOWER モジュール	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）

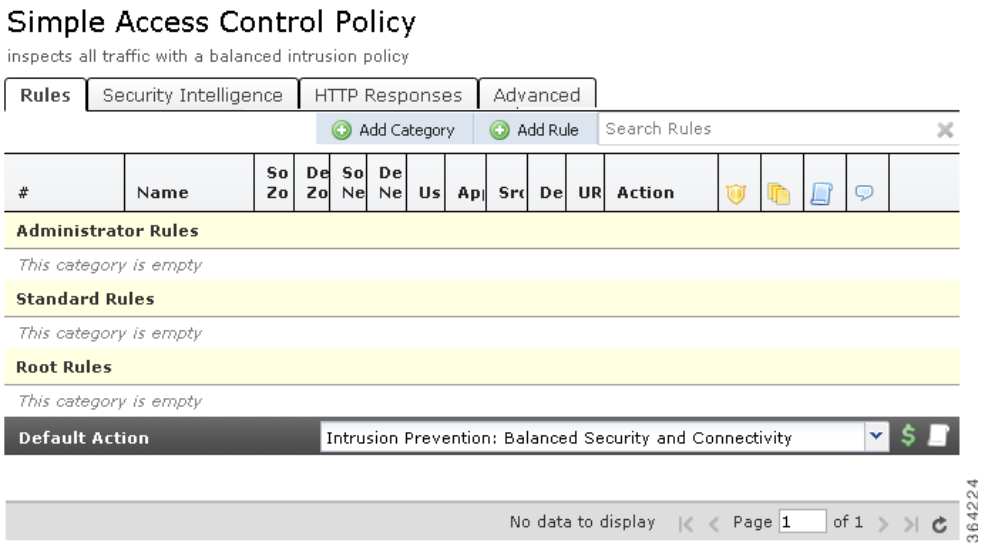
表 *4-3*　アクセス コントロール ポリシーの管理操作（続き）

目的	操作	参照先
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（4-17 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（4-18 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

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。



ルールの追加および整理などを行うには、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ています。この条件は単純または複雑のどちらでも構いません。その使用法は特定のライセンスによって異なります。

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 アクションを使用して、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ブロックまたは信頼することができます。また、侵入の有無についてトラフィックを検査することもできます。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、デフォルト処理の設定およびネットワーク トラフィックのインスペクション（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（33-10 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、ブロックされた URL のカスタム Web ページの表示（8-15 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。

- ユーザが要求した各 URL に対し、ASA FirePOWER モジュール データベースに保存される文字数。接続で検出された URL のロギング（33-14 ページ）を参照してください。
- ユーザが最初のブロックをバイパスした後に Web サイトを再度ブロックするまでの時間間隔。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（8-15 ページ）を参照してください。

- ネットワーク分析および侵入ポリシーの設定。この設定を使用して、ネットワークやゾーンに合わせて多くの前処理オプションを調整したり、侵入インスペクションのデフォルト動作を設定することができます。トラフィックの前処理のカスタマイズ（17-1 ページ）を参照してください。
- 転送およびネットワーク プリプロセッサの詳細設定。この設定は、アクセス コントロール ポリシーを適用する場合に、すべてのネットワークとゾーンにグローバルに適用されます。トランスポート/ネットワークの詳細設定の構成（21-1 ページ）を参照してください。
- ネットワークのホスト オペレーティング システムに基づいて、パッシブ展開でパケット フラグメントおよび TCP ストリームの再構成を改善する適応型プロファイル。パッシブ展開における前処理の調整（22-1 ページ）を参照してください。
- 侵入インスペクション、ファイル制御、ファイル ストレージ、および高度なマルウェア防御のパフォーマンス オプション。侵入防御パフォーマンスの調整（10-6 ページ）および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（10-17 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:

ステップ 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。

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

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。

ステップ 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。

ステップ 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（4-12 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

[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、失効したポリシーに赤色のステータス テキストが付いています。

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およびファイル ポリシーのいずれかの変更: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、またはアクセス 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、ポート、URL、および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、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、オブジェクト マネージャを使用してセキュリティ ゾーンを変更できます([設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [オブジェクト管理(Object Management)])。

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。

ステップ 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、ポリシーの更新を ASA FirePOWER モジュール が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。

ステップ 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。

ステップ 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（4-18 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（23-9 ページ）を参照してください。

ステップ 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

展開環境の設定に ASA FirePOWER モジュールを使用した後に、その設定に変更を加える場合はいつでも、影響を受けるデバイスに新しい設定を導入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。

ステップ 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。

ステップ 2　[展開（Deploy）] をクリックします。

ステップ 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。

ASA FirePOWER モジュール適用するために最大 5 分の時間がかかります。ASA FirePOWER モジュール含めるまたはアクセス 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。

アクセス コントロール ポリシーおよびルールのトラブルシューティング

ライセンス:任意

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
	error	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を含むポリシーや、設定の誤り(条件で空のオブジェクト グループを使用する、クラウド通信を有効にしないで URL 条件を設定するなど)によってトラフィックを照合できないルールを含むポリシーなど、不適切なポリシーが適用される可能性があります。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、対象の 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(8-13 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（4-14 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（4-15 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（4-15 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、重要なリソースを独占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、ネットワーク トラフィックを評価するために ASA FirePOWER モジュール が使用する拡張基準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の検査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応じて異なります。1 つの侵入ポリシーを各許可ルールおよびインタラクティブ ブロック ルール、さらにデフォルト アクションに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。

サポートされる侵入ポリシーの数を超えた場合は、アクセス コントロール ポリシーを再評価してください。いくつかの侵入ポリシーまたは変数セットを統合したほうがよいでしょう。

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

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

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、マルウェアのインスペクションにはリソースの処理が必要なため、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）よりも前にトラフィックを検査しないルール（信頼、ブロック）を配置することで、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

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合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および 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が提供されます。

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（4-18 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:

ステップ **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。

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

システムによってレポートが生成されます。コンピュータにレポートを保存するようにプロンプトが出されます。

アクセス コントロール ポリシーの比較

ライセンス：任意

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。

  このツールを使用すると、モジュール インターフェイスで両方のポリシーの差異を強調表示して、それらを検討したり操作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（4-18 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（4-19 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

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 (4-19 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

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(4-17 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、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、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:

ステップ **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。

ステップ **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。

ステップ **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。

ステップ 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。

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

比較ビューが表示されます。

ステップ 6　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プロンプトが出されます。

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

悪意のあるインターネット コンテンツに対する第一の防衛ラインとして、ASA FirePOWER モジュールにはセキュリティ インテリジェンス機能があります。これを使用することで、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、リソースを集中的に使用する詳細な分析の必要がなくなります。セキュリティ インテリジェンスのフィルタリングには、Protectionライセンスが必要です。

セキュリティ インテリジェンスは、既知の好ましくないレピュテーションが含まれる IP アドレスを送信元/宛先とするトラフィックをブロックすることにより機能します。このトラフィック フィルタリングは、他のどのポリシー ベースのインスペクション、分析、またはトラフィック処理よりも先に行われます。

IP アドレスでトラフィックを手動で制限することで、セキュリティ インテリジェンス フィルタリングと同様の機能を実行するアクセス コントロール ルールを作成することができます。ただし、アクセス コントロール ルールは対象範囲が広く、設定の難易度が高いだけでなく、動的フィードを使用した自動更新に対応できません。

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たトラフィックは即座にブロックされるため、他のさらなるインスペクションの対象にはなりません(侵入、エクスプロイト、マルウェアなどの有無)。オプションで、セキュリティ インテリジェンス フィルタリングには「モニタ専用」設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブラックリスト登録されたであろう接続をシステムが分析できるだけでなく、ブラックリストに一致する接続がログに記録され、接続終了セキュリティ インテリジェンス イベントが生成されます。

便宜上、シスコはインテリジェンス フィード(時に *Sourcefire* インテリジェンス フィードとも呼ばれます)を提供します。これは、VRT によってレピュテーションに欠けると判断された IP アドレスのコレクションからなり、これらのコレクションは定期的に更新されます。インテリジェンス フィードは、オープン リレー、既知の攻撃者、偽の IP アドレス(bogon)などを追跡します。この機能を組織の固有のニーズに適するようにカスタマイズできます。例を次に示します。

- サードパーティ フィード:インテリジェンス フィードをサードパーティのレピュテーション フィードで補足できます。そのフィードはシステムが シスコ フィードと同様に自動的に更新できます。
- カスタム ブラックリスト:システムは、ユーザが自身のニーズに応じてさまざまな方法で特定の IP アドレスを手動でブラックリスト登録することを許可します。
- セキュリティ ゾーンによるブラックリスト登録の強制:パフォーマンスを向上させるには、スパムのブラックリスト登録を電子メール トラフィックを処理するゾーンに制限するなどして、強制を適用することができます。

- ブラックリスト登録の代わりにモニタリング：特にパッシブ展開で、展開を実装する前のフィードのテストに有用です。違反しているセッションをブロックする代わりに単にモニタして、接続終了イベントを生成できます。
- 誤検出をなくすためのホワイトリスト登録：ブラックリストの範囲が広すぎる場合、または（たとえば、重要なリソースに）許可するトラフィックを誤ってブロックした場合、ブラックリストをカスタム ホワイトリストで上書きできます。

セキュリティ インテリジェンス フィルタリングを実行するためにセキュリティ インテリジェンスを実行するアクセス コントロール ポリシーを設定する方法、およびこのフィルタリングが生成するイベント データを表示する方法については、次の項を参照してください。

- セキュリティ インテリジェンス戦略の選択（5-2 ページ）
- セキュリティ インテリジェンスのホワイトリストおよびブラックリストの作成（5-4 ページ）
- セキュリティ インテリジェンス（ブラックリスト登録）の決定のロギング（33-8 ページ）

セキュリティ インテリジェンス戦略の選択

ライセンス：Protection

ブラックリストを作成する最も簡単な方法は、オープン リレーとなることが分かっている IP アドレス、既知の攻撃者、不正な IP アドレス（bogon）などを追跡する、インテリジェンス フィードを使用することです。インテリジェンス フィードは定期的に更新されるため、インテリジェンス フィードを使用することで、システムがネットワーク トラフィックのフィルタリングに最新の情報を使用することが保証されます。ただし、セキュリティに対する脅威（マルウェア、スパム、ボットネット、フィッシングなど）を表す不正な IP アドレスが現れては消えるペースが速すぎて、新しいポリシーを更新して適用するには間に合わないこともあります。

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

- リストとは、ASA FirePOWER モジュールにアップロードする IP アドレスの静的リストのことです。ASA FirePOWER モジュール
- フィードとは、ASA FirePOWER モジュールが定期的にインターネットからダウンロードする、IP アドレスの動的リストのことです。インテリジェンス フィードは、特殊なタイプのフィードです。

インターネット アクセス要件を含め、セキュリティ インテリジェンスのリストとフィードを設定する方法の詳細については、セキュリティ インテリジェンス リストとフィードの操作（2-4 ページ）を参照してください。

セキュリティ インテリジェンスのグローバル ブラックリストの使用

分析の過程で、グローバル ブラックリストを作成することができます。たとえば、エクスプロイトの試行に関連した侵入イベントでルーティング可能な IP アドレスのセットに気付いた場合、それらの IP アドレスをブラックリストに入れることができます。ASA FirePOWER モジュールではすべてのアクセス コントロール ポリシーで、このグローバル ブラックリスト（および関連するグローバル ホワイトリスト）を使用してセキュリティ インテリジェンス フィルタリングを行います。これらのグローバル リストを管理する方法の詳細については、グローバル ホワイトリストおよびブラックリストの操作（2-7 ページ）を参照してください。

（注）　グローバル ブラックリスト（またはグローバル ホワイトリスト。以下を参照）のフィードの更新および追加では、展開環境全体にわたって自動的にその変更が実装されますが、セキュリティ インテリジェンス オブジェクトに対するその他の変更には、アクセス コントロール ポリシーの再適用が必要になります。詳細については、表 2-1（ 2-6 ページ）を参照してください。

ネットワーク オブジェクトの使用

さらに、ブラックリストを作成するもう 1 つの簡単な方法として、IP アドレス、IP アドレス ブロック、あるいは IP アドレスのコレクションを表すネットワーク オブジェクトまたはネットワーク オブジェクト グループを使用することもできます。ネットワーク オブジェクトの作成および変更の詳細については、ネットワーク オブジェクトの操作（2-4 ページ）を参照してください。

セキュリティ インテリジェンスのホワイトリストの使用

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

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

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

さらに細かく制御するには、接続の送信元または宛先 IP アドレスが特定のセキュリティ ゾーン内にあるかどうかに基づいて、セキュリティ インテリジェンス フィルタリングを適用することができます。

上述のホワイトリストの例を拡張するとしたら、不適切に分類された IP アドレスをホワイトリストに登録した後、組織でそれらの IP アドレスにアクセスする必要があるユーザが使用しているセキュリティ ゾーンを使用して、ホワイトリストのオブジェクトを制限するという方法が考えられます。この方法では、ビジネス ニーズを持つユーザだけが、ホワイトリストに登録された IP アドレスにアクセスできます。別の例として、サードパーティのスパム フィードを使用して、電子メール サーバのセキュリティ ゾーンのトラフィックをブラックリスト登録することができます。

接続のモニタリング（ブラックリスト登録ではなく）

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

たとえば、サードパーティのフィードを使用したブロッキングを実装する前に、そのフィードをテストする必要があるとします。フィードをモニタ専用に設定すると、ブロックされるはずの接続をシステムで詳細に分析できるだけでなく、そのような接続のそれぞれをログに記録して、評価することもできます。

パッシブ展開環境では、パフォーマンスを最適化するために、シスコでは常にモニタ専用の設定を使用することを推奨しています。パッシブに展開されたデバイスはトラフィック フローに影響を与えることができないため、トラフィックをブロックするようにシステムを構成しても何のメリットもありません。また、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。

セキュリティ インテリジェンスのホワイトリストおよびブラックリストの作成

ライセンス：Protection

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

デフォルトでは、アクセス コントロール ポリシーは、任意のゾーンに適用される、ASA FirePOWER モジュールのグローバル ホワイトリストおよびブラックリストを使用します。これらのリストはアナリストによって入力されます。ポリシーのそれぞれについて、これらのグローバル リストを使用しないように選択することができます。

(注)　入力したグローバル ホワイトリストまたはブラックリストを使用するアクセス コントロール ポリシーをProtectionのライセンスがない他のデバイスに適用することはできません。いずれかのグローバル リストに IP アドレスを追加した場合は、ポリシーのセキュリティ インテリジェンス設定から空でないリストを削除してからでないと、ポリシーを適用できません。詳細については、グローバル ホワイトリストおよびブラックリストの操作（2-7 ページ）を参照してください。

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

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

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

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

ネットマスク /0 のネットワーク オブジェクトはホワイトリストまたはブラックリストに追加できますが、ネットマスク /0 を使用したアドレス ブロックは無視され、これらのアドレスに基づいたホワイトリストおよびブラックリスト フィルタリングは行われないことに注意してください。セキュリティ インテリジェンス フィードからのネットマスク /0 のアドレス ブロックも無視されます。すべてのトラフィックをモニタまたはブロックする場合は、セキュリティ インテリジェンス フィルタリングの代わりに、[モニタ（Monitor）] または [ブロック（Block）] ルール アクションでアクセス コントロール ルールを使用し、[送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] のデフォルト値 **any** のをそれぞれ使用します。

アクセス コントロール ポリシーのセキュリティ インテリジェンス ホワイトリストおよびブラックリストを作成する方法:

ステップ 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。

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

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。

ステップ 3　[セキュリティ インテリジェンス(Security Intelligence)] タブを選択します。

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

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

ロギングを有効にしてからでないと、ブラックリスト登録されたオブジェクトをモニタ専用に設定することはできません。詳細は、セキュリティ インテリジェンス(ブラックリスト登録)の決定のロギング(33-8 ページ)を参照してください。

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

複数のオブジェクトを選択するには、Shift キーまたは Ctrl キーを使用するか、右クリックして [すべて選択(Select All)] を選択します。

ヒント　リストに含める既存のオブジェクトを検索できます。組織のニーズを満たす既存のオブジェクトがない場合は、その場でオブジェクトを作成することもできます。詳細については、ホワイトリストまたはブラックリストに追加するオブジェクトの検索(5-6 ページ)を参照してください。

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

デフォルトでは、オブジェクトは制約されません。つまり、オブジェクトのゾーンは [任意(Any)] に設定されます。[任意(Any)] を使用しない場合、制約の基準にできるゾーンは 1 つだけです。複数のゾーンでオブジェクトのセキュリティ インテリジェンス フィルタリングを適用するには、ゾーンのそれぞれについて、オブジェクトをホワイトリストまたはブラックリストに追加する必要があります。また、グローバル ホワイトリストまたはブラックリストをゾーンによって制約することはできません。

ステップ 7　[ホワイトリストに追加(Add to Whitelist)] または [ブラックリストに追加(Add to Blacklist)] をクリックします。

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

選択したオブジェクトは、ホワイトリストまたはブラックリストに追加されます。

ヒント　オブジェクトをリストから削除するには、そのオブジェクトの削除アイコン( )をクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択(Select All)] を選択した後、右クリックして [選択対象を削除(Delete Selected)] を選択します。グローバル リストを削除する場合は、選択した操作を確認する必要があります。ホワイトリストまたはブラックリストからオブジェクトを削除しても、そのオブジェクトは ASA FirePOWER モジュールから削除されません。

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

ステップ 9　オプションで、ブラックリスト登録されたオブジェクトをモニタ専用に設定するには、[ブラックリスト（Blacklist）] にリストされている該当するオブジェクトを右クリックし、[モニタ専用（ブロックしない（Monitor-only (do not block)] を選択します。

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

ステップ 10　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

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（4-12 ページ） を参照してください。

ホワイトリストまたはブラックリストに追加するオブジェクトの検索

ライセンス：Protection

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

ブラックリストまたはホワイトリストに追加するオブジェクトを検索する方法：

ステップ 1　[名前または値で検索（Search by name or value）] フィールドにクエリを入力します。

検索文字列を入力すると、[使用可能なオブジェクト（Available Objects）] リストが更新されて、検索文字列と一致する項目が表示されます。検索文字列をクリアするには、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（ ）をクリックします。

ネットワーク オブジェクトの名前、またはネットワーク オブジェクトに設定されている値を基準に検索できます。たとえば `Texas Office` という名前の個別ネットワーク オブジェクトがあり、`192.168.3.0/24` という値が設定されていて、`US Offices` というグループ オブジェクトに含まれる場合、`Tex` などの部分的または完全な検索文字列を入力するか、または `3` などの値を入力することにより、両方のオブジェクトを表示できます。

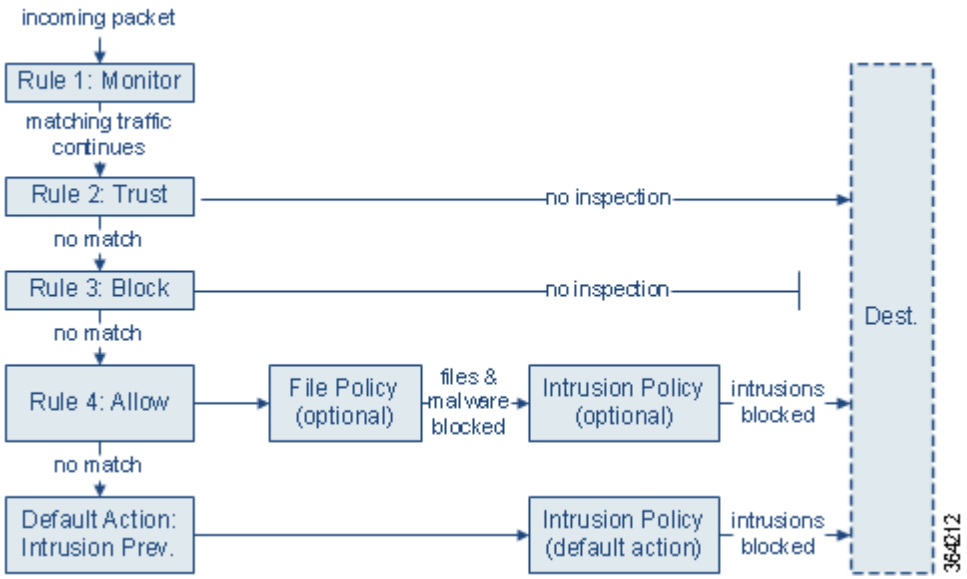
アクセス コントロール ルールを使用したトラフィック フローの調整

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。

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、および一部のデコードと前処理は、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。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。条件は単純または複雑にできます。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(6-2 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 ポリシーおよびルールのトラブルシューティング(4-13 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

アクセス コントロール ポリシー内で、アクセス コントロール ルールはネットワーク トラフィックを処理する詳細な方法を提供しています。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、またはユーザ別にトラフィックを照合できます。条件は単純または複雑にできます。条件の使用は、多くの場合のライセンスによって異なります。

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。

ロギング（**Logging**）

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。

コメント（**Comments**）

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 ポリシーおよびルールのトラブルシューティング（4-13 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。

ステップ 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。

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 ページが表示され、[ルール（Rules）] タブに焦点が置かれています。

ステップ 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。

アクセス コントロール ルール エディタが表示されます。

ステップ 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。

ステップ 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（6-4 ページ） を参照してください。
- ルールの [アクション（Action）] を選択します。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（6-7 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（6-5 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（10-1 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（33-1 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。

ステップ 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（4-12 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

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（4-15 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。

ステップ 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。

ステップ 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：機能によって異なる

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。条件は単純または複雑にできます。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、システムはすべてのルールを評価し、ネットワーク トラフィックを評価するために ASA FirePOWER モジュール が使用する拡張基準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 ポリシーおよびルールのトラブルシューティング（4-13 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
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。

表 6-1　アクセス コントロール ルール条件のタイプ（続き）

条件	トラフィックの照合	詳細
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（7-5 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。
ユーザ	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。

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、ルール条件によっては、ポリシーを適用する前に、ライセンス付与された特定の機能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の要件（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

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 ルールの条件に一致しないトラフィックを処理します（デフォルト処理の設定およびネットワーク トラフィックのインスペクション（4-5 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 フローを分析してロギングできますが、影響を与えることはありません。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（6-8 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（6-9 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（10-1 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（33-10 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

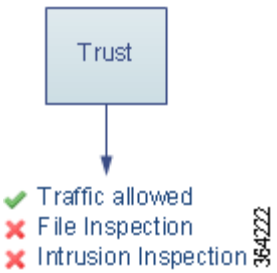
モニタ アクションはトラフィック フローに影響を与えません。つまり、一致するトラフィックがただちに許可または拒否されることはありません。その代わり、追加のルールに照らしてトラフィックが照合され、許可/拒否が決定されます。モニタ ルール以外の一致する最初のルールが、トラフィック フローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、システムはデフォルト アクションを使用します。

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、モニタされた接続のロギングについて（33-5 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

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。

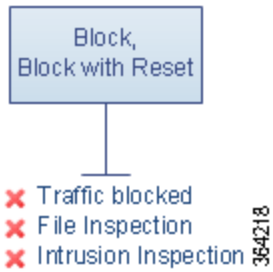


信頼されたネットワーク トラフィックは、接続の開始および終了の両方でログに記録できます。詳細については、信頼されている接続のロギングについて（33-5 ページ）を参照してください。

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

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、いかなる追加のインスペクションも行われません。リセット付きブロック ルールでは接続のリセットも行います。



HTTP トラフィックの場合は、Web 要求がブロックされた際に、接続が拒否されたことを説明するカスタム ページでデフォルトのブラウザまたはサーバ ページを上書き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。ブロックされた URL のカスタム Web ページの表示(8-15 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(33-5 ページ)を参照してください。

注意　サービス妨害(DoS)攻撃時にブロックされた TCP 接続をロギングすると、複数の同様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

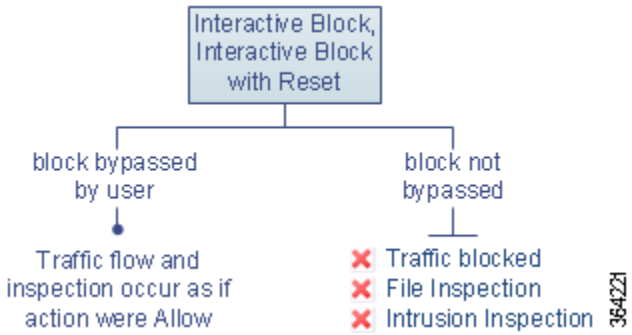
ライセンス:任意

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。

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付きインタラクティブ 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。システムは接続の開始イベントと終了イベント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

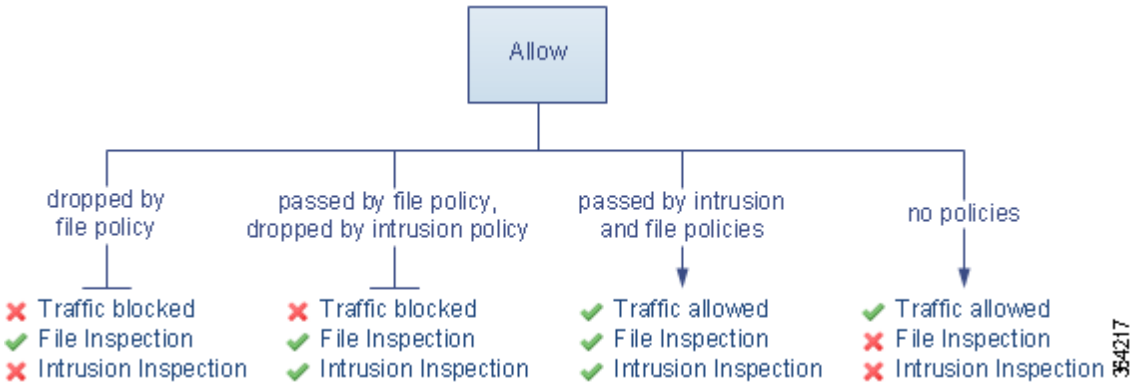
許可アクションにより、一致したトラフィックの通過が許可されます。トラフィックを許可すると、関連付けられた侵入ポリシーまたはファイル ポリシー（またはその両方）を使用して、ネットワーク トラフィックをさらに検査およびブロックすることができます。

- 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、オプションで、有害なパケットをドロップできます。
- 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。
- マルウェア 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（10-1 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（6-9 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

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。

ステップ 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。

ステップ 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。

ステップ 3　コメントを入力し、[OK] をクリックします。

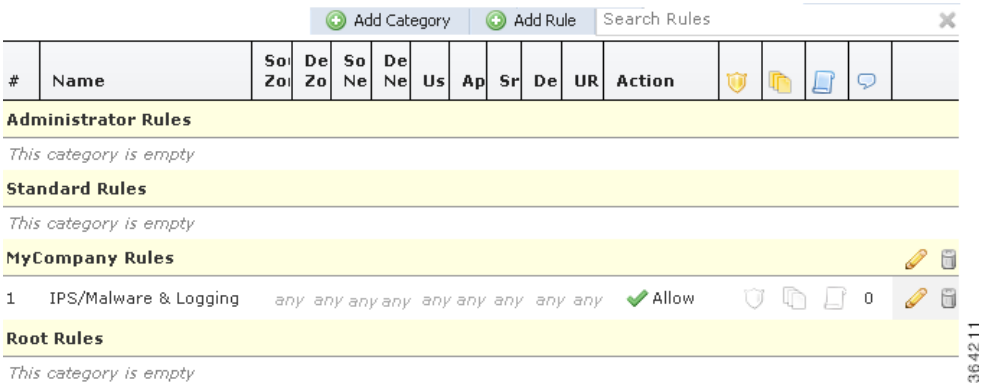
コメントが保存されます。ルールを保存するまでこのコメントを編集または削除できます。

ステップ 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

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（10-1 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	
	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（33-10 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、ポリシーのすべての警告が一覧表示されたポップアップ 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（アクセス コントロール ポリシーおよびルールのトラブルシューティング（4-13 ページ） を参照）。
	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（6-2 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

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。

ステップ 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。

ステップ 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

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（6-2 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。

ステップ 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。

ステップ 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（4-12 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

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（6-14 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

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（6-2 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。

ステップ 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。

ステップ 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。

ステップ 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(4-12 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

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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ネットワークベースのルールによるトラフィックの制御

アクセス コントロール ポリシー内のアクセス コントロール ルールは、ネットワーク トラフィックのロギングや処理の詳細な制御を行います。ネットワークベースの条件によって、次の条件の 1 つ以上を使用してネットワークを通過するトラフィックを管理できます。

- 送信元と宛先セキュリティ ゾーン
- 送信元と宛先 IP アドレスまたは地理的位置
- トランスポート層プロトコルおよび ICMP コード オプションも含む、送信元と宛先ポート

ネットワークベースの条件を互いに組み合わせたり、他のタイプの条件と組み合わせて、アクセス コントロール ルールを作成することができます。これらのアクセス コントロール ルールは単純または複雑にすることができ、複数の条件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 ルールの詳細については、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。

（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、および一部のデコードと前処理は、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。

表 **7-1** ネットワークベースのアクセス コントロール ルールのライセンス要件

要件	位置情報制御	他のすべてのネットワークベースの制御
ライセンス	任意	任意

ネットワークベースのアクセス コントロール ルールの作成については、以下を参照してください。

- 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）
- 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）
- ポートおよび ICMP コードによるトラフィックの制御（7-5 ページ）

セキュリティ ゾーンによるトラフィックの制御

ライセンス:任意

アクセス コントロール ルール内のゾーン条件によって、その送信元および宛先セキュリティ ゾーン別にトラフィックを制御することができます。セキュリティ ゾーンは、1 つ以上のインターフェイスのグループです。

単純な例として、2 つのゾーン、内部と外部を作成し、デバイス上のインターフェイスの最初のペアをそれらのゾーンに割り当てることができます。内部側のネットワークに接続されたホストは、保護されている資産を表します。

このシナリオを拡張するには、追加で同様に設定されたデバイスを配置して、複数の異なるロケーションで同様のリソースを保護することができます。これらのデバイスのそれぞれは、その内部のセキュリティ ゾーンにある資産を保護します。

ヒント　内部(または外部)のすべてのインターフェイスを 1 つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティ ポリシーが意味をなすグループ化を選択します。ゾーン作成の詳細については、セキュリティ ゾーンの操作(2-37 ページ)を参照してください。

この展開では、これらのホストにインターネットへの無制限アクセスを提供できますが、それでもやはり、着信トラフィックで侵入およびマルウェアの有無を検査することでホストを保護したい場合があります。

アクセス コントロールを使用してこれを実現するには、[宛先ゾーン(Destination Zones)] が [内部(Internal)] に設定されているゾーン条件を持つアクセス コントロール ルールを設定します。この単純なアクセス コントロール ルールは、内部ゾーンの任意のインターフェイスからデバイスを離れるトラフィックを照合します。

一致するトラフィックが侵入やマルウェアについて確実に検査されるようにするには、ルール アクションとして [許可(Allow)] を選択し、そのルールを侵入ポリシーとファイル ポリシーに関連付けます。詳細については、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(6-7 ページ)および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(10-1 ページ)を参照してください。

より複雑なルールを作成する場合は、1 つのゾーン条件で [送信元ゾーン(Source Zones)] および [宛先ゾーン(Destination Zones)] それぞれに対し、最大 50 のゾーンを追加できます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン(Destination Zones)] に追加します。

  パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブなインターフェイスで構成されるゾーンを [宛先ゾーン(Destination Zones)] 条件で使用することはできません。
- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [送信元ゾーン(Source Zones)] に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

ゾーン条件を作成する際、警告アイコンは無効な設定を示します。詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング(4-13 ページ)を参照してください。

ゾーン別にトラフィックを制御するには、次の手順を実行します。

ステップ 1　ゾーン別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（6-2 ページ）を参照してください。

ステップ 2　ルール エディタで、[ゾーン（Zones）] タブを選択します。

[ゾーン（Zones）] タブが表示されます。

ステップ 3　[利用可能なゾーン（Available Zones）] から追加するゾーンを見つけて選択します。

追加するゾーンを検索するには、[利用可能なゾーン（Available Zones）] リストの上にある [名前で検索（Search by name）] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

クリックすると、ゾーンを選択できます。複数のゾーンを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

ステップ 4　[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックして、選択したゾーンを適切なリストに追加します。

選択したゾーンをドラッグ アンド ドロップすることもできます。

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。設定変更の展開（4-12 ページ）を参照してください。

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

ライセンス：機能によって異なる

アクセス コントロール ルール内のネットワーク条件によって、その送信元および宛先 IP アドレス別にトラフィックを制御することができます。次のいずれかの操作を実行できます。

- 制御するトラフィックの送信元および宛先 IP アドレスを明示的に指定します。または、
- IP アドレスを地理的位置に関連付ける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します。

ネットワークベースのアクセス コントロール ルールの条件を作成するには、IP アドレスと地理的位置を手動で指定できます。または、再利用可能で名前を 1 つ以上の IP アドレス、アドレス ブロック、国、大陸などに関連付けるネットワーク オブジェクトおよび位置情報オブジェクトを使用してネットワーク条件を設定できます。

ヒント　ネットワーク オブジェクトまたは位置情報オブジェクトを作成した後、それを使用して、アクセス コントロール ルールを作成するだけでなく、システムの モジュール インターフェイスの他のさまざまな場所で IP アドレスを表すことができます。これらのオブジェクトはオブジェクト マネージャを使用して作成できます。また、アクセス コントロール ルールの設定時にネットワーク オブジェクトをオンザフライで作成することもできます。詳細については、再利用可能なオブジェクトの管理（2-1 ページ）を参照してください。

地理的位置別にトラフィックを制御するルールを作成する場合は、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必要があります。このため、シスコではASA FirePOWER モジュールの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推奨しています。位置情報データベースの更新（43-21 ページ）を参照してください。

表 *7-2*　ネットワーク条件のライセンス要件

要件	位置情報制御	**IP** アドレス制御
ライセンス	任意	任意

1 つのネットワーク条件で [送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] それぞれに対し、最大 50 の項目を追加でき、ネットワークベースの設定と位置情報ベースの設定を組み合わせることができます。

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[送信元ネットワーク（Source Networks）] を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先ネットワーク（Destination Networks）] を設定します。

送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

ネットワーク条件を作成する際、警告アイコンは無効な設定を示します。詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（4-13 ページ）を参照してください。

ネットワークまたは地理的位置別にトラフィックを制御するには、次の手順を実行します。

ステップ 1　ネットワーク別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（6-2 ページ）を参照してください。

ステップ 2　ルール エディタで、[ネットワーク（Networks）] タブを選択します。

[ネットワーク（Networks）] タブが表示されます。

ステップ 3　[利用可能なネットワーク（Available Networks）] から、次のように追加するネットワークを見つけて選択します。

- 追加するネットワーク オブジェクトとグループを表示するには [ネットワーク（Networks）] タブをクリックします。位置情報オブジェクトを表示するには [位置情報（Geolocation）] タブをクリックします。
- ここでネットワーク オブジェクトを作成してリストに追加するには、[利用可能なネットワーク（Available Networks）] リストの上にある追加アイコン（ ）をクリックし、ネットワーク オブジェクトの操作（2-4 ページ）の手順に従います。
- 追加するネットワーク オブジェクトまたは位置情報オブジェクトを検索するには、適切なタブを選択し、[利用可能なネットワーク（Available Networks）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックして、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

ステップ 4　[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5　手動で指定する送信元または宛先 IP アドレスまたはアドレス ブロックを追加します。

[送信元ネットワーク（Source Networks）] リストまたは [宛先ネットワーク（Destination Networks）] リストの下にある [IP アドレスの入力（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 [追加（Add）] をクリックします。

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。設定変更の展開（4-12 ページ）を参照してください。

ポートおよび ICMP コードによるトラフィックの制御

ライセンス：任意

アクセス コントロール ルール内のネットワーク条件によって、その送信元および宛先ポート別にトラフィックを制御することができます。このコンテンツでは、「ポート」は次のいずれかを示します。

- 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。システムは、カッコ内に記載されたプロトコル番号 + オプションの関連ポートまたはポート範囲を使用してこの設定を表します。例：TCP(6)/22。
- 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。例：ICMP(1):3:3
- ポートを使用しない他のプロトコルを使用してトラフィックを制御できます。

ポート ベースのアクセス コントロール ルールの条件を作成するときは、手動でポートを指定できます。または、再利用可能で名前を 1 つ以上のポートに関連付けるポート オブジェクトを使用してポート条件を設定できます。

ヒント　ポート オブジェクトを作成した後、それを使用して、アクセス コントロール ルールを作成するだけでなく、システムの モジュール インターフェイスの他のさまざまな場所でポートを表すことができます。ポート オブジェクトは、オブジェクト マネージャを使用して作成するか、またはアクセス コントロール ルールの設定時にオンザフライで作成できます。詳細については、ポート オブジェクトの操作（2-11 ページ）を参照してください。

1 つのネットワーク条件で [選択した送信元ポート（Selected Source Ports）] および [選択した宛先ポート（Selected Destination Ports）] それぞれに対し、最大 50 の項目を追加できます。

- ポートからのトラフィックを照合するには、[選択した送信元ポート（Selected Source Ports）] を設定します。

  送信元ポートだけを条件に追加する場合は、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、DNS over TCP および DNS over UDP の両方を 1 つのアクセス コントロール ルールの送信元ポート条件として追加できます。

- ポートへのトラフィックを照合するには、[選択した宛先ポート（Selected Destination Ports）] を設定します。

  宛先ポートだけを条件に追加する場合は、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。

- 特定の選択した送信元ポートから発生し、特定の選択した宛先ポートに向かうトラフィックを照合するには、両方設定します。

  送信元ポートと宛先ポートの両方を条件に追加する場合は、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、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。

ポート条件を作成する際は、次の点に注意します。

- 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 ポートを追加すると、アクセス コントロール ルールは要求されていないエコー応答だけを照合します。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。
- 宛先ポート条件として GRE（47）プロトコルを使用すると、アクセス コントロール ルールに追加できるのは他のネットワークベースの条件、つまり、ゾーン、およびネットワーク条件のみです。レピュテーションまたはユーザ ベースの条件を追加する場合は、ルールを保存できません。

ポート条件を作成する際、警告アイコンは無効な設定を示します。たとえば、オブジェクト マネージャを使用して使用中のポート オブジェクトを編集し、それらのオブジェクト グループを使用するルールを無効にできます。詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（4-13 ページ）を参照してください。

ポート別にトラフィックを制御するには、次の手順を実行します。

ステップ 1　ポート別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（6-2 ページ）を参照してください。

ステップ 2　ルール エディタで、[ポート（Ports）] タブを選択します。

[ポート（Ports）] タブが表示されます。

ステップ 3　[使用可能なポート（Available Ports）] から、次のように追加するポートを見つけて選択します。

- ここでポート オブジェクトを作成してリストに追加するには、[使用可能なポート（Available Ports）] リストの上にある追加アイコン（  ）をクリックし、ポート オブジェクトの操作（2-11 ページ）の手順に従います。
- 追加するポート オブジェクトおよびグループを検索するには、[使用可能なポート（Available Ports）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトのポートの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。たとえば、「80」と入力すると、シスコ提供の HTTP ポート オブジェクトが ASA FirePOWER モジュールに表示されます。

  オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

ステップ 4　[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5　手動で指定する送信元ポートまたは宛先ポートを追加します。

- 送信元ポートの場合は、[選択した送信元ポート（Selected Source Ports）] リストの下の [プロトコル（Protocol）] ドロップダウンリストから [TCP] または [UDP] を選択します。次に、ポートを入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。
- 宛先ポートの場合は、[選択した宛先ポート（Selected Destination Ports）] リストの下の [プロトコル（Protocol）] ドロップダウンリストからプロトコル（すべてのプロトコルの場合は [すべて（All）]）を選択します。リストに表示されない割り当てられていないプロトコルの数字を入力することもできます。

  [ICMP] または [IPv6-ICMP] を選択すると、ポップアップ ウィンドウが表示され、タイプと関連するコードを選択できます。ICMP の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 [英語] および http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml [英語] を参照してください。

  プロトコルを指定しない場合、またはオプションで TCP または UDP を指定した場合は、ポートを入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。

[追加（Add）] をクリックします。ASA FirePOWER モジュールでは、無効なポート設定はルール条件に追加されません。

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。設定変更の展開（4-12 ページ） を参照してください。

レピュテーション ベースのルールによるトラフィックの制御

アクセス コントロール ポリシー内のアクセス コントロール ルールは、ネットワーク トラフィックのロギングや処理の詳細な制御を行います。アクセス コントロール ルールのレピュテーション ベースの条件を使用することで、ネットワーク トラフィックを文脈によって解釈可能にし、必要に応じて制限することで、ネットワークを通過できるトラフィックを管理できます。アクセス コントロール ルールは、次のタイプのレピュテーション ベースの制御を管理します。

- アプリケーション条件を使用することで、アプリケーション制御を実行できます。これによって、個々のアプリケーションだけでなく、アプリケーションの基本的な特性であるタイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグに基づいてアプリケーション トラフィックが制御されます。
- URL 条件を使用することで、*URL* フィルタリングを実行できます。これによって、個々の Web サイトだけでなく、Web サイトのシステムによって割り当てられたカテゴリおよびレピュテーションに基づいて Web トラフィックが制御されます。

レピュテーション ベースの条件を互いに組み合わせたり、他のタイプの条件と組み合わせて、アクセス コントロール ルールを作成することができます。これらのアクセス コントロール ルールは単純または複雑にすることができ、複数の条件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 ルールの詳細については、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。

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、および一部のデコードと前処理は、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。レピュテーション ベースのアクセス コントロールには、次のライセンスが必要です。

表 **8-1**　レピュテーション ベースのアクセス コントロール ルールのライセンス要件

要件	アプリケーション管理	**URL** フィルタリング（**cat.& rep.**）	**URL** フィルタリング（手動）
ライセンス	Control	URL フィルタリング（URL Filtering）	任意

アクセス コントロール ルールにレピュテーション ベースの条件を追加する方法については、以下を参照してください。

- アプリケーション トラフィックの制御（8-2 ページ）
- URL のブロッキング（8-8 ページ）

ASA FirePOWER モジュールは、他のタイプのレピュテーション ベースの制御を実行できますが、アクセス コントロール ルールを使用してこれらを設定しないでください。詳細については、以下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、最初の防御ラインとして、接続の発信元または宛先のレピュテーションに基づいてトラフィックを制限する方法について説明します。
- 侵入防御パフォーマンスの調整（10-6 ページ）では、マルウェアおよび他のタイプの禁止されたファイルの送信を検出、追跡、保存、分析、およびブロックする方法について説明します。

アプリケーション トラフィックの制御

ライセンス：Control

ASA FirePOWER モジュールが IP トラフィックを分析するときは、ネットワークで一般的に使用されるアプリケーションを識別および分類できます。

アプリケーション制御について

アクセス コントロール ルールのアプリケーション条件を使用することで、このアプリケーション制御を実行することができます。1 つのアクセス コントロール ルール内には、トラフィックを制御するアプリケーションを指定する方法がいくつかあります。

- カスタム アプリケーションなどの個々のアプリケーションを選択できます。
- システムによって提供されるアプリケーション フィルタを使用できます。このフィルタは、アプリケーションの基本的な特性であるタイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグに基づいて編成されたアプリケーションの名前付きセットです。
- 選択したアプリケーション（カスタム アプリケーションを含む）をグループ化するカスタム アプリケーション フィルタを作成し、使用できます。

アプリケーション フィルタを使用することで、アクセス コントロール ルールに対しアプリケーション条件をすぐに作成することができます。このフィルタによって、ポリシーの作成と管理が簡素化され、システムは Web トラフィックを期待通りに確実に制御します。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを作成できます。ユーザがそれらのアプリケーションの 1 つを使用しようとすると、セッションがブロックされます。

また、Cisco は、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にディテクタを更新し追加します。アプリケーションの特性に基づいたフィルタを使用することで、システムは最新のディテクタを使用してアプリケーション トラフィックをモニタします。

アプリケーション条件の作成

トラフィックがアプリケーション条件を持つアクセス コントロール ルールに一致するには、トラフィックが [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加したフィルタまたはアプリケーションの 1 つに一致している必要があります。

1 つのアプリケーション条件において、最大 50 の項目を [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加できます。以下はそれぞれ 1 つの項目としてカウントされます。

- 個別またはカスタムな組み合わせの、[アプリケーション フィルタ（Application Filters）] リストからの 1 つ以上のフィルタ。この項目は、特性によってグループ化されたアプリケーションのセットを表します。

- [使用可能なアプリケーション（Available Applications）] リストでアプリケーションの検索を保存することで作成されるフィルタ。この項目は、部分文字列の一致によってグループ化されたアプリケーションのセットを表します。
- [使用可能なアプリケーション（Available Applications）] リストからの個々のアプリケーション。

モジュール インターフェイスでは、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。

アプリケーション条件を持つ各ルールに対し、アクセス コントロール ポリシーを追加すると、システムは一意のアプリケーションのリストを生成して照合することに留意してください。つまり、完全なカバレッジを確保するために、重複フィルタおよび個々に指定されたアプリケーションを使用できます。

（注）　暗号化されたトラフィックの場合、システムは [SSL プロトコル（SSL Protocol）] とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグがないアプリケーションは、暗号化されていないトラフィックでのみ検出できます。

詳細については、次の項を参照してください。

- トラフィックとアプリケーション フィルタの一致（8-3 ページ）
- 個々のアプリケーションからのトラフィックの照合（8-4 ページ）
- アクセス コントロール ルールへのアプリケーション条件の追加（8-6 ページ）
- アプリケーション制御の制約事項（8-7 ページ）

トラフィックとアプリケーション フィルタの一致

ライセンス：Control

アクセス コントロール ルールでアプリケーション条件を作成するときは、[アプリケーション フィルタ（Application Filters）] リストを使用して、特性によってグループ化されたトラフィックを照合するアプリケーションのセットを作成します。

アクセス コントロール ルール内でアプリケーションをフィルタリングするメカニズムは、オブジェクト マネージャを使用して再利用可能なカスタム アプリケーション フィルタを作成するメカニズムと同じです。アプリケーション フィルタの操作（2-13 ページ）を参照してください。また、オンザフライで作成した多数のフィルタを、アクセス コントロール ルールに新規の再利用可能なフィルタとして保存できます。ユーザが作成したフィルタはネストすることができないため、別のユーザが作成したフィルタを含むフィルタは保存できません。

フィルタの組み合わせ方について

フィルタを単独または組み合わせて選択すると、[使用可能なアプリケーション（Available Applications）] リストが更新され、条件を満たすアプリケーションのみが表示されます。システムによって提供されるフィルタは組み合わせて選択できますが、カスタム フィルタはできません。

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
```

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 [使用可能なアプリケーション（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（リスク）タイプで Medium（中）および High（高）フィルタを選択し、Business Relevance（ビジネスとの関連性）タイプで Medium（中）および High（高）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 [中（Medium）] または [高（High）] の [リスク（Risk）] タイプと [中（Medium）] または [高（High）] の [ビジネスとの関連性（Business Relevance）] タイプの両方に含まれるアプリケーションだけを表示します。

フィルタの検索および選択

フィルタを選択するには、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。また、システムによって提供されるフィルタ タイプ（[リスク（Risks）]、[ビジネスとの関連性（Business Relevance）]、[タイプ（Types）]、[カテゴリ（Categories）]、または [タグ（Tags）]）を右クリックして、[すべて選択（Check All）] または [すべて選択解除（Uncheck All）] を選択します。

フィルタを検索するには、[使用可能なフィルタ（Available Filters）] リストの上にある [名前で検索（Search by name）] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するフィルタが表示されます。

フィルタを選択したら、[使用可能なアプリケーション（Available Applications）] リストを使用してそのフィルタをルールに追加し、個々のアプリケーションからのトラフィックの照合（8-4 ページ）の手順に従います。

個々のアプリケーションからのトラフィックの照合

ライセンス：Control

アクセス コントロール ルールでアプリケーション条件を作成するときは、[使用可能なアプリケーション（Available Applications）] リストを使用して、トラフィックを照合するアプリケーションを作成します。

アプリケーションのリストの参照

条件の作成を初めて開始するときは、リストは制約されておらず、システムが検出するすべてのアプリケーションを一度に 100 個ずつ表示します。

- アプリケーションを確認していくには、リストの下にある矢印をクリックします。
- アプリケーションの特性に関するサマリー情報と参照できるインターネットの検索リンクが示されているポップアップ ウィンドウを表示するには、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。

照合するアプリケーションの検索

照合するアプリケーションを見つけやすくするために、[使用可能なアプリケーション（Available Applications）] リストを次のように制約できます。

- アプリケーションを検索するには、リスト上部にある [名前で検索（Search by name）] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するアプリケーションが表示されます。
- フィルタを適用してアプリケーションを制約するには、[アプリケーション フィルタ（Application Filters）] リストを使用します（トラフィックとアプリケーション フィルタの一致（8-3 ページ）を参照）。フィルタを適用すると、[使用可能なアプリケーション（Available Applications）] リストが更新されます。

制約されると、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] オプションが [使用可能なアプリケーション（Available Applications）] リストの上部に表示されます。このオプションを使用して、制約されたリスト内のすべてのアプリケーションを [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストにすべて一度に追加できます。

（注）　[アプリケーション フィルタ（Application Filters）] リストで 1 つ以上のフィルタを選択し、しかも [使用可能なアプリケーション（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 [使用可能なアプリケーション（Available Applications）] リストが AND 演算を使って結合されます。つまり [フィルタに一致するすべてのアプリケーション（All apps matching the filter）] 条件には、[使用可能なアプリケーション（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、[使用可能なアプリケーション（Available Applications）] リストの上で入力された検索文字列が含まれます。

条件内で照合する単一アプリケーションの選択

照合するアプリケーションを検索したら、それをクリックして選択します。複数のアプリケーションを選択するには、Shift キーおよび Ctrl キーを使用するか、または現在制約されているビュー内のすべてのアプリケーションを選択するには右クリックして [すべて選択（Select All）] を選択します。

単一のアプリケーション条件では、それらを個別に選択することで、最大 50 のアプリケーションを照合できます。50 を超えるアプリケーションを追加するには、複数のアクセス コントロール ルールを作成するか、またはフィルタを使用してアプリケーションをグループ化します。

条件のフィルタに一致するすべてのアプリケーションの選択

[アプリケーション フィルタ（Application Filters）] リストで検索またはフィルタを使用して制約されると、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] オプションが [使用可能なアプリケーション（Available Applications）] リストの上部に表示されます。

このオプションを使用して、制約された [使用可能なアプリケーション（Available Applications）] リスト内のアプリケーションのセット全体を [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに同時に追加できます。アプリケーションを個別に追加するのとは対照的に、このアプリケーションのセットを追加すると、そのセットを構成する個々のアプリケーションの数にかかわらず、最大 50 のアプリケーションに対してただ 1 つのアイテムとしてカウントされます。

このようにアプリケーション条件を作成するときは、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加するフィルタの名前は、フィルタに表されているフィルタ タイプ + 各タイプの最大 3 つの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（リスク）タイプの 2 つのフィルタと Business Relevance（ビジネスとの関連性）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,...
```

[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] で追加するフィルタに表されないフィルタ タイプは、追加するフィルタの名前に含まれません。これらのフィルタ タイプは *any* に設定されています。つまり、これらのフィルタ タイプはフィルタを制約しないので、任意の値が許可されます。

[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] の複数のインスタンスをアプリケーション条件に追加でき、各インスタンスは [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストで個別の項目としてカウントされます。たとえば、リスクが高いすべてのアプリケーションを 1 つの項目として追加し、選択内容をクリアしてから、ビジネスとの関連性が低いすべてのアプリケーションを別の項目として追加できます。このアプリケーション条件は、リスクが高いアプリケーションまたはビジネスとの関連性が低いアプリケーションに一致します。

アクセス コントロール ルールへのアプリケーション条件の追加

ライセンス：Control

トラフィックがアプリケーション条件を持つアクセス コントロール ルールに一致するには、トラフィックが [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加したフィルタまたはアプリケーションの 1 つに一致している必要があります。

1 条件ごとに最大 50 の項目を追加でき、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。アプリケーション条件を作成する際、警告アイコンは無効な設定を示します。詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（4-13 ページ）を参照してください。

アプリケーション トラフィックを制御するには、次の手順を実行します。

ステップ 1　アプリケーション別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（6-2 ページ）を参照してください。

ステップ 2　ルール エディタで、[アプリケーション（Applications）] タブを選択します。

[アプリケーション（Applications）] タブが表示されます。

ステップ 3　オプションで、フィルタを使用して [使用可能なアプリケーション（Available Applications）] リストに表示されるアプリケーションのリストを制約します。

[アプリケーション フィルタ（Application Filters）] リストで 1 つ以上のフィルタを選択します。詳細については、トラフィックとアプリケーション フィルタの一致（8-3 ページ）を参照してください。

ステップ 4　[使用可能なアプリケーション（Available Applications）] リストから追加するアプリケーションを見つけて選択します。

個々のアプリケーションを検索して選択するか、またはリストが制約されている場合は、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] を選択できます。詳細については、個々のアプリケーションからのトラフィックの照合（8-4 ページ）を参照してください。

ステップ 5　[ルールに追加（Add to Rule）] をクリックして、選択したアプリケーションを [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加します。

選択したアプリケーションとフィルタをドラッグ アンド ドロップすることもできます。フィルタは [フィルタ（Filters）] という見出しの下に表示され、アプリケーションは [アプリケーション（Applications）] という見出しの下に表示されます。

ヒント　このアプリケーション条件に別のフィルタを追加する前に、[すべてのフィルタをクリア（Clear All Filters）] をクリックして既存の選択内容をクリアします。

ステップ 6　必要に応じて、[選択済みのアプリケーションとフィルタ（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、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カスタム フィルタを保存できます。

このオンザフライで作成されたフィルタを管理するには、オブジェクト マネージャを使用します。アプリケーション フィルタの操作（2-13 ページ）を参照してください。別のユーザが作成したフィルタを含むフィルタは保存できないことに注意してください。ユーザが作成したフィルタはネストできません。

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。設定変更の展開（4-12 ページ）を参照してください。

アプリケーション制御の制約事項

ライセンス：Control

アプリケーション制御を実行する際は、次の点に注意してください。

アプリケーション識別の速度

システムは、以下の動作の前にアプリケーション制御を実行することはできません。

- モニタ対象の接続がクライアントとサーバの間で確立される前
- システムがセッションでアプリケーションを識別する前

この識別は 3 ～ 5 パケット以内で行う必要があります。これらの最初のパケットの 1 つがアプリケーション条件を含むアクセス コントロール ルール内の他のすべての条件に一致するが、識別が完了していない場合、アクセス コントロール ポリシーはパケットの通過を許可します。この動作により接続が確立され、アプリケーションの識別が可能になります。便宜を図るため、影響を受けるルールは情報アイコン（ ）でマークされます。

許可されたパケットは、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（デフォルト アクション侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもない）により検査されます。詳細については、アクセス コントロールのデフォルト侵入ポリシーの設定（17-1 ページ）を参照してください。

システムは識別を終えると、アクセス コントロール ルール アクションおよび関連付けられている侵入ポリシーおよびファイル ポリシーをそのアプリケーション条件に一致する残りのセッション トラフィックに適用します。

暗号化されたトラフィックの処理

システムは、SMTPS、POP、FTPS、TelnetS および IMAPS など StartTLS を使用して、暗号化される前のアプリケーション トラフィックを識別し、フィルタリングできます。また、TLS クライアントの hello メッセージ内の Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。

これらのアプリケーションは、[SSL プロトコル（SSL Protocol）] とタグ付けされています。このタグがないアプリケーションは、暗号化されていないトラフィックでのみ検出できます。

ペイロードのないアプリケーション トラフィック パケットの処理

システムは、アプリケーションが識別される接続内に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。

参照されるトラフィックの処理

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。

複数のプロトコルを使用するアプリケーション トラフィックの制御（**Skype**）

システムは、Skype の複数のタイプの アプリケーション トラフィックを検出できます。Skype のトラフィックを制御するためのアプリケーション条件を作成する場合は、個々のアプリケーションを選択するのではなく、[アプリケーション フィルタ（Application Filters）] リストから [Skype] タグを選択します。これにより、システムは同じ方法で Skype のすべてのトラフィックを検出して制御できるようになります。詳細については、トラフィックとアプリケーション フィルタの一致（8-3 ページ）を参照してください。

URL のブロッキング

ライセンス：機能によって異なる

アクセス コントロール ルールの URL 条件を使用することで、ネットワーク上のユーザがアクセスできる Web サイトを制限することができます。この機能は、*URL フィルタリング*と呼ばれます。アクセス コントロールを使用してブロックする（または逆に許可する）URL を指定するには 2 つの方法があります。

- 各ライセンスを使用して、個々の URL または URL のグループを手動で指定することで、Web トラフィックへのきめ細かなカスタム コントロールを実現できます。
- URL フィルタリング（URL Filtering）ライセンスを使用して、URL の一般的な分類、またはカテゴリ、およびリスク レベル、またはレピュテーションに基づいて、Web サイトへのアクセスを制御することもできます。システムは接続ログ、侵入イベント、およびアプリケーションの詳細にこのカテゴリとレピュテーション データを表示します。

（注）　イベントで URL カテゴリおよびレピュテーション情報を表示するには、URL 条件を使用して少なくとも 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。

Web サイトをブロックするときは、ユーザのブラウザにデフォルト動作を許可するか、またはシステムによって提供される一般的なページまたはカスタム ページを表示できます。また、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する機会をユーザに与えることができます。

メモリ リソースの制約により、ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X、および 71xx ファミリ デバイスは、他のモデル（ASA5545-X、ASA5555-X、ASA5585-X など）で使用されるデータベースよりも小規模な URL カテゴリ データベースを使用します。

この小規模なデータベースには、よく参照されるドメインのサブドメインでよく参照されるエントリは含まれません。たとえば、mail.google.com はこの小規模データベースには含まれず、その結果、mail.google.com は Web ベースのメールとしてではなく、検索エンジンとして分類されます。

表 ***8-2***　　***URL*** フィルタリングのライセンス要件

要件	カテゴリおよびレピュテーション ベース	手動
ライセンス	URL フィルタリング（URL Filtering）	任意

詳細については、以下を参照してください。

- レピュテーション ベースの URL ブロッキングの実行（8-9 ページ）
- 手動による URL ブロッキングの実行（8-11 ページ）
- URL の検出とブロッキングの制約事項（8-13 ページ）
- ユーザが URL ブロックをバイパスすることを許可する（8-13 ページ）
- ブロックされた URL のカスタム Web ページの表示（8-15 ページ）

レピュテーション ベースの URL ブロッキングの実行

ライセンス:URL フィルタリング（URL Filtering）

URL フィルタリング（URL Filtering）ライセンスを使用して、ASA FirePOWER モジュールが Cisco クラウドから取得する要求された URL のカテゴリおよびレピュテーションに基づいて、Web サイトへのユーザのアクセスを制御できます。

- 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（Auctions）] カテゴリ、monster.com は [求職（Job Search）] 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、[高リスク（High Risk）]（レベル 1）から [ウェルノウン（Well Known）]（レベル 5）の範囲にまたがるものとなる可能性があります。

（注）　カテゴリおよびレピュテーション ベースの URL 条件を持つアクセス コントロール ルールを有効にする前に、Cisco クラウドとの通信を有効にする必要があります。これにより、ASA FirePOWER モジュールは URL データを取得できるようになります。詳細については、クラウド通信の有効化（41-2 ページ）を参照してください。

レピュテーション ベースの URL ブロッキングの利点

URL のカテゴリおよびレピュテーションにより、アクセス コントロール ルールの URL 条件をすぐに作成することができます。たとえば、[乱用薬物（Abused Drugs）] カテゴリ内の高リスク URL をすべて識別してブロックするアクセス コントロール ルールを作成できます。ユーザがそのカテゴリとレピュテーションの組み合わせで 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。

Cisco クラウドからカテゴリ データおよびレピュテーション データを使用することで、ポリシーの作成と管理も簡素化されます。この方法では、システムが Web トラフィックを期待通りに確実に制御します。最後に、クラウドは新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは確実に最新の情報を使用して要求された URL をフィルタします。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。

次に例をいくつか示します。

- 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（Gaming）] 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。
- ルールがすべてのマルウェア サイトをブロックし、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 を [ブログ（Blog）] から [マルウェア（Malware）] に再分類でき、システムはそのサイトをブロックできます。
- ルールがリスクの高いソーシャル ネットワーキング サイトをブロックし、だれかがプロファイル ページに悪意のあるペイロードへのリンクが含まれる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（Benign sites）] から [高リスク（High Risk）] に変更でき、システムでそれをブロックできます。

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 ASA FirePOWER モジュールがクラウドと通信できない場合は、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 ルールがその 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 に手動でカテゴリやレピュテーションを割り当てることはできません。

URL 条件の作成

1 つの URL 条件で、照合する最大 50 の項目を [選択済み URL（Selected URLs）] に追加できます。任意でレピュテーションによって制限された各 URL カテゴリは、1 つの項目としてカウントされます。URL 条件でリテラル URL および URL オブジェクトを使用することもできますが、これ

らの項目はレピュテーションで制限できないことに注意してください。詳細については、手動による URL ブロッキングの実行（8-11 ページ）を参照してください。

レピュテーションでリテラル URL または URL オブジェクトを制限できないことに注意してください。

URL 条件を作成する際、警告アイコンは無効な設定を示します。詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（4-13 ページ）を参照してください。

カテゴリ データおよびレピュテーション データを使用した要求された URL によるトラフィックの制御

ステップ 1　URL 別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（6-2 ページ）を参照してください。

ステップ 2　ルール エディタで、[URL（URLs）] タブを選択します。

[URL（URLs）] タブが表示されます。

ステップ 3　[カテゴリおよび URL（Categories and URLs）] リストから追加する URL のカテゴリを見つけて選択します。カテゴリに関係なく Web トラフィックを照合するには、[任意（Any）] カテゴリを選択します。

追加するカテゴリを検索するには、[カテゴリおよび URL（Categories and URLs）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、カテゴリ名を入力します。入力すると、リストが更新されて一致するカテゴリが表示されます。

カテゴリを選択するには、そのカテゴリをクリックします。複数のカテゴリを選択するには、Shift キーおよび Ctrl キーを使用します。

ヒント　右クリックしてすべてのカテゴリを選択できますが、このようにすべてのカテゴリを追加すると、1 つのアクセス コントロール ルールに対する項目の最大値 50 を超えます。代わりに [任意（Any）] を使用してください。

ステップ 4　オプションで、[レピュテーション（Reputations）] リストからレピュテーション レベルをクリックして、カテゴリの選択内容を制限します。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（Any）]（つまりすべてのレベル）を設定します。

選択できるレピュテーション レベルは 1 つだけです。レピュテーション レベルを選択すると、アクセス コントロール ルールはその目的に応じて異なる動作をします。

- ルールによって Web アクセスをブロックまたはモニタする場合（ルール アクションが [ブロック（Block）]、[リセットしてブロック（Block with reset）]、[インタラクティブ ブロック（Interactive Block）]、[リセットしてインタラクティブ ブロック（Interactive Block with reset）]、または [モニタ（Monitor）]）、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レピュテーションもすべて選択されます。たとえば疑わしいサイト（レベル 2）をブロックまたはモニタするようルールを設定した場合、高リスク（レベル 1）のサイトも自動的にブロックまたはモニタされます。
- ルールによって Web アクセスがそれを信頼またはさらに検査するかどうかを許可する場合（ルール アクションが [許可（Allow）] または [信頼する（Trust）]）、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さが弱いレピュテーションもすべて選択されます。たとえば無害なサイト（**Benign sites**）（レベル 4）を許可するようルールを設定した場合、有名（**Well known**）（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。

ステップ 5　[ルールに追加（Add to Rule）] をクリックするか、または選択した項目をドラッグ アンド ドロップして、[選択済み URL（Selected URLs）] リストに追加します。

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。設定変更の展開（4-12 ページ） を参照してください。

手動による URL ブロッキングの実行

ライセンス：任意

カテゴリおよびレピュテーションで URL フィルタリングを補完するか、または選択的に上書きするには、手動で個々の URL または URL のグループを指定することで、Web トラフィックを制御できます。これにより、許可またはブロックされた Web トラフィックに対するきめ細かなカスタム制御を行うことができます。特殊なライセンスなしでこのタイプの URL フィルタリングを実行することもできます。

アクセス コントロール ルールに許可またはブロックする URL を手動で指定するには、単一のリテラル URL を入力できます。または、再利用可能で名前を URL または IP アドレスに関連付ける URL オブジェクトを使用して URL 条件を設定できます。

ヒント　URL オブジェクトを作成した後、それを使用して、アクセス コントロール ルールを作成するだけでなく、システムのモジュール インターフェイスの他のさまざまな場所で URL を表すことができます。これらのオブジェクトはオブジェクト マネージャを使用して作成できます。また、アクセス コントロール ルールの設定時に URL オブジェクトをオンザフライで作成することもできます。詳細については、URL オブジェクトの操作（2-12 ページ）を参照してください。

URL 条件で URL を手動で指定する

手動で入力することで、許可またはブロックされる Web トラフィックに対する正確な制御が実現できますが、手動で指定した URL をレピュテーションで制限することはできません。また、ルールに予期しない結果がないことを確認する必要があります。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手動で入力した URL の値が、モニタ対象ホストから要求された URL の一部に一致する場合、アクセス コントロール ルールの URL 条件が満たされます。

したがって、URL 条件（URL オブジェクトを含む）に URL を手動で指定する場合は、影響を受ける可能性がある他のトラフィックを慎重に考慮する必要があります。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/

別の例として、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。

暗号化された Web トラフィックの手動ブロッキング

アクセス コントロール ルールの URL 条件は以下を行います。

- Web トラフィック（HTTP または HTTPS）の暗号化プロトコルを無視します。

たとえば、アクセス コントロール ルールは、http://example.com/ へのトラフィックを https://example.com/ へのトラフィックと同じものとして処理します。HTTP または HTTPS トラフィックのみに一致するアクセス コントロール ルールを設定するには、アプリケーション条件をルールに追加します。詳細については、URL のブロッキング（8-8 ページ）を参照してください。

- トラフィックを暗号化するために使用する公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合し、また、サブジェクト共通名に含まれるサブドメインを無視します。

  手動で HTTPS トラフィックをフィルタリングする場合は、サブドメイン情報を含めないでください。

URL 条件を作成する際、警告アイコンは無効な設定を示します。詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（4-13 ページ）を参照してください。

許可またはブロックする **URL** を手動で指定して **Web** トラフィックを制御するには、次の手順を実行します。

ステップ **1**　URL 別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（6-2 ページ）を参照してください。

ステップ **2**　ルール エディタで、[URL（URLs）] タブを選択します。

[URL（URLs）] タブが表示されます。

ステップ **3**　[カテゴリおよび URL（Categories and URLs）] リストから追加する URL オブジェクトおよびグループを見つけて選択します。

- URL オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[カテゴリおよび URL（Categories and URLs）] リストの上にある追加アイコン（  ）をクリックします。URL オブジェクトの操作（2-12 ページ）を参照してください。
- 追加する URL オブジェクトおよびグループを検索するには、[カテゴリおよび URL（Categories and URLs）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクト内の URL または IP アドレスの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用します。右クリックしてすべての **URL** オブジェクトおよびカテゴリを選択できますが、このように URL を追加すると、1 つのアクセス コントロール ルールに対する項目の最大値 50 を超えます。

ステップ **4**　[ルールに追加（Add to Rule）] をクリックするか、または選択した項目を [選択済み URL（Selected URLs）] リストに追加します。

選択した項目をドラッグ アンド ドロップすることもできます。

ステップ **5**　手動で指定するリテラル URL を追加します。このフィールドでは、ワイルドカード（*）は使用できません。

[選択済み URL（Selected URLs）] リストの下にある [URL の入力（Enter URL）] プロンプトをクリックし、URL または IP アドレスを入力して、[追加（Add）] をクリックします。

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。設定変更の展開（4-12 ページ）を参照してください。

URL の検出とブロッキングの制約事項

ライセンス：任意

URL の検出とブロッキングを実行する際は、次の点に注意してください。

URL 識別の速度

システムは以下の動作の前に URL をフィルタリングできません。

- モニタ対象の接続がクライアントとサーバの間で確立される前
- システムがセッションで HTTP または HTTPS アプリケーションを識別する前
- システムが要求された URL を識別する前（クライアントの hello メッセージまたはサーバ証明書から暗号化されたセッションの場合）

この識別は 3 ～ 5 パケット以内で行う必要があります。これらの最初のパケットの 1 つが URL 条件を含むアクセス コントロール ルール内の他のすべての条件に一致するが、識別が完了していない場合、アクセス コントロール ポリシーはパケットの通過を許可します。この動作により接続が確立され、URL の識別が可能になります。便宜を図るため、影響を受けるルールは情報アイコン（ ）でマークされます。

許可されたパケットは、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（デフォルト アクション侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもない）により検査されます。詳細については、アクセス コントロールのデフォルト侵入ポリシーの設定（17-1 ページ）を参照してください。

システムは識別を終えると、アクセス コントロール ルール アクションおよび関連付けられている侵入ポリシーおよびファイル ポリシーをその URL 条件に一致する残りのセッション トラフィックに適用します。

暗号化された Web トラフィックの処理

URL 条件を持つアクセス コントロール ルールを使用して暗号化された Web トラフィックを評価する際、システムは以下を行います。

- 暗号化プロトコルを無視します。ルールに URL 条件はあるがプロトコルを指定するアプリケーション条件はない場合、アクセス コントロール ルールは HTTPS および HTTP 両方のトラフィックを照合します。
- トラフィックを暗号化するために使用する公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合し、サブジェクト共通名に含まれるサブドメインを無視します。
- （設定した場合でも）HTTP 応答ページを表示しません。

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ません。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。

ユーザが URL 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

アクセス コントロール ルールを使用してユーザの HTTP Web 要求をブロックする場合は、ルール アクションを [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定することで、ユーザは警告 *HTTP* 応答ページをクリック スルーすることによりブロックをバイパスできます。システムによって提供される汎用応答ページを表示するか、またはカスタム HTML を入力できます。

デフォルトでは、システムによってユーザは後続のアクセスで警告ページを表示することなく、10 分（600 秒）間ブロックをバイパスすることができます。期間を 1 年に設定したり、ユーザに毎回ブロックをバイパスするように強制できます。

ユーザがブロックをバイパスしない場合、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ます。また、接続をリセットすることもできます。一方、ユーザがブロックをバイパスすると、システムによってトラフィックが許可されます。このトラフィックを許可するということは、侵入、マルウェアおよび禁止されているファイルの有無について暗号化されていないペイロードを引き続き検査できることを意味します。ブロックをバイパスした後、ロードされなかったページの要素をロードするために、ページを更新しなければならない場合があることに注意してください。

インタラクティブ HTTP 応答ページは、ブロック ルールに設定する応答ページとは別に設定することに注意してください。たとえば、インタラクションなしでセッションがブロックされたユーザにはシステムによって提供されるページを表示できますが、クリックして続行できるユーザに対しては、カスタム ページを表示できます。詳細については、ブロックされた URL のカスタム Web ページの表示（8-15 ページ）を参照してください。

ヒント　アクセス コントロール ポリシーのすべてのルールに対してインタラクティブ ブロッキングを素早く無効にするには、システムによって提供されるページもカスタム ページも表示しないでください。これにより、システムはインタラクションなしでインタラクティブ ブロック ルールに一致するすべての接続をブロックします。

ユーザに **Web** サイト ブロックをバイパスするように許可するには、次の手順を実行します。

ステップ **1**　URL 条件を持つ Web トラフィックに一致するアクセス コントロール ルールを作成します。

レピュテーション ベースの URL ブロッキングの実行（8-9 ページ）および手動による URL ブロッキングの実行（8-11 ページ）を参照してください。

ステップ **2**　アクセス コントロール ルール アクションが [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] であることを確認します。

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（6-7 ページ）を参照してください。

ステップ **3**　ユーザがブロックをバイパスし、ルールに対してインスペクションおよびロギング オプションを必要に応じて選択すると仮定します。許可ルールと同様に次のようになります。

- いずれかのタイプのインタラクティブ ブロック ルールをファイルおよび侵入ポリシーに関連付けることができます。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（10-1 ページ）を参照してください。
- 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。

  システムが最初にユーザに警告すると、ロギングされた接続開始イベントを [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションでマークすることに留意してください。ユーザがブロックをバイパスすると、セッションが記録される追加の接続イベントに許可アクションが付きます。詳細については、アクセス コントロールの処理に基づく接続のロギング（33-10 ページ）を参照してください。

ステップ **4**　オプションで、システムが警告ページを再表示する前にユーザがブロックをバイパスしてから経過する時間を設定します。

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（8-15 ページ）を参照してください。

ステップ 5　オプションで、ユーザにブロックをバイパスすることを許可するために表示するカスタム ページを作成し、使用します。

ブロックされた URL のカスタム Web ページの表示（8-15 ページ）を参照してください。

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

ライセンス：任意

デフォルトでは、システムによってユーザは後続のアクセスで警告ページを表示することなく、10 分（600 秒）間インタラクティブ ブロックをバイパスすることができます。期間を 1 年に設定したり、ゼロに設定してユーザに毎回ブロックをバイパスするように強制できます。この制限は、ポリシー内のすべてのインタラクティブ ブロック ルールに適用されます。ルールごとに制限を設定することはできません。

ユーザ バイパスの期限が切れるまでの時間の長さをカスタマイズするには、次の手順を実行します。

ステップ 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。

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

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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 4　[全般設定（General Settings）] の横にある編集アイコン（）をクリックします。

[全般設定（General Settings）] ポップアップ ウィンドウが表示されます。

ステップ 5　[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)）] フィールドに、ユーザ バイパスの期限が切れるまでの経過時間を秒数で入力します。

0 ～ 31536000（1 年）の間の任意の数を指定できます。ゼロを指定すると、ユーザはブロックを毎回強制的にバイパスします。

ステップ 6　[OK] をクリックします。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 7　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。詳細については、設定変更の展開（4-12 ページ）を参照してください。

ブロックされた URL のカスタム Web ページの表示

ライセンス：任意

システムによってユーザの HTTP Web 要求がブロックされたときに、ユーザのブラウザに表示される内容は、アクセス コントロール ルールのアクションを使用して、セッションをどのようにブロックするかによって異なります。次から選択できます。

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

システムによって提供される汎用応答ページを表示するか、またはカスタム HTML を入力できます。カスタム テキストを入力する際には、使用した文字数がカウンタで示されます。

各アクセス コントロール ポリシーで、インタラクティブ HTTP 応答ページは、インタラクションなしで、つまりブロック ルールを使用してトラフィックをブロックするために使用する応答ページとは別に設定します。たとえば、インタラクションなしでセッションがブロックされたユーザにはシステムによって提供されるページを表示できますが、クリックして続行できるユーザに対しては、カスタム ページを表示できます。

HTTP 応答ページをユーザに確実に表示できるかは、ネットワーク設定、トラフィック負荷、およびページのサイズによって異なります。カスタム応答ページを作成する場合は、より小さいページが正常に表示されやすいことに留意してください。

HTTP 応答ページの設定方法:

ステップ **1**　Web トラフィックをモニタするアクセス コントロール ポリシーを編集します。

詳細については、アクセス コントロール ポリシーの編集（4-8 ページ）を参照してください。

ステップ **2**　[HTTP 応答（HTTP Responses）] タブを選択します。

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

ステップ **3**　[ブロック レスポンス ページ（Block Response Page）] および [インタラクティブ ブロック レスポンス ページ（Interactive Block Response Page）] の場合、ドロップダウンリストから応答を選択します。各ページには、次の選択肢があります。

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

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

ステップ **4**　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。詳細については、設定変更の展開（4-12 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: レルムとユーザ

次の項では、ネットワークでユーザ トラフィックを制御する方法について説明します。

レルム、ユーザ、ユーザ グループ、および ISE 属性のアクセス コントロール ルール条件

ライセンス：Control

ユーザ制御を実行する（レルム全体、個々のユーザ、ユーザ グループ、または ISE 属性に基づいてアクセス コントロール ルール条件を作成する）前に、次のことを行う必要があります。

- モニタ対象の Microsoft Active Directory または LDAP サーバのそれぞれに対し、レルムを設定する。レルムに対してユーザのダウンロードを有効にすると、FirePOWER Management Center は定期的および自動的に、新規に報告されたかすでに報告済みの権限のあるユーザおよびユーザ グループのメタデータをダウンロードするようサーバに照会します。
- レルムを認証方式に関連付けるために、アイデンティティ ポリシーを作成する。
- 1 つ以上のユーザ エージェントまたは ISE デバイス、あるいはキャプティブ ポータルを設定する。ISE 属性の条件を使用するには、ISE を設定する必要があります。

  ユーザ エージェント、ISE およびキャプティブ ポータルは、アクセス コントロール ルール条件でユーザ制御に使用できる、権限のあるユーザ データを収集します。アイデンティティ ソースは、指定したユーザがホストにログイン、ログアウトしたり、LDAP または AD クレデンシャルを使用して認証する際にモニタします。

（注） ユーザ エージェントまたは ISE デバイスのモニタ対象に多くのユーザ グループを設定した場合、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、FirePOWER Management Center のユーザ制限が原因で、システムが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、レルム、ユーザ、またはユーザ グループ条件をもつアクセス コントロール ルールが想定どおりに適用されない可能性があります。

1 つのユーザ条件で、最大 50 のレルム、ユーザおよびグループを [選択されたユーザ（Selected Users）] に追加できます。ユーザ グループを持つ条件は、そのグループのメンバー（サブグループのメンバーを含む）のいずれかが送信元/宛先であるトラフィックを照合します。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 グループを含めると、自動的に、すべてのセカンダリ グループのメンバーを含む、そのグループのすべてのメンバーが含まれます。ただし、アクセス コントロール ルールでセカンダリ グループを使用する場合は、明示的にセカンダリ グループを含める必要があります。

（注）　アクセス コントロール ルールがネットワーク トラフィックを評価する前に、ハードウェア ベースの高速パス ルール、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、SSL インスペクション、ユーザ識別、および一部のデコードと前処理が行われます。

ユーザ アクセス コントロール ルールに関するトラブルシューティング

ライセンス: Control

ユーザ アクセス コントロール ルールの予期しない動作に気付いたら、ルール、アイデンティティ ソース、またはレルムの設定を調整することを検討してください。

レルム、ユーザ、またはユーザ グループに対するアクセス コントロール ルールが適用されない

ユーザ エージェントまたは ISE デバイスのモニタ対象に多くのユーザ グループを設定した場合、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、FirePOWER Management Center のユーザ制限が原因で、システムがユーザ レコードをドロップすることがあります。その結果、レルムまたはユーザ条件を使用するアクセス コントロール ルールが想定どおりに適用されない可能性があります。

ユーザ グループまたはユーザ グループ内のユーザに対するアクセス コントロール ルールが想定どおりに適用されない

ユーザ グループ条件を含むアクセス コントロール ルールを設定する場合は、LDAP または Active Directory サーバでユーザ グループを設定している必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、FirePOWER Management Center はユーザ グループ制御を実行できません。

セカンダリ グループ内のユーザに対するアクセス コントロール ルールが想定どおりに適用されない

Active Directory サーバのセカンダリ グループのメンバーであるユーザを含めるか除外するユーザ グループ条件を含むアクセス コントロール ルールを設定する場合、サーバは報告するユーザの数を制限していることがあります。

デフォルトでは、Active Directory サーバはセカンダリ グループから報告するユーザの数を制限します。この制限は、セカンダリ グループ内のすべてのユーザが FirePOWER Management Center に報告され、ユーザ条件を含むアクセス コントロール ルールでの使用に適するようにカスタマイズする必要があります。

アクセス コントロール ルールが、初めて表示されたユーザに一致していない

システムは、以前に表示されていないユーザからのアクティビティを検出すると、サーバから情報を取得します。システムがこの情報を正常に取得するまで、このユーザに表示されるアクティビティは、一致するアクセス コントロール ルールによって処理されません。代わりに、ユーザ セッションは、一致する次のアクセス コントロール ルール（またはアクセス コントロール ポリシーのデフォルト アクション）によって処理されます。

たとえば、次のような状況が考えられます。

- ユーザ グループのメンバーであるユーザが、ユーザ グループ条件を含むアクセス コントロール ルールに一致しない。
- ユーザ データ取得に使用されたサーバが Active Directory サーバである場合に、ISE またはユーザ エージェントによって報告されたユーザがアクセス コントロール ルールに一致しない。

これにより、システムがユーザ データをイベント ビューおよび分析ツールに表示するのが遅れる可能性があることに注意してください。

アクセス コントロール ルールへのレルム、ユーザ、またはユーザ グループ条件の追加

ライセンス: Control

はじめる前に

- ユーザ アイデンティティ ソース（30-1 ページ）の説明に従って、1 つ以上の権限のあるユーザ アイデンティティ ソースを設定します。
- レルムの作成（29-5 ページ）の説明に従って、レルムを設定します。アクセス コントロール ルールでレルム、ユーザ、またはユーザ グループ条件を設定できるようにするには、その前にユーザによるダウンロード（自動またはオンデマンド）が実行される必要があります。

ステップ 1　アクセス コントロール ルール エディタで、[ユーザ（Users）] タブを選択します。

ステップ 2　[使用可能なレルム（Available Realms）] リストで名前または値で検索してレルムを選択します。

ステップ 3　[使用可能なユーザ（Available Users）] リストで名前または値で検索してレルムを選択します。

ステップ 4　[ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5　ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の展開（4-12 ページ）を参照してください。

アクセス コントロール ルールへの ISE 属性条件の追加

ライセンス: Control

はじめる前に

- ISE 接続の設定（30-6 ページ）の説明に従って ISE を設定します。

ステップ 1　アクセス コントロール ルール エディタで、[ISE 属性（ISE Attributes）] タブを選択します。

ステップ 2　[使用可能な ISE セッション属性（Available ISE Session Attributes）] リストで名前または値で検索して属性を選択します。

ステップ 3　[使用可能な ISE メタデータ（Available ISE Metadata）] リストで名前または値で検索してメタデータを選択します。

ステップ 4　[ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ヒント　[ロケーションの IP アドレスの追加（Add a Location IP Address）] フィールドを使用して、条件にロケーションの IP 属性を追加することもできます。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 5　ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の展開（4-12 ページ）を参照してください。

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

侵入ポリシーとファイル ポリシーは連携して、トラフィックがその宛先に許可される前の最後の防御ラインとして機能します。

- 侵入ポリシーは、システムの侵入防御機能を制御します。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（15-1 ページ）を参照してください。
- ファイル ポリシーは、システムのネットワークベースのファイル制御および高度なマルウェア防御（AMP）機能を制御します。ファイル ポリシーの概要と作成（32-4 ページ）を参照してください。

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（ブラックリスト登録）およびトラフィックのデコードと前処理は、ネットワーク トラフィックが侵入、禁止されたファイル、およびマルウェアの有無について検査される前に行われます。アクセス コントロール ルールおよびアクセス コントロールのデフォルト アクションによって、侵入ポリシーおよびファイル ポリシーで検査されるトラフィックが決まります。

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ことで、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。

侵入防御および AMP では、次の表に示すように、特定のライセンス済み機能を有効にする必要があります。

表 ***10-1*** 侵入インスペクションおよびファイル インスペクションのライセンスの要件

機能	説明	ライセンス
侵入防御	侵入およびエクスプロイトを検出し、任意でブロックします	Protection
ファイル制御	ファイル タイプの伝送を検出し、任意でブロックします	Protection
高度なマルウェア防御（AMP）	マルウェアの伝送を検出、追跡し、任意でブロックします	マルウェア

侵入、禁止されたファイル、およびマルウェアの有無についてトラフィックを検査する詳細については、以下を参照してください。

- 許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション（10-2 ページ）
- 侵入防御パフォーマンスの調整（10-6 ページ）
- 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（10-17 ページ）

許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション

ライセンス：Protectionまたはマルウェア

侵入ポリシーおよびファイル ポリシーは、トラフィックがその宛先に許可される前の最後の防衛ラインとして、システムの侵入防御、ファイル制御、および AMP 機能を制御します。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、デコードと前処理、およびアクセス コントロール ルールの選択は、侵入インスペクションおよびファイル インスペクションの前に行われます。

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ことで、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。アクセス コントロール ルールの条件は単純または複雑にできます。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。アクセス コントロール ルールのアクションによって、システムが一致するトラフィックをどのように処理するかが決まります。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（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。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（6-7 ページ）を参照してください。

インタラクティブ ブロック ルールには、許可ルールと同じインスペクション オプションがあることに留意してください。これにより、あるユーザが警告ページをクリック スルーすることによってブロックされた Web サイトをバイパスした場合に、悪意のあるコンテンツがないかトラフィックを検査できます。詳細については、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（6-9 ページ）を参照してください。

ポリシー内のモニタ アクセス コントロール ルール以外のいずれにも一致しないトラフィックは、デフォルト アクションで処理されません。システムはデフォルト アクションによって許可されたトラフィックに対し侵入の有無を検査できますが、禁止されたファイルまたはマルウェアの有無は検査できないことに注意してください。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 ポリシーを関連付けることはできません。

（注）　場合によっては、接続がアクセス コントロール ポリシーによって分析される場合、システムはトラフィックを処理するアクセス コントロール ルール（存在する場合）を決定する前に、その接続の最初の数パケットを処理し通過を許可する必要があります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。詳細については、アクセス コントロールのデフォルト侵入ポリシーの設定（17-1 ページ）を参照してください。

上記のシナリオの詳細と、ファイル ポリシーおよび侵入ポリシーをアクセス コントロール ルールおよびアクセス コントロールのデフォルト アクションに関連付ける手順については、以下を参照してください。

- ファイル インスペクションおよび侵入インスペクションの順序について（10-3 ページ）
- AMP またはファイル制御を実行するアクセス コントロール ルールの設定（10-4 ページ）
- 侵入防御を実行するアクセス コントロール ルールの設定（10-5 ページ）
- デフォルト処理の設定およびネットワーク トラフィックのインスペクション（4-5 ページ）

ファイル インスペクションおよび侵入インスペクションの順序について

ライセンス:Protectionまたはマルウェア

(注)　侵入防御のデフォルト アクションによって許可されたトラフィックは、侵入の有無について検査されますが、禁止されたファイルまたはマルウェアの有無については検査されません。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 ポリシーを関連付けることはできません。

同じルールでファイル インスペクションと侵入インスペクションの両方を実行する必要はありません。許可ルールまたはインタラクティブ ブロック ルールに一致する接続の場合:

- 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まります
- 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まります

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。

アクセス コントロール ルールによって処理される単一接続の場合、ファイル インスペクションは侵入インスペクションの前に行われます。つまり、システムは侵入のためファイル ポリシーによってブロックされたファイルを検査しません。ファイル インスペクション内では、タイプによる単純なブロッキングの方が、マルウェア インスペクションおよびブロッキングよりも優先されます。

(注)　ファイルがセッションで検出されブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

たとえば、アクセス コントロール ルールで定義された特定のネットワーク トラフィックを正常に許可するシナリオを考えてください。ただし、予防措置として、実行可能ファイルのダウンロードをブロックし、ダウンロードされた PDF のマルウェア インスペクションを行って検出された場合はブロックし、トラフィックに対して侵入インスペクションを実行する必要があるとします。

一時的に許可するトラフィックの特性に一致するルールを持つアクセス コントロール ポリシーを作成し、それを侵入ポリシーとファイル ポリシーの両方に関連付けます。ファイル ポリシーはすべての実行可能ファイルのダウンロードをブロックし、マルウェアを含む PDF も検査およびブロックします。

- まず、システムはファイル ポリシーで指定された単純なタイプ マッチングに基づいて、すべての実行可能ファイルのダウンロードをブロックします。それらはすぐにブロックされるため、これらのファイルはマルウェア クラウド ルックアップの対象にも侵入インスペクションの対象にもなりません。
- 次に、システムは、ネットワーク上のホストにダウンロードされた PDF に対するマルウェア クラウド ルックアップを実行します。マルウェア ファイルの性質を持つ PDF はすべてブロックされ、侵入インスペクションの対象にはなりません。
- 最後に、システムはアクセス コントロール ルールに関連付けられている侵入ポリシーを使用して、ファイル ポリシーでブロックされなかったファイルを含む残りのトラフィック全体を検査します。

AMP またはファイル制御を実行するアクセス コントロール ルールの設定

ライセンス：Protectionまたはマルウェア

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールをファイル ポリシーに関連付けることができます。ファイル インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なるファイルおよびマルウェアのインスペクション プロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムはファイル ポリシーの設定に従って禁止されたファイル（マルウェアを含む）を検出すると、イベントを自動的にロギングします。ログ ファイルまたはマルウェア イベントが必要ない場合は、アクセス コントロール ルールごとにこのロギングを無効にできます。アクセス コントロール ルールにファイル ポリシーを関連付けた後、アクセス コントロール ルール エディタの [ロギング（Logging）] タブで [ログファイル（Log Files）] チェックボックスをオフにします。詳細については、許可された接続のファイルおよびマルウェア イベント ロギングの無効化（33-7 ページ）を参照してください。

また、システムは、呼び出し元のアクセス コントロール ルールのロギング設定にかかわらず、関連付けられた接続の終了をロギングします。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（自動）（33-3 ページ）を参照してください。

アクセス コントロール ルールにファイル ポリシーを関連付けるには、次の手順を実行します。

ステップ 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（Access Control）] 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。

ステップ 2　アクセス コントロール ルールを使用して AMP またはファイル制御を設定するアクセス 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。

ステップ 3　新しいルールを作成するか、または既存のルールを編集します。アクセス コントロール ルールの作成および編集（6-2 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 エディタが表示されます。

ステップ 4　ルール アクションが [許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定されていることを確認します。

ステップ 5　[インスペクション（Inspection）] タブを選択します。

[インスペクション（Inspection）] タブが表示されます。

ステップ 6　アクセス コントロール ルールに一致するトラフィックを検査する場合は [ファイル ポリシー（File Policy）] を選択し、または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場合は [なし（None）] を選択します。

表示される編集アイコン（）をクリックし、ポリシーを編集できます。ファイル ポリシーの作成（32-10 ページ）を参照してください。

ステップ 7　[追加（Add）] 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。変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。設定変更の展開（4-12 ページ）を参照してください。

侵入防御を実行するアクセス コントロール ルールの設定

ライセンス：Protection

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールを侵入ポリシーに関連付けることができます。侵入インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なる侵入インスペクション プロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セット使用します。セット内の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

ヒント　システムによって提供される侵入ポリシーを使用する場合であっても、シスコは、正確にネットワーク環境を反映するためにシステムの侵入変数を設定することを強く推奨します。少なくとも、デフォルトのセットにあるデフォルトの変数を変更します。定義済みのデフォルトの変数の最適化（2-16 ページ）を参照してください。

異なる侵入ポリシー変数セットのペアを各許可ルールおよびインタラクティブ ブロック ルール（およびデフォルト アクション）と関連付けることができますが、ターゲット デバイスが設定されたとおりにインスペクションを実行するのに必要なリソースが不足している場合は、アクセス コントロール ポリシーを適用できません。詳細については、パフォーマンスを向上させるためのルールの簡素化（4-14 ページ）を参照してください。

システムによって提供される侵入ポリシーとカスタム侵入ポリシーについて

シスコは、複数の侵入ポリシーを ASA FirePOWER モジュールとともに提供します。システムによって提供される侵入ポリシーを使用して、シスコ 脆弱性調査チーム（VRT）のエクスペリエンスを活用することができます。これらのポリシーでは、VRT は侵入ルールおよびプリプロセッサルールの状態を設定し、詳細設定の初期設定も提供します。システムによって提供されるポリシーをそのまま使用するか、またはカスタム ポリシーのベースとして使用できます。カスタム ポリシーを作成すれば、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。

お客様が独自に作成するカスタム ポリシーに加えて、システムは初期インライン 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 つの侵入ポリシーは、ベースとして Balanced Security and Connectivity 侵入ポリシーを使用します。両者の唯一の相違点は、[インライン時にドロップ（Drop When Inline）] 設定です。インライン ポリシーではドロップ動作が有効化され、パッシブ ポリシーでは無効化されています。詳細については、システム付属ポリシーとカスタム ポリシーの比較（15-7 ページ）を参照してください。

接続イベントおよび侵入イベントのロギング

アクセス コントロール ルールによって呼び出された侵入ポリシーが侵入を検出すると、侵入イベントを生成します。また、システムはアクセス コントロール ルールのロギング設定に関係なく、侵入が発生した接続の終了を自動的にロギングします。侵入に関連付けられる接続（自動）（33-3 ページ）を参照してください。

アクセス コントロール ルールに侵入ポリシーを関連付けるには、次の手順を実行します。

ステップ 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（Access Control）] 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。

ステップ 2　アクセス コントロール ルールを使用して侵入インスペクションを設定するアクセス 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。

ステップ 3　新しいルールを作成するか、または既存のルールを編集します。アクセス コントロール ルールの作成および編集（6-2 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 エディタが表示されます。

ステップ 4　ルール アクションが [許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定されていることを確認します。

ステップ 5　[インスペクション（Inspection）] タブを選択します。

[インスペクション（Inspection）] タブが表示されます。

ステップ 6　システムによって提供されるまたはカスタムの侵入ポリシーを選択するか、またはアクセス 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にするには [なし（None）] を選択します。

カスタム侵入ポリシーを選択する場合は、表示される編集アイコン（）をクリックし、ポリシーを編集できます。侵入ポリシーの編集（23-4 ページ）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` 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　オプションで、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。

表示される編集アイコン（）をクリックし、編集セットを編集できます。変数セットの使用（2-15 ページ）を参照してください。

ステップ 8　[保存（Save）] 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。変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。設定変更の展開（4-12 ページ）を参照してください。

侵入防御パフォーマンスの調整

ライセンス：Protection

シスコは、侵入行為のトラフィックを分析する際のシステムのパフォーマンスを向上するための機能を提供しています。これらのパフォーマンス設定は、各アクセス コントロール ポリシーごとに設定し、その設定はその親のアクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシーに適用されます。

詳細については、以下を参照してください。

- 侵入に対するパターン一致の制限（10-7 ページ）では、イベント キューで許可されるパケット数を指定し、より大きなストリームに再構築されるパケットのインスペクションを有効または無効にする方法を説明します。
- 侵入ルールの正規表現制限のオーバーライド（10-8 ページ）では、Perl 適合正規表現（PCRE）のデフォルトの一致および再帰の制限をオーバーライドする方法を説明します。
- パケットごとに生成される侵入イベントの制限（10-9 ページ）では、ルール処理イベント キュー設定を構成する方法を説明します。

- パケットおよび侵入ルール遅延しきい値の設定（10-10 ページ）では、デバイスの遅延をパケットおよびルール遅延しきい値構成の許容レベルで保持する必要性とセキュリティのバランスを実現する方法を説明します。
- 侵入パフォーマンス統計情報のロギングの設定（10-16 ページ）では、基本的なパフォーマンス モニタリングおよびレポート パラメータを設定する方法について説明します。

侵入に対するパターン一致の制限

ライセンス：Protection

イベント キューで許可するパケット数を指定できます。ストリーム再構成の前後に、より大きなストリームに再構築されるパケットのインスペクションを有効または無効にできます。

イベント キューの設定：

ステップ 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（Access Control）] 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[パフォーマンス設定（Performance Settings）] の横にある編集アイコン（ ）をクリックし、表示されるポップアップ ウィンドウで [パターン一致の制限（Pattern Matching Limits）] タブを選択します。

ステップ 5　次のオプションを修正できます。

- [パケットごとに分析するパターン状態の最大値（Maximum Pattern States to Analyze Per Packet）] フィールドに、キューに含めるイベントの最大値の値を入力します。
- ストリーム再構成の前後で、データのより大きなストリームに再構築されるパケットを検査するには、[今後の再構成の対象となるトラフィックでコンテンツ チェックを無効にする（Disable Content Checks on Traffic Subject to Future Reassembly）] を選択します。再構成の前後の検査はより多くの処理オーバーヘッドを必要とするため、パフォーマンスが低下する可能性があります。
- ストリーム再構成の前後で、データのより大きなストリームに再構築されるパケットのインスペクションを無効にするには、[今後の再構成の対象となるトラフィックでコンテンツ チェックを無効にする（Disable Content Checks on Traffic Subject to Future Reassembly）] をオフにします。検査を無効にすると、ストリームの検査の処理オーバーヘッドが減少し、パフォーマンスが向上する場合があります。

ステップ 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。設定変更の展開（4-12 ページ）を参照してください。

侵入ルールの正規表現制限のオーバーライド

ライセンス：Protection

パケット ペイロードの内容を検査するための侵入ルールで使用される PCRE のデフォルトの一致および再帰の制限をオーバーライドできます。侵入ルールにおける `pcre` キーワードの使用については、PCRE を使用したコンテンツの検索（27-38 ページ）を参照してください。デフォルトの制限によってパフォーマンスの最低レベルが確保されます。これらの制限をオーバーライドすると、セキュリティが向上する可能性がありますが、非効率的な正規表現に対してパケット評価を許可することで、パフォーマンスが著しく影響を受ける可能性もあります。

注意　非効率的なパターンの影響に関する知識があり、侵入ルールの作成経験が豊富であるユーザ以外は、デフォルトの PCRE の制限をオーバーライドしないでください。

次の表に、デフォルトの制限をオーバーライドするように設定できるオプションを示します。

表 ***10-2***　正規表現の制約オプション

オプション	説明
検索結果の制限状態（Match Limit State）	[制限に合わせる（Match Limit）] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [デフォルト（Default）] を選択して、[制限に合わせる（Match Limit）] に設定した値を使用する • [無制限（Unlimited）] を選択して、無制限の数の試行を許可する • [カスタム（Custom）] を選択して、[制限に合わせる（Match Limit）] に対して 1 以上の制限を指定するか、または PCRE の一致の評価を完全に無効化するために 0 を指定する
制限に合わせる（Match Limit）	PCRE 正規表現で定義されたパターンに一致することを試行する回数を指定します。
検索結果の再起制限状態（Match Recursion Limit State）	[再起制限に合わせる（Match Recursion Limit）] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [デフォルト（Default）] を選択して、[再起制限に合わせる（Match Recursion Limit）] に設定した値を使用する • [無制限（Unlimited）] を選択して、無制限の数の再帰を許可する • [カスタム（Custom）] を選択して、[再起制限に合わせる（Match Recursion Limit）] に対して 1 以上の制限を指定するか、または PCRE の再帰を完全に無効化するために 0 を指定する [再起制限に合わせる（Match Recursion Limit）] が意味を持つためには、[制限に合わせる（Match Limit）] よりも小さい必要があることに注意してください。
再起制限に合わせる（Match Recursion Limit）	パケット ペイロードに対して PCRE 正規表現を評価する際の再帰数を指定します。

PCRE オーバーライドの設定：

ステップ **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（Access Control）] 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定(Advanced)] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[パフォーマンス設定(Performance Settings)] の横にある編集アイコン( )をクリックし、表示されるポップアップ ウィンドウで [正規表現制限(Regular Expression Limits)] タブを選択します。

ステップ 5　正規表現の制約オプションの表の任意のオプションを変更できます。

ステップ 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。設定変更の展開(4-12 ページ)を参照してください。

パケットごとに生成される侵入イベントの制限

ライセンス:Protection

ルール エンジンがルールに対してトラフィックを評価する場合、特定のパケットまたはパケット ストリームに生成されたイベントをイベント キューに配置し、キュー内の上位のイベントをユーザ インターフェイスに報告します。複数のイベントが発生した場合、ルール エンジンが 1 個のパケットまたはパケット ストリームに対して複数のイベントを記録するように選択できます。これらのイベントのロギングにより、報告されたイベントを超えて情報を収集することができます。このオプションを設定する場合、キュー内に配置可能なイベントの数および記録されるイベントの数を指定できます。また、キュー内のイベントの順序を決定する条件を選択できます。

次の表に、1 個のパケットまたはストリームに対して記録されるイベントの数を決定するために設定できるオプションを示します。

表 *10-3*　侵入イベント ロギング制限のオプション

オプション	説明
パケットごとに保存されるイベントの最大数(Maximum Events Stored Per Packet)	特定のパケットまたはパケット ストリームに対して保存できるイベントの最大数。
パケットごとにログに記録されるイベントの最大数(Maximum Events Logged Per Packet)	特定のパケットまたはパケット ストリームに対して記録されるイベントの数。これは、[パケットごとに保存されるイベントの最大数(Maximum Events Stored Per Packet)] 値を超えてはいけません。
イベント ロギングの順位決定の基準(Prioritize Event Logging By)	イベント キュー内のイベントの順序を決定するために使用する値。最上位のイベントがユーザ インターフェイスから報告されます。次の中から選択できます。 • `priority`。イベントの優先順位によってキュー内のイベントを並べ替えます。 • `content_length`。最も長い識別コンテンツの一致によってイベントを並べ替えます。イベントがコンテンツ長によって並べ替えられる場合、ルール イベントは常にデコーダ イベントおよびプリプロセッサ イベントよりも優先されます。

1 個のパケットまたはストリームに対して記録されるイベント数の設定:

ステップ 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(Access Control)] 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定(Advanced)] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[パフォーマンス設定(Performance Settings)] の横にある編集アイコン( )をクリックし、表示されるポップアップ ウィンドウで [侵入イベント ロギング制限(Intrusion Event Logging Limits)] タブを選択します。

ステップ 5　侵入イベント ロギング制限のオプションの表の任意のオプションを変更できます。

ステップ 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。設定変更の展開(4-12 ページ)を参照してください。

パケットおよび侵入ルール遅延しきい値の設定

ライセンス:Protection

デバイスの遅延をパケットおよびルール遅延しきい値構成の許容レベルで保持する必要性とセキュリティのバランスを保つことができます。詳細については、以下を参照してください。

- パケット遅延しきい値構成について(10-10 ページ)
- パケット遅延しきい値構成の設定(10-12 ページ)
- ルール遅延しきい値構成について(10-13 ページ)
- ルール遅延しきい値構成の設定(10-14 ページ)

パケット遅延しきい値構成について

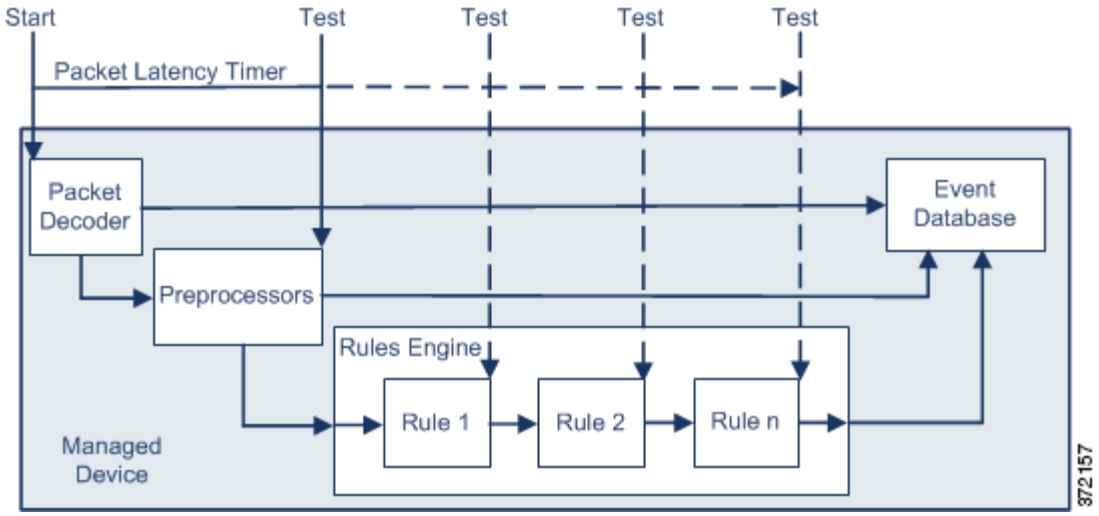
ライセンス:Protection

パケット遅延しきい値構成を有効にすることで、遅延を許容レベルで保持する必要性とセキュリティのバランスを取ることができます。パケット遅延しきい値構成は、該当するデコーダ、プリプロセッサ、およびルールによるパケット処理の総経過時間を測定し、処理時間が設定可能なしきい値を超えるとパケットのインスペクションを終了します。

パケット遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値構成は、厳密なタイミングを強制しないソフトウェア ベースの遅延実装です。

遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。ただし、パケット遅延しきい値構成では、セキュリティと接続性のバランスを取るために使用可能なツールが用意されています。

デコーダの処理の開始時に各パケットのタイマーが起動します。タイミングは、パケットのすべての処理が終了するか、または処理時間がタイミング テスト ポイントでしきい値を超えるまで継続します。



上の図に示すように、パケット遅延タイミングは次のテスト ポイントでテストされます。

- すべてのデコーダおよびプリプロセッサの処理の完了後、ルールの処理が開始される前
- 各ルールによる処理の後

処理時間が任意のテスト ポイントでしきい値を超えると、パケットの検査は停止します。

ヒント　パケットの合計処理時間にルーチン TCP ストリームまたは IP フラグメント再構成の時間は含まれません。

パケット遅延しきい値構成は、パケットを処理するデコーダ、プリプロセッサ、またはルールによってトリガーされるイベントに影響を与えません。該当するデコーダ、プリプロセッサ、またはルールは、パケットが完全に処理されるか、または遅延しきい値を超えたためにパケット処理が終了されるか、どちらか先に発生した時点まで通常通りトリガーされます。廃棄ルールがインライン展開の侵入を検知すると、その廃棄ルールがイベントをトリガーし、パケットは廃棄されます。

（注）　パケット遅延しきい値違反のためにパケットの処理が終了した後は、ルールに対してパケットは評価されません。イベントを引き起こす可能性があったルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

廃棄ルールの詳細については、ルール状態の設定（24-21 ページ）を参照してください。

パケット遅延のしきい値は、パッシブおよびインライン展開の両方でシステムのパフォーマンスを向上させ、インライン展開では過度の処理時間を必要とするパケットの検査を停止することにより遅延を低減できます。これらのパフォーマンス上のメリットは、以下のような場合にもたらされます。

- パッシブ展開およびインライン展開の両方で、複数のルールによるパケットの順次検査に長時間かかる場合
- インライン展開で、ユーザが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット処理を遅らせる場合

パッシブ展開では、パケットの処理を停止しても、処理が単に次のパケットに移るだけで、ネットワーク パフォーマンスの回復につながらない可能性があります。

パケット遅延しきい値構成の設定

ライセンス：Protection

次の表に、パケット遅延しきい値構成でユーザが設定できるオプションを示します。

表 ***10-4***　パケット遅延しきい値構成オプション

オプション	説明
しきい値（マイクロ秒）（Threshold (microseconds)）	パケットのインスペクションが終了する時間をマイクロ秒単位で指定します。推奨される最小しきい値の設定については、最小のパケット遅延しきい値設定の表を参照してください。

ルール 134:3 を有効にして、パケット遅延しきい値を超えたためにシステムがパケットのインスペクションを終了するイベントを生成できます。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

システム パフォーマンスおよびパケット遅延の測定に影響する要因は、CPU 速度、データ レート、パケット サイズ、プロトコル タイプなど多数あります。このためシスコは、ユーザ独自の計算によってご自身のネットワーク環境に合った設定を行うまで、次の表のしきい値設定を使用することを推奨します。

表 ***10-5***　最小のパケット遅延しきい値設定

データ レート	最小しきい値設定（マイクロ秒）
1 Gbps	100
100 Mbps	250
5 Mbps	1000

独自の設定を計算する場合は、次の項目を決定します。

- 1 秒あたりの平均パケット数
- 1 パケットあたりの平均マイクロ秒数

パケット インスペクションを不必要に中断することがないように、ネットワークの 1 パケットあたりの平均マイクロ秒数に重要な安全係数を乗算します。

たとえば、最小のパケット遅延しきい値設定の表では、1 ギガビット環境で 100 マイクロ秒の最小パケット遅延しきい値を推奨しています。この最小推奨値は、1 秒あたり平均 250,000 パケットを示すテスト データに基づいています。これは、1 マイクロ秒あたり 0.25 パケット、言い換えると 1 パケットあたり 4 マイクロ秒に相当します。25 倍すると推奨最小しきい値の 100 マイクロ秒が得られます。

パケット遅延しきい値の設定：

ステップ **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（Access Control）] 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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [パケット処理（Packet Handling）] タブを選択します。

ステップ 5　推奨される最小しきい値の設定については、最小のパケット遅延しきい値設定の表を参照してください。

ステップ 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。設定変更の展開（4-12 ページ）を参照してください。

ルール遅延しきい値構成について

ライセンス：Protection

ルール遅延しきい値構成を有効にすることで、遅延を許容レベルで保持する必要性とセキュリティのバランスを取ることができます。ルール遅延しきい値構成は、各ルールが個別のパケットの処理に費やした時間を測定し、処理時間が遅延しきい値ルールをある回数（設定可能）連続して超えた場合は、そのルールに違反した処理を、関連するルールのグループとともに指定された期間中断し、中断期間終了後にルールを回復します。

ルール遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値構成は、厳密なタイミングを強制しないソフトウェア ベースの遅延実装です。

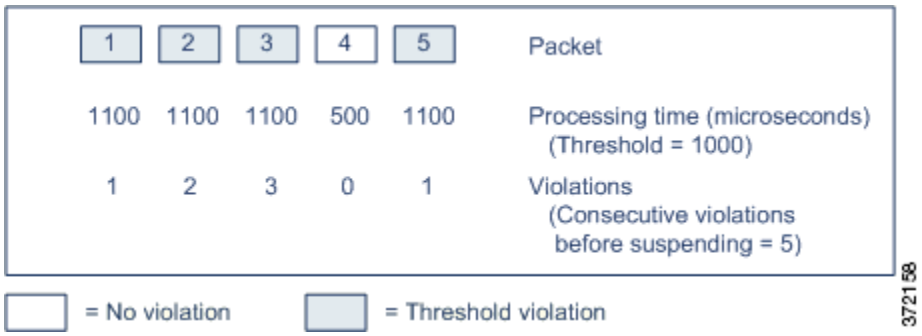
遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。ただし、ルール遅延しきい値構成では、セキュリティと接続性のバランスを取るために使用可能なツールが用意されています。

パケットがルールのグループに対して処理されるたびに、タイマーが処理時間を測定します。ルール処理時間が指定されたルール遅延しきい値を超えると、システムでカウンタが増加します。連続したしきい値違反の数が指定した数に達すると、システムは次のアクションを実行します。

- 指定された時間、ルールを一時停止する
- ルールが一時停止されたことを示すイベントをトリガーとして使用する
- 一時停止期間が過ぎたらルールを再度有効にする
- ルールが再び有効になったことを示すイベントをトリガーとして使用する

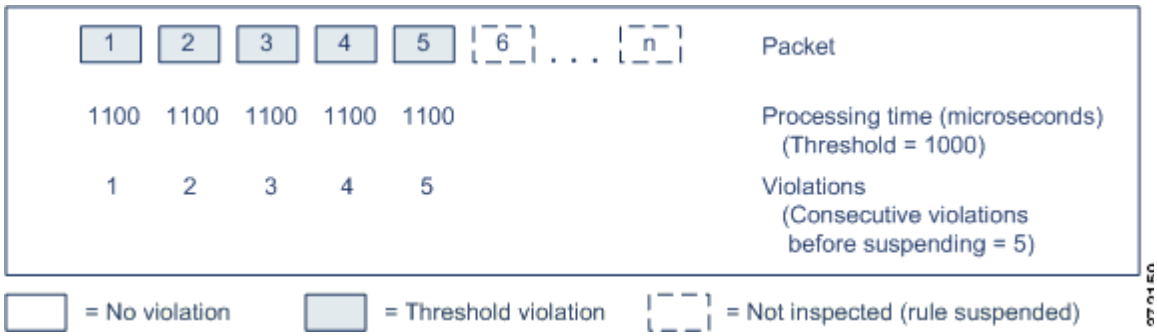
ルールのグループが一時停止しているか、またはルール違反が連続していない場合は、カウンタがゼロになります。ルールを一時停止する前に連続する違反の一部を許可することにより、パフォーマンスへの影響がわずかであると考えられる散発的なルール違反を無視し、繰り返しルール遅延しきい値を超えるルールのより重大な影響に焦点を当てることができます。

次の例は、ルールが一時停止にならない、5 つの連続したルール処理時間を示します。



上の例で、最初の 3 個の各パケットの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反し、違反カウンタは各違反のたびに増加します。4 個目のパケット処理はしきい値に違反しないので、違反カウンタはゼロにリセットされます。5 個目のパケットはしきい値に違反し、違反カウンタは 1 から再開します。

次の例は、ルールが一時停止になる、5 つの連続したルール処理時間を示します。



2 番目の例で、5 個のパケットのそれぞれの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反します。各パケットの 1100 マイクロ秒というルール処理時間が指定された連続する 5 回の違反に対する 1000 マイクロ秒というしきい値に違反するため、ルールのグループは一時停止されます。図中のパケット 6 から n で表される後続のパケットは、一時停止期間が経過するまで、一時停止されたルールに対して検査されません。ルールが再有効化された後にさらにパケットが発生すると、違反カウンタはゼロから再開されます。

ルール遅延しきい値構成は、パケットを処理するルールによってトリガーされる侵入イベントに影響を及ぼしません。ルール処理時間がしきい値を超えるかどうかにかかわらず、パケット内で検出されるすべての侵入に対して、ルールはイベントをトリガーします。侵入を検知するルールがインライン展開の廃棄ルールである場合、パケットは廃棄されます。廃棄ルールがパケット内で侵入を検出し、その結果ルールが一時停止されると、廃棄ルールは侵入イベントをトリガーし、パケットは廃棄され、そのルールと関連するすべてのルールが一時停止されます。廃棄ルールの詳細については、ルール状態の設定（24-21 ページ）を参照してください。

（注）　パケットは一時停止されたルールに対して評価されません。イベントを引き起こす可能性があった一時停止ルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

ルール遅延しきい値構成は、パッシブとインラインの両方の展開でシステムのパフォーマンスを向上することができます。また、パケットの処理に最も多くの時間を必要とするルールを一時停止することで、インライン展開の遅延を減らすことができます。設定可能な時間が過ぎるまで、パケットは一時停止されたルールに対して再度評価されず、過負荷のデバイスに回復の時間が与えられます。これらのパフォーマンス上のメリットは、以下のような場合にもたらされます。

- 短期間で作成され、ほとんどテストされていないルールが過剰な処理時間を必要とする場合
- ユーザが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット インスペクションを遅らせる場合

ルール遅延しきい値構成の設定

ライセンス：Protection

ルール遅延しきい値、一時停止されるルールの一時停止時間、ルールを一時停止する前に発生する必要がある連続したしきい値違反の回数の変更を行うことができます。

ルールによるパケット処理時間が、[ルール停止前の連続しきい値違反（Consecutive Threshold Violations Before Suspending Rule）] で指定された回数連続して [しきい値（Threshold）] を超えると、ルール遅延しきい値構成は [停止時間（Suspension Time）] で指定された時間、ルールを一時停止します。

ルール 134:1 を有効にして、ルールが一時停止されるときにイベントを生成できます。また、ルール 134:2 を有効にして、一時停止されたルールが有効化されるときにイベントを生成できます。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

次の表に、ルール遅延しきい値構成でユーザが設定できるオプションを示します。

表 ***10-6***　ルール遅延しきい値構成オプション

オプション	説明
しきい値（Threshold）	ルールがパケットを検査する際に超えることができない時間をマイクロ秒単位で指定します。推奨される最小しきい値の設定については、最小のルール遅延しきい値設定の表を参照してください。
ルール停止前の連続しきい値違反（Consecutive Threshold Violations Before Suspending Rule）	ルールが一時停止される前に、ルールによるパケットの検査時間が [しきい値（Threshold）] で設定された時間を超えることができる、連続した回数を指定します。
停止時間（Suspension Time）	ルールのグループを一時停止する秒数を指定します。

システム パフォーマンスの測定に影響する要因は、CPU 速度、データ レート、パケット サイズ、プロトコル タイプなど多数あります。このためシスコは、ユーザ独自の計算によってご自身のネットワーク環境に合った設定を行うまで、次の表のしきい値設定を使用することを推奨します。

表 ***10-7***　最小のルール遅延しきい値設定

データ レート	最小しきい値設定（マイクロ秒）
1 Gbps	500
100 Mbps	1250
5 Mbps	5000

独自の設定を計算する場合は、次の項目を決定します。

- 1 秒あたりの平均パケット数
- 1 パケットあたりの平均マイクロ秒数

ルールを不必要に一時停止することがないように、ネットワークの 1 パケットあたりの平均マイクロ秒数に重要な安全係数を乗算します。

ルール遅延しきい値の設定:

ステップ **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（Access Control）] 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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] の横にある編集アイコン（ ）をクリックし、表示されるポップアップ ウィンドウで [ルール処理（Rule Handling）] タブを選択します。

ステップ 5　ルール遅延しきい値構成オプションの表の任意のオプションを設定できます。

推奨される最小しきい値の設定については、最小のルール遅延しきい値設定の表を参照してください。

ステップ 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。設定変更の展開（4-12 ページ）を参照してください。

侵入パフォーマンス統計情報のロギングの設定

ライセンス：Protection

デバイスがそのパフォーマンスをモニタおよび報告する動作に関する基本的なパラメータを設定できます。次のオプションを設定することにより、システムがデバイスのパフォーマンス統計情報を更新する間隔を指定できます。

[サンプル時間（秒）（Sample time (seconds)）] と **[パケットの最小数（Minimum number of packets）]**

パフォーマンス統計情報の各更新の間で指定した秒数が経過すると、システムは指定したパケット数を分析したかを検証します。分析していた場合、システムはパフォーマンス統計情報を更新します。それ以外の場合、システムは指定したパケット数を分析するまで待機します。

トラブルシューティング オプション：**[ログ セッション/プロトコル分布（Log Session/Protocol Distribution）]**

トラブルシューティングの電話中に、プロトコル分布、パケット長、およびポートの統計情報のログを取るようにサポートから依頼される場合があります。

注意　このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

トラブルシューティング オプション：**[概要（Summary）]**

トラブルシューティングの電話中に、Snort® プロセスのシャット ダウンまたは再起動時に限り、パフォーマンス統計情報を計算するようにシステムを設定するようにサポートから依頼される場合があります。このオプションを有効にするには、[ログ セッション/プロトコル分布（Log Session/Protocol Distribution）] トラブルシューティング オプションも有効にする必要があります。

注意　このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

基本的なパフォーマンス統計情報パラメータの設定：

ステップ 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（Access Control）] 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定(Advanced)] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[パフォーマンス設定(Performance Settings)] の横にある編集アイコン( )をクリックし、表示されるポップアップ ウィンドウで [パフォーマンス統計情報(Performance Statistics)] タブを選択します。

ステップ 5　前述のように、[サンプル時間(Sample time)] または [パケットの最小数(Minimum number of packets)] を変更します。

ステップ 6　任意で、サポートによって求められた場合にのみ、[トラブルシューティング オプション(Troubleshoot Options)] セクションを展開し、そのオプションを変更します。

ステップ 7　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。設定変更の展開(4-12 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

ライセンス:Protectionまたはマルウェア

ファイル制御あるいはマルウェアの検出またはブロッキングを行うためにファイル ポリシーを使用する場合は、次の表にリストするオプションを設定できます。ファイル サイズを増やすと、システムのパフォーマンスに影響を与える可能性があることに注意してください。

表 *10-8*　アクセス コントロール ファイルおよびマルウェア検出の詳細オプション

フィールド	説明	デフォルト値	範囲	注記
ファイルタイプを検知する前に検閲するバイト数制限(**Limit the number of bytes inspected when doing file type detection**)	ファイル タイプを検出するときに検査するバイト数を指定します。	1460 バイト、または TCP パケットの最大セグメント サイズ	0 ～ 4294967295 (4GB)	制限を取り除くには、0 に設定します。 ほとんどの場合、システムは最初のパケットによって、一般的なファイル タイプを特定できます。
SHA-256 ハッシュ値を計算するファイルの上限サイズ(バイト)(**Do not calculate SHA-256 hash values for files larger than (in bytes)**)	システムが特定のサイズを超えるファイルを保管すること、ファイルで Collective Security Intelligence クラウド ルックアップを実行すること、またはカスタム検出リストに追加されたファイルをブロックすることを防止します。	10485760 (10MB)	0 ～ 4294967295 (4GB)	制限を取り除くには、0 に設定します。

表 10-8　アクセス コントロール ファイルおよびマルウェア検出の詳細オプション（続き）

フィールド	説明	デフォルト値	範囲	注記
ファイルを許可するのにかかるマルウェア ブロックのクラウド ルックアップの制限時間（秒）（**Allow file if cloud lookup for Block Malware takes longer than (seconds)**）	マルウェア クラウド ルックアップの実行中に、システムが [マルウェア ブロック（Block Malware）] ルールに一致し、性質がキャッシュに入れられていないファイルを保持する期間を指定します。システムが性質を取得する前にこの期間が満了すると、ファイルが渡されます。「使用不可」の性質はキャッシュに入れられません。	2 秒	0 ～ 30 秒	このオプションは最大 30 秒に設定できますが、シスコではデフォルト値を使用して、接続失敗によってトラフィックがブロックされないようにすることを推奨します。サポートに連絡することなくこのオプションを 0 に設定しないでください。

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を設定するには、次の手順を実行します。

ステップ 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（Access Control）] 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ファイルおよびマルウェアの設定（Files and Malware Settings）] の横にある編集アイコン（ ）をクリックします。

[ファイルおよびマルウェアの設定（Files and Malware Settings）] ポップアップ ウィンドウが表示されます。

ステップ 5　アクセス コントロール ファイルおよびマルウェア検出の詳細オプションの表の任意のオプションを設定できます。

ステップ 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。設定変更の展開（4-12 ページ）を参照してください。

トラフィック復号の概要

デフォルトでは、ASA FirePOWER モジュールはセキュア ソケット レイヤ（SSL）または Transport Layer Security（TLS）プロトコルで暗号化されたトラフィックを検査できません。アクセス コントロールの一部として *SSL* インスペクション機能を使用すると、暗号化トラフィックのインスペクションを実行せずにブロックしたり、暗号化または復号されたトラフィックをアクセス コントロールで検査したりできます。暗号化されたセッションをモジュールが処理するときは、トラフィックの詳細がログに記録されます。暗号化トラフィックのインスペクションと暗号化セッションのデータ分析を組み合わせることで、ネットワーク内の暗号化されたアプリケーションやトラフィックをより詳細に把握したり制御したりできます。

モジュールで TCP 接続での SSL または TLS ハンドシェイクが検出されると、そのトラフィックを復号できるかどうかが判定されます。復号できない場合は、設定されたアクションが適用されます。以下のアクションを設定できます。

- 暗号化されたトラフィックをブロックし、オプションで TCP 接続をリセットする
- 暗号化されたトラフィックを復号しない

暗号化されたトラフィックの通過が SSL インスペクション設定で許可される場合、または SSL インスペクションが設定されていない場合は、そのトラフィックがアクセス コントロール ルールによって処理されることに注意してください。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、システムは暗号化ペイロードの侵入およびファイル インスペクションを無効にしています。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。詳細については、アクセス コントロール ルールの作成および編集（6-2 ページ）およびSSL プリプロセッサの使用（19-78 ページ）を参照してください。

モジュールによるトラフィックの復号が可能な場合は、それ以上のインスペクションなしでトラフィックをブロックするか、復号されていないトラフィックをアクセス コントロールによって評価するか、あるいは次のいずれかの方法を使用して復号します。

- 既知の秘密キーを使用して復号する。外部ホストがネットワーク上のサーバとの SSL ハンドシェイクを開始すると、交換されたサーバ証明書とアプライアンスにアップロード済みのサーバ証明書が照合されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号します。
- サーバ証明書の再署名によって復号する。ネットワーク上のホストが外部サーバとの SSL ハンドシェイクを開始すると、交換されたサーバ証明書がアップロード済みの認証局（CA）証明書で再署名されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号します。

復号されたトラフィックに対しては、はじめから暗号化されていないトラフィックと同じ処理と分析が施されます。これには、ネットワーク、レピュテーション、ユーザ ベースのアクセス コントロール、侵入の検知と防止、高度なマルウェア防御が該当します。復号されたトラフィックのポスト分析をブロックしない場合、トラフィックは再暗号化されて宛先ホストに渡されます。

（注）　トラフィックのブロックや発信トラフィックの復号など、いくつかの SSL インスペクション アクションはトラフィックのフローを変更します。これらのアクションを実行できるのは、インラインに配置されたASA FirePOWER モジュールです。パッシブに配置された ASA FirePOWER モジュールは、トラフィック フローを変更できません。ただし、これらのデバイスでも着信トラフィックを復号することは可能です。詳細については、例:パッシブ展開でのトラフィック復号（11-5 ページ）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。

- SSL インスペクションの要件（11-2 ページ）
- SSL インスペクション アプライアンス展開の分析（11-4 ページ）

SSL インスペクションの要件

ライセンス:機能によって異なる

構成設定やライセンスに加え、デバイスをネットワーク上にどのように展開しているかにより、暗号化トラフィックの制御や復号に適用できるアクションが異なります。

SSL インスペクションの一部の機能では、公開キー証明書と秘密キーのペアが必要です。暗号化セッションの特性に応じてトラフィックを復号したり制御したりするためには、証明書および秘密キーのペアを ASA FirePOWER モジュールにアップロードする必要があります。

詳細については、次の項を参照してください。

- SSL インスペクションをサポートする ASA FirePOWER モジュールの導入（11-2 ページ）
- SSL インスペクションのライセンス要件（11-3 ページ）
- SSL ルールを設定するために必要な情報の収集（11-3 ページ）

SSL インスペクションをサポートする ASA FirePOWER モジュールの導入

ライセンス:任意

に設定および展開された デバイスASA FirePOWER モジュールでは、トラフィック フローの変更が可能です。これらのデバイスでは、着信および発信トラフィックのモニタリング、ブロック、許可、および復号を行うことができます。

パッシブに設定および展開された ASA FirePOWER モジュールでは、トラフィック フローを変更することはできません。これらのデバイスで行えるのは、着信トラフィックのモニタリング、許可、および復号だけです。パッシブ展開では、一時 Diffie-Hellman（DHE）および楕円曲線 Diffie-Hellman（ECDHE）の暗号スイートを使用した暗号化トラフィックの復号はサポートされません。

最適な展開タイプを決定するときは、マッピングされたアクション、既存のネットワーク展開、および全体的な要件のリストを確認してください。詳細については、SSL インスペクション アプライアンス展開の分析（11-4 ページ）を参照してください。

SSL インスペクションのライセンス要件

ライセンス:機能によって異なる

ライセンスによっては、いくつかの条件を組み合わせて暗号化トラフィックの処理方法を決定できます。ASA FirePOWER モジュールでは、ご使用の展開環境でサポートされない機能を示すために、警告アイコン(⚠)および確認ダイアログ ボックスを使用します。警告アイコンの上にポインタを置くと詳細が表示されます。

アクセス コントロール ポリシーの一部として SSL ポリシーを適用すると、SSL ポリシーで復号されたトラフィックがこのアクセス コントロール ポリシーにより検査されます。アクセス コントロールのライセンスの詳細については、アクセス コントロールのライセンスおよびロール要件(4-2 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 ポリシーの一部として SSL ポリシーを適用するためのライセンス要件を示します。

表 *11-1*　*SSL* インスペクションのライセンスの要件

SSL ポリシーの機能	ライセンス
ゾーン、ネットワーク、ポート、または SSL 関連の基準に基づいて、暗号化されたトラフィックを処理する	任意
位置情報のデータを使用して暗号化トラフィックを処理する	任意
アプリケーションまたはユーザの条件を使用して暗号化トラフィックを処理する	Control
URL カテゴリおよびレピュテーション データを使用して暗号化されたトラフィックをフィルタ処理する	URL フィルタリング(URL Filtering)

SSL ルールを設定するために必要な情報の収集

ライセンス:機能に依存

SSL インスペクションは、サポートする公開キー インフラストラクチャ(PKI)の多くの情報に依存しています。照合ルールの条件を設定するときは、その組織におけるトラフィック パターンについて検討する必要があります。次の表に示す情報を収集しておく必要があります。

表 *11-2*　*SSL* ルール条件の設定に必要な情報

一致対象	必要な情報
自己署名サーバ証明書を含む、検出されたサーバ証明書	サーバ証明書
信頼できるサーバ証明書	CA 証明書
検出されたサーバ証明書のサブジェクトまたは発行元	サーバ証明書のサブジェクト DN または発行元 DN

詳細については、SSL ルールを使用したトラフィック復号の調整(14-1 ページ)を参照してください。

ルールの適用先となる暗号化トラフィックの復号、ブロック、モニタリングが不要かどうか、または復号が必要かどうかについて検討します。その結果を、SSL ルールのアクション、復号できないトラフィックのアクション、および SSL ポリシーのデフォルト アクションに反映させます。トラフィックを復号する場合は、次の表に示す情報を収集しておく必要があります。

表 ***11-3*** ***SSL*** 復号に必要な情報

復号の対象	必要な情報
制御対象のサーバへの着信トラフィック	サーバ証明書のファイルと秘密キー ファイルのペア
外部サーバへの発信トラフィック	CA 証明書のファイルと秘密キー ファイルのペア CA 証明書と秘密キーを生成することもできます。

詳細については、ルール アクションを使用した暗号化トラフィックの処理と検査の決定（13-9 ページ）を参照してください。

これらの情報を収集したら、システムにアップロードして、再利用可能なオブジェクトを設定します。詳細については、再利用可能なオブジェクトの管理（2-1 ページ）を参照してください。

SSL インスペクション アプライアンス展開の分析

ライセンス：機能に依存

ここでは Life Insurance Example, Inc.（LifeIns）という架空の生命保険会社で使われる複数のシナリオを例にして、同社のプロセス監査で利用されている暗号化トラフィックの SSL インスペクションについて解説します。LifeIns はそのビジネス プロセスに基づいて、以下の展開を計画しています。

- カスタマー サービス部門では、単一の ASA FirePOWER デバイスをパッシブ展開する
- 契約審査部門では、単一の ASA FirePOWER デバイスをインライン展開する

カスタマー サービスのビジネス プロセス

LifeIns はすでに顧客対応用の Web サイトを構築済みです。LifeIns は、保険契約に関する見込み顧客からの暗号化された質問や要求を、Web サイトや電子メールで受け取ります。LifeIns のカスタマー サービスは、これらの要求を処理して 24 時間以内に必要な情報を返信しなければなりません。カスタマー サービスでは、着信するコンタクト メトリックのコレクションを拡張したいと思っています。LifeIns では、すでにカスタマー サービスに対する内部監査用のレビューが確立されています。

また、LifeIns は暗号化された申請書もオンラインで受信します。カスタマー サービス部門は申請書を 24 時間以内に処理し、申請書類のファイルを契約審査部門に送信しなければなりません。カスタマー サービスでは、オンライン フォームからの不正な申請をすべて除外するようにしていますが、この作業が同部門での作業のかなりの部分を占めています。

契約審査部門のビジネス プロセス

LifeIns の契約審査担当者は、Medical Repository Example, LLC（MedRepo）という医療データ リポジトリに、オンラインで暗号化された医療情報要求を送信します。MedRepo はこれらの要求を評価し、LifeIns に暗号化されたレコードを 72 時間以内に送信します。その後は契約審査担当者が申請書類を査定し、保険契約および保険料に関連する判定を送信します。契約審査部門では、そのメトリック コレクションを拡張したいと思っています。

最近、不明な送信元からのスプーフィング（なりすまし）応答が LifeIns に送られてくるようになりました。LifeIns の契約審査担当者はインターネット使用に関する適切なトレーニングを受けていますが、LifeIns の IT 部門はまず、医療応答の形式で送られてくる暗号化トラフィックをすべて分析し、すべてのスプーフィング行為をブロックしたいと考えています。

LifeIns では、経験の浅い契約審査担当者に対して 6 ヵ月のトレーニング期間を設けています。最近、こうした契約審査担当者が MedRepo のカスタマー サービス部門への暗号化された医療規制リクエストの送信を正しく行わない事例がありました。そのため MedRepo から LifeIns に複数の苦情が提出されています。LifeIns は、新任の契約審査担当者用のトレーニング期間を延長し、契約審査担当者から MedRepo への要求についても監査を入れることを計画しています。

詳細については、次の項を参照してください。

- 例：パッシブ展開でのトラフィック復号（11-5 ページ）
- 例：インライン展開でのトラフィック復号（11-7 ページ）

例：パッシブ展開でのトラフィック復号

ライセンス：機能に依存

LifeIns のビジネス要件では、カスタマー サービスに次の要求をしています。

- すべての要求と申請書類を 24 時間以内に処理する
- 着信するコンタクト メトリックのコレクション プロセスを改善する
- 着信した不正な申請書類を特定して廃棄する

カスタマー サービス部門では、追加の監査用レビューを必要としません。

LifeIns ではカスタマー サービス デバイスのパッシブ展開を計画しています。

外部ネットワークからのトラフィックは LifeIns のルータに送信されます。ルータはトラフィックをカスタマー サービス部門にルーティングし、検査用にトラフィックのコピーを ASA FirePOWER モジュールに送信します。

管理する ASA FirePOWER モジュールでは、[アクセス コントロール（Access Control）] および [SSL エディタ（SSL Editor）] のカスタム ロールを持つユーザにより、次の SSL インスペクションの設定を行います。

- カスタマー サービス部門に送信された暗号化トラフィックをすべてログに記録する
- オンラインの申請フォームからカスタマー サービスに送信された暗号化トラフィックを復号する
- カスタマー サービスに送信された他の暗号化トラフィックは、オンライン リクエスト フォームからのトラフィックも含め、すべて復号しない

さらに、復号された申請フォーム トラフィック中に偽の申請データが含まれていないかを検査し、検出された場合はログに記録するためのアクセス コントロールも設定します。

次のシナリオでは、ユーザからカスタマー サービスにオンライン フォームが送信されます。ユーザのブラウザは、サーバとの TCP 接続を確立してから、SSL ハンドシェイクを開始します。ASA FirePOWER モジュールは、このトラフィックのコピーを受信します。クライアントとサーバが SSL ハンドシェイクを完了することで、暗号化されたセッションが確立されます。システムは、ハンドシェイクと接続の詳細に応じて、接続のログを記録し、暗号化トラフィックのコピーを処理します。

詳細については、次のトピックを参照してください。

- パッシブ展開で暗号化トラフィックをモニタする（11-6 ページ）
- パッシブ展開で暗号化トラフィックを復号しない（11-6 ページ）
- パッシブ展開で暗号化トラフィックを秘密キーで検査する（11-6 ページ）

パッシブ展開で暗号化トラフィックをモニタする

ライセンス:任意

システムは、カスタマー サービスに送信されるすべての SSL 暗号化トラフィックについて、接続のログを記録します。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`info`）を送信します。クライアントがこれを暗号化（`AaBb`）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、ASA FirePOWER モジュールにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（`AaBb`）を受信し、これをプレーン テキスト（`info`）に復号します。
4. モジュールはトラフィックを復号しません。

   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、モジュールは接続イベントを生成します。
5. ASA FirePOWER モジュールが接続イベントを受信します。

パッシブ展開で暗号化トラフィックを復号しない

ライセンス:任意

保険契約に関する要求を含むすべての SSL 暗号化トラフィックは復号されずに許可され、接続のログが記録されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`info`）を送信します。クライアントがこれを暗号化（`AaBb`）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、ASA FirePOWER モジュールにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（`AaBb`）を受信し、これをプレーン テキスト（`info`）に復号します。
4. ASA FirePOWER モジュールはトラフィックを復号しません。

   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、モジュールは接続イベントを生成します。
5. ASA FirePOWER モジュールが接続イベントを受信します。

パッシブ展開で暗号化トラフィックを秘密キーで検査する

ライセンス:任意

申請フォームのデータを含むすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。

（注）　パッシブ展開の場合、DHE または ECDHE 暗号スイートで暗号化されたトラフィックは、既知の秘密キーを使って復号することはできません。

有効な申請フォームの情報を含むトラフィックについては、接続のログが記録されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（form）を送信します。クライアントがこれを暗号化（AaBb）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、ASA FirePOWER モジュールにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（AaBb）を受信し、これをプレーン テキスト（form）に復号します。
4. ASA FirePOWER モジュールは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、暗号化トラフィックをプレーン テキスト（form）に復号します。

   アクセス コントロール ポリシーは、復号されたトラフィックの処理を継続します。偽の申請書であることを示す情報は検出されません。セッション終了後、モジュールは接続イベントを生成します。
5. ASA FirePOWER モジュールは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、復号されたトラフィックに偽の申請データが含まれていた場合、接続および偽のデータについてのログが記録されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（fake）を送信します。クライアントがこれを暗号化（CcDd）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、デバイスにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（CcDd）を受信し、これをプレーン テキスト（fake）に復号します。
4. ASA FirePOWER モジュールは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、暗号化トラフィックをプレーン テキスト（fake）に復号します。

   アクセス コントロール ポリシーは、復号されたトラフィックの処理を継続して、偽の申請書であることを示す情報を検出します。モジュールは侵入イベントを生成します。セッション終了後、デバイスは接続イベントを生成します。
5. ASA FirePOWER モジュールは、暗号化および復号されたトラフィックの情報とともに、接続イベントおよび偽の申請データの侵入イベントを受信します。

例:インライン展開でのトラフィック復号

ライセンス:機能に依存

LifeIns のビジネス要件では、契約審査部門に次の要求をしています。

- 新採用および経験の浅い契約審査担当者を監査し、MedRepo への情報要求が適切なすべての規則に準じていることを検証する
- その契約審査によるメトリック コレクション プロセスを改善する
- MedRepo が送信元と思われるすべての要求を調査し、スプーフィング行為を排除する
- 契約審査部門から MedRepo のカスタマー サービス部門へのすべての不適切な規制要求を排除する
- 経験豊富な契約審査担当者は監査しない

LifeIns の契約審査部門では、デバイスのインライン展開を計画しています。

MedRepo のネットワークからのトラフィックは、MedRepo のルータに流されます。そこから LifeIns のネットワークにトラフィックがルーティングされます。管理対象デバイスはトラフィックを受信し、許可されたトラフィックを LifeIns のルータに転送して、ASA FirePOWER モジュールにイベントを送信します。LifeIns のルータは、トラフィックを宛先ホストにルーティングします。

ASA FirePOWER モジュールでは、次の SSL インスペクションの設定を行います。

- 契約審査部門に送信された暗号化トラフィックをすべてログに記録する
- LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信された暗号化トラフィックをすべてブロックする
- MedRepo から LifeIns の契約審査部門宛て、および LifeIns の経験の浅い契約審査担当者から MedRepo のリクエスト部門宛てに送信される暗号化トラフィックをすべて復号する
- 経験豊富な契約審査担当者から送信される暗号化トラフィックは復号しない

さらに、カスタムの侵入ポリシーと以下の設定を使用して、復号トラフィックを検査するアクセス コントロールを設定します。

- 復号トラフィックでスプーフィング行為が検出された場合はそのトラフィックをブロックし、スプーフィング行為をログに記録する
- 規制に準拠しない情報を含んでいる復号トラフィックをブロックし、不適切な情報をログに記録する
- 他の暗号化および復号されたトラフィックをすべて許可する

許可された復号トラフィックは、再暗号化されて宛先ホストに転送されます。

次のシナリオでは、ユーザが情報をオンラインでリモート サーバに送信します。ユーザのブラウザは、サーバとの TCP 接続を確立してから、SSL ハンドシェイクを開始します。モジュールはこのトラフィックを受信し、ハンドシェイクと接続の詳細に応じて、システムが接続をログに記録し、トラフィックを処理します。システムがトラフィックをブロックした場合、TCP 接続も切断されます。トラフィックがブロックされない場合、クライアントとサーバが SSL ハンドシェイクを完了することで、暗号化されたセッションが確立されます。

詳細については、次のトピックを参照してください。

- インライン展開で暗号化トラフィックをモニタする（11-8 ページ）
- インライン展開で特定ユーザからの暗号化トラフィックを許可する（11-9 ページ）
- インライン展開で暗号化トラフィックをブロックする（11-9 ページ）
- インライン展開で暗号化トラフィックを秘密キーで検査する（11-10 ページ）
- インライン展開で特定ユーザの暗号化トラフィックを、再署名された証明書で検査する（11-10 ページ）

インライン展開で暗号化トラフィックをモニタする

ライセンス：任意

契約審査部門で送受信されるすべての SSL 暗号化トラフィックについて、接続のログが記録されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`help`）を送信します。クライアントがこれを暗号化（`AaBb`）し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。

3. ASA FirePOWER モジュール はトラフィックを復号しません。

   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. 契約審査部門のサーバは、暗号化された情報の要求（AaBb）を受信し、これをプレーン テキスト（help）に復号します。
6. ASA FirePOWER モジュールが接続イベントを受信します。

インライン展開で特定ユーザからの暗号化トラフィックを許可する

ライセンス：Control

経験豊富な契約審査担当者から送信されるすべての SSL 暗号化トラフィックは復号されずに許可され、接続のログが記録されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（help）を送信します。クライアントがこれを暗号化（AaBb）し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. ASA FirePOWER モジュールはトラフィックを復号しません。

   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. リクエスト部門のサーバは、暗号化された情報の要求（AaBb）を受信し、これをプレーン テキスト（help）に復号します。
6. ASA FirePOWER モジュールが接続イベントを受信します。

インライン展開で暗号化トラフィックをブロックする

ライセンス：任意

LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信されるすべての SMTPS 電子メール トラフィックは SSL ハンドシェイク時にブロックされ、追加の検査なしで接続のログが記録されます。

次のステップが実行されます。

1. カスタマー サービス部門のサーバは、クライアント ブラウザから SSL ハンドシェイクの確立要求を受信すると、SSL ハンドシェイクの次のステップとして、サーバ証明書（cert）を LifeIns の契約審査担当者に送信します。
2. MedRepo のルータが証明書を受信し、これを LifeIns の契約審査担当者にルーティングします。
3. ASA FirePOWER モジュールは追加の検査を行わずにトラフィックをブロックし、TCP 接続を終了します。これにより、接続イベントが生成されます。
4. 内部ルータは、ブロックされたトラフィックを受信しません。
5. 契約審査担当者は、ブロックされたトラフィックを受信しません。
6. ASA FirePOWER モジュールが接続イベントを受信します。

インライン展開で暗号化トラフィックを秘密キーで検査する

ライセンス:任意

MedRepo から LifeIns の契約審査部門に送信されるすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。復号には、アップロードされたサーバ秘密キーを使って取得されたセッション キーが使用されます。正規のトラフィックは許可され、再暗号化されて契約審査部門に送信されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求(`stats`)を送信します。クライアントがこれを暗号化(`AaBbC`)し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. 外部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
3. ASA FirePOWER モジュールは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト(`stats`)に復号します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続します。スプーフィング行為は検出されません。デバイスは暗号化トラフィック(`AaBbC`)を転送し、セッション終了後に接続イベントを生成します。
4. 内部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
5. 契約審査部門のサーバは、暗号化された情報(`AaBbC`)を受信し、これをプレーン テキスト(`stats`)に復号します。
6. ASA FirePOWER モジュールは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、スプーフィング行為の復号トラフィックはすべてドロップされ、接続およびスプーフィング行為についてのログが記録されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求(`spoof`)を送信しますが、このトラフィックは改変されており、発信元が MedRepo, LLC であるかのように偽装されています。クライアントがこれを暗号化(`FfGgH`)し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. ASA FirePOWER モジュールは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト(`spoof`)に復号します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続し、スプーフィング行為を検出します。ASA FirePOWER モジュールはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。
3. 内部ルータは、ブロックされたトラフィックを受信しません。
4. 契約審査部門のサーバは、ブロックされたトラフィックを受信しません。
5. ASA FirePOWER モジュールは、暗号化および復号されたトラフィックの情報とともに、接続イベントおよびスプーフィング行為の侵入イベントを受信します。

インライン展開で特定ユーザの暗号化トラフィックを、再署名された証明書で検査する

ライセンス:Control

新任および経験の浅い契約審査担当者から MedRepo のリクエスト部門に送信されるすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。復号には、再署名されたサーバ証明書を使って取得されたセッション キーが使用されます。正規のトラフィックは許可され、再暗号化されて MedRepo に送信されます。

（注）　インライン展開においてサーバ証明書の再署名によりトラフィックを復号する場合、ASA FirePOWER モジュールは中間者（man-in-the-middle）として機能します。ここでは 2 つの SSL セッション（クライアントと ASA FirePOWER モジュール の間に 1 つ、ASA FirePOWER モジュール とサーバの間に 1 つ）が作成されます。その結果、暗号セッションの詳細はセッションごとに異なります。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（help）を送信します。クライアントがこれを暗号化（AaBb）し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. ASA FirePOWER モジュールは、再署名されたサーバ証明書と秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（help）に復号します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続します。不適切な要求は検出されません。モジュールはトラフィックを再暗号化（CcDd）して、送信を許可します。セッション終了後、接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. リクエスト部門のサーバは、暗号化された情報（CcDd）を受信し、これをプレーン テキスト（help）に復号します。
6. ASA FirePOWER モジュールは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。

（注）　再署名されたサーバ証明書で暗号化されたトラフィックにより、信頼できない証明書についての警告がクライアントのブラウザに表示されます。この問題を避けるには、組織のドメイン ルートにある信頼できる証明書ストアまたはクライアントの信頼できる証明書ストアに CA 証明書を追加します。

これに対し、規制要件を満たさない情報を含んでいる復号トラフィックは、すべてドロップされます。接続および非準拠情報についてのログが記録されます。

次のステップが実行されます。

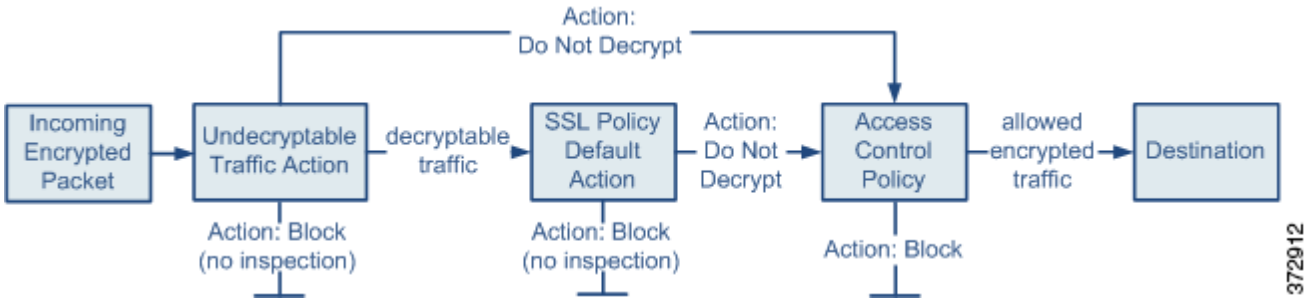
1. ユーザが規制要件に準拠していない要求をプレーン テキスト（regs）で送信します。クライアントがこれを暗号化（EeFf）し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. ASA FirePOWER モジュールは、再署名されたサーバ証明書と秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（regs）に復号します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続し、不適切な要求を検出します。モジュールはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。
4. 外部ルータは、ブロックされたトラフィックを受信しません。
5. リクエスト部門のサーバは、ブロックされたトラフィックを受信しません。
6. ASA FirePOWER モジュールは、暗号化および復号されたトラフィックの情報とともに、接続イベントおよび不適切な要求の侵入イベントを受信します。

SSL ポリシー クイック スタート ガイド

SSL ポリシーは、ネットワーク上の暗号化トラフィックをシステムがどのように処理するかを決定します。SSL ポリシーを、1 つまたは複数設定できます。SSL ポリシーをアクセス コントロール ポリシーに関連付け、そのアクセス コントロール ポリシーを適用します。ASA FirePOWER モジュールで TCP ハンドシェイクが検出されると、アクセス コントロール ポリシーは最初にトラフィックの処理と検査をします。次に TCP 接続上で SSL 暗号化セッションが識別された場合は、SSL ポリシーが引き継いで、暗号化トラフィックの処理および復号を行います。同時に適用できる SSL ポリシーは 1 つだけです。

最も単純な SSL ポリシーは、次の図のように、単一のデフォルト アクションで暗号化トラフィックを処理するように適用先のデバイスに指示します。デフォルト アクションは、それ以上のインスペクションなしで復号可能なトラフィックをブロックするか、あるいは復号可能なトラフィックを復号されていない状態でアクセス コントロールによって検査するように設定できます。システムは、暗号化されたトラフィックを許可するか、またはブロックできます。ASA FirePOWER モジュールは復号できないトラフィックを検出すると、トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号しないままにして、アクセス コントロールによる検査を行います。



この章では、単純な SSL 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、編集、更新、比較などの SSL ポリシー管理の基本情報も含まれています。詳細については、以下を参照してください。

- 基本 SSL ポリシーの作成（12-2 ページ）
- SSL ポリシーの編集（12-7 ページ）
- アクセス コントロールを使用した復号設定の適用（12-9 ページ）
- 現在のトラフィック復号設定のレポートの生成（12-10 ページ）
- SSL ポリシーの比較（12-11 ページ）

より複雑な SSL ポリシーでは、各種の復号できないトラフィックをさまざまなアクションで処理できます。また、認証局（CA）が証明書を発行したか、または暗号化証明書を信頼するかどうかに応じてトラフィックを制御したり、SSL ルールを使ってきめ細かな暗号化トラフィックの制御およびログの記録を行ったりできます。これらのルールには、単純なものや複雑なものがあり、複数の基準を使用して暗号化トラフィックの照合および検査を行います。基本的な SSL ポリシーの作成後は、個々の展開環境に応じた調整の詳細について、次の章を参照してください。

- 再利用可能なオブジェクトの管理（2-1 ページ）では、再利用可能な公開キー インフラストラクチャ（PKI）オブジェクトおよびその他の SSL インスペクション関連オブジェクトを設定して、トラフィックの復号や暗号化トラフィックの制御を強化する方法を説明しています。
- ネットワーク トラフィックの接続のロギング（33-1 ページ）では、復号可能および復号できない暗号化トラフィックに対するログの設定法を説明しています。
- アクセス コントロールを使用した復号設定の適用（12-9 ページ）では、SSL 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を説明しています。
- アクセス コントロール ポリシーの開始（4-1 ページ）では、アクセス コントロール ポリシーをデバイスに適用する方法を説明しています。
- 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、復号トラフィックを検査するアクセス コントロール ルールの設定法を説明しています。
- SSL ルール クイック スタート ガイド（13-1 ページ）では、暗号化トラフィックの処理とログを記録する SSL ルールの設定法を説明しています。
- SSL ルールを使用したトラフィック復号の調整（14-1 ページ）では、特定の暗号化トラフィックと SSL ルール条件の一致度を向上させる設定法を説明しています。

基本 SSL ポリシーの作成

ライセンス：任意

新しい SSL ポリシーを作成するために最低限必要な操作は、そのポリシーに一意の名前を付けて、ポリシーのデフォルト アクションを指定することです。新しいポリシーのデフォルト アクションを選択する際には、次のオプションがあります。

- [復号しない（Do not decrypt）] は、[復号しない（Do not decrypt）] デフォルト アクションでポリシーを作成します。
- [ブロック（Block）] は、[ブロック（Block）] デフォルト アクションでポリシーを作成します。
- [リセットしてブロック（Block with reset）] は、[リセットしてブロック（Block with reset）] デフォルト アクションでポリシーを作成します。

デフォルト アクションは、SSL ポリシーを作成した後で変更できます。デフォルト アクションの選択に関するガイダンスについては、暗号化トラフィックのデフォルトの処理と検査の設定（12-4 ページ）を参照してください。

新しい SSL ポリシーにはシステムが復号できないトラフィックのデフォルト アクションも含まれています。それは、ユーザが復号できないトラフィックに対して選択したデフォルト アクションを継承する、ブロックする、あるいはトラフィックを復号せずアクセス コントロールで検査するなどのアクションです。復号できないトラフィックに対するアクションは、SSL ポリシーの作成後に変更できます。復号できないトラフィック アクションの選択に関するガイダンスについては、復号できないトラフィックのデフォルト処理の設定（12-5 ページ）を参照してください。

SSL ポリシーのページ（[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [SSL]）で、オプションの説明とともに、現在のすべての SSL ポリシーを名前別に表示できます。このページのオプションを使用して、さまざまな操作を行うことができます。具体的には、ポリシーの比較、新規ポリシーの作成、ポリシーのコピー、各ポリシーに最近保存された設定をすべてリストするレポートの表示、ポリシーの編集、ポリシーの削除などです。

次の表で、SSL ポリシーのページでポリシーを管理するために実行可能なアクションについて説明します。

表 *12-1*　*SSL* ポリシー管理アクション

目的	操作
新しい SSL 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。詳細については、基本 SSL ポリシーの作成（12-2 ページ）を参照してください。
既存の SSL ポリシーの設定を変更する	編集アイコン（ ）をクリックします。詳細については、SSL ポリシーの編集（12-7 ページ）を参照してください。
SSL 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。詳細については、SSL ポリシーの比較（12-11 ページ）を参照してください。
SSL ポリシーをコピーする	コピー アイコン（ ）をクリックします。コピーしたポリシーの編集の詳細については、SSL ポリシーの編集（12-7 ページ）を参照してください。
SSL ポリシーの現在の構成設定を示す PDF レポートを表示する	レポート アイコン（ ）をクリックします。詳細については、現在のトラフィック復号設定のレポートの生成（12-10 ページ）を参照してください。
SSL ポリシーを削除する	削除アイコン（ ）をクリックし、[OK] をクリックします。続行するかどうかを尋ねるプロンプトで、ポリシー内に別のユーザの未保存の変更が存在するかどうかも通知されます。

SSL ポリシーを作成する手順:

ステップ **1**　**[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）]** > [ポリシー（Policies）] > [SSL] の順に選択します。

[SSL ポリシー（SSL Policy）] ページが表示されます。

ステップ **2**　[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。

ステップ **3**　[デフォルト アクション（Default Action）] で、デフォルト アクションを指定します。

選択したデフォルト アクションは、SSL ポリシーの作成後に変更できることに注意してください。詳細については、暗号化トラフィックのデフォルトの処理と検査の設定（12-4 ページ）を参照してください。

ステップ **4**　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

[SSL ポリシー エディタ（SSL Policy Editor）] ページが表示されます。詳細については、SSL ポリシーの編集（12-7 ページ）を参照してください。

暗号化トラフィックのデフォルトの処理と検査の設定

ライセンス：任意

SSL ポリシーのデフォルト アクションは、ポリシーのモニタ以外のルールと一致しない復号可能な暗号化トラフィックについてシステムがどのように処理するかを決定します。SSL ルールがまったく含まれない SSL ポリシーを適用する場合、ネットワーク上のすべての復号可能トラフィックの処理方法を、デフォルト アクションが決定します。システムが復号できない暗号化トラフィックを処理する方法の詳細については、復号できないトラフィックのデフォルト処理の設定（12-5 ページ）を参照してください。

次の表に、選択可能なデフォルト アクションとそれが暗号化トラフィックに対して行う処理をリストします。デフォルト アクションでブロックされた暗号化トラフィックに対しては、システムはいかなる種類のインスペクションも行わないことに注意してください。

表 ***12-2*** ***SSL*** 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	暗号化トラフィックに対して行う処理
ブロック（Block）	それ以上のインスペクションは行わずに SSL セッションをブロックする
リセットしてブロック（Block with reset）	それ以上のインスペクションは行わずに SSL セッションをブロックし、TCP 接続をリセットする
復号しない（Do not decrypt）	アクセス コントロールを使用して暗号化トラフィックを検査する

SSL ポリシーを最初に作成する場合、デフォルト アクションによって処理される接続のログは、デフォルトでは無効化されています。デフォルト アクションと同様に、この設定もポリシー作成後に変更できます。

次の手順で、ポリシーの編集の際に SSL ポリシーのデフォルト アクションを設定する方法を説明します。SSL ポリシーを編集するための詳細な手順については SSL ポリシーの編集（12-7 ページ）を参照してください。

SSL ポリシーのデフォルト アクションを設定する方法：

ステップ **1**　**[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] >** [ポリシー（Policies）] > [SSL] の順に選択します。

[SSL ポリシー（SSL Policy）] ページが表示されます。

ステップ **2**　設定する SSL ポリシーの横にある編集アイコン（ ）をクリックします。

SSL ポリシー エディタが表示されます。

ステップ **3**　[デフォルト アクション（Default Action）] を選択します。詳細については、SSL ポリシーのデフォルト アクション の表を参照してください。

ステップ **4**　SSL ルールによる復号可能接続のロギング（33-15 ページ）の説明に従って、デフォルト アクションのロギング オプションを設定します。

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

[SSL ポリシー エディタ（SSL Policy Editor）] ページが表示されます。詳細については、SSL ポリシーの編集（12-7 ページ）を参照してください。

復号できないトラフィックのデフォルト処理の設定

ライセンス:任意

システムによる復号や検査ができない特定タイプの暗号化トラフィックの処理については、SSL ポリシー レベルで、復号できないトラフィックのアクションを設定できます。SSL ルールがまったく含まれない SSL ポリシーを適用する場合、ネットワーク上のすべての復号できない暗号化トラフィックの処理方法は、復号できないトラフィックのアクションが決定します。

復号できないトラフィックのタイプによって、次の選択ができます。

- 接続をブロックする
- 接続をブロックした後でリセットする
- アクセス コントロールを使用して暗号化トラフィックを検査する
- SSL ポリシーのデフォルト アクションを継承する

次の表に、復号できないトラフィックのタイプを示します。

表 ***12-3***　復号できないトラフィック タイプ

タイプ	説明	デフォルト アクション	利用可能なアクション
圧縮されたセッション（Compressed Session）	SSL セッションはデータ圧縮メソッドを適用します。	デフォルト アクションを継承する（Inherit default action）	復号しない（Do not decrypt） ブロック（Block） リセットしてブロック（Block with reset） デフォルト アクションを継承する（Inherit default action）
SSLv2 セッション（SSLv2 Session）	セッションは SSL バージョン 2 で暗号化されます。 トラフィックが復号可能となるのは、クライアントの HELLO メッセージが SSL 2.0 で、送信トラフィックの残りが SSL 3.0 であることに注意してください。	デフォルト アクションを継承する（Inherit default action）	復号しない（Do not decrypt） ブロック（Block） リセットしてブロック（Block with reset） デフォルト アクションを継承する（Inherit default action）
不明な暗号スイート（Unknown Cipher Suite）	システムが認識できない暗号スイートです。	デフォルト アクションを継承する（Inherit default action）	復号しない（Do not decrypt） ブロック（Block） リセットしてブロック（Block with reset） デフォルト アクションを継承する（Inherit default action）
サポートされていない暗号スイート（Unsupported Cipher Suite）	検出された暗号スイートに基づく復号を、システムはサポートしていません。	デフォルト アクションを継承する（Inherit default action）	復号しない（Do not decrypt） ブロック（Block） リセットしてブロック（Block with reset） デフォルト アクションを継承する（Inherit default action）

表 12-3　復号できないトラフィック タイプ（続き）

タイプ	説明	デフォルト アクション	利用可能なアクション
セッションが未キャッシュ（Session not cached）	SSL セッションでセッションの再利用が有効化されており、クライアントとサーバがセッション ID を使ってセッションを再確立しているが、システムでセッション ID がキャッシュされていません。	デフォルト アクションを継承する（Inherit default action）	復号しない（Do not decrypt） ブロック（Block） リセットしてブロック（Block with reset） デフォルト アクションを継承する（Inherit default action）
ハンドシェイク エラー（Handshake Errors）	SSL ハンドシェイクのネゴシエーション中にエラーが発生しました。	デフォルト アクションを継承する（Inherit default action）	復号しない（Do not decrypt） ブロック（Block） リセットしてブロック（Block with reset） デフォルト アクションを継承する（Inherit default action）
復号エラー（Decryption Errors）	トラフィックの復号中にエラーが発生しました。	ブロック（Block）	ブロック（Block） リセットしてブロック（Block With Reset）

SSL ポリシーを最初に作成する場合、デフォルト アクションによって処理される接続のログは、デフォルトでは無効化されています。復号できないトラフィックの処理ではデフォルト アクションのログ設定も適用されるため、復号できないトラフィックのアクションで処理される接続のログは、デフォルトでは無効化されています。デフォルトのロギング設定の詳細については、SSL ルールによる復号可能接続のロギング（33-15 ページ）を参照してください。

（注）　クライアントとデバイスの間に HTTP プロキシがあって、クライアントとサーバが CONNECT HTTP メソッドを使用してトンネル SSL 接続を確立する場合、システムはトラフィックを復号できません。システムによるこのトラフィックの処理法は、ハンドシェイク エラー（**Handshake Errors**）の復号できないアクションが決定します。詳細については、復号アクション：さらに検査するためにトラフィックを復号（13-11 ページ）を参照してください。

ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号できないことに注意してください。このトラフィックはアクセス コントロールを使用して引き続き検査できるため、復号できないトラフィック アクションでは処理されません。このトラフィックを許可するには、サーバ証明書の共通名または識別名と一致させるために、[復号しない（Do not decrypt）] アクションを使用して SSL ルールを設定します。

復号できないトラフィックのデフォルト処理を設定する方法：

ステップ 1　**[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] >** [ポリシー（Policies）] > [SSL] の順に選択します。

[SSL ポリシー（SSL Policy）] ページが表示されます。

ステップ 2　設定する SSL ポリシーの横にある編集アイコン（ ）をクリックします。

SSL ポリシー エディタが表示されます。

ステップ 3　[復号不可のアクション（Undecryptable Actions）] タブを選択します。

[復号不可のアクション（Undecryptable Actions）] タブが表示されます。

ステップ 4　各フィールドで、復号できないトラフィック タイプで実行するアクションを選択するか、あるいは SSL ポリシーのデフォルト アクションを適用するかを指定します。詳細については、SSL ポリシーのデフォルト アクション の表を参照してください。

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

変更を反映させるには、関連付けたアクセス 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（4-12 ページ）を参照してください）。

SSL ポリシーの編集

ライセンス：任意

SSL ポリシー エディタでは、ポリシーの設定と SSL ルールの編成ができます。SSL ポリシーの設定では、ポリシーに一意の名前を付け、デフォルト アクションを指定する必要があります。次のことも実行できます。

- SSL ルールを追加、編集、削除、有効化/無効化する
- 信頼できる CA 証明書を追加する
- システムが復号できない暗号化トラフィックに対する処理を決定する
- デフォルト アクションおよび復号できないトラフィック アクションで処理されるトラフィックのログを記録する

SSL ポリシーの作成または変更後は、SSL ポリシーをアクセス コントロール ポリシーに関連付け、そのアクセス コントロール ポリシーを適用します。カスタム ユーザ プロファイルを作成して、ユーザごとに、ポリシーの設定、編成、適用のための異なる権限を割り当てることもできます。

次の表は、SSL ポリシー エディタで実行可能な設定アクションを示しています。

表 *12-4*　*SSL* ポリシーの設定アクション

目的	操作
ポリシーの名前または説明を変更する	[名前（Name）] フィールドまたは [説明（Description）] フィールドをクリックして、必要に応じて文字を削除し、新しい名前または説明を入力します。
デフォルト アクションを設定する	詳細については、暗号化トラフィックのデフォルトの処理と検査の設定（12-4 ページ）を参照してください。
復号できないトラフィックのデフォルト処理を設定する	詳細については、復号できないトラフィックのデフォルト処理の設定（12-5 ページ）を参照してください。
デフォルト アクションと復号できないトラフィック アクションの接続をログに記録する	詳細については、SSL ルールによる復号可能接続のロギング（33-15 ページ）を参照してください。
信頼できる CA 証明書を追加する	詳細については、外部認証局の信頼（14-22 ページ）を参照してください。
ユーザごとに異なる権限を割り当てる	詳細については、SSL ルールを設定するために必要な情報の収集（11-3 ページ）を参照してください。
ポリシーの変更を保存する	[保存（Save）] をクリックします。
ポリシーの変更をキャンセルする	[キャンセル（Cancel）] をクリックします。変更を行った場合は、次に [OK] をクリックします。

表 12-4　SSL ポリシーの設定アクション（続き）

目的	操作
ポリシーにルールを追加する	[ルールの追加（Add Rule）] をクリックします。詳細については、SSL ルールの概要と作成（13-4 ページ）を参照してください。 ヒント　ルールの行の空白部分を右クリックし、[新規ルールの挿入（Insert new rule）] を選択するという方法もあります。
既存のルールを編集する	ルールの横にある編集アイコン（  ）をクリックします。詳細については、SSL ルールの概要と作成（13-4 ページ）を参照してください。 ヒント　ルールを右クリックして、[編集（Edit）] を選択することもできます。
ルールを削除する	ルールの横にある削除アイコン（  ）をクリックし、[OK] をクリックします。 ヒント　選択したルールの行の空白部分を右クリックして [削除（Delete）] を選択した後、[OK] をクリックして、選択した 1 つ以上のルールを削除するという方法もあります。
既存のルールを有効または無効にする	選択したルールを右クリックして [状態（State）] を選択した後、[無効（Disable）] または [有効（Enable）] を選択します。無効なルールはグレーで表示され、ルール名の下に [（無効）（(disabled)）] というマークが付きます。
特定のルール属性の設定ページを表示する	ルールの行で、該当する条件のカラムに示されている名前、値、またはアイコンをクリックします。たとえば、[送信元ネットワーク（Source Networks）] カラムに示されている名前または値をクリックすると、選択したルールの [ネットワーク（Networks）] ページが表示されます。詳細については、SSL ルールを使用したトラフィック復号の調整（14-1 ページ）を参照してください。

設定を変更すると、変更がまだ保存されていないことを通知するメッセージが表示されます。変更を維持するには、ポリシー 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、[SSL ポリシー（SSL 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。

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

SSL ポリシーを編集する手順:

ステップ 1　**[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] >** [ポリシー（Policies）] > [SSL] の順に選択します。

[SSL ポリシー（SSL Policy）] ページが表示されます。

ステップ 2　次の選択肢があります。

- ポリシーを設定する場合は、SSL ポリシーの設定アクションの表で説明されているすべての操作を使用できます。
- ポリシー ルールを編成する場合は、ポリシー内の SSL ルールの管理（13-13 ページ）の表で説明されているすべての操作を使用できます。

ステップ 3　設定を保存または廃棄します。次の選択肢があります。

- 変更を保存し、編集を続行する場合は、[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。
- 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。

  変更は廃棄され、[SSL ポリシー（SSL Policy）] ページが表示されます。

アクセス コントロールを使用した復号設定の適用

ライセンス：任意

SSL ポリシーに何らかの変更をした後は、関連付けられたアクセス コントロール ポリシーの適用が必要です。詳細については、設定変更の展開（4-12 ページ）を参照してください。

SSL ポリシーを適用する場合は、次の点に注意してください。

- 適用された SSL ポリシー、または現在適用されている SSL ポリシーを削除することはできません。
- アクセス コントロール ポリシーを適用すると、関連付けられた SSL ポリシーが自動的に適用されます。SSL ポリシーを個別に適用することはできません。

（注）　パッシブ展開では、システムがトラフィック フローに影響を与えることはありません。適用しようとするアクセス コントロール ポリシーが参照する SSL ポリシーが、暗号化トラフィックをブロックするか、またはサーバ証明書の再署名によるトラフィックの復号が設定されている場合、システムから警告が出されます。またパッシブ展開では、一時 Diffie-Hellman（DHE）および楕円曲線 Diffie-Hellman（ECDHE）暗号スイートを使用した暗号化トラフィックの復号がサポートされません。

SSL ポリシーとアクセス コントロール ポリシーを関連付ける方法：

ステップ 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。

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

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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 4　[全般設定（General Settings）] の横にある編集アイコン（）をクリックします。

[全般設定（General Settings）] ポップアップ ウィンドウが表示されます。

ステップ 5　[暗号化接続の検査に使用する SSL ポリシー（SSL Policy to use for inspecting encrypted connections）] ドロップダウンから SSL ポリシーを選択します。

ステップ 6　[OK] をクリックします。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 7　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

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（4-12 ページ） を参照してください。

現在のトラフィック復号設定のレポートの生成

ライセンス:任意

SSL ポリシー レポートは、特定の時点でのポリシーとルール設定の記録です。このレポートは、監査目的や、現行の設定を調べるために使用できます。

ヒント　また、ポリシーを現在適用されているポリシーまたは別のポリシーと比較する SSL 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、SSL ポリシーの比較（12-11 ページ）を参照してください。

SSL ポリシー レポートには、次の表で説明するセクションが含まれます。

表 ***12-5***　***SSL*** ポリシー レポートのセクション

セクション	説明
タイトル ページ	ポリシー レポートの名前、ポリシーが最後に変更された日時、その変更を行ったユーザの名前が記載されます。
目次	レポートの内容が記載されます。
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。
デフォルト アクション（Default Action）	デフォルト アクションが記載されます。
デフォルト ロギング（Default Logging）	デフォルト接続ログの設定が記載されます。
ルール（Rule）	ルール カテゴリ別に、ポリシーに含まれる各ルールのルール アクションおよび条件が記載されます。
信頼できる CA 証明書（Trusted CA Certificates）	自動的に信頼できる CA 証明書が記載されます。該当するのは、検出されたトラフィックの暗号化にそれらの証明書が使用されている場合、あるいは信頼のチェーン内にある他の証明書が使用されている場合です。
復号不可のアクション（Undecryptable Actions）	復号できないトラフィック タイプが検出された場合に適用されるアクションが記載されます。
参照オブジェクト（Referenced Objects）	ポリシーで使用されている個々のすべてのオブジェクトおよびグループ オブジェクトの名前と設定が、各オブジェクトが設定されている条件タイプ別（ネットワーク、ポート、タグなど）に記載されます。

SSL ポリシー レポートを表示する方法:

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [SSL] の順に選択します。

[SSL ポリシー（SSL Policy）] ページが表示されます。

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

システムによってレポートが生成されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

SSL ポリシーの比較

ライセンス:任意

ポリシー変更が組織の標準に準拠しているかどうかを確認するため、またはシステムのパフォーマンスを最適化するために、2 つの SSL ポリシーの差異を確認することができます。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。

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

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

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

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

- SSL ポリシー比較ビューの使用(12-11 ページ)
- SSL ポリシー比較レポートの使用(12-12 ページ)

SSL ポリシー比較ビューの使用

ライセンス:任意

比較ビューには、両方のポリシーが左右に並べて表示されます。それぞれのポリシーは、比較ビューの左右のタイトル バーに示される名前で特定されます。現在実行されている設定ではない 2 つのポリシーを比較する場合、最後に変更された日時とその変更を行ったユーザがポリシー名と共に表示されます。2 つのポリシー間の差異は、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 *12-6*　*SSL* ポリシー比較のビューのアクション

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。

表 12-6　SSL ポリシー比較のビューのアクション（続き）

目的	操作
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、SSL ポリシー比較レポートの使用（12-12 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。

SSL ポリシー比較レポートの使用

ライセンス：任意

SSL ポリシー比較レポートは、ポリシー比較ビューによって示される 2 つの SSL ポリシー間または 1 つのポリシーと現在適用されているポリシーの間のすべての差異を PDF 形式で表示する記録です。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。

アクセス可能な任意のポリシーに関して、比較ビューから SSL 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。SSL ポリシー比較レポートには、現在のトラフィック復号設定のレポートの生成（12-10 ページ）で説明しているセクションが含まれます。

ヒント　同様の手順を使用して、アクセス コントロール ポリシー、ネットワーク解析ポリシー、侵入ポリシー、ファイル ポリシー、システム ポリシー、またはヘルス ポリシーを比較できます。

2 つの SSL ポリシーを比較する方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [SSL] の順に選択します。

[SSL ポリシー（SSL Policy）] が表示されます。

ステップ 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。

ステップ 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。

ステップ 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。

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

比較ビューが表示されます。

ステップ 6　オプションで、[比較レポート（Comparison Report）] をクリックして、SSL ポリシー比較レポートを生成します。

SSL ポリシー比較レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

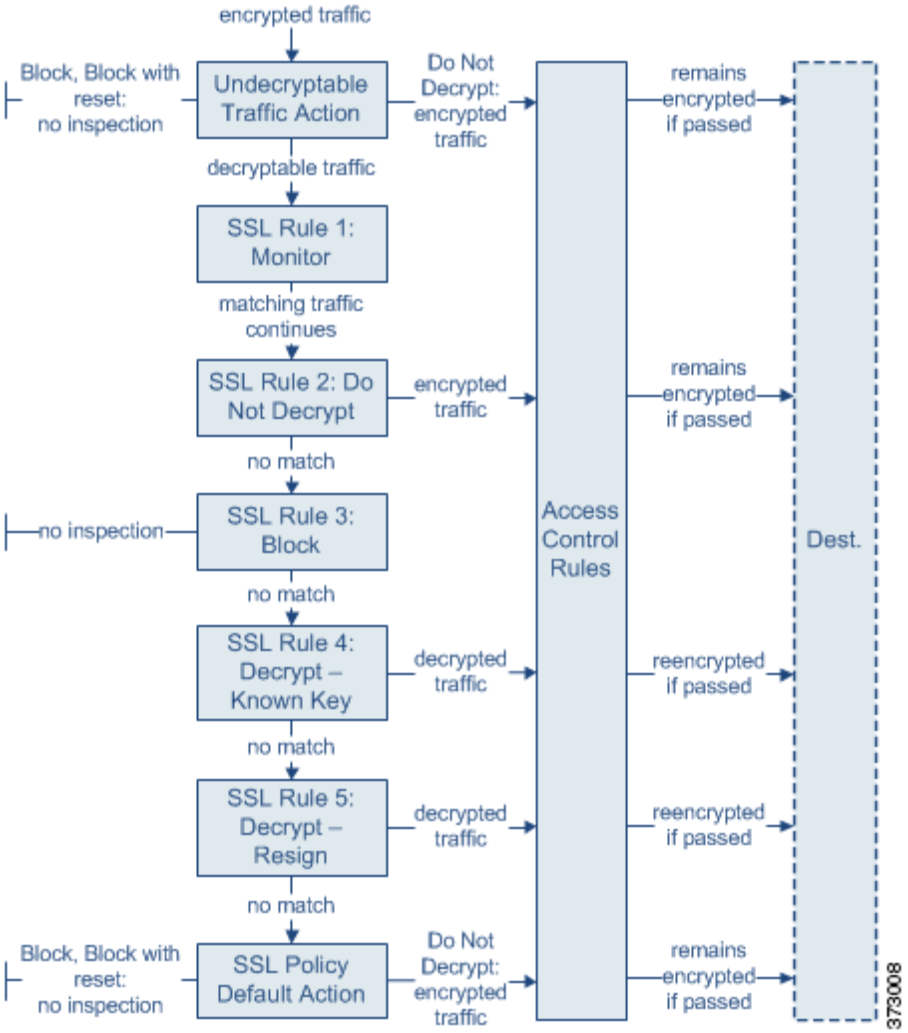
SSL ルール クイック スタート ガイド

SSL ポリシー内に各種の *SSL* ルールを設定することで、それ以上のインスペクションなしでトラフィックをブロックする、トラフィックを復号せずにアクセス コントロールで検査する、あるいはアクセス コントロールの分析用にトラフィックを復号するなど、きめ細かな暗号化トラフィックの処理メソッドを構築できます。

ASA FirePOWER モジュールは指定した順序で SSL ルールをトラフィックと照合します。ほとんどの場合、モジュールによる暗号化トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の SSL ルールに従って行われます。こうした条件には、単純なものと複雑なものがあります。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、ユーザ、証明書、証明書の識別名、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを制御できます。

また、各ルールには 1 つのアクションがあり、一致するトラフィックの復号後にオプションでモニタするか、ブロックするか、または一致したトラフィックをアクセス コントロールで検査するかを決定します。システムがブロックした暗号化トラフィックは、それ以上のインスペクションが行われないことに注意してください。暗号化されたトラフィックおよび復号できないトラフィックは、アクセス コントロールを使用して検査します。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、モジュールは暗号化ペイロードの侵入およびファイル検査を無効化します。

次のシナリオは、インライン展開での SSL ルールによるトラフィックの処理を要約しています。



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。

- 復号できないトラフィック アクション（**Undecryptable Traffic Action**）は、暗号化されたトラフィックを最初に評価します。復号できないトラフィックについて、モジュールはそれ以上のインスペクションなしでブロックするか、あるいはアクセス コントロールによる検査用に渡します。一致しなかった暗号化トラフィックは、次のルールへと進められます。
- **SSL** ルール **1**：モニタ（**SSL Rule 1: Monitor**）は、暗号化トラフィックを次に評価します。モニタ ルールは、暗号化トラフィックのログ記録と追跡を行いますが、トラフィック フローには影響しません。モジュール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。
- **SSL** ルール **2**：復号しない（**SSL Rule 2: Do Not Decrypt**）は、暗号化トラフィックを 3 番目に評価します。一致したトラフィックは復号されません。モジュールはこのトラフィックをアクセス コントロールにより検査しますが、ファイルや侵入インスペクションは行いません。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。
- **SSL** ルール **3**：ブロック（**SSL Rule 3: Block**）は、暗号化トラフィックを 4 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、引き続き次のルールと照合されます。

- **SSL** ルール **4**：復号 **-** 既知のキー（**SSL Rule 4: Decrypt - Known Key**）は、暗号化トラフィックを 5 番目に評価します。ネットワークへの着信トラフィックで一致したものは、ユーザのアップロードする秘密キーを使用して復号されます。復号トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、モジュールがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL** ルール **5**：復号 **-** 再署名（**SSL Rule 5: Decrypt - Resign**）は、最後のルールです。トラフィックがこのルールに一致した場合、モジュールはアップロードされた CA 証明書を使用してサーバ証明書を再署名してから、中間者（man-in-the-middle）としてトラフィックを復号します。復号トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、モジュールがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL** ポリシーのデフォルト アクション（**SSL Policy Default Action**）は、どの SSL ルールにも一致しなかったすべてのトラフィックを処理します。デフォルト アクションでは、暗号化トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号しないで、アクセス コントロールによる検査を行います。

詳細については、次の項を参照してください。

- サポートする検査情報の設定（13-3 ページ）
- SSL ルールの概要と作成（13-4 ページ）
- ポリシー内の SSL ルールの管理（13-13 ページ）

サポートする検査情報の設定

ライセンス：任意

暗号化セッションの特性に基づいた暗号化トラフィックの制御および暗号化トラフィックの復号には、再利用可能な公開キー インフラストラクチャ（PKI）オブジェクトの作成が必要です。この情報の追加は、信頼できる認証局（CA）の証明書の SSL ポリシーへのアップロード時、SSL ルール条件の作成時、およびプロセスでの関連オブジェクトの作成時に、臨機応変に実行できます。ただし、これらのオブジェクトを事前に設定しておくと、不適切なオブジェクトが作成される可能性を抑制できます。

証明書とキー ペアによる暗号化トラフィックの復号

セッション暗号化に使用するサーバ証明書と秘密キーをアップロードして内部証明書オブジェクトを設定しておくと、ASA FirePOWER モジュールは着信する暗号化トラフィックを復号できます。[復号 - 既知のキー（Decrypt - Known Key）] アクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、モジュールはアップロードされた秘密キーを使用してセッションを復号します。

CA 証明書と秘密キーをアップロードして内部 CA オブジェクトを設定した場合、モジュールは発信トラフィックの復号もできます。[復号 - 再署名（Decrypt - Resign）] アクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、システムはクライアント ブラウザに渡されたサーバ証明書を再署名した後、中間者（man-in-the-middle）としてセッションを復号します。

詳細については、次の各項を参照してください。

- 内部証明書オブジェクトの使用（2-49 ページ）
- 内部認証局オブジェクトの使用（2-42 ページ）

暗号化セッションの特性に基づいたトラフィック制御

ASA FirePOWER モジュールによる暗号化トラフィックの制御は、セッションのネゴシエートに使用されるサーバ証明書または暗号スイートに基づいて実行できます。複数の異なる再利用可能オブジェクトの 1 つを設定し、SSL ルール条件でオブジェクトを参照してトラフィックを照合することができます。次の表に、設定できる再利用可能なオブジェクトのタイプを示します。

設定する内容	暗号化トラフィック制御に使用する条件
1 つまたは複数の暗号スイートが含まれる暗号スイートのリスト	暗号化セッションのネゴシエートに使用される暗号スイートが、暗号スイート リストにある暗号スイートのいずれかに一致する。
組織が信頼する CA 証明書のアップロードによる信頼できる CA オブジェクト	この信頼できる CA は、次のいずれかにより、セッションの暗号化に使用されたサーバ証明書を信頼する。 • CA が証明書を直接発行した。 • サーバ証明書を発行した中間 CA に CA が証明書を発行した。
サーバ証明書のアップロードによる外部証明書オブジェクト	セッションの暗号化に使用されたサーバ証明書が、アップロードされたサーバ証明書と一致する。
発行元の識別名または証明書サブジェクトを含む識別名オブジェクト	セッション暗号化に使用された証明書で、サブジェクトまたは発行元の共通名、国、組織、組織単位のいずれかが、設定された識別名と一致する。

詳細については、次の各項を参照してください。

- 位置情報オブジェクトの操作（2-50 ページ）
- 信頼できる認証局オブジェクトの使用（2-46 ページ）
- 外部証明書オブジェクトの使用（2-48 ページ）
- 識別名オブジェクトの操作（2-39 ページ）

SSL ルールの概要と作成

ライセンス：任意

SSL ポリシー内で、SSL ルールによってネットワーク トラフィックを処理するためのきめ細かなメソッドが提供されます。各 SSL ルールには、一意の名前以外にも、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、モジュールはネットワーク 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**）

SSL ポリシーのルールには 1 から始まる番号が付いています。モジュールは、ルール番号の昇順で、ルールを上から順に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。こうした条件では、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、ユーザ、証明書、証明書のサブジェクトまたは発行元、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを照合できます。条件には、単純なものと複雑なものがあり、デバイスのライセンスによって用途が異なります。

アクション（**Action**）

ルールのアクションによって、一致するトラフィックをモジュールがどのように処理するかが決まります。一致したトラフィックに対して行うことができ処理は、モニタ、信頼、ブロック、または復号です。復号したトラフィックには、さらにインスペクションが適用されます。モジュールは、ブロックされた暗号化トラフィックと信頼された暗号化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。

ログ

ルールのロギング設定によって、モジュールが処理するトラフィックについて記録するレコードが管理されます。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。SSL ポリシーでの設定に従って、モジュールが暗号化セッションをブロックするか、あるいはインスペクションなしで渡すことを許可するときに、その接続をログに記録できます。アクセス コントロール ルールに従ってより詳細な評価を行うために復号した接続をログに記録するようにモジュールを強制することも可能です。これはその後でどのようなトラフィックの処理や検査がなされるかに関係なく行うことができます。接続のログは、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。

ヒント　SSL ルールを適切に作成して順序付けることは複雑な作業ですが、効果的な展開を構築する上で不可欠な作業です。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。予期したとおりにトラフィックが確実に処理されるようにするために、SSL ポリシー インターフェイスには、ルールに関する強力な警告およびエラーのフィードバック システムが用意されています。詳細については、SSL ルールのトラブルシューティング（13-17 ページ）を参照してください。

SSL ルールを作成または変更する手順:

ステップ **1**　**[**設定（**Configuration**）**] > [ASA FirePOWER** 設定（**ASA FirePOWER Configuration**）**] >** [ポリシー（Policies）] > [SSL] の順に選択します。

[SSL ポリシー（SSL Policy）] ページが表示されます。

ステップ **2**　ルールを追加する SSL ポリシーの横にある編集アイコン（）をクリックします。

SSL ポリシー エディタが表示され、[ルール（Rules）] タブにフォーカスが移動します。

ステップ **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。

SSL ルール エディタが表示されます。

ステップ **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。

ステップ 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。SSL ルールの評価順序の指定（13-6 ページ）を参照してください。
- ルールの [アクション（Action）] を選択します。ルール アクションを使用した暗号化トラフィックの処理と検査の決定（13-9 ページ）を参照してください。
- ルールの条件を設定します。条件を使用した、ルールによる暗号化トラフィックの処理の指定（13-7 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。SSL ルールによる復号可能接続のロギング（33-15 ページ）を参照してください。

ステップ 6　[保存（Save）] をクリックしてルールを保存します。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

SSL ルールの評価順序の指定

ライセンス：任意

SSL ルールを最初に作成するときに、ルール エディタの [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。SSL ポリシーの SSL ルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルール番号の昇順で、SSL ルールを上から順にトラフィックと照合します。

ほとんどの場合、モジュールによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の SSL ルールに従って行われます。モニタ ルールの場合を除き（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）、いずれかのルールとトラフィックが一致した後、モジュールは優先順位の低い追加ルールとの突き合わせによるトラフィックの評価は続行しません。

ヒント　適切な SSL ルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、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、SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避（13-18 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、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。カスタム カテゴリを追加できますが、ASA FirePOWER モジュール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、SSL ルールの位置またはカテゴリの変更（13-15 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。

ステップ 1　SSL ルール エディタの [挿入（Insert）] ドロップダウン リストで [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。

ステップ 1　SSL ルール エディタの [挿入（Insert）] ドロップダウン リストで [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。

条件を使用した、ルールによる暗号化トラフィックの処理の指定

ライセンス：機能によって異なる

SSL ルールの条件は、ルールで処理する暗号化トラフィックのタイプを特定します。条件には、単純なものと複雑なものがあり、ルールごとに複数の条件タイプを指定できます。トラフィックにルールが適用されるのは、トラフィックがルールの条件をすべて満たしている場合だけです。

ルールに対し特定の条件を設定しない場合、モジュール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、証明書の条件が設定され、バージョンの条件が設定されていないルールは、セッション SSL または TLS のバージョンにかかわりなく、セッションのネゴシエーションに使用されるサーバ証明書に基づいてトラフィックを評価します。

SSL ルールを追加および編集するときは、ルール エディタ下部の左側にあるタブを使用して、ルール条件の追加と編集を行います。SSL ルールに追加できる条件を次の表に示します。

表 *13-1*　*SSL* ルールの条件タイプ

条件	一致する暗号化トラフィック	詳細
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、ネットワーク ゾーンによる暗号化トラフィックの制御（14-2 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	IP アドレスを明示的に指定できます。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暗号化トラフィックの制御（14-4 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 ポートに基づいて暗号化トラフィックを制御できます。ポート条件を作成するには、ポートによる暗号化トラフィックの制御（14-6 ページ）を参照してください。
ユーザ	セッションに関与するユーザによる	暗号化されたモニタ対象セッションの関連ホストにログインしている LDAP ユーザに基づいて暗号化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、ユーザ ベースの暗号化トラフィックの制御（14-7 ページ）を参照してください。

表 13-1　SSL ルールの条件タイプ（続き）

条件	一致する暗号化トラフィック	詳細
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	タイプ、リスク、ビジネスとの関連性、カテゴリの基本的な特性に従って、フィルタ アクセスまたは暗号化セッションの各アプリケーションへの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、アプリケーションベースの暗号化トラフィックの制御（14-8 ページ）を参照してください。
カテゴリ	証明書サブジェクトの識別名に基づいてセッションで要求される URL	URL の一般分類とリスク レベルに基づいて、ネットワークのユーザがアクセスできる Web サイトを制限できます。URL 条件の作成については、URL カテゴリおよびレピュテーションによる暗号化トラフィックの制御（14-14 ページ）を参照してください。
識別名	暗号化セッションのネゴシエートに使用されたサーバ証明書のサブジェクトまたは発行元の識別名	サーバ証明書を発行した CA またはサーバ証明書ホルダーに基づいて、暗号化トラフィックを制御できます。識別名条件の作成については、証明書の識別名による暗号化トラフィックの制御（14-18 ページ）を参照してください。
証明書（Certificates）	暗号化セッションのネゴシエートに使用されるサーバ証明書	暗号化セッションのネゴシエート用にユーザのブラウザに渡されるサーバ証明書に基づいて、暗号化されたトラフィックを制御できます。証明書条件の作成については、証明書ステータスによる暗号化トラフィックの制御（14-22 ページ）を参照してください。
証明書のステータス（Certificate Status）	暗号化セッションのネゴシエートに使用されるサーバ証明書のプロパティ	サーバ証明書のステータスに基づいて、暗号化トラフィックを制御できます。証明書ステータス条件の作成については、証明書ステータスによる暗号化トラフィックの制御（14-22 ページ）を参照してください。
暗号スイート	暗号化セッションのネゴシエートに使用する暗号スイート	暗号化セッションのネゴシエート用にサーバで選択された暗号スイートに基づいて、暗号化トラフィックを制御できます。暗号スイート条件の作成については、暗号スイートによる暗号化トラフィックの制御（14-26 ページ）を参照してください。
バージョン	セッションの暗号化に使用される SSL または TLS のバージョン	セッションの暗号化に使用される SSL または TLS のバージョンに基づいて、暗号化トラフィックを制御できます。バージョン条件の作成については、暗号化プロトコルのバージョンによるトラフィックの制御（14-28 ページ）を参照してください。

暗号化トラフィックの制御と確認は可能ですが、トラフィックの制御に、検出されたアプリケーション、URL カテゴリ、またはユーザを使用するには追加ライセンスが必要です。また過度に複雑なルールは、多くのリソースを消費し、状況によってはポリシーを適用できなくなる場合があります。詳細については、SSL ルールのトラブルシューティング（13-17 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暗号化トラフィックの処理と検査の決定

ライセンス:任意

すべての SSL ルールには、一致する暗号化トラフィックに対して次の判定をする関連アクションがあります。

- 処理:まず、ルール アクションは、ASA FirePOWER モジュールがルールの条件に一致する暗号化トラフィックに対して、モニタ、信頼、ブロック、または復号を行うかどうかを判定します。
- ロギング:ルール アクションは一致する暗号化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を判定します。

SSL インスペクション設定では、次のように復号されたトラフィックの処理、検査、ログ記録を行います。

- SSL ポリシーの復号できないアクションは、ASA FirePOWER モジュールが復号できないトラフィックを処理します。復号できないトラフィックのデフォルト処理の設定（12-5 ページ）を参照してください。
- ポリシーのデフォルト アクションは、モニタ以外のどの SSL 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。暗号化トラフィックのデフォルトの処理と検査の設定（12-4 ページ）を参照してください。

ASA FirePOWER モジュールが暗号化セッションを信頼またはブロックしたときに、接続イベントをログに記録できます。アクセス コントロール ルールに従ってより詳細な評価を行うために復号した接続をログに記録するようにモジュールを強制することも可能です。これはその後でどのようなトラフィックの処理や検査がなされるかに関係なく行うことができます。暗号化セッションの接続ログには、セッションの暗号化に使用される証明書など、暗号化の詳細が含まれます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続（[ブロック（Block）]、[リセットしてブロック（Block with reset）]）の場合、システムは即座にセッションを終了してイベントを生成します。
- 信頼された接続（[復号しない（Do not decrypt）]）の場合、システムはセッション終了時にイベントを生成します。

ルール アクションの詳細および、ルール アクションが処理とログに与える影響の詳細については、次のセクション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（13-10 ページ）
- [復号しない（Do Not Decrypt）] アクション:暗号化トラフィックを検査なしで転送（13-10 ページ）
- [ブロック（Block）] アクション:検査なしで暗号化トラフィックをブロック（13-10 ページ）
- 復号アクション:さらに検査するためにトラフィックを復号（13-11 ページ）
- ポリシー内の SSL ルールの管理（13-13 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

[モニタ（Monitor）] アクションは暗号化トラフィック 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、信頼するか、ブロックするか、復号するかが決定されます。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、ASA FirePOWER モジュールはデフォルト 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、ルールのロギング設定または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、モジュールは接続の終了時に常にログに記録します。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グに記録されます。

[復号しない（Do Not Decrypt）] アクション：暗号化トラフィックを検査なしで転送

ライセンス：任意

[復号しない（Do not decrypt）] アクションは、アクセス コントロール ポリシーのルールおよびデフォルト アクションに従って暗号化トラフィックを評価するため転送します。一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、こうしたトラフィックに一致するルール数が少なくなる場合があります。侵入やファイル インスペクションなど、暗号化トラフィックのディープ インスペクションは実行できません。

[ブロック（Block）] アクション：検査なしで暗号化トラフィックをブロック

ライセンス：任意

[ブロック（Block）] および [リセットしてブロック（Block with reset）] アクションは、アクセス コントロール ルールの [ブロック（Block）] と [リセットしてブロック（Block with reset）] アクションに類似しています。これらのアクションは、クライアントとサーバによる SSL 暗号化セッションの確立と暗号化トラフィックの転送を防止します。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。

ブロックされた暗号化トラフィックに対しては、ASA FirePOWER モジュールは設定された応答ページを表示しないことに注意してください。その代わりに、ユーザの要求する禁止された URL の接続は、リセットされるか、またはタイムアウトになります。詳細については、ブロックされた URL のカスタム Web ページの表示（8-15 ページ）を参照してください。

ヒント　パッシブまたはインライン（タップ モード）展開では、デバイスがトラフィックを直接検査しないので、[ブロック（Block）] と [リセットしてブロック（Block with reset）] アクションを使用できないことに注意してください。パッシブまたはインライン（タップ モード）インターフェイスを含むセキュリティ ゾーン条件内で、[ブロック（Block）] と [リセットしてブロック（Block with reset）] アクションを使用したルールを作成すると、ポリシー エディタでルールの横に警告アイコン（⚠）が表示されます。

復号アクション: さらに検査するためにトラフィックを復号

ライセンス: 任意

[復号 - 既知のキー（Decrypt - Known Key）] および [復号 - 再署名（Decrypt - Resign）] アクションは、暗号化トラフィックを復号します。ASA FirePOWER モジュールはアクセス コントロールを使用して復号されたトラフィックを検査します。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。ここでは、侵入、禁止ファイル、マルウェアの検出とブロックができます。モジュールは、許可されたトラフィックを再暗号化してから宛先に渡します。

[復号 - 既知のキー（Decrypt - Known Key）] アクションを設定した場合は、1 つまたは複数のサーバ証明書と秘密キー ペアをアクションに関連付けることができます。トラフィックがルールに一致して、トラフィックの暗号化に使用された証明書とアクションに関連付けられた証明書が一致した場合、モジュールは適切な秘密キーを使用してセッションの暗号化と復号キーを取得します。秘密キーへのアクセスが必要なため、このアクションが最も適しているのは、組織の管理下にあるサーバへの入力トラフィックを復号する場合です。

同様に [復号 - 再署名（Decrypt - Resign）] アクションには、1 つの認証局証明書と秘密キーを関連付けることができます。トラフィックがこのルールに一致した場合、システムは CA 証明書を使用してサーバ証明書を再署名してから、中間者（man-in-the-middle）として機能します。ここでは、1 つはクライアントとデバイスの間、もう 1 つはデバイスとサーバの間をつなぐ、2 つの SSL セッションが作成されます。各セッションにはさまざまな暗号セッションの詳細が含まれており、モジュールはこれを使用することでトラフィックの復号と再暗号化が行えます。このアクションは、証明書の秘密キーを各自の管理下にあるキーに置き換えてセッション キーを取得するため、発信トラフィックに適しています。

サーバ証明書の再署名では、証明書の公開キーを CA 証明書の公開キーに置き換えるか、あるいは証明書全体が置き換えられます。通常、サーバ証明書全体を置き換える場合は、SSL 接続が確立された時点で、証明書が信頼できる認証局によって署名されていないことがクライアント ブラウザで警告されます。ただし、その CA をクライアント ブラウザで信頼できることがポリシーに設定されている場合、ブラウザは証明書が信頼できないことについて警告しません。オリジナルのサーバ証明書が自己署名の場合、ASA FirePOWER モジュールは証明書全体を置き換えて再署名する CA を信頼しますが、ユーザのブラウザは証明書が自己署名されていることを警告しません。この場合、サーバ証明書の公開キーを交換するだけで、クライアント ブラウザは証明書が自己署名であることを警告します。

[復号 - 再署名（Decrypt - Resign）] アクションをルールに設定すると、ルールによるトラフィックの照合は、設定されている他のルール条件に加えて、参照する内部 CA 証明書の署名アルゴリズム タイプに基づいて実施されます。各 [復号 - 再署名（Decrypt - Resign）] アクションにはそれぞれ 1 つの CA 証明書が関連付けられるので、異なる署名アルゴリズムで暗号化された複数のタイプの発信トラフィックを復号化する SSL ルールは作成できません。また、ルールに追加する暗号スイートと外部証明書のオブジェクトのすべては、関連する CA 証明書の暗号化アルゴリズム タイプに一致する必要があります。

たとえば、楕円曲線暗号（EC）アルゴリズムで暗号化された発信トラフィックが [復号 - 再署名（Decrypt - Resign）] ルールに一致するのは、アクションが EC ベースの CA 証明書を参照している場合だけです。証明書と暗号スイートのルール条件を作成する場合は、EC ベースの外部証明書と暗号スイートをルールに追加する必要があります。同様に、RSA ベースの CA 証明書を参照する [復号 - 再署名（Decrypt - Resign）] ルールは、RSA アルゴリズムで暗号化された発信トラフィックとのみ一致します。EC アルゴリズムで暗号化された発信トラフィックは、設定されている他のルール条件がすべて一致したとしても、このルールには一致しません。

次の点に注意してください。

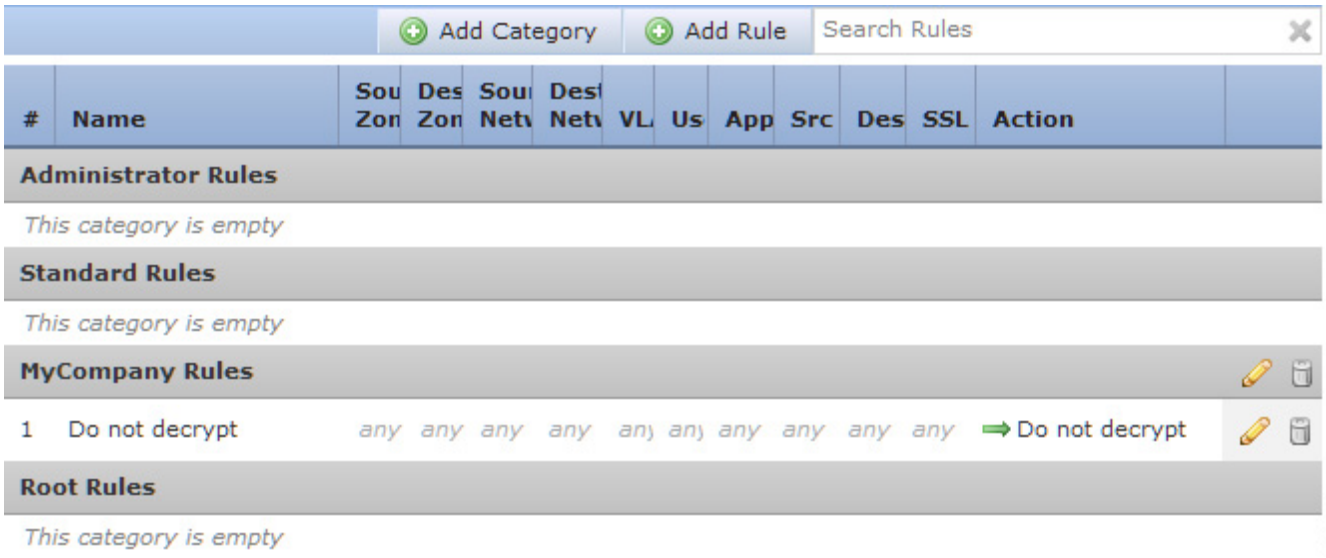
- SSL 接続の確立に使用される暗号スイートが Diffie-Hellman Ephemeral（DHE）または楕円曲線 Diffie-Hellman Ephemeral（ECDHE）キー交換アルゴリズムを適用している場合、パッシブ展開では [復号 - 既知のキー（Decrypt - Known Key）] アクションを使用できません。SSL ポリシーの対象がパッシブまたはインライン（タップ モード）インターフェイスであり、そのポリシーに含まれる [復号 - 既知のキー（Decrypt - Known Key）] ルールで DHE または ECDHE を含む暗号スイート条件が使われている場合、ASA FirePOWER モジュールによりルールの横に情報アイコン（）が表示されます。パッシブまたはインライン（タップ モード）インターフェイスを含む SSL ルールに後からゾーン条件を追加すると、モジュールにより警告アイコン（）が表示されます。
- デバイスはトラフィックを直接検査しないため、パッシブまたはインライン（タップ モード）展開では [復号 - 再署名（Decrypt - Resign）] アクションを使用できません。セキュリティ ゾーン内にパッシブまたはインライン（タップ モード）インターフェイスを含む [復号 - 再署名（Decrypt - Resign）] アクションを指定してルールを作成すると、ポリシー エディタでルールの横に警告アイコン（）が表示されます。SSL ポリシーの対象がパッシブまたはインライン（タップ モード）インターフェイスであり、ポリシーに [復号 - 再署名（Decrypt - Resign）] ルールが含まれている場合、モジュールではルールの横に情報アイコン（）が表示されます。パッシブまたはインライン（タップ モード）インターフェイスを含む SSL ルールに後からゾーン条件を追加すると、モジュールにより警告アイコン（）が表示されます。パッシブまたはインライン（タップ モード）インターフェイスを含むデバイスに、[復号 - 再署名（Decrypt - Resign）] ルールを含む SSL ポリシーを適用した場合、このルールに一致する SSL セッションはすべて失敗します。
- サーバ証明書の再署名に使用する CA をクライアントが信頼していない場合、証明書が信頼できないという警告がユーザに出されます。これを防ぐには、クライアントの信頼できる CA ストアに CA 証明書をインポートします。または、組織にプライベート PKI がある場合は、組織の全クライアントにより自動的に信頼されるルート CA が署名する中間 CA 証明書を発行して、その CA 証明書をデバイスにアップロードすることもできます。
- ASA FirePOWER モジュールでは、匿名の暗号スイートで暗号化されたトラフィックは復号できません。匿名の暗号スイートを **Cipher Suite** 条件に追加した場合、SSL ルールに [復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Decrypt - Known Key）] アクションを使用できません。
- クライアントとデバイスの間に HTTP プロキシがあり、クライアントとサーバが CONNECT HTTP メソッドを使用してトンネル SSL 接続を確立する場合、ASA FirePOWER モジュールはトラフィックを復号できません。モジュールによるこのトラフィックの処理法は、ハンドシェイク エラー（**Handshake Errors**）の復号できないアクションが決定します。詳細については、復号できないトラフィックのデフォルト処理の設定（12-5 ページ）を参照してください。
- [復号 - 既知のキー（Decrypt - Known Key）] アクションを指定して SSL ルールを作成した場合は、[識別名（Distinguished Name）] や [証明書（Certificate）] 条件による照合はできません。ここでの前提は、このルールがトラフィックと一致する場合、証明書、サブジェクト DN、および発行元 DN は、ルールに関連付けられた証明書とすでに一致済みであることです。詳細については、ルール アクションを使用した暗号化トラフィックの処理と検査の決定（13-9 ページ）を参照してください。
- 内部 CA オブジェクトを作成して証明書署名要求（CSR）の生成を選択した場合は、オブジェクトに署名付き証明書をアップロードするまで、この CA を [復号 - 再署名（Decrypt - Resign）] アクションに使用できません。詳細については、新しい署名付き証明書の取得およびアップロード（2-44 ページ）を参照してください。
- [復号 - 再署名（Decrypt - Resign）] アクションをルールに設定し、1 つまたは複数の外部証明書オブジェクトまたは暗号スイートで署名アルゴリズム タイプの不一致が生じた場合、ポリシー エディタでルールの横に情報アイコン（）が表示されます。すべての外部証明書オブジェクトまたはすべての暗号スイートで署名アルゴリズム タイプの不一致が生じた場合、ポリシーのルールの横には警告アイコン（）が表示され、SSL ポリシーに関連付けたアクセス コントロール ポリシーは適用できなくなります。詳細については、証明書による暗号化トラフィックの制御（14-21 ページ）および暗号スイートによる暗号化トラフィックの制御（14-26 ページ）を参照してください。

- [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションのアクセス コントロール ルールと復号トラフィックが一致する場合、ASA FirePOWER モジュールは一致する接続をインタラクションなしでブロックし、応答ページを表示しません。
- インライン正規化プリプロセッサで [余剰ペイロードの正規化（Normalize Excess Payload）] オプションを有効にすると、プリプロセッサによる復号トラフィックの標準化時に、パケットがドロップされてトリミングされたパケットに置き換えられる場合があります。これにより SSL セッションは終了しません。トラフィックが許可された場合、トリミングされたパケットは SSL セッションの一部として暗号化されます。このオプションの詳細については、インライン トラフィックの正規化（21-6 ページ）を参照してください。
- ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号できません。このトラフィックを許可するには、サーバ証明書の共通名または識別名と一致させるために、[復号しない（Do not decrypt）] アクションを使用して SSL ルールを設定します。

ポリシー内の SSL ルールの管理

ライセンス：任意

SSL ポリシー エディタの [ルール（Rules）] タブでは、以下の図に示すように、ポリシー内の SSL ルールの追加、編集、検索、移動、有効化、無効化、削除、その他の管理が行えます。



各ルールについて、ポリシー エディタでは、その名前、条件のサマリー、およびルール アクションが表示されます。警告、エラー、その他の重要な情報がアイコンで示されます。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。アイコンの詳細については、SSL ルールのトラブルシューティング（13-17 ページ）を参照してください。

SSL ルールの管理の詳細については、次を参照してください。

- SSL ルールの検索（13-14 ページ）
- SSL ルールの有効化と無効化（13-14 ページ）
- SSL ルールの位置またはカテゴリの変更（13-15 ページ）

SSL ルールの検索

ライセンス：任意

スペースおよび印刷可能な特殊文字を含む英数字文字列を使用して、SSL 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）] 列と [アプリケーション（Applications）] 列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。

ステップ 1　検索するポリシーの SSL 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から 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。

ステップ 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。

SSL ルールの有効化と無効化

ライセンス：任意

作成した SSL ルールは、デフォルトで有効になっています。ルールを無効にすると、ASA FirePOWER モジュールはネットワーク 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。SSL ポリシーのルール リストを表示すると、無効なルールはグレー表示されますが、変更は可能です。またはルール エディタを使用して SSL ルールを有効化または無効化できることに注意してください。SSL ルールの概要と作成（13-4 ページ）を参照してください。

SSL ルールの状態を変更するには、次の手順に従います。

ステップ 1　有効または無効にするルールを含むポリシーの SSL 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）] を選択します。

ステップ 2　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

SSL ルールの位置またはカテゴリの変更

ライセンス：任意

SSL ルールを編成しやすいように、SSL ポリシーには、Administrator Rules（管理者ルール）、Standard Rules（標準ルール）、Root Rules（ルート ルール）という、ASA FirePOWER モジュールが提供する 3 つのルール カテゴリが用意されています。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。

- SSL ルールの移動（13-15 ページ）
- 新しい SSL ルール カテゴリの追加（13-16 ページ）

SSL ルールの移動

ライセンス：任意

適切な SSL ルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

次の手順は、SSL ポリシー エディタを使用して 1 つまたは複数のルールを同時に移動する方法を説明しています。またはルール エディタを使用して個々の SSL ルールを移動することもできます。SSL ルールの概要と作成（13-4 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。

ステップ 1　移動するルールを含むポリシーの SSL ポリシー エディタで、ルールごとに空白部分をクリックして、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。

ステップ 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 SSL ポリシーの間では、SSL ルールのコピー アンド ペーストはできないことに注意してください。

ステップ 3　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

新しい SSL ルール カテゴリの追加

ライセンス:任意

SSL ルールを編成しやすいように、SSL ポリシーには、Administrator Rules（管理者ルール）、Standard Rules（標準ルール）、Root Rules（ルート ルール）という、ASA FirePOWER モジュールが提供する 3 つのルール カテゴリが用意されています。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。

ステップ 1　ルール カテゴリを追加するポリシーの SSL 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。

ステップ 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。

ステップ 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。

ステップ 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。

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

SSL ルールのトラブルシューティング

ライセンス:任意

SSL ルールを適切に作成して順序付けることは複雑な作業ですが、効果的な展開を構築する上で不可欠な作業です。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。ASA FirePOWER モジュールによりトラフィックが予期したとおりに確実に処理されるようにするために、SSL ポリシー インターフェイスには、ルールに関する強力な警告およびエラーのフィードバック システムが用意されています。

各ルールについては、次の表に示すように、ポリシー エディタのアイコンによる警告とエラーの表示がされます。アイコンにポインタを合わせると、警告、エラー、情報の内容を示すテキストを確認できます。

表 *13-2*　*SSL* のエラー アイコン

アイコン	説明	詳細
	警告	問題によっては、ルールやその他の警告を示している SSL ポリシーに適用できる場合があります。この場合、間違いのある設定には効果がありません。たとえば、プリエンプションされたルールはトラフィックを評価しません。ただし、警告アイコンがライセンス エラーまたはモデルの不一致を示している場合は、問題が解消されるまでそのポリシーは適用できません。 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。
	error	ルールまたはその他の SSL ポリシー設定にエラーがある場合、問題が解消されるまでそのポリシーは適用できません。
	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。これらの問題は重大ではなく、ポリシーの適用を妨げません。

SSL ルールを適切に設定することは、ネットワーク トラフィックの処理に必要なリソースの軽減にも寄与します。複雑なルールを作成したり、ルールの順番が不適切であったりすると、パフォーマンスに影響す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。

- 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（13-17 ページ）
- SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避（13-18 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

ライセンス:任意

SSL ルールを適切に設定して順序付けることは、効果的な展開を構築する上で不可欠な要素です。SSL ポリシーの内部では、SSL ルールで他のルールのプリエンプションが発生したり、無効な設定が含まれたりする場合があります。これらの問題を示すために、警告およびエラーのアイコンが表示されます。

ルールのプリエンプションの警告について

SSL 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: do not decrypt Administrators
Rule 2: block Administrators
```

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。

無効な設定の警告について

SSL 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 SSL 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。

- URL カテゴリ条件を含むルールは有効であったものの、URL フィルタリング（URL Filtering）ライセンスを持たないモジュールをターゲットにすることで無効になる可能性があります。その時点で、ルールの横にエラー アイコンが表示され、ポリシーをそのデバイスに適用できなくなります。適用可能にするには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、または適切なライセンスを有効にする必要があります。
- [復号 - 再署名（Decrypt-Resign）] ルールを作成し、後でパッシブ インターフェイスでセキュリティ ゾーンをゾーン条件に追加した場合、ルールの横に警告アイコンが表示されます。パッシブ展開では証明書の再署名によるトラフィックの復号はできないので、パッシブ インターフェイスをルールから削除するか、またはルール アクションを変更するまで、このルールには効果がありません。
- ルールにユーザを追加した後、LDAP ユーザ認識設定を変更してそのユーザを除外すると、ユーザはアクセス コントロールの対象ユーザではなくなるため、そのルールは効果がなくなります。

SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避

ライセンス：任意

SSL ポリシーのルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルール番号の昇順で、ルールを上から順に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。

適切な SSL ルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、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、ある一人のユーザからの発信トラフィックは詳細な解析用に復号するが（[復号 - 再署名（Decrypt-Resign）] ルールを使用）、その部門の他のすべてのユーザからのトラフィックは復号しない場合は（[復号しない（Do not decrypt）] ルールを使用）、この順序で 2 つの SSL 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。

ここで 1 つのシナリオとして、信頼できる CA（Good CA）が悪意のあるエンティティ（Bad CA）に間違って CA 証明書を発行してしまい、その証明書を取り消していない状況を考えてみましょう。信頼できない CA によって発行された証明書で暗号化されたトラフィックはブロックしたいが、信頼できる CA の信頼チェーン内にあるそれ以外のトラフィックは許可したいとします。ここで必要となるのは、CA 証明書およびすべての中間 CA 証明書をアップロードし、その後に次のようにルールを順序付けることです。

```
Rule 1: Block issuer CN=www.badca.com
Rule 2: Do not decrypt issuer CN=www.goodca.com
```

ルールを入れ替える場合は次のようになります。

```
Rule 1: Do not decrypt issuer CN=www.goodca.com
Rule 2: Block issuer CN=www.badca.com
```

最初のルールは Good CA によって信頼されたすべてのトラフィックに一致し、その中には Bad CA によって信頼されたトラフィックも含まれます。どのトラフィックも 2 番目のルールに一致しないため、悪意のあるトラフィックはブロックされずに許可される可能性があります。

証明書でピニングしたサイトからのトラフィックを許可するルールの配置

証明書のピニングを行うと、SSL セッションが確立される前に、サーバの公開キー証明書が、サーバにすでに関連付けられているブラウザの証明書と一致しているかどうかを、クライアントのブラウザが強制的に確認します。[復号 - 再署名（Decrypt - Resign）] アクションにはサーバ証明書を変更してからクライアントに渡すという動作が含まれているため、ブラウザがすでにその証明書をピニングしている場合は、変更された証明書が拒否されます。

たとえば、クライアント ブラウザが、証明書のピニングを使用するサイト `windowsupdate.microsoft.com` に接続されており、そのトラフィックと一致する SSL ルールを [復号 - 再署名（Decrypt - Resign）] アクションを使用して設定すると、ASA FirePOWER モジュールはサーバ証明書に再署名してから、クライアント ブラウザに渡します。この変更されたサーバ証明書は、ブラウザでピニングした `windowsupdate.microsoft.com` の証明書と一致しないため、クライアント ブラウザは接続を拒否します。

このトラフィックを許可するには、サーバ証明書の共通名または識別名と一致させるために、[復号しない（Do not decrypt）] アクションを使用して SSL ルールを設定します。SSL ポリシーでは、このルールを、トラフィックと一致するすべての [復号 - 再署名（Decrypt - Resign）] ルールの前に配置してください。Web サイトに正常に接続された後で、クライアント ブラウザから、ピニングされた証明書を取得できます。また、接続が成功した場合も、失敗した場合も、ログに記録された接続イベントから証明書を表示できます。

トラフィックを復号するルールは後方に配置する

トラフィックの復号はリソースを必要とする処理なので、トラフィックの復号を実行しないルール（[復号しない（Do not decrypt）]、[ブロック（Block）]）を、実行するルール（[復号 - 既知のキー（Decrypt-Known Key）]、[復号 - 再署名（Decrypt-Resign）]）より前に配置することで、パフォーマンスが向上する可能性があります。この理由は、トラフィックの復号には多量のリソースを消費するものがあるからです。また、[ブロック（Block）] ルールにより、ASA FirePOWER モジュールが復号やインスペクションの対象とするはずのトラフィックが迂回する可能性があります。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
- それ以上のインスペクションを行わずにトラフィックをブロックする [ブロック（Block）] ルール
- 暗号化トラフィックを復号しない [復号しない（Do not decrypt）] ルール
- 既知の秘密キーを使用して着信トラフィックを復号する [復号 - 既知のキー（Decrypt-Known Key）] ルール
- サーバ証明書に再署名することによって発信トラフィックを復号する [復号 - 再署名（Decrypt-Resign）] ルール

パフォーマンスを改善する SSL インスペクション設定

ライセンス:任意

複雑な SSL ポリシーおよびルールは、多量のリソースを消費する可能性があります。SSL ポリシーが適用されると、ASA FirePOWER モジュールはすべてのルールをまとめて評価し、デバイスがネットワーク トラフィックの評価に使用する基準の拡張セットを作成します。デバイスでサポートされる SSL ルールの最大数を超えていることを警告するポップアップ ウィンドウが表示される場合があります。この最大値は、デバイスの物理メモリやプロセッサ数などの、さまざまな要因によって異なります。

ルールの単純化

次のガイドラインは、SSL ルールの単純化とパフォーマンスの向上に役立ちます。

- 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。

  SSL ルール条件で使用するオブジェクトに要素を結合しても、パフォーマンスは向上しないことに注意してください。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。

トラフィック復号の設定

トラフィック復号を設定する際は、次の注意事項に従ってください。

- トラフィックの復号では、トラフィックを復号し、アクセス コントロールを使用して検査する処理のリソースを必要とします。処理対象を絞り込んだ復号ルールを作成すると、ASA FirePOWER モジュールが復号するトラフィック量が、処理対象が広範な復号ルールより減るので、結果として、トラフィック復号に必要な処理のリソースも削減されます。暗号化トラフィックは、いったん復号した後にアクセス コントロール ルールを使用して許可またはブロックするのではなく、できるだけブロックするかまたは復号しないことを選択します。
- ルート発行元 CA に基づいてトラフィックを信頼するように証明書ステータスの条件を設定する場合は、ルート CA 証明書およびルート CA 信頼チェーン内のすべての中間 CA 証明書を SSL ポリシーにアップロードするようにします。信頼できる CA の信頼チェーン内のすべてのトラフィックは復号なしで許可されるようになり、不要な復号は実施されません。

SSL ルールを使用したトラフィック復号の調整

ASA FirePOWER モジュールで検査されるすべての暗号化トラフィックには、基本的な SSL ルールに基づいたアクションが適用されます。暗号化トラフィックをより詳細に復号および制御するには、特定タイプのトラフィックの処理およびログ記録を制御するルール条件を設定します。各 SSL ルールには 0 個、1 個、または複数の条件を設定できますが、トラフィックに SSL ルールが適用されるのは、そのルールのすべての条件にトラフィックが一致する場合のみです。

(注) トラフィックがルールに一致すると、ASA FirePOWER モジュールはそのルールのアクションをトラフィックに適用します。ログの記録が指定されている場合、接続が終了した時点でトラフィックに関するログが記録されます。詳細については、ルール アクションを使用した暗号化トラフィックの処理と検査の決定（13-9 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（33-10 ページ）を参照してください。

各ルール条件には、照合するトラフィックのプロパティを 1 つまたは複数指定できます。たとえば、以下のプロパティを指定できます。

- 通過するセキュリティ ゾーン、IP アドレスおよびポート、送信元または宛先の国などのトラフィック フロー
- 検出された IP アドレスに関連付けられたユーザ
- トラフィックで検出されたアプリケーションなどのトラフィック ペイロード
- 接続の暗号化に使用された SSL/TLS プロトコル バージョン、暗号スイート、サーバ証明書などの接続暗号化
- サーバ証明書の識別名に指定された URL のカテゴリおよびレピュテーション

詳細については、次の項を参照してください。

- SSL ルールによる復号可能接続のロギング（33-15 ページ）
- ネットワーク ベースの条件による暗号化トラフィックの制御（14-2 ページ）
- レピュテーションによる暗号化トラフィックの制御（14-8 ページ）
- 暗号化のプロパティに基づいたトラフィックの制御（14-18 ページ）

ネットワーク ベースの条件による暗号化トラフィックの制御

ライセンス:任意

SSL ポリシーに追加する SSL ルールにより、暗号化トラフィックの処理やログ記録を詳細に制御できます。ネットワークベースの条件を使用して、ネットワークを通過する暗号化トラフィックを管理できます。以下の条件を使用できます。

- 送信元と宛先セキュリティ ゾーン
- 送信元と宛先 IP アドレスまたは地理的位置
- 送信元と宛先のポート

ネットワークベースの複数の条件を組み合わせたり、他のタイプの条件と組み合わせたりして、SSL ルールを作成できます。これらの SSL ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。SSL ルールの詳細については、SSL ルール クイック スタート ガイド(13-1 ページ)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。

- ネットワーク ゾーンによる暗号化トラフィックの制御(14-2 ページ)
- ネットワークまたは地理的位置による暗号化トラフィックの制御(14-4 ページ)
- ポートによる暗号化トラフィックの制御(14-6 ページ)

ネットワーク ゾーンによる暗号化トラフィックの制御

ライセンス:任意

SSL ルールでゾーン条件を設定すると、暗号化トラフィックの送信元および宛先のセキュリティ ゾーンに応じてそのトラフィックを制御できます。

セキュリティ ゾーンは、1 つ以上のインターフェイスのグループです。検出モードと呼ばれる、デバイスの初期セットアップ時に選択するオプションによって、ASA FirePOWER モジュールが最初にデバイスのインターフェイスをどのように設定するか、およびこれらのインターフェイスがセキュリティ ゾーンに属するかどうかが決定します。

単純な例として、インライン検出モードを選択したデバイスでは、ASA FirePOWER モジュールにより内部と外部の 2 つのゾーンが作成され、そのデバイスの最初のインターフェイスのペアがそれらのゾーンに割り当てられます。内部側のネットワークに接続されたホストは、保護されている資産を表します。

ヒント　内部(または外部)のすべてのインターフェイスを 1 つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティ ポリシーが意味をなすグループ化を選択します。ゾーン作成の詳細については、セキュリティ ゾーンの操作(2-37 ページ)を参照してください。

この展開では、これらのホストにインターネットへの無制限アクセスを提供できますが、着信する暗号化トラフィックを復号および検査してホストを保護しなければなりません。

SSL インスペクションでこれを実現するには、[宛先ゾーン(Destination Zone)] を [内部(Internal)] に設定したゾーン条件を SSL ルールに定義します。この単純な SSL ルールでは、内部ゾーンのいずれかのインターフェイスからデバイスを離れるトラフィックが照合されます。

より複雑なルールを作成する場合は、1 つのゾーン条件で [送信元ゾーン（Source Zones）] および [宛先ゾーン（Destination Zones）] それぞれに対し、最大 50 のゾーンを追加できます。

- 特定のゾーンのインターフェイスからデバイスを離れる暗号化トラフィックを照合するには、そのゾーンを [宛先ゾーン（Destination Zones）] に追加します。

  パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブなインターフェイスで構成されるゾーンを [宛先ゾーン（Destination Zones）] 条件で使用することはできません。
- 特定のゾーンのインターフェイスからデバイスに入る暗号化トラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。

送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

ゾーン内のすべてのインターフェイスが同じタイプ（インライン、パッシブ、スイッチド、またはルーテッド）である必要があるため、SSL ルールのゾーン条件で使用されているすべてのゾーンが同じタイプでなければならないことに注意してください。つまり、異なるタイプのゾーンを送信元/宛先とする暗号化トラフィックを照合する単一ルールを定義することはできません。

ゾーンにインターフェイスが含まれていないなど、無効な設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

ゾーン条件に基づいて暗号化トラフィックを制御するには、次の手順を実行します。

ステップ 1　ゾーンに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（13-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[ゾーン（Zones）] タブを選択します。

[ゾーン（Zones）] タブが表示されます。

ステップ 3　[利用可能なゾーン（Available Zones）] から追加するゾーンを見つけて選択します。

追加するゾーンを検索するには、[利用可能なゾーン（Available Zones）] リストの上にある [名前で検索（Search by name）] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

クリックすると、ゾーンを選択できます。複数のゾーンを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

ステップ 4　[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックして、選択したゾーンを適切なリストに追加します。

選択したゾーンをドラッグ アンド ドロップすることもできます。

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、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

ネットワークまたは地理的位置による暗号化トラフィックの制御

ライセンス：任意

SSL ルールでネットワーク条件を設定すると、暗号化トラフィックの送信元および宛先の IP アドレスに応じてそのトラフィックを制御および復号できます。次のいずれかの操作を実行できます。

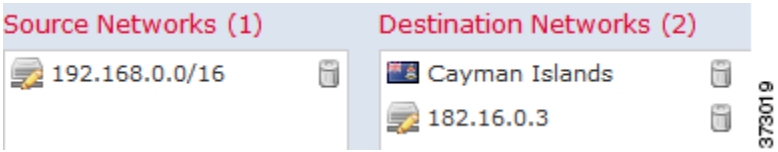
- 制御する暗号化トラフィックの送信元および宛先の IP アドレスを明示的に指定する。
- IP アドレスを地理的位置に関連付ける位置情報機能を使用して、その送信元または宛先の国または大陸に基づいて暗号化トラフィックを制御する。

ネットワークベースの SSL ルールの条件を作成する場合、IP アドレスと地理的位置を手動で指定できます。または、再利用可能で名前を 1 つ以上の IP アドレス、アドレス ブロック、国、大陸などに関連付けるネットワーク オブジェクトおよび位置情報オブジェクトを使用してネットワーク条件を設定できます。

ヒント　ネットワーク オブジェクトや位置情報オブジェクトを作成しておくと、それを使用して SSL ルールを作成したり、モジュール インターフェイスのさまざまな場所で IP アドレスを表すオブジェクトとして使用したりできます。これらのオブジェクトはオブジェクト マネージャを使用して作成できます。また、SSL ルールの設定時にネットワーク オブジェクトをオンザフライで作成することもできます。詳細については、再利用可能なオブジェクトの管理（2-1 ページ）を参照してください。

地理的位置別にトラフィックを制御するルールを作成する場合は、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必要があります。このため、シスコではASA FirePOWER モジュールの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推奨しています。位置情報データベースの更新（43-21 ページ）を参照してください。

次の図は、内部ネットワークから発信され、ケイマン諸島（Cayman Islands）または海外にある持ち株会社のサーバ（182.16.0.3）のリソースにアクセスしようとする暗号化接続をブロックする SSL ルールのネットワーク条件を示しています。



この例では、持ち株会社のサーバの IP アドレスを手動で指定し、ケイマン諸島の IP アドレスを表すASA FirePOWER モジュール提供の位置情報オブジェクト Cayman Islands を使用しています。

1 つのネットワーク条件で [送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] それぞれに対し、最大 50 の項目を追加でき、ネットワークベースの設定と位置情報ベースの設定を組み合わせることができます。

- 特定の IP アドレスまたは地理的位置からの暗号化トラフィックを照合するには、[送信元ネットワーク（Source Networks）] を設定します。
- 特定の IP アドレスまたは地理的位置への暗号化トラフィックを照合するには、[宛先ネットワーク（Destination Networks）] を設定します。

送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信される暗号化トラフィックの照合を行う必要があります。

ネットワーク条件を作成する際、警告アイコンは無効な設定を示します。アイコンの上にポインタを置くと詳細が表示されます。

ネットワークまたは地理的位置別にトラフィックを制御するには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

ステップ 1　ネットワークに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（13-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[ネットワーク（Networks）] タブを選択します。

[ネットワーク（Networks）] タブが表示されます。

ステップ 3　[利用可能なネットワーク（Available Networks）] から、次のように追加するネットワークを見つけて選択します。

- 追加するネットワーク オブジェクトとグループを表示するには [ネットワーク（Networks）] タブをクリックします。位置情報オブジェクトを表示するには [位置情報（Geolocation）] タブをクリックします。
- ここでネットワーク オブジェクトを作成してリストに追加するには、[利用可能なネットワーク（Available Networks）] リストの上にある追加アイコン（ ）をクリックし、ネットワーク オブジェクトの操作（2-4 ページ）の手順に従います。
- 追加するネットワーク オブジェクトまたは位置情報オブジェクトを検索するには、適切なタブを選択し、[利用可能なネットワーク（Available Networks）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックして、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

ステップ 4　[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5　手動で指定する送信元または宛先 IP アドレスまたはアドレス ブロックを追加します。

[送信元ネットワーク（Source Networks）] リストまたは [宛先ネットワーク（Destination Networks）] リストの下にある [IP アドレスの入力（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 [追加（Add）] をクリックします。

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、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

ポートによる暗号化トラフィックの制御

ライセンス：任意

SSL ルールでポート条件を設定すると、暗号化トラフィックの送信元および宛先の TCP ポートに応じてそのトラフィックを制御できます。ポートベースの SSL ルールの条件を作成するときは、手動で TCP ポートを指定できます。または、再利用可能で名前を 1 つ以上のポートに関連付けるポート オブジェクトを使用してポート条件を設定できます。

ヒント　ポート オブジェクトを作成しておくと、それを使用して SSL ルールを作成したり、モジュール インターフェイスのさまざまな場所でポートを表すオブジェクトとして使用したりできます。ポート オブジェクトは、オブジェクト マネージャを使用して作成できます。また、SSL ルールの設定時に作成することもできます。詳細については、ポート オブジェクトの操作（2-11 ページ）を参照してください。

1 つのネットワーク条件で [選択した送信元ポート（Selected Source Ports）] および [選択した宛先ポート（Selected Destination Ports）] それぞれに対し、最大 50 の項目を追加できます。

- 特定の TCP ポートからの暗号化トラフィックを照合するには、[選択した送信元ポート（Selected Source Ports）] を設定します。
- 特定の TCP ポートへの暗号化トラフィックを照合するには、[選択した宛先ポート（Selected Destination Ports）] を設定します。
- [選択した送信元ポート（Selected Source Ports）] および [選択した宛先ポート（Selected Destination Ports）] の両方を設定すると、特定の送信元（Source）TCP ポートから発信されかつ特定の宛先（Destination）TCP ポートに送信される暗号化トラフィックが照合されます。

[選択した送信元ポート（Selected Source Ports）] および [選択した宛先ポート（Selected Destination Ports）] リストで設定できるのは TCP ポートだけです。非 TCP ポートを含んでいるポート オブジェクトは、[使用可能なポート（Available Ports）] リストでグレー表示されます。

ポート条件を作成する際、警告アイコンは無効な設定を示します。たとえば、オブジェクト マネージャを使用して使用中のポート オブジェクトを編集し、それらのオブジェクト グループを使用するルールを無効にできます。アイコンの上にポインタを置くと詳細が表示されます。

ポート別にトラフィックを制御するには、次の手順を実行します。

ステップ 1　TCP ポートに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（13-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[ポート（Ports）] タブを選択します。

[ポート（Ports）] タブが表示されます。

ステップ 3　[使用可能なポート（Available Ports）] で、追加する TCP ポートを選択します。

- ここで TCP ポート オブジェクトを作成してリストに追加するには、[使用可能なポート（Available Ports）] リストの上にある追加アイコン（ ）をクリックし、ポート オブジェクトの操作（2-11 ページ）の手順に従います。
- 追加する TCP ベースのポート オブジェクトおよびグループを検索するには、[使用可能なポート（Available Ports）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトのポートの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。たとえば、「443」と入力すると、ASA FirePOWER モジュール提供の HTTPS ポート オブジェクトがASA FirePOWER モジュールに表示されます。

TCP ベースのポート オブジェクトをクリックして選択します。複数の TCP ベースのポート ジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。または、右クリックして [すべて選択（Select All）] を選択します。非 TCP ベースのポートを含んでいるオブジェクトは、ポート条件に追加できません。

ステップ 4　[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5　送信元または宛先のポートを手動で指定するには、[選択した送信元ポート（Selected Source Ports）] または [選択した宛先ポート（Selected Destination Ports）] リストの下にある [ポート（Port）] にポート番号を入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。

ステップ 6　[追加（Add）] をクリックします。

ASA FirePOWER モジュールでは、無効なポート設定はルール条件に追加されません。

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、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

ユーザ ベースの暗号化トラフィックの制御

ライセンス：Control

SSL ルールでユーザ条件を設定すると、Microsoft Active Directory サーバから取得されるユーザに応じてそのトラフィックを制御できます。SSL ルールのユーザ条件では、ホストにログインする LDAP ユーザに基づいてトラフィックのネットワーク通過を許可するユーザ制御が可能になります。

ユーザ制御は、アクセス コントロールされたユーザと IP アドレスを関連付けることによって機能します。展開されたエージェントは、ホストにログインまたはホストからログアウトするとき、または他の理由で Active Directory クレデンシャルで認証する場合に、指定されたユーザをモニタします。たとえば、組織は一元化された認証のために Active Directory に依存するサービスまたはアプリケーションを使用できます。

ユーザ条件を設定した SSL ルールとトラフィックを一致させるには、モニタ対象のセッションにおける送信元または宛先ホストの IP アドレスと、ログインするアクセス コントロールされたユーザを関連付ける必要があります。個々のユーザまたはユーザが属しているグループに基づいてトラフィックを制御できます。

複数のユーザ条件を組み合わせたり、他のタイプの条件と組み合わせたりして、SSL ルールを作成できます。これらの SSL ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。SSL ルールの詳細については、SSL ルールの概要と作成（13-4 ページ）を参照してください。

ユーザ制御機能を使用するには、Control ライセンスが必要です。また、サポートされるのは LDAP ユーザとグループ（アクセス コントロールされたユーザ）だけで、Microsoft Active Directory サーバをモニタするユーザ エージェントからのログインおよびログアウト レコードが使用されます。

ユーザ条件を含む SSL ルールを作成する前に、組織内の少なくとも 1 つの Microsoft Active Directory サーバと ASA FirePOWER モジュール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も指定されます。

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 クレデンシャル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 ASA FirePOWER モジュールに送信します。これらのレコードによりユーザが IP アドレスに関連付けられ、これに基づいてユーザ条件を含んでいる SSL ルールがトリガー可能になります。

ユーザ条件に基づいて暗号化トラフィックを制御するには、次の手順を実行します。

ステップ 1　ユーザに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（13-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[ユーザ（Users）] タブを選択します。

[ユーザ（Users）] タブが表示されます。

ステップ 3　追加するユーザを検索するには、[使用可能なユーザ（Available Users）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、ユーザ名を入力します。入力を開始するとリストが更新され、一致するユーザが表示されます。

ユーザをクリックして選択します。複数のユーザを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのユーザを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ 4　[ルールに追加（Add to Rule）] をクリックして、選択したユーザを [選択されたユーザ（Selected Users）] リストに追加します。

選択したユーザをドラッグ アンド ドロップでリストに追加することもできます。

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、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

レピュテーションによる暗号化トラフィックの制御

ライセンス：Controlまたは URL フィルタリング（URL Filtering）

SSL ルールでレピュテーション ベース条件を設定すると、ネットワーク トラフィックをコンテキスト化して状況に応じて制限することで、ネットワーク通過を許可する暗号化トラフィックを管理できます。SSL ルールでのレピュテーション ベースの制御には、以下のタイプがあります。

- アプリケーション条件によるアプリケーション制御では、個々のアプリケーションだけでなく、アプリケーションの基本的な特性（タイプ、リスク、ビジネスとの関連性、およびカテゴリ）に基づいてアプリケーション トラフィックを制御できます。
- URL 条件では、Web サイトに割り当てられたカテゴリおよびレピュテーションに基づいて Web トラフィックを制御できます。

レピュテーションベースの複数の条件を組み合わせたり、他のタイプの条件と組み合わせたりして、SSL ルールを作成できます。これらの SSL ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。

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 ベースの暗号化トラフィックの制御（14-8 ページ）
- URL カテゴリおよびレピュテーションによる暗号化トラフィックの制御（14-14 ページ）

アプリケーション ベースの暗号化トラフィックの制御

ライセンス：Control

FireSIGHT システムは、暗号化された IP トラフィックを分析するときに、ネットワーク上で一般的に使用されている暗号化アプリケーションを識別および分類してから暗号化セッションを復号します。ASA FirePOWER モジュールはこうした検出ベースのアプリケーション認識機能を使用して、ネットワーク上の暗号化されたアプリケーション トラフィックを制御できます。

SSL ルールのアプリケーション条件では、このアプリケーション制御を行います。1 つの SSL ルールにおいて、トラフィックの制御対象とするアプリケーションを複数の方法で指定できます。

- カスタム アプリケーションなどの個々のアプリケーションを選択できます。
- ASA FirePOWER モジュール提供のアプリケーション フィルタを使用する。このフィルタは、基本的な特性（タイプ、リスク、ビジネスとの関連性、およびカテゴリ）に基づいてアプリケーションをグループ化して名前を付けたものを指します。
- 選択したアプリケーション（カスタム アプリケーションを含む）をグループ化するカスタム アプリケーション フィルタを作成し、使用できます。

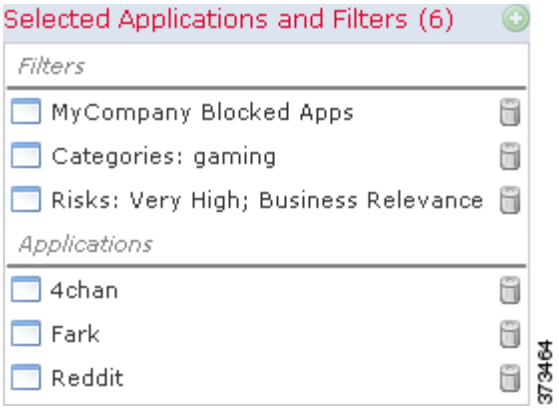
（注）　アクセス コントロール ルールを使用してアプリケーション トラフィックをフィルタ処理する場合、フィルタ条件としてアプリケーション タグを使用できます。ただし、暗号化トラフィックはアプリケーション タグでフィルタ処理できません。そのことには意味がないからです。ASA FirePOWER モジュールが暗号化トラフィックのアプリケーションを検出するにはタグ付きの **SSL** プロトコルである必要があり、このタグが付けられていないアプリケーションは、非暗号化トラフィックまたは復号されたトラフィックでしか検出できません。

アプリケーション フィルタを利用すると、SSL ルールのアプリケーション条件を簡単に作成できます。このフィルタによって、ポリシーの作成と管理が簡素化され、モジュールは Web トラフィックを期待通りに確実に制御します。たとえば、暗号化トラフィックのリスクが高くビジネスとの関連性の低いアプリケーションをすべて識別して復号する SSL ルールを作成できます。ユーザがこれらのアプリケーションの使用を試みると、アクセス コントロールによってセッションが復号されて検査されます。

また、シスコ は、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にディテクタを更新し追加します。独自のディテクタを作成し、そのディテクタが検出するアプリケーションに特性（リスク、関連性など）を割り当てることもできます。アプリケーションの特性に基づいたフィルタを使用することで、モジュールは最新のディテクタを使用してアプリケーション トラフィックをモニタします。

アプリケーション条件を設定した SSL ルールとトラフィックを一致させるには、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加したいずれかのアプリケーションまたはフィルタにトラフィックが一致する必要があります。

次の図は、MyCompany のアプリケーション、リスクが高くビジネスとの関連性の低いすべてのアプリケーション、ゲーム アプリケーション、およびいくつかの指定アプリケーションからなるカスタム グループを復号する、SSL ルールのアプリケーション条件を示しています。



1 つのアプリケーション条件において、最大 50 の項目を [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加できます。以下はそれぞれ 1 つの項目としてカウントされます。

- 個別またはカスタムな組み合わせの、[アプリケーション フィルタ（Application Filters）] リストからの 1 つ以上のフィルタ。この項目は、特性によってグループ化されたアプリケーションのセットを表します。
- [使用可能なアプリケーション（Available Applications）] リストにあるアプリケーションの検索結果を保存することで作成されたフィルタ。この項目は、部分文字列の一致によってグループ化されたアプリケーションのセットを表します。
- [使用可能なアプリケーション（Available Applications）] リストからの個々のアプリケーション。

モジュール インターフェイスでは、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。

SSL ポリシーの適用時には、ASA FirePOWER モジュールは、アプリケーション条件を持つルールごとに一致する固有のアプリケーションのリストを生成することに注意してください。つまり、完全なカバレッジを確保するために、重複フィルタおよび個々に指定されたアプリケーションを使用できます。

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 フィルタと暗号化トラフィックの照合（14-10 ページ）
- 個々のアプリケーションからのトラフィックの照合（14-11 ページ）
- SSL ルールへのアプリケーション条件の追加（14-13 ページ）
- 暗号化されたアプリケーションの制御に対する制限（14-14 ページ）

アプリケーション フィルタと暗号化トラフィックの照合

ライセンス：Control

SSL ルールのアプリケーション条件を作成するには、[アプリケーション フィルタ（Application Filters）] リストを使用して、照合するトラフィックの特性を基にアプリケーションをグループ化します。

便宜上、ASA FirePOWER モジュールは、指定された基準を使用して、検出したアプリケーションのそれぞれを特徴付けます。これらの基準をフィルタとして使用したり、フィルタのカスタムな組み合わせを作成してアプリケーション制御を実行したりできます。

SSL ルールでのアプリケーション フィルタの機能は、オブジェクト マネージャを使用した再利用可能なカスタム アプリケーション フィルタの作成と同じです（アプリケーション フィルタの操作（2-13 ページ）を参照してください）。また、オンザフライで作成した多数のフィルタを、アクセス コントロール ルールに新規の再利用可能なフィルタとして保存できます。ユーザが作成したフィルタはネストすることができないため、別のユーザが作成したフィルタを含むフィルタは保存できません。

フィルタの組み合わせ方について

フィルタを単独または組み合わせて選択すると、[使用可能なアプリケーション（Available Applications）] リストが更新され、条件を満たすアプリケーションのみが表示されます。ASA FirePOWER モジュールによって提供されるフィルタは組み合わせて選択できますが、カスタム フィルタはできません。

モジュールは、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
```

Medium（中）フィルタに 110 個のアプリケーション、High（高）フィルタに 82 個のアプリケーションが含まれる場合、[使用可能なアプリケーション（Available Applications）] リストにはこれら 192 個のアプリケーションがすべて表示されます。

モジュールは、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（リスク）タイプで Medium（中）および High（高）フィルタを選択し、Business Relevance（ビジネスとの関連性）タイプで Medium（中）および High（高）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、モジュールは Medium（中）または High（高）の Risk（リスク）タイプと Medium（中）または High（高）の Business Relevance（ビジネスとの関連性）タイプの両方に含まれるアプリケーションだけを表示します。

フィルタの検索および選択

フィルタを選択するには、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。シスコ提供のフィルタ タイプ（[リスク（Risks）]、[ビジネス関連性（Business Relevance）]、[タイプ（Types）]、または [カテゴリ（Categories）]）を右クリックして、[すべて選択（Check All）] または [すべて選択解除（Uncheck All）] を選択することもできます。

フィルタを検索するには、[使用可能なフィルタ（Available Filters）] リストの上にある [名前で検索（Search by name）] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するフィルタが表示されます。

フィルタを選択したら、[使用可能なアプリケーション（Available Applications）] リストを使用してそのフィルタをルールに追加し、個々のアプリケーションからのトラフィックの照合（14-11 ページ）の手順に従います。

個々のアプリケーションからのトラフィックの照合

ライセンス：Control

SSL ルールのアプリケーション条件を作成するには、[使用可能なアプリケーション（Available Applications）] リストを使用して、照合するトラフィックのアプリケーションを選択します。

アプリケーションのリストの参照

条件の作成を初めて開始するときは、リストは制約されておらず、モジュールが検出するすべてのアプリケーションを一度に 100 個ずつ表示します。

- アプリケーションを確認していくには、リストの下にある矢印をクリックします。
- アプリケーションの特性に関するサマリー情報と参照できるインターネットの検索リンクが示されているポップアップ ウィンドウを表示するには、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。

照合するアプリケーションの検索

照合するアプリケーションを見つけやすくするために、[使用可能なアプリケーション（Available Applications）] リストを次のように制約できます。

- アプリケーションを検索するには、リスト上部にある [名前で検索（Search by name）] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するアプリケーションが表示されます。
- フィルタを適用してアプリケーションを制約するには、[アプリケーション フィルタ（Application Filters）] リストを使用します（アプリケーション フィルタと暗号化トラフィックの照合（14-10 ページ）を参照）。フィルタを適用すると、[使用可能なアプリケーション（Available Applications）] リストが更新されます。

制約されると、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] オプションが [使用可能なアプリケーション（Available Applications）] リストの上部に表示されます。このオプションを使用して、制約されたリスト内のすべてのアプリケーションを [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストにすべて一度に追加できます。

（注）　[アプリケーション フィルタ（Application Filters）] リストで 1 つ以上のフィルタを選択し、しかも [使用可能なアプリケーション（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 [使用可能なアプリケーション（Available Applications）] リストが AND 演算を使って結合されます。つまり [フィルタに一致するすべてのアプリケーション（All apps matching the filter）] 条件には、[使用可能なアプリケーション（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、[使用可能なアプリケーション（Available Applications）] リストの上で入力された検索文字列が含まれます。

条件内で照合する単一アプリケーションの選択

照合するアプリケーションを検索したら、それをクリックして選択します。複数のアプリケーションを選択するには、Shift キーおよび Ctrl キーを使用するか、または現在制約されているビュー内のすべてのアプリケーションを選択するには右クリックして [すべて選択（Select All）] を選択します。

1 つのアプリケーション条件において、アプリケーションの個別選択で追加できる最大数は 50 です。50 を超えるアプリケーションを追加するには、複数の SSL ルールを作成するか、フィルタを使用してアプリケーションをグループ化する必要があります。

条件のフィルタに一致するすべてのアプリケーションの選択

[アプリケーション フィルタ（Application Filters）] リストで検索またはフィルタを使用して制約されると、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] オプションが [使用可能なアプリケーション（Available Applications）] リストの上部に表示されます。

このオプションを使用して、制約された [使用可能なアプリケーション（Available Applications）] リスト内のアプリケーションのセット全体を [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに同時に追加できます。アプリケーションを個別に追加するのとは対照的に、このアプリケーションのセットを追加すると、そのセットを構成する個々のアプリケーションの数にかかわらず、最大 50 のアプリケーションに対してただ 1 つのアイテムとしてカウントされます。

このようにアプリケーション条件を作成するときは、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加するフィルタの名前は、フィルタに表されているフィルタ タイプ + 各タイプの最大 3 つの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（リスク）タイプの 2 つのフィルタと Business Relevance（ビジネスとの関連性）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,...
```

[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] で追加するフィルタに表されないフィルタ タイプは、追加するフィルタの名前に含まれません。[選択済みのアプリケーションとフィルタ（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 [任意（any）] 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制約しないので、任意の値が許可されます。

[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] の複数のインスタンスをアプリケーション条件に追加でき、各インスタンスは [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストで個別の項目としてカウントされます。たとえば、リスクが高いすべてのアプリケーションを 1 つの項目として追加し、選択内容をクリアしてから、ビジネスとの関連性が低いすべてのアプリケーションを別の項目として追加できます。このアプリケーション条件は、リスクが高いアプリケーションまたはビジネスとの関連性が低いアプリケーションに一致します。

SSL ルールへのアプリケーション条件の追加

ライセンス：Control

アプリケーション条件を設定した SSL ルールと暗号化トラフィックを一致させるには、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加したいずれかのアプリケーションまたはフィルタにトラフィックが一致する必要があります。

1 条件ごとに最大 50 の項目を追加でき、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。アプリケーション条件を作成する際、警告アイコンは無効な設定を示します。アイコンの上にポインタを置くと詳細が表示されます。

アプリケーション条件に基づいて暗号化トラフィックを制御するには、次の手順を実行します。

ステップ 1　アプリケーションに応じたトラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（13-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[アプリケーション（Applications）] タブを選択します。

[アプリケーション（Applications）] タブが表示されます。

ステップ 3　オプションで、フィルタを使用して [使用可能なアプリケーション（Available Applications）] リストに表示されるアプリケーションのリストを制約します。

[アプリケーション フィルタ（Application Filters）] リストで 1 つ以上のフィルタを選択します。詳細については、アプリケーション フィルタと暗号化トラフィックの照合（14-10 ページ）を参照してください。

ステップ 4　[使用可能なアプリケーション（Available Applications）] リストから追加するアプリケーションを見つけて選択します。

個々のアプリケーションを検索して選択するか、またはリストが制約されている場合は、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] を選択できます。詳細については、個々のアプリケーションからのトラフィックの照合（14-11 ページ）を参照してください。

ステップ 5　[ルールに追加（Add to Rule）] をクリックして、選択したアプリケーションを [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加します。

選択したアプリケーションとフィルタをドラッグ アンド ドロップすることもできます。フィルタは [フィルタ（Filters）] という見出しの下に表示され、アプリケーションは [アプリケーション（Applications）] という見出しの下に表示されます。

ヒント　このアプリケーション条件に別のフィルタを追加する前に、[すべてのフィルタをクリア（Clear All Filters）] をクリックして既存の選択内容をクリアします。

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、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

暗号化されたアプリケーションの制御に対する制限

ライセンス：Control

アプリケーション制御を実行する際は、次の点に注意してください。

暗号化されたアプリケーションの識別

この ASA FirePOWER モジュールでは、StartTLS を使用して暗号化される非暗号化アプリケーションを識別できます。これには、SMTPS、POPS、FTPS、TelnetS、IMAPS などのアプリケーションが含まれます。また、TLS クライアントの hello メッセージ内の Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。

アプリケーション識別の速度

ASA FirePOWER モジュールは、以下のすべての処理が完了するまで暗号化トラフィックのアプリケーション制御を実行できません。

- 暗号化された接続がクライアントとサーバ間で確立される。
- 暗号化セッション内のアプリケーションがモジュールにより識別される。

この識別が行われるのは、サーバ証明書が交換された後です。ハンドシェイク中に交換されるトラフィックでアプリケーションの識別が完了する前に、アプリケーション条件を含んでいる SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。この動作により、ハンドシェイクが完了し、アプリケーションを識別できるようになります。便宜を図るため、影響を受けるルールは情報アイコン（ ）でマークされます。

モジュールによる識別が完了すると、アプリケーション条件に一致する残りのセッション トラフィックに SSL ルールのアクションが適用されます。

URL カテゴリおよびレピュテーションによる暗号化トラフィックの制御

ライセンス：URL フィルタリング（URL Filtering）

SSL ルールの URL 条件では、ネットワーク上のユーザからアクセス可能な暗号化 Web サイト トラフィックの処理と復号を行います。要求された URL は、SSL ハンドシェイク時に提供される情報に基づいて検出されます。URL フィルタリング（URL Filtering）ライセンスでは、URL の一般的な分類であるカテゴリと、リスク レベルであるレピュテーションに基づいた Web サイトへのアクセス コントロールが可能です。

（注）　特定の URL に対するトラフィックの処理と復号は、識別名の SSL ルール条件を定義することで行えます。証明書のサブジェクト識別名にある共通名属性には、サイトの URL が含まれています。詳細については、証明書の識別名による暗号化トラフィックの制御（14-18 ページ）を参照してください。

詳細については、以下を参照してください。

- レピュテーション ベースの URL ブロッキングの実行（14-14 ページ）
- URL 検出とブロッキングの制約事項（14-17 ページ）

レピュテーション ベースの URL ブロッキングの実行

ライセンス：URL フィルタリング（URL Filtering）

URL フィルタリング（URL Filtering）ライセンスでは、要求された URL のカテゴリおよびレピュテーションに基づいて、Web サイトへのユーザ アクセスを制御できます。

- 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（Auctions）] カテゴリ、monster.com は [求職（Job Search）] 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、[高リスク（High Risk）]（レベル 1）から [ウェルノウン（Well Known）]（レベル 5）の範囲にまたがるものとなる可能性があります。

URL のカテゴリおよびレピュテーションは FireSIGHT システムがシスコクラウドから取得するもので、これを利用して SSL ルールの URL 条件を簡単に作成できます。たとえば、[乱用薬物（Abused Drugs）] カテゴリの高リスク URL をすべて識別してブロックする SSL ルールを作成できます。ユーザが暗号化接続でこのカテゴリおよびレピュテーションの URL にアクセスすると、そのセッションはブロックされます。

（注）　カテゴリとレピュテーション ベースの URL 条件の SSL ルールを使用するには、シスコクラウドとの通信を有効にしておく必要があります。これにより、ASA FirePOWER モジュールは URL データを取得できるようになります。詳細については、クラウド通信の有効化（41-2 ページ）を参照してください。

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、ポリシーの作成と管理がより簡単になります。また、暗号化された Web トラフィックの制御についての信頼度も向上します。最後に、クラウドは新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、モジュールは確実に最新の情報を使用して要求された URL をフィルタします。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（Gaming）] に分類されると、これらのサイトをモジュール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（Blog）] から [マルウェア（Malware）] に変更することができ、モジュールはそのサイトをブロックできます。
- ルールがリスクの高いソーシャル ネットワーキング サイトをブロックし、だれかがプロファイル ページに悪意のあるペイロードへのリンクが含まれる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（Benign sites）] から [高リスク（High Risk）] に変更でき、モジュールでそれをブロックできます。

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ASA FirePOWER モジュールがクラウドと通信できない場合、カテゴリやレピュテーションに基づく URL 条件を含む SSL ルールがトリガーされないことに注意してください。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

次の図は、すべてのマルウェア サイト、すべてのリスクの高いサイト、およびすべての安全でないソーシャル ネットワーキング サイトをブロックするアクセス コントロール ルールの URL 条件を示します。

ヒント　トラフィックを復号してからアクセス コントロールでブロックする場合、ユーザは警告ページをクリックして閉じることでブロックをバイパスできます。詳細については、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（6-9 ページ）を参照してください。

1 つの URL 条件で [選択したカテゴリ（Selected Categories）] リストに最大 50 の項目を追加できます。任意でレピュテーションによって制限された各 URL カテゴリは、1 つの項目としてカウントされます。

次の表では、前述の条件を作成する方法を要約します。レピュテーションでリテラル URL または URL オブジェクトを制限できないことに注意してください。

表 ***14-1***　例：***URL*** 条件の作成

ブロックする対象	選択するカテゴリまたは **URL** オブジェクト	選択するレピュテーション
マルウェア サイト（レピュテーションに関係なく）	マルウェア サイト（Malware Sites）	任意（Any）
高リスクの URL（レベル 1）	任意（Any）	1 - 高リスク（High Risk）
無害（benign）よりも大きいリスクがあるソーシャル ネットワーキング サイト（レベル 1 ～ 3）	ソーシャル ネットワーク（Social Network）	3 - セキュリティ リスクのある無害なサイト（Benign sites with security risks）

URL 条件を作成する際、警告アイコンは無効な設定を示します。アイコンの上にポインタを置くと詳細が表示されます。また、アクセス コントロール ポリシーおよびルールのトラブルシューティング（4-13 ページ）を参照してください。

カテゴリ データおよびレピュテーション データを使用した要求された **URL** によるトラフィックの制御

ステップ **1**　URL に応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（13-4 ページ）を参照してください。

ステップ **2**　SSL ルール エディタで、[カテゴリ（Categories）] タブを選択します。

[カテゴリ（Categories）] タブが表示されます。

ステップ **3**　[カテゴリ（Categories）] リストで、追加する URL カテゴリを選択します。カテゴリを指定せずにすべての暗号化 Web トラフィックと一致させるには、[任意（Any）] カテゴリを選択します。

追加可能なカテゴリを検索するには、[カテゴリ（Categories）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、カテゴリ名を入力します。入力すると、リストが更新されて一致するカテゴリが表示されます。

カテゴリを選択するには、そのカテゴリをクリックします。複数のカテゴリを選択するには、Shift キーおよび Ctrl キーを使用します。

ヒント　右クリックで表示される [すべて選択（Select All）] も利用できますが、この方法ですべてのカテゴリを追加すると、SSL ルールの最大項目数 50 を超えてしまいます。代わりに [任意（Any）] を使用してください。

ステップ 4　オプションで、[レピュテーション（Reputations）] リストからレピュテーション レベルをクリックして、カテゴリの選択内容を制限します。レピュテーション レベルを指定しない場合、モジュールはデフォルトとして [任意（Any）]（つまりすべてのレベル）を設定します。

選択できるレピュテーション レベルは 1 つだけです。レピュテーションのレベルを選択すると、SSL ルールはその目的に応じて異なる動作をします。

- ルールで Web アクセスのブロックまたはトラフィックの復号を行う場合（ルール アクションが、[ブロック（Block）]、[リセットしてブロック（Block with reset）]、[復号 - 既知のキー（Decrypt - Known Key）]、[復号 - 再署名（Decrypt - Resign）]、または [モニタ（Monitor）] の場合）、選択したレピュテーション レベルよりも厳しいすべてのレピュテーションも自動的に選択されます。たとえば疑わしいサイト（**Suspicious sites**）（レベル 2）をブロックするようルールを設定した場合、高リスク（**High Risk**）（レベル 1）のサイトも自動的にブロックされます。
- ルールで Web アクセスを許可して、アクセス コントロールに従わせる場合（ルール アクションが [復号しない（Do not decrypt）] の場合）、選択したレピュテーション レベルよりも厳しくないすべてのレピュテーションも自動的に選択されます。たとえば無害なサイト（**Benign sites**）（レベル 4）を許可するようルールを設定した場合、有名（**Well known**）（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、モジュールは、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。

ステップ 5　[ルールに追加（Add to Rule）] をクリックして、選択した項目を [選択したカテゴリ（Selected Categories）] リストに追加します。

選択した項目をドラッグ アンド ドロップすることもできます。

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、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

URL 検出とブロッキングの制約事項

ライセンス：URL フィルタリング（URL Filtering）

URL の検出とブロッキングを実行する際は、次の点に注意してください。

URL 識別の速度

モジュールによる URL のカテゴリ分類は、以下のすべての処理が完了するまで実行されません。

- モニタ対象の接続がクライアントとサーバの間で確立される。
- セッション内の HTTPS アプリケーションがモジュールにより識別される。
- 要求された URL をモジュールがクライアントの hello メッセージまたはサーバ証明書に基づいて識別する。

この識別が行われるのは、サーバ証明書が交換された後です。ハンドシェイク中に交換されるトラフィックで URL 識別が完了する前に、URL 条件を含んでいる SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。この動作により接続が確立され、URL の識別が可能になります。便宜を図るため、影響を受けるルールは情報アイコン（ ）でマークされます。

モジュールによる識別が完了すると、URL 条件に一致する残りのセッション トラフィックに SSL ルールのアクションが適用されます。

メモリの制約上、一部のモデルでは、小規模でそれほど細分化されていないカテゴリとレピュテーションによって URL フィルタリングが実行されます。たとえば、親 URL のサブサイトがそれぞれ異なる URL カテゴリとレピュテーションを持っている場合、一部のデバイスでは、すべてのサブサイトに対して親 URL のデータが使用されます。具体的な例として、システムは google.com カテゴリとレピュテーションを使用して mail.google.com を評価します。これに該当するデバイスは、71xx ファミリ と次の ASA モデルです。ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X。

仮想デバイスの場合は、インストール ガイドを参照して、レピュテーション ベースの URL フィルタリングを実行するための適切なメモリ量の割り当てを確認してください。

URL での検索クエリ パラメータ

モジュールでは、URL 条件の照合に URL 内の検索クエリ パラメータを使用しません。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。

暗号化のプロパティに基づいたトラフィックの制御

ライセンス:任意

暗号化接続の特性に基づいて暗号化トラフィックの処理および復号を行う SSL ルールを作成できます。セッションの暗号化に使用されている暗号スイートまたはプロトコル バージョンを検出して、それに応じてトラフィックを処理できます。また、サーバ証明書を検出して、以下の特性に基づいてトラフィックを処理することもできます。

- サーバ証明書自体。
- 証明書の発行元。証明書が CA で発行されているか自己署名されているか。
- 証明書のホルダー。
- 証明書ステータス。証明書が有効であるか、発行元の CA により無効にされているかなど。

複数の暗号スイートを 1 つのルールで検出したり、証明書の発行元や証明書ホルダーを検出したりする場合は、再利用可能な暗号スイートのリストおよび識別名オブジェクトを作成してルールに追加できます。サーバ証明書および特定の証明書ステータスを検出するには、ルール用の外部証明書と外部 CA オブジェクトの作成が必要です。

詳細については、次の項を参照してください。

- 証明書の識別名による暗号化トラフィックの制御（14-18 ページ）
- 証明書による暗号化トラフィックの制御（14-21 ページ）
- 証明書ステータスによる暗号化トラフィックの制御（14-22 ページ）
- 暗号スイートによる暗号化トラフィックの制御（14-26 ページ）
- 暗号化プロトコルのバージョンによるトラフィックの制御（14-28 ページ）

証明書の識別名による暗号化トラフィックの制御

ライセンス:任意

SSL ルールで識別名条件を設定すると、証明書ホルダーまたはサーバ証明書を発行した CA に応じて暗号化トラフィックを処理および検査できます。発行元の識別名を基準にすると、サイトのサーバ証明書を発行した CA に基づいてトラフィックを処理できます。

ルール条件を設定する場合は、手動でリテラル値を指定するか、識別名オブジェクトを参照するか、または複数のオブジェクトを含んでいる識別名グループを参照できます。

（注）　[復号 - 既知のキー（Decrypt - Known Key）] アクションを選択した場合、識別名条件を設定することはできません。このアクションでは、トラフィック復号用のサーバ証明書の選択が必要であるため、トラフィックの照合はすでにこの証明書で行われています。詳細については、復号アクション：さらに検査するためにトラフィックを復号（13-11 ページ）を参照してください。

複数のサブジェクトおよび発行元の識別名との照合を単一の証明書ステータスのルール条件で行うことも可能ですが、ルールとの照合で一致する必要があるのは 1 つの共通名または識別名だけです。

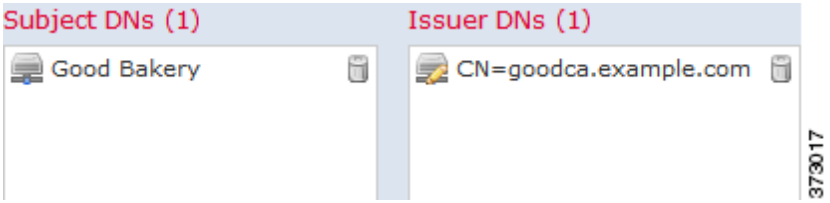
識別名を手動で追加する場合、共通名属性（**CN**）を含めることができます。「CN=」なしで共通名を追加すると、オブジェクトの保存時に「CN=」が追加されます。

さらに、次の表に示す属性を含む識別名を追加することもできます。属性はカンマで区切って使用します。

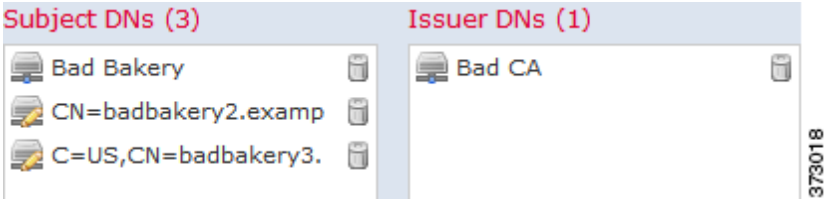
表 ***14-2***　　識別名の属性

属性（**Attribute**）	説明	使用可能な値
C	国コード（Country Code）	2 つの英字
CN	Common Name	最大 64 個の英数字、バックスラッシュ（\）、ハイフン（-）、引用符（"）、アスタリスク（*）、ピリオド（.）、またはスペース文字
O	Organization	
OU	組織	

次の図は、goodbakery.example.com に対して発行された証明書および goodca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。これらの証明書で暗号化されたトラフィックは許可され、アクセス コントロールにより制御されます。



次の図は、badbakery.example.com および関連ドメインに対して発行された証明書および badca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。これらの証明書で暗号化されたトラフィックは、再署名された証明書を使用して復号されます。



1 つの識別名条件で、[サブジェクト DN（Subject DNs）] リストおよび [発行元 DN（Issuer DNs）] リストにそれぞれ最大 50 のリテラル値および識別名オブジェクトを追加できます。

ASA FirePOWER モジュール提供の識別名オブジェクト グループである Sourcefire Undecryptable Sites には、モジュールで復号できないトラフィックの Web サイトが含まれています。このグループを識別名条件に追加すると、該当する Web サイトとのトラフィックがブロックしたり復号を無効にしたりでき、これらのトラフィックの復号に使用されるシステム リソースの浪費を回避できます。グループ内の各エントリは変更できますが、このグループを削除することはできません。システムによる更新によりこのリストのエントリが変更されることがありますが、モジュールではユーザによる変更が保持されます。

証明書のサブジェクトまたは発行元の識別名に基づいて暗号化トラフィックを検査するには、次の手順を実行します。

ステップ 1　証明書のサブジェクトまたは発行元の識別名に応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（13-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[DN] タブを選択します。

[DN] タブが表示されます。

ステップ 3　[使用可能な DN（Available DNs）] で、追加する識別名を選択します。

- ここで識別名オブジェクトを作成してリストに追加するには、[使用可能な DN（Available DNs）] リストの上にある追加アイコン（ ）をクリックし、識別名オブジェクトの操作（2-39 ページ）の手順に従います。
- 追加する識別名オブジェクトおよびグループを検索するには、[使用可能な DN（Available DNs）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

ステップ 4　次の選択肢があります。

- [サブジェクトに追加（Add to Subject）] をクリックして、選択したオブジェクトを [サブジェクト DN（Subject DNs）] リストに追加します。
- [発行元に追加（Add to Issuer）] をクリックして、選択したオブジェクトを [発行元 DN（Issuer DNs）] リストに追加します。

選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5　手動で指定するリテラル共通名または識別名がある場合は、それらを追加します。

[サブジェクト DN（Subject DNs）] または [発行元 DN（Issuer DNs）] リストの下にある [DN または CN の入力（Enter DN or CN）] プロンプトをクリックし、共通名または識別名を入力して [追加（Add）] をクリックします。

ステップ 6　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

証明書による暗号化トラフィックの制御

ライセンス:任意

SSL ルールで証明書条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書に応じて暗号化トラフィックを処理および検査できます。1 つの条件に 1 つまたは複数の証明書を設定でき、トラフィックの証明書がいずれかの条件の証明書と一致するとそのルールが適用されます。

証明書ベースの SSL ルール条件を作成するときにサーバ証明書をアップロードしたり、再利用可能な外部証明書オブジェクトとして保存してサーバ証明書の名前を関連付けたりできます。また、既存の外部証明書オブジェクトやオブジェクト グループを使用して証明書条件を設定することもできます。

ルール条件の [使用可能な証明書(Available Certificates)] フィールドでは、外部証明書オブジェクトやオブジェクト グループを証明書の識別名に関する以下の特性に基づいて検索できます。

- サブジェクトまたは発行元の共通名(CN)
- サブジェクトまたは発行元の組織(O)
- サブジェクトまたは発行元の組織単位(OU)

1 つの証明書のルール条件で複数の証明書を照合することもでき、トラフィックの暗号化に使用されている証明書がアップロードされた証明書のいずれかと一致した場合、その暗号化トラフィックはルールに一致したと判定されます。

1 つの証明書条件で、[選択した証明書(Selected Certificates)] リストに最大 50 の外部証明書オブジェクトおよび外部証明書オブジェクト グループを追加できます。

次の点に注意してください。

- [復号 - 既知のキー(Decrypt - Known Key)] アクションも選択すると、証明書条件を設定できなくなります。このアクションでは、トラフィック復号用のサーバ証明書の選択が必要であるため、トラフィックの照合はすでにこの証明書で行われていることになります。詳細については、復号アクション:さらに検査するためにトラフィックを復号(13-11 ページ)を参照してください。
- 証明書条件に外部証明書オブジェクトを設定する場合、暗号スイート条件に追加する暗号スイートまたは [復号 - 再署名(Decrypt - Resign)] アクションに関連付ける内部 CA オブジェクトのいずれかが、外部証明書の署名アルゴリズム タイプと一致する必要があります。たとえば、ルールの証明書条件で EC ベースのサーバ証明書を参照する場合は、追加する暗号スイート、または [復号 - 再署名(Decrypt - Resign)] アクションに関連付ける CA 証明書も EC ベースでなければなりません。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。詳細については、暗号スイートによる暗号化トラフィックの制御(14-26 ページ)および復号アクション:さらに検査するためにトラフィックを復号(13-11 ページ)を参照してください。

サーバ証明書に基づいて暗号化トラフィックを検査するには、次の手順を実行します。

ステップ 1　サーバ証明書に応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成(13-4 ページ)を参照してください。

ステップ 2　SSL ルール エディタで、[証明書(Certificate)] タブを選択します。

[証明書(Certificate)] タブが表示されます。

ステップ 3　[使用可能な証明書（Available Certificates）] で、追加するサーバ証明書を選択します。

- ここで外部証明書オブジェクトを作成してリストに追加するには、[使用可能な証明書（Available Certificates）] リストの上にある追加アイコン（  ）をクリックし、外部証明書オブジェクトの使用（2-48 ページ）の手順に従います。
- 追加する証明書オブジェクトおよびグループを検索するには、[使用可能な証明書（Available Certificates）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

ステップ 4　[ルールに追加（Add to Rule）] をクリックして、選択したオブジェクトを [サブジェクト証明書（Subject Certificates）] リストに追加します。

選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

証明書ステータスによる暗号化トラフィックの制御

ライセンス：任意

SSL ルールで証明書ステータス条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書のステータス（有効、失効済み、有効期限切れ、未有効化、自己署名、信頼できる CA によって署名済みなど）に応じて暗号化トラフィックの処理および検査できます。

CA が証明書を発行したか失効したかを確認するには、ルートおよび中間 CA 証明書とその関連 CRL をオブジェクトとしてアップロードする必要があります。その後で SSL ポリシーの信頼できる CA 証明書のリストに、これらの信頼できる CA のオブジェクトを追加します。

証明書ステータスの SSL ルール条件では、各ステータスの有無を基準にしたトラフィックの照合ができます。1 つのルール条件で複数のステータスを選択でき、いずれかのステータスと証明書が一致すれば、ルールとトラフィックが一致したと判定されます。

詳細については、以下を参照してください。

- 外部認証局の信頼（14-22 ページ）
- 証明書ステータスでのトラフィックの照合（14-24 ページ）

外部認証局の信頼

ライセンス：任意

SSL ポリシーでルートおよび中間 CA 証明書を追加することで信頼できる CA が設定され、トラフィックの暗号化に使用されているサーバ証明書の検証に、これらの信頼できる CA を使用できるようになります。検証されたサーバ証明書には、信頼できる CA によって署名された証明書が含まれます。

信頼できる CA 証明書の中にアップロードされた証明書失効リスト（CRL）が含まれている場合は、信頼できる CA により、暗号化証明書が失効されているかどうかも確認できます。詳細については、信頼できる CA オブジェクトへの証明書失効リストの追加（2-47 ページ）を参照してください。

SSL ポリシーに信頼できる CA 証明書を追加した後は、トラフィックと照合するさまざまな証明書ステータス条件を SSL ルールに設定することができます。詳細については、「信頼できる認証局オブジェクトの使用（2-46 ページ）」と「証明書ステータスによる暗号化トラフィックの制御（14-22 ページ）」を参照してください。

ヒント　信頼できるルート CA の信頼チェーン内にあるすべての証明書を、信頼できる CA 証明書のリストにアップロードしますが、これにはルート CA 証明書およびすべての中間 CA 証明書が含まれます。これを行わないと、中間 CA から発行された信頼できる証明書の検出が困難になります。

SSL ポリシーを作成すると、ASA FirePOWER モジュールにより、[信頼できる CA 証明書（Trusted CA Certificates）] タブにデフォルトの信頼できる CA オブジェクト グループ Cisco Trusted Authorities が入力されます。このグループ内の各エントリは変更が可能で、SSL ポリシーにこのグループを含めるかどうかを選択できます。このグループを削除することはできません。システムによる更新によりこのリストのエントリが変更されることがありますが、ユーザによる変更は保持されます。詳細については、基本 SSL ポリシーの作成（12-2 ページ）を参照してください。

ポリシーに信頼できる **CA** を追加するには、次の手順を実行します。

ステップ 1　**[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] >** [ポリシー（Policies）] > [SSL] の順に選択します。

[SSL ポリシー（SSL Policy）] ページが表示されます。

ステップ 2　設定する SSL ポリシーの横にある編集アイコン（ ）をクリックします。

SSL ポリシー エディタが表示されます。

ステップ 3　[信頼できる CA 証明書（Trusted CA Certificates）] タブを選択します。

[信頼できる CA 証明書（Trusted CA Certificates）] ページが表示されます。

ステップ 4　[使用可能な信頼できる CA（Available Trusted CAs）] で、追加する信頼できる CA を選択します。

- ここで信頼できる CA のオブジェクトを作成してリストに追加するには、[使用可能な信頼できる CA（Available Trusted CAs）] リストの上にある追加アイコン（ ）をクリックし、信頼できる認証局オブジェクトの使用（2-46 ページ）の手順に従います。
- 追加する信頼できる CA オブジェクトおよびグループを検索するには、[使用可能な信頼できる CA（Available Trusted CAs）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

ステップ 5　[ルールに追加（Add to Rule）] をクリックして、選択したオブジェクトを [選択した信頼できる CA（Selected Trusted CAs）] リストに追加します。

選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 6　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

証明書ステータスでのトラフィックの照合

ライセンス:任意

証明書ステータス ベースのルール条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書のステータスに基づいて暗号化トラフィックを照合できます。次の操作を実行できます。

- サーバ証明書のステータスをチェックする。
- 証明書にステータスがないことをチェックする。
- 証明書ステータスの有無のチェックをスキップする。

複数の証明書ステータスの有無の一致を単一の証明書ステータスのルール条件で選択することも可能ですが、ルールとの照合で証明書が一致する必要があるのは 1 つの基準だけです。

次の表は、暗号化用のサーバ証明書のステータスを基準に、ASA FirePOWER モジュールが暗号化トラフィックを評価する方法を示しています。

表 ***14-3***　証明書ステータスのルール条件の基準

ステータスの確認	**Yes** を設定	**No** を設定
失効（Revoked）	ポリシーは、サーバ証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれています。	ポリシーは、サーバ証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれていません。
自己署名（Self-signed）	検出されたサーバ証明書が、同じサブジェクトと発行元の識別名を含んでいます。	検出されたサーバ証明書が、異なるサブジェクトと発行元の識別名を含んでいます。
有効（Valid）	以下のすべてを満たしています。 • 証明書を発行した CA をポリシーが信頼しています。 • 署名が有効です。 • 発行元が有効です。 • ポリシーの信頼できる CA のいずれも証明書を失効させていません。 • 現在の日付が証明書の有効期間の開始日と終了日の範囲内にあります。	以下の 1 つ以上を満たしています。 • 証明書を発行した CA をポリシーが信頼していません。 • 署名が無効です。 • 発行元が無効です。 • ポリシーの信頼できる CA の 1 つが証明書を失効させています。 • 現在の日付が証明書の有効期間の開始日より前です。 • 現在の日付が証明書の有効期限の終了日より後です。
署名が無効（Invalid signature）	証明書の内容に対して証明書の署名が適切に検証されません。	証明書の内容に対して証明書の署名が適切に検証されます。
発行元が無効（Invalid issuer）	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されていません。	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されています。
期限切れ	現在の日付が証明書の有効期限の終了日より後です。	現在の日付が証明書の有効期限の終了日であるかそれより前です。
まだ無効（Not yet valid）	現在の日付が証明書の有効期間の開始日より前です。	現在の日付が証明書の有効期間の開始日であるかそれより後です。

次の例を考えてみます。組織は Verified Authority という認証局を信頼しています。組織は Spammer Authority という認証局を信頼していません。システム管理者は、Verified Authority の証明書、および Verified Authority の発行した中間 CA 証明書をアップロードします。Verified Authority が以前に発行した証明書の 1 つを失効させたため、システム管理者は Verified Authority から配布された CRL をアップロードします。

次の図は、有効な証明書をチェックする証明書ステータスのルール条件を示しています。これにより、Verified Authority から発行されたが CRL には登録されておらず、現状で有効期間の開始日と終了日の範囲内にあるかどうかがチェックされます。この設定では、これらの証明書で暗号化されたトラフィックはアクセス コントロールにより復号および検査されません。

次の図は、ステータスが存在しないことをチェックする証明書ステータスのルール条件を示しています。この設定では、期限切れになっていない証明書を使用して暗号化されたトラフィックと照合し、そのトラフィックをモニタします。

次の図は、さまざまなステータスの有無に一致する証明書ステータスのルール条件を示しています。この設定でルールが一致するのは、着信トラフィックを暗号化した証明書が無効なユーザが発行元、自己署名、無効、または期限切れであった場合で、そうしたトラフィックを既知のキーで復号します。

1 つの証明書が複数のステータスに一致する場合でも、ルールがトラフィックに行うアクションは一度に 1 つだけであることに注意してください。

サーバ証明書のステータスで暗号化トラフィックを検査するには、次の手順を実行します。

ステップ 1　サーバ証明書のステータスに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（13-4 ページ）を参照してください。

ステップ 2　SSL ルール エディタで、[証明書のステータス（Cert Status）] タブを選択します。

[証明書のステータス（Cert Status）] タブが表示されます。

ステップ 3　各証明書ステータスには次のオプションがあります。

- 該当する証明書ステータスが存在するときに照合する場合は、[はい（Yes）] を選択します。
- 該当する証明書ステータスが存在しないときに照合する場合は、[いいえ（No）] を選択します。
- 該当する証明書ステータスを照合しない場合は [照合しない（Do Not Match）] を選択します。

ステップ 4　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

暗号スイートによる暗号化トラフィックの制御

ライセンス：任意

SSL ルールで暗号スイート条件を設定すると、暗号化セッションのネゴシエートに使用される暗号スイートに応じて暗号化トラフィックを処理および検査できます。暗号スイートのルール条件に追加できる、シスコ定義の暗号スイートが提供されています。複数の暗号スイートを含む、暗号スイートのリストのオブジェクトを追加することもできます。暗号スイートのリストの詳細については、位置情報オブジェクトの操作（2-50 ページ）を参照してください。

（注）　新しい暗号スイートを追加することはできません。定義済みの暗号スイートは変更も削除もできません。

1 つの暗号スイート条件で、[選択した暗号スイート（Selected Cipher Suites）] リストに最大 50 の暗号スイートおよび暗号スイート リストを追加できます。

次の点に注意してください。

- 展開でサポートされていない暗号スイートを追加した場合、その SSL ポリシーに関連付けられたアクセス コントロール ポリシーを適用することはできません。たとえば、パッシブ展開では、一時 Diffie-Hellman（DHE）および一時的楕円曲線 Diffie-Hellman（ECDHE）暗号スイートを使用したトラフィックの復号がサポートされません。これらの暗号スイートでルールを作成した場合、アクセス コントロール ポリシーは適用できません。

- 暗号スイート条件に暗号スイートを設定する場合は、証明書条件に追加する外部証明書オブジェクト、または [復号 - 再署名（Decrypt - Resign）] アクションに関連付ける内部 CA オブジェクトが、暗号スイートの署名アルゴリズム タイプと一致している必要があります。たとえば、ルールの暗号スイート条件で EC ベースの暗号スイートを参照する場合は、追加するサーバ証明書、または [復号 - 再署名（Decrypt - Resign）] アクションに関連付ける CA 証明書も EC ベースでなければなりません。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。詳細については、暗号スイートによる暗号化トラフィックの制御（14-26 ページ）および復号アクション: さらに検査するためにトラフィックを復号（13-11 ページ）を参照してください。
- ASA FirePOWER モジュールでは、匿名の暗号スイートで暗号化されたトラフィックは復号できません。匿名の暗号スイートを **Cipher Suite** 条件に追加した場合、SSL ルールに [復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Decrypt - Known Key）] アクションを使用できません。

暗号化トラフィックを暗号スイートで検査するには、次の手順を実行します。

ステップ **1**　暗号スイートに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（13-4 ページ）を参照してください。

ステップ **2**　SSL ルール エディタで、[暗号スイート（Cipher Suite）] タブを選択します。

[暗号スイート（Cipher Suite）] タブが表示されます。

ステップ **3**　[使用可能な暗号スイート（Available Cipher Suites）] で、追加する暗号スイートを選択します。

- ここで暗号スイート リストを作成してリストに追加するには、[使用可能な暗号スイート（Available Cipher Suites）] リストの上にある追加アイコン（ ）をクリックし、位置情報オブジェクトの操作（2-50 ページ）の手順に従います。
- 追加する暗号スイートおよびリストを検索するには、[使用可能な暗号スイート（Available Cipher Suites）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、暗号スイートの名前または暗号スイートの値を入力します。入力を開始するとリストが更新され、一致する暗号スイートが表示されます。

暗号スイートをクリックして選択します。複数の暗号スイートを選択するには、Shift キーまたは Ctrl キーを使用します。すべての暗号スイートを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ **4**　[ルールに追加（Add to Rule）] をクリックして、選択した暗号スイートを [選択した暗号スイート（Selected Cipher Suites）] リストに追加します。

選択した暗号スイートをドラッグ アンド ドロップでリストに追加することもできます。

ステップ **5**　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

暗号化プロトコルのバージョンによるトラフィックの制御

ライセンス：任意

SSL ルールでセッション条件を設定すると、トラフィックの暗号化に使用されている SSL または TLS のバージョンに応じて暗号化トラフィックを検査できます。SSL バージョン 3.0 または TLS バージョン 1.0、1.1、1.2 のいずれかで暗号化されたトラフィックとの照合を選択できます。デフォルトでは、ルールの作成時にすべてのプロトコルのバージョンが選択されます。複数のバージョンが選択されている場合、いずれかのバージョンと一致する暗号化トラフィックがルールに一致したと判定されます。ルール条件を保存するには、最低 1 つのプロトコル バージョンを選択する必要があります。

（注）　バージョンのルール条件で SSL バージョン 2.0 を選択することはできません。これは、ASA FirePOWER モジュールが SSL バージョン 2.0 で暗号化されたトラフィックの復号をサポートしていないためです。復号できないアクションを設定すれば、それ以上のインスペクションなしで、これらのトラフィックを許可またはブロックできます。詳細については、SSL ルールによる復号可能接続のロギング（33-15 ページ）を参照してください。

暗号化トラフィックを **SSL** または **TLS** のバージョンで検査するには、次の手順を実行します。

ステップ **1**　暗号化プロトコルのバージョンに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（13-4 ページ）を参照してください。

ステップ **2**　SSL ルール エディタで、[バージョン（Version）] タブを選択します。

[バージョン（Version）] タブが表示されます。

ステップ **3**　照合するプロトコル バージョンを選択します。**SSL v3.0**、**TLS v1.0**、**TLS v1.1**、または **TLS v1.2** を選択できます。

ステップ **4**　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス 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（4-12 ページ）を参照してください）。

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

ネットワーク分析ポリシーと侵入ポリシーは、ASA FirePOWER モジュール 侵入検知および防御の機能の一部として連携して動作します。侵入検知という用語は、一般に、ネットワーク トラフィックへの侵入の可能性を受動的に分析し、セキュリティ分析用に攻撃データを保存するプロセスを指します。侵入防御という用語には、侵入検知の概念が含まれますが、さらにネットワークを通過中の悪意のあるトラフィックをブロックしたり変更したりする機能も追加されます。

侵入防御の展開では、システムがパケットを検査するときに次のことが行われます。

- ネットワーク分析ポリシーは、特に侵入の試みの前兆を示している可能性がある異常トラフィックに対し、そのトラフィックがさらに評価されるようにトラフィックを復号化および前処理する方法を制御します。
- 侵入ポリシーでは侵入およびプリプロセッサ ルール（総称的に「侵入ルール」とも呼ばれる）を使用し、パターンに基づき、デコードされたパケットを検査して攻撃の可能性を調べます。侵入ポリシーは変数セットとペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映することができます。

ネットワーク分析ポリシーと侵入ポリシーは、どちらも親のアクセス コントロール ポリシーによって呼び出されますが、呼び出されるタイミングが異なります。システムでトラフィックが分析される際には、侵入防御（追加の前処理と侵入ルール）フェーズよりも前に、別途ネットワーク分析（デコードと前処理）フェーズが実行されます。ネットワーク分析ポリシーと侵入ポリシーを一緒に使用すると、広範囲で詳細なパケット インスペクションを行うことができます。このポリシーは、ホストとそのデータの可用性、整合性、機密性を脅かす可能性のあるネットワーク トラフィックの検知、通知および防御に役立ちます。

ASA FirePOWER モジュール には、同様の名前（Balanced Security and Connectivity など）が付いた複数のネットワーク分析ポリシーと侵入ポリシーが付属しており、それらは相互に補完して連携します。システム付属のポリシーを使用することで、シスコ脆弱性調査チーム（VRT）の経験を活用できます。これらのポリシーでは、VRT は侵入ルールおよびプリプロセッサ ルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。

また、カスタムのネットワーク分析ポリシーや侵入ポリシーも作成できます。最も有効な方法でトラフィックを検査するようにカスタム ポリシーの設定を調整できます。同様のポリシーエディタを使用し、ネットワーク分析ポリシーや侵入ポリシーを作成、編集、保存、管理します。いずれかのタイプのポリシーを編集するときには、ユーザ インターフェイスの左側にナビゲーション パネルが表示され、右側にさまざまな設定ページが表示されます。

この章では、ネットワーク分析ポリシーおよび侵入ポリシーによって管理される各種設定の概要、ポリシーが連携してトラフィックを検査し、ポリシー違反のレコードを生成するしくみ、および、ポリシー エディタの基本的な操作方法について説明します。また、カスタム ポリシーとシステム付属のポリシーを比較して、それらの使用上の利点と制約についても説明します。詳細については、次の項を参照してください。

- ポリシーが侵入についてトラフィックを検査する仕組み（15-2 ページ）
- システム付属ポリシーとカスタム ポリシーの比較（15-7 ページ）
- ナビゲーション パネルの使用（15-14 ページ）
- 競合の解決とポリシー変更の確定（15-15 ページ）

侵入展開をカスタマイズするには、次の手順について以下を参照してください。

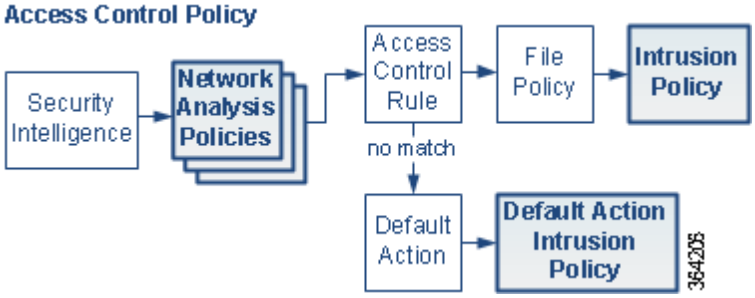
- 変数セットの使用（2-15 ページ）には、ネットワーク環境を正確に反映させるためのシステムの侵入変数の設定方法が記載されています。カスタム ポリシーを使用しない場合でも、シスコでは、デフォルトの変数セットのデフォルト変数を変更することを強く推奨しています。高度なユーザは、1 つ以上のカスタム侵入ポリシーとペアリングするために、カスタム変数セットを作成して使用できます。
- 侵入ポリシーを使用する前に（23-1 ページ）では、単純なカスタム侵入ポリシーを作成および編集する方法について説明します。
- 侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（10-1 ページ）には、親アクセス コントロール ポリシーに侵入ポリシーを関連付け、侵入ポリシーを使用して目的のトラフィックのみを検査するためのシステムの設定方法が記載されています。また、侵入ポリシー パフォーマンスの詳細オプションを設定する方法についても説明します。
- トランスポート/ネットワークの詳細設定の構成（21-1 ページ）には、すべてのトラフィックにグローバルに適用される、トランスポートとネットワーク プリプロセッサの詳細な設定方法が記載されています。これらの詳細設定は、ネットワーク分析ポリシーまたは侵入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。
- ネットワーク分析ポリシーの開始（18-1 ページ）では、単純なカスタム ネットワーク分析ポリシーを作成および編集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による前処理のカスタマイズ（17-3 ページ）には、デフォルトのネットワーク分析ポリシーの変更方法が記載されています。また、上級ユーザ向けに前処理の調整方法も記載されています。一致したトラフィックの前処理にカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーンやネットワークに合わせて前処理を調整できます。
- ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）では、大規模な組織または複雑な展開環境で、ポリシー階層と呼ばれるビルディング ブロックを使用して、複数のネットワーク分析ポリシーまたは侵入ポリシーをより効率的に管理する方法について説明します。

ポリシーが侵入についてトラフィックを検査する仕組み

ライセンス：Protection

アクセス コントロールの展開の一部としてシステムがトラフィックを分析すると、ネットワーク分析（復号化と前処理）フェーズが侵入防御（侵入ルールおよび詳細設定）フェーズとは別にその前に実行されます。

次の図は、侵入防御および高度なマルウェア防御（AMP）のインライン展開におけるトラフィック分析の順序を簡略化して示しています。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てトラフィックを検査するしくみ、およびそれらのポリシーが呼び出される順序が示されています。ネットワーク分析ポリシーおよび侵入ポリシーの選択フェーズが強調表示されています。



インライン展開では、図に示したプロセスのほぼすべてのステップで、システムは追加のインスペクションなしでトラフィックをブロックできます。セキュリティ インテリジェンス、ネットワーク分析ポリシー、ファイル ポリシー、および侵入ポリシーのすべてで、トラフィックをドロップまたは変更できます。

同様に、プロセスの各ステップで、パケットによってシステムがイベントを生成する場合があります。侵入イベントおよびプリプロセッサ イベント（まとめて侵入イベントと呼ばれることもあります）は、パケットまたはその内容がセキュリティ リスクを表す可能性があることを示すものです。

単一の接続の場合は、図に示すように、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、一部の前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定には影響しません。

詳細については、以下を参照してください。

- デコード、正規化、前処理：ネットワーク分析ポリシー（15-3 ページ）
- アクセス コントロール ルール：侵入ポリシーの選択（15-5 ページ）
- 侵入インスペクション：侵入ポリシー、ルール、変数セット（15-5 ページ）
- 侵入イベントの生成（15-7 ページ）

デコード、正規化、前処理：ネットワーク分析ポリシー

ライセンス：Protection

デコードと前処理を実行しないと、プロトコルの相違によりパターン マッチングを行えなくなるので、侵入についてトラフィックを適切に評価できません。ポリシーが侵入についてトラフィックを検査する仕組み（15-2 ページ）の図に示すように、ネットワーク分析ポリシーは、次の時点でこれらのトラフィック処理タスクを制御します。

- 暗号化トラフィックがセキュリティ インテリジェンスによってフィルタリングされた後
- ファイルポリシーまたは侵入ポリシーによってトラフィックを検査できるようになる前

ネットワーク分析ポリシーは、フェーズでのパケット処理を制御します。最初に、システムは最初の 3 つの TCP/IP 層を通ったパケットを復号化し、次にプロトコル異常の正規化、前処理、および検出に進みます。

- パケット デコーダは、パケット ヘッダーとペイロードを、プリプロセッサや以降の侵入ルールで簡単に使用できる形式に変換します。TCP/IP スタックの各レイヤのデコードは、データリンク層から開始され、ネットワーク層、トランスポート層へと順番に行われます。パケット デコーダは、パケット ヘッダーのさまざまな異常動作も検出します。詳細については、パケットのデコードについて（21-17 ページ）を参照してください。
- インライン展開では、インライン正規化プリプロセッサは、攻撃者が検出を免れる可能性を最小限にするために、トラフィックを再フォーマット（正規化）します。その他のプリプロセッサや侵入ルールによる検査用にパケットを準備し、システムで処理されるパケットがネットワーク上のホストで受信されるパケットと同じものになるようにします。詳細については、インライン トラフィックの正規化（21-6 ページ）を参照してください。
- さまざまなネットワーク層およびトランスポート層のプリプロセッサは、IP フラグメントを悪用する攻撃を検出し、チェックサム検証、TCP および UDP セッションの前処理を実行します。トランスポート層およびネットワーク層の前処理の設定（21-1 ページ）を参照してください。

  トランスポートおよびネットワーク プリプロセッサの一部の詳細設定は、アクセス コントロール ポリシーで処理されるすべてのトラフィック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。トランスポート/ネットワークの詳細設定の構成（21-1 ページ）を参照してください。
- 各種のアプリケーション層プロトコル デコーダは、特定タイプのパケット データを侵入ルール エンジンで分析可能な形式に正規化します。アプリケーション層プロトコルのエンコードを正規化することにより、システムはデータ表現が異なるパケットに同じコンテンツ関連の侵入ルールを効果的に適用し、大きな結果を得ることができます。詳細については、アプリケーション層プリプロセッサの使用（19-1 ページ）を参照してください。
- Modbus と DNP3 SCADA のプリプロセッサは、トラフィックの異常を検出し、データを侵入ルールに提供します。Supervisory Control and Data Acquisition（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャ プロセス、および設備プロセスからのデータをモニタ、制御、取得します。詳細については、SCADA の前処理の設定（20-1 ページ）を参照してください。
- 一部のプリプロセッサでは、Back Orifice、ポートスキャン、SYN フラッドおよび他のレートベース攻撃など、特定の脅威を検出できます。特定の脅威の検出（25-1 ページ）を参照してください。

  侵入ポリシーで、ASCII テキストのクレジット カード番号や社会保障番号などのセンシティブ データを検出するセンシティブ データ プリプロセッサを設定することに注意してください。センシティブ データの検出（25-21 ページ）を参照してください。

新たに作成されたアクセス コントロール ポリシーでは、1 つのデフォルト ネットワーク分析ポリシーが、同じ親アクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシー向けのすべてのトラフィックの前処理を制御します。初期段階では、デフォルトで Balanced Security and Connectivity ネットワーク分析ポリシーが使用されますが、別のシステム付属ポリシーやカスタム ネットワーク分析ポリシーに変更できます。より複雑な展開では、上級ユーザは、一致したトラフィックの前処理にさまざまなカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーンやネットワークに合わせてトラフィックの前処理オプションを調整できます。詳細については、システム付属ポリシーとカスタム ポリシーの比較（15-7 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:侵入ポリシーの選択

ライセンス:Protection

最初の前処理の後、トラフィックはアクセス コントロール ルール(設定されている場合)によって評価されます。ほとんどの場合、パケットが一致する最初のアクセス コントロール ルールがそのトラフィックを処理するルールとなります。一致するトラフィックをモニタ、信頼、ブロック、または許可できます。

アクセス コントロール ルールでトラフィックを許可した場合は、マルウェア、禁止ファイル、侵入について、この順序でトラフィックを検査できます。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はアクセス コントロール ポリシーのデフォルト アクションによって処理され、侵入の有無についても検査されます。

(注)　どのネットワーク分析ポリシーによって前処理されるかに関わらず、すべてのパケットは、設定されているアクセス コントロール ルールと上から順に照合されます(したがって、侵入ポリシーによる検査の対象となります)。詳細については、カスタム ポリシーに関する制約事項(15-12 ページ)を参照してください。

ポリシーが侵入についてトラフィックを検査する仕組み(15-2 ページ)の図では、次のように、インラインの侵入防御と AMP の展開で、デバイスを経由したトラフィックのフローを示しています。

- アクセス コントロール ルールは、一致したトラフィックが次のステップに進むことを許可します。次に、トラフィックは、ファイル ポリシーによって禁止ファイルとマルウェアの有無を検査され、その後侵入ポリシーによって侵入の有無を検査されます。
- このシナリオでは、アクセス コントロール ポリシーのデフォルト アクションで、一致したトラフィックを許可しています。次に、トラフィックは侵入ポリシーによって検査されます。アクセス コントロール ルールまたはデフォルトのアクションに侵入ポリシーを関連付けるときは、異なる侵入ポリシーを使用できます(ただし必須ではありません)。

ブロックされたトラフィックや信頼済みトラフィックは検査されないので、図の例には、ブロック ルールや信頼ルールは含まれていません。詳細については、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(6-7 ページ)およびデフォルト処理の設定およびネットワーク トラフィックのインスペクション(4-5 ページ)を参照してください。

侵入インスペクション:侵入ポリシー、ルール、変数セット

ライセンス:Protection

トラフィックが宛先に向かうことを許可する前に、システムの最終防御ラインとして侵入防御を使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーの主な機能は、どの侵入ルールおよびプリプロセッサ ルールを有効にしてどのように設定するかを管理することです。

侵入ルールおよびプリプロセッサ ルール

侵入ルールはキーワードと引数のセットとして指定され、ネットワーク上の脆弱性を悪用する試みを検出します。システムは侵入ルールを使用してネットワーク トラフィックを分析し、トラフィックがルールの条件に合致しているかどうかをチェックします。システムは各ルールで指定された条件をパケットに照らし合わせます。ルールで指定されたすべての条件にパケット データが一致する場合、ルールがトリガーされます。

システムには、VRT によって作成された次のタイプのルールが含まれています。

- 共有オブジェクト侵入ルール：コンパイルされており、変更できません（ただし、送信元と宛先のポートや IP アドレスなどのルール ヘッダー情報を除く）
- 標準テキスト侵入ルール：ルールの新しいカスタム インスタンスとして保存および変更できます。
- プリプロセッサ ルール：ネットワーク分析ポリシーのプリプロセッサおよびパケット デコーダ検出オプションに関連付けられています。プリプロセッサ ルールはコピーまたは編集できません。ほとんどのプリプロセッサ ルールはデフォルトで無効になっています。イベントを生成し、インライン展開で、違反パケットをドロップするためにプリプロセッサを使用するには、ルールを有効にする必要があります。

システムで侵入ポリシーに従ってパケットを処理する際には、最初にルール オプティマイザが、基準（トランスポート層、アプリケーション プロトコル、保護されたネットワークへの入出力方向など）に基づいて、サブセット内のすべてのアクティブなルールを分類します。次に、侵入ルール エンジンが、各パケットに適用する適切なルールのサブセットを選択します。最後に、マルチルール検索エンジンが 3 種類の検索を実行して、トラフィックがルールに一致するかどうかを検査します。

- プロトコル フィールド検索は、アプリケーション プロトコル内の特定のフィールドでの一致を検索します。
- 汎用コンテンツ検索は、パケット ペイロードの ASCII またはバイナリ バイトでの一致を検索します。
- パケット異常検索では、特定のコンテンツが含まれているかどうかではなく、確立されたプロトコルに違反しているパケット ヘッダーやペイロードが検索されます。

カスタム侵入ポリシーでは、ルールを有効化および無効化し、独自の標準テキスト ルールを記述および追加することで、検出を調整できます。

変数セット

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セット使用します。セット内の大部分の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスとポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

システムには、定義済みのデフォルト変数から構成される 1 つのデフォルト変数セットが含まれています。大部分のシステム付属の共有オブジェクトのルールと標準テキスト ルールは、定義済みのデフォルト変数を使用して、ネットワークおよびポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 `$HOME_NET` を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 `$EXTERNAL_NET` を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Web サーバに対するエクスプロイトを検出するルールは、`$HTTP_SERVERS` 変数および `$HTTP_PORTS` 変数を使用します。

ヒント　システム付属の侵入ポリシーを使用する場合でも、シスコでは、デフォルトセットの主要なデフォルト変数を変更すること強く推奨します。ネットワーク環境を正確に反映する変数を使用すると、処理が最適化され、システムによって疑わしいアクティビティに関連するシステムをモニタできます。高度なユーザは、1 つ以上のカスタム侵入ポリシーとペアリングするために、カスタム変数セットを作成して使用できます。詳細については、定義済みのデフォルトの変数の最適化（2-16 ページ）を参照してください。

侵入イベントの生成

ライセンス：Protection

侵入されている可能性を特定すると、システムは侵入イベントまたはプリプロセッサ イベント（総称的に「侵入イベント」とも呼ばれる）を生成します。データを確認して、ネットワーク アセットに対する攻撃を的確に把握できます。インライン展開では、システムは、有害であると判明しているパケットをドロップまたは置き換えることがきます。

各侵入イベントにはイベント ヘッダーがあり、イベント名と分類、送信元と宛先の IP アドレス、ポート、イベントを生成したプロセス、およびイベントの日時に関する情報、さらに攻撃の送信元とそのターゲットに関するコンテキスト情報が含まれています。パケットベースのイベントの場合は、イベントをトリガーしたパケットのデコードされたパケット ヘッダーとペイロードのコピーも記録されます。

パケット デコーダ、プリプロセッサ、および侵入ルール エンジンはすべて、システムによるイベントの生成を引き起こします。次に例を示します。

- （ネットワーク分析ポリシーで設定された）パケット デコーダが 20 バイト（オプションやペイロードのない IP データグラムのサイズ）未満の IP パケットを受け取った場合、デコーダはこれを異常なトラフィックと解釈します。パケットを検査する侵入ポリシー内の付随するデコーダ ルールが有効な場合、システムは後でプリプロセッサ イベントを生成します。
- IP 最適化プリプロセッサが重複する一連の IP フラグメントを検出した場合、プリプロセッサはこれを潜在的な攻撃と解釈して、付随するプリプロセッサ ルールが有効な場合、システムはプリプロセッサ イベントを生成します。
- 侵入ルール エンジン内では、ほとんどの 標準テキスト ルール および 共有オブジェクトのルール はパケットによってトリガーされた場合に侵入イベントを生成するように記述されます。

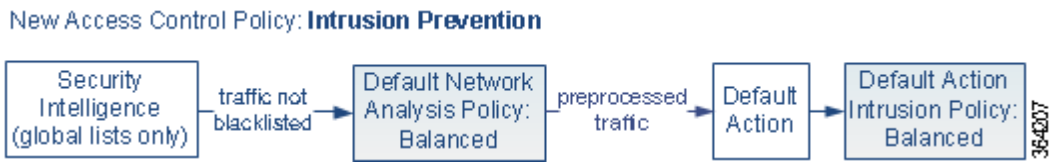
デバイスに侵入イベントが蓄積されると、ユーザは攻撃の可能性について分析を開始できます。システムは、ユーザが侵入イベントを確認し、ネットワーク環境とセキュリティ ポリシーのコンテキストでそのイベントが重要であるかどうかを評価するために必要なツールを提供します。

システム付属ポリシーとカスタム ポリシーの比較

ライセンス：Protection

新しいアクセス コントロール ポリシーを作成することは、ASA FirePOWER モジュール を使用してトラフィック フローを管理する最初のステップの 1 つです。デフォルトでは、新しく作成されたアクセス コントロール ポリシーは、システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーを呼び出してトラフィックを検査します。

次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理および侵入防御のフェーズが強調表示されています。



以下の点に注意してください。

- デフォルトのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が制御されます。初期段階では、システムによって提供される *Balanced Security and Connectivity* ネットワーク分析ポリシーがデフォルトです。
- アクセス コントロール ポリシーのデフォルト アクションがシステムによって提供される *Balanced Security and Connectivity* 侵入ポリシーで指定された通りに悪意のないすべてのトラフィックを許可する。
- ポリシーがデフォルトのセキュリティ インテリジェンス オプション（グローバルのホワイトリストおよびブラックリストのみ）で暗号化されたトラフィックを復号化せず、アクセス コントロール ルールを使用してネットワーク トラフィックの特別な処理およびインスペクションを実行しない。

侵入防御展開を調整するために実行できるシンプルなステップは、システム付属のネットワーク分析ポリシーと侵入ポリシーの別のセットをデフォルトとして使用することです。シスコでは、ASA FirePOWER モジュール とともにこれらのポリシーを提供しています。

または、カスタム ポリシーを作成して使用することで、侵入防御展開を調整できます。それらのポリシーに設定されているプリプロセッサ オプション、侵入ルール、およびその他の詳細設定が、ネットワークのセキュリティ ニーズに適合しない場合があります。設定できるネットワーク分析ポリシーおよび侵入ポリシーを調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

詳細については、以下を参照してください。

- システム付属のポリシーについて（15-8 ページ）
- カスタム ポリシーの利点（15-9 ページ）
- カスタム ポリシーに関する制約事項（15-12 ページ）

システム付属のポリシーについて

ライセンス：Protection

シスコ は、ネットワーク分析ポリシーおよび侵入ポリシーの複数のペアを ASA FirePOWER モジュール とともに提供します。システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーを使用して、シスコ 脆弱性調査チーム（VRT）のエクスペリエンスを活用することができます。これらのポリシーでは、VRT は侵入ルールおよびプリプロセッサ ルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。システムによって提供されるポリシーをそのまま使用するか、またはカスタム ポリシーのベースとして使用できます。

ヒント　システム付属のネットワーク分析ポリシーと侵入ポリシーを使用する場合でも、ネットワーク環境が正確に反映されるように、システムの侵入変数を設定する必要があります。少なくとも、デフォルトのセットにある主要なデフォルトの変数を変更します。定義済みのデフォルトの変数の最適化（2-16 ページ） を参照してください。

新たな脆弱性が発見されると、VRT は侵入ルールの更新をリリースします。これらのルール更新により、システム付属のネットワーク分析ポリシーや侵入ポリシーが変更され、侵入ルールやプリプロセッサ ルールの新規作成または更新、既存ルールのステータスの変更、デフォルトのポリシー設定の変更が実施されます。ルールの更新では、システムによって提供されるポリシーからのルールが削除されたり、新しいルール カテゴリの提供やデフォルトの変数セットの変更が行われることがあります。

ルール更新によって展開が影響を受けると、システムは、影響を受けた侵入ポリシーやネットワーク分析ポリシー、およびそれらの親のアクセス コントロール ポリシーを失効として扱います。変更を有効にするには、更新されたポリシーを再適用する必要があります。

必要に応じて、影響を受けた侵入ポリシーを（単独で、または影響を受けたアクセス コントロール ポリシーと組み合わせて）自動的に再適用するように、ルールの更新を設定できます。これにより、新たに検出されたエクスプロイトおよび侵入から保護するために展開環境を容易に自動的に最新に維持することができます。

前処理の設定を最新の状態に保つには、アクセス コントロール ポリシーを再適用する必要があります。これにより、現在実行されているものとは異なる、関連するネットワーク分析ポリシー、ファイル ポリシーが再適用され、前処理とパフォーマンスの詳細設定オプションのデフォルト値も更新できるようになります。詳細については、ルールの更新とローカル ルール ファイルのインポート（43-10 ページ）を参照してください。

シスコでは、次のネットワーク分析ポリシーと侵入ポリシーを ASA FirePOWER モジュール とともに提供しています。

Balanced Security and Connectivity ネットワーク分析ポリシーと侵入ポリシー

これらのポリシーは、速度と検出の両方を目的として作成されています。これらを一緒に使用することは、ほとんどの組織にとって最適な出発点となります。ほとんどの場合、システムは Balanced Security and Connectivity のポリシーおよび設定をデフォルトとして使用します。

Connectivity Over Security ネットワーク分析ポリシーと侵入ポリシー

これらのポリシーは、（すべてのリソースに到達可能な）接続がネットワーク インフラストラクチャのセキュリティよりも優先される組織向けに作成されています。この侵入ポリシーは、Security over Connectivity ポリシー内で有効になっているルールよりもはるかに少ないルールを有効にします。トラフィックをブロックする最も重要なルールだけが有効にされます。

Security over Connectivity ネットワーク分析ポリシーと侵入ポリシー

これらのポリシーは、ネットワーク インフラストラクチャのセキュリティがユーザの利便性よりも優先される組織向けに作られています。この侵入ポリシーは、正式なトラフィックに対して警告またはドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。

No Rules Active 侵入ポリシー

No Rules Active 侵入ポリシーでは、すべての侵入ルールと詳細設定が無効化されます。このポリシーは、他のシステムによって提供されるポリシーのいずれかで有効になっているルールをベースにするのではなく、独自の侵入ポリシーを作成する場合の出発点を提供します。

注意　シスコでは、試験用に別のポリシー Experimental Policy 1 を使用しています。シスコ の担当者から指示された場合を除き、このポリシーを使用しないでください。

カスタム ポリシーの利点

ライセンス：Protection

システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーに設定されたプリプロセッサ オプション、侵入ルール、およびその他の詳細設定は、組織のセキュリティ ニーズに十分に対応しない場合があります。

カスタム侵入ポリシーを作成すると、環境内のシステムのパフォーマンスを向上させ、ネットワークで発生する悪意のあるトラフィックやポリシー違反を重点的に観察できるようになります。設定できるカスタム ポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

すべてのカスタム ポリシーには基本ポリシー（別名「基本レイヤ」）があり、それによって、ポリシー内のすべてのコンフィギュレーションのデフォルト設定が定義されます。レイヤは、複数のネットワーク分析ポリシーまたは侵入ポリシーを効率的に管理するために使用できるビルディング ブロックです。ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ほとんどの場合、カスタム ポリシーはシステム付属のポリシーに基づきますが、別のカスタム ポリシーを使用することもできます。ただし、すべてのカスタム ポリシーには、ポリシー チェーンの根本的な基礎としてシステム付属ポリシーが含まれています。システム付属のポリシーはルールの更新によって変更される可能性があるので、カスタム ポリシーを基本として使用している場合でも、ルールの更新をインポートするとポリシーに影響が及びます。ルールの更新によってポリシーが影響を受けると、モジュール インターフェイスは影響を受けたポリシーを失効として扱います。詳細については、ルール更新がシステムによって提供される基本ポリシーを変更することを許可する（16-4 ページ）を参照してください。

詳細については、以下を参照してください。

- カスタム ネットワーク分析ポリシーの利点（15-10 ページ）
- カスタム侵入ポリシーの利点（15-11 ページ）

カスタム ネットワーク分析ポリシーの利点

ライセンス：Protection

デフォルトでは、アクセス コントロール ポリシーで処理されるすべてのトラフィックが、1 つのネットワーク分析ポリシーによって前処理されます。これは、後でパケットを検査する侵入ポリシー（および侵入ルール セット）に関係なく、すべてのパケットが同じ設定に基づいて復号化および前処理されることを意味します。

初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。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（17-4 ページ）を参照してください。

使用可能な調整オプションはプリプロセッサによって異なりますが、プリプロセッサおよびデコーダを調整できる方法には次のものがあります。

- モニタしているトラフィックに適用されないプリプロセッサを無効にできます。たとえば、HTTP Inspect プリプロセッサは HTTP トラフィックを正規化します。ネットワークに Microsoft Internet Information Services（IIS）を使用する Web サーバが含まれていないことが確実な場合は、IIS 特有のトラフィックを検出するプリプロセッサ オプションを無効にすることで、システム処理のオーバーヘッドを軽減できます。

  （注）　カスタム ネットワーク分析ポリシーでプリプロセッサが無効化されているときに、パケットを有効な侵入ルールまたはプリプロセッサ ルールと照合して評価するために、プリプロセッサを使用する必要がある場合、システムはプリプロセッサを有効化して使用します。ただし、ネットワーク分析ポリシーのユーザ インターフェイスではプリプロセッサは無効なままになります。

- 必要に応じて、特定のプリプロセッサのアクティビティを集中させるポートを指定します。たとえば、DNS サーバの応答をモニタするための追加ポートを特定できます。

複雑な環境での高度なユーザの場合は、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを別々に前処理するように調整することができます。そして、異なるセキュリティ ゾーンまたはネットワークを使用したトラフィックの前処理を制御するためにそれらのポリシーを使用するようにシステムを設定できます。

（注）　カスタム ネットワーク分析ポリシー（特に複数のネットワーク分析ポリシー）を使用して前処理を調整することは、高度なタスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一のパケットを検査するネットワーク分析ポリシーと侵入ポリシーが相互補完することを許可する場合は、注意する必要があります。詳細については、カスタム ポリシーに関する制約事項（15-12 ページ）を参照してください。

カスタム侵入ポリシーの利点

ライセンス：Protection

侵入防御を実行するように初期設定して、新規にアクセス コントロール ポリシーを作成した場合、そのポリシーでは、デフォルト アクションはすべてのトラフィックを許可しますが、最初にシステム付属の Balanced Security and Connectivity 侵入ポリシーでトラフィックをチェックします。アクセス コントロール ルールを追加するか、またはデフォルト アクションを変更しない限り、すべてのトラフィックがその侵入ポリシーによって検査されます。システム付属ポリシーとカスタム ポリシーの比較（15-7 ページ）の図を参照してください。

侵入防御展開をカスタマイズするために、複数の侵入ポリシーを作成し、それぞれがトラフィックを異なる方法で検査するように調整できます。次に、どのポリシーがどのトラフィックを検査するかを指定するルールを、アクセス コントロール ポリシーに設定します。アクセス コントロール ルールは単純でも複雑でもかまいません。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、ユーザなど、複数の基準を使用してトラフィックを照合および検査します。ポリシーが侵入についてトラフィックを検査する仕組み（15-2 ページ）のシナリオでは、トラフィックが 2 つの侵入ポリシーのいずれかによって検査される展開を示しています。

侵入ポリシーの主な機能は、次のように、どの侵入ルールおよびプリプロセッサ ルールを有効にしてどのように設定するかを管理することです。

- 各侵入ポリシーで、環境に適用されるすべてのルールが有効になっていることを確認し、環境に適用されないルールを無効化することによって、パフォーマンスを向上させます。インライン展開では、どのルールによって悪質なパケットをドロップまたは変更するかを指定できます。詳細については、ルール状態の設定（24-21 ページ）を参照してください。
- 新しいエクスプロイトを検出したりセキュリティ ポリシーを適用するように、既存のルールを変更し、必要に応じて新しい 標準テキスト ルール を記述することができます。侵入ルールの概要と作成（27-1 ページ）を参照してください。

侵入ポリシーに対して行えるその他のカスタマイズは次のとおりです。

- 機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。特定の脅威（Back Orifice 攻撃、何種類かのポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃）を検出するプリプロセッサは、ネットワーク分析ポリシーで設定します。詳細については、特定の脅威の検出（25-1 ページ）を参照してください。
- グローバルしきい値を設定すると、侵入ルールに一致するトラフィックが、指定期間内に特定のアドレスまたはアドレス範囲で送受信される回数に基づいて、イベントが生成されます。これにより、大量のイベントによってシステムに過剰な負荷がかかることを回避できます。詳細については、侵入イベント ロギングのグローバルな制限（26-1 ページ）を参照してください。
- また、個々のルールまたは侵入ポリシー全体に対して、侵入イベント通知を抑制し、しきい値を設定することで、大量のイベントによってシステムに過剰な負荷がかかることを回避することもできます。詳細については、ポリシー単位の侵入イベント通知のフィルタリング（24-23 ページ）を参照してください。

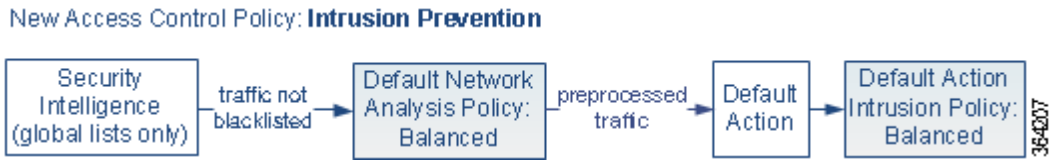
- 侵入イベントに加えて、syslog ファシリティへのロギングを有効にしたり、イベント データを SNMP トラップ サーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。詳細については、侵入ルールの外部アラートの設定（36-1 ページ）を参照してください。

カスタム ポリシーに関する制約事項

ライセンス：Protection

前処理および侵入インスペクションは密接に関連しているため、単一パケットを処理して検査するネットワーク分析ポリシーと侵入ポリシーが互いに補完することを許可する設定を行う場合は慎重になる必要があります。

デフォルトでは、システムは 1 つのネットワーク分析ポリシーを使用して、すべてのトラフィックを前処理します。次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理および侵入防御のフェーズが強調表示されています。



アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が、デフォルトのネットワーク分析ポリシーによってどのように制御されるのか注意してください。初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。

前処理を調整する簡単な方法は、カスタム ネットワーク分析ポリシーを作成し、それをデフォルトとして使用することです（カスタム ネットワーク分析ポリシーの利点（15-10 ページ）の概要を参照）。ただし、カスタム ネットワーク分析ポリシーでプリプロセッサが無効化されているときに、前処理されたパケットを有効な侵入ルールまたはプリプロセッサ ルールと照合して評価する必要がある場合、システムはプリプロセッサを有効化して使用します。ただし、ネットワーク分析ポリシーのユーザ インターフェイスではプリプロセッサは無効なままになります。

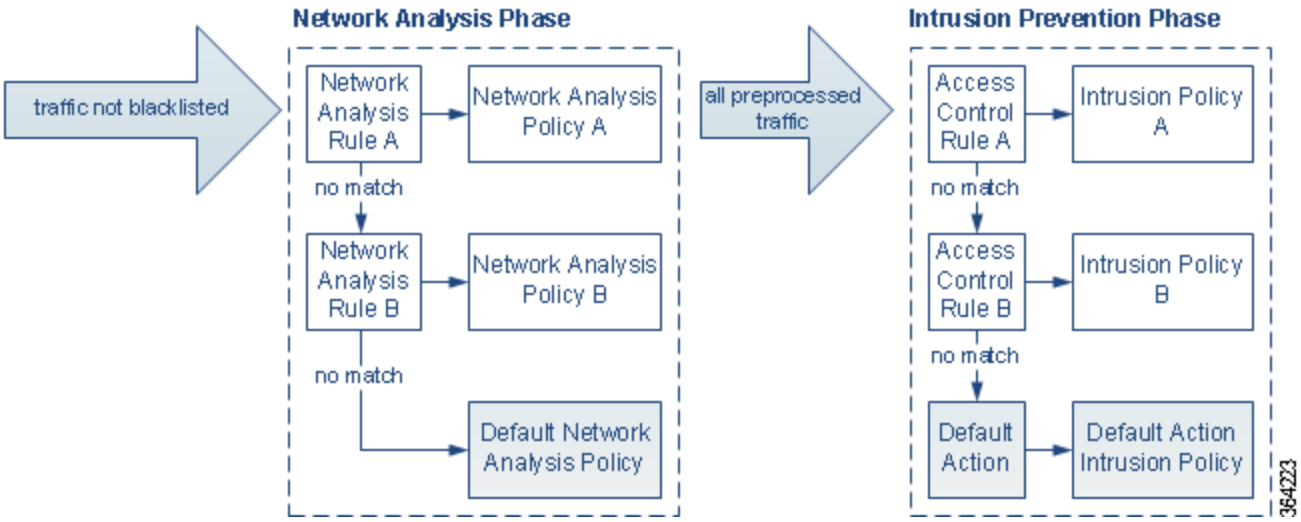
（注）　プリプロセッサを無効にするパフォーマンス上の利点を得るには、侵入ポリシーでそのプリプロセッサを必要とするルールが有効になっていないことを確認する必要があります。

複数のカスタム ネットワーク分析ポリシーを使用する場合は、さらに課題があります。複雑な展開内の上級ユーザの場合は、一致したトラフィックの前処理にカスタム ネットワーク分析ポリシーを割り当てることにより、特定のセキュリティ ゾーンやネットワークに合わせて前処理を調整できます。これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。各ルールにはネットワーク分析ポリシーが関連付けられており、ルールに一致するトラフィックの前処理を制御します。

ヒント　アクセス コントロール ポリシーの詳細設定としてネットワーク分析ルールを設定します。ASA FirePOWER モジュール の他のタイプのルールとは異なり、ネットワーク分析ルールは、ネットワーク分析ポリシーに含まれるのではなく、ネットワーク分析ポリシーを呼び出します。

システムは、ルール番号の昇順で、設定済みネットワーク分析ルールとパケットを照合します。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。これにより非常に柔軟にトラフィックを前処理できます。ただし、留意すべき点として、パケットがどのネットワーク分析ポリシーによって前処理されるかに関係なく、すべてのパケットは、それら独自のプロセスにおいて引き続きアクセス コントロール ルールと照合されます(つまり、侵入ポリシーにより検査される可能性があります)。つまり、特定のネットワーク分析ポリシーでパケットを前処理しても、そのパケットが確実に特定の侵入ポリシーで検査されるわけではありません。アクセス コントロール ポリシーを設定するときは、そのポリシーが正しいネットワーク分析ポリシーおよび侵入ポリシーを呼び出して特定のパケットを評価するように、慎重に行う必要があります。

次の図は、侵入防御(ルール)フェーズよりも前に、別にネットワーク分析ポリシー(前処理)の選択フェーズが発生するしくみを詳細に示しています。簡略化するために、図ではファイル/マルウェア インスペクション フェーズが省かれています。また、デフォルトのネットワーク分析ポリシーおよびデフォルト アクションの侵入ポリシーを強調表示しています。



このシナリオでは、アクセス コントロール ポリシーは、2 つのネットワーク分析ルールとデフォルトのネットワーク分析ポリシーで設定されています。

- Network Analysis Rule A は、一致するトラフィックを Network Analysis Policy A で前処理します。その後、このトラフィックを Intrusion Policy A で検査されるようにすることができます。
- Network Analysis Rule B は、一致するトラフィックを Network Analysis Policy B で前処理します。その後、このトラフィックを Intrusion Policy B で検査されるようにすることができます。
- 残りのトラフィックはすべて、デフォルトのネットワーク分析ポリシーにより前処理されます。その後、このトラフィックをアクセス コントロール ポリシーのデフォルト アクションに関連付けられた侵入ポリシーによって検査されるようにすることができます。

システムはトラフィックを前処理した後、侵入についてトラフィックを検査できます。図では、2 つのアクセス コントロール ルールとデフォルト アクションが含まれるアクセス コントロール ポリシーを示しています。

- アクセス コントロール ルール A は、一致したトラフィックを許可します。トラフィックはその後、Intrusion Policy A によって検査されます。
- アクセス コントロール ルール B は、一致したトラフィックを許可します。トラフィックはその後、Intrusion Policy B によって検査されます。
- アクセス コントロール ポリシーのデフォルト アクションは一致したトラフィックを許可します。トラフィックはその後、デフォルト アクションの侵入ポリシーによって検査されます。

各パケットの処理は、ネットワーク分析ポリシーと侵入ポリシーのペアにより制御されますが、このペアはユーザに合わせて調整されません。アクセス コントロール ポリシーが誤って設定されているため、ネットワーク分析ルール A とアクセス コントロール ルール A が同じトラフィックを処理しない場合を想定してください。たとえば、特定のセキュリティ ゾーンのトラフィックの処理をポリシー ペアによって制御することを意図している場合に、誤まって、異なるゾーンを使用するように 2 つのルールの条件を設定したとします。この誤設定により、トラフィックが誤って前処理される可能性があります。したがって、ネットワーク分析ルールおよびカスタム ポリシーを使用した前処理の調整は、高度なタスクです。

単一の接続の場合は、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、一部の前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定には影響しません。

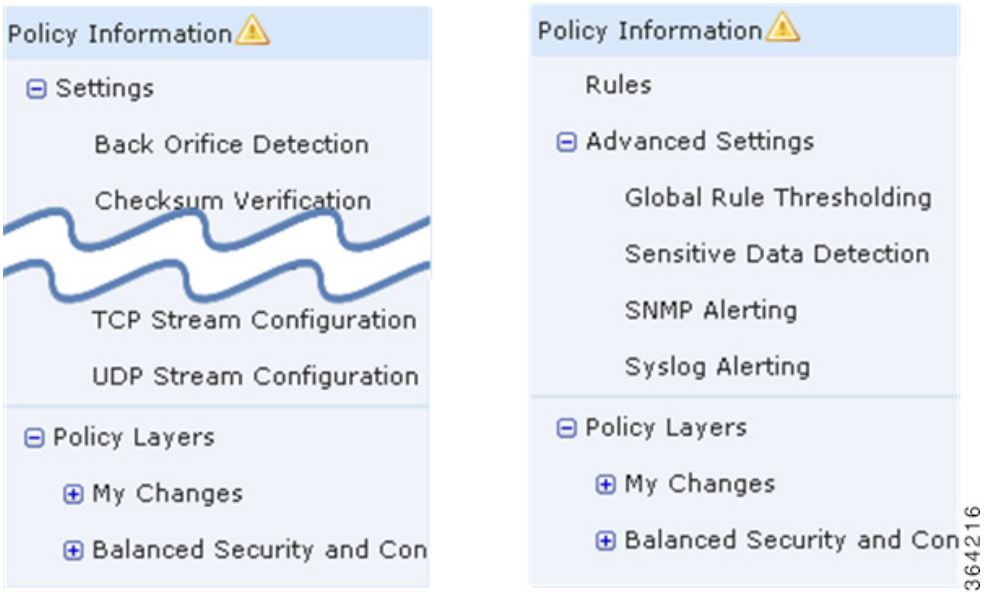
ナビゲーション パネルの使用

ライセンス：Protection

ネットワーク分析ポリシーおよび侵入ポリシーは、同様のユーザ インターフェイスを使用して、設定の変更を編集および保存します。以下を参照してください。

- ネットワーク分析ポリシーの編集（18-4 ページ）
- 侵入ポリシーの編集（23-4 ページ）

ナビゲーション パネルは、いずれかのタイプのポリシーを編集する際にユーザ インターフェイスの左側に表示されます。次の図は、ネットワーク分析ポリシー（左）および侵入ポリシー（右）のナビゲーション パネルを示しています。



ナビゲーション パネルは境界線によって複数のポリシー設定項目リンクに分割されており、ポリシー層との直接対話により（下側）または直接対話なしで（上側）ポリシー設定項目を設定できます。いずれかの設定ページに移動するには、ナビゲーション パネル内の名前をクリックします。ナビゲーション パネルで影付きで強調表示されている項目は、現在の設定ページを示しています。たとえば、上の図では、[ポリシー情報（Policy Information）] ページがナビゲーション パネルの右側に表示されます。

[ポリシー情報（Policy Information）]

[ポリシー情報（Policy Information）] ページには、一般的に使用される設定の設定オプションが示されます。上記のネットワーク分析ポリシー パネルの図に示すように、ポリシーに未保存の変更がある場合は、ナビゲーション パネルの [ポリシー情報（Policy Information）] の横にポリシー変更アイコン（  ）が表示されます。アイコンは、変更を保存すると消えます。

[ルール（Rules）]（侵入ポリシーのみ）

侵入ポリシーの [ルール（Rules）] ページでは、共有オブジェクトのルール、標準テキスト ルール、およびプリプロセッサ ルールのルール ステータスとその他の設定項目を設定できます。詳細については、ルールを使用した侵入ポリシーの調整（24-1 ページ）を参照してください。

[設定（Settings）]（ネットワーク分析ポリシー）および **[詳細設定（Advanced Settings）]**（侵入ポリシー）

ネットワーク分析ポリシーの [設定（Settings）] ページでは、プリプロセッサを有効または無効にしたり、プリプロセッサの設定ページにアクセスしたりできます。[設定（Settings）] リンクを展開すると、ポリシー内で有効になっているすべてのプリプロセッサの個々の設定ページへのサブリンクが表示されます。詳細については、ネットワーク分析ポリシーでのプリプロセッサの設定（18-7 ページ）を参照してください。

侵入ポリシーの [詳細設定（Advanced Settings）] ページでは、詳細設定を有効または無効にしたり、詳細設定の設定ページにアクセスしたりできます。[詳細設定（Advanced Settings）] リンクを展開すると、ポリシー内で有効になっているすべての詳細設定を個々に設定する設定ページへのサブリンクが表示されます。詳細については、侵入ポリシーの詳細設定の設定（23-7 ページ）を参照してください。

[ポリシー層（Policy Layers）]

[ポリシー層（Policy Layers）] ページには、ネットワーク分析ポリシーまたは侵入ポリシーを構成する階層の要約が表示されます。[ポリシー層（Policy Layers）] リンクを展開すると、ポリシー内の階層に関する概要ページへのサブリンクが表示されます。各階層のサブリンクを展開すると、その階層で有効になっているすべてのルール、プリプロセッサ、または詳細設定の設定ページへのサブリンクがさらに表示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

競合の解決とポリシー変更の確定

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシーを編集するときは、システムが認識する前にその変更を保存（またはコミット）する必要があります。

（注）　保存後は、変更を反映させるためにネットワーク分析ポリシーまたは侵入ポリシーを適用する必要があります。保存しないでポリシーを適用すると、最後に保存された設定が使用されます。侵入ポリシーは単独で再適用できますが、ネットワーク分析ポリシーは親のアクセス コントロール ポリシーとともに適用されます。

編集競合の解決

[ネットワーク分析ポリシー（Network Analysis Policy）] ページと [侵入ポリシー（Intrusion Policy）] ページには、各ポリシーに未保存の変更があるかどうかが表示されます。ネットワーク分析ポリシーの編集（18-4 ページ）および侵入ポリシーの編集（23-4 ページ）を参照してください。

シスコでは、同時に 1 人だけがポリシーを編集することを推奨しています。同じユーザとして複数のユーザ インターフェース インスタンス経由で同じネットワーク分析ポリシーまたは侵入ポリシーを編集中に、1 つのインスタンスの変更を保存する場合、他のインスタンスの変更は保存できません。

設定の依存関係の解決

特定の分析を実行する場合、多くのプリプロセッサ ルールとセキュリティ ルールでは、最初に特定の方法でトラフィックをデコードまたは前処理するか、他の依存関係を割り当てる必要があります。ネットワーク分析ポリシーまたは侵入ポリシーを保存すると、システムが必要な設定を自動的に有効にするか、または次のように無効な設定はトラフィックに影響しないことが警告されます。

- SNMP ルール アラートを追加しても、SNMP アラートを設定しなかった場合は、侵入ポリシーを保存できません。SNMP アラートを設定するか、またはルール アラートを無効にしてから、再度保存します。
- 侵入ポリシーに有効なセンシティブ データ ルールが含まれているときに、センシティブ データ プリプロセッサが有効になっていない場合は、侵入ポリシーを保存できません。システムがプリプロセッサを有効にしてポリシーを保存するように許可するか、またはルールを無効にしてから、再度保存します。
- ネットワーク分析ポリシーで必要なプリプロセッサを無効にしても、ポリシーを引き続き保存できます。ただし、ユーザ インターフェイスでプリプロセッサが無効になっていても、システムは無効になっているプリプロセッサを自動的に現在の設定で使用します。詳細については、カスタム ポリシーに関する制約事項（15-12 ページ）を参照してください。
- ネットワーク分析ポリシーでインライン モードを無効にしても、インライン正規化プリプロセッサが有効になっている場合は、ポリシーを引き続き保存できます。ただし、正規化設定が無視されることが警告されます。インライン モードを無効化すると他の設定が無視されるので、プリプロセッサは、チェックサム検証やレート ベース攻撃の防御を含めて、トラフィックを変更またはブロックできます。詳細については、インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（18-6 ページ）およびインライン トラフィックの正規化（21-6 ページ）を参照してください。

ポリシー変更のコミット、破棄、およびキャッシュ

ネットワーク分析ポリシーまたは侵入ポリシーの編集時に、変更を保存しないでポリシー エディタを終了した場合、それらの変更はシステムによってキャッシュされます。システムからログアウトした場合や、システム クラッシュが発生した場合でも、変更はキャッシュされます。システム キャッシュには、1 つのネットワーク分析ポリシーと 1 つの侵入ポリシーの未保存の変更しか格納されないので、同じタイプの別のポリシーを編集する場合は、その前に、行った変更を確定または破棄する必要があります。システムは、ユーザが最初のポリシーへの変更を保存せずに別のポリシーを編集したり、侵入ルールの更新をインポートした場合に、キャッシュされた変更内容を破棄します。

ネットワーク分析ポリシー エディタまたは侵入ポリシー エディタの [ポリシー情報（Policy Information）] ページでポリシーの変更内容をコミットまたは破棄できます。ネットワーク分析ポリシーの編集（18-4 ページ）および侵入ポリシーの編集（23-4 ページ）を参照してください。

次の表に、ネットワーク分析ポリシーまたは侵入ポリシーへの変更を保存または破棄する方法の概要を示します。

表 ***15-1***　ネットワーク分析ポリシーまたは侵入ポリシーへの変更のコミット

目的	**[ポリシー情報（Policy Information）]** ページでの操作
ポリシーへの変更を保存する	[変更を確定（Commit Changes）] をクリックします。 任意で、コメントを入力します。[OK] をクリックしてコミットを続行します。
すべての未保存の変更を破棄する	[変更の破棄（Discard Changes）] をクリックし、次に [OK] をクリックして変更を破棄し、[侵入ポリシー（Intrusion Policy）] ページに移動します。変更を破棄しない場合は、[キャンセル（Cancel）] をクリックして、[ポリシー情報（Policy Information）] ページに戻ります。
ポリシーを終了するが、変更をキャッシュする	任意のメニューまたは別のページへの他のパスを選択します。終了時に、表示されたプロンプトで [ページを移動（Leave page）] をクリックするか、[ページを移動しない（Stay on page）] をクリックして高度なエディタに残ります。

ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用

多数の ASA FirePOWER モジュールが存在する大規模な組織では、さまざまな部署や事業部門、場合によっては異なる企業の固有のニーズをサポートするために、多数の侵入ポリシーおよびネットワーク分析ポリシーが存在することがあります。両方のポリシー タイプでの設定はレイヤと呼ばれる構成要素に含まれており、それを使用することで効率的に複数のポリシーを管理することができます。

侵入ポリシーおよびネットワーク分析ポリシーのレイヤは、原則的に同じ方法で動作します。ポリシー タイプの作成および編集は、レイヤを意識せずに行えます。ポリシー設定を変更でき、ポリシーにユーザ レイヤを追加していない場合は、システムによって自動的に変更内容が単一の設定可能なレイヤ（最初は *My Changes* という名前が付けられています）に含められます。必要に応じて、最大 200 までレイヤを追加できます。それらのレイヤでは、設定の組み合わせを自由に設定できます。ユーザ レイヤのコピー、マージ、移動、削除を実行できます。最も重要なこととして、個々のユーザ レイヤを同じタイプの他のポリシーと共有できます。

詳細については、次の各項を参照してください。

- レイヤ スタックについて（16-1 ページ）では、基本ポリシーを構成するユーザ設定可能な組み込み型のレイヤについて説明します。
- レイヤの管理（16-6 ページ）では、ポリシー内でレイヤを使用する方法について説明します。

レイヤ スタックについて

ライセンス：Protection

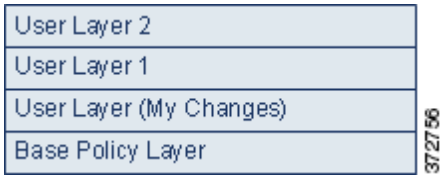
レイヤを追加していないネットワーク分析ポリシーまたは侵入ポリシーには、組み込み型で読み取り専用の基本ポリシー レイヤと、デフォルトで「My Changes」という名前が付けられているユーザ設定可能な単一のレイヤが含まれます。ユーザ設定可能なレイヤのコピー、マージ、移動、または削除を実行できます。また、任意のユーザ設定可能なレイヤを同じタイプの他のポリシーと共有できるように設定できます。

各ポリシー レイヤには、ネットワーク分析ポリシー内のすべてのプリプロセッサまたは侵入ポリシー内のすべての侵入ルールと詳細設定の完全な設定が含まれます。最下部の基本ポリシー レイヤには、ポリシーの作成時に選択した基本ポリシーのすべての設定が含まれます。上位レイヤの設定は、下位レイヤの同じ設定よりも優先されます。レイヤで明示的に設定されていない機能は、明示的に設定されている次の高いレイヤから設定を継承します。

システムはレイヤをフラット化します。つまり、ネットワーク トラフィックの処理時にすべての設定の蓄積効果のみを適用します。

ヒント　基本ポリシーのデフォルト設定のみに基づいて侵入ポリシーおよびネットワーク分析ポリシーを作成できます。

次の図は、基本ポリシー レイヤと初期設定の My Changes レイヤに加え、2 つのユーザ設定可能なレイヤ *User Layer 1* と *User Layer 2* が示されたレイヤ スタックの例を示しています。この図では、ユーザが追加したユーザ設定可能な各レイヤは、スタックの最上位のレイヤに配置されていることに注目してください。図の User Layer 2 は、最後に追加され、スタックの最上位にあります。



複数のレイヤを使用する場合は、次の点に注意してください。

- 以下のいずれかを実行する場合、ポリシー内の最上位のレイヤが読み取り専用レイヤであるか、またはポリシー間のレイヤの共有（16-10 ページ）で説明されてる共有レイヤであるときに、ユーザ設定可能なレイヤが最上位のレイヤとして侵入ポリシーに自動的に追加されます。
  - 侵入ポリシーの [ルール（Rules）] ページからルール操作（つまり、ルール状態、イベント フィルタリング、動的状態、または警告）を変更する。詳細については、ルールを使用した侵入ポリシーの調整（24-1 ページ）を参照してください。
  - プリプロセッサ、侵入ルール、または詳細設定の有効化、無効化、または変更を実行する。

  システムによって追加されたレイヤのすべての設定は、新しいレイヤで発生した変更を除いてすべて継承されます。
- 最上位レイヤが共有レイヤの場合、次のアクションのいずれかを実行すると、システムはレイヤを追加します。
  - 他のポリシーとの最上位レイヤの共有
  - ポリシーへの共有レイヤの追加
- ルール更新にポリシーの変更を許可しているかどうかに関わらず、ルール更新での変更は、レイヤで行った変更を上書きしません。これは、ルール更新での変更が、基本ポリシー レイヤのデフォルト設定を決定する基本ポリシーで行われるためです。変更は常により上位のレイヤに加えられ、その変更によって、ルール更新が基本ポリシーに加えた変更が上書きされます。詳細については、ルールの更新とローカル ルール ファイルのインポート（43-10 ページ）を参照してください。

詳細については、基本レイヤについて（16-2 ページ）を参照してください。

基本レイヤについて

ライセンス：Protection

侵入ポリシーまたはネットワーク分析ポリシーの基本レイヤ（基本ポリシーとも呼ばれる）は、ポリシーのすべての設定のデフォルト設定を定義し、ポリシーの最下位に位置します。新しいポリシーを作成し、新しいレイヤを追加しないで設定を変更すると、その変更は My Changes レイヤに保存され、基本ポリシーの設定を上書きしますが変更はしません。

詳細については、次の各項を参照してください。

- システムによって提供される基本ポリシーについて（16-3 ページ）
- カスタム基本ポリシーについて（16-3 ページ）

システムによって提供される基本ポリシーについて

ライセンス：Protection

シスコは、ネットワーク分析ポリシーおよび侵入ポリシーの複数のペアを ASA FirePOWER モジュールとともに提供します。システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーを使用して、シスコ 脆弱性調査チーム（VRT）のエクスペリエンスを活用することができます。これらのポリシーでは、VRT は侵入ルールおよびプリプロセッサ ルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。これらのシステムによって提供されるポリシーをそのまま使用したり、カスタム ポリシーのベースとして使用することができます。

システムによって提供されるポリシーをベースとして使用する場合、ルール更新をインポートすると、基本ポリシー内の設定が変更される場合があります。しかし、これらの変更内容をシステムによって提供される基本ポリシーに自動的に反映しないようにカスタム ポリシーを設定できます。これにより、ルール更新のインポートとは関係ないスケジュールで、システムによって提供される基本ポリシーを手動で更新できます。いずれの場合も、ルール更新が基本ポリシーに加えた変更によって My Changes または他のレイヤの設定が変更または上書きされることはありません。詳細については、ルール更新がシステムによって提供される基本ポリシーを変更することを許可する（16-4 ページ）を参照してください。

システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。詳細については、システム付属のポリシーについて（15-8 ページ）を参照してください。

カスタム基本ポリシーについて

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシーでシステムによって提供されるポリシーを基本ポリシーとして使用しない場合は、カスタム ポリシーをベースとして使用できます。デバイスのパフォーマンスと、生成されたイベントに効率的に応答できる能力の両方を向上させるために、ご自身に最も重要な方法でトラフィックを検査するようにカスタム ポリシーの設定を調整できます。

最大 5 つのカスタム ポリシーをチェーンすることができます。5 つのうちの 4 つのポリシーで事前に作成されたポリシーが基本ポリシーとして使用され、5 つ目のポリシーでシステムによって提供されたポリシーをベースとして使用する必要があります。

別のポリシーのベースとして使用するカスタム ポリシーに加えた変更は、ベースとして使用するポリシーのデフォルト設定として自動的に使用されます。また、すべてのポリシーにはポリシー チェーン内の最終的なベースとしてシステムによって提供されるポリシーがあるので、カスタム基本ポリシーを使用していてもルール更新のインポートがポリシーに影響を与える場合があります。チェーン内の最初のカスタム ポリシー（システムによって提供されるポリシーをベースとして使用するポリシー）によってルール更新がその基本ポリシーを変更することが許可されている場合は、ポリシーが影響を受ける可能性があります。この設定の変更の詳細については、ルール更新がシステムによって提供される基本ポリシーを変更することを許可する（16-4 ページ）を参照してください。

これらの設定に関係なく、基本ポリシーへの変更（ルール更新による変更、または基本ポリシーとして使用するカスタム ポリシーを変更する場合）によって My Changes または他のレイヤの設定が変更または上書きされることはありません。

基本ポリシーの変更

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシーに対し異なる基本ポリシーを選択できます。また、オプションで、上位レイヤの変更に影響を与えることなく、ルール更新がシステムによって提供される基本ポリシーを変更することを許可することができます。

基本ポリシーの変更方法：

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー情報（Policy Information）] をクリックします。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 2　[基本ポリシー（Base Policy）] ドロップダウンリストから基本ポリシーを選択します。

ステップ 3　オプションで、システムによって提供される基本ポリシーを選択する場合は、[基本ポリシーの管理（Manage Base Policy）] をクリックして、侵入ルールの更新によって基本ポリシーが自動的に変更されるかどうかを指定します。

詳細については、ルール更新がシステムによって提供される基本ポリシーを変更することを許可する（16-4 ページ）を参照してください。

ステップ 4　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

ルール更新がシステムによって提供される基本ポリシーを変更することを許可する

ライセンス：Protection

インポートするルール更新によって、システムによって提供されるポリシーには、ネットワーク分析プリプロセッサの設定変更、侵入ポリシーの詳細設定の変更、新規および更新済みの侵入ルール、および既存ルールの状態の変更が提供されます。ルール更新では、ルールを削除したり、新しいルール カテゴリとデフォルト変数を提供したりすることもできます。詳細については、ルールの更新とローカル ルール ファイルのインポート（43-10 ページ）を参照してください。

ルール更新は、プリプロセッサ、詳細設定およびルールの変更とともに、システムによって提供されるポリシーを常に変更します。デフォルト変数とルール カテゴリに対する変更はシステム レベルで処理されます。詳細については、システムによって提供される基本ポリシーについて（16-3 ページ）を参照してください。

システムによって提供されるポリシーを基本ポリシーとして使用するときは、ルール更新が基本ポリシー（この場合はシステムによって提供されるポリシーのコピー）を変更することを許可することができます。ルール更新で基本ポリシーの更新を許可する場合は、新しいルール更新によって、基本ポリシーとして使用するシステムによって提供されるポリシーに対する変更と同じ変更が基本ポリシーにも加えられます。対応する設定を変更しなかった場合は、基本ポリシー内の設定によって、ポリシー内の設定が決定されます。ただし、ルール更新では、ポリシー内で行った変更は上書きされません。

ルール更新で基本ポリシーの更新を許可しない場合は、1 つ以上のルール更新のインポート後に、基本ポリシーを手動で更新できます。

ルール更新では、侵入ポリシー内のルール状態またはルール更新で基本の侵入ポリシーの更新が許可されているかどうかに関係なく、VRT が削除した侵入ルールが常に削除されます。ネットワーク トラフィックに変更を再適用するまで、現在適用されている侵入ポリシー ルールは次のように動作します。

- 無効になっているルールは無効のままになります。
- [イベントを生成する（Generate Events）] に設定されたルールでは、トリガーされたときのイベントの生成が継続されます。
- [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールでは、トリガーされたときのイベントの生成と違反パケットのドロップが継続されます。

次の両方の条件が満たされていない限り、ルール更新でカスタム基本ポリシーは変更されません。

- ルール更新が親ポリシーのシステムによって提供される基本ポリシー（つまり、カスタム基本ポリシーの起源となるポリシー）を変更することを許可している。
- 親の基本ポリシー内の対応する設定が上書きされる親ポリシー内の変更を実施していない。

両方の条件が満たされている場合は、親ポリシーを保存したときに、ルール更新内の変更が子ポリシー（つまり、カスタム基本ポリシーを使用したポリシー）に渡されます。

たとえば、ルール更新で以前に無効になっていた侵入ルールを有効にして、親の侵入ポリシー内のルール状態を変更していない場合は、親ポリシーを保存したときに、変更されたルール状態が基本ポリシーに渡されます。

同様に、ルール更新でデフォルトのプリプロセッサ設定を変更し、親のネットワーク分析ポリシーの設定を変更していない場合は、変更された設定は親ポリシーを保存したときに基本ポリシーに渡されます。

詳細については、基本ポリシーの変更（16-4 ページ）を参照してください。

ルール更新がシステムによって提供される基本ポリシーを変更することを許可する方法:

ステップ 1　システムによって提供されるポリシーを基本ポリシーとして使用するポリシーの編集時に、ナビゲーション パネルで [ポリシー情報（Policy Information）] をクリックします。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 2　[基本ポリシーの管理（Manage Base Policy）] をクリックします。

[基本ポリシー（Base Policy）] 概要ページが表示されます。

ステップ 3　[新しいルール更新のインストール時に更新（Update when a new Rule Update is installed）] チェックボックスをオンまたはオフにします。

このチェックボックスをオフにしてポリシーを保存してから、ルール更新をインポートすると、[基本ポリシー（Base Policy）] 概要ページに [今すぐ更新（Update Now）] ボタンが表示され、そのページ上のステータス メッセージが更新されて、ポリシーが期限切れであることが示されます。必要に応じて、[今すぐ更新（Update Now）] をクリックして、最近インポートしたルール更新内の変更で基本ポリシーを更新できます。

ステップ 4　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

レイヤの管理

ライセンス：Protection

[ポリシー層（Policy Layers）] ページでは、ネットワーク分析ポリシーまたは侵入ポリシーの完全なレイヤ スタックの単一ページの概要を示します。このページでは、共有レイヤおよび非共有レイヤの追加、レイヤのコピー、マージ、移動、および削除、各レイヤの概要ページへのアクセス、各レイヤ内の有効、無効、および上書きされている設定の設定ページへのアクセスを行うことができます。

各レイヤについて、次の情報が表示されます。

- レイヤが組み込み型レイヤ、共有ユーザ レイヤ、または非共有ユーザ レイヤであるかどうか
- どのレイヤに最上位の（つまり効果的な）プリプロセッサまたは詳細設定が含まれているか（機能名別に）
- 侵入ポリシーで、状態がレイヤで設定されている侵入ルールの数、および各ルール状態に設定されているルールの数

各レイヤのサマリにある機能名は、以下のように、設定がレイヤで有効、無効、上書き、または継承されているかを示します。

機能の状態	機能名
レイヤで有効	プレーン テキストで表示
レイヤで無効	取り消し線が引かれる
上位レイヤの設定によって上書きされる	イタリック テキストで表示
下位レイヤから継承される	表示されない

このページには、有効なすべてのプリプロセッサ（ネットワーク分析）または詳細設定（侵入）、また侵入ポリシーの場合は侵入ルールの最終的な効果の概要も示されます。

次の表に、[ポリシー層（Policy Layers）] ページで使用できるアクションを示します。

表 **16-1**　ネットワーク分析レイヤおよび侵入ポリシー レイヤの設定アクション

目的	操作
[ポリシー情報（Policy Information）] ページの表示	[ポリシーの概要（Policy Summary）] をクリックします。 [ポリシー情報（Policy Information）] ページで実行できる操作については、ルールを使用した侵入ポリシーの調整（24-1 ページ）、ネットワーク分析ポリシーの開始（18-1 ページ）、および侵入ポリシーを使用する前に（23-1 ページ）を参照してください。
レイヤのサマリ ページの表示	レイヤの行でレイヤ名をクリックするか、またはユーザ レイヤの横にある編集アイコン（  ）をクリックします。表示アイコン（  ）をクリックして、共有レイヤの読み取り専用のサマリ ページにアクセスすることもできます。 レイヤのサマリ ページで実行できる操作については、ポリシー間のレイヤの共有（16-10 ページ）、レイヤ内のプリプロセッサと詳細設定の設定（16-15 ページ）、およびレイヤでの侵入ルールの設定（16-11 ページ）を参照してください。
レイヤ レベルのプリプロセッサまたは詳細設定の設定ページへのアクセス	レイヤの行で機能名をクリックします。基本ポリシーと共有レイヤでは、設定ページが読み取り専用であることに注意してください。詳細については、レイヤ内のプリプロセッサと詳細設定の設定（16-15 ページ）を参照してください。
ルール状態のタイプ別にフィルタリングされたレイヤ レベルのルール設定ページへのアクセス	レイヤのサマリでドロップしてイベントを生成する（  ）、イベントを生成する（  ）、または無効（）のアイコンをクリックします。選択したルール状態に設定されているルールがレイヤに含まれていない場合、ルールは表示されません。

表 **16-1**　ネットワーク分析レイヤおよび侵入ポリシー レイヤの設定アクション（続き）

目的	操作
ポリシーへのレイヤの追加	レイヤの追加（16-7 ページ）を参照してください。
別のポリシーからの共有レイヤの追加	ポリシー間のレイヤの共有（16-10 ページ）を参照してください。
レイヤの名前または説明の変更	レイヤの名前および説明の変更（16-8 ページ）を参照してください。
レイヤの移動、コピー、または削除	レイヤの移動、コピー、および削除（16-8 ページ）を参照してください。
すぐ下のレイヤとのレイヤのマージ	レイヤのマージ（16-9 ページ）を参照してください。

[ポリシー層（**Policy Layers**）**]** ページの使用方法：

ステップ **1**　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。
[ポリシー層（Policy Layers）] サマリ ページが表示されます。

ステップ **2**　ネットワーク分析レイヤおよび侵入ポリシー レイヤの設定アクションの表にある操作を実行できます。

ステップ **3**　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

レイヤの追加

ライセンス：Protection

最大 200 のレイヤをネットワーク分析ポリシーまたは侵入ポリシーに追加できます。レイヤを追加すると、ポリシーで最上位レイヤとして表示されます。初期状態はすべての機能に対して [継承（Inherit）] で、侵入ポリシーでは、イベントのフィルタリング、動的状態、またはルール アクションのアラートは設定されません。

ネットワーク分析ポリシーまたは侵入ポリシーへのレイヤの追加方法：

ステップ **1**　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。
[ポリシー層（Policy Layers）] ページが表示されます。

ステップ **2**　[ユーザ レイヤ（User Layers）] の横にあるレイヤの追加アイコン（ ）をクリックします。
[レイヤの追加（Add Layer）] ポップアップ ウィンドウが表示されます。

ステップ **3**　一意のレイヤの名前を入力し、[OK] をクリックします。
新しいレイヤが [ユーザ レイヤ（User Layers）] の下に最上位レイヤとして表示されます。

ステップ **4**　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

レイヤの名前および説明の変更

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシー内のユーザ設定可能なレイヤの名前を変更できます。また、オプションで、レイヤの編集時に表示される説明を追加または変更できます。

レイヤ名の変更方法および説明の追加/変更方法：

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。

[ポリシー層（Policy Layers）] ページが表示されます。

ステップ 2　編集するユーザ レイヤの横にある編集アイコン（ ）をクリックします。

レイヤのサマリ ページが表示されます。

ステップ 3　次の操作を実行できます。

- レイヤの名前を変更します。
- レイヤの説明を追加または変更します。

ステップ 4　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

レイヤの移動、コピー、および削除

ライセンス：Protection

初期の My Changes レイヤを含む、ネットワーク分析ポリシーまたは侵入ポリシー内のユーザ レイヤをコピー、移動、または削除できます。次の考慮事項に注意してください。

- レイヤをコピーすると、そのコピーが最上位レイヤとして表示されます。
- 共有レイヤをコピーすると、非共有コピーが作成されます。そのコピーは、任意で後で他のポリシーと共有できます。
- 共有レイヤは削除できません。共有が有効になっているレイヤで別のポリシーと共有していないものは、共有レイヤではありません。

レイヤのコピー、移動、削除方法：

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。

[ポリシー層（Policy Layers）] ページが表示されます。

ステップ 2　次の操作を実行できます。

- レイヤをコピーするには、コピーするレイヤのコピー アイコン（ ）をクリックします。

  ページが更新され、レイヤのコピーが最上位のレイヤとして表示されます。

- レイヤを [ユーザ レイヤ（User Layers）] ページ領域内で上下に移動させるには、レイヤ サマリ内の任意の空いている場所をクリックし、位置矢印（）が移動するレイヤの上または下の行を指すまでドラッグします。

  画面が更新され、レイヤが新しい場所に表示されます。
- レイヤを削除するには、削除するレイヤの削除アイコン（  ）をクリックし、[OK] をクリックします。

  ページが更新され、レイヤは削除されます。

ステップ 3　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

レイヤのマージ

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシー内のユーザ設定可能なレイヤを、その下にある次のユーザ レイヤとマージできます。マージされたレイヤは、どちらかのレイヤに固有だったすべての設定を保持します。また、両方のレイヤに同じプリプロセッサ、侵入ルール、または詳細設定が含まれていた場合、上位のレイヤの設定を受け入れます。マージされたレイヤでは、下位レイヤの名前が保持されます。

他のポリシーに追加する共有レイヤを作成するポリシーでは、共有レイヤのすぐ上の非共有レイヤと共有レイヤをマージできますが、共有レイヤをその下の非共有レイヤとマージすることはできません。

別のポリシーに作成した共有レイヤを追加するポリシーでは、共有レイヤをそのすぐ下の非共有レイヤとマージできますが、作成されたレイヤは共有されなくなります。非共有レイヤをその下の共有レイヤとマージすることはできません。

ユーザ レイヤをその下のユーザ レイヤとマージする方法：

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。

[ポリシー層（Policy Layers）] ページが表示されます。

ステップ 2　2 つのレイヤの上部にあるマージ アイコン（  ）をクリックし、[OK] をクリックします。

ページが更新され、レイヤがその下のレイヤとマージされます。

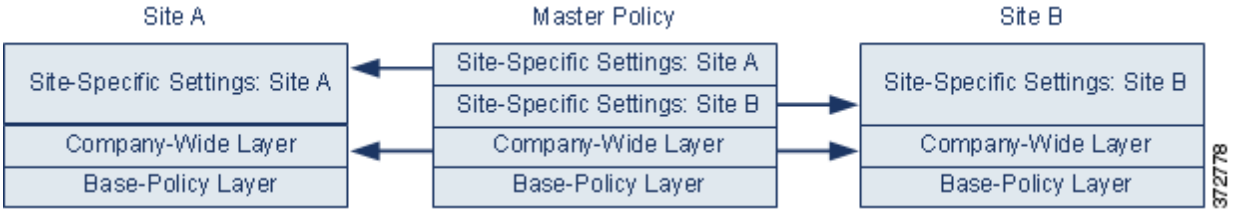
ステップ 3　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

ポリシー間のレイヤの共有

ライセンス：Protection

ユーザ設定可能なレイヤを同じタイプの他のポリシー（侵入またはネットワーク分析）と共有できます。共有レイヤ内の設定を変更し、変更をコミットすると、共有レイヤを使用するすべてのポリシーが更新され、影響を受けたすべてのポリシーのリストが提供されます。レイヤを作成したポリシー内の共有レイヤ機能の設定のみを変更できます。

以下の図には、サイト固有のポリシーのソースとして機能するマスター ポリシーの例が示されています。



図のマスター ポリシーには、Site A と Site B のポリシーに適用可能な設定を持つ全社的レイヤが含まれます。また、各ポリシーのサイト固有のレイヤも含まれます。たとえば、ネットワーク分析ポリシーの場合、Site A にはモニタ対象ネットワークに Web サーバがないため、保護したり、HTTP インスペクション プリプロセッサのオーバーヘッドを処理したりする必要はありませんが、両方のサイトで TCP ストリームの前処理が必要になる場合があります。両方のサイトで共有する全社的レイヤで TCP ストリーム処理を有効にし、Site A で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを無効にして、Site B で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを有効にできます。サイト固有のポリシーで上位レイヤの設定を編集することで、必要に応じて、設定の調整によって各サイトのポリシーをさらに調整することもできます。

この例のマスター ポリシーでフラット化された設定値そのものがトラフィックをモニタするのに役立つ訳ではありませんが、サイト固有のポリシーを設定および更新する際に時間が節約されるため、ポリシー層で活用することができます。

その他にも多くのレイヤ設定が可能です。たとえば、企業、部門、またはネットワークごとにポリシー層を定義できます。侵入ポリシーの場合は、一方のレイヤに詳細設定を含め、もう一方にルール設定を含めることもできます。

ヒント　基本ポリシーが共有するレイヤが作成されたカスタム ポリシーである場合、ポリシーに共有レイヤを追加することはできません。変更を保存しようとすると、ポリシーに循環依存関係が含まれていることを示すエラー メッセージが表示されます。詳細については、カスタム基本ポリシーについて（16-3 ページ）を参照してください。

他のポリシーとレイヤを共有するには、次の手順を実行する必要があります。

- 共有するレイヤのレイヤ サマリ ページで共有を有効にします。
- 共有するポリシーの [ポリシー層（Policy Layers）] ページで共有レイヤを追加します。

別のポリシーで使用されているレイヤの共有を無効にすることはできません。まずレイヤを他のポリシーから削除するか、他のポリシーを削除する必要があります。

他のポリシーとのレイヤ共有を有効化/無効化する方法:

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層(Policy Layers)] をクリックします。

[ポリシー層(Policy Layers)] ページが表示されます。

ステップ 2　その他のポリシーと共有するレイヤの横にある編集アイコン( )をクリックします。

レイヤのサマリ ページが表示されます。

ステップ 3　[共有(Sharing)] チェックボックスをオン(有効)またはオフ(無効)にします。

ステップ 4　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

ポリシーへの共有レイヤの追加方法:

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層(Policy Layers)] をクリックします。

[ポリシー層(Policy Layers)] ページが表示されます。

ステップ 2　[ユーザ レイヤ(User Layers)] の横にある共有レイヤの追加アイコン( )をクリックします。

[共有レイヤの追加(Add Shared Layer)] ポップアップ ウィンドウが表示されます。

ステップ 3　[共有レイヤの追加(Add Shared Layer)] ドロップダウンリストから追加する共有レイヤを選択し、[OK] をクリックします。

[ポリシー層(Policy Layers)] サマリ ページが表示され、選択した共有レイヤがポリシーの最上位レイヤとして表示されます。

その他のポリシーに共有レイヤがない場合、ドロップダウンリストは表示されません。ポップアップ ウィンドウで [OK] または [キャンセル(Cancel)] をクリックすると、[ポリシー層(Policy Layers)] サマリ ページに戻ります。

ステップ 4　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

レイヤでの侵入ルールの設定

ライセンス:Protection

侵入ポリシーでは、ユーザ設定可能な任意のレイヤで、ルールのルール状態、イベント フィルタリング、動的状態、アラート、およびルール コメントを設定できます。変更を加えるレイヤにアクセスした後、そのレイヤの [ルール(Rules)] ページの設定を、侵入ポリシーの [ルール(Rules)] ページの設定と同じように追加します。ルールを使用した侵入ポリシーの調整(24-1 ページ)を参照してください。

レイヤの [ルール(Rules)] ページで個々のレイヤ設定を表示することも、[ルール(Rules)] ページのポリシー ビューですべての設定の最終的な効果を表示することもできます。[ルール(Rules)] ページのポリシー ビューのルール設定を変更する場合、ポリシーの最上位のユーザ設定可能なレイヤを変更します。[ルール(Rules)] ページにあるレイヤ ドロップダウンリストを使用して、別のレイヤに切り替えることができます。

次の表では、複数のレイヤで同じ種類の設定を構成した場合の結果について説明しています。

表 **16-2**　レイヤ ルールの設定

設定可能なレイヤ数	設定の種類	目的
1	ルール状態	下位レイヤのルールに対して設定されたルール状態を上書きします。また、下位レイヤで設定されたそのルールのすべてのしきい値、抑制、レートベースのルール状態、およびアラートを無視します。詳細については、ルール状態の設定（24-21 ページ）を参照してください。 基本ポリシーまたは下位レイヤからルールのルール状態を継承したい場合は、ルール状態を [継承（Inherit）] に設定します。侵入ポリシーの [ルール（Rules）] ページで作業している場合は、ルール状態を [継承（Inherit）] に設定できないことに注意してください。 また、特定のレイヤについてルール状態の設定を [ルール（Rules）] ページで表示すると色分けされて表示されることにも留意してください。有効な状態が下位レイヤで設定されているルールは黄色で強調表示され、有効な状態が上位レイヤで設定されているルールは赤色で強調表示され、有効な状態が現在のレイヤで設定されている場合は強調表示されません。侵入ポリシーの [ルール（Rules）] ページはすべてのルール設定の最終的な効果の複合ビューであるため、ルール状態はこのページでは色分けされません。
1	しきい値 SNMP アラート	下位レイヤのルールの同じ種類の設定を上書きします。しきい値を設定すると、レイヤのルールの既存のしきい値が上書きされることに注意してください。詳細については、「イベントしきい値の設定（24-23 ページ）」と「SNMP アラートの追加（24-34 ページ）」を参照してください。
1 つ以上	抑制 レート ベースのルール状態	選択した各ルールの同じ種類の設定を、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせます。ルール状態が設定されているレイヤより下の設定は無視されます。詳細については、「侵入ポリシー単位の抑制の設定（24-28 ページ）」と「動的ルール状態の追加（24-31 ページ）」を参照してください。
1 つ以上	コメント	ルールにコメントを追加します。コメントは、ポリシー固有またはレイヤ固有ではなく、ルール固有です。任意のレイヤの 1 つのルールに 1 つ以上のコメントを追加できます。詳細については、ルールに関するルール コメントの追加（24-9 ページ）を参照してください。

たとえば、あるレイヤでルール状態を [ドロップしてイベントを生成する（Drop and Generate Events）] に設定し、それよりも上位のレイヤで [無効（Disabled）] に設定した場合、侵入ポリシーの [ルール（Rules）] ページには、ルールが無効であることが示されます。

別の例として、あるレイヤでルールの送信元ベースの抑制を 192.168.1.1 に設定し、別のレイヤでそのルールの宛先ベースの抑制を 192.168.1.2 に設定した場合、[ルール（Rules）] ページには、送信元アドレス 192.168.1.1 と宛先アドレス 192.168.1.2 に関するイベントを抑制する累積的な結果が示されます。抑制およびレート ベースのルール状態の設定では、選択した各ルールの同じ種類の設定が、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせられることに注意してください。ルール状態が設定されているレイヤより下の設定は無視されます。

レイヤでのルールの変更方法:

ステップ 1　侵入ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] を展開し、変更するポリシー レイヤを展開します。

ステップ 2　変更するポリシー レイヤのすぐ下にある [ルール（Rules）] をクリックします。

レイヤの [ルール（Rules）] ページが表示されます。

レイヤ ルールの設定の表のいずれかの設定を変更できます。侵入ルールの設定の詳細については、ルールを使用した侵入ポリシーの調整（24-1 ページ）を参照してください。

編集可能なレイヤから個々の設定を削除するには、そのレイヤの [ルール（Rules）] ページでルール メッセージをダブルクリックして、ルールの詳細を表示します。削除する設定の横にある [削除（Delete）] をクリックして [OK] を 2 回クリックします。

ステップ 3　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

マルチレイヤ ルール設定の削除

ライセンス：Protection

侵入ポリシーの [ルール（Rules）] ページで 1 つ以上のルールを選択し、侵入ポリシーの複数のレイヤから特定のタイプのイベント フィルタ、動的状態、またはアラートを同時に削除できます。

システムは、すべての設定を削除するか、ルール状態がルールに対して設定されているレイヤに遭遇するまで、下位方向にある各レイヤの同じ種類の設定を削除します。ルール状態が設定されているレイヤに遭遇したら、そのレイヤから設定を削除し、設定タイプの削除を停止します。

共有レイヤまたは基本ポリシーで同じタイプの設定に遭遇したときに、ポリシーの最上位のレイヤが編集可能である場合、システムはそのルールの残りの設定およびルール状態をその編集可能なレイヤにコピーします。そうではない場合、ポリシーの最上位のレイヤが共有レイヤであれば、システムは新しい編集可能なレイヤをその共有レイヤの上に作成し、そのルールの残りの設定およびルール状態をその編集可能なレイヤにコピーします。

（注）　共有レイヤまたは基本ポリシーから派生したルール設定を削除すると、下位レイヤまたは基本ポリシーからこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーからの変更を無視しないようにするには、最上位のレイヤのサマリ ページでルール状態を [継承（Inherit）] に設定します。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

複数のレイヤのルール設定を削除する方法:

ステップ 1　侵入ポリシーの編集中に、ナビゲーション パネルで [ポリシー情報（Policy Information）] のすぐ下にある [ルール（Rules）] をクリックします。

ヒント　また、任意のレイヤの [ルール（Rules）] ページでレイヤのドロップダウンリストから [ポリシー（Policy）] を選択するか、[ポリシー情報（Policy Information）] ページの [ルールの管理（Manage Rules）] を選択することもできます。

侵入ポリシーの [ルール（Rules）] ページが表示されます。

ステップ 2　複数の設定を削除するルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

ルールの検索については、侵入ポリシー内のルール フィルタリングについて（24-10 ページ）および侵入ポリシー内のルール フィルタの設定（24-19 ページ）を参照してください。

ステップ 3　次の選択肢があります。

- ルールのすべてのしきい値を削除するには、[イベント フィルタリング（Event Filtering）] > [しきい値の削除（Remove Thresholds）] を選択します。
- ルールのすべての抑制を削除するには、[イベント フィルタリング（Event Filtering）] > [抑制の削除（Remove Suppressions）] を選択します。
- ルールのすべてのレート ベースのルール状態を削除するには、[動的状態（Dynamic State）] > [レート ベースのルール状態の削除（Remove Rate-Based Rule States）] を選択します。
- ルールのすべての SNMP アラート設定を削除するには、[アラート（Alerting）] > [SNMP アラートの削除（Remove SNMP Alerts）] を選択します。

確認のポップアップ ウィンドウが表示されます。

（注）　共有レイヤまたは基本ポリシーから派生したルール設定を削除すると、下位レイヤまたは基本ポリシーからこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーからの変更を無視しないようにするには、最上位のレイヤのサマリ ページでルール状態を [継承（Inherit）] に設定します。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

ステップ 4　[OK] をクリックします。

システムは選択された設定を削除し、ルールの残りの設定をポリシーの最上位の編集可能なレイヤにコピーします。システムが残りの設定をコピーする方法に影響を与える条件については、この手順の概要を参照してください。

ステップ 5　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

カスタム基本ポリシーからのルール変更の受け入れ

ライセンス：Protection

レイヤを追加していないカスタム ネットワーク分析ポリシーまたは侵入ポリシーが別のカスタム ポリシーを基本ポリシーとして使用するとき、以下を行う場合は、そのルール状態を継承するようにルールを設定する必要があります。

- 基本ポリシーのルールに設定されたイベント フィルタ、動的状態、または SNMP アラートを削除する場合
- 基本ポリシーとして使用する他のカスタム ポリシー内のルールに行った後続の変更をルールが受け入れるようにする場合

次の手順では、これを実現する方法について説明します。レイヤを追加したポリシーでこれらのルールの設定を受け入れるには、マルチレイヤ ルール設定の削除（16-13 ページ）を参照してください。

レイヤを追加しなかったポリシー内でのルール変更を受け入れる方法:

ステップ 1　侵入ポリシーの編集中に、ナビゲーション パネルで [ポリシー層(Policy Layers)] リンクを展開し、[My Changes] リンクを展開します。

ステップ 2　[My Changes] のすぐ下にある [ルール(Rules)] リンクをクリックします。

My Changes レイヤの [ルール(Rules)] ページが表示されます。

ステップ 3　設定を受け入れるルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

ルールの検索については、侵入ポリシー内のルール フィルタリングについて(24-10 ページ)および侵入ポリシー内のルール フィルタの設定(24-19 ページ)を参照してください。

ステップ 4　[ルール状態(Rule State)] ドロップダウンリストから、[継承(Inherit)] を選択します。

ステップ 5　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

レイヤ内のプリプロセッサと詳細設定の設定

ライセンス:Protection

ネットワーク分析ポリシーでプリプロセッサを設定するときと、侵入ポリシーで詳細詳細を設定するときのメカニズムは同様です。プリプロセッサの有効化および無効化はネットワーク分析の [設定(Settings)] ページで行うことができ、侵入ポリシーの詳細設定の有効化および無効化は侵入ポリシーの [詳細設定(Advanced Settings)] ページで行うことができます。これらのページでは、すべての関連機能の有効な状態の概要も示されます。たとえば、ネットワーク分析 SSL プリプロセッサが、あるレイヤでは無効になっていて上位レイヤでは有効になっている場合、[設定(Settings)] ページにはプリプロセッサが有効であるとして表示されます。これらのページで行った変更は、ポリシーの最上位レイヤに表示されます。

また、プリプロセッサまたは詳細設定を有効化または無効化したり、ユーザ設定可能なレイヤのサマリ ページの設定ページにアクセスしたりできます。このページで、レイヤの名前および説明を変更し、レイヤを同じタイプの他のポリシーと共有するかどうかを設定できます。詳細については、ポリシー間のレイヤの共有(16-10 ページ)を参照してください。ナビゲーション パネルの [ポリシー層(Policy Layers)] の下のレイヤの名前を選択することによって、別のレイヤのサマリ ページに切り替えることができます。

プリプロセッサまたは詳細設定を有効にすると、その機能の設定ページへのサブリンクがナビゲーション パネルのレイヤの名前の下に表示され、編集アイコン( )がそのレイヤのサマリ ページの機能の横に表示されます。レイヤで機能を無効にしたり、[継承(Inherit)] に設定した場合はこれらは表示されません。

プリプロセッサまたは詳細設定の状態(有効または無効)を設定すると、下位レイヤでのその機能の状態と構成設定が上書きされます。プリプロセッサまたは詳細設定についてその状態と設定を基本ポリシーまたは下位レイヤから継承する場合、状態を [継承(Inherit)] に設定します。[設定(Settings)] または [詳細設定(Advanced Settings)] ページで操作するときには、[継承(Inherit)] の選択項目は使用できないことに注意してください。

各レイヤのサマリ ページに表示される色分けは、次のように有効な設定が上位レイヤ、下位レイヤ、または現在のレイヤにあることを示します。

- 赤色：有効な設定は上位レイヤにあります
- 黄色：有効な設定は下位レイヤにあります
- 陰影なし：有効な設定は現在のレイヤにあります

[設定（Settings）] および [詳細設定（Advanced Settings）] ページは、関連するすべての設定の複合ビューであるため、これらのページは有効な設定の位置を示すためにカラー コーディングを使用しません。

システムは、機能が有効にされている最上位レイヤの設定を使用します。設定を明示的に変更しなかった場合は、デフォルト設定が使用されます。たとえば、あるレイヤでネットワーク分析 DCE/RPC プリプロセッサを有効にして変更し、それより上位のレイヤでプリプロセッサを有効にするが変更はしない場合、システムは上位レイヤのデフォルト設定を使用します。

次の表に、ユーザ設定可能なレイヤのサマリ ページで実行できる操作を示します。

表 ***16-3***　レイヤのサマリ ページの操作

目的	操作
レイヤの名前または説明の変更	[名前（Name）] または [説明（Description）] の新しい値を入力します。
他の侵入ポリシーとのレイヤの共有	[他のポリシーによるこのレイヤの使用を許可（Allow this layer to be used by other policies）] を選択します。 詳細については、ポリシー間のレイヤの共有（16-10 ページ）を参照してください。
現在のレイヤのプリプロセッサ/詳細設定の有効化または無効化	機能の横にある [有効（Enabled）] または [無効（Disabled）] をクリックします。 有効にすると、設定ページへのサブリンクがナビゲーション パネルのレイヤ名の下に表示され、編集アイコン（  ）が機能の横のサマリ ページに表示されます。 無効にすると、サブリンクと編集アイコンが削除されます。
現在のレイヤの下にある最上位レイヤの設定からのプリプロセッサ/詳細設定の状態および設定の継承	[継承（Inherit）] をクリックします。 ページが更新され、機能を有効にした場合は、ナビゲーション パネルでの機能のサブリンクと編集アイコンは表示されなくなります。
有効なプリプロセッサ/詳細設定の設定ページへのアクセス	現在の設定を変更するには、編集アイコン（）または機能のサブリンクをクリックします。 Back Orifice プリプロセッサにはユーザ設定可能なオプションがないことに注意してください。

ユーザ レイヤのプリプロセッサ/詳細設定を変更する方法：

ステップ **1**　ポリシーの編集中に、ナビゲーション パネルで [ポリシー層（Policy Layers）] を展開し、変更するレイヤの名前をクリックします。

レイヤのサマリ ページが表示されます。

ステップ **2**　レイヤのサマリ ページの操作の表にある操作を実行できます。

ステップ **3**　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

トラフィックの前処理のカスタマイズ

アクセス コントロール ポリシーにおける詳細設定の多くは、設定のために特定の専門知識を要する侵入検知設定と予防設定を制御します。通常、詳細設定はほとんど、あるいはまったく変更する必要がありません。詳細設定は導入環境ごとに異なります。

この章では、次の設定を行う方法について説明します。

- 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（17-1 ページ）では、システムがトラフィックを検査する方法を正確に決定する前に、最初にそのトラフィックを検査するために使用される、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を変更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による前処理のカスタマイズ（17-3 ページ）では、一致するトラフィックを前処理するためのカスタム ネットワーク分析ポリシーを割り当てることで、特定のセキュリティ ゾーン、およびネットワークに対する特定のトラフィック前処理オプションを調整する方法を説明します。

他の章では、アクセス コントロール ポリシーに対するポリシー全体の前処理とパフォーマンスのオプションを説明します。詳細については、以下を参照してください。

- トランスポート/ネットワークの詳細設定の構成（21-1 ページ）
- パッシブ展開における前処理の調整（22-1 ページ）
- 侵入防御パフォーマンスの調整（10-6 ページ）
- 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（10-17 ページ）

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

ライセンス：任意

各アクセス コントロール ポリシーは、システムがトラフィックを検査する方法を正確に決定する前に、デフォルトの侵入ポリシーを使用してそのトラフィックを最初に検査します。これは、場合によってシステムがトラフィックを処理するアクセス コントロール ルール（存在する場合）を決定する前に、接続の最初の数パケットを処理し通過を許可する必要があるため必要となります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。

システムはクライアントとサーバの間で接続が完全に確立される前にアプリケーションを識別したり URL をフィルタ処理することはできないので、デフォルトの侵入ポリシーは、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に特に有用です。たとえば、パケッ

トがアプリケーションまたは URL 条件を持つアクセス コントロール ルールのその他のすべての条件に一致する場合、そのパケットと後続のパケットは、接続が確立されてアプリケーションまたは URL の識別が完了するまで通過することを許可されます。通常は 3 ～ 5 パケットです。

システムはこれらの許可されたパケットをデフォルトの侵入ポリシーで検査し、これによってイベントを生成したり、インラインで配置されている場合は、悪意のあるトラフィックをブロックできます。システムが接続を処理する必要があるアクセス コントロール ルールまたはデフォルト アクションを識別した後、接続内の残りのパケットが適宜処理され検査されます。

アクセス コントロール ポリシーを作成する場合、そのデフォルトの侵入ポリシーは最初に選択したデフォルト アクションによって異なります。アクセス コントロールの初期のデフォルト侵入ポリシーは次のとおりです。

- [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）]（システムによって提供されるポリシー）は、最初に [侵入防御（Intrusion Prevention）] デフォルト アクションを選択した場合のアクセス コントロール ポリシーのデフォルトの侵入ポリシーです。
- No Rules Active は、最初に [すべてのトラフィックをブロックする（Block all traffic）] デフォルト アクションを選択した場合のアクセス コントロール ポリシーのデフォルトの侵入ポリシーです。このオプションを選択すると、前述の許可されたパケットでの侵入インスペクションが無効になりますが、侵入データが必要なければ、パフォーマンスを向上できます。

（注）　侵入インスペクションを実行していない場合は、デフォルトの侵入ポリシーとして No Rules Active ポリシーを保持してください。詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（4-13 ページ）を参照してください。

アクセス コントロール ポリシーを作成後にデフォルト アクションを変更する場合は、デフォルトの侵入ポリシーが自動的に変更されないことに注意してください。手動で変更するには、アクセス コントロール ポリシーの詳細オプションを使用します。

アクセス コントロール ポリシーのデフォルト侵入ポリシーを変更するには、次の手順を実行します。

ステップ 1　デフォルトの侵入ポリシーを変更するアクセス コントロール ポリシーで、[詳細設定（Advanced）] タブを選択し、[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] セクションの横にある編集アイコン（）をクリックします。

[ネットワーク分析ポリシー（Network Analysis Policies）] ダイアログボックスが表示されます。

ステップ 2　[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）] ドロップダウンリストから、デフォルトの侵入ポリシーを選択します。システムによって作成されたポリシーまたはユーザが作成したポリシーを選択できます。

ユーザが作成したポリシーを選択した場合は、編集アイコン（）をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

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

ステップ 3　[OK] をクリックして変更を保存します。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。

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

ライセンス:任意

ネットワーク分析ポリシーは、特に侵入の試みの前兆となるかもしれない異常トラフィックに対し、そのトラフィックがさらに評価されるようにトラフィックをデコードおよび前処理する方法を制御します。このトラフィックの前処理は、セキュリティ インテリジェンスのブラックリスト登録の後に行われますが、侵入ポリシーがパケットを詳細に検査する前に行われます。デフォルトでは、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)] ネットワーク分析ポリシーは、アクセス コントロール ポリシーによって処理されるすべてのトラフィックに適用されます。

ヒント　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)] ネットワーク分析ポリシーおよび [バランスの取れたセキュリティと接続(Balanced Security and Connectivity)] 侵入ポリシーは共に機能し、侵入ルールの更新の際に両方とも更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。

前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。カスタム ネットワーク分析ポリシーの作成(18-2 ページ) を参照してください。使用可能な調整オプションは、プリプロセッサによって異なります。

複雑な環境での高度なユーザの場合は、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを別々に前処理するように調整することができます。そして、異なるセキュリティ ゾーンまたはネットワークを使用したトラフィックの前処理を制御するためにそれらのポリシーを使用するようにシステムを設定できます。

これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。各ルールに含まれる内容は、次のとおりです。

- 一連のルール条件。前処理の対象となる特定のトラフィックを識別します
- 関連付けられたネットワーク分析ポリシー。すべてのルールの条件を満たすトラフィックを前処理するために使用できます

システムがトラフィックを前処理するときに、パケットはルール番号の上位から下位の順序でネットワーク分析ルールに照合されます。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

(注)　プリプロセッサを無効にしているが、システムは有効になっている侵入ルールまたはプリプロセッサ ルールと照合して前処理されたパケットを評価する必要がある場合、システムはプリプロセッサを自動的に有効にして使用します。しかし、ネットワーク分析ポリシー インターフェイスでは無効のままです。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、高度なタスクです。前処理および侵入インスペクションは密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーが互いに補完することを許可する場合は慎重になる必要があります。詳細については、カスタム ポリシーに関する制約事項(15-12 ページ)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(17-4 ページ)
- ネットワーク分析ルールを使用して前処理するトラフィックの指定(17-4 ページ)
- ネットワーク分析ルールの管理(17-8 ページ)

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

ライセンス:任意

デフォルトでは、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)] ネットワーク分析ポリシーは、アクセス コントロール ポリシーによって処理されるすべてのトラフィックに適用されます。トラフィックの前処理オプションを調整するためにネットワーク分析ルールを追加する場合は、デフォルトのネットワーク分析ポリシーがそのルールで処理されないすべてのトラフィックを前処理します。

アクセス コントロール ポリシーの詳細設定によって、このデフォルト ポリシーを変更することができます。

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するには、次の手順を実行します。

ステップ **1**　デフォルトのネットワーク分析ポリシーを変更するアクセス コントロール ポリシーで、[詳細設定(Advanced)] タブを選択し、[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] セクションの横にある編集アイコン( )をクリックします。

[ネットワーク分析ポリシー(Network Analysis Policies)] ダイアログボックスが表示されます。

ステップ **2**　[デフォルトのネットワーク分析ポリシー(Default Network Analysis Policy)] ドロップダウンリストから、デフォルトのネットワーク分析ポリシーを選択します。システムによって作成されたポリシーまたはユーザが作成したポリシーを選択できます。

ユーザが作成したポリシーを選択した場合は、編集アイコン( )をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

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

ステップ **3**　[OK] をクリックして変更を保存します。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。

ネットワーク分析ルールを使用して前処理するトラフィックの指定

ライセンス:任意

アクセス コントロール ポリシーの詳細設定で、ネットワーク分析ルールを使用してネットワーク トラフィックへの前処理設定を調整できます。アクセス コントロール ルールと同様に、ネットワーク分析ルールには 1 から始まる番号が付いています。

システムがトラフィックを前処理するときに、パケットはルール番号の昇順で上から順にネットワーク分析ルールに照合され、すべてのルールの条件が一致する最初のルールに従ってトラフィックが前処理されます。次の表に、ルールに追加できる条件を示します。

表 **17-1**　ネットワーク分析ルール条件のタイプ

条件	トラフィックの照合	詳細
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、ゾーンごとのトラフィックの前処理(17-6 ページ)を参照してください。

表 **17-1**　ネットワーク分析ルール条件のタイプ（続き）

条件	トラフィックの照合	詳細
ネットワーク	その送信元または宛先 IP アドレスによる	IP アドレスを明示的に指定できます。ネットワーク条件を作成するには、ネットワークごとのトラフィックの前処理（17-7 ページ）を参照してください。

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ゾーン条件を持たないルールは、その入力または出力インターフェイスに関係なく、送信元または宛先 IP アドレスに基づいてトラフィックを評価します。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。

カスタム ネットワーク分析ルールを追加するには、次の手順を実行します。

ステップ **1**　カスタム前処理設定を作成するアクセス コントロール ポリシーで、[詳細設定（Advanced）] タブを選択して、[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] セクションの横にある編集アイコン（ ）をクリックします。

[ネットワーク分析ポリシー（Network Analysis Policies）] ダイアログボックスが表示されます。カスタム ネットワーク分析ルールを追加していない場合、モジュール インターフェイスにはカスタム ルールがないことが示され、追加している場合は、設定している数が表示されます。

ヒント　新しいウィンドウで [ネットワーク分析ポリシー（Network Analysis Policies）] ページを表示するには、[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。このページは、カスタム ネットワーク分析ポリシーを表示および編集するために使用します。ネットワーク分析ポリシーの管理（18-3 ページ）を参照してください。

ステップ **2**　[ネットワーク分析ルール（Network Analysis Rules）] の横にある、所持しているカスタム ルールの数を示したステートメントをクリックします。

ダイアログボックスが展開され、カスタム ルールが表示されます（ある場合）。

ステップ **3**　[ルールの追加（Add Rule）] をクリックします。

ネットワーク分析ルール エディタが表示されます。

ステップ **4**　ルールの条件を作成します。次の基準を使用して、NAP の前処理を制限できます。

- ゾーンごとのトラフィックの前処理（17-6 ページ）
- ネットワークごとのトラフィックの前処理（17-7 ページ）

ステップ **5**　[ネットワーク分析（Network Analysis）] タブをクリックし、[ネットワーク分析ポリシー（Network Analysis Policy）] ドロップダウンリストからポリシーを選択することによって、ネットワーク分析ポリシーをルールに関連付けます。

システムは、ユーザが選択したネットワーク分析ポリシーを使用して、すべてのルールの条件を満たすトラフィックを前処理します。ユーザが作成したポリシーを選択した場合は、編集アイコン（ ）をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

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

ステップ 6　[追加(Add)] をクリックします。

このルールは他のルールの後に追加されます。ルールの評価順序を変更する場合は、ネットワーク分析ルールの管理(17-8 ページ)を参照してください。

ゾーンごとのトラフィックの前処理

ライセンス:任意

ネットワーク分析ルール内のゾーン条件によって、その送信元および宛先セキュリティ ゾーン別にトラフィックを前処理することができます。セキュリティ ゾーンは 1 つ以上のインターフェイスのグループです。ゾーン作成の詳細については、セキュリティ ゾーンの操作(2-37 ページ)を参照してください。

1 つのゾーン条件で [送信元ゾーン(Source Zones)] および [宛先ゾーン(Destination Zones)] それぞれに対し、最大 50 のゾーンを追加できます。

- ゾーン内のインターフェイスからデバイスから発信するトラフィックを照合するには、そのゾーンを [宛先ゾーン(Destination Zones)] に追加します。パッシブに展開されたデバイスはトラフィックを送信しないので、宛先ゾーン条件でパッシブ インターフェイスから構成されるゾーンは使用できないことに注意してください。
- ゾーン内のインターフェイスからデバイスに着信するトラフィックを照合するには、そのゾーンを [送信元ゾーン(Source Zones)] に追加します。

送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

警告アイコン(⚠)は、インターフェイスが含まれていないゾーンなどの無効な設定を示します。詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング(4-13 ページ)を参照してください。

ゾーン別にトラフィックを前処理するには、次の手順を実行します。

ステップ 1　ゾーン別にトラフィックを前処理するアクセス コントロール ポリシーで、新しいネットワーク分析ルールを作成するか、または既存のルールを編集します。

詳細な手順については、ネットワーク分析ルールを使用して前処理するトラフィックの指定(17-4 ページ)を参照してください。

ステップ 2　ネットワーク分析ルール エディタで、[ゾーン(Zones)] タブを選択します。

[ゾーン(Zones)] タブが表示されます。

ステップ 3　[利用可能なゾーン(Available Zones)] から追加するゾーンを見つけて選択します。

追加するゾーンを検索するには、[利用可能なゾーン(Available Zones)] リストの上にある [名前で検索(Search by name)] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

クリックすると、ゾーンを選択できます。複数のゾーンを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択(Select All)] を選択します。

ステップ 4　[送信元に追加(Add to Source)] または [宛先に追加(Add to Destination)] をクリックして、選択したゾーンを適切なリストに追加します。

選択したゾーンをドラッグ アンド ドロップすることもできます。

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。設定変更の展開(4-12 ページ) を参照してください。

ネットワークごとのトラフィックの前処理

ライセンス:任意

ネットワーク分析ルール内のネットワーク条件によって、その送信元および宛先 IP アドレス別にトラフィックを前処理することができます。前処理するトラフィックに対し送信元と宛先 IP アドレスを手動で指定でき、または、再利用可能で名前を 1 つ以上の IP アドレスおよびアドレスブロックに関連付けるネットワーク オブジェクトでネットワーク条件を設定できます。

ヒント　ネットワーク オブジェクトを作成した後、それを使用して、ネットワーク分析ルールを作成するだけでなく、システムのモジュール インターフェイスの他のさまざまな場所で IP アドレスを表すことができます。これらのオブジェクトはオブジェクト マネージャを使用して作成できます。また、ネットワーク分析ルールの設定時にネットワーク オブジェクトをオンザフライで作成することもできます。詳細については、ネットワーク オブジェクトの操作（2-4 ページ）を参照してください。

1 つのネットワーク条件で [送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] それぞれに対し、最大 50 の項目を追加できます。

- IP アドレスからのトラフィックを照合するには、[送信元ネットワーク（Source Networks）] を設定します。
- IP アドレスへのトラフィックを照合するには、[宛先ネットワーク（Destination Networks）] を設定します。

送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

ネットワーク条件を作成する際、警告アイコン（⚠）は無効な設定を示します。詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（4-13 ページ）を参照してください。

ネットワーク別にトラフィックを前処理するには、次の手順を実行します。

ステップ 1　ネットワーク別にトラフィックを前処理するアクセス コントロール ポリシーで、新しいネットワーク分析ルールを作成するか、または既存のルールを編集します。

詳細な手順については、ネットワーク分析ルールを使用して前処理するトラフィックの指定（17-4 ページ）を参照してください。

ステップ 2　ネットワーク分析ルール エディタで、[ネットワーク（Networks）] タブを選択します。

[ネットワーク（Networks）] タブが表示されます。

ステップ 3　[利用可能なネットワーク（Available Networks）] から、次のように追加するネットワークを見つけて選択します。

- ここでネットワーク オブジェクトを作成してリストに追加するには、[利用可能なネットワーク（Available Networks）] リストの上にある追加アイコン（⊕）をクリックし、ネットワーク オブジェクトの操作（2-4 ページ）の手順に従います。
- 追加するネットワークを検索するには、[利用可能なネットワーク（Available Networks）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

ステップ 4　[送信元に追加(Add to Source)] または [宛先に追加(Add to Destination)] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 5　手動で指定する送信元または宛先 IP アドレスまたはアドレス ブロックを追加します。

[送信元ネットワーク(Source Networks)] リストまたは [宛先ネットワーク(Destination Networks)] リストの下にある [IP アドレスの入力(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 [追加(Add)] をクリックします。

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。設定変更の展開(4-12 ページ) を参照してください。

ネットワーク分析ルールの管理

ライセンス:任意

ネットワーク分析ルールは、これらの条件に一致するトラフィックを前処理する方法を指定する設定および条件の単純なセットにすぎません。既存のアクセス コントロール ポリシーの詳細オプションでネットワーク分析ルールを作成および編集します。各ルールは 1 つのポリシーにのみ属します。

カスタム ネットワーク分析ルールを編集するには、次の手順を実行します。

ステップ 1　カスタム前処理設定を変更するアクセス コントロール ポリシーで、[詳細設定(Advanced)] タブを選択して、[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] セクションの横にある編集アイコン( )をクリックします。

[ネットワーク分析ポリシー(Network Analysis Policies)] ダイアログボックスが表示されます。カスタム ネットワーク分析ルールを追加していない場合、モジュール インターフェイスにはカスタム ルールがないことが示され、追加している場合は、設定している数が表示されます。

ステップ 2　[ネットワーク分析ルール(Network Analysis Rules)] の横にある、所持しているカスタム ルールの数を示したステートメントをクリックします。

ダイアログボックスが展開され、カスタム ルールが表示されます(ある場合)。

ステップ 3　カスタム ルールを編集します。次の選択肢があります。

- ルールの条件を編集する、またはルールによって呼び出されるネットワーク分析ポリシーを変更するには、ルールの横にある編集アイコン( )をクリックします。
- ルールの評価順序を変更するには、ルールをクリックして正しい位置にドラッグします。複数のルールを選択するには、Shift キーおよび Ctrl キーを使用します。
- ルールを削除するには、ルールの横にある削除アイコン( )をクリックします。

ステップ 4　[OK] をクリックして変更を保存します。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。設定変更の展開(4-12 ページ) を参照してください。

ネットワーク分析ポリシーの開始

ネットワーク分析ポリシーは、多数のトラフィックの前処理オプションを制御し、アクセス コントロール ポリシーの詳細設定で呼び出されます。ネットワーク分析に関する前処理は、セキュリティ インテリジェンスのブラックリスト登録の後に行われますが、アクセス コントロール ルールがパケットを詳細に検査する前、および侵入インスペクションまたはファイル インスペクションが開始される前に行われます。

デフォルトでは、システムは *Balanced Security and Connectivity* ネットワーク分析ポリシーを使用して、アクセス コントロール ポリシーによって処理されるすべてのトラフィックを前処理します。ただし、この前処理を実行するために別のデフォルトのネットワーク分析ポリシーを選択できます。便宜を図るため、システムによっていくつかの変更不可能なネットワーク分析ポリシーが提供されます。これらのポリシーは、脆弱性調査チーム（VRT）によってセキュリティおよび接続の一定のバランスがとれるように調整されています。カスタム前処理設定を使用して、このデフォルト ポリシーをカスタム ネットワーク分析ポリシーと置き換えることもできます。

ヒント　システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。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（15-1 ページ）には、ネットワーク分析ポリシーと侵入ポリシーが連携してトラフィックを検査するしくみの概要、およびナビゲーション パネルの使用、競合の解決、変更のコミットに関する基本事項が記載されています。

また、複数のカスタム ネットワーク分析ポリシーを作成し、別のトラフィックを前処理するように割り当てることで、特定のセキュリティ ゾーンおよびネットワークに対するトラフィックの前処理オプションを調整することもできます。

（注）　前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、高度なタスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する必要があります。システムは、ユーザのポリシーを調整せず、設定ミスの際はデフォルトのオプションを使用します。詳細については、カスタム ポリシーに関する制約事項（15-12 ページ）を参照してください。

この章では、単純なカスタム ネットワーク分析ポリシーを作成する方法について説明します。この章には、ネットワーク分析ポリシーの管理（編集、比較など）に関する基本情報も含まれています。詳細については、以下を参照してください。

- インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（18-6 ページ）
- 現在のネットワーク分析設定のレポートの生成（18-10 ページ）
- 2 つのネットワーク分析ポリシーまたはリビジョンの比較（18-11 ページ）

カスタム ネットワーク分析ポリシーの作成

ライセンス：任意

新しいネットワーク分析ポリシーを作成するときは、一意の名前を付け、基本ポリシーを指定し、インライン モードを選択する必要があります。

基本ポリシーはネットワーク分析ポリシーのデフォルト設定を定義します。新しいポリシーの設定の変更は、基本ポリシーの設定を変更するのではなく、オーバーライドします。システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。詳細については、基本レイヤについて（16-2 ページ）を参照してください。

ネットワーク分析ポリシーのインライン モードでは、プリプロセッサでトラフィックを変更（正規化）したりドロップしたりして、攻撃者が検出を回避する可能性を最小限にすることができます。パッシブな展開では、インライン モードに関係なく、システムはトラフィック フローに影響を与えることができないことに注意してください。詳細については、インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（18-6 ページ）を参照してください。

ネットワーク分析ポリシーを作成するには、次の手順を実行します。

ステップ 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ 6　[ポリシーの作成（Create Policy）] をクリックします。

別のポリシー内に未保存の変更が存在する場合は、[ネットワーク分析ポリシー（Network Analysis Policy）] ページに戻るかどうか尋ねられたときに [キャンセル（Cancel）] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ネットワーク分析ポリシーの作成（Create Network Analysis Policy）] ポップアップ ウィンドウが表示されます。

ステップ 7　[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。

ステップ 8　[基本ポリシー(Base Policy)] で最初の基本ポリシーを指定します。

基本ポリシーとしてシステムによって提供されるポリシーまたはカスタム ポリシーを使用できます。

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

ステップ 9　プリプロセッサがインライン展開でトラフィックに影響を与えるようにするかどうかを指定します。

- プリプロセッサがトラフィックに影響を与えるようにするには、[インライン モード(Inline Mode)] を有効にします。
- プリプロセッサがトラフィックに影響を与えないようにするには、[インライン モード(Inline Mode)] を無効にします。

ステップ 10　ポリシーを作成します。

- 新しいポリシーを作成して [ネットワーク分析ポリシー(Network Analysis Policy)] ページに戻るには、[ポリシーの作成(Create Policy)] をクリックします。新しいポリシーには基本ポリシーと同じ設定項目が含まれています。
- ポリシーを作成し、高度なネットワーク分析ポリシー エディタでそれを開いて編集するには、[ポリシーの作成と編集(Create and Edit Policy)] をクリックします(ネットワーク分析ポリシーの編集(18-4 ページ) を参照)。

ネットワーク分析ポリシーの管理

ライセンス:任意

[ネットワーク分析ポリシー(Network Analysis Policy)] ページで、現在のカスタム ネットワーク分析ポリシーを次の情報とともに確認できます。

- ポリシーが最後に変更された日時(ローカル時間)とそれを変更したユーザ
- プリプロセッサがトラフィックに影響を与えることを許可する [インライン モード(Inline Mode)] 設定が有効になっているかどうか
- トラフィックを前処理するためにアクセス コントロール ポリシーがどのネットワーク分析ポリシーを使用しているか
- ポリシーに保存されていない変更があるかどうか、およびポリシーを現在編集している人(いれば)に関する情報

[ネットワーク分析ポリシー(Network Analysis Policy)] ページのオプションを使用することで、次の表にあるアクションを実行できます。

表 *18-1*　ネットワーク分析ポリシーの管理操作

目的	操作	参照先
新しいネットワーク分析ポリシーを作成する	[ポリシーの作成(Create Policy)] をクリックします。	カスタム ネットワーク分析ポリシーの作成(18-2 ページ)。
既存のネットワーク分析ポリシーを編集する	編集アイコン( )をクリックします。	ネットワーク分析ポリシーの編集(18-4 ページ)。

表 18-1　ネットワーク分析ポリシーの管理操作（続き）

目的	操作	参照先
ネットワーク分析ポリシー内の現在の構成設定がリストされた PDF レポートを表示する	レポート アイコン（  ）をクリックします。	現在のネットワーク分析設定のレポートの生成（18-10 ページ）
2 つのネットワーク分析ポリシーまたは同じポリシーの 2 つのリビジョンの設定を比較する	[ポリシーの比較（Compare Policies）] をクリックします。	2 つのネットワーク分析ポリシーまたはリビジョンの比較（18-11 ページ）。
ネットワーク分析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。アクセス コントロール ポリシーが参照しているネットワーク分析ポリシーは削除できません。	

ネットワーク分析ポリシーの編集

ライセンス：任意

新しいネットワーク分析ポリシーを作成すると、そのポリシーには基本ポリシーと同じ設定が付与されます。次の表に、ニーズに合わせて新しいポリシーを調整するために実行できる最も一般的な操作を示します。

表 18-2　ネットワーク分析ポリシーの編集操作

目的	操作	参照先
プリプロセッサがトラフィックを編集またはドロップすることを許可する	[ポリシー情報（Policy Information）] ページで [インライン モード（Inline Mode）] チェック ボックスをオンにします。	インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（18-6 ページ）
基本ポリシーを変更する	[ポリシー情報（Policy Information）] ページの [基本ポリシー（Base Policy）] ドロップダウン リストから、基本ポリシーを選択します。	基本ポリシーの変更（16-4 ページ）
基本ポリシーの設定を表示する	[ポリシー情報（Policy Information）] ページで [基本ポリシーの管理（Manage Base Policy）] をクリックします。	基本レイヤについて（16-2 ページ）
プリプロセッサの設定を有効化、無効化、または編集する	ナビゲーション パネルで [設定（Settings）] をクリックします。	ネットワーク分析ポリシーでのプリプロセッサの設定（18-7 ページ）
ポリシー層を管理する	ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。	ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）

ネットワーク分析ポリシーの調整時、特にプリプロセッサを無効化するときは、プリプロセッサおよび侵入ルールによっては、トラフィックを特定の方法で最初にデコードまたは前処理する必要があることに留意してください。必要なプリプロセッサを無効にすると、システムは現在の設定で自動的にプリプロセッサを使用しますが、ネットワーク分析ポリシーのモジュール インターフェイスではプリプロセッサは無効のままになります。

（注）　前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する必要があります。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、高度なタスクです。詳細については、カスタム ポリシーに関する制約事項（15-12 ページ）を参照してください。

システムは、ユーザごとに 1 つのネットワーク分析ポリシーをキャッシュします。ネットワーク分析ポリシーの編集中に、任意のメニューまたは別のページへの他のパスを選択した場合、変更内容はそのページを離れてもシステム キャッシュにとどまります。上の表に示す実行可能な操作の他に、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（15-1 ページ）では、ナビゲーション パネルの使用、競合の解決、および変更のコミットに関する情報を記載しています。

ネットワーク分析ポリシーを編集するには、次の手順を実行します。

ステップ 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ 6　設定するネットワーク分析ポリシーの横にある編集アイコン（）をクリックします。

ネットワーク分析ポリシー エディタが表示され、[ポリシー情報（Policy Information）] ページがフォーカスされ、左側にナビゲーション パネルが配置されます。

ステップ 7　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。

ステップ 8　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する

ライセンス:任意

インライン展開では、プリプロセッサによってはトラフィックを変更およびブロックできます。次に例を示します。

- インライン正規化プリプロセッサは、パケットを正規化し、他のプリプロセッサおよび侵入ルール エンジンで分析されるようにパケットを準備します。また、プリプロセッサの [回復不能な TCP ヘッダーの異常をブロック(Block Unrecoverable TCP Header Anomalies)] および [これらの TCP オプションを許可(Allow These TCP Options)] オプションを使用して、特定のパケットをブロックすることもできます。詳細については、インライン トラフィックの正規化(21-6 ページ)を参照してください。
- システムは無効なチェックサムを持つパケットをドロップできます。チェックサムの検証(21-5 ページ)を参照してください。
- システムはレート ベースの攻撃防御設定に一致するパケットをドロップできます。レートベース攻撃の防止(25-10 ページ)を参照してください。

ネットワーク分析ポリシーで設定したプリプロセッサがトラフィックに影響を与えるようにするには、プリプロセッサを有効にして正しく設定し、さらにデバイスをインラインで正しく展開する必要があります。最後に、ネットワーク分析ポリシーの [インライン モード(Inline Mode)] 設定を有効にする必要があります。

実際にトラフィックを変更せずに、設定がインライン展開でどのように機能するかを評価する場合は、インライン モードを無効にできます。パッシブ展開では、インライン モードに関係なくシステムはトラフィックに影響を与えられないことに注意してください。

ヒント　インライン展開では、シスコはインライン モードを有効にし、[TCP ペイロードの正規化(Normalize TCP Payload)] オプションを有効にしたままインライン正規化プリプロセッサを設定することを推奨しています。パッシブ展開の場合、シスコは、適応型プロファイルを設定することを推奨しています。

プリプロセッサがインライン展開でトラフィックに影響を与えることを許可するには、次の手順を実行します。

ステップ 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定(Advanced)] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] の横にある編集アイコン( )をクリックします。

[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] をクリックします。

[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン( )をクリックします。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 7　プリプロセッサがトラフィックに影響を与えるようにするかどうかを指定します。

- プリプロセッサがトラフィックに影響を与えるようにするには、[インライン モード(Inline Mode)] を有効にします。
- プリプロセッサがトラフィックに影響を与えないようにするには、[インライン モード(Inline Mode)] を無効にします。

ステップ 8　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

ネットワーク分析ポリシーでのプリプロセッサの設定

ライセンス:任意

プリプロセッサは、トラフィックを正規化し、プロトコルの異常を識別することで、トラフィックの詳細な検査に備えます。プリプロセッサは、ユーザが設定したプリプロセッサ オプションをパケットがトリガーしたときに、プリプロセッサ イベントを生成します。デフォルトで有効になるプリプロセッサや、それぞれのデフォルト設定は、ネットワーク分析ポリシーの基本ポリシーに応じて決まります。

ネットワーク分析ポリシーのナビゲーション パネルで [設定(Settings)] を選択すると、ポリシーによりタイプ別のプリプロセッサがリストされます。[設定(Settings)] ページで、ネットワーク分析ポリシーのプリプロセッサを有効または無効にしたり、プリプロセッサの設定ページにアクセスしたりできます。

プリプロセッサを設定するには、それを有効にする必要があります。プリプロセッサを有効にすると、そのプリプロセッサに関する設定ページへのサブリンクがナビゲーション パネル内の [設定(Settings)] リンクの下に表示され、この設定ページへの [編集(Edit)] リンクが [設定(Settings)] ページのプリプロセッサの横に表示されます。

ヒント　プリプロセッサの設定を基本ポリシーの設定に戻すには、プリプロセッサ設定ページで [デフォルトに戻す(Revert to Defaults)] をクリックします。プロンプトが表示されたら、復元することを確認します。

プリプロセッサを無効にすると、サブリンクと [編集(Edit)] リンクは表示されなくなりますが、設定は保持されます。特定の分析を実行するには、多くのプリプロセッサおよび侵入ルールで、トラフィックをまず特定の方法でデコードまたは前処理する必要があることに注意してください。必要なプリプロセッサを無効にすると、システムは現在の設定で自動的にプリプロセッサを使用しますが、ネットワーク分析ポリシーのモジュール インターフェイスではプリプロセッサは無効のままになります。

（注）　多くの場合、プリプロセッサの設定には特定の専門知識が必要で、通常は、ほとんどあるいはまったく変更を必要としません。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、高度なタスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する必要があります。詳細については、カスタム ポリシーに関する制約事項（15-12 ページ）を参照してください。

プリプロセッサの設定を変更するには、その設定とネットワークへの潜在的影響を理解する必要があります。次の各項には、プリプロセッサごとの固有の設定詳細情報へのリンクがあります。

アプリケーション層プリプロセッサ

アプリケーション層プロトコル デコーダは、特定のタイプのパケット データを、侵入ルール エンジンで分析できる形式に正規化します。

表 ***18-3***　　アプリケーション層プリプロセッサの設定

設定	参照先
DCE/RPC の設定	DCE/RPC トラフィックのデコード（19-2 ページ）
DNS の設定	DNS ネーム サーバ応答におけるエクスプロイトの検出（19-16 ページ）
FTP および Telnet の設定	FTP および Telnet トラフィックのデコード（19-20 ページ）
HTTP の設定	HTTP トラフィックのデコード（19-34 ページ）
Sun RPC の設定	Sun RPC プリプロセッサの使用（19-51 ページ）
SIP の設定	Session Initiation Protocol のデコード（19-53 ページ）
GTP コマンド チャネルの設定	GTP コマンド チャネルの設定（19-58 ページ）
IMAP の設定	IMAP トラフィックのデコード（19-59 ページ）
POP の設定	POP トラフィックのデコード（19-63 ページ）
SMTP の設定	SMTP トラフィックのデコード（19-66 ページ）
SSH の設定	SSH プロプロセッサによるエクスプロイトの検出（19-74 ページ）
SSL の設定	SSL プリプロセッサの使用（19-78 ページ）

SCADA プリプロセッサ

Modbus と DNP3 のプリプロセッサは、トラフィックの異常を検出し、インスペクションのためにデータを侵入ルール エンジンに提供します。

表 ***18-4***　　***SCADA*** プリプロセッサの設定

設定	参照先
Modbus の設定	Modbus プリプロセッサの設定（20-1 ページ）
DNP3 の設定	DNP3 プリプロセッサの設定（20-3 ページ）

トランスポート層/ネットワーク層プリプロセッサ

ネットワーク層とトランスポート層のプリプロセッサは、ネットワーク層とトランスポート層でエクスプロイトを検出します。パケットがプリプロセッサに送信される前に、パケット デコーダにより、パケット ヘッダーとペイロードが、プリプロセッサや侵入ルール エンジンで簡単に使用できる形式に変換されます。また、パケット ヘッダー内でさまざまな異常動作が検出されます。

表 *18-5*　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

設定	参照先
チェックサム検証	チェックサムの検証（21-5 ページ）
インライン正規化	インライン トラフィックの正規化（21-6 ページ）
IP 最適化	IP パケットの最適化（21-12 ページ）
パケットのデコード	パケットのデコードについて（21-17 ページ）
TCP ストリームの設定	TCP ストリームの前処理の使用（21-21 ページ）
UDP ストリームの設定	UDP ストリームの前処理の使用（21-33 ページ）

一部のトランスポートおよびネットワーク プリプロセッサの詳細設定は、アクセス コントロール ポリシーを適用するすべてのネットワークおよびゾーンにグローバルに適用されることに注意してください。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。トランスポート/ネットワークの詳細設定の構成（21-1 ページ）を参照してください。

特定の脅威の検出

Back Orifice プリプロセッサは、Back Orifice マジック クッキーについて UDP トラフィックを分析します。スキャン アクティビティを報告するようにポートスキャン ディテクタを設定できます。レート ベースの攻撃防御は、ネットワークを圧迫することを意図した SYN フラッドや膨大な同時接続からネットワークを保護するのに役立ちます。

表 *18-6*　特定の脅威の検出の設定

設定	参照先
Back Orifice の検出	Back Orifice の検出（25-1 ページ）
ポートスキャン検出	ポートスキャンの検出（25-3 ページ）
レート ベースの攻撃防御	レート ベース攻撃の防止（25-10 ページ）

侵入ポリシーで、ASCII テキストのクレジット カード番号や社会保障番号などのセンシティブ データを検出するセンシティブ データ プリプロセッサを設定することに注意してください。詳細については、センシティブ データの検出（25-21 ページ）を参照してください。

現在のネットワーク分析設定のレポートの生成

ライセンス：任意

ネットワーク分析ポリシー レポートは、特定の時点でのポリシー設定の記録です。システムは、基本ポリシー内の設定とポリシー層の設定を統合して、基本ポリシーに起因する設定とポリシー層に起因する設定を区別しません。

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 *18-7*　ネットワーク分析ポリシー 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。また、インライン正規化を有効にできるかどうか、現在のルール更新のバージョン、および基本ポリシーが現在のルール更新にロックされているかどうかも示されます。
設定	有効なすべてのプリプロセッサの設定とその構成を表示します。

また、2 つのネットワーク分析ポリシーや同じポリシーの 2 つのリビジョンを比較する比較レポートを生成することもできます。詳細については、2 つのネットワーク分析ポリシーまたはリビジョンの比較（18-11 ページ）を参照してください。

ネットワーク分析ポリシー レポートを表示するには、次の手順を実行します。

ステップ 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ 6　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。ネットワーク分析ポリシー レポートを生成する前に、必ず変更をコミットしてください。コミットされた変更だけがレポートに表示されます。

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。

2 つのネットワーク分析ポリシーまたはリビジョンの比較

ライセンス:任意

組織の標準に準拠しているかを確認する目的や、システム パフォーマンスを最適化する目的でポリシーの変更を検討するために、2 つのネットワーク分析ポリシーの相違点を調べることができます。2 つのネットワーク分析ポリシーまたは同じネットワーク分析ポリシーの 2 つのリビジョンを比較できます。比較した後に、必要に応じて、2 つのポリシーまたはポリシー リビジョン間の違いを記録した PDF レポートを生成できます。

ネットワーク分析ポリシーまたはポリシーのリビジョンを比較するために使用できる、次の 2 つのツールがあります。

- 比較ビューは、2 つのネットワーク分析ポリシーまたはネットワーク分析ポリシー リビジョン間の差異のみを横並び形式で表示します。各ポリシーまたはポリシー リビジョンの名前が比較ビューの左右のタイトル バーに表示されます。

  これを使用して、モジュール インターフェイスで差異を強調表示したまま、両方のポリシーのリビジョンを表示したり移動したりできます。

- 比較レポートは、2 つのネットワーク分析ポリシーまたはネットワーク分析ポリシー リビジョン間の差異のみを記録しています。これは PDF 形式であるという以外は、ネットワーク分析ポリシー レポートと類似した形式です。

  これを使用して、ポリシーの比較を保存、コピー、出力、共有して、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。

- ネットワーク分析ポリシー比較ビューの使用（18-11 ページ）
- ネットワーク分析ポリシー比較レポートの使用（18-12 ページ）

ネットワーク分析ポリシー比較ビューの使用

ライセンス:任意

比較ビューは、両方のポリシーまたはポリシー リビジョンを横並び形式で表示します。各ポリシーまたはポリシー リビジョンは、比較ビューの左右のタイトル バーに表示される名前で見分けます。ポリシー名とともに、最後に変更された時刻と、最後に変更したユーザが表示されます。

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 18-8　ネットワーク分析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、ネットワーク分析ポリシー比較レポートの使用 (18-12 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 つのポリシーまたはポリシー リビジョン間の差異のみをリストする PDF ドキュメントを作成します。

ネットワーク分析ポリシー比較レポートの使用

ライセンス:任意

ネットワーク分析ポリシー比較レポートは、ネットワーク分析ポリシー比較ビューで特定された 2 つネットワーク分析ポリシー間または同じネットワーク分析ポリシーの 2 つのリビジョン間のすべての差異の記録を示す、PDF 形式のレポートです。このレポートを使用して、2 つのネットワーク分析ポリシーの設定の間の差異をさらに調べ、その結果を保存して配信することができます。

ネットワーク分析ポリシー比較レポートは、アクセス可能な任意のポリシーに関して、比較ビューから生成できます。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。ネットワーク分析ポリシー比較レポートは、表 18-7 (18-10 ページ)に記載されているセクションで構成されます。

ヒント　同様の手順を使用して、アクセス コントロール ポリシー、侵入ポリシー、またはファイル ポリシーを比較できます。

2 つのネットワーク分析ポリシーまたはポリシー リビジョンを比較するには、次の手順を実行します。

ステップ 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定(Advanced)] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（ ）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ 6　[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。

ステップ 7　[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。

- 同じポリシーの 2 つのリビジョンを比較するには、[その他のリビジョン（Other Revision）] を選択します。

  ページが更新され、[ポリシー（Policy）]、[（リビジョン A（Revision A）] および [リビジョン B（Revision B）] ドロップダウン リストが表示されます。

ステップ 8　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。
- 同じポリシーの 2 つのリビジョンを比較する場合は、[ポリシー（Policy）] を選択し、[リビジョン A（Revision A）] および [リビジョン B（Revision B）] ドロップダウン リストから、比較するタイムスタンプ付きリビジョンを選択します。

ステップ 9　ポリシー比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ 10　必要に応じて、ネットワーク分析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。

ネットワーク分析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。

アプリケーション層プリプロセッサの使用

ネットワーク分析ポリシーにアプリケーション層プリプロセッサを設定します。これにより、侵入ポリシーで有効になっているルールを使った検査に向けてトラフィックが準備されます。詳細については、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（15-1 ページ）を参照してください。

アプリケーション層プロトコルにより、同一データをさまざまな方法で表すことができます。シスコは、特定タイプのパケット データを侵入ルール エンジンが分析可能なフォーマットに正規化する、アプリケーション層プロトコル デコーダを提供しています。アプリケーション層プロトコル エンコードを正規化することにより、ルール エンジンでさまざまなデータ形式のパケットに同じコンテンツ関連ルールを効果的に適用し、有意な結果を得ることができます。

ほとんどの場合、侵入ルールで関連するプリプロセッサ ルールが有効になっていないと、プリプロセッサはイベントを生成しません。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

詳細については、次の各項を参照してください。

- DCE/RPC トラフィックのデコード（19-2 ページ）では、DCE/RPC プリプロセッサについて説明し、回避の試行を防いで DCE/RPC トラフィックでの異常を検出するようにプリプロセッサを設定する方法を説明します。
- DNS ネーム サーバ応答におけるエクスプロイトの検出（19-16 ページ）では、DNS プリプロセッサについて説明し、DNS ネームサーバ応答における 3 種類のエクスプロイトを検出するようにプリプロセッサを設定する方法について説明します。
- FTP および Telnet トラフィックのデコード（19-20 ページ）では、FTP/Telnet デコーダについて説明し、FTP および Telnet トラフィックを正規化およびデコードするようにデコーダを設定する方法について説明します。
- HTTP トラフィックのデコード（19-34 ページ）では、HTTP デコーダについて説明し、HTTP トラフィックを正規化するようにデコーダを設定する方法について説明します。
- Sun RPC プリプロセッサの使用（19-51 ページ）では、RPC デコーダについて説明し、RPC トラフィックを正規化するようにデコーダを設定する方法について説明します。
- Session Initiation Protocol のデコード（19-53 ページ）では、SIP プリプロセッサを使用して SIP トラフィックをデコードし、SIP トラフィックの異常を検出する方法を説明します。
- GTP コマンド チャネルの設定（19-58 ページ）では、GTP プリプロセッサを使用して、パケット デコーダによって抽出された GTP コマンド チャネル メッセージをルール エンジンに提供する方法について説明します。
- IMAP トラフィックのデコード（19-59 ページ）では、IMAP プリプロセッサを使用して IMAP トラフィックをデコードし、IMAP トラフィックの異常を検出する方法を説明します。

- POP トラフィックのデコード（19-63 ページ）では、POP プリプロセッサを使用して POP トラフィックをデコードし、POP トラフィックの異常を検出する方法を説明します。
- SMTP トラフィックのデコード（19-66 ページ）では、SMTP デコーダについて説明し、SMTP トラフィックをデコードおよび正規化するようにデコーダを設定する方法について説明します。
- SSH プロプロセッサによるエクスプロイトの検出（19-74 ページ）では、SSH 暗号化トラフィック内のエクスプロイトを識別して処理する方法について説明します。
- SSL プリプロセッサの使用（19-78 ページ）では、SSL プリプロセッサを使用して暗号化トラフィックを特定し、そのトラフィックのインスペクションを停止して誤検出を排除する方法について説明します。
- SCADA の前処理の設定（20-1 ページ）では、Modbus および DNP3 プリプロセッサを使用して、対応するトラフィックの異常を検出し、特定のプロトコル フィールドを検査するためにデータを侵入ルール エンジンに提供する方法を説明します。

DCE/RPC トラフィックのデコード

ライセンス：Protection

DCE/RPC プロトコルにより、別々のネットワーク ホスト上のプロセスが、同一ホストに配置されている場合と同様に通信できます。通常、このようなプロセス間通信はホスト間で TCP および UDP 経由で転送されます。TCP 転送では、DCE/RPC が Windows Server Message Block（SMB）プロトコルまたは Samba でさらにカプセル化されることがあります。Samba は、Windows や UNIX/Linux 系のオペレーティング システムから構成される混合環境でプロセス間通信に使用されるオープンソースの SMB 実装です。また、ネットワーク上の Windows IIS Web サーバでは IIS RPC over HTTP が使用されることがあります。IIS RPC over HTTP は、プロキシ TCP により伝送される DCE/RPC トラフィックに、ファイアウォールを介して分散通信を提供します。

DCE/RPC プリプロセッサ オプションとその機能の説明には、Microsoft による DCE/RPC の実装である MSRPC が含まれることに注意してください。SMB のオプションと機能についての説明は、SMB と Samba の両方に当てはまります。

ほとんどの DCE/RPC エクスプロイトは、DCE/RPC サーバ（ネットワーク上の Windows または Samba が稼働している任意のホスト）を対象とした DCE/RPC クライアント要求で発生します。またエクスプロイトはサーバ応答でも発生することがあります。DCE/RPC プリプロセッサは、TCP、UDP、および SMB トランスポートでカプセル化された DCE/RPC 要求と応答を検出します。これには、RPC over HTTP バージョン 1 を使用して TCP により伝送される DCE/RPC も含まれます。プリプロセッサは DCE/RPC データ ストリームを分析し、DCE/RPC トラフィックにおける異常な動作と回避技術を検出します。また、SMB データ ストリームを分析し、異常な SMB 動作と回避技術を検出します。

IP 最適化プリプロセッサによる IP 最適化および TCP ストリーム プリプロセッサによる TCP ストリームの再構成に加えて、DCE/RPC プリプロセッサは、SMB のセグメント化解除と DCE/RPC の最適化も行います。TCP ストリームの前処理の使用（21-21 ページ）および IP パケットの最適化（21-12 ページ）を参照してください。

最後に、DCE/RPC プリプロセッサはルール エンジンで処理できるように DCE/RPC トラフィックを正規化します。特定の DCE/RPC ルール キーワードを使用して DCE/RPC サービス、操作、およびスタブ データを検出する方法については、DCE/RPC キーワード（27-62 ページ）を参照してください。

DCE/RPC プリプロセッサを設定するには、プリプロセッサの機能を制御するグローバル オプションを変更するか、IP アドレスと稼働している Windows または Samba のバージョンによってネットワーク上の DCE/RPC サーバを識別する 1 つ以上のターゲットベース サーバ ポリシーを指定します。

ジェネレータ ID（GID）が 132 または 133 の DCE/RPC プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があります。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

詳細については、次の各項を参照してください。

- グローバル DCE/RPC オプションの選択（19-3 ページ）
- ターゲットベース DCE/RPC サーバ ポリシーについて（19-4 ページ）
- DCE/RPC トランスポートについて（19-6 ページ）
- DCE/RPC ターゲットベース ポリシー オプションの選択（19-9 ページ）
- DCE/RPC プリプロセッサの設定（19-13 ページ）

グローバル DCE/RPC オプションの選択

ライセンス：Protection

グローバル DCE/RPC プリプロセッサ オプションは、プリプロセッサの機能を制御します。[到達したメモリ容量（Memory Cap Reached）] オプション以外のこれらのオプションを変更すると、パフォーマンスまたは検出機能に悪影響を及ぼす可能性があります。プリプロセッサについて、またプリプロセッサと有効にされている DCE/RPC ルールとの間の相互作用について十分に理解していない場合は、これらのオプションを変更しないでください。特に [最大フラグメント サイズ（Maximum Fragment Size）] オプションと [再構成しきい値（Reassembly Threshold）] オプションは、ルールが検出する必要がある深さと同じかそれ以上にしてください。詳細については、コンテンツ一致の制約（27-18 ページ）およびByte_Jump と Byte_Test の使用（27-33 ページ）を参照してください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

最大フラグメント サイズ

[最適化の有効化（Enable Defragmentation）] が選択されている場合、DCE/RPC フラグメントの許容最大長を 1514 バイトから 65535 バイトまでの範囲で指定します。これよりも大きなフラグメントの場合、プリプロセッサは処理のためにフラグメントの一部を切り捨て、指定のサイズにしてから最適化を行いますが、実際のパケットは変更されません。空白フィールドの場合、このオプションは無効になります。

再構成しきい値

[最適化の有効化（Enable Defragmentation）] が選択されている場合、0 を指定するとこのオプションは無効になり、1 バイトから 65535 バイトの範囲内の値を指定すると、それが、フラグメント化された DCE/RPC の最小バイト数となります。また該当する場合は、再構成されたパケットをルール エンジンに送信する前にキューに入れるセグメント化 SMB のバイト数が指定されます。低い値を指定すると、早期検出の可能性が高くなりますが、パフォーマンスに悪影響を及ぼす可能性があります。このオプションを有効にする場合は、パフォーマンスの影響をテストしておく必要があります。

最適化の有効化

フラグメント化された DCE/RPC トラフィックを最適化するかどうかを指定します。無効にすると、プリプロセッサは引き続き異常を検出して DCE/RPC データをルール エンジンに送信しますが、フラグメント化された DCE/RPC データでのエクスプロイトを見落とすリスクがあります。

このオプションには、DCE/RPC トラフィックを最適化しないという柔軟性がありますが、ほとんどの DCE/RPC エクスプロイトでは、フラグメント化を利用してエクスプロイトを隠ぺいする試みが行われます。このオプションを無効にすると、ほとんどの既知のエクスプロイトがバイパスされ、検出漏れが大量に発生します。

到達したメモリ容量

プリプロセッサに割り当てられた最大メモリ制限に達したか、またはこの制限を超過したことを検出します。最大メモリ制限に達したか、またはこの制限を超過した場合、プリプロセッサはメモリ キャップ イベントを引き起こしたセッションに関連付けられているすべての保留データを解放し、セッションのそれ以降の部分を無視します。

このオプションのイベントを生成するには、ルール 133:1 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

SMB セッションの自動検出ポリシー

SMB `Session Setup AndX` 要求および応答に指定されている Windows または Samba のバージョンを検出します。検出されたバージョンが、[ポリシー（Policy）] 設定オプションで設定されている Windows または Samba のバージョンと異なる場合、そのセッションに限り、検出されたバージョンが設定バージョンをオーバーライドします。詳細については、ターゲットベース DCE/RPC サーバ ポリシーについて（19-4 ページ）を参照してください。

たとえば、[ポリシー（Policy）] に Windows XP を設定した場合に、プリプロセッサが Windows Vista を検出すると、プリプロセッサはそのセッションでは Windows Vista ポリシーを使用します。その他の設定は引き続き有効です。

DCE/RPC トランスポートが SMB ではない場合は（トランスポートが TCP または UDP の場合）、バージョンを検出できず、ポリシーを自動的に設定できません。

このオプションを有効にするには、ドロップダウン リストで次のいずれかを選択します。

- サーバ/クライアント トラフィックでポリシー タイプを検査するには、[クライアント（Client）] を選択します。
- クライアント/サーバ トラフィックでポリシー タイプを検査するには、[サーバ（Server）] を選択します。
- サーバ/クライアント トラフィックとクライアント/サーバ トラフィックの両方でポリシー タイプを検査するには、[両方（Both）] を選択します。

ターゲットベース DCE/RPC サーバ ポリシーについて

ライセンス：Protection

ターゲットベースのサーバ ポリシーを 1 つ以上作成することにより、指定したタイプのサーバが処理するのと同様の方法で DCE/RPC トラフィックを検査するように、DCE/RPC プリプロセッサを設定することができます。ターゲットベースのポリシーの設定では、ネットワーク上の指定ホストで実行されている Windows または Samba のバージョンの識別、トランスポート プロトコルの有効化、DCE/RPC トラフィックをこれらのホストに伝送するポートの指定、その他のサーバ固有のオプションの設定などを行います。

Windows および Samba の DCE/RPC の実装は大きく異なります。たとえば、Windows のすべてのバージョンは、DCE/RPC トラフィックの最適化時に最初のフラグメントの DCE/RPC コンテキスト ID を使用しますが、Samba のすべてのバージョンは、最後のフラグメントのコンテキスト ID を使用します。また、特定の関数呼び出しを識別するために、Windows Vista では最初のフラグメントの opnum（操作番号）ヘッダー フィールドを使用しますが、Samba とその他のすべてのバージョンの Windows では最後のフラグメントの opnum フィールドを使用します。

Windows と Samba の SMB の実装にも、大きな違いがあります。たとえば、Windows は名前付きパイプの操作時に SMB OPEN および READ コマンドを認識しますが、Samba はこれらのコマンドを認識しません。

DCE/RPC プリプロセッサを有効にすると、デフォルトのターゲットベース ポリシーが自動的に有効になります。（任意）異なるバージョンの Windows または Samba を実行している他のホストを対象とするターゲットベース ポリシーを追加できます。追加するには、[ポリシー（Policy）] ドロップダウン リストから適切なバージョンを選択します。デフォルトのターゲットベース ポリシーは、別のターゲットベース ポリシーに含まれていないホストに適用されます。

それぞれのターゲットベース ポリシーで、1 つ以上のトランスポートを有効にして、それぞれの検出ポートを指定できます。また、自動検出ポートを有効にして指定することもできます。詳細については、DCE/RPC トランスポートについて（19-6 ページ）を参照してください。

その他のターゲットベースのポリシー オプションも設定できます。指定した 1 つ以上の共有 SMB リソースへの接続が試行された場合にそれを検出するように、プリプロセッサを設定できます。SMB トラフィックでファイルを検出し、検出されたファイルで指定のバイト数のデータを検査するように、プリプロセッサを設定できます。また、SMB プロトコルに関する知識を持つユーザだけが変更すべき拡張オプションを変更できます。このオプションでは、連結された SMB AndX コマンドの数が指定された最大数を超えた場合にそのことを検出するようにプリプロセッサを設定できます。

各ターゲットベースのポリシーでは次の設定が可能です。

- 1 つ以上のトランスポートを有効にし、それぞれについて検出ポート を指定します。
- 自動検出ポートを有効にして指定します。詳細については、DCE/RPC トランスポートについて（19-6 ページ）を参照してください。
- 指定した 1 つ以上の共有 SMB リソースへの接続が試行された場合にそのことを検出するように、プリプロセッサを設定します。
- SMB トラフィックでファイルを検出し、検出されたファイルで指定された数のバイトを検査するように、プリプロセッサを設定します。
- SMB プロトコルの知識を持つユーザだけが変更すべき拡張オプションを変更できます。このオプションでは、連結された SMB AndX コマンドの数が指定された最大数を超えた場合にそのことを検出するようにプリプロセッサを設定します。

[SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] グローバル オプションを有効にすると、SMB が DCE/RPC トランスポートの場合に、ターゲット ポリシーに対して設定されているポリシー タイプをセッションごとに自動的にオーバーライドできます。SMB セッションの自動検出ポリシー（19-4 ページ）を参照してください。

DCE/RPC プリプロセッサで SMB トラフィック ファイル検出を有効にする他に、オプションでこれらのファイルを検出してブロックするように、ファイル ポリシーを設定できます。詳細については、「ファイル ポリシーの作成（32-10 ページ）」と「ファイル ルールの操作（32-11 ページ）」を参照してください。

DCE/RPC トランスポートについて

ライセンス：Protection

各ターゲットベース ポリシーでは、TCP、UDP、SMB、および RPC over HTTP トランスポートのうち 1 つ以上を有効にできます。トランスポートを有効にする場合は、1 つ以上の検出ポート（DCE/RPC トラフィックを伝送することがわかっているポート）を指定する必要があります。（任意）自動検出ポートを有効にして指定できます。プリプロセッサは、自動検出ポートとして指定されたポートを最初にテストして、そのポートが DCE/RPC トラフィックを伝送しているかどうかを判別し、DCE/RPC トラフィックを検出した場合にのみ処理を続行します。

シスコでは、デフォルトの検出ポート（ウェルノウン ポートまたは各プロトコルで一般に使用されているポート）を使用することを推奨しています。検出ポートを追加するのは、デフォルト以外のポートで DCE/RPC トラフィックを検出した場合だけです。

自動検出ポートを有効にする場合は、エフェメラル ポート範囲全体に対応するよう、自動検出ポートが 1024 から 65535 の範囲に設定されていることを確認してください。注意点として、[RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）] オプションまたは [SMB 自動検出ポート（SMB Auto-Detect Ports）] オプションで自動検出ポートを有効にしたり指定したりすることはほとんどありません。これは、指定されているデフォルト検出ポートを除き、どちらの場合もトラフィックが発生することはほとんどなく、その見込みも少ないためです。また、自動検出は、トランスポート検出ポートによって識別されていないポートでのみ発生する点にも注意してください。トランスポートごとに自動検出ポートを有効または無効にする際の推奨事項については、DCE/RPC ターゲットベース ポリシー オプションの選択（19-9 ページ）を参照してください。

Windows のターゲットベース ポリシーでは、ネットワークのトラフィックに一致するように、1 つ以上の任意のトランスポートのポートを任意の組み合わせで指定できます。しかし、Samba のターゲットベース ポリシーでは SMB トランスポートのポートだけを指定できます。

少なくとも 1 つのトランスポートが有効になっている DCE/RPC ターゲットベース ポリシーを追加した場合を除き、デフォルトの ターゲットベース ポリシーでは少なくとも 1 つの DCE/RPC トランスポートを有効にする必要があります。たとえば、すべての DCE/RPC 実装に対してホストを指定し、未指定のホストにはデフォルトのターゲットベース ポリシーを適用したくない場合があります。そのような場合は、デフォルトのターゲットベース ポリシーのトランスポートを有効化しないようにします。

詳細については、次の各項を参照してください。

- コネクションレス型およびコネクション型 DCE/RPC トラフィックについて（19-6 ページ）
- RPC over HTTP トランスポートについて（19-8 ページ）

コネクションレス型およびコネクション型 DCE/RPC トラフィックについて

ライセンス：Protection

DCE/RPC メッセージは、2 種類の DCE/RPC Protocol Data Unit（PDU）の 1 つに準拠します。

- コネクション型 DCE/RPC PDU プロトコル

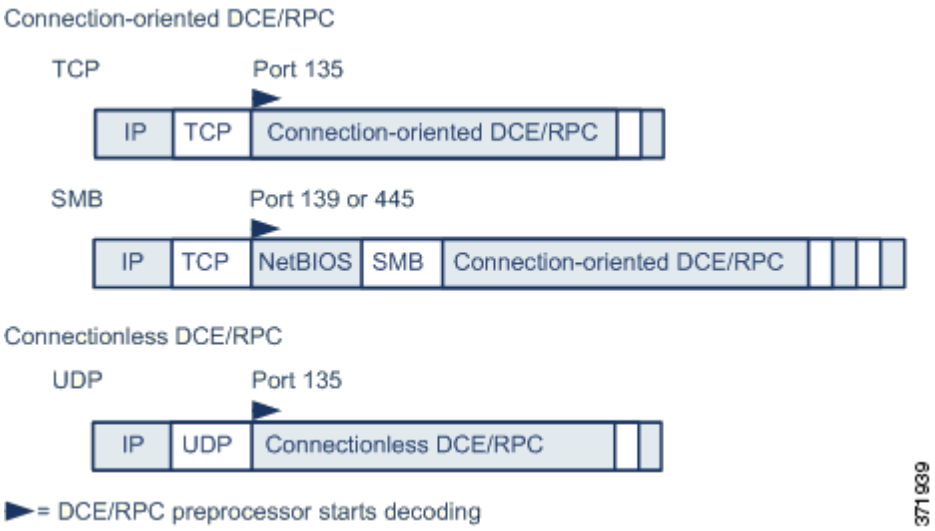
  DCE/RPC プリプロセッサは、TCP、SMB、および RPC over HTTP トランスポートでコネクション型 DCE/RPC を検出します。

- コネクションレス型 DCE/RPC PDU プロトコル

  DCE/RPC プリプロセッサは、UDP トランスポートでコネクションレス型 DCE/RPC を検出します。

この 2 つの DCE/RPC PDU プロトコルには、それぞれ固有のヘッダーとデータ特性があります。たとえば、コネクション型 DCE/RPC のヘッダーの長さは通常は 24 バイトですが、コネクションレス型 DCE/RPC のヘッダーの長さは 80 バイト（固定）です。また、フラグメント化コネクションレス型 DCE/RPC のフラグメントの正しい順序は、コネクションレス型トランスポートでは処理できないため、代わりに、コネクションレス型 DCE/RPC ヘッダーの値によって維持する必要があります。これとは対照的に、コネクション型 DCE/RPC の正しいフラグメント順序はトランスポート プロトコルによって維持されます。DCE/RPC プリプロセッサは、これらや他のプロトコル固有の特性を使用して、異常やその他の検知回避技術について両方のプロトコルをモニタし、トラフィックをデコードおよび最適化してからルール エンジンに渡します。

次の図は、DCE/RPC プリプロセッサが各種トランスポートの DCE/RPC トラフィックの処理を開始するポイントを示します。



この図の次の点に注意してください。

- ウェルノウン TCP または UDP ポート 135 は、TCP および UDP トランスポートの DCE/RPC トラフィックを特定します。
- この図には RPC over HTTP は含まれていません。

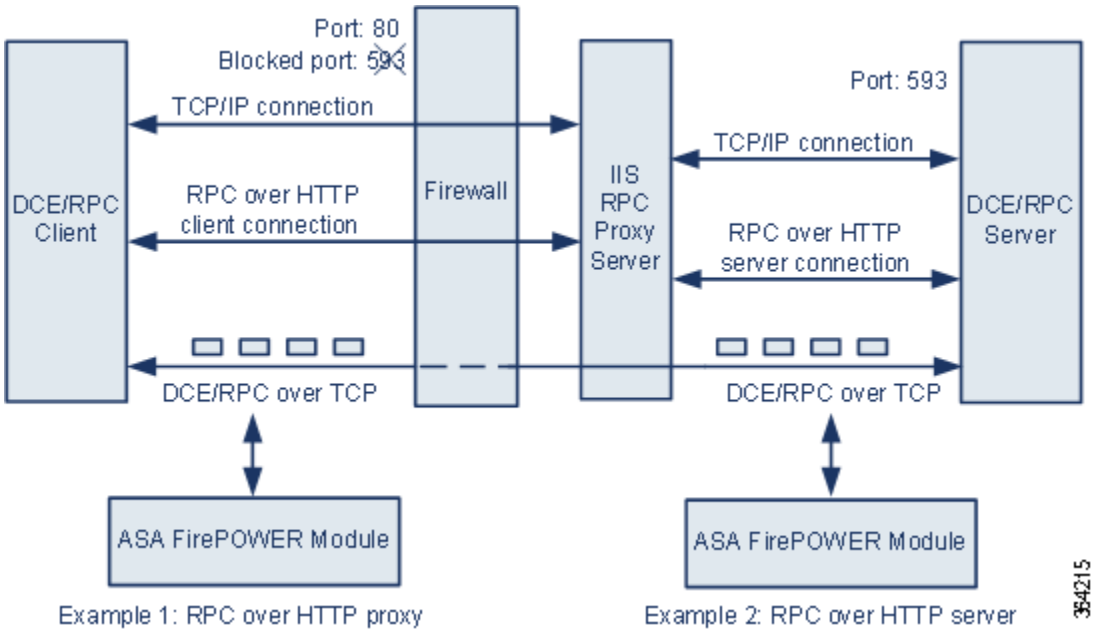
  RPC over HTTP の場合、コネクション型 DCE/RPC は、図に示すように、HTTP を介した初期セットアップ シーケンスの後、TCP 経由で直接伝送されます。詳細については、RPC over HTTP トランスポートについて（19-8 ページ）を参照してください。
- DCE/RPC プリプロセッサは通常、NetBIOS セッション サービス用のウェルノウン TCP ポート 139 か、同様に実装されたウェルノウン Windows ポート 445 で SMB トラフィックを受信します。

  SMB には DCE/RPC 伝送以外にも多数の機能があるため、プリプロセッサは SMB トラフィックが DCE/RPC トラフィックを伝送しているかどうかをまず検査します。伝送していない場合は処理を停止し、伝送している場合は処理を続行します。
- IP によりすべての DCE/RPC トランスポートがカプセル化されます。
- TCP は、すべてのコネクション型 DCE/RPC を伝送します。
- UDP はコネクションレス型 DCE/RPC を伝送します。

RPC over HTTP トランスポートについて

ライセンス：Protection

Microsoft RPC over HTTP では、次の図に示すように、DCE/RPC トラフィックをトンネリングして、ファイアウォールを通過させることができます。DCE/RPC プリプロセッサは Microsoft RPC over HTTP バージョン 1 を検出します。



Microsoft IIS プロキシ サーバと DCE/RPC サーバは、同じホストまたは別々のホストにインストールできます。いずれの場合でも、個別のプロキシ オプションとサーバ オプションがあります。この図の次の点に注意してください。

- DCE/RPC サーバはポート 593 で DCE/RPC クライアント トラフィックをモニタしますが、ファイアウォールはこのポート 593 をブロックします。

  通常、ファイアウォールではデフォルトでポート 593 がブロックされます。

- RPC over HTTP は、ファイアウォールによって許可される可能性が高いウェルノウン HTTP ポート 80 を使用して、HTTP 経由で DCE/RPC を伝送します。
- 例 1 のように、DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間のトラフィックをモニタする場合は、[RPC over HTTP プロキシ（RPC over HTTP proxy）] オプションを選択します。
- 例 2 のように、Microsoft IIS RPC プロキシ サーバと DCE/RPC サーバが異なるホスト上にあり、デバイスが 2 つのサーバ間のトラフィックをモニタしている場合は、[RPC over HTTP サーバ（RPC over HTTP server）] オプションを選択します。
- RPC over HTTP により DCE/RPC クライアントとサーバ間でのプロキシ セットアップが完了した後、トラフィックは TCP を経由したコネクション型 DCE/RPC だけで構成されます。

DCE/RPC ターゲットベース ポリシー オプションの選択

ライセンス：Protection

各ターゲットベース ポリシーでは、次に示すさまざまなオプションを指定できます。[到達したメモリ容量（Memory Cap Reached）] および [SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] オプション以外のオプションを変更すると、パフォーマンスまたは検出機能に悪影響を及ぼす可能性があります。プリプロセッサについて、またプリプロセッサと有効にされている DCE/RPC ルールとの間の相互作用について十分に理解していない場合は、これらのオプションを変更しないでください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ネットワーク（**Networks**）

DCE/RPC ターゲットベース サーバ ポリシーを適用するホストの IP アドレス。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを指定できます。ASA FirePOWER モジュール での IPv4 および IPv6 アドレス ブロックの指定については、IP アドレスの表記規則（1-4 ページ）を参照してください。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

また、ターゲットベース ポリシーがトラフィックを処理するようにするには、識別するネットワークがターゲットベース ポリシーを設定するネットワーク分析ポリシーによって処理されるネットワーク、およびゾーンに一致するかまたはサブセットになっている必要があることにも注意してください。詳細については、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（17-3 ページ）を参照してください。

ポリシー（**Policy**）

モニタ対象ネットワーク セグメントのターゲット ホストが使用する Windows または Samba DCE/RPC の実装。これらのポリシーの詳細については、ターゲットベース DCE/RPC サーバ ポリシーについて（19-4 ページ）を参照してください。

[SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] グローバル オプションを有効にすると、SMB が DCE/RPC トランスポートの場合に、このオプションの設定をセッションごとに自動的にオーバーライドできます。SMB セッションの自動検出ポリシー（19-4 ページ）を参照してください。

SMB の無効な共有（**SMB Invalid Shares**）

1 つ以上の SMB 共有リソースを識別する、大文字と小文字を区別しない英数字テキスト文字列です。指定した共有リソースへの接続が試行されると、プリプロセッサがそのことを検出します。複数の共有をカンマで区切って指定できます。また必要に応じて、共有を引用符で囲むこともできます。これは、以前のソフトウェア バージョンでは必須でしたが、現在は必須ではありません。次に例を示します。

```
"C$", D$, "admin", private
```

SMB ポートと SMB トラフィックの両方の検出が有効に設定されている場合、プリプロセッサは SMB トラフィックで無効な共有を検出します。

ほとんどの場合、Windows により名前が指定されたドライブを無効な共有として指定するには、このドライブにドル記号を付加する必要があることに注意してください。たとえば、ドライブ C は C$ または "C$" として指定します。

このオプションのイベントを生成するには、ルール 133:26 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

SMB 最大 AndX チェーン（SMB Maximum AndX Chain）

連結された SMB AndX コマンドの最大数（0 から 255）です。通常、多数の連結 AndX コマンドは異常な動作を表し、場合によっては回避試行を示している可能性があります。連結コマンドを許可しない場合は 1 を指定し、連結コマンドの数の検出を無効にするには 0 を指定します。

プリプロセッサは最初に連結コマンドの数をカウントし、関連する SMB プリプロセッサ ルールが有効であり、連結コマンドの数が設定されている値と等しいかそれ以上の場合にはイベントを生成することに注意してください。その後、処理が続行されます。

（注）　SMB プロトコルに詳しいユーザだけがこのオプションのデフォルト設定を変更するようにしてください。

このオプションのイベントを生成するには、ルール 133:20 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

RPC プロキシ トラフィックのみ（RPC proxy traffic only）

[RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）] が有効である場合、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみであるか、または他の Web サーバ トラフィックを含んでいる可能性があるかどうかを示します。たとえば、ポート 80 はプロキシ トラフィックとその他の Web サーバ トラフィックの両方を伝送する可能性があります。

このオプションが無効になっている場合は、プロキシ トラフィックとその他の Web サーバ トラフィックの両方が想定されます。たとえばサーバが専用プロキシ サーバである場合などに、このオプションを有効にします。有効にすると、プリプロセッサはトラフィックを調べて DCE/RPC を伝送しているかどうかを判別し、伝送していない場合はそのトラフィックを無視し、伝送している場合は処理を続行します。このオプションを有効にすることで機能が追加されるのは、[RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）] チェックボックスも有効にされている場合だけであることに注意してください。

RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）

デバイスが DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間に配置されている場合に、指定の各ポートで RPC over HTTP によりトンネリングされている DCE/RPC トラフィックの検出を有効にします。RPC over HTTP トランスポートについて（19-8 ページ）を参照してください。

有効である場合、DCE/RPC トラフィックが確認されるポートを追加できますが、Web サーバは一般に DCE/RPC トラフィックとその他のトラフィックの両方にデフォルト ポートを使用するため、この操作が必要になることはあまりありません。有効である場合、[RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）] は有効にしませんが、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみであり、その他の Web サーバ トラフィックを含んでいない場合は、[RPC プロキシ トラフィックのみ（RPC Proxy Traffic Only）] を有効にします。

RPC over HTTP サーバ ポート（**RPC over HTTP Server Ports**）

Microsoft IIS RPC プロキシ サーバと DCE/RPC サーバが異なるホスト上に配置されており、デバイスがこの 2 つのサーバ間のトラフィックをモニタしている場合、指定の各ポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの検出を有効にします。RPC over HTTP トランスポートについて（19-8 ページ）を参照してください。

一般に、このオプションを有効にするときは、ネットワーク上のプロキシ Web サーバに注意を払わない場合でも、1025 ～ 65535 のポート範囲で [RPC over HTTP サーバ自動検出ポート（RPC over HTTP Server Auto-Detect Ports）] も有効にする必要があります。場合によっては RPC over HTTP サーバ ポートを再設定することがあり、その際には再設定したサーバ ポートをこのオプションのポート リストに追加する必要があることに注意してください。

TCP ポート（**TCP Ports**）

指定の各ポートでの TCP の DCE/RPC トラフィックの検出を有効にします。

正当な DCE/RPC トラフィックとエクスプロイトは、さまざまなポートを使用する可能性があります。ポート 1024 より大きい番号のポートが一般的です。通常、このオプションを有効にする場合は、1025 ～ 65535 のポート範囲で [TCP 自動検出ポート（TCP Auto-Detect Ports）] も有効にする必要があります。

UDP ポート

指定の各ポートでの UDP の DCE/RPC トラフィックの検出を有効にします。

正当な DCE/RPC トラフィックとエクスプロイトは、さまざまなポートを使用する可能性があります。ポート 1024 より大きい番号のポートが一般的です。通常、このオプションを有効にする場合は、1025 ～ 65535 のポート範囲で [UDP 自動検出ポート（UDP Auto-Detect Ports）] も有効にする必要があります。

SMB ポート（**SMB Ports**）

指定の各ポートでの SMB の DCE/RPC トラフィックの検出を有効にします。

デフォルトの検出ポートを使用した SMB トラフィックが発生することがあります。他のポートはほとんどありません。通常はデフォルト設定を使用してください。

RPC over HTTP プロキシ自動検出ポート（**RPC over HTTP Proxy Auto-Detect Ports**）

デバイスが DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間に配置されている場合に、指定のポートで RPC over HTTP によりトンネリングされている DCE/RPC トラフィックの自動検出を有効にします。RPC over HTTP トランスポートについて（19-8 ページ）を参照してください。

有効である場合は、一時ポート範囲全体をカバーするため、一般にポート範囲として 1025 から 65535 を指定します。

RPC over HTTP サーバ自動検出ポート（**RPC over HTTP Server Auto-Detect Ports**）

Microsoft IIS RPC プロキシ サーバおよび DCE/RPC サーバが異なるホスト上に配置されており、デバイスがこの 2 つのサーバ間のトラフィックをモニタしている場合、指定のポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの自動検出を有効にします。RPC over HTTP トランスポートについて（19-8 ページ）を参照してください。

TCP 自動検出ポート（**TCP Auto-Detect Ports**）

指定のポートで TCP の DCE/RPC トラフィックの自動検出を有効にします。

UDP 自動検出ポート（**UDP Auto-Detect Ports**）

指定の各ポートで UDP の DCE/RPC トラフィックの自動検出を有効にします。

SMB 自動検出ポート（**SMB Auto-Detect Ports**）

SMB の DCE/RPC トラフィックの検出を有効にします。

SMB ファイル インスペクション（**SMB File Inspection**）

ファイル検出のための SMB トラフィックのインスペクションを有効にします。次の選択肢があります。

- ファイル インスペクションを無効にするには、[オフ（Off）] を選択します。
- SMB でファイル データを検査するが、DCE/RPC トラフィックは検査しない場合は、[ファイルのみ（Only）] を選択します。このオプションを選択すると、ファイルと DCE/RPC トラフィックの両方を検査する場合よりもパフォーマンスが向上する可能性があります。
- SMB でファイルと DCE/RPC トラフィックの両方を検査するには、[オン（On）] を選択します。このオプションを選択すると、パフォーマンスに影響する可能性があります。

SMB トラフィックでの次のファイルについてのインスペクションはサポートされていません。

- SMB 2.x および SMB 3.x で転送されたファイル
- このオプションを有効にしてポリシーを適用する前に確立された TCP または SMB セッションで転送されたファイル
- 1 つの TCP または SMB セッションで同時に転送されたファイル
- 複数の TCP または SMB セッションにわたって転送されたファイル
- メッセージ署名のネゴシエート時など、非連続データを使用して転送されたファイル
- 同一オフセットに異なるデータが含まれており、データがオーバーラップしている転送ファイル
- リモート クライアントがファイル サーバに保存し、そのクライアントで編集用に開かれたファイル

SMB ファイル インスペクションの深さ（**SMB File Inspection Depth**）

[SMB ファイル インスペクション（SMB File Inspection）] が [ファイルのみ（Only）] または [オン（On）] に設定されている場合に、SMB トラフィックでファイルが検出された時に検査されるデータのバイト数です。次のいずれかを指定します。

- `1` から `2147483647`（約 2GB）までの範囲内の整数
- `0`：ファイル全体を検査する場合
- `-1`：ファイル インスペクションを無効にする場合

このフィールドには、アクセス コントロール ポリシーで定義されている値と等しいか、それよりも小さい値を入力します。[ファイルタイプを検知する前に検閲するバイト数制限（Limit the number of bytes inspected when doing file type detection）] で定義されている値よりも大きい値をこのオプションに設定すると、アクセス コントロール ポリシーの設定が、有効な最大値として使用されます。詳細については、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（10-17 ページ）参照してください。

[SMB ファイル インスペクション（SMB File Inspection）] が [オフ（Off）] に設定されている場合、このフィールドは無効になります。

DCE/RPC プリプロセッサの設定

ライセンス：Protection

DCE/RPC プリプロセッサのグローバル オプションと、1 つ以上のターゲットベース サーバ ポリシーを設定できます。

ジェネレータ ID（GID）133 のルールを有効にしていない場合、プリプロセッサはイベントを生成しません。特定の検出オプションに関連付けられているルールについては、グローバル DCE/RPC オプションの選択（19-3 ページ）、DCE/RPC ターゲットベース ポリシー オプションの選択（19-9 ページ）、および ルール状態の設定（24-21 ページ）を参照してください。

さらに、ほとんどの DCE/RPC プリプロセッサ ルールでは、SMB、コネクション型 DCE/RPC、またはコネクションレス型 DCE/RPC のトラフィックで異常や検知回避技術が検出されると、イベントが生成されます。トラフィック タイプ別に有効にできるルールを次の表に示します。

表 ***19-1***　トラフィックに関連する ***DCE/RPC*** ルール

トラフィック	プリプロセッサ ルール **GID:SID**
SMB	133:2 ～ 133:26、133:48 ～ 133:57
コネクション型 DCE/RPC	133:27 ～ 133:39
コネクションレス型 DCE/RPC	133:40 ～ 133:43

DCE/RPC プリプロセッサを設定する方法：

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **4**　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ **5**　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ **6**　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ **7**　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ 8　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [DCE/RPC 設定（DCE/RPC Configuration）] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[DCE/RPC 設定（DCE/RPC Configuration）] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 9　グローバル DCE/RPC オプションの選択（19-3 ページ）で説明するオプションを変更できます。

ステップ 10　次の 2 つの対処法があります。

- 新しいターゲットベースのポリシーを追加します。ページの左側で [サーバ（Servers）] の横にある追加アイコン（）をクリックします。[ターゲットの追加（Add Target）] ポップアップ ウィンドウが表示されます。1 つ以上の IP アドレスを [サーバ アドレス（Server Address）] フィールドに指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。ASA FirePOWER モジュールでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-4 ページ）を参照してください。

  デフォルト ポリシーを含め、最大 255 個のポリシーを設定できます。

  ターゲットベース ポリシーがトラフィックを処理するようにするには、識別するネットワークがターゲットベース ポリシーを設定するネットワーク分析ポリシーによって処理されるネットワーク、およびゾーンに一致するかまたはサブセットになっている必要があることに注意してください。詳細については、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（17-3 ページ）を参照してください。

  ページの左側のサーバ リストに新しい項目が表示され、選択されていることを示すために強調表示されます。[設定（Configuration）] セクションが更新され、追加したプロフィールの現行設定が反映されます。

- 既存のターゲットベースのポリシーの設定を変更します。ページ左側の [サーバ（Servers）] の下で追加したポリシーの設定済みアドレスをクリックするか、または [デフォルト（default）] をクリックします。

  選択したエントリが強調表示され、[設定（Configuration）] セクションが更新されて、選択したポリシーの現在の設定が表示されます。既存のポリシーを削除するには、削除するポリシーの横にある削除アイコン（  ）をクリックします。

ステップ 11　変更できるターゲットベース ポリシー オプションは次のとおりです。

- DCE/RPC のターゲットベース サーバ ポリシーを適用する 1 つ以上のホストを指定するには、[ネットワーク（Networks）] フィールドに、1 つの IP アドレスまたはアドレス ブロック、あるいはこのいずれかまたは両方をカンマで区切ったリストを入力します。

  デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを指定できます。デフォルト ポリシーでは [ネットワーク（Networks）] の設定を変更できないことに注意してください。デフォルト ポリシーは、別のポリシーで指定されていないネットワーク内のすべてのサーバに適用されます。

- ネットワーク セグメントの指定ホストに適用するポリシーのタイプを指定するには、[ポリシー（Policy）] ドロップダウン リストから、いずれかの Windows または Samba ポリシー タイプを選択します。

  [SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] グローバル オプションを有効にすると、SMB が DCE/RPC トランスポートの場合に、このオプションの設定をセッションごとに自動的にオーバーライドできます。SMB セッションの自動検出ポリシー（19-4 ページ）を参照してください。

- 指定の共有 SMB リソースへの接続が試行された場合にそのことを検出するようにプリプロセッサを設定するには、[SMB の無効な共有（SMB Invalid Shares）] フィールドに、共有リソースを示す文字列を 1 つまたは複数指定します。文字列の大文字と小文字は区別されず、複数の文字列はカンマで区切って指定します。オプションで、個々の文字列を引用符で囲むこともできます。これは、以前のソフトウェア バージョンでは必須でしたが、現在は必須ではありません。

  たとえば、C$、D$、admin、および private という名前の共有リソースを検出するには、次のように入力します。

  ```
  "C$", D$, "admin", private
  ```

  SMB の無効な共有を検出するには、[SMB ポート（SMB Ports）] または [SMB 自動検出ポート（SMB Auto-Detect Ports）] も有効にして、[SMB トラフィック（SMB Traffics）] グローバル オプションを有効にする必要があります。

  ほとんどの場合、Windows により名前が指定されたドライブを無効な共有として指定するには、このドライブにドル記号を付加する必要があることにも注意してください。たとえば、ドライブ C を指定するには `c$` または `"c$"` と入力します。

- SMB の DCE/RPC トラフィックで検出されたファイルを検査し、DCE/RPC トラフィックの分析はしない場合は、[SMB ファイル インスペクション（SMB File Inspection）] ドロップダウン リストから [ファイルのみ（Only）] を選択します。SMB の DCE/RPC トラフィックで検出されたファイルと DCE/RPC トラフィックを検査するには、[SMB ファイル インスペクション（SMB File Inspection）] ドロップダウン リストから [ファイルのみ（On）] を選択します。[SMB ファイル インスペクションの深さ（SMB File Inspection Depth）] フィールドに、検出されたファイル内の検査対象バイト数を入力します。検出されたファイル全体を検査するには、`0` を入力します。

- 連結された SMB AndX コマンドの最大許容数を指定するには、[SMB AndX の最大チェーン（SMB Maximum AndX Chains）] のフィールドに 0 ～ 255 を入力します。連結されたコマンドを許可しない場合は `1` を指定します。この機能を無効にするには、`0` を入力するか、またはこのオプションを空白のままにします。

  （注）　SMB プロトコルに詳しいユーザだけが [SMB AndX の最大チェーン（SMB Maximum AndX Chains）] オプションのデフォルト設定を変更するようにしてください。

- Windows ポリシー トランスポートの DCE/RPC トラフィックを伝送することが判明しているポートで、DCE/RPC トラフィックを処理できるようにするには、検出トランスポートの横のチェック ボックスをオンまたはオフにします。またオプションで、伝送用のポートを追加または削除できます。

  Windows ポリシー用に、[RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）]、[RPC over HTTP サーバ ポート（RPC over HTTP Server Ports）]、[TCP ポート（TCP Ports）]、および [UDP ポート（UDP Ports）] のいずれか 1 つまたは任意の組み合わせを選択します。[RPC over HTTP プロキシ（RPC over HTTP proxy）] が有効であり、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみである場合（つまり、他の Web サーバ トラフィックが含まれていない場合）は、[RPC プロキシ トラフィックのみ（RPC Proxy Traffic Only）] を選択します。

  Samba ポリシー用に [SMB ポート（SMB Ports）] を選択します。

  ほとんどの場合はデフォルト設定を使用します。詳細については、DCE/RPC トランスポートについて（19-6 ページ）、RPC over HTTP トランスポートについて（19-8 ページ）、および DCE/RPC ターゲットベース ポリシー オプションの選択（19-9 ページ）を参照してください。

  1 つのポートを入力するか、ダッシュ（-）で区切ったポート番号範囲、またはポート番号と範囲をカンマで区切ったリストを入力できます。

- 指定されたポートが DCE/RPC トラフィックを伝送するかどうかを調べて、伝送する場合に処理を続行するには、自動検出トランスポートの横のチェック ボックスをオンまたはオフにします。さらに、必要に応じて、伝送用のポートを追加または削除します。

  Windows ポリシー用に、[RPC over HTTP サーバ自動検出ポート（RPC over HTTP Server Auto-Detect Ports）]、[TCP 自動検出ポート（TCP Auto-Detect Ports）]、[UDP 自動検出ポート（UDP Auto-Detect Ports）] のいずれかまたは任意の組み合わせを選択します。

  ただし、[RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）] または [SMB 自動検出ポート（SMB Auto-Detect Ports）] を選択することはほとんどありません。

  通常、エフェメラル ポート範囲全体をカバーするために、有効にする自動検出ポートに対して 1025 ～ 65535 のポート範囲を指定します。詳細については、DCE/RPC トランスポートについて（19-6 ページ）、RPC over HTTP トランスポートについて（19-8 ページ）、および DCE/RPC ターゲットベース ポリシー オプションの選択（19-9 ページ）を参照してください。

詳細については、DCE/RPC ターゲットベース ポリシー オプションの選択（19-9 ページ）を参照してください。

ステップ 12　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

DNS ネーム サーバ応答におけるエクスプロイトの検出

ライセンス：Protection

DNS プリプロセッサは、DNS ネーム サーバ応答を検査し、次に示す特定のエクスプロイトがあるかどうかを確認します。

- RData テキスト フィールドに対するオーバーフローの試行
- 古い DNS リソース レコード タイプ
- 試験的な DNS リソース レコード タイプ

詳細については、次の各項を参照してください。

- DNS プリプロセッサ リソース レコード インスペクションについて（19-16 ページ）
- RData テキスト フィールドに対するオーバーフローの試行の検出（19-18 ページ）
- 古い DNS リソース レコード タイプの検出（19-18 ページ）
- 試験的な DNS リソース レコード タイプの検出（19-18 ページ）
- DNS プリプロセッサの設定（19-19 ページ）

DNS プリプロセッサ リソース レコード インスペクションについて

ライセンス：Protection

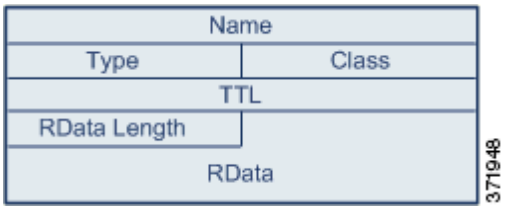
最も一般的なタイプの DNS ネーム サーバ応答には、応答を求めたクエリ内のドメイン名に対応する 1 つ以上の IP アドレスが示されています。その他のタイプのサーバ応答には、たとえば、電子メール メッセージの宛先や、元のクエリの対象のサーバからは取得できない情報を提供できるネームサーバの位置などが記述されています。

DNS 応答は、メッセージ ヘッダー、1 つ以上の要求を含む [質問（Question）] セクション、および [質問（Question）] セクションの要求に対応する 3 つのセクション（[応答（Answer）]、[権威（Authority）]、および [追加情報（Additional Information）]）で構成されます。この 3 セクションの応答には、ネーム サーバに保持されているリソース レコード（RR）の情報が反映されます。次の表で、これらの 3 つのセクションについて説明します。

表 *19-2*　*DNS* ネーム サーバ *RR* 応答

セクション	内容	例
応答	クエリに対する特定の回答を提供する 1 つ以上のリソース レコード（オプション）	ドメイン名に対応する IP アドレス
権限（Authority）	権威ネーム サーバを指し示す 1 つ以上のリソース レコード（オプション）	応答の権威ネーム サーバの名前
その他の情報	[応答（Answer）] セクションに関連する追加情報を提供する 1 つ以上のリソース レコード（オプション）	クエリ対象の別のサーバの IP アドレス

さまざまなタイプのリソース レコードがありますが、これらはすべて一貫して次の構造を保っています。



理論上、すべてのタイプのリソース レコードを、ネーム サーバ応答メッセージの [応答（Answer）]、[権威（Authority）]、または [追加情報（Additional Information）] セクションで使用できます。DNS プリプロセッサは、検出されたエクスプロイトについて、3 つの各応答セクションのすべてのリソース レコードを検査します。

[タイプ（Type）] および [RData] リソース レコード フィールドは、DNS プリプロセッサでは特に重要です。[タイプ（Type）] フィールドは、リソース レコードのタイプを示します。[RData]（リソース データ）フィールドは、応答の内容を示します。[RData] フィールドのサイズと内容は、リソース レコードのタイプによって異なります。

DNS メッセージは通常、UDP トランスポート プロトコルを使用しますが、信頼性のある配信を必要とするメッセージ タイプである場合や、メッセージ サイズが UDP で処理可能なサイズを超えている場合は、TCP を使用します。DNS プリプロセッサは、UDP および TCP の両方のトラフィックで DNS サーバ応答を検査します。

DNS プリプロセッサは、ミッドストリームで検出された TCP セッションを検査せず、ドロップされたパケットが原因でセッションの状態が失われるとインスペクションを終了します。

DNS プリプロセッサ用に設定する一般的なポートは、ウェルノウン ポート 53 です。これは、DNS ネーム サーバが UDP および TCP の両方で DNS メッセージに使用するポートです。

RData テキスト フィールドに対するオーバーフローの試行の検出

ライセンス：Protection

リソース レコード タイプが TXT（テキスト）の場合、RData フィールドは可変長の ASCII テキスト フィールドになります。

DNS プリプロセッサの [RData テキスト フィールドに対するオーバーフローの試行の検出（Detect Overflow attempts on RData Text fields）] オプションを選択した場合は、MITRE の Current Vulnerabilities and Exposures データベースの CVE-2006-3441 エントリで指定されている特定の脆弱性が検出されます。これは、Microsoft Windows 2000 Service Pack 4、Windows XP Service Pack 1 および Service Pack 2、Windows Server 2003 Service Pack 1 の既知の脆弱性です。攻撃者はこの脆弱性を悪用して、[RData] テキスト フィールドの長さの誤算を引き起こし、結果としてバッファ オーバーフローを発生させるよう悪意をもって作られたネーム サーバ応答をホストに送信するか受信させることで、ホストを完全に制御できます。

アップグレードによってこの脆弱性が修正されていないオペレーティング システムが稼働しているホストがネットワーク内に含まれている可能性がある場合は、この機能を有効にする必要があります。

このオプションのイベントを生成するには、ルール 131:3 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

古い DNS リソース レコード タイプの検出

ライセンス：Protection

RFC 1035 ではさまざまなリソース レコード タイプが古いタイプとして指定されています。これらは古いレコード タイプであるため、一部のシステムはこれらのレコード タイプに対応しておらず、エクスプロイトの対象となることがあります。このようなレコード タイプを含めるようにネットワークを意図的に設定している場合を除き、通常の DNS 応答でこのようなレコード タイプが検出されることは想定されません。

既知の古いリソース レコード タイプを検出するようにシステムを設定できます。次の表に、これらのレコード タイプとその説明を示します。

表 *19-3*　古い *DNS* リソース レコード タイプ

RR タイプ	コード（Code）	説明
3	MD	メールの宛先
4	MF	メールのフォワーダ

このオプションのイベントを生成するには、ルール 131:1 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

試験的な DNS リソース レコード タイプの検出

ライセンス：Protection

RFC 1035 ではさまざまなリソース レコード タイプが試験的なタイプとして指定されています。これらは試験的なレコード タイプであるため、一部のシステムはこれらのレコード タイプに対応しておらず、エクスプロイトの対象となることがあります。このようなレコード タイプを含めるようにネットワークを意図的に設定している場合を除き、通常の DNS 応答でこのようなレコード タイプが検出されることは想定されません。

既知の試験的なレコード タイプを検出するようにシステムを設定できます。次の表に、これらのレコード タイプとその説明を示します。

表 *19-4*　試験的な *DNS* リソース レコード タイプ

RR タイプ	コード（Code）	説明
7	MB	メールボックスのドメイン名
8	MG	メール グループ メンバー
9	MR	メール リネーム ドメイン名
10	NUL	空白のリソース レコード

このオプションのイベントを生成するには、ルール 131:2 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

DNS プリプロセッサの設定

ライセンス：Protection

DNS プリプロセッサを設定するには、次の手順に従います。このページのオプションの設定の詳細については、RData テキスト フィールドに対するオーバーフローの試行の検出（19-18 ページ）、古い DNS リソース レコード タイプの検出（19-18 ページ）、および試験的な DNS リソース レコード タイプの検出（19-18 ページ）を参照してください。

DNS プリプロセッサを設定するには、次の手順を実行します。

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **4**　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ **5**　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ **6**　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定(Settings)] をクリックします。

[設定(Settings)] ページが表示されます。

ステップ 8　[アプリケーション層プリプロセッサ(Application Layer Preprocessors)] の下の [DNS 設定(DNS Configuration)] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[DNS 設定(DNS Configuration)] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(16-1 ページ)を参照してください。

ステップ 9　(任意)[設定(Settings)] 領域の次の項目を変更できます。

- [ポート(Ports)] フィールドに、DNS プリプロセッサが DNS サーバ応答をモニタする 1 つ以上の送信元ポートを指定します。複数のポートを指定する場合は、カンマで区切ります。
- RData テキスト フィールドでのバッファ オーバーフロー試行の検出を有効にするには、[RData テキスト フィールドでのオーバーフロー試行の検出(Detect Overflow Attempts on RData Text fields)] チェック ボックスをオンにします。
- 古いリソース レコード タイプを検出できるようにするには、[古い DNS RR タイプの検出(Detect Obsolete DNS RR Types)] チェック ボックスをオンにします。
- 試験的なリソース レコード タイプを検出できるようにするには、[試験的な RR タイプの検出(Detect Experimental DNS RR Types)] チェック ボックスをオンにします。

ステップ 10　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

FTP および Telnet トラフィックのデコード

ライセンス:Protection

FTP/Telnet デコーダは FTP および Telnet データ ストリームを分析して、ルール エンジンによる処理の前に FTP および Telnet コマンドを正規化します。

ジェネレータ ID(GID)125 および 126 の FTP および Telnet プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があります。詳細については、ルール状態の設定(24-21 ページ)を参照してください。

詳細は、次のトピックを参照してください。

グローバル FTP および Telnet オプションについて

ライセンス：Protection

FTP/Telnet デコーダがパケットのステートフル インスペクションまたはステートレス インスペクションを実行するかどうか、デコーダが暗号化 FTP または Telnet セッションを検出するかどうか、およびデコーダが暗号化データの検出後にデータ ストリームの検査を続行するかどうかを決定するグローバル オプションを設定できます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ステートフル インスペクション（**Stateful Inspection**）

選択されている場合、FTP/Telnet デコーダは状態を保存し、各パケットにセッション コンテキストを提供し、再構成されたセッションだけを検査します。選択されていない場合、セッション コンテキストなしで個々のパケットを分析します。

FTP データ転送を検査するには、このオプションを選択する必要があります。

暗号化トラフィックの検出（**Detect Encrypted Traffic**）

暗号化 Tenet および FTP セッションを検出します。

このオプションのイベントを生成するには、ルール 125:7 および 126:2 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

暗号化データの検査を続行（**Continue to Inspect Encrypted Data**）

プリプロセッサに対し、データ ストリームの暗号化後もデータ ストリームの検査を続行し、最終的にデコードされたデータを検索するように指示します。

グローバル FTP/Telnet オプションの設定

ライセンス：Protection

ステートレスまたはステートフル インスペクションを実行するかどうか、暗号化トラフィックを検出するかどうか、および暗号化されていると判定されたデータ ストリームの暗号化データの検査をデコーダが続行するかどうかを制御するために、FTP/Telnet デコーダのグローバル オプションを設定する必要があります。グローバル設定の詳細については、グローバル FTP および Telnet オプションについて（19-21 ページ）を参照してください。

グローバル オプションを設定するには、次の手順を実行します。

ステップ 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（  ）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

[詳細設定（Advanced Settings）] ページが表示されます。

ステップ 8　[アプリケーション層プロプロセッサ（Application Layer Preprocessors）] の下の [FTP と Telnet の構成（FTP and Telnet Configuration）] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[FTP と Telnet の構成（FTP and Telnet Configuration）] ページが表示されます。

ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ヒント　このページのその他オプションの設定の詳細については、Telnet オプションの設定（19-23 ページ）、サーバレベルの FTP オプションの設定（19-28 ページ）、および クライアントレベル FTP オプションの設定（19-32 ページ）を参照してください。

ステップ 9　（任意）[グローバル設定（Global Settings）] ページ領域の次の項目を変更できます。

- FTP パケットを含む再構成された TCP ストリームを検査するには、[ステートフル インスペクション（Stateful Inspection）] を選択します。再構成されていないパケットだけを検査するには、[ステートフル インスペクション（Stateful Inspection）] をクリアします。
- 暗号化トラフィックを検出するには、[暗号化トラフィックの検出（Detect Encrypted Traffic）] を選択します。暗号化トラフィックを無視するには、[暗号化トラフィックの検出（Detect Encrypted Traffic）] をクリアします。
- 必要に応じて、ストリームが再度復号され処理可能になる場合に備えて、暗号化後もストリームの検査を続行する場合は、[続行（Continue）] を選択します。

ステップ 10　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

Telnet オプションについて

ライセンス：Protection

FTP/Telnet デコーダによる Telnet コマンドの正規化を有効または無効にし、特定の異常ケースを有効または無効にし、許容可能な Are You There（AYT）攻撃数のしきい値を設定できます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート（**Ports**）

Telnet トラフィックを正規化するポートを示します。インターフェイスで、複数のポートをカンマで区切って指定します。

正規化（**Normalize**）

指定のポートへの Telnet トラフィックを正規化します。

異常検知（Detect Anomalies）

対応する SE（サブネゴシエーション終了）がない Telnet SB（サブネゴシエーション開始）の検出を有効にします。

Telnet がサポートするサブネゴシエーションは、SB（サブネゴシエーション開始）で開始し、SE（サブネゴシエーション終了）で終了していなければなりません。しかし、一部の Telnet サーバ実装では、対応する SE のない SB が無視されます。これは、回避事例につながるおそれのある異常な動作です。FTP はコントロール接続で Telnet プロトコルを使用するため、FTP もこの動作の影響を受けます。

この異常が Telnet トラフィックで検出される場合にイベントを生成するにはルール 126:3 を有効にし、FTP コマンド チャネルで検出される場合にイベントを生成するにはルール 125:9 を有効にできます。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

Are You There 攻撃のしきい値（**Are You There Attack Threshold Number**）

連続する AYT コマンドの数が指定のしきい値を超えた場合にそのことを検出します。シスコは、AYT しきい値に 20 以下の値を設定することを推奨します。

このオプションのイベントを生成するには、ルール 126:1 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

Telnet オプションの設定

ライセンス：Protection

正規化を有効または無効にし、特定の異常ケースを有効または無効にし、許容可能な Are You There（AYT）攻撃数のしきい値を制御することができます。Telnet オプションの詳細については、Telnet オプションについて（19-23 ページ）を参照してください。

Telnet オプションを設定するには、次の手順を実行します。

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ 8　[アプリケーション層プロプロセッサ（Application Layer Preprocessors）] の下の [FTP と Telnet の構成（FTP and Telnet Configuration）] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[FTP と Telnet の構成（FTP and Telnet Configuration）] ページが表示されます。

ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ヒント　このページのその他オプションの設定の詳細については、グローバル FTP/Telnet オプションの設定（19-21 ページ）、サーバレベルの FTP オプションの設定（19-28 ページ）、および クライアント レベル FTP オプションの設定（19-32 ページ）を参照してください。

ステップ 9　（任意）[Telnet 設定（Telnet Settings）] ページ領域の次の項目を変更できます。

- [ポート（Ports）] フィールドに、Telnet トラフィックをデコードする 1 つ以上のポートを指定します。通常、Telnet は TCP ポート 23 に接続します。複数のポートを指定する場合は、カンマで区切ります。

注意　暗号化トラフィック（SSL）はデコードできないので、ポート 22（SSH）を追加すると、予想外の結果が生じる可能性があります。

- Telnet 正規化を有効または無効にするには、Telnet プロトコル オプションの [正規化（Normalize）] チェック ボックスをオンまたはオフにします。
- 異常検出を有効または無効にするには、Telnet プロトコル オプションの [異常検知（Detect Anomalies）] チェック ボックスをオンまたはオフにします。
- 許容する連続 AYT コマンドの数を [Are You There 攻撃のしきい値（Are You There Attack Threshold Number）] に指定します。

ヒント　シスコは、AYT しきい値としてデフォルト値以下の値を設定することを推奨します。

ステップ 10　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

サーバレベルの FTP オプションについて

ライセンス：Protection

複数の FTP サーバでデコード オプションを設定できます。作成する各サーバ プロファイルには、トラフィックをモニタするサーバのサーバ IP アドレスとポートが含まれます。検証する FTP コマンドと、特定のサーバで無視する FTP コマンドを指定し、コマンドの最大パラメータ長を設定できます。また、デコーダが特定のコマンドで検証する特定のコマンド構文を設定し、代替最大コマンド パラメータ長を設定することもできます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ネットワーク

FTP サーバの 1 つ以上の IP アドレスを指定するには、このオプションを使用します。

1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。設定できる最大文字数は 1024 文字です。デフォルト プロファイルを含め最大 255 個のプロファイルを設定できます。ASA FirePOWER モジュールでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-4 ページ）を参照してください。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたはアドレス ブロックは指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

また、ターゲットベース ポリシーがトラフィックを処理するようにするには、識別するネットワークがターゲットベース ポリシーを設定するネットワーク分析ポリシーによって処理されるネットワーク、およびゾーンに一致するかまたはサブセットになっている必要があることにも注意してください。詳細については、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（17-3 ページ）を参照してください。

ポート

デバイスがトラフィックをモニタする FTP サーバのポートを指定するには、このオプションを使用します。インターフェイスで、複数のポートをカンマで区切って指定します。

File Get コマンド（File Get Commands）

サーバからクライアントにファイルを転送するために使用する FTP コマンドを定義するには、このオプションを使用します。サポートからの指示がない限り、これらの値を変更しないでください。

File Put コマンド（File Put Commands）

クライアントからサーバにファイルを転送するために使用する FTP コマンドを定義するには、このオプションを使用します。サポートからの指示がない限り、これらの値を変更しないでください。

追加 **FTP** コマンド（**Additional FTP Commands**）

デコーダが検出するコマンドを追加で指定するには、この行を使用します。複数のコマンドを追加する場合は、コマンドをスペースで区切ってください。

デフォルト最大パラメータ長（**Default Max Parameter Length**）

代替最大パラメータ長が設定されていないコマンドの最大パラメータ長を検出するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:3 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

代替最大パラメータ長（**Alternate Max Parameter Length**）

異なる最大パラメータ長を検出するコマンドを指定し、それらのコマンドの最大パラメータ長を指定するには、このオプションを使用します。[追加（Add）] をクリックして行を追加し、特定のコマンドで検出する異なる最大パラメータ長を指定します。

フォーマット文字列攻撃の検査コマンド（**Check Commands for String Format Attacks**）

指定されたコマンドでフォーマット文字列攻撃を検査するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:5 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

コマンドの妥当性（**Command Validity**）

特定のコマンドの有効な形式を入力するには、このオプションを使用します。FTP 通信の一部として受信したパラメータの構文を検証する FTP コマンド パラメータ検証ステートメントの作成については、FTP コマンド パラメータ検証ステートメントの作成（19-27 ページ）を参照してください。[追加（Add）] をクリックして、コマンド検証行を追加します。

このオプションのイベントを生成するには、ルール 125:2 および 125:4 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

FTP 転送を無視（**Ignore FTP Transfers**）

データ転送チャネルで状態インスペクション以外のすべてのインスペクションを無効にして FTP データ転送のパフォーマンスを改善するには、このオプションを使用します。

FTP コマンドでの **Telnet** エスケープ コードの検出（**Detect Telnet Escape Codes within FTP Commands**）

FTP コマンド チャネルで Telnet コマンドが使用された場合にそのことを検出するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:1 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

正規化時に消去コマンドを無視（**Ignore Erase Commands during Normalization**）

[FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）] が選択されている場合に、FTP トラフィックの正規化時に Telnet の文字および行の消去コマンドを無視するには、このオプションを使用します。この設定は、FTP サーバによる Telnet 消去コマンドの処理方法と一致する必要があります。一般に、新しい FTP サーバは Telnet 消去コマンドを無視しますが、ほとんどの古いサーバは Telnet 消去コマンドを処理する点に注意してください。

トラブルシューティング：**FTP** コマンドの検証設定のログを記録（**Troubleshooting Options**：**Log FTP Command Validation Configuration**）

トラブルシューティングについてサポートに問い合わせた際に、サーバ用にリストされている FTP コマンドごとに設定情報を出力するように、システムを設定することを指示される場合があります。

注意　このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響を与えるので、サポートからガイダンスを受けた場合にのみ変更してください。

FTP コマンド パラメータ検証ステートメントの作成

ライセンス：Protection

FTP コマンドに対する検証ステートメントを設定するときには、複数の代替パラメータをスペースで区切って指定できます。2 つのパラメータ間にバイナリ OR 関係を作成するには、検証ステートメントでこの 2 つのパラメータをパイプ文字（|）で区切って指定します。パラメータを大カッコ（[]）で囲むと、これらのパラメータがオプションであることを示します。パラメータを中カッコ（{}）で囲むと、これらのパラメータが必須であることを示します。

FTP 通信の一部として受信したパラメータの構文を検証する FTP コマンド パラメータ検証ステートメントを作成できます。詳細については、サーバレベルの FTP オプションについて（19-25 ページ）を参照してください。

FTP コマンド パラメータ検証ステートメントに使用できるパラメータを次の表に示します。

表 *19-5*　*FTP* コマンド パラメータ

使用するパラメータ	実行される検証
`int`	示されるパラメータが整数である必要があります。
`number`	示されるパラメータが 1 ～ 255 の範囲内の整数である必要があります。
`char` *_chars*	示されるパラメータが単一文字であり、かつ `_chars` 引数に指定した文字の 1 つである必要があります。 たとえば、検証引数 `char SBC` を使用して `MODE` のコマンド検証を定義すると、`MODE` コマンドのパラメータが、文字 `S`（Stream モードを示す）、文字 `B`（Block モードを示す）、または文字 `C`（Compressed モードを示す）を含んでいるかどうかが検証されます。
`date _datefmt`	`_datefmt` に `#` が含まれている場合、示されるパラメータは数値である必要があります。 `_datefmt` に `C` が含まれている場合、示されるパラメータは文字である必要があります。 `_datefmt` にリテラル文字列が含まれている場合、示されるパラメータはリテラル文字列に一致している必要があります。
`string`	示されるパラメータが文字列である必要があります。
`host_port`	示されるパラメータは、RFC 959（Network Working Group による File Transfer Protocol 仕様）で定義されている有効なホスト ポート指定子である必要があります。

上記の表の構文を必要に応じて組み合わせることにより、トラフィックを検証する必要がある各 FTP コマンドを正しく検証するパラメータ検証ステートメントを作成できます。

（注）　TYPE コマンドに複合式を含める場合は、式をスペースで囲んでください。また、式内の各オペランドをスペースで囲んでください。たとえば、`char A|B` ではなく `char A | B` と入力します。

サーバレベルの FTP オプションの設定

ライセンス：Protection

サーバ レベルでさまざまなオプションを設定できます。追加する FTP サーバごとに、モニタ対象のポート、検証対象のコマンド、コマンドのデフォルト最大パラメータ長、特定のコマンドの代替パラメータ長、および特定のコマンドの検証構文を指定できます。また、FTP チャネルでフォーマット文字列攻撃や Telnet コマンドを調べるかどうか、および各コマンドの設定情報を出力するかどうかを選択できます。サーバレベルの FTP オプションの詳細については、サーバレベルの FTP オプションについて（19-25 ページ）を参照してください。

サーバレベルの **FTP** オプションの設定方法：

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **4**　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ **5**　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ **6**　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ **7**　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ **8**　[アプリケーション層プロプロセッサ（Application Layer Preprocessors）] の下の [FTP と Telnet の構成（FTP and Telnet Configuration）] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[FTP と Telnet の構成（FTP and Telnet Configuration）] ページが表示されます。

ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ヒント　このページのその他オプションの設定の詳細については、グローバル FTP/Telnet オプションの設定（19-21 ページ）、Telnet オプションの設定（19-23 ページ）、および クライアントレベル FTP オプションの設定（19-32 ページ）を参照してください。

ステップ 9　次の 2 つの対処法があります。

- 新しいサーバ プロファイルを追加します。ページの左側で [FTP サーバ（FTP Server）] の横にある追加アイコン（ ）をクリックします。[ターゲットの追加（Add Target）] ポップアップ ウィンドウが表示されます。クライアントの 1 つ以上の IP アドレスを [サーバ アドレス（Server Address）] フィールドに指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト ポリシーを含め最大 255 個のポリシーを設定できます。ASA FirePOWER モジュールでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-4 ページ）を参照してください。

  ターゲットベース ポリシーがトラフィックを処理するようにするには、識別するネットワークがターゲットベース ポリシーを設定するネットワーク分析ポリシーによって処理されるネットワーク、およびゾーンに一致するかまたはサブセットになっている必要があることに注意してください。詳細については、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（17-3 ページ）を参照してください。

  ページの左側の FTP サーバのリストに新しい項目が表示され、選択されていることを示すために強調表示されます。[設定（Configuration）] セクションが更新され、追加したプロフィールの現行設定が反映されます。

- 既存のサーバ プロファイルの設定を変更します。ページ左側の [FTP サーバ（FTP Server）] の下で追加したプロファイルの設定済みアドレスをクリックするか、または [デフォルト（default）] をクリックします。

  選択した項目が強調表示され、[設定（Configuration）] セクションが更新され、選択したプロファイルの現行設定が表示されます。既存のプロファイルを削除するには、削除するプロファイルの横にある削除アイコン（ ）をクリックします。

ステップ 10　（任意）[設定（Configuration）] ページ領域の次の項目を変更できます。

- [ネットワーク（Networks）] フィールドにリストされているアドレスを変更し、ページの他の領域をクリックします。

  ページの左側で、強調表示されているアドレスが更新されます。

  デフォルト プロファイルでは [ネットワーク（Network）] の設定を変更できないことに注意してください。デフォルト プロファイルは、別のプロファイルで指定されていないネットワーク上のすべてのサーバに適用されます。

- FTP トラフィックをモニタするポートを指定します。ポート 21 は FTP トラフィック用のウェルノウン ポートです。

- [File Get コマンド（File Get Commands）] フィールドで、サーバからクライアントにファイルを転送するために使用される FTP コマンドを更新します。

- [File Put コマンド（File Put Commands）] フィールドで、クライアントからサーバにファイルを転送するために使用される FTP コマンドを更新します。

（注）　サポートからの指示がない限り、[File Get コマンド（File Get Commands）] フィールドと [File Put コマンド（File Put Commands）] フィールドの値は変更しないでください。

- FTP/Telnet プリプロセッサによりデフォルトで検査される FTP コマンド以外に、追加の FTP コマンドを検出するには、[追加 FTP コマンド（Additional FTP Commands）] フィールドに、コマンドをスペースで区切って入力します。

  追加 FTP コマンドは、必要な数だけ追加できます。

（注）　追加できるコマンドには、XPWD、XCWD、XCUP、XMKD、XRMD があります。これらのコマンドの詳細については、RFC 775（Network Working Group によるディレクトリに基づく FTP コマンドの仕様）を参照してください。

- [デフォルト最大パラメータ長（Default Max Parameter Length）] フィールドに、コマンド パラメータの最大長をバイト数で指定します。
- 特定のコマンドで異なる最大パラメータ長を検出するには、[代替最大パラメータ長（Alternate Max Parameter Length）] の横の [追加（Add）] をクリックします。表示される行の最初のテキスト ボックスに、最大パラメータ長を指定します。2 番目のテキスト ボックスに、この代替最大パラメータ長を適用するコマンドをスペースで区切って指定します。

  代替最大パラメータ長は、必要な数だけ追加できます。
- 特定のコマンドでフォーマット文字列攻撃を検査するには、[フォーマット文字列攻撃の検査コマンド（Check Commands for String Format Attacks）] テキスト ボックスにコマンドをスペースで区切って指定します。
- コマンドの有効な形式を指定するには、[コマンドの妥当性（Command Validity）] の横の [追加（Add）] をクリックします。検証対象のコマンドを指定してから、コマンド パラメータの検証ステートメントを入力します。検証ステートメントの構文の詳細については、サーバレベルの FTP オプションについて（19-25 ページ）を参照してください。
- データ転送チャネルで状態インスペクション以外のすべてのインスペクションを無効にして、FTP データ転送のパフォーマンスを改善するには、[FTP 転送を無視（Ignore FTP Transfers）] を有効にします。

（注）　データ転送を検査するには、グローバル FTP/Telnet オプション [ステートフル インスペクション（Stateful Inspection）] を選択する必要があります。グローバル オプションの設定の詳細については、グローバル FTP および Telnet オプションについて（19-21 ページ）を参照してください。

- Telnet コマンドが FTP コマンド チャネルで使用された場合にそのことを検出するには、[FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）] を選択します。
- FTP トラフィックの正規化時に Telnet の文字消去コマンドおよび行消去コマンドを無視するには、[正規化時に消去コマンドを無視（Ignore Erase Commands during Normalization）] を有効にします。

ステップ 11　サポートから指示された場合にのみ、オプションで、関連するトラブルシューティング オプションを変更します。そのためには、[トラブルシューティング オプション（Troubleshooting Options）] の横にある [+] 記号をクリックします。

ステップ 12　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

クライアントレベルの FTP オプションについて

ライセンス：Protection

FTP クライアントのプロファイルを作成できます。各プロファイル内で、クライアントからの FTP 応答の最大応答長を指定できます。また、デコーダが特定のクライアントの FTP コマンド チャネルでのバウンス攻撃と telnet コマンドの使用を検出するかどうかを設定できます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ネットワーク

FTP クライアントの 1 つ以上の IP アドレスを指定するには、このオプションを使用します。

1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト プロファイルを含め最大 255 個のプロファイルを設定できます。ASA FirePOWER モジュールでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-4 ページ）を参照してください。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたはアドレス ブロックは指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

また、ターゲットベース ポリシーがトラフィックを処理するようにするには、識別するネットワークがターゲットベース ポリシーを設定するネットワーク分析ポリシーによって処理されるネットワーク、およびゾーンに一致するかまたはサブセットになっている必要があることにも注意してください。詳細については、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（17-3 ページ）を参照してください。

最大応答長（**Max Response Length**）

FTP クライアントからの応答文字列の最大長を指定するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:6 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

FTP バウンス試行の検出（**Detect FTP Bounce Attempts**）

FTP バウンス攻撃を検出するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:8 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

FTP バウンスの許可（**Allow FTP Bounce to**）

FTP PORT コマンドを FTP バウンス攻撃として扱わない追加のホストとそれらのホスト上のポートのリストを設定するには、このオプションを使用します。

FTP コマンドでの **Telnet** エスケープ コードの検出（**Detect Telnet Escape Codes within FTP Commands**）

FTP コマンド チャネルで Telnet コマンドが使用された場合にそのことを検出するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:1 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

正規化時に消去コマンドを無視（**Ignore Erase Commands during Normalization**）

[FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）] が選択されている場合に、FTP トラフィックの正規化時に Telnet の文字および行の消去コマンドを無視するには、このオプションを使用します。この設定は、FTP クライアントによる Telnet 消去コマンドの処理方法に一致している必要があります。一般に、新しい FTP クライアントは Telnet 消去コマンドを無視しますが、ほとんどの古いクライアントは Telnet 消去コマンドを処理する点に注意してください。

クライアントレベル FTP オプションの設定

ライセンス：Protection

クライアントからの FTP トラフィックをモニタするように、FTP クライアントのクライアント プロファイルを設定できます。クライアントをモニタするために設定できるオプションの詳細については、クライアントレベルの FTP オプションについて（19-31 ページ）を参照してください。Telnet オプションの詳細については、Telnet オプションについて（19-23 ページ）を参照してください。その他の FTP オプションの詳細については、サーバレベルの FTP オプションについて（19-25 ページ）およびグローバル FTP および Telnet オプションについて（19-21 ページ）を参照してください。

クライアントレベルの **FTP** オプションの設定方法：

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **4**　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ **5**　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ **6**　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ **7**　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ 8　[アプリケーション層プロプロセッサ（Application Layer Preprocessors）] の下の [FTP と Telnet の構成（FTP and Telnet Configuration）] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[FTP と Telnet の構成（FTP and Telnet Configuration）] ページが表示されます。

ステップ 9　次の 2 つの対処法があります。

- 新しいクライアント プロファイルを追加します。ページの左側で [FTP クライアント（FTP Client）] の横にある追加アイコン（ ）をクリックします。[ターゲットの追加（Add Target）] ポップアップ ウィンドウが表示されます。クライアントの 1 つ以上の IP アドレスを [クライアント アドレス（Client Address）] フィールドに指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト ポリシーを含め最大 255 個のポリシーを設定できます。ASA FirePOWER モジュールでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-4 ページ）を参照してください。

  ターゲットベース ポリシーがトラフィックを処理するようにするには、識別するネットワークがターゲットベース ポリシーを設定するネットワーク分析ポリシーによって処理されるネットワーク、およびゾーンに一致するかまたはサブセットになっている必要があることに注意してください。詳細については、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（17-3 ページ）を参照してください。

  ページの左側の FTP クライアントのリストに新しい項目が表示され、選択されていることを示すために強調表示されます。[設定（Configuration）] セクションが更新され、追加したプロフィールの現行設定が反映されます。

- 既存のクライアント プロファイルの設定を変更します。ページ左側の [FTP クライアント（FTP Client）] の下で追加したプロファイルの設定済みアドレスをクリックするか、または [デフォルト（default）] をクリックします。

  選択した項目が強調表示され、[設定（Configuration）] セクションが更新され、選択したプロファイルの現行設定が表示されます。既存のプロファイルを削除するには、削除するプロファイルの横にある削除アイコン（ ）をクリックします。

ステップ 10　（任意）[設定（Configuration）] ページ領域の次の項目を変更できます。

- オプションで、[ネットワーク（Networks）] フィールドにリストされているアドレスを変更し、ページの他の領域をクリックします。

  ページの左側で、強調表示されているアドレスが更新されます。

  デフォルト プロファイルでは [ネットワーク（Network）] の設定を変更できないことに注意してください。デフォルト プロファイルは、別のプロファイルで指定されていないネットワーク上のすべてのクライアント ホストに適用されます。

- [最大応答長（Max Response Length）] フィールドに、FTP クライアントからの応答の最大長をバイト単位で指定します。

- FTP バウンス攻撃を検出するには、[FTP] を選択します。

  FTP/Telnet デコーダは、FTP PORT コマンドが発行されたとき、指定のホストがクライアントの指定のホストと一致しない場合にそのことを検出します。

- FTP PORT コマンドを FTP バウンス攻撃として扱わない追加のホストとポートのリストを設定するには、[FTP バウンスの許可（Allow FTP Bounce to）] フィールドに、各ホスト（または CIDR 形式のネットワーク）、コロン（:）、およびポートまたはポート範囲をこの順序で指定します。ホストのポート範囲を入力するには、範囲の開始ポートと範囲の最終ポートをダッシュ（-）でつなげて表します。複数のホストを入力するには、ホスト項目をカンマで区切って入力します。

たとえば、ホスト 192.168.1.1 に対する FTP PORT コマンドをポート 21 で許可し、ホスト 192.168.1.2 に対するコマンドをポート 22 ～ 1024 のいずれかで許可するには、次のように入力します。

```
192.168.1.1:21, 192.168.1.2:22-1024
```

ASA FirePOWER モジュール で CIDR 表記およびプレフィクス長を使用する方法の詳細については、IP アドレスの表記規則（1-4 ページ）を参照してください。

（注）　1 つのホストの個々の複数のポートを指定するには、ポート定義ごとにホストの IP アドレスを繰り返す必要があります。たとえば、192.168.1.1 のポート 22 と 25 を指定するには、`192.168.1.1:22, 192.168.1.1:25` と入力します。

- Telnet コマンドが FTP コマンド チャネルで使用された場合にそのことを検出するには、[FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）] を選択します。
- FTP トラフィックの正規化時に Telnet の文字消去コマンドおよび行消去コマンドを無視するには、[正規化時に消去コマンドを無視（Ignore Erase Commands During Normalization）] を選択します。

ステップ 11　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

HTTP トラフィックのデコード

ライセンス：Protection

HTTP Inspect プリプロセッサは、次の処理を行います。

- ネットワーク上の Web サーバに送信される HTTP 要求と Web サーバから受信する HTTP 応答をデコードおよび正規化する。
- HTTP 関連の侵入ルールのパフォーマンス向上のために、Web サーバに送信されたメッセージを URI、非 cookie ヘッダー、cookie ヘッダー、メソッド、メッセージ ボディの各コンポーネントに分ける。
- HTTP 関連の侵入ルールのパフォーマンス向上のために、Web サーバから受信したメッセージをステータス コード、ステータス メッセージ、非 set-cookie ヘッダー、cookie ヘッダー、および応答ボディの各コンポーネントに分ける。
- URI エンコード攻撃の可能性を検出する。
- 正規化データを追加ルール処理に使用できるようにする。

HTTP トラフィックはさまざまな形式でエンコードされている可能性があり、このことが、ルールによる適切な検査の実施を困難にしています。HTTP Inspect は 14 種類のエンコードをデコードし、HTTP トラフィックが最良のインスペクションを受けられるようにします。

HTTP Inspect のオプションは、グローバルに設定するか、1 つのサーバで設定するか、またはサーバ リストに対して設定することができます。

HTTP Inspect プリプロセッサを使用するときは、次の点に注意してください。

- プリプロセッサ エンジンは HTTP の正規化をステートレスに実行します。つまり、パケット単位で HTTP 文字列を正規化し、TCP ストリーム プリプロセッサにより再構成された HTTP 文字列のみを処理できます。

- ジェネレータ ID（GID）119 の HTTP プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があります。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

詳細については、次の各項を参照してください。

- グローバル HTTP 正規化オプションの選択（19-35 ページ）
- グローバル HTTP 設定オプションの設定（19-36 ページ）
- サーバレベル HTTP 正規化オプションの選択（19-37 ページ）
- サーバレベル HTTP 正規化エンコード オプションの選択（19-45 ページ）
- HTTP サーバ オプションの設定（19-48 ページ）
- 追加の HTTP Inspect プリプロセッサ ルールの有効化（19-50 ページ）

グローバル HTTP 正規化オプションの選択

ライセンス：Protection

HTTP Inspect プリプロセッサのグローバル HTTP オプションは、プリプロセッサの機能を制御します。Web サーバ ポートとして指定されていないポートが HTTP トラフィックを受信する場合の HTTP 正規化を有効または無効にするには、このオプションを使用します。

次の点に注意してください。

- [無制限の圧縮解除（Unlimited Decompression）] を有効にすると、変更のコミット時に [圧縮データの最大深さ（Maximum Compressed Data Depth）] および [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] オプションが自動的に 65535 に設定されます。詳細については、サーバレベル HTTP 正規化オプションの選択（19-37 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と、アクセス コントロール ルールに関連付けられている侵入ポリシーで、[圧縮データの最大深さ（Maximum Compressed Data Depth）] と [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] オプションの値が異なる場合は、最も大きな値が使用されます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

異常な **HTTP** サーバの検出（**Detect Anomalous HTTP Servers**）

Web サーバ ポートとして指定されていないポートに送信された HTTP トラフィックまたはこのポートで受信した HTTP トラフィックを検出します。

（注）　このオプションをオンにする場合は、[HTTP 設定（HTTP Configuration）] ページで、HTTP トラフィックを受信するすべてのポートがサーバ プロファイルにリストされていることを確認してください。確認せずにこのオプションと関連するプリプロセッサ ルールを有効にすると、サーバとの間の通常のトラフィックによってイベントが生成されます。デフォルトのサーバ プロファイルには、HTTP トラフィックに一般に使用されるすべてのポートが含まれていますが、このプロファイルを変更した場合は、イベントの生成を防ぐために別のプロファイルにそれらのポートを追加する必要があります。

このオプションのイベントを生成するには、ルール 120:1 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

HTTP プロキシ サーバの検出（**Detect HTTP Proxy Servers**）

[HTTP プロキシの使用を許可（Allow HTTP Proxy Use）] オプションで定義されていないプロキシ サーバを使用する HTTP トラフィックを検出します。

このオプションのイベントを生成するには、ルール 119:17 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

圧縮データの最大深さ（**Maximum Compressed Data Depth**）

[圧縮データの検査（Inspect Compressed Data）]（および任意で、[SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））]、[SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））]、または [PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））]）が有効な場合に、圧縮解除する圧縮データの最大サイズを設定します。指定できるバイト数は 1 ～ 65535 です。

圧縮解除データの最大深さ（**Maximum Decompressed Data Depth**）

[圧縮データの検査（Inspect Compressed Data）]（および任意で、[SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））]、[SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））]、または [PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））]）が有効な場合に、正規化された圧縮データの最大サイズを設定します。指定できるバイト数は 1 ～ 65535 です。

グローバル **HTTP** 設定オプションの設定

ライセンス：Protection

非標準ポートへの HTTP トラフィックとプロキシ サーバを使用する HTTP トラフィックの検出を設定できます。グローバル HTTP 設定オプションの詳細については、グローバル HTTP 正規化オプションの選択（19-35 ページ）を参照してください。

グローバル **HTTP** 設定オプションを設定するには、次の手順を実行します。

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **4**　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ **5**　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ 8　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [HTTP 設定（HTTP Configuration）] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[HTTP 設定（HTTP Configuration）] ページが表示されます。

ステップ 9　グローバル HTTP 正規化オプションの選択（19-35 ページ）で説明するグローバル オプションを変更できます。

ステップ 10　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

サーバレベル HTTP 正規化オプションの選択

ライセンス：Protection

サーバレベルのオプションは、モニタ対象サーバごとに設定するか、すべてのサーバに対してグローバルに設定するか、またはサーバ リストに対して設定することができます。また、事前定義のサーバ プロファイルを使用してこれらのオプションを設定するか、またはご使用の環境のニーズに合わせて個別に設定することができます。これらのオプション、またはこれらのオプションを設定するデフォルト プロファイルの 1 つを使用して、トラフィックを正規化する HTTP サーバ ポート、正規化するサーバ応答ペイロードの量、および正規化するエンコードのタイプを指定します。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ネットワーク

1 つ以上のサーバの IP アドレスを指定するには、このオプションを使用します。1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。

デフォルト プロファイルを含めてプロファイルの合計数は最大 255 ですが、さらに、HTTP サーバ リストに最大 496 文字（約 26 エントリ）を含めることができ、すべてのサーバ プロファイルに対して合計 256 のアドレス エントリを指定できます。ASA FirePOWER モジュール での IPv4 CIDR 表記と IPv6 プレフィクス長の使用法については、IP アドレスの表記規則（1-4 ページ）を参照してください。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

また、ターゲットベース ポリシーがトラフィックを処理するようにするには、識別するネットワークがターゲットベース ポリシーを設定するネットワーク分析ポリシーによって処理されるネットワーク、およびゾーンに一致するかまたはサブセットになっている必要があることにも注意してください。詳細については、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（17-3 ページ）を参照してください。

ポート

プリプロセッサ エンジンが HTTP トラフィックを正規化するポート。ポート番号が複数ある場合は、カンマで区切ります。

サイズ超過のディレクトリ長（**Oversize Dir Length**）

指定された値よりも長い URL ディレクトリを検出します。

このオプションのイベントを生成するには、ルール 119:15 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

クライアント フローの深さ（**Client Flow Depth**）

[ポート（Ports）] で定義されているクライアント側 HTTP トラフィックについて、ルールで検査される raw HTTP パケットのバイト数（ヘッダーとペイロード データを含む）を指定します。ルール内の HTTP コンテンツ ルール オプションによって要求メッセージの特定の部分が検査される場合は、[クライアント フローの深さ（Client Flow Depth）] は適用されません。詳細については、HTTP コンテンツ オプション（27-24 ページ）を参照してください。

-1 ～ 1460 の値を指定できます。シスコは、[クライアント フローの深さ（Client Flow Depth）] をその最大値に設定することを推奨しています。次のいずれかを指定します。

- 1 ～ 1460 を指定すると、最初のパケットで指定のバイト数が検査されます。最初のパケットのバイト数が指定のバイト数よりも少ない場合は、パケット全体が検査されます。指定された値は、セグメント化されたパケットと再構成されたパケットの両方に適用されることに注意してください。

  また、値 300 を指定すると、通常は、多くのクライアント要求ヘッダーの終わりにある大きな HTTP Cookie のインスペクションが排除されることにも注意してください。

- 0 を指定すると、すべてのクライアント側トラフィックが検査されます。これにはセッション内の複数のパケットが含まれ、必要な場合には 1460 バイトの制限を超えることもあります。この値はパフォーマンスに影響する可能性があることに注意してください。

- -1 を指定すると、クライアント側のすべてのトラフィックが無視されます。

サーバ フローの深さ（**Server Flow Depth**）

[ポート（Ports）] で指定されたサーバ側 HTTP トラフィックについて、ルールで検査される raw HTTP パケットのバイト数を指定します。[HTTP 応答の検査（Inspect HTTP Responses）] が無効である場合は raw ヘッダーとペイロードが検査され、[HTTP 応答の検査（Inspect HTTP Response）] が有効である場合は、raw 応答ボディのみが検査されます。

[サーバ フローの深さ（Server Flow Depth）] では、[ポート（Ports）] で定義されているサーバ側 HTTP トラフィックについて、ルールで検査されるセッション内の raw サーバ応答データのバイト数を指定します。このオプションを使用して、HTTP サーバ応答データのインスペクションのレベルとパフォーマンスのバランスを調整できます。ルール内の HTTP コンテンツ オプションによって要求メッセージの特定の部分が検査される場合は、Server Flow Depth は適用されません。詳細については、HTTP コンテンツ オプション（27-24 ページ）を参照してください。

クライアント フローの深さ（Client Flow Depth）とは異なり、サーバ フローの深さ（Server Flow Depth）では、ルールが検査するバイト数を、HTTP 要求パケットごとではなく、HTTP 応答ごとのバイト数として指定します。

-1 ～ 65535 の値を指定できます。シスコは、[サーバ フローの深さ（Server Flow Depth）] をその最大値に設定することを推奨しています。次のいずれかの値を指定できます。

- 1 ～ 65535 の範囲の値:

  [HTTP 応答の検査（Inspect HTTP Responses）] が有効である場合、raw HTTP 応答ボディのみが検査され、raw HTTP ヘッダーは検査されません。また、[圧縮データの検査（Inspect Compressed Data）] が有効である場合は、圧縮解除データも検査されます。

  [HTTP 応答の検査（Inspect HTTP Responses）] が無効である場合、raw パケット ヘッダーとペイロードが検査されます。

  セッションの応答バイト数が指定の値よりも少ない場合は、そのセッションで、ルールにより（必要に応じて複数パケットにわたって）すべての応答パケットが完全に検査されます。セッションの応答バイト数が指定の値よりも多い場合、そのセッションで、ルールにより（必要に応じて複数パケットにわたって）指定のバイト数だけが検査されます。

  フローの深さ（Flow Depth）の値が小さいと、[ポート（Ports）] で定義されているサーバ側トラフィックを対象とするルールで、検出漏れが発生する可能性があります。これらのルールのほとんどは HTTP ヘッダーまたはコンテンツ（通常、非ヘッダー データの先頭の約 100 バイト以内）を対象とします。通常はヘッダーの長さは 300 バイト未満ですが、ヘッダー サイズは異なることがあります。

  指定された値は、セグメント化されたパケットと再構成されたパケットの両方に適用されることにも注意してください。

- 0 を指定すると、[ポート（Port）] で定義されているすべての HTTP サーバ側トラフィックでパケット全体が検査されます。これにはセッションでの 65535 バイトよりも大きな応答データも含まれます。

  この値はパフォーマンスに影響する可能性があることに注意してください。

- -1

  [HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合、raw HTTP ヘッダーだけが検査され、raw HTTP 応答ボディは検査されません。

  [HTTP 応答の検査（Inspect HTTP Responses）] が無効である場合、[ポート（Ports）] で定義されているすべてのサーバ側トラフィックは無視されます。

最大ヘッダー長（**Maximum Header Length**）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効である場合は、HTTP 要求、および HTTP 応答で、指定されている最大バイト数よりも長いヘッダー フィールドを検出します。値 0 を指定すると、このオプションが無効になります。有効にするには、1 ～ 65535 の値を指定します。

このオプションのイベントを生成するには、ルール 119:19 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

最大ヘッダー数（**Maximum Number of Headers**）

HTTP 要求でヘッダー数がこの設定を超えている場合にそのことを検出します。有効にするには、1 ～ 1024 の値を指定します。

このオプションのイベントを生成するには、ルール 119:20 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

最大スペース数（**Maximum Number of Spaces**）

折りたたみ行のスペースの数が HTTP 要求のこの設定と等しいか、超えている場合にそのことを検出します。値 0 を指定すると、このオプションが無効になります。有効にするには、1 ～ 65535 の値を指定します。

このオプションのイベントを生成するには、ルール 119:26 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

HTTP クライアント ボディの抽出の深さ（**HTTP Client Body Extraction Depth**）

HTTP クライアント要求のメッセージ ボディから抽出するバイト数を指定します。侵入ルールを使用して抽出データを検査するには、`content` または `protected_content` キーワードを [HTTP クライアント ボディ（HTTP Client Body）] オプションと共に選択します。詳細については、HTTP コンテンツ オプション（27-24 ページ）を参照してください。

-1 ～ 65495 の値を指定します。クライアント ボディを無視するには、-1 を指定します。クライアント ボディ全体を抽出するには、0 を指定します。抽出対象のバイト数を指定すると、システム パフォーマンスが向上することがある点に注意してください。また、侵入ルールで [HTTP クライアント ボディ（HTTP Client Body）] オプションが機能するためには、0 ～ 65495 の値を指定する必要があります。

小さいチャンク サイズ（**Small Chunk Size**）

チャンクが小さいとみなされるサイズの最大バイト数を指定します。1 ～ 255 の値を指定します。値 0 を指定すると、異常な小さなセグメントの連続の検出が無効になります。詳細については、[連続する小さいチャンク（Consecutive Small Chunks）] オプションを参照してください。

連続する小さいチャンク（**Consecutive Small Chunks**）

チャンク転送エンコードを使用するクライアント トラフィックまたはサーバ トラフィックで異常に大量であるとみなされる、連続する小さなチャンクの数を指定します。[小さいチャンク サイズ（Small Chunk Size）] オプションは、小さなチャンクの最大サイズを指定します。

たとえば、10 バイト以下のチャンクが 5 つ連続していることを検出するには、[小さいチャンク サイズ（Small Chunk Size）] に 10 を設定し、[連続する小さいチャンク（Consecutive Small Chunks）] に 5 を設定します。

大量の小さなチャンクが検出される場合にイベントをトリガーするには、クライアント トラフィックの場合はプリプロセッサ ルール 119:27 を有効にし、サーバ トラフィックの場合はルール 120:7 を有効にします。[小さいチャンク サイズ（Small Chunk Size）] が有効であり、このオプションが 0 または 1 に設定されている場合にこれらのルールを有効にすると、指定されたサイズ以下のすべてのチャンクでイベントがトリガーとして使用されます。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

HTTP メソッド（**HTTP Methods**）

システムがトラフィックで検出すると予期される、GET および POST 以外の HTTP 要求メソッドを指定します。複数の値はカンマで区切ります。

侵入ルールでは、HTTP メソッドのコンテンツを検索するために、`content` または `protected_content` キーワードが **HTTP Method** 引数と共に使用されます。HTTP コンテンツ オプション（27-24 ページ）を参照してください。GET、POST、およびこのオプションで設定されているメソッド以外のメソッドがトラフィックで検出される場合にイベントを生成するには、ルール 119:31 を有効にします。

アラートなし（**No Alerts**）

関連するプリプロセッサ ルールが有効である場合に、侵入イベントを無効にします。

（注）　このオプションでは、HTTP 標準テキスト ルールと共有オブジェクトのルールは無効になりません。

HTTP ヘッダーの正規化（**Normalize HTTP Headers**）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合は、要求ヘッダーと応答ヘッダーの非 cookie データの正規化が有効になります。[HTTP 応答の検査（Inspect HTTP Responses）] が有効ではない場合は、要求ヘッダーと応答ヘッダーで cookie を含む HTTP ヘッダー全体の正規化が有効になります。

HTTP Cookie の検査（**Inspect HTTP Cookies**）

HTTP 要求ヘッダーからの cookie の抽出を有効にします。また、[HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合は、応答ヘッダーからの set-cookie データの抽出も有効になります。cookie の抽出が不要な場合は、このオプションを無効にするとパフォーマンスが向上します。

`Cookie:` および `Set-Cookie:` のヘッダー名、ヘッダー行の先頭のスペース、およびヘッダー行の末尾の `CRLF` は、cookie の一部ではなくヘッダーの一部として検査されます。

HTTP ヘッダーの **Cookie** の正規化（**Normalize Cookies in HTTP headers**）

HTTP 要求ヘッダーの cookie の正規化を有効にします。[HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合は、応答ヘッダーの set-cookie データの正規化も有効になります。このオプションを選択する前に、[HTTP Cookie の検査（Inspect HTTP Cookies）] を選択する必要があります。

HTTP プロキシの使用を許可（**Allow HTTP Proxy Use**）

モニタ対象 Web サーバを HTTP プロキシとして使用できるようにします。このオプションは、HTTP 要求のインスペクションでのみ使用されます。

URI のみの検査（**Inspect URI Only**）

正規化された HTTP 要求パケットの URI 部分のみを検査します。

HTTP 応答の検査（**Inspect HTTP Responses**）

HTTP 応答の拡張インスペクションが有効になり、プリプロセッサは、HTTP 要求メッセージのデコードと正規化の他に、ルール エンジンによるインスペクションのために応答フィールドを抽出します。このオプションを有効にすると、応答ヘッダー、ボディ、ステータス コードなどがシステムにより抽出されます。また [HTTP Cookie の検査（Inspect HTTP Cookies）] が有効な場合は、set-cookie データも抽出されます。詳細については、HTTP コンテンツ オプション（27-24 ページ）、HTTP エンコードのタイプと位置によるイベントの生成（27-98 ページ）、および特定のペイロード タイプを指し示す（27-102 ページ）を参照してください。

このオプションのイベントを生成するには、ルール 120:2 および 120:3 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

UTF エンコードを **UTF-8** に正規化（**Normalize UTF Encodings to UTF-8**）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合、HTTP 応答内の UTF-16LE、UTF-16BE、UTF-32LE、および UTF32-BE エンコードが検出され、UTF-8 に正規化されます。

このオプションのイベントを生成するには、ルール 120:4 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

圧縮データの検査（**Inspect Compressed Data**）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合は、HTTP 応答ボディ内の gzip および deflate 互換圧縮データの圧縮解除と、正規化された圧縮解除データのインスペクションが有効になります。システムは、チャンク HTTP 応答データと非チャンク HTTP 応答データを検査します。システムは、必要に応じて複数のパケットにわたり圧縮解除データをパケット単位で検査します。つまり、システムが異なるパケットの圧縮解除データをインスペクションのために結合させることはありません。[圧縮データの最大深さ（Maximum Compressed Data Depth）]、[圧縮解除データの最大深さ（Maximum Decompressed Data Depth）]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバ フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、`file_data` ルール キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（27-102 ページ）を参照してください。

無制限の圧縮解除（**Unlimited Decompression**）

[圧縮データの検査（Inspect Compressed Data）]（および任意で、[SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））]、[SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））]、または [PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））]）が有効な場合、複数のパケットにわたって [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] がオーバーライドされます。つまり、このオプションにより、複数のパケットにわたる無制限の圧縮解除が有効になります。このオプションを有効にしても、単一パケット内での [圧縮データの最大深さ（Maximum Compressed Data Depth）] または [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] には影響しないことに注意してください。また、このオプションを有効にすると、変更のコミット時に、[圧縮データの最大深さ（Maximum Compressed Data Depth）] と [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] が 65535 に設定されることにも注意してください。グローバル HTTP 正規化オプションの選択（19-35 ページ）を参照してください。

Javascript の正規化（**Normalize Javascript**）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合、HTTP 応答ボディ内での Javascript の検出と正規化を有効にします。プリプロセッサは unescape 関数や decodeURI 関数、String.fromCharCode メソッドなどの難読化 Javascript データを正規化します。プリプロセッサは、unescape、decodeURI、および decodeURIComponent 関数内の次のエンコードを正規化します。

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

プリプロセッサは連続するスペースを検出し、1 つのスペースに正規化します。このオプションが有効である場合、設定フィールドでは、難読化 Javascript データで許容する連続スペースの最大数を指定できます。入力できる値は、1 ～ 65535 です。値 0 を指定すると、このフィールドに関連付けられているプリプロセッサ ルール（120:10）が有効かどうかに関係なく、イベントの生成が無効になります。

プリプロセッサは、Javascript の正符号（+）演算子も正規化し、この演算子を使用して文字列を連結します。

`file_data` キーワードを使用して、侵入ルールに対し正規化された Javascript データを指し示すことができます。詳細については、特定のペイロード タイプを指し示す（27-102 ページ）を参照してください。

このオプションのイベントを生成するには、次に示すように、ルール 120:9、120:10、および 120:11 を有効にします。

表 *19-6*　*[Javascript* の正規化（*Normalize Javascript*）*]* オプションのルール

ルール	イベントがトリガーとして使用される条件
120:9	プリプロセッサ内の難読化レベルが 2 以上である。
120:10	Javascript 難読化データで連続するスペースの数が、許容される連続スペースの最大数として設定された値以上である。
120:11	エスケープされたデータまたはエンコードされたデータに、複数のエンコード タイプが含まれている。

詳細については、ルール状態の設定（24-21 ページ）を参照してください。

SWF ファイルの圧縮解除（**LZMA**）（**Decompress SWF File**（**LZMA**））および **SWF** ファイルの圧縮解除（**Deflate**）（**Decompress SWF File**（**Deflate**））

[HTTP Inspect の応答（HTTP Inspect Responses）] が有効な場合、これらのオプションは、HTTP 要求の HTTP 応答ボディ内にあるファイルの圧縮部分を圧縮解除します。

（注）　HTTP GET 応答で見つかったファイルの圧縮部分のみを圧縮解除できます。

- [SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））] は、Adobe ShockWave Flash（`.swf`）ファイルの LZMA 互換の圧縮部分を圧縮解除します。
- [SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））] は、Adobe ShockWave Flash（`.swf`）ファイルの deflate 互換の圧縮部分を圧縮解除します。

[圧縮データの最大深さ（Maximum Compressed Data Depth）]、[圧縮解除データの最大深さ（Maximum Decompressed Data Depth）]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバ フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、`file_data` ルール キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（27-102 ページ）を参照してください。

このオプションのイベントを生成するには、次に示すように、ルール 120:12 および 120:13 を有効にします。

表 *19-7*　*[SWF* ファイルの圧縮解除（*Decompress SWF File*）*]* オプションのルール

ルール	イベントがトリガーとして使用される条件
120:12	deflate ファイルの圧縮解除に失敗
120:13	LZMA ファイルの圧縮解除に失敗

PDF ファイルの圧縮解除（**Deflate**）（**Decompress PDF File**（**Deflate**））

[HTTP Inspect の応答（HTTP Inspect Responses）] が有効な場合、[PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate）] は、HTTP 要求の HTTP 応答ボディ内にある Portable Document Format（`.pdf`）ファイルの deflate 互換の圧縮部分を圧縮解除します。システムは、`/FlateDecode` ストリーム フィルタが付いた PDF ファイルだけを圧縮解除できます。他のフィルタ（`/FlateDecode /FlateDecode` など）はサポートしていません。

（注）　HTTP GET 応答で見つかったファイルの圧縮部分のみを圧縮解除できます。

[圧縮データの最大深さ（Maximum Compressed Data Depth）]、[圧縮解除データの最大深さ（Maximum Decompressed Data Depth）]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバ フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、`file_data` ルール キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（27-102 ページ）を参照してください。

このオプションのイベントを生成するには、次に示すように、ルール 120:14、120:15、120:16、および 120:17 を有効にします。

表 *19-8*　*[PDF* ファイルの圧縮解除（***Deflate***）（***Decompress PDF File***（***Deflate***））*]* オプションのルール

ルール	イベントがトリガーとして使用される条件
120:14	ファイルの圧縮解除に失敗
120:15	圧縮タイプがサポート対象外のタイプであるため、ファイルの圧縮解除に失敗
120:16	PDF ストリーム フィルタがサポート対象外のフィルタであるため、ファイルの圧縮解除に失敗
120:17	ファイルの解析に失敗

元のクライアント **IP** アドレスの抽出（**Extract Original Client IP Address**）

X-Forwarded-For（XFF）ヘッダー、True-Client-IP、またはカスタム定義の HTTP ヘッダーから、元のクライアント IP アドレスを抽出できるようにします。侵入イベント ビューで、抽出された元のクライアント IP アドレスを表示できます。詳細については、イベントの表示（34-1 ページ）を参照してください。

このオプションのイベントを生成するには、ルール 119:23、119:29、および 119:30 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

XFF ヘッダーの優先順位（**XFF Header Priority**）

[元のクライアント IP アドレスの抽出（Extract Original Client IP Address）] が有効な場合、システムが元のクライアント IP の HTTP ヘッダーを処理する順序を指定します。モニタ対象ネットワークで、X-Forwarded-For（XFF）または True-Client-IP 以外の元のクライアント IP ヘッダーが発生すると予測される場合は、[追加（Add）] をクリックしてプライオリティ リストに追加のヘッダー名を追加できます。追加したら、各ヘッダー タイプの横にある上下矢印アイコンを使用して、優先順位を調整します。HTTP 要求に複数の XFF ヘッダーがある場合は、優先順位が最も高いヘッダーだけが処理されます。

URI のログ（**Log URI**）

raw URI が存在する場合に、HTTP 要求パケットから raw URI を抽出できるようにし、このセッションで生成されるすべての侵入イベントにこの URI を関連付けます。

このオプションが有効である場合、侵入イベント テーブル ビューの [HTTP URI] 列に、抽出された URI の先頭 50 文字を表示できます。パケット ビューでは、URI 全体（最大 2048 バイト）を表示できます。詳細については、イベントの表示（34-1 ページ）を参照してください。

ホスト名のログ（**Log Hostname**）

ホスト名が存在する場合に、HTTP 要求の Host ヘッダーからホスト名を抽出できるようにし、このセッションで生成されるすべての侵入イベントにこのホスト名を関連付けます。複数の Host ヘッダーがある場合は、1 番目のヘッダーからホスト名を抽出します。

このオプションが有効である場合、侵入イベント テーブル ビューの [HTTP ホスト名（HTTP Hostname）] 列に、抽出されたホスト名の先頭 50 文字を表示できます。パケット ビューでは、ホスト名全体（最大 256 バイト）を表示できます。詳細については、イベントの表示（34-1 ページ）を参照してください。

このオプションのイベントを生成するには、ルール 119:25 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

プリプロセッサとルール 119:24 が有効である場合は、HTTP 要求で複数の Host ヘッダーが検出される場合でも、プリプロセッサはこのオプションの設定に関係なく、侵入イベントを生成することに注意してください。詳細については、追加の HTTP Inspect プリプロセッサ ルールの有効化（19-50 ページ）を参照してください。

プロファイル（**Profile**）

HTTP トラフィック向けに正規化されたエンコードのタイプを指定します。システムには、ほとんどのサーバに適用できるデフォルト プロファイル、Apache サーバと IIS サーバ用のデフォルト プロファイル、およびモニタ対象トラフィックのニーズに合わせて調整できるカスタムのデフォルト設定があります。詳細については、サーバレベル HTTP 正規化エンコード オプションの選択（19-45 ページ）を参照してください。

サーバレベル HTTP 正規化エンコード オプションの選択

ライセンス：Protection

サーバレベルの HTTP 正規化オプションを選択することで、HTTP トラフィック向けに正規化するエンコード タイプを指定し、このタイプのエンコードを含むトラフィックに対してイベントを生成させることができます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ASCII エンコーディング

エンコードされた ASCII 文字をデコードし、ルール エンジンが ASCII エンコード URI でイベントを生成するかどうかを指定します。

このオプションのイベントを生成するには、ルール 119:1 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

UTF-8 エンコーディング

URI の標準 UTF-8 Unicode シーケンスをデコードします。

このオプションのイベントを生成するには、ルール 119:6 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

Microsoft %U エンコーディング

%u とその後に続く 4 文字を使用する IIS %u エンコード スキームをデコードします。この 4 文字は、IIS Unicode コードポイントに関連する 16 進数のエンコード値です。

ヒント　正規のクライアントが %u エンコードを使用することはほとんどないため、シスコは、%u エンコードによってエンコードされている HTTP トラフィックをデコードすることを推奨します。

このオプションのイベントを生成するには、ルール 119:3 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

ベア バイト **UTF-8** エンコーディング

ベア バイト エンコードをデコードします。ベア バイト エンコードでは、UTF-8 値のデコード時に非 ASCII 文字が有効な値として使用されます。

ヒント　ベア バイト エンコードにより、ユーザは IIS サーバをエミュレートし、非標準エンコードを正しく解釈することができます。正規のクライアントはこの方法で UTF-8 をエンコードしないため、シスコでは、このオプションを有効にすることを推奨しています。

このオプションのイベントを生成するには、ルール 119:4 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

Microsoft IIS エンコーディング

Unicode コードポイント マッピングを使用してデコードします。

ヒント　これは主に攻撃と回避の試行で見られるため、シスコはこのオプションを有効にすることを推奨します。

このオプションのイベントを生成するには、ルール 119:7 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

二重エンコーディング

要求 URI を 2 回通過し、それぞれでデコードを実行するようにすることで、IIS 二重エンコード トラフィックをデコードします。これは通常は攻撃シナリオでのみ検出されるため、シスコはこのオプションを有効にすることを推奨します。

このオプションのイベントを生成するには、ルール 119:2 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

マルチスラッシュ難読化

1 つの行内の複数のスラッシュを 1 つのスラッシュに正規化します。

このオプションのイベントを生成するには、ルール 119:8 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

IIS バックスラッシュ難読化

バックスラッシュをスラッシュに正規化します。

このオプションのイベントを生成するには、ルール 119:9 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

ディレクトリ トラバーサル

ディレクトリ トラバーサルおよび自己参照用ディレクトリを正規化します。一部の Web サイトはディレクトリ トラバーサルを使用してファイルを参照するため、このタイプのトラフィックに対してイベントを生成するために、関連するプリプロセッサ ルールを有効にすると、誤検出が発生する可能性があります。

このオプションのイベントを生成するには、ルール 119:10 および 119:11 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

タブ難読化

スペース区切り記号としてタブを使用する非 RFC 標準を正規化します。Apache やその他の非 IIS Web サーバは、URL の区切り文字としてタブ文字（0x09）を使用します。

（注）　このオプションの設定に関係なく、空白文字（0x20）がタブの前にある場合、HTTP Inspect プリプロセッサはそのタブをスペースとして扱います。

このオプションのイベントを生成するには、ルール 119:12 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

無効な **RFC** デリミタ

URI データの改行（\ n）を正規化します。

このオプションのイベントを生成するには、ルール 119:13 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

webroot ディレクトリ トラバーサル

URL の初期ディレクトリを越えて横断するディレクトリ トラバーサルを検出します。

このオプションのイベントを生成するには、ルール 119:18 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

タブ **URI** デリミタ

URI の区切り文字としてタブ文字（0x09）を有効にします。Apache、新しいバージョンの IIS、およびその他の一部の Web サーバは、URL の区切り文字としてタブ文字を使用します。

（注）　このオプションの設定に関係なく、空白文字（0x20）がタブの前にある場合、HTTP Inspect プリプロセッサはそのタブをスペースとして扱います。

非 **RFC** 文字

対応するフィールドに追加された非 RFC 文字リストが、着信または発信 URI データ内に含まれている場合にそれを検出します。このフィールドを変更する場合は、バイト文字を表す 16 進表記を使用します。このオプションを設定する場合は、値を慎重に設定してください。非常に一般的な文字を使用すると、イベントが大量に発生する可能性があります。

このオプションのイベントを生成するには、ルール 119:14 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

最大チャンク エンコーディング サイズ

URI データで異常に大きなチャンク サイズを検出します。

このオプションのイベントを生成するには、ルール 119:16 および 119:22 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

パイプラインのデコードを無効にする

パイプライン処理された要求の HTTP デコードを無効にします。このオプションが無効である場合、パイプラインで待機する HTTP 要求には、デコードおよび分析は行われず、汎用パターン マッチングを使用した検査のみが行われるため、パフォーマンスが向上します。

Non-Strict URI 解析

Non-Strict URI 解析を有効にします。このオプションは、「GET /index.html abc xo qr \n」という形式の非標準 URI を受け入れるサーバでのみ使用します。このオプションを使用すると、デコーダは URI が 1 番目のスペースと 2 番目のスペースで囲まれているものと想定します。これは、2 番目のスペースの後に有効な HTTP 識別子がない場合でも同様です。

拡張 **ASCII** エンコーディング

HTTP 要求 URI の拡張 ASCII 文字の解析を有効にします。このオプションは、カスタム サーバ プロファイルでのみ使用可能であり、Apache、IIS、またはすべてのサーバ向けに提供されるデフォルト プロファイルでは使用できないことに注意してください。

HTTP サーバ オプションの設定

ライセンス：Protection

HTTP サーバ オプションを設定するには、次の手順に従います。HTTP サーバ オプションの詳細については、サーバレベル HTTP 正規化オプションの選択（19-37 ページ）および サーバレベル HTTP 正規化エンコード オプションの選択（19-45 ページ）を参照してください。

サーバレベルの **HTTP** 設定オプションの設定方法：

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **4**　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ **5**　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ **6**　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ 8　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [HTTP 設定（HTTP Configuration）] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[HTTP 設定（HTTP Configuration）] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 9　次の 2 つの対処法があります。

- 新しいサーバ プロファイルを追加します。ページの左側で [サーバ（Servers）] の横にある追加アイコン（  ）をクリックします。[ターゲットの追加（Add Target）] ポップアップ ウィンドウが表示されます。クライアントの 1 つ以上の IP アドレスを [サーバ アドレス（Server Address）] フィールドに指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。リストに入力できる文字数は最大 496 文字、すべてのサーバ プロファイルで指定できるアドレス項目の総数は 256、作成できるプロファイルの総数はデフォルト プロファイルを含めて 255 です。ASA FirePOWER モジュールでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-4 ページ）を参照してください。

  ターゲットベース ポリシーがトラフィックを処理するようにするには、識別するネットワークがターゲットベース ポリシーを設定するネットワーク分析ポリシーによって処理されるネットワーク、およびゾーンに一致するかまたはサブセットになっている必要があることに注意してください。詳細については、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（17-3 ページ）を参照してください。

  ページの左側のサーバ リストに新しい項目が表示され、選択されていることを示すために強調表示されます。[設定（Configuration）] セクションが更新され、追加したプロフィールの現行設定が反映されます。

- 既存のプロファイルの設定を変更します。ページ左側の [サーバ（Servers）] の下で追加したプロファイルの設定済みアドレスをクリックするか、または [デフォルト（default）] をクリックします。

  選択した項目が強調表示され、[設定（Configuration）] セクションが更新され、選択したプロファイルの現行設定が表示されます。既存のプロファイルを削除するには、削除するプロファイルの横にある削除アイコン（  ）をクリックします。

ステップ 10　オプションで、[ネットワーク（Networks）] フィールドにリストされているアドレスを変更し、ページの他の領域をクリックします。

ページの左側で、強調表示されているアドレスが更新されます。

デフォルト プロファイルでは [ネットワーク（Network）] の設定を変更できないことに注意してください。デフォルト プロファイルは、別のプロファイルで指定されていないネットワーク上のすべてのサーバに適用されます。

ステップ 11　[ポート（Ports）] フィールドに、HTTP Inspect でトラフィックを検査するポートを指定します。複数のポートを指定する場合は、カンマで区切ります。

ステップ 12　サーバレベル HTTP 正規化オプションの選択（19-37 ページ）で説明するその他のオプションを変更できます。

ステップ 13　次の手順に従ってサーバ プロファイルを選択します。

- 独自のサーバ プロファイルを作成するには、[カスタム（Custom）] を選択します（詳細については、サーバレベル HTTP 正規化エンコード オプションの選択（19-45 ページ）を参照）。
- すべてのサーバに対して適切な標準のデフォルト プロファイルを使用するには、[すべて（All）] を選択します。
- デフォルトの IIS プロファイルを使用するには、[IIS] を選択します。
- デフォルトの Apache プロファイルを使用するには、[Apache] を選択します。

ステップ 14　[カスタム（Custom）] を選択すると、カスタム オプションが表示されます。

ステップ 15　プロファイルで、使用する HTTP デコード オプションを設定します。

使用可能な正規化オプションの詳細についてはサーバレベル HTTP 正規化オプションの選択（19-37 ページ）、参照してください。

ステップ 16　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

追加の HTTP Inspect プリプロセッサ ルールの有効化

ライセンス：Protection

特定の設定オプションに関連付けられていない HTTP Inspect プリプロセッサ ルールのイベントを生成するには、次の表の「プリプロセッサ ルール GID：SID」列のルールを有効にできます。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

表 19-9　追加の *HTTP Inspect* プリプロセッサ ルール

プリプロセッサ ルール **GID:SID**	説明
120:5	HTTP 応答トラフィックで UTF-7 エンコードが検出された場合にイベントが生成されます。UTF-7 は、SMTP トラフィックなどで 7 ビット パリティが必要な場合にのみ使用してください。
119:21	HTTP 要求ヘッダーに複数の `content-length` フィールドがある場合にイベントが生成されます。
119:24	HTTP 要求に複数の Host ヘッダーがある場合に、イベントが生成されます。
119:28 120:8	これらのルールを有効にする場合、イベントは生成されません。
119:32	トラフィックで HTTP バージョン 0.9 が検出されると、イベントが生成されます。TCP ストリームの設定も有効にする必要があることに注意してください。TCP ストリームの前処理の使用（21-21 ページ）を参照してください。
119:33	エスケープされていないスペースが HTTP URI に含まれている場合に、イベントが生成されます。
119:34	TCP 接続に 24 以上のパイプライン処理された HTTP 要求が含まれている場合に、イベントが生成されます。

Sun RPC プリプロセッサの使用

ライセンス：Protection

RPC（Remote Procedure Call）正規化では、フラグメント化された RPC レコードが 1 つのレコードに正規化されるので、ルール エンジンがそのレコード全体を検査できます。たとえば、攻撃者が RPC `admind` が実行されているポートの検出を試行するとします。一部の UNIX ホストは、RPC `admind` を使用してリモート分散システム タスクを実行します。ホストが弱い認証を実行する場合、悪意のあるユーザがリモート管理のコントロールを獲得できることがあります。Snort ID（SID）が 575 の標準テキスト ルール（ジェネレータ ID：1）は、この攻撃を検出するために、特定のロケーションでコンテンツを検索し、不適切な `portmap GETPORT` 要求を特定します。

ポート
: トラフィックを正規化するポートを示します。インターフェイスで、複数のポートをカンマで区切って指定します。一般的な RPC ポートは 111 および 32771 です。ネットワークが他のポートに RPC トラフィックを送信する場合は、それらのポートの追加を検討してください。

RPC フラグメント化レコードの検出（**Detect fragmented RPC records**）
: RPC フラグメント化レコードを検出します。

  このオプションのイベントを生成するには、ルール 106:1 および 106:5 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

1 パケットの複数レコードの検出（**Detect multiple records in one packet**）
: パケット（または再構成されたパケット）ごとに、複数の RPC 要求を検出します。

  このオプションのイベントを生成するには、ルール 106:2 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

1 フラグメントを超えるフラグメント化レコード合計の検出（**Detect fragmented record sums which exceed one fragment**）
: 現在のパケット長を超える再構成されたフラグメント化レコード長を検出します。

  このオプションのイベントを生成するには、ルール 106:3 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

1 パケットのサイズを超える単一フラグメント レコードの検出（**Detect single fragment records which exceed the size of one packet**）
: 部分的なレコードを検出します。

  このオプションのイベントを生成するには、ルール 106:4 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

Sun RPC プリプロセッサの設定

ライセンス：Protection

Sun RPC プリプロセッサを設定するには、次の手順を使用できます。Sun RPC プリプロセッサ設定オプションの詳細については、Sun RPC プリプロセッサの使用（19-51 ページ）を参照してください。

Sun RPC プリプロセッサを設定するには、次の手順を実行します。

ステップ 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ 8　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [Sun RPC 設定（Sun RPC Configuration）] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[Sun RPC 設定（Sun RPC Configuration）] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 9　[ポート（Ports）] フィールドに、RPC トラフィックをデコードするポートの番号を入力します。複数のポートを指定する場合は、カンマで区切ります。

ステップ 10　[Sun RPC 設定（Sun RPC Configuration）] ページの次の検出オプションを選択またはクリアできます。

- **RPC** フラグメント化レコードの検出（**Detect fragmented RPC records**）
- **1** パケットの複数レコードの検出（**Detect multiple records in one packet**）
- **1** パケットを超えるフラグメント化レコード合計の検出（**Detect fragmented record sums which exceed one packet**）
- **1** パケットのサイズを超える単一フラグメント レコードの検出（**Detect single fragment records which exceed the size of one packet**）

ステップ 11　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

Session Initiation Protocol のデコード

ライセンス：Protection

Session Initiation Protocol（SIP）は、インターネット テレフォニー、マルチメディア会議、インスタント メッセージング、オンライン ゲーム、ファイル転送などのクライアント アプリケーションの 1 人以上のユーザに対し、1 つ以上のセッションのコール設定、変更、およびティアダウンを提供します。各 SIP 要求の *method* フィールドは要求の目的を示し、要求 URI により要求の送信先が指定されます。各 SIP 応答のステータス コードは、要求されたアクションの結果を示します。

SIP を使用してコールがセットアップされた後、後続の音声およびビデオによる通信は Real-time Transport Protocol（RTP）により処理されます。セッションのこの部分は、コール チャネル、データ チャネル、または音声/ビデオ データ チャネルと呼ばれることがあります。RTP は、データチャネル パラメータ ネゴシエーション、セッション通知、およびセッションへの招待のために、SIP メッセージ ボディ内で Session Description Protocol（SDP）を使用します。

SIP プリプロセッサは次の処理を実行します。

- SIP 2.0 トラフィックのデコードおよび分析
- SDP データが存在する場合はこのデータを含む SIP ヘッダーとメッセージ ボディを抽出し、抽出したデータを今後のインスペクションのためにルール エンジンに受け渡す
- 条件（SIP パケットにおける異常または既知の脆弱性、順序が正しくないコール シーケンス、または無効なコール シーケンス）が検出され、対応するプリプロセッサ ルールが有効である場合にイベントを生成する
- コール チャネルを無視する（オプション）

プリプロセッサは、SIP メッセージ ボディに組み込まれている SDP メッセージに示されているポートに基づいて RTP チャネルを識別しますが、RTP プロトコル インスペクションを実行しません。

SIP プリプロセッサを使用するときは、次の点に注意してください。

- UDP は通常、SIP でサポートされるメディア セッションを伝送します。UDP ストリームの前処理により、SIP プリプロセッサに対し SIP セッション トラッキングが提供されます。
- SIP ルール キーワードにより、SIP パケット ヘッダーまたはメッセージ ボディを指し示し、検出対象を特定の SIP メソッドまたはステータス コードのパケットに限定できます。詳細については、SIP キーワード（27-65 ページ）を参照してください。
- 有効である場合、関連するルール（ジェネレータ ID（GID）140）も有効にしていないと、抽出したデータをルール エンジンに送信するまで、プリプロセッサはイベントを生成しません。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

詳細については、次の各項を参照してください。

- SIP プリプロセッサ オプションの選択（19-54 ページ）
- SIP プリプロセッサの設定（19-56 ページ）
- 追加の SIP プリプロセッサ ルールの有効化（19-57 ページ）

SIP プリプロセッサ オプションの選択

ライセンス：Protection

変更できる SIP プリプロセッサ オプションについて以下で説明します。

[要求 URI の最大長（Maximum Request URI Length）]、[コール ID の最大長（Maximum Call ID Length）]、[要求名の最大長（Maximum Request Name Length）]、[送信元の最大長（Maximum From Length）]、[送信先の最大長（Maximum To Length）]、[経由の最大長（Maximum Via Length）]、[連絡先の最大長（Maximum Contact Length）]、および [コンテンツの最大長（Maximum Content Length）] オプションでは、1 ～ 65535 バイト、または 0 バイトを指定できます。0 を指定すると、関連するルールが有効であるかかどうかに関係なく、このオプションのイベント生成が無効になります。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

SIP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。ポート番号が複数ある場合は、カンマで区切ります。

検査するメソッド（**Methods to Check**）

検出する SIP メソッドを指定します。次に示す現在定義されている SIP メソッドを指定できます。

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

メソッドでは大文字と小文字が区別されません。メソッド名には英字、数字、下線文字を使用できます。その他の特殊文字は使用できません。複数のメソッドはカンマで区切ります。

新しい SIP メソッドが今後定義される可能性があるため、設定には、現在定義されていない英字文字列を含めることができます。システムでは最大 32 個のメソッド（現在定義されている 21 個のメソッドと追加の 11 個のメソッド）がサポートされます。システムは、設定される未定義のメソッドをすべて無視します。

合計 32 個のメソッドには、このオプションに指定するメソッドの他に、侵入ルールで `sip_method` キーワードを使用して指定するメソッドも含まれます。詳細については、sip_method（27-66 ページ）を参照してください。

セッション内のダイアログ最大数（**Maximum Dialogs within a Session**）

ストリーム セッション内で許容されるダイアログの最大数を指定します。この数より多くのダイアログが作成されると、ダイアログの数が、指定されている最大数以下になるまで、最も古いダイアログから順に削除されます。また、ルール 140:27 が有効である場合にもイベントがトリガーとして使用されます。

1 ～ 4194303 の整数を指定できます。

要求 **URI** の最大長（**Maximum Request URI Length**）

[要求 URI（Request-URI）] ヘッダー フィールドの最大許容バイト数を指定します。ルール 140:3 が有効である場合、URI がこれよりも長いとイベントがトリガーとして使用されます。[要求 URI（Request-URI）] フィールドは、要求の宛先のパスまたはページを示します。

コール ID の最大長（**Maximum Call ID Length**）

要求または応答の [コール ID（Call-ID）] ヘッダー フィールドの最大許容バイト数を指定します。ルール 140:5 が有効である場合、コール ID がこれよりも長いとイベントがトリガーとして使用されます。[コール ID（Call-ID）] フィールドによって、要求や応答内の SIP セッションが一意に識別されます。

要求名の最大長（**Maximum Request Name Length**）

要求名で許容される最大バイト数を指定します。要求名は、CSeq トランザクション ID に指定されるメソッドの名前です。ルール 140:7 が有効である場合、要求名がこれよりも長いとイベントがトリガーとして使用されます。

送信元の最大長（**Maximum From Length**）

要求または応答の [送信元（From）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:9 が有効である場合、[送信元（From）] がこれよりも長いとイベントがトリガーとして使用されます。[送信元（From）] フィールドは、メッセージの発信側を識別します。

送信先の最大長（**Maximum To Length**）

要求または応答の [送信先（To）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:11 が有効である場合、[送信先（To）] がこれよりも長いとイベントがトリガーとして使用されます。[送信先（To）] フィールドは、メッセージの受信側を識別します。

経由の最大長（**Maximum Via Length**）

要求または応答の [経由（Via）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:13 が有効である場合、[経由（Via）] がこれよりも長いとイベントがトリガーとして使用されます。[経由（Via）] フィールドには要求がたどるパスが示され、応答の場合は受信者情報が示されます。

連絡先の最大長（**Maximum Contact Length**）

要求または応答の [連絡先（Contact）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:15 が有効である場合、[連絡先（Contact）] がこれよりも長いとイベントがトリガーとして使用されます。[連絡先（Contact）] フィールドには、後続のメッセージについての連絡先を指定する URI が示されます。

コンテンツの最大長（**Maximum Content Length**）

要求または応答のメッセージ ボディのコンテンツで許容される最大バイト数を指定します。ルール 140:16 が有効である場合、コンテンツがこれよりも長いとイベントがトリガーとして使用されます。

音声/ビデオ データ チャネルを無視（**Ignore Audio/Video Data Channel**）

データ チャネル トラフィックのインスペクションを有効または無効にします。このオプションを有効にすると、プリプロセッサはその他の非データ チャネル SIP トラフィックのインスペクションを続行するので注意してください。

SIP プリプロセッサの設定

ライセンス：Protection

SIP プリプロセッサを設定するには、次の手順に従います。

SIP プリプロセッサを設定するには、次の手順を実行します。

ステップ **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。

ステップ **2** 編集するアクセス 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。

ステップ **3** [詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **4** [ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ **5** [ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ **6** 編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ **7** 左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ **8** [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SIP 設定（SIP Configuration）] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[SIP 設定（SIP Configuration）] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ **9** SIP プリプロセッサ オプションの選択（19-54 ページ）で説明するオプションを変更できます。

ステップ **10** ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

追加の SIP プリプロセッサ ルールの有効化

ライセンス：Protection

次の表に示す SIP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。その他の SIP プリプロセッサ ルールと同様に、これらのルールによってイベントを生成する場合は、これらのルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（24-21 ページ）を参照してください。

表 *19-10*　追加の *SIP* プリプロセッサ ルール

プリプロセッサ ルール **GID:SID**	説明
140:1	プリプロセッサがモニタしている SIP セッションの数が、システムで許容される最大数である場合に、イベントが生成されます。
140:2	SIP 要求で [要求 URI（Request URI）] 必須フィールドが空である場合に、イベントが生成されます。
140:4	SIP 要求または応答の [コール ID（Call ID）] ヘッダー フィールドが空である場合に、イベントが生成されます。
140:6	SIP 要求または応答の CSeq フィールドのシーケンス番号値が、231 未満の 32 ビット符号なし整数ではない場合に、イベントが生成されます。
140:8	SIP 要求または応答で [送信元（From）] ヘッダー フィールドが空である場合に、イベントが生成されます。
140:10	SIP 要求または応答で [送信先（To）] ヘッダー フィールドが空である場合に、イベントが生成されます。
140:12	SIP 要求または応答で [経由（Via）] ヘッダー フィールドが空である場合に、イベントが生成されます。
140:14	SIP 要求または応答で [連絡先（Contact）] 必須ヘッダー フィールドが空である場合に、イベントが生成されます。
140:17	UDP トラフィック内の 1 つの SIP 要求または応答パケットに複数のメッセージが含まれている場合に、イベントが生成されます。SIP の旧バージョンでは複数メッセージがサポートされていますが、SIP 2.0 ではパケットあたり 1 メッセージだけがサポートされていることに注意してください。
140:18	UDP トラフィック内の SIP 要求または応答のメッセージ ボディの実際の長さが、SIP 要求または応答の [コンテンツ長（Content-Length）] ヘッダー フィールドの指定値と一致しない場合に、イベントが生成されます。
140:19	プリプロセッサが SIP 応答の [CSeq] フィールドのメソッド名を認識しない場合に、イベントが生成されます。
140:20	SIP サーバが、認証済み招待メッセージに対してチャレンジを送信しない場合に、イベントが生成されます。これは InviteReplay 請求攻撃の場合に発生することに注意してください。
140:21	コール セットアップの前にセッション情報が変更されると、イベントが生成されます。これは FakeBusy 請求攻撃の場合に発生することに注意してください。
140:22	応答ステータス コードが 3 桁の数値ではない場合に、イベントが生成されます。
140:23	[コンテンツ タイプ（Content-Type）] ヘッダー フィールドにコンテンツ タイプが指定されておらず、メッセージ ボディにデータが含まれている場合に、イベントが生成されます。
140:24	SIP バージョンが 1、1.1、または 2.0 のいずれでもない場合に、イベントが生成されます。

表 19-10　追加の SIP プリプロセッサ ルール（続き）

プリプロセッサ ルール GID:SID	説明
140:25	SIP 要求で、[CSeq] ヘッダーで指定されたメソッドとメソッド フィールドが一致しない場合に、イベントが生成されます。
140:26	プリプロセッサが SIP 要求のメソッド フィールドに指定されたメソッドを認識しない場合に、イベントが生成されます。

GTP コマンド チャネルの設定

ライセンス：Protection

General Packet Radio Service（GPRS）Tunneling Protocol（GTP）により、GTP コア ネットワークを介した通信が実現します。GTP プリプロセッサは、GTP トラフィックの異常を検出し、コマンド チャネル シグナリング メッセージをインスペクションのためにルール エンジンに転送します。GTP コマンド チャネル トラフィックでエクスプロイトがあるかどうかを検査するには、`gtp_version`、`gtp_type`、および `gtp_info` ルール キーワードを使用します。

1 つの構成オプションで、プリプロセッサが GTP コマンド チャネル メッセージを検査するポートのデフォルト設定を変更できます。

イベントを生成するには、次の表に示す GTP プリプロセッサ ルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（24-21 ページ）を参照してください。

表 19-11　GTP プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
143:1	プリプロセッサが無効なメッセージの長さを検出すると、イベントが生成されます。
143:2	プリプロセッサが無効な情報要素の長さを検出すると、イベントが生成されます。
143:3	プリプロセッサが誤った順序の情報要素を検出すると、イベントが生成されます。

GTP プリプロセッサが GTP コマンド メッセージをモニタするポートを変更するには、次の手順を使用します。

GTP コマンド チャネルを設定するには、次の手順を実行します。

ステップ 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] をクリックします。

[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定(Settings)] をクリックします。

[設定(Settings)] ページが表示されます。

ステップ 8　[アプリケーション層プリプロセッサ(Application Layer Preprocessors)] の下の [GTP コマンド チャネル設定(GTP Command Channel Configuration)] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[GTP コマンド チャネル設定(GTP Command Channel Configuration)] ページが表示されます。

ステップ 9　オプションで、プリプロセッサが GTP コマンド メッセージを検査するポートを変更します。0 ～ 65535 の整数を指定できます。複数のポートを指定する場合はカンマで区切ります。

ステップ 10　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

IMAP トラフィックのデコード

ライセンス:Protection

Internet Message Application Protocol(IMAP)は、リモート IMAP サーバから電子メールを取得するときに使用されます。IMAP プリプロセッサはサーバ/クライアント IMAP4 トラフィックを検査し、関連するプリプロセッサ ルールが有効な場合は、異常なトラフィックがあるとイベントを生成します。プリプロセッサは、クライアント/サーバ IMAP4 トラフィックの電子メール添付ファイルを抽出してデコードし、添付ファイル データをルール エンジンに送信することもできます。添付ファイル データを指し示すには、侵入ルールで `file_data` キーワードを使用します。詳細については、特定のペイロード タイプを指し示す(27-102 ページ)を参照してください。

抽出とデコードでは、複数の添付ファイル(存在する場合)や、複数パケットにまたがる大きな添付ファイルなども処理されます。

IMAP プリプロセッサ ルールによりイベントを生成するには、それらのルールを有効にする必要があります。IMAP プリプロセッサ ルールのジェネレータ ID(GID)は 141 です。詳細については、ルール状態の設定(24-21 ページ)を参照してください。

詳細については、次の各項を参照してください。

- IMAP プリプロセッサ オプションの選択(19-60 ページ)
- IMAP プリプロセッサの設定(19-61 ページ)
- 追加の IMAP プリプロセッサ ルールの有効化(19-62 ページ)

IMAP プリプロセッサ オプションの選択

ライセンス：Protection

変更できる IMAP プリプロセッサ オプションを以下で説明します。

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 デコーディングの深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）] オプションの値が以下のポリシーで異なる場合は、最も大きい値が使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

詳細については、「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（17-4 ページ）」と「ネットワーク分析ルールを使用して前処理するトラフィックの指定（17-4 ページ）」を参照してください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

IMAP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。ポート番号が複数ある場合は、カンマで区切ります。

Base64 デコーディングの深さ（**Base64 Decoding Depth**）

各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、すべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

Base64 デコードが有効である場合、ルール 141:4 を有効にして、デコードの失敗時にイベントを生成することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

7 ビット**/8** ビット**/**バイナリのデコーディングの深さ（**7-Bit/8-Bit/Binary Decoding Depth**）

デコードを必要としない各 MIME 電子メール添付ファイルから抽出するデータの最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出する場合は 0 を指定します。非デコード データを無視するには、-1 を指定します。

Quoted-Printable（**QP**）のデコーディングの深さ（**Quoted-Printable Decoding Depth**）

各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての QP エンコード データをデコードする場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。

quoted-printable デコードが有効な場合は、ルール 141:6 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。

Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）

各 Unix-to-Unix エンコード（UU エンコード）電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての UU エンコード データをデコードする場合は 0 を指定します。UU エンコード データを無視するには、-1 を指定します。

Unix-to-Unix デコードが有効な場合は、ルール 141:7 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。

IMAP プリプロセッサの設定

ライセンス：Protection

IMAP プリプロセッサを設定するには、次の手順に従います。IMAP プリプロセッサ設定オプションの詳細については、IMAP プリプロセッサ オプションの選択（19-60 ページ）を参照してください。

IMAP プリプロセッサを設定するには、次の手順を実行します。

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **4**　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ **5**　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ **6**　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ **7**　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ 8　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [IMAP 設定（IMAP Configuration）] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[IMAP 設定（IMAP Configuration）] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 9　IMAP トラフィックをデコードする必要があるポートを指定します。ポート番号が複数ある場合は、カンマで区切ります。

ステップ 10　次に示す電子メール添付ファイル タイプの任意の組み合わせから抽出してデコードするデータの最大バイト数を指定します。

- **Base64** デコーディングの深さ（**Base64 Decoding Depth**）
- **7** ビット**/8** ビット**/**バイナリのデコーディングの深さ（**7-Bit/8-Bit/Binary Decoding Depth**）（プレーン テキスト、jpeg イメージ、mp3 ファイルなどの各種マルチパート コンテンツ タイプを含む）
- **Quoted-Printable**（**QP**）のデコーディングの深さ（**Quoted-Printable Decoding Depth**）
- **Unix-to-Unix**（**UU**）のデコーディングの深さ（**Unix-to-Unix Decoding Depth**）

タイプごとに 1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出し、必要に応じてデコードする場合は 0 を指定します。添付ファイル タイプのデータを無視するには、-1 を指定します。

添付ファイル データを検査するには、侵入ルールで `file_data` キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（27-102 ページ）を参照してください。

ステップ 11　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

追加の IMAP プリプロセッサ ルールの有効化

ライセンス：Protection

次の表に示す IMAP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。その他の IMAP プリプロセッサ ルールと同様に、これらのルールによってイベントを生成する場合は、これらのルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（24-21 ページ）を参照してください。

表 *19-12*　追加の *IMAP* プリプロセッサ ルール

プリプロセッサ ルール **GID:SID**	説明
141:1	プリプロセッサが RFC 3501 に定義されていないクライアント コマンドを検出すると、イベントが生成されます。
141:2	プリプロセッサが RFC 3501 に定義されていないサーバ応答を検出すると、イベントが生成されます。
141:3	プリプロセッサが使用しているメモリの量が、システムでの最大許容量に達している場合に、イベントが生成されます。この時点で、プリプロセッサはメモリが使用可能になるまでデコードを停止します。

POP トラフィックのデコード

ライセンス：Protection

Post Office Protocol（POP）は、リモート POP メール サーバから電子メールを取得するときに使用されます。POP プリプロセッサはサーバ/クライアント POP3 トラフィックを検査し、関連するプリプロセッサ ルールが有効である場合は、異常なトラフィックがあるとイベントを生成します。プリプロセッサは、クライアント/サーバ POP3 トラフィックで電子メール添付ファイルを抽出してデコードし、添付ファイル データをルール エンジンに送信することもできます。添付ファイル データを指し示すには、侵入ルールで `file_data` キーワードを使用します。詳細については、特定のペイロード タイプを指し示す（27-102 ページ）を参照してください。

抽出とデコードでは、複数の添付ファイル（存在する場合）や、複数パケットにまたがる大きな添付ファイルなども処理されます。

POP プリプロセッサ ルールによりイベントを生成するには、それらのルールを有効にする必要があります。POP プリプロセッサ ルールのジェネレータ ID（GID）は 142 です。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

詳細については、次の各項を参照してください。

- POP プリプロセッサ オプションの選択（19-63 ページ）
- POP プリプロセッサの設定（19-64 ページ）
- 追加の POP プリプロセッサ ルールの有効化（19-66 ページ）

POP プリプロセッサ オプションの選択

ライセンス：Protection

変更できる POP プリプロセッサ オプションを以下で説明します。

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 デコーディングの深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）] の各オプションの値が、アクセス コントロール ポリシーに関連付けられている侵入ポリシーと、アクセス コントロール ルールに関連付けられている侵入ポリシーの間で異なる場合は、最も大きな値が使用されることに注意してください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

POP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。ポート番号が複数ある場合は、カンマで区切ります。

Base64 デコーディングの深さ（**Base64 Decoding Depth**）

各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、すべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

Base64 デコードが有効である場合、ルール 142:4 を有効にして、デコードの失敗時にイベントを生成することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

7 ビット**/8** ビット**/**バイナリのデコーディングの深さ（**7-Bit/8-Bit/Binary Decoding Depth**）

デコードを必要としない各 MIME 電子メール添付ファイルから抽出するデータの最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出する場合は 0 を指定します。非デコード データを無視するには、-1 を指定します。

Quoted-Printable（**QP**）のデコーディングの深さ（**Quoted-Printable Decoding Depth**）

各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての QP エンコード データをデコードする場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。

quoted-printable デコードが有効な場合は、ルール 142:6 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

Unix-to-Unix（**UU**）のデコーディングの深さ（**Unix-to-Unix Decoding Depth**）

各 Unix-to-Unix エンコード（UU エンコード）電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての UU エンコード データをデコードする場合は 0 を指定します。UU エンコード データを無視するには、-1 を指定します。

Unix-to-Unix デコードが有効な場合は、ルール 142:7 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

POP プリプロセッサの設定

ライセンス：Protection

POP プリプロセッサを設定するには、次の手順に従います。POP プリプロセッサ設定オプションの詳細については、POP プリプロセッサ オプションの選択（19-63 ページ）を参照してください。

POP プリプロセッサを設定するには、次の手順を実行します。

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（  ）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ 8　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [POP 設定（POP Configuration）] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[POP 設定（POP Configuration）] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 9　IMAP トラフィックをデコードする必要があるポートを指定します。ポート番号が複数ある場合は、カンマで区切ります。

ステップ 10　次に示す電子メール添付ファイル タイプの任意の組み合わせから抽出してデコードするデータの最大バイト数を指定します。

- **Base64** デコーディングの深さ（**Base64 Decoding Depth**）
- **7** ビット**/8** ビット**/**バイナリのデコーディングの深さ（**7-Bit/8-Bit/Binary Decoding Depth**）（プレーン テキスト、jpeg イメージ、mp3 ファイルなどの各種マルチパート コンテンツ タイプを含む）
- **Quoted-Printable**（**QP**）のデコーディングの深さ（**Quoted-Printable Decoding Depth**）
- **Unix-to-Unix**（**UU**）のデコーディングの深さ（**Unix-to-Unix Decoding Depth**）

タイプごとに 1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出し、必要に応じてデコードする場合は 0 を指定します。添付ファイル タイプのデータを無視するには、-1 を指定します。

添付ファイル データを検査するには、侵入ルールで `file_data` キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（27-102 ページ）を参照してください。

ステップ 11　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

追加の POP プリプロセッサ ルールの有効化

ライセンス：Protection

次の表に示す POP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。その他の POP プリプロセッサ ルールと同様に、これらのルールによってイベントを生成する場合は、これらのルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（24-21 ページ）を参照してください。

表 *19-13*　追加の *POP* プリプロセッサ ルール

プリプロセッサ ルール **GID:SID**	説明
142:1	プリプロセッサが RFC 1939 に定義されていないクライアント コマンドを検出すると、イベントが生成されます。
142:2	プリプロセッサが RFC 1939 に定義されていないサーバ応答を検出すると、イベントが生成されます。
142:3	プリプロセッサが使用しているメモリの量が、システムでの最大許容量に達している場合に、イベントが生成されます。この時点で、プリプロセッサはメモリが使用可能になるまでデコードを停止します。

SMTP トラフィックのデコード

ライセンス：Protection

SMTP プリプロセッサはルール エンジンに対し、SMTP コマンドを正規化するように指示します。このプリプロセッサは、クライアント/サーバ トラフィックで電子メール添付ファイルを抽出してデコードします。またソフトウェアのバージョンによっては、SMTP トラフィックによりトリガーされた侵入イベントの表示時にコンテキストを提供するため、電子メール ファイル名、アドレス、およびヘッダー データを抽出します。

SMTP プリプロセッサを使用するときは、次の点に注意してください。

- ジェネレータ ID（GID）124 の SMTP プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があります。詳細については、ルール状態の設定（24-21 ページ）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。

- SMTP デコードについて（19-66 ページ）
- SMTP デコードの設定（19-71 ページ）
- SMTP 最大デコード メモリ アラートの有効化（19-74 ページ）

SMTP デコードについて

ライセンス：Protection

正規化を有効または無効にし、SMTP デコーダが検出する異常トラフィックのタイプを制御するオプションを設定できます。

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 デコーディングの深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）] の各オプションの値が、アクセス コントロール ポリシーに関連付けられている侵入ポリシーと、アクセス コントロール ルールに関連付けられている侵入ポリシーの間で異なる場合は、最も大きな値が使用されることに注意してください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

SMTP トラフィックを正規化するポートを指定します。0 ～ 65535 の整数を指定できます。複数のポートを指定する場合は、カンマで区切ります。

ステートフル インスペクション（**Stateful Inspection**）

選択されている場合、SMTP デコーダは状態を保存し、各パケットのセッション コンテキストを提供し、再構成されたセッションだけを検査します。選択されていない場合、セッション コンテキストなしで個々のパケットを分析します。

正規化（**Normalize**）

[すべて（All）] に設定すると、すべてのコマンドが正規化されます。コマンドの後に複数のスペース文字があるかどうかを確認します。

[なし（None）] に設定すると、コマンドは正規化されません。

[Cmds] に設定すると、[カスタム コマンド（Custom Commands）] にリストされているコマンドが正規化されます。

カスタム コマンド（**Custom Commands**）

[正規化（Normalize）] が [Cmds] に設定されている場合に、リストされているコマンドが正規化されます。

正規化する必要があるコマンドをテキスト ボックスに指定します。コマンドの後に複数のスペース文字があるかどうかを確認します。

スペース文字（ASCII 0x20）とタブ文字（ASCII 0x09）は、正規化のためにスペース文字としてカウントされます。

データを無視（**Ignore Data**）

メール データを処理せず、MIME メール ヘッダー データだけを処理します。

TLS データを無視（**Ignore TLS Data**）

Transport Layer Security プロトコルで暗号化されたデータを処理しません。

アラートなし（**No Alerts**）

関連するプリプロセッサ ルールが有効である場合に、侵入イベントを無効にします。

不明なコマンドの検出（**Detect Unknown Commands**）

SMTP トラフィックで不明なコマンドを検出します。

このオプションのイベントを生成するには、ルール 124:5 および 124:6 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

コマンドラインの最大長（**Max Command Line Len**）

SMTP コマンドラインがこの値より長い場合にそのことを検出します。コマンドラインの長さを検出しない場合は、0 を指定します。

RFC 2821（Network Working Group による Simple Mail Transfer Protocol 仕様）では、コマンドラインの最大長として 512 が推奨されています。

このオプションのイベントを生成するには、ルール 124:1 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

ヘッダー行の最大長（**Max Header Line Len**）

SMTP データ ヘッダー行がこの値より長い場合にそのことを検出します。データ ヘッダー行の長さを検出しない場合は、0 を指定します。

このオプションのイベントを生成するには、ルール 124:2 および 124:7 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

応答行の最大長（**Max Response Line Len**）

SMTP 応答行がこの値より長い場合にそのことを検出します。応答行の長さを検出しない場合は、0 を指定します。

RFC 2821 では、応答行の最大長として 512 が推奨されています。

このオプションのイベントを生成するには、ルール 124:3 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

代替のコマンドラインの最大長（**Alt Max Command Line Len**）

指定のコマンドの SMTP コマンドラインがこの値より長い場合にそのことを検出します。指定したコマンドのコマンドライン長を検出しない場合は、0 を指定します。多数のコマンドに対して、さまざまなデフォルト ライン長が設定されています。

この設定は、指定されたコマンドの [コマンドラインの最大長（Max Command Line Len）] の設定をオーバーライドします。

このオプションのイベントを生成するには、ルール 124:3 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

無効なコマンド（**Invalid Commands**）

これらのコマンドがクライアント側から送信された場合にそのことを検出します。

このオプションのイベントを生成するには、ルール 124:5 および 124:6 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

有効なコマンド（**Valid Commands**）

このリストのコマンドを許可します。

このリストが空の場合でも、プリプロセッサにより許可される有効なコマンドは、ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR です。

（注）　RCPT TO および MAIL FROM は SMTP コマンドです。プリプロセッサ設定では、コマンド名 RCPT と MAIL がそれぞれ使用されます。プリプロセッサはコード内で RCPT および MAIL を正しいコマンド名にマッピングします。

このオプションのイベントを生成するには、ルール 124:4 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

データ コマンド（**Data Commands**）

RFC 5321 に基づく SMTP DATA コマンドによるデータの送信と同じ方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

バイナリ データ コマンド（**Binary Data Commands**）

RFC 3030 に基づく BDAT コマンドによるデータの送信と類似の方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

認証コマンド（**Authentication Commands**）

クライアントおよびサーバ間で認証交換を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

xlink2state の検出（**Detect xlink2state**）

X-Link2State Microsoft Exchange バッファ データ オーバーフロー攻撃の一部であるパケットを検出します。インライン展開では、システムはこれらのパケットをドロップすることもできます。

このオプションのイベントを生成するには、ルール 124:8 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

Base64 デコーディングの深さ（**Base64 Decoding Depth**）

[データを無視（Ignore Data）] が無効である場合、各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、すべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータをデコードしません。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

Base64 デコードが有効である場合、ルール 124:10 を有効にして、デコードの失敗時にイベントを生成することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

このオプションは、廃止されたオプション [MIME デコーディングの有効化（Enable MIME Decoding）] および [MIME デコーディングの最大の深さ（Maximum MIME Decoding Depth）] の代わりに使用されます。廃止されたこれらのオプションは、既存の侵入ポリシーでは後方互換性を維持する目的で引き続きサポートされています。

7 ビット**/8** ビット**/**バイナリのデコーディングの深さ（**7-Bit/8-Bit/Binary Decoding Depth**）

[データを無視（Ignore Data）] が無効である場合、デコードを必要としない各 MIME 電子メール添付ファイルから抽出する最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出する場合は 0 を指定します。非デコード データを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータを抽出しません。

Quoted-Printable（**QP**）のデコーディングの深さ（**Quoted-Printable Decoding Depth**）

[データを無視（Ignore Data）] が無効な場合、各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。

1 ～ 65535 バイトを指定するか、または、パケットのすべての QP エンコード データをデコードする場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータをデコードしません。

quoted-printable デコードが有効な場合は、ルール 124:11 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）

[データを無視（Ignore Data）] が無効な場合、各 Unix-to-Unix（UU エンコード）電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての UU エンコード データをデコードする場合は 0 を指定します。UU エンコード データを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータをデコードしません。

Unix-to-Unix デコードが有効な場合は、ルール 124:13 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

MIME 添付ファイル名のログ（Log MIME Attachment Names）

MIME Content-Disposition ヘッダーからの MIME 添付ファイル名の抽出を有効にして、セッションで生成されるすべての侵入イベントにこのファイル名を関連付けます。複数ファイル名がサポートされています。

このオプションが有効である場合、侵入イベントのテーブル ビューの [電子メール添付（Email Attachment）] 列に、イベントに関連付けられているファイル名が表示されます。詳細については、イベントの表示（34-1 ページ）を参照してください。

受信者アドレスのログ（**Log To Addresses**）

SMTP RCPT TO コマンドからの受信者の電子メール アドレスの抽出を有効にし、セッションで生成されるすべての侵入イベントにこの受信者アドレスに関連付けます。複数の受信者がサポートされます。

このオプションが有効である場合、侵入イベントのテーブル ビューの [電子メール受信者（Email Recipient）] 列に、イベントに関連付けられている受信者が表示されます。詳細については、イベントの表示（34-1 ページ）を参照してください。

送信者アドレスのログ（**Log From Addresses**）

SMTP MAIL FROM コマンドからの送信者の電子メール アドレスの抽出を有効にし、セッションで生成されるすべての侵入イベントにこの送信者アドレスを関連付けます。複数の送信者アドレスがサポートされます。

このオプションが有効である場合、侵入イベントのテーブル ビューの [電子メール送信者（Email Sender）] 列に、イベントに関連付けられている送信者が表示されます。詳細については、イベントの表示（34-1 ページ）を参照してください。

ヘッダーのログ（**Log Headers**）

電子メール ヘッダーの抽出を有効にします。抽出されるバイト数は、[ヘッダーのログの深さ（Header Log Depth）] に指定されている値によって決まります。

キーワード `content` または `protected_content` を使用して、電子メール ヘッダー データをパターンとして使用する侵入ルールを作成できます。侵入イベント パケット ビューに、抽出された電子メール ヘッダーが表示されます。詳細については、イベントの表示（34-1 ページ）を参照してください。

ヘッダーのログの深さ（**Header Log Depth**）

[ヘッダーのログ（Log Headers）] が有効である場合、抽出する電子メールヘッダーのバイト数を指定します。0 ～ 20480 バイトを指定できます。値 0 を指定すると、[ヘッダーのログ（Log Headers）] が無効になります。

SMTP デコードの設定

ライセンス：Protection

侵入ポリシーの [SMTP の設定（SMTP Configuration）] ページを使用して、SMTP 正規化を設定できます。SMTP プリプロセッサ設定オプションの詳細については、SMTP デコードについて（19-66 ページ）を参照してください。

SMTP デコード オプションの設定方法：

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **4**　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ **5**　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ **6**　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ **7**　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ **8**　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SMTP 設定（SMTP Configuration）] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[SMTP 設定（SMTP Configuration）] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ **9**　SMTP トラフィックをデコードする必要があるポートを、カンマで区切って指定します。

ステップ 10 SMTP パケットを含む再構成された TCP ストリームを調べるには、[ステートフル インスペクション（Stateful Inspection）] を選択します。再構成されていない SMTP パケットだけを検査するには、[ステートフル インスペクション（Stateful Inspection）] をクリアします。

ステップ 11 正規化オプションを設定します。

- すべてのコマンドを正規化するには、[すべて（All）] を選択します。
- [カスタム コマンド（Custom Commands）] に指定されているコマンドだけを正規化するには、[Cmds] を選択して、正規化するコマンドを指定します。複数のコマンドはスペースで区切ります。
- コマンドを正規化しない場合は、[なし（None）] を選択します。
- MIME メール ヘッダー データ以外のメール データを無視するには、[データを無視（Ignore Data）] をオンにします。
- Transport Security Layer プロトコルで暗号化されたデータを無視するには、[TLS データを無視（Ignore TLS Data）] をオンにします。
- 関連するプリプロセッサ ルールが有効である場合にイベント生成を無効にするには、[アラートなし（No Alerts）] をオンにします。
- SMTP データで不明なコマンドを検出するには、[不明なコマンドの検出（Detect Unknown Commands）] を選択します。

ステップ 12 [コマンドラインの最大長（Max Command Line Len）] フィールドに、コマンドラインの最大長を指定します。

ステップ 13 [ヘッダー行の最大長（Max Header Line Len）] フィールドに、データ ヘッダー行の最大長を指定します。

ステップ 14 [応答行の最大長（Max Response Line Len）] フィールドに、応答行の最大長を指定します。

（注） RCPT TO および MAIL FROM は SMTP コマンドです。プリプロセッサ設定では、コマンド名 RCPT と MAIL がそれぞれ使用されます。プリプロセッサはコード内で RCPT および MAIL を正しいコマンド名にマッピングします。

ステップ 15 必要に応じて、[代替のコマンドラインの最大長（Alt Max Command Line Len）] の横にある [追加（Add）] をクリックして、代替最大コマンドライン長を指定するコマンドを追加します。続いてライン長を指定し、このライン長を適用するコマンドをスペースで区切って指定します。

ステップ 16 [無効なコマンド（Invalid Commands）] フィールドに、無効として扱う検出対象コマンドを指定します。複数のコマンドはスペースで区切ります。

ステップ 17 [有効なコマンド（Valid Commands）] フィールドに、有効として扱うコマンドを指定します。複数のコマンドはスペースで区切ります。

（注） [有効なコマンド（Valid Commands）] リストが空の場合でも、プリプロセッサにより有効なコマンドとして許可されるコマンドは、ATRN、AUTH、BDAT、DATA、DEBUG、EHLO、EMAL、ESAM、ESND、ESOM、ETRN、EVFY、EXPN、HELO、HELP、IDENT、MAIL、NOOP、QUIT、RCPT、RSET、SAML、SOML、SEND、ONEX、QUEU、STARTTLS、TICK、TIME、TURN、TURNME、VERB、VRFY、X-EXPS、X-LINK2STATE、XADR、XAUTH、XCIR、XEXCH50、XGEN、XLICENSE、XQUE、XSTA、XTRN、XUSR です。

ステップ 18 [データ コマンド（Data Commands）] フィールドに、RFC 5321 に基づく SMTP DATA コマンドによるデータの送信と同じ方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

ステップ 19 [バイナリ データ コマンド（Binary Data Commands）] フィールドに、RFC 3030 に基づく BDAT コマンドによるデータの送信と類似の方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

ステップ 20 [認証コマンド（Authentication Commands）] フィールドに、クライアントとサーバの間で認証交換を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

ステップ 21 X-Link2State Microsoft Exchange バッファ データ オーバーフロー攻撃の一部であるパケットを検出するには、[xlink2state の検出（Detect xlink2state）] を選択します。

ステップ 22 各種電子メール添付ファイルで抽出およびデコードするデータの最大バイト数を指定するには、次に示す添付ファイル タイプの値を指定します。

- **Base64** デコーディングの深さ（**Base64 Decoding Depth**）
- **7** ビット/**8** ビット/バイナリのデコーディングの深さ（**7-Bit/8-Bit/Binary Decoding Depth**）（プレーン テキスト、jpeg イメージ、mp3 ファイルなどの各種マルチパート コンテンツ タイプを含む）
- **Quoted-Printable**（**QP**）のデコーディングの深さ（**Quoted-Printable Decoding Depth**）
- **Unix-to-Unix**（**UU**）のデコーディングの深さ（**Unix-to-Unix Decoding Depth**）

1 ～ 65535 バイトを指定するか、または、当該タイプのパケットのすべてのデータを抽出し、必要に応じてデコードする場合は 0 を指定します。添付ファイル タイプのデータを無視するには、-1 を指定します。

抽出したデータを検査するには、侵入ルールで `file_data` キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（27-102 ページ）を参照してください。

また、クロスパケット データや複数の TCP セグメントにわたるデータを抽出してデコードするには、SMTP の [ステートフル インスペクション（Stateful Inspection）] オプションも選択する必要があります。

ステップ 23 SMTP トラフィックによりトリガーとして使用された侵入イベントとコンテキスト情報を関連付けるためのオプションを設定します。

- 侵入イベントに関連付ける MIME 添付ファイル名を抽出できるようにするには、[MIME 添付ファイル名のログ（Log MIME Attachment Names）] を選択します。
- 受信者の電子メール アドレスを抽出できるようにするには、[受信者アドレスのログ（Log To Addresses）] を選択します。
- 侵入イベントに関連付ける送信者の電子メール アドレスを抽出できるようにするには、[送信者アドレスのログ（Log From Addresses）] を選択します。
- 侵入イベントに関連付ける電子メール ヘッダーを抽出し、電子メール ヘッダーを検査するルールを作成できるようにするには、[ヘッダーのログ（Log Headers）] を選択します。

  ヘッダー情報は侵入イベント パケット ビューに表示されることに注意してください。また、キーワード `content` または `protected_content` と共に電子メール ヘッダー データをパターンとして使用する侵入ルールを作成することもできます。詳細については、イベントの表示（34-1 ページ）を参照してください。

  オプションで [ヘッダーのログの深さ（Header Log Depth）] に、抽出する電子メール ヘッダーのバイト数 0 ～ 20480 を指定できます。値 0 を指定すると、[ヘッダーのログ（Log Headers）] が無効になります。

ステップ 24 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

SMTP 最大デコード メモリ アラートの有効化

ライセンス：Protection

有効になっているプリプロセッサが次のタイプのエンコード データのデコードに使用しているメモリの容量がシステムの最大許容メモリ量に達した場合にイベントを生成するには、SMTP プリプロセッサ ルール 124:9 を有効にします。

- Base64
- 7 ビット/8 ビット/バイナリ
- Quoted-printable
- Unix-to-Unix

最大デコード メモリを超えた場合、メモリが使用可能になるまで、プリプロセッサはこれらのタイプのエンコード データのデコードを停止します。このプリプロセッサ ルールは、1 つの特定の設定オプションに関連付けられていません。ルールの有効化については、ルール状態の設定（24-21 ページ）を参照してください。

SSH プロプロセッサによるエクスプロイトの検出

ライセンス：Protection

SSH プリプロセッサは、チャレンジレスポンス バッファ オーバーフロー エクスプロイト、CRC-32 エクスプロイト、SecureCRT SSH クライアント バッファ オーバーフロー エクスプロイト、プロトコル不一致、不正な SSH メッセージ方向を検出します。このプリプロセッサは、バージョン 1 または 2 ではないバージョン文字列も検出します。

チャレンジレスポンス バッファ オーバーフロー攻撃と CRC-32 攻撃はいずれもキー交換の後に発生するので、暗号化されています。いずれの攻撃でも、20 KB を超える普通よりも大きなペイロードが認証チャレンジ直後にサーバに送信されます。CRC-32 攻撃の対象となるのは SSH バージョン 1 のみであり、チャレンジレスポンス バッファ オーバーフロー エクスプロイトの対象となるのは SSH バージョン 2 のみです。バージョン文字列は、セッションの開始時に読み取られます。バージョン文字列の違いを除き、この両方の攻撃は同様に扱われます。

SecureCRT SSH エクスプロイトとプロトコル不一致攻撃は、鍵交換前に接続をセキュリティで保護しようとするときに発生します。SecureCRT エクスプロイトでは、非常に長いプロトコル ID 文字列がクライアントに送信され、これが原因でバッファ オーバーフローが発生します。プロトコル不一致は、非 SSH クライアント アプリケーションがセキュア SSH サーバに接続しようとした場合、またはサーバとクライアントのバージョン番号が一致しない場合に発生します。

指定のポートまたは一連のポートでトラフィックを検査するか、または SSH トラフィックを自動的に検出するように、プリプロセッサを設定できます。指定バイト数に達するまでに指定数の暗号化パケットが渡されたか、指定パケット数に達するまでにバイト数が指定最大バイト数を超えるまで、SSH トラフィックの検査が続行されます。最大バイト数を超えた場合は、CRC-32（SSH バージョン 1）または チャレンジレスポンス バッファ オーバーフロー（SSH バージョン 2）攻撃が発生したとみなされます。また、SecureCRT エクスプロイト、プロトコル不一致、および不正なメッセージ方向を検出できます。プリプロセッサは、設定していない場合でもバージョン 1 または 2 以外のバージョン文字列を検出することに注意してください。

SSH プリプロセッサを使用するときは、次の点に注意してください。

- ジェネレータ ID（GID）128 の SSH プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があります。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

- SSH プリプロセッサは、ブルート フォース攻撃には対処しません。ブルート フォース攻撃の試行については、動的ルール状態の追加（24-31 ページ）を参照してください。

詳細については、次の各項を参照してください。

- SSH プリプロセッサ オプションの選択（19-75 ページ）
- SSH プリプロセッサの設定（19-77 ページ）

SSH プリプロセッサ オプションの選択

ライセンス：Protection

このセクションでは、SSH プリプロセッサを設定するときに使用できるオプションについて説明します。

次のいずれかが発生すると、プリプロセッサはセッションのトラフィックの検査を停止します。

- この数の暗号化パケットで、サーバとクライアント間で有効な交換が行われた場合。接続は続行します。
- 検査対象の暗号化パケットの数に達する前に、[サーバ応答がないまま送信されたバイト数（Number of Bytes Sent Without Server Response）] に達した場合。この場合、攻撃があったものと想定されます。

[検査する暗号化パケットの数（Number of Encrypted Packets to Inspect）] に達するまでの有効な各サーバ応答により、[サーバ応答がないまま送信されたバイト数（Number of Bytes Sent Without Server Response）] がリセットされ、パケット カウントが続行します。

次に示す SSH のプリプロセッサの設定例で説明します。

- [サーバ ポート（Server Ports）]：22
- [自動検出ポート（Autodetect Ports）]：off
- [プロトコル バージョン ストリングの最大長（Maximum Length of Protocol Version String）]：80
- [検査する暗号化パケットの数（Number of Encrypted Packets to Inspect）]：25
- [サーバ応答がないまま送信されたバイト数（Number of Bytes Sent Without Server Response）]：19,600
- 検出オプションはすべて有効です。

この例では、プリプロセッサはポート 22 のトラフィックだけを検査します。つまり、自動検出が無効であるため、指定されたポートでのみ検査をします。

また、次のいずれかが発生すると、この例のプリプロセッサはトラフィックの検査を停止します。

- クライアントが 25 個の暗号化パケットを送信したが、すべてのパケットのデータ合計が 19,600 バイト以下であった。攻撃はなかったと想定されます。
- クライアントが、25 個の暗号化パケットで 19,600 バイトを超えるデータを送信した。この場合、この例のセッションは SSH バージョン 2 セッションであるため、プリプロセッサはこの攻撃がチャレンジレスポンス バッファ オーバーフロー攻撃であるとみなします。

この例のプリプロセッサは、トラフィックの処理時に以下の状況が発生しているかどうかも検出します。

- 80 バイトより長いバージョン文字列によりトリガーとして使用されるサーバ オーバーフロー（これは SecureCRT エクスプロイトを示します）
- プロトコルの不一致
- 誤った方向に流れるパケット

最後に、プリプロセッサは、バージョン 1 または 2 以外のすべてのバージョン文字列を自動的に検出します。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

サーバ ポート（**Server Ports**）

SSH プリプロセッサがトラフィックを検査する必要があるポートを指定します。

1 つのポート、または複数のポートをカンマで区切ったリストを設定できます。

自動検出ポート（**Autodetect Ports**）

SSH トラフィックを自動的に検出するようにプリプロセッサを設定します。

このオプションが選択されている場合、プリプロセッサはすべてのトラフィックで SSH バージョン番号を検査します。クライアント パケットにもサーバ パケットにもバージョン番号が含まれていない場合は、処理が停止します。無効である場合、プリプロセッサは [サーバ ポート（Server Ports）] オプションで指定されているトラフィックだけを検査します。

検査する暗号化パケットの最大数（**Number of Encrypted Packets to Inspect**）

セッションあたりの検査対象の暗号化パケットの数を指定します。

このオプションをゼロに設定すると、すべてのトラフィックの通過が許可されます。

検査対象の暗号化パケットの数を減らすと、一部の攻撃が検出されなくなることがあります。検査対象の暗号化パケットの数を増やすと、パフォーマンスに悪影響を及ぼす可能性があります。

サーバ応答がないまま送信されたバイト数（**Number of Bytes Sent Without Server Response**）

SSH クライアントが、応答を得ることなく、サーバに送信できる最大バイト数を指定します。この最大バイト数を超えると、チャレンジレスポンス バッファ オーバーフロー攻撃または CRC-32 攻撃であるとみなされます。

プリプロセッサがチャレンジレスポンス バッファ オーバーフローまたは CRC-32 エクスプロイトを誤検出する場合は、このオプションの値を増やしてください。

プロトコル バージョン ストリングの最大長（**Maximum Length of Protocol Version String**）

サーバのバージョン文字列の最大許容バイト数を指定します。この値を超えると、SecureCRT エクスプロイトとみなされます。

チャレンジレスポンス バッファ オーバーフロー攻撃の検出（**Detect Challenge-Response Buffer Overflow Attack**）

チャレンジレスポンス バッファ オーバーフロー エクスプロイトの検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:1 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

SSH1 CRC-32 攻撃の検出（**Detect SSH1 CRC-32 Attack**）

CRC-32 エクスプロイトの検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:2 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

サーバ オーバーフローの検出（**Detect Server Overflow**）

SecureCRT SSH クライアント バッファ オーバーフロー エクスプロイトの検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:3 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

プロトコル不一致の検出（**Detect Protocol Mismatch**）

プロトコル不一致の検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:4 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

正しくないメッセージ方向の検出（**Detect Bad Message Direction**）

トラフィックのフロー方向が正しくない場合（つまり、推定されるサーバがクライアント トラフィックを生成したり、クライアントがサーバ トラフィックを生成したりした場合）の検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:5 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

特定のペイロードに正しくないペイロード サイズの検出（**Detect Payload Size Incorrect for the Given Payload**）

SSH パケットに指定された長さが IP ヘッダーに指定されている合計長と矛盾する場合や、メッセージが切り捨てられる場合、つまり完全な SSH ヘッダーを形成できる十分なデータがない場合などの、誤ったペイロード サイズのパケットの検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:6 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

正しくないバージョン ストリングの検出（**Detect Bad Version String**）

有効である場合、プリプロセッサは、設定していない場合でもバージョン 1 または 2 以外のバージョン文字列を検出することに注意してください。

このオプションのイベントを生成するには、ルール 128:7 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

SSH プリプロセッサの設定

ライセンス：Protection

このセクションでは、SSH プリプロセッサを設定する方法について説明します。

SSH プリプロセッサを設定するには、次の手順を実行します。

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（  ）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ 8　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SSH 設定（SSH Configuration）] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[SSH 設定（SSH Configuration）] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 9　[SSH の設定（SSH Configuration）] プリプロセッサ ページのすべてのオプションを変更できます。詳細については、SSH プリプロセッサ オプションの選択（19-75 ページ）を参照してください。

ステップ 10　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

SSL プリプロセッサの使用

ライセンス：Protection

システムは暗号化されたトラフィックの内容を分析できませんが、トラフィック検査の試行を続行するように SSL プリプロセッサ オプションを設定できます。このように設定すると誤検出が発生することがあり、検出リソースを無駄に使用することになります。しかし SSL プリプロセッサを使用することで、システムは SSL セッションの開始時に交換されるハンドシェイクと鍵交換メッセージの内容を分析し、セッションが暗号化される時点を判別できます。SSL 前処理がアクティブな場合、暗号化されたらただちにシステムによりセッション インスペクションを一時停止するようにできます。TCP ストリームの前処理が SSL プリプロセッサを使用できるようになっていることを確認する必要があります。

詳細については、次の項を参照してください。

- SSL 前処理について（19-79 ページ）
- SSL プリプロセッサ ルールの有効化（19-79 ページ）
- SSL プリプロセッサの設定（19-80 ページ）

SSL 前処理について

ライセンス：Protection

SSL プリプロセッサは暗号化データのインスペクションを停止します。これにより誤検出を排除できます。SSL プリプロセッサは、SSL ハンドシェイクを検査するときに状態情報を保持し、そのセッションの状態と SSL バージョンの両方を追跡します。セッションの状態が暗号化されていることをプリプロセッサが検出すると、そのセッションのトラフィックは暗号化されているものとしてシステムによりマークされます。暗号化の確立時に、暗号化セッションですべてのパケットの処理を停止するようにシステムを設定できます。

パケットごとに、IP ヘッダー、TCP ヘッダー、および TCP ペイロードがトラフィックに含まれており、このトラフィックが SSL 前処理用に指定されているポートで発生することが SSL プリプロセッサにより確認されます。次に示す状況では、対象トラフィックについて、トラフィックが暗号化されているかどうかが判別されます。

- システムがセッションのすべてのパケットを監視し、[サーバ側のデータを信頼する（Server side data is trusted）] が有効にされておらず、サーバとクライアントの両方からの完了メッセージ、および Application レコードが存在するが Alert レコードがない各側からの 1 つ以上のパケットが、セッションに含まれている。
- システムがトラフィックの一部を検出せず、[サーバ側のデータを信頼する（Server side data is trusted）] が有効にされておらず、Alert レコードによる応答がない Application レコードが存在する各側からの 1 つ以上のパケットが、セッションに含まれている。
- システムがセッションのすべてのパケットを監視し、[サーバ側のデータを信頼する（Server side data is trusted）] が有効であり、クライアントからの完了メッセージ、および Application レコードが存在するが Alert レコードがないクライアントからの 1 つ以上のパケットが、セッションに含まれている。
- システムがトラフィックの一部を検出せず、[サーバ側のデータを信頼する（Server side data is trusted）] が有効であり、Alert レコードによる応答がない Application レコードが存在するクライアントからの 1 つ以上のパケットが、セッションに含まれている。

暗号化トラフィックの処理を停止することを選択する場合、セッションが暗号化されているものとしてマークされると、そのセッションのその後のパケットは無視されます。

（注）　ルール内で SSL 状態またはバージョン情報を使用するには、キーワード `ssl_state` および `ssl_version` をルールに追加します。詳細については、セッションからの SSL 情報の抽出（27-57 ページ）を参照してください。

SSL プリプロセッサ ルールの有効化

ライセンス：Protection

有効である場合、SSL プリプロセッサは、SSL セッション開始時に交換されるハンドシェイクと鍵交換メッセージの内容を検査します。

ジェネレータ ID（GID）137 の SSL プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があることに注意してください。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

次の表に、有効にできる SSL プリプロセッサ ルールを示します。

表 *19-14*　*SSL* プリプロセッサ ルール

プリプロセッサ ルール **GID:SID**	説明
137:1	server hello の後の client hello（これは無効で、異常な動作とみなされる）を検出します。
137:2	[サーバ側のデータを信頼する（Server side data is trusted）] が無効な場合に、client hello のない server hello を検出します。これは無効であり、異常な動作としてみなされます。詳細については、SSL プリプロセッサの設定（19-80 ページ）を参照してください。

SSL プリプロセッサの設定

ライセンス：Protection

デフォルトでは、暗号化トラフィックの検査が試行されます。SSL プリプロセッサを有効にすると、セッションが暗号化されたときにそのことを検出します。SSL プリプロセッサが有効にされると、ルール エンジンがこのプリプロセッサを呼び出し、SSL の状態およびバージョン情報を取得できるようになります。侵入ポリシーでキーワード `ssl_state` および `ssl_version` を使用してルールを有効にする場合は、そのポリシーで SSL プリプロセッサも有効にする必要があります。

また、暗号化セッションによるインスペクションと再構成を無効にするには、[暗号化トラフィックのインスペクションを停止（Stop inspecting encrypted traffic）] オプションを有効にします。SSL プリプロセッサによりセッションの状態が維持されるため、セッションのすべてのトラフィックのインスペクションを無効にできます。システムが暗号化セッションのトラフィックのインスペクションを停止するのは、SSL 前処理が有効であり、かつ [暗号化トラフィックのインスペクションを停止（Stop inspecting encrypted traffic）] オプションが選択されている場合だけです。

サーバ トラフィックのみに基づいて暗号化トラフィックを識別するには、[サーバ側のデータを信頼する（Server side data is trusted）] オプションを有効にできます。つまり、トラフィックが暗号化されていることを示すサーバ側のデータが信頼されます。SSL プリプロセッサは通常、クライアント トラフィックと、そのトラフィックに対するサーバの応答の両方を調べ、セッションが暗号化されているかどうかを判別します。ただし、セッションの両側を検出できない場合には、システムはトランザクションを暗号化されているものとしてマークしないため、セッションが暗号化されていることを示す SSL サーバを信頼できます。[サーバ側のデータを信頼する（Server side data is trusted）] オプションを有効にする場合は、[暗号化トラフィックのインスペクションを停止（Stop inspecting encrypted traffic）] オプションも有効にして、システムが暗号化セッションのトラフィックの検査を続行しないようにする必要があることに注意してください。

プリプロセッサがトラフィックで暗号化セッションをモニタするポートを指定できます。

（注）　SSL プリプロセッサは、SSL モニタの対象として指定されたポートで SSL 以外のトラフィックを検出すると、そのトラフィックを SSL トラフィックとしてデコードすることを試みた後、破損しているものとしてマークします。

SSL プリプロセッサを設定するには、次の手順を実行します。

ステップ **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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定(Advanced)] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] の横にある編集アイコン()をクリックします。

[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] をクリックします。

[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン()をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定(Settings)] をクリックします。

[設定(Settings)] ページが表示されます。

ステップ 8　[アプリケーション層プリプロセッサ(Application Layer Preprocessors)] の下の [SSL 設定(SSL Configuration)] を有効にしているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[SSL 設定(SSL Configuration)] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(16-1 ページ)を参照してください。

ステップ 9　SSL プリプロセッサが、暗号化されたセッションのトラフィックをモニタする必要があるポートを、カンマで区切って入力します。[ポート(Ports)] フィールドに指定されるポートでのみ、暗号化トラフィックが検査されます。

ステップ 10　[暗号化トラフィックのインスペクションを停止(Stop inspecting encrypted traffic)] チェック ボックスをクリックして、セッションが暗号化されているものとしてマークされた後のそのセッションでのトラフィックのインスペクションを有効または無効にします。

ステップ 11　[サーバ側のデータを信頼する(Server side data is trusted)] チェック ボックスをクリックして、クライアント側トラフィックのみに基づく暗号化トラフィックの識別を有効または無効にします。

ステップ 12　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

SCADA の前処理の設定

ネットワーク分析ポリシーに Supervisory Control and Data Acquisition（SCADA）プリプロセッサを設定します。これによりトラフィックに対して、侵入ポリシーで有効になっているルールを使用した検査を実行できるようになります。詳細については、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（15-1 ページ）を参照してください。

SCADA プロトコルは、製造、水処理、配電、空港、輸送システムなど、工業プロセス、インフラストラクチャ プロセス、および設備プロセスからのデータをモニタ、制御、取得します。ASA FirePOWER モジュールは、ネットワーク分析ポリシーの一部として設定できる Modbus および DNP3 SCADA プロトコル用のプリプロセッサを提供します。

対応する侵入ポリシーで Modbus または DNP3 キーワードを含むルールを有効にすると、システムは現在の設定で自動的に Modbus または DNP3 プロセッサをそれぞれ使用しますが、ネットワーク分析ポリシーのモジュール インターフェイスではプリプロセッサは無効のままになります。詳細については、Modbus キーワード（27-77 ページ）およびDNP3 キーワード（27-79 ページ）を参照してください。

詳細については、次の各項を参照してください。

- Modbus プリプロセッサの設定（20-1 ページ）
- DNP3 プリプロセッサの設定（20-3 ページ）

Modbus プリプロセッサの設定

ライセンス：Protection

Modbus プロトコルは 1979 年に Modicon が初めて発表した、広く利用されている SCADA プロトコルです。Modbus プリプロセッサは、Modbus トラフィックの異常を検出し、ルール エンジンによる処理のために Modbus プロトコルをデコードします。ルール エンジンは Modbus キーワードを使用して特定のプロトコル フィールドにアクセスします。詳細については、Modbus キーワード（27-77 ページ）を参照してください。

1 つの構成オプションで、プリプロセッサが Modbus トラフィックを検査するポートのデフォルト設定を変更できます。

イベントを生成するには、次の表に示す Modbus プリプロセッサ ルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（24-21 ページ）を参照してください。

表 *20-1*　*Modbus* プリプロセッサ ルール

プリプロセッサ ルール **GID:SID**	説明
144:1	Modbus の見出しの長さが、Modbus 機能コードに必要な長さと一致していない場合に、イベントが生成されます。 各 Modbus 機能の要求と応答には期待される形式があります。メッセージの長さが、期待される形式と一致しない場合に、このイベントが生成されます。
144:2	Modbus プロトコル ID がゼロ以外の場合に、イベントが生成されます。プロトコル ID フィールドは、Modbus と共にその他のプロトコルを多重伝送するために使用されます。プリプロセッサはこのような他のプロトコルを処理しないため、代わりにこのイベントが生成されます。
144:3	プリプロセッサが予約済み Modbus 機能コードを検出すると、イベントが生成されます。

Modbus プリプロセッサの使用について、ネットワークに Modbus 対応デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。

Modbus プリプロセッサがモニタするポートを変更するには、次の手順を用いることができます。

Modbus プリプロセッサを設定するには、次の手順を実行します。

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **4**　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ **5**　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ **6**　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ **7**　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ 8　[SCADA プリプロセッサ（SCADA Preprocessors）] の [Modbus の設定（Modbus Configuration）] が有効になっているかどうかに応じて、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[Modbus の設定（Modbus Configuration）] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 9　オプションで、プリプロセッサが Modbus トラフィックを検査するポートを変更します。0 ～ 65535 の整数を指定できます。複数のポートを指定する場合はカンマで区切ります。

ステップ 10　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

DNP3 プリプロセッサの設定

ライセンス：Protection

Distributed Network Protocol（DNP3）は、当初は発電所間で一貫性のある通信を実現する目的で開発された SCADA プロトコルです。DNP3 も、水処理、廃棄物処理、輸送などさまざまな産業分野で幅広く利用されるようになっています。

DNP3 プリプロセッサは、DNP3 トラフィックの異常を検出し、ルール エンジンによる処理のために DNP3 プロトコルをデコードします。ルール エンジンは、DNP3 キーワードを使用して特定のプロトコル フィールドにアクセスします。詳細については、DNP3 キーワード（27-79 ページ）を参照してください。

イベントを生成するには、次の表に示す DNP3 プリプロセッサ ルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（24-21 ページ）を参照してください。

表 *20-2*　*DNP3* プリプロセッサ ルール

プリプロセッサ ルール **GID:SID**	説明
145:1	[無効な CRC を記録（Log bad CRC）] が有効である場合に、無効なチェックサムを含むリンク層フレームがプリプロセッサにより検出されると、イベントが生成されます。
145:2	無効な長さの DNP3 リンク層フレームがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:3	再構成中に無効なシーケンス番号のトランスポート層セグメントがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:4	完全なフラグメントを再構成する前に DNP3 再構成バッファがクリアされると、イベントが生成されます。このことは、FIR フラグを伝送するセグメントが、他のセグメントがキューに入れられた後で現れる場合に発生します。
145:5	予約済みアドレスを使用する DNP3 リンク層フレームをプリプロセッサが検出すると、イベントが生成されます。
145:6	予約済み機能コードを使用する DNP3 要求または応答をプリプロセッサが検出すると、イベントが生成されます。

DNP3 プリプロセッサの使用について、ネットワークに DNP3 対応デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。詳細については、TCP ストリームの前処理の設定（21-30 ページ）を参照してください。

設定できる DNP3 プリプロセッサ オプションを以下に説明します。

ポート

指定された各ポートでの DNP3 トラフィックのインスペクションを有効にします。1 つのポートを指定するか、複数のポートをカンマで区切ったリストを指定できます。各ポートに 0 ～ 65535 の値を指定できます。

無効な **CRC** を記録（**Log bad CRCs**）

有効である場合、DNP3 リンク層フレームに含まれているチェックサムが検証されます。無効なチェックサムを含むフレームは無視されます。

無効なチェックサムが検出されたときにイベントを生成するには、ルール 145:1 を有効にします。

DNP3 プリプロセッサを設定するには、以下の手順を実行します。

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **4**　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ **5**　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ **6**　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ **7**　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ **8**　[SCADA プリプロセッサ（SCADA Preprocessors）] の下の [DNP3 の設定（DNP3 Configuration）] を有効にしているかどうかに応じて、次の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[DNP3 の設定（DNP3 Configuration）] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 9　オプションで、プリプロセッサが DNP3 トラフィックを検査するポートを変更します。0 ～ 65535 の整数を指定できます。複数のポートを指定する場合はカンマで区切ります。

ステップ 10　オプションで、[無効な CRC を記録（Log bad CRCs）] チェック ボックスをオンまたはオフにして、DNP3 リンク層フレームに含まれているチェックサムを検証し、無効なチェックサムのフレームを無視するかどうかを指定します。

ステップ 11　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、ネットワーク分析ポリシーの編集操作 の表を参照してください。

トランスポート層およびネットワーク層の前処理の設定

ネットワーク分析ポリシー内のネットワーク層プリプロセッサでほとんどのトランスポートを設定します。これにより、侵入ポリシーで有効になっているルールを使った検査に向けてトラフィックが準備されます。詳細については、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（15-1 ページ）を参照してください。

トランスポート層およびネットワーク層のプリプロセッサは、IP フラグメンテーション、チェックサム検証、TCP および UDP セッションの前処理を悪用する攻撃を検出します。パケットがプリプロセッサに送信される前に、パケット デコーダはパケット ヘッダーとペイロードを、プリプロセッサおよび侵入ルール エンジンで簡単に使用できるフォーマットに変換し、パケット ヘッダー内でさまざまな変則的動作を検出します。インライン正規化プリプロセッサは、パケットをデコードした後、他のプリプロセッサにパケットを送信する前に、インライン型展開を対象にトラフィックを正規化します。

ネットワーク分析ポリシーで設定したトランスポート層およびネットワーク層のプリプロセッサ設定は、ゾーン、またはネットワークによって調整できます。一部のトランスポート層およびネットワーク層の設定はすべてのトラフィックにグローバルに適用され、アクセス コントロール ポリシーでこれらを設定します。

トランスポート/ネットワークの詳細設定の構成

ライセンス：Protection

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 ポリシーを適用するすべてのネットワークおよびゾーン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。

次の項では、これらの設定について説明します。

侵入廃棄ルールでのアクティブ応答の開始

ライセンス：Protection

廃棄ルールは、ルール状態が [ドロップしてイベントを生成する（Drop and Generate Events）] に設定された侵入ルールまたはプリプロセッサ ルールです。インライン展開では、システムは TCP または UDP 廃棄ルールに応答するために、トリガーしたパケットをドロップし、そのパケットが開始されたセッションをブロックします。パッシブ展開の場合、システムがパケットをドロップすることはできません。また、セッションをブロックすることもありませんが、アクティブ応答を使用する場合はその限りではありません。

ヒント　UDP データ ストリームは一般にセッションという観点では考慮されないため、ストリーム プリプロセッサがカプセル化 IP データグラム ヘッダーの送信元および宛先 IP アドレス フィールドと UDP ヘッダーのポート フィールドを使用してフローの方向を判別し、UDP セッションを識別する方法については、UDP ストリームの前処理の使用（21-33 ページ）で詳しく説明しています。

[最大アクティブ応答数（Maximum Active Responses）] オプションを設定することで、問題のあるパケットによって TCP または UDP 廃棄ルールがトリガーされた時点で、1 つ以上のアクティブ応答を開始して、より正確かつ明示的に TCP 接続または UDP セッションを閉じることができます。

インライン展開でアクティブ応答が有効にされている場合、システムは TCP 廃棄ルールへの応答として、トリガーしたパケットをドロップし、クライアントとサーバの両方のトラフィックに TCP リセット（RST）パケットを挿入します。システムはパッシブ展開でパケットをドロップできません。アクティブ応答がパッシブ展開で有効になっている場合、システムは TCP 接続のクライアント側とサーバ側の両方に TCP リセットを送信することによって TCP 廃棄ルールに応答します。インライン展開またはパッシブ展開でアクティブ応答が有効にされていると、システムはセッションの両端に ICMP 到達不能パケットを送信することによって UDP セッションを閉じます。リセットは接続やセッションに影響を与えるのに間に合うまでに到着する可能性が高いため、アクティブ応答はインライン展開で最も効果を発揮します。

[最大アクティブ応答数（Maximum Active Responses）] オプションの設定方法によっては、接続またはセッションのいずれかの側からさらにトラフィックが発生しているようであれば、システムが追加のアクティブ応答を開始することもできます。システムは、指定された間隔（秒数）で、指定された最大回数まで追加のアクティブ応答を開始します。

アクティブ応答の最大数を設定する方法については、TCP グローバル オプションの選択（21-22 ページ）を参照してください。

[最大アクティブ応答数（Maximum Active Responses）] の設定とは関係なく、**resp** または **react** ルールがトリガーされた場合にも、アクティブ応答が開始されることに注意してください。ただし、[最大アクティブ応答数（Maximum Active Responses）] は、廃棄ルールに対するアクティブ応答の最大数を制御するのと同じ方法で、**resp** および **react** ルールに対して追加のアクティブ応答をシステムが開始するかどうかを制御します。詳細については、ルール キーワードを使用したアクティブ応答の開始（27-87 ページ）を参照してください。

`config response` コマンドを使用して、使用するアクティブ応答インターフェイス、およびパッシブ展開で試行する TCP リセットの回数を設定することもできます。詳細については、アクティブ応答のリセット試行とインターフェイスの設定（27-90 ページ）を参照してください。

プリプロセッサ ルールは、次のオプションに関連付けられていません。

最大アクティブ応答数（**Maximum Active Responses**）

TCP 接続あたりのアクティブ応答の最大数を 1 ～ 25 の範囲で指定します。アクティブ応答が開始された接続でさらにトラフィックが発生し、前のアクティブ応答を送信してから [最小応答秒数（Minimum Response Seconds）] を超えるトラフィックが発生した場合、システムは指定された最大数に達するまで、別のアクティブ応答を送信します。0 を設定すると、廃棄

ルールによってトリガーされるアクティブ応答が無効になり、**resp** または **react** ルールによってトリガーされる追加のアクティブ応答も無効になります。詳細については、侵入廃棄ルールでのアクティブ応答の開始（21-2 ページ）およびルール キーワードを使用したアクティブ応答の開始（27-87 ページ）を参照してください。

最小応答秒数（**Minimum Response Seconds**）

[最小応答秒数（Maximum Active Responses）] に達するまで、システムがアクティブ応答を開始した接続で発生した追加のトラフィックに対して次のアクティブ応答を送信するまで待機する時間を 1 ～ 300 秒の範囲で指定します。

廃棄ルールでのアクティブ応答の開始方法：

ステップ **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。

ステップ **2** 編集するアクセス 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。

ステップ **3** [詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **4** [ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ **5** [ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ **6** 編集するアクセス 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。

ステップ **7** [詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **8** [転送またはネットワークレイヤープリプロセッサ設定（Transport/Network Layer Preprocessor Settings）] の横にある編集アイコン（）をクリックします。

[転送またはネットワークレイヤープリプロセッサ設定（Transport/Network Layer Preprocessor Settings）] ポップアップ ウィンドウが表示されます。

ステップ **9** 次の選択肢があります。

- TCP 接続 1 つあたりの [最大アクティブ応答数（Maximum Active Responses）] を 1 ～ 25 の値で指定します。0 を設定すると、廃棄ルールによってトリガーされるアクティブ応答が無効になり、**resp** または **react** ルールによってトリガーされる追加のアクティブ応答も無効になります。
- [最大アクティブ応答数（Maximum Active Responses）] が発生するか、またはシステムがアクティブ応答を開始した接続で追加のトラフィックが次のアクティブ応答をもたらすまで待機する [最小応答秒数（Maximum Active Responses）] を 1 ～ 300 の値で指定します。

ステップ **10** [OK] をクリックします。

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（4-12 ページ）を参照してください。

トラブルシューティング:セッション終了メッセージのロギング

ライセンス:Protection

トラブルシューティングの電話中に、個別の接続が指定したしきい値を超えた場合にメッセージを記録するようにシステムを設定することをサポートから依頼される場合があります。このオプションの設定を変更するとパフォーマンスに影響するので、必ずサポートのガイダンスに従って実行してください。

セッション終了メッセージの記録方法:

ステップ 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定(Advanced)] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] の横にある編集アイコン( )をクリックします。

[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] をクリックします。

[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するアクセス 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。

ステップ 7　[詳細設定(Advanced)] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 8　[転送またはネットワークレイヤープリプロセッサ設定(Transport/Network Layer Preprocessor Settings)] の横にある編集アイコン( )をクリックします。

[転送またはネットワークレイヤープリプロセッサ設定(Transport/Network Layer Preprocessor Settings)] ポップアップ ウィンドウが表示されます。

ステップ 9　[トラブルシューティング オプション(Troubleshooting Options)] を展開します。

ステップ 10　[セッション終了ロギングしきい値(Session Termination Logging Threshold)] にメッセージの記録を開始するバイト数を指定します。セッションが終了し、そのバイト数を超えている場合はメッセージが記録されます。

上限は 1 GB ですが、デバイス上でストリーム処理のために割り振られるメモリの量によっても制限されます。

ステップ 11　[OK] をクリックします。

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(4-12 ページ)を参照してください。

チェックサムの検証

ライセンス：Protection

システムは、あらゆるプロトコル レベルのチェックサムを検証することで、IP、TCP、UDP、および ICMP による送信データが完全に受信されていることを確認できます。さらに基本的なレベルで、パケットが転送中に改ざんされたり、誤って変更されたりしていないことも確認できます。チェックサムはアルゴリズムを使用して、パケットでのプロトコルの整合性を検証します。システムが終端のホストでパケットに書き込まれた値を計算し、それがチェックサムと同じであれば、そのパケットは変更されていないと見なされます。

チェックサムの検証を無効にすると、ネットワークが侵入攻撃にさらされる危険があります。システムは、チェックサム検証イベントを生成しないことに注意してください。インライン展開では、パケットのチェックサムが正しくない場合、そのパケットをドロップするようにシステムを設定できます。

チェックサム検証の設定方法：

ステップ 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシーの編集（Edit Policy）] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ 8　[トランスポートまたはネットワーク レイヤー プロセッサ（Transport/Network Layer Preprocessors）] で [チェックサム検証（Checksum Verification）] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[チェックサム検証（Checksum Verification）] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 9　[チェックサム検証（Checksum Verification）] セクションの以下のオプションはいずれも、パッシブまたはインライン展開では [有効（Enabled）] または [無効（Disabled）] に設定できます。インライン展開では、[ドロップ（Drop）] に設定することもできます。

- **ICMP** チェックサム（**ICMP Checksums**）
- **IP** チェックサム（**IP Checksums**）
- **TCP** チェックサム（**TCP Checksums**）
- **UDP** チェックサム（**UDP Checksums**）

違反パケットをドロップするには、オプションを [ドロップ（Drop）] に設定することに加え、関連付けられているネットワーク分析ポリシーの [インライン モード（Inline Mode）] も有効にする必要があることに注意してください。詳細については、インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（18-6 ページ）を参照してください。また、パッシブ展開で、これらのオプションを [ドロップ（Drop）] に設定すると、オプションを [有効（Enabled）] に設定した場合と同じ効果があることに注意してください。

ステップ 10　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

インライン トラフィックの正規化

ライセンス：Protection

インライン正規化プリプロセッサは、インライン展開で攻撃者が検出を免れる可能性を最小限にするために、トラフィックを正規化します。ネットワーク分析ポリシーでインライン正規化プリプロセッサを有効にすると、システムは次の 2 つの状態をテストして、ユーザがインライン展開を使用していることを確認します。

- [インライン モード（Inline Mode）] がポリシーで有効になっている。インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（18-6 ページ）を参照してください。
- インライン正規化が有効なアクセス コントロール ポリシーがインラインで展開されているデバイスに適用されている。

上記の両方の条件に一致した場合のみ、プリプロセッサは指定されたトラフィックを正規化します。

IPv4、IPv6、ICMPv4、ICMPv6、TCP トラフィックを任意に組み合わせて正規化を指定できます。ほとんどの正規化は、パケット単位で行われ、インライン正規化プリプロセッサによって処理されます。ただし、TCP ストリーム プリプロセッサは、TCP ペイロードの正規化を含む、ほとんどの状態関連パケットおよびストリームの正規化を処理します。

インライン正規化は、パケット デコーダによるデコードの直後に行われます。その後で、別のプリプロセッサによる処理が行われます。正規化は、パケット層の内部から外部への方向で行われます。

インライン正規化プリプロセッサはイベントを生成しません。インライン正規化プリプロセッサの役割は、インライン展開の別のプリプロセッサおよびルール エンジンで使用できるようにパケットを準備することです。また、システムが処理するパケットが、ネットワーク上のホストで受信したパケットと同じであるようにする役割もあります。

ヒント　インライン展開の場合、シスコでは、インライン正規化プリプロセッサの設定で [TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にすることを推奨しています。パッシブ展開の場合、シスコでは、適応型プロファイルを設定することを推奨しています。詳細については、パッシブ展開における前処理の調整（22-1 ページ）を参照してください。

最小 **TTL**（**Minimum TTL**）

[TTL のリセット（Reset TTL）] がこのオプションに設定する値 1 ～ 255 以上の値に設定されている場合、このオプションは以下を指定します。

- [IPv4 の正規化（Normalize IPv4）] が有効にされている場合は、[IPv4 存続可能時間（TTL）（IPv4 Time to Live (TTL)）] フィールドの最小許容値。TTL のパケット値がこの値を下回る場合、[TTL のリセット（Reset TTL）] に設定された値に正規化されます。
- [IPv6 の正規化（Normalize IPv6）] が有効にされている場合は、[IPv6 ホップ リミット（IPv6 Hop Limit）] フィールドの最小許容値。ホップ リミットの値がこの値を下回る場合、[TTL のリセット（Reset TTL）] に設定された値に正規化されます。

  このフィールドが空白の場合、システムは値が 1 であると想定します。

  デコーダ ルール カテゴリで以下のルールを有効にすると、このオプションに対するイベントを生成できます。

- 指定の最小値を下回る TTL が設定された IPv4 パケットが検出された場合にイベントを生成するには、ルール 116:428 を有効にします。
- 指定の最小値を下回るホップ リミットが設定された IPv6 パケットが検出された場合にイベントを生成するには、ルール 116:270 を有効にします。

  詳細については、パケットのデコードの設定（21-20 ページ）のパケット デコーダの [プロトコル ヘッダーの異常の検出（Detect Protocol Header Anomalies）] オプションを参照してください。

TTL のリセット（**Reset TTL**）

このオプションに設定した値 1 ～ 255 が [最小 TTL（Minimum TTL）] 値を上回る場合、以下のフィールドが正規化されます。

- [IPv4 の正規化（Normalize IPv4）] が有効にされている場合は、[IPv4 TTL] フィールド
- [IPv6 の正規化（Normalize IPv6）] が有効にされている場合は、[IPv6 ホップ リミット（IPv6 Hop Limit）] フィールド

  パケット値が [最小 TTL（Minimum TTL）] を下回る場合、システムはパケットの TTL またはホップ リミットの値をこのオプションに対して設定された値に変更して、パケットを正規化します。このオプションを値 0 または [最小 TTL（Minimum TTL）] を下回る値に設定すると、オプションは無効になります。このフィールドが空白の場合、システムは値が 0 であると想定します。

IPv4 の正規化（**Normalize IPv4**）

IPv4 トラフィックの正規化を有効にします。このオプションが有効にされていて、[TTL のリセット（Reset TTL）] に設定された値が TTL 正規化を有効にしている場合、システムは必要に応じて TTL フィールドも正規化します。このオプションを有効にする場合、[フラグメント禁止ビットの正規化（Normalize Don't Fragment Bits）] および [リザーブド ビットの正規化（Normalize Reserved Bits）] オプションも有効にすることができます。

このオプションを有効にすると、システムは以下の基本の IPv4 正規化を実行します。

- 過剰なペイロードを持つパケットを、IP ヘッダーに指定されたデータグラム長まで切り捨てます。
- [差別化サービス（DS）（Differentiated Services (DS)）] フィールド（旧称 [タイプ オブ サービス（TOS）（Type of Service (TOS)）] フィールド）をクリアします。
- すべてのオプション オクテットを 1（[操作なし（No Operation）]）に設定します。

フラグメント禁止ビットの正規化（**Normalize Don't Fragment Bit**）

[IPv4 フラグ（IPv4 Flags）] ヘッダー フィールドの単一ビットの [フラグメント禁止（Don't Fragment）] サブフィールドをクリアします。このオプションを有効にすると、ダウンストリームのルータがパケットをドロップする代わりに、必要に応じてパケットをフラグメント化できます。また、このオプションを有効にすることで、ドロップされるパケットを巧妙に作成してポリシーを回避する試みを防ぐこともできます。このオプションを選択するには、[IPv4 の正規化（Normalize IPv4）] を有効にする必要があります。

リザーブド ビットの正規化（**Normalize Reserved Bit**）

[IPv4 フラグ（IPv4 Flags）] ヘッダー フィールドの単一ビットの [予約済み（Reserved）] サブフィールドをクリアします。通常は、このオプションを有効にします。このオプションを選択するには、[IPv4 の正規化（Normalize IPv4）] を有効にする必要があります。

TOS ビットの正規化（**Normalize TOS Bit**）

1 バイトの [差別化サービス（Differentiated Services）]（旧称 [タイプ オブ サービス（Type of Service）]）フィールドをクリアします。このオプションを選択するには、[IPv4 の正規化（Normalize IPv4）] を有効にする必要があります。

余剰ペイロードの正規化（**Normalize Excess Payload**）

過剰なペイロードを持つパケットを、IP ヘッダーに指定されたデータグラム長にレイヤ 2（たとえば、イーサネット）ヘッダーを合計した長さにまで切り捨てます。ただし、最小フレーム長より小さく切り捨てることはしません。このオプションを選択するには、[IPv4 の正規化（Normalize IPv4）] を有効にする必要があります。

IPv6 の正規化（**Normalize IPv6**）

[ホップバイホップ オプション（Hop-by-Hop Options）] および [宛先オプション（Destination Options）] 拡張ヘッダーに含まれるすべてのオプション タイプ フィールドを 00（スキップして処理を続行）に設定します。このオプションが有効にされていて、[TTL のリセット（Reset TTL）] に設定された値がホップ リミット正規化を有効にしている場合、システムは必要に応じてホップ リミット フィールドも正規化します。

ICMPv4 の正規化（**Normalize ICMPv4**）

ICMPv4 トラフィックのエコー（要求）およびエコー応答メッセージで 8 ビットのコード フィールドをクリアします。

ICMPv6 の正規化（**Normalize ICMPv6**）

ICMPv6 トラフィックのエコー（要求）およびエコー応答メッセージで 8 ビットのコード フィールドをクリアします。

予約済みビットの正規化またはクリア（**Normalize/Clear Reserved Bits**）

TCP ヘッダーの予約ビットをクリアします。

オプション パディング バイトの正規化またはクリア（**Normalize/Clear Option Padding Bytes**）

TCP オプションのパディング バイトをクリアします。

URG=0 の場合に緊急ポインタをクリア（**Clear Urgent Pointer if URG=0**）

緊急（URG）制御ビットが設定されていない場合、16 ビットの TCP ヘッダー [緊急ポインタ（Urgent Pointer）] フィールドをクリアします。

空のペイロードに設定された緊急ポインタまたは **URG** をクリア（**Clear Urgent Pointer/URG on Empty Payload**）

ペイロードがない場合、TCP ヘッダー [緊急ポインタ（Urgent Pointer）] フィールドおよび URG 制御ビットをクリアします。

緊急ポインタが設定されていない場合 **URG** をクリア（**Clear URG if Urgent Pointer is Not Set**）

緊急ポインタが設定されていない場合、TCP ヘッダー URG 制御ビットをクリアします。

緊急ポインタの正規化（**Normalize Urgent Pointer**）

ポインタがペイロード長を上回る場合、2 バイトの TCP ヘッダー [緊急ポインタ（Urgent Pointer）] フィールドをペイロード長に設定します。

TCP ペイロードの正規化（**Normalize TCP Payload**）

再送信されるデータの一貫性が確保されるように [TCP データ（TCP Data）] フィールドの正規化を有効にします。正しく再構成できないセグメントはすべてドロップされます。

SYN に関するデータを削除（**Remove Data on SYN**）

TCP オペレーティング システム ポリシーが Mac OS 以外の場合、同期（SYN）パケットのデータを削除します。

このオプションによって、ルール 129:2 のイベント生成も無効になります。

RST に関するデータを削除（**Remove Data on RST**）

TCP リセット（RST）パケットからデータを削除します。

データをウィンドウにトリミング（**Trim Data to Window**）

[TCP データ（TCP Data）] フィールドを [ウィンドウ（Window）] フィールドに指定されたサイズにまで切り捨てます。

データを **MSS** にトリミング（**Trim Data to MSS**）

ペイロードが MSS より長い場合、[TCP データ（TCP Data）] フィールドを最大セグメント サイズ（MSS）にまで切り捨てます。

回復不能な **TCP** ヘッダーの異常をブロック（**Block Unrecoverable TCP Header Anomalies**）

このオプションを有効にすると、システムは無効になり受信ホストによってブロックされる可能性が高い異常な TCP パケット（正規化されている場合）をブロックします。たとえば、システムは確立されたセッションの後に送信された SYN パケットをブロックします。

また、システムは、ルールが有効にされているかどうかに関係なく、以下に示す TCP ストリーム プリプロセッサ ルールのいずれかに一致するパケットもドロップします。

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 ～ 129:19

[ブロックされたパケットの合計（Total Blocked Packets）] パフォーマンス グラフは、インライン展開でブロックされたパケット数を追跡し、パッシブ展開では、インライン展開でブロックされたであろう数を追跡します。

明示的な混雑通知（**ECN**）（**Explicit Congestion Notification**）

明示的輻輳通知（ECN）フラグのパケット単位またはストリーム単位の正規化を以下のように有効にします。

- [パケット（Packet）] を選択すると、ネゴシエーションに関係なく、パケット単位で ECN フラグがクリアされます。
- [ストリーム（Stream）] を選択すると、ECN の使用がネゴシエートされていない場合、ストリーム単位で ECN フラグがクリアされます。

  [ストリーム（Stream）] を選択した場合、この正規化が実行されるようにするには、TCP ストリーム プリプロセッサの [TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）] オプションも有効にされている必要があります。詳細については、TCP ポリシーのオプションの選択（21-24 ページ）を参照してください。

これらの **TCP** オプションを許可（**Allow These TCP Options**）

トラフィックで許可する特定の TCP オプションの正規化を無効にします。

明示的に許可されたオプションは、正規化されません。オプションを [操作なし（No Operation）]（TCP オプション 1）に設定して明示的に許可していないオプションは、正規化されます。

最大セグメント サイズ（MSS）、ウィンドウ スケール、およびタイムスタンプ TCP のオプションは TCP パフォーマンスを最適化するために一般的に使用されるため、システムは、これらのオプションを常に許可します。システムは、[これらの TCP オプションを許可（Allow These TCP Options）] の設定に関係なく、これらの一般的に使用されるオプションを正規化します。他のそれほど一般的に使用されないオプションについては、システムは自動的に許可しません。

特定のオプションを許可するには、オプション キーワード、オプション番号、またはこの両方のカンマ区切りリストを設定します。以下に、一例を示します。

```
sack, echo, 19
```

オプション キーワードを指定するということは、そのキーワードと関連付けられた 1 つ以上の TCP オプションの番号を指定することと同じです。たとえば、`sack` を指定することは、TCP オプション 4（Selective Acknowledgment Permitted）および TCP オプション 5（Selective Acknowledgment）を指定することと同じです。オプション キーワードでは、大文字と小文字が区別されません。

また、`any` を指定すると、すべての TCP オプションが許可されるため、実質的にすべての TCP オプションの正規化が無効にされます。

次の表に、許可する TCP オプションを指定する方法を要約します。フィールドを空のままにすると、システムは MSS、ウィンドウ スケール、およびタイムスタンプのオプションのみを許可します。

指定する内容	許可されるオプション
sack	TCP オプション 4（Selective Acknowledgment Permitted）および 5（Selective Acknowledgment）
エコー	TCP オプション 6（Echo Request）および 7（Echo Reply）
partial_order	TCP オプション 9（Partial Order Connection Permitted）および 10（Partial Order Service Profile）
conn_count	TCP 接続数オプション 11（CC）、12（CC.New）、および 13（CC.Echo）
alt_checksum	TCP オプション 14（Alternate Checksum Request）および 15（Alternate Checksum）
md5	TCP オプション 19（MD5 Signature）
オプション番号 2 ～ 255	キーワードのないオプションを含む、特定のオプション
任意	すべての TCP オプション（この設定は、実質的に TCP オプションの正規化を無効にします）

このオプションに any を指定しない場合、正規化には次のものが含まれます。

- MSS、ウィンドウ スケール、タイムスタンプ、およびその他の明示的に許可されたオプションを除き、すべてのオプションのバイトを [操作なし（No Operation）]（TCP オプション 1）に設定します。
- タイムスタンプは存在していても無効な場合、あるいは有効であってもネゴシエートされない場合、タイムスタンプ オクテットを [操作なし（No Operation）] に設定します。
- タイムスタンプがネゴシエートされるものの、存在しない場合、パケットをブロックします。
- 確認応答（ACK）制御ビットが設定されていない場合、[タイム スタンプ エコー応答（TSecr）（Time Stamp Echo Reply (TSecr)）] オプション フィールドをクリアします。
- SYN 制御ビットが設定されていない場合、[MSS] および [ウィンドウ スケール（Window Scale）] オプションを [操作なし（No Operation）]（TCP オプション 1）に設定します。

インライン正規化プリプロセッサの設定方法:

ステップ 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシーの編集（Edit Policy）] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ 8　[トランスポートまたはネットワーク レイヤー プロセッサ（Transport/Network Layer Preprocessors）] で [インライン正規化（Inline Normalization）] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[インライン正規化（Inline Normalization）] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 9　インライン トラフィックの正規化（21-6 ページ）で説明されている任意のオプションを設定できます。

ステップ 10　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

IP パケットの最適化

ライセンス：Protection

最大伝送ユニット（MTU）より大きいために IP データグラムが複数の小さい IP データグラムに分割されると、その IP データグラムはフラグメント化されたことになります。単一の IP データグラム フラグメントには、隠れた攻撃を識別するのに十分な情報が含まれない場合があります。そのため、攻撃者はエクスプロイトの検出を免れるために、フラグメント化されるパケットで攻撃データを送信する可能性があります。IP 最適化プリプロセッサは、ルール エンジンが IP データグラムに対してルールを実行する前に、パケットに仕込まれた攻撃をルールで識別しやすくするために、フラグメント化された IP データグラムを再構成します。フラグメント化されたデータグラムを再構成できない場合、それらのデータグラムに対しては、ルールが実行されません。

IP 最適化プリプロセッサのルールにイベントを生成させるには、これらのルール（ジェネレータ ID（GID）が 123 のルール）を有効にする必要があります。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

詳細については、次の各項を参照してください。

- IP フラグメンテーションのエクスプロイトについて（21-12 ページ）
- ターゲットベースの最適化ポリシー（21-13 ページ）
- 最適化オプションの選択（21-14 ページ）
- IP 最適化の設定（21-15 ページ）

IP フラグメンテーションのエクスプロイトについて

ライセンス：Protection

IP 最適化を有効にすると、ネットワーク上のホストに対する攻撃（ティアドロップ攻撃など）や、システム自体に対するリソース消費攻撃（Jolt2 攻撃など）を検出するのに役立ちます。

ティアドロップ攻撃は、特定のオペレーティング システムのバグを悪用して、そのオペレーティング システムがオーバーラップした IP フラグメントを再構成しようとするとクラッシュするように仕掛けます。IP 最適化プリプロセッサを有効にして、オーバーラップしたフラグメントを識別するように設定すれば、該当するフラグメントを識別できます。IP 最適化プリプロセッサは、ティアドロップ攻撃などのオーバーラップ フラグメント攻撃で、最初のパケットを検出するだけで、同じ攻撃での後続のパケットは検出しません。

Jolt2 攻撃では、IP 最適化機能を酷使させるという方法でサービス妨害攻撃を仕掛けるために、フラグメント化された同じ IP パケットのコピーを大量に送信します。IP 最適化プリプロセッサでは、メモリ使用量の上限によって、このような攻撃を阻止し、包括的検査においてシステムを自己防衛状態にします。システムは攻撃によって過負荷にならず、運用可能な状態を維持し、ネットワーク トラフィックの検査を続行します。

フラグメント化されたパケットを再構成する方法は、オペレーティング システムによって異なります。ホストがどのオペレーティング システムで実行されているのかを攻撃者が特定できれば、その攻撃者はターゲット ホストが特定の方法で再構成するように不正なパケットをフラグメント化することも可能です。モニタ対象のネットワーク上でホストを実行しているオペレーティング システムは、システムには不明です。したがって、プリプロセッサがパケットを誤った

方法で再構成して検査し、それによってエクスプロイトが検出されないままパス スルーする可能性があります。このような攻撃を軽減するために、ネットワーク上のホストごとに適切な方法でパケットを最適化するよう、最適化プリプロセッサを設定できるようになっています。詳細については、ターゲットベースの最適化ポリシー（21-13 ページ）を参照してください。

適応型プロファイルを使用することで、パケットのターゲット ホストのホスト オペレーティング システム情報に応じて、IP 最適化プリプロセッサに適用するターゲットベースのポリシーが動的に選択されるようにすることができます。詳細については、パッシブ展開における前処理の調整（22-1 ページ）を参照してください。

ターゲットベースの最適化ポリシー

ライセンス：Protection

ホストのオペレーティング システムは、パケットを再構成する際に優先するパケット フラグメントを判断するために、3 つの基準を使用します。それは、オペレーティング システムがフラグメントを受信した順序、フラグメントのオフセット（パケットの先頭からのフラグメントの距離（バイト単位））、オーバーラップ フラグメントとの相対開始位置および終了位置です。これらの基準はすべてのオペレーティング システムで使用されているものの、フラグメント化されたパケットを再構成するときに優先するフラグメントは、オペレーティング システムによって異なります。したがって、ネットワーク上で異なるオペレーティング システムを使用する 2 台のホストが、同じオーバーラップ フラグメントをまったく異なる方法で再構成する場合も考えられます。

いずれかのホストのオペレーティング システムを認識している攻撃者が、オーバーラップしたパケット フラグメントに不正なコンテンツを忍ばせて送信することによって、エクスプロイトの検出を免れ、そのホストを悪用する可能性があります。このパケットが他のホストで再構成されて検査されても、パケットに害はないように見えますが、ターゲット ホストで再構成される場合には不正なエクスプロイトが含まれています。ただし、モニタ対象のネットワーク セグメントで稼働するオペレーティング システムを認識するように IP 最適化プリプロセッサを設定すれば、このプリプロセッサがターゲット ホストと同じ方法でフラグメントを再構成することによって、攻撃を識別できます。

ターゲット ホストのオペレーティング システムに応じて、7 つの最適化ポリシーのうちのいずれかを使用するように IP 最適化プリプロセッサを設定できます。以下の表に、7 つのポリシーと、それぞれのポリシーを使用するオペレーティング システムを記載します。First と Last というポリシー名は、これらのポリシーが元のオーバーラップ パケットまたは後続のオーバーラップ パケットのどちらを優先するかを反映しています。

表 **21-1**　ターゲットベースの最適化ポリシー

ポリシー	オペレーティング システム
BSD	AIX
	FreeBSD
	IRIX
	VAX/VMS
BSD-right	HP JetDirect
ファースト	Mac OS
	HP-UX
Linux	Linux
	OpenBSD
Last	Cisco IOS
Solaris	SunOS
Windows	Windows

最適化オプションの選択

ライセンス：Protection

IP 最適化を有効または無効にすることだけを選択することもできますが、シスコでは、それよりも細かいレベルで、有効にする IP 最適化プリプロセッサの動作を指定することを推奨しています。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

[事前に割り当てられたフラグメント（Preallocated Fragments）] グローバル オプションを設定できます。

事前に割り当てられたフラグメント（**Preallocated Fragments**）

プリプロセッサが一度に処理できる個々のフラグメントの最大数。事前割り当てするフラグメント ノードの数を指定すると、静的メモリ割り当てが有効になります。

⚠

注意　個々のフラグメントの処理には、約 1550 バイトのメモリが使用されます。プリプロセッサで個々のフラグメントを処理するために必要なメモリが、デバイスに事前定義された使用可能なメモリ量の制限を上回る場合は、デバイスのメモリ制限が優先されます。

IP 最適化ポリシーごとに、以下のオプションを設定できます。

ネットワーク

最適化ポリシーを適用するホスト（複数可）の IP アドレス。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを指定できます。ASA FirePOWER モジュールでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-4 ページ）を参照してください。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

また、ターゲットベース ポリシーがトラフィックを処理するようにするには、識別するネットワークがターゲットベース ポリシーを設定するネットワーク分析ポリシーによって処理されるネットワーク、およびゾーンに一致するかまたはサブセットになっている必要があることにも注意してください。詳細については、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（17-3 ページ）を参照してください。

ポリシー

モニタ対象ネットワーク セグメント上のホスト一式に使用する最適化ポリシー。7 つのポリシー（BSD、BSD-Right、First、Linux、Last、Solaris、Windows）の中から選択できます。これらのポリシーの詳細については、ターゲットベースの最適化ポリシー（21-13 ページ）を参照してください。

タイムアウト（**Timeout**）

プリプロセッサ エンジンがフラグメント化されたパケットを再構成する際に使用できる最大時間（秒数）を指定します。指定された時間内にパケットを再構成できない場合、プリプロセッサ エンジンはパケットの再構成試行を停止し、受信したフラグメントを破棄します。

最小 **TTL**（**Minimum TTL**）

パケットに許容される最小 TTL 値を指定します。このオプションは、TTL ベースの挿入攻撃を検出します。

このオプションのイベントを生成するには、ルール 123:1 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

異常検知（**Detect Anomalies**）

オーバーラップ フラグメントのようなフラグメンテーション問題を識別します。

以下のルールを有効にすることで、このオプションに対するイベントを生成できます。

- 123:1 ～ 123:4
- 123:5（BSD ポリシー）
- 123:6 ～ 123:8

オーバーラップ範囲（**Overlap Limit**）

セッションで最適化を停止する条件とする、セッションでのオーバーラップ セグメントの検出数を 0（無制限）～ 255 の範囲で指定します。このオプションを設定するには、[異常検知（Detect Anomalies）] を有効にする必要があります。値が空白の場合、このオプションは無効になります。

このオプションのイベントを生成するには、ルール 123:12 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

最小フラグメント サイズ（**Minimum Fragment Size**）

パケットを不正と見なす条件とする、検出されたフラグメント（最後のフラグメントを除く）の最小サイズを 0（無制限）～ 255 バイトの間で指定します。このオプションを設定するには、[異常検知（Detect Anomalies）] を有効にする必要があります。値が空白の場合、このオプションは無効になります。

このオプションのイベントを生成するには、ルール 123:13 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

IP 最適化の設定

ライセンス：Protection

IP 最適化プリプロセッサを設定するには、次の手順を実行します。IP 最適化プリプロセッサの設定オプションの詳細については、最適化オプションの選択（21-14 ページ）を参照してください。

IP 最適化の設定方法：

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（  ）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシーの編集（Edit Policy）] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ 8　[トランスポートまたはネットワーク レイヤー プロセッサ（Transport/Network Layer Preprocessors）] で [IP 最適化（IP Defragmentation）] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[IP 最適化（IP Defragmentation）] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 9　必要に応じて、[グローバル設定（Global Settings）] ページ領域にある [事前に割り当てられたフラグメント（Preallocated Fragments）] の設定を変更できます。

ステップ 10　次の 2 つの対処法があります。

- 新しいターゲットベースのポリシーを追加します。ページの左側で [サーバ（Servers）] の横にある追加アイコン（  ）をクリックします。[ターゲットの追加（Add Target）] ポップアップ ウィンドウが表示されます。[ホスト アドレス（Host Address）] フィールドに 1 つまたは複数の IP アドレスを指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のターゲットベースのポリシーを作成できます。ASA FirePOWER モジュールで IP アドレス ブロックを使用する方法については、IP アドレスの表記規則（1-4 ページ）を参照してください。

  ターゲットベース ポリシーがトラフィックを処理するようにするには、識別するネットワークがターゲットベース ポリシーを設定するネットワーク分析ポリシーによって処理されるネットワーク、およびゾーンに一致するかまたはサブセットになっている必要があることに注意してください。詳細については、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（17-3 ページ）を参照してください。

  ページの左側にあるターゲットのリストに新しいエントリが表示されます。このエントリは、強調表示によって選択された状態であることが示されます。また、[設定（Configuration）] セクションが更新されて、追加したポリシーの現在の構成が反映されます。

- 既存のターゲットベースのポリシーの設定を変更します。ページの左側の [ホスト（Hosts）] に追加されているポリシーの設定済みアドレスをクリックするか、[デフォルト（default）] をクリックします。

選択したエントリが強調表示され、[設定（Configuration）] セクションが更新されて、選択したポリシーの現在の設定が表示されます。既存のターゲットベースのポリシーを削除するには、削除するポリシーの横にある削除アイコン（ ）をクリックします。

ステップ 11　オプションで、[設定（Configuration）] ページ領域にあるオプションのいずれかを変更できます。

ステップ 12　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

パケットのデコードについて

ライセンス：Protection

キャプチャしたパケットをプリプロセッサに送信する前に、システムはパケットをパケット デコーダに送信します。パケット デコーダは、プリプロセッサやルール エンジンが容易に使用できる形式に、パケット ヘッダーおよびペイロードを変換します。データリンク層から開始して、ネットワーク層、トランスポート層へと、各スタック層が順にデコードされます。

注意すべき点として、パケット デコーダのルールにイベントを生成させるには、これらのルール（ジェネレータ ID（GID）が 116 のルール）を有効にする必要があります。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

GTP データ チャネルのデコード（**Decode GTP Data Channel**）

カプセル化された GTP（General Packet Radio Service（GPRS）トンネリング プロトコル）データ チャネルをデコードします。デフォルトでは、デコーダはポート 3386 ではバージョン 0 のデータをデコードし、ポート 2152 ではバージョン 1 のデータをデコードします。`GTP_PORTS` デフォルト変数を使用して、カプセル化された GTP トラフィックを識別するポートを変更できます。詳細については、定義済みのデフォルトの変数の最適化（2-16 ページ）を参照してください。

このオプションのイベントを生成するには、ルール 116:297 および 116:298 を有効にします。

非標準ポートでの **Teredo** の検出（**Detect Teredo on Non-Standard Ports**）

ポート 3544 以外の UDP ポートで識別される IPv6 トラフィックの Teredo トンネリングを検査します。

IPv6 トラフィックが存在する場合、システムは常にこのトラフィックを検査します。デフォルトでは、IPv6 インスペクションには 4in6、6in4、6to4、および 6in6 トンネリング方式が含まれます。また、UDP ヘッダーがポート 3544 を指定している場合は、Teredo トンネリングも含まれます。

IPv4 ネットワークでは、IPv4 ホストが Teredo プロトコルを使用して、IPv4 ネットワーク アドレス変換（NAT）デバイスを介して IPv6 トラフィックをトンネリングできます。Teredo は、IPv6 パケットを IPv4 UDP データグラムにカプセル化して、IPv4 NAT デバイスの背後で IPv6 接続を許可します。システムは通常、UDP ポート 3544 を使用して Teredo トラフィックを識別します。ただし、攻撃者が検出を免れるために標準以外のポートを使用する可能性も考えられます。[非標準ポートでの Teredo の検出（Detect Teredo on Non-Standard Ports）] を有効にすることで、システムに Teredo トンネリングのすべての UDP ペイロードを検査させることができます。

Teredo のデコードは、外側のネットワーク層に IPv4 が使用されている場合に限り、最初の UDP ヘッダーに対してのみ行われます。UDP データが IPv6 データにカプセル化されるため、Teredo IPv6 層の後に 2 つ目の UDP 層が存在する場合、ルール エンジンは UDP 侵入ルールを使用して、内側および外側の両方の UDP 層を分析します。

policy-other ルール カテゴリの侵入ルール 12065、12066、12067、および 12068 は Teredo トラフィックを検出しますが、デコードは行わないので注意してください。(任意) これらのルールを使用してインライン展開で Teredo トラフィックをドロップすることができます。ただし、[非標準ポートでの Teredo の検出 (Detect Teredo on Non-Standard Ports)] を有効にする場合は、これらのルールを無効化するか、トラフィックをドロップせずにイベントを生成するように設定する必要があります。詳細については、「侵入ポリシー内のルールのフィルタリング (24-10 ページ)」と「ルール状態の設定 (24-21 ページ)」を参照してください。

過剰な長さの値の検出 (**Detect Excessive Length Value**)

パケット ヘッダーが実際のパケット長を超えるパケット長を指定しているかどうかを検出します。

このオプションのイベントを生成するには、ルール 116:6、116:47、116:97、および 116:275 を有効にします。

無効な **IP** オプションの検出 (**Detect Invalid IP Options**)

無効な IP オプションを使用したエクスプロイトを識別するために、無効な IP ヘッダー オプションを検出します。たとえば、ファイアウォールに対するサービス妨害攻撃は、システムをフリーズさせる原因になります。ファイアウォールが無効なタイムスタンプおよび IP セキュリティ オプションを解析しようとして、ゼロ長のチェックに失敗すると、回復不可能な無限ループが発生します。ルール エンジンはゼロ長のオプションを識別し、ファイアウォールでの攻撃を軽減するために使用できる情報を提供します。

このオプションのイベントを生成するには、ルール 116:4 および 116:5 を有効にします。詳細については、ルール状態の設定 (24-21 ページ) を参照してください。

試験的な **TCP** オプションの検出 (**Detect Experimental TCP Options**)

試験的な TCP オプションが設定された TCP ヘッダーを検出します。以下の表は、それらのオプションを示しています。

TCP オプション	説明
9	半順序接続許可 (Partial Order Connection Permitted)
10	半順序サービス プロファイル (Partial Order Service Profile)
18	Alternate Checksum Request
15	Alternate Checksum Data
18	Trailer Checksum
20	Space Communications Protocol Standards (SCPS)
21	Selective Negative Acknowledgements (SCPS)
22	Record Boundaries (SCPS)
23	Corruption (SPCS)
24	SNAP
26	TCP 圧縮フィルタ (TCP Compression Filter)

これらのオプションは試験的なものであるため、一部のシステムでは考慮されず、悪用される恐れがあります。

（注）　上記の表に記載されている試験的オプションに加えて、26 より大きいオプション番号を持つ TCP オプションは、試験的オプションと見なされます。

このオプションのイベントを生成するには、ルール 116:58 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

廃止された **TCP** オプションの検出（**Detect Obsolete TCP Options**）

廃止された TCP オプションが設定された TCP ヘッダーを検出します。これらのオプションは廃止されたものであるため、一部のシステムでは考慮されず、悪用される恐れがあります。以下の表は、それらのオプションを示しています。

TCP オプション	説明
6	エコー（Echo）
7	エコー応答（Echo Reply）
16	Skeeter
17	Bubba
19	MD5 Signature（MD5 認証）
25	Unassigned（未定義）

このオプションのイベントを生成するには、ルール 116:57 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

T/TCP の検出（**Detect T/TCP**）

CC.ECHO オプションが設定された TCP ヘッダーを検出します。CC.ECHO オプションは、TCP for Transactions（T/TCP）が使用されていることを確認します。T/TCP ヘッダー オプションは幅広く使用されていないため、一部のシステムでは考慮されず、悪用される恐れがあります。

このオプションのイベントを生成するには、ルール 116:56 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

その他の **TCP** オプションの検出（**Detect Other TCP Options**）

他の TCP デコード イベント オプションでは検出されない無効な TCP オプションが設定された TCP ヘッダーを検出します。たとえば、このオプションは、無効な長さ、またはオプション データが TCP ヘッダーに収まらない長さの TCP オプションを検出します。

このオプションのイベントを生成するには、ルール 116:54、116:55、および 116:59 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

プロトコル ヘッダー異常の検出（**Detect Protocol Header Anomalies**）

より具体的な IP および TCP デコーダ オプションでは検出されない他のデコード エラーを検出します。たとえば、このデコーダは、不正な形式のデータリンク プロトコル ヘッダーを検出する場合があります。

このオプションに対するイベントを生成するには、他のパケット デコーダ オプションに明示的に関連付けられていないパケット デコーダのルールを有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

異常な IPv6 トラフィックによってトリガーされるイベントを生成するルールは、116:270 ～ 116:274、116:275 ～ 116:283、116:291、116:292、116:295、116:296、116:406、116:458、116:460、116:461 です。

インライン正規化プリプロセッサの [最小 TTL（Minimum TTL）] オプションに関連する以下のルールについても注意してください。

- 指定の最小値を下回る TTL が設定された IPv4 パケットが検出された場合にイベントを生成するには、ルール 116:428 を有効にします。
- 指定の最小値を下回るホップ リミットが設定された IPv6 パケットが検出された場合にイベントを生成するには、ルール 116:270 を有効にします。

詳細については、インライン トラフィックの正規化（21-6 ページ）のインライン正規化の [最小 TTL（Minimum TTL）] オプションを参照してください。

パケットのデコードの設定

ライセンス：Protection

パケットのデコードは、[パケット デコーディング（Packet Decoding）] 設定ページで設定できます。パケットのデコード設定オプションの詳細については、パケットのデコードについて（21-17 ページ）を参照してください。

パケットのデコードの設定方法：

ステップ 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシーの編集（Edit Policy）] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定(Settings)] をクリックします。

[設定(Settings)] ページが表示されます。

ステップ 8　[トランスポートまたはネットワーク レイヤー プロセッサ(Transport/Network Layer Preprocessors)] で [パケット デコーディング(Packet Decoding)] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[パケット デコーディング(Packet Decoding)] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー階層を示します。詳細については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

ステップ 9　[パケット デコーディング(Packet Decoding)] ページの任意の検出オプションを有効または無効にできます。詳細については、パケットのデコードについて(21-17 ページ)を参照してください。

ステップ 10　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

TCP ストリームの前処理の使用

ライセンス:Protection

TCP プロトコルは、接続で生じ得るさまざまな状態を定義します。各 TCP 接続は、送信元と宛先の IP アドレス、および送信元と宛先のポートによって識別されます。TCP では、接続パラメータ値が同じ接続は、一度に 1 つしか存在できません。

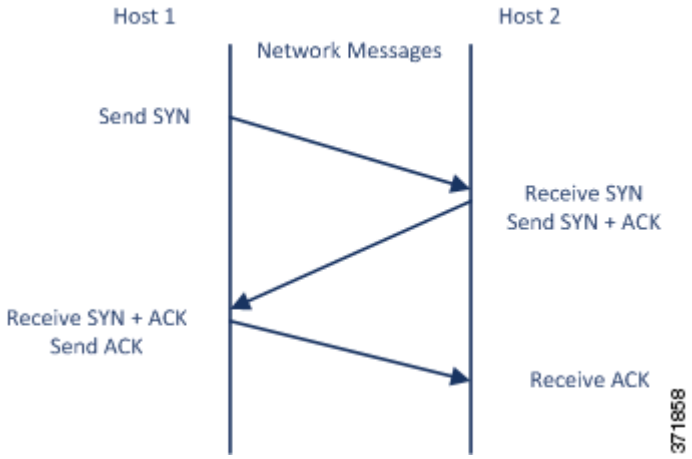
TCP ストリーム プリプロセッサのルールにイベントを生成させるには、それらのルール(ジェネレータ ID(GID)が 129 のルール)を有効にする必要があります。詳細については、ルール状態の設定(24-21 ページ)を参照してください。

詳細については、次の各項を参照してください。

状態関連の TCP エクスプロイトについて

ライセンス：Protection

侵入ルールに `established` 引数と組み合わせた `flow` キーワードを追加すると、侵入ルール エンジンはステートフル モードでルールとフロー ディレクティブに一致するパケットを検査します。ステートフル モードでは、クライアントとサーバの間で正当な 3 ウェイ ハンドシェイクによって確立された TCP セッションの一部であるトラフィックだけが評価されます。以下の図に、3 ウェイ ハンドシェイクを示します。



確立された TCP セッションの一部として識別できない TCP トラフィックをプリプロセッサが検出するようにシステムを設定することは可能です。しかし、このようなイベントは、システムをすぐに過負荷状態に陥らせ、しかも意味のあるデータを提供しないため、通常の使用法では推奨されません。

Stick や Snot などの攻撃では、システムの自身に対する広範なルール セットとパケット インスペクションを悪用します。これらのツールは、Snort ベースの侵入ルールのパターンに基づいてパケットを生成し、ネットワークに送信します。ステートフル インスペクションに対して設定するルールに `flow` または `flowbits` キーワードを含めなければ、パケットのそれぞれがルールをトリガーするため、システムが過負荷状態になります。ステートフル インスペクションを使用することで、確立された TCP セッションに含まれず、意味のある情報を提供しないこれらのパケットを無視できます。ステートフル インスペクションを実行すると、ルール エンジンは確立された TCP セッションに含まれる攻撃のみを検出するため、アナリストが stick や snot によって大量に生成されるイベントに時間を取られることがなくなります。

TCP グローバル オプションの選択

ライセンス：Protection

TCP ストリーム プリプロセッサには、TCP ストリーム プリプロセッサの動作を制御するグローバル オプションが 1 つあります。

プリプロセッサ ルールは、このオプションに関連付けられていません。

パケット タイプ パフォーマンスの向上（**Packet Type Performance Boost**）

送信元ポートおよび宛先ポートの両方を `any` に設定した TCP ルールで、`flow` または `flowbits` オプションが使用されている場合を除き、有効化された侵入ルールに指定されていないポートおよびアプリケーション プロトコルのすべてについて、TCP トラフィックを無視するように設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。

ターゲットベースの TCP ポリシーについて

ライセンス：Protection

オペレーティング システムによって、TCP の実装方法は異なります。たとえば、セッションをリセットするために、Windows やその他のオペレーティング システムの一部では TCP リセット セグメントに正確な TCP シーケンス番号を割り当てる必要があるのに対し、Linux や他のオペレーティング システムではシーケンス番号の範囲を使用できます。この例の場合、ストリーム プリプロセッサは、シーケンス番号に基づき、宛先ホストがリセットにどのように応答するかを正確に把握しなければなりません。ストリーム プリプロセッサがセッションの追跡を停止するのは、宛先ホストがリセットが有効であると見なした場合のみです。したがって、プリプロセッサがストリームの検査を停止した後は、パケットを送信することによって攻撃が検出を免れることはできません。TCP の実装方法の違いには、オペレーティング システムで TCP タイムスタンプ オプションを採用しているかどうか、採用している場合にはどのようにタイムスタンプを処理するか、そしてオペレーティング システムで SYN パケットのデータを受け入れるか、無視するかどうかも含まれます。

また、オーバーラップ TCP セグメントを再構成する方法も、オペレーティング システムによって異なります。オーバーラップ TCP セグメントは、確認応答済み TCP トラフィックの通常の再送信を反映する場合があります。あるいは、ホストのオペレーティング システムを認識している攻撃者が、エクスプロイトの検出を免れるためにオーバーラップ セグメントに不正なコンテンツを忍ばせて送信し、そのホストを悪用しようとしている場合もあります。ただし、モニタ対象のネットワーク セグメント上で稼働するオペレーティング システムを認識するようにストリーム プリプロセッサを設定すれば、そのプリプロセッサがターゲット ホストと同じ方法でセグメントを再構成することによって、攻撃を識別できます。

モニタ対象のネットワーク セグメント上のさまざまなオペレーティング システムに合わせて TCP ストリーム インスペクションおよび再構成を調整するために、1 つ以上の TCP ポリシーを作成することができます。ポリシーごとに、13 のオペレーティング システム ポリシーのうちの 1 つを特定します。異なるオペレーティング システムを使用するホストのいずれか、あるいはすべてを識別するために必要な数だけ TCP ポリシーを使用し、各 TCP ポリシーを特定の IP アドレスまたはアドレス ブロックにバインドします。デフォルトの TCP ポリシーは、他の TCP ポリシーで指定されていないモニタ対象ネットワーク上のすべてのホストに適用されます。したがって、デフォルトの TCP ポリシーに IP アドレス、CIDR ブロック、またはプレフィックス長を指定する必要はありません。

適応型プロファイルを使用することで、パケットのターゲット ホストのホスト オペレーティング システム情報に応じて、TCP ストリーム プリプロセッサに適用するターゲットベースのポリシーが動的に選択されるようにすることができます。詳細については、パッシブ展開における前処理の調整（22-1 ページ）を参照してください。

以下の表に、オペレーティング システム ポリシーとそれを使用するホスト オペレーティング システムをリストします。

表 *21-2*　*TCP* オペレーティング システム ポリシー

ポリシー	オペレーティング システム
ファースト	不明な OS
Last	Cisco IOS
BSD	AIX FreeBSD OpenBSD
Linux	Linux 2.4 カーネル Linux 2.6 カーネル

表 21-2　TCP オペレーティング システム ポリシー（続き）

ポリシー	オペレーティング システム
Old Linux	Linux 2.2 以前のカーネル
Windows	Windows 98
	Windows NT
	Windows 2000
	Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista
Solaris	Solaris OS
	SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 以降
HPUX 10	HP-UX 10.2 以前
Mac OS	Mac OS 10（Mac OS X）

ヒント　First オペレーティング システム ポリシーは、ホストのオペレーティング システムが不明な場合にはある程度の保護対策になります。ただし、攻撃を見逃す可能性もあります。オペレーティング システムが既知であれば、ポリシーを編集して、その正しいオペレーティング システムを指定してください。

TCP ポリシーのオプションの選択

ライセンス：Protection

以下に、ストリーム プリプロセッサの検査対象とする TCP トラフィックを識別して制御するために設定できるオプションをリストし、説明します。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ネットワーク（**Network**）

TCP ストリーム再構成ポリシーを適用するホストの IP アドレスを指定します。

単一の IP アドレスまたはアドレス ブロックを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを指定できます。ASA FirePOWER モジュールでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-4 ページ）を参照してください。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

また、ターゲットベース ポリシーがトラフィックを処理するようにするには、識別するネットワークがターゲットベース ポリシーを設定するネットワーク分析ポリシーによって処理されるネットワーク、およびゾーンに一致するかまたはサブセットになっている必要があることにも注意してください。詳細については、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（17-3 ページ）を参照してください。

ポリシー（**Policy**）

TCP ポリシーを適用するターゲット ホスト（複数可）のオペレーティング システムを識別します。[Mac OS] 以外のポリシーを選択すると、システムは同期（SYN）パケットからデータを削除し、ルール 129:2 に対するイベントの生成を無効にします。

詳細については、ターゲットベースの TCP ポリシーについて（21-23 ページ）を参照してください。

タイムアウト（**Timeout**）

侵入ルール エンジンが非アクティブなストリームを状態テーブルで保持する秒数（1 ～ 86400 秒）。指定された期間内にストリームが再構成されない場合、侵入ルール エンジンはそのストリームを状態テーブルから削除します。

（注）　ネットワーク トラフィックがデバイスの帯域幅制限に到達しやすいセグメントにデバイスが展開されている場合は、処理のオーバーヘッド量を削減するために、この値を大きい値（たとえば、600 秒）に設定することを検討する必要があります。

最大 **TCP** ウィンドウ（**Maximum TCP Window**）

受信側ホストで指定されている TCP ウィンドウの最大許容サイズを 1 ～ 1073725440 バイトの範囲で指定します。値を 0 に設定すると、TCP ウィンドウ サイズのチェックが無効になります。

注意　上限は RFC で許可される最大ウィンドウ サイズです。これは、攻撃者が検出を回避できないようにすることを目的としていますが、あまりにも大きな最大ウィンドウ サイズを設定すると、システム自体がサービス妨害を招く可能性があります。

このオプションのイベントを生成するには、ルール 129:6 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

オーバーラップ範囲（**Overlap Limit**）

セッションで許容するオーバーラップ セグメントの数を 0（無制限）～ 255 の範囲で指定します。セッションで、この指定された値に達すると、セグメントの再構成が停止します。[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされていて、それに付随するプリプロセッサ ルールが有効にされている場合、イベントも生成されます。

このオプションのイベントを生成するには、ルール 129:7 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

フラッシュ ファクタ（**Flush Factor**）

インライン展開では、ここで設定するサイズ減少なしのセグメントの数（1 ～ 2048）の後にサイズが減少したセグメントが検出されると、システムは検出用に累積されたセグメント データをフラッシュします。値を 0 に設定すると、要求または応答の終わりを示す可能性のあるこのセグメント パターンの検出が無効になります。このオプションを有効にするには、インライン正規化の [TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にする必要があることに注意してください。詳細については、インライン トラフィックの正規化（21-6 ページ）を参照してください。

ステートフル インスペクションの異常（**Stateful Inspection Anomalies**）

TCP スタックの異常な動作を検出します。付随するプリプロセッサ ルールが有効にされている場合、TCP/IP スタックが不完全に作成されていると、多数のイベントが生成される可能性があります。

以下のルールを有効にすることで、このオプションに対するイベントを生成できます。

- 129:1 ～ 129:5
- 129:6（Mac OS のみ）
- 129:8 ～ 129:11
- 129:13 ～ 129:19

詳細については、ルール状態の設定（24-21 ページ）を参照してください。

TCP セッションのハイジャック（**TCP Session Hijacking**）

3 ウェイ ハンドシェイク中に TCP 接続の両端から検出されたハードウェア（MAC）アドレスの有効性を、セッションで受信した後続のパケットに照合して検査することにより、TCP セッション ハイジャックを検出します。[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされていて、2 つの対応するプリプロセッサ ルールのいずれかが有効にされている場合、接続のどちらかの側の MAC アドレスが一致しないと、システムがイベントを生成します。

このオプションのイベントを生成するには、ルール 129:9 および 129:10 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

連続する小さなセグメント（**Consecutive Small Segments**）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされている場合、連続する小さな TCP セグメントの許容数を 1 ～ 2048 の範囲で指定します。値を 0 に設定すると、連続する小さなセグメントのチェックが無効になります。

このオプションは、[小さなセグメント サイズ（Small Segment Size）] オプションと同時に設定し、両方とも無効にするか、両方にゼロ以外の値を設定する必要があります。通常は、それぞれのセグメントの長さが 1 バイトであったとしても、ACK が介在することなく 2000 個もの連続するセグメントを受信することはないので注意してください。

このオプションのイベントを生成するには、ルール 129:12 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

小さなセグメント サイズ（**Small Segment Size**）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされている場合、小さいと見なされる TCP セグメントのサイズを 1 ～ 2048 バイトの範囲で指定します。値を 0 に設定すると、小さいセグメントのサイズの指定が無効になります。

このオプションは、[連続する小さなセグメント（Consecutive Small Segments）] オプションと同時に設定し、両方とも無効にするか、両方にゼロ以外の値を設定する必要があります。2048 バイトの TCP セグメントは、標準的な 1500 バイトのイーサネット フレームより大きいことに注意してください。

小さなセグメントを無視するポート（**Ports Ignoring Small Segments**）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）]、[連続する小さなセグメント（Consecutive Small Segments）]、および [小さなセグメント サイズ（Small Segment Size）] が有効にされている場合、必要に応じて、小さい TCP セグメントの検出を無視する 1 つ以上のポートのカンマ区切りリストを指定します。このオプションを空白のままにすると、ポートはすべて無視されないように指定されます。

リストには任意のポートを追加できますが、このリストが適用されるのは、TCP ポリシーの [ストリーム再構成を実行（Perform Stream Reassembly on）] ポート リストに指定されているポートのみです。

TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）

TCP スリーウェイ ハンドシェイクの完了時に確立されたセッションだけを処理することを指定します。パフォーマンスを向上させ、SYN フラッド攻撃から保護し、部分的に非同期の環境での運用を可能にするには、このオプションを無効にします。確立された TCP セッションには含まれていない情報を送信して誤検出を発生させようとする攻撃を回避するには、このオプションを有効にします。

このオプションのイベントを生成するには、ルール 129:20 を有効にします。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

3 ウェイ ハンドシェイク タイムアウト（3-Way Handshake Timeout）

[TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）] が有効にされている場合、ハンドシェイクを完了するまでの時間制限を 0（無制限）～ 86400 秒（24 時間）の範囲で指定します。このオプションの値を変更するには、[TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）] を有効にする必要があります。

パケット サイズ パフォーマンスの向上（**Packet Size Performance Boost**）

再構成バッファで大きいパケットをキューに入れないようにプリプロセッサを設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。1 ～ 20 バイトの小さなパケットを使用した検出回避の試行から保護するには、このオプションを無効にします。すべてのトラフィックが非常に大きなパケットからなるため、そのような攻撃は起こらないと確信できる場合は、このオプションを有効にします。

レガシー再構成（**Legacy Reassembly**）

パケットを再構成する際に、廃止されたストリーム 4 プリプロセッサをエミュレートするようにストリーム プリプロセッサを設定します。これにより、ストリーム プリプロセッサで再構成されたイベントを、ストリーム 4 プリプロセッサで再構成された、同じデータ ストリームに基づくイベントと比較できます。

非同期ネットワーク（**Asynchronous Network**）

モニタ対象ネットワークが非同期ネットワーク（システムにトラフィックの半分だけが見えるネットワーク）であるかどうかを指定します。このオプションを有効にすると、システムは TCP ストリームを再構成しないため、パフォーマンスが向上します。

クライアント ポート、サーバ ポート、両ポートでのストリーム再構成の実行（**Perform Stream Reassembly on Client Ports, Server Ports, Both Ports**）

ストリーム プリプロセッサの再構成対象とするトラフィックを識別するクライアント ポート、サーバ ポート、またはその両方のカンマ区切りリストを指定します。ストリーム再構成のオプションの選択（21-28 ページ）を参照してください。

クライアント サービス、サーバ サービス、両サービスでのストリーム再構成の実行（**Perform Stream Reassembly on Client Services, Server Services, Both Services**

ストリーム プリプロセッサの再構成対象とするトラフィックで識別するクライアント サービス、サーバ サービス、またはその両方のサービスを指定します。ストリーム再構成のオプションの選択（21-28 ページ）を参照してください。

トラブルシューティング オプション：最大キューイング バイト（**Troubleshooting Options: Maximum Queued Bytes**）

トラブルシューティングの電話中に、TCP 接続の片側でキューイングできるデータの量を指定するようにサポートから依頼される場合があります。値 0 は、無制限のバイト数を指定します。

注意　このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

トラブルシューティング オプション：最大キューイング セグメント（**Troubleshooting Options**：**Maximum Queued Segments**）

トラブルシューティングの電話中に、TCP 接続の片側でキューイングできるデータ セグメントの最大バイト数を指定するようにサポートから依頼される場合があります。値 0 は、無制限のデータ セグメント バイト数を指定します。

注意　このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

TCP ストリームの再構成

ライセンス：Protection

ストリーム プリプロセッサは、TCP セッションでのサーバからクライアントへの通信ストリーム、クライアントからサーバへの通信ストリーム、またはその両方の通信ストリームに含まれるすべてのパケットを収集して再構成します。これにより、ルール エンジンは、特定のストリームに含まれる個々のパケットだけを検査するのではなく、ストリームを再構成された単一のエンティティとして検査できます。

詳細については、次の各項を参照してください。

- ストリームベースの攻撃について（21-28 ページ）
- ストリーム再構成のオプションの選択（21-28 ページ）

ストリームベースの攻撃について

ライセンス：Protection

ストリーム再構成により、ルール エンジンは、個々のパケットを検査する場合には検出できない可能性のあるストリームベースの攻撃を識別できます。ルール エンジンの再構成対象とする通信ストリームは、ネットワークのニーズに応じて指定できます。たとえば、Web サーバ上のトラフィックをモニタする際に、独自の Web サーバから不正なトラフィックを受信する可能性がほとんどないため、クライアント トラフィックだけを検査するという場合もあります。

ストリーム再構成のオプションの選択

ライセンス：Protection

各 TCP ポリシーに、ストリーム プリプロセッサが再構成するトラフィックを識別するポートのカンマ区切りのリストを指定できます。適応型プロファイルが有効にされている場合、再構成するトラフィックを識別するサービスを、ポートの代わりとして、あるいはポートと組み合わせてリストすることもできます。適応型プロファイルを有効にして使用する方法については、パッシブ展開における前処理の調整（22-1 ページ）を参照してください。

ポート、サービス、またはその両方を指定できます。クライアント ポート、サーバ ポート、またはその両方を任意に組み合わせた個別のポート リストを指定できます。また、クライアント サービス、サーバ サービス、またはその両方を任意に組み合わせた個別のサービス リストを指定することもできます。たとえば、以下を再構成する必要があるとします。

- クライアントからの SMTP（ポート 25）トラフィック
- FTP サーバ応答（ポート 21）
- 両方向の Telnet（ポート 23）トラフィック

この場合、以下のように設定できます。

- クライアント ポートとして、23, 25 を指定
- サーバ ポートとして、21, 23 を指定

あるいは、以下のように設定することもできます。

- クライアント ポートとして、25 を指定
- サーバ ポートとして、21 を指定
- 両方のポートとして、23 を指定

さらに、ポートとサービスを組み合わせた以下の設定例は、適応型プロファイルが有効にされている場合、有効になります。

- クライアント ポートとして、23 を指定
- クライアント サービスとして、smtp を指定
- サーバ ポートとして、21 を指定
- サーバ サービスとして、telnet を指定

all を引数として指定して、すべてのポートに対して再構成を指定することもできますが、シスコではポートを all に設定しないよう推奨しています。この設定では、このプリプロセッサで検査するトラフィックの量が増え、不必要にパフォーマンスが低下するためです。

TCP 再構成には、自動的かつ透過的にその他のプリプロセッサに追加するポートが含まれています。しかし、他のプリプロセッサの設定に追加した TCP 再構成リストにポートを明示的に追加する場合は、これらの追加したポートは通常処理されます。これには、次のプリプロセッサのポート リストが含まれています。

- FTP/Telnet（サーバ レベル FTP）
- DCE/RPC
- HTTP Inspect
- SMTP
- Session Initiation Protocol
- POP
- IMAP
- SSL

ポートを無効にする（たとえば !77）と、TCP ストリーム プリプロセッサがそのポートのトラフィックを処理しなくなるのでパフォーマンスを向上できます。

追加のトラフィック タイプ（クライアント、サーバ、両方）を再構成すると、リソースの需要が増大することに注意してください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

クライアント ポートでのストリーム再構成の実行（**Perform Stream Reassembly on Client Ports**）

接続のクライアント側のポートに基づくストリームの再構成を有効にします。つまり、Web サーバ、メール サーバ、または一般に $HOME_NET で指定された IP アドレスによって定義されたその他の IP アドレスを宛先とするストリームが再構成されます。不正なトラフィックがクライアントから発生する可能性がある場合は、このオプションを使用します。

クライアント サービスでのストリーム最高性の実行（**Perform Stream Reassembly on Client Services**）

接続のクライアント側のサービスに基づくストリーム再構成を有効にします。不正なトラフィックがクライアントから発生する可能性がある場合は、このオプションを使用します。

この機能には、Protection および Control ライセンスが必要です。

サーバ ポートでのストリーム再構成の実行（**Perform Stream Reassembly on Server Ports**）

接続のサーバ側のポートに基づくストリーム再構成のみを有効にします。つまり、Web サーバ、メール サーバ、または一般に $EXTERNAL_NET で指定された IP アドレスによって定義されたその他の IP アドレスから発信されたストリームが再構成されます。サーバ側の攻撃を監視する必要がある場合は、このオプションを使用します。ポートを指定しないことによって、このオプションを無効にできます。

サーバ サービスでのストリーム再構成の実行（**Perform Stream Reassembly on Server Services**）

接続のサーバ側のサービスに基づくストリーム再構成のみを有効にします。サーバ側の攻撃を監視する必要がある場合は、このオプションを使用します。サービスを指定しないことによって、このオプションを無効にできます。

この機能には、Protection および Control ライセンスが必要です。

両方のポートでのストリーム再構成の実行（**Perform Stream Reassembly on Both Ports**）

接続のクライアント側とサーバ側の両方のポートに基づくストリーム再構成を有効にします。同じポートで、不正なトラフィックがクライアントとサーバ間のいずれの方向でも移動する可能性がある場合は、このオプションを使用します。ポートを指定しないことによって、このオプションを無効にできます。

両方のサービスでのストリーム再構成の実行（**Perform Stream Reassembly on Both Services**）

接続のクライアント側とサーバ側の両方のサービスに基づくストリーム再構成を有効にします。同じサービスで、不正なトラフィックがクライアントとサーバ間のいずれの方向でも移動する可能性がある場合は、このオプションを使用します。サービスを指定しないことによって、このオプションを無効にできます。

この機能には、Protection および Control ライセンスが必要です。

TCP ストリームの前処理の設定

ライセンス：Protection

TCP ポリシーを含め、TCP ストリームの前処理を設定できます。TCP ストリーム プリプロセッサの設定オプションの詳細については、TCP ポリシーのオプションの選択（21-24 ページ）を参照してください。

TCP セッションを追跡するストリーム プリプロセッサを設定する方法：

ステップ **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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定(Advanced)] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] の横にある編集アイコン( )をクリックします。

[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] をクリックします。

[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシーの編集(Edit Policy)] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定(Settings)] をクリックします。

[設定(Settings)] ページが表示されます。

ステップ 8　[トランスポートまたはネットワーク レイヤー プロセッサ(Transport/Network Layer Preprocessors)] で [TCP ストリームの構成(TCP Stream Configuration)] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[TCP ストリームの構成(TCP Stream Configuration)] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(16-1 ページ)を参照してください。

ステップ 9　必要に応じて、[グローバル設定(Global Settings)] の下にある [パケット タイプ パフォーマンスの向上(Packet Type Performance Boost)] を変更します。詳細については、TCP グローバル オプションの選択(21-22 ページ)を参照してください。

ステップ 10　次の 2 つの対処法があります。

- 新しいターゲットベースのポリシーを追加します。ページの左側の [ホスト(Hosts)] の横にある追加アイコン( )をクリックします。[ターゲットの追加(Add Target)] ポップアップ ウィンドウが表示されます。[ホスト アドレス(Host Address)] フィールドに 1 つまたは複数の IP アドレスを指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロックを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のターゲットベースのポリシーを作成できます。ASA FirePOWER モジュールで IP アドレス ブロックを使用する方法については、IP アドレスの表記規則(1-4 ページ)を参照してください。

  ターゲットベース ポリシーがトラフィックを処理するようにするには、識別するネットワークがターゲットベース ポリシーを設定するネットワーク分析ポリシーによって処理されるネットワーク、およびゾーンに一致するかまたはサブセットになっている必要があることに注意してください。詳細については、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(17-3 ページ)を参照してください。

  ページの左側にあるターゲットのリストに新しいエントリが表示されます。このエントリは、強調表示によって選択された状態であることが示されます。また、[設定(Configuration)] セクションが更新されて、追加したポリシーの現在の構成が反映されます。

- 既存のターゲットベースのポリシーの設定を変更します。ページの左側の [ホスト（Hosts）] に追加されているポリシーの設定済みアドレスをクリックするか、[デフォルト（default）] をクリックします。

  選択したエントリが強調表示され、[設定（Configuration）] セクションが更新されて、選択したポリシーの現在の設定が表示されます。既存のターゲットベースのポリシーを削除するには、削除するポリシーの横にある削除アイコン（ ）をクリックします。

ステップ 11　必要に応じて、[設定（Configuration）] にある任意の TCP ポリシー オプションを変更します。

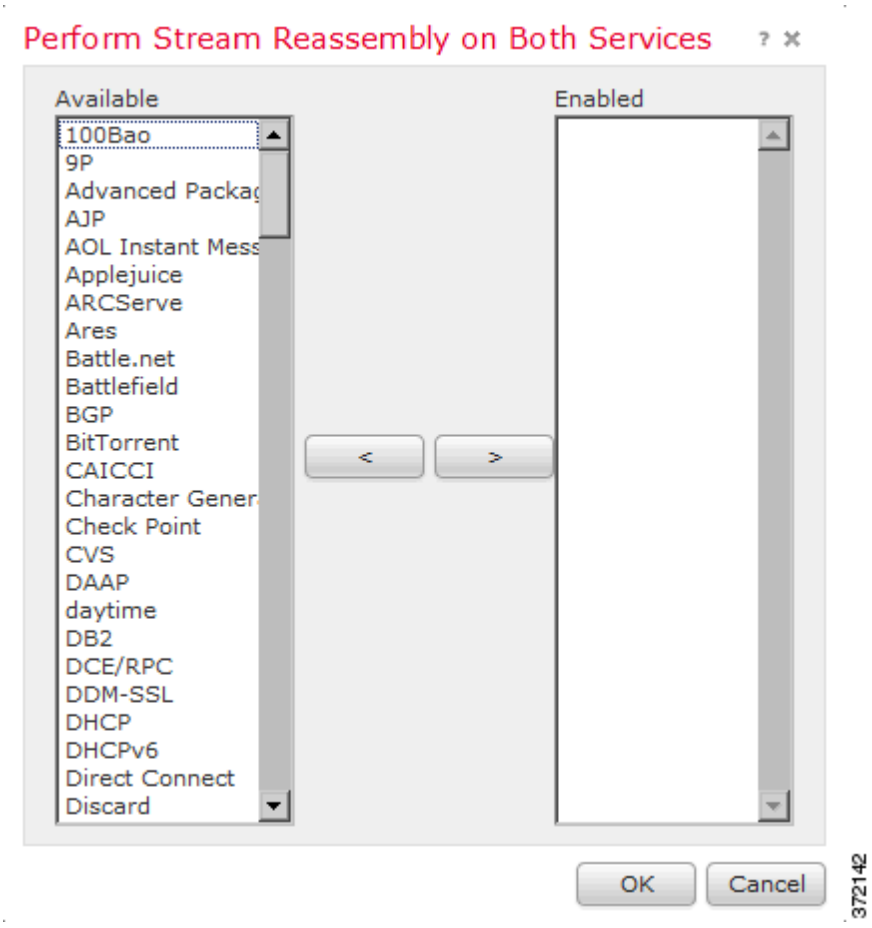
クライアント サービス、サーバ サービス、またはその両方に基づくストリーム再構成の設定を変更するには、ステップ 12 に進みます。そうでない場合は、ステップ 15 に進みます。

詳細については、TCP ポリシーのオプションの選択（21-24 ページ）およびストリーム再構成のオプションの選択（21-28 ページ）を参照してください。

ステップ 12　クライアント サービス、サーバ サービス、またはその両方に基づくストリーム再構成の設定を変更するには、変更するフィールドの内側をクリックするか、そのフィールドの横にある [編集（Edit）] をクリックします。

選択したフィールドのポップアップ ウィンドウが表示されます。

たとえば、次の図は、[両サービスでのストリーム再構成の実行（Perform Stream Reassembly on Both Services）] ポップアップ ウィンドウを示しています。



適応型プロファイルを有効にすることで、ネットワークで検出されたサービスに基づいてストリーム プリプロセッサが再構成するトラフィックをモニタできます。詳細については、パッシブ展開における前処理の調整（22-1 ページ）を参照してください。

ステップ 13　次の 2 つの選択肢があります。

- モニタするサービスを追加するには、左側の [選択可能（Available）] リストで 1 つまたは複数のサービスを選択してから、右矢印（>）ボタンをクリックします。
- サービスを削除するには、右側の [有効（Enabled）] リストで削除するサービスを選択してから、左矢印（<）ボタンをクリックします。

複数のサービス ディテクタを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。また、クリック アンド ドラッグ操作で、複数の隣接するサービス ディテクタを選択することもできます。

ステップ 14　[OK] をクリックして、選択した項目を追加します。

[TCP ストリームの構成（TCP Stream Configuration）] ページが表示され、サービスが更新されます。

ステップ 15　任意で、サポートによって求められた場合にのみ、[トラブルシューティング オプション（Troubleshooting Options）] を展開し、TCP ストリーム前処理ポリシー設定のいずれかを変更します。詳細については、TCP ポリシーのオプションの選択（21-24 ページ）を参照してください。

ステップ 16　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

UDP ストリームの前処理の使用

ライセンス：Protection

UDP ストリームの前処理が行われるのは、ルール エンジンがパケットを処理するために使用する UDP ルールに、以下の引数のいずれかを使用した `flow` キーワード（TCP または UDP クライアントまたはサーバ フローへのルールの適用（27-54 ページ）を参照）が含まれる場合です。

- `Established`
- `To Client`
- `From Client`
- `To Server`
- `From Server`

UDP はコネクションレス型プロトコルであり、2 つのエンドポイントが通信チャネルを確立してデータを交換し、チャネルを終了する手段は提供していません。UDP データ ストリームは一般に、セッションという観点で考慮されません。ただし、ストリーム プリプロセッサは、カプセル化 IP データグラム ヘッダーの送信元および宛先 IP アドレス フィールドと、UDP ヘッダーのポート フィールドを使用して、フローの方向を判断し、セッションを識別します。セッションが終了するのは、設定可能タイマを超過した時点か、または、いずれかのエンドポイントがもう一方のエンドポイントが到達不能であるか要求されたサービスが到達不能であることを通知する ICMP メッセージを受信した時点です。

システムは UDP ストリームの前処理に関連するイベントを生成しないことに注意してください。ただし、関連するパケット デコーダ ルールを有効にすることで、UDP プロトコル ヘッダーの異常を検出することができます。パケット デコーダによって生成されるイベントについては、パケットのデコードについて（21-17 ページ）を参照してください。

UDP ストリームの前処理の設定

ライセンス：Protection

UDP ストリームの前処理を設定できます。

UDP セッションを追跡するストリーム プリプロセッサを設定する方法：

ステップ **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。

ステップ **2** 編集するアクセス 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。

ステップ **3** [詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **4** [ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ **5** [ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ **6** 編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシーの編集（Edit Policy）] ページが表示されます。

ステップ **7** 左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ **8** [トランスポートまたはネットワーク レイヤー プロセッサ（Transport/Network Layer Preprocessors）] で [UDP ストリームの構成（UDP Stream Configuration）] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[UDP ストリームの構成（UDP Stream Configuration）] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ **9** 必要に応じて、[タイムアウト（Timeout）] 値を設定し、プリプロセッサが非アクティブなストリームを状態テーブルに保持する期間を 1 ～ 86400 秒の範囲で指定します。指定した時間内に追加のデータグラムが現れなかった場合、プリプロセッサはそのストリームを状態テーブルから削除します。

ステップ 10　必要に応じて、[パケット タイプ パフォーマンスの向上（Packet Type Performance Boost）] を選択し、送信元および宛先ポートの両方を `any` に設定した UDP ルールで `flow` または `flowbits` オプションが使用されている場合を除き、有効化されたルールに指定されていないポートおよびアプリケーション プロトコルのすべてについて、UDP トラフィックを無視するように設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。

ステップ 11　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

パッシブ展開における前処理の調整

通常、システムはネットワーク分析ポリシーの静的な設定を使用して、トラフィックの前処理と分析を行います。ただし、適応型プロファイル機能により、トラフィックを得られるホスト情報と関連付けそれに応じてトラフィックを処理することにより、システムはネットワーク トラフィックに対応できます。

ホストがトラフィックを受信すると、ホストで実行されているオペレーティング システムは IP フラグメントを再構成します。再構成に使用する順序は、オペレーティング システムによって異なります。同様に、各オペレーティング システムはさまざまな方法で TCP を実装することがあるため、TCP ストリームの再構成の方法も異なる可能性があります。プリプロセッサが宛先ホストのオペレーティング システムで使用されているものとは異なる形式を使用してデータを再構成すると、受信ホストでの再構成時に悪意のある可能性があるコンテンツをシステムが見逃す可能性があります。

ヒント パッシブ展開の場合、シスコでは、適応型プロファイルを設定することを推奨しています。インライン展開の場合、シスコでは、インライン正規化プリプロセッサの設定で [TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にすることを推奨しています。詳細については、インライン トラフィックの正規化（21-6 ページ）を参照してください。

適応型プロファイルを使用したパケット フラグメントと TCP ストリームの再構成の改善に関する詳細については、次のトピックを参照してください。

- 適応型プロファイルについて（22-1 ページ）
- 適応型プロファイルの設定（22-3 ページ）

適応型プロファイルについて

ライセンス：Protection

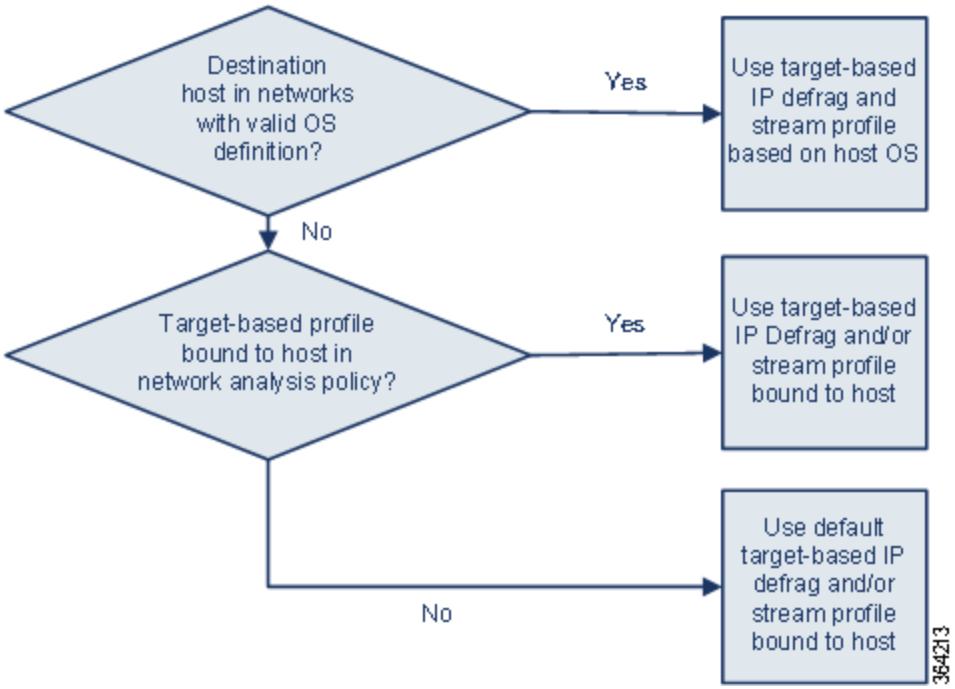
適応型プロファイルは、IP 最適化と TCP ストリームの前処理に最適なオペレーティング システム プロファイルの使用を可能にします。適応型プロファイルにより影響を受けるネットワーク分析ポリシーの側面の詳細については、IP パケットの最適化（21-12 ページ）およびTCP ストリームの前処理の使用（21-21 ページ）を参照してください。

プリプロセッサによる適応型プロファイルの使用

ライセンス：Protection

適応型プロファイルは、ターゲット ホストのオペレーティング システムと同じ方法で、IP パケットの最適化およびストリームの再構成を行うのに役立ちます。その後、侵入ルール エンジンは宛先ホストによって使用されるものと同じ形式でデータを分析します。

適応型プロファイルは、次の図に示すように、ターゲット ホストのホスト プロファイルのオペレーティング システムに基づいて、適切なオペレーティング システム プロファイルに切り替わります。



たとえば、10.6.0.0/16 サブネットに適合型プロファイルを設定し、Linux にデフォルトの [IP 最適化（IP Defragmentation）] ターゲット ベース ポリシーを設定します。設定を行う ASA FirePOWER モジュールには 10.6.0.0/16 サブネットが含まれています。

デバイスは、10.6.0.0/16 サブネットにないホスト A からのトラフィックを検出すると、Linux ターゲット ベース ポリシーを使用して IP フラグメントを再構成します。一方、10.6.0.0/16 サブネットにあるホスト B からのトラフィックを検出した場合、デバイスはホスト B のオペレーティング システムのデータを取得します。このマップでは、ホスト B が Microsoft Windows XP Professional を実行しています。システムは、Windows ターゲット ベース プロファイルを使用して、ホスト B に送信されるトラフィックの IP 最適化を実行します。

IP 最適化プリプロセッサの詳細については、IP パケットの最適化（21-12 ページ）を参照してください。ストリーム プリプロセッサの詳細については、TCP ストリームの前処理の使用（21-21 ページ）を参照してください。

適応型プロファイルの設定

ライセンス：Protection

ホスト情報を使用して IP 最適化および TCP ストリームの前処理に使用するターゲット ベース プロファイルを判別するために、適応型プロファイルを設定できます。

適応型プロファイルを設定する際、適応型プロファイルを特定のネットワークにバインドする必要があります。正常に適応型プロファイルを使用するには、そのネットワークがデバイスでモニタされるセグメントにある必要があります。

IP アドレス、アドレスのブロック、またはアクセス コントロール ポリシーのデフォルトの侵入ポリシーにリンクされた変数セットにおいて、設定された適切な値を使用したネットワーク変数を指定することで、トラフィックの処理に適応型プロファイルが使用される、ネットワーク内のホストを指定できます。詳細については、アクセス コントロールのデフォルト侵入ポリシーの設定（17-1 ページ）を参照してください。

これらのアドレス指定方法を単独で使用したり、次の例に示すように、IP アドレス、アドレス ブロック、または変数をカンマで区切ったリストとして組み合わせて使用したりすることができます。

```
192.168.1.101, 192.168.4.0/24, $HOME_NET
```

アドレス ブロックの指定の詳細については、IP アドレスの表記規則（1-4 ページ）を参照してください。

ヒント　any という値の変数を使用するか、またはネットワーク値として 0.0.0.0/0 を指定することにより、適合型プロファイルをネットワーク内のすべてのホストに適用できます。

適合型プロファイルの設定：

ステップ 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[検出拡張の設定（Detection Enhancement Settings）] の横にある編集アイコン（）をクリックします。

[検出拡張の設定（Detection Enhancement Settings）] ポップアップ ウィンドウが表示されます。

ステップ 5　[検出拡張の設定（Detection Enhancement Settings）] を選択して、適合型プロファイルを有効にします。

ステップ 6　必要に応じて、[適合型プロファイル - 属性の更新間隔（Adaptive Profiles - Attribute Update Interval）] フィールドに、データの同期の間隔（分）を入力します。

（注）　このオプションの値を大きくすると、大規模なネットワークのパフォーマンスを向上できます。

ステップ 7　[適合型プロファイル - ネットワーク（Adaptive Profiles - Networks）] フィールドに、適合型プロファイルを使用するネットワーク内のホストを識別する、特定の IP アドレス、アドレス ブロック、または変数、またはこれらのアドレス指定方法を含むカンマ区切りのリストを入力します。

変数の設定の詳細については、変数セットの使用（2-15 ページ）を参照してください。

ステップ 8　[OK] をクリックして設定内容を維持します。

侵入ポリシーを使用する前に

侵入ポリシーは定義済みの侵入検知のセットであり、セキュリティ違反についてトラフィックを検査し、インライン展開の場合は、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーは、アクセス コントロール ポリシーによって呼び出され、システムの最終防御ラインとして、トラフィックが宛先に到達することを許可するかどうかを判定します。

シスコは、複数の侵入ポリシーを ASA FirePOWER モジュールとともに提供します。システム付属のポリシーを使用することで、シスコ脆弱性調査チーム（VRT）の経験を活用できます。これらのポリシーに対して、VRT は侵入およびプリプロセッサ ルールの状態（有効または無効）を設定し、他の詳細設定の初期設定も行います。ルールを有効にすると、ルールに一致するトラフィックに対して侵入イベントが生成されます（さらに、必要に応じてトラフィックがブロックされます）。ルールを無効にすると、ルールの処理が停止されます。

ヒント

システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。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（15-1 ページ）には、ネットワーク分析ポリシーと侵入ポリシーが連携してトラフィックを検査するしくみの概要、およびナビゲーション パネルの使用、競合の解決、変更のコミットに関する基本事項が記載されています。

カスタム侵入ポリシーを作成すると、以下を実行できます。

- ルールを有効化/無効化することに加え、独自のルールを作成して追加し、検出を調整する。
- 外部アラート、センシティブ データの前処理、グローバル ルールのしきい値設定など、さまざまな詳細設定を設定する。
- レイヤを構成要素として使用し、複数の侵入ポリシーを効率的に管理する。

留意事項として、侵入ポリシーを調整する場合（特にルールを有効化して追加する場合）、一部の侵入ルールでは、最初に特定の方法でトラフィックをデコードまたは前処理する必要があります。侵入ポリシーによって検査される前に、パケットはネットワーク分析ポリシーの設定に従って前処理されます。必要なプリプロセッサを無効にすると、システムは現在の設定で自動的にプリプロセッサを使用しますが、ネットワーク分析ポリシーのユーザ インターフェイスではプリプロセッサは無効のままになります。

（注）

前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する必要があります。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、高度なタスクです。詳細については、カスタム ポリシーに関する制約事項（15-12 ページ）を参照してください。

カスタム侵入ポリシーを設定した後、それを 1 つ以上のアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに関連付けることによって、カスタム侵入ポリシーをアクセス コントロール設定の一部として使用できます。これによって、システムは、最終宛先に渡す前に、特定の許可されたトラフィックを侵入ポリシーによって検査します。変数セットを侵入ポリシーと組み合わて使用することにより、ホーム ネットワークと外部ネットワークに加えて、必要に応じてネットワーク上のサーバを正確に反映させることができます。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（10-1 ページ）を参照してください。

この章では、単純なカスタム侵入ポリシーの作成方法について説明します。この章には、侵入ポリシーの管理（編集、比較など）に関する基本情報も記載されています。詳細については、以下を参照してください。

カスタム侵入ポリシーの作成

ライセンス：Protection

新しい侵入ポリシーを作成する場合は、一意の名前を付けて基本ポリシーを指定し、ドロップ動作を指定する必要があります。

基本ポリシーは侵入ポリシーのデフォルト設定を定義します。新しいポリシーの設定の変更は、基本ポリシーの設定を変更するのではなく、オーバーライドします。システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。詳細については、基本レイヤについて（16-2 ページ）を参照してください。

侵入ポリシーのドロップ動作、または [インライン時にドロップ（Drop when Inline）] の設定によって、廃棄ルール（ルール状態が [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されている侵入ルールまたはプリプロセッサ ルール）、およびトラフィックに影響を与えるその他の侵入ポリシー設定のシステムにおける処理方法が決まります。悪意のあるパケットをドロップまたは置き換える場合は、インライン展開でドロップ動作を有効にする必要があります。パッシブ展開では、ドロップ動作に関わらず、システムはトラフィック フローに影響を与えることはできません。詳細については、インライン展開でのドロップ動作の設定（23-6 ページ）を参照してください。

侵入ポリシーを作成する方法：

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ヒント　また、別の 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。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。

ステップ 2　[ポリシーの作成(Create Policy)] をクリックします。

別のポリシー内に未保存の変更が存在する場合は、[侵入ポリシー(Intrusion Policy)] ページに戻るかどうか尋ねられたときに [キャンセル(Cancel)] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[侵入ポリシーの作成(Create Intrusion Policy)] ポップアップ ウィンドウが表示されます。

ステップ 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。

ステップ 4　[基本ポリシー(Base Policy)] で最初の基本ポリシーを指定します。

システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

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

ステップ 5　インライン展開でのシステムのドロップ動作を設定します。

- 侵入ポリシーによるトラフィックへの影響およびイベントの生成を許可するには、[インライン時にドロップ(Drop when Inline)] を有効にします。
- 侵入ポリシーによるトラフィックへの影響を回避し、イベントの生成のみを許可するには、[インライン時にドロップ(Drop when Inline)] を無効にします。

ステップ 6　ポリシーを作成します。

- 新しいポリシーを作成して、[侵入ポリシー(Intrusion Policy)] ページに戻るには、[ポリシーの作成(Create Policy)] をクリックします。新しいポリシーには基本ポリシーと同じ設定項目が含まれています。
- ポリシーを作成し、高度な侵入ポリシー エディタでそれを開いて編集するには、[ポリシーの作成と編集(Create and Edit Policy)] をクリックします(侵入ポリシーの編集(23-4 ページ)を参照)。

侵入ポリシーの管理

ライセンス:Protection

[侵入ポリシー(Intrusion Policy)] ページ([設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)])で、現在のカスタム侵入ポリシーを次の情報とともに確認できます。

- ポリシーが最後に変更された日時(ローカル時間)
- [インライン時にドロップ(Drop when Inline)] 設定が有効になっているかどうか。この設定が有効な場合、インライン展開でトラフィックをドロップしたり変更することができます。
- トラフィックを検査するために侵入ポリシーを使用しているアクセス コントロール ポリシー
- ポリシーに保存されていない変更があるかどうか

[侵入ポリシー(Intrusion Policy)] ページのオプションを使用して、次の表のアクションを実行できます。

表 *23-1*　侵入ポリシー管理操作

目的	操作	参照先
新しい侵入ポリシーを作成する	[ポリシーの作成(Create Policy)]をクリックします。	カスタム侵入ポリシーの作成(23-2 ページ)
既存の侵入ポリシーを編集する	編集アイコン( )をクリックします。	侵入ポリシーの編集(23-4 ページ)
侵入ポリシーを再適用する	適用アイコン( )をクリックします。	侵入ポリシーの適用(23-8 ページ)
侵入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)
侵入ポリシーの現在の構成設定を示す PDF レポートを表示する	レポート アイコン( )をクリックします。	現在の侵入設定のレポートの生成(23-9 ページ)
2 つの侵入ポリシーまたは同じポリシーの 2 つのリビジョンの設定を比較する	[ポリシーの比較(Compare Policies)]をクリックします。	2 つの侵入ポリシーまたはリビジョンの比較(23-9 ページ)
侵入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。アクセス コントロール ポリシーが参照している侵入ポリシーは削除できません。	

侵入ポリシーの編集

ライセンス:Protection

新しい侵入ポリシーを作成すると、そのポリシーには基本ポリシーと同じ侵入ルールと詳細設定が付与されます。次の表では、侵入ポリシーの編集時に実行する最も一般的な操作について説明しています。

表 *23-2*　侵入ポリシーの編集操作

目的	操作	参照先
インライン展開でドロップ動作を指定する	[ポリシー情報(Policy Information)]ページの [インライン時にドロップ(Drop when Inline)] チェック ボックスをオンまたはオフにします。	インライン展開でのドロップ動作の設定(23-6 ページ)
基本ポリシーを変更する	[ポリシー情報(Policy Information)]ページの [基本ポリシー(Base Policy)] ドロップダウン リストから、基本ポリシーを選択します。	基本ポリシーの変更(16-4 ページ)
基本ポリシーの設定を表示する	[ポリシー情報(Policy Information)]ページで [基本ポリシーの管理(Manage Base Policy)]をクリックします。	基本レイヤについて(16-2 ページ)
侵入ルールを表示または設定する	[ポリシー情報(Policy Information)]ページで [ルールの管理(Manage Rules)]をクリックします。	侵入ポリシー内のルールの表示(24-3 ページ)

表 23-2　侵入ポリシーの編集操作（続き）

目的	操作	参照先
現在のルール状態別に侵入ルールのフィルタビューを表示する、またオプションでそれらのルールを設定する	[ポリシー情報（Policy Information）] ページの [ルールの管理（Manage Rules）] で、[イベントを生成する（Generate Events）] または [ドロップしてイベントを生成する（Drop and Generate Events）] が設定されているルールの番号の横にある [表示（View）] をクリックします。	侵入ポリシー内のルールのフィルタリング（24-10 ページ）
詳細設定を有効化、無効化、または編集する	ナビゲーション パネルで [詳細設定（Advanced Settings）] をクリックします。	侵入ポリシーの詳細設定の設定（23-7 ページ）
ポリシー層を管理する	ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。	ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）

留意事項として、侵入ポリシーを調整する場合（特にルールを有効化して追加する場合）、一部の侵入ルールでは、最初に特定の方法でトラフィックをデコードまたは前処理する必要があります。侵入ポリシーによって検査される前に、パケットはネットワーク分析ポリシーの設定に従って前処理されます。必要なプリプロセッサを無効にすると、システムは現在の設定で自動的にプリプロセッサを使用しますが、ネットワーク分析ポリシーのユーザ インターフェイスではプリプロセッサは無効のままになります。

（注）　前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する必要があります。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、高度なタスクです。詳細については、カスタム ポリシーに関する制約事項（15-12 ページ）を参照してください。

システムは、1 つの侵入ポリシーをキャッシュします。侵入ポリシーの編集中に、メニューまたは別のページへのパスを選択すると、そのページから移動しても、変更内容はシステム キャッシュに残ります。上の表に示す実行できるアクションの他に、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（15-1 ページ）では、競合の解決および変更のコミットに関する情報を記載しています。

侵入ポリシーの編集方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ 2　設定する侵入ポリシーの横にある編集アイコン（ ）をクリックします。

侵入ポリシー エディタが開き、[ポリシー情報（Policy Information）] ページとその左端にナビゲーション パネルが表示されます。

ステップ 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。

ステップ 4　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

インライン展開でのドロップ動作の設定

ライセンス：Protection

インライン展開では、侵入ポリシーによってトラフィックを変更したりブロックすることができます。

- 廃棄ルールを使用すると、一致したパケットをドロップして、侵入イベントを生成できます。侵入またはプリプロセッサの廃棄ルールを設定するには、そのステータスを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定します（ルール状態の設定（24-21 ページ）を参照）。
- 侵入ルールでは、`replace` キーワードを使用して悪意のあるコンテンツを置き換えることができます（インライン展開でのコンテンツの置換（27-31 ページ）を参照）。

侵入ルールがトラフィックに影響するには、廃棄ルールおよびコンテンツを置換するルールを適切に設定し、システムをインラインで正しく展開する必要があります。最後に、侵入ポリシーのドロップ動作（[インライン時にドロップ（Drop when Inline）] 設定）を有効にします。

（注）　FTP を介してマルウェア ファイルの転送をブロックするには、ネットワーク ベースの高度なマルウェア防御（AMP）を設定するだけではなく、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で [インライン時にドロップ（Drop when Inline）] を有効にする必要があります。デフォルトの侵入ポリシーを確認または変更するには、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（17-1 ページ）を参照してください。

設定がインライン展開で実際にトラフィックに影響を与えることなくどのように機能するかを評価する場合は、ドロップ動作を無効にできます。その場合、システムは侵入イベントを生成しますが、廃棄ルールをトリガーしたパケットをドロップしません。結果を確認したら、ドロップ動作を有効化できます。

パッシブ展開では、ドロップ動作に関係なくシステムはトラフィックに影響を与えることができないことに注意してください。つまり、パッシブ展開では、[ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールは [イベントを生成する（Generate Events）] に設定されたルールと同様に動作します。システムは侵入イベントを生成しますが、パケットをドロップできません。

侵入イベントを表示する際に、ワークフローにインライン結果を含めることができます。インライン結果は、トラフィックが実際にドロップされたのか、あるいはドロップが想定に過ぎなかったのかを示します。パケットが廃棄ルールに一致した場合、インライン結果は次のようになります。

- ドロップ動作が有効な正しく設定されたインライン展開によりドロップされたパケットの場合は `Dropped`
- デバイスがパッシブで展開されている、またはドロップ動作が無効であるため、パケットがドロップされなかった場合は `Would have dropped`。展開に関係なく、システムがプルーニングしている間に検出されるパケットのインライン結果は、常に `Would have dropped` です。

インライン展開での侵入ポリシーのドロップ動作の設定方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（）をクリックします。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 3　ポリシーのドロップ動作を設定します。

- 侵入ルールによるトラフィックへの影響およびイベントの生成を許可するには、[インライン時にドロップ（Drop when Inline）] を有効にします。
- 侵入ルールによるトラフィックへの影響を回避し、イベントの生成のみを許可するには、[インライン時にドロップ（Drop when Inline）] を無効にします。

ステップ 4　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

侵入ポリシーの詳細設定の設定

ライセンス：Protection

侵入ポリシーの詳細設定を設定するには、特定の専門知識が必要です。デフォルトで有効になる詳細設定や、詳細設定ごとのデフォルトは、侵入ポリシーの基本ポリシーに応じて決まります。

侵入ポリシーのナビゲーション パネルで [詳細設定（Advanced Settings）] を選択すると、ポリシーの詳細設定がタイプ別に一覧表示されます。[詳細設定（Advanced Settings）] ページでは、侵入ポリシーの詳細設定を有効または無効にしたり、詳細設定の設定ページにアクセスすることができます。

詳細設定を行うには、それを有効にする必要があります。詳細設定を有効にすると、その詳細設定に関する設定ページへのサブリンクがナビゲーション パネル内の [詳細設定（Advanced Settings）] リンクの下に表示され、この設定ページへの [編集（Edit）] リンクが [詳細設定（Advanced Settings）] ページ上の詳細設定の横に表示されます。

ヒント　詳細設定の設定を基本ポリシーの設定に戻すには、詳細設定の設定ページで [デフォルトに戻す（Revert to Defaults）] をクリックします。プロンプトが表示されたら、復元することを確認します。

詳細設定を無効にすると、サブリンクと [編集（Edit）] リンクは表示されなくなりますが、設定は保持されます。侵入ポリシーの一部の設定（センシティブ データ ルール、侵入ルールの SNMP アラート）では、詳細設定を有効化して適切に設定する必要があります。このように誤って設定された侵入ポリシーは保存できません（競合の解決とポリシー変更の確定（15-15 ページ）を参照）。

詳細設定を変更する場合、変更する設定と、その変更がネットワークに及ぼす可能性のある影響について理解していることが必要です。次の項では、詳細設定ごとに固有の設定の詳細情報へのリンクを記述します。

特定の脅威の検出（**Specific Threat Detection**）

機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。このプリプロセッサの設定方法については、センシティブ データの検出（25-21 ページ）を参照してください。

特定の脅威（Back Orifice 攻撃、何種類かのポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレート ベース攻撃）を検出するプリプロセッサは、ネットワーク分析ポリシーで設定します。詳細については、特定の脅威の検出（25-1 ページ）を参照してください。

侵入ルールしきい値（**Intrusion Rule Thresholds**）

グローバル ルールのしきい値を設定すると、しきい値を使用して、システムが侵入イベントを記録したり表示したりする回数を制限できるので、多数のイベントでシステムが圧迫されないようにすることができます。詳細については、侵入イベント ロギングのグローバルな制限（26-1 ページ）を参照してください。

外部レスポンス（**External Responses**）

ユーザ インターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、システム ログ（syslog）ファシリティへのロギングを有効にしたり、イベント データを SNMP トラップ サーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。詳細については、以下を参照してください。

- SNMP 応答の設定（36-3 ページ）
- syslog 応答の設定（36-6 ページ）

侵入ポリシーの適用

ライセンス：Protection

アクセス コントロールを使用して侵入ポリシーを適用（設定変更の展開（4-12 ページ）を参照）した後は、その侵入ポリシーをいつでも再適用できます。これにより、アクセス コントロール ポリシーを再適用せずに、モニタ対象ネットワーク上で侵入ポリシーを変更できます。再適用中は、比較レポートを表示して、最後に侵入ポリシーが適用されてから加えられた変更を確認できます。

侵入ポリシーを再適用する際は次の点に注意してください。

- 侵入ポリシーの再適用タスクは、定期的に実行するようにスケジュールできます（侵入ポリシーの適用の自動化（39-5 ページ）を参照）。
- ルール更新をインポートするときに、インポートの完了後に自動的に侵入ポリシーを適用できます。このオプションを有効にしなかった場合は、ルール更新によって変更されたポリシーを手動で再適用する必要があります。詳細については、ルールの更新とローカル ルール ファイルのインポート（43-10 ページ）を参照してください。

侵入ポリシーを再適用する方法：

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

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

[侵入ポリシーの再適用（Reapply Intrusion Policy）] ウィンドウが開きます。

ステップ **3**　[再適用（Reapply）] をクリックします。

ポリシーが再適用されます。タスク キューを使用して適用のステータスをモニタできます（[モニタリング（Monitoring）] > [ASA FirePOWER モニタリング（ASA FirePOWER Monitoring）] > [タスクのステータス（Task Status）]）。詳細については、タスク キューの表示（C-1 ページ）を参照してください。

現在の侵入設定のレポートの生成

ライセンス：Protection

侵入ポリシー レポートは、特定の時点におけるポリシー設定の記録です。システムは、基本ポリシー内の設定とポリシー層の設定を統合して、基本ポリシーに起因する設定とポリシー層に起因する設定を区別しません。

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 *23-3*　侵入ポリシー 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、侵入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。インライン展開でパケットのドロップが有効になっているか無効になっているか、現在のルール更新のバージョン、および基本ポリシーが現在のルール更新にロックされているかどうかが示されます。
詳細設定（Advanced Settings）	すべての有効化されている侵入ポリシーの設定項目およびその設定を一覧表示します。
ルール（Rule）	有効になっているすべてのルールとその動作を一覧表示します。

また、2 つの侵入ポリシーまたは同じポリシーの 2 つのリビジョンを比較する比較レポートを生成することもできます。詳細については、2 つの侵入ポリシーまたはリビジョンの比較（23-9 ページ）を参照してください。

侵入ポリシー レポートを表示する方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ 2　レポートを生成する侵入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。侵入ポリシー レポートを生成する前に未確定の変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

システムが侵入ポリシー レポートを生成します。コンピュータにレポートを保存するようにプロンプトが出されます。

2 つの侵入ポリシーまたはリビジョンの比較

ライセンス：Protection

ポリシー変更が組織の標準に準拠しているかどうかを確認するため、またはシステムのパフォーマンスを最適化するために、2 つの侵入ポリシーの違いを確認することができます。アクセス可能な侵入ポリシーの場合は、2 つの侵入ポリシーまたは同じ侵入ポリシーの 2 つのリビジョンを比較できます。比較した後に、必要に応じて、2 つのポリシーまたはポリシー リビジョン間の違いを記録した PDF レポートを生成できます。

侵入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。

- 比較ビューには、2 つの侵入ポリシーまたは侵入ポリシー リビジョン間の違いだけが並べて表示されます。各ポリシーの名前が比較ビューの左右のタイトル バーに表示されます。

  これを使用して、ユーザ インターフェイスで相違点を強調表示したまま、両方のポリシーのリビジョンを表示し移動することができます。

- 比較レポートは、2 つの侵入ポリシーまたは侵入ポリシー リビジョン間の違いのみを記録したもので、PDF であるという以外は、侵入ポリシー レポートと類似した形式になっています。

  これを使用して、ポリシーの比較を保存、コピー、出力、共有して、さらに検証することができます。

侵入ポリシー比較ツールとその使い方の詳細については、以下を参照してください。

- 侵入ポリシー比較ビューの使用（23-10 ページ）
- 侵入ポリシー比較レポートの使用（23-11 ページ）

侵入ポリシー比較ビューの使用

ライセンス：Protection

比較ビューには、両方の侵入ポリシーまたはポリシー リビジョンが並べて表示されます。それぞれのポリシーまたはポリシー リビジョンは、比較ビューの左右のタイトル バーに表示された名前で識別されます。最終変更時刻と最終変更ユーザがポリシー名の右側に表示されます。[侵入ポリシー（Intrusion Policy）] ページにはポリシーが最後に変更された時刻が現地時間で表示されますが、侵入ポリシー レポートでは変更時刻が UTC でリストされることに注意してください。2 つの侵入ポリシーまたはポリシー リビジョン間の違いが強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーまたはポリシー リビジョンで違うことを意味します。違いは赤色のテキストで表示されます。
- 緑色は強調表示された設定が一方のポリシーまたはポリシー リビジョンだけにあるが、他方にないことを意味します。

次の表内の操作を実行できます。

表 ***23-4***　侵入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。
新しい侵入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、侵入ポリシー比較レポートの使用を参照してください。
侵入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 つのポリシーまたはリビジョンの相違点だけがリストされた PDF です。

侵入ポリシー比較レポートの使用

ライセンス：Protection

侵入ポリシー比較レポートは、PDF で提供される、侵入ポリシー比較ビューで特定された 2 つの侵入ポリシー間または同じ侵入ポリシーの 2 つのリビジョン間のすべての違いを記録したものです。このレポートは、2 つの侵入ポリシー構成間の違いをさらに調査し、その結果を保存して共有するために使用できます。

侵入ポリシー比較レポートは、アクセス可能な任意の侵入ポリシーの比較ビューから生成できます。侵入ポリシー レポートを生成する前に未確定の変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

侵入ポリシー比較レポートの形式は 1 つの例外（侵入ポリシー レポートには侵入ポリシー内のすべての設定が含まれる）を除いて侵入ポリシー レポートと同じであり、侵入ポリシー比較レポートにはポリシー間で異なる設定のみがリストされます。

構成に応じて、侵入ポリシー比較レポートに侵入ポリシー レポートのセクションの表に示す 1 つ以上のセクションを含めることができます。

ヒント　同様の手順を使用して、アクセス コントロール ポリシー、ネットワーク分析ポリシー、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 つの侵入ポリシーまたは同じポリシーの **2** つのリビジョンを比較する方法：

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ **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。

ステップ **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。
- 同じポリシーの 2 つのリビジョンを比較するには、[その他のリビジョン（Other Revision）] を選択します。

侵入ポリシー レポートを生成する前に変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

ステップ **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。
- 同じポリシーの 2 つのリビジョンを比較する場合は、[ポリシー（Policy）] ドロップダウンリストからポリシーを選択してから、[リビジョン A（Revision A）] と [リビジョン B（Revision B）] ドロップダウンリストから比較するリビジョンを選択します。

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

比較ビューが表示されます。

ステップ **6**　侵入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。

ステップ **7**　侵入ポリシー 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プロンプトが出されます。

ルールを使用した侵入ポリシーの調整

侵入ポリシーの [ルール] ページを使用して、共有オブジェクトのルール、標準テキスト ルール、およびプリプロセッサ ルールに関するルール状態とその他の設定を構成できます。

ルールは、ルール状態を [イベントを生成する（Generate Events）] または [ドロップしてイベントを生成する（Drop and Generate Events）] に設定することによって有効にします。ルールを有効にすると、システムがそのルールと一致するトラフィックに対するイベントを生成します。ルールを無効にすると、ルールの処理が停止されます。オプションで、インライン展開で [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールによって、一致するトラフィックに対するイベントが生成され、そのトラフィックが破棄されるように、侵入ポリシーを設定できます。詳細については、インライン展開でのドロップ動作の設定（23-6 ページ）を参照してください。パッシブ展開では、[ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールによって、一致するトラフィックに対するイベントが生成されるだけです。

ルールのサブセットを表示するようにルールをフィルタ処理することによって、ルール状態やルール設定を変更するルールのセットを正確に選択できます。

侵入ルールまたはルールの引数にプリプロセッサの無効化が必要な場合、システムは現在の設定で自動的にプリプロセッサを使用しますが、ネットワーク分析ポリシーのユーザ インターフェイスではプリプロセッサは無効のままになります。詳細については、カスタム ポリシーに関する制約事項（15-12 ページ）を参照してください。

詳細については、次の各項を参照してください。

- 侵入防御ルール タイプについて（24-2 ページ）では、侵入ポリシーで表示または設定可能な侵入ルールとプリプロセッサ ルールについて説明します。
- 侵入ポリシー内のルールの表示（24-3 ページ）では、[ルール（Rules）] ページでルールの順序を変更したり、ページ上のアイコンを解釈したり、ルール詳細に焦点を当てたりするための方法について説明します。
- 侵入ポリシー内のルールのフィルタリング（24-10 ページ）では、ルール フィルタを使用して、ルール設定を適用するルールを見つける方法について説明します。
- ルール状態の設定（24-21 ページ）では、[ルール（Rules）] ページでルールを有効または無効にする方法について説明します。
- ポリシー単位の侵入イベント通知のフィルタリング（24-23 ページ）では、特定のルールに対するイベント フィルタリングしきい値の設定方法と特定のルールの抑制方法について説明します。
- 動的ルール状態の追加（24-31 ページ）では、一致するトラフィックでレート異常が検出されたときに動的にトリガーとして使用されるルール状態の設定方法について説明します。
- SNMP アラートの追加（24-34 ページ）では、SNMP アラートを特定のルールに関連付ける方法について説明します。
- ルール コメントの追加（24-35 ページ）では、侵入ポリシー内のルールにコメントを追加する方法について説明します。

侵入防御ルール タイプについて

ライセンス：Protection

侵入ポリシーには、侵入ルールとプリプロセッサ ルールという 2 つのルール タイプが含まれています。

侵入ルールは、ネットワーク上の脆弱性を悪用する試みを検出するキーワードと引数の指定されたセットで、ネットワーク トラフィックを分析してルール内の基準が満たされているかどうかをチェックします。システムは各ルールで指定された条件をパケットに照らし合わせます。ルールで指定されたすべての条件にパケット データが一致する場合、ルールがトリガーされます。システムには、シスコ脆弱性調査チーム（VRT）が作成した次の 2 種類の侵入ルールが付属しています。共有オブジェクトのルールは、コンパイルされ、変更できません（送信元ポート、宛先ポート、IP アドレスなどのルール ヘッダー情報を除く）。標準テキスト ルールは、ルールの新しいカスタム インスタンスとして保存して変更できます。

システムには、プリプロセッサに関連付けられたルールであるプリプロセッサ ルールとパケット デコーダ検出オプションも付属しています。プリプロセッサ ルールはコピーまたは編集できません。ほとんどのプリプロセッサ ルールがデフォルトで無効になっているため、システムにプリプロセッサ ルールに対するイベントの生成とインライン展開での違反パケットの破棄を指示する場合は、これらのルールを有効にする（つまり、[イベントを生成する（Generate Events）] または [ドロップしてイベントを生成する（Drop and Generate Events）] に設定する）必要があります。

VRT が、システムに付属のデフォルト侵入ポリシー用のシスコの共有オブジェクトのルール、標準テキスト ルール、およびプリプロセッサ ルールのデフォルト ルール状態を決定します。

次の表で、ASA FirePOWER モジュールに付属しているルールの各タイプについて説明します。

表 **24-1**　ルール タイプ

タイプ	説明
共有オブジェクトのルール	C ソース コードからコンパイルされたバイナリ モジュールとして配布されるシスコ脆弱性調査チーム（VRT）によって作成された侵入ルール。共有オブジェクトのルールを使用して、標準テキスト ルールでは不可能な方法で攻撃を検出できます。共有オブジェクトのルール内のルール キーワードと引数は変更できません。実行できるのは、ルール内で使用されている変数の変更か、送信元ポート、宛先ポート、IP アドレスなどの要素の変更とカスタム共有オブジェクトのルールとしてのルールの新しいインスタンスの保存のみです。共有オブジェクトのルールには、GID（ジェネレータ ID）の 3 が割り当てられます。詳細については、既存のルールの変更（27-108 ページ）を参照してください。
標準テキスト ルール	VRT によって作成された侵入ルール、コピーされて新しいカスタム ルールとして保存された侵入ルール、ルール エディタを使用して作成された侵入ルール、またはユーザがローカル マシン上で作成してインポートしたローカル ルールとしてインポートされた侵入ルール。VRT によって作成された標準ルール内のルール キーワードと引数は変更できません。実行できるのは、ルール内で使用されている変数の変更か、送信元ポート、宛先ポート、IP アドレスなどの要素の変更とカスタム標準テキスト ルールとしてのルールの新しいインスタンスの保存のみです。詳細については、既存のルールの変更（27-108 ページ）、侵入ルールの概要と作成（27-1 ページ）、およびローカル ルール ファイルのインポート（43-16 ページ）を参照してください。VRT によって作成された標準テキスト ルールには、GID（ジェネレータ ID）の 1 が割り当てられます。ルール エディタを使用して作成した、または、ローカル ルールとしてインポートしたカスタム標準テキスト ルールには 1000000 以上の SID（シグニチャ ID）が割り当てられます。
プリプロセッサ ルール	パケット デコーダの検出オプションまたは ASA FirePOWER モジュールに付属のプリプロセッサの 1 つに関連付けられたルール。プリプロセッサ ルールによってイベントを生成するには、プリプロセッサ ルールを有効にする必要があります。このルールには、デコーダ固有またはプリプロセッサ固有の GID（ジェネレータ ID）が割り当てられます。

侵入ポリシー内のルールの表示

ライセンス：Protection

侵入ポリシーでのルールの表示方法を調整でき、複数の条件によってルールをソートできます。特定のルールの詳細を表示して、ルール設定、ルール ドキュメント、およびその他のルール仕様を確認することもできます。

[ルール（Rules）] ページには次の 4 つの主な機能領域があります。

- フィルタリング機能：詳細については、侵入ポリシー内のルールのフィルタリング（24-10 ページ）を参照してください。
- ルール属性メニュー：詳細については、ルール状態の設定（24-21 ページ）、ポリシー単位の侵入イベント通知のフィルタリング（24-23 ページ）、動的ルール状態の追加（24-31 ページ）、SNMP アラートの追加（24-34 ページ）、およびルール コメントの追加（24-35 ページ）を参照してください。
- ルール一覧：詳細については、[ルール（Rules）] ページのカラムの表を参照してください。
- ルールの詳細：詳細については、ルール詳細の表示（24-5 ページ）を参照してください。

さまざまな基準に基づいてルールをソートすることもできます。詳細については、ルール画面のソート（24-4 ページ）を参照してください。

カラム見出しとして使用されているアイコンは、設定項目にアクセスするためのメニュー バー内のメニューに対応していることに注意してください。たとえば、[ルール状態（Rule State）] メニューは、[ルール状態（Rule State）] カラムと同じアイコン（）でマークされています。

次の表に、[ルール（Rules）] ページのカラムの説明を示します。

表 **24-2**　　*[ルール（**Rules**）]* ページのカラム

見出し	説明	詳細
GID	ルールのジェネレータ ID（GID）を表す整数。	イベントの表示（34-1 ページ）
SID	ルールの一意の識別子として機能する Snort ID（SID）を表す整数。	イベントの表示（34-1 ページ）
メッセージ	このルールによって生成されるイベントに含まれるメッセージ。ルールの名前としても機能します。	イベント メッセージの定義（27-12 ページ）
	ルールのルール状態。次の 3 つのうちのいずれかの状態になります。 • ドロップしてイベントを生成する（） • イベントを生成する（） • 無効（） ルール状態アイコンをクリックすることによって、ルールの [ルール状態の設定（Set rule state）] ダイアログ ボックスにアクセスできることに注意してください。	ルール状態の設定（24-21 ページ）
	ルールに適用されるイベントしきい値やイベント抑制などのイベント フィルタ。	ポリシー単位の侵入イベント通知のフィルタリング（24-23 ページ）
	ルールの動的ルール状態。指定されたレート異常が発生した場合に有効になります。	動的ルール状態の追加（24-31 ページ）
	ルールに対して設定されたアラート（現在は SNMP アラートのみ）。	SNMP アラートの追加（24-34 ページ）
	ルールに追加されたコメント。	ルール コメントの追加（24-35 ページ）

レイヤのドロップダウンリストを使用して、ポリシー内の他のレイヤの [ルール(Rules)] ページに切り替えることもできます。ポリシーにレイヤを追加しなかった場合にドロップダウンリストに表示される編集可能なビューはポリシーの [ルール(Rules)] ページと、元は `My Changes` という名前だったポリシー階層の [ルール(Rules)] ページだけであることに注意してください。これらのビューの一方を変更すると、もう一方も同じように変更されることにも注意してください。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(16-1 ページ)を参照してください。ドロップダウンリストには、読み取り専用の基本ポリシーの [ルール(Rules)] ページも表示されます。基本ポリシーの詳細については、基本レイヤについて(16-2 ページ)を参照してください。

侵入ポリシー内のルールを表示する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 3　[ポリシー情報(Policy Information)] ページで [ルール(Rules)] をクリックします。

[ルール(Rules)] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ナビゲーション パネルの境界線の上にある [ルール(Rules)] を選択すると、同じルール一覧が表示されることに注意してください。このビューでポリシー内のすべてのルール属性を表示して設定できます。

ルール画面のソート

ライセンス:Protection

[ルール(Rules)] ページでは、見出しタイトルまたはアイコンをクリックすることによって、ルールをいずれかのカラムでソートできます。

見出しまたはアイコン上の上矢印(▲)または下矢印(▶)は、そのカラムを基準として、その方向にソートが実行されることを意味していることに注意してください。

侵入ポリシー内でルールをソートする方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 3　[ルール(Rules)] をクリックします。

[ルール(Rules)] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　ソートの基準とするカラムの一番上のタイトルまたはアイコンをクリックします。

ルールがそのカラムのカラム見出しに表示された矢印が示す方向でソートされます。反対方向でソートするには、見出しを再度クリックします。ソート順と矢印が反転します。

ルール詳細の表示

ライセンス:Protection

[ルールの詳細(Rule Detail)] ビューで、ルール ドキュメントおよびルール オーバーヘッドを表示できます。また、ルール固有の機能を表示および追加できます。

脆弱性にマップされていないローカル ルールにはオーバーヘッドがないことに注意してください。

表 24-3　ルールの詳細

項目	説明	詳細
要約	ルールの概要。ルール ベースのイベントでは、ルール ドキュメントに概要情報が含まれている場合にこの行が表示されます。	イベントの表示(34-1 ページ)
ルール状態(Rule State)	ルールの現在のルール状態。ルール状態が設定された階層も示します。	ルール状態の設定(24-21 ページ)、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(16-1 ページ)
しきい値	このルールに現在設定されているしきい値と、ルールのしきい値を追加するための機能。	ルールのしきい値の設定(24-6 ページ)
抑制(Suppressions)	このルールに現在設定されている抑制設定と、ルールの抑制を追加するための機能。	ルールの抑制の設定(24-7 ページ)
動的状態(Dynamic State)	このルールに現在設定されているレート ベースのルール状態と、ルールの動的ルール状態を追加するための機能。	ルールの動的ルール状態の設定(24-8 ページ)
アラート(Alerts)	このルールに現在設定されているアラートと、ルールのアラートを追加するための機能。現在は、SNMP アラートのみがサポートされています。	ルールの SNMP アラートの設定(24-9 ページ)
説明	このルールに追加されたコメントと、ルールのコメントを追加するための機能。	ルールに関するルール コメントの追加(24-9 ページ)
資料	シスコ脆弱性調査チーム(VRT)から提供される現在のルールのルール ドキュメント。	イベントの表示(34-1 ページ)

ルール詳細を表示する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 3　[ルール(Rules)] をクリックします。

[ルール(Rules)] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　ルール詳細を表示するルールを強調表示します。

ステップ 5　[詳細の表示(Show details)] をクリックします。

[ルールの詳細(Rule Detail)] ビューが表示されます。詳細を再度非表示にするには、[詳細の非表示(Hide details)] をクリックします。

ヒント　[ルール(Rules)] ビューでルールをダブルクリックすることによって、[ルールの詳細(Rule Detail)] を開くこともできます。

ルールのしきい値の設定

ライセンス:Protection

[ルールの詳細(Rule Detail)] ページで、ルールの単一のしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。しきい値設定の詳細については、イベントしきい値の設定(24-23 ページ)を参照してください。

無効な値を入力するとフィールドに復元アイコン( )が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細でしきい値を設定する方法:

ステップ 1　[しきい値(Thresholds)] の横にある [追加(Add)] をクリックします。

[しきい値の設定(Set Threshold)] ダイアログボックスが表示されます。

ステップ 2　[タイプ(Type)] ドロップダウンリストから、設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベント インスタンス数に通知を制限する場合は、[制限(Limit)] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[しきい値(Threshold)] を選択します。
- 指定されたイベント インスタンス数後に期間あたり 1 回ずつ通知を提供する場合は、[両方(Both)] を選択します。

ステップ 3　[追跡対象(Track By)] ドロップダウンリストから、[送信元(Source)] または [宛先(Destination)] を選択し、イベント インスタンスが送信元 IP アドレスまたは宛先 IP アドレスのどちらによって追跡されるかを指定します。

ステップ 4　[カウント(Count)] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

ステップ 5　[秒(Seconds)] フィールドで、イベント インスタンスを追跡する期間(秒数)を指定する 0 から 2147483647 までの数を入力します。

ステップ 6　[OK] をクリックします。

システムが、しきい値を追加し、[イベント フィルタリング(Event Filtering)] カラムのルールの横にイベント フィルタ アイコン( )を表示します。ルールに複数のイベント フィルタを追加すると、アイコン上にイベント フィルタの数が表示されます。

ルールの抑制の設定

ライセンス:Protection

[ルールの詳細(Rule Detail)] ページで、ルールの 1 つまたは複数の抑制を設定できます。抑制の詳細については、侵入ポリシー単位の抑制の設定(24-28 ページ)を参照してください。

無効な値を入力するとフィールドに復元アイコン( )が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細で抑制を設定する方法:

ステップ 1　[抑制(Suppressions)] の横にある [追加(Add)] をクリックします。

[抑制の追加(Add Suppression)] ダイアログボックスが表示されます。

ステップ 2　[抑制タイプ(Suppression Type)] ドロップダウンリストから、次のいずれかのオプションを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[ルール(Rule)] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元(Source)] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先(Destination)] を選択します。

ステップ 3　抑制タイプに [送信元(Source)] または [宛先(Destination)] を選択した場合は、[ネットワーク(Network)] フィールドが表示されます。[ネットワーク(Network)] フィールドで、IP アドレス、アドレス ブロック、またはこれらを任意に組み合わせたカンマ区切りのリストを入力します。侵入ポリシーがアクセス コントロール ポリシーのデフォルト アクションに関連付けられている場合は、デフォルト アクション変数セットでネットワーク変数を指定または列挙することもできます。

IPv4 CIDR および IPv6 プレフィックス長アドレス ブロックを使用する方法については、IP アドレスの表記規則(1-4 ページ)を参照してください。

ステップ 4　[OK] をクリックします。

システムが、抑制条件を追加し、抑制するルールの横にある [イベント フィルタリング(Event Filtering)] カラムのルールの横にイベント フィルタ アイコン( )を表示します。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

ルールの動的ルール状態の設定

ライセンス：Protection

[ルールの詳細（Rule Detail）] ページで、ルールの 1 つまたは複数の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2 つの動的ルール状態が競合している場合は、最初のアクションが実行されることに注意してください。動的ルール状態の詳細については、動的ルール状態について（24-31 ページ）を参照してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細で動的ルール状態を設定する方法：

ステップ 1　[動的状態（Dynamic State）] の横にある [追加（Add）] をクリックします。

[レート ベースのルール状態の追加（Add Rate-Based Rule State）] ダイアログボックスが表示されます。

ステップ 2　[追跡対象（Track By）] ドロップダウンリストから、ルール一致の追跡方法を指定するオプションを選択します。

- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[送信元（Source）] を選択します。
- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[宛先（Destination）] を選択します。
- そのルールのすべての一致を追跡する場合は、[ルール（Rule）] を選択します。

ステップ 3　オプションで、[追跡対象（Track By）] を [送信元（Source）] または [宛先（Destination）] に設定した場合は、[ネットワーク（Network）] フィールドに追跡する各ホストの IP アドレスを入力します。

IPv4 CIDR および IPv6 プレフィックス長表記を使用する方法については、IP アドレスの表記規則（1-4 ページ）を参照してください。

ステップ 4　[レート（Rate）] の隣で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [カウント（Count）] フィールドで、0 ～ 2147483647 の整数を使用して、しきい値として使用するルール一致の数を指定します。
- [秒（Seconds）] フィールドで、0 ～ 2147483647 の整数を使用して、攻撃を追跡する期間を表す秒数を指定します。

ステップ 5　[新しい状態（New State）] ドロップダウンリストから、条件が満たされたときに実行すべき新しいアクションを選択します。

- イベントを生成する場合は、[イベントを生成する（Generate Events）] を選択します。
- インライン展開でイベントを生成し、イベントをトリガーしたパケットを破棄する場合、または、パッシブ展開でイベントを生成する場合は、[ドロップしてイベントを生成する（Drop and Generate Events）] を選択します。
- アクションを実行しない場合は、[無効（Disabled）] を選択します。

ステップ 6　[タイムアウト（Timeout）] フィールドに、1 ～ 2147483647（約 68 年）の整数を使用して、新しいアクションを有効にしておく秒数を入力します。タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションがタイムアウトしないようにする場合は、0 を指定します。

ステップ 7　[OK] をクリックします。

システムが、動的ルール状態を追加し、[動的状態（Dynamic State）] カラムのルールの横に動的状態アイコン（ ）を表示します。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

必須フィールドを空白にした場合は、フィールドに値を入力する必要があることを伝えるエラー メッセージが表示されます。

ルールの SNMP アラートの設定

ライセンス：Protection

[ルールの詳細（Rule Detail）] ページで、ルールの SNMP アラートを設定できます。SNMP アラートの詳細については、SNMP アラートの追加（24-34 ページ）を参照してください。

ルール詳細で **SNMP** アラートを追加する方法：

ステップ 1　[アラート（Alerts）] の横にある [SNMP アラートの追加（Add SNMP Alert）] をクリックします。

システムが、アラートを追加し、[アラート（Alerting）] カラムのルールの横にアラート アイコン（ ）を表示します。ルールに複数のアラートを追加した場合は、アイコン上にアラートの数が表示されます。

ルールに関するルール コメントの追加

ライセンス：Protection

[ルールの詳細（Rule Detail）] ページで、ルールに関するルール コメントを追加できます。ルール コメントの詳細については、ルール コメントの追加（24-35 ページ）を参照してください。

ルール詳細でコメントを追加する方法：

ステップ 1　[コメント（Comments）] の横にある [追加（Add）] をクリックします。

[コメントの追加（Add Comment）] ダイアログボックスが表示されます。

ステップ 2　[コメント（Comments）] フィールドに、ルール コメントを入力します。

ステップ 3　[OK] をクリックします。

システムが、コメントを追加し、[コメント（Comments）] カラムのルールの横にコメント アイコン（ ）を表示します。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

ヒント　ルール コメントを削除するには、ルール コメント セクションで [削除（Delete）] をクリックします。侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけ、コメントを削除できることに注意してください。侵入ポリシーの変更がコミットされた後は、ルール コメントを削除できなくなります。

侵入ポリシー内のルールのフィルタリング

ライセンス：Protection

[ルール（Rules）] ページに表示するルールは、1 つの基準または 1 つ以上の基準の組み合わせに基づいてフィルタ処理できます。

作成したフィルタが [フィルタ（Filter）] テキストボックスに表示されます。フィルタ パネルでキーワードとキーワード引数をクリックしてフィルタを作成できます。複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[カテゴリ（Category）] で [プリプロセッサ（preprocessor）] を選択してから、[ルール コンテンツ（Rule Content）] > [GID] の順に選択して、「116」と入力すると、プリプロセッサ ルールで、かつ、GID が 116 のすべてのルールを取得する「`Category:"preprocessor" GID:"116"`」というフィルタが返されます。

[カテゴリ（Category）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[プラットフォーム特有（Platform Specific）]、[プリプロセッサ（Preprocessor）]、および [優先度（Priority）] の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、Shift キーを押しながら、[カテゴリ（Category）] から [os-linux] と [os-windows] を選択すれば、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,os-linux"`」というフィルタを作成できます。

フィルタ パネルを表示するには、表示アイコン（  ）をクリックします。

フィルタ パネルを非表示にするには、非表示アイコン（  ）をクリックします。

詳細は、次のトピックを参照してください。

- 侵入ポリシー内のルール フィルタリングについて（24-10 ページ）
- 侵入ポリシー内のルール フィルタの設定（24-19 ページ）

侵入ポリシー内のルール フィルタリングについて

ライセンス：Protection

ルール フィルタ キーワードは、ルール状態やイベント フィルタなどのルール設定を適用するルールを見つけやすくします。[ルール（Rules）] ページのフィルタ パネルで必要な引数を選択することによって、キーワードでフィルタ処理すると同時に、キーワードの引数を選択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。

- 侵入ポリシー ルール フィルタを作成するためのガイドライン（24-10 ページ）
- ルール構成フィルタについて（24-13 ページ）
- ルール コンテンツ フィルタについて（24-15 ページ）
- ルール カテゴリについて（24-18 ページ）
- ルール フィルタの直接編集（24-18 ページ）

侵入ポリシー ルール フィルタを作成するためのガイドライン

ライセンス：Protection

ほとんどの場合、フィルタを作成するときに、侵入ポリシー内の [ルール（Rules）] ページの左側にあるフィルタ パネルを使用して必要なキーワード/引数を選択できます。

フィルタ パネルでは、ルール フィルタがルール フィルタ グループに分類されます。多くのルール フィルタ グループにサブ基準が含まれているため、探している特定のルールを簡単に見つけることができます。一部のルール フィルタには、展開して個別のルールにドリルダウンするための複数のレベルが設定されています。

フィルタ パネル内の項目は、場合によって、フィルタ タイプ グループを表したり、キーワードを表したり、キーワードの引数を表したりします。次の経験則をフィルタの作成に役立ててください。

- キーワード（[ルール設定（Rule Configuration）]、[ルール コンテンツ（Rule Content）]、[プラットフォーム特有（Platform Specific）]、および [優先度（Priority）]）以外のフィルタ タイプ グループ見出しを選択すると、そのグループが展開されて使用可能なキーワードが一覧表示されます。

  基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定するためのポップアップ ウィンドウが表示されます。

  そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

- キーワード（[カテゴリ（Category）]、[分類（Classifications）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[優先度（Priority）]、および [ルール アップデート（Rule Update）]）になっているフィルタ タイプ グループ見出しを選択すると、使用可能な引数が一覧表示されます。

  このタイプのグループから項目を選択すると、適用される引数とキーワードがすぐにフィルタに追加されます。キーワードがすでにフィルタ内に存在していた場合は、そのグループに対応するキーワードの既存の引数が置き換えられます。

  たとえば、フィルタ パネルの [カテゴリ（Category）] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキストボックスに追加されます。その後で、[カテゴリ（Category）] で [os-windows] をクリックすると、フィルタが「`Category:"os-windows"`」に変更されます。

- [ルール コンテンツ（Rule Content）] の下の [参照（Reference）] はキーワードであり、その下に特定の参照 ID タイプが列挙されます。参照キーワードのいずれかを選択すると、引数を指定するためのポップアップ ウィンドウが表示され、キーワードが既存のフィルタに追加されます。キーワードがすでにフィルタ内で使用されていた場合は、既存の引数が指定した新しい引数に置き換えられます。

  たとえば、フィルタ パネルで [ルール コンテンツ（Rule Content）] > [参照（Reference）] > [CVE ID] の順にクリックすると、ポップアップ ウィンドウが開いて CVE ID を指定するよう求められます。「`2007`」と入力すると、「`CVE:"2007"`」がフィルタ テキストボックスに追加されます。別の例では、フィルタ パネルで [ルール コンテンツ（Rule Content）] > [参照（Reference）] の順にクリックすると、ポップアップ ウィンドウが開いて、参照を指定するよう求められます。「`2007`」と入力すると、「`Reference:"2007"`」がフィルタ テキストボックスに追加されます。

- 複数のグループからルール フィルタ キーワードを選択した場合は、各フィルタ キーワードがフィルタに追加され、既存のキーワードが維持されます（同じキーワードの新しい値で上書きされなかった場合）。

  たとえば、フィルタ パネルの [カテゴリ（Category）] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキストボックスに追加されます。その後で、[Microsoft 脆弱性（Microsoft Vulnerabilities）] で [MS00-006] をクリックすると、フィルタが「`Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`」に変更されます。

- 複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[カテゴリ（Category）] で [プリプロセッサ（preprocessor）] を選択してから、[ルール コンテンツ（Rule Content）] > [GID] の順に選択して、「`116`」と入力すると、プリプロセッサ ルールで、かつ、GID が 116 のすべてのルールを取得する「`Category:"preprocessor" GID:"116"`」というフィルタが返されます。

- [カテゴリ（Category）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[プラットフォーム特有（Platform Specific）]、および [優先度（Priority）] の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、Shift キーを押しながら、[カテゴリ（Category）] から [os-linux] と [os-windows] を選択すれば、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,app-detect"`」というフィルタを作成できます。

複数のフィルタ キーワード/引数のペアで同じルールが取得される場合があります。たとえば、ルールが **dos** カテゴリでフィルタ処理された場合と **High** 優先度でフィルタ処理された場合はともに、DOS Cisco attempt rule（SID 1545）が表示されます。

（注）　シスコ VRT がルール更新メカニズムを使用してルール フィルタを追加または削除する場合があります。

[ルール（Rules）] ページ上のルールは、共有オブジェクトのルール（ジェネレータ ID 3）と標準テキスト ルール（ジェネレータ ID 1）のどちらかであることに注意してください。次の表に、さまざまなルール フィルタの説明を示します。

表 **24-4**　ルール フィルタ グループ

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
ルール設定（Rule Configuration）	ルールの設定に基づいてルールを検索します。ルール構成フィルタについて（24-13 ページ）を参照してください。	なし	グループ	キーワード
ルール コンテンツ（Rule Content）	ルールの内容に基づいてルールを検索します。ルール コンテンツ フィルタについて（24-15 ページ）を参照してください。	なし	グループ	キーワード
カテゴリ（Category）	ルール エディタで使用されるルール カテゴリに基づいてルールを検索します。ローカル ルールはローカル サブグループに表示されることに注意してください。ルール カテゴリについて（24-18 ページ）を参照してください。	○	キーワード	引数
分類（Classifications）	ルールによって生成されるイベントのパケット画面内に表示される攻撃分類に基づいてルールを検索します。侵入イベント分類の定義（27-13 ページ）を参照してください。	なし	キーワード	引数
Microsoft 脆弱性（Microsoft Vulnerabilities）	Microsoft セキュリティ情報番号に従ってルールを検索します。	○	キーワード	引数
Microsoft ワーム（Microsoft Worms）	Microsoft Windows ホストに影響する特定のワームに基づいてルールを検索します。	○	キーワード	引数
プラットフォーム特有（Platform Specific）	オペレーティング システムの特定のバージョンとの関連性に基づいてルールを検索します。 ルールが複数のオペレーティング システムまたは 1 つのオペレーティング システムの複数のバージョンに影響する場合があることに注意してください。たとえば、SID 2260 を有効にすると、Mac OS X、IBM AIX、およびその他のオペレーティング システムの複数のバージョンに影響します。	○	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。

表 **24-4**　ルール フィルタ グループ（続き）

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
プリプロセッサ（Preprocessors）	個別のプリプロセッサのルールを検索します。 プリプロセッサが有効になっている場合にプリプロセッサ オプションに対するイベントを生成するためには、そのオプションに関連付けられたプリプロセッサ ルールを有効にする必要があることに注意してください。ルール状態の設定（24-21 ページ）を参照してください。	○	グループ	サブグループ
[プライオリティ（Priority）]	高、中、および低の優先度に基づいてルールを検索します。 ルールに割り当てられた分類によってその優先度が決定されます。これらのグループは、さらにルール カテゴリに分類されます。ローカル ルール（つまり、ユーザが作成したルール）は優先度グループに表示されないことに注意してください。	○	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
ルール アップデート（Rule Update）	特定のルール更新を通して追加または変更されたルールを検索します。ルール更新ごとに、更新内のすべてのルール、更新でインポートされた唯一の新しいルール、または更新によって変更された唯一の既存のルールを表示します。	なし	キーワード	引数

ルール構成フィルタについて

ライセンス：Protection

[ルール（Rules）] ページに表示されたルールをいくつかのルール構成設定でフィルタ処理できます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定するためのポップアップ ウィンドウが表示されます。

そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

フィルタ処理に使用可能なルール構成設定に関する詳細については、次の手順を参照してください。

ルール状態フィルタを使用する方法：

ステップ **1**　[ルール設定（Rule Configuration）] で、[ルール状態（Rule State）] をクリックします。

ステップ **2**　[ルール状態（Rule State）] ドロップダウンリストから、フィルタ条件のルール状態を選択します。

- イベントを生成するだけのルールを検索するには、[イベントを生成する（Generate Events）] を選択して、[OK] をクリックします。
- イベントを生成して一致するパケットをドロップするよう設定されたルールを検索するには、[ドロップしてイベントを生成する（Drop and Generate Events）] を選択して、[OK] をクリックします。
- 無効になっているルールを検索するには、[無効（Disabled）] を選択して、[OK] をクリックします。

最新のルール状態に基づいてルールを表示するように [ルール（Rules）] ページが更新されます。

しきい値フィルタを使用する方法:

ステップ 1　[ルール設定(Rule Configuration)] で、[しきい値(Threshold)] をクリックします。

ステップ 2　[しきい値(Threshold)] ドロップダウンリストから、フィルタ条件のしきい値設定を選択します。

- しきい値タイプが `limit` のルールを検索するには、[制限(Limit)] を選択して、[OK] をクリックします。
- しきい値タイプが `threshold` のルールを検索するには、[しきい値(Threshold)] を選択して、[OK] をクリックします。
- しきい値タイプが `both` のルールを検索するには、[両方(Both)] を選択して、[OK] をクリックします。
- しきい値が `source` によって追跡されるルールを検索するには、[送信元(Source)] を選択して、[OK] をクリックします。
- しきい値が `Destination` によって追跡されるルールを検索するには、[宛先(Destination)] を選択して、[OK] をクリックします。
- しきい値が設定された任意のルールを検索するには、[すべて(All)] を選択して、[OK] をクリックします。

フィルタで指定されたしきい値のタイプがルールに適用されているルールを表示するように [ルール(Rules)] ページが更新されます。

抑制フィルタを使用する方法:

ステップ 1　[ルール設定(Rule Configuration)] で、[抑制(Suppression)] をクリックします。

ステップ 2　[抑制(Suppression)] ドロップダウンリストから、フィルタ条件の抑制設定を選択します。

- イベントがそのルールによって検査されるパケットに抑制されたルールを検索するには、[ルール別(By Rule)] を選択して、[OK] をクリックします。
- イベントがトラフィックの送信元に基づいて抑制されるルールを検索するには、[送信元別(By Source)] を選択して、[OK] をクリックします。
- イベントがトラフィックの宛先に基づいて抑制されるルールを検索するには、[宛先別(By Destination)] を選択して、[OK] をクリックします。
- 抑制が設定された任意のルールを検索するには、[すべて(All)] を選択して、[OK] をクリックします。

フィルタで指定された抑制のタイプがルールに適用されているルールを表示するように [ルール(Rules)] ページが更新されます。

動的状態フィルタを使用する方法:

ステップ 1　[ルール設定(Rule Configuration)] で、[動的状態(Dynamic State)] をクリックします。

ステップ 2　[動的状態(Dynamic State)] ドロップダウンリストから、フィルタ条件の抑制設定を選択します。

- 動的状態がそのルールによって検査されるパケットに設定されたルールを検索するには、[ルール別(By Rule)] を選択して、[OK] をクリックします。
- 動的状態がトラフィックの送信元に基づくパケットに設定されたルールを検索するには、[送信元別(By Source)] を選択して、[OK] をクリックします。

- 動的状態がトラフィックの宛先に基づいて設定されたルールを検索するには、[宛先別（By Destination）] を選択して、[OK] をクリックします。
- `Generate Events` の動的状態が設定されたルールを検索するには、[イベントを生成する（Generate Events）] を選択して、[OK] をクリックします。
- `Drop and Generate Events` の動的状態が設定されたルールを検索するには、[ドロップしてイベントを生成する（Drop and Generate Events）] を選択して、[OK] をクリックします。
- `Disabled` の動的状態が設定されたルールを検索するには、[無効（Disabled）] を選択して、[OK] をクリックします。
- 抑制が設定された任意のルールを検索するには、[すべて（All）] を選択して、[OK] をクリックします。

フィルタで指定された動的ルール状態がルールに適用されているルールを表示するように [ルール（Rules）] ページが更新されます。

アラート フィルタの使用方法:

ステップ **1**　[ルール設定（Rule Configuration）] で、[アラート（Alert）] をクリックします。

ステップ **2**　[アラート（Alert）] ドロップダウンリストから、**SNMP** 別にフィルタ処理するアラート設定を選択します。

ステップ **3**　[OK] をクリックします。

[ルール（Rules）] ページが更新され、アラート フィルタを適用したルールが表示されます。

コメント フィルタを使用する方法:

ステップ **1**　[ルール設定（Rule Configuration）] で、[コメント（Comment）] をクリックします。

ステップ **2**　[コメント（Comment）] フィールドに、フィルタ条件のコメント テキスト文字列を入力し、[OK] をクリックします。

ルールに適用されるコメントにフィルタで指定された文字列が含まれているルールを表示するように [ルール（Rules）] ページが更新されます。

ルール コンテンツ フィルタについて

ライセンス：Protection

[ルール（Rules）] ページに表示されたルールをいくつかのルール コンテンツ項目でフィルタ処理できます。たとえば、ルールの SID を検索することによって、ルールをすばやく取得できます。特定の宛先ポートに送信されるトラフィックを検査するすべてのルールを検索することもできます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定するためのポップアップ ウィンドウが表示されます。

そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [ルール コンテンツ（Rule Content）] で [SID] をクリックすると、ポップアップ ウィンドウが開いて SID の入力が促されます。「1045」と入力すると、「SID:"1045"」がフィルタ テキストボックスに追加されます。その後で、再度 [SID] をクリックして、SID フィルタを「1044」に変更すると、フィルタが「SID:"1044"」に変更されます。

フィルタ処理に使用可能なルール コンテンツの詳細については、次の表を参照してください。

表 **24-5**　ルール コンテンツ フィルタ

このフィルタを使用する場合のクリック対象	次の操作	結果
メッセージ	フィルタ条件のメッセージ文字列を入力して、[OK] をクリックします。	メッセージ フィールドで指定された文字列を含むルールを検索します。
SID	フィルタ条件の SID 番号を入力して、[OK] をクリックします。	指定された SID が割り当てられたルールを検索します。
GID	フィルタ条件の GID 番号を入力して、[OK] をクリックします。	指定された GID が割り当てられたルールを検索します。
参照	フィルタ条件の参照文字列を入力して、[OK] をクリックします。 フィルタ条件とする特定のタイプの参照に対する文字列を入力するには、[CVE ID]、[URL]、[Bugtraq ID]、[Nessus ID]、[Arachnids ID]、または [Mcafee ID] を選択し、文字列を入力して [OK] をクリックします。	参照フィールドで指定された文字列を含むルールを検索します。
アクション	フィルタ処理するアクションを選択します。 • アラート ルールを検索するには、[アラート（Alert）] を選択して、[OK] をクリックします。 • パス ルールを検索するには、[パス（Pass）] を選択して、[OK] をクリックします。	alert または pass で始まるルールを検索します。
プロトコル	フィルタ条件のプロトコル（[ICMP]、[IP]、[TCP]、または [UDP]）を選択し、[OK] をクリックします。	選択されたプロトコルを含むルールを検索します。
方向	フィルタ処理する方向設定を選択します。 • 特定の方向に移動するトラフィックを検査するルールを検索するには、[指向性（Directional）] を選択して、[OK] をクリックします。 • 送信元と宛先の間をどちらの方向にも移動するトラフィックを検査するルールを検索するには、[双方向（Bidirectional）] を選択して、[OK] をクリックしてします。	ルールに、指定された方向設定が含まれているかどうかに基づいてルールを検索します。

表 24-5　ルール コンテンツ フィルタ（続き）

このフィルタを使用する場合のクリック対象	次の操作	結果
ソース IP	フィルタ条件の送信元 IP アドレスを入力して、[OK] をクリックします。 有効な IP アドレス、CIDR ブロック/プレフィックス長、または $HOME_NET や $EXTERNAL_NET などの変数を使用してフィルタ処理できることに注意してください。	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用するルールを検索します。
宛先 IP（Destination IP）	フィルタ条件の宛先 IP アドレスを入力して、[OK] をクリックします。 有効な IP アドレス、CIDR ブロック/プレフィックス長、または $HOME_NET や $EXTERNAL_NET などの変数を使用してフィルタ処理できることに注意してください。	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用するルールを検索します。
ソース ポート	フィルタ条件の送信元ポートを入力して、[OK] をクリックします。 ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。	指定された送信元ポートを含むルールを検索します。
接続先ポート（Destination port）	フィルタ条件の宛先ポートを入力して、[OK] をクリックします。 ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。	指定された宛先ポートを含むルールを検索します。
ルールのオーバーヘッド	フィルタ条件のルール オーバーヘッドの量（[低（Low）]、[中（Medium）]、[高（High）]、または [非常に高い（Very High）]）を選択し、[OK] をクリックします。	選択されたルール オーバーヘッドを伴うルールを検索します。
メタデータ	フィルタ条件のメタデータのキーと値のペアをスペースで区切って入力し、[OK] をクリックします。 たとえば、HTTP アプリケーション プロトコルに関連するメタデータを使用したルールを検索するには、「metadata:"service http"」と入力します。	一致するキーと値のペアを含むメタデータを使用したルールを検索します。

ルール カテゴリについて

ライセンス：Protection

ASA FirePOWER モジュールは、ルールが検出するトラフィックのタイプに基づいてカテゴリにルールを配置します。[ルール（Rules）] ページで、ルール カテゴリでフィルタ処理することによって、カテゴリ内のすべてのルールにルール属性を設定できます。たとえば、ネットワーク上に Linux ホストが存在しない場合は、**os-linux** カテゴリでフィルタ処理してから、表示されたすべてのルールを無効にすることによって、**os-linux** カテゴリ全体を無効にすることができます。

（注）　シスコ VRT がルール更新メカニズムを使用してルール カテゴリを追加または削除する場合があります。

ルール フィルタの直接編集

ライセンス：Protection

フィルタ パネルでフィルタをクリックしたときに入力される特殊なキーワードとその引数を変更するようにフィルタを編集できます。[ルール（Rules）] ページのカスタム フィルタはルール エディタで使用されるものと同様に機能しますが、フィルタ パネルを通してフィルタを選択したときに表示される構文を使用して、[ルール（Rules）] ページのフィルタに入力されたキーワードのいずれかを使用することもできます。今後使用するキーワードを決定するには、右側のフィルタ パネルで該当する引数をクリックします。フィルタ キーワードと引数構文がフィルタ テキストボックスに表示されます。

特定の値のみをサポートするキーワードの引数のリストを表示するには、ルール構成フィルタについて（24-13 ページ）、ルール コンテンツ フィルタについて（24-15 ページ）、およびルール カテゴリについて（24-18 ページ）を参照してください。キーワードのカンマ区切りの複数の引数は [カテゴリ（Category）] と [優先度（Priority）] のフィルタ タイプでしかサポートされないことに注意してください。

引用符内のキーワードと引数、文字列、およびリテラル文字列と一緒に、複数のフィルタ条件を区切るスペースを使用できます。ただし、正規表現、ワイルドカード文字、および否定文字（!）、「大なり」記号（>）、「小なり」記号（<）などの特殊な演算子をフィルタに含めることはできません。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[カテゴリ（Category）]、[メッセージ（Message）]、および [SID] の各フィールドで指定された単語が検索されます。

すべてのキーワード、キーワード引数、および文字列では大文字と小文字が区別されません。`gid` キーワードと `sid` キーワードを除くすべての引数と文字列が部分文字列として扱われます。`gid` と `sid` の引数は、完全一致のみを返します。

各ルール フィルタに、次の形式で 1 つ以上のキーワードを含めることができます。

`Keyword``:"`*`argument`*`"`

ここで、*`Keyword`* はルール タイプの表に示すフィルタ グループ内のキーワードのいずれかで、*`argument`* は二重引用符で囲まれ、キーワードに関連した特定のフィールド内で検索される単一の大文字と小文字が区別されない英数字文字列です。キーワードは先頭文字を大文字にして入力する必要があることに注意してください。

`gid` と `sid` を除くすべてのキーワードの引数が部分文字列として扱われます。たとえば、引数 `123` によって `"12345"`、`"41235"`、`"45123"` などが返されます。`gid` と `sid` の引数は完全一致のみを返します。たとえば、`sid:3080` は `SID 3080` のみを返します。

各ルール フィルタに、1 つ以上の英数字文字列を含めることもできます。文字列はルールの [メッセージ（Message）] フィールド、シグニチャ ID、およびジェネレータ ID を検索します。たとえば、文字列 `123` は、ルール メッセージ内の文字列 `"Lotus123"` や `"123mania"` などを返し、`SID 6123` や `SID 12375` なども返します。ルールの [メッセージ（Message）] フィールドの詳細については、イベント メッセージの定義（27-12 ページ）を参照してください。部分的な SID を検索するには、1 つ以上の文字列を使ってフィルタ処理できます。

すべての文字列では大文字と小文字が区別されず、部分的な文字列として扱われます。たとえば、文字列 `ADMIN`、`admin`、または `Admin` はすべて、`"admin"`、`"CFADMIN"`、`"Administrator"` などを返します。

文字列を引用符で囲むと、完全一致を返すことができます。たとえば、引用符付きのリテラル文字列 `"overflow attempt"` は完全一致のみを返しますが、引用符なしの 2 つの文字列 `overflow` と `attempt` で構成されるフィルタは `"overflow attempt"`、`"overflow multipacket attempt"`、`"overflow with evasion attempt"` などを返します。

複数のキーワード、文字列、またはその両方をスペースで区切って任意に組み合わせて入力することで、フィルタ結果を絞り込むことができます。結果には、すべてのフィルタ条件に一致するルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のフィルタはそれぞれ同じルールを返します。

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

侵入ポリシー内のルール フィルタの設定

ライセンス：Protection

[ルール（Rules）] ページで、ルールのサブセットを表示するようにルールをフィルタ処理できます。その後、任意のページ機能を使用できます。これは、特定のカテゴリのすべてのルールのしきい値を設定する場合などに便利です。フィルタ処理されている場合もされていない場合も、リスト内のルールで同じ機能を使用できます。たとえば、新しいルール状態を、フィルタ処理されたリスト内のルールまたはフィルタ処理されていないリスト内のルールに適用できます。

侵入ポリシー内の [ルール（Rules）] ページの左側にあるフィルタ パネルから事前定義のフィルタ キーワードを選択できます。フィルタを選択すると、ページに、すべての一致するルールが表示されるか、どのルールも一致しなかったことが表示されます。

使用可能なすべてのキーワードと引数の詳細と、フィルタ パネルでのフィルタの作成方法については、侵入ポリシー内のルール フィルタリングについて（24-10 ページ）を参照してください。

フィルタにキーワードを追加してさらに絞り込むことができます。入力されたフィルタは、ルール データベース全体を検索して、一致するすべてのルールを返します。前回のフィルタ結果がページに表示されている状態でフィルタを入力すると、そのページの内容が消去され、代わりに新しいフィルタの結果が返されます。

また、フィルタを選択したとき、または、フィルタを選択後にその中の引数値を変更したときに指定したものと同じキーワードと引数の構文を使用してフィルタを入力することもできます。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[カテゴリ（Category）]、[メッセージ（Message）]、および [SID] の各フィールドで指定された単語が検索されます。

侵入ポリシー内の特定のルールに対してフィルタ処理する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 3　[ルール(Rules)] をクリックします。

[ルール(Rules)] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。フィルタ内に存在するキーワードの引数をクリックすると、既存の引数が置き換えられることに注意してください。詳細については、次の各項を参照してください。

- 侵入ポリシー ルール フィルタを作成するためのガイドライン(24-10 ページ)
- ルール構成フィルタについて(24-13 ページ)
- ルール コンテンツ フィルタについて(24-15 ページ)
- ルール カテゴリについて(24-18 ページ)
- ルール フィルタの直接編集(24-18 ページ)

ページが、すべての一致するルールを表示するように更新され、フィルタと一致するルールの数がフィルタ テキストボックスの上に表示されます。

ステップ 5　新しい設定を適用する 1 つ以上のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

ステップ 6　オプションで、ページに表示されているルールを通常の方法で変更します。詳細については、次の各項を参照してください。

- [ルール(Rules)] ページ上でルールを有効または無効にする方法については、ルール状態の設定(24-21 ページ)を参照してください。
- ルールにしきい値設定と抑制を追加する方法については、ポリシー単位の侵入イベント通知のフィルタリング(24-23 ページ)を参照してください。
- 一致するトラフィックでレート異常が発生したときにトリガーされる動的ルール状態を設定する方法については、動的ルール状態の追加(24-31 ページ)を参照してください。
- SNMP アラートを特定のルールに追加する方法については、SNMP アラートの追加(24-34 ページ)を参照してください。
- ルールにルール コメントを追加する方法については、ルール コメントの追加(24-35 ページ)を参照してください。

ステップ 7　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理(23-3 ページ)」と「侵入ポリシーの編集(23-4 ページ)」を参照してください。

ルール状態の設定

ライセンス：Protection

シスコ脆弱性調査チーム（VRT）が、各デフォルト ポリシー内の侵入ルールとプリプロセッサ ルールのデフォルト状態を設定します。たとえば、ルールを Security over Connectivity デフォルト ポリシーでは有効にして、Connectivity over Security デフォルト ポリシーでは無効にすることができます。作成された侵入ポリシー ルールは、作成時に使用されたデフォルト ポリシー内のルールのデフォルト状態を継承します。

ルールを [イベントを生成する（Generate Events）]、[ドロップしてイベントを生成する（Drop and Generate Events）]、または [無効（Disable）] に個別に設定することも、状態を変更するルールを選択するためのさまざまな要素でルールをフィルタ処理することもできます。インライン展開では、インライン侵入展開で [ドロップしてイベントを生成する（Drop and Generate Events）] ルール状態を使用して悪意のあるパケットをドロップできます。[ドロップしてイベントを生成する（Drop and Generate Events）] ルール状態のルールはイベントを生成しますが、パッシブ展開ではパケットをドロップしないことに注意してください。ルールを [イベントを生成する（Generate Events）] または [ドロップしてイベントを生成する（Drop and Generate Events）] に設定すると、ルールが有効になります。ルールを [無効（Disable）] に設定すると、ルールが無効になります。

2 つのシナリオについて考えてみます。最初のシナリオでは、特定のルールのルール状態が [イベントを生成する（Generate Events）] に設定されます。悪意のあるパケットがネットワークを通過してルールをトリガーすると、そのパケットが宛先に送信され、システムが侵入イベントを生成します。2 つ目のシナリオでは、同じルールのルール状態が、インライン展開で [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていると仮定します。この場合は、悪意のあるパケットがネットワークを通過すると、システムがそのパケットをドロップして、侵入イベントを生成します。パケットがターゲットに到達することはありません。

侵入ポリシーでは、ルールの状態を次のいずれかに設定できます。

- システムで特定の侵入試行を検出して、一致したトラフィックが見つかった時点で侵入イベントを生成する場合は、ルール状態を [イベントを生成する（Generate Events）] に設定します。
- システムで特定の侵入試行を検出してから、インライン展開で一致するトラフィックが見つかった時点で攻撃を含むパケットをドロップし、侵入イベントを生成する場合、あるいは、パッシブ展開で一致するトラフィックが見つかった時点で侵入イベントを生成する場合は、ルール状態を [ドロップしてイベントを生成する（Drop and Generate Events）] に設定します。

  システムでパケットをドロップする場合は、インライン展開で侵入ポリシーを廃棄ルールに設定する必要があることに注意してください。詳細については、インライン展開でのドロップ動作の設定（23-6 ページ）を参照してください。
- システムで一致するトラフィックを評価しない場合は、ルール状態を [無効（Disable）] に設定します。

廃棄ルールを使用するには、次の手順を実行する必要があります。

- 侵入ポリシーで [インライン時にドロップ（Drop when Inline）] オプションを有効にします。
- ルールと一致するすべてのパケットをドロップする必要があるすべてのルールのルール状態を [ドロップしてイベントを生成する（Drop and Generate Events）] に設定します。
- 侵入ポリシーに関連付けられたアクセス コントロール ルールを含むアクセス コントロール ポリシーを、インライン展開に適用します。

[ルール（Rules）] ページのルールのフィルタ処理は、廃棄ルールとして設定するルールを探すときに役立ちます。詳細については、侵入ポリシー内のルールのフィルタリング（24-10 ページ）を参照してください。

ルール構造、ルール キーワードとそのオプション、およびルール作成構文については、侵入ルールの概要と作成（27-1 ページ）を参照してください。

VRT がルール更新を使用してデフォルト ポリシー内の 1 つ以上のルールのデフォルト状態を変更する場合があります。ルール更新での基本ポリシーの更新を許可すると、ポリシーの作成時に使用されたデフォルト ポリシー（または基礎となるデフォルト ポリシー）のデフォルト状態が変更されたときの、そのポリシー内のルールのデフォルト状態の変更も許可することになります。ただし、ルール状態を変更している場合は、ルール更新でその変更が上書きされないことに注意してください。

1 つ以上のルールのルール状態を変更する方法:

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ **2**　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

このページには、有効なルールの総数、[イベントを生成する（Generate Events）] に設定された有効なルールの総数、および [ドロップしてイベントを生成する（Drop and Generate Events）] に設定された有効なルールの総数が表示されることに注意してください。また、パッシブ展開では、[ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールで行われるのはイベントの生成のみであることにも注意してください。

ステップ **3**　[ルール（Rules）] をクリックします。

[ルール（Rules）] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ **4**　ルール状態を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて（24-10 ページ）および侵入ポリシー内のルール フィルタの設定（24-19 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ **5**　ルール状態を設定する 1 つ以上のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

ステップ **6**　次の選択肢があります。

- トラフィックが選択されたルールと一致したときにイベントを生成するには、[ルール状態（Rule State）] > [イベントを生成する（Generate Events）] の順に選択します。
- インライン展開でトラフィックが選択されたルールと一致したときにイベントを生成し、そのトラフィックをドロップするには、[ルール状態（Rule State）] > [ドロップしてイベントを生成する（Drop and Generate Events）] の順に選択します。
- 選択されたルールと一致するトラフィックを検査しないようにするには、[ルール状態（Rule State）] > [無効（Disable）] の順に選択します。

（注）　シスコでは、侵入ポリシー内のすべての侵入ルールを有効にしないことを強く推奨しています。すべてのルールが有効になっている場合は、デバイスのパフォーマンスが低下する可能性があります。代わりに、できるだけネットワーク環境に合わせてルール セットを調整してください。

ステップ 7　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、「侵入ポリシーの管理（23-3 ページ）」と「侵入ポリシーの編集（23-4 ページ）」を参照してください。

ポリシー単位の侵入イベント通知のフィルタリング

ライセンス：Protection

侵入イベントの重要度は、発生頻度、送信元 IP アドレス、または宛先 IP アドレスに基づいて設定できます。イベントが特定の回数発生するまで注意が必要ない場合もあります。たとえば、何者かがサーバにログインしようとしても、特定の回数失敗するまで、気にする必要はありません。一方、ほんの少数の発生を見れば、広範な問題があることを理解できる場合もあります。たとえば、Web サーバに対して DoS 攻撃が行われた場合は、少数の侵入イベントの発生を確認しただけで、その状況に対処しなければならないことが分かります。同じイベントが何百回も確認されれば、システムの機能が麻痺します。

詳細については、次の各項を参照してください。

- イベントしきい値の設定（24-23 ページ）では、発生回数に基づくイベントの表示頻度を指定するしきい値の設定方法について説明します。イベント単位およびポリシー単位でしきい値を設定できます。
- 侵入ポリシー単位の抑制の設定（24-28 ページ）では、指定されたイベントの通知を各ポリシー内の送信元 IP アドレス単位または宛先 IP アドレス単位で抑制する方法について説明します。

イベントしきい値の設定

ライセンス：Protection

指定された期間内にイベントが生成された回数に基づいて、システムが侵入イベントを記録して表示する回数を制限するための個別のルールのしきい値を侵入ポリシー単位で設定できます。これにより、大量の同じイベントが原因で機能が麻痺するのを避けることができます。しきい値は、共有オブジェクトのルール単位、標準テキスト ルール単位、またはプリプロセッサ ルール単位で設定できます。

詳細については、次の項を参照してください。

- イベントしきい値の設定について（24-24 ページ）
- 侵入イベントしきい値の追加と変更（24-25 ページ）
- 侵入イベントしきい値の表示と削除（24-27 ページ）
- ルールのしきい値の設定（24-6 ページ）

イベントしきい値の設定について

ライセンス：Protection

まず、しきい値タイプを指定する必要があります。次の表に示すオプションの中から選択できます。

表 ***24-6***　しきい値設定オプション

オプション	説明
制限（Limit）	指定された数のパケット（count 引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [制限（Limit）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。
しきい値（Threshold）	指定された数のパケット（count 引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [しきい値（Threshold）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[秒（Seconds）] と [カウント（Count）] のカウンタを 0 にリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。
両方	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [両方（Both）] に、[カウント（Count）] を 2 に、[秒（Seconds）] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される）。

次に、トラッキングを指定する必要があります。これにより、イベントしきい値が送信元 IP アドレス単位と宛先 IP アドレス単位のどちらで計算されるかが決まります。次の表の中から、システムがイベント インスタンスを追跡する方法を指定するためのオプションの 1 つを選択します。

表 ***24-7***　***IP*** しきい値設定オプション

オプション	説明
ソース（Source）	送信元 IP アドレス単位でイベント インスタンス カウントを計算します。
[接続先（Destination）]	宛先 IP アドレス単位でイベント インスタンス カウントを計算します。

最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 *24-8*　インスタンス/時間のしきい値設定オプション

オプション	説明
メンバー数(Count)	しきい値を満たすために必要な、追跡する IP アドレス単位で指定された期間単位のイベントインスタンスの数。
秒(Seconds)	カウントがリセットされるまでの秒数。しきい値タイプを [制限(limit)] に、トラッキングを [送信元 IP(Source IP)] に、[カウント(count)] を 10 に、[秒(seconds)] を 10 に設定した場合は、システムが指定された送信元ポートから 10 秒間に発生した最初の 10 のイベントを記録して表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。

侵入イベントのしきい値設定は、単独で使用することも、レート ベースの攻撃防御、detection_filter キーワード、および侵入イベント抑制のいずれかと組み合わせて使用することもできます。詳細については、動的ルール状態の追加(24-31 ページ)、イベントのフィルタリング(27-91 ページ)、および 侵入ポリシー単位の抑制の設定(24-28 ページ)を参照してください。

詳細については、次の各項を参照してください。

- 侵入イベントしきい値の追加と変更(24-25 ページ)
- ルールのしきい値の設定(24-6 ページ)
- 侵入イベントしきい値の表示と削除(24-27 ページ)

侵入イベントしきい値の追加と変更

ライセンス:Protection

1 つ以上の特定のルールのしきい値を設定できます。既存のしきい値設定を個別にまたは同時に変更することもできます。それぞれに 1 つずつのしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

しきい値設定の表示方法と削除方法については、侵入イベントしきい値の表示と削除(24-27 ページ)を参照してください。

また、すべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。詳細については、侵入イベント ロギングのグローバルな制限(26-1 ページ)を参照してください。

無効な値を入力するとフィールドに復元アイコン( )が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

イベントしきい値を追加または変更する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 3　[ルール(Rules)] をクリックします。

[ルール(Rules)] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　しきい値を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて(24-10 ページ)および侵入ポリシー内のルール フィルタの設定(24-19 ページ)を参照してください。

ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　しきい値を設定する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

ステップ 6　[イベント フィルタリング(Event Filtering)] > [しきい値(Threshold)] の順に選択します。

[しきい値(thresholding)] ポップアップ ウィンドウが表示されます。

ステップ 7　[タイプ(Type)] ドロップダウンリストから、設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベント インスタンス数に通知を制限する場合は、[制限(Limit)] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[しきい値(Threshold)] を選択します。
- 指定されたイベント インスタンス数後に期間あたり 1 回ずつ通知を提供する場合は、[両方(Both)] を選択します。

ステップ 8　[追跡対象(Track By)] ドロップダウンリストから、イベント インスタンスが送信元 IP アドレスまたは宛先 IP アドレスのどちらによって追跡されるかを選択します。

ステップ 9　[カウント(Count)] フィールドで、しきい値として使用するイベント インスタンスの数を指定します。

ステップ 10　[秒(Seconds)] フィールドで、イベント インスタンスを追跡する期間を表す秒数を指定します。

ステップ 11　[OK] をクリックします。

システムが、しきい値を追加し、[イベント フィルタリング(Event Filtering)] カラムのルールの横にイベント フィルタ アイコン( )を表示します。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がイベント フィルタの数を示します。

ステップ 12　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理(23-3 ページ)」と「侵入ポリシーの編集(23-4 ページ)」を参照してください。

侵入イベントしきい値の表示と削除

ライセンス：Protection

既存のしきい値設定を表示または削除することができます。[ルールの詳細（Rules Details）] ビューを使用してしきい値の既存の設定を表示することによって、それらがシステムに適切かどうかを確認できます。そうでない場合は、新しいしきい値を追加して既存の値を上書きすることができます。

すべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできることに注意してください。詳細については、侵入イベント ロギングのグローバルな制限（26-1 ページ）を参照してください。

しきい値を表示または削除する方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 3　[ルール（Rules）] をクリックします。

[ルール（Rules）] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　表示または削除する、しきい値が設定されたルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて（24-10 ページ）および侵入ポリシー内のルール フィルタの設定（24-19 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　表示または削除する、しきい値が設定された 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

ステップ 6　選択したルールのしきい値を削除するには、[イベント フィルタリング（Event Filtering）] > [しきい値の削除（Remove Thresholds）] の順に選択します。表示される確認のポップアップ ウィンドウで [OK] をクリックします。

ヒント　特定のしきい値を削除するために、ルールを強調表示して、[詳細の表示（Show Details）] をクリックすることもできます。しきい値設定を展開して、削除するしきい値設定の横にある [削除（Delete）] をクリックします。[OK] をクリックして、設定の削除を確認します。

ページが更新され、しきい値が削除されます。

ステップ 7　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、「侵入ポリシーの管理（23-3 ページ）」と「侵入ポリシーの編集（23-4 ページ）」を参照してください。

侵入ポリシー単位の抑制の設定

ライセンス：Protection

特定の IP アドレスまたは IP アドレスの範囲が特定のルールまたはプリプロセッサをトリガーしたときの侵入イベント通知を抑制できます。これは、誤検出を回避するのに役立ちます。たとえば、特定のエクスプロイトのように見えるパケットを伝送しているメール サーバが存在する場合は、そのメール サーバによってトリガーとして使用されたイベントに関するイベント通知を抑制できます。ルールはすべてのパケットに対してトリガーとして使用されますが、本物の攻撃に対するイベントだけが表示されます。

侵入イベント抑制は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベントしきい値構成のいずれかと組み合わせて使用することもできることに注意してください。詳細については、動的ルール状態の追加（24-31 ページ）、イベントのフィルタリング（27-91 ページ）、および イベントしきい値の設定（24-23 ページ）を参照してください。

詳細については、次の各項を参照してください。

- 侵入イベントの抑制（24-28 ページ）
- 抑制条件の表示と削除（24-30 ページ）

侵入イベントの抑制

ライセンス：Protection

ルールに関する侵入イベント通知を抑制できます。ルールに関する通知が抑制されると、ルールはトリガーとして使用されますが、イベントは生成されません。ルールの 1 つまたは複数の抑制を設定できます。リスト内の最初の抑制に最も高いプライオリティが割り当てられます。2 つの抑制が競合している場合は、最初の抑制のアクションが実行されることに注意してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

イベント表示を抑制する方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 3　[ルール（Rules）] をクリックします。

[ルール（Rules）] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4　抑制を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて（24-10 ページ）および侵入ポリシー内のルール フィルタの設定（24-19 ページ）を参照してください。

ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　抑制条件を設定する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

ステップ 6　[イベント フィルタリング（Event Filtering）] > [抑制（Suppression）] の順に選択します。

[抑制（suppression）] ポップアップ ウィンドウが表示されます。

ステップ 7　次の [抑制タイプ（Suppression Type）] オプションのいずれかを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[ルール（Rule）] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元（Source）] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先（Destination）] を選択します。

ステップ 8　抑制タイプとして [送信元（Source）] または [宛先（Destination）] を選択した場合は、[ネットワーク（Network）] フィールドに、IP アドレス、アドレス ブロック、または送信元 IP アドレスまたは宛先 IP アドレスとして指定する変数、あるいは、これらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。

IPv4 CIDR および IPv6 プレフィックス長アドレス ブロックを使用する方法については、IP アドレスの表記規則（1-4 ページ）を参照してください。

ステップ 9　[OK] をクリックします。

システムが、抑制条件を追加し、抑制するルールの横にある [イベント フィルタリング（Event Filtering）] カラムのルールの横にイベント フィルタ アイコン（  ）を表示します。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がイベント フィルタの数を示します。

ステップ 10　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理（23-3 ページ）」と「侵入ポリシーの編集（23-4 ページ）」を参照してください。

抑制条件の表示と削除

ライセンス：Protection

既存の抑制条件を表示または削除することもできます。たとえば、メール サーバがエクスプロイトのように見えるパケットを普段から送信しているという理由で、そのメール サーバの IP アドレスから送信されたパケットに関するイベント通知を抑制できます。その後、そのメール サーバが使用停止になり、その IP アドレスが別のホストに再割り当てされたら、その送信元 IP アドレスの抑制条件を削除する必要があります。

定義された抑制条件を表示または削除する方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 3　[ルール（Rules）] をクリックします。

[ルール（Rules）] ページが表示されます。デフォルトで、ページにはルールがメッセージのアルファベット順に一覧表示されます。

ステップ 4　抑制を表示または削除するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて（24-10 ページ）および侵入ポリシー内のルール フィルタの設定（24-19 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　抑制を表示または削除する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

ステップ 6　次の 2 つの対処法があります。

- ルールのすべての抑制を削除するには、[イベント フィルタリング（Event Filtering）] > [抑制の削除（Remove Suppressions）] を選択します。表示される確認のポップアップ ウィンドウで [OK] をクリックします。
- 特定の抑制設定を削除するには、ルールを強調表示して、[詳細の表示（Show Details）] をクリックします。抑制設定を展開して、削除する抑制設定の横にある [削除（Delete）] をクリックします。[OK] をクリックして、選択した設定の削除を確認します。

ページが更新され、抑制設定が削除されます。

ステップ 7　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、「侵入ポリシーの管理（23-3 ページ）」と「侵入ポリシーの編集（23-4 ページ）」を参照してください。

動的ルール状態の追加

ライセンス：Protection

レート ベースの攻撃は、ネットワークまたはホストに過剰なトラフィックを送信することによって、低速化または正規の要求の拒否を引き起こし、ネットワークまたはホストを混乱させようとします。レート ベースの防御を使用して、特定のルールの過剰なルール一致に対応してルール アクションを変更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。

- 動的ルール状態について（24-31 ページ）
- 動的ルール状態の設定（24-32 ページ）

動的ルール状態について

ライセンス：Protection

侵入ポリシーにレート ベースのフィルタを含めることにより、一定期間においてルールの一致が過剰に発生した時点を検出できます。インライン展開されたデバイス上でこの機能を使用して、指定された時刻のレート ベースの攻撃をブロックしてから、ルール一致がイベントを生成するだけでトラフィックをドロップしないルール状態に戻すことができます。

レート ベースの攻撃防御は、異常なトラフィック パターンを識別し、正規の要求に対するそのトラフィックの影響を最小限に抑えようとします。特定の宛先 IP アドレスに送信されるトラフィックまたは特定の送信元 IP アドレスから送信されるトラフィックの過剰なルール一致を識別できます。また、検出されたすべてのトラフィックを通して特定のルールの過剰な一致に対処することもできます。

侵入ポリシーでは、侵入ルールまたはプリプロセッサ ルールのレート ベースのフィルタを設定できます。レート ベースのフィルタは次の 3 つの要素で構成されます。

- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率
- レートを超えた時点で実行される新しいアクション（[イベントを生成する（Generate Events）]、[ドロップしてイベントを生成する（Drop and Generate Events）]、および [無効（Disable）] の 3 種類がある）
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウトに達すると、レートがしきい値を下回っていれば、ルールのアクションがルールの初期設定に戻ります。

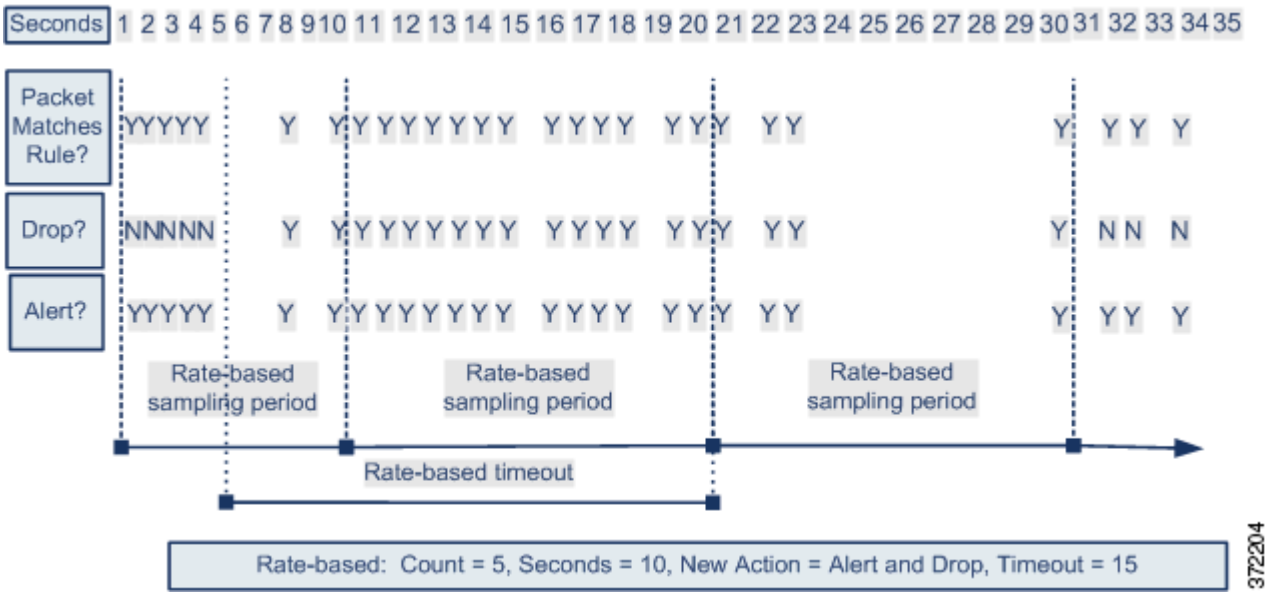
インライン展開のレート ベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レート ベースの設定を使用しない場合、[イベントを生成する（Generate Events）] に設定されたルールはイベントを生成しますが、システムはそのようなルールに関するパケットをドロップしません。ただし、攻撃トラフィックが、レート ベースの基準が設定されたルールと一致した場合は、そのようなルールが最初から [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていなかったとしても、レート アクションがアクティブな期間にパケットのドロップが実行されます。

（注）　レート ベースのアクションは、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

同じルールに対して複数のレート ベースのフィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレート ベースのフィルタ アクションが競合している場合は、最初のレート ベースのフィルタのアクションが実行されることに注意してください。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。パスワードを検出しようとする試行が繰り返されると、レート ベース攻撃防止が設定されたルールがトリガーされます。レート ベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [ドロップしてイベントを生成する（Drop and Generate Events）] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または過去のサンプリング期間のしきい値を上回っている場合は、新しいアクションが継続されます。新しいアクションは、サンプリング レートがしきい値レートを下回るサンプリング期間の終了後にのみ、[イベントを生成する（Generate Events）] に戻ります。



動的ルール状態の設定

ライセンス：Protection

ルールと一致したすべてのパケットをドロップするのではなく、指定された期間に特定の一致率に達した場合にルールと一致したパケットをドロップするために、ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] 状態に設定しない場合があります。動的ルール状態を使用すれば、ルールのアクションの変更をトリガーするレート、あるレートに達したときに変更すべきアクション、および新しいアクションの継続時間を設定できます。

アクションの変更をトリガーするために特定のヒット数が発生する必要のあるカウントと秒数を指定することによって、そのルールのヒット数を設定します。加えて、タイムアウトが発生したらアクションをルールの以前の状態に戻すタイムアウトを設定できます。

同じルールに対して複数の動的状態フィルタを定義できます。侵入ポリシー内のルール詳細に列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレート ベースのフィルタ アクションが競合している場合は、最初のレート ベースのフィルタのアクションが実行されることに注意してください。

無効な値を入力するとフィールドに復元アイコン( )が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

（注）　動的ルール状態は、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

動的ルール状態を追加する方法:

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 3　[ルール（Rules）] をクリックします。

[ルール（Rules）] ページが表示されます。

ステップ 4　動的ルール状態を追加するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて（24-10 ページ）および侵入ポリシー内のルール フィルタの設定（24-19 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　動的ルール状態を追加する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

ステップ 6　[動的状態（Dynamic State）] > [レート ベースのルール状態の追加（Add Rate-Based Rule State）] の順に選択します。

[レート ベースのルール状態の追加（Add Rate-Based Rule State）] ダイアログボックスが表示されます。

ステップ 7　[追跡対象（Track By）] ドロップダウンリストから、ルール一致の追跡方法を選択します。

- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[送信元（Source）] を選択します。
- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[宛先（Destination）] を選択します。
- そのルールのすべての一致を追跡する場合は、[ルール（Rule）] を選択します。

ステップ 8　[追跡対象（Track By）] を [送信元（Source）] または [宛先（Destination）] に設定した場合は、[ネットワーク（Network）] フィールドに追跡する各ホストのアドレスを入力します。

単一の IP アドレス、アドレス ブロック、変数、またはこれらの任意の組み合わせで構成されたカンマ区切りのリストを指定できます。IPv4 CIDR および IPv6 プレフィックス長アドレス ブロックを使用する方法については、IP アドレスの表記規則（1-4 ページ）を参照してください。

ステップ 9　[レート（Rate）] の隣で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [カウント（Count）] フィールドで、1 ～ 2147483647 の整数を使用して、しきい値として使用するルール一致の数を指定します。
- [秒（Seconds）] フィールドで、1 ～ 2147483647 の整数を使用して、攻撃を追跡する期間を表す秒数を指定します。

ステップ 10　[新しい状態（New State）] ドロップダウンリストから、条件が満たされたときに実行すべき新しいアクションを指定します。

- イベントを生成する場合は、[イベントを生成する（Generate Events）] を選択します。
- インライン展開でイベントを生成し、イベントをトリガーしたパケットをドロップする場合、または、パッシブ展開でイベントを生成する場合は、[ドロップしてイベントを生成する（Drop and Generate Events）] を選択します。
- アクションを実行しない場合は、[無効（Disabled）] を選択します。

ステップ 11　[タイムアウト（Timeout）] フィールドに、新しいアクションを有効にしておく秒数を入力します。タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションのタイムアウトを阻止する場合は、[0] を指定するか、[タイムアウト（Timeout）] フィールドを空白のままにします。

ステップ 12　[OK] をクリックします。

システムが、動的ルール状態を追加し、[動的状態（Dynamic State）] カラムのルールの横に動的状態アイコン（  ）を表示します。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

必須フィールドを空白にした場合は、フィールドに値を入力する必要があることを伝えるエラー メッセージが表示されます。

ヒント　一連のルールのすべての動的ルール設定を削除するには、[ルール（Rules）] ページでルールを選択してから、[動的状態（Dynamic State）] > [レート ベース状態の削除（Remove Rate-Based States）] の順に選択します。また、ルールのルール詳細から個別のレート ベースのルール状態フィルタを削除するには、ルールを選択して、[詳細の表示（Show Details）] をクリックしてから、削除するレート ベースのフィルタのそばにある [削除（Delete）] をクリックします。

ステップ 13　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理（23-3 ページ）」と「侵入ポリシーの編集（23-4 ページ）」を参照してください。

SNMP アラートの追加

ライセンス：Protection

ASA FirePOWER モジュールの SNMP アラートを設定する場合は、ルールがイベントを生成したときに SNMP アラートを提供するように特定のルールを設定できます。詳細については、SNMP 応答の使用（36-1 ページ）を参照してください。

SNMP アラートを設定する方法:

ステップ **1** [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

ステップ **2** 編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ **3** [ルール(Rules)] をクリックします。

[ルール(Rules)] ページが表示されます。

ステップ **4** SNMP アラートを設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて(24-10 ページ)および侵入ポリシー内のルール フィルタの設定(24-19 ページ)を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ **5** SNMP アラートを設定する 1 つまたは複数のルールを選択します。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

ステップ **6** [アラート(Alerting)] > [SNMP アラートの追加(Add SNMP Alert)] の順に選択します。

システムが、アラートを追加し、[アラート(Alerting)] カラムのルールの横にアラート アイコン( )を表示します。ルールに複数のアラート タイプを追加した場合は、アイコン上の数字がアラート タイプの数を示します。

ヒント　ルールから SNMP アラートを削除するには、そのルールの横にあるチェックボックスをクリックして、[アラート(Alerting)] > [SNMP アラートの削除(Remove SNMP Alerts)] の順に選択してから、[OK] をクリックして削除を確認します。

ステップ **7** ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、「侵入ポリシーの管理(23-3 ページ)」と「侵入ポリシーの編集(23-4 ページ)」を参照してください。

ルール コメントの追加

ライセンス:Protection

ルールにコメントを追加することができます。追加したコメントは、[ルール(Rules)] ページ上の [ルールの詳細(Rule Details)] ビューで確認できます。

コメントを含む侵入ポリシーの変更をコミットしてから、ルールの [編集(Edit)] ページで [ルール コメント(Rule Comment)] をクリックしてコメントを表示することもできます。ルールの編集の詳細については、既存のルールの変更(27-108 ページ)を参照してください。

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。

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 3　[ルール(Rules)] をクリックします。

[ルール(Rules)] ページが表示されます。

ステップ 4　コメントを追加するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて(24-10 ページ)および侵入ポリシー内のルール フィルタの設定(24-19 ページ)を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

ステップ 5　コメントを追加する 1 つまたは複数のルールを選択します。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

ステップ 6　[コメント(Comments)] > [ルール コメントの追加(Add Rule Comment)] の順に選択します。

[コメントの追加(Add Comment)] ダイアログボックスが表示されます。

ステップ 7　[コメント(Comments)] フィールドに、ルール コメントを入力します。

ステップ 8　[OK] をクリックします。

システムが、コメントを追加し、[コメント(Comments)] カラムのルールの横にコメント アイコン( )を表示します。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

ヒント　ルール コメントを削除するには、そのルールを強調表示して、[詳細の表示(Show Details)] をクリックしてから、[コメント(Comments)] セクションで [削除(Delete)] をクリックします。侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけ、コメントを削除できることに注意してください。侵入ポリシーの変更がコミットされた後は、ルール コメントを削除できなくなります。

ステップ 9　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理(23-3 ページ)」と「侵入ポリシーの編集(23-4 ページ)」を参照してください。

特定の脅威の検出

ネットワーク分析ポリシーでさまざまなプリプロセッサを使用して、モニタ対象ネットワークへの特定の攻撃、たとえば、Back Orifice 攻撃、複数のポートスキャン タイプ、過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレート ベース攻撃などを検出できます。侵入ルールまたはルールの引数にプリプロセッサの無効化が必要な場合、システムは現在の設定で自動的にプリプロセッサを使用しますが、ネットワーク分析ポリシーのユーザ インターフェイスではプリプロセッサは無効のままになることに注意してください。詳細については、カスタム ポリシーに関する制約事項（15-12 ページ）を参照してください。

侵入ポリシーで設定するセンシティブ データ検出を使用して、センシティブな数値データの保護なし送信を検出することもできます。

特定の脅威の検出の詳細については、次の項を参照してください。

- Back Orifice の検出（25-1 ページ）では、Back Orifice 攻撃の検出について説明しています。
- ポートスキャンの検出（25-3 ページ）では、各種のポートスキャンについて概説し、ポートスキャン検出を使用して、攻撃に発展する前にネットワークに対する脅威を識別する方法を説明しています。
- レート ベース攻撃の防止（25-10 ページ）では、サービス妨害（DoS）および SYN フラッド攻撃を制約する方法を説明しています。
- センシティブ データの検出（25-21 ページ）では、ASCII テキストのセンシティブ データ（クレジット カード番号や社会保障番号など）を検出してイベントを生成する方法を説明しています。

Back Orifice の検出

ライセンス：Protection

ASA FirePOWER モジュール は、Back Orifice プログラムの存在を検出するプリプロセッサを提供しています。Back Orifice プログラムにより Windows ホストに対する管理者アクセス権を取得される可能性があります。Back Orifice プリプロセッサは、UDP トラフィックを分析し、パケットの最初の 8 バイトにあり XOR で暗号化されている、Back Orifice magic Cookie「`*!*QWTY?`」を調べます。

Back Orifice プリプロセッサには設定ページがありますが、設定オプションはありません。Back Orifice プリプロセッサが有効になっていても、以下の表にリストするプリプロセッサ ルールを有効にしなければ、対応するイベントは生成されません。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

表 *25-1*　*Back Orifice GID:SID*

プリプロセッサ ルール **GID:SID**	説明
105:1	Back Orifice トラフィック検出
105:2	Back Orifice クライアント トラフィック検出
105:3	Back Orifice サーバ トラフィック検出
105:4	Back Orifice Snort バッファ攻撃検出

[Back Orifice 検知（**Back Orifice Detection**）**]** ページを表示する方法：

ステップ **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。

ステップ **2**　編集するアクセス 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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ **4**　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

ステップ **5**　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

ステップ **6**　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ **7**　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

ステップ **8**　[特定の脅威検知（Specific Threat Detection）] の下の [Back Orifice 検知（Back Orifice Detection）] が有効になっているかどうかによって、2 つの選択肢があります。

- プリプロセッサが有効になっている場合は、[編集（Edit）] をクリックします。
- プリプロセッサが無効になっている場合は、[有効（Enabled）] をクリックしてから、[編集（Edit）] をクリックします。

[Back Orifice 検知（Back Orifice Detection）] ページが表示されます。ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ **9**　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

ポートスキャンの検出

ライセンス：Protection

ポートスキャンとは、攻撃者が攻撃の準備段階としてよく使用する、ネットワーク調査の形式です。ポートスキャンでは、攻撃者が特別に細工したパケットをターゲット ホストに送信します。攻撃者は多くの場合、ホストが応答するパケットを調べることで、ホストでどのポートが開かれているか、そして開かれているポートでどのアプリケーション プロトコルが実行されているかを、直接あるいは推論によって判断できます。

ポートスキャン検出が有効になっていても、侵入ポリシーの [ルール（Rules）] ページでジェネレータ ID（GID）が 122 に設定されたルールを有効にしなければ、ポートスキャン ディテクタの有効になっているポートスキャン タイプがポートスキャン イベントを生成しないことに注意してください。詳細については、「ルール状態の設定（24-21 ページ）」と「表 25-5（25-8 ページ）」を参照してください。

ポートスキャンは、それ自体では攻撃の証拠になりません。実際、攻撃者が使用するポートスキャン手法の中には、正当なユーザがネットワークで使用する可能性があるものもあります。Ciscoのポートスキャン ディテクタは、アクティビティのパターンを検出するという方法で、悪意のあるポートスキャンの可能性があるものを判別できるように設計されています。

攻撃者がネットワークを調査するために複数の手法を使用することはよくあります。通常、攻撃者は異なる複数のプロトコルを使用して、ターゲット ホストからさまざまな応答を引き出します。その目的は、ブロックされた特定タイプのプロトコルを基に、使用できる可能性のあるプロトコルを絞り込んでいくことです。以下の表に、ポートスキャン ディテクタでアクティブにできるプロトコルを記載します。

表 ***25-2***　プロトコル タイプ

プロトコル	説明
TCP	TCP プローブを検出します。たとえば、SYN スキャン、ACK スキャン、TCP connect() スキャン、および Xmas tree、FIN、NULL といった異常なフラグを組み合わせたスキャンなどです。
UDP	UDP プローブを検出します。たとえば、ゼロ バイトの UDP パケットなどです。
ICMP	ICMP エコー要求（ping）を検出します。
IP	IP プロトコル スキャンを検出します。これらのスキャンは、攻撃者が開いているポートを見つけようとしているのではなく、ターゲット ホストでサポートされている IP プロトコルを発見しようとするためのスキャンであるため、TCP スキャンおよび UDP スキャンとは異なります。

（注）　イベントがポートスキャン接続ディテクタによって生成され場合、プロトコル番号は 255 に設定されます。デフォルトでは、ポートスキャンに特定のプロトコルは関連付けられません。したがって、Internet Assigned Numbers Authority（IANA）にはプロトコル番号が割り当てられません。IANA では 255 を予約番号として指定しているため、ポートスキャン イベントでは、そのイベントに関連付けられている番号がないことを示すために、この番号が使用されます。

一般に、ターゲット ホストの数、スキャン側ホストの数、およびスキャン対象のポートの数に応じて、ポートスキャンは 4 つのタイプに分けられます。以下の表に、検出できるポートスキャン アクティビティのタイプを記載します。

表 *25-3*　ポートスキャンのタイプ

タイプ	説明
ポートスキャン検出	1 対 1 のポートスキャン。攻撃者が 1 つまたは少数のホストを使用して、単一のターゲット ホスト上の複数のポートをスキャンする場合です。 1 対 1 の ポートスキャンには次のような特徴があります。 • 少数のホストを使用してスキャン • 単一のホストをスキャン • 多数のポートをスキャン このオプションでは、TCP、UDP、および IP ポートスキャンが検出されます。
ポートスイープ	1 対多のポートスイープ。攻撃者が 1 つまたは少数のホストを使用して、複数のターゲット ホスト上の単一のポートをスキャンする場合です。 ポートスイープには次のような特徴があります。 • 少数のホストを使用してスキャン • 多数のホストをスキャン • 少数の固有のポートをスキャン このオプションでは、TCP、UDP、ICMP、および IP ポートスイープが検出されます。
デコイ ポートスキャン	1 対 1 のポートスキャン。攻撃者がスプーフィングしたソース IP アドレスを実際のスキャン IP アドレスに混在させる場合です。 デコイ ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 少数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン デコイ ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。
分散型ポートスキャン	多対 1 のポートスキャン。複数のホストが単一のホストをクエリして開いているポートを調べる場合です。 分散型ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 多数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン 分散型ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。

ポートスキャン ディテクタは、主にプローブ対象ホストからの否定応答に基づいて、プローブに関する情報を取得します。たとえば、Web クライアントが Web サーバに接続するときに、クライアントはサーバのポート 80/tcp が開いていることを頼りに、そのポートを使用します。ただし、攻撃者がサーバを調査するときには、攻撃者にはそのサーバが Web サービスを提供するかどうかについての事前知識はありません。ポートスキャン ディテクタは否定応答（つまり、ICMP 到達不能または TCP RST パケット）を見つけると、その応答を潜在的ポートスキャンとして記録します。否定応答をフィルタリングするデバイス（ファイアウォールやルータなど）の向こう側にターゲット ホストがある場合、このプロセスはさらに困難になります。この場合、ポートスキャン ディテクタは、選択された機密レベルに基づいてフィルタリングされた ポートスキャン イベントを生成することができます。

以下の表に、選択可能な 3 つの機密レベルを記載します。

表 *25-4*　機密レベル

レベル	説明
低	ターゲット ホストからの否定応答だけが検出されます。誤検出を抑えるためには、この機密レベルを選択します。ただし、特定のタイプのポートスキャン（時間をかけたスキャン、フィルタリングされたスキャン）が見逃される可能性があることに注意してください。 このレベルを使用すると、ポートスキャン検出の所要時間が最短になります。
中	ホストへの接続数に基づいてポートスキャンが検出されます。したがって、フィルタリングされたポートスキャンを検出できます。ただし、ネットワーク アドレス変換プログラムやプロキシなど、ホストが非常にアクティブな場合は、誤検出が発生する可能性があります。 [スキャン済みの無視（Ignore Scanned）] フィールドに、アクティブなホストの IP アドレスを追加すると、そのような誤検出を軽減できます。 このレベルを使用すると、ポートスキャン検出の所要時間が長くなります。
高	期間に基づいてポートスキャンが検出されます。したがって、時間ベースのポートスキャンを検出できます。ただし、このオプションを使用する場合は、[スキャン済みの無視（Ignore Scanned）] および [スキャナの無視（Ignore Scanner）] フィールドに IP アドレスを指定するという方法で、時間をかけて慎重にディテクタを調整してください。 このレベルを使用すると、ポートスキャン検出の所要時間が大幅に長くなります。

詳細については、次の各項を参照してください。

- ポートスキャン検出の設定（25-5 ページ）
- ポートスキャン イベントについて（25-7 ページ）

ポートスキャン検出の設定

ライセンス：Protection

ポートスキャン検出の設定オプションを使用して、ポートスキャン ディテクタによるスキャン アクティビティのレポート方法を微調整できます。

ポートスキャン検出が有効になっていても、[ルール（Rules）] ページでジェネレータ ID（GID）が 122 に設定されたルールを有効にしなければ、ポートスキャン ディテクタの有効になっているポートスキャン タイプがポートスキャン イベントを生成しないことに注意してください。詳細については、ルール状態の設定（24-21 ページ）とポートスキャン検出 SID（GID:122）の表を参照してください。

ポートスキャン検出を設定する方法：

Admin/Intrusion Admin

ステップ **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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定(Advanced)] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] の横にある編集アイコン( )をクリックします。

[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] をクリックします。

[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーで保存されていない変更内容を保存する詳細については、[was Committing Intrusion Policy Changes; update xref] を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定(Settings)] をクリックします。

[設定(Settings)] ページが表示されます。

ステップ 8　[特定の脅威検知(Specific Threat Detection)] の [ポートスキャン検出(Portscan Detection)] が有効になっているかどうかに応じて、2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

  [ポートスキャン検出(Portscan Detection)] ページが表示されます。ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(16-1 ページ)を参照してください。

ステップ 9　[プロトコル(Protocol)] フィールドに、以下のプロトコルのうち、有効にするプロトコルを指定します。

- TCP
- UDP
- ICMP
- IP

Ctrl キーまたは Shift キーを押しながらクリックすることによって複数のプロトコルを選択するか、個々のプロトコルをクリアします。詳細については、プロトコル タイプ の表を参照してください。

TCP を介してスキャンを検出するには TCP ストリーム処理が有効になっていること、UDP を介してスキャンを検出するには UDP ストリーム処理が有効になっていることが必要です。

ステップ 10　[スキャン タイプ(Scan Type)] フィールドに、以下の中から検出対象のポートスキャンを指定します。

- ポートスキャン検出
- ポートスイープ
- デコイ ポートスキャン
- 分散型ポートスキャン

複数のプロトコルを選択または選択解除するには、Ctrl キーまたは Shift キーを押しながらクリックします。詳細については、ポートスキャンのタイプ の表を参照してください。

ステップ 11　[機密レベル（Sensitivity Level）] リストで、使用するレベル（低、中、または高）を選択します。

詳細については、機密レベル の表を参照してください。

ステップ 12　オプションで、[IP の監視（Watch IP）] フィールドに、ポートスキャン アクティビティの兆候を監視するホストを指定します。すべてのネットワーク トラフィックを監視する場合は、このフィールドを空白のままにします。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-4 ページ）を参照してください。

ステップ 13　オプションで、[スキャナの無視（Ignore Scanners）] フィールドに、スキャナとして無視するホストを指定します。ネットワーク上で特にアクティブになっていないホストを指定するには、このフィールドを使用します。このホスト リストは、時間経過とともに変更しなければならない場合があります。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-4 ページ）を参照してください。

ステップ 14　オプションで、[スキャン済みの無視（Ignore Scanned）] フィールドに、スキャンのターゲットとして無視するホストを指定します。ネットワーク上で特にアクティブになっていないホストを指定するには、このフィールドを使用します。このホスト リストは、時間経過とともに変更しなければならない場合があります。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-4 ページ）を参照してください。

ステップ 15　オプションで、ミッドストリームで取得されたセッションのモニタを中断する場合は、[ACK スキャンの検出（Detect Ack Scans）] チェックボックスをオフにします。

（注）　ミッドストリーム セッションの検出は ACK スキャンの識別に役立ちますが、過大トラフィックで大量のパケットがドロップされるネットワークでは、誤ったイベントが生成されがちです。

ステップ 16　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

ポートスキャン イベントについて

ライセンス：Protection

ポートスキャン検出が有効になっていても、ジェネレータ ID（GID）122 と Snort® ID（SID）1 ～ 27 のどれかが設定されたルールを有効にしなければ、有効にした各ポートスキャン タイプのイベントは生成されません。詳細については、ルール状態の設定（24-21 ページ）を参照してください。以下の表の「プリプロセッサ ルール SID」列に、各ポートスキャン タイプに対して有効にする必要があるプリプロセッサ ルールの SID をリストします。

表 *25-5*　ポートスキャン検出 *SID*（*GID:122*）

ポートスキャン タイプ	プロトコル:	機密レベル	プリプロセッサ ルール **SID**
ポートスキャン検出	TCP	低（Low）	1
		[中（Medium）] または [高（High）]	5
	UDP	低（Low）	17
		[中（Medium）] または [高（High）]	21
	ICMP	低（Low）	イベントを生成しません。
		[中（Medium）] または [高（High）]	イベントを生成しません。
	IP	低（Low）	9
		[中（Medium）] または [高（High）]	13
ポートスイープ	TCP	低（Low）	3、27
		[中（Medium）] または [高（High）]	7
	UDP	低（Low）	19
		[中（Medium）] または [高（High）]	23
	ICMP	低（Low）	25
		[中（Medium）] または [高（High）]	26
	IP	低（Low）	11
		[中（Medium）] または [高（High）]	15
デコイ ポートスキャン	TCP	低（Low）	2
		[中（Medium）] または [高（High）]	6
	UDP	低（Low）	18
		[中（Medium）] または [高（High）]	22
	ICMP	低（Low）	イベントを生成しません。
		[中（Medium）] または [高（High）]	イベントを生成しません。
	IP	低（Low）	10
		[中（Medium）] または [高（High）]	18
分散型ポートスキャン	TCP	低（Low）	4
		[中（Medium）] または [高（High）]	8
	UDP	低（Low）	20
		[中（Medium）] または [高（High）]	24
	ICMP	低（Low）	イベントを生成しません。
		[中（Medium）] または [高（High）]	イベントを生成しません。
	IP	低（Low）	12
		[中（Medium）] または [高（High）]	16

関連するプリプロセッサ ルールを有効にすると、ポートスキャン ディテクタによって侵入イベントが生成されるようになります。生成されたイベントは、他のすべての侵入イベントと同じように表示できます。ただし、ポートスキャン イベントのパケット ビューに表示される情報は、他のタイプの侵入イベントとは異なります。ここでは、ポートスキャン イベントのパケット ビューに表示されるフィールドと、これらのフィールドの情報を使用してネットワークで行われたプローブのタイプを把握する方法を説明します。

侵入イベント ビューを出発点に、ポートスキャン イベントのパケット ビューまでドリルダウンします。

各ポートスキャン イベントは複数のパケットに基づくため、単一のポートスキャン パケットをダウンロードすることはできません。ただし、ポートスキャン パケット ビューで、使用可能なすべてのパケット情報を確認できます。

（注）　イベントがポートスキャン接続ディテクタによって生成され場合、プロトコル番号は 255 に設定されます。デフォルトでは、ポートスキャンに特定のプロトコルは関連付けられません。したがって、Internet Assigned Numbers Authority（IANA）にはプロトコル番号が割り当てられません。IANA では 255 を予約番号として指定しているため、ポートスキャン イベントでは、そのイベントに関連付けられている番号がないことを示すために、この番号が使用されます。

以下の表に、ポートスキャン イベントのパケット ビューに表示される情報を記載します。

表 ***25-6***　　ポートスキャン パケット ビュー

情報	説明
デバイス（Device）	イベントを検出したデバイス。
時刻（Time）	イベントが発生した時刻。
メッセージ（Message）	プリプロセッサによって生成されたイベント メッセージ。
送信元 IP（Source IP）	スキャン側ホストの IP アドレス。
宛先 IP（Destination IP）	スキャンされたホストの IP アドレス。
プライオリティ カウント（Priority Count）	スキャンされたホストからの否定応答（TCP RST、ICMP 到達不能など）の数。否定応答の数が多ければ多いほど、プライオリティ カウントが高くなります。
接続数（Connection Count）	ホスト上でアクティブな接続数。この値は、TCP や IP などの接続ベースのスキャンより正確です。
IP カウント（IP Count）	スキャン対象のホストに接続する IP アドレスが変更された回数。たとえば、最初の IP アドレスが 10.1.1.1、2 番目の IP アドレスが 10.1.1.2、3 番目の IP アドレスが 10.1.1.1 の場合、IP カウントは 3 となります。 プロキシや DNS サーバなどのアクティブ ホストでは、この数値はそれほど正確ではありません。
スキャナ/スキャン対象 IP 範囲（Scanner/Scanned IP Range）	スキャン対象ホストまたはスキャン側ホスト（スキャンのタイプに依存）の IP アドレスの範囲。ポートスイープの場合、このフィールドにはスキャン対象ホストの IP アドレス範囲が示されます。ポートスキャンの場合は、スキャン側ホストの IP アドレス範囲が示されます。
ポート/プロトコル カウント（Port/Proto Count）	TCP および UDP ポートスキャンの場合は、スキャン対象のポートが変更された回数です。たとえば、スキャンされた最初のポートが 80、2 番目のポートが 8080、3 番目のポートが再び 80 の場合、ポート カウントは 3 となります。 IP プロトコル ポートスキャンの場合は、スキャン対象ホストに接続するために使用されたプロトコルが変更された回数です。
ポート/プロトコル範囲（Port/Proto Range）	TCP および UDP ポートスキャンの場合は、スキャンされたポートの範囲です。 IP プロトコル ポートスキャンの場合は、スキャン対象ホストへの接続試行で使用された IP プロトコル番号の範囲です。
開いているポート（Open Ports）	スキャン対象ホストで開かれた TCP ポート。このフィールドは、ポートスキャンで 1 つ以上の開かれたポートが検出された場合にのみ表示されます。

レート ベース攻撃の防止

ライセンス：Protection

レート ベース攻撃とは、接続の頻度または攻撃を行うための反復試行に依存する攻撃のことです。レート ベースの検出基準を使用することで、レート ベース攻撃が行われていることを検出し、攻撃が発生するごとに対応できます。また、攻撃が収まった後は、通常の検出設定に戻すことができます。レート ベースの検出を設定する方法の詳細については、以下のトピックを参照してください。

- レート ベース攻撃の防止について（25-10 ページ）
- レート ベース攻撃防止とその他のフィルタ（25-13 ページ）
- レート ベース攻撃防止の設定（25-19 ページ）
- 動的ルール状態について（24-31 ページ）
- 動的ルール状態の設定（24-32 ページ）

レート ベース攻撃の防止について

ライセンス：Protection

レート ベース フィルタを含めたネットワーク分析ポリシーを設定することで、ネットワーク上のホストを対象とした過剰なアクティビティを検出できます。インライン モードで導入されているデバイスでこの機能を使用すると、指定の期間だけレート ベース攻撃をブロックし、その後イベントだけを生成しトラフィックをドロップしないように戻すことができます。

レート ベースの攻撃防御は、異常なトラフィック パターンを識別し、正規の要求に対するそのトラフィックの影響を最小限に抑えようとします。一般に、レート ベース攻撃には次のいずれかの特性があります。

- 任意のトラフィックで、ネットワーク上のホストに対して過剰な未完了接続が発生する。これは、SYN フラッド攻撃を意味します。

  SYN 攻撃の検出を設定するには、SYN 攻撃の防止（25-12 ページ）を参照してください。

- 任意のトラフィックで、ネットワーク上のホストに対して過剰な接続が発生する。これは、TCP/IP 接続フラッド攻撃を意味します。

  同時接続の検出を設定するには、同時接続の制御（25-13 ページ）を参照してください。

- 1 つ以上の特定の宛先 IP アドレスへのトラフィック、または 1 つ以上の特定の送信元 IP アドレスからのトラフィックで、ルールとの一致が過剰に発生する。

  送信元または宛先ベースの動的ルール状態を設定するには、動的ルール状態の設定（24-32 ページ）を参照してください。

- すべてのトラフィックで、特定のルールとの一致が過剰に発生する。

  ルール ベースの動的ルール状態を設定するには、動的ルール状態の設定（24-32 ページ）を参照してください。

ネットワーク分析ポリシーでは、ポリシー全体に対して SYN フラッドまたは TCP/IP 接続フラッドの検出を設定できます。侵入ポリシーでは、個々の侵入ルールまたはプリプロセッサ ルールに対してレート ベース フィルタを設定できます。ルール 135:1 および 135:2 に手動でレート ベース フィルタを追加しても、効果はありません。GID:135 のルールでは、クライアントを送信元の値、サーバを宛先の値として使用します。詳細については、「SYN 攻撃の防止（25-12 ページ）」と「同時接続の制御（25-13 ページ）」を参照してください。

各レート ベース フィルタには、以下のコンポーネントが含まれます。

- ポリシー全体またはルール ベースの送信元/宛先の設定の場合、ネットワーク アドレスの指定
- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率
- レートを超過した場合に実行する新しいアクション

  ポリシー全体に対してレート ベースを設定すると、システムはレート ベース攻撃を検出した時点でイベントを生成します。インライン導入では、オプションでトラフィックをドロップすることもできます。個々のルールにレート ベース アクションを設定する場合は、[イベントを生成する（Generate Events）]、[ドロップしてイベントを生成する（Drop and Generate Events）]、[無効にする（Disable）] の 3 つのうちから選択できます。
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウト期間が満了し、レートがしきい値を下回っている場合、ルールのアクションはそのルールに最初に設定されたアクションに戻ります。ポリシー全体に適用される設定の場合、アクションは、トラフィックと一致する個々のルールのアクションに戻ります。一致するアクションがなければ、アクションは停止されます。

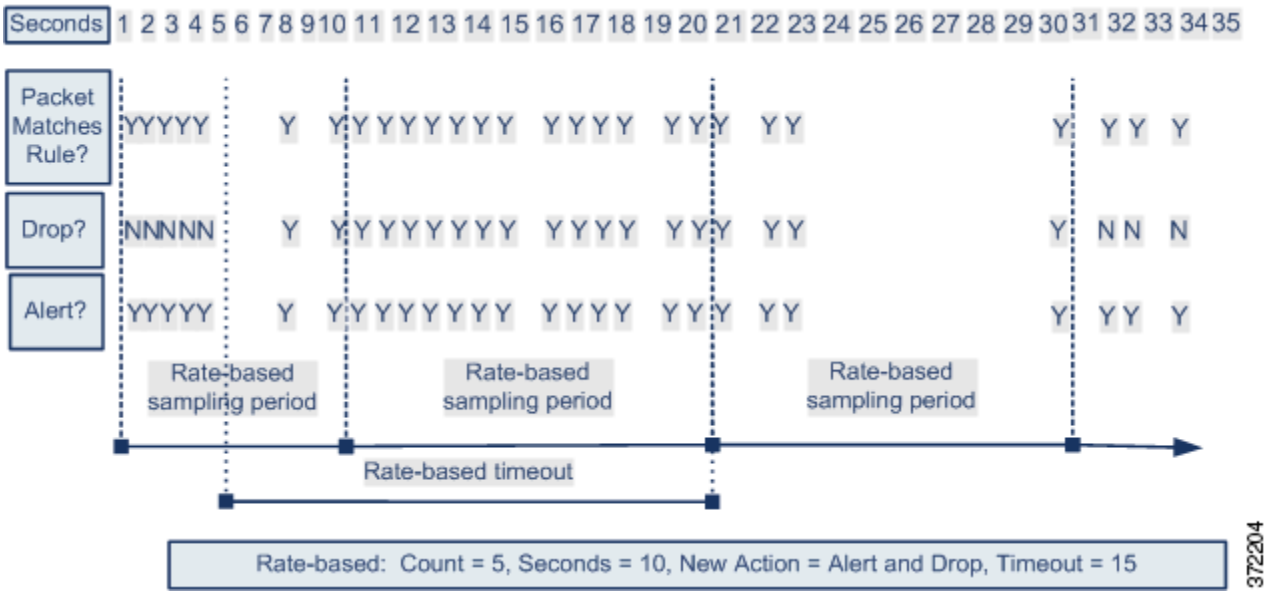
インライン展開のレート ベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レート ベースの設定が使用されていない場合、ルールが [イベントを生成する（Generate Events）] に設定されていればイベントが生成されますが、パケットがドロップされることはありません。ただし、攻撃トラフィックが、レート ベースの基準が設定されたルールと一致した場合は、そのようなルールが最初から [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていなかったとしても、レート アクションがアクティブな期間にパケットのドロップが実行されます。

（注）　レート ベースのアクションは、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。ただし、ポリシー レベルでレート ベース フィルタを設定すると、指定した期間内の過剰な数の SYN パケットまたは SYN/ACK インタラクションを含むトラフィックに対してイベントを生成するか、イベントを生成してトラフィックをドロップすることができます。

同じルールに対して複数のレート ベースのフィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレート ベース フィルタ アクションが競合する場合は、最初のレート ベース フィルタのアクションが実行されることに注意してください。同様に、ポリシー全体に対するレート ベース フィルタと個々のルールに設定されたレート ベース フィルタが競合する場合は、ポリシー全体のレート ベース フィルタが優先されます。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。パスワードを検出しようとする試行が繰り返されると、レート ベース攻撃防止が設定されたルールがトリガーされます。レート ベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [ドロップしてイベントを生成する（Drop and Generate Events）] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または過去のサンプリング期間のしきい値を上回っている場合は、新しいアクションが継続されます。新しいアクションが元の「イベントの生成」アクションに戻されるのは、サンプリング期間の完了時にサンプルリング レートがしきい値を下回っている場合のみです。



SYN 攻撃の防止

ライセンス：Protection

ネットワークのホストを SYN フラッドから保護するには、SYN 攻撃防止オプションを利用します。一定期間中に認められたパケットの数を基準に、個々のホストまたはネットワーク全体を保護することができます。パッシブ導入のデバイスでは、イベントを生成できます。インライン導入のデバイスでは、不正なパケットをドロップすることもできます。タイムアウト期間の満了時にレート条件に達しなくなっていれば、イベントの生成およびパケットのドロップが停止します。

たとえば、1 つの IP アドレスからの SYN パケットの最大許容数を 10 に設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

このオプションを有効にすると、ルール 135:1 もアクティブになります。このルールを手動でアクティブにしても効果はありません。ルール状態は常に [無効（Disabled）] として表示され、変更されることはありません。このオプションを有効にすると、定義されたレート条件を超過した時点で、ルールによってイベントが生成されます。

同時接続の制御

ライセンス：Protection

ネットワーク上のホストでの TCP/IP 接続数を制限することで、サービス妨害（DoS）攻撃や、ユーザによる過剰なアクティビティを防止できます。システムが、指定の IP アドレスまたはアドレス範囲で正常に行われている接続が設定された許容数に達したことを検出すると、以降の接続に対してイベントを生成します。タイムアウト期間が満了するまでは、レート条件に達しなくなっても、レート ベースのイベント生成が続行されます。インライン導入では、レート条件がタイムアウトになるまでパケットをドロップするように設定できます。

たとえば、1 つの IP アドレスからの同時接続の最大許容数を 10 に設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

このオプションを有効にすると、ルール 135:2 もアクティブになります。このルールを手動でアクティブにしても効果はありません。ルール状態は常に [無効（Disabled）] として表示され、変更されることはありません。このオプションを有効にすると、定義されたレート条件を超過した時点で、ルールによってイベントが生成されます。

レート ベース攻撃防止とその他のフィルタ

ライセンス：Protection

トラフィック自体またはシステムが生成するイベントをフィルタリングする手段としては、`detection_filter` キーワード、しきい値および抑制機能も使用できます。レート ベース攻撃防止は、単独で使用することも、しきい値構成、抑制、または `detection_filter` キーワードと任意に組み合わせて使用することもできます。

詳細については、以下の例を参照してください。

- レート ベース攻撃防止と検出フィルタリング（25-13 ページ）
- 動的ルール状態としきい値または抑制（25-15 ページ）
- ポリシー全体のレート ベース検出としきい値構成または抑制（25-16 ページ）
- 複数のフィルタリング方法によるレート ベース検出（25-17 ページ）

レート ベース攻撃防止と検出フィルタリング

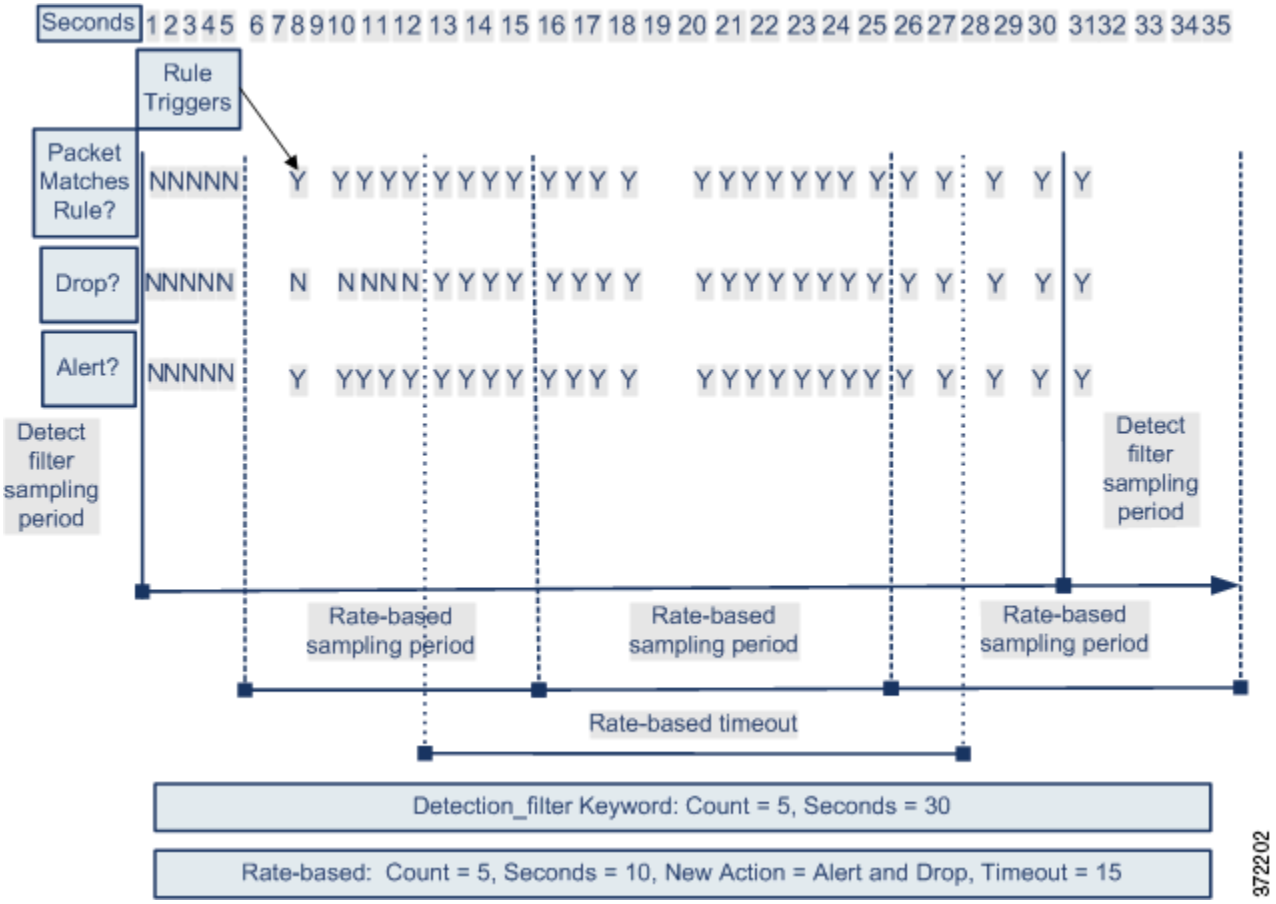
ライセンス：Protection

`detection_filter` キーワードを使用すると、指定の期間内にルール一致のしきい値に達するまで、ルールはトリガーされません。ルールに `detection_filter` キーワードが含まれている場合、システムは指定の期間、ルールのパターンに一致する着信パケットの数を追跡します。システムはそのルールについて、特定の送信元 IP アドレスからのヒット数、または特定の宛先 IP アドレスからのヒット数をカウントできます。レートがルールのレートを超過すると、そのルールに関するイベント通知が開始されます。

以下に、攻撃者がブルートフォース ログインを仕掛ける例を示します。パスワードの検出試行が繰り返されると、カウントが 5 に設定された `detection_filter` キーワードも含むルールがトリガーされます。このルールには、レート ベース攻撃防止が設定されています。10 秒以内にルールに 5 回ヒットすると、レート ベースの設定により、ルール属性が 20 秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。

図に示されているように、最初の 5 個のパケットがルールに一致しても、イベントは生成されません。それは、レートが detection_filter キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに 5 個のパケットが通過するまでは、レート ベースの基準によって新しいルールとして [ドロップしてイベントを生成する（Drop and Generate Events）] がトリガーされることはありません。

レート ベースの基準に一致すると、イベントが生成されて、パケットがドロップされます。これは、レート ベースのタイムアウト期間が満了し、かつレートがしきい値未満になるまで続きます。20 秒が経過すると、レート ベース アクションがタイムアウトになります。タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。タイムアウトが発生した時点で、サンプリングされたレートは前のサンプリング期間のしきい値レートを超過しているため、レート ベースのアクションは続行されます。



この例には示されていませんが、[ドロップしてイベントを生成する（Drop and Generate Events）] ルール状態を detection_filter キーワードと組み合わせて使用することで、ルールのヒット数が指定のレートに達するとトラフィックのドロップが開始されるようにすることができることにも注意してください。ルールにレート ベースの設定を使用するかどうかを決定する際は、ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定した場合の結果と detection_filter キーワードを含めた場合の結果が同じであるかどうか、あるいは侵入ポリシーでレートとタイムアウトの設定を管理する必要があるかどうかを検討してください。詳細については、ルール状態の設定（24-21 ページ）を参照してください。

動的ルール状態としきい値または抑制

ライセンス：Protection

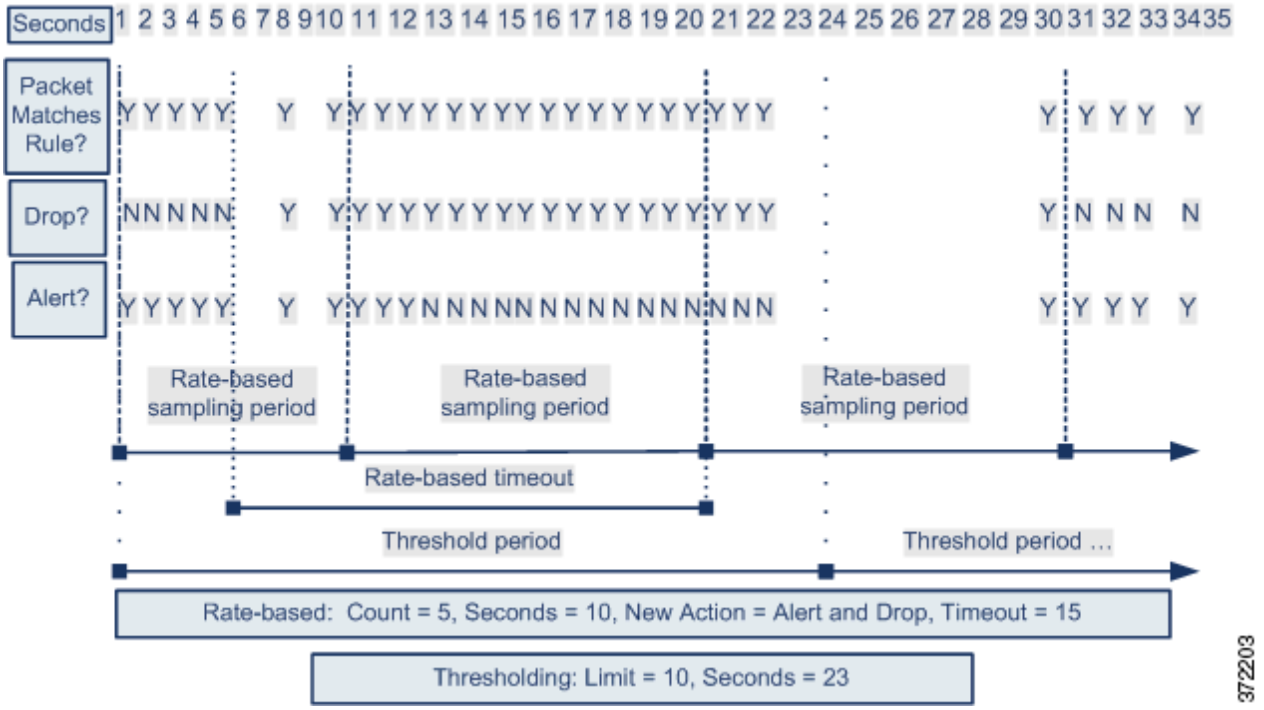
しきい値および抑制を使用して、ルールに関するイベント通知の数を制限するか、またはイベント通知を一切抑制することにより、過剰なイベントが生成されないようにすることができます。しきい値と抑制で使用可能なオプションの詳細については、イベントしきい値の設定（24-23 ページ）および侵入ポリシー単位の抑制の設定（24-28 ページ）を参照してください。

抑制をルールに適用すると、システムは、レート ベースのアクションが変更されたとしても、そのルールに関するイベント通知を、該当するすべての IP アドレスに対して抑制します。一方、しきい値とレート ベースの基準との間の相互作用はさらに複雑になります。

以下に、攻撃者がブルートフォース ログインを仕掛ける例を示します。パスワードを検出しようとする試行が繰り返されると、レート ベース攻撃防止が設定されたルールがトリガーされます。10 秒以内にルールに 5 回ヒットすると、レート ベースの設定により、ルール属性が 15 秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。さらに、上限しきい値により、ルールで生成可能なイベントの数が 23 秒間で 10 に制限されます。

図に示されているように、最初の 5 個のパケットが一致すると、ルールはイベントを生成します。5 個のパケットがルールに一致した後、レート ベースの基準が新しいアクションとして [ドロップしてイベントを生成する（Drop and Generate Events）] をトリガーし、次の 5 個のパケットがルールに一致した時点でイベントが生成され、パケットをドロップします。10 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成することなくドロップします。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが続行されます。新しいアクションが元の [イベントを生成する（Generate Events）] アクションに戻されるのは、サンプリング期間の完了時にサンプルリング レートがしきい値を下回っている場合のみです。



この例には示されていませんが、しきい値に達した後に、レート ベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の 10 に達してシステムがイベントの生成を停止し、14 番目のパケットでアクションが [イベントを生成する（Generate Events）] から [ドロップしてイベントを生成する（Drop and Generate Events）] に変更されると、システムはアクションが変更されたことを示す 11 番目のイベントを生成します。

ポリシー全体のレート ベース検出としきい値構成または抑制

ライセンス：Protection

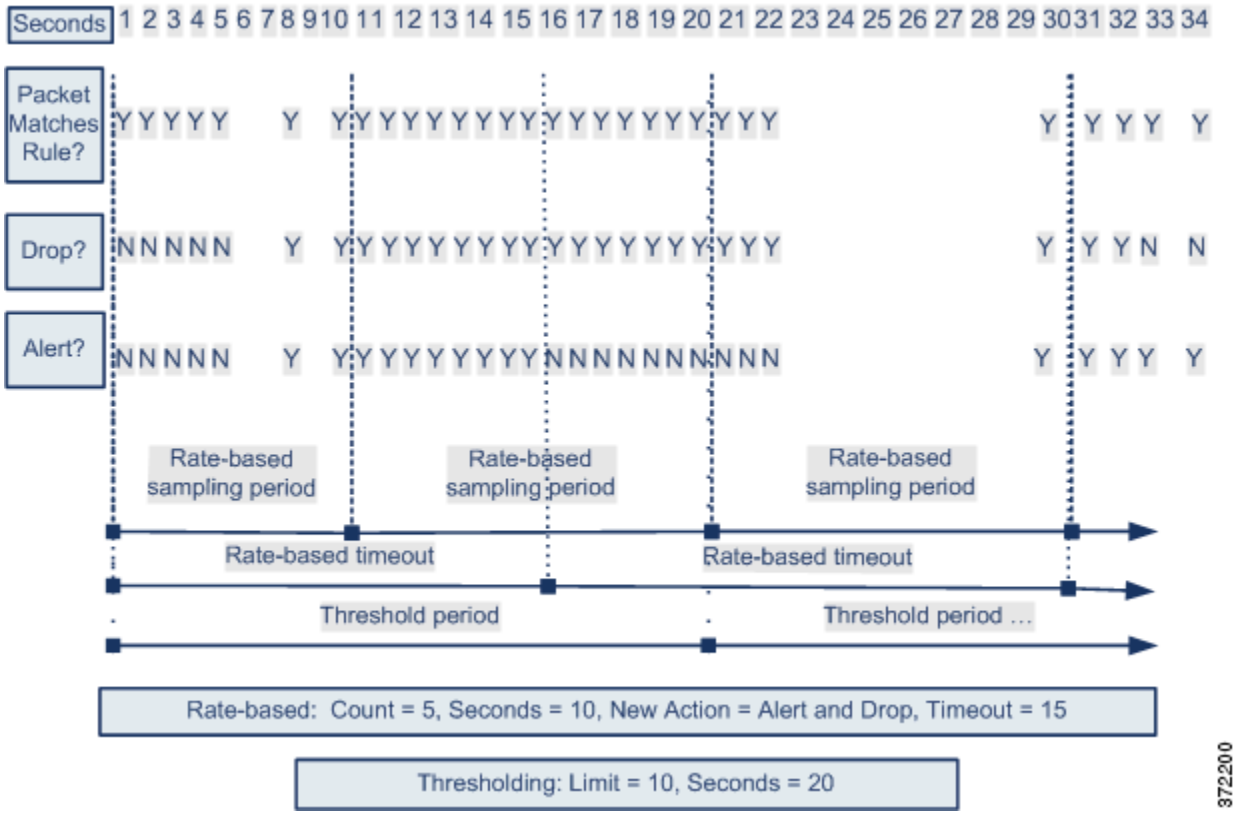
しきい値および抑制を使用して、送信元または宛先に関するイベント通知の数を制限するか、またはイベント通知を一切抑制することにより、過剰なイベントが生成されないようにすることができます。しきい値と抑制で使用可能なオプションの詳細については、グローバルしきい値の設定（26-3 ページ）、イベントしきい値の設定（24-23 ページ）、および侵入ポリシー単位の抑制の設定（24-28 ページ）を参照してください。

抑制がルールに適用されている場合、ポリシー全体またはルール固有のレート ベースの設定によって、レート ベースのアクションが変更されたとしても、該当するすべての IP アドレスに対してそのルールに関するイベント通知が抑制されます。一方、しきい値とレート ベースの基準との間の相互作用はさらに複雑になります。

以下に、ネットワーク上のホストに対して、攻撃者がサービス妨害（DoS）攻撃を仕掛ける例を示します。同じ送信元から多数のホストに対して同時接続が行われると、ポリシー全体の [同時接続の制御（Control Simultaneous Connections）] 設定がトリガーされます。この設定は、1 つの送信元からの接続数が 10 秒間で 5 つに達すると、イベントを生成して悪意のあるトラフィックをドロップします。さらに、グローバル上限しきい値により、ルールまたは設定で生成可能なイベントの数が 20 秒間で 10 件に制限されます。

この図に示されているように、ポリシー全体の設定により、一致する最初の 10 個のパケットに対してイベントが生成され、トラフィックがドロップされます。10 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリングされたレートが、現在または前のサンプリング期間のしきい値レートを超過している場合、レート ベースのアクションによるイベントの生成とトラフィックのドロップが続行されます。レート ベース アクションが停止するのは、サンプリング期間が完了した時点で、サンプリングされたレートがしきい値レートを下回っている場合のみです。



この例には示されていませんが、しきい値に達した後に、レート ベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の 10 に達してシステムがイベントの生成を停止し、14 番目のパケットでアクションが [ドロップしてイベントを生成する（Drop and Generate Events）] に変更されると、システムはアクションが変更されたことを示す 11 番目のイベントを生成します。

複数のフィルタリング方法によるレート ベース検出

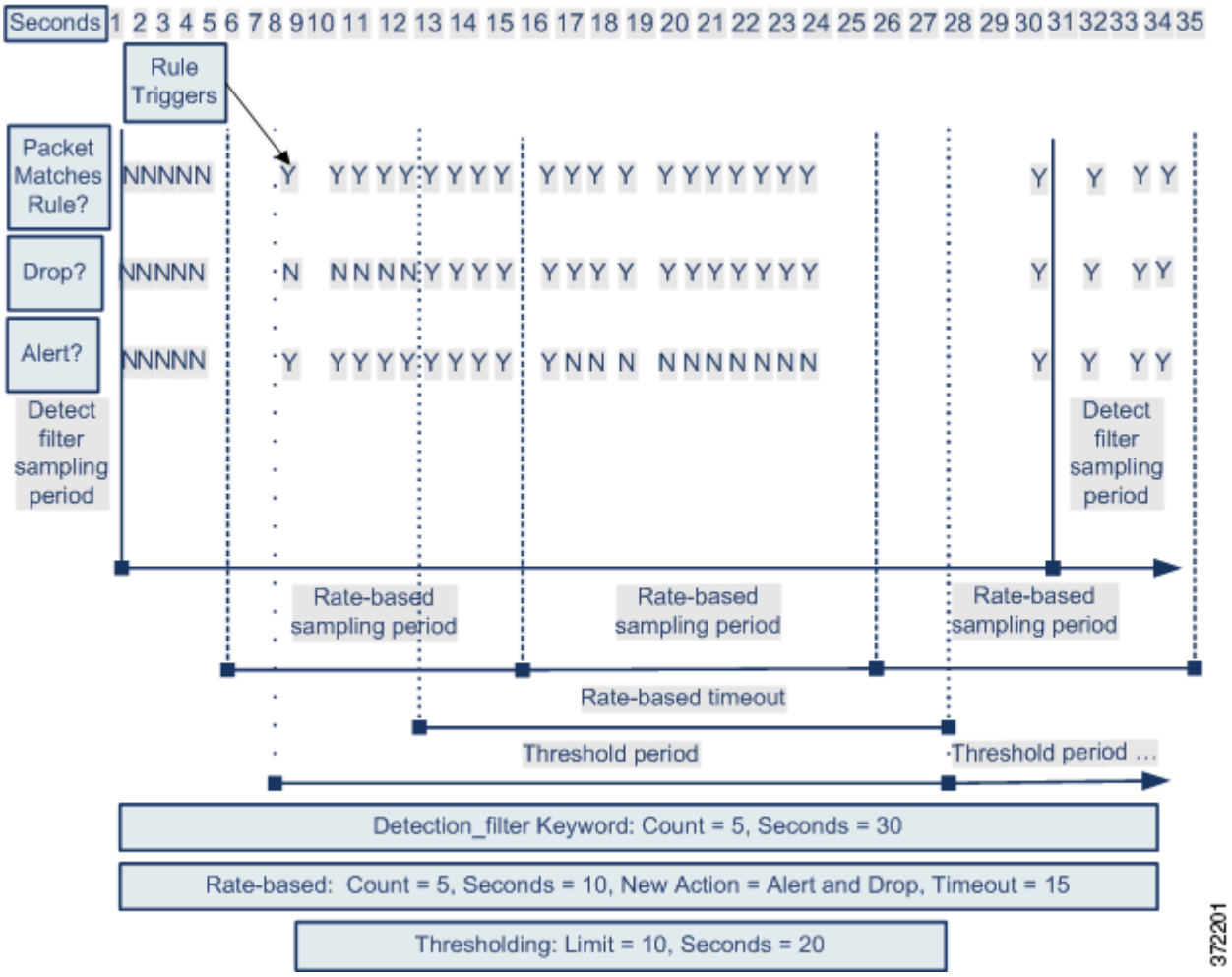
ライセンス：Protection

`detection_filter` キーワード、しきい値構成または抑制、およびレート ベースの基準のすべてが同じトラフィックに適用されるという状況が発生することもあります。抑制をルールに適用すると、レート ベースの変更が発生しても、指定の IP アドレスに対するイベントの生成は抑制されます。

以下に、攻撃者がブルートフォース ログインを仕掛ける例で、`detection_filter` キーワード、レート ベースのフィルタリング、およびしきい値が相互作用する場合を説明します。パスワードの検出試行が繰り返されると、カウントが 5 に設定された `detection_filter` キーワードを含むルールがトリガーされます。このルールには、レート ベース攻撃防止も設定されています。その設定では、15 秒間にルールのヒット数が 5 に達すると、ルール属性が 30 秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。さらに、上限しきい値により、ルールによって生成されるイベントは 30 秒間で 10 件に制限されます。

図に示されているように、最初の 5 個のパケットがルールに一致しても、イベント通知は行われません。それは、detection_filter キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに 5 個のパケットが通過するまでは、レート ベースの基準によって新しいルールとして [ドロップしてイベントを生成する（Drop and Generate Events）] がトリガーされることはありません。レート ベースの基準が満たされると、システムは 11 個目から 15 個目のパケットに対してイベントを生成し、パケットをドロップします。15 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

レート ベースのタイムアウトが発生した後は、それに続くレート ベースのサンプリング期間中、パケットが引き続きドロップされることに注意してください。サンプリング レートが前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが続行されます。



レート ベース攻撃防止の設定

ライセンス:Protection

ポリシー レベルでレート ベース攻撃防止を設定することで、SYN フラッド攻撃を阻止できます。特定の送信元からの過剰な接続、または特定の宛先への過剰な接続を阻止することもできます。

レート ベース攻撃防止の設定方法:

Admin/Intrusion Admin

ステップ 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。

ステップ 2　編集するアクセス 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。

ステップ 3　[詳細設定(Advanced)] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4　[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] の横にある編集アイコン( )をクリックします。

[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] ポップアップ ウィンドウが表示されます。

ステップ 5　[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] をクリックします。

[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] ポップアップ ウィンドウが表示されます。

ステップ 6　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 7　左側のナビゲーション パネルで [設定(Settings)] をクリックします。

[設定(Settings)] ページが表示されます。

ステップ 8　[特定の脅威検知(Specific Threat Detection)] の下にある [レート ベース攻撃の防止(Rate-Based Attack Prevention)] が有効になっているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[レート ベース攻撃の防止(Rate-Based Attack Prevention)] ページが表示されます。ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(16-1 ページ)を参照してください。

ステップ 9　次の 2 つの対処法があります。

- ホストのフラッディングを目的とする不完全な接続を防ぐには、[SYN 攻撃の防止(SYN Attack Prevention)] の下にある [追加(Add)] をクリックします。

  [SYN 攻撃の防止(SYN Attack Prevention)] ダイアログボックスが表示されます。

- 過剰な数の接続を防ぐには、[同時接続の制御（Control Simultaneous Connections）] の下にある [追加（Add）] をクリックします。

  [同時接続の制御（Control Simultaneous Connections）] ダイアログボックスが表示されます。

ステップ 10　トラフィックを追跡する方法を選択します。

- 特定の送信元または送信元の範囲からのすべてのトラフィックを追跡するには、[追跡対象（Track By）] ドロップダウンリストから [送信元（Source）] を選択し、[ネットワーク（Network）] フィールドに単一の IP アドレスまたはアドレス ブロックを入力します。
- 特定の宛先または宛先の範囲へのすべてのトラフィックを追跡するには、[追跡対象（Track By）] ドロップダウンリストから [宛先（Destination）] を選択し、[ネットワーク（Network）] フィールドに単一の IP アドレスまたはアドレス ブロックを入力します。

システムは、[ネットワーク（Network）] フィールドに含まれる各 IP アドレスのトラフィックを個別に追跡することに注意してください。ある特定の IP アドレスからの設定されたレートを超過するトラフィックがある場合、その IP アドレスに関するイベントだけが生成されることになります。例として、ネットワーク設定で `10.1.0.0/16` の送信元 CIDR ブロックを設定し、10 個の同時接続が開始された時点でイベントを生成するようにシステムを設定するとします。10.1.4.21 から 8 つの接続が開始され、10.1.5.10 から 6 つの接続が開始されている場合、いずれの送信元も開始されている接続がトリガーを引き起こす数になっていないため、システムはイベントを生成しません。一方、10.1.4.21 から 11 個の同時接続が開始されている場合、システムは 10.1.4.21 からの接続に対してだけイベントを生成します。

CIDR 表記およびプレフィックス長を使用する方法の詳細については、IP アドレスの表記規則（1-4 ページ）を参照してください。

ステップ 11　レート追跡設定をトリガーとして使用するレートを指定します。

- SYN 攻撃に対する設定の場合は、[レート（Rate）] フィールドに、一定の秒数あたりの SYN パケット数を指定します。
- 同時接続に対する設定の場合は、[カウント（Count）] フィールドに、接続数を指定します。

ステップ 12　レート ベース攻撃防止設定に一致するパケットをドロップするには、[ドロップ（Drop）] を選択します。

ステップ 13　[タイムアウト（Timeout）] フィールドに、イベント生成のタイムアウト期間を指定します。この期間を経過すると、SYN または同時接続のパターンに一致するトラフィックに対するイベント生成が（該当する場合はドロップも）停止されます。

注意　タイムアウト値には 1 ～ 1,000,000 の整数を指定できます。ただし、インライン導入では、大きいタイムアウト値を指定するとホストへの接続が完全にブロックされる可能性があります。

ステップ 14　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

センシティブ データの検出

ライセンス：Protection

社会保障番号、クレジット カード番号、運転免許証番号などのセンシティブ データは、インターネットに意図的に、または誤って漏洩される可能性があります。システムには、ASCII テキストのセンシティブ データに関するイベントを検出し、生成できるセンシティブ データ プロセッサが用意されています。このプロセッサは、特に誤って漏洩されたデータの検出に役立ちます。

このシステムは、暗号化または難読化されたセンシティブ データ、あるいは圧縮または符号化された形式のセンシティブ データ（たとえば、Base64 でエンコードされた電子メールの添付ファイルなど）の検出は行いません。たとえば、システムは電話番号 (555)123-4567 を検出しますが、(5 5 5) 1 2 3 - 4 5 6 7 のようにスペースで難読化されたバージョン、あるいは (555)-123-4567 のように HTML コードが介在するバージョンは検出しません。ただし、(555)-123-4567 のように、HTML にコーディングされた番号のパターンの途中にコードが入っていなければ検出されます。

ヒント　センシティブ データ プリプロセッサでは、FTP または HTTP を使用してアップロードおよびダウンロードされる暗号化されていない Microsoft Word ファイル内のセンシティブ データを検出できます。これが可能である理由は、Word ファイルが ASCII テキストとフォーマット設定コマンドを分けてグループ化する方式だからです。

システムはトラフィックに対して個別のデータ タイプを照合することによって、TCP セッションごとにセンシティブ データを検出します。侵入ポリシーの、各データ タイプのデフォルト設定およびすべてのデータ タイプに適用されるグローバル オプションのデフォルト設定は変更できます。Ciscoでは、事前定義された、よく使用されるデータ タイプを用意しています。カスタム データ タイプを作成することも可能です。

センシティブ データのプリプロセッサ ルールは、各データ タイプに関連付けられます。各データ タイプのセンシティブ データ検出とイベント生成を有効にするには、そのデータ タイプに対応するプリプロセッサ ルールを有効にします。設定ページのリンクを使用すると、センシティブ データ ルールにフィルタリングされたビューが [ルール（Rules）] ページに表示されます。このビューで、ルールを有効または無効にしたり、その他のルール属性を設定したりできます。

変更を侵入ポリシーに保存する際に提示されるオプションによって、データ タイプに関連付けられたルールが有効になっていてセンシティブ データ検出が無効になっている場合には、自動的にセンシティブ データ プリプロセッサを有効にすることができます。

詳細については、次の各項を参照してください。

- センシティブ データ検出の導入（25-22 ページ）
- グローバル センシティブ データ検出オプションの選択（25-22 ページ）
- 個別データ タイプ オプションの選択（25-23 ページ）
- 定義済みデータ タイプの使用（25-24 ページ）
- センシティブ データ検出の設定（25-25 ページ）
- モニタするアプリケーション プロトコルの選択（25-27 ページ）
- 特殊な場合：FTP トラフィックでのセンシティブ データの検出（25-29 ページ）
- カスタム データ タイプの使用（25-29 ページ）

センシティブ データ検出の導入

ライセンス：Protection

センシティブ データ検出は、システムのパフォーマンスに非常に大きな影響を与える可能性があるため、Ciscoは以下のガイドラインに従うことを推奨しています。

- デフォルト ポリシー No Rules Active をベースになる侵入ポリシーとして選択します。詳細については、システムによって提供される基本ポリシーについて（16-3 ページ）を参照してください。
- 次の設定が対応するネットワーク分析ポリシーで有効になっていることを確認します。
  - [アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [FTP と Telnet の構成（FTP and Telnet Configuration）]
  - [トランスポートまたはネットワーク レイヤ プロセッサ（Transport/Network Layer Preprocessors）] の下の [IP 最適化（IP Defragmentation）] および [TCP ストリームの構成（TCP Stream Configuration）]
- センシティブ データ設定のある侵入ポリシーを含むアクセス コントロール ポリシーは、センシティブ データ検出用に予約済みのデバイスに適用します。詳細については、設定変更の展開（4-12 ページ）を参照してください。

グローバル センシティブ データ検出オプションの選択

ライセンス：Protection

グローバル センシティブ データ プリプロセッサ オプションは、プリプロセッサの動作を制御します。以下のことを指定するグローバル オプションを変更できます。

- プリプロセッサが、ルールをトリガーしたパケットで、クレジット カード番号または社会保障番号の下位 4 桁を除くすべての桁を置換するかどうか
- センシティブ データをモニタする、ネットワーク上の宛先ホスト
- イベントの生成基準となる、単一のセッションでの全データ タイプの合計オカレンス数

グローバル センシティブ データ オプションはポリシーに固有であり、すべてのデータ タイプに適用されることに注意してください。

次のグローバルなセンシティブ データ検出オプションを設定できます。

マスク（**Mask**）

ルールをトリガーしたパケットで、クレジット カード番号および社会保障番号の下位 4 桁を除くすべての桁を「X」に置換します。ユーザ インターフェイスの侵入イベント パケット ビューおよびダウンロードされたパケットでは、マスクされた番号が表示されます。

ネットワーク

センシティブ データをモニタする 1 つ以上の宛先ホストを指定します。単一の IP アドレス、アドレス ブロック、あるいはこのいずれかまたは両方のカンマ区切りリストを指定できます。空白のフィールドは、`any` として解釈されます。これは、任意の宛先 IP アドレスを意味します。IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-4 ページ）を参照してください。

グローバルしきい値（**Global Threshold**）

グローバルしきい値イベントの生成基準となる、単一セッションでの全データ タイプの合計オカレンス数を指定します。データ タイプの組み合わせを問わず、プリプロセッサは指定された数のデータ タイプを検出すると、グローバルしきい値イベントを生成します。1 ～ 65535 の値を指定できます。

Ciscoでは、このオプションに、ポリシーで有効にする個々のデータ タイプに対するしきい値のどれよりも大きい値を設定することを推奨しています。詳細については、個別データ タイプ オプションの選択（25-23 ページ）を参照してください。

グローバルしきい値については、以下の点に注意してください。

- 複数のデータ タイプを合わせたオカレンス数を検出してイベントを生成するには、プリプロセッサ ルールの 139:1 を有効にする必要があります。侵入ポリシーでルールを有効にする方法については、ルール状態の設定（24-21 ページ）を参照してください。
- プリプロセッサが生成するグローバルしきい値イベントは、セッションあたり最大 1 件です。
- グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立しています。つまり、グローバルしきい値に達すると、個別データ タイプに対するイベントしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も当てはまります。

個別データ タイプ オプションの選択

ライセンス：Protection

個別のデータ タイプによって、指定した宛先ネットワーク トラフィックで検出しイベントを生成できるセンシティブ データを特定します。以下のことを指定するデータ タイプ オプションのデフォルト設定を変更できます。

- 検出されたデータ タイプに対して単一のセッションごとのイベントを生成する基準とするしきい値
- 各データ タイプをモニタする宛先ポート
- 各データ タイプをモニタするアプリケーション プロトコル

最低でも、データ タイプごとにイベントしきい値を指定し、モニタする少なくとも 1 つのポートまたはアプリケーション プロトコルを指定する必要があります。

Ciscoで用意している各定義済みデータ タイプでは、デフォルト値が変更されない限り、アクセス不能な `sd_pattern` キーワードを使用して、トラフィックで検出する組み込みデータ パターンを定義します。定義済みデータ タイプのリストについては、表 25-8（25-25 ページ）を参照してください。カスタム データ タイプを作成して、そのデータ タイプに対し、単純な正規表現を使用して独自のデータ パターンを指定することもできます。詳細については、カスタム データ タイプの使用（25-29 ページ）を参照してください。

データ タイプの名前とパターンはシステム全体に適用されることに注意してください。その他すべてのデータ タイプ オプションはポリシーに固有です。

次の表に、設定できるデータ タイプ オプションを記載します。

表 *25-7*　個別データ タイプ オプション

オプション	説明
データ タイプ	データ タイプの一意の名前を表示します。
しきい値（Threshold）	イベント生成の基準とする、データ タイプのオカレンス数を指定します。有効にしたデータ タイプに対してしきい値を設定せずにポリシーを保存しようとすると、エラー メッセージが表示されます。1 ～ 255 の値を指定できます。 プリプロセッサが検出したデータ タイプに対して生成するイベント数は、セッションごとに 1 つであることに注意してください。グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立していることにも注意してください。つまり、データ タイプ イベントしきい値に達すると、グローバルしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も当てはまります。
宛先ポート（Destination Ports）	データ タイプでモニタする宛先ポートを指定します。単一のポート、複数のポートをカンマで区切ったリスト、または任意の宛先ポートを意味する any を指定できます。データ タイプのルールを有効にした場合、そのデータ タイプに対して少なくとも 1 つのポートまたはアプリケーション プロトコルを設定せずにポリシーを保存しようとすると、エラー メッセージが表示されます。
アプリケーション プロトコル（Application Protocols） この機能には、Control ライセンスが必要です。	データ タイプでモニタする最大 8 つのアプリケーション プロトコルを指定します。データ タイプのルールを有効にした場合、そのデータ タイプに対して少なくとも 1 つのポートまたはアプリケーション プロトコルを設定せずにポリシーを保存しようとすると、エラー メッセージが表示されます。 データ タイプのアプリケーション プロトコルを選択する方法の詳細については、モニタするアプリケーション プロトコルの選択（25-27 ページ）を参照してください。
パターン	カスタム データ タイプの場合、検出するパターンを指定します（Cisco提供のデータ タイプのデータ パターンは事前に定義されています）。詳細については、カスタム データ タイプの使用（25-29 ページ）を参照してください。ユーザ インターフェイスには、定義済みデータ タイプの組み込みパターンは表示されません。 カスタム データ パターンと定義済みデータ パターンは、システム全体に適用されることに注意してください。

定義済みデータ タイプの使用

ライセンス：Protection

それぞれの侵入ポリシーには、よく使用されるデータ パターンを検出するために事前に定義されたデータ タイプが含まれています。これらのデータ パターンには、クレジット カード番号、電子メールアドレス、米国の電話番号、および米国の社会保障番号などがあります（番号にはハイフン付きのパターン、ハイフン抜きのパターンがあります）。各定義済みデータ タイプは、ジェネレータ ID（GID）が 138 に設定された単一のセンシティブ データ プリプロセッサに関連付けられます。ポリシーで使用する各データ タイプに対し、検出およびイベント生成を有効にするには、侵入ポリシーで関連付けられたセンシティブ データ ルールを有効にする必要があります。侵入ポリシーでルールを有効にする方法については、ルール状態の設定（24-21 ページ）を参照してください。

センシティブ データ ルールを有効にするには、設定ページに表示されるリンクを利用できます。このリンクを使用すると、すべての定義済みセンシティブ データ ルールおよびカスタム センシティブ データ ルールを表示するフィルタリングされたビューの [ルール(Rules)] ページが表示されます。また、センシティブ データ ルールのフィルタ カテゴリを選択して、[ルール(Rules)] ページに定義済みセンシティブ データ ルールだけを表示することもできます。詳細については、侵入ポリシー内のルールのフィルタリング(24-10 ページ)を参照してください。定義済みセンシティブ データ ルールは、[ルール エディタ(Rule Editor)] ページ([ポリシー(Policies)] > [侵入(Intrusion)] > [ルール エディタ(Rule Editor)])にもリストされます。このページでは、センシティブ データ ルール カテゴリに属する定義済みセンシティブ データ ルールを確認できますが、これらのルールを編集することはできません。

以下の表に、データ タイプを記載し、各データ タイプを検出してイベントを生成するために有効にしなければならない、対応するプリプロセッサ ルールをリストします。

表 **25-8**　センシティブ データ タイプ

データ タイプ	説明	プリプロセッサ ルール **GID:SID**
クレジット カード番号	Visa®、MasterCard®、Discover®、および American Express® の 15 桁または 16 桁のクレジット カード番号(通常の区切り文字として使用されるハイフンまたはスペースが含まれるパターンと含まれないパターン)に一致します。また、Luhn アルゴリズムを使用してクレジット カード番号の検査数字を確認します。	138:2
電子メール アドレス	電子メール アドレスに一致します。	138:5
米国の電話番号	米国の電話番号(`(\d\{3\}) ?\d\{3\}-\d\{4\}` のパターンに準拠)に一致します。	138:6
米国の社会保障番号(ハイフンなし)	米国の 9 桁の社会保障番号(有効な 3 桁のエリア番号と有効な 2 桁のグループ番号が含まれ、ハイフンを使用していない番号)に一致します。	138:4
米国の社会保障番号(ハイフンあり)	米国の 9 桁の社会保障番号(有効な 3 桁のエリア番号と有効な 2 桁のグループ番号が含まれ、ハイフンを使用した番号)に一致します。	138:3
カスタム(Custom)	指定されたトラフィックでユーザ定義のデータ パターンに一致します。詳細については、カスタム データ タイプの使用(25-29 ページ)を参照してください。	138:>999999

社会保障番号以外の 9 桁の番号からの誤検出を軽減するために、プリプロセッサでは、各社会保障番号の 4 桁のシリアル番号の前にある 3 桁のエリア番号と 2 桁のグループ番号を検証するアルゴリズムを使用します。プリプロセッサは 2009 年 11 月末までの社会保障グループ番号を検証します。

センシティブ データ検出の設定

ライセンス:Protection

デフォルトのグローバル設定および個別データ タイプの設定を変更できます。検出する各データ タイプのプリプロセッサ ルールを有効にする必要もあります。

ポリシーでセンシティブ データ プリプロセッサ ルールを有効にして、センシティブ データ検出を有効にしていなければ、変更をポリシーに保存する際に、センシティブ データ検出を有効にするよう求めるプロンプトが出されます。詳細については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

以下の表に、[センシティブ データの検出（Sensitive Data Detection）] ページで実行できる操作を記載します。

表 **25-9**　センシティブ データ設定の操作

目的	操作
グローバル設定を変更する	ユーザが変更できるグローバル設定については、表 25-6（25-9 ページ）を参照してください。
データ タイプ オプションを変更する	[ターゲット（Targets）] ページ領域で、データ タイプの名前をクリックします。 [設定（Configuration）] ページ領域が更新され、データ タイプの現在の設定が表示されます。ユーザが変更できるオプションについては、個別データ タイプ オプションの表を参照してください。
データ タイプでモニタするアプリケーション プロトコルを追加または削除する この機能には、Control ライセンスが必要です。	[アプリケーション プロトコル（Application Protocols）] フィールド内をクリックするか、このフィールドの横にある [編集（Edit）] をクリックします。[アプリケーション プロトコル（Application Protocols）] ポップアップ ウィンドウが表示されます。 • モニタするアプリケーション プロトコル（最大 8 つ）を追加するには、左側の [選択可能（Available）] リストからアプリケーション プロトコルを 1 つ以上選択して、右矢印（>）ボタンをクリックします。 • アプリケーション プロトコルを削除するには、右側の [有効（Enabled）] リストから削除するアプリケーション プロトコルを選択して、左矢印（<）ボタンをクリックします。 複数のアプリケーション プロトコルを選択する場合は、Ctrl または Shift キーを押しながらクリックします。また、クリックしてドラッグすることによって、隣接する複数のアプリケーション プロトコルを選択することもできます。 （注）　FTP トラフィックでセンシティブ データを検出するには、`Ftp data` アプリケーション プロトコルを追加する必要があります。詳細については、特殊な場合：FTP トラフィックでのセンシティブ データの検出（25-29 ページ）を参照してください。
カスタム データ タイプを作成する	ページ左側の [データ タイプ（Data Types）] の横にある [+] 記号をクリックします。[データ タイプの追加（Add Data Type）] ポップアップ ウィンドウが表示されます。 データ タイプの一意の名前と、このデータ タイプで検出するパターンを指定して、[OK] をクリックします。編集を破棄するには [キャンセル（Cancel）] をクリックします。詳細については、カスタム データ タイプの使用（25-29 ページ）を参照してください。
センシティブ データ プリプロセッサ ルールを表示する	[グローバル設定（Global Settings）] ページ領域の上に表示されている [センシティブ データ検出ルールの設定（Configure Rules for Sensitive Data Detection）] リンクをクリックします。[ルール（Rules）] ページの表示がフィルタリングされ、すべてのセンシティブ データ プリプロセッサ ルールのリストが表示されます。 オプションで、リストされているルールを有効または無効にすることができます。侵入ポリシーで使用する各データ タイプのセンシティブ データ プリプロセッサ ルールを有効にする必要があることに注意してください。詳細については、ルール状態の設定（24-21 ページ）を参照してください。 [ルール（Rules）] ページで使用可能なその他の操作（ルールの抑制、レート ベース攻撃の防止など）のセンシティブ データ ルールも設定できます。詳細については、ルールを使用した侵入ポリシーの調整（24-1 ページ）を参照してください。 [戻る（Back）] をクリックして [センシティブ データの検出（Sensitive Data Detection）] ページに戻ります。

センシティブ データ検出を設定する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [詳細設定(Advanced Settings)] をクリックします。

[詳細設定(Advanced Settings)] ページが表示されます。

ステップ 4　[特定の脅威検知(Specific Threat Detection)] の下にある [センシティブ データの検出(Sensitive Data Detection)] が有効になっているかどうかによって、2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[センシティブ データの検出(Sensitive Data Detection)] ページが表示されます。ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(16-1 ページ)を参照してください。

ステップ 5　センシティブ データ設定の操作の表で説明されている操作を実行できます。

ステップ 6　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

モニタするアプリケーション プロトコルの選択

ライセンス:Control

各データ タイプでモニタするアプリケーション プロトコルを最大 8 つ指定できます。

各データ タイプをモニタするアプリケーション プロトコルまたはポートを少なくとも 1 つ指定する必要があります。ただし、FTP トラフィックでセンシティブ データを検出する場合を除き、Ciscoでは最も包括的なカバレッジにするために、アプリケーション プロトコルを指定する際には対応するポートを指定することを推奨しています。たとえば、HTTP を指定する場合は、既知の HTTP ポート 80 も設定します。このように設定すると、ネットワークの新しいホストが HTTP を実装する場合には、システムは新しい HTTP アプリケーション プロトコルを検出する間、ポート 80 をモニタします。

FTP トラフィックでセンシティブ データを検出する場合は、`FTP data` アプリケーション プロトコルを指定する必要があります。ポート番号を指定する利点はありません。詳細については、特殊な場合:FTP トラフィックでのセンシティブ データの検出(25-29 ページ)を参照してください。

センシティブ データを検出するためにアプリケーション プロトコルを変更する方法:
Admin/Intrusion Admin

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [詳細設定(Advanced Settings)] をクリックします。

[詳細設定(Advanced Settings)] ページが表示されます。

ステップ 4　[特定の脅威検知(Specific Threat Detection)] の下にある [センシティブ データの検出(Sensitive Data Detection)] が有効になっているかどうかによって、2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[センシティブ データの検出(Sensitive Data Detection)] ページが表示されます。

ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(16-1 ページ)を参照してください。

ステップ 5　[データ タイプ(Data Types)] にリストされているデータ タイプ名をクリックして、変更するデータ タイプを選択します。

[設定(Configuration)] 領域が更新されて、選択したデータ タイプの現在の設定が表示されます。

ステップ 6　[アプリケーション プロトコル(Application Protocols)] フィールド内をクリックするか、このフィールドの横にある [編集(Edit)] をクリックします。

[アプリケーション プロトコル(Application Protocols)] ポップアップ ウィンドウが表示されます。

ステップ 7　次の 2 つの選択肢があります。

- モニタするアプリケーション プロトコル(最大 8 つ)を追加するには、左側の [選択可能(Available)] リストからアプリケーション プロトコルを 1 つ以上選択して、右矢印(>)ボタンをクリックします。
- アプリケーション プロトコルを削除するには、右側の [有効(Enabled)] リストから削除するアプリケーション プロトコルを選択して、左矢印(<)ボタンをクリックします。

複数のアプリケーション プロトコルを選択する場合は、Ctrl または Shift キーを押しながらクリックします。また、クリックしてドラッグすることによって、隣接する複数のアプリケーション プロトコルを選択することもできます。

(注)　FTP トラフィックでセンシティブ データを検出するには、`FTP data` アプリケーション プロトコルを追加する必要があります。詳細については、特殊な場合:FTP トラフィックでのセンシティブ データの検出(25-29 ページ)を参照してください。

ステップ 8　[OK] をクリックしてアプリケーション プロトコルを追加します。

[センシティブ データの検出(Sensitive Data Detection)] ページが表示され、アプリケーション プロトコルが更新されます。

特殊な場合：FTP トラフィックでのセンシティブ データの検出

ライセンス：Control

一般に、センシティブ データをモニタするトラフィックを決めるには、導入でのモニタ対象のポートを指定するか、あるいはオプションで、アプリケーション プロトコルを指定します。ただし、FTP トラフィックでセンシティブ データを検出するには、ポートまたはアプリケーション プロトコルを指定するだけでは不十分です。FTP トラフィックのセンシティブ データは、FTP アプリケーション プロトコルのトラフィックで検出されますが、FTP アプリケーション プロトコルは断続的に発生し、一時的なポート番号を使用するため、センシティブ データを検出するのが困難です。FTP トラフィックでセンシティブ データを検出するには、以下の設定を含めることが必須となります。

- `FTP data` アプリケーション プロトコルを指定します。

  `FTP data` アプリケーション プロトコルを指定すると、FTP トラフィックでのセンシティブ データの検出が可能になります。詳細については、モニタするアプリケーション プロトコルの選択（25-27 ページ）を参照してください。

  FTP トラフィックでセンシティブ データを検出するという特殊な場合では、`FTP data` アプリケーション プロトコルを指定すると、検出が呼び出される代わりに、FTP トラフィックでセンシティブ データを検出するために FTP/Telnet プロセッサの高速処理が呼び出されます。詳細については、FTP および Telnet トラフィックのデコード（19-20 ページ）を参照してください。

- 設定に、センシティブ データをモニタするポートが少なくとも 1 つ含まれていることを確認します。

  FTP トラフィックでセンシティブ データを検出することだけが目的の場合を除き（そのような場合はほとんどありません）、FTP ポートを指定する必要はありません。通常のセンシティブ データ設定には、HTTP ポートや電子メール ポートなどの他のポートが含まれることになります。モニタ対象の FTP ポートを 1 つだけ指定し、他のポートを指定しない場合、Cisco では、FTP コマンド ポート `23` を指定することを推奨しています。詳細については、センシティブ データ検出の設定（25-25 ページ）を参照してください。

カスタム データ タイプの使用

ライセンス：Protection

指定するデータ パターンを検出するためのカスタム データ タイプを作成および変更することができます。たとえば、病院で患者番号を保護するためのデータ タイプを作成したり、大学で固有の番号パターンを持つ学生番号を検出するためのデータ タイプを作成したりすることが考えられます。

作成するカスタム データ タイプごとに、単一のセンシティブ データ プリプロセッサ ルールも作成します。このルールのジェネレータ ID（GID）は 138 で、Snort ID は 1000000 以上（これは、ローカル ルールの SID）です。ポリシーで特定のデータ タイプを検出してイベントを生成するには、そのカスタム データ タイプに関連付けられたセンシティブ データ ルールを有効にする必要があります。侵入ポリシーでルールを有効にする方法については、ルール状態の設定（24-21 ページ）を参照してください。

センシティブ データ ルールを有効にするには、設定ページに表示されるリンクを利用できます。このリンクを使用すると、すべての定義済みセンシティブ データ ルールおよびカスタム センシティブ データ ルールを表示するフィルタリングされたビューの [ルール（Rules）] ページが表示されます。また、[ルール（Rules）] ページでローカル ルールのフィルタリング カテゴリを選択することで、カスタム センシティブ データ ルールをローカル カスタム ルールとともに表示できます。詳細については、侵入ポリシー内のルールのフィルタリング（24-10 ページ）を参照してください。カスタム センシティブ データ ルールは、[ルール エディタ（Rule Editor）] ページには表示されないことに注意してください。

作成するカスタム データ タイプは、すべての侵入ポリシーに追加されます。特定のカスタム データ タイプを検出してイベントを生成するには、使用するポリシーで、そのカスタム データ タイプに関連付けられたセンシティブ データ ルールを有効にする必要があります。

データ タイプとそのデータ タイプに関連付けるルールを作成するには、[センシティブ データの検出（Sensitive Data Detection）] 設定ページを使用する必要があることに注意してください。ルール エディタを使用してセンシティブ データ ルールを作成することはできません。

詳細については、次の各項を参照してください。

- カスタム データ タイプのデータ パターンの定義（25-30 ページ）
- カスタム データ タイプの設定（25-32 ページ）
- カスタム データ タイプの名前と検出パターンの編集（25-33 ページ）

カスタム データ タイプのデータ パターンの定義

ライセンス：Protection

カスタム データ タイプのデータ パターンを定義するには、以下の要素からなる単純な正規表現のセットを使用します。

- 3 つのメタ文字
- メタ文字をリテラル文字として使用するためのエスケープ文字
- 6 文字クラス

メタ文字は正規表現内で特別な意味を持つリテラル文字です。以下の表に、カスタム データ パターンを定義する際に使用できるメタ文字を記載します。

表 **25-10**　センシティブ データ パターンのメタ文字

メタ文字	説明	例
`?`	先行する文字またはエスケープ シーケンスのゼロまたは 1 つのオカレンスに一致します。つまり、先行する文字またはエスケープ シーケンスはオプションです。	`colou?r` は、`color` または `colour` に一致します。
`{n}`	先行する文字またはエスケープ シーケンスの *n* 回の繰り返しに一致します。	次の例を参考にしてください。 `\d{2}` は、`55`、`12` などに一致します。 `\l{3}` は、`AbC`、`www` などに一致します。 `\w{3}` は、`a1B`、`25C` などに一致します。 `x{5}` は、`xxxxx` に一致します。
`\`	メタ文字を実際の文字として使用できます。また、事前定義された文字クラスを指定するためにも使われます。センシティブ データ パターンで使用できる文字クラスについては、表 25-12（25-31 ページ）を参照してください。	`\?` は疑問符に一致します。 `\\` はバックスラッシュに一致します。 `\d` は数字に一致します。

以下の表に記載する文字をリテラル文字としてセンシティブ データ プリプロセッサに正しく解釈させるには、バックスラッシュで文字をエスケープする必要があります。

表 **25-11**　センシティブ データ パターンのエスケープ文字

使用するエスケープ文字	表現されるリテラル文字
\?	?
\{	{
\}	}
\\	\

以下の表に、カスタム センシティブ データ パターンを定義する際に使用できる文字クラスを記載します。

表 **25-12**　センシティブ データ パターンの文字クラス

文字クラス	説明	文字クラスの定義
\d	ASCII 文字の数字 0 ～ 9 に一致します。	0 ～ 9
\D	ASCII 文字の数字ではないバイトに一致します。	0 ～ 9 以外
\l（小文字の「エル」）	任意の ASCII 文字に一致します。	a-zA-Z
\L	ASCII 文字ではないバイトに一致します。	a-zA-Z 以外
\w	任意の ASCII 英数字に一致します。 PCRE 正規表現とは異なり、アンダースコア（_）は含まれないことに注意してください。	a-zA-Z0-9
\W	ASCII 英数字でないバイトに一致します。	a-zA-Z0-9 以外

プリプロセッサは、そのまま入力された文字を、正規表現の一部ではなく、リテラル文字として扱います。たとえば、データ パターン 1234 は `1234` に一致します。

以下に、定義済みセンシティブ データ ルール 138:4 で使用するデータ パターンの例を示します。このパターンでは、エスケープされた数値の文字クラス、複数個を示すメタ文字およびオプション指定子のメタ文字、リテラル ハイフン（-）文字、および左右の括弧 () 文字を使用して、米国の電話番号を検出します。

```
(\d{3}) ?\d{3}-\d{4}
```

カスタム データ パターンを作成する際には注意が必要です。以下に、電話番号を検出するための別のデータ パターンを示します。このパターンでは有効な構文を使用しているものの、多数の誤検出が発生する可能性があります。

```
(?\d{3})? ?\d{3}-?\d{4}
```

上記の 2 番目の例では、オプションの括弧、オプションのスペース、オプションのハイフンを組み合わせているため、目的とする以下のパターンの電話番号が検出されます。

- `(555)123-4567`
- `555123-4567`
- `5551234567`

ただし、2 番目の例のパターンでは、以下の潜在的に無効なパターンも検出されて、結果的に誤検出となります。

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

最後に、説明目的の極端な例として、小規模な企業ネットワーク上のすべての宛先トラフィックで小さいイベントしきい値を使用して、小文字の a を検出するデータ パターンを作成するとします。このようなデータ パターンは、わずか数分で文字通り数百万ものイベントを生成することになり、システムを過負荷に陥らせる可能性があります。

カスタム データ タイプの設定

ライセンス：Protection

基本的には、カスタム データ タイプにも、定義済みデータ タイプを設定する場合と同じデータ タイプ オプションを設定します。すべてのデータ タイプに共通の設定オプションを設定する方法については、個別データ タイプ オプションの選択（25-23 ページ）を参照してください。また、カスタム データ タイプにも名前とデータ パターンを指定する必要があります。

カスタム データ タイプを作成すると、そのカスタム データ タイプに関連付けられたカスタム センシティブ データ プリプロセッサ ルールが作成されます。このルールは、カスタム データ タイプを使用する各ポリシーで有効にしなければならないことに注意してください。侵入ポリシーでルールを有効にする方法については、ルール状態の設定（24-21 ページ）を参照してください。

カスタム データ タイプを作成または変更する方法：

Admin/Intrusion Admin

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [詳細設定（Advanced Settings）] をクリックします。

[詳細設定（Advanced Settings）] ページが表示されます。

ステップ 4　[特定の脅威検知（Specific Threat Detection）] の下にある [センシティブ データの検出（Sensitive Data Detection）] が有効になっているかどうかによって、2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[センシティブ データの検出（Sensitive Data Detection）] ページが表示されます。

ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 5　次の選択肢があります。

- カスタム データ タイプを作成するには、ページ左側の [データ タイプ（Data Types）] の横にある [+] 記号をクリックします。[データ タイプの追加（Add Data Type）] ポップアップ ウィンドウが表示されます。

  データ タイプの一意の名前と、このデータ タイプで検出するパターンを指定して、[OK] をクリックします。編集を破棄するには [キャンセル（Cancel）] をクリックします。詳細については、カスタム データ タイプの名前と検出パターンの編集（25-33 ページ）を参照してください。

  [センシティブ データの検出（Sensitive Data Detection）] ページが表示されます。[OK] をクリックすると、ページが更新されて変更が反映されます。

- 定義済みデータ タイプとカスタム データ タイプに共通のオプションを変更するには、[ターゲット(Targets)] ページ領域でデータ タイプ名をクリックします。

  [設定(Configuration)] ページ領域が更新され、データ タイプの現在の設定が表示されます。詳細については、センシティブ データ検出の設定(25-25 ページ)を参照してください。
- システム全体に適用されるカスタム データ タイプの名前およびデータ パターンを編集するには、カスタム データ タイプの名前と検出パターンの編集(25-33 ページ)を参照してください。
- カスタム データ タイプを削除するには、削除するデータ タイプの横にある削除アイコン( )をクリックしてから、[OK] をクリックします。データ タイプの削除を中止する場合は、[キャンセル(Cancel)] をクリックします。

  データ タイプのセンシティブ データ ルールがいずれかの侵入ポリシーで有効にされている場合、そのデータ タイプを削除することはできません。カスタム データ タイプを削除すると、そのカスタム データ タイプはすべての侵入ポリシーから削除されます。

カスタム データ タイプの名前と検出パターンの編集

ライセンス:Protection

システム全体に適用されるカスタム センシティブ データ ルールの名前および検出パターンを変更できます。これらの設定を変更すると、システム上の他のすべてのポリシーに変更が適用されます。変更したカスタム データ タイプを使用する侵入ポリシーが含まれるアクセス コントロール ポリシーを再適用する必要があることにも注意してください。

カスタム データ タイプの名前とデータ パターンを除き、カスタム データ タイプと定義済みデータ タイプのすべてのデータ タイプ オプションは、ポリシーに固有です。カスタム データ タイプで名前とデータ パターンを除くオプションを変更する方法については、個別データ タイプ オプションの選択(25-23 ページ)を参照してください。

カスタム データ タイプの名前およびデータ パターンを編集する方法:

Admin/Intrusion Admin

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [詳細設定(Advanced Settings)] をクリックします。

[詳細設定(Advanced Settings)] ページが表示されます。

ステップ 4　[特定の脅威検知(Specific Threat Detection)] の下にある [センシティブ データの検出(Sensitive Data Detection)] が有効になっているかどうかによって、2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[センシティブ データの検出（Sensitive Data Detection）] ページが表示されます。

ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 5　[ターゲット（Targets）] ページ領域で、変更するカスタム データ タイプの名前をクリックします。

ページが更新されて、データ タイプの現在の設定が表示されます。また、[設定（Configuration）] ページ領域の右上隅に、[データ タイプの名前およびパターンの編集（Edit Data Type Name and Pattern）] リンクが表示されます。

ステップ 6　[データ タイプの名前およびパターンの編集（Edit Data Type Name and Pattern）] リンクをクリックします。

[データ タイプの編集（Edit Data Type）] ポップアップ ウィンドウが表示されます。

ステップ 7　データ タイプの名前、パターン、またはその両方を変更して、[OK] をクリックします。編集を破棄する場合は、[キャンセル（Cancel）] をクリックします。データ パターンを指定する方法については、カスタム データ タイプのデータ パターンの定義（25-30 ページ）を参照してください。

[センシティブ データの検出（Sensitive Data Detection）] ページが表示されます。[OK] をクリックすると、ページに変更が反映されます。

侵入イベント ロギングのグローバルな制限

システムが侵入イベントを記録して表示する回数を制限するしきい値を使用できます。侵入ポリシーの一部としてしきい値を設定すると、ルールに一致するトラフィックが指定期間内に特定のアドレスまたはアドレス範囲で送受信される回数に基づいて、イベントが生成されます。これにより、多数のイベントでいっぱいになることを回避できます。この機能を使用するには Protection ライセンスが必要です。

イベント通知しきい値は、次の 2 種類の方法で設定できます。

- すべてのトラフィックに対するグローバルしきい値を設定して、指定された期間に特定の送信元または宛先からのイベントが記録され表示される頻度を制限できます。詳細については、しきい値について（26-1 ページ）およびグローバルしきい値の設定（26-3 ページ）を参照してください。
- 侵入ポリシー設定での共有オブジェクトのルール、標準テキスト ルール、プリプロセッサ ルールごとにしきい値を設定できます。イベントしきい値の設定（24-23 ページ）を参照してください。

しきい値について

ライセンス：Protection

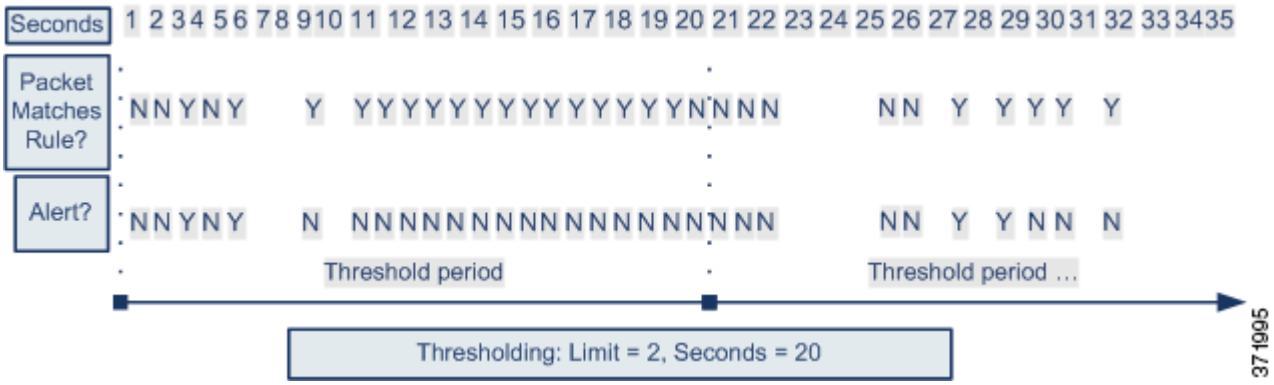
デフォルトでは、侵入ポリシーごとに、グローバル ルールしきい値が含まれます。デフォルトのしきい値では、各ルールのイベント生成が、同じ宛先に送られるトラフィックで 60 秒あたり 1 つのイベントに制限されます。このグローバルしきい値は、デフォルトですべての侵入ルールとプリプロセッサ ルールに適用されます。しきい値は侵入ポリシーの [詳細設定（Advanced Settings）] ページで無効にできることに注意してください。

特定のルールで個々のしきい値を設定することにより、このしきい値を上書きすることもできます。たとえば、グローバル制限しきい値を 60 秒ごとに 5 個のイベントに設定してから、SID 1315 について特定のしきい値として 60 秒ごとに 10 個のイベントに設定できます。他のすべてのルールでは 60 秒ごとに 6 個以上のイベントは生成されませんが、SID 1315 では 60 秒ごとに最大 10 個のイベントが生成されます。

ルール ベースのしきい値の設定の詳細については、イベントしきい値の設定（24-23 ページ）を参照してください。

次の図は、特定のルールに関して攻撃を受けている例を示します。グローバル制限しきい値では、各ルールのイベント生成が、20 秒あたり 2 つのイベントに制限されます。

期間は 1 秒で始まり 21 秒で終わることに注意してください。期間が終了すると、サイクルが再び開始され、次の 2 つのルール一致によってイベントが生成されます。その後、その期間にさらにイベントが生成されることはありません。



しきい値のオプションについて

ライセンス：Protection

しきい値を使用して、期間内に特定数のイベントのみが生成されるように制限するか、イベントセットごとに 1 つのイベントが生成されるように制限することで、侵入イベントの生成を制限できます。グローバルしきい値を設定する際は、最初にしきい値のタイプを指定する必要があります。以下の表を参照してください。

表 ***26-1***　　しきい値設定オプション

オプション	説明
制限（Limit）	指定された数のパケット（count 引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [制限（Limit）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。
しきい値（Threshold）	指定された数のパケット（count 引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [しきい値（Threshold）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[秒（Seconds）] と [カウント（Count）] のカウンタを 0 にリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。
両方	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [両方（Both）] に、[カウント（Count）] を 2 に、[秒（Seconds）] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される）。

次に、トラッキングを指定します。これにより、イベント インスタンスの数が送信元 IP アドレスと宛先 IP アドレスのどちらに基づいて計算されるかが決まります。最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 *26-2*　　インスタンス/時間のしきい値設定オプション

オプション	説明
メンバー数（Count）	しきい値を満たすために必要な、トラッキング IP アドレスまたはアドレス範囲ごとの、指定された期間でのイベント インスタンスの数。
秒（Seconds）	カウントがリセットされるまでの秒数。しきい値タイプを [制限（Limit）] に、トラッキングを [送信元（Source）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 10 に設定した場合、特定の送信元ポートで 10 秒間に発生した最初の 10 のイベントを記録し表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。

グローバルしきい値の設定

ライセンス：Protection

一定の期間に各ルールによって生成されるイベントの数を管理するために、グローバルしきい値を設定できます。グローバルしきい値を設定すると、特定のしきい値を上書きしない各ルールでそのしきい値が適用されます。しきい値の設定の詳細については、しきい値について（26-1 ページ）を参照してください。

デフォルトでは、ユーザのシステムにグローバルしきい値が設定されます。デフォルト値は次のとおりです。

- タイプ（Type）：制限（Limit）
- 追跡対象（Track By）：宛先（Destination）
- カウント（Count）：1
- 秒（Seconds）：60

グローバルしきい値の設定方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [詳細設定（Advanced Settings）] をクリックします。

[詳細設定（Advanced Settings）] ページが表示されます。

ステップ 4　[侵入ルールしきい値（Intrusion Rule Thresholds）] の [グローバル ルールのしきい値構成（Global Rule Thresholding）] が有効になっているかどうかに応じて、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[グローバル ルールのしきい値構成（Global Rule Thresholding）] ページが表示されます。ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 5　[タイプ（Type）] オプション ボタンから、seconds 引数で指定された時間内に適用するしきい値のタイプを選択します。詳細については、しきい値設定オプションの表を参照してください。

- count 引数で指定された制限を超えるまで、ルールをトリガーとして使用したパケットごとにイベントを記録して表示する場合、[制限（Limit）] を選択します。
- ルールをトリガーとして使用し、count 引数で設定されたしきい値と同じかその倍数であるインスタンスを表すパケットごとに 1 つのイベントを記録して表示する場合、[しきい値（Threshold）] を選択します。
- count 引数によって指定された数のパケットがルールをトリガーとして使用した後に 1 つのイベントを記録して表示する場合、[両方（Both）] を選択します。

ステップ 6　[追跡対象（Track By）] ドロップダウンリストからトラッキング方法を選択します。

- 特定の送信元 IP アドレスからのトラフィックでルールの一致を識別するには、[送信元（Source）] を選択します。
- 特定の宛先 IP アドレスへのトラフィックでルールの一致を識別するには、[宛先（Destination）] を選択します。

ステップ 7　[カウント（Count）] フィールドで以下を実行します。

- [制限（Limit）] しきい値では、しきい値を満たすために必要な、追跡する IP アドレス単位で指定された期間単位のイベント インスタンスの数を指定します。
- [しきい値（Threshold）] しきい値では、しきい値として使用するルールの一致回数を指定します。

ステップ 8　[秒（Seconds）] フィールドで以下を実行します。

- [制限（Limit）] しきい値では、攻撃を追跡する期間の秒数を指定します。
- [しきい値（Threshold）] しきい値では、カウントをリセットするまでの経過時間（秒数）を指定します。指定された秒数が経過する前であっても、[カウント（Count）] フィールドで示されている数のルールが一致すると、カウントはリセットされるのでご注意ください。

ステップ 9　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

グローバルしきい値の無効化

ライセンス：Protection

デフォルトでは、グローバル制限しきい値は、宛先へのトラフィックでのイベントの数を 60 秒あたり 1 個のイベントに制限しています。デフォルトで特定のルールに関するイベントにしきい値を適用し、すべてのルールにしきい値を適用しない場合、最高位のポリシー階層でグローバルしきい値を無効にできます。

グローバルしきい値を無効にする方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

ステップ 3　左側のナビゲーション パネルで [設定(Settings)] をクリックします。

[設定(Settings)] ページが表示されます。

ステップ 4　[侵入ルールしきい値(Intrusion Rule Thresholds)] で、[グローバル ルールのしきい値構成(Global Rule Thresholding)] を無効化します。

ステップ 5　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、競合の解決とポリシー変更の確定(15-15 ページ)を参照してください。

侵入ルールの概要と作成

侵入ルールは特定のキーワードと引数のセットです。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それがルール内の基準を満たしているかどうか検査することにより、ネットワークの脆弱性を悪用しようとする試みを検出できます。システムは各ルールで指定された条件をパケットに照らし合わせます。ルールで指定されたすべての条件にパケット データが一致する場合、ルールがトリガーされます。ルールがアラート ルールである場合は、侵入イベントが生成されます。パス ルールである場合は、トラフィックが無視されます。侵入イベントは、ASA FirePOWER モジュール インターフェイスから表示して評価できます。

注意 作成した侵入ルールを実稼働環境で使用する前に、制御されたネットワーク環境で必ずテストしてください。不適切に作成された侵入ルールは、システムのパフォーマンスに重大な影響を与える可能性があります。

次の点に注意してください。

- インライン展開の廃棄ルールでは、システムがパケットを破棄してイベントを生成します。廃棄ルールの詳細については、ルール状態の設定（24-21 ページ）を参照してください。
- シスコ は、2 つのタイプの侵入ルール 共有オブジェクトのルール と 標準テキスト ルール を提供します。シスコ 脆弱性調査チーム（VRT）は 共有オブジェクトのルール を使用することで、従来の 標準テキスト ルール では不可能な方法で脆弱性に対する攻撃を検出できます。共有オブジェクトのルール を作成することはできません。独自の侵入ルールを作成するときには、標準テキスト ルール を作成します。

発生する可能性のあるイベントのタイプを調整するために、カスタム 標準テキスト ルール を作成することができます。このマニュアルでは特定のエクスプロイトの検出を目的とするルールについて説明することもありますが、優秀なルールのほとんどは、特定の既知のエクスプロイトではなく既知の脆弱性を悪用しようとするトラフィックをターゲットとすることに注意してください。ルールを作成してルールのイベント メッセージを指定することにより、攻撃とポリシー回避を示唆するトラフィックをより簡単に識別できます。イベントの評価の詳細については、イベントの表示（34-1 ページ）を参照してください。

カスタム侵入ポリシーでカスタム標準テキスト ルールを有効にすると、一部のルール キーワードと引数では、トラフィックを特定の方法で最初に復号化または前処理する必要があることに留意してください。この章では、前処理を制御するネットワーク分析ポリシーで設定する必要があるオプションについて説明します。必要なプリプロセッサを無効にすると、システムは現在の設定で自動的にそのプリプロセッサを使用しますが、ネットワーク分析ポリシーの ユーザ インターフェイスではプリプロセッサは無効のままになることに注意してください。

（注） 前処理インスペクションと侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは互いに補完する必要があります。特に複数のカスタム ネットワーク分析ポリシーを使用した前処理の調整は、高度なタスクです。詳細については、カスタム ポリシーに関する制約事項（15-12 ページ）を参照してください。

詳細については、次の各項を参照してください。

- ルール構造について（27-2 ページ）では、ルール ヘッダーやルール オプションなど、有効な標準テキスト ルール を構成するコンポーネントについて説明します。
- ルール ヘッダーについて（27-3 ページ）では、ルール ヘッダーの内容について詳しく説明します。
- ルールでのキーワードと引数について（27-10 ページ）では、ASA FirePOWER モジュールで使用可能な侵入ルール キーワードの使い方と構文について説明します。
- ルールの構築（27-105 ページ）では、ルール エディタを使用して新しいルールを作成する方法を説明します。
- [ルール エディタ（Rule Editor）] ページでのルールのフィルタ処理（27-110 ページ）では、特定のルールを見つけやすくするためにルールのサブセットを表示する方法について説明します。

ルール構造について

ライセンス：Protection

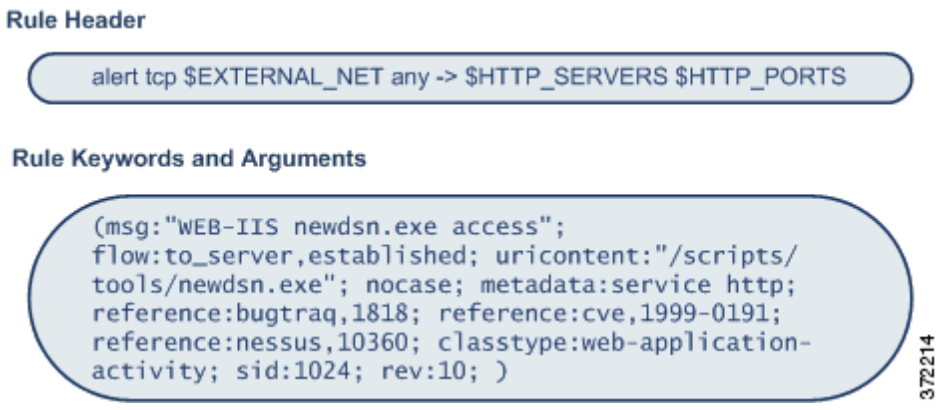
すべての 標準テキスト ルール には、ルール ヘッダーとルール オプションという 2 つの論理セクションが含まれています。ルール ヘッダーの内容は次のとおりです。

- ルールのアクションまたはタイプ
- プロトコル
- 送信元および宛先の IP アドレスとネットマスク
- 送信元から宛先へのトラフィック フローを示す方向インジケータ
- 送信元ポートと宛先ポート

ルール オプション セクションの内容は次のとおりです。

- イベント メッセージ
- キーワードとそのパラメータおよび引数
- ルールをトリガーとして使用するためにパケットのペイロードが一致しなければならないパターン
- パケットのどの部分をルール エンジンで検査するかの指定

次の図に、ルールの構成要素を示します。



ルールのオプション セクションは、カッコで囲まれたセクションであることに注意してください。ルール エディタは、標準テキスト ルール の作成を支援する使いやすいインターフェイスを備えています。

ルール ヘッダーについて

ライセンス：Protection

それぞれの 標準テキスト ルール と 共有オブジェクトのルール には、パラメータと引数からなるルール ヘッダーが含まれています。ルール ヘッダーの構成要素を以下に示します。

次の表では、上記のルール ヘッダーの各部分について説明します。

表 *27-1*　ルール ヘッダーの値

ルール ヘッダーのコンポーネント	値の例	機能
操作	`alert`	トリガー時に侵入イベントを生成します。
プロトコル	`tcp`	TCP トラフィックのみをテストします。
送信元 IP アドレス	`$EXTERNAL_NET`	内部ネットワーク上に存在しないホストから送られてきたトラフィックをテストします。
送信元ポート	任意	発信元ホスト上の任意のポートから送られてきたトラフィックをテストします。
演算子	`->`	（このネットワーク上の Web サーバに向かう）外部トラフィックをテストします。
宛先 IP アドレス	`$HTTP_SERVERS`	この内部ネットワーク上の Web サーバとして指定された任意のホストに送られるトラフィックをテストします。
宛先ポート	`$HTTP_PORTS`	この内部ネットワーク上の HTTP ポートに送られるトラフィックをテストします。

（注）　前述の例では、ほとんどの侵入ルールの場合と同様に、デフォルト変数が使用されています。変数のリスト、機能、および設定方法の詳細については、変数セットの使用（2-15 ページ）を参照してください。

ルール ヘッダー パラメータの詳細については、以下の項を参照してください。

- ルール アクションの指定（27-4 ページ）では、ルール タイプについて説明し、ルールのトリガー時に実行されるアクションを指定する方法について説明します。

- プロトコルの指定（27-4 ページ）では、ルールによるテスト対象となるトラフィックのトラフィック プロトコルを定義する方法について説明します。
- 侵入ルールでの IP アドレスの指定（27-5 ページ）では、ルール ヘッダーで個別の IP アドレスと IP アドレス ブロックを定義する方法について説明します。
- 侵入ルールでのポートの定義（27-9 ページ）では、ルール ヘッダーで個別のポートとポート範囲を定義する方法について説明します。
- 方向の指定（27-10 ページ）では、使用可能な演算子について説明し、ルールでテストすべきトラフィック伝送方向を指定する方法について説明します。

ルール アクションの指定

ライセンス：Protection

各ルール ヘッダーには、パケットがルールをトリガーとして使用したときにシステムで行われるアクションを指定するパラメータが 1 つ含まれています。アクションが *alert* に設定されたルールは、それをトリガーとして使用したパケットに関する侵入イベントを生成し、そのパケットの詳細をログに記録します。アクションが *pass* に設定されたルールは、それをトリガーとして使用したパケットに関するイベントを生成せず、そのパケットの詳細も記録しません。

（注）　インライン展開において、ルール状態が [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールは、それをトリガーとして使用したパケットに関する侵入イベントを生成します。また、パッシブ展開で廃棄ルールを適用した場合は、ルールがアラート ルールとして機能します。廃棄ルールの詳細については、ルール状態の設定（24-21 ページ）を参照してください。

デフォルトでは、パス ルールがアラート ルールをオーバーライドします。パス ルールを作成することで、アラート ルールを無効にする代わりに、パス ルールで定義された基準を満たすパケットが特定の状況でアラート ルールをトリガーとして使用しないことを指定できます。たとえば、ユーザ "anonymous" として FTP サーバにログインする試行を検索するルールをアクティブのままにする必要があるとします。ただし、1 つ以上の正式な匿名 FTP サーバがネットワークに存在する場合、そのような特定のサーバで匿名ユーザにより最初のルールがトリガーとして使用されないことを指定するパス ルールを作成し、アクティブにすることができます。

ルール エディタで、[アクション（Action）] リストからルール タイプを選択します。ルール エディタを使ってルール ヘッダーを作成する手順の詳細については、ルールの構築（27-105 ページ）を参照してください。

プロトコルの指定

ライセンス：Protection

各ルール ヘッダーで、ルールにより検査されるトラフィックのプロトコルを指定する必要があります。次のネットワーク プロトコルを分析対象として指定できます。

- ICMP（Internet Control Message Protocol）
- インターネット プロトコル（IP）

（注）　プロトコルが `ip` に設定されている場合、システムは侵入ルール ヘッダー内のポート定義を無視します。詳細については、侵入ルールでのポートの定義（27-9 ページ）を参照してください。

- 伝送制御プロトコル（TCP）
- ユーザ データグラム プロトコル（UDP）

TCP、UDP、ICMP、IGMP など、IANA によって割り当てられたすべてのプロトコルを検査するには、プロトコル タイプとして **IP** を使用します。IANA によって割り当てられたプロトコルの完全なリストについては、http://www.iana.org/assignments/protocol-numbers を参照してください。

（注）　現在のところ、IP ペイロード内の次のヘッダー（TCP ヘッダーなど）でパターンを照合するルールを作成することはできません。代わりに、最後にデコードされたプロトコルからコンテンツ照合が始まります。次善策として、ルール オプションを使用して TCP ヘッダー内のパターンを照合できます。

ルール エディタで、[プロトコル（Protocol）] リストからプロトコル タイプを選択します。ルール エディタを使用してルール ヘッダーを作成する手順の詳細については、ルールの構築（27-105 ページ）を参照してください。

侵入ルールでの IP アドレスの指定

ライセンス：Protection

パケット検査の対象を、特定の IP アドレスから発信されたパケットまたは特定の IP アドレスに向かうパケットに制限すると、システムが実行しなければならないパケット検査の量が減ります。さらに、ルールをより具体化し、送信元および宛先 IP アドレスが疑わしい動作を示していないパケットに対してルールがトリガーとして使用される可能性をなくすと、誤検出も減ります。

ヒント　システムは IP アドレスのみを認識し、送信元/宛先 IP アドレスのホスト名を受け入れません。

ルール エディタの [Source IPs] フィールドと [Destination IPs] フィールドで、送信元および宛先の IP アドレスを指定します。ルール エディタを使用してルール ヘッダーを作成する手順の詳細については、ルールの構築（27-105 ページ）を参照してください。

標準テキスト ルール の作成時には、必要に応じて、さまざまな方法で IPv4 アドレスと IPv6 アドレスを指定できます。単一の IP アドレス、`any`、IP アドレス リスト、CIDR 表記、プレフィクス長、ネットワーク変数、またはネットワーク オブジェクトあるいはネットワーク オブジェクト グループを指定できます。加えて、1 つの特定の IP アドレスまたは IP アドレスのセットを除外するよう指定できます。IPv6 アドレスを指定するときには、RFC 4291 で定義された任意のアドレス指定規則を使用できます。

次の表では、送信元と宛先の IP アドレスを指定するさまざまな方法を要約します。

表 **27-2**　送信元/宛先 **IP** アドレスの構文

指定する項目	使用するフィルタ	例
任意の IP アドレス	任意	任意
1 つの特定の IP アドレス	IP アドレス 同じルール内に IPv4 と IPv6 の送信元アドレスと宛先アドレスを混在させないでください。	`192.168.1.1` `2001:db8::abcd`
IP アドレスのリスト	複数の IP アドレスをカンマで区切り、それを大カッコ（`[]`）で囲む	`[192.168.1.1,192.168.1.15]` `[2001:db8::b3ff, 2001:db8::0202]`

表 27-2　送信元/宛先 IP アドレスの構文（続き）

指定する項目	使用するフィルタ	例
IP アドレスのブロック	IPv4 CIDR ブロックまたは IPv6 アドレス プレフィクス表記	192.168.1.0/24 2001:db8::/32
特定の 1 つの IP アドレスまたはアドレス セットを除くすべて	! 文字を、否定する 1 つ以上の IP アドレスの前に付ける	!192.168.1.15 !2001:db8::0202:b3ff:fe1e
特定の 1 つ以上の IP アドレスを除く、IP アドレス ブロック内のすべて	アドレス ブロックの後に、否定されるアドレスのリストまたはブロック	[10.0.0/8, !10.2.3.4, !10.1.0.0/16] [2001:db8::/32, !2001:db8::8329, !2001:db8::0202]
ネットワーク変数で定義された IP アドレス	$ で始まる大文字の変数名 プリプロセッサ ルールは、侵入ルールで使われているネットワーク変数で定義されたホストとは無関係に、イベントをトリガーできることに注意してください。詳細については、変数セットの使用（2-15 ページ）を参照してください。	$HOME_NET
IP アドレス変数で定義されたアドレスを除く、すべての IP アドレス	!$ で始まる大文字の変数名 詳細については、侵入ルールで IP アドレスを除外する（27-8 ページ）を参照してください。	!$HOME_NET
ネットワーク オブジェクトまたはネットワーク オブジェクト グループで定義された IP アドレス	!{object_name} という形式でオブジェクト名またはグループ名。 詳細については、ネットワーク オブジェクトの操作（2-4 ページ）を参照してください。	${192.168sub16}
ネットワーク オブジェクトまたはネットワーク オブジェクト グループで定義されたアドレスを除く、すべての IP アドレス	オブジェクト名またはグループ名を中カッコ（{}）で囲み、その前に !$ を付ける。 詳細については、ネットワーク オブジェクトの操作（2-4 ページ）を参照してください。	!${192.168sub16}

送信元および宛先の IP アドレスを指定するために使用可能な構文の詳細と、変数を使って IP アドレスを指定する方法については、以下の項を参照してください。

- IP アドレスの表記規則（1-4 ページ）。
- 変数セットの使用（2-15 ページ）
- 任意の IP アドレスの指定（27-7 ページ）
- 複数の IP アドレスの指定（27-7 ページ）
- ネットワーク オブジェクトの指定（27-8 ページ）
- 侵入ルールで IP アドレスを除外する（27-8 ページ）

任意の IP アドレスの指定

ライセンス：Protection

任意の IPv4 または IPv6 アドレスを示す「any」という単語を、ルールの送信元 IP アドレスまたは宛先 IP アドレスとして指定できます。

たとえば、次のルールでは [Source IPs] フィールドと [Destination IPs] フィールドで引数 **any** を使用して、任意の IPv4 または IPv6 の送信元または宛先アドレスを持つパケットを評価します。

```
alert tcp any any -> any any
```

また、任意の IPv6 アドレスを示すために :: を指定することもできます。

複数の IP アドレスの指定

ライセンス：Protection

次の例に示すように、カンマを使って複数の IP アドレスを区切り、オプションで、非拒否リストを大カッコで囲むことにより、個別の IP アドレスを列挙できます。

```
[192.168.1.100,192.168.1.103,192.168.1.105]
```

IPv4 アドレスと IPv6 アドレスのいずれかだけを列挙することも、任意に組み合わせて列挙することもできます（次の例を参照）。

```
[192.168.1.100,2001:db8::1234,192.168.1.105]
```

以前のソフトウェア リリースでは IP アドレス リストを大カッコで囲む必要がありましたが、現在ではこれが必須でないことに注意してください。また、オプションで、リストを入力するときに各カンマの前または後にスペースを含めることができます。

（注）　否定リストは、大カッコで囲む必要があります。詳細については、侵入ルールで IP アドレスを除外する（27-8 ページ）を参照してください。

また、IPv4 クラスレス ドメイン間ルーティング（CIDR）表記または IPv6 プレフィクス長を使用してアドレス ブロックを指定することもできます。次に例を示します。

- 192.168.1.0/24 は、サブネット マスク 255.255.255.0 の 192.168.1.0 ネットワーク内の IPv4 アドレス、つまり 192.168.1.0 ～ 192.168.1.255 を指定します。詳細については、IP アドレスの表記規則（1-4 ページ）を参照してください。
- 2001:db8::/32 は、プレフィクス長 32 ビットの 2001:db8:: ネットワーク内の IPv6 アドレス、つまり 2001:db8:: ～ 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff を指定します。

ヒント　IP アドレスのブロックを指定する必要があるが、CIDR またはプレフィクス長表記を単独で使ってそれを表現できない場合は、1 つの IP アドレス リスト内でいくつかの CIDR ブロックとプレフィクス長を使用できます。

ネットワーク オブジェクトの指定

ライセンス：Protection

次の構文を使用して、ネットワーク オブジェクトまたはネットワーク オブジェクト グループを指定できます。

```
${object_name | group_name}
```

引数の説明

- *object_name* はネットワーク オブジェクトの名前です
- *group_name* はネットワーク オブジェクト グループの名前です

ネットワーク オブジェクトとネットワーク オブジェクト グループの作成方法については、ネットワーク オブジェクトの操作（2-4 ページ）を参照してください。

`192.168sub16` という名前のネットワーク オブジェクトと `all_subnets` という名前のネットワーク オブジェクト グループをすでに作成済みであるとします。ネットワーク オブジェクトを使用して IP アドレスを特定するには、たとえば次のように指定できます。

```
${192.168sub16}
```

ネットワーク オブジェクト グループを使用するには、次のように指定できます。

```
${all_subnets}
```

さらに、ネットワーク オブジェクトとネットワーク オブジェクト グループで否定を使用することもできます。次に例を示します。

```
!${192.168sub16}
```

詳細については、侵入ルールで IP アドレスを除外する（27-8 ページ）を参照してください。

侵入ルールで IP アドレスを除外する

ライセンス：Protection

感嘆符（`!`）を使用すると、指定した IP アドレスを否定できます。つまり、1 つ以上の特定の IP アドレスを除く、すべての IP アドレスに一致させることができます。たとえば、`!192.168.1.1` は、192.168.1.1 以外の任意の IP アドレスを指定し、`!2001:db8:ca2e::fa4c` は、2001:db8:ca2e::fa4c 以外の任意の IP アドレスを指定します。

IP アドレスのリストを否定するには、`!` を大カッコで囲んだ IP アドレスのリストの前に置きます。たとえば、`![192.168.1.1,192.168.1.5]` は、192.168.1.1 または 192.168.1.5 を除く任意の IP アドレスを定義します。

（注）　IP アドレスのリストを否定するには、大カッコを使用する必要があります。

否定文字と一緒に IP アドレス リストを使用する場合は注意が必要です。たとえば、`[!192.168.1.1,!192.168.1.5]` を使用して 192.168.1.1 と 192.168.1.5 を除く任意のアドレスに一致させると、システムはこの構文を「192.168.1.1 以外のすべて、または 192.168.1.5 以外のすべて」と解釈します。

192.168.1.5 は 192.168.1.1 ではなく、192.168.1.1 は 192.168.1.5 ではないため、この両方の IP アドレスが `[!192.168.1.1,!192.168.1.5]` という IP アドレス値に一致します。つまり、実質的に「`any`」を使用するのと同じです。

代わりに、`![192.168.1.1,192.168.1.5]` を使用してください。システムはこの構文を「**192.168.1.1** でなく、しかも 192.168.1.5 でない」と解釈し、大カッコ内に列挙されたものを除くすべての IP アドレスに一致します。

論理的に言って、`any` と一緒に否定を使用できないことに注意してください。any を否定すると「アドレスなし」を意味することになります。

侵入ルールでのポートの定義

ライセンス：Protection

ルール エディタの [Source Port] フィールドと [Destination Port] フィールドで、送信元および宛先ポートを指定します。ルール エディタを使用してルール ヘッダーを作成する手順の詳細については、ルールの構築（27-105 ページ）を参照してください。

ルール ヘッダー内で使われるポート番号を定義するために、ASA FirePOWER モジュールは特殊なタイプの構文を使用します。

（注）　プロトコルが `ip` に設定されている場合、システムは侵入ルール ヘッダー内のポート定義を無視します。詳細については、プロトコルの指定（27-4 ページ）を参照してください。

次の例に示すように、カンマでポートを区切ることによって、ポートのリストを指定できます。

```
80, 8080, 8138, 8600-9000, !8650-8675
```

オプションで、次の例に示すように、ポート リストを大カッコで囲むこともできます（以前のソフトウェア バージョンではこれが必須でしたが、現在は必須ではありません）。

```
[80, 8080, 8138, 8600-9000, !8650-8675]
```

なお、次の例に示すように、ポート リストの否定を大カッコで囲む必要があることに注意してください。

```
![20, 22, 23]
```

また、侵入ルール内の送信元ポートや宛先ポートのリストには最大で 64 文字を含めることができます。

次の表に、使用可能な構文を要約します。

表 **27-3**　送信元/宛先ポートの構文

指定する項目	用途	例
任意のポート	任意	任意
1 つの特定のポート	ポート番号	`80`
ポートの範囲	範囲内の最初のポート番号と最後のポート番号をダッシュでつなぐ	`80-443`
1 つの特定のポートに等しい、またはより小さいすべてのポート	ポート番号の前にダッシュを付ける	`-21`
1 つの特定のポートに等しい、またはより大きいすべてのポート	ポート番号の後ろにダッシュを付ける	`80-`
1 つの特定のポートまたはポート範囲を除く、すべてのポート	! 文字を、否定するポート、ポート リスト、またはポート範囲の前に付ける 論理的に言って、*any* を除くすべてのポート指定と一緒に否定を使用できます。any を否定すると「ポートなし」を意味することに注意してください。	`!20`
ポート変数で定義されるすべてのポート	`$` で始まる大文字の変数名 詳細については、ポート変数の操作（2-29 ページ）を参照してください。	`$HTTP_PORTS`
ポート変数で定義されるポートを除く、すべてのポート	`$` で始まる大文字の変数名	`!$HTTP_PORTS`

方向の指定

ライセンス：Protection

ルールによる検査対象となるパケットが進むべき方向を、ルール ヘッダー内で指定できます。以下の表は、それらのオプションを示しています。

表 **27-4**　ルール ヘッダー内の方向オプション

使用するフィルタ	テスト対象
指向性	指定された送信元 IP アドレスから指定された宛先 IP アドレスに向かうトラフィックのみ
双方向	指定された送信元 IP アドレスと宛先 IP アドレスの間を移動するすべてのトラフィック

ルール エディタを使用してルール ヘッダーを作成する手順の詳細については、ルールの構築（27-105 ページ）を参照してください。

ルールでのキーワードと引数について

ライセンス：Protection

ルール言語では、キーワードを組み合わせることによってルールの動作を指定できます。キーワードとそれに関連する値（引数と呼ばれる）は、ルール エンジンによって検査されるパケットおよびパケット関連値をシステムがどのように評価するかを決定します。ASA FirePOWER モジュールでは現在、コンテンツ マッチング、プロトコル固有のパターン マッチング、状態固有のマッチングなどのインスペクション機能を実行するためのキーワードがサポートされています。キーワードあたり最大 100 個の引数を定義し、互換性のある任意の数のキーワードを組み合わせて非常に具体的なルールを作成できます。これにより、誤検出や検出漏れの可能性が減少し、受け取った侵入情報に集中的に取り組むことができます。

また、適応型プロファイルを使用すると、ルール メタデータとホスト情報に基づいて特定のパケットに対するアクティブ ルール処理を動的に調整できます。詳細については、パッシブ展開における前処理の調整（22-1 ページ）を参照してください。

詳細については、次の各項を参照してください。

- 侵入イベント詳細の定義（27-12 ページ）では、イベントのメッセージ、プライオリティ情報、およびルールで検出されたエクスプロイトに関する外部情報への参照を定義するためのキーワードの構文と使用法について説明します。
- コンテンツ一致の検索（27-15 ページ）では、`content` または `protected_content` キーワードを使用して、パケット ペイロードの内容を検査する方法について説明します。
- コンテンツ一致の制約（27-18 ページ）では、`content` または `protected_content` キーワードを変更するキーワードの使用方法について説明します。
- インライン展開でのコンテンツの置換（27-31 ページ）では、インライン展開で `replace` キーワードを使用して、長さの等しい指定されたコンテンツを置き換える方法について説明します。
- Byte_Jump と Byte_Test の使用（27-33 ページ）では、`byte_jump` キーワードと `byte_test` キーワードを使用して、パケット内のどの位置でルール エンジンがコンテンツ マッチング検査を開始すべきか、どのバイトを評価すべきかについて計算する方法を説明します。
- PCRE を使用したコンテンツの検索（27-38 ページ）では、`pcre` キーワードを使用して、ルール内で Perl 互換の正規表現を使用する方法について説明します。

- ルールにメタデータを追加する（27-45 ページ）では、metadata キーワードを使用して、ルールに情報を追加する方法について説明します。
- IP ヘッダー値の検査（27-48 ページ）では、パケットの IP ヘッダー内の値を検査するキーワードの構文と使用法について説明します。
- ICMP ヘッダー値の検査（27-50 ページ）では、パケットの ICMP ヘッダー内の値を検査するキーワードの構文と使用法について説明します。
- TCP ヘッダー値とストリーム サイズの検査（27-52 ページ）では、パケットの TCP ヘッダー内の値を検査するキーワードの構文と使用法について説明します。
- TCP ストリーム再構築の有効化と無効化（27-56 ページ）では、接続での検査対象トラフィックがルールの条件と一致した場合に、単一接続のストリーム再構築を有効/無効にする方法について説明します。
- セッションからの SSL 情報の抽出（27-57 ページ）では、暗号化されたトラフィックからバージョン情報と状態情報を抽出するキーワードの使用法と構文について説明します。
- パケット データをキーワード引数の中に読み込む（27-85 ページ）では、パケットから変数の中に値を読み込み、あとでそれを同じルール内で使用することにより、その値を特定の他のキーワードの引数として指定する方法を説明します。
- アプリケーション層プロトコル値の検査（27-59 ページ）では、アプリケーション層プロトコル プロパティを検査するキーワードの使用法と構文について説明します。
- パケット特性の検査（27-82 ページ）では、dsize、sameIP、isdataat、fragoffset および cvs キーワードの使用法と構文について説明します。
- ルール キーワードを使用したアクティブ応答の開始（27-87 ページ）では、resp キーワードを使用して TCP 接続または UDP セッションをアクティブに閉じる方法、react キーワードを使用して HTML ページを送信した後で TCP 接続をアクティブに閉じる方法、および config response コマンドを使用してアクティブ応答インターフェイスとパッシブ展開での TCP リセット試行回数を指定する方法について説明します。
- イベントのフィルタリング（27-91 ページ）では、指定された時間内に指定されたパケット数がルールの検出基準を満たさない限り、ルールでイベントがトリガーとして使用されないようにする方法を説明します。
- 攻撃後トラフィックの評価（27-92 ページ）では、ホストまたはセッションに関する追加のトラフィックをログに記録する方法について説明します。
- 複数のパケットに及ぶ攻撃の検出（27-93 ページ）では、単一セッション内の複数パケットに及ぶ攻撃からパケットに状態名を割り当てた後、その状態に応じてパケットを分析および警告する方法について説明します。
- HTTP エンコードのタイプと位置によるイベントの生成（27-98 ページ）では、正規化の前に、HTTP 要求または応答 URI、ヘッダー、または（set-cookies を含む）cookie 内のエンコード タイプに基づいてイベントを生成する方法について説明します。
- ファイル タイプとバージョンの検出（27-100 ページ）では、file_type キーワードまたは file_group キーワードを使用して、特定のファイル タイプまたはファイル バージョンを指し示す方法について説明します。
- 特定のペイロード タイプを指し示す（27-102 ページ）では、HTTP 応答エンティティ本体、SMTP ペイロード、またはエンコードされた電子メール添付ファイルの先頭を指し示す方法について説明します。
- パケット ペイロードの先頭を指し示す（27-103 ページ）では、パケット ペイロードの先頭を指し示す方法について説明します。
- Base64 データのデコードと検査（27-104 ページ）では、base64_decode キーワードと base64_data キーワードを使用して、特に HTTP 要求内の Base64 データをデコードして検査する方法について説明します。

侵入イベント詳細の定義

ライセンス：Protection

標準テキスト ルール を作成するときには、ルールで攻撃試行を検出する対象となる脆弱性についてのコンテキスト情報を含めることができます。また、脆弱性データベースへの外部参照を含めたり、組織内でイベントに設定するプライオリティを定義したりすることもできます。アナリストがイベントを認識すると、そのプライオリティ、エクスプロイト、および既知の対策についての情報をすぐに入手できます。

イベント関連のキーワードに関する詳細は、以下の項を参照してください。

- イベント メッセージの定義（27-12 ページ）
- イベント プライオリティの定義（27-12 ページ）
- 侵入イベント分類の定義（27-13 ページ）
- イベント参照の定義（27-15 ページ）

イベント メッセージの定義

ライセンス：Protection

ルールのトリガー時にメッセージとして表示される、意味のあるテキストを指定できます。メッセージを読むと、ルールで攻撃試行を検出する対象となった脆弱性の特性をすぐに理解できます。中カッコ（{}）を除く、印字可能な任意の標準 ASCII 文字を使用できます。システムは、メッセージ全体を囲んでいる引用符を取り除きます。

ヒント　ルール メッセージの指定は必須です。また、空白文字のみ、1 つ以上の引用符のみ、1 つ以上のアポストロフィのみ、あるいは空白文字/引用符/アポストロフィだけの組み合わせでメッセージを構成することはできません。

ルール エディタでイベント メッセージを定義するには、[メッセージ（Message）] フィールドにイベント メッセージを入力します。ルール エディタを使用してルールを作成する方法については、ルールの構築（27-105 ページ）を参照してください。

イベント プライオリティの定義

ライセンス：Protection

デフォルトでは、ルールのイベント分類からルールのプライオリティが派生します。ただし、`priority` キーワードをルールに追加すると、ルールの分類プライオリティをオーバーライドできます。

ルール エディタを使ってプライオリティを指定するには、[検出オプション（Detection Options）] リストから [priority] を選択して、ドロップダウンリストから [high]、[medium]、または [low] を選択します。たとえば、Web アプリケーション攻撃を検出するルールに **high** プライオリティを割り当てるには、`priority` キーワードをルールに追加して、プライオリティとして [high] を選択します。ルール エディタを使用してルールを作成する方法については、ルールの構築（27-105 ページ）を参照してください。

侵入イベント分類の定義

ライセンス：Protection

ルールごとに、イベントのパケット表示に含める攻撃分類を指定できます。次の表に、それぞれの分類の名前と番号を示します。

表 **27-5**　ルール分類

番号	分類名	説明
1	not-suspicious	不審ではないトラフィック
2	unknown	不明なトラフィック
3	bad-unknown	有害な可能性のあるトラフィック
4	attempted-recon	情報漏えいが試行された
5	successful-recon-limited	情報漏えいが発生
6	successful-recon-largescale	大規模な情報漏えい
7	attempted-dos	サービス妨害が試行された
8	successful-dos	サービス妨害（DoS）
9	attempted-user	ユーザ特権の獲得が試行された
10	unsuccessful-user	ユーザ特権の獲得が失敗した
11	successful-user	ユーザ特権の獲得に成功
12	attempted-admin	管理者特権の獲得が試行された
13	successful-admin	管理者特権の獲得に成功
18	rpc-portmap-decode	RPC クエリのデコード
15	shellcode-detect	実行可能コードが検出された
16	string-detect	疑わしい文字列が検出された
17	suspicious-filename-detect	疑わしいファイル名が検出された
18	suspicious-login	疑わしいユーザ名を使用したログイン試行が検出された
19	system-call-detect	システム コールが検出された
20	tcp-connection	TCP 接続が検出された
21	trojan-activity	ネットワーク トロイの木馬が検出された
22	unusual-client-port-connection	通常とは異なるポートをクライアントが使用していた
23	network-scan	ネットワーク スキャンの検出
24	denial-of-service	サービス妨害攻撃の検出
25	non-standard-protocol	非標準プロトコルまたはイベントの検出
26	protocol-command-decode	一般的なプロトコル コマンド デコード
27	web-application-activity	脆弱な可能性のある Web アプリケーションへのアクセス
36	web-application-attack	Web アプリケーション攻撃
29	misc-activity	その他のアクティビティ
30	misc-attack	その他の攻撃
31	icmp-event	一般的な ICMP イベント

表 27-5　ルール分類（続き）

番号	分類名	説明
32	inappropriate-content	不適切な内容が検出された
33	policy-violation	企業プライバシー侵害の可能性
34	default-login-attempt	デフォルトのユーザ名とパスワードによるログイン試行
35	sdf	機密データ
36	malware-cnc	既知のマルウェア コマンドと制御トラフィック
37	client-side-exploit	既知のクライアント側エクスプロイト試行
38	file-format	既知の悪意のあるファイルまたはファイル ベースのエクスプロイト

ルール エディタで分類を指定するには、[分類（Classification）] リストから分類を 1 つ選択します。ルール エディタの詳細については、新しいルールの作成（27-106 ページ）を参照してください。

カスタム分類の追加

ライセンス：Protection

定義したルールによって生成されるイベントのパケット表示記述の内容をもっとカスタマイズする必要がある場合には、カスタム分類を作成します。

[分類（Classification）] リストに分類を追加するには、次の手順を実行します。

ステップ 1　**[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] > [ルール エディタ（Rule Editor）]** の順に選択します。

[ルール エディタ（Rule Editor）] ページが表示されます。

ステップ 2　[ルールの作成（Create Rule）] をクリックします。

[ルールの作成（Create Rule）] ページが表示されます。

ステップ 3　[分類（Classification）] ドロップダウンリストで、[分類の編集（Edit Classifications）] をクリックします。

ポップアップ ウィンドウが表示されます。

ステップ 4　[分類名（Classification Name）] フィールドに分類の名前を入力します。

最大で 255 文字の英数字を使用できますが、40 文字を超えるとページが読みにくくなります。<>()\\\q"&$; 文字および空白文字はサポートされていません。

ステップ 5　[分類の説明（Classification Description）] フィールドに、分類の説明を入力します。

最大 255 文字の英数字およびスペースを使用できます。<>()\\\q"&$; 文字はサポートされていません。

ステップ 6　[プライオリティ（Priority）] リストからプライオリティを選択します。

[high]、[medium]、または [low] を選択できます。

ステップ 7　[追加（Add）] をクリックします。

新しい分類がリストに追加され、ルール エディタで使用できるようになります。

ステップ 8　[完了（Done）] をクリックします。

イベント参照の定義

ライセンス：Protection

reference キーワードを使用すると、イベントに関する外部 Web サイトや追加情報への参照を追加できます。参照を追加すると、アナリストは参照情報をすぐに利用できるため、パケットがルールをトリガーとして使用した理由を特定するのに役立ちます。次の表に、既知のエクスプロイトや攻撃についてのデータを提供する外部システムをいくつか示します。

表 *27-6*　外部攻撃識別システム

システム ID（System ID）	説明	ID の例
bugtraq	[Bugtraq] ページ	8550
cve	[Common Vulnerabilities and Exposure] ページ	CAN-2003-0702
mcafee	[McAfee] ページ	98574
URL	Web サイト参照	www.example.com?exploit=14
msb	Microsoft セキュリティ情報	MS11-082
nessus	[Nessus] ページ	10039
secure-url	セキュア Web サイト参照（https://...）	intranet/exploits/exploit=14 任意のセキュア Web サイトで secure-url を使用できることに注意してください。

ルール エディタを使用して参照を指定するには、[検出オプション（Detection Options）] リストから [参照（reference）] を選択し、対応するフィールドに次のように値を入力します。

id_system,*id*

ここで、*id_system* はプレフィクスとして使用されるシステム、*id* は Bugtraq ID、CVE 番号、Arachnids ID、または URL（http:// なし）です。

たとえば、Bugtraq ID 17134 に記載されている Microsoft Commerce Server 2002 サーバ上の認証バイパス脆弱性を指定するには、[参照（reference）] フィールドに次のように入力します。

bugtraq,17134

参照をルールに追加するときには、次の点に注意してください。

- カンマの後ろにスペースを入力しないでください。
- システム ID に大文字を使用しないでください。

ルール エディタを使用してルールを作成する方法については、ルールの構築（27-105 ページ）を参照してください。

コンテンツ一致の検索

ライセンス：Protection

content キーワードまたは protected_content キーワードを使用すると、パケット内で検出すべき内容（コンテンツ）を指定できます。詳細については、次の各項を参照してください。

- content キーワードの使用（27-16 ページ）
- protected_content キーワードの使用（27-16 ページ）
- コンテンツ マッチングの設定（27-17 ページ）

content キーワードの使用

content キーワードを使用すると、ルール エンジンはパケット ペイロードまたはストリームの中でその文字列を検索します。たとえば、いずれかの content キーワードの値として /bin/sh と入力した場合、ルール エンジンはパケット ペイロード内で文字列 /bin/sh を検索します。

ASCII 文字列、16 進コンテンツ（バイナリ バイト コード）、またはその両方の組み合わせを使用してコンテンツを照合できます。キーワード値の中で 16 進コンテンツをパイプ文字（|）で囲みます。たとえば、|90C8 C0FF FFFF|/bin/sh のように 16 進コンテンツと ASCII コンテンツを混在させることができます。

1 つのルール内で複数のコンテンツ マッチングを指定できます。これを行うには、content キーワードの追加のインスタンスを使用します。コンテンツ マッチングごとに、ルールをトリガーとして使用させるにはパケット ペイロードまたはストリームでコンテンツ一致が見つからなければならないことを指定できます。

protected_content キーワードの使用

protected_content キーワードを使用すると、ルール引数を設定する前に、検索コンテンツ文字列をエンコードすることができます。キーワードを設定する前に、ルール作成者がハッシュ関数（SHA-512、SHA-256、または MD5）を使用して文字列をエンコードします。

content キーワードの代わりに protected_content キーワードを使用した場合でも、ルール エンジンがパケット ペイロードまたはストリームの中で文字列を検索する方法に違いはなく、ほとんどのキーワード オプションが想定どおりに機能します。次の表は、protected_content キーワード オプションと content キーワード オプションの間の例外的な相違点を要約しています。

表 *27-7*　*protected_content* オプションの例外

オプション	説明
ハッシュ タイプ（Hash Type）	protected_content ルール キーワードの新しいオプション。詳細については、Hash Type（27-19 ページ）を参照してください。
[大文字小文字の区別なし（Case Insensitive）]	未サポート
次の範囲内（Within）	未サポート
奥行き（Depth）	未サポート
長さ（Length）	protected_content ルール キーワードの新しいオプション。詳細については、長さ（Length）（27-22 ページ）を参照してください。
高速パターン マッチ機能を使用（Use Fast Pattern Matcher）	未サポート
高速パターン マッチ機能のみ（Fast Pattern Matcher Only）	未サポート
高速パターン マッチ機能オフセットおよび長さ（Fast Pattern Matcher Offset and Length）	未サポート

シスコ では、protected_content キーワードを含むルールに 1 つ以上の content キーワードを含めることを推奨しています。こうすると、ルール エンジンが常に高速パターン マッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルール内の protected_content キーワードの前に content キーワードを配置します。ルールに 1 つ以上の content キーワードが含まれている場合は、content キーワードの Use Fast Pattern Matcher 引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。

コンテンツ マッチングの設定

ほとんどの場合、content または protected_content キーワードの後ろに修飾子を付けることによって、コンテンツを検索すべき位置、検索で大文字/小文字を区別するかどうか、その他のオプションを指定する必要があります。content および protected_content キーワードの修飾子の詳細については、コンテンツ一致の制約を参照してください。

ルールでイベントがトリガーとして使用されるためには、すべてのコンテンツ マッチングが真でなければならないことに注意してください。つまり、各コンテンツ マッチングは相互に AND 関係にあります。

また、インライン展開では、有害なコンテンツを照合した後でそれを同じ長さの独自のテキスト文字列に置き換えるルールをセットアップできることにも注意してください。詳細については、インライン展開でのコンテンツの置換（27-31 ページ）を参照してください。

照合するコンテンツを入力するには、次の手順を実行します。

ステップ 1　[コンテンツ（content）] フィールドに、検索する内容を入力します（たとえば `|90C8 C0FF FFFF|/bin/sh`）。

指定したコンテンツ以外のコンテンツを検索するには、[一致しない（Not）] チェック ボックスをオンにします。

注意　[一致しない（Not）] オプションが選択された 1 つの content キーワードだけを含むルールを作成した場合、侵入ポリシーの効果がなくなる可能性があります。詳細については、注（27-20 ページ）を参照してください。

ステップ 2　オプションで、content キーワードを変更したり、キーワードの制約を追加したりするキーワードを追加します。

他のキーワードの詳細については、ルールでのキーワードと引数について（27-10 ページ）を参照してください。content キーワードの制約の詳細については、コンテンツ一致の制約（27-18 ページ）を参照してください。

ステップ 3　ルールの作成または編集を続けます。

詳細については、新しいルールの作成（27-106 ページ）または既存のルールの変更（27-108 ページ）を参照してください。

照合する保護されたコンテンツを入力するには、次の手順を実行します。

ステップ 1　SHA-512、SHA-256、または MD5 ハッシュ ジェネレータを使用して、検索するコンテンツをエンコードします（たとえば SHA-512 ハッシュ ジェネレータを使って文字列 `Sample1` に対して実行します）。

ジェネレータが文字列のハッシュを出力します。

ステップ 2　[protected_content] フィールドに、ステップ 1 で生成したハッシュを入力します（たとえば `B20AABAF59605118593404BD42FE69BD8D6506EE7F1A71CE6BB470B1DF848C814BC5DBEC2081999F15691A71FAECA5FBA4A3F8B8AB56B7F04585DA6D73E5DD15`）。

指定したコンテンツ以外のコンテンツを検索するには、[一致しない（Not）] チェック ボックスをオンにします。

注意　[一致しない(Not)] オプションが選択された 1 つの protected_content キーワードだけを含むルールを作成した場合、侵入ポリシーの効果がなくなる可能性があります。詳細については、注(27-20 ページ)を参照してください。

ステップ 3　[Hash Type] ドロップダウンリストから、ステップ 1 で使用したハッシュ関数(例えば **SHA-512**)を選択します。なお、ステップ 2 で入力されたハッシュ内のビット数がハッシュ タイプと一致する必要があります。一致しない場合、システムはルールを保存しません。詳細については、Hash Type(27-19 ページ)を参照してください。

ヒント　シスコ設定の **Default** を選択した場合、システムはハッシュ関数として SHA-512 を想定します。

ステップ 4　必須の [長さ(Length)] フィールドに値を入力します。この値は、元の(ハッシュされていない)検索文字列の長さに対応する必要があります(たとえば、ステップ 2 の文字列 Sample1 の長さは 7 です)。

詳細については、長さ(Length)(27-22 ページ)を参照してください。

ステップ 5　[オフセット(Offset)] フィールドまたは [距離(Distance)] フィールドに値を入力します。1 つのキーワード設定内に [オフセット(Offset)] オプションと [距離(Distance)] オプションを混在させることはできません。

詳細については、protected_content キーワードでの検索位置オプションの使用(27-23 ページ)を参照してください。

ステップ 6　オプションで、protected_content キーワードを変更する制約オプションを追加します。

詳細については、コンテンツ一致の制約(27-18 ページ)を参照してください。

ステップ 7　オプションで、protected_content キーワードを変更する追加のキーワードを指定します。

詳細については、ルールでのキーワードと引数について(27-10 ページ)を参照してください。

ステップ 8　ルールの作成または編集を続けます。

詳細については、新しいルールの作成(27-106 ページ)または既存のルールの変更(27-108 ページ)を参照してください。

コンテンツ一致の制約

ライセンス:Protection

content または protected_content キーワードを変更するパラメータを使用すると、コンテンツ検索の位置や大文字/小文字の区別を制約できます。content または protected_content キーワードを変更するオプションを設定して、検索対象となるコンテンツを指定します。

詳細については、次の項を参照してください。

- [大文字小文字の区別なし(Case Insensitive)](27-19 ページ)
- Hash Type(27-19 ページ)
- 生データ(Raw Data)(27-20 ページ)
- 注(27-20 ページ)
- 検索位置オプション(27-21 ページ)
- HTTP コンテンツ オプション(27-24 ページ)
- 高速パターン マッチ機能を使用(Use Fast Pattern Matcher)(27-28 ページ)

[大文字小文字の区別なし（Case Insensitive）]

ライセンス：Protection

（注）　このオプションは protected_content キーワードの設定ではサポートされません。詳細については、protected_content キーワードの使用（27-16 ページ）を参照してください。

ASCII 文字列でコンテンツ一致を検索するときに大文字/小文字の区別を無視するようルール エンジンに指示できます。検索で大文字/小文字を区別しないようにするには、コンテンツ検索の指定で [大文字小文字の区別なし（Case Insensitive）] をオンにします。

コンテンツ検索時に **[大文字小文字の区別なし（Case Insensitive）]** を指定するには、次の手順を実行します。

ステップ 1　追加する content キーワードに関して [大文字小文字の区別なし（Case Insensitive）] を選択します。

ステップ 2　ルールの作成または編集を続けます。

詳細については、コンテンツ一致の制約、コンテンツ一致の検索（27-15 ページ）、新しいルールの作成（27-106 ページ）、または 既存のルールの変更（27-108 ページ）を参照してください。

Hash Type

ライセンス：Protection

（注）　このオプションは protected_content キーワードでのみ設定できます。詳細については、protected_content キーワードの使用（27-16 ページ）を参照してください。

[Hash Type] ドロップダウンを使用して、検索文字列のエンコードに使われたハッシュ関数を特定します。システムは、protected_content 検索文字列のハッシュ方式として SHA-512、SHA-256、および MD5 をサポートしています。選択したハッシュ タイプとハッシュされたコンテンツの長さが一致しない場合、システムはルールを保存しません。

システムは自動的に、シスコ設定のデフォルト値を選択します。[デフォルト（Default）] が選択される場合、ルールには具体的なハッシュ関数が含まれず、システムはハッシュ関数として SHA-512 を想定します。

保護されたコンテンツ検索の実行時にハッシュ関数を指定するには、次の手順を実行します。

ステップ 1　[Hash Type] ドロップダウンリストから、追加する protected_content キーワードのハッシュとして [デフォルト（Default）]、[SHA-512]、[SHA-256]、または [MD5] を選択します。

ヒント　シスコ設定の **Default** を選択した場合、システムはハッシュ関数として SHA-512 を想定します。詳細については、Hash Type（27-19 ページ）を参照してください。

ステップ 2　ルールの作成または編集を続けます。詳細については、コンテンツ一致の制約、コンテンツ一致の検索（27-15 ページ）、新しいルールの作成（27-106 ページ）、または 既存のルールの変更（27-108 ページ）を参照してください。

生データ（Raw Data）

ライセンス：Protection

[生データ（Raw Data）] オプションを使用すると、ルール エンジンは、正規化されたペイロード データ（ネットワーク分析ポリシーによってデコードされたデータ）を分析する前にオリジナルのパケット ペイロードを分析します。引数値は使用されません。正規化の前に、ペイロード内の Telnet ネゴシエーション オプションを検査するために Telnet トラフィックを分析する場合に、このキーワードを使用できます。

同じ `content` または `protected_content` キーワードの中で、[生データ（Raw Data）] オプションを HTTP コンテンツ オプションと一緒に使用することはできません。詳細については、HTTP コンテンツ オプション（27-24 ページ）を参照してください。

ヒント　HTTP トラフィック内で raw データを検査するかどうか、および検査される raw データの量を決定するために HTTP Inspect プリプロセッサの [クライアントフローの深さ（Client Flow Depth）] オプションと [サーバフローの深さ（Server Flow Depth）] オプションを設定できます。詳細については、サーバレベル HTTP 正規化オプションの選択（19-37 ページ）を参照してください。

raw データを分析するには、次の手順を実行します。

ステップ **1**　追加する `content` または `protected_content` キーワードの [生データ（Raw Data）] チェック ボックスを選択します。

ステップ **2**　ルールの作成または編集を続けます。詳細については、コンテンツ一致の制約、コンテンツ一致の検索（27-15 ページ）、新しいルールの作成（27-106 ページ）、または 既存のルールの変更（27-108 ページ）を参照してください。

注

ライセンス：Protection

指定したコンテンツと一致しないコンテンツを検索するには、[一致しない（Not）] オプションを選択します。[一致しない（Not）] オプションが選択された `content` または `protected_content` キーワードを含むルールを作成する場合には、そのルール内に、[一致しない（Not）] オプションが選択されていない別の `content` または `protected_content` キーワードを 1 つ以上含める必要があります。

注意　`content` または `protected_content` キーワードの [一致しない（Not）] オプションを選択する場合は、その 1 つのキーワードだけ含むルールを作成しないでください。侵入ポリシーの効果がなくなる可能性があります。

たとえば、SMTP ルール 1:2541: 9 に 3 つの `content` キーワードが含まれており、そのうち 1 つで [一致しない（Not）] オプションが選択されているとします。[一致しない（Not）] オプションが選択されたキーワード以外のすべての `content` キーワードを仮に削除すると、このルールに基づくカスタム ルールが無効になります。このようなルールを侵入ポリシーに追加すると、そのポリシーの効果がなくなる可能性があります。

指定したコンテンツに一致しないコンテンツを検索するには、次の手順を実行します。

ステップ 1　追加する content または protected_content キーワードの [一致しない(Not)] チェック ボックスを選択します。

ヒント　同じ content キーワードで、[一致しない(Not)] チェック ボックスと [高速パターン マッチ機能を使用(Use Fast Pattern Matcher)] チェック ボックスを同時に選択することはできません。

ステップ 2　[一致しない(Not)] オプションが選択されていない他の 1 つ以上の content または protected_content キーワードをルールに含めます。

ステップ 3　ルールの作成または編集を続けます。詳細については、コンテンツ一致の制約、コンテンツ一致の検索(27-15 ページ)、新しいルールの作成(27-106 ページ)、または 既存のルールの変更(27-108 ページ)を参照してください。

検索位置オプション

ライセンス:Protection

検索位置オプションを使用すると、指定したコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。各オプションの詳細については、以下を参照してください。

- 奥行き(Depth)(27-21 ページ)
- 距離(Distance)(27-22 ページ)
- 長さ(Length)(27-22 ページ)
- オフセット(Offset)(27-22 ページ)
- 次の範囲内(Within)(27-22 ページ)

content または protected_content キーワード内で検索位置オプションを使用する方法については、以下を参照してください。

- content キーワードでの検索位置オプションの使用(27-23 ページ)
- protected_content キーワードでの検索位置オプションの使用(27-23 ページ)

奥行き(**Depth**)

(注)　このオプションは、content キーワードを設定する場合にのみサポートされます。詳細については、content キーワードの使用(27-16 ページ)を参照してください。

オフセット値の先頭からの(またはオフセットが設定されていない場合はパケット ペイロード先頭からの)コンテンツ検索の最大の深さをバイト単位で指定します。

たとえば、ルールのコンテンツ値が cgi-bin/phf、offset 値が 3、depth 値が 22 である場合、ルール ヘッダーで指定されたパラメータを満たすパケット内で、cgi-bin/phf 文字列との一致の検索がバイト位置 3 から始まり、22 バイト処理した後(バイト 25)停止します。

指定したコンテンツの長さ以上の、最大 65535 バイトまでの値を指定する必要があります。値 0 は指定できません。

デフォルトの深さは、「パケットの末尾まで検索」です。

距離（**Distance**）

以前に見つかったコンテンツ一致から数えて、指定されたバイト数の後に出現する後続のコンテンツ一致を見つけるようルール エンジンに指示します。

Distance（距離）カウンタはバイト 0 から始まるため、最後に見つかったコンテンツ一致から順方向に移動すべきバイト数よりも 1 つ少ない数値を指定してください。たとえば 4 を指定した場合、5 番目のバイトから検索が始まります。

-65535 ～ 65535 バイトを値として指定できます。負の `Distance` 値を指定した場合は、検索を開始するバイト位置がパケットの先頭から外れる可能性があります。実際にはパケットの第 1 バイトから検索が開始されますが、計算ではパケットの外側のバイトも考慮されます。たとえば、パケット内の現在の位置が第 5 バイトで、次のコンテンツ ルール オプションで `Distance` 値 -10 および `Within` 値 20 が指定された場合、検索はペイロードの先頭から開始され、[Within] オプションが 15 に調整されます。

デフォルトの距離は 0 で、これは最後のコンテンツ一致の後のパケット内の現在位置という意味です。

長さ（**Length**）

（注）　このオプションは、`protected_content` キーワードを設定する場合にのみサポートされます。詳細については、protected_content キーワードの使用（27-16 ページ）を参照してください。

Length `protected_content` キーワード オプションは、ハッシュされていない検索文字列の長さをバイト単位で示します。

たとえば、コンテンツ `Sample1` を使ってセキュア ハッシュを生成した場合には、**Length** 値として `7` を使用します。このフィールドに値を入力することは必須です。

オフセット（**Offset**）

パケット ペイロードの先頭を基準とする、コンテンツの検索を開始するパケット ペイロード内の位置をバイト単位で指定します。-65535 ～ 65535 バイトを値として指定できます。

オフセット カウンタはバイト 0 から始まるため、パケット ペイロードの先頭から順方向に移動すべきバイト数よりも 1 つ少ない数値を指定してください。たとえば 7 を指定した場合は、8 番目のバイトから検索が始まります。

デフォルトのオフセットは 0 で、これはパケットの先頭を意味します。

次の範囲内（**Within**）

（注）　このオプションは、`content` キーワードを設定する場合にのみサポートされます。詳細については、content キーワードの使用（27-16 ページ）を参照してください。

[次の範囲内（Within）] オプションを使用すると、ルールをトリガーとして使用させるには、最後に見つかったコンテンツ一致の末尾以降、指定のバイト数以内に次のコンテンツ一致が発生する必要があることを指示できます。たとえば **Within** 値として `8` を指定した場合、次のコンテンツ一致がパケット ペイロードの次の 8 バイト以内に発生する必要があります。発生しない場合は、ルールをトリガーとして使用する基準が満たされません。

指定したコンテンツの長さ以上の、最大 65535 バイトまでの値を指定できます。

[次の範囲内（Within）] のデフォルトは「パケットの末尾まで検索」です。

content キーワードでの検索位置オプションの使用

次のように、2 つの content 位置ペアのいずれかを使用すると、指定したコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

- パケット ペイロードの先頭を基準にして検索する場合は、[オフセット（Offset）] と [奥行き（Depth）] を一緒に使用します。
- 現在の検索位置を基準にして検索する場合は、[距離（Distance）] と [次の範囲内（Within）] を一緒に使用します。

ペアに含まれるオプションのどちらか 1 つだけを指定した場合は、そのペアのもう 1 つのオプションのデフォルトが想定されます。

[オフセット（Offset）] および [奥行き（Depth）] オプションと、[距離（Distance）] および [次の範囲内（Within）] オプションを混合することはできません。たとえば、[オフセット（Offset）] と [次の範囲内（Within）] をペアにすることはできません。1 つのルール内で任意の数の位置オプションを使用できます。

位置が指定されない場合は、[オフセット（Offset）] と [奥行き（Depth）] のデフォルトが想定されます。つまり、コンテンツ検索はパケット ペイロードの先頭から始まってパケットの末尾まで続きます。

また、既存の byte_extract 変数を使用して位置オプションの値を指定することもできます。詳細については、パケット データをキーワード引数の中に読み込む（27-85 ページ）を参照してください。

ステップ 1　**Web** インターフェイスを使用して **content keyword** 追加する content キーワードのフィールドに値を入力します。次の選択肢があります。

- オフセット（**Offset**）
- 奥行き（**Depth**）
- 距離（**Distance**）
- 次の範囲内（**Within**）

1 つのルール内で任意の数の位置オプションを使用できます。

ステップ 2　ルールの作成または編集を続けます。詳細については、コンテンツ一致の制約（27-18 ページ）、コンテンツ一致の検索（27-15 ページ）、新しいルールの作成（27-106 ページ）、または 既存のルールの変更（27-108 ページ）を参照してください。

protected_content キーワードでの検索位置オプションの使用

次のように、必須の [長さ（Length）] protected_content 位置オプションを [オフセット（Offset）] または [距離（Distance）] 位置オプションと組み合わせて使用すると、指定されたコンテンツの検索をどこから開始するか、どこまで検索するかを指定できます。

- パケット ペイロードの先頭を基準にして、保護された文字列を検索するには、[長さ（Length）] と [オフセット（Offset）] を一緒に使用します。
- 現在の検索位置を基準にして、保護された文字列を検索するには、[長さ（Length）] と [距離（Distance）] を一緒に使用します。

ヒント　1 つのキーワード設定内で [オフセット（Offset）] オプションと [距離（Distance）] オプションを混合することはできませんが、1 つのルール内では任意の数の位置オプションを使用できます。

位置が指定されない場合は、デフォルトが想定されます。つまり、コンテンツ検索はパケット ペイロードの先頭から始まってパケットの末尾まで続きます。

また、既存の byte_extract 変数を使用して位置オプションの値を指定することもできます。詳細については、パケット データをキーワード引数の中に読み込む（27-85 ページ）を参照してください。

protected_content キーワードの中で検索位置の値を指定するには、次の手順を実行します。

ステップ 1　追加する protected_content キーワードのフィールドに値を入力します。次の選択肢があります。

- 長さ（**Length**）（必須）
- オフセット（**Offset**）
- 距離（**Distance**）

1 つの protected_content キーワード内で [オフセット（Offset）] オプションと [距離（Distance）] オプションを混合することはできませんが、1 つのルール内では任意の数の位置オプションを使用できます。

ステップ 2　ルールの作成または編集を続けます。詳細については、コンテンツ一致の制約（27-18 ページ）、コンテンツ一致の検索（27-15 ページ）、新しいルールの作成（27-106 ページ）、または 既存のルールの変更（27-108 ページ）を参照してください。

HTTP コンテンツ オプション

ライセンス：Protection

HTTP content または protected_content キーワード オプションを使用すると、HTTP Inspect プリプロセッサによってデコードされた HTTP メッセージ内でコンテンツ一致を検索する位置を指定できます。

次の 2 つのオプションは、HTTP 応答内のステータス フィールドを検索します。

- **HTTP** ステータス コード（**HTTP Status Code**）
- **HTTP** ステータス メッセージ（**HTTP Status Message**）

ルール エンジンは未加工の正規化されていないステータス フィールドを検索しますが、ここでは、他の raw HTTP フィールドと正規化された HTTP フィールドを併用する際に考慮すべき制限についての説明を簡略化するために、これらのオプションが別個に列挙されていることに注意してください。

次の 5 つのオプションは、必要に応じて HTTP 要求、応答、またはその両方の中で正規化フィールドを検索します（詳細については、HTTP コンテンツ オプション（27-24 ページ）を参照してください）。

- **HTTP URI**
- **HTTP** メソッド（**HTTP Method**）
- **HTTP** ヘッダー（**HTTP Header**）
- **HTTP Cookie**
- **HTTP** クライアント ボディ（**HTTP Client Body**）

次の 3 つのオプションは、必要に応じて HTTP 要求、応答、またはその両方の中で未加工の（正規化されていない）非ステータス フィールドを検索します（詳細については、HTTP コンテンツ オプション（27-24 ページ）を参照してください）。

- **HTTP Raw URI**
- **HTTP raw** ヘッダー（**HTTP Raw Header**）
- **HTTP Raw Cookie**

HTTP content オプションを選択する場合は、次のガイドラインに従ってください。

- HTTP content オプションは TCP トラフィックにのみ適用されます。
- パフォーマンスへの悪影響を避けるために、指定したコンテンツが出現する可能性のあるメッセージ部分だけを選択してください。

  たとえば、ショッピング カート メッセージの場合のように大きな cookie がトラフィックに含まれている可能性がある場合は、HTTP cookie ではなく HTTP ヘッダーの中で指定のコンテンツを検索することができます。
- HTTP Inspect プリプロセッサの正規化機能を活用し、パフォーマンスを向上させるには、作成するすべての HTTP 関連ルールの中に、[HTTP URI]、[HTTP メソッド（HTTP Method）]、[HTTP ヘッダー（HTTP Header）]、または [HTTP クライアント ボディ（HTTP Client Body）] オプションが選択された少なくとも 1 つの content または protected_content キーワードを含めてください。
- HTTP content または protected_content キーワード オプションと組み合わせて replace キーワードを使用することはできません。

単一の正規化された HTTP オプションまたはステータス フィールドを指定できます。または、複数の正規化 HTTP オプションとステータス フィールドを任意に組み合わせて、コンテンツ領域をマッチング対象にすることもできます。ただし、HTTP フィールド オプションを使用する場合には次の制限事項に注意してください。

- 同じ content または protected_content キーワードの中で、[生データ（Raw Data）] オプションを HTTP オプションと一緒に使用することはできません。
- raw HTTP フィールド オプション（[HTTP Raw URI]、[HTTP raw ヘッダー（HTTP Raw Header）]、または [HTTP Raw Cookie]）と、それぞれに対応する正規化されたオプション（[HTTP URI]、[HTTP ヘッダー（HTTP Header）]、または [HTTP Cookie]）を同じ content または protected_content キーワード内で一緒に使用することはできません。
- [高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] を、次の 1 つ以上の HTTP フィールド オプションと組み合わせて選択することはできません。

  [HTTP Raw URI]、[HTTP raw ヘッダー（HTTP Raw Header）]、[HTTP Raw Cookie]、[HTTP Cookie]、[HTTP メソッド（HTTP Method）]、[HTTP ステータス メッセージ（HTTP Status Message）]、または [**HTTP** ステータス コード（**HTTP Status Code**）]

  ただし、次のいずれかの正規化フィールドを検索するために高速パターン マッチ機能を使用する content または protected_content キーワードでは、上記のオプションを含めることができます。

  [HTTP URI]、[HTTP ヘッダー（HTTP Header）]、または [**HTTP** クライアント ボディ（**HTTP Client Body**）]

  たとえば、[HTTP Cookie]、[HTTP ヘッダー（HTTP Header）]、および [高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] を選択した場合、ルール エンジンは HTTP cookie と HTTP ヘッダーの両方でコンテンツを検索しますが、高速パターン マッチ機能は HTTP cookie ではなく、HTTP ヘッダーにのみ適用されます。
- 制限付きオプションと制限なしオプションを併用した場合、高速パターン マッチ機能は、指定された制限なしフィールドのみを検索することで、ルール エディタにルールを渡して（制限付きフィールドの評価を含む）完全な評価を行うべきかどうかを検査します。詳細については、高速パターン マッチ機能を使用（Use Fast Pattern Matcher）（27-28 ページ）を参照してください。

HTTP content および protected_content キーワード オプションに関する以下のリストでは、前述した制限事項が各オプションの説明に反映されています。

HTTP URI

正規化された要求 URI フィールド内でコンテンツ一致を検索するには、このオプションを選択します。

このオプションと pcre キーワードの HTTP URI(U)オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。詳細については、Snort 固有の正規表現後の修飾子の表を参照してください。

(注)　パイプライン処理された HTTP 要求パケットには複数の URI が含まれています。[HTTP URI] が選択されている場合、パイプライン処理された HTTP 要求パケットをルール エンジンが検出すると、そのパケット内のすべての URI でコンテンツ一致が検索されます。

HTTP Raw URI

正規化された要求 URI フィールド内でコンテンツ一致を検索するには、このオプションを選択します。

このオプションと pcre キーワードの HTTP URI(U)オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。詳細については、Snort 固有の正規表現後の修飾子の表を参照してください。

(注)　パイプライン処理された HTTP 要求パケットには複数の URI が含まれています。[HTTP URI] が選択されている場合、パイプライン処理された HTTP 要求パケットをルール エンジンが検出すると、そのパケット内のすべての URI でコンテンツ一致が検索されます。

HTTP メソッド(HTTP Method)

(URI で識別されるリソースに対して行う GET や POST などのアクションを特定する)要求メソッド フィールド内のコンテンツ一致を検索するには、このオプションを選択します。

HTTP ヘッダー(HTTP Header)

HTTP 要求内の(cookie を除く)正規化されたヘッダー フィールドでコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [HTTP 応答の検査(Inspect HTTP Responses)] オプションが有効になっている場合は応答内でも検索されます。

このオプションと pcre キーワードの HTTP ヘッダー(H)オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。詳細については、Snort 固有の正規表現後の修飾子の表を参照してください。

HTTP raw ヘッダー(HTTP Raw Header)

HTTP 要求内の(cookie を除く)raw ヘッダー フィールドでコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [HTTP 応答の検査(Inspect HTTP Responses)] オプションが有効になっている場合は応答内でも検索されます。

このオプションと pcre キーワードの HTTP raw ヘッダー(D)オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。詳細については、Snort 固有の正規表現後の修飾子の表を参照してください。

HTTP Cookie

正規化された HTTP クライアント要求ヘッダー内で識別される cookie でコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションが有効になっている場合は応答 set-cookie データ内でも検索されます。システムは、メッセージ本文に含まれる cookie を本文の内容として扱うことに注意してください。

cookie 内だけで一致を検索するには、HTTP Inspect プリプロセッサの [HTTP Cookie の検査（Inspect HTTP Cookies）] オプションを有効にする必要があります。これを有効にしない場合、ルール エンジンは cookie を含むヘッダー全体を検索します。詳細については、サーバレベル HTTP 正規化オプションの選択（19-37 ページ）を参照してください。

次の点に注意してください。

- このオプションと `pcre` キーワードの HTTP cookie（C）オプションを一緒に使用して、同じコンテンツを検索することはできません。詳細については、Snort 固有の正規表現後の修飾子の表を参照してください。
- `Cookie:` ヘッダー名と `Set-Cookie:` ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す `CRLF` は cookie の一部としてではなく、ヘッダーの一部として検査されます。

HTTP Raw Cookie

raw HTTP クライアント要求ヘッダー内で識別される cookie でコンテンツ一致を検索するには、このオプションを選択します。また、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションが有効になっている場合は応答 set-cookie データ内でも検索されます。システムは、メッセージ本文に含まれる cookie を本文の内容として扱うことに注意してください。

cookie 内だけで一致を検索するには、HTTP Inspect プリプロセッサの [HTTP Cookie の検査（Inspect HTTP Cookies）] オプションを有効にする必要があります。これを有効にしない場合、ルール エンジンは cookie を含むヘッダー全体を検索します。詳細については、サーバレベル HTTP 正規化オプションの選択（19-37 ページ）を参照してください。

次の点に注意してください。

- このオプションと `pcre` キーワードの HTTP raw cookie（K）オプションを一緒に使用して同じコンテンツを検索することはできません。詳細については、Snort 固有の正規表現後の修飾子の表を参照してください。
- `Cookie:` ヘッダー名と `Set-Cookie:` ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す `CRLF` は cookie の一部としてではなく、ヘッダーの一部として検査されます。

HTTP クライアント ボディ（HTTP Client Body）

HTTP クライアント要求内のメッセージ本文でコンテンツ一致を検索するには、このオプションを選択します。

このオプションが機能するためには、HTTP Inspect プリプロセッサの [HTTP クライアント ボディ（HTTP Client Body）Extraction Depth] オプションで 0 ～ 65535 の値を指定する必要があることに注意してください。詳細については、サーバレベル HTTP 正規化オプションの選択（19-37 ページ）を参照してください。

HTTP ステータス コード（HTTP Status Code）

HTTP 応答内の 3 桁のステータス コードでコンテンツ一致を検索するには、このオプションを選択します。

このオプションで一致が返されるようにするには、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションを有効にする必要があります。詳細については、サーバレベル HTTP 正規化オプションの選択（19-37 ページ）を参照してください。

HTTP ステータス メッセージ（**HTTP Status Message**）

HTTP 応答のステータス コードに付加されるテキスト記述の中でコンテンツ一致を検索するには、このオプションを選択します。

このオプションで一致が返されるようにするには、HTTP Inspect プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションを有効にする必要があります。詳細については、サーバレベル HTTP 正規化オプションの選択（19-37 ページ）を参照してください。

TCP トラフィックのコンテンツ検索を実行する場合に **HTTP content** オプションを指定するには、次の手順を実行します。

ステップ **1**　オプションで、HTTP Inspect プリプロセッサの正規化を活用して、パフォーマンスを向上させるには、以下のように選択します。

- 追加する `content` または `protected_content` キーワードの [HTTP URI]、[HTTP Raw URI]、[HTTP メソッド（HTTP Method）]、[HTTP ヘッダー（HTTP Header）]、[HTTP raw ヘッダー（HTTP Raw Header）]、または [HTTP クライアント ボディ（HTTP Client Body）] オプションから少なくとも 1 つ
- [HTTP Cookie] または [HTTP Raw Cookie] オプション

ステップ **2**　ルールの作成または編集を続けます。詳細については、コンテンツ一致の制約（27-18 ページ）、コンテンツ一致の検索（27-15 ページ）、新しいルールの作成（27-106 ページ）、または 既存のルールの変更（27-108 ページ）を参照してください。

高速パターン マッチ機能を使用（**Use Fast Pattern Matcher**）

ライセンス：Protection

（注）　これらのオプションは、`protected_content` キーワードの設定ではサポートされません。詳細については、protected_content キーワードの使用（27-16 ページ）を参照してください。

高速パターン マッチ機能は、パケットをルール エンジンに渡す前に、評価するルールをすばやく決定します。この初期決定により、パケット評価で使用されるルール数が大幅に減るため、パフォーマンスが向上します。

デフォルトで、高速パターン マッチ機能は、ルールで指定された最長のコンテンツをパケットで検索します。これは、不必要なルール評価をできるだけ減らすためです。次の例のようなルール フラグメントがあるとします。

```
alert tcp any any -> any 80 (msg:"Exploit"; content:"GET";
http_method; nocase; content:"/exploit.cgi"; http_uri;
nocase;)
```

ほとんどすべての HTTP クライアント要求にはコンテンツ `GET` が含まれていますが、コンテンツ `/exploit.cgi` を含む要求は稀です。`GET` を高速パターン コンテンツとして使用した場合、ルール エンジンはほとんどのケースでこのルールを評価し、一致はほとんど検出されないでしょう。しかし、`/exploit.cgi` を使用するとほとんどのクライアントの `GET` 要求は評価されないため、パフォーマンスが向上します。

指定されたコンテンツが高速パターン マッチ機能で検出された場合にのみ、ルール エンジンはパケットをルールに照らして評価します。たとえば、ルール内の 1 つの content キーワードでコンテンツ short を指定し、別のキーワードで longer、さらに 3 番目のキーワードで longest を指定した場合、高速パターン マッチ機能はコンテンツ longest を使用し、ルール エンジンがペイロード内で longest を検出した場合にのみ、ルールが評価されます。

より短い検索パターンを高速パターン マッチ機能で使用するよう指定するには、[高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] オプションを使用できます。理論的には、指定したパターンの方が最長パターンよりもパケット内で見つかる可能性が低いため、より的を絞って対象のエクスプロイトを識別できます。

[高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] と他のオプションを同じ content キーワード内で選択する場合は、次の制限事項に注意してください。

- ルールごとに 1 回だけ、[高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] を指定できます。
- [高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] と [一致しない（Not）] を組み合わせて選択した場合は、[距離（Distance）]、[次の範囲内（Within）]、[オフセット（Offset）]、または [奥行き（Depth）] を使用できません。
- [高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] を、次のいずれかの HTTP フィールド オプションと組み合わせて選択することはできません。

  [HTTP Raw URI]、[HTTP raw ヘッダー（HTTP Raw Header）]、[HTTP Raw Cookie]、[HTTP Cookie]、[HTTP メソッド（HTTP Method）]、[HTTP ステータス メッセージ（HTTP Status Message）]、または [**HTTP** ステータス コード（**HTTP Status Code**）]

  ただし、次のいずれかの正規化フィールドを検索するために高速パターン マッチ機能を使用する content キーワードでは、上記のオプションを含めることができます。

  [HTTP URI]、[HTTP ヘッダー（HTTP Header）]、または [**HTTP** クライアント ボディ（**HTTP Client Body**）]

  たとえば、[HTTP Cookie]、[HTTP ヘッダー（HTTP Header）]、および [高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] を選択した場合、ルール エンジンは HTTP cookie と HTTP ヘッダーの両方でコンテンツを検索しますが、高速パターン マッチ機能は HTTP cookie ではなく、HTTP ヘッダーにのみ適用されます。

  raw HTTP フィールド オプション（[HTTP Raw URI]、[HTTP raw ヘッダー（HTTP Raw Header）]、または [HTTP Raw Cookie]）と、それぞれに対応する正規化されたオプション（[HTTP URI]、[HTTP ヘッダー（HTTP Header）]、または [HTTP Cookie]）を同じ content キーワード内で一緒に使用することはできないことに注意してください。詳細については、HTTP コンテンツ オプション（27-24 ページ）を参照してください。

  制限付きオプションと制限なしオプションを併用した場合、高速パターン マッチ機能は、指定された制限なしフィールドのみを検索することで、ルール エンジンにパケットを渡して（制限付きフィールドの評価を含む）完全な評価を行うべきかどうかを検査します。
- オプションで、[高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] を選択した場合には [高速パターン マッチ機能のみ（Fast Pattern Matcher Only）] または [高速パターン マッチ機能オフセットおよび長さ（Fast Pattern Matcher Offset and Length）] を選択することもできますが、この両方は選択できません。
- Base64 データの検査時には高速パターン マッチ機能を使用できません（詳細については、Base64 データのデコードと検査（27-104 ページ）を参照してください）。

[高速パターン マッチ機能のみ(**Fast Pattern Matcher Only**)**]** の使用

[高速パターン マッチ機能のみ(Fast Pattern Matcher Only)] オプションを使用すると、content キーワードをルール オプションとしてではなく、高速パターン マッチ機能オプションとしてのみ使用できます。指定したコンテンツをルール エンジンで評価する必要がない場合、このオプションを使ってリソースを節約できます。たとえば、ペイロード内のいずれかの場所にコンテンツ 12345 が存在することだけを必要とするルールがあるとします。高速パターン マッチ機能でパターンが検出された場合に、ルール内の追加のキーワードに照らしてパケットを評価できます。パターン 12345 が含まれているかどうかを判断するために、ルール エンジンがパケットを再評価する必要はありません。

指定されたコンテンツに関連する他の条件がルールに含まれている場合は、このオプションを使用しないでください。たとえば、別のルール条件で abcd が 1234 の前に出現するかどうかを判断する場合には、このオプションを使ってコンテンツ 1234 を検索しないでください。[高速パターン マッチ機能のみ(Fast Pattern Matcher Only)] を指定すると、指定されたコンテンツがルール エンジンによって検索されないため、このケースではルール エンジンが相対的な位置を判断できません。

このオプションを使用するときには、次の条件に注意してください。

- 指定されたコンテンツは位置に依存しない、つまり、ペイロードのどこにでも出現する可能性があるため、位置オプション([距離(Distance)]、[次の範囲内(Within)]、[オフセット(Offset)]、[奥行き(Depth)]、[高速パターン マッチ機能オフセットおよび長さ(Fast Pattern Matcher Offset and Length)])を使用することはできません。
- このオプションを [一致しない(Not)] と組み合わせて使用することはできません。
- このオプションを [高速パターン マッチ機能オフセットおよび長さ(Fast Pattern Matcher Offset and Length)] と組み合わせて使用することはできません。
- 大文字/小文字を区別しない方法ですべてのパターンが高速パターン マッチ機能に挿入されるため、指定したコンテンツは「大文字/小文字の区別なし」として扱われます。これは自動的に処理されるため、このオプションの選択時に [大文字小文字の区別なし(Case Insensitive)] を選択する必要はありません。
- [高速パターン マッチ機能のみ(Fast Pattern Matcher Only)] オプションを使用する content キーワードの直後に、現在の検索位置を基準にして検索位置を設定する次のキーワードを続けないようにしてください。
- isdataat
- pcre
- content([距離(Distance)] または [次の範囲内(Within)] が選択されている場合)
- content([HTTP URI] が選択されている場合)
- asn1
- byte_jump
- byte_test
- byte_extract
- base64_decode

[高速パターン マッチ機能オフセットおよび長さ(**Fast Pattern Matcher Offset and Length**)**]** の指定

[高速パターン マッチ機能オフセットおよび長さ(Fast Pattern Matcher Offset and Length)] オプションを使用すると、検索するコンテンツの一部分を指定できます。これにより、パターンが非常に長く、ルールの一致の可能性を判断するのにパターンの一部分だけで十分な場合に、メモリ消費を抑えることができます。高速パターン マッチ機能によってルールが選択されたときに、パターン全体がルールに照らして評価されます。

次の構文に従い、検索を開始する位置（オフセット）およびコンテンツ内をどれほど検索するか（長さ）をバイト単位で指定することにより、高速パターン マッチ機能で使用する部分を決定します。

offset,*length*

たとえば、次のコンテンツに対して

```
1234567
```

次のようにオフセットと長さのバイト数を指定した場合、

```
1,5
```

高速パターン マッチ機能はコンテンツ `23456` のみを検索します。

このオプションを [高速パターン マッチ機能のみ（Fast Pattern Matcher Only）] と一緒に使用できないことに注意してください。

高速パターン マッチ機能で検索されるコンテンツを指定するには、次の手順を実行します。

ステップ 1　追加する `content` キーワードに関して [高速パターン マッチ機能を使用（Use Fast Pattern Matcher）] を選択します。

ステップ 2　オプションで、指定したパターンがパケット内に存在するかどうかをルール エンジン評価なしで判断するには [高速パターン マッチ機能のみ（Fast Pattern Matcher Only）] を選択します。

指定されたコンテンツが高速パターン マッチ機能で検出された場合にのみ、評価が開始されます。

ステップ 3　オプションで、次の構文に従い、コンテンツの検索場所となるパターンの部分を [高速パターン マッチ機能オフセットおよび長さ（Fast Pattern Matcher Offset and Length）] で指定します。

offset,*length*

ここで、*offset* は検索の開始場所となるコンテンツ先頭からのバイト数を指定し、*length* は検索を続けるバイト数を指定します。

ステップ 4　ルールの作成または編集を続けます。詳細については、コンテンツ一致の制約（27-18 ページ）、PCRE を使用したコンテンツの検索（27-38 ページ）、新しいルールの作成（27-106 ページ）、または既存のルールの変更（27-108 ページ）を参照してください。

インライン展開でのコンテンツの置換

ライセンス：Protection

インライン展開で `replace` キーワードを使用すると、指定したコンテンツを置き換えることができます。

`replace` キーワードを使用するには、`content` キーワードを使って特定の文字列を検索するカスタム 標準テキスト ルール を作成します。その後、`replace` キーワードを使用して、コンテンツを置き換える文字列を指定します。置換値とコンテンツ値は同じ長さである必要があります。

（注）　`protected_content` キーワード内でハッシュされたコンテンツを置き換えるために `replace` キーワードを使用することはできません。詳細については、protected_content キーワードの使用（27-16 ページ）を参照してください。

オプションで、以前の ASA FirePOWER モジュール ソフトウェア バージョンとの下位互換性を維持するために、置換文字列を引用符で囲むことができます。引用符を含めない場合は、それらが自動的にルールに追加されるため、構文的に正しいルールになります。置換テキストの一部として先行引用符または後続引用符を含めるには、次の例に示すように、バックスラッシュを使ってエスケープする必要があります。

```
"replacement text plus \\"quotation\\" marks""
```

1 つのルール内に複数の `replace` キーワードを含めることができますが、`content` キーワードごとに 1 つずつしか含めることができません。ルールによって検出されたコンテンツの最初のインスタンスだけが置き換えられます。

次に、`replace` キーワードの使用例を示します。

- エクスプロイトを含んでいる着信パケットをシステムが検出した場合、有害な文字列を無害な文字列に置き換えることができます。このテクニックは、有害なパケットを単に破棄するよりも効果的である場合があります。破棄されたパケットを攻撃者が単に再送信し続け、やがてネットワーク防御を通り抜けるか、ネットワークを氾濫させるという攻撃シナリオがあります。パケットを破棄する代わりに別の文字列に置き換えることで、脆弱ではないターゲットに対して攻撃が実行されたと攻撃者に思い込ませることができます。
- （たとえば Web サーバの）脆弱なバージョンが稼働しているかどうかを調べる偵察攻撃が懸念される場合は、発信パケットを検出して、バナーを独自のテキストに置き換えることができます。

（注）　置換ルールを使用するインライン侵入ポリシー内でルール状態が [イベントを生成する（Generate Events）] に設定されていることを確認してください。ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定した場合はパケットが破棄され、コンテンツが置き換えられません。

文字列置換プロセスでは、宛先ホストがエラーなしでパケットを受信できるように、パケットチェックサムがシステムによって自動的に更新されます。

`replace` キーワードを HTTP 要求メッセージ `content` キーワード オプションと組み合わせて使用できないことに注意してください。詳細については、「コンテンツ一致の検索（27-15 ページ）」と「HTTP コンテンツ オプション（27-24 ページ）」を参照してください。

インライン展開でコンテンツを置き換えるには、次の手順を実行します。

ステップ 1　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [コンテンツ（content）] を選択して、**[オプションを追加（Add Option）]** をクリックします。

`content` キーワードが表示されます。

ステップ 2　[コンテンツ（content）] フィールドで、検出するコンテンツを指定します。オプションで、該当する引数を選択します。HTTP 要求メッセージ `content` キーワード オプションを `replace` キーワードと一緒に使用できないことに注意してください。

ステップ 3　ドロップダウンリストで [replace] を選択して、**[オプションを追加（Add Option）]** をクリックします。

`replace` キーワードが `content` キーワードの下に表示されます。

ステップ 4　[replace:] フィールドで、指定したコンテンツに対する置換文字列を指定します。

Byte_Jump と Byte_Test の使用

ライセンス：Protection

byte_jump と byte_test を使用すると、パケット内のどの位置でルール エンジンがデータ マッチング検査を開始すべきか、どのバイトを評価すべきかを計算できます。

また、byte_jump および byte_test **DCE/RPC** 引数を使用すると、DCE/RPC プリプロセッサで処理されるトラフィック用にいずれかのキーワードを調整できます。**DCE/RPC** 引数を使用するときには、他の特定の DCE/RPC キーワードと組み合わせて byte_jump と byte_test を使用することもできます。詳細については、「DCE/RPC トラフィックのデコード（19-2 ページ）」と「DCE/RPC キーワード（27-62 ページ）」を参照してください。

詳細については、次の各項を参照してください。

- byte_jump（27-33 ページ）
- byte_test（27-36 ページ）

byte_jump

ライセンス：Protection

byte_jump キーワードは、指定されたバイト セグメントで定義されるバイト数を計算し、指定したオプションに応じて、指定されたバイト セグメントの末尾から順方向に、またはパケット ペイロードの先頭から、パケット内でそのバイト数だけスキップします。パケットの特定のバイト セグメントが、パケット内の可変データに含まれるバイト数を示す場合には、これが役立ちます。

次の表では、byte_jump キーワードで必要な引数を説明します。

表 ***27-8*** ***byte_jump*** の必須の引数

引数	説明
Bytes	パケットから計算するバイト数。
Offset	ペイロード内で処理を開始するバイト数。offset カウンタはバイト 0 から始まるため、パケット ペイロードの先頭、または最後に見つかったコンテンツ一致から順方向にジャンプさせるバイト数から 1 を差し引いて offset 値を計算してください。 また、既存の byte_extract 変数を使用してこの引数の値を指定することもできます。詳細については、パケット データをキーワード引数の中に読み込む（27-85 ページ）を参照してください。

次の表で説明するオプションを使用すると、必須の引数に指定された値をシステムがどのように解釈するかを定義できます。

表 ***27-9*** ***byte_jump*** の追加のオプション引数

引数	説明
Relative	最後に見つかったコンテンツ一致で検出された最後のパターンを基準にしてオフセットを計算します。
Align	変換されたバイト数を、次の 32 ビット境界に切り上げます。

表 27-9　byte_jump の追加のオプション引数（続き）

引数	説明
Multiplier	ルール エンジンで最終的な byte_jump 値を算出するために、パケットから得られた byte_jump 値に掛ける値を示します。 つまり、ルール エンジンは、指定されたバイト セグメントで定義されるバイト数だけスキップする代わりに、Multiplier 引数で指定される整数を乗算したバイト数だけスキップします。
Post Jump Offset	他の byte_jump 引数を適用した後に、順方向または逆方向にスキップするバイト数（-63535 ～ 63535）。正の値は順方向にスキップし、負の値は逆方向にスキップします。無効にするには、フィールドを空白のままにするか、0 を入力します。 **DCE/RPC** 引数を選択したときに適用されない byte_jump 引数については、エンディアンネス引数の表の **DCE/RPC** 引数を参照してください。
From Beginning	スキップするバイト数を示すバイト セグメントの末尾からではなく、パケット ペイロードの先頭から数えて、指定されたバイト数だけペイロード内をスキップするようルール エンジンに指示します。

DCE/RPC、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

byte_jump キーワードでどのようにバイト数を計算するかを定義するには、次の表に示す引数から選択できます（どの引数も指定されない場合は、ネットワーク バイト順が使用されます）。

表 27-10　エンディアンネス引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に byte_jump キーワードを指定します。詳細については、DCE/RPC トラフィックのデコード（19-2 ページ）を参照してください。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。**Number Type**、**Endian**、および **From Beginning** 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて byte_jump を使用することもできます。詳細については、DCE/RPC キーワード（27-62 ページ）を参照してください。

次の表に示すいずれか 1 つの引数を使用して、パケット内のストリング データをシステムがどのように表示するかを定義します。

表 ***27-11*** ***Number Type*** 引数

引数	説明
Hexadecimal String	変換後のストリング データを 16 進形式で表現します。
Decimal String	変換後のストリング データを 10 進形式で表現します。
Octal String	変換後のストリング データを 8 進形式で表現します。

たとえば、次のような値を `byte_jump` に設定した場合、

- Bytes = 4
- Offset = 12
- Relative enabled
- Align enabled

ルール エンジンは、最後に見つかったコンテンツ一致から 13 バイト後に出現する 4 つのバイトで記述される数値を計算して、そのバイト数だけパケット内を順方向にスキップします。たとえば、ある特定のパケット内で計算される 4 つのバイトが `00 00 00 1F` である場合、ルール エンジンはこれを 31 に変換します。`align` が指定されている（次の 32 ビット境界まで移動するようエンジンに指示する）ため、ルール エンジンはパケット内を 32 バイト先までスキップします。

あるいは、次のような値を `byte_jump` に設定した場合、

- Bytes = 4
- Offset = 12
- From Beginning enabled
- Multiplier = 2

ルール エンジンは、パケットの先頭から 13 バイト後に出現する 4 つのバイトで記述される数値を計算します。その後、その数値に 2 を掛けてスキップする総バイト数を計算します。たとえば、ある特定のパケット内で計算される 4 つのバイトが `00 00 00 1F` である場合、ルール エンジンはこれを 31 に変換し、それに 2 を掛けて 62 にします。[From Beginning] が有効になっているため、ルール エンジンはパケット内の最初の 63 バイトをスキップします。

byte_jump を使用するには、次の手順を実行します。

ステップ **1**　ドロップダウンリストで [byte_jump] を選択して、[オプションを追加（Add Option）] をクリックします。

[byte_jump] セクションが、選択された最後のキーワードの下に表示されます。

byte_test

ライセンス：Protection

byte_test キーワードは、指定されたバイト セグメント内のバイト数を計算し、指定した演算子と値に基づいてそれらを比較します。

次の表に、byte_test キーワードで必要な引数を説明します。

表 27-12　byte_test の必須の引数

引数	説明
Bytes	パケットから計算するバイト数。1 ～ 10 バイトを指定できます。
Operator and Value	指定された値を <、>、=、!、&、^、!>、!<、!=、!& または !^ で比較します。 たとえば、[!1024 と指定した場合、byte_test は指定された数値を変換し、それが 1024 と等しくなければイベントが生成されます（他のすべてのキーワード パラメータが一致する場合）。 ! と != は同等であることに注意してください。 また、既存の byte_extract 変数を使用してこの引数の値を指定することもできます。詳細については、パケット データをキーワード引数の中に読み込む（27-85 ページ）を参照してください。
Offset	ペイロード内で処理を開始するバイト数。offset カウンタはバイト 0 から始まるため、パケット ペイロードの先頭、または最後に見つかったコンテンツ一致から順方向にカウントするバイト数から 1 を差し引いて offset 値を計算してください。 また、既存の byte_extract 変数を使用してこの引数の値を指定することもできます。詳細については、パケット データをキーワード引数の中に読み込む（27-85 ページ）を参照してください。

次の表に示す引数を使用すると、システムで byte_test 引数がどのように使用されるかをさらに定義できます。

表 27-13　byte_test の追加のオプション引数

引数	説明
Relative	最後に見つかったパターン一致を基準にしてオフセットを計算します。
Align	変換されたバイト数を、次の 32 ビット境界に切り上げます。

DCE/RPC、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

検査対象となるバイトを byte_test キーワードでどのように計算するか定義するには、次の表の中から引数を選択します。どの引数も指定しない場合は、ネットワーク バイト順が使用されます。

表 *27-14*　*byte_test* のエンディアンネス引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に `byte_test` キーワードを指定します。詳細については、DCE/RPC トラフィックのデコード（19-2 ページ）を参照してください。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。**Number Type** 引数と **Endian** 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて `byte_test` を使用することもできます。詳細については、DCE/RPC キーワード（27-62 ページ）を参照してください。

次の表に示すいずれか 1 つの引数を使用して、パケット内のストリング データをシステムがどのように表示するかを定義できます。

表 *27-15*　*Number Type byte-test* 引数

引数	説明
Hexadecimal String	変換後のストリング データを 16 進形式で表現します。
Decimal String	変換後のストリング データを 10 進形式で表現します。
Octal String	変換後のストリング データを 8 進形式で表現します。

たとえば、次のような値を `byte_test` に指定した場合、

- Bytes = 4
- Operator and Value > 128
- Offset = 8
- Relative enabled

ルール エンジンは、最後に見つかったコンテンツ一致から（それを基準にして）9 バイト後に出現する 4 つのバイトで記述される数値を計算し、その計算値が 128 バイトを超えた場合に、ルールがトリガーとして使用されます。

byte_test を使用するには、次の手順を実行します。

ステップ **1**　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [byte_test] を選択して、[オプションを追加（Add Option）] をクリックします。

[byte_test] セクションが、選択された最後のキーワードの下に表示されます。

PCRE を使用したコンテンツの検索

ライセンス：Protection

pcre キーワードを使用すると、指定されたコンテンツをパケット ペイロード内で検査するために Perl 互換正規表現（PCRE）を使用できます。PCRE を使用すると、同じ内容のわずかなバリエーションにそれぞれ一致する複数のルールを作成する手間が省けます。

正規表現は、さまざまな方法で表現されることのあるコンテンツを検索する場合に役立ちます。パケットのペイロード内でコンテンツを検索するときには、コンテンツがさまざまな属性を持つ可能性があることを考慮すべき場合があります。

侵入ルールで使われる正規表現構文は完全な正規表現ライブラリのサブセットであり、完全なライブラリ内のコマンドで使用される構文とはいくつかの点で異なることに注意してください。ルール エディタを使用して pcre キーワードを追加するときには、次の形式で完全な値を入力します。

```
!/pcre/ ismxAEGRBUIPHDMCKSY
```

引数の説明

- ! はオプションの否定です（正規表現に一致しないパターンを照合する場合にこれを使用します）。
- */pcre/* は Perl 互換正規表現です。
- ismxAEGRBUIPHDMCKSY は修飾子オプションの任意の組み合わせです。

また、次の表に示す文字をエスケープする必要があることに注意してください。これにより、パケット ペイロード内で特定のコンテンツを検索するために PCRE でこれらの文字を使用した場合、ルール エンジンがそれを正しく解釈するようになります。

表 ***27-16***　エスケープする ***PCRE*** 文字

エスケープする必要のある文字	バックスラッシュを使用した場合	**16** 進コードを使用した場合
#（ナンバー記号）	\\#	\\x23
;（セミコロン）	\\;	\\x3B
|（縦棒）	\\\|	\\x7C
:（コロン）	\\:	\\x3A

ヒント　オプションで、Perl 互換正規表現を引用符で囲むことができます。たとえば、*pcre_expression* は "*pcre_expression*" となります。引用符が任意ではなく必須であった旧バージョンに慣れている経験豊富なユーザのために、引用符を使用するオプションが提供されています。保存後のルールをルール エディタで表示すると、引用符が表示されません。

また、m?regex? を使用することもできます。ここで、? は / 以外の区切り文字です。正規表現内でスラッシュと一致させる必要があり、バックスラッシュを使ってそれをエスケープしたくない場合には、これを使用できます。たとえば、m?*regex*? ismxAEGRBUIPHDMCKSY を使用できます。ここで *regex* は Perl 互換正規表現、ismxAEGRBUIPHDMCKSY は修飾子オプションの任意の組み合わせです。正規表現の構文の詳細については、Perl 互換正規表現の基本（27-39 ページ）を参照してください。

以下の項では、有効な pcre キーワードの値を作成する方法について詳しく説明します。

- Perl 互換正規表現の基本（27-39 ページ）では、Perl 互換正規表現で使われる一般的な構文について説明します。
- PCRE 修飾子のオプション（27-40 ページ）では、正規表現を変更するために使用できるオプションについて説明します。
- PCRE キーワード値の例（27-43 ページ）では、ルールにおける pcre キーワードの使用例を示します。

Perl 互換正規表現の基本

ライセンス：Protection

pcre キーワードでは、標準の Perl 互換正規表現（PCRE）構文を使用できます。以下の項では、この構文について説明します。

ヒント　ここでは PCRE で使用可能な基本的な構文について説明しますが、Perl および PCRE 専用のオンライン リファレンスやブックで、さらに詳しい情報を参照することもできます。

メタ文字

ライセンス：Protection

メタ文字は正規表現内で特別な意味を持つリテラル文字です。メタ文字を正規表現内で使用するときには、その前にバックスラッシュを付けて「エスケープする」必要があります。

次の表に、PCRE で使用可能なメタ文字について説明し、それぞれの例を示します。

表 27-17　PCRE メタ文字

メタ文字	説明	例
.	改行以外の任意の文字と一致します。修飾オプションとして s が使用されている場合は、改行文字も含まれます。	abc. は、abcd、abc1abc# などと一致します。
*	ある文字または式の 0 回以上の出現と一致します。	abc* は、abc、abcc、abccc、abcccccc などと一致します。
?	ある文字または式の 0 回または 1 回の出現と一致します。	abc? は、abc と一致します。
+	ある文字または式の 1 回以上の出現と一致します。	abc+ は、abc、abcc、abccc、abcccccc などと一致します。
()	式をグループ化します。	(abc)+ は、abc、abcabc、abcabcabc などと一致します。
	ある文字または式の一致回数の限度を指定します。下限と上限を設定する場合には、下限と上限をカンマで区切ります。	a{4,6} は、aaaa、aaaaa、または aaaaaa と一致します。 (ab){2} は abab と一致します。
[]	文字クラスを定義できます。セットの中で記述される任意の文字または文字の組み合わせに一致します。	[abc123] は、a または b または c などと一致します。
^	文字列の先頭でコンテンツを照合します。また、文字クラスの中で否定としても使用されます。	^in は、info 内の "in" と一致しますが、bin では一致しません。[^a] は、a を含まない任意の文字列と一致します。

表 27-17　PCRE メタ文字（続き）

メタ文字	説明	例
$	文字列の末尾でコンテンツを照合します。	ce$ は、announce 内の "ce" と一致しますが、cent では一致しません。
|	OR 式を示します。	(MAILTO|HELP) は、MAILTO または HELP と一致します。
\\	メタ文字を実際の文字として使用できます。また、事前定義された文字クラスを指定するためにも使われます。	\\. はピリオドと一致し、* はアスタリスクと一致し、\\\\ はバックスラッシュと一致します。\\d は数字と一致し、\\w は英数字と一致します。PCRE での文字クラスの使用方法については、文字クラス（27-40 ページ）を参照してください。

文字クラス

ライセンス：Protection

文字クラスには、英字、数字、英数字、および空白文字があります。大カッコで囲んで独自の文字クラスを作成できます（メタ文字（27-39 ページ）を参照）。また、事前定義のクラスをさまざまな文字タイプのショートカットとして使用することもできます。追加の修飾子なしで文字クラスを使用すると、1 つの文字クラスは 1 桁または 1 文字に一致します。

次の表に、PCRE で使用できる事前定義の文字クラスの説明と例を示します。

表 27-18　PCRE 文字クラス

文字クラス	説明	文字クラスの定義
\\d	数字（桁）と一致します。	[0-9]
\\D	数字以外の任意の文字と一致します。	[^0-9]
\\w	英数字（語）と一致します。	[a-zA-Z0-9_]
\\W	英数字以外の任意の文字と一致します。	[^a-zA-Z0-9_]
\\s	スペース、復帰、タブ、改行、および改ページを含む空白文字と一致します。	[\\r\\t\\n\\f]
\\S	空白文字以外の任意の文字と一致します。	[^ \\r\\t\\n\\f]

PCRE 修飾子のオプション

ライセンス：Protection

pcre キーワードの値の中で正規表現構文を指定した後、修飾オプションを使用できます。これらの修飾子は、Perl、PCRE、および Snort 固有の処理機能を実行します。修飾子は、常に PCRE 値の末尾に、次の形式で出現します。

/*pcre*/ismxAEGRBUIPHDMCKSY

ここで、ismxAEGRBUPHMC には、次の表に示す任意の修飾オプションを含めることができます。

ヒント　オプションで、正規表現と修飾オプションを引用符で囲むことができます（たとえば "/pcre/ismxAEGRBUIPHDMCKSY"）。引用符が任意ではなく必須であった旧バージョンに慣れている経験豊富なユーザのために、引用符を使用するオプションが提供されています。保存後のルールをルール エディタで表示すると、引用符が表示されません。

次の表に、Perl 処理機能を実行するために使用できるオプションを説明します。

表 27-19　Perl 関連の正規表現後オプション

オプション	説明
i	正規表現で大文字と小文字を区別しないようにします。
s	ドット文字(.)改行または \\n 文字を除くすべての文字を表します。オプションとして "s" を使用すると、これをオーバーライドして、改行文字を含むすべての文字をドット文字に一致させることができます。
m	デフォルトで、1 つの文字列は複数文字からなる単一行として扱われ、^ と $ は特定の文字列の先頭および末尾に一致します。オプションとして "m" を使用すると、^ および $ はバッファの先頭または末尾だけでなく、バッファ内の改行文字の直前または直後のコンテンツとも一致します。
x	エスケープされた(バックスラッシュが先行する)場合、および文字クラスに含まれる場合を除き、空白データ文字がパターン内に出現してもそれを無視します。

次の表に、正規表現の後ろに使用できる PCRE 修飾子の説明を示します。

表 27-20　PCRE 関連の正規表現後オプション

オプション	説明
A	文字列の先頭でパターンが一致する必要があります(正規表現で ^ を使用した場合と同じ)。
E	対象の文字列の末尾でのみ一致するように $ を設定します。(E を伴わない $ は、それが改行である場合には最後の文字の直前とも一致しますが、他の改行文字の直前とは一致しません)。
G	デフォルトで、* + および ? は「最長マッチ」を実行します。つまり、複数の一致が見つかった場合、最も長い一致が選択されます。G 文字を使用するとこの動作が変更され、常に最初の一致がこれらの文字で選択されます。ただし後ろに疑問符(?)が続く場合を除きます。たとえば、*? +? および ?? は、G 修飾子を使った構造内で最長マッチを実行し、疑問符が付加されない *、+、または ? が出現した場合は最長マッチを実行しません。

次の表に、正規表現の後ろに使用できる Snort 固有の修飾子の説明を示します。

表 27-21　Snort 固有の正規表現後の修飾子

オプション	説明
R	ルール エンジンで見つかった最後の一致の末尾を基準にして、一致するコンテンツを検索します。
B	プリプロセッサによってデコードされる前のデータ内のコンテンツを検索します(このオプションは、content または protected_content キーワードとともに Raw Data 引数を使用する場合に似ています)。
U	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージの URI 内のコンテンツを検索します。このオプションと content または protected_content キーワードの [HTTP URI] オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。詳細については、HTTP コンテンツ オプション(27-24 ページ)を参照してください。 (注)　パイプライン処理された HTTP 要求パケットには複数の URI が含まれています。U オプションを含む PCRE 式を使用すると、ルール エンジンは、パイプライン処理された HTTP 要求パケット内の最初の URI でのみコンテンツ一致を検索します。パケット内のすべての URI を検索するには、U オプションを使った PCRE 式を一緒に使用するかどうかに関係なく、[HTTP URI] を選択した content または protected_content キーワードを使用してください。

表 27-21　*Snort* 固有の正規表現後の修飾子（続き）

オプション	説明
I	HTTP Inspect プリプロセッサによってデコードされた raw HTTP 要求メッセージの URI 内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの [HTTP Raw URI] オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。詳細については、HTTP コンテンツ オプション（27-24 ページ）を参照してください。
P	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージ本文の中でコンテンツを検索します。詳細については、HTTP コンテンツ オプション（27-24 ページ）で、`content` および `protected_content` キーワードの [HTTP クライアント ボディ（HTTP Client Body）] オプションを参照してください。
H	HTTP Inspect プリプロセッサによってデコードされた HTTP 要求または応答メッセージの（cookie を除く）ヘッダー内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの [HTTP ヘッダー（HTTP Header）] オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。詳細については、HTTP コンテンツ オプション（27-24 ページ）を参照してください。
D	HTTP Inspect プリプロセッサによってデコードされた未加工の HTTP 要求または応答メッセージの（cookie を除く）ヘッダー内のコンテンツを検索します。このオプションと `content` または `protected_content` キーワードの [HTTP raw ヘッダー（HTTP Raw Header）] オプションを一緒に使用して、同じコンテンツを検索できないことに注意してください。詳細については、HTTP コンテンツ オプション（27-24 ページ）を参照してください。
M	HTTP Inspect プリプロセッサによってデコードされた正規化済み HTTP 要求メッセージのメソッド フィールド内のコンテンツを検索します。メソッド フィールドは、URI で識別されるリソースに対して実行すべきアクション（GET、PUT、CONNECT など）を特定します。詳細については、HTTP コンテンツ オプション（27-24 ページ） で、`content` および `protected_content` キーワードの [HTTP メソッド（HTTP Method）] オプションを参照してください。
C	HTTP Inspect プリプロセッサの [HTTP Cookie の検査（Inspect HTTP Cookies）] オプションが有効になっている場合は、HTTP 要求ヘッダーの cookie 内の正規化済みコンテンツを検索します。さらに、プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションが有効になっている場合は、HTTP 応答ヘッダーの set-cookie 内も検索します。[HTTP Cookie の検査（Inspect HTTP Cookies）] が有効になっていない場合は、cookie または set-cookie データを含むヘッダー全体を検索します。 次の点に注意してください。 • メッセージ本文に含まれる cookie は、本文のコンテンツとして扱われます。 • このオプションと `content` または `protected_content` キーワードの [HTTP Cookie] オプションを一緒に使用して、同じコンテンツを検索することはできません。詳細については、HTTP コンテンツ オプション（27-24 ページ）を参照してください。 • `Cookie:` ヘッダー名と `Set-Cookie:` ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す `CRLF` は cookie の一部としてではなく、ヘッダーの一部として検査されます。

表 27-21　Snort 固有の正規表現後の修飾子（続き）

オプション	説明
K	HTTP Inspect プリプロセッサの [HTTP Cookie の検査（Inspect HTTP Cookies）] オプションが有効になっている場合は、HTTP 要求ヘッダーの cookie 内の未加工のコンテンツを検索します。さらに、プリプロセッサの [HTTP 応答の検査（Inspect HTTP Responses）] オプションが有効になっている場合は、HTTP 応答ヘッダーの set-cookie 内も検索します。[HTTP Cookie の検査（Inspect HTTP Cookies）] が有効になっていない場合は、cookie または set-cookie データを含むヘッダー全体を検索します。 次の点に注意してください。 • メッセージ本文に含まれる cookie は、本文のコンテンツとして扱われます。 • このオプションと content または protected_content キーワードの [HTTP Raw Cookie] オプションを一緒に使用して、同じコンテンツを検索することはできません。詳細については、HTTP コンテンツ オプション（27-24 ページ）を参照してください。 • Cookie: ヘッダー名と Set-Cookie: ヘッダー名、ヘッダー行の先行スペース、およびヘッダー行の終わりを示す CRLF は cookie の一部としてではなく、ヘッダーの一部として検査されます。
S	HTTP 応答内の 3 桁のステータス コードを検索します。詳細については、HTTP コンテンツ オプション（27-24 ページ）で、content および protected_content キーワードの [HTTP ステータス コード（HTTP Status Code）] オプションを参照してください。
Y	HTTP 応答内のステータス コードに付加されるテキスト記述を検索します。詳細については、HTTP コンテンツ オプション（27-24 ページ）で、content および protected_content キーワードの [HTTP ステータス メッセージ（HTTP Status Message）] オプションを参照してください。

（注）　U オプションと R オプションを組み合わせて使用しないでください。パフォーマンスの問題が発生する可能性があります。また、他の HTTP コンテンツ オプション（I、P、H、D、M、C、K、S または Y）と組み合わせて U オプションを使用しないでください。

PCRE キーワード値の例

ライセンス：Protection

次に、pcre で入力できる値の例を示し、それぞれの例で何が一致するかを説明します。

- **/feedback[(\\d{0,1})]?\\.cgi/U**

  この例では、URI データにのみ配置された、feedback の後に 0 個または 1 個の数字、さらに .cgi が続くインスタンスをパケット ペイロード内で検索します。

  この例は以下のものと一致します。

- feedback.cgi
- feedback1.cgi
- feedback2.cgi
- feedback3.cgi

  この例は、以下のものとは一致しません。

- feedbacka.cgi
- feedback11.cgi
- feedback21.cgi
- feedbackzb.cgi
- **/^ez(\\w{3,5})\\.cgi/iU**

  この例では、先頭の ez の後に 3 ～ 5 文字の単語、さらに .cgi が続く文字列をパケット ペイロード内で検索します。この検索では大文字と小文字を区別せず、URI データだけを検索します。

この例は以下のものと一致します。

- `EZBoard.cgi`
- `ezman.cgi`
- `ezadmin.cgi`
- `EZAdmin.cgi`

この例は、以下のものとは一致しません。

- `ezez.cgi`
- `fez.cgi`
- `abcezboard.cgi`
- `ezboardman.cgi`
- **`/mail(file|seek)\\.cgi/U`**

この例では、URI データ内の `mail` の後に `file` と `seek` のどちらかが続く文字列をパケット ペイロードで検索します。

この例は以下のものと一致します。

- `mailfile.cgi`
- `mailseek.cgi`

この例は、以下のものとは一致しません。

- `MailFile.cgi`
- `mailfilefile.cgi`
- **`m?http\\\\x3a\\x2f\\x2f.*(\\n|\\t)+?U`**

この例では、任意の数の文字の後ろにある、HTTP 要求内のタブまたは改行文字を示す URI コンテンツをパケット ペイロード内で検索します。この例では、`m?regex?` を使用して、式で `http\\:\\/\\/` を使用しないようにしています。コロンの前にバックスラッシュがあることに注意してください。

この例は以下のものと一致します。

- `http://www.example.com?scriptvar=x&othervar=\\n\\..\\..`
- `http://www.example.com?scriptvar=\\t`

この例は、以下のものとは一致しません。

- `ftp://ftp.example.com?scriptvar=&othervar=\\n\\..\\..`
- `http://www.example.com?scriptvar=|/bin/sh -i|`
- **`m?http\\\\x3a\\x2f\\x2f.*=\\|.*\\|+?sU`**

この例では、(改行を含む)任意の数の文字の後に 1 つの等号、さらに任意の数の文字または空白を含むパイプ文字が続くという構成の URL をパケット ペイロード内で検索します。この例では、`m?regex?` を使用して、式で `http\\:\\/\\/` を使用しないようにしています。

この例は以下のものと一致します。

- `http://www.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?input=|cat /etc/passwd|`

この例は、以下のものとは一致しません。

- `ftp://ftp.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?value=x&input?|cat /etc/passwd|`
- **`/[0-9a-f]{2}\\:[0-9a-f]{2}\\:[0-9a-f]{2}\\:[0-9a-f]{2}\\:[0-9a-f]{2}\\:[0-9a-f]{2}/i`**

この例では、MAC アドレスをパケット ペイロード内で検索します。コロン文字がバックスラッシュでエスケープされていることに注意してください。

ルールにメタデータを追加する

ライセンス：Protection

metadata キーワードを使用すると、記述情報をルールに追加できます。追加した情報を使用して、ニーズに合う方法でルールを整理/識別したり、ルールを検索したりできます。

システムは次の形式に基づいてメタデータを検証します。

```
key value
```

ここで、*key* と *value* は、スペースで区切られた記述の組み合わせです。これは、シスコ 提供のルールにメタデータを追加するために シスコ VRT で使用されている形式です。

または、次の形式を使用することもできます。

```
key=value
```

たとえば、*key value* 形式で次のようにカテゴリとサブカテゴリを使用して、作成者と日付によってルールを識別できます。

```
author SnortGuru_20050406
```

1 つのルール内で複数の metadata キーワードを使用できます。また、以下の例に示すように、単一の metadata キーワード内で複数の *key value* ステートメントをカンマで区切ることもできます。

```
author SnortGuru_20050406, revised_by SnortUser1_20050707,
revised_by SnortUser2_20061003, revised_by
SnortUser1_20070123
```

使用できる形式は *key value* と *key=value* だけに限定されません。ただし、これらの形式に基づく検証に起因する制限事項を知っておく必要があります。

制限されている文字の回避

ライセンス：Protection

次の文字制限に注意してください。

- metadata キーワード内でセミコロン(;)やコロン(:)を使用しないでください。
- カンマを使用する場合には、複数の *key value* または *key=value* ステートメントの区切り文字としてカンマが解釈されることに注意してください。次に例を示します。

  ```
  key value, key value, key value
  ```

- 等号(=)または空白文字を使用する場合には、それらの文字が *key* と *value* の間の区切り文字として解釈されることに注意してください。次に例を示します。

  ```
  key value
  key=value
  ```

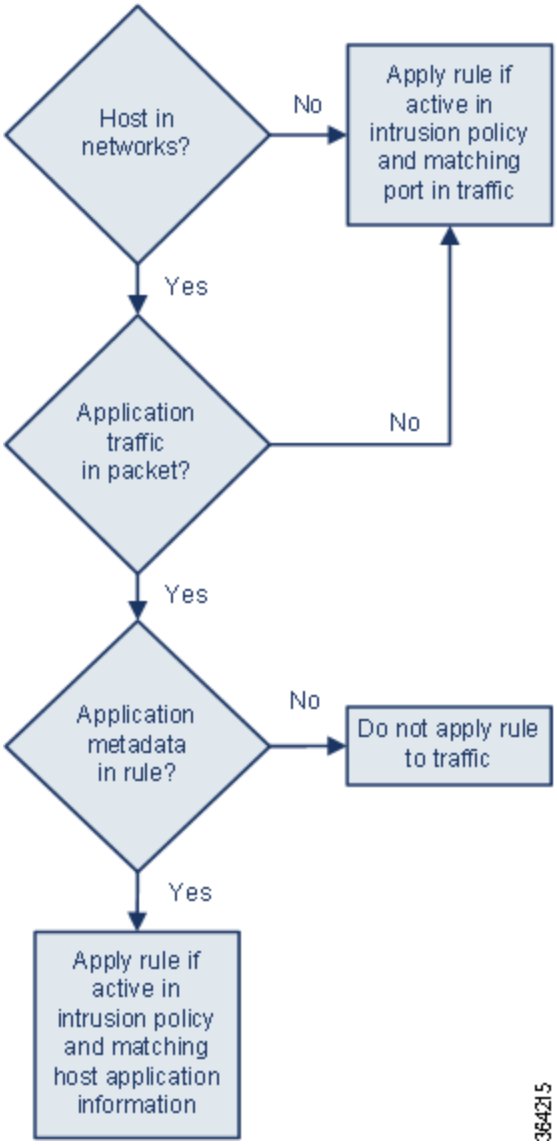
その他のすべての文字が使用可能です。

service メタデータの追加

ライセンス：Protection

ルール エンジンは、トラフィックを分析して処理するために、パケット内のホストに関するアプリケーション プロトコル情報を照合する service メタデータ付きのアクティブ ルールを適用します。これが一致しない場合、システムはルールをトラフィックに適用しません。ホストにアプリケーション プロトコル情報が存在しない場合、またはルールに service メタデータが含まれない場合、システムはルール内のポートに照らしてトラフィック内のポートを検査し、ルールをトラフィックに適用するかどうかを判断します。

次の図は、アプリケーション情報に基づくトラフィックとルールの照合を示しています。



アプリケーション プロトコルの識別によってルールを照合するには、`metadata` キーワードと *`key value`* ステートメントを定義する必要があります。その際、*`key`* として `service`、および *`value`* としてアプリケーションを指定します。たとえば、次に示す `metadata` キーワード内の *`key value`* ステートメントは、ルールを HTTP トラフィックに関連付けます。

```
service http
```

次の表では、最も一般的なアプリケーション値について説明します。

(注)　表に含まれないアプリケーションを定義するために支援が必要な場合は、サポート担当にお問い合わせください。

表 *27-22*　*service* 値

値	説明
dcerpc	分散コンピューティング環境/リモート プロシージャ コール システム
dns	ドメイン ネーム システム
finger	Finger User Information Protocol
FTP	File Transfer Protocol
ftp-data	File Transfer Protocol（データ チャネル）
http	ハイパーテキスト転送プロトコル
imap	Internet Message Access Protocol
isakmp	Internet Security Association and Key Management Protocol
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
netbios-ssn	NETBIOS Session Service
nntp	Network News Transfer Protocol
oracle	Oracle Net Services
pop2	Post Office Protocol バージョン 2
pop3	Post Office Protocol バージョン 3
smtp	Simple Mail Transfer Protocol
ssh	セキュア シェル ネットワーク プロトコル
telnet	Telnet ネットワーク プロトコル
tftp	トリビアル ファイル転送プロトコル
x11	X Window システム

予約済みメタデータの回避

ライセンス：Protection

metadata キーワードでは、次の単語を単一の引数として、または *key value* ステートメント内のキーとして使用しないでください。これらは VRT 用に予約されています。

```
アプリケーション
Engine
impact_flag
os
policy
rule-type
rule-flushing
soid
```

（注）　ローカル ルールを適切に機能させるために制限付きメタデータをどうしても追加する必要がある場合は、サポート担当にお問い合わせください。詳細については、ローカル ルール ファイルのインポート（43-16 ページ）を参照してください。

IP ヘッダー値の検査

ライセンス：Protection

キーワードを使用すると、パケットの IP ヘッダーの中で攻撃やセキュリティ ポリシー違反の可能性を識別できます。詳細については、次の各項を参照してください。

- フラグメント ビットと予約済みビットの検査（27-48 ページ）
- IP ヘッダー識別値の検索（27-49 ページ）
- 指定された IP オプションの識別（27-49 ページ）
- 指定された IP プロトコル番号の識別（27-49 ページ）
- パケットのタイプ オブ サービスの検査（27-50 ページ）
- パケットの存続可能時間値の検査（27-50 ページ）

フラグメント ビットと予約済みビットの検査

ライセンス：Protection

`fragbits` キーワードは、IP ヘッダー内のフラグメント ビットと予約ビットを検査します。パケットごとに、予約ビット、More Fragments ビット、および Don't Fragment ビットを任意に組み合わせて検査できます。

表 ***27-23*** ***Fragbits*** 引数の値

引数	説明
R	予約済みビット
M	More Fragments ビット
D	Don’t Fragment ビット

`fragbits` キーワードを使ってルールを微調整するために、次の表に示す演算子をルール内の引数値の後ろに指定できます。

表 ***27-24*** ***Fragbit*** 演算子

演算子	説明
プラス記号（+）	パケットは、指定されたすべてのビットと一致する必要があります。
アスタリスク（*）	パケットは、指定されたどのビットと一致することもできます。
感嘆符（!）	指定されたどのビットも設定されていない場合、パケットが基準を満たします。

たとえば、（他のビットの有無とは無関係に）少なくとも予約済みビットが設定されたパケットに対してイベントを生成するには、`fragbits` 値として `R+` を使用します。

IP ヘッダー識別値の検索

ライセンス：Protection

id キーワードは、キーワード引数で指定される値に照らして IP ヘッダー フラグメント識別フィールドを検査します。一部のサービス拒否ツールやスキャナは、このフィールドを、容易に検出できる特定の番号に設定します。たとえば、Synscan ポートスキャンを検出する SID 630 では、id 値が 39426（スキャナから伝送されるパケットの ID 番号として使われる静的な値）に設定されます。

（注）　id 引数値は数値でなければなりません。

指定された IP オプションの識別

ライセンス：Protection

IPopts キーワードを使用すると、指定された IP ヘッダー オプションをパケット内で検索できます。次の表に、使用可能な引数値を示します。

表 *27-25*　*IPoption* 引数

引数	説明
rr	経路を記録
eol	リストの末尾
nop	オペレーションなし
ts	タイム スタンプ
sec	IP セキュリティ オプション
lsrr	厳密でない送信元ルーティング
ssrr	厳密な送信元ルーティング
satid	ストリーム識別子

アナリストが最も頻繁に監視するのは、厳密な送信元ルーティングと厳密でない送信元ルーティングです。これらのオプションは送信元 IP アドレスのスプーフィングを示している可能性があるためです。

指定された IP プロトコル番号の識別

ライセンス：Protection

ip_proto キーワードを使用すると、キーワードの値として指定された IP プロトコルを含むパケットを識別できます。IP プロトコルは 0 ～ 255 の数値として指定できます。プロトコル番号の完全なリストについては、http://www.iana.org/assignments/protocol-numbers を参照してください。これらの番号を、<、>、または ! 演算子と組み合わせることができます。たとえば、ICMP 以外のプロトコルを使用しているトラフィックを検査するには、!1 を ip_proto キーワードの値として使用します。1 つのルール内で ip_proto キーワードを複数回にわたって使用できます。ただし、ルール エンジンはキーワードの複数インスタンスをブール和関係（AND）と解釈することに注意してください。たとえば、ip_proto:!3; ip_proto:!6 を含むルールを作成した場合、このルールは GGP プロトコルおよび TCP プロトコルを使用するトラフィックを無視します。

パケットのタイプ オブ サービスの検査

ライセンス：Protection

一部のネットワークでは、ネットワーク上を移動するパケットの優先度を設定するタイプ オブ サービス（ToS）値が使用されます。`tos` キーワードを使用すると、キーワードの引数で指定された値に照らしてパケットの IP ヘッダー ToS 値を検査できます。`tos` キーワードを使用するルールは、ToS が指定の値に設定され、しかもルール内の残りの基準を満たすパケットに対してトリガーとして使用されます。

（注）　`tos` の引数値は数値でなければなりません。

[ToS] フィールドは IP ヘッダー プロトコルでは非推奨になり、[Differentiated Services Code Point (DSCP)] フィールドに置き換えられています。

パケットの存続可能時間値の検査

ライセンス：Protection

パケットの存続可能時間（time-to-live、ttl）値は、パケットが破棄される前に生成できるホップ数を示します。`ttl` キーワードを使用すると、キーワードの引数として指定された値または値の範囲に照らしてパケットの IP ヘッダー ttl 値を検査できます。`ttl` キーワード パラメータを 0 や 1 などの低い値に設定すると役立つことがあります。これは、低い存続可能時間値がトレースルートや侵入回避の試みを示している場合があるためです（なお、このキーワードの適切な値はデバイスの配置やネットワーク トポロジによって異なります）。次の構文を使用します。

- TTL 値に特定の 1 つの値を設定するには、0 ～ 255 の整数を使用します。値の前に等号（=）を付けることもできます（たとえば `5` または `=5` を指定できます）。
- TTL 値の範囲を指定するには、ハイフン（-）を使用します（たとえば、`0-2` は 0 ～ 2 のすべての値、`-5` は 0 ～ 5 のすべての値、`5-` は 5 ～ 255 のすべての値をそれぞれ指定します）。
- 特定の値より大きい TTL 値を指定するには、「大なり」記号（>）を使用します（たとえば、`>3` は 3 より大きいすべての値を指定します）。
- 特定の値以上の TTL 値を指定するには、「大なりイコール」記号（>=）を使用します（たとえば、`>=3` は 3 以上のすべての値を指定します）。
- 特定の値より小さい TTL 値を指定するには、「小なり」記号（<）を使用します（たとえば、`<3` は 3 より小さいすべての値を指定します）。
- 特定の値以下の TTL 値を指定するには、「小なりイコール」記号（<=）を使用します（たとえば、`<=3` は 3 以下のすべての値を指定します）。

ICMP ヘッダー値の検査

ライセンス：Protection

ASA FirePOWER モジュールでサポートされるキーワードを使用すると、ICMP パケット ヘッダー内の攻撃やセキュリティ ポリシー違反を識別できます。なお、ほとんどの ICMP タイプおよびコードを検出する事前定義ルールがあることに注意してください。既存のルールを有効にするか、既存のルールに基づいてローカル ルールを作成することを考慮してください。ICMP ルールを最初から作成するよりも、ニーズを満たすルールを見つける方が時間の節約になる可能性があります。

ICMP 固有のキーワードの詳細については、以下の項を参照してください。

- 静的な ICMP ID 値とシーケンス値の識別（27-51 ページ）
- ICMP メッセージ タイプの検査（27-51 ページ）
- ICMP メッセージ コードの検査（27-52 ページ）

静的な ICMP ID 値とシーケンス値の識別

ライセンス：Protection

ICMP の識別番号とシーケンス番号は、ICMP 応答と ICMP 要求を関連付けるうえで役立ちます。通常のトラフィックでは、これらの値はパケットに動的に割り当てられます。一部のコバート チャネルおよび Distributed Denial of Server（DDoS）プログラムは、静的な ICMP ID およびシーケンス値を使用します。次のキーワードを使用すると、静的な値を含む ICMP パケットを識別できます。

icmp_id

`icmp_id` キーワードは、ICMP エコー要求または応答パケットの ICMP ID 番号を検査します。ICMP ID 番号に対応する数値を `icmp_id` キーワードの引数として使用します。

icmp_seq

`icmp_seq` キーワードは、ICMP エコー要求または応答パケットの ICMP シーケンスを検査します。ICMP シーケンス番号に対応する数値を `icmp_seq` キーワードの引数として使用します。

ICMP メッセージ タイプの検査

ライセンス：Protection

`itype` キーワードを使用して、特定の ICMP メッセージ タイプ値を含むパケットを検索します。有効な ICMP タイプ値または無効な ICMP タイプ値を指定して、さまざまなタイプのトラフィックを検査できます（ICMP タイプ番号の完全なリストについては http://www.iana.org/assignments/icmp-parameters [英語]または http://www.faqs.org/rfcs/rfc792.html [英語]を参照してください）。たとえば、サービス拒否攻撃やフラッディング攻撃を発生させるために攻撃者が範囲外の ICMP タイプ値を設定することがあります。

「小なり」（<）と「大なり」（>）を使用して `itype` 引数値の範囲を指定できます。

次に例を示します。

- <35
- >36
- 3<>55

ヒント　ICMP タイプ番号の完全なリストについては、http://www.iana.org/assignments/icmp-parameters [英語] または http://www.faqs.org/rfcs/rfc792.html [英語] を参照してください。

ICMP メッセージ コードの検査

ライセンス：Protection

ICMP メッセージには、宛先が到達不能である場合の詳細を示すコード値が含まれることがあります。（ICMP メッセージ コードの完全なリストと、それぞれに関連するメッセージ タイプについては、http://www.iana.org/assignments/icmp-parameters [英語] の第 2 項を参照してください）。

`icode` キーワードを使用すると、特定の ICMP コード値を含むパケットを識別できます。有効な ICMP コード値と無効な ICMP コード値のいずれかを指定することにより、さまざまなタイプのトラフィックを検査できます。

「小なり」（<）と「大なり」（>）を使用して `icode` 引数値の範囲を指定できます。

次に例を示します。

- 35 より小さい値を検索するには `<35` と指定します。
- 36 より大きい値を検索するには `>36` と指定します。
- 3 ～ 55 の間にある値を検索するには、`3<>55` と指定します。

ヒント　`icode` キーワードと `itype` キーワードを一緒に使用すると、両方に一致するトラフィックを識別できます。たとえば、ICMP 宛先到達不能コード タイプと ICMP ポート到達不能コード タイプを含む ICMP トラフィックを特定するには、値 3 の `itype` キーワード（宛先到達不能）と、値 3 の `icode` キーワード（ポート到達不能）を指定します。

TCP ヘッダー値とストリーム サイズの検査

ライセンス：Protection

ASA FirePOWER モジュールでは、パケットの TCP ヘッダーと TCP ストリーム サイズを使って試行される攻撃を識別するためのキーワードを使用できます。TCP 固有のキーワードの詳細については、以下の項を参照してください。

- TCP 確認応答値の検査（27-52 ページ）
- TCP フラグ組み合わせの検査（27-53 ページ）
- TCP または UDP クライアントまたはサーバ フローへのルールの適用（27-54 ページ）
- 静的な TCP シーケンス番号の識別（27-55 ページ）
- 特定のサイズの TCP ウィンドウの識別（27-55 ページ）
- 特定のサイズの TCP ストリームの識別（27-55 ページ）

TCP 確認応答値の検査

ライセンス：Protection

`ack` キーワードを使用すると、パケットの TCP 確認応答番号と特定の値を比較できます。パケットの TCP 確認応答番号が、`ack` キーワードに指定された値と一致した場合に、ルールがトリガーとして使用されます。

`ack` の引数値は数値でなければなりません。

TCP フラグ組み合わせの検査

ライセンス：Protection

flags キーワードを使用すると、複数の TCP フラグを任意に組み合わせて指定できます。検査対象のパケットでこれらが設定されている場合、ルールがトリガーとして使用されます。

（注）　従来、flags の値として A+ を使用していたケースでは、代わりに値 established を含む flow キーワード使用してください。一般に、フラグのすべての組み合わせが検出されるようにするには、フラグの使用時に値 stateless を含む flow キーワードを使用する必要があります。flow キーワードの詳細については、TCP または UDP クライアントまたはサーバ フローへのルールの適用（27-54 ページ）を参照してください。

次の表に示す flags キーワードの値を確認または無視することができます。

表 27-26　*flag* の引数

引数	TCP フラグ
ACK	データを確認応答します。
Psh	このパケットでデータが送信される必要があります。
Syn	新しい接続。
Urg	パケットに緊急データが含まれています。
Fin	接続が閉じられました。
Rst	接続が異常終了しました。
CWR	ECN 輻輳ウィンドウが減少しました。旧 R1 引数（下位互換性を維持するために引き続きサポートされています）。
ECE	ECN エコー。旧 R2 引数（下位互換性を維持するために引き続きサポートされています）。

ヒント　明示的輻輳通知（ECN）の詳細については、http://www.faqs.org/rfcs/rfc3168.html で情報を参照してください。

flags キーワードを使用する場合、複数のフラグに対する照合方法をシステムに指示するための演算子を使用できます。次の表に、これらの演算子の説明を示します。

表 27-27　*flags* と一緒に使用する演算子

演算子	説明	例
すべて	パケットは、指定されたすべてのフラグを含んでいる必要があります。	Urg と all を選択すると、パケットが緊急フラグを含んでいる必要があること、および他のフラグが含まれる可能性があることを指定できます。
任意	パケットは、指定された任意のフラグを含むことができます。	Ack、Psh、および any を選択すると、ルールをトリガーとして使用するためには Ack と Psh のどちらか（または両方）のフラグが設定される必要があること、およびパケット内で他のフラグも設定されている可能性があることを指定できます。
ノット	パケットは、指定されたフラグセットを含んではなりません。	Urg と not を選択すると、このルールをトリガーとして使用するパケットに関して緊急フラグが設定されないことを指定できます。

TCP または UDP クライアントまたはサーバ フローへのルールの適用

ライセンス：Protection

flow キーワードを使用すると、セッション特性に基づいてルールで検査されるパケットを選択できます。flow キーワードを使用することで、ルールの適用対象となるトラフィック フロー方向を指定して、クライアント フローとサーバ フローのどちらかにルールを適用できます。flow キーワードによるパケット検査の方法を指定するには、分析すべきトラフィックの方向、検査するパケットの状態、およびパケットが再構築ストリームの一部かどうかを設定できます。

ルールの処理時に、パケットのステートフル インスペクションが実行されます。ステートレス トラフィック（セッション コンテキストが確立されていないトラフィック）を TCP ルールで無視するには、flow キーワードをルールに追加して、そのキーワードに **Established** 引数を選択する必要があります。UDP ルールでステートレス トラフィックを無視するには、flow キーワードをルールに追加して、**Established** 引数と方向引数のどちらか（または両方）を選択する必要があります。これにより、TCP または UDP ルールでパケットのステートフル インスペクションが実行されます。

方向引数を追加した場合、ルール エンジンは、指定された方向と一致するフローを伴う確立された状態のパケットだけを検査します。たとえば、TCP または UDP 接続が検出されたときトリガーとして使用されるルールに、flow キーワードおよび established 引数と From Client 引数を追加した場合、ルール エンジンはクライアントから送信されたパケットだけを検査します。

ヒント　パフォーマンスを最大にするには、必ず TCP ルールまたは UDP セッション ルールに flow キーワードを含めてください。

フローを指定するには、[ルールの作成（Create Rule）] ページの [検出オプション（Detection Options）] リストで [flow] キーワードを選択し、[オプションを追加（Add Option）] をクリックします。次に、フィールドごとに表示されるリストから引数を選択します。

次の表に、flow キーワードで指定できるストリーム関連引数の説明を示します。

表 ***27-28***　状態に関連する ***flow*** 引数

引数	説明
Established	確立された接続でトリガーとして使用されます。
Stateless	ストリーム プロセッサの状態に関係なくトリガーとして使用されます。

次の表に、flow キーワードで指定できる方向オプションの説明を示します。

表 ***27-29***　***flow*** の方向引数

引数	説明
To Client	サーバ応答でトリガーとして使用されます。
To Server	クライアント応答でトリガーとして使用されます。
From Client	クライアント応答でトリガーとして使用されます。
From Server	サーバ応答でトリガーとして使用されます。

From Server と To Client の機能が同じであること、および To Server と From Client の機能も同じであることに注意してください。これらのオプションは、ルールに文脈と読みやすさを加味するために提供されています。たとえば、サーバからクライアントへの攻撃を検出するよう設計されたルールを作成する場合は、From Server を使用します。一方、クライアントからサーバへの攻撃を検出するように設計されたルールを作成する場合は、From Client を使用します。

次の表に、flow キーワードで指定できるストリーム関連引数の説明を示します。

表 27-30　*flow* のストリーム関連引数

引数	説明
Ignore Stream Traffic	再構築されたストリーム パケットでトリガーとして使用されません。
Only Stream Traffic	再構築されたストリーム パケットでのみトリガーとして使用されます。

たとえば、flow キーワードの値として To Server, Established, Only Stream Traffic を使用すると、ストリーム プリプロセッサで再構築された、確立済みセッションでクライアントからサーバに移動するトラフィックを検出できます。

静的な TCP シーケンス番号の識別

ライセンス：Protection

seq キーワードを使用すると、静的なシーケンス番号値を指定できます。パケットのシーケンス番号が、指定された引数と一致する場合、そのキーワードを含むルールがトリガーとして使用されます。このキーワードはあまり使用されませんが、静的シーケンス番号付きの生成済みパケットを使用する攻撃やネットワーク スキャンを識別するうえでこれが役立ちます。

特定のサイズの TCP ウィンドウの識別

ライセンス：Protection

window キーワードを使用すると、特定の TCP ウィンドウ サイズを指定できます。このキーワードを含むルールは、指定された TCP ウィンドウ サイズのパケットが検出されるたびにトリガーとして使用されます。このキーワードはあまり使用されませんが、静的 TCP ウィンドウ サイズ付きの生成済みパケットを使用する攻撃やネットワーク スキャンを識別するうえでこれが役立ちます。

特定のサイズの TCP ストリームの識別

ライセンス：Protection

次に示す形式で、stream_size キーワードとストリーム プリプロセッサを組み合わせて使用すると、TCP ストリームのサイズをバイト単位で特定できます。

direction,*operator*,*bytes*

ここで、*bytes* はバイト数です。引数内の各オプションをカンマ(,)で区切る必要があります。

次の表に、stream_size キーワードで指定できる大文字/小文字を区別しない方向オプションについて説明します。

表 27-31　*stream_size* キーワードの方向引数

引数	説明
client	指定されたストリーム サイズに一致するクライアントからのストリームでトリガーとして使用されます。
server	指定されたストリーム サイズに一致するサーバからのストリームでトリガーとして使用されます。

表 27-31　*stream_size* キーワードの方向引数（続き）

引数	説明
both	指定されたストリーム サイズに一致するクライアントからのトラフィックとサーバからのトラフィックの両方によってトリガーとして使用されます。 たとえば `both, >, 200` という引数は、クライアントからのトラフィックが 200 バイトを超え、しかもサーバからのトラフィックが 200 バイトを超えている場合にトリガーとして使用されます。
either	指定されたストリーム サイズに一致するクライアントまたはサーバからのトラフィック（どちらか先に出現した方）によってトリガーとして使用されます。 たとえば `either, >, 200` という引数は、クライアントからのトラフィックが 200 バイトを超えるか、またはサーバからのトラフィックが 200 バイトを超えている場合にトリガーとして使用されます。

次の表に、`stream_size` キーワードで使用できる演算子の説明を示します。

表 27-32　*stream_size* キーワードの引数演算子

演算子	説明
=	次の値と等しい
!=	等しくない
>	より大きい
<	より少ない
>=	右辺と比較して大きいか等しい
<=	右辺と比較して小さいか等しい

たとえば、クライアントからサーバに移動する 5001216 バイト以上の TCP ストリームを検出するには、`stream_size` キーワードの引数として `client, >=, 5001216` を使用できます。

TCP ストリーム再構築の有効化と無効化

ライセンス：Protection

`stream_reassemble` キーワードを使用すると、接続での検査対象トラフィックがルールの条件と一致した場合に、1 つの接続の TCP ストリーム再構築を有効/無効にすることができます。オプションで、このキーワードを 1 つのルール内で複数回使用することができます。

ストリーム再構築を有効または無効にするには、次の構文を使用します。

```
enable|disable, server|client|both, option, option
```

次の表に、`stream_reassemble` キーワードで使用できるオプション引数の説明を示します。

表 27-33　*stream_reassemble* のオプション引数

引数	説明
noalert	ルールで他にどの検出オプションが指定されているかに関係なく、イベントを生成しません。
fastpath	一致の検出時に残りの接続トラフィックを無視します。

たとえば、次のルールは、HTTP 応答で 200 OK ステータス コードが検出される接続に対してイベントを生成せずに、TCP クライアント側ストリーム再構築を無効にします。

```
alert tcp any 80 -> any any (flow:to_client, established; content: "200 OK";
stream_reassemble:disable, client, noalert
```

stream_reassemble を使用するには、次の手順を実行します。

ステップ **1**　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [stream_reassemble] を選択して、[オプションを追加（Add Option）] をクリックします。

[stream_reassemble] セクションが表示されます。

セッションからの **SSL** 情報の抽出

ライセンス：Protection

SSL ルール キーワードを使用すると、Secure Sockets Layer（SSL）プリプロセッサを呼び出し、暗号化セッションのパケットから SSL のバージョンとセッション状態に関する情報を抽出できます。

SSL または Transport Layer Security（TLS）を使用する暗号化セッションを確立するためにクライアントとサーバが通信するとき、ハンドシェイク メッセージが交換されます。セッション中に伝送されるデータは暗号化されますが、ハンドシェイク メッセージは暗号化されません。

SSL プリプロセッサは、特定のハンドシェイク フィールドから状態とバージョンの情報を抽出します。ハンドシェイク内の 2 つのフィールドは、セッション暗号化に使われる SSL または TLS のバージョンとハンドシェイクのステージを示します。

詳細については、次の項を参照してください。

- ssl_state（27-57 ページ）
- ssl_version（27-58 ページ）

ssl_state

ライセンス：Protection

`ssl_state` キーワードを使用すると、暗号化されたセッションの状態情報と照合することができます。同時に使用される複数の SSL バージョンを検査するには、1 つのルール内で複数の `ssl_version` キーワードを使用します。

ルールで `ssl_state` キーワードが使用されている場合、ルール エンジンは SSL プリプロセッサを呼び出して、トラフィック内の SSL 状態情報を検査します。

たとえば、チャレンジ長が非常に長く、データが多すぎる `ClientHello` メッセージを送信することによってサーバ上のバッファ オーバーフローを引き起こそうとする攻撃者の試みを検出するには、`ssl_state` キーワードと引数 `client_hello` を使用し、異常に大きなパケットを検査することができます。

SSL 状態に関する複数の引数を指定するには、カンマ区切りのリストを使用します。複数の引数を列挙した場合、システムは OR 演算子を使ってそれらを評価します。たとえば、引数として `client_hello` および `server_hello` を指定すると、システムは `client_hello` または `server_hello` のどちらかを含むトラフィックに照らしてルールを評価します。

次のように、引数を否定することもできます。

```
!client_hello, !unknown
```

接続が一連の状態のそれぞれに到達したことを確認するには、ssl_state ルール オプションを使用する複数のルールを使う必要があります。ssl_state キーワードは、次の識別子を引数として受け入れます。

表 **27-34**　ssl_state の引数

引数	目的
client_hello	クライアントが暗号化セッションを要求する、メッセージ タイプ ClientHello のハンドシェイク メッセージを照合します。
server_hello	クライアントからの暗号化セッション要求に対してサーバが応答する、メッセージ タイプ ServerHello のハンドシェイク メッセージを照合します。
client_keyx	サーバからのキーの受信を確認するためにクライアントがサーバにキーを伝送する、メッセージ タイプ ClientKeyExchange のハンドシェイク メッセージを照合します。
server_keyx	サーバからのキーの受信を確認するためにクライアントがサーバにキーを伝送する、メッセージ タイプ ServerKeyExchange のハンドシェイク メッセージを照合します。
unknown	任意のハンドシェイク メッセージ タイプを照合します。

ssl_version

ライセンス：Protection

ssl_version キーワードを使用すると、暗号化セッションのバージョン情報を照合できます。ルールで ssl_version キーワードが使用されている場合、ルール エンジンは SSL プリプロセッサを呼び出して、トラフィック内の SSL バージョン情報を検査します。

たとえば、SSL バージョン 2 にバッファ オーバーフロー脆弱性があることがわかっている場合、ssl_version キーワードで sslv2 引数を使用して、その SSL バージョンを使用するトラフィックを識別できます。

SSL バージョンに関する複数の引数を指定するには、カンマ区切りのリストを使用します。複数の引数を列挙した場合、システムは OR 演算子を使ってそれらを評価します。たとえば、SSLv2 を使用していない暗号化トラフィックを識別するには、ssl_version:ssl_v3,tls1.0,tls1.1,tls1.2 をルールに追加できます。このルールは、SSL バージョン 3、TLS バージョン 1.0、TLS バージョン 1.1、または TLS バージョン 1.2 を使用するトラフィックを評価します。

ssl_version キーワードは、次の SSL/TLS バージョン識別子を引数として受け入れます。

表 **27-35**　ssl_version の引数

引数	目的
sslv2	Secure Sockets Layer（SSL）バージョン 2 を使用してエンコードされたトラフィックを照合します。
sslv3	Secure Sockets Layer（SSL）バージョン 3 を使用してエンコードされたトラフィックを照合します。
tls1.0	Transport Layer Security（TLS）バージョン 1.0 を使用してエンコードされたトラフィックを照合します。
tls1.1	Transport Layer Security（TLS）バージョン 1.1 を使用してエンコードされたトラフィックを照合します。
tls1.2	Transport Layer Security（TLS）バージョン 1.2 を使用してエンコードされたトラフィックを照合します。

アプリケーション層プロトコル値の検査

ライセンス：Protection

アプリケーション層プロトコル値の正規化と検査はプリプロセッサによってほとんど実行されますが、以下の項で説明するキーワードを使用すると、アプリケーション層値をさらに検査できます。

RPC

ライセンス：Protection

`rpc` キーワードは、TCP または UDP パケット内の Open Network Computing Remote Procedure Call（RPC ONC）サービスを識別します。これにより、ホスト上の RPC プログラムの識別試行を検出することができます。ネットワークで実行中のいずれかの RPC サービスを悪用できるかどうか判断するために、侵入者は RPC ポートマッパーを使用できます。また、ポートマッパーを使用せずに RPC を実行中の他のポートへのアクセスを試みることもできます。次の表に、`rpc` キーワードで使用できる引数を列挙します。

表 ***27-36***　　***rpc*** キーワードの引数

引数	説明
アプリケーション	RPC アプリケーション番号
手順	呼び出される RPC プロシージャ
version	RPC バージョン

`rpc` キーワードの引数を指定するには、次の構文を使用します。

`application,procedure,version`

ここで、*`application`* は RPC アプリケーション番号、*`procedure`* は RPC プロシージャ番号、*`version`* は RPC バージョン番号です。`rpc` キーワードのすべての引数を指定する必要があります。引数のいずれかを指定できない場合は、アスタリスク（`*`）で置き換えてください。

たとえば、任意のプロシージャまたはバージョンの RPC ポートマッパー（100000 という番号で示される RPC アプリケーション）を検索するには、引数として `100000,*,*` を使用します。

ASN.1

ライセンス：Protection

asn1 キーワードを使用すると、さまざまな有害エンコードを検索しながら、パケットまたはパケットの一部分をデコードできます。

次の表に、asn1 キーワードの引数について説明します。

表 *27-37*　*asn.1* キーワードの引数

引数	説明
Bitstring Overflow	無効な、リモートで悪用可能なビットストリング エンコードを検出します。
Double Overflow	標準バッファより大きい二重 ASCII エンコードを検出します。これは、Microsoft Windows での悪用可能な機能として知られていますが、現時点でどのサービスが悪用可能かは不明です。
Oversize Length	指定された引数より大きい ASN.1 タイプ長を検出します。たとえば Oversize Length を 500 に設定した場合、500 を上回る ASN.1 タイプによってルールがトリガーとして使用されます。
Absolute Offset	パケット ペイロードの先頭からの絶対オフセットを設定します（offset カウンタがバイト 0 から始まることに注意してください）。たとえば SNMP パケットをデコードするには、Absolute Offset を 0 に設定し、Relative Offset を設定しません。Absolute Offset として正または負の値が可能です。
Relative Offset	これは、最後に見つかったコンテンツ一致、pcre、または byte_jump からの相対オフセットです。コンテンツ "foo" の直後の ASN.1 シーケンスをデコードするには、Relative Offset を 0 に設定し、Absolute Offset を設定しません。Relative Offset として正または負の値が可能です。（オフセット カウンタが 0 から始まることに注意してください。）

たとえば、Microsoft ASN.1 ライブラリにおける既知の脆弱性ではバッファ オーバーフローが発生し、攻撃者は特別に細工した認証パケットを使ってその状態を悪用できます。システムが asn.1 データをデコードするとき、パケット内のエクスプロイト コードは、システム レベル特権付きでホスト上で動作したり、DoS 状態を引き起したりすることができます。次のルールは、asn1 キーワードを使用して、この脆弱性を悪用する試みを検出します。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445
(flow:to_server, established; content:"|FF|SMB|73|"; nocase;
offset:4; depth:5;
asn1:bitstring_overflow,double_overflow,oversize_length
100,relative_offset 54;)
```

上記のルールの場合、任意のポートおよび $EXTERNAL_NET 変数で定義された任意の IP アドレスから発信され、ポート 445 を使用する $HOME_NET 変数で定義された任意の IP アドレスに向かう TCP トラフィックに対して、イベントが生成されます。加えて、サーバへの TCP 接続が確立された時点でのみルールを実行します。その後、ルールは特定の位置にある特定のコンテンツを検査します。最後に、ルールは asn1 キーワードを使用して、ビットストリング エンコードと二重 ASCII エンコードを検出し、最後に見つかったコンテンツ一致の末尾から 55 バイト目以降、長さ 100 バイトを超える asn.1 タイプ長を識別します（offset カウンタがバイト 0 から始まることに注意してください。）

urilen

ライセンス：Protection

urilen キーワードと HTTP Inspect プリプロセッサを組み合わせて使用すると、特定の長さ、最大長を下回る、最小長を上回る、または指定された範囲内の URI を HTTP トラフィック内で検査できます。

HTTP Inspect プリプロセッサがパケットを正規化して検査した後、ルール エンジンはルールに照らしてそのパケットを評価し、urilen キーワードで指定された長さ条件に URI が一致するかどうか判断します。このキーワードを使用すると、URI 長の脆弱性を悪用しようとする試みを検出できます。たとえばバッファ オーバーフローを発生させて、攻撃者が DoS 状態を引き起こしたり、システム レベル特権付きでホスト上でコードを実行したりしようと試みる可能性があります。

ルール内で urilen キーワードを使用するときには、次の点に注意してください。

- 必ず flow:established キーワードおよび他の 1 つ以上のキーワードを組み合わせて、urilen キーワードを使用してください。
- ルール プロトコルは常に TCP です。詳細については、プロトコルの指定（27-4 ページ）を参照してください。
- ターゲット ポートは常に HTTP ポートです。詳細については、「侵入ルールでのポートの定義（27-9 ページ）」と「定義済みのデフォルトの変数の最適化（2-16 ページ）」を参照してください。

URI 長を指定するときには、10 進のバイト数、「小なり」（<）、および「大なり」（>）を使用します。

次に例を示します。

- 5 バイト長の URI を検出するには、5 を指定します。
- 5 バイト長を下回る URI を検出するには、< 5 （1 つの空白文字で区切る）を指定します。
- 5 バイト長を上回る URI を検出するには、> 5 （1 つの空白文字で区切る）を指定します。
- 3 ～ 5 バイト長の URI を検出するには、3 <> 5 （<> の前後に空白文字を 1 つずつ含む）を指定します。

たとえば、eDirectory バージョン 8.8 に同梱されている Novell のサーバ モニタリングおよび診断ユーティリティ iMonitor バージョン 2.4 に既知の脆弱性があるとします。長すぎる URI を含むパケットはバッファ オーバーフローを発生させるため、攻撃者はシステム レベル特権付きでホスト上で動作したり、DoS 状態を引き起こしたりできる特別に細工したパケットを使ってその状態を悪用できます。次のルールは、urilen キーワードを使用して、この脆弱性を悪用する試みを検出します。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"EXPLOIT eDirectory 8.8 Long URI iMonitor buffer
overflow attempt";flow:to_server,established;
urilen:> 8192; uricontent:"/nds/"; nocase;
classtype:attempted-admin; sid:x; rev:1;)
```

上記のルールの場合、任意のポートおよび $EXTERNAL_NET 変数で定義された任意の IP アドレスから発信され、$HTTP_PORTS 変数で定義されたポートを使用して、$HOME_NET 変数で定義された任意の IP アドレスに向かう TCP トラフィックに対して、イベントが生成されます。加えて、サーバへの TCP 接続が確立された時点でのみ、パケットがルールに照らして評価されます。ルールは、urilen キーワードを使用して、長さ 8192 バイトを超える URI を検出します。最後に、ルールは、大文字/小文字を区別しない特定のコンテンツ /nds/ を URI で検索します。

DCE/RPC キーワード

ライセンス：Protection

次の表に示す 3 つの DCE/RPC キーワードを使用すると、DCE/RPC セッション トラフィックでエクスプロイトを監視できます。これらのキーワードを含むルールを処理するとき、システムは DCE/RPC プリプロセッサを呼び出します。詳細については、DCE/RPC トラフィックのデコード（19-2 ページ）を参照してください。

表 ***27-38*** ***DCE/RPC*** キーワード

使用するフィルタ	使用方法	検出対象
dce_iface	単独	特定の DCE/RPC サービスを識別するパケット
dce_opnum	dce_iface の後ろ	特定の DCE/RPC サービス オペレーションを識別するパケット
dce_stub_data	dce_iface + dce_opnum の後ろ	特定の処理要求または応答を定義するスタブ データ

表に示されているように、dce_opnum の前に必ず dce_iface を配置し、dce_stub_data の前に必ず dce_iface + dce_opnum を配置する必要があることに注意してください。

また、これらの DCE/RPC キーワードを他のルール キーワードと組み合わせて使用することもできます。DCE/RPC ルールでは、**DCE/RPC** 引数が選択された状態で byte_jump、byte_test、byte_extract の各キーワードを使用することに注意してください。詳細については、Byte_Jump と Byte_Test の使用（27-33 ページ）およびパケット データをキーワード引数の中に読み込む（27-85 ページ）を参照してください。

シスコ では、DCE/RPC キーワードを含むルールに 1 つ以上の content キーワードを含めることを推奨しています。こうすると、ルール エンジンが常に高速パターン マッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルールに 1 つ以上の content キーワードが含まれている場合は、content キーワードの 高速パターン マッチ機能を使用（**Use Fast Pattern Matcher**）引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。詳細については、「コンテンツ一致の検索（27-15 ページ）」と「高速パターン マッチ機能を使用（Use Fast Pattern Matcher）（27-28 ページ）」を参照してください。

次のケースでは、DCE/RPC バージョンおよび隣接ヘッダー情報を一致コンテンツとして使用できます。

- ルールに他の content キーワードが含まれていない
- ルールにもう 1 つ content キーワードが含まれているが、DCE/RPC バージョンおよび隣接情報が、他方の content よりも特有のパターンを表している

  たとえば、DCE/RPC バージョンおよび隣接情報は通常、1 バイトのコンテンツよりも特有です。

次に示すバージョンおよび隣接情報コンテンツ一致のいずれか 1 つを使用して、ルール限定を終了する必要があります。

- コネクション型 DCE/RPC ルールでは、コンテンツ |05 00 00|（メジャー バージョン 05、マイナー バージョン 00、および要求 PDU（プロトコル データ ユニット）タイプ 00）を使用します。
- コネクションレス型 DCE/RPC ルールでは、コンテンツ |04 00|（バージョン 04、要求 PDU タイプ 00）を使用します。

いずれの場合も、DCE/RPC プリプロセッサで完了済みの処理を繰り返すことなく高速パターン マッチ機能を呼び出すために、ルール内の最後のキーワードとしてバージョンおよび隣接情報の content キーワードを配置してください。ルールの末尾に配置される content キーワードは、高速パターン マッチ機能を呼び出す手段として使われるバージョン コンテンツに当てはまりますが、ルール内の他のコンテンツ一致には必ずしも当てはまらないことに注意してください。

詳細については、次の各項を参照してください。

- dce_iface（27-63 ページ）
- dce_opnum（27-64 ページ）
- dce_stub_data（27-65 ページ）

dce_iface

ライセンス：Protection

dce_iface キーワードを使用すると、特定の DCE/RPC サービスを識別できます。

オプションで、dce_iface キーワードを dce_opnum キーワードおよび dce_stub_data キーワードと組み合わせて使用すると、検査する DCE/RPC トラフィックをさらに限定することができます。詳細については、「dce_opnum（27-64 ページ）」と「dce_stub_data（27-65 ページ）」を参照してください。

固定型 16 バイト Universally Unique Identifier（UUID）は、それぞれの DCE/RPC サービスに割り当てられるアプリケーション インターフェイスを識別します。たとえば、UUID 4b324fc8-670-01d3-1278-5a47bf6ee188 は、srvsvc サービスとしても知られる DCE/RPC lanmanserver サービスを識別します。このサービスは、ピアツーピア プリンタ、ファイル、および SMB 名前付きパイプを共有するためのさまざまな管理機能を提供します。DCE/RPC プリプロセッサは UUID および関連するヘッダー値を使用して DCE/RPC セッションを追跡します。

インターフェイス UUID は、次のように、ハイフンで区切られた 5 つの 16 進文字列で構成されます。

```
<4hexbytes>-<2hexbytes>-<2hexbytes>-<2hexbytes>-<6hexbytes>
```

次に示す netlogon インターフェイスの UUID のように、ハイフンを含む UUID 全体を入力することで、インターフェイスを指定します。

```
12345678-1234-abcd-ef00-01234567cffb
```

UUID 内の最初の 3 つの文字列はビッグ エンディアン バイト順で指定される必要があることに注意してください。通常、公開されたインターフェイス リストやプロトコル アナライザには UUID が正しいバイト順で表示されますが、それを入力する前に UUID バイト順を変更しなければならない場合もあります。次に示すメッセンジャー サービス UUID の場合、リトル エンディアン バイト順の最初の 3 つの文字列を含む未加工 ASCII テキストで表示されることがあります。

```
f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc
```

この同じ UUID を dce_iface キーワードに指定するには、次のようにハイフンを挿入し、最初の 3 つの文字列をビッグ エンディアン バイト順で配置できます。

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

1 つの DCE/RPC セッションに複数のインターフェイスへの要求を含めることができますが、1 つのルールには 1 つの dce_iface キーワードだけを含めてください。追加のインターフェイスを検出するには、追加のルールを作成します。

DCE/RPC アプリケーション インターフェイスにはインターフェイス バージョン番号も割り当てられます。オプションで、インターフェイス バージョンを指定できます。その際、バージョンが指定値に等しい、等しくない、指定値より小さい、または大きいことを示す演算子を使用します。

TCP セグメンテーションや IP フラグメンテーションに加えて、コネクション型とコネクションレス型の両方の DCE/RPC をフラグメント化することができます。通常、先頭以外の DCE/RPC フラグメントを指定のインターフェイスに関連付けるのはあまり効率的ではありません。このようにすると、多数の誤検出が発生する可能性があります。ただし、柔軟性を維持するために、オプションで、指定されたインターフェイスに照らしてすべてのフラグメントを評価できます。

次の表に、dce_iface キーワードの引数を要約します。

表 **27-39**　dce_iface の引数

引数	説明
Interface UUID	DCE/RPC トラフィック内で検出対象となる特定のサービスのアプリケーション インターフェイスを識別する、ハイフンを含む UUID。指定されたインターフェイスに関連付けられた任意の要求がインターフェイス UUID に一致します。
Version	オプションで、アプリケーション インターフェイス バージョン番号 0 ～ 65535 と、検出対象のバージョンが指定した値より大きい(>)、小さい(<)、等しい(=)、または等しくない(!)を示す演算子。
All Fragments	オプションで、関連するすべての DCE/RPC フラグメント内のインターフェイスの照合、およびインターフェイス バージョン(指定されている場合)での照合を有効にします。この引数はデフォルトで無効になっています。これは、最初のフラグメントまたはフラグメント化されていないパケット全体が指定のインターフェイスに関連付けられている場合にのみ、キーワードが一致することを意味します。この引数を有効にすると、誤検出が発生する可能性があることに注意してください。

dce_opnum

ライセンス:Protection

dce_opnum キーワードを DCE/RPC プリプロセッサと組み合わせて使用すると、DCE/RPC サービスが提供する 1 つ以上の特定のオペレーションを識別するパケットを検出できます。

クライアント関数呼び出しは、DCE/RPC 仕様で「オペレーション」と呼ばれる特定のサービス関数を要求します。オペレーション番号(opnum)は DCE/RPC ヘッダー内の特定のオペレーションを識別します。エクスプロイトは特定のオペレーションを標的にすることがあります。

たとえば UUID 12345678-1234-abcd-ef00-01234567cffb は、数十種類のオペレーションを提供する netlogon サービスのインターフェイスを識別します。その 1 つがオペレーション 6(NetrServerPasswordSet オペレーション)です。

オペレーション用のサービスを識別するには、dce_opnum キーワードの前に dce_iface キーワードを指定する必要があります。詳細については、dce_iface(27-63 ページ)を参照してください。

特定のオペレーションを示す 1 つの 10 進数値(0 ～ 65535 の範囲)、ハイフンで区切られたオペレーション範囲、またはカンマ区切りのオペレーション/範囲リストを任意の順序で指定できます。

次の例は、すべて有効な netlogon オペレーション番号を表しています。

```
15
15-18
15, 18-20
15, 20-22, 17
15, 18-20, 22, 24-26
```

dce_stub_data

ライセンス：Protection

dce_stub_data キーワードを DCE/RPC プリプロセッサと組み合わせて使用すると、他のルール オプションとは無関係に、スタブ データの先頭からインスペクションを開始するようルール エンジンに指示できます。dce_stub_data キーワードの後に続くパケット ペイロード ルール オプションは、スタブ データ バッファを基準にして適用されます。

DCE/RPC スタブ データは、クライアント プロシージャ コールと DCE/RPC ランタイム システム（DCE/RPC の中核をなすルーチンとサービスを提供するメカニズム）の間のインターフェイスを提供します。DCE/RPC エクスプロイトは、DCE/RPC パケットのスタブ データ部分で識別されます。スタブ データは特定のオペレーションまたは関数呼び出しに関連付けられているため、必ず dce_stub_data の前に dce_iface と dce_opnum を指定して、関連するサービスとオペレーションを識別してください。

dce_stub_data キーワードには引数がありません。詳細については、「dce_iface（27-63 ページ）」と「dce_opnum（27-64 ページ）」を参照してください。

SIP キーワード

ライセンス：Protection

4 つの SIP キーワードを使用すると、SIP セッション トラフィックでエクスプロイトを監視できます。

SIP プロトコルはサービス拒否（DoS）攻撃に対して脆弱であることに注意してください。このような攻撃に対処するルールでは、レート ベース攻撃の防止を活用できます。詳細については、「動的ルール状態の追加（24-31 ページ）」と「レート ベース攻撃の防止（25-10 ページ）」を参照してください。

詳細については、次の各項を参照してください。

- sip_header（27-65 ページ）
- sip_body（27-66 ページ）
- sip_method（27-66 ページ）
- sip_stat_code（27-67 ページ）

sip_header

ライセンス：Protection

sip_header キーワードを使用すると、抽出された SIP 要求または応答ヘッダーの先頭から検査を開始し、検査対象をヘッダー フィールドに限定することができます。

sip_header キーワードには引数がありません。詳細については、「sip_method（27-66 ページ）」と「sip_stat_code（27-67 ページ）」を参照してください。

次の例のルール フラグメントは SIP ヘッダーを指し示し、CSeq ヘッダー フィールドに一致します。

```
alert udp any any -> any 5060 ( sip_header; content:"CSeq"; )
```

sip_body

ライセンス：Protection

sip_body キーワードを使用すると、抽出された SIP 要求または応答メッセージ本文の先頭から検査を開始し、検査対象をメッセージ本文に限定することができます。

sip_body キーワードには引数がありません。

次の例のルール フラグメントは SIP メッセージ本文を指し示し、抽出された SDP データの c（接続情報）フィールド内の特定の IP アドレスに一致します。

```
alert udp any any -> any 5060 ( sip_body; content:"c=IN 192.168.12.14"; )
```

ルールが SDP コンテンツの検索だけに限定されないことに注意してください。SIP プリプロセッサはメッセージ本文全体を抽出し、それをルール エンジンで使用できるようにします。

sip_method

ライセンス：Protection

各 SIP 要求内の *method*（メソッド）フィールドは要求の目的を識別します。sip_method キーワードを使用すると、SIP 要求の中で特定のメソッドを検査することができます。複数のメソッドはカンマで区切ります。

次に示す現在定義されている SIP メソッドを指定できます。

```
ack、benotify、bye、cancel、do、info、invite、join、message、notify、options、prack、publish、quath、
refer、register、service、sprack、subscribe、unsubscribe、update
```

メソッドでは大文字と小文字が区別されません。複数のメソッドをカンマで区切ることができます。

今後、新しい SIP メソッドが定義される可能性があるため、カスタム メソッド、つまり現在定義されている SIP メソッド以外のメソッドを指定することもできます。可能なフィールド値は RFC 2616 で定義されています。=、(、) などの制御文字と区切り文字を除いて、すべての文字を使用できます。除外されている区切り文字の完全なリストについては、RFC 2616 を参照してください。指定されたカスタム メソッドがトラフィックで検出されると、システムはパケット ヘッダーを検査しますが、メッセージは検査されません。

システムでは最大 32 個のメソッド（現在定義されている 21 個のメソッドと追加の 11 個のメソッド）がサポートされます。システムは、設定される未定義のメソッドをすべて無視します。合計 32 個のメソッドには、[Methods to Check] SIP プリプロセッサ オプションを使って指定されるメソッドが含まれることに注意してください。詳細については、SIP プリプロセッサ オプションの選択（19-54 ページ）を参照してください。

否定を使用する場合は、1 つのメソッドだけを指定できます。次に例を示します。

```
!invite
```

ただし、1 つのルール内の複数の sip_method キーワードが **AND** 演算で結合されることに注意してください。たとえば、invite と cancel を除くすべての抽出されたメソッドを検査するには、次のような 2 つの否定付き sip_method キーワードを使用します。

```
sip_method: !invite
sip_method: !cancel
```

シスコ では、sip_method キーワードを含むルールに 1 つ以上の content キーワードを含めることを推奨しています。こうすると、ルール エンジンが常に高速パターン マッチ機能を使用することで処理速度が上がり、パフォーマンスが向上します。ルールに 1 つ以上の content キーワードが含まれている場合は、content キーワードの 高速パターン マッチ機能を使用（**Use Fast Pattern Matcher**）引数が有効になっているかどうかに関係なく、ルール エンジンが高速パターン マッチ機能を使用することに注意してください。詳細については、「コンテンツ一致の検索（27-15 ページ）」と「高速パターン マッチ機能を使用（Use Fast Pattern Matcher）（27-28 ページ）」を参照してください。

sip_stat_code

ライセンス：Protection

各 SIP 応答内の 3 桁のステータス コードは、要求されたアクションの結果を示します。sip_stat_code キーワードを使用すると、SIP 応答の中で特定のステータス コードを検査することができます。

1 桁の応答タイプ番号 1 ～ 9、特定の 3 桁の番号 100 ～ 999、またはこれらを任意に組み合わせたカンマ区切りリストを指定できます。リスト内のいずれか 1 つの番号が SIP 応答内のコードに一致する場合、そのリストが一致します。

次の表に、指定可能な SIP ステータス コード値の説明を示します。

表 *27-40*　sip_stat_code 値

検出対象	指定する内容	例	検出結果
1 つの特定のステータス コード	3 桁のステータス コード	189	189
指定された 1 桁で始まる 3 桁のコード	1 桁	1	1xx、つまり 100、101、102 など
値のリスト	特定のコードおよび 1 桁を任意に組み合わせてカンマで区切る	222, 3	222 および 300、301、302 など

また、ルールに content キーワードが含まれているかどうかに関係なく、sip_stat_code キーワードを使って指定された値を検索するためにルール エンジンが高速パターン マッチ機能を使用しないことにも注意してください。

GTP キーワード

ライセンス：Protection

3 つの GSRP トンネリング プロトコル（GTP）キーワードを使用すると、GTP バージョン、メッセージ タイプ、および情報要素をコマンド チャネル内で検査できます。content や byte_jump などの他の侵入ルール キーワードと組み合わせて GTP キーワードを使用することはできません。gtp_info または gtp_type キーワードを使用するそれぞれのルールで、gtp_version キーワードを使用する必要があります。

詳細については、次の各項を参照してください。

- gtp_version（27-67 ページ）
- gtp_type（27-68 ページ）
- gtp_info（27-72 ページ）

gtp_version

gtp_version キーワードを使用すると、GTP 制御メッセージの中で GTP バージョン 0、1、または 2 を検査することができます。

定義されているメッセージ タイプと情報要素は GTP バージョンによって異なるため、gtp_type または gtp_info キーワードを使用するときには、このキーワードを使用する必要があります。値として 0、1、または 2 を指定できます。

GTP バージョンを指定するには、次の手順を実行します。

ステップ 1　[ルールの作成(Create Rule)] ページで、ドロップダウンリストから [gtp_version] を選択して、**[**オプションを追加(**Add Option**)**]** をクリックします。

`gtp_version` キーワードが表示されます。

ステップ 2　GTP バージョンを特定するために、`0`、`1`、または `2` を指定します。

gtp_type

それぞれの GTP メッセージは、数値と文字列で構成されるメッセージ タイプによって識別されます。`gtp_type` キーワードを `gtp_version` キーワードと組み合わせて使用すると、トラフィック内で特定の GTP メッセージ タイプを検査できます。

次の例に示すように、メッセージ タイプとして定義済みの 10 進数値、定義済み文字列、あるいはどちらか(または両方)を任意に組み合わたカンマ区切りリストを指定できます。

```
10, 11, echo_request
```

リスト内のそれぞれの値または文字列を照合するとき、システムは OR 演算を使用します。値と文字列を列挙する順序は重要ではありません。リスト内のいずれか 1 つの値または文字列の一致により、キーワードが一致します。認識されない文字列または範囲外の値を含むルールを保存しようとすると、エラーが発生します。

表に示されているように、GTP バージョンに応じて、同じメッセージ タイプの値が異なる場合があることに注意してください。たとえば `sgsn_context_request` メッセージ タイプの値は GTPv0 と GTPv1 では 50 ですが、GTPv2 では 130 です。

パケット内のバージョン番号に応じて、`gtp_type` キーワードは異なる値と一致します。上記の例の場合、GTPv0 または GTPv1 パケットではキーワードがメッセージ タイプ値 50 と一致しますが、GTPv2 パケットでは値 130 と一致します。パケット内のメッセージ タイプ値が、パケットで指定されたバージョンの既知の値でない場合は、キーワードがパケットと一致しません。

メッセージ タイプに整数を指定した場合、パケット内で指定されたバージョンとは無関係に、キーワード内のメッセージ タイプが GTP パケット内の値と一致すればキーワードが一致します。

次の表に、GTP メッセージ タイプごとにシステムで認識される定義済みの値と文字列を示します。

表 ***27-41***　***GTP*** メッセージ タイプ

値	**Version 0**	**Version 1**	**Version 2**
1	echo_request	echo_request	echo_request
2	echo_response	echo_response	echo_response
3	version_not_supported	version_not_supported	version_not_supported
4	node_alive_request	node_alive_request	該当なし
5	node_alive_response	node_alive_response	該当なし
6	redirection_request	redirection_request	該当なし
7	redirection_response	redirection_response	該当なし
16	create_pdp_context_request	create_pdp_context_request	該当なし
17	create_pdp_context_response	create_pdp_context_response	該当なし
18	update_pdp_context_request	update_pdp_context_request	該当なし

表 27-41　GTP メッセージ タイプ（続き）

値	Version 0	Version 1	Version 2
19	update_pdp_context_response	update_pdp_context_response	該当なし
20	delete_pdp_context_request	delete_pdp_context_request	該当なし
21	delete_pdp_context_response	delete_pdp_context_response	該当なし
22	create_aa_pdp_context_request	init_pdp_context_activation_request	該当なし
23	create_aa_pdp_context_response	init_pdp_context_activation_response	該当なし
24	delete_aa_pdp_context_request	該当なし	該当なし
25	delete_aa_pdp_context_response	該当なし	該当なし
26	error_indication	error_indication	該当なし
27	pdu_notification_request	pdu_notification_request	該当なし
36	pdu_notification_response	pdu_notification_response	該当なし
29	pdu_notification_reject_request	pdu_notification_reject_request	該当なし
30	pdu_notification_reject_response	pdu_notification_reject_response	該当なし
31	該当なし	supported_ext_header_notification	該当なし
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response
36	note_ms_present_request	note_ms_present_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	該当なし	該当なし	change_notification_request
39	該当なし	該当なし	change_notification_response
48	identification_request	identification_request	該当なし
49	identification_response	identification_response	該当なし
50	sgsn_context_request	sgsn_context_request	該当なし
51	sgsn_context_response	sgsn_context_response	該当なし
52	sgsn_context_ack	sgsn_context_ack	該当なし
53	該当なし	forward_relocation_request	該当なし
54	該当なし	forward_relocation_response	該当なし
55	該当なし	forward_relocation_complete	該当なし
72	該当なし	relocation_cancel_request	該当なし
57	該当なし	relocation_cancel_response	該当なし
58	該当なし	forward_srns_contex	該当なし
59	該当なし	forward_relocation_complete_ack	該当なし
60	該当なし	forward_srns_contex_ack	該当なし
64	該当なし	該当なし	modify_bearer_command
65	該当なし	該当なし	modify_bearer_failure_indication

表 *27-41*　*GTP* メッセージ タイプ（続き）

値	Version 0	Version 1	Version 2
66	該当なし	該当なし	delete_bearer_command
67	該当なし	該当なし	delete_bearer_failure_indication
68	該当なし	該当なし	bearer_resource_command
69	該当なし	該当なし	bearer_resource_failure_indication
70	該当なし	ran_info_relay	downlink_failure_indication
71	該当なし	該当なし	trace_session_activation
72	該当なし	該当なし	trace_session_deactivation
73	該当なし	該当なし	stop_paging_indication
95	該当なし	該当なし	create_bearer_request
96	該当なし	mbms_notification_request	create_bearer_response
97	該当なし	mbms_notification_response	update_bearer_request
98	該当なし	mbms_notification_reject_request	update_bearer_response
99	該当なし	mbms_notification_reject_response	delete_bearer_request
100	該当なし	create_mbms_context_request	delete_bearer_response
101	該当なし	create_mbms_context_response	delete_pdn_request
102	該当なし	update_mbms_context_request	delete_pdn_response
103	該当なし	update_mbms_context_response	該当なし
104	該当なし	delete_mbms_context_request	該当なし
105	該当なし	delete_mbms_context_response	該当なし
112	該当なし	mbms_register_request	該当なし
113	該当なし	mbms_register_response	該当なし
114	該当なし	mbms_deregister_request	該当なし
115	該当なし	mbms_deregister_response	該当なし
116	該当なし	mbms_session_start_request	該当なし
117	該当なし	mbms_session_start_response	該当なし
118	該当なし	mbms_session_stop_request	該当なし
119	該当なし	mbms_session_stop_response	該当なし
120	該当なし	mbms_session_update_request	該当なし
121	該当なし	mbms_session_update_response	該当なし
128	該当なし	ms_info_change_request	identification_request
129	該当なし	ms_info_change_response	identification_response
130	該当なし	該当なし	sgsn_context_request
131	該当なし	該当なし	sgsn_context_response
132	該当なし	該当なし	sgsn_context_ack
133	該当なし	該当なし	forward_relocation_request
134	該当なし	該当なし	forward_relocation_response

表 *27-41*　*GTP* メッセージ タイプ（続き）

値	Version 0	Version 1	Version 2
135	該当なし	該当なし	forward_relocation_complete
136	該当なし	該当なし	forward_relocation_complete_ack
137	該当なし	該当なし	forward_access
138	該当なし	該当なし	forward_access_ack
139	該当なし	該当なし	relocation_cancel_request
140	該当なし	該当なし	relocation_cancel_response
141	該当なし	該当なし	configuration_transfer_tunnel
149	該当なし	該当なし	detach
150	該当なし	該当なし	detach_ack
151	該当なし	該当なし	cs_paging
152	該当なし	該当なし	ran_info_relay
153	該当なし	該当なし	alert_mme
154	該当なし	該当なし	alert_mme_ack
155	該当なし	該当なし	ue_activity
156	該当なし	該当なし	ue_activity_ack
160	該当なし	該当なし	create_forward_tunnel_request
161	該当なし	該当なし	create_forward_tunnel_response
162	該当なし	該当なし	suspend
163	該当なし	該当なし	suspend_ack
164	該当なし	該当なし	復帰
165	該当なし	該当なし	resume_ack
166	該当なし	該当なし	create_indirect_forward_tunnel_request
167	該当なし	該当なし	create_indirect_forward_tunnel_response
168	該当なし	該当なし	delete_indirect_forward_tunnel_request
169	該当なし	該当なし	delete_indirect_forward_tunnel_response
170	該当なし	該当なし	release_access_bearer_request
171	該当なし	該当なし	release_access_bearer_response
176	該当なし	該当なし	downlink_data
177	該当なし	該当なし	downlink_data_ack
179	該当なし	該当なし	pgw_restart
180	該当なし	該当なし	pgw_restart_ack
200	該当なし	該当なし	update_pdn_request
201	該当なし	該当なし	update_pdn_response
211	該当なし	該当なし	modify_access_bearer_request
212	該当なし	該当なし	modify_access_bearer_response
231	該当なし	該当なし	mbms_session_start_request

表 *27-41*　*GTP* メッセージ タイプ（続き）

値	Version 0	Version 1	Version 2
232	該当なし	該当なし	mbms_session_start_response
233	該当なし	該当なし	mbms_session_update_request
234	該当なし	該当なし	mbms_session_update_response
235	該当なし	該当なし	mbms_session_stop_request
236	該当なし	該当なし	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	該当なし
241	data_record_transfer_response	data_record_transfer_response	該当なし
254	該当なし	end_marker	該当なし
255	pdu	pdu	該当なし

GTP メッセージ タイプを指定するには、次の手順を実行します。

ステップ **1**　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [gtp_type] を選択して、**[**オプションを追加（**Add Option**）**]** をクリックします。

`gtp_type` キーワードが表示されます。

ステップ **2**　メッセージ タイプとして定義済みの 10 進数値（0 ～ 255 の範囲）、定義済み文字列、あるいはそのいずれか（または両方）を任意に組み合わせたカンマ区切りのリストを指定します。システムで認識される値と文字列については、GTP メッセージ タイプの表を参照してください。

gtp_info

1 つの GTP メッセージには多数の情報要素が含まれることがあり、それぞれの要素は定義済み数値および定義済み文字列によって識別されます。`gtp_info` キーワードを `gtp_version` キーワードと組み合わせて使用すると、指定された情報要素の先頭から検査を開始し、検査対象を指定の情報要素に限定することができます。

情報要素に対して定義された 10 進数値と定義された文字列のどちらでも指定できます。単一の値または文字列を指定することも、1 つのルール内で複数の `gtp_info` キーワードを使って複数の情報要素を検査することもできます。

1 つのメッセージに同じタイプの複数の情報要素が含まれている場合は、すべてが照合対象として検査されます。情報要素が無効な順序で出現する場合は、最後のインスタンスだけが検査されます。

GTP バージョンに応じて、同じ情報要素の値が異なる場合があることに注意してください。たとえば `cause` 情報要素の値は GTPv0 と GTPv1 では 1 ですが、GTPv2 では 2 です。

パケット内のバージョン番号に応じて、`gtp_info` キーワードは異なる値と一致します。上記の例の場合、GTPv0 または GTPv1 パケットではキーワードが情報要素値 1 と一致しますが、GTPv2 パケットでは値 2 と一致します。パケット内の情報要素値が、パケットで指定されたバージョンの既知の値でない場合は、キーワードがパケットと一致しません。

情報要素に整数を指定した場合、パケット内で指定されたバージョンとは無関係に、キーワード内のメッセージ タイプが GTP パケット内の値と一致すればキーワードが一致します。

次の表に、GTP 情報要素ごとにシステムで認識される値と文字列を示します。

表 *27-42*　*GTP* 情報要素

値	**Version 0**	**Version 1**	**Version 2**
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	recovery
4	tlli	tlli	該当なし
5	p_tmsi	p_tmsi	該当なし
6	qos	該当なし	該当なし
8	recording_required	recording_required	該当なし
9	認証	認証	該当なし
11	map_cause	map_cause	該当なし
12	p_tmsi_sig	p_tmsi_sig	該当なし
13	ms_validated	ms_validated	該当なし
18	recovery	recovery	該当なし
15	selection_mode	selection_mode	該当なし
16	flow_label_data_1	teid_1	該当なし
17	flow_label_signalling	teid_control	該当なし
18	flow_label_data_2	teid_2	該当なし
19	ms_unreachable	teardown_ind	該当なし
20	該当なし	nsapi	該当なし
21	該当なし	ranap	該当なし
22	該当なし	rab_context	該当なし
23	該当なし	radio_priority_sms	該当なし
24	該当なし	radio_priority	該当なし
25	該当なし	packet_flow_id	該当なし
26	該当なし	charging_char	該当なし
27	該当なし	trace_ref	該当なし
36	該当なし	trace_type	該当なし
29	該当なし	ms_unreachable	該当なし
71	該当なし	該当なし	apn
72	該当なし	該当なし	ambr
73	該当なし	該当なし	ebi
74	該当なし	該当なし	ip_addr
75	該当なし	該当なし	mei
76	該当なし	該当なし	msisdn
77	該当なし	該当なし	indication
78	該当なし	該当なし	pco

表 *27-42*　*GTP* 情報要素（続き）

値	Version 0	Version 1	Version 2
79	該当なし	該当なし	paa
80	該当なし	該当なし	bearer_qos
80	該当なし	該当なし	flow_qos
82	該当なし	該当なし	rat_type
83	該当なし	該当なし	serving_network
84	該当なし	該当なし	bearer_tft
85	該当なし	該当なし	tad
86	該当なし	該当なし	uli
87	該当なし	該当なし	f_teid
88	該当なし	該当なし	tmsi
89	該当なし	該当なし	cn_id
90	該当なし	該当なし	s103pdf
91	該当なし	該当なし	s1udf
92	該当なし	該当なし	delay_value
93	該当なし	該当なし	bearer_context
94	該当なし	該当なし	charging_id
95	該当なし	該当なし	charging_char
96	該当なし	該当なし	trace_info
97	該当なし	該当なし	bearer_flag
99	該当なし	該当なし	pdn_type
100	該当なし	該当なし	pti
101	該当なし	該当なし	drx_parameter
103	該当なし	該当なし	gsm_key_tri
104	該当なし	該当なし	umts_key_cipher_quin
105	該当なし	該当なし	gsm_key_cipher_quin
106	該当なし	該当なし	umts_key_quin
107	該当なし	該当なし	eps_quad
108	該当なし	該当なし	umts_key_quad_quin
109	該当なし	該当なし	pdn_connection
110	該当なし	該当なし	pdn_number
111	該当なし	該当なし	p_tmsi
112	該当なし	該当なし	p_tmsi_sig
113	該当なし	該当なし	hop_counter
114	該当なし	該当なし	ue_time_zone
115	該当なし	該当なし	trace_ref
116	該当なし	該当なし	complete_request_msg

表 *27-42*　*GTP* 情報要素（続き）

値	Version 0	Version 1	Version 2
117	該当なし	該当なし	guti
118	該当なし	該当なし	f_container
119	該当なし	該当なし	f_cause
120	該当なし	該当なし	plmn_id
121	該当なし	該当なし	target_id
123	該当なし	該当なし	packet_flow_id
124	該当なし	該当なし	rab_contex
125	該当なし	該当なし	src_rnc_pdcp
126	該当なし	該当なし	udp_src_port
127	charge_id	charge_id	apn_restriction
128	end_user_address	end_user_address	selection_mode
129	mm_context	mm_context	src_id
130	pdp_context	pdp_context	該当なし
131	apn	apn	change_report_action
132	protocol_config	protocol_config	fq_csid
133	gsn	gsn	channel
134	msisdn	msisdn	emlpp_pri
135	該当なし	qos	node_type
136	該当なし	authentication_qu	fqdn
137	該当なし	tft	ti
138	該当なし	target_id	mbms_session_duration
139	該当なし	utran_trans	mbms_service_area
140	該当なし	rab_setup	mbms_session_id
141	該当なし	ext_header	mbms_flow_id
142	該当なし	trigger_id	mbms_ip_multicast
143	該当なし	omc_id	mbms_distribution_ack
144	該当なし	ran_trans	rfsp_index
145	該当なし	pdp_context_pri	uci
146	該当なし	addi_rab_setup	csg_info
147	該当なし	sgsn_number	csg_id
148	該当なし	common_flag	cmi
149	該当なし	apn_restriction	service_indicator
150	該当なし	radio_priority_lcs	detach_type
151	該当なし	rat_type	ldn
152	該当なし	user_loc_info	node_feature
153	該当なし	ms_time_zone	mbms_time_to_transfer

表 *27-42*　*GTP* 情報要素（続き）

値	Version 0	Version 1	Version 2
154	該当なし	imei_sv	throttling
155	該当なし	camel	arp
156	該当なし	mbms_ue_context	epc_timer
157	該当なし	tmp_mobile_group_id	signalling_priority_indication
158	該当なし	rim_routing_addr	tmgi
159	該当なし	mbms_config	mm_srvcc
160	該当なし	mbms_service_area	flags_srvcc
161	該当なし	src_rnc_pdcp	nmbr
162	該当なし	addi_trace_info	該当なし
163	該当なし	hop_counter	該当なし
164	該当なし	plmn_id	該当なし
165	該当なし	mbms_session_id	該当なし
166	該当なし	mbms_2g3g_indicator	該当なし
167	該当なし	enhanced_nsapi	該当なし
168	該当なし	mbms_session_duration	該当なし
169	該当なし	addi_mbms_trace_info	該当なし
170	該当なし	mbms_session_repetition_num	該当なし
171	該当なし	mbms_time_to_data	該当なし
173	該当なし	bss	該当なし
174	該当なし	cell_id	該当なし
175	該当なし	pdu_num	該当なし
177	該当なし	mbms_bearer_capab	該当なし
178	該当なし	rim_routing_disc	該当なし
179	該当なし	list_pfc	該当なし
180	該当なし	ps_xid	該当なし
181	該当なし	ms_info_change_report	該当なし
182	該当なし	direct_tunnel_flags	該当なし
183	該当なし	correlation_id	該当なし
184	該当なし	bearer_control_mode	該当なし
185	該当なし	mbms_flow_id	該当なし
186	該当なし	mbms_ip_multicast	該当なし
187	該当なし	mbms_distribution_ack	該当なし
188	該当なし	reliable_inter_rat_handover	該当なし
189	該当なし	rfsp_index	該当なし
190	該当なし	fqdn	該当なし
191	該当なし	evolved_allocation1	該当なし

表 27-42　GTP 情報要素（続き）

値	Version 0	Version 1	Version 2
192	該当なし	evolved_allocation2	該当なし
193	該当なし	extended_flags	該当なし
194	該当なし	uci	該当なし
195	該当なし	csg_info	該当なし
196	該当なし	csg_id	該当なし
197	該当なし	cmi	該当なし
198	該当なし	apn_ambr	該当なし
199	該当なし	ue_network	該当なし
200	該当なし	ue_ambr	該当なし
201	該当なし	apn_ambr_nsapi	該当なし
202	該当なし	ggsn_backoff_timer	該当なし
203	該当なし	signalling_priority_indication	該当なし
204	該当なし	signalling_priority_indication_nsapi	該当なし
205	該当なし	high_bitrate	該当なし
206	該当なし	max_mbr	該当なし
251	charging_gateway_addr	charging_gateway_addr	該当なし
255	private_extension	private_extension	private_extension

次の手順に従って、GTP 情報要素を指定できます。

GTP 情報要素を指定するには、次の手順を実行します。

ステップ 1　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [gtp_info] を選択して、**[**オプションを追加（**Add Option**）**]** をクリックします。

`gtp_info` キーワードが表示されます。

ステップ 2　情報要素に関する 1 つの定義済み 10 進数値（0 ～ 255）または 1 つの定義済み文字列を指定します。システムで認識される値と文字列については、GTP 情報要素の表を参照してください。

Modbus キーワード

ライセンス：Protection

Modbus キーワードを使用すると、Modbus 要求または応答内の [データ（Data）] フィールドの先頭を指し示したり、Modbus 機能コードと照合したり、Modbus ユニット ID と照合することができます。Modbus キーワードを単独で使用することも、`content` や `byte_jump` など他のキーワードと組み合わせて使用することもできます。

詳細については、次の各項を参照してください。

- modbus_data（27-78 ページ）
- modbus_func（27-78 ページ）
- modbus_unit（27-79 ページ）

modbus_data

modbus_data キーワードを使用すると、Modbus 要求または応答内の [データ（Data）] フィールドの先頭を指し示すことができます。

[Modbus データ（Modbus Data）] フィールドの先頭を指し示すには、次の手順を実行します。

ステップ 1　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [modbus_data] を選択して、**[オプションを追加（Add Option）]** をクリックします。

modbus_data キーワードが表示されます。

modbus_data キーワードには引数がありません。

modbus_func

modbus_func キーワードを使用すると、Modbus アプリケーション層要求または応答ヘッダー内の [Function Code] フィールドを照合できます。Modbus 機能コードとして、1 つの定義済み 10 進数値または 1 つの定義済み文字列を指定できます。

次の表に、Modbus 機能コードとしてシステムで認識される定義済みの値と文字列を示します。

表 ***27-43***　***Modbus*** 機能コード

値	文字列
1	read_coils
2	read_discrete_inputs
3	read_holding_registers
4	read_input_registers
5	write_single_coil
6	write_single_register
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
17	report_slave_id
20	read_file_record
21	write_file_record
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue
43	encapsulated_interface_transport

Modbus 機能コードを指定するには、次の手順を実行します。

ステップ 1　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [modbus_func] を選択して、**[**オプションを追加（**Add Option**）**]** をクリックします。

`modbus_func` キーワードが表示されます。

ステップ 2　機能コード用の 1 つの定義済み 10 進数値（0 ～ 255）または 1 つの定義済み文字列を指定します。システムで認識される値と文字列については、Modbus 機能コード の表を参照してください。

modbus_unit

`modbus_unit` キーワードを使用すると、Modbus 要求または応答ヘッダー内の [ユニット ID（Unit ID）] フィールドで 1 つの 10 進数値を照合できます。

Modbus ユニット **ID** を指定するには、次の手順を実行します。

ステップ 1　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [modbus_unit] を選択して、**[**オプションを追加（**Add Option**）**]** をクリックします。

`modbus_unit` キーワードが表示されます。

ステップ 2　10 進数値（0 ～ 255 の範囲）を 1 つ指定します。

DNP3 キーワード

ライセンス：Protection

DNP3 キーワードを使用すると、アプリケーション層フラグメントの先頭を指し示したり、DNP3 要求および応答での DNP3 機能コードやオブジェクトを照合したり、DNP3 応答での内部通知フラグを照合することができます。DNP3 キーワードを単独で使用することも、`content` や `byte_jump` など他のキーワードと組み合わせて使用することもできます。

詳細については、次の各項を参照してください。

- dnp3_data（27-79 ページ）
- dnp3_func（27-80 ページ）
- dnp3_ind（27-81 ページ）
- dnp3_obj（27-82 ページ）

dnp3_data

`dnp3_data` キーワードを使用すると、再構築された DNP3 アプリケーション層フラグメントの先頭を指し示すことができます。

DNP3 プリプロセッサは、リンク層フレームをアプリケーション層フラグメントに再構築します。`dnp3_data` キーワードは、各アプリケーション層フラグメントの先頭を指し示します。他のルール オプションは、16 バイトごとにデータを分離してチェックサムを追加せずに、フラグメント内の再構築されたデータを照合することができます。

再構築された **DNP3** フラグメントの先頭を指すには、次の手順を実行します。

ステップ **1**　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [modbus_data] を選択して、**[**オプションを追加（**Add Option**）**]** をクリックします。

`dnp3_data` キーワードが表示されます。

`dnp3_data` キーワードには引数がありません。

dnp3_func

`dnp3_func` キーワードを使用すると、DNP3 アプリケーション層要求または応答ヘッダー内の [Function Code] フィールドを照合できます。DNP3 機能コードとして、1 つの定義済み 10 進数値または 1 つの定義済み文字列を指定できます。

次の表に、DNP3 機能コードとしてシステムで認識される定義済みの値と文字列を示します。

表 ***27-44***　***DNP3*** 機能コード

値	文字列
0	confirm
1	read
2	write
3	選択
4	operate
5	direct_operate
6	direct_operate_nr
7	immed_freeze
8	immed_freeze_nr
9	freeze_clear
10	freeze_clear_nr
11	freeze_at_time
12	freeze_at_time_nr
13	cold_restart
18	warm_restart
15	initialize_data
16	initialize_appl
17	start_appl
18	stop_appl
19	save_config
20	enable_unsolicited
21	disable_unsolicited
22	assign_class
23	delay_measure

表 *27-44*　*DNP3* 機能コード（続き）

値	文字列
24	record_current_time
25	open_file
26	close_file
27	delete_file
36	get_file_info
29	authenticate_file
30	abort_file
31	activate_config
32	authenticate_req
33	authenticate_err
129	response
130	unsolicited_response
131	authenticate_resp

DNP3 機能コードを指定するには、次の手順を実行します。

ステップ **1**　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [dnp3_func] を選択して、**[**オプションを追加（**Add Option**）**]** をクリックします。

`dnp3_func` キーワードが表示されます。

ステップ **2**　機能コード用の 1 つの定義済み 10 進数値（0 ～ 255）または 1 つの定義済み文字列を指定します。システムで認識される値と文字列については、DNP3 機能コードの表を参照してください。

dnp3_ind

`dnp3_ind` キーワードを使用すると、DNP3 アプリケーション層応答ヘッダー内の [内部通知（Internal Indications）] フィールド内のフラグを照合できます。

1 つの既知のフラグ、または次の例のようなカンマ区切りのフラグ リストを示す文字列を指定できます。

```
class_1_events, class_2_events
```

複数のフラグを指定した場合、キーワードはリスト内の任意のフラグと一致します。いくつかのフラグの組み合わせを検出するには、1 つのルール内で `dnp3_ind` キーワードを複数回使用します。

定義済みの DNP3 内部通知フラグとしてシステムによって認識される文字列構文を以下に示します。

```
class_1_events
class_2_events
class_3_events
need_time
local_control
device_trouble
device_restart
no_func_code_support
object_unknown
parameter_error
event_buffer_overflow
```

```
already_executing
config_corrupt
reserved_2
reserved_1
```

DNP3 内部通知フラグを指定するには、次の手順を実行します。

ステップ 1　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [dnp3_ind] を選択して、**[**オプションを追加（**Add Option**）**]** をクリックします。

`dnp3_ind` キーワードが表示されます。

ステップ 2　1 つの既知のフラグ、またはカンマ区切りのフラグ リストを示す文字列を指定できます。

dnp3_obj

`dnp3_obj` キーワードを使用すると、要求または応答内の DNP3 オブジェクト ヘッダーを照合できます。

DNP3 データは、アナログ入力やバイナリ入力など、さまざまなタイプの一連の DNP3 オブジェクトで構成されます。各タイプは、それぞれ 10 進数値で識別されるグループを使って区別されます（アナログ入力グループ、バイナリ入力グループなど）。各グループ内のオブジェクトは、それぞれオブジェクト データ形式を指定するオブジェクト バリエーションによってさらに区別されます（16 ビット整数、32 ビット整数、短精度浮動小数点など）。また、オブジェクト バリエーションの各タイプは 10 進数値でも識別可能です。

オブジェクト ヘッダーを識別する際には、オブジェクト ヘッダー グループのタイプを示す 10 進数値とオブジェクト バリエーションのタイプを示す 10 進数値を指定します。この 2 つの組み合わせによって DNP3 オブジェクトの特定のタイプが定義されます。

DNP3 オブジェクトを指定するには、次の手順を実行します。

ステップ 1　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [dnp3_obj] を選択して、**[**オプションを追加（**Add Option**）**]** をクリックします。

`dnp3_obj` キーワードが表示されます。

ステップ 2　既知のオブジェクト グループを識別するために 1 つの 10 進数値（0 ～ 255）を指定し、既知のオブジェクト バリエーション タイプを識別するために別の 10 進数値（0 ～ 255）を指定します。

パケット特性の検査

ライセンス：Protection

特定のパケット特性を持つパケットに対してのみイベントを生成するルールを作成できます。ASA FirePOWER モジュールには、パケット特性を評価するための次のキーワードが備わっています。

- dsize（27-83 ページ）
- isdataat（27-83 ページ）
- sameip（27-84 ページ）
- fragoffset（27-84 ページ）
- cvs（27-84 ページ）

dsize

ライセンス：Protection

dsize キーワードはパケット ペイロード サイズを検査します。「大なり」演算子と「小なり」演算子（<、>）を使って値の範囲を指定することができます。次の構文をに従って範囲を指定できます。

```
>number_of_bytes
<number_of_bytes
number_of_bytes<>number_of_bytes
```

たとえば、400 バイトを超えるパケット サイズを指定するには、dtype 値として >400 を使用します。500 バイト未満のパケット サイズを指定するには、<500 を使用します。400 ～ 500 バイトのパケットに対してルールをトリガーとして使用するよう指定するには、400<>500 を使用します。

注意　dsize キーワードは、プリプロセッサによってデコードされる前のパケットを検査します。

isdataat

ライセンス：Protection

isdataat キーワードは、ペイロード内の特定の位置にデータが存在することを確認するよう、ルール エンジンに指示します。

次の表に、isdataat キーワードで使用可能な引数を列挙します。

表 *27-45*　*isdataat* の引数

引数	タイプ	説明
Offset	必須	ペイロード内の特定の位置。たとえば、パケット ペイロード内のバイト位置 50 にデータが出現することを検査するには、オフセット値として 50 を指定します。A ! 修飾子は、isdataat 検査の結果を否定します。特定の量のデータがペイロードに存在しない場合、警告を出します。 また、既存の byte_extract 変数を使用してこの引数の値を指定することもできます。詳細については、パケット データをキーワード引数の中に読み込む（27-85 ページ）を参照してください。
Relative	オプション	最後に見つかったコンテンツ一致を基準にして相対的な位置を計算します。相対位置を指定する場合は、カウンタがバイト 0 から始まることに注意してください。最後に見つかったコンテンツ一致から順方向に移動するバイト数から 1 を差し引いて位置を計算します。たとえば、最後に見つかったコンテンツ一致から 9 バイト後にデータが出現すべきことを指定するには、相対オフセットとして 8 を指定します。
Raw Data	オプション	ASA FirePOWER モジュールプリプロセッサによるデコードやアプリケーション層の正規化が行われる前の、元のパケット ペイロードにデータが配置されていることを指定します。前のコンテンツ一致が未加工パケット データ内に存在していた場合は、この引数を **Relative** と一緒に使用できます。

たとえば、foo というコンテンツを検索するルールで isdataat の値が次のように指定される場合、

- Offset = !10
- Relative = enabled

ルール エンジンが foo の後ろからペイロード末尾までに 10 バイトを検出しない場合、システムは警告を出します。

isdataat を使用するには、次の手順を実行します。

ステップ 1　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [isdataat] を選択して、[オプションを追加（Add Option）] をクリックします。

[isdataat] セクションが表示されます。

sameip

ライセンス：Protection

sameip キーワードは、パケットの送信元と宛先の IP アドレスが同じであることを検査します。このキーワードは引数を受け入れません。

fragoffset

ライセンス：Protection

fragoffset キーワードは、フラグメント化されたパケットのオフセットを検査します。一部のエクスプロイト（WinNuke サービス拒否攻撃など）では、特定のオフセットを持つ手動生成されたパケット フラグメントが使われるため、このキーワードが役立ちます。

たとえば、フラグメント化されたパケットのオフセットが 31337 バイトかどうかを検査するには、fragoffset 値として 31337 を指定します。

fragoffset キーワードの引数を指定するときには、次の演算子を使用できます。

表 ***27-46***　***fragoffset*** キーワードの引数演算子

演算子	説明
!	ノット
>	より大きい
<	より少ない

(!) 演算子を < または > と組み合わせて使用できないことに注意してください。

cvs

ライセンス：Protection

cvs キーワードは、Concurrent Versions System（CVS）トラフィック内で不正な形式の CVS エントリを検査します。攻撃者は不正な形式のエントリを使用して、ヒープ オーバーフローを強制的に発生させ、CVS サーバ上で有害コードを実行することができます。このキーワードを使用すると、2 つの既知の CVS 脆弱性 CVE-2004-0396（CVS 1.11.x ～ 1.11.15 と 1.12.x ～ 1.12.7）および CVS-2004-0414（CVS 1.12.x ～ 1.12.8 と 1.11.x ～ 1.11.16）に対する攻撃を識別できます。cvs キーワードは、正しい形式のエントリであることを検査して、不正な形式のエントリが検出された場合はアラートを生成します。

CVS が動作するポートをルールに含める必要があります。さらに、トラフィックが発生する可能性のあるポートを TCP ポリシー内のストリーム再構築用のポート リストに追加することで、CVS セッションの状態を保持できるようにする必要があります。ストリーム再構築が行われるクライアント ポートのリストには、TCP ポート 2401（pserver）と 514（rsh）が含まれています。ただし、サーバが xinetd サーバ（つまり pserver）として動作する場合は、任意の TCP ポート上で動作できることに注意してください。すべての非標準ポートを、ストリーム再構築の [Client Ports] リストに追加します。詳細については、ストリーム再構成のオプションの選択（21-28 ページ）を参照してください。

不正な形式の **CVS** エントリを検出するには、次の手順を実行します。

ステップ **1**　cvs オプションをルールに追加し、キーワード引数として「invalid-entry」と入力します。

パケット データをキーワード引数の中に読み込む

ライセンス：Protection

byte_extract キーワードを使用すると、指定したバイト数をパケットから変数の中に読み込むことができます。後で、その変数を、同じルール内で他の検出キーワードの特定の引数の値として使用できます。

たとえば、パケット データに含まれるバイト数が特定のバイト セグメントで記述されている場合、パケットからデータ サイズを抽出するには、これが役立ちます。たとえば、特定のバイト セグメントにおいて、後続データが 4 バイト構成であると記述されている場合、データ サイズ 4 バイトを抽出して変数値として使用できます。

byte_extract を使用するとき、1 つのルール内で最大 2 つの異なる変数を同時に作成できます。byte_extract 変数を何回でも再定義できます。同じ変数名と別の変数定義を使って新しい byte_extract キーワードを入力した場合、その前の変数定義がオーバーライドされます。

次の表で、byte_extract キーワードで必要な引数について説明します。

表 ***27-47***　***byte_extract*** の必須引数

引数	説明
Bytes to Extract	パケットから抽出するバイト数。1、2、3、または 4 バイトを指定できます。
Offset	ペイロード内でデータの抽出を開始するバイト数。-65534 ～ 65535 バイトを指定できます。オフセット カウンタはバイト 0 から始まるため、順方向に数えるバイト数から 1 を差し引いてオフセット値を計算してください。たとえば、順方向に 8 バイト数えるには 7 を指定します。ルール エンジンは、パケット ペイロードの先頭から（**Relative** も一緒に指定した場合は最後に見つかったコンテンツ一致の後から）順方向に数えます。なお、負の数値を指定できるのは、**Relative** を一緒に指定した場合だけです。詳細については、byte_extract の追加のオプション引数 の表を参照してください。
Variable Name	他の検出キーワードの引数で使用する変数名。英数字の文字列を指定できます（ただし文字で始まる必要があります）。

抽出対象のデータを見つける方法をさらに詳しく定義するには、次の表に示す引数を使用できます。

表 ***27-48*** ***byte_extract*** の追加のオプション引数

引数	説明
Multiplier	パケットから抽出された値の乗数。0 ～ 65535 を指定できます。乗数を指定しない場合のデフォルト値は 1 です。
Align	抽出された値を、最も近い 2- バイトまたは 4- バイト境界に調整します。**Multiplier** も一緒に選択した場合、システムはこの調整の前に乗数を適用します。
Relative	ペイロードの先頭ではなく、最後に見つかったコンテンツ一致の末尾を基準にして **Offset** を計算します。詳細については、byte_extract の必須引数の表を参照してください。

DCE/RPC、**Endian**、または **Number Type** のうち 1 つだけを指定できます。

検査対象となるバイトを `byte_extract` キーワードでどのように計算するか定義するには、次の表の中から引数を選択できます。どの引数も選択しない場合、ルール エンジンは ビッグ エンディアン バイト順を使用します。

表 ***27-49*** ***byte_extract*** のエンディアンネス引数

引数	説明
Big Endian	デフォルトのネットワーク バイト順であるビッグ エンディアン バイト順でデータを処理します。
Little Endian	リトル エンディアン バイト順でデータを処理します。
DCE/RPC	DCE/RPC プリプロセッサで処理されるトラフィック用に `byte_extract` キーワードを指定します。詳細については、DCE/RPC トラフィックのデコード（19-2 ページ）を参照してください。 DCE/RPC プリプロセッサがビッグ エンディアンまたはリトル エンディアン バイト順を決定します。**Number Type** 引数と **Endian** 引数は適用されません。 この引数を有効にした場合は、他の特定の DCE/RPC キーワードと組み合わせて `byte_extract` を使用することもできます。詳細については、DCE/RPC キーワード（27-62 ページ）を参照してください。

データを読み取るときの数値タイプを ASCII 文字列として指定できます。パケット内のストリング データをシステムがどのように認識するかを定義するには、次の表のいずれかの引数を選択できます。

表 ***27-50*** ***byte_extract*** の ***Number Type*** 引数

引数	説明
Hexadecimal String	抽出されたストリング データを 16 進形式で読み取ります。
Decimal String	抽出されたストリング データを 10 進形式で読み取ります。
Octal String	抽出されたストリング データを 8 進形式で読み取ります。

たとえば、`byte_extract` の値を次のように指定した場合、

- Bytes to Extract = 4
- Variable Name = var

- Offset = 8
- Relative = enabled

ルール エンジンは、最後に見つかったコンテンツ一致から（それを基準にして）9 バイト後に出現する、4 バイトで表現される数値を `var` という名前の変数の中に読み込みます。後でこの変数を、特定のキーワード引数の値としてルール内で指定できます。

`byte_extract` キーワードで定義した変数を指定できるキーワード引数を、次の表に列挙します。

表 ***27-51*** ***byte_extract*** 変数を使用できる引数

キーワード	引数	詳細
content	Depth、Offset、Distance、Within	コンテンツ一致の制約（27-18 ページ）
byte_jump	Offset	byte_jump（27-33 ページ）
byte_test	Offset、Value	byte_test（27-36 ページ）
isdataat	Offset	isdataat（27-83 ページ）

byte_extract を使用するには、次の手順を実行します。

ステップ **1**　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [byte_extract] を選択して、[オプションを追加（Add Option）] をクリックします。

[byte_extract] セクションが、選択した最後のキーワードの下に表示されます。

ルール キーワードを使用したアクティブ応答の開始

ライセンス：Protection

システムは、トリガーとして使用された TCP ルールに応答して TCP 接続を閉じるために、またはトリガーとして使用された UDP ルールに応答して UDP セッションを閉じるために、アクティブ応答を開始できます。2 つのキーワードにより、別々の方法でアクティブ応答を開始できます。どちらかのキーワードを含むルールをパケットがトリガーとして使用すると、システムは 1 つのアクティブ応答を開始します。`config response` コマンドを使用して、使用するアクティブ応答インターフェイス、およびパッシブ展開で試行する TCP リセットの回数を設定することもできます。

リセットは接続やセッションに影響を与えるのに間に合うまでに到着する可能性が高いため、アクティブ応答はインライン展開で最も効果を発揮します。たとえば、インライン展開での `react` キーワードに応答して、システムは接続の両端用のトラフィックに TCP リセット（RST）パケットを直接挿入し、通常はこれによって接続が閉じます。

（パッシブ展開ではシステムがパケットを挿入できない、攻撃者がアクティブ応答を無視または回避するよう選択する可能性があるなど）さまざまな理由で、アクティブ応答はファイアウォールの代わりとして想定されていません。

アクティブ応答は戻って来ることがあるため、システムは TCP リセットによる TCP リセットの開始を許可しません。これにより、アクティブ応答が無限に続くことを防止できます。また、システムは、標準的な慣行に従って ICMP 到達不能パケットによる ICMP 到達不能パケットの開始を許可しません。

侵入ルールがアクティブ応答をトリガーとして使用した後、接続またはセッションで追加のトラフィックを検出するよう、TCP ストリーム プリプロセッサを設定できます。追加のトラフィックが検出されると、プリプロセッサは、指定された最大値まで、追加のアクティブ応答を接続またはセッションの両端に送信します。詳細については、侵入廃棄ルールでのアクティブ応答の開始（21-2 ページ）を参照してください。

アクティブ応答を開始するために使用できるキーワードに固有の情報については、以下の項を参照してください。

- タイプ別、方向別のアクティブ応答の開始（27-88 ページ）
- TCP リセット前の HTML ページの送信（27-89 ページ）
- アクティブ応答のリセット試行とインターフェイスの設定（27-90 ページ）

タイプ別、方向別のアクティブ応答の開始

ライセンス：Protection

`resp` キーワードを使用すると、ルール ヘッダーで TCP プロトコルと UDP プロトコルのどちらが指定されているかに基づいて、TCP 接続または UDP セッションにアクティブに（能動的に）応答できます。詳細については、プロトコルの指定（27-4 ページ）を参照してください。

キーワード引数を使用すると、パケットの方向、および TCP リセット（RST）パケットと ICMP 到達不能パケットのどちらをアクティブ応答として使用するかを指定できます。

任意の TCP リセット引数または ICMP 到達不能引数を使用して、TCP 接続を閉じることができます。UDP セッションを閉じるには、ICMP 到達不能引数だけを使用する必要があります。

また、さまざまな TCP リセット引数を使用することで、パケットの送信元、宛先、またはその両方にアクティブ応答を送ることができます。すべての ICMP 到達不能引数はパケット送信元に送られます。ICMP ネットワーク、ホスト、またはポートのどの到達不能パケットを使用するか（または 3 つすべてを使用するか）を指定できます。

ルールがトリガーとして使用されたときに ASA FirePOWER モジュールで実行されるアクションを正確に指定するために、`resp` キーワードで使用できる引数を次の表に列挙します。

表 ***27-52***　　***resp*** の引数

引数	説明
reset_source	ルールをトリガーとして使用したパケットを送信元エンドポイントに TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている `rst_snd` を指定することもできます。
reset_dest	ルールをトリガーとして使用したパケットの宛先であるエンドポイントに TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている `rst_rcv` を指定することもできます。
reset_both	送信側エンドポイントと受信側エンドポイントの両方に TCP リセット パケットを送ります。この代わりに、下位互換性のためにサポートされている `rst_all` を指定することもできます。
icmp_net	送信側に ICMP ネットワーク到達不能メッセージを送ります。
icmp_host	送信側に ICMP ホスト到達不能メッセージを送ります。
icmp_port	送信側に ICMP ポート到達不能メッセージを送ります。この引数は、UDP トラフィックを終了するために使われます。
icmp_all	送信側に次の ICMP メッセージを転送します。 • ネットワーク到達不能 • ホスト到達不能 • ポート到達不能

たとえば、ルールがトリガーとして使用されたときに接続の両側をリセットするようルールを設定するには、`resp` キーワードの値として `reset_both` を使用します。

次のように、カンマ区切りのリストを使用して複数の引数を指定できます。

```
argument,argument,argument
```

使用するアクティブ応答インターフェイスおよびパッシブ展開での TCP リセット試行回数を設定するために config response コマンドを使用する方法については、アクティブ応答のリセット試行とインターフェイスの設定（27-90 ページ）を参照してください。

アクティブ応答を指定するには、次の手順を実行します。

ステップ 1　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [resp] を選択して、**[オプションを追加（Add Option）]** をクリックします。

resp キーワードが表示されます。

ステップ 2　[resp] フィールドで、resp の引数の表にある引数を指定します。複数の引数を指定する場合は、カンマ区切りのリストを使用します。

TCP リセット前の HTML ページの送信

ライセンス：Protection

react キーワードを使用すると、パケットがルールをトリガーとして使用した時点でデフォルト HTML ページを TCP 接続クライアントに送信できます。HTML ページの送信後に、システムは TCP リセット パケットを使って接続の両端へのアクティブ応答を開始します。react キーワードは UDP トラフィックのアクティブ応答をトリガーとして使用しません。

オプションで、次の引数を指定できます。

```
msg
```

msg 引数を使用する react ルールがパケットによってトリガーとして使用されると、HTML ページにルール イベント メッセージが表示されます。イベント メッセージのフィールドについては、ルール構造について（27-2 ページ）を参照してください。

msg 引数を指定しない場合、HTML ページには次のメッセージが含まれます。

```
You are attempting to access a forbidden site.
Consult your system administrator for details.
```

（注）　アクティブ応答は戻って来ることがあるため、HTML 応答ページによって react ルールがトリガーとして使用されないようにしてください（結果としてアクティブ応答が無限に続く可能性があります）。シスコ では、react ルールを十分にテストしてから実稼動環境でアクティブにするよう推奨しています。

使用するアクティブ応答インターフェイスおよびパッシブ展開での TCP リセット試行回数を設定するために config response コマンドを使用する方法については、アクティブ応答のリセット試行とインターフェイスの設定（27-90 ページ）を参照してください。

アクティブ応答を開始する前に **HTML** ページを送信するには、次の手順を実行します。

ステップ 1　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [react] を選択して、**[オプションを追加（Add Option）]** をクリックします。

react キーワードが表示されます。

ステップ 2　次の 2 つの選択肢があります。

- 接続を閉じる前に、ルール用に設定されたイベント メッセージを含む HTML ページをクライアントに送信するには、[react] フィールドに「msg」と入力します。

- 接続を閉じる前に、次のデフォルト メッセージを含む HTML ページをクライアントに送信するには、[react] フィールドを空白のままにします。

```
You are attempting to access a forbidden site.
Consult your system administrator for details.
```

アクティブ応答のリセット試行とインターフェイスの設定

ライセンス：Protection

config response コマンドを使用すると、`resp` ルールと `react` ルールによって開始される TCP リセットの動作を詳細に設定できます。また、このコマンドは、廃棄ルールによって開始されるアクティブ応答の動作にも影響を与えます（詳細については、侵入廃棄ルールでのアクティブ応答の開始（21-2 ページ）を参照してください）。

config response コマンドを使用するには、高度な USER_CONF 変数内の別個の 1 行にこれを挿入します。USER_CONF 変数の使用方法については、拡張変数について（2-31 ページ）を参照してください。

注意　機能の説明またはサポート担当の指示に従う場合を除き、侵入ポリシー機能を設定するために高度な `USER_CONF` 変数を使用しないでください。競合または重複する設定が存在すると、システムが停止します。

アクティブ応答リセット試行、アクティブ応答インターフェイス、またはその両方を指定するには、次の手順を実行します。

ステップ 1　アクティブ応答の回数のみを指定するのか、アクティブ応答インターフェイスのみを指定するのか、またはその両方を指定するのかに応じて、高度な USER_CONF 変数内の別個の 1 行に `config response` コマンドの 1 つの形式を挿入します。次の選択肢があります。

- アクティブ応答の試行回数のみを指定するには、次のコマンドを挿入します。
  `config response: attempts att`

  例：`config response: attempts 10`
- アクティブ応答インターフェイスのみを指定するには、次のコマンドを挿入します。
  `config response: device dev`

  例：`config response: device eth0`
- アクティブ応答の試行回数とアクティブ応答インターフェイスの両方を指定するには、次のコマンドを挿入します。
  `config response: attempts att, device dev`

  例：`config response: attempts 10, device eth0`

  引数の説明

  att は、受信側ホストにパケットを受け入れさせるために、現在の接続枠で各 TCP リセット パケットを挿入する試行回数（1 ～ 20）です。この連続試行はパッシブ展開でのみ効果があります。インライン展開の場合、システムはトリガー パケットの代わりにリセット パケットをストリームに直接挿入します。システムは、ICMP 到達可能アクティブ応答を 1 つだけ送信します。

  dev は、パッシブ展開でシステムからアクティブ応答を送信したり、インライン展開でアクティブ応答を挿入したりするための代替インターフェイスです。

イベントのフィルタリング

ライセンス：Protection

detection_filter キーワードを使用すると、指定された時間内に指定された数のパケットがルールをトリガーとして使用しない限り、ルールでイベントが生成されないようにすることができます。これにより、早すぎるタイミングでルールがイベントを生成することを回避できます。たとえば、数秒間にログイン試行が 2 ～ 3 回失敗することは想定の範囲内ですが、同じ時間内に多数の試行が発生した場合はブルートフォース アタックを示唆している可能性があります。

detection_filter キーワードの必須の引数は、送信元/宛先のどちらの IP アドレスをシステムで追跡するか、イベントをトリガーする前に検出基準が満たされるべき回数、およびカウントの継続時間を定義します。

イベントのトリガーを遅らせるには、次の構文を使用します。

```
track by_src/by_dst, count count, seconds number_of_seconds
```

track 引数は、ルールの検出基準を満たすパケット数をカウントするときに、パケットの送信元 IP アドレスと宛先 IP アドレスのどちらを使用するかを指定します。システムでイベント インスタンスを追跡する方法を指定するには、次の表の中から引数値を選択します。

表 **27-53**　**detection_filter** の追跡引数

引数	説明
by_src	送信元 IP アドレスによる検出基準カウント。
by_dst	宛先 IP アドレスによる検出基準カウント。

count 引数は、ルールでイベントを生成する前に、指定された時間内に指定された IP アドレスのルールをトリガーすべきパケットの数を指定します。

seconds 引数は、ルールでイベントを生成する前に、指定された数のパケットがルールをトリガーすべき時間枠を秒数で指定します。

パケット内でコンテンツ foo を検索するルールが、次の引数を含む detection_filter キーワードを使用するとします。

```
track by_src, count 10, seconds 20
```

この例のルールは、特定の送信元 IP アドレスから 20 秒以内に 10 個のパケットで foo を検出するまでは、イベントを生成しません。システムが最初の 20 秒以内に foo を含むパケットを 7 つしか検出しなかった場合は、イベントが生成されません。しかし、最初の 20 秒間で foo が 40 回出現した場合は、ルールで 30 個のイベントが生成され、20 秒が経過するとカウントが再開されます。

しきい値と **detection_filter** キーワードの比較

detection_filter キーワードは、非推奨の threshold キーワードに代わるものです。threshold キーワードは、下位互換性を維持するために引き続きサポートされていますが、侵入ポリシー内で設定されるしきい値と同じ機能です。

detection_filter キーワードは、パケットがルールをトリガーとして使用する前に適用される検出機能です。ルールは、指定されたパケット カウントの前に検出されたトリガー パケットに関してイベントを生成しません。また、インライン展開では、パケットを破棄するようルールで設定されていても、そのようなパケットを破棄しません。逆に、指定されたパケット カウントの後に出現する、ルールをトリガーとして使用するパケットに関してルールはイベントを生成します。また、インライン展開でパケットを破棄するよう設定されている場合は、そのようなパケットを破棄します。

しきい値は、検出アクションを発生させないイベント通知機能です。これは、パケットがイベントをトリガーとして使用した後に適用されます。インライン展開において、パケットを破棄するよう設定されたルールは、ルールしきい値とは無関係に、ルールをトリガーとして使用するすべてのパケットを破棄します。

侵入ポリシー内で `detection_filter` キーワードを侵入イベントしきい値、侵入イベント抑制、およびレート ベースの攻撃防御機能と任意に組み合わせて使用できることに注意してください。また、侵入ポリシー内の侵入イベントしきい値機能と組み合わせて非推奨の `threshold` キーワードを使用するインポートされたローカル ルールを有効にした場合、ポリシー検証が失敗することに注意してください。詳細については、イベントしきい値の設定（24-23 ページ）、侵入ポリシー単位の抑制の設定（24-28 ページ）、動的ルール状態の設定（24-32 ページ）、およびローカル ルール ファイルのインポート（43-16 ページ）を参照してください。

攻撃後トラフィックの評価

ライセンス：Protection

ホストまたはセッションに関する追加のトラフィックをログに記録するようシステムに指示するには、`tag`キーワードを使用します。`tag` キーワードを使って検出するトラフィックのタイプと量を指定するときには、次の構文を使用します。

`tagging_type, count, metric, optional_direction`

次の 3 つの表に、その他の使用可能な引数について説明します。

2 つのタイプのタグ機能から選択できます。次の表に、これらのタグ機能の説明を示します。侵入ルールでルール ヘッダー オプションのみを設定した場合、session タグ引数タイプによって、同じセッションからのパケットが別のセッションからのパケットのように記録されることに注意してください。同じセッションからのパケットをまとめてグループ化するには、同じ侵入ルール内で 1 つ以上のルール オプション（`flag` キーワードや `content` キーワードなど）を設定します。

表 ***27-54***　　***tag*** の引数

引数	説明
session	ルールをトリガーとして使用したセッション内のパケットをログに記録します。
ホスト	ルールをトリガーとして使用したパケットを送信したホストからのパケットをログに記録します。ホストからのトラフィックのみ（`src`）、またはホストへのトラフィックのみ（`dst`）を記録する方向修飾子を追加できます。

ログに記録するトラフィック量を指定するには、次の引数を使用します。

表 ***27-55***　　***count*** 引数

引数	説明
count	ルールがトリガーとして使用された後にログに記録するパケット数または秒数。 この単位を指定するには、count 引数の後に測定基準引数を使用します。

次の表の中から、トラフィックの時間または量ごとにログで使用する測定基準を選択してください。

注意　高−帯域ネットワークでは、1 秒あたり数千パケットが発生する可能性があり、多数のパケットにタグを付けるとパフォーマンスに重大な影響が及ぶ可能性があるため、必ずネットワーク環境に合わせてこの設定を調整してください。

表 27-56　ログの測定基準引数

引数	説明
packets	ルールのトリガー後に、カウントで指定されるパケット数をログに記録します。
秒	ルールのトリガー後に、カウントで指定される秒数の間、トラフィックを記録します。

たとえば、次の tag キーワード値を使用するルールがトリガーとして使用された場合、

```
host, 30, seconds, dst
```

次の 30 秒間にクライアントからホストに送信されるすべてのパケットがログに記録されます。

複数のパケットに及ぶ攻撃の検出

ライセンス：Protection

状態名をセッションに割り当てるには、flowbits キーワードを使用します。すでに名前が付けられた状態に基づいてセッション内の後続パケットを分析することにより、システムは単一セッション内で複数のパケットに及ぶエクスプロイトを検出して警告を出すことができます。

flowbits 状態名は、セッションの特定部分でパケットに割り当てられるユーザ定義のラベルです。パケットの内容に基づいてパケットに状態名を付けると、警告の必要のないパケットと有害なパケットを区別しやすくなります。最大 1024 個の状態名を定義できます。たとえば、ログイン成功後にのみ発生することがわかっている有害パケットについて警告するには、flowbits キーワードを使用して、初期ログイン試行を構成するパケットを除去することにより、有害パケットのみに焦点を絞ることができます。このような機能を実装するには、まず、セッション内のすべてのログイン確立済みパケットに logged_in 状態のラベルを付けるルールを作成した後、2 番目のルールを作成し、最初のルールで設定された状態を持つパケットを検査してそのようなパケットだけを処理する flowbits をそのルールに含めます。ユーザがログイン済みかどうかを判断するために flowbits を使用する例については、state_name を使用した flowbits の例（27-95 ページ）を参照してください。

オプションの *group name* を使用すると、状態のグループに状態名を含めることができます。1 つの状態名は複数のグループに属することができます。グループに関連付けられていない状態は相互排他的ではないため、トリガーとして使用されたルールがグループに関連付けられていない状態を設定した場合、現在設定されている他の状態には影響がありません。グループに状態名を含めて、同じグループ内の別の状態を解除することで誤検出を防止する方法については、誤検出を発生させる flowbits の例（27-96 ページ）の例を参照してください。

次の表に、flowbits キーワードで使用できる演算子、状態、およびグループのさまざまな組み合わせについて説明します。なお、状態名には、英数字、ピリオド（.）、アンダースコア（_）、およびダッシュ（-）を含めることができます。

表 27-57　*flowbits* のオプション

演算子	状態オプション	グループ	説明
設定	state_name	オプション	パケットに関する指定された状態を設定します。グループが定義されている場合は、指定されたグループ内で状態を設定します。
	state_name&state_name	オプション	パケットに関する指定された状態を設定します。グループが定義されている場合は、指定されたグループ内で状態を設定します。

表 *27-57*　***flowbits*** のオプション（続き）

演算子	状態オプション	グループ	説明
setx	state_name	入力必須	指定されたグループ内でパケットに関して指定された状態を設定し、グループ内の他のすべての状態を解除します。
	state_name&state_name	入力必須	指定されたグループ内でパケットに関して指定された状態を設定し、グループ内の他のすべての状態を解除します。
unset	state_name	グループなし	パケットに関する指定された状態を解除します。
	state_name&state_name	グループなし	パケットに関する指定された状態を解除します。
	すべて	入力必須	指定されたグループ内のすべての状態を解除します。
toggle	state_name	グループなし	指定された状態が設定されている場合はそれを解除し、指定された状態が解除されている場合にはそれを設定します。
	state_name&state_name	グループなし	指定された複数の状態が設定されている場合はそれらを解除し、指定された複数の状態が解除されている場合はそれらを設定します。
	すべて	入力必須	指定されたグループ内で設定されているすべての状態を解除し、指定されたグループ内で解除されているすべての状態を設定します。
isset	state_name	グループなし	指定された状態がパケット内で設定されているかどうかを判別します。
	state_name&state_name	グループなし	指定された複数の状態がパケット内で設定されているかどうかを判別します。
	state_name|state_name	グループなし	指定されたいずれかの状態がパケット内で設定されているかどうかを判別します。
	任意	入力必須	指定されたグループ内で、いずれかの状態が設定されているかどうかを判別します。
	すべて	入力必須	指定されたグループ内で、すべての状態が設定されているかどうかを判別します。
isnotset	state_name	グループなし	指定された状態がパケット内で設定されていないかどうかを判別します。
	state_name&state_name	グループなし	指定された複数の状態がパケット内で設定されていないかどうかを判別します。
	state_name|state_name	グループなし	指定されたいずれかの状態が、パケット内で設定されていないかどうかを判別します。
	任意	入力必須	パケット内でいずれかの状態が設定されていないかどうかを判別します。
	すべて	入力必須	パケット内ですべての状態が設定されていないかどうかを判別します。
リセット	（状態なし）	オプション	すべてのパケットのすべての状態を解除します。グループが指定されている場合、グループ内のすべての状態を解除します。
noalert	（状態なし）	グループなし	イベント生成を抑制するには、これを他の演算子と組み合わせて使用します。

flowbits キーワードを使用するときには、次の点に注意してください。

- setx 演算子を使用する場合、指定した状態は、指定したグループ以外のグループに属することができません。
- setx 演算子を複数回定義して、それぞれのインスタンスで別々の状態と同じグループを指定できます。
- setx 演算子を使用してグループを指定する場合、そのグループに対して set、toggle、unset 演算子を使用することはできません。
- isset 演算子と isnotset 演算子は、指定された状態がグループに含まれるかどうかに関係なく、その状態を評価します。
- 侵入ポリシーの保存時、侵入ポリシーの再適用時、および(アクセス コントロール ポリシーで参照される侵入ポリシー数に関係なく)アクセス コントロール ポリシーの適用時には、グループ指定のない isset または isnotset 演算子を含むルールを有効にした場合、対応する状態名とプロトコルに関する flowbits 割り当て(set、setx、unset、toggle)に影響する 1 つ以上のルールを有効にしないと、対応する状態名の flowbits 割り当てに影響するすべてのルールが有効になります。
- 侵入ポリシーの保存時、侵入ポリシーの再適用時、および(アクセス コントロール ポリシーで参照される侵入ポリシー数に関係なく)アクセス コントロール ポリシーの適用時には、グループを指定した isset 演算子または isnotset 演算子を含むルールを有効にした場合、flowbits 割り当て(set、setx、unset、toggle)に影響し、対応するグループ名を定義するすべてのルールもまた有効になります。

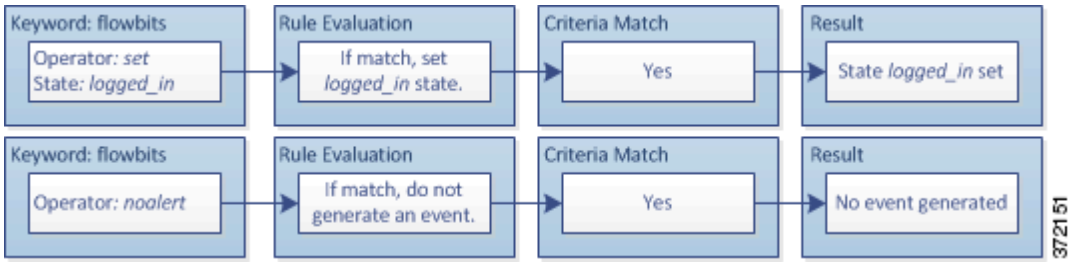
state_name を使用した **flowbits** の例

Bugtraq ID #1110 に記述されている IMAP 脆弱性について考えてみます。この脆弱性は、IMAP の実装(具体的には LIST、LSUB、RENAME、FIND、および COPY コマンド)で見られます。ただし、攻撃者がこの脆弱性を悪用するには、IMAP サーバにログインする必要があります。IMAP サーバからの LOGIN 確認とそれに続くエクスプロイトは必然的に別々のパケットに存在するため、このエクスプロイトを検出する非フロー ベースのルールを作成するのは困難です。flowbits キーワードを使って一連のルールを作成すると、ユーザが IMAP サーバにログイン済みかどうかを追跡し、ログイン済みの場合はいずれかの攻撃が検出された時点でイベントを生成することができます。ユーザがログイン済みでない場合、攻撃によって脆弱性が悪用されることはないため、イベントが生成されません。

下記の 2 つのルール フラグメントはこの例を示しています。最初のルール フラグメントは IMAP サーバからの IMAP ログイン確認を検索します。

```
alert tcp any 143 -> any any (msg:"IMAP login"; content:"OK
LOGIN"; flowbits:set,logged_in; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。

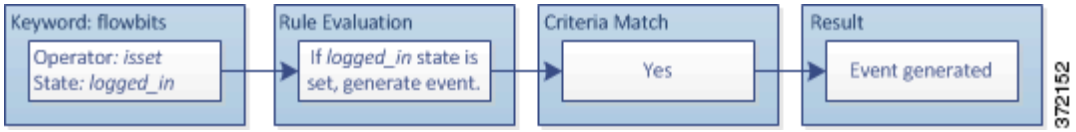


flowbits:set は logged_in 状態を設定しますが、flowbits:noalert がアラートを抑制することに注意してください。これは、IMAP サーバ上で多数の無害なログイン セッションが見つかる可能性があるためです。

次のルール フラグメントは LIST 文字列を検索しますが、セッション内の先行パケットの結果として logged_in 状態が設定済みでない限り、イベントを生成しません。

```
alert tcp any any -> any 143 (msg:"IMAP LIST";
content:"LIST"; flowbits:isset,logged_in;)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。



この場合、最初のフラグメントを含むルールが先行パケットによってトリガーとして使用した場合、2 番目のフラグメントを含むルールがトリガーとして使用し、イベントを生成します。

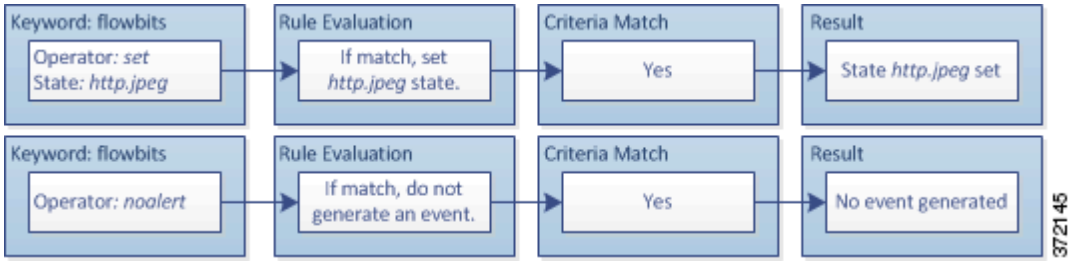
誤検出を発生させる **flowbits** の例

後続パケット内コンテンツが、効力を失った状態を持つルールに一致することによって誤検出イベントが発生する可能性があります。複数のルールで設定された複数の状態名をグループに含めることでこれを回避できます。次の例は、複数の状態名をグループに含めない場合に誤検出が発生する可能性があることを示しています。

1 つのセッションで次の 3 つのルール フラグメントがこの順序でトリガーとして使用される場合を考えてみます。

```
(msg:"JPEG transfer"; content:"image/";pcre:"/^Content-
Type\\x3a(\\s*|\\s*\\r?\\n\\s+)image\\x2fp?jpe?g/smi";
flowbits:set,http.jpeg; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。

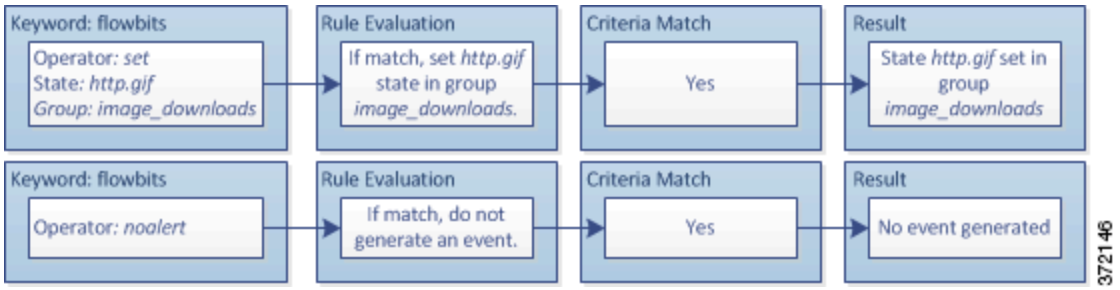


最初のルール フラグメント内の content キーワードと pcre キーワードが JPEG ファイル ダウンロードを照合し、flowbits:set,http.jpeg が http.jpeg flowbits 状態を設定し、flowbits:noalert はルールでのイベント生成を抑制します。イベントが生成されない理由は、このルールの目的がファイル ダウンロードを検出して flowbits 状態を設定することだからです。これにより、1 つ以上のコンパニオン ルールで状態名を検査して有害コンテンツを探し、有害コンテンツが検出された時点でイベントを生成できます。

次のルール フラグメントは、上記の JPEG ファイル ダウンロードに続く GIF ファイル ダウンロードを検出します。

```
(msg:"GIF transfer"; content:"image/"; pcre:"/^Content-
Type\\x3a(\\s*|\\s*\\r?\\n\\s+)image\\x2fgif/smi";
flowbits:set,http.tif,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。

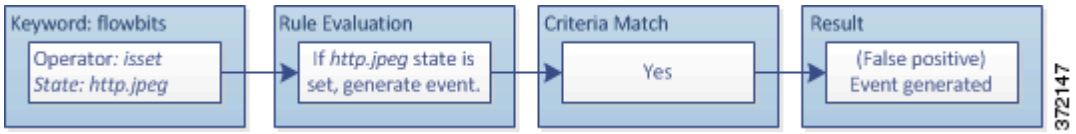


2 番目のルール内の content キーワードと pcre キーワードは GIF ファイル ダウンロードを照合し、flowbits:set,http.tif は http.tif flowbit 状態を設定し、flowbits:noalert はルールでのイベント生成を抑制します。最初のルール フラグメントで設定された http.jpeg 状態が不要になっても引き続き設定されていることに注意してください。これは、後続の GIF ダウンロードが検出されたときに JPEG ダウンロードが既に終了しているはずであるためです。

次に示す 3 番目のルール フラグメントは最初のルール フラグメントのコンパニオンです。

```
(msg:"JPEG exploit";
flowbits:isset,http.jpeg;content:"|FF|"; pcre:"
/\\xFF[\\xE1\\xE2\\xED\\xFE]\\x00[\\x00\\x01]/";)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。



3 番目のルール フラグメントでは、もはや無意味になった http.jpeg 状態が設定されていることを flowbits:isset,http.jpeg が判別し、content と pcre は（GIF ファイルでは無害でも）JPEG ファイル内では有害とみなされるコンテンツを照合します。3 番目のルール フラグメントによって、JPEG ファイル内に存在しないエクスプロイトに関する誤検出イベントが生成されます。

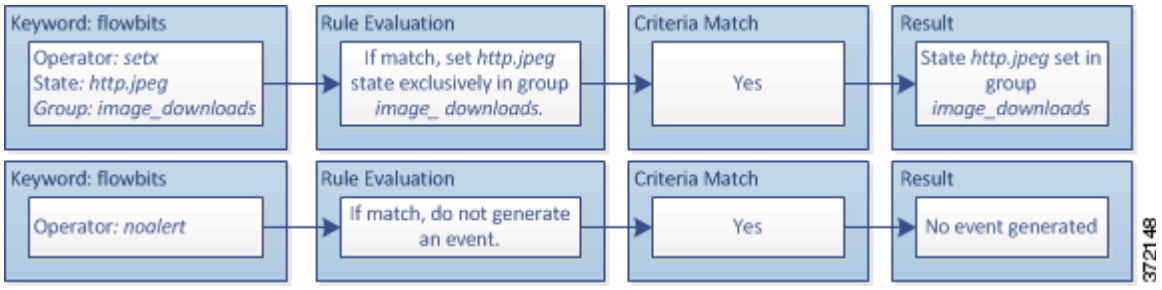
誤検出を防止するための **flowbits** の例

次の例は、状態名をグループに含めて setx 演算子を使用することで、どのように誤検出を防止できるかを示しています。

前の例とほぼ同じケースを考えます。ただし、最初の 2 つのルールで、同じ状態グループに 2 つの異なる状態名が含まれるようになった点が異なります。

```
(msg:"JPEG transfer"; content:"image/";pcre:"/^Content-
Type\\x3a(\\s*|\\s*\\r?\\n\\s+)image\\x2fp?jpe?g/smi";
flowbits:setx,http.jpeg,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。

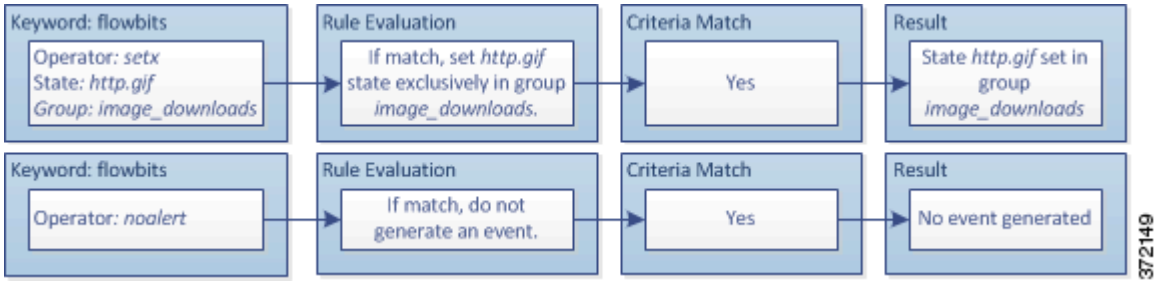


最初のルール フラグメントが JPEG ファイル ダウンロードを検出すると、flowbits:setx,http.jpeg,image_downloads キーワードが flowbits 状態を http.jpeg に設定し、その状態を image_downloads グループに含めます。

その後、次のルールが後続の GIF ファイル ダウンロードを検出します。

```
(msg:"GIF transfer"; content:"image/"; pcre:"/^Content-
Type\\x3a(\\s*|\\s*\\r?\\n\\s+)image\\x2fgif/smi";
flowbits:setx,http.tif,image_downloads; flowbits:noalert;)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。

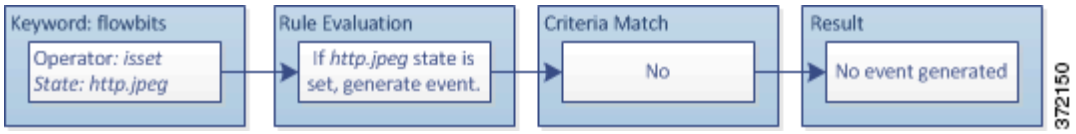


2 番目のルール フラグメントが GIF ダウンロードに一致すると、flowbits:setx,http.tif,image_downloads キーワードが http.tif flowbits 状態を設定し、グループ内の他の状態である http.jpeg を設定解除します。

次に示す 3 番目のルール フラグメントで誤検出は発生しません。

```
(msg:"JPEG exploit";
flowbits:isset,http.jpeg;content:"|FF|"; pcre:"/
\\xFF[\\xE1\\xE2\\xED\\xFE]\\x00[\\x00\\x01]/";)
```

次の図は、上記のルール フラグメントにおける flowbits キーワードの効果を示しています。



flowbits:isset,http.jpeg が false であるため、ルール エンジンはルールの処理を停止し、イベントは生成されません。こうして、GIF ファイル内のコンテンツが JPEG ファイルに関するエクスプロイト コンテンツと一致した場合でも誤検出が回避されます。

HTTP エンコードのタイプと位置によるイベントの生成

ライセンス：Protection

http_encode キーワードを使用すると、HTTP URI、HTTP ヘッダー内の非 cookie データ、HTTP 要求ヘッダー内の cookie、HTTP 応答内の set-cookie データのいずれかにおいて、正規化前の HTTP 要求または応答内のエンコード タイプに基づいてイベントを生成できます。

http_encode キーワードを使用してルールに関する一致を返すには、HTTP 応答と HTTP cookie を検査するように HTTP Inspect プリプロセッサを設定する必要があります。詳細については、「HTTP トラフィックのデコード（19-34 ページ）」と「サーバレベル HTTP 正規化オプションの選択（19-37 ページ）」を参照してください。

また、侵入ルール内の http_encode キーワードで特定のエンコード タイプによってイベントがトリガーとして使用されるようにするには、HTTP Inspect プリプロセッサ設定で個々の特定のエンコード タイプのデコード オプションとアラート オプションの両方を有効にする必要があります。詳細については、サーバレベル HTTP 正規化エンコード オプションの選択（19-45 ページ）を参照してください。

なお、base36 エンコード タイプは非推奨になりました。下位互換性を維持するために、既存のルールでは base36 引数を使用できますが、これによってルール エンジンが base36 トラフィックを検査することはありません。

次の表は、このオプションでイベントを生成できる、HTTP URI、ヘッダー、cookie、および set-cookie のエンコード タイプを説明しています。

表 ***27-58*** ***http_encode*** エンコード タイプ

エンコード タイプ	説明
utf8	HTTP Inspect プリプロセッサによるデコードで UTF8 エンコード タイプが有効になっている場合、指定された場所で UTF-8 エンコードを検出します。
double_encode	HTTP Inspect プリプロセッサによるデコードで二重エンコード タイプが有効になっている場合、指定された場所で二重エンコードを検出します。
non_ascii	非 ASCII 文字が検出されても、検出されたエンコード タイプが有効になっていない場合に、指定された場所で非 ASCII 文字を検出します。
uencode	HTTP Inspect プリプロセッサによるデコードで Microsoft %u エンコード タイプが有効になっている場合、指定された場所で Microsoft %u エンコードを検出します。
bare_byte	HTTP Inspect プリプロセッサによるデコードで空白バイト エンコード タイプが有効になっている場合、指定された場所で空白バイト エンコードを検出します。

侵入ルール内で **HTTP** エンコード タイプと位置を識別するには、次の手順を実行します。

ステップ **1**　`http_encode` キーワードをルールに追加します。

ステップ **2**　[Encoding Location] ドロップダウンリストで、指定したエンコード タイプを HTTP URI、ヘッダー、または cookie（set-cookie を含む）のどこで検索するかを選択します。

ステップ **3**　次のいずれかの形式を使用して、1 つ以上のエンコード タイプを指定します。

```
encode_type
encode_type|encode_type|encode_type...
!encode_type
```

ここで、*encode_type* は次のいずれかです。

```
utf8, double_encode, non_ascii, uencode, bare_byte
```

否定（!）演算子と OR（|）演算子を一緒に使用できないことに注意してください。

ステップ **4**　オプションで、複数の `http_encode` キーワードを同じルールに追加すると、それぞれの条件が AND 結合されます。たとえば、次の条件を含む 2 つのキーワードを入力します。

最初のキーワード `http_encode` では：

- **Encoding Location**: `HTTP URI`
- **Encoding Type**: `utf8`

追加のキーワード `http_encode` では：

- **Encoding Location**: `HTTP URI`
- **Encoding Type**: `uencode`

この設定例は、HTTP URI において UTF-8 および Microsoft IIS %u エンコードを検索します。

ファイル タイプとバージョンの検出

ライセンス: Protection

file_type および file_group キーワードを使用すると、ファイルのタイプおよびバージョンに基づいて FTP、HTTP、SMTP、IMAP、POP3、および NetBIOS-ssn（SMB）経由で送信されたファイルを検出できます。1 つの侵入ルール内で複数の file_type キーワードや file_group キーワードを使用しないでください。

ヒント　脆弱性データベース（VDB）を更新すると、最新のファイル タイプ、バージョン、およびグループがルール エディタに表示されます。詳細については、脆弱性データベースの更新（43-8 ページ）を参照してください。

file_type または file_group キーワードに一致するトラフィックに対し侵入イベントを生成するには、特定のプリプロセッサを有効にする必要があります。

表 ***27-59***　***file_type*** および ***file_group*** の侵入イベントの生成

伝送プロトコル	必要なプリプロセッサまたはプリプロセッサ オプション
[FTP]	FTP/Telnet のプリプロセッサおよび [Normalize TCP Payload] インライン正規化プリプロセッサオプション。FTP および Telnet トラフィックのデコード（19-20 ページ）および インライン トラフィックの正規化（21-6 ページ）を参照してください。
HTTP	HTTP Inspect プリプロセッサ。HTTP トラフィックのデコード（19-34 ページ）を参照してください。
SMTP	SMTP プリプロセッサ。SMTP トラフィックのデコード（19-66 ページ）を参照してください。
IMAP	IMAP プリプロセッサ。IMAP トラフィックのデコード（19-59 ページ）を参照してください。
POP3	POP プリプロセッサ。POP トラフィックのデコード（19-63 ページ）を参照してください。
NetBIOS-ssn (SMB)	[SMB File Inspection] DCE/RPC プリプロセッサ オプション。DCE/RPC トラフィックのデコード（19-2 ページ）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。

- file_type（27-100 ページ）
- file_group（27-101 ページ）

file_type

file_type キーワードを使用すると、トラフィック内で検出対象となるファイルのタイプとバージョンを指定できます。ファイル タイプ引数（**JPEG** や **PDF** など）は、トラフィックで検出するファイルの形式を識別します。

（注）　同じ侵入ルール内で file_type キーワードを別の file_type キーワードまたは file_group キーワードと一緒に使用しないでください。

デフォルトでは [任意のバージョン（Any Version）] が選択されますが、一部のファイル タイプではバージョン オプション（たとえば PDF バージョン **1.7**）を選択することにより、トラフィックで検出対象となる特定のファイル タイプ バージョンを識別できます。

最新のファイル タイプとバージョンを表示して設定するには、VDB を更新してください。詳細については、脆弱性データベースの更新（43-8 ページ）を参照してください。

侵入ルール内でファイル タイプとバージョンを選択するには、次の手順を実行します。

ステップ **1**　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [file_type] を選択して、**[**オプションを追加（**Add Option**）**]** をクリックします。

`file_type` キーワードが表示されます。

ステップ **2**　ドロップダウンリストから 1 つ以上のファイル タイプを選択します。ファイル タイプを選択すると、引数が自動的にルールに追加されます。

ルールからファイル タイプ引数を削除するには、削除するファイル タイプの横にある削除アイコン（ ）をクリックします。

ステップ **3**　オプションで、各ファイル タイプのターゲット バージョンをカスタマイズします。デフォルトでは [任意のバージョン（Any Version）] が選択されますが、いくつかのファイル タイプでは、個別のターゲット バージョンを選択できます。

（注）　VDB を更新すると、最新のファイル タイプとバージョンがルール エディタに表示されます。[任意のバージョン（Any Version）] を選択した場合、新しいバージョンが今後の VDB 更新に追加されたときにそのバージョンを含めるよう、システムによってルールが設定されます。

file_group

`file_group` キーワードを使用すると、トラフィック内で検出する類似のファイル タイプからなる シスコ 定義のグループを選択できます（マルチメディア、オーディオなど）。また、ファイル グループには、グループ内の各ファイル タイプに関する シスコ 定義のバージョンも含まれています。

（注）　同じ侵入ルール内で `file_group` キーワードを別の `file_group` キーワードまたは `file_type` キーワードと一緒に使用しないでください。

最新のファイル グループを表示して設定するには、VDB を更新してください。詳細については、脆弱性データベースの更新（43-8 ページ）を参照してください。

侵入ルール内でファイル グループを選択するには、次の手順を実行します。

ステップ **1**　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [file_group] を選択して、**[**オプションを追加（**Add Option**）**]** をクリックします。

`file_group` キーワードが表示されます。

ステップ **2**　ルールに追加するファイル グループを選択します。

特定のペイロード タイプを指し示す

ライセンス：Protection

file_data キーワードは、content、byte_jump、byte_test、pcre などの他のキーワードで使用可能な位置引数の参照として機能するポインタです。file_data キーワードが指し示すデータのタイプは、検出されるトラフィックによって決まります。file_data キーワードを使用すると、次のペイロード タイプの先頭を指し示すことができます。

- HTTP 応答本文

  HTTP 応答パケットを検査するには、HTTP Inspect プリプロセッサを有効にして、HTTP 応答を検査するようプリプロセッサを設定する必要があります。詳細については、HTTP トラフィックのデコード（19-34 ページ）、およびサーバレベル HTTP 正規化オプションの選択（19-37 ページ）の「**HTTP** 応答の検査（**Inspect HTTP Responses**）」を参照してください。HTTP Inspect プリプロセッサが HTTP 応答本文データを検出した場合に、file_data キーワードが一致します。

- 非圧縮 gzip ファイル データ

  HTTP 応答本文内の非圧縮 gzip ファイルを検査するには、HTTP Inspect プリプロセッサを有効にする必要があり、さらに HTTP 応答を検査して HTTP 応答本文内の gzip 圧縮ファイルを復元するようプリプロセッサを設定する必要があります。詳細については、HTTP トラフィックのデコード（19-34 ページ）、およびサーバレベル HTTP 正規化オプションの選択（19-37 ページ）の「**HTTP** 応答の検査（**Inspect HTTP Responses**）」と「圧縮データの検査（**Inspect Compressed Data**）」の各オプションを参照してください。file_data キーワードは、HTTP Inspect プリプロセッサが HTTP 応答本文内で非圧縮 gzip データを検出した場合に一致します。

- 正規化された JavaScript

  正規化された JavaScript データを検査するには、HTTP Inspect プリプロセッサを有効にして、HTTP 応答を検査するようプリプロセッサを設定する必要があります。詳細については、HTTP トラフィックのデコード（19-34 ページ）、および サーバレベル HTTP 正規化オプションの選択（19-37 ページ）の「**HTTP** 応答の検査（**Inspect HTTP Responses**）」を参照してください。file_data キーワードは、HTTP Inspect プリプロセッサが応答本文データ内で JavaScript を検出した場合に一致します。

- SMTP ペイロード

  SMTP ペイロードを検査するには、SMTP プリプロセッサを有効にする必要があります。詳細については、SMTP デコードの設定（19-71 ページ）を参照してください。file_data キーワードは、SMTP プリプロセッサが SMTP データを検出した場合に一致します。

- SMTP、POP、または IMAP トラフィック内のエンコードされた電子メール添付ファイル

  SMTP、POP、または IMAP トラフィック内の電子メール添付ファイルを検査するには、それぞれ SMTP、POP、または IMAP プリプロセッサを単独で、または任意に組み合わせて有効にする必要があります。その後、有効にしたプリプロセッサごとに、デコード対象のそれぞれの添付ファイル エンコード タイプをデコードするようプリプロセッサが設定されていることを確認する必要があります。プリプロセッサごとに設定可能な添付ファイル デコード オプションは、[Base64 Decoding Depth]、[7-Bit/8-Bit/Binary Decoding Depth]、[Quoted-Printable Decoding Depth]、および [Unix-to-Unix Decoding Depth] です。詳細については、IMAP トラフィックのデコード（19-59 ページ）、POP トラフィックのデコード（19-63 ページ）、および SMTP トラフィックのデコード（19-66 ページ）を参照してください。

  1 つのルール内で複数の file_data キーワードを使用できます。

特定のペイロード タイプの先頭を指し示すには、次の手順を実行します。

ステップ 1　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [file_data] を選択して、[オプションを追加（**Add Option**）] をクリックします。

`file_data` キーワードが表示されます。

`file_data` キーワードには引数がありません。

パケット ペイロードの先頭を指し示す

ライセンス：Protection

`pkt_data` キーワードは、`content`、`byte_jump`、`byte_test`、`pcre` などの他のキーワードで使用可能な位置引数の参照として機能するポインタです。

正規化された FTP、Telnet、または SMTP トラフィックが検出された場合、`pkt_data` キーワードは、正規化されたパケット ペイロードの先頭を指します。その他のトラフィックが検出された場合、`pkt_data` キーワードは、未加工の TCP または UDP ペイロードの先頭を指します。

侵入ルールで検査するために、該当するトラフィックをシステムで正規化するには、次の正規化オプションを有効にする必要があります。

- FTP トラフィックを検査用に正規化するには、FTP および Telnet プリプロセッサの [FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape codes within FTP commands）] オプションを有効にする必要があります（サーバレベルの FTP オプションの設定（19-28 ページ）を参照）。
- Telnet トラフィックを検査用に正規化するには、FTP & Telnet プリプロセッサの [正規化（Normalize）] Telnet オプションを有効にする必要があります（Telnet オプションについて（19-23 ページ）を参照）。
- SMTP トラフィックを検査用に正規化するには、SMTP プリプロセッサの [正規化（Normalize）] オプションを有効にする必要があります（SMTP デコードについて（19-66 ページ）を参照）。

1 つのルール内で複数の `pkt_data` キーワードを使用できます。

パケット ペイロードの先頭を指し示すには、次の手順を実行します。

ステップ 1　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [pkt_data] を選択して、[オプションを追加（**Add Option**）] をクリックします。

`pkt_data` キーワードが表示されます。

`pkt_data` キーワードには引数がありません。

Base64 データのデコードと検査

ライセンス：Protection

base64_decode キーワードと base64_data キーワードを組み合わせて使用すると、指定したデータを Base64 データとしてデコードおよび検査するようルール エンジンに指示できます。たとえば HTTP PUT および POST 要求内の Base64 エンコード HTTP 認証要求ヘッダーと Base64 エンコード データを検査する場合に、これが役立つ可能性があります。

これらのキーワードは特に、HTTP 要求内の Base64 データをデコードして検査するうえで役立ちます。また、長いヘッダー行を複数行に拡張するために HTTP で使われるのと同じ方法でスペース文字やタブ文字を使用する SMTP などのプロトコルでも、これらを使用できます。この行拡張（折り返しとも言う）を使用するプロトコル内に行拡張が存在しない場合、後続スペース/タブを伴わない復帰または改行が出現した箇所で検査が終了します。

詳細については、次の各項を参照してください。

- base64_decode（27-104 ページ）
- base64_data（27-105 ページ）

base64_decode

ライセンス：Protection

base64_decode キーワードは、パケット データを Base64 データとしてデコードするようルール エンジンに指示します。オプションの引数を使用すると、デコードするバイト数と、デコードを開始するデータ内の位置を指定できます。

base64_decode キーワードは 1 つのルール内で 1 回だけ使用可能です。また、少なくとも 1 つの base64_data キーワードのインスタンスの前にこれを配置する必要があります。詳細については、base64_data（27-105 ページ）を参照してください。

Base64 データをデコードする前に、ルール エンジンは、複数行にわたって折り返された長いヘッダーを元どおりに広げます。ルール エンジンが次のいずれかに遭遇するとデコードが終了します。

- ヘッダー行の末尾
- デコード対象として指定されたバイト数
- パケットの末尾

次の表に、base64_decode キーワードで使用可能な引数の説明を示します。

表 ***27-60***　　***base64_decode*** のオプション引数

引数	説明
Bytes	デコードするバイト数を指定します。これを指定しない場合、ヘッダー行の末尾またはパケット ペイロード末尾のどちらかが先に出現するまでデコードが続行されます。ゼロ以外の正の値を指定できます。
Offset	パケット ペイロードの先頭を基準にしたオフセットを決定します。さらに **Relative** も指定した場合は、現在の検査位置を基準にしたオフセットを決定します。ゼロ以外の正の値を指定できます。
Relative	現在の検査位置を基準にして検査することを指定します。

Base64 データをデコードするには、次の手順を実行します。

ステップ 1　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [base64_decode] を選択して、**[**オプションを追加（**Add Option**）**]** をクリックします。

`base64_decode` キーワードが表示されます。

ステップ 2　オプションで、base64_decode のオプション引数の表に示す引数のいずれかを選択します。

base64_data

ライセンス：Protection

`base64_data` キーワードは、`base64_decode` キーワードを使ってデコードされた Base64 データを検査するための参照を提供します。`base64_data` キーワードは、デコードされた Base64 データの先頭から検査を開始するよう設定します。オプションで、`content` や `byte_test` などの他のキーワードで使用可能な位置引数を使用して、検査位置をさらに指定することもできます。

`base64_decode` キーワードを使用した後に `base64_data` キーワードを少なくとも 1 回使用する必要があります。オプションで、`base64_data` を複数回使用して、デコードされた Base64 データの先頭に戻ることができます。

Base64 データを検査するときには、次の点に注意してください。

- 高速パターン マッチ機能を使用できません（詳細については、高速パターン マッチ機能を使用（Use Fast Pattern Matcher）（27-28 ページ）を参照してください）。
- 中間的な HTTP コンテンツ引数を使ってルール内で Base64 検査を中断する場合は、Base64 データをさらに検査する前に、別の `base64_data` キーワードをルールに挿入する必要があります（詳細については、HTTP コンテンツ オプション（27-24 ページ）を参照してください）。

デコードされた **Base64** データを検査するには、次の手順を実行します。

ステップ 1　[ルールの作成（Create Rule）] ページで、ドロップダウンリストから [base64_data] を選択して、**[**オプションを追加（**Add Option**）**]** をクリックします。

`base64_data` キーワードが表示されます。

ルールの構築

ライセンス：Protection

独自のカスタム 標準テキスト ルール を作成することもできますが、シスコ 提供の既存の 標準テキスト ルール や 共有オブジェクトのルール を変更して、それを新しいルールとして保存することもできます。シスコ 提供の 共有オブジェクトのルール では、送信元/宛先ポートおよび IP アドレスなどのルール ヘッダー情報だけを変更できることに注意してください。共有オブジェクトのルール 内のルール キーワードとルール引数を変更することはできません。

詳細については、次の各項を参照してください。

- 新しいルールの作成（27-106 ページ）
- 既存のルールの変更（27-108 ページ）
- ルールにコメントを追加する（27-109 ページ）
- カスタム ルールの削除（27-109 ページ）

新しいルールの作成

ライセンス：Protection

独自の 標準テキスト ルール を作成できます。

カスタム 標準テキスト ルール では、ルール ヘッダー設定、ルール キーワード、およびルール引数を設定できます。オプションで、特定のプロトコルを使用する、特定の IP アドレスまたはポートを行き来するトラフィックだけをルールで照合するよう、ルール ヘッダーを設定できます。

新しいルールを作成した後、`GID:SID:Rev` という形式のルール番号を使用することで、そのルールをすばやく見つけることができます。すべての 標準テキスト ルール のルール番号は 1 から始まります。ルール番号の 2 番目の部分である Snort ID（SID）番号は、それがローカル ルールまたは シスコ 提供のルールのどちらであるかを示します。新しいルールを作成すると、システムは、ローカル ルールとして次に使用可能な Snort ID 番号をそのルールに割り当て、ローカル ルール カテゴリ内にルールを保存します。ローカル ルールの Snort ID 番号は 1,000,000新しいローカル ルールが作成されるたびに SID が 1 ずつ増えます。ルール番号の最後の部分はリビジョン番号です。新しいルールのリビジョン番号は 1 です。カスタム ルールを変更するたびに、リビジョン番号が 1 ずつ増えます。

（注）　システムは、インポートされた侵入ポリシー内のカスタム ルールに新しい SID を割り当てます。詳細については、設定のインポートおよびエクスポート（B-1 ページ）を参照してください。

ルール エディタを使用してカスタム 標準テキスト ルール を作成するには、次の手順を実行します。

ステップ 1　**[**設定（**Configuration**）**] > [ASA FirePOWER** 設定（**ASA FirePOWER Configuration**）**] > [**ポリシー（**Policies**）**] > [**侵入ポリシー（**Intrusion Policy**）**] > [**ルール エディタ（**Rule Editor**）**]** の順に選択します。

[ルール エディタ（Rule Editor）] ページが表示されます。

ステップ 2　[ルールの作成（Create Rule）] をクリックします。

[ルールの作成（Create Rule）] ページが表示されます。

ステップ 3　[Message] フィールドに、イベントと一緒に表示するメッセージを入力します。

イベント メッセージの詳細については、イベント メッセージの定義（27-12 ページ）を参照してください。

ヒント　ルール メッセージの指定は必須です。また、空白文字のみ、1 つ以上の引用符のみ、1 つ以上のアポストロフィのみ、あるいは空白文字/引用符/アポストロフィだけの組み合わせでメッセージを構成することはできません。

ステップ 4　[分類（Classification）] リストから、イベントのタイプを表す分類を選択します。

使用可能な分類の詳細については、侵入イベント分類の定義（27-13 ページ）を参照してください。

ステップ 5　[アクション（Action）] リストから、作成するルールのタイプを選択します。次のいずれかを使用できます。

- トラフィックがルールをトリガーとして使用したときにイベントを生成するルールを作成するには、[alert] を選択します。
- ルールをトリガーとして使用したトラフィックを無視するルールを作成するには、[pass] を選択します。

ステップ 6　[プロトコル（Protocol）] リストから、ルールで検査するパケットのトラフィック プロトコル（**tcp**、**udp**、**icmp**、または **ip**）を選択します。

プロトコル タイプの選択方法については、プロトコルの指定（27-4 ページ）を参照してください。

ステップ 7　[Source IPs] フィールドで、ルールをトリガーとして使用するトラフィックの送信元 IP アドレスまたはアドレス ブロックを入力します。[Destination IPs] フィールドで、ルールをトリガーとして使用するトラフィックの宛先 IP アドレスまたはアドレス ブロックを入力します。

ルール エディタで指定できる IP アドレス構文の詳細については、侵入ルールでの IP アドレスの指定（27-5 ページ）を参照してください。

ステップ 8　[Source Port] フィールドで、ルールをトリガーとして使用するトラフィックの送信元ポート番号を入力します。[Destination Port] フィールドで、ルールをトリガーとして使用するトラフィックの受信側ポート番号を入力します。

（注）　プロトコルが `ip` に設定されている場合、システムは侵入ルール ヘッダー内のポート定義を無視します。

ルール エディタで指定できるポート構文の詳細については、侵入ルールでのポートの定義（27-9 ページ）を参照してください。

ステップ 9　[方向（Direction）] リストから、ルールをトリガーとして使用するトラフィックの方向を示す演算子を選択します。次のいずれかを使用できます。

- **[**指向性（**Directional**）**]**: 送信元 IP アドレスから宛先 IP アドレスに移動するトラフィックを照合します
- **[**双方向（**Bidirectional**）**]**: 双方向に移動するトラフィックを照合します

ステップ 10　[検出オプション（Detection Options）] リストから、使用するキーワードを選択します。

ステップ 11　[オプションを追加（Add Option）] をクリックします。

ステップ 12　追加したキーワードで指定する引数を入力します。ルール キーワードとその使用方法については、ルールでのキーワードと引数について（27-10 ページ）を参照してください。

キーワードと引数を追加するときには、次の操作を実行することもできます。

- 追加した後のキーワードを並べ替えるには、移動するキーワードの横にある上矢印または下矢印をクリックします。
- キーワードを削除するには、そのキーワードの横にある [X] をクリックします。

追加するキーワード オプションごとに、ステップ 10 ～ 12 を繰り返します。

ステップ 13　ルールを保存するには、[新規保存（Save As New）] をクリックします。

システムは、ルール番号シーケンスの中でローカル ルールとして次に使用可能な Snort ID（SID）番号をルールに割り当て、ローカル ルール カテゴリ内にルールを保存します。

新しい（または変更された）ルールを適切な侵入ポリシー内で有効にして、侵入ポリシーをアクセス コントロール ポリシーの一部として適用するまでは、そのルールに照らしたトラフィックの評価が開始しません。詳細については、設定変更の展開（4-12 ページ）を参照してください。

既存のルールの変更

ライセンス：Protection

カスタム 標準テキスト ルール を変更できます。シスコ 提供の 標準テキスト ルール または 共有オブジェクトのルール を変更して保存すると、そのルールの 1 つ以上の新しいインスタンスが作成されます。

ルールを作成したり、シスコ のルールを変更したりすると、新しいルールまたはリビジョンがローカル ルール カテゴリにコピーされ、100000 より大きい次に使用可能な Snort ID（SID）がそのルールに割り当てられます。

共有オブジェクトのルール では、ヘッダー情報だけを変更することができます。共有オブジェクトのルール 内で使用されるルール キーワードやその引数を変更することはできません。共有オブジェクトのルール のヘッダー情報を変更して変更内容を保存すると、ルールの新しいインスタンスが作成され、ジェネレータ ID（GID）3、およびカスタム ルールとして次に使用可能な SID が割り当てられます。ルール エディタは、共有オブジェクトのルール の新しいインスタンスを予約済み `soid` キーワードにリンクします。これにより、新しく作成されたルールが VRT 作成のルールにマップされます。作成した 共有オブジェクトのルール のインスタンスを削除できますが、シスコ 提供の 共有オブジェクトのルール は削除できません。詳細については、「ルール ヘッダーについて（27-3 ページ）」と「カスタム ルールの削除（27-109 ページ）」を参照してください。

（注）　共有オブジェクトのルール のプロトコルを変更しないでください。変更した場合、ルールの効果がなくなる可能性があります。

ルールを変更するには、次の手順を実行します。

ステップ 1　**[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] > [ルール エディタ（Rule Editor）]** の順に選択します。

[ルール エディタ（Rule Editor）] ページが表示されます。

ステップ 2　変更する 1 つ以上のルールを探します。次の選択肢があります。

- ルール カテゴリを参照することによってルールを探すには、フォルダを通して該当するルールまで移動し、そのルールの横にある編集アイコン（ ）をクリックします。
- ページに表示するルールを絞り込むことによってルールを探すには、ルール リストの左上にあるフィルタ アイコン（ ）で示されるテキスト ボックスにルール フィルタを入力します。該当するルールまで移動して、そのルールの横にある編集アイコン（ ）をクリックします。詳細については、[ルール エディタ（Rule Editor）] ページでのルールのフィルタ処理（27-110 ページ）を参照してください。

ルール エディタが開いて、選択したルールが表示されます。

共有オブジェクトのルール を選択した場合は、ルール ヘッダー情報だけがルール エディタに表示されることに注意してください。[ルール エディタ（Rule Editor）] ページで 共有オブジェクトのルールを識別するには、リストの中で数字の 3（GID）で始まる項目を探します（たとえば 3:1000004）。

ステップ 3　ルールを変更して（ルール オプションの詳細については新しいルールの作成（27-106 ページ）を参照）、[新規保存（Save As New）] をクリックします。

ルールがローカル ルール カテゴリに保存されます。

ヒント　システム ルールの代わりに、ローカルで変更したルールを使用するには、ルール状態の設定（24-21 ページ）の手順に従ってシステム ルールを非アクティブにした後、ローカル ルールをアクティブにします。

ステップ 4　変更を適用するには、設定変更の展開（4-12 ページ）の説明に従って侵入ポリシーをアクセス コントロール ポリシーの一部として適用し、アクティブにします。

ルールにコメントを追加する

ライセンス：Protection

任意の侵入ルールにコメントを追加できます。これにより、ルールや、特定されたエクスプロイトまたはポリシー違反に関するコンテキストおよび情報を提供できます。

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。

ステップ 1　**[**設定（**Configuration**）**] > [ASA FirePOWER** 設定（**ASA FirePOWER Configuration**）**] > [**ポリシー（**Policies**）**] > [**侵入ポリシー（**Intrusion Policy**）**] > [**ルール エディタ（**Rule Editor**）**]** の順に選択します。

[ルール エディタ（Rule Editor）] ページが表示されます。

ステップ 2　注釈を付けるルールを探します。次の選択肢があります。

- ルール カテゴリを参照することによってルールを探すには、フォルダを通して該当するルールまで移動し、そのルールの横にある編集アイコン（  ）をクリックします。
- ページに表示するルールを絞り込むことによってルールを探すには、ルール リストの左上にあるフィルタ アイコン（  ）で示されるテキスト ボックスでルール フィルタを入力します。該当するルールまで移動して、そのルールの横にある編集アイコン（  ）をクリックします。詳細については、[ルール エディタ（Rule Editor）] ページでのルールのフィルタ処理（27-110 ページ）を参照してください。

ルール エディタが表示されます。

ステップ 3　[ルール コメント（Rule Comment）] をクリックします。

[ルール コメント（Rule Comment）] ページが表示されます。

ステップ 4　テキスト ボックスにコメントを入力し、[コメントの追加（Add Comment）] をクリックします。

コメント テキスト ボックスにコメントが保存されます。

カスタム ルールの削除

ライセンス：Protection

侵入ポリシーで現在有効になっていないカスタム ルールを削除することができます。シスコ 提供の 標準テキスト ルール や 共有オブジェクトのルール ルールは削除できません。

削除されたルールは削除済みカテゴリに保存されます。削除済みのルールを、新しいルールの基準として使用することができます。ルールの編集方法については、既存のルールの変更（27-108 ページ）を参照してください。

侵入ポリシーの [ルール（Rules）] ページには削除済みカテゴリが表示されないため、削除したカスタム ルールを有効にすることはできません。

なお、[ルールのアップデート（Rule Updates）] ページですべてのローカル ルールを削除することもできます。たとえば、ワンタイム ルール更新の使用（43-11 ページ）を参照してください。

詳細については、次の各項を参照してください。

- カスタム ルールの作成方法については、新しいルールの作成（27-106 ページ）を参照してください。
- ローカル ルールのインポート方法については、ルールの更新とローカル ルール ファイルのインポート（43-10 ページ）を参照してください。
- ルール状態の設定方法については、ルール状態の設定（24-21 ページ）を参照してください。

カスタム ルールを削除するには、次の手順を実行します。

ステップ 1　**[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] > [ルール エディタ（Rule Editor）]** の順に選択します。

[ルール エディタ（Rule Editor）] ページが表示されます。

ステップ 2　次の 2 つの選択肢があります。

- [ローカル ルールの削除（Delete Local Rules）] をクリックしてから、[OK] をクリックします。

  変更内容が保存された侵入ポリシー内で現在有効になっていないすべてのルールは、ローカル ルール カテゴリから削除され、削除済みカテゴリに移動されます。
- フォルダを通してローカル ルール カテゴリまで移動します。ローカル ルール カテゴリをクリックして展開してから、削除するルールの横にある削除アイコン（ ）をクリックします。

  ルールがローカル ルール カテゴリから削除され、削除済みカテゴリに移動されます。

  カスタム 標準テキスト ルール にはジェネレータ ID（GID）1 が割り当てられ（たとえば 1:1000012）、カスタム 共有オブジェクトのルール には GID として 3 が割り当てられる（たとえば 3:1000005）ことに注意してください。

ヒント　また、ヘッダー情報を変更して保存した 共有オブジェクトのルール もローカル ルール カテゴリに保管され、それらは GID 3 で列挙されます。独自に変更した 共有オブジェクトのルール を削除できますが、元の 共有オブジェクトのルール は削除できません。

[ルール エディタ（Rule Editor）] ページでのルールのフィルタ処理

ライセンス：Protection

[ルール エディタ（Rule Editor）] ページ上でルールをフィルタ処理して、ルールのサブセットを表示させることができます。たとえば、あるルールまたはその状態を変更したいが、数千ものルールの中からそれを見つけるのが困難な場合に、この機能が役立つことがあります。

フィルタを入力すると、1 つ以上の一致するルールを含むフォルダがページに表示され、一致するルールがない場合はメッセージが表示されます。フィルタには、特殊なキーワードとその引数、文字列、引用符で囲んだリテラル文字列、さらに複数のフィルタ条件を区切るスペースを含めることができます。ただし、正規表現、ワイルドカード文字、および否定文字（!）、「大なり」記号（>）、「小なり」記号（<）などの特殊な演算子をフィルタに含めることはできません。

すべてのキーワード、キーワード引数、および文字列では大文字と小文字が区別されません。`gid` キーワードと `sid` キーワードを除き、すべての引数と文字列は部分的な文字列として扱われます。`gid` と `sid` の引数は、完全一致のみを返します。

オプションで、フィルタ処理前の元のページで 1 つのフォルダを展開すると、その後のフィルタ処理でそのフォルダ内の一致が返されるときにフォルダが展開したままになります。探しているルールが多数のルールを含むフォルダ内に存在する場合には、これが役立つことがあります。

1 つのフィルタを後続の別のフィルタで制約することはできません。入力されたフィルタは、ルール データベース全体を検索して、一致するすべてのルールを返します。前回のフィルタ結果がページに表示されている状態でフィルタを入力すると、そのページの内容が消去され、代わりに新しいフィルタの結果が返されます。

フィルタ処理されている場合もされていない場合も、リスト内のルールで同じ機能を使用できます。たとえば、[ルール エディタ（Rule Editor）] ページでは、リストがフィルタ処理されているかどうかに関わらず、リスト内のルールを編集できます。

詳細については、次の各項を参照してください。

- ルール フィルタでのキーワードの使用（27-111 ページ）
- ルール フィルタでの文字列の使用（27-112 ページ）
- ルール フィルタでのキーワードと文字列の組み合わせ（27-113 ページ）
- ルールのフィルタリング（27-113 ページ）

ルール フィルタでのキーワードの使用

ライセンス：Protection

各ルール フィルタに、次の形式で 1 つ以上のキーワードを含めることができます。

keyword:*argument*

ここで、*keyword* はルール フィルタ キーワードの表のいずれかのキーワード、*argument* はキーワードに関連する特定のフィールドで検索される単一の、大文字/小文字を区別しない英数字文字列です。

`gid` と `sid` を除くすべてのキーワードの引数は、部分的な文字列として扱われます。たとえば、引数 `123` によって `"12345"`、`"41235"`、`"45123"`, などが返されます。`gid` と `sid` の引数は完全一致のみを返します。たとえば、`sid:3080` によって SID 3080 のみが返されます。

ヒント　部分的な SID を検索するには、1 つ以上の文字列を使ってフィルタ処理できます。詳細については、ルール フィルタでの文字列の使用（27-112 ページ）を参照してください。

次の表に、ルールのフィルタ処理に使用できる特定のフィルタリング キーワードと引数を示します。

表 ***27-61***　ルール フィルタ キーワード

キーワード	説明	例
`arachnids`	ルール参照内の Arachnids ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。詳細については、イベント参照の定義（27-15 ページ）を参照してください。	`arachnids:181`
`bugtraq`	ルール参照内の Bugtraq ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。詳細については、イベント参照の定義（27-15 ページ）を参照してください。	`bugtraq:2120`

表 27-61　ルール フィルタ キーワード（続き）

キーワード	説明	例
cve	ルール参照内の CVE 番号全体またはその一部分に基づいて 1 つ以上のルールを返します。詳細については、イベント参照の定義（27-15 ページ）を参照してください。	cve:2003-0109
gid	引数 1 は 標準テキスト ルール を返します。引数 3 は 共有オブジェクトのルール を返します。詳細については、表 24-1（24-2ページ）を参照してください。	gid:3
mcafee	ルール参照内の McAfee ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。詳細については、イベント参照の定義（27-15 ページ）を参照してください。	mcafee:10566
msg	ルールの [メッセージ（Message）] フィールド（イベント メッセージとも呼ばれる）の全体またはその一部分に基づいて 1 つ以上のルールを返します。詳細については、イベント メッセージの定義（27-12 ページ）を参照してください。	msg:chat
nessus	ルール参照内の Nessus ID 全体またはその一部分に基づいて 1 つ以上のルールを返します。詳細については、イベント参照の定義（27-15 ページ）を参照してください。	nessus:10737
ref	ルール参照内またはルールの [メッセージ（Message）] フィールド内の単一の英数字文字列の全体または一部分に基づいて、1 つ以上のルールを返します。詳細については、「イベント参照の定義（27-15 ページ）」と「イベント メッセージの定義（27-12 ページ）」を参照してください。	ref:MS03-039
SID	完全に一致するシグニチャ ID を持つルールを返します。	sid:235
URL	ルール参照内の URL 全体またはその一部分に基づいて 1 つ以上のルールを返します。詳細については、イベント参照の定義（27-15 ページ）を参照してください。	url:faqs.org

ルール フィルタでの文字列の使用

ライセンス：Protection

各ルール フィルタに 1 つ以上の英数字文字列を含めることができます。文字列はルールの [メッセージ（Message）] フィールド、シグニチャ ID、およびジェネレータ ID を検索します。たとえば、文字列 123 を指定するとルール メッセージ内の文字列 "Lotus123" や "123mania" などが返され、さらに SID 6123、SID 12375 なども返されます。ルールの [メッセージ（Message）] フィールドの詳細については、イベント メッセージの定義（27-12 ページ）を参照してください。

すべての文字列では大文字と小文字が区別されず、部分的な文字列として扱われます。たとえば、文字列 ADMIN、admin、または Admin はすべて、"admin"、"CFADMIN"、"Administrator" などを返します。

文字列を引用符で囲むと、完全一致を返すことができます。たとえば、引用符付きのリテラル文字列 "overflow attempt" は完全一致のみを返しますが、引用符なしの 2 つの文字列 overflow と attempt で構成されるフィルタは "overflow attempt"、"overflow multipacket attempt"、"overflow with evasion attempt" などを返します。

ルール フィルタでのキーワードと文字列の組み合わせ

ライセンス：Protection

複数のキーワード、文字列、またはその両方をスペースで区切って任意に組み合わせて入力することで、フィルタ結果を絞り込むことができます。結果には、すべてのフィルタ条件に一致するルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のフィルタはそれぞれ同じルールを返します。

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

ルールのフィルタリング

ライセンス：Protection

ステップ 1　[ルール エディタ（Rule Editor）] ページ上でルールをフィルタ処理して、ルールのサブセットを表示させると、特定のルールを見つけやすくなります。その後、コンテキスト メニューで使用可能な機能の選択など、任意のページ機能 **[**設定（**Configuration**）**] > [ASA FirePOWER** 設定（**ASA FirePOWER Configuration**）**] > [**ポリシー（**Policies**）**] > [**侵入ポリシー（**Intrusion Policy**）**] > [**ルール エディタ（**Rule Editor**）**]** の順に選択します。

[ルール エディタ（Rule Editor）] ページが表示されます。

ルール フィルタ機能は、[ルール エディタ（Rule Editor）] ページで編集するルールを見つけるときに特に役立つことがあります。詳細については、既存のルールの変更（27-108 ページ）を参照してください。

ステップ 2　オプションで、[ルールのグループ化基準（Group Rules By）] リストで別のグループ化方法を選択します。

ヒント　すべてのサブグループ内のルールの合計数が多い場合は、フィルタリングに長い時間がかかることがあります。これは、個別のルールの数がかなり少なくても、ルールが複数のカテゴリに出現することがあるためです。

ステップ 3　オプションで、展開するグループの横にあるフォルダをクリックします。

フォルダが展開されて、そのグループ内のルールが表示されます。ルール グループによっては、さらに展開可能なサブグループが存在します。

また、ルールがどのグループに含まれているか予想できる場合は、フィルタ処理前の元のページでそのグループを展開しておくと便利なことがあります。その後のフィルタ処理でそのフォルダ内の一致が返されるとき、およびフィルタ消去アイコン（ ）をクリックしてフィルタ処理前のページに戻ったときに、グループが展開されたままになります。

ステップ 4　フィルタ テキスト ボックスをアクティブにするには、ルール リストの左上にあるテキスト ボックス内のフィルタ アイコン（ ）の右側をクリックします。

ステップ 5　フィルタ制約を入力し、Enter キーを押します。

フィルタには、キーワードと引数、引用符付きまたは引用符なしの文字列、および複数の条件を区切るスペースを含めることができます。詳細については、[ルール エディタ（Rule Editor）] ページでのルールのフィルタ処理（27-110 ページ）を参照してください。

ページが更新されて、一致するルールを少なくとも 1 つ含むグループが表示されます。

ステップ 6　オプションで、まだ開いていないフォルダを開くと、一致するルールが表示されます。次のフィルタリング選択肢があります。

- 新しいフィルタを入力するには、フィルタ テキスト ボックス内にカーソルを移動してクリックし、そのボックスをアクティブにしてから、フィルタを入力して Enter キーを押します。
- フィルタ処理された現在のリストを消去してフィルタ処理されていないの元のページに戻すには、フィルタ消去アイコン（ ✖ ）をクリックします。

ステップ 7　オプションで、ページに表示されているルールを通常の方法で変更します。既存のルールの変更（27-108 ページ）を参照してください。

変更内容を有効にするには、設定変更の展開（4-12 ページ）の説明に従って、アクセス コントロール ポリシーの侵入ポリシー部分を適用します。

アイデンティティ データの概要

アイデンティティ ポリシーを設定してユーザ エージェント、ISE デバイス、またはキャプティブ ポータルを使用すると、ネットワークのユーザに関するデータを取得できます。

アイデンティティ データの用途

アイデンティティ データを収集することにより、次のようなさまざまな機能を活用できます。

- レルム、ユーザ、ユーザ グループ、および ISE 属性の条件を使用してアクセス コントロール ルールを作成することによるユーザ制御の実行
- システムが特定の影響フラグ付きの侵入イベントを生成した場合に、SNMP トラップまたは syslog によりアラートを通知

ユーザ検出の基礎

アイデンティティ ポリシーを使用してネットワーク上のユーザ アクティビティをモニタできます。これにより、脅威、エンドポイント、およびネットワーク インテリジェンスをユーザ ID 情報に関連付けることができます。ネットワーク動作、トラフィック、およびイベントを個別のユーザに直接リンクすることによって、ポリシー違反、攻撃、またはネットワークの脆弱性の発生源の特定に役立てることができます。たとえば、以下について決定できます。

- 脆弱（レベル 1:赤）影響レベルの侵入イベントの対象になっているホストの所有者
- 内部攻撃またはポートスキャンを開始した人物
- ホスト重要度の高いサーバの不正アクセスを試みている人物
- 不合理な容量の帯域幅を使用している人物
- 重要なオペレーティング システム更新を適用しなかった人物
- 会社の IT ポリシーに違反してインスタント メッセージング ソフトウェアまたはピアツーピア ファイル共有アプリケーションを使用している人物

この情報を利用して ASA FirePOWER モジュールの他の機能を使用すると、リスクを軽減し、アクセス コントロールを実行し、その他を中断から保護するアクションを実行することができます。これらの機能により、監査制御が大幅に改善され、規制の順守が促進されます。

ユーザのアイデンティティ ソースを設定すると、ユーザ認識とユーザ制御を実行できます。

ユーザ認識
: ユーザ データを表示し、分析する機能

ユーザ制御

ユーザ認識から得られた結論に基づいて、ネットワーク トラフィックでユーザまたはユーザ アクティビティをブロックするようにユーザ アクセス コントロール ルール条件を設定する機能。

（アイデンティティ ポリシーで参照される）権限のあるアイデンティティ ソースからユーザ データを取得できます。

アイデンティティ ソースは、権限のあるサーバがユーザ ログインを検証した場合に権限のあるようになります。権限のあるログインから取得したデータを使用すると、ユーザ認識とユーザ制御を実行できます。権限のあるユーザ ログインは、パッシブ認証とアクティブ認証から得られます。

- パッシブ認証は、ユーザが外部サーバ経由で認証されるときに発生します。ASA FirePOWER モジュールでサポートされているパッシブな認証方式は、ユーザ エージェントと ISE だけです。
- アクティブ認証は、ユーザが FirePOWER デバイス経由で認証されるときに発生します。ASA FirePOWER モジュールでサポートされているアクティブ認証方式は、キャプティブ ポータルだけです。

次の表に、ASA FirePOWER モジュールでサポートされているユーザ アイデンティティ ソースの概要を示します。

表 ***28-1***

ユーザ アイデンティティ ソース	サーバ要件	ソース タイプ	認証タイプ	ユーザ認識	ユーザ アクセス コントロール	詳細
ユーザ エージェント	Microsoft Active Directory	権限のあるログイン	パッシブ	○	○	ユーザ エージェントのアイデンティティ ソース（30-2 ページ）
ISE	Microsoft Active Directory	権限のあるログイン	パッシブ	○	○	Identity Services Engine（ISE）のアイデンティティ ソース（30-4 ページ）
キャプティブ ポータル	LDAP または Microsoft Active Directory	権限のあるログイン	アクティブ	○	○	キャプティブ ポータルのアイデンティティ ソース（30-6 ページ）

展開するアイデンティティ ソースを選択する際には、以下を検討してください。

- 失敗した認証アクティビティを記録するには、キャプティブ ポータルを使用する必要があります。失敗した認証試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。
- キャプティブ ポータルを使用するには、センシング インターフェイス（ルーテッド インターフェイスなど）に IP アドレスがあるアプライアンスを展開する必要があります。

ユーザ **ID** の展開

システムがユーザ ログインから、またはアイデンティティ ソースからユーザ データを検出すると、ログインのユーザは、ユーザ データベースのユーザのリストに対してチェックされます。ログイン ユーザが既存のユーザと一致した場合は、ログインからのデータがそのユーザに割り当てられます。ログインが SMTP トラフィック内に存在しない場合は、既存のユーザと一致しないログインによって新しいユーザが作成されます。SMTP トラフィック内の一致しないログインは破棄されます。

ユーザ アクティビティ データベース

デバイスのユーザ アクティビティ データベースには、設定されたすべてのアイデンティティ ソースによって報告されたネットワーク上のユーザ アクティビティのレコードが含まれます。システムがイベントを記録するのは以下のような状況です。

- 個別のログインまたはログオフを検出したとき
- 新しいユーザを検出したとき
- 手動でユーザが削除されたとき
- データベース内に存在しないユーザをシステムが検出したものの、ユーザ数の制限に達したためにそのユーザを追加できなかったとき

ユーザ データベース

ユーザ データベースには、設定されたアイデンティティ ソースによって報告された各ユーザに関するレコードが含まれます。

- デバイスに保存できるユーザの総数は、モデルによって異なります。制限に達した場合、新規ユーザを追加できるようにユーザを（手動またはデータベースの消去により）削除する必要があります。

アイデンティティ ソースが特定のユーザ名を除外するように設定されている場合は、そのようなユーザ名のユーザ アクティビティ データは ASA FirePOWER モジュールに報告されません。これらの除外されたユーザ名はデータベースに残りますが、IP アドレスに関連付けられません。

現在のユーザ **ID**

システムは、同じホストに対して異なるユーザによる複数のログインを検出すると、特定のホストにログインするユーザは一度に 1 人だけであり、ホストの現在のユーザが最後の権限のあるユーザ ログインであると見なします。複数のユーザがリモート セッション経由でログインしている場合は、サーバによって報告された最後のユーザが ASA FirePOWER モジュールに報告されるユーザです。

システムは、同じホストに対して異なるユーザによる複数のログインを検出すると、ユーザが初めて特定のホストにログインした時点を記録し、それ以降のログインを無視します。あるユーザが特定のホストにログインしている唯一の人物の場合は、システムが記録する唯一のログインがオリジナルのログインです。

ただし、そのホストに別のユーザがログインした時点で、システムは新しいログインを記録します。その後で、オリジナルのユーザが再度ログインすると、その人物の新しいログインが記録されます。

ユーザ データベースの制限

デバイス モデルにより、モニタ可能なユーザの数、ユーザ制御を実行するために使用可能なユーザの数が決定します。

（注）　展開に ASA5506-X、ASA5508-X、または ASA5516-X デバイスが含まれる場合、最大 2,000 の権限のあるユーザを保存できます。

ASA FirePOWERユーザ制限

デバイスにより、モニタできる個々のユーザ数が決まります。システムが新しいユーザのアクティビティを検出すると、そのユーザは Users データベースに追加されます。ユーザは、ユーザ エージェント、ISE、キャプティブ ポータルを使用して検出できます。

レルムとアイデンティティ ポリシー

レルムは、同じクレデンシャルを共有する 1 つ以上の LDAP または Microsoft Active Directory サーバで構成されます。ユーザおよびユーザ グループ クエリー、ユーザ アクセス コントロールを実行したり、ユーザ エージェント、ISE、キャプティブ ポータルを設定したりする場合、レルムを設定する必要があります。1 つ以上のレルムを設定すると、アイデンティティ ポリシーを設定できます。

アイデンティティ ポリシーは、ネットワーク上のトラフィックを権限のあるアイデンティティ ソースおよびレルムと関連付けます。アイデンティティ ポリシーを設定した後、アクセス コントロール ポリシーに関連付け、アクセス コントロール ポリシーをデバイスに展開できます。

レルムの基礎

ライセンス:任意

レルムは、ASA FirePOWER モジュールとモニタリングの対象サーバ間の接続を確立します。レルムでは、サーバの接続設定と認証フィルタの設定を指定します。レルムでは次のことを実行できます。

- アクティビティをモニタするユーザとユーザ グループとユーザを指定する。
- 権限のあるユーザのユーザ メタデータについてサーバに照会できるようにする。

レルム内のディレクトリとして複数のサーバを追加できますが、同じ基本レルム情報を共有する必要があります。レルム内のディレクトリは、LDAP サーバのみ、または AD サーバのみである必要があります。レルムを有効にすると、保存された変更は次回 ASA FirePOWER モジュールがサーバに照会するときに適用されます。

ユーザ認識を行うには、サポートされるすべてのサーバ タイプのレルムを設定する必要があります。モジュールは、これらの接続を使用して、POP3 および IMAP ユーザに関連付けられたデータについてサーバに照会します。モジュールは、POP3 および IMAP ログイン内の電子メール アドレスを使用して、Active Directory、OpenLDAP、または Oracle Directory Server Enterprise Edition サーバ上の LDAP ユーザに関連付けます。たとえば、LDAP ユーザと電子メール アドレスが同じユーザの POP3 ログインをデバイスが検出すると、モジュールは LDAP ユーザのメタデータをそのユーザに関連付けます。

ユーザのアクセス コントロールを実行するために以下を設定できます。

- ユーザ エージェントまたは ISE デバイス用に設定された AD サーバのレルム。
- キャプティブ ポータル用に設定された Oracle または OpenLDAP サーバのレルム。

(ユーザ認識またはユーザ制御のために) レルムを設定してユーザをダウンロードする場合、ASA FirePOWER モジュールはサーバに定期的に照会し、前回のクエリ以降にアクティビティが検出された新規ユーザおよび更新されたユーザのメタデータを取得します。

ユーザ アクティビティ データはユーザ アクティビティ データベースに保存され、ユーザのアイデンティティ データはユーザ データベースに保存されます。アクセス コントロールで保存できる使用可能なユーザの最大数はデバイス モデルによって異なります。含めるユーザとグループを選択するときは、ユーザの総数がモデルの上限より少ないことを確認してください。アクセス コントロール パラメータの範囲が広すぎる場合、ASA FirePOWER モジュールはできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数をタスク キューで報告します。

（注）　LDAP サーバからモジュールによって検出されたユーザを削除しても、ASA FirePOWER モジュールはユーザ データベースからそのユーザを削除しません。そのため、手動で削除する必要があります。ただし、LDAP に対する変更は、ASA FirePOWER モジュールが次に権限のあるユーザのリストを更新したときにアクセス コントロール ルールに反映されます。

レルムがサポートされているサーバ

ライセンス：任意

レルムを設定して次のサーバ タイプに接続すると、ASA FirePOWER モジュールからの TCP/IP アクセスを提供できます。

表 ***29-1***　　レルムがサポートされているサーバ

サーバ タイプ（**Server Type**）	ユーザ認識によるデータ取得のサポート	ユーザ エージェントによるデータ取得のサポート	**ISE** によるデータ取得のサポート	キャプティブ ポータルによるデータ取得のサポート
Windows Server 2003、Windows Server 2008、および Windows Server 2012 上の Microsoft Active Directory	○	○	○	○（NTLM キャプティブ ポータルを使用する場合、Windows Server 2003 を除く）
Windows Server 2003 と Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0	○	×	×	○
Linux 上の OpenLDAP	○	×	×	○

サーバ グループの設定に関して次の点に注意してください。

- ユーザ グループまたはグループ内のユーザに対してユーザ制御を実行する場合、サーバでユーザ グループを設定する必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、ASA FirePOWER モジュールはユーザ グループ制御を実行できません。

  最大で 1500 のユーザを含むように LDAP または AD サーバ グループのサイズを制限することを推奨します。サイズ超過のグループを含める（または除外する）ようにレルムを設定したり、サイズ超過のユーザ グループをターゲットにしたアクセス コントロール ルールを作成したりすると、パフォーマンス上の問題が生じる可能性があります。

- デフォルトでは、AD サーバはセカンダリ グループから報告するユーザの数を制限します。セカンダリ グループのすべてのユーザが ASA FirePOWER モジュールに報告されるようにこの制限をカスタマイズする必要があります。

サポートされるサーバ フィールド名

ライセンス：任意

レルムのサーバは、ASA FirePOWER モジュールがサーバからユーザ メタデータを取得できるように、次の表にリストされているフィールド名を使用する必要があります。サーバ上のフィールド名が正しくない場合、ASA FirePOWER モジュールはそのフィールドの情報を使ってデータベースに入力できなくなります。

表 ***29-2*** ***ASA FirePOWER*** フィールドへのサーバ フィールドのマッピング

メタデータ	**ASA FirePOWER** モジュール	**Active Directory**	**Oracle Directory Server**	**OpenLDAP**
LDAP ユーザ名	[ユーザ名（Username）]	samaccountname	cn uid	cn uid
first name	名	givenname	givenname	givenname
last name	姓	sn	sn	sn
email address	E メール	メール アドレス userprincipalname（mail に値が設定されていない場合）	メール アドレス	メール アドレス
部署	部署名（Department）	部署 distinguishedname（department に値が設定されていない場合）	部署	ou
telephone number	電話	telephonenumber	適用対象外	telephonenumber

レルムに関する問題のトラブルシューティング

ライセンス:任意

予期しないサーバ接続の動作に気付いたら、レルム設定、デバイス設定、またはサーバ設定の調整を検討してください。

予期しない時間にユーザ タイムアウトが発生する

予期しない間隔でユーザ タイムアウトが実行されていることに気付いたら、ユーザ エージェントまたは ISE デバイスの時間が ASA FirePOWER モジュールの時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。

レルム設定で指定したようにユーザが含まれない、または除外されない

Active Directory サーバのセカンダリ グループのメンバーであるユーザを含めるか除外する、Active Directory サーバのレルムを設定する場合、報告するユーザ数をサーバが制限していることがあります。

デフォルトでは、Active Directory サーバはセカンダリ グループから報告するユーザの数を制限します。セカンダリ グループのすべてのユーザが ASA FirePOWER モジュールに報告されるようにこの制限をカスタマイズする必要があります。

ユーザのダウンロードが遅い

ユーザのダウンロードが遅いことに気付いたら、LDAP および AD サーバ グループに最大 1500 のユーザが含まれることを確認します。サイズ超過のユーザ グループを含めるか除外するようにレルムを設定すると、パフォーマンスの問題が発生する可能性があります。

アイデンティティ ポリシーの基礎

ライセンス:任意

アイデンティティ ポリシーには、アイデンティティ ルールが含まれます。アイデンティティ ルールでは、トラフィックのセットを、レルムおよび認証方式（パッシブ認証、アクティブ認証、または認証なし）と関連付けます。

アイデンティティ ルールで呼び出す前に、使用するレルムおよび認証方式を完全に設定しておく必要があります。

- [設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [統合（Integration）] > [レルム（Realms）] でアイデンティティ ポリシー外のレルムを設定します。
- [設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [統合（Integration）] > [アイデンティティ ソース（Identity Sources）] でパッシブ認証のアイデンティティ ソース、ユーザ エージェント、および ISE を設定します。
- アイデンティティ ポリシー内で、アクティブ認証のアイデンティティ ソース、キャプティブ ポータルを設定します。

1 つ以上のアイデンティティ ポリシーを設定した後、アクセス コントロール ポリシーの 1 つのアイデンティティ ポリシーを呼び出す必要があります。ネットワークのトラフィックがアイデンティティ ルールの条件と一致し、認証方式がパッシブまたはアクティブであるとき、モジュールはトラフィックを指定されたレルムと関連付け、指定されたアイデンティティ ソースを使用してトラフィックのユーザを認証します。

アイデンティティ ポリシーを設定しない場合、モジュールはユーザ認証を実行しません。

レルムの作成

ライセンス：Control

レルムの作成方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [統合（Integration）] の順に選択します。

ステップ 2　[レルム（Realms）] をクリックします。

ステップ 3　[新しいレルム（New Realm）] をクリックします。

ステップ 4　基本的なレルム情報の設定（29-7 ページ）の説明に従って基本的なレルム情報を設定します。

ステップ 5　レルム ディレクトリの設定（29-8 ページ）の説明に従ってディレクトリを設定します。

ステップ 6　ユーザの自動ダウンロードの設定（29-8 ページ）の説明に従ってユーザとユーザ グループのダウンロード（アクセス コントロールに必要）を設定します。

ステップ 7　レルム設定を保存します。

ステップ 8　オプションで、レルム ユーザ セッション タイムアウトの設定（29-9 ページ）の説明に従ってレルムを編集し、デフォルトのユーザ セッション タイムアウトの設定を変更します。

ステップ 9　レルム設定を保存します。

次の作業

- レルムの有効化または無効化（29-18 ページ）の説明に従い、レルムを有効にします。
- オプションで、タスクのステータスをモニタします。[タスクのステータス（Task Status）] ページ（[モニタリング（Monitoring）] > [ASA FirePOWER モニタリング（ASA FirePOWER Monitoring）] > [タスクのステータス（Task Status）]）を参照してください。

レルム フィールド

ライセンス：任意

次のフィールドを使用してレルムを設定します。

レルムの設定フィールド

AD プライマリ ドメイン（AD Primary Domain）
AD レルムのみの場合に、ユーザを認証する必要がある Active Directory サーバのドメイン。

説明（**Description**）
（任意）レルムの説明。

[ディレクトリ ユーザ名（Directory Username）] と **[ディレクトリ パスワード（Directory Password）]**
取得するユーザ情報に適切な権限を持っているユーザの識別用のユーザ名とパスワード。

ベース **DN**（**Base DN**）

ASA FirePOWER モジュールがユーザ データの検索を開始するサーバのディレクトリ ツリー。

通常、ベース DN には、企業ドメインおよび部門を示す基本構造があります。たとえば、Example 社のセキュリティ（Security）部門のベース DN は、ou=security,dc=example,dc=com となります。

グループ **DN**（**Group DN**）

ASA FirePOWER モジュールがグループ属性を持つユーザを検索するサーバのディレクトリ ツリー。

グループ属性（**Group Attribute**）

サーバのグループ属性：[メンバー（Member）]、[独自のメンバー（Unique Member）]、[カスタム（Custom）]。

[名前（**Name**）**]**

レルムの一意の名前。

タイプ（**Type**）

レルム、AD、または LDAP のタイプ。

ユーザ セッションのタイムアウト：認証されたユーザ（**User Session Timeout: Authenticated Users**）

ユーザ セッションがタイムアウトされるまでの最大時間（分単位）。

パッシブ認証されたユーザのセッションがタイムアウトした場合、ユーザは [不明（Unknown）] と識別され、現在のセッションはアクセス コントロール ルールの設定に応じて許可またはブロックされます。モジュールは、次回ログイン時にユーザを再度識別します。

アクティブ認証された（キャプティブ ポータル）ユーザのセッションがタイムアウトした場合、ユーザは再認証を要求されます。

ユーザ セッションのタイムアウト：認証に失敗したユーザ（**User Session Timeout: Failed Authentication Users**）

アクティブ認証の試行失敗後にユーザのセッションがタイムアウトとなる時間（分単位）。認証に失敗したユーザのセッションがタイムアウトすると、ユーザは再認証を要求されます。

ユーザ セッションのタイムアウト：ゲスト ユーザ（**User Session Timeout: Guest Users**）

アクティブ認証された（キャプティブ ポータル）ゲスト ユーザのセッションがタイムアウトされるまでの最大時間（分単位）。ユーザのセッションがタイムアウトすると、ユーザは再認証を要求されます。

レルムのディレクトリ フィールド

これらの設定は、レルム内の個々のサーバ（ディレクトリ）に適用されます。

暗号化（**Encryption**）

サーバ接続に使用する暗号化方式。暗号化方式を指定する場合、このフィールドにホスト名を指定する必要があります。

ホスト名**/IP** アドレス（**Hostname/IP Address**）

サーバのホスト名または IP アドレス。

[ポート（Port）]

サーバ接続に使用するポート。

SSL 証明書（**SSL Certificate**）

サーバへの認証に使用する SSL 証明書。SSL 証明書を使用するには、[暗号化（Encryption）] タイプを設定する必要があります。

認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IP アドレス（Hostname/IP Address）] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用し、証明書内で computer1.example.com を使用した場合は、接続が失敗します。

ユーザのダウンロード フィールド

アクセス コントロールのためにダウンロードする（**Download for access control**）

このチェックボックスをオンにすると、ユーザ データの自動ダウンロードが設定されます。ユーザ認識と、状況によっては、ユーザのアクセス コントロールのためにデータを使用できます。

ダウンロードの頻度を設定するには、[自動ダウンロードの開始時間（Begin automatic download at）] および [繰り返し設定（Repeat every）] ドロップダウン メニューを使用します。

基本的なレルム情報の設定

ライセンス：Control

基本的なレルム情報の設定方法：

ステップ **1** [新しいレルムの追加（Add New Realm）] ページで、[名前（Name）] とオプションで [説明（Description）] を入力します。

ステップ **2** ドロップダウン リストから [タイプ（Type）] を選択します。

ステップ **3** AD レルムを設定する場合は、[AD プライマリ ドメイン（AD Primary Domain）] を入力します。

ステップ **4** 取得するユーザ情報に適切な権限を持っているユーザの識別用の [ディレクトリ ユーザ名（Directory Username）] と [ディレクトリ パスワード（Directory Password）] を入力します。

ステップ **5** ディレクトリの [ベース DN（Base DN）] を入力します。

ステップ **6** ディレクトリの [グループ DN（Group DN）] を入力します。

ステップ **7** オプションで、ドロップダウン リストから [グループ属性（Group Attribute）] を選択します。

ステップ **8** [OK] をクリックします。

次の作業

- レルム ディレクトリの設定（29-8 ページ）の説明に従ってレルム ディレクトリを設定します。

レルム ディレクトリの設定

ライセンス:Control

レルム ディレクトリの設定方法:

ステップ 1　[ディレクトリ(Directory)] タブで、[ディレクトリの追加(Add Directory)] をクリックします。

ステップ 2　サーバのホスト名/IP アドレスとポートを入力します。

ステップ 3　暗号化モードを選択します。

ステップ 4　オプションで、ドロップダウン リストから SSL 証明書を選択します。追加アイコン( )をクリックすると、オブジェクトを即座に作成することができます。

ステップ 5　接続をテストする場合は、[テスト(Test)] をクリックします。

ステップ 6　[OK] をクリックします。

次の作業

- オプションで、ユーザの自動ダウンロードの設定(29-8 ページ)の説明に従ってユーザの自動ダウンロードを設定します。

ユーザの自動ダウンロードの設定

ライセンス:Control

含めるグループを指定しなかった場合、ASA FirePOWER モジュールは指定されたパラメータと一致するすべてのグループのユーザ データを取得します。パフォーマンス上の理由から、アクセス コントロールに使用するユーザを表すグループだけを明示的に含めることをお勧めします。

ユーザの自動ダウンロードの設定方法:

ステップ 1　[ユーザのダウンロード(User Download)] タブで、[(ユーザのアクセス コントロールに必要な)ユーザとグループをダウンロードする(Download users and groups (required for user access control))] チェックボックスをオンにします。

ステップ 2　ドロップダウン リストから [自動ダウンロードの開始時間(Begin automatic download at)] の時間を選択します。

ステップ 3　[繰り返し設定(Repeat Every)] ドロップダウン リストからダウンロード間隔を選択します。

ステップ 4　ダウンロードからユーザ グループを含めるか除外するには、[選択可能なグループ(Available Groups)] 列からユーザ グループを選択し、[含めるに追加(Add to Include)] または [除外に追加(Add to Exclude)] をクリックします。

ステップ 5　個々のユーザを含めるか除外するには、[含めるグループ(Groups to Include)] または [除外するグループ(Groups to Exclude)] の下のフィールドにユーザを入力し、[追加(Add)] をクリックします。

(注)　ダウンロードからユーザを除外すると、そのユーザを条件として使用するアクセス コントロール ルールを作成できなくなります。複数のユーザはカンマで区切ります。このフィールドでは、アスタリスク(*)をワイルドカード文字として使用できます。

レルム ユーザ セッション タイムアウトの設定

ライセンス：Control

（注）　予期しない間隔でモジュールがユーザ タイムアウトを実行していることに気付いたら、ユーザ エージェントまたは ISE デバイスの時間が ASA FirePOWER モジュールの時間と同期されていることを確認します。

レルム ユーザ セッション タイムアウトを設定する方法：

ステップ 1　[レルム設定（Realm Configuration）] タブを選択します。

ステップ 2　[認証済みユーザ（Authenticated Users）]、[認証に失敗したユーザ（Failed Authentication Users）]、および [ゲスト ユーザ（Guest Users）] にユーザ セッション タイムアウト値を入力します。

ステップ 3　[保存（Save）] をクリックするか、レルムの編集を続けます。

アイデンティティ ポリシーの設定

ライセンス：Control

はじめる前に

- レルムの作成（29-5 ページ）の説明に従って 1 つ以上のレルムを作成し、有効にします。

アイデンティティ ポリシーの設定方法：

アクセス：Admin/Access Admin/Network Admin

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アイデンティティ ポリシー（Identity Policy）] の順に選択します。

ステップ 2　[名前（Name）] を入力し、任意で [説明（Description）] を入力します。

ステップ 3　ポリシーにルールを追加する場合は、アイデンティティ ルールの作成（29-13 ページ）の説明に従って [ルールの追加（Add Rule）] をクリックします。

ステップ 4　ルール カテゴリを追加する場合は、アイデンティティ ルール カテゴリの追加（29-20 ページ）の説明に従って [カテゴリの追加（Add Category）] をクリックします。

ステップ 5　キャプティブ ポータルを使用するアクティブ認証を設定する場合は、キャプティブ ポータル（アクティブ認証）の設定（29-10 ページ）の説明に従って [アクティブ認証（Active Authentication）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の展開（4-12 ページ）を参照してください。

キャプティブ ポータル(アクティブ認証)フィールド

ライセンス:任意

次のフィールドを使用して、キャプティブ ポータルを設定します。

サーバ証明書(**Server Certificate**)
: キャプティブ ポータル デーモンが示すサーバ証明書。

[ポート(**Port**)**]**
: キャプティブ ポータル接続に使用するポート番号。このフィールドのポート番号は、`captive-portal` CLI コマンドを使用して ASA FirePOWER デバイスで設定したポート番号と一致している必要があります。

最大ログイン試行回数(**Maximum login attempts**)
: ユーザのログイン要求がモジュールによって拒否されるまでに許容されるログイン試行失敗の最大数。

アクティブ認証回答ページ(**Active Authentication Response Page**)
: キャプティブ ポータル ユーザに表示する、ASA FirePOWER モジュールで提供されている、またはカスタムの HTTP 応答ページ。応答ページを表示する場合は、認証タイプとして HTTP 応答ページを使用するアイデンティティ ルールを設定する必要があります。

キャプティブ ポータル(アクティブ認証)の設定

ライセンス:Control

キャプティブ ポータルの詳細については、キャプティブ ポータルのアイデンティティ ソース(30-6 ページ)を参照してください。

はじめる前に

- デバイスが 1 つ以上のASA FirePOWERデバイスをバージョン 9.5(2) 以降を実行しているルーテッド モードで管理していることを確認します。
- キャプティブ ポータルに使用するポート宛てのトラフィックを許可するようにアクセス コントロール ルールを設定します。
- HTTPS トラフィックでキャプティブ ポータルを使用してアクティブ認証を実行する場合は、キャプティブ ポータルを使用して認証するユーザから送信されたトラフィックを復号する SSL ルールを作成する必要があります。
- キャプティブ ポータル接続でトラフィックを復号する場合、キャプティブ ポータルに使用するポート宛てのトラフィックを復号する SSL ルールを作成します。
- `captive-portal` ASA CLI コマンドを使用してアクティブ認証のキャプティブ ポータルを有効にし、『*ASA Firewall Configuration Guide*』(バージョン 9.5(2) 以降)の説明に従ってポートを定義します。
  http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html [英語]。

キャプティブ ポータルの設定方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [アイデンティティ ポリシー(Identity Policy)] を選択し、アイデンティティ ポリシーを編集します。

ステップ 2　[アクティブ認証(Active Authentication)] をクリックします。

ステップ 3　ドロップダウン リストから、該当する [サーバ証明書(Server Certificate)] を選択します。オプションで、追加アイコン( )をクリックしてオブジェクトを即座に作成します。

ステップ 4　[ポート(Port)] を入力し、[最大ログイン試行回数(Maximum login attempts)] を指定します。

ステップ 5　オプションで、HTTP 応答ページでユーザを認証するには、[アクティブ認証回答ページ(Active Authentication Response Page)] を選択します。

ステップ 6　[保存(Save)] をクリックします。

ステップ 7　アイデンティティ ルールの作成(29-13 ページ)の説明に従って [アクション(Action)] として [アクティブ認証(Active Authentication)] を使用するアイデンティティ ルールを設定します。ステップ 5 で応答ページを選択した場合は、[認証タイプ(Authentication Type)] として HTTP 応答ページを選択する必要もあります。

次の作業

- 設定変更を展開します。設定変更の展開(4-12 ページ)を参照してください。

アクティブ認証からのアプリケーションの除外

ライセンス:Control

アプリケーション(HTTP ユーザエージェント文字列によって指定される)を選択し、キャプティブ ポータル(アクティブ認証)から除外することができます。これにより、選択されたアプリケーションからのトラフィックが認証を受けずにアイデンティティ ポリシーを通過できるようになります。

アプリケーションをアクティブ認証から除外する方法:

ステップ 1　アイデンティティ ルール エディタ ページの [レルムおよび設定(Realm & Settings)] タブで、[アプリケーション フィルタ(Application Filters)] リストのシスコ提供のフィルタを使用して、フィルタに追加するアプリケーションのリストを絞り込みます。

- リストを展開および縮小するには、各フィルタ タイプの横にある矢印をクリックします。
- フィルタ タイプを右クリックし、[すべて選択(Check All)] または [すべて選択解除(Uncheck All)] をクリックします。このリストには、各タイプで選択したフィルタ数が示されることに注意してください。
- 表示されるフィルタを絞り込むには、[名前で検索(Search by name)] フィールドに検索文字列を入力します。これは、カテゴリとタグの場合に特に有効です。検索をクリアするには、クリア アイコン( )をクリックします。
- フィルタのリストを更新し、選択したフィルタをすべてクリアするには、リロード アイコン( )をクリックします。
- すべてのフィルタと検索フィールドをクリアするには、[すべてのフィルタをクリア(Clear All Filters)] をクリックします。

（注）　リストには一度に 100 のアプリケーションが表示されます。

ステップ 2　[使用可能なアプリケーション（Available Applications）] リストから、フィルタに追加するアプリケーションを選択します。

- 前の手順で指定した制約を満たすすべてのアプリケーションを追加するには、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] を選択します。
- 表示される個別のアプリケーションを絞り込むには、[名前で検索（Search by name）] フィールドに検索文字列を入力します。検索をクリアするには、クリア アイコン（ ）をクリックします。
- 使用可能な個別のアプリケーションのリストを参照するには、リストの下部にあるページング アイコンを使用します。
- アプリケーションのリストを更新し、選択したアプリケーションをすべてクリアするには、リロード アイコン（ ）をクリックします。

ステップ 3　外部認証から除外する、選択したアプリケーションを追加します。クリックしてドラッグするか、[ルールに追加（Add to Rule）] をクリックできます。結果は次のもので構成されています。

- 選択したアプリケーション フィルタ
- 選択した個別の使用可能なアプリケーション、または [フィルタに一致するすべてのアプリケーション（All apps matching the filter）]

次の作業

- アイデンティティ ルールの作成（29-13 ページ）の説明に従ってアイデンティティ ルールの設定を続けます。

アイデンティティ ポリシーとアクセス コントロール ポリシーの関連付け

ライセンス：Control

ASA FirePOWER モジュールに同時に適用できるアイデンティティ ポリシーは 1 つだけです。アイデンティティ ポリシーを個別に適用することはできません。適用されたアイデンティティ ポリシー、または現在適用されているアイデンティティ ポリシーを削除することはできません。

アイデンティティ ポリシーとアクセス コントロール ポリシーを関連付ける方法：

ステップ 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。

ステップ 2　[詳細設定（Advanced）] タブを選択します。

ステップ 3　[アイデンティティ ポリシーの設定（Identity Policy Settings）] の横にある編集アイコン（ ）をクリックします。

ステップ 4　ドロップダウンからアイデンティティ ポリシーを選択します。

ステップ 5　[OK] をクリックします。

ステップ 6　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックして変更を保存します。

アイデンティティ ルールの作成

ライセンス：Control

アイデンティティ ルールの作成方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アイデンティティ ポリシー（Identity Policy）] の順に選択します。

ステップ 2　[ルールの追加（Add Rule）] をクリックします。

ステップ 3　基本的なアイデンティティ ルール情報の設定（29-14 ページ）の説明に従ってアイデンティティ ルールの基本的な情報を設定します。

ステップ 4　オプションで、アイデンティティ ルールへのゾーン条件の追加（29-16 ページ）の説明に従ってゾーン条件を追加します。

ステップ 5　オプションで、アイデンティティ ルールへのネットワークまたは位置情報条件の追加（29-15 ページ）の説明に従ってネットワークまたは位置情報の条件を追加します。

ステップ 6　オプションで、アイデンティティ ルールへのポート条件の追加（29-15 ページ）の説明に従ってポート条件を追加します。

ステップ 7　アイデンティティ ルールでのレルムの関連付けとアクティブ認証設定の設定（29-16 ページ）の説明に従ってルールをレルムに関連付けます。

ステップ 8　[追加（Add）] をクリックします。

ステップ 9　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の展開（4-12 ページ）を参照してください。

アイデンティティ ルール フィールド

次のフィールドを使用して、アイデンティティ ルールを設定します。

[有効（Enabled）]

このオプションを選択すると、アイデンティティ ポリシーのアイデンティティ ルールが有効になります。このオプションの選択を解除すると、アイデンティティ ルールが無効になります。

[アクション（Action）]

指定されたレルムでユーザに実行する認証のタイプ。パッシブ認証（ユーザ エージェントまたは ISE）、アクティブ認証（キャプティブ ポータル）、または認証なしを選択できます。アイデンティティ ルールのアクションとして選択する前に、認証方式、またはアイデンティティ ソースを完全に設定する必要があります。

レルム

指定されたアクションを実行するユーザが含まれるレルム。アイデンティティ ルールのレルムとして選択する前に、レルムを完全に設定する必要があります。

パッシブ認証でユーザを識別できない場合はアクティブ認証を使用する（**Use active authentication if passive authentication cannot identify user**）

このオプションを選択すると、パッシブ認証でユーザを識別できない場合にアクティブ認証を使用してユーザが認証されます。このオプションを選択するには、アクティブ認証（キャプティブ ポータル）を設定する必要があります。

このオプションを無効にすると、パッシブ認証で識別できないユーザは [不明（Unknown）] と識別されます。このフィールドを表示するには、パッシブ認証に対するルール アクションを設定する必要があります。

認証でユーザを識別できない場合は特別 **ID/**ゲストとして識別する（**Identify as Special Identities/Guest if authentication cannot identify user**）

このオプションを選択すると、ASDM インターフェイスのすべてのエリアで不明ユーザが特別 **ID/**ゲストとして識別されます。このフィールドを表示するには、ルール アクションをアクティブ認証に設定するか、[パッシブ認証でユーザを識別できない場合はアクティブ認証を使用する（Use active authentication if passive authentication cannot identify user）] を選択する必要があります。

認証タイプ（**Authentication Type**）

アクティブ認証を実行するために使用する方法です。選択は、レルム、LDAP、または AD のタイプによって異なります。

- 暗号化されていない HTTP 基本認証（BA）接続を使用してユーザを認証するには、[HTTP 基本（HTTP Basic）] を選択します。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。
- NT LAN Manager（NTLM）接続を使用してユーザを認証する場合は、[NTLM] を選択します。この選択は AD レルムを選択するときにのみ使用できます。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。アイデンティティ ルール認証タイプとして [NTLM] を選択した場合、アイデンティティ ルールのレルムとして Windows Server 2003 を使用することはできません。
- キャプティブ ポータル サーバが認証接続に HTTP 基本認証または NTLM を選択できるようにするには、[HTTP ネゴシエート（HTTP Negotiate）] を選択します。この選択は AD レルムを選択するときにのみ使用できます。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。
- ASA FirePOWER モジュールで提供されている、またはカスタムの HTTP 応答ページを使用してユーザを認証する場合は、[HTTP 応答ページ（HTTP Response Page）] を選択します。ユーザは設定された応答ページを使用してネットワークにログインします。

基本的なアイデンティティ ルール情報の設定

ライセンス：Control

基本的なアイデンティティ ルール情報の設定方法：

ステップ **1**　アイデンティティ ルール エディタ ページで、[名前（Name）] を入力します。

ステップ **2**　ルールを有効にするかどうかを指定します。

ステップ **3**　ルール カテゴリにルールを追加するには、アイデンティティ ルール カテゴリの追加（29-20 ページ）を参照してください。

ステップ **4**　ドロップダウン リストからルールの [アクション（Action）] を選択します。

ステップ **5**　[追加（Add）] をクリックするか、ルールの編集を続けます。

アイデンティティ ルールへのネットワークまたは位置情報条件の追加

ライセンス：Control

アイデンティティ ルールにネットワークまたは位置情報条件を追加する方法：

ステップ 1　アイデンティティ ルール エディタ ページで、[ネットワーク（Networks）] タブを選択します。

ステップ 2　[利用可能なネットワーク（Available Networks）] から、次のように追加するネットワークを見つけます。

- ネットワーク オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[利用可能なネットワーク（Available Networks）] リストの上にある追加アイコン（ ）をクリックします。
- 追加するネットワーク オブジェクトまたは位置情報オブジェクトを検索するには、適切なタブを選択し、[利用可能なネットワーク（Available Networks）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックして、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3　オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ 4　[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。

ステップ 5　手動で指定する送信元または宛先 IP アドレスまたはアドレス ブロックを追加します。[送信元ネットワーク（Source Networks）] リストまたは [宛先ネットワーク（Destination Networks）] リストの下にある [IP アドレスの入力（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 [追加（Add）] をクリックします。

ステップ 6　[追加（Add）] をクリックするか、ルールの編集を続けます。

アイデンティティ ルールへのポート条件の追加

ライセンス：Control

アイデンティティ ルールにポート条件を追加する方法：

ステップ 1　アイデンティティ ルール エディタ ページで、[ポート（Ports）] タブを選択します。

ステップ 2　[利用可能なポート（Available Ports）] から追加する TCP ポートを次のように探します。

- TCP ポート オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[利用可能なポート（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 TCP ベースのポート オブジェクトおよびグループを検索するには、[利用可能なポート（Available Ports）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトのポートの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。たとえば、「443」と入力すると、提供の HTTPS ポート オブジェクトが ASA FirePOWER モジュールに表示されます。

ステップ 3　TCP ベースのポート オブジェクトを 1 つ選択するには、クリックします。TCP ベースのポート オブジェクトをすべて選択するには、右クリックして [すべて選択（Select All）] を選択します。非 TCP ベースのポートを含んでいるオブジェクトは、ポート条件に追加できません。

ステップ 4　[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。

ステップ 5　送信元または宛先のポートを手動で指定するには、[選択した送信元ポート（Selected Source Ports）] または [選択した宛先ポート（Selected Destination Ports）] リストの下にある [ポート（Port）] にポート番号を入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。

ステップ 6　[追加（Add）] をクリックします。

（注）　ASA FirePOWER モジュールでは、無効なポート設定はルール条件に追加されません。

ステップ 7　[追加（Add）] をクリックするか、ルールの編集を続けます。

アイデンティティ ルールへのゾーン条件の追加

ライセンス：Control

アイデンティティ ルールにゾーン条件を追加する方法：

ステップ 1　アイデンティティ ルール エディタ ページで、[ゾーン（Zones）] タブを選択します。

ステップ 2　[利用可能なゾーン（Available Zones）] から追加するゾーンを見つけます。追加するゾーンを検索するには、[利用可能なゾーン（Available Zones）] リストの上にある [名前で検索（Search by name）] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

ステップ 3　クリックすると、ゾーンを選択できます。すべてのゾーンを選択するには、右クリックして [すべて選択（Select All）] を選択します。

ステップ 4　[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。

ステップ 5　[追加（Add）] をクリックするか、ルールの編集を続けます。

アイデンティティ ルールでのレルムの関連付けとアクティブ認証設定の設定

ライセンス：Control

アイデンティティ ルールをレルムに関連付け、オプションで、アクティブ認証の追加設定を設定します。

アイデンティティ ルールをレルムに関連付ける方法：

ステップ 1　アイデンティティ ルール エディタ ページで、[レルムおよび設定（Realm & Settings）] タブを選択します。

ステップ 2　ドロップダウン リストから [レルム（Realm）] を選択します。

ステップ 3　オプションで、[パッシブ認証でユーザを識別できない場合にアクティブ認証を使用（Use active authentication if passive authentication cannot identify user）] チェックボックスをオンにします。このチェックボックスは、パッシブ認証ルールを設定するときにのみ表示されます。

ステップ 4　ステップ 3 でチェックボックスをオンにした場合、またはこれがアクティブ認証ルールである場合、ステップ 4 に進みます。それ以外の場合は、ステップ 8 に進みます。

ステップ 5　オプションで、[認証でユーザを識別できない場合は特別 ID/ゲストとして識別する（Identify as Special Identities/Guest if authentication cannot identify user）] チェックボックスを選択します。

ステップ 6　ドロップダウン リストから [認証タイプ（Authentication Type）] を選択します。

ステップ 7　オプションで、[HTTP ユーザ エージェントの除外（Exclude HTTP User-Agents）] を使用して、アクティブ認証からのアプリケーションの除外（29-11 ページ）の説明に従って特定のアプリケーション トラフィックをアクティブ認証から除外します。

ステップ 8　[追加（Add）] をクリックするか、ルールの編集を続けます。

レルムの管理

ライセンス：Control

レルムの管理方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [統合（Integration）] > [レルム（Realms）] の順に選択します。

ステップ 2　レルムを削除する場合は、削除アイコン（ ）をクリックします。

ステップ 3　レルムを編集する場合は、レルムの横にある編集アイコン（ ）をクリックし、レルムの作成（29-5 ページ）の説明に従って変更を行います。

ステップ 4　レルムを有効または無効にするには、レルムの有効化または無効化（29-18 ページ）の説明に従って、有効または無効にするレルムの横の [状態（State）] スライダをクリックします。

ステップ 5　ユーザとユーザ グループをオンデマンドでダウンロードする場合は、オンデマンドでのユーザとユーザ グループのダウンロード（29-18 ページ）の説明に従って [ダウンロード（Download）] アイコン（ ）をクリックします。

ステップ 6　レルムをコピーする場合は、コピー アイコン（ ）をクリックします。

ステップ 7　レルムを比較する場合は、レルムの比較（29-17 ページ）を参照してください。

レルムの比較

ライセンス：Control

レルムの比較方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [統合（Integration）] > [レルム（Realms）] の順に選択します。

ステップ 2　[レルムの比較（Compare Realms）] をクリックします。

ステップ 3　[比較対象（Compare Against）] ドロップダウン リストから [レルムの比較（Compare Realm）] を選択します。

ステップ 4　[レルム A（Realm A）] および [レルム B（Realm B）] ドロップダウン リストから比較するレルムを選択します。

ステップ 5　[OK] をクリックします。

ステップ 6　個々の変更を選択する場合は、タイトル バーの上の [前へ（Previous）] または [次へ（Next）] をクリックします。

ステップ 7　オプションで、[比較レポート（Comparison Report）] をクリックして、レルム比較レポートを生成します。

ステップ 8　オプションで、[新しい比較（New Comparison）] をクリックして、新しいレルム比較ビューを生成します。

オンデマンドでのユーザとユーザ グループのダウンロード

ライセンス：Control

レルムのユーザ ダウンロード パラメータまたはグループ ダウンロード パラメータを変更する場合、またはサーバでユーザまたはグループを変更して変更をユーザ制御にすぐに反映させる場合は、サーバからのオンデマンド ユーザ ダウンロードの実行を ASA FirePOWER モジュールに強制できます。

ASA FirePOWER モジュールがサーバから取得可能なユーザの最大数はデバイス モデルによって異なります。レルムのダウンロード パラメータの範囲が広すぎる場合、ASA FirePOWER モジュールはできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数をタスク キューで報告します。

はじめる前に

- レルムの有効化または無効化（29-18 ページ）の説明に従い、レルムを有効にします。

ユーザとユーザ グループをオンデマンドでダウンロードする方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [統合（Integration）] > [レルム（Realms）] の順に選択します。

ステップ 2　ユーザとユーザ グループをダウンロードするレルムの横のダウンロード アイコン（ ）をクリックします。

次の作業

- オプションで、タスクのステータスをモニタします。[タスクのステータス（Task Status）] ページ（[モニタリング（Monitoring）] > [ASA FirePOWER モニタリング（ASA FirePOWER Monitoring）] > [タスクのステータス（Task Status）]）を参照してください。

レルムの有効化または無効化

ライセンス：Control

レルムが有効になっていなければ、ASA FirePOWER モジュールがサーバに問い合わせることはできません。クエリーを停止するには、レルムを無効にします。

レルムを有効または無効にする方法:

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [統合（Integration）] > [レルム（Realms）] の順に選択します。

ステップ 2　有効または無効にするレルムの横にある [状態（State）] スライダをクリックします。

次の作業

- オプションで、タスクのステータスをモニタします。[タスクのステータス（Task Status）] ページ（[モニタリング（Monitoring）] > [ASA FirePOWER モニタリング（ASA FirePOWER Monitoring）] > [タスクのステータス（Task Status）]）を参照してください。

アイデンティティ ポリシーの管理

ライセンス：Control

アイデンティティ ポリシーの管理方法:

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アイデンティティ ポリシー（Identity Policy）] の順に選択します。

ステップ 2　ポリシーをコピーする場合は、コピー アイコン（  ）をクリックします。

ステップ 3　ポリシーのレポートを生成する場合は、レポート アイコン（  ）をクリックします。

アイデンティティ ルールの管理

ライセンス：Control

アイデンティティ ルールを管理する方法:

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アイデンティティ ポリシー（Identity Policy）] の順に選択します。

ステップ 2　アイデンティティ ルールを編集する場合は、編集アイコン（  ）をクリックし、アイデンティティ ルールの作成（29-13 ページ）の説明に従って変更を行います。

ステップ 3　アイデンティティ ルールを削除する場合は、削除アイコン（  ）をクリックします。

ステップ 4　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の展開（4-12 ページ）を参照してください。

アイデンティティ ルール カテゴリの追加

ライセンス:Control

アイデンティティ ルール カテゴリを追加する方法:

ステップ **1** アイデンティティ ルール エディタ ページでは、次の選択肢があります。

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

ステップ **2** [OK] をクリックします。

(注)　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。

ステップ **3** [追加(Add)] をクリックするか、ルールの編集を続けます。

ユーザ アイデンティティ ソース

ASA FirePOWER モジュールは、次のアイデンティティ ソースをサポートしています。

- 権限のあるユーザ エージェント レポートは、ユーザ認識とユーザ アクセス コントロールに関するユーザ データを収集します。ホストにログインまたはホストからログアウトするとき、または Active Directory クレデンシャルで認証するときにユーザをモニタするようにユーザ エージェントを設定するには、ユーザ エージェントのアイデンティティ ソース（30-2 ページ）を参照してください。
- 権限のある *Identity Services Engine*（*ISE*）レポートは、ユーザ認識とユーザ アクセス コントロールに関するユーザ データを収集します。ISE が展開されていて、Active Directory ドメイン コントローラ（DC）を使用した認証時にユーザをモニタするように ISE を設定する場合は、Identity Services Engine（ISE）のアイデンティティ ソース（30-4 ページ）を参照してください。
- 権限のあるキャプティブ ポータル認証はアクティブにネットワークのユーザを認証し、ユーザ認識とユーザ制御に関するユーザ データを収集します。キャプティブ ポータル認証を実行するために仮想ルータまたは FirePOWER Threat Defense デバイスを設定する場合は、キャプティブ ポータルのアイデンティティ ソース（30-6 ページ）を参照してください。

これらのアイデンティティ ソースからのデータは、ASA FirePOWER モジュール ユーザ データベースおよびユーザ アクティビティ データベースに保存されます。データベース サーバ クエリーを設定すると、モジュールに新しいデータを自動的にダウンロードすることができます。

ASA FirePOWER モジュールでのユーザ検出の詳細については、ユーザ検出の基礎（28-1 ページ）を参照してください。

ユーザ アイデンティティ ソースに関する問題のトラブルシューティング

ライセンス：任意

ユーザ アイデンティティ ソースに関する問題のトラブルシューティングについては、次の各項を参照してください。

ユーザ エージェント

ユーザ エージェントの接続に関する問題が発生した場合は、『*FirePOWER User Agent Configuration Guide*』を参照してください。

ユーザ エージェントによって報告されるユーザ データに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにないユーザ エージェント ユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。状況によっては、システムが Active Directory サーバからこの情報を正常に取得するために 60 分かかることもあります。データ取得が成功するまで、ユーザ エージェント ユーザから見えるアクティビティはアクセス コントロール ルールで処理され、Web インターフェイスに表示されません。

ISE

ISE 接続に問題が起こった場合は、次のことを確認してください。

- ISE と FirePOWER システムを正常に統合するには、ISE 内の pxGrid アイデンティティ マッピング機能を有効にする必要があります。
- すべての ISE システム証明書と FirePOWER Management Center 証明書には、**serverAuth** と **clientAuth** 拡張キー使用値が含まれている必要があります。
- ISE デバイスの時間は、FirePOWER Management Center の時間と同期されている必要があります。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。
- 展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。
- 展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

ISE によって報告されるユーザ データに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにない ISE ユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。状況によっては、システムが Active Directory サーバからこの情報を正常に取得するために 60 分かかることもあります。データ取得が成功するまで、ISE ユーザから見えるアクティビティはアクセス コントロール ルールで処理され、Web インターフェイスに表示されません。

キャプティブ ポータル

キャプティブ ポータル認証に関する問題が発生した場合は、次の点に注意してください。

- キャプティブ ポータル ユーザがログイン クレデンシャルを入力すると、システムはクレデンシャルをサーバのデータに対して確認します。状況によっては、ユーザ データがまだデータベースにない場合、Active Directory サーバからこの情報を正常に取得するために 60 分かかることもあります。データ取得が成功するまで、キャプティブ ポータル ユーザは認証されません。

  キャプティブ ポータル ユーザが 25 秒後に認証されていない場合、エラー メッセージが表示され、キャプティブ ポータル ユーザのセッションがタイムアウトします。ユーザはキャプティブ ポータルのログインを再試行する必要があります。

ユーザ エージェントのアイデンティティ ソース

ライセンス:任意

ユーザ エージェントはパッシブな認証方法であり、ASA FirePOWER モジュールでサポートされる権限のあるアイデンティティ ソースの 1 つです。ASA FirePOWER モジュールと統合すると、エージェントは、ホストにログインまたはホストからログアウトするとき、または Active Directory クレデンシャルで認証するときにユーザをモニタします。ユーザ エージェントは失敗したログイン試行を報告しません。ユーザ エージェントから取得されたデータは、ユーザ認識とユーザ制御に使用できます。パッシブ認証はアイデンティティ ポリシーで呼び出します。

ユーザ エージェントをインストールして使用することで、ユーザ制御を実行できます。つまり、エージェントがユーザと IP アドレスを関連付け、これによりユーザの条件によるアクセス コントロール ルールをトリガーできるようになります。1 つのエージェントを使用して、最大 5 つの Active Directory サーバでユーザ アクティビティをモニタできます。

ユーザ エージェントは段階的な設定が必要であり、以下が含まれます。

- エージェントがインストールされたコンピュータまたはサーバ。
- ASA FirePOWER モジュールとエージェントがインストールされたコンピュータまたは Active Directory サーバとの間の接続。
- ASA FirePOWER モジュールとアイデンティティ レルム内のディレクトリとして設定されたモニタ対象 LDAP サーバとの間の接続。

エージェントは、以下を実行しているコンピュータまたはサーバにインストールできます。

- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2012

コンピュータはまた、モニタする Microsoft Active Directory サーバとデバイスに TCP/IP アクセスできる必要があります。また、サポートされるいずれかのオペレーティング システムを実行する Active Directory サーバにエージェントをインストールすることもできます。リアルタイム データの取得を実行する場合、サーバは Windows Server 2008 または Windows Server 2012 を実行している必要があります。

段階的なユーザ エージェントの設定とサーバの要件の詳細については、『*User Agent Configuration Guide*』を参照してください。

ASA FirePOWER モジュール接続は、ログインとログオフがユーザ エージェントによって検出されたユーザのメタデータを取得可能にするだけでなく、アクセス コントロール ルール内で使用するユーザとグループを指定するためにも使用されます。エージェントが特定のユーザ名を除外するように設定されている場合は、そのようなユーザ名のログイン データは ASA FirePOWER モジュールに報告されません。ユーザ エージェント データは、デバイスのユーザ データベースとユーザ アクティビティ データベースに保存されます。

（注）　ユーザ エージェントは $ 記号で終わる Active Directory ユーザ名を ASA FirePOWER モジュールに送信できません。これらのユーザをモニタする場合は、最後の $ の文字を削除する必要があります。

複数のユーザがリモート セッションを使用してホストにログインしている場合は、エージェントがそのホストからのログインを正確に検出しない場合があります。これを防ぐ方法については、『*User Agent Configuration Guide*』を参照してください。

ユーザ エージェント接続の設定

ライセンス：Control

はじめる前に

- ユーザ アクセス コントロールを実装する場合は、レルムの作成（29-5 ページ）の説明に従ってユーザ エージェント接続用の Active Directory レルムを設定して有効にします。

ユーザ エージェント接続の設定方法:

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [統合（Integration）] > [アイデンティティ ソース（Identity Sources）] の順に選択します。

ステップ 2　[サービス タイプ（Service Type）] に [ユーザ エージェント（User Agent）] を選択し、ユーザ エージェント接続を有効にします。

（注）　接続を無効にするには、[なし（None）] を選択します。

ステップ 3　[新規エージェントの追加（Add New Agent）] ボタンをクリックして新しいエージェントを追加します。

ステップ 4　エージェントをインストールするコンピュータの [ホスト名（Hostname）] または [アドレス（Address）] を入力します。IPv4 アドレスを使用する必要があります。IPv6 アドレスを使用してユーザ エージェントに接続するように ASA FirePOWER モジュールを設定することはできません。

ステップ 5　[追加（Add）] をクリックします。

ステップ 6　接続を削除するには、削除アイコン（ ）をクリックして、その削除を確認します。

次の作業

- 『*FirePOWER User Agent Configuration Guide*』で説明されているユーザ エージェントの設定を続行します。

Identity Services Engine（ISE）のアイデンティティ ソース

ライセンス:任意

Cisco Identity Services Engine（ISE）内の pxGrid アイデンティティ マッピング機能はパッシブな認証方法であり、ASA FirePOWER モジュールでサポートされる権限のあるアイデンティティ ソースの 1 つです。ASA FirePOWER モジュールと統合すると、この ISE 機能によって、Active Directory ドメイン コントローラ（DC）を使用した認証時にユーザをモニタします。ISE は失敗したログイン試行を報告しません。ISE から取得されたデータは、ASA FirePOWER モジュールでユーザ認識とユーザ制御に使用できます。パッシブ認証はアイデンティティ ポリシーで呼び出します。

注意　多数のユーザ グループをモニタするように ISE を設定する場合、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、レルムまたはユーザ条件を使用するアクセス コントロール ルールが想定どおりに適用されない可能性があります。

（注）　ISE デバイスの時間が ASA FirePOWER モジュールの時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。

また、ISE 接続を設定すると、ASA FirePOWER モジュールのデータベースに ISE 属性データとして、[セキュリティ グループ タグ（SGT）（Security Group Tag (SGT)）]、[エンドポイント プロファイル（Endpoint Profile）]、および [エンドポイント ロケーション（Endpoint Location）] が入力されます。ISE 属性は、ユーザ認識とアクセス コントロール ルールの条件に使用できます。

セキュリティ グループ タグ（**SGT**）（**Security Group Tag (SGT)**）

SGT 属性は、パケットが信頼できる TrustSec ネットワークに入るときに Cisco TrustSec によって適用されます。ISE を設定すると、モジュールはユーザとその SGT を識別します。これはアクセス コントロールに使用できます。

エンドポイント ロケーション（**Endpoint Location**）

[エンドポイント ロケーション（Endpoint Location）] 属性は Cisco ISE によって適用され、エンドポイント デバイスの IP アドレスを特定します。

エンドポイント プロファイル（**Endpoint Profile**）

[エンドポイント プロファイル（Endpoint Profile）] 属性は Cisco ISE によって適用され、各パケットのエンドポイント デバイス タイプを特定します。

Cisco ISE 製品の詳細については、『*Cisco Identity Services Engine Administrator Guide*』を参照してください。

ISE フィールド

次のフィールドを使用して ISE への接続を設定します。

プライマリおよびセカンダリ ホスト名/**IP** アドレス（**Primary and Secondary Host Name/IP Address**）

プライマリ（およびオプションでセカンダリ）ISE サーバのホスト名または IP アドレス。

pxGrid サーバ **CA**（**pxGrid Server CA**）

pxGrid フレームワークの認証局。展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

MNT サーバ **CA**（**MNT Server CA**）

一括ダウンロード実行時の ISE 証明書の認証局。展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

MC サーバ証明書（**MC Server Certificate**）

ISE への接続時、または一括ダウンロードの実行時に ASA FirePOWER モジュールが ISE に提供する必要がある証明書およびキー。

ISE ネットワーク フィルタ（**ISE Network Filter**）

ISE がモニタするネットワークを制限するために設定できるオプション フィルタ。フィルタを指定する場合、ISE はそのフィルタ内のネットワークをモニタします。次の方法でフィルタを指定できます。

- すべて指定する場合はフィールドを空白のままにします。
- CIDR 表記を使用して単一の IPv4 アドレス ブロックを入力します。
- CIDR 表記を使用して IPv4 アドレス ブロックのリストをカンマで区切って入力します。

ISE 接続の設定

ライセンス:Control

ユーザ エージェント接続の設定方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [統合(Integration)] > [アイデンティティ ソース(Identity Sources)] の順に選択します。

ステップ 2　[サービス タイプ(Service Type)] に [Identity Services Engine] を選択し、ISE 接続を有効にします。

(注)　接続を無効にするには、[なし(None)] を選択します。

ステップ 3　[プライマリ ホスト名/IP アドレス(Primary Host Name/IP Address)] と、オプションで [セカンダリ ホスト名/IP アドレス(Secondary Host Name/IP Address)] を入力します。

ステップ 4　[pxGrid サーバ CA(pxGrid Server CA)]、[MNT サーバ CA(MNT Server CA)]、および [MC サーバ証明書(MC Server Certificate)] ドロップダウンリストから適切な証明書を選択します。オプションで、追加アイコン( )をクリックしてオブジェクトを即座に作成します。

ステップ 5　オプションで、CIDR ブロック表記を使用して **ISE** ネットワーク フィルタを入力します。

ステップ 6　接続をテストする場合は、[テスト(Test)] をクリックします。

キャプティブ ポータルのアイデンティティ ソース

ライセンス:任意

キャプティブ ポータルは、ASA FirePOWER モジュールでサポートされる権限のあるアイデンティティ ソースの 1 つです。ASA FirePOWER モジュールでサポートされる唯一のアクティブな認証方式であり、ユーザはデバイスを通じてネットワークに認証できます。

キャプティブ ポータル経由のアクティブ認証は、HTTP および HTTPS トラフィックのみで実行されます。HTTPS トラフィックでキャプティブ ポータルを実行する場合は、キャプティブ ポータルを使用して認証するユーザから送信されたトラフィックを復号する SSL ルールを作成する必要があります。

設定して展開すると、指定レルムのユーザはバージョン 9.5(2) 以降を実行しているルーテッド モードの ASA FirePOWER デバイス経由で認証されます。キャプティブ ポータルから取得された認証データはユーザ認識とユーザ制御に使用できます。

キャプティブ ポータルはまた、失敗した認証の試行を記録します。失敗した試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。キャプティブ ポータルで報告される失敗した認証アクティビティのユーザ アクティビティ タイプは [認証失敗ユーザ(Failed Auth User)] です。

`captive-portal` ASA CLI コマンドを使用して、使用バージョンの『*ASA Firewall Configuration Guide*』の説明に従ってキャプティブ ポータルのアクティブ認証を有効にします(http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html [英語])。アイデンティティ ポリシーのキャプティブ ポータルの設定を続け、アイデンティティ ルールのアクティブ認証を呼び出します。アイデンティティ ポリシーはアクセス コントロール ポリシーで呼び出されます。詳細については、キャプティブ ポータル(アクティブ認証)の設定(29-10 ページ)を参照してください。

キャプティブ ポータルは、設定された 1 つ以上のルーテッド インターフェイスを使用してデバイスによってのみ実行できます。

アクセス コントロール ルールおよび SSL ルールの次の要件に注意してください。

- キャプティブ ポータルに使用する IP アドレスおよびポート宛てのトラフィックを許可するようにアクセス コントロール ルールを設定する必要があります。宛先ポートがアクセス コントロール ポリシーで許可されない場合、トラフィックはキャプティブ ポータルを使用して認証できません。
- HTTPS トラフィックでキャプティブ ポータルを使用してアクティブ認証を実行する場合は、キャプティブ ポータルを使用して認証するユーザから送信されたトラフィックを復号する SSL ルールを作成する必要があります。
- キャプティブ ポータル接続でトラフィックを復号する場合、キャプティブ ポータルに使用するポート宛てのトラフィックを復号する SSL ルールを作成する必要があります。

ASA FirePOWER モジュール サーバのダウンロード

ライセンス:任意

ASA FirePOWER モジュールと LDAP または AD サーバ間の接続により、次の特定の検出されたユーザのユーザおよびユーザ グループのメタデータを取得することができます。

- キャプティブ ポータルで認証された、あるいはユーザ エージェントまたは ISE で報告された LDAP および AD ユーザ。このメタデータは、ユーザ認識とユーザ制御に使用できます。
- トラフィック ベースの検出で検出された POP3 と IMAP ユーザ ログイン（ユーザが LDAP または AD ユーザと同じ電子メール アドレスを持つ場合）。このメタデータは、ユーザ認識に使用できます。

ASA FirePOWER モジュール ユーザ データベース サーバ接続はレルム内のディレクトリとして設定します。ユーザ認識とユーザ制御のためにレルムのユーザおよびユーザ グループ データをダウンロードするには、[アクセス コントロールのためのユーザおよびユーザ グループのダウンロード（Download users and user groups for access control）] チェックボックスをオンにする必要があります。

ASA FirePOWER モジュールは、ユーザごとに次の情報とメタデータを取得します。

- LDAP ユーザ名
- 姓と名
- 電子メール アドレス
- 部署
- 電話番号

DNS ポリシー

次のトピックでは、DNS ポリシー、DNS ルール、および DNS ポリシーを導入する方法について説明します。

DNS ポリシーの概要

ライセンス：任意

DNS ベースのセキュリティ インテリジェンスにより、クライアントが要求したドメイン名に基づいて、トラフィックをホワイトリスト/ブラックリストに登録できるようになります。シスコが提供するドメイン名のインテリジェンスを使用して、トラフィックをフィルタリングできます。また、環境に合わせて、ドメイン名のカスタム リストやフィードを設定することも可能です。DNS ベースのセキュリティ インテリジェンスによるフィルタリングが実行されるタイミングは、ハードウェアレベルの処理およびトラフィックの復号が行われた後で、かつ、他のほとんどのポリシーベースのインスペクション、分析、トラフィック処理が行われる前です。

DNS ポリシーによってブラックリスト登録されたトラフィックは即座にブロックされるため、他のさらなるインスペクションの対象にはなりません（侵入、エクスプロイト、マルウェアなどについて）。ブラックリストをホワイトリストで上書きしてアクセス コントロール ルールによる評価を強制することができます。また、セキュリティ インテリジェンス フィルタリングに「モニタ専用」設定を使用でき、パッシブ展開環境ではこの設定が推奨されます。この設定では、ブラックリスト登録されたであろう接続を ASA FirePOWER モジュールが分析できるだけでなく、ブラックリストに一致する接続がログに記録され、接続終了セキュリティ インテリジェンス イベントが生成されます。

DNS ポリシーおよび関連付けられた DNS ルールを使用して DNS ベースのセキュリティ インテリジェンスを設定します。これを導入するには、アクセス コントロール ポリシーに DNS ポリシーを関連付けてから設定を導入する必要があります。

DNS ポリシーのコンポーネント

ライセンス：任意

DNS ポリシーにより、ドメイン名ベースの接続をホワイトリストまたはブラックリストに登録できるようになります。次のリストに、DNS ポリシーの作成後に変更可能な設定を示します。

名前（**Name**）と説明（**Description**）

各 DNS ポリシーには固有の名前が必要です。説明は任意です。

ルール（**Rule**）

ルールは、ドメイン名に基づいてネットワーク トラフィックを処理する詳細な方法を提供します。DNS ポリシーのルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルール番号の昇順で、DNS ルールを上から順にトラフィックと照合します。

DNS ポリシーを作成すると、ASA FirePOWER モジュールはこれをデフォルトのグローバル DNS ホワイトリスト ルールおよびデフォルトのグローバル DNS ブラックリスト ルールに入力します。各ルールは、それぞれのカテゴリの先頭に固定されます。これらのルールは変更できませんが無効にすることはできます。ルールはモジュールにより次の順序で評価されます。

- グローバル DNS ホワイトリスト ルール（有効な場合）
- ホワイトリスト ルール
- グローバル DNS ブラックリスト ルール（有効な場合）
- ブラックリスト ルールおよびモニタ ルール

通常、モジュールによるドメイン名ベースのネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。トラフィックに一致する DNS ルールがない場合、モジュールは、関連付けられたアクセス コントロール ポリシー ルールに基づいてトラフィックの評価を続行します。DNS ルール条件は単純または複雑のどちらでも構いません。

DNS ポリシーの編集

ライセンス：Protection

DNS ポリシーの編集は、1 つのブラウザ ウィンドウを使用して、一度に 1 人のみで行う必要があります。複数のユーザが同じポリシーを保存を試みた場合、最初に保存された一連の変更だけが保持されます。

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 30 分間操作が行われないと警告が表示されます。60 分後には、モジュールにより変更が破棄されます。

DNS ポリシーを編集する方法：

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [DNS ポリシー（DNS Policy）] の順に選択します。

ステップ **2**　DNS ポリシーを編集します。

- 名前（Name）と説明（Description）：名前または説明を変更するには、該当のフィールドをクリックし、新しい情報を入力します。
- ルール（Rules）：DNS ルールを追加、分類、有効化、無効化、または管理するには、[ルール（Rules）] タブをクリックし、DNS ルールの作成と編集（31-3 ページ）の説明に従って進みます。

ステップ **3**　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の展開（4-12 ページ）を参照してください。

DNS ルール

ライセンス:任意

DNS ルールは、ホストが要求するドメイン名に基づいてトラフィックを処理します。セキュリティ インテリジェンスの一部として、この評価は、トラフィックの復号の後、アクセス コントロール評価の前に適用されます。

ASA FirePOWER モジュールは指定した順序で DNS ルールをトラフィックと照合します。ほとんどの場合、モジュールによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。DNS ルールを作成すると、モジュールは、モニタ ルールとブラックリスト ルールの前にホワイトリスト ルールを配置し、最初にホワイトリスト ルールに対してトラフィックを評価します。

各 DNS ルールには、一意の名前以外にも、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、ASA FirePOWER モジュールはネットワーク 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**)

DNS ポリシーのルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルール番号の昇順で、ルールを上から順に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。DNS ルールには、DNS フィードまたはリスト条件が含まれている必要があり、セキュリティ ゾーンまたはネットワークによってトラフィックと照合することができます。

アクション(**Action**)

ルールのアクションによって、一致するトラフィックを ASA FirePOWER モジュールがどのように処理するかが決まります。

- ホワイトリストに登録されたトラフィックは許可され、アクセス コントロールによるさらなるインスペクションの対象になります。
- モニタ対象のトラフィックは、残りの DNS ブラックリスト ルールにより、さらなる評価の対象となります。DNS ブラックリスト ルールに一致しないトラフィックは、アクセス コントロール ルールに検査されます。そのトラフィックのセキュリティ インテリジェンス イベントは、モジュールにより記録されます。
- ブラックリストに登録されたトラフィックは、追加のインスペクションなしでドロップされます。[検出されないドメイン(Domain Not Found)] 応答を返すか、シンクホール サーバに DNS クエリをリダイレクトすることもできます。

DNS ルールの作成と編集

ライセンス:Protection

DNS ポリシーでは、ホワイトリスト ルールおよびブラックリスト ルールに最大で合計 32767 の DNS リストを追加できます。つまり、DNS ポリシー リストの数は 32767 を超えることができません。

DNS ルールを作成および編集する方法:

ステップ **1** [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [DNS ポリシー(DNS Policy)] の順に選択します。

ステップ **2** 次の選択肢があります。

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

ステップ **3** 名前を入力します。

ステップ **4** 以下のルール コンポーネントを設定するか、デフォルトを受け入れます。

- アクション(Action):ルールのアクションを選択します。DNS ルールのアクション(31-5 ページ)を参照してください。
- 条件(Conditions):ルールの条件を設定します。DNS ルールの条件(31-6 ページ)を参照してください。
- 有効(Enabled):ルールを有効にするかどうかを指定します。

ステップ **5** [追加(Add)] または [OK] をクリックします。

ステップ **6** [ASA FirePOWER の変更の保存(Store ASA FirePOWER Changes)] をクリックします。

DNS ルールの管理

ライセンス:任意

DNS ポリシー エディタの [ルール(Rules)] タブでは、ポリシー内の DNS ルールの追加、編集、移動、有効化、無効化、削除、その他の管理が行えます。

各ルールについて、ポリシー エディタでは、その名前、条件のサマリー、およびルール アクションが表示されます。他のアイコンにより、警告( )、エラー( )、その他の重要な情報( )が示されます。無効なルールはグレー表示され、ルール名の下に [無効(disabled)] というマークが付きます。

DNS ルールの有効化と無効化

ライセンス:Protection

作成した DNS ルールは、デフォルトで有効になっています。ルールを無効にすると、ASA FirePOWER モジュールはネットワーク 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。DNS ポリシーのルール リストを表示すると、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、DNS ルール エディタを使用して DNS ルールを有効または無効にできることに注意してください。

DNS ルールを有効または無効にする方法:

ステップ **1** [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [DNS ポリシー(DNS Policy)] の順に選択します。

ステップ **2** 有効または無効にするルールを含む DNS 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。

ステップ **3** [OK] をクリックします。

ステップ 4　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の展開（4-12 ページ）を参照してください。

DNS ルールの評価順序

ライセンス：任意

DNS ポリシーのルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルール番号の昇順で、DNS ルールを上から順にトラフィックと照合します。ほとんどの場合、モジュールによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。

- モニタ ルールでは、モジュールはまずトラフィックを記録し、その後、優先順位の低い DNS ブラックリスト ルールに対してトラフィックを評価を続行します。
- モニタ ルール以外では、トラフィックがルールに一致した後、モジュールは優先順位の低い追加の DNS ルールに対してトラフィックの評価は続行しません。

ルールの順序については、以下の点い注意してください。

- グローバル ホワイトリストは常に先頭で、他のすべてのルールよりも優先されます。
- ホワイトリスト セクションはブラックリスト セクションよりも優先され、ホワイトリスト ルールは常に他のルールよりも優先されます。
- グローバル ブラックリストは常にブラックリスト セクションの先頭で、他のモニタ ルールおよびとブラックリスト ルールよりも優先されます。
- ブラックリスト セクションには、モニタ ルールおよびブラックリスト ルールが含まれます。
- 初めて DNS ルールを作成したときは、ホワイトリスト アクションを割り当てるとそれはモジュールによりホワイトリスト セクションの最後に配置され、他のアクションを割り当てるとブラックリスト セクションの最後に配置されます。

ルールをドラッグ アンド ドロップして順序を変えて、評価の順序を変更することができます。

DNS ルールのアクション

ライセンス：任意

すべての DNS 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：まずルール アクションは、モジュールがルールの条件に一致するトラフィックをホワイトリスト登録、モニタ、またはブラックリスト登録するかどうかを制御します。
- 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。

インラインで展開されたデバイスのみがトラフィックをブラックリスト登録できることに留意してください。パッシブに展開されたデバイスは、トラフィックをホワイトリスト登録およびロギングできますが、トラフィックに影響を与えることはできません。

ホワイトリスト アクション

ホワイトリスト 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。トラフィックをホワイトリスト登録すると、そのトラフィックは、照合するアクセス コントロール ルール、またはアクセス コントロール ポリシーのデフォルト アクションによるさらなるインスペクションの対象になります。

モジュールは、ホワイトリストの一致はロギングしません。ただし、ホワイトリストに登録された接続のロギングは、接続の最終的な傾向によって異なります。

[モニタ（Monitor）] アクション

[モニタ（Monitor）] 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ホワイトリスト登録されたりブラックリスト登録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 DNS ルールが、モジュールがトラフィックをブラックリスト登録するかどうかを決定します。一致する追加のルールがなければ、トラフィックはアクセス コントロール評価の対象となります。

DNS ポリシーによってモニタされる接続については、ASA FirePOWER モジュールは、接続終了セキュリティ インテリジェンスと接続イベントをロギングします。

[ブラックリスト（Blacklist）] アクション

[ブラックリスト（Blacklist）] アクションは、いかなる種類のインスペクションなしで、トラフィックをブラックリスト登録します。

- [ドロップ（Drop）] アクションはトラフィックをドロップします。
- [検出されないドメイン（Domain Not Found）] アクションは、存在しないインターネット ドメインの応答を DNS クエリに返し、これによりクライアントが DNS 要求を解決することを防ぎます。
- [シンクホール（Sinkhole）] アクションは、応答内のシンクホール オブジェクトの IPv4 または IPv6 アドレスを DNS クエリに返します。シンクホール サーバは、IP アドレスへの後続の接続をロギングするか、またはロギングしてブロックすることができます。[シンクホール（Sinkhole）] アクションを設定する場合、シンクホール オブジェクトも設定する必要があります。

[ドロップ（Drop）] または [検出されないドメイン（Domain Not Found）] アクションに基づいてブラックリスト登録された接続については、モジュールは接続開始セキュリティ インテリジェンス イベントと接続イベントをロギングします。ブラックリスト登録されたトラフィックは追加のインスペクションなしですぐに拒否されるため、ログに記録できる固有の接続の終了イベントはありません。

[シンクホール（Sinkhole）] アクションに基づいてブラックリスト登録された接続については、ロギングはシンクホール オブジェクト設定によって異なります。シンクホール オブジェクトを、シンクホール接続をロギングのみするよう設定している場合、モジュールは、後続の接続の接続終了イベントをロギングします。シンクホール オブジェクトを、シンクホール接続をロギングしてブロックするよう設定している場合、モジュールは、後続の接続の接続開始イベントをロギングし、その後、その接続をブロックします。

DNS ルールの条件

ライセンス：任意

DNS 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。条件は単純または複雑のどちらでも構いません。DNS フィードまたはリスト条件を定義する必要があります。さらに、セキュリティ ゾーンまたはネットワークによってトラフィックを制御できます。

DNS ルールに条件を追加するときは、以下に留意してください。

- ルールに対し特定の条件を設定しない場合、モジュールはその基準に基づいてトラフィックを照合しません。
- 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。
- 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、単一ルールを使用して、最大 50 の DNS リストおよびフィードに基づいてトラフィックをブラックリスト登録できます。

DNS およびセキュリティ ゾーンに基づくトラフィックの制御

ライセンス：Protection

DNS ルール内のゾーン条件によって、その送信元および宛先セキュリティ ゾーン別にトラフィックを制御することができます。セキュリティ ゾーンは、1 つ以上のインターフェイスのグループです。検出モードと呼ばれる、デバイスの初期セットアップ時に選択するオプションによって、モジュールが最初にデバイスのインターフェイスをどのように設定するか、およびこれらのインターフェイスがセキュリティ ゾーンに属するかどうかが決定します。

DNS およびセキュリティ ゾーンに基づいてトラフィックを制御する方法：

ステップ **1**　DNS ルール エディタで、[ゾーン（Zones）] タブをクリックします。

ステップ **2**　[利用可能なゾーン（Available Zones）] から追加するゾーンを見つけて選択します。追加するゾーンを検索するには、[利用可能なゾーン（Available Zones）] リストの上にある [名前で検索（Search by name）] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

ステップ **3**　クリックして 1 つのゾーンを選択するか、右クリックして [すべて選択（Select All）] を選択します。

ステップ **4**　[送信元に追加（Add to Source）] をクリックします。

ヒント　選択したゾーンをドラッグ アンド ドロップすることもできます。

ステップ **5**　ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の展開（4-12 ページ）を参照してください。

DNS およびネットワークに基づくトラフィックの制御

ライセンス：Protection

DNS ルール内のネットワーク条件によって、その送信元 IP アドレス別にトラフィックを制御することができます。制御するトラフィックに対し、明示的に送信元 IP アドレスを指定できます。

DNS およびネットワークに基づいてトラフィックを制御する方法：

ステップ **1**　DNS ルール エディタで、[ネットワーク（Networks）] タブをクリックします。

ステップ **2**　[利用可能なネットワーク（Available Networks）] から、次のように追加するネットワークを見つけて選択します。

- ここでネットワーク オブジェクトを追加するには（後で条件に追加できます）、[利用可能なネットワーク（Available Networks）] リストの上にある追加アイコン（ ）をクリックし、ネットワーク オブジェクトの操作（2-4 ページ）の説明に従って進みます。
- 追加するネットワーク オブジェクトを検索するには、[利用可能なネットワーク（Available Networks）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3　[送信元に追加（Add to Source）] をクリックします。

ヒント　選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 4　手動で指定する送信元 IP アドレスまたはアドレス ブロックを追加します。[送信元ネットワーク（Source Networks）] リストの下にある [IP アドレスの入力（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 [追加（Add）] をクリックします。

ステップ 5　ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の展開（4-12 ページ）を参照してください。

DNS リスト、フィード、またはカテゴリに基づくトラフィックの制御

ライセンス：Protection

DNS リスト、フィード、またはカテゴリがクライアントから要求されたドメイン名を含む場合、DNS ルール内の DNS 条件によりトラフィックを制御することができます。DNS ルール内の DNS 条件を定義する必要があります。

グローバルまたはカスタムのホワイトリストまたはブラックリストを DNS 条件に追加するかどうかに関わらず、ASA FirePOWER モジュールは設定されたルール アクションをトラフィックに適用します。たとえばルールにグローバル ホワイトリストを追加し、[ドロップ（Drop）] アクションを設定すると、モジュールはホワイトリスト登録されている必要があるすべてのトラフィックをブラックリスト登録します。

DNS リスト、フィード、またはカテゴリに基づいてトラフィックを制御する方法：

ステップ 1　DNS ルール エディタで、[DNS] タブをクリックします。

ステップ 2　次のように、[DNS リストおよびフィード（DNS Lists and Feeds）] から追加する DNS リストおよびフィードを検索して選択します。

- ここで DNS リストまたはフィードを追加するには（後で条件に追加できます）、[DNS リストおよびフィード（DNS Lists and Feeds）] リストの上にある追加アイコン（ ）をクリックし、インテリジェンス フィードの操作（2-7 ページ）の説明に従って進みます。
- 追加する DNS リスト、フィード、またはカテゴリを検索するには、[DNS リストおよびフィード（DNS Lists and Feeds）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3　[ルールに追加（Add to Rule）] をクリックします。

ヒント　選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 4　ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の展開（4-12 ページ）を参照してください。

DNS ポリシーの導入

ライセンス:任意

DNS ポリシー設定は、更新を終了した後、変更を有効にするためにアクセス コントロール ポリシーの一部として導入する必要があります。次の手順を実行する必要があります。

- セキュリティ インテリジェンスのホワイトリストおよびブラックリストの作成（5-4 ページ）で説明されているように、DNS ポリシーをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します。設定変更の展開（4-12 ページ）を参照してください。

マルウェアと禁止されたファイルのブロッキング

悪意のあるソフトウェア、つまりマルウェアは、複数のルートで組織のネットワークに入る可能性があります。マルウェアの影響を特定して軽減するために、ASA FirePOWER モジュールのファイル制御、および高度なマルウェア防御の各コンポーネントを使用すると、マルウェアやその他の種類のファイルがネットワーク トラフィックで伝送されるのを検出、追跡、保存、分析、および任意でブロックすることができます。

全体的なアクセス コントロール設定の一部として、マルウェア防御とファイル制御を実行するようにシステムを設定できます。作成してアクセス コントロール ルールに関連付けたファイル ポリシーは、ルールに一致するネットワーク トラフィックを処理します。

ファイル ポリシーはどのライセンスでも作成可能ですが、マルウェア防御とファイル制御の一部の操作を行うには、次の表に示すように、ライセンス供与される特定の機能を ASA FirePOWER モジュールで有効にする必要があります。

表 **32-1** 侵入インスペクションおよびファイル インスペクションのライセンスおよびアプライアンスの要件

機能	説明	追加する必要のあるライセンス
侵入防御	侵入およびエクスプロイトを検出し、任意でブロックします	Protection
ファイル制御	ファイル タイプの伝送を検出し、任意でブロックします	Protection
高度なマルウェア防御（AMP）	マルウェアの伝送を検出、追跡し、任意でブロックします	マルウェア

詳細については、以下を参照してください。

- マルウェア防御とファイル制御について（32-1 ページ）
- ファイル ポリシーの概要と作成（32-4 ページ）

マルウェア防御とファイル制御について

ライセンス：Protection、マルウェア、またはすべて

高度なマルウェア防御機能を使用すると、ネットワークで伝送されるマルウェア ファイルを検出、追跡、分析、およびオプションでブロックするよう ASA FirePOWER モジュールを設定できます。

システムは、PDF、Microsoft Office 文書など多数のファイル タイプに潜むマルウェアを検出し、オプションでブロックできます。ASA FirePOWER モジュールは、特定のアプリケーション プロトコル ベースのネットワーク トラフィック内で、これらのファイル タイプの伝送をモニタします。ASA FirePOWER モジュールは該当するファイルを検出します。次に、ASA FirePOWER モジュールはファイルの SHA-256 ハッシュ値を使用してマルウェア クラウド ルックアップを実行します。これらの結果に基づき、シスコ クラウドは ASA FirePOWER モジュールにファイルの性質を返します。

クラウドにあるファイルの性質が不正確だとわかっている場合、次のようにして、ファイルの SHA-256 値をファイル リストに追加できます。

- クラウドがクリーンの性質を割り当てた場合と同じ方法でファイルを扱うには、クリーン リストにファイルを追加します。
- クラウドがマルウェアの性質を割り当てた場合と同じ方法でファイルを扱うには、カスタム検出リストにファイルを追加します。

あるファイルの SHA-256 値がファイル リスト内で検出されると、システムはマルウェア ルックアップの実行もファイルの性質の検査も行わずに、適切なアクションを実行します。ファイルの SHA 値を計算するには、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）] アクションと [マルウェア ブロック（Block Malware）] アクションのどちらか、および一致するファイル タイプを使用して、ファイル ポリシー内のルールを設定する必要があることに注意してください。ファイル ポリシーごとに、クリーン リストまたはカスタム検出リストの使用を有効にできます。

ファイルを検査またはブロックするには、ASA FirePOWER モジュールで Protectionライセンスを有効にする必要があります。また、ファイル リストへのファイルの追加を行うにはマルウェア ライセンスを有効にする必要があります。

ファイルの性質について

システムは、シスコ クラウドから返される性質に基づいてファイルの性質を決定します。シスコ クラウドから返された情報、ファイル リストへの追加操作、または脅威スコアに応じて、ファイルの性質は次のいずれかになります。

- マルウェア（Malware）：クラウドでそのファイルがマルウェアとして分類されていることを示します。
- クリーン（Clean）：クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。
- 不明（Unknown）：クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。クラウドはそのファイルをまだ分類していません。
- カスタム検出（Custom Detection）：ユーザがカスタム検出リストにファイルを追加したことを示します。
- 使用不可（Unavailable）：ASA FirePOWER モジュールがマルウェア クラウド ルックアップを実行できなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。

ヒント　高速連続で複数の使用不可（Unavailable）なマルウェア イベントが発生した場合は、クラウド接続およびポート設定を確認してください。詳細については、セキュリティ、インターネット アクセス、および通信ポート（D-1 ページ）を参照してください。

ファイルの性質に基づき、ASA FirePOWER モジュールはファイルをブロックするか、またはファイルのアップロード/ダウンロードをブロックするよう、管理対象デバイスに指示します。パフォーマンスを改善させるために、SHA-256 値に基づくファイルの性質がシステムですでにわかっている場合、アプライアンスは シスコ クラウドに照会する代わりに、キャッシュ済みの性質を使用します。

ファイルの性質は変更される可能性があることに注意してください。たとえば、クラウドによる判定の結果、以前はクリーンであると考えられていたファイルが今はマルウェアとして識別されるようになったり、その逆、つまりマルウェアと識別されたファイルが実際にはクリーンであったりする可能性があります。あるファイルに関するマルウェア ルックアップを先週実行した後、そのファイルの性質が変更された場合は、クラウドが ASA FirePOWER モジュールに通知を送ります。これにより、そのファイルの伝送が次回検出されたときにシステムは適切なアクションを実行できます。変更されたファイルの性質は、レトロスペクティブな性質と呼ばれます。

マルウェア クラウド ルックアップから戻されたファイルの性質には、存続可能時間（TTL）値が割り当てられます。ファイルの性質が更新されないまま、TTL 値で指定された期間にわたって保持された後は、キャッシュ情報が消去されます。性質には次の TTL 値が割り当てられます。

- クリーン（Clean）：4 時間
- 不明（Unknown）：1 時間
- マルウェア（Malware）：1 時間

キャッシュに照らしたマルウェア クラウド ルックアップの結果、キャッシュ済み性質がタイムアウトになったことが識別されると、システムはファイルの性質を判別するために新しいルックアップを実行します。

ファイル制御について

マルウェア ファイル伝送のブロックに加えて、（マルウェアを含むかどうかにかかわらず）特定のタイプのすべてのファイルをブロックする必要がある場合は、ファイル制御機能により防御網を広げることができます。マルウェア防御の場合と同様に、ASA FirePOWER モジュールはネットワーク トラフィック内で特定のファイル タイプの伝送をモニタし、そのファイルをブロックまたは許可します。

システムでマルウェアを検出できるすべてのファイル タイプだけでなく、さらに多数のファイル タイプに対するファイル制御がサポートされています。これらのファイル タイプは、マルチメディア（swf、mp3）、実行可能ファイル（exe、トレント）、PDF などの基本的なカテゴリにグループ分けされます。ファイル制御はマルウェア防御とは異なり、シスコ クラウドへの照会を必要としないことに注意してください。

マルウェア防御とファイル制御の設定

ライセンス：Protectionまたはマルウェア

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ことで、全体的なアクセス コントロール設定の一部として、マルウェア防御とファイル制御を設定します。この関連付けにより、アクセス コントロール ルールの条件と一致するトラフィック内のファイルを通過させる前に、システムは必ずファイルを検査するようになります。

ファイルのポリシーには、その親であるアクセス コントロール ポリシーと同様に、各ルールの条件に一致したファイルをシステムがどのように処理するかを決定するルールが含まれています。ファイル タイプ、アプリケーション プロトコル、転送方向の違いに応じて異なるアクションを実行する別個のファイル ルールを設定できます。

あるファイルがルールに一致する場合、ルールで以下を実行できます。

- 単純なファイル タイプ照合に基づいてファイルを許可またはブロックする
- マルウェア ファイルの性質に基づいてファイルをブロックする
- さらに、ファイル ポリシーでは以下を実行できます。クリーン リストまたはカスタム検出リストのエントリに基づいて、ファイルがクリーンまたはマルウェアである場合と同じ方法で自動的にファイルを扱う

単純な例として、ユーザによる実行可能ファイルのダウンロードをブロックするファイル ポリシーを導入できます。ファイル ポリシーについて、およびファイル ポリシーとアクセス コントロール ルールとの関連付けについての詳細は、ファイル ポリシーの概要と作成（32-4 ページ）を参照してください。

マルウェア防御とファイル制御に基づくイベントのロギング

ライセンス：Protectionまたはマルウェア

ASA FirePOWER モジュールは、システムのファイル インスペクションおよび処理のレコードを、キャプチャされたファイル、ファイル イベント、およびマルウェア イベントとしてログ記録します。

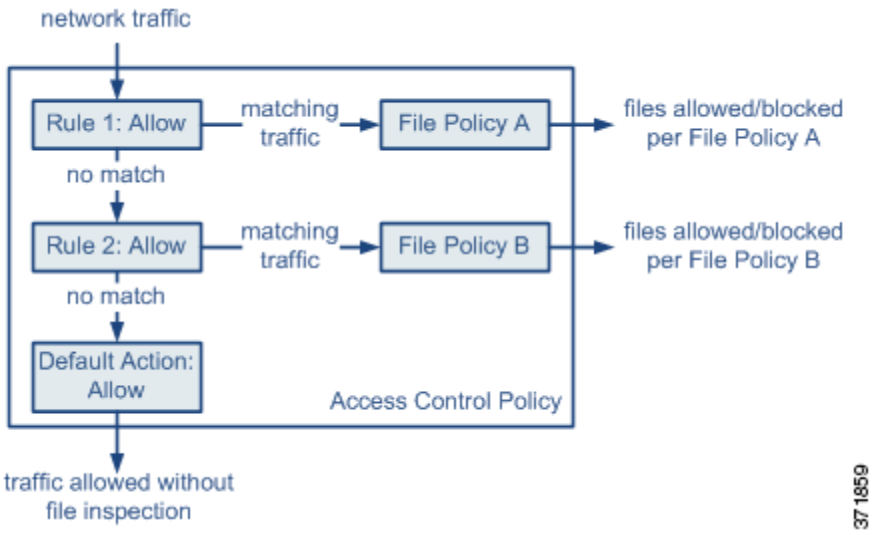
- ファイル イベントは、システムがネットワーク トラフィック内で検出した（およびオプションでブロックした）ファイルを表します。
- マルウェア イベントは、システムがネットワーク トラフィック内で検出した（およびオプションでブロックした）マルウェア ファイルを表します。
- レトロスペクティブ マルウェア イベント：性質がマルウェア ファイルから変更されたファイル。

ファイル内のマルウェアを検出するために、システムはまずファイル自体を検出する必要があるため、ネットワーク トラフィック内のマルウェア検出/ブロックに基づいてシステムがマルウェア イベントを生成するときには、ファイル イベントも生成します。

ファイル ポリシーの概要と作成

ライセンス：Protectionまたはマルウェア

ファイル ポリシーは、いくつかの設定からなるセットです。システムは全体的なアクセス コントロール設定の一部としてこれを使用して、高度なマルウェア防御とファイル制御を実行できます。



このポリシーには 2 つのアクセス コントロール ルールがあり、両方とも許可アクションを使用し、ファイル ポリシーに関連付けられています。このポリシーのデフォルト アクションもまた「トラフィックの許可」ですが、ファイル ポリシー インスペクションはありません。このシナリオでは、トラフィックは次のように処理されます。

- ルール 1 に一致するトラフィックはファイル ポリシー A で検査されます。
- ルール 1 に一致しないトラフィックはルール 2 に照らして評価されます。ルール 2 に一致するトラフィックはファイル ポリシー B で検査されます。
- どちらのルールにも一致しないトラフィックは許可されます。デフォルト アクションにファイル ポリシーを関連付けることはできません。

ファイルのポリシーには、その親であるアクセス コントロール ポリシーと同様に、各ルールの条件に一致したファイルをシステムがどのように処理するかを決定するルールが含まれています。ファイル タイプ、アプリケーション プロトコル、転送方向の違いに応じて異なるアクションを実行する別個のファイル ルールを設定できます。

ファイルがルールに一致すると、ルールは以下を実行できます。

- 単純なファイル タイプ照合に基づいてファイルを許可またはブロックする
- マルウェア ファイルの性質に基づいてファイルをブロックする
- さらに、ファイル ポリシーでは以下を実行できます。クリーン リストまたはカスタム検出リストのエントリに基づいて、ファイルがクリーンまたはマルウェアである場合と同じ方法で自動的にファイルを扱う

1 つのファイル ポリシーを、[許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションを含むアクセス コントロール ルールに関連付けることができます。その後、システムはそのファイル ポリシーを使用して、アクセス コントロール ルールの条件を満たすネットワーク トラフィックを検査します。異なるファイル ポリシーを個々のアクセス コントロール ルールに関連付けることにより、ネットワークで伝送されるファイルを識別/ブロックする方法をきめ細かく制御できます。ただし、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トラフィックを検査するためにファイル ポリシーを使用できないことに注意してください。詳細については、許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション（10-2 ページ）を参照してください。

ファイル ルール

ファイル ポリシーの中でファイル ルールを設定します。次の表に、ファイル ルールのコンポーネントを示します。

表 **32-2**　ファイル ルールのコンポーネント

ファイル ルールのコンポーネント	説明
アプリケーション プロトコル	システムは、FTP、HTTP、SMTP、IMAP、POP3、および NetBIOS-ssn（SMB）を介して伝送されるファイルを検出し、検査できます。パフォーマンスを向上させるには、ファイル ルールごとに、これらのアプリケーション プロトコルのうち 1 つだけでファイルを検出するよう限定できます。
転送の方向	ダウンロードされるファイルに対して、FTP、HTTP、IMAP、POP3、および NetBIOS-ssn（SMB）の着信トラフィックを検査できます。アップロードされるファイルに対しては、FTP、HTTP、SMTP、および NetBIOS-ssn（SMB）の発信トラフィックを検査できます。

表 32-2　ファイル ルールのコンポーネント（続き）

ファイル ルールのコンポーネント	説明
ファイルのカテゴリとタイプ	システムは、さまざまなタイプのファイルを検出できます。これらのファイル タイプは、マルチメディア（swf、mp3）、実行可能ファイル（exe、トレント）、PDF などの基本的なカテゴリにグループ分けされます。個々のファイル タイプを検出したり、ファイル タイプ カテゴリ全体を検出したりするよう、ファイル ルールを設定できます。 たとえば、すべてのマルチメディア ファイルをブロックしたり、ShockWave Flash（swf）ファイルのみをブロックしたりできます。または、ユーザが BitTorrent（torrent）ファイルをダウンロードしたときにアラートを出すよう、システムを設定できます。 ⚠ 注意　頻繁にトリガーされるファイル ルールは、システム パフォーマンスに影響を与える可能性があります。たとえば、HTTP トラフィックでマルチメディア ファイルを検出しようとすると（たとえば YouTube は多量の Flash コンテンツを伝送します）、膨大な数のイベントが生成される可能性があります。
ファイル ルール アクション	ファイル ルールのアクションによって、ルールの条件に一致したトラフィックをシステムが処理する方法が決定されます。 （注）　ファイル ルールは数値上の順番ではなく、ルール アクションの順番で評価されます。詳細は、次の項ファイル ルール アクションと評価順序を参照してください。

ファイル ルール アクションと評価順序

各ファイル ルールには、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する 1 つのアクションが関連付けられます。1 つのファイル ポリシー内に、ファイル タイプ、アプリケーション プロトコル、転送方向の違いに応じて異なるアクションを実行する別々のルールを設定できます。複数のルール アクションは、以下のようなルール アクション順になります。

- [ファイル ブロック（Block Files）] ルールを使用すると、特定のファイル タイプをブロックできます。
- [マルウェア ブロック（Block Malware）] ルールを使用すると、特定のファイル タイプの SHA-256 ハッシュ値を計算した後、クラウド ルックアップ プロセスを使用して、ネットワークを通過するファイルにマルウェアが含まれているかどうかまず判断し、脅威を示すファイルをブロックできます。
- [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] ルールを使用すると、ネットワークを通過するファイルの伝送を許可しながら、クラウド ルックアップに基づいてそのファイルのマルウェアの性質をログに記録できます。
- [ファイル検出（Detect Files）] ルールを使用すると、ファイルの伝送を許可しながら、特定のファイル タイプの検出を記録できます。

各ファイル ルール アクションごとに、ファイル転送がブロックされたときに接続をリセットするオプション、およびキャプチャされたファイルを ASA FirePOWER モジュールに保存するオプションを設定できます。次の表に、各ファイル アクションで使用可能なオプションの詳細を示します。

表 *32-3*　　ファイル ルール アクション

アクション	接続をリセットするか
ファイル ブロック（Block Files）	はい（推奨）
マルウェア ブロック（Block Malware）	はい（推奨）
ファイル検出（Detect Files）	いいえ
マルウェア クラウド ルックアップ（Malware Cloud Lookup）	いいえ

ファイルとマルウェアの検出、キャプチャ、およびブロッキングに関する注意事項と制約事項

ファイルとマルウェアの検出、キャプチャ、およびブロッキングの動作に関して、以下の詳細および制限に注意してください。

- ファイルがセッションで検出されブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。
- ファイルの終わりを示す End of File マーカーが検出されない場合、転送プロトコルとは無関係に、そのファイルは [マルウェア ブロック（Block Malware）] ルールでもカスタム検出リストでもブロックされません。システムは、End of File マーカーで示されるファイル全体の受信が完了するまでファイルのブロックを待機し、このマーカーが検出された後にファイルをブロックします。
- FTP ファイル転送で End of File マーカーが最終データ セグメントとは別に伝送される場合、マーカーがブロックされ、ファイル転送失敗が FTP クライアントに表示されますが、実際にはそのファイルは完全にディスクに転送されます。
- FTP は、さまざまなチャネルを介してコマンドおよびデータを転送します。パッシブの展開では、FTP データ セッションとその制御セッションからのトラフィックは同じ Snort に負荷分散されない場合があります。
- ファイルがアプリケーション プロトコル条件を持つルールに一致する場合、ファイル イベントの生成は、システムがファイルのアプリケーション プロトコルを正常に識別した後に行われます。識別されていないファイルは、ファイル イベントを生成しません。
- FTP に関する [マルウェア ブロック（Block Malware）] ルールを持つファイル ポリシーを使用するアクセス コントロール ポリシーでは、[インライン時にドロップ（Drop when Inline）] を無効にした侵入ポリシーをデフォルト アクションに設定した場合、システムはルールに一致するファイルやマルウェアの検出でイベントを生成しますが、ファイルをドロップしません。FTP ファイア転送をブロックし、ファイル ポリシーを選択するアクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを使用するには、[インライン時にドロップ（Drop when Inline）] を有効にした侵入ポリシーを選択する必要があります。
- [ファイル ブロック（Block Files）] アクションおよび [マルウェア ブロック（Block Malware）] アクションを持つファイル ルールでは、最初のファイル転送試行後 24 時間で検出される、同じファイル、URL、サーバ、クライアント アプリケーションを使った新しいセッションをブロックすることにより、HTTP 経由のファイル ダウンロードの自動再開をブロックします。
- まれに、HTTP アップロード セッションからのトラフィックが不適切である場合、システムはトラフィックを正しく再構築できなくなり、トラフィックのブロックやファイル イベントの生成を行いません。
- [ファイル ブロック（Block Files）] ルールでブロックされる NetBIOS-ssn 経由ファイル転送（SMB ファイル転送など）の場合、宛先ホストでファイルが見つかることがあります。ただし、ダウンロード開始後にファイルがブロックされ、結果としてファイル転送が不完全になるため、そのファイルは使用できません。

- （SMB ファイル転送など）NetBIOS-ssn 経由で転送されるファイルを検出またはブロックするファイル ルールを作成した場合、ファイル ポリシーを呼び出すアクセス コントロール ポリシーの適用前に開始された、確立済み TCP または SMB セッションで転送されるファイルに対しては、検査が行われません。このため、これらのファイルは検出/ブロックされません。
- パッシブ展開でファイルをブロックするよう設定されたルールは、一致するファイルをブロックしません。接続ではファイル伝送が続行されるため、接続の開始をログに記録するルールを設定した場合、この接続に関して複数のイベントが記録されることがあります。
- POP3、POP、SMTP、または IMAP セッションでのすべてのファイル名の合計バイト数が 1024 を超えると、セッションのファイル イベントでは、ファイル名バッファがいっぱいになった後で検出されたファイルの名前が正しく反映されないことがあります。
- SMTP 経由でテキスト ベースのファイルを送信すると、一部のメール クライアントは改行を CRLF 改行文字標準に変換します。MAC ベースのホストはキャリッジ リターン（CR）文字を使用し、Unix/Linux ベースのホストはライン フィード（LF）文字を使用するので、メール クライアントによる改行変換によってファイルのサイズが変更される場合があります。一部のメール クライアントは、認識できないファイル タイプを処理する際に改行変換を行うようデフォルト設定されていることに注意してください。
- シスコでは、[ファイル ブロック（Block Files）] アクションと [マルウェア ブロック（Block Malware）] アクションで [接続のリセット（Reset Connection）] を有効にすることを推奨しています。これにより、ブロックされたアプリケーション セッションが TCP 接続リセットまで開いたままになることを防止できます。接続をリセットしない場合、TCP 接続が自身をリセットするまで、クライアント セッションが開いたままになります。
- [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] アクションまたは [マルウェア ブロック（Block Malware）] アクションを使ってファイル ルールが設定されている場合、ASA FirePOWER モジュールがクラウドとの接続を確立できないと、クラウド接続が復元されるまで、システムは設定済みルール アクション オプションを実行できません。

ファイル ルールの評価例

番号順にルールが評価されるアクセス コントロール ポリシーとは異なり、ファイル ポリシーでは ファイル ルール アクションと評価順序（32-6 ページ）に従ってファイルが処理されます。つまり、（優先度の高い順に）単純なブロッキング、次にマルウェア インスペクションとブロッキング、さらにその次に単純な検出とロギングとなります。例として、1 つのファイル ポリシー内に、PDF ファイルを処理する 4 つのルールがあるとします。モジュール インターフェイスで表示される順序に関係なく、これらのルールは次の順序で評価されます。

表 **32-4**　ファイル ルールの評価順序の例

アプリケーション プロトコル	方向	アクション	アクションのオプション	結果
SMTP	アップロード（Upload）	ファイル ブロック（Block Files）	接続のリセット（Reset Connection）	ユーザが電子メールで PDF ファイルを送信することをブロックし、接続をリセットします。
FTP	ダウンロード（Download）	マルウェア ブロック（Block Malware）	接続のリセット（Reset Connection）	ファイル転送を介したマルウェア PDF ファイルのダウンロードをブロックし、接続をリセットします。
POP3 IMAP	ダウンロード（Download）	マルウェア クラウド ルックアップ（Malware Cloud Lookup）		電子メールで受信された PDF ファイルに対してマルウェア検査を行います。
任意	任意	ファイル検出（Detect Files）	なし	ユーザが Web 上で（つまり HTTP 経由で）PDF ファイルを表示すると、それを検出してログに記録しますが、トラフィックは許可します。

ASA FirePOWER モジュールでは、矛盾するファイル ルールを示すために警告アイコン（  ）を使用します。

システムで検出されるすべてのファイル タイプに対してマルウェア分析を実行できるわけではないことに注意してください。[アプリケーション プロトコル（Application Protocol）]、[転送の方向（Direction of Transfer）]、および [アクション（Action）] ドロップダウン リストで値を選択すると、システムはファイル タイプのリストを限定します。

ファイル イベント、マルウェア イベントおよびアラートのロギング

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、一致するトラフィックに関するファイル イベントとマルウェア イベントのロギングが自動的に有効になります。ファイルを検査するときに、システムは次のタイプのイベントを生成できます。

- ファイル イベント：検出またはブロックされたファイル、および検出されたマルウェア ファイルを表します
- マルウェア イベント：検出されたマルウェア ファイルを表します
- 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に関する「マルウェア」ファイルの性質が変更された場合に、生成されます

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るか、ファイルがキャプチャされると、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自動的に記録します。

（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るファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。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。

これらの接続イベントごとに、

- [ファイル（Files）] フィールドには、接続で検出されたファイル数（マルウェア ファイルを含む）を示すアイコン（  ）が含まれます。このアイコンをクリックすると、それらのファイルのリスト、およびマルウェア ファイルの性質が表示されます。
- [理由（Reason）] フィールドには、接続イベントがログに記録された理由が示されます。これはファイル ルール アクションに応じて次のように異なります。
  - ファイル モニタ（File Monitor）：[ファイル検出（Detect Files）] ルールおよび [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] ファイル ルールの場合、およびクリーン リスト内のファイルの場合
  - ファイル ブロック（File Block）：[ファイル ブロック（Block Files）] ルールまたは [マルウェア ブロック（Block Malware）] ファイル ルールの場合
  - ファイル カスタム検出（File Custom Detection）：カスタム検出リストにあるファイルをシステムが検出した場合
  - ファイル復帰許可（File Resume Allow）：ファイル送信がはじめに [ファイル ブロック（Block Files）] ルールまたは [マルウェア ブロック（Block Malware）] ファイル ルールによってブロックされた場合。ファイルを許可する新しいアクセス コントロール ポリシーが適用された後、HTTP セッションが自動的に再開しました。
  - ファイル復帰ブロック（File Resume Block）：ファイル送信がはじめに [ファイル検出（Detect Files）] ルールまたは [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] ファイル ルールによって許可された場合。ファイルをブロックする新しいアクセス コントロール ポリシーが適用された後、HTTP セッションが自動的に停止しました。
- ファイルやマルウェアがブロックされた接続では、[アクション（Action）] が [ブロック（Block）] になります。

ASA FirePOWER モジュールで生成されるすべての種類のイベントと同様に、ファイル イベントとマルウェア イベントを表示および分析できます。また、マルウェア イベントを使用してSNMP または syslog によるアラートを発行したりすることもできます。

インターネット アクセス

システムはポート 443 を使用して、ネットワーク ベース AMP 用のマルウェア クラウド ルックアップを実行します。ASA FirePOWER モジュールでこのポートをアウトバウンドに開く必要があります。

ファイル ポリシーの管理

[ファイル ポリシー(File Policies)] ページ([ポリシー(Policies)] > [ファイル(Files)])でファイル ポリシーの作成、編集、削除、および比較を行います。ここには既存のファイル ポリシーのリストと、それらの最終更新日が表示されます。

ファイル ポリシーの適用アイコン( )をクリックするとダイアログ ボックスが表示され、そのファイル ポリシーを使用するアクセス コントロール ポリシーが示された後、[アクセス コントロール ポリシー(Access Control Policy)] ページにリダイレクトされます。これは、ファイル ポリシーが親アクセス コントロール ポリシーの一部と見なされ、ファイル ポリシーを単独で適用できないためです。新しいファイル ポリシーを使用したり、既存のファイル ポリシーの変更内容を適用したりするには、親アクセス コントロール ポリシーを適用/再適用する必要があります。

保存済みまたは適用済みのアクセス コントロール ポリシーで使われているファイル ポリシーは削除できないことに注意してください。

ファイル ポリシーの管理の詳細については、次の項を参照してください。

- ファイル ポリシーの作成(32-10 ページ)
- ファイル ルールの操作(32-11 ページ)
- 2 つのファイル ポリシーの比較(32-14 ページ)

ファイル ポリシーの作成

ライセンス:Protectionまたはマルウェア

ファイル ポリシーを作成して、その中でルールを設定すると、それをアクセス コントロール ポリシーで使用できるようになります。

ヒント　既存のファイル ポリシーのコピーを作成するには、コピー アイコン( )をクリックして、表示されるダイアログ ボックスで新しいポリシーの固有名を入力します。その後、そのコピーを変更できます。

ファイル ポリシーを作成する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [ファイル(Files)] の順に選択します。

[ファイル ポリシー(File Policies)] ページが表示されます。

ステップ 2　[新しいファイル ポリシー(New File Policy)] をクリックします。

[新しいファイル ポリシー(New File Policy)] ダイアログ ボックスが表示されます。

新しいポリシーの場合、ポリシーが使用中でないことがモジュール インターフェイスに示されます。使用中のファイル ポリシーを編集している場合は、そのファイル ポリシーを使用しているアクセス コントロール ポリシーの数がモジュール インターフェイスに示されます。どちらの場合も、テキストをクリックすると [アクセス コントロール ポリシー(Access Control Policies)] ページに移動できます(アクセス コントロール ポリシーの開始(4-1 ページ)を参照)。

ステップ 3　新しいポリシーの [名前(Name)] とオプションの [説明(Description)] を入力してから、[保存(Save)] をクリックします。

[ファイル ポリシー ルール(File Policy Rules)] タブが表示されます。

ステップ 4　ファイル ポリシーに 1 つ以上のルールを追加します。

ファイル ルールを使用すると、ロギング、ブロック、またはマルウェア スキャンの対象となるファイル タイプを詳細に制御できます。ファイル ルールの追加については、ファイル ルールの操作(32-11 ページ)を参照してください。

ステップ 5　詳細オプションを設定します。詳細については、ファイル ポリシーの詳細オプション([一般(General)])の設定(32-13 ページ)を参照してください。

ステップ 6　[ASA FirePOWER 変更の保存(Store ASA FirePOWER Changes)] をクリックします。

新しいポリシーを使用するには、アクセス コントロール ルールにファイル ポリシーを追加してから、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。既存のファイル ポリシーを編集している場合は、そのファイル ポリシーを使用するすべてのアクセス コントロール ポリシーを再適用する必要があります。

ファイル ルールの操作

ライセンス:Protectionまたはマルウェア

効果を発揮するには、ファイル ポリシーに 1 つ以上のルールが含まれている必要があります。新しいファイル ポリシーを作成するとき、または既存のポリシーを編集するときに表示される [ファイル ポリシー ルール(File Policy Rules)] ページで、ルールを作成、編集、および削除します。このページには、ポリシー内のすべてのルールがリストされ、各ルールの基本的な特性も示されます。

また、このページでは、このファイル ポリシーを使用するアクセス コントロール ポリシーの数も通知されます。この通知をクリックすると、親ポリシーのリストが表示され、オプションで [アクセス コントロール ポリシー(Access Control Policies)] ページに進むことができます。

ファイル ルールを作成する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [ファイル(Files)] の順に選択します。

[ファイル ポリシー(File Policies)] ページが表示されます。

ステップ 2　次の選択肢があります。

- 新しいポリシーにルールを追加するには、[新しいファイル ポリシー(New File Policy)] をクリックして、新しいポリシーを作成します(ファイル ポリシーの作成(32-10 ページ)を参照)。
- 既存のポリシーにルールを追加するには、ポリシーの横にある編集アイコン( )をクリックします。

ステップ 3　表示される [ファイル ポリシー ルール(File Policy Rules)] ページで、[ファイル ルールの追加(Add File Rule)] をクリックします。

[ファイル ルールの追加(Add File Rule)] ダイアログ ボックスが表示されます。

ステップ 4　ドロップダウンリストから、[アプリケーション プロトコル(Application Protocol)] を選択します。

デフォルトの [任意(Any)] は、HTTP、SMTP、IMAP、POP3、FTP、および NetBIOS-ssn(SMB)トラフィック内のファイルを検出します。

ステップ 5　ドロップダウンリストから [転送の方向（Direction of Transfer）] を選択します。

ダウンロードされるファイルに関して、以下のタイプの着信トラフィックを検査できます。

- HTTP
- IMAP
- POP3
- FTP
- NetBIOS-ssn（SMB）

アップロードされるファイルに関して、以下のタイプの発信トラフィックを検査できます。

- HTTP
- FTP
- SMTP
- NetBIOS-ssn（SMB）

[任意（Any）] を使用すると、ユーザが送信しているか受信しているかには関係なく、多数のアプリケーション プロトコルを介したファイルが検出されます。

ステップ 6　ファイル ルールの [アクション（Action）] を選択します。詳細については、ファイル ルール アクション の表を参照してください。

[ファイル ブロック（Block Files）] または [マルウェア ブロック（Block Malware）] を選択すると、[接続のリセット（Reset Connection）] がデフォルトで有効になります。ファイル転送のブロックが発生した接続をリセットしないようにするには、[接続のリセット（Reset Connection）] チェックボックスをクリアします。

（注）　シスコでは、[接続のリセット（Reset Connection）] を有効のままにしておくことを推奨しています。これにより、ブロックされたアプリケーション セッションが TCP 接続リセットまで開いたままになることを防止できます。

ファイル ルールのアクションの詳細については、ファイル ルール アクションと評価順序（32-6 ページ）を参照してください。

ステップ 7　[ファイル タイプ（File Types）] を 1 つ以上選択します。複数のファイル タイプを選択するには、Shift キーと Ctrl キーを使用します。ファイル タイプのリストを、次のようにフィルタ処理できます。

- [ファイル タイプ カテゴリ（File Type Categories）] を 1 つ以上選択します。
- 名前または説明でファイル タイプを検索します。たとえば、Microsoft Windows 固有のファイルのリストを表示するには、[名前および説明の検索（Search name and description）] フィールドに `Windows` と入力します。

ファイル ルールで使用できるファイル タイプは、[アプリケーション プロトコル（Application Protocol）]、[転送の方向（Direction of Transfer）]、および [アクション（Action）] での選択内容に応じて変化します。

たとえば、[転送の方向（Direction of Transfer）] で [ダウンロード（Download）] を選択すると、ファイル イベントが過剰になることを防止するために、[グラフィック（Graphics）] カテゴリから [GIF]、[PNG]、[JPEG]、[TIFF]、および [ICO] が削除されます。

ステップ 8　選択したファイル タイプを [選択済みのファイル カテゴリとタイプ（Selected Files Categories and Types）] リストに追加します。

- [追加（Add）] をクリックすると、選択したファイル タイプがルールに追加されます。

- 1 つ以上のファイル タイプを [選択済みのファイル カテゴリとタイプ（Selected Files Categories and Types）] リストの中にドラッグ アンド ドロップします。
- カテゴリを選択して [選択済みカテゴリにあるすべてのタイプ（All types in selected Categories）] をクリックしてから、[追加（Add）] をクリックするか、選択項目を [選択済みのファイル カテゴリとタイプ（Selected Files Categories and Types）] リストの中にドラッグ アンド ドロップします。

ステップ **9**　[ASA FirePOWER 変更の保存（Store ASA FirePOWER Changes）] をクリックします。

ファイル ルールがポリシーに追加されます。既存のファイル ポリシーを編集している場合、変更内容を有効にするには、そのファイル ポリシーを使用するすべてのアクセス コントロール ポリシーを再適用する必要があります。

ファイル ポリシーの詳細オプション（[一般（General）]）の設定

ライセンス：マルウェア

ファイル ポリシーでは、[一般（General）] セクションにある以下の詳細オプションを設定できます。

表 ***32-5***　ファイル ポリシーの詳細オプション（***[一般（General）]***）

フィールド	説明	デフォルト値
カスタム検知リストを有効にする（**Enable Custom Detection List**）	これを選択すると、カスタム検出リストにあるファイルが検出されたときに、そのファイルをブロックします。	有効（enabled）
クリーンリストを有効にする（**Enable Clean List**）	これを選択すると、クリーン リストにあるファイルが検出されたときに、そのファイルを許可します。	有効（enabled）

ファイル ポリシーの詳細オプション（**[一般（General）]**）を設定するには、次の手順を実行します。

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [ファイル（Files）] の順に選択します。

[ファイル ポリシー（File Policies）] ページが表示されます。

ステップ **2**　編集するポリシーの横にある編集アイコン（ ）をクリックします。

[ファイル ポリシー ルール（File Policy Rules）] ページが表示されます。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

[詳細設定（Advanced）] タブが表示されます。

ステップ **4**　ファイル ポリシーの詳細オプション（[一般（General）]）の表に示されているようにオプションを変更します。

ステップ **5**　[ASA FirePOWER 変更の保存（Store ASA FirePOWER Changes）] をクリックします。

編集したファイル ポリシーを使用するすべてのアクセス コントロール ポリシーを再適用する必要があります。

2 つのファイル ポリシーの比較

ライセンス：Protection

変更後のポリシーが組織の標準に準拠することを確かめたり、システム パフォーマンスを最適化したりする目的で、任意の 2 つのファイル ポリシー間の違いや、同じポリシーの 2 つのリビジョン間の違いを調べることができます。

ファイル ポリシーの比較ビューには、2 つのポリシーまたはリビジョンが並んで表示され、各ポリシー名の横には最終変更時刻と最後に変更したユーザが表示されます。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。

[前へ（Previous）] と [次へ（Next）] をクリックすると、前後の相違箇所に移動できます。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。オプションで、ファイル ポリシーの比較レポートを生成できます。これは PDF 版の比較ビューです。

2 つのファイル ポリシーを比較する方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [ファイル（Files）] の順に選択します。

[ファイル ポリシー（File Policies）] ページが表示されます。

ステップ 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）] ダイアログ ボックスが表示されます。

ステップ 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。

- 2 つの異なるポリシーを比較するには、[実行中の設定（Running Configuration）] または [他のポリシー（Other Policy）] を選択します。この 2 つのオプションの違いは、[実行中の設定（Running Configuration）] を選択した場合、現在適用されている一連のファイル ポリシーの中からのみ、比較対象の 1 つを選択できます。
- 同じポリシーの複数のバージョンを比較するには、[その他のリビジョン（Other Revision）] を選択します。

ダイアログ ボックスの表示が更新され、比較オプションが示されます。

ステップ 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、比較対象のポリシーとして [ポリシー A（Policy A）] または [ターゲット/実行中の設定 A（Target/Running Configuration A）] のどちらかと、[ポリシー B（Policy B）] とを選択します。
- 同じポリシーのバージョン間を比較する場合、対象の [ポリシー（Policy）] を選択してから、2 つのリビジョン [リビジョン A（Revision A）] と [リビジョン B（Revision B）] を選択します。リビジョンは、日付とユーザ名別にリストされます。

ステップ 5　[OK] をクリックします。

比較ビューが表示されます。

オプションで、[比較レポート（Comparison Report）] をクリックして、ファイル ポリシー比較レポートを生成します。コンピュータにレポートを保存するようにプロンプトが出されます。

ネットワーク トラフィックの接続のロギング

デバイスがネットワーク上でホストによって生成されたトラフィックをモニタするとき、デバイスは検出した接続のログを生成できます。アクセス コントロール ポリシーでさまざまな設定を行うことで、ログする接続の種類、接続をログする時期、およびデータを保存する場所のきめ細かい制御を行うことができます。また、アクセス コントロール ルールの特定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。

ほとんどの場合、接続の開始および終了で接続をログに記録できます。接続をログに記録すると、システムによって接続イベントが生成されます。接続がレピュテーション ベースのセキュリティ インテリジェンス機能によってブラックリスト登録（ブロック）される場合は、セキュリティ インテリジェンス イベントと呼ばれる特別な種類の接続イベントをログに記録することもできます。

接続イベントには、検出されたセッションに関するデータも含まれています。

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。

接続データのロギングの詳細については、以下を参照してください。

どの接続をログに記録するかの決定

ライセンス：任意

アクセス コントロール ポリシーのさまざまな設定を使用して、ASA FirePOWER モジュールがモニタする接続をログに記録できます。ほとんどの場合、接続の開始および終了で接続をログに記録できます。しかし、ブロックされたトラフィックは追加のインスペクションなしですぐに拒否されるため、システムがログに記録できるのはブロックまたはブラックリスト登録されたトラフィックの接続開始イベントのみです。ログに記録できる固有の接続終了イベントはありません。

接続イベントをログに記録すると、イベント ビューアでそれを表示できます。また、外部の syslog または SNMP トラップ サーバに接続データを送信できます。

ヒント　ASA FirePOWER モジュールを使用して接続データの詳細な分析を実行するためには、シスコ はクリティカルな接続の終了を記録することを推奨します。

詳細については、以下を参照してください。

- クリティカルな接続のロギング（33-2 ページ）
- 接続の開始および終了のロギング（33-3 ページ）
- ASA FirePOWER モジュールまたは外部サーバへの接続のロギング（33-4 ページ）
- アクセス コントロール ルール アクションがどのようにロギングに影響を及ぼすかについて（33-4 ページ）
- 接続ロギングのライセンス要件（33-7 ページ）

クリティカルな接続のロギング

ライセンス：任意

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。目標が生成するイベントの数を抑えパフォーマンスを向上させることである場合は、分析のために重要な接続のロギングのみを有効にします。しかし、プロファイリングの目的でネットワーク トラフィックの広範な表示が必要な場合は、追加の接続のロギングを有効にできます。アクセス コントロール ポリシーでさまざまな設定を行うことで、ログする接続の種類、接続をログする時期、およびデータを保存する場所のきめ細かい制御を行うことができます。

注意　サービス妨害（DoS）攻撃時にブロックされた TCP 接続をロギングすると、複数の同様のイベントによってシステムが過負荷状態にな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。

設定するロギングに加えて、禁止されたファイル、マルウェア、または侵入の試みをシステムが検出した場合には、ほとんどの接続を自動的にログに記録します。システムはこれらの接続終了イベントを保存し、さらなる分析に使用します。すべての接続イベントは、自動的にログ記録された理由を [アクション（Action）] および [理由（Reason）] フィールドで反映します。

セキュリティ インテリジェンス ブラックリスト登録の決定（オプション）

接続がレピュテーション ベースのセキュリティ インテリジェンス機能によってブラックリスト登録（ブロック）される場合は、その接続をログに記録できます。オプションで、セキュリティ インテリジェンス フィルタリングには「モニタ専用」設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブラックリスト登録されるはずの接続をシステムがさらに分析できるだけでなく、ブラックリストと一致する接続をログに記録することもできます。

セキュリティ インテリジェンス ロギングを有効にすると、ブラックリストの一致によってセキュリティ インテリジェンス イベントおよび接続イベントが生成されます。セキュリティ インテリジェンス イベントは特殊なタイプの接続イベントで、個別に表示および分析できるだけでなく、個別に保存およびプルーニングできます。詳細については、セキュリティ インテリジェンス（ブラックリスト登録）の決定のロギング（33-8 ページ）を参照してください。

アクセス コントロールの処理（オプション）

接続がアクセス コントロール ルールまたはアクセス 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場合は、その接続をログに記録できます。クリティカルな接続のみをログに記録できるように、このロギングはアクセス コントロール ルールごとに設定します。詳細については、アクセス コントロールの処理に基づく接続のロギング（33-10 ページ）を参照してください。

侵入に関連付けられる接続（自動）

アクセス コントロール ルールによって呼び出された侵入ポリシー（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）が侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を自動的にロギングします。

しかし、アクセス コントロールのデフォルト アクションに関連付けられた侵入ポリシー（デフォルト処理の設定およびネットワーク トラフィックのインスペクション（4-5 ページ）を参照）によって侵入イベントが生成された場合、システムは関連する接続の終了を自動的にログに記録しません。代わりに、デフォルトのアクション接続のロギングを明示的に有効にする必要があります。これは、接続データをログに記録する必要がない、侵入防御専用の展開環境に役立ちます。

侵入がブロックされた接続では、接続ログ内の接続のアクションは [ブロック（Block）]、理由は [侵入ブロック（Intrusion Block）] ですが、侵入インスペクションを実行するには、許可ルールを使用する必要があります。

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（自動）

アクセス コントロール ルールによって呼び出されたファイル ポリシーが禁止されたファイル（マルウェアを含む）を検出してファイル イベントまたはマルウェア イベントを生成すると、システムはアクセス コントロール ルールのロギング設定に関係なく、ファイルが検出された接続の終了を自動的にロギングします。この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るファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。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。

ファイルがブロックされた接続の場合、接続ログにおける接続のアクションは [ブロック（Block）] ですが、ファイルおよびマルウェアのインスペクションを実行するには、許可ルールを使用する必要があります。接続の原因は、[ファイル モニタ（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 [マルウェア ブロック（Malware Block）] または [ファイル ブロック（File Block）]（ファイルがブロックされた）です。

接続の開始および終了のロギング

ライセンス：任意

システムが接続を検出すると、ほとんどの場合、その開始および終了をログに記録できます。

しかし、ブロックされたトラフィックは追加のインスペクションなしですぐに拒否されるため、多くの場合、ユーザがログに記録できるのはブロックまたはブラックリスト登録されたトラフィックの接続開始イベントのみです。ログに記録できる固有の接続終了イベントはありません。

（注）　単一のブロックされていない接続の場合、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ます。

何らかの理由で接続をモニタすると、接続終了ロギングが強制されることに注意してください。モニタされた接続のロギングについて（33-5 ページ）を参照してください。

次の表では、接続開始イベントと接続終了イベントの違い（それぞれをロギングする利点を含む）を詳細に説明します。

表 *33-1*　接続開始イベントと接続終了イベントの比較

	接続開始イベント	接続終了イベント
次の場合に生成可能です	システムが接続の開始を検出した場合（または、イベントの生成がアプリケーションまたは URL の識別に依存する場合は最初の数パケットの後）	システムが以下の場合 • 接続のクローズを検出した場合 • 一定期間後に接続の終了を検出しない場合 • メモリ制約によりセッションを追跡できなくなった場合
次のものについてロギングが可能です	セキュリティ インテリジェンスまたはアクセス コントロール ルールによって評価されたすべての接続。	すべての接続は設定可能ですが、システムはブロックされた接続またはブラックリスト登録された接続の終了をロギングできません。
次を含みます	最初のパケット（または、イベントの生成がアプリケーションまたは URL の識別に依存する場合は最初の数パケット）で判定できる情報のみ	接続開始イベント内のすべての情報と、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）
次の場合に有用です	次のものをロギングする場合 • セキュリティ インテリジェンス ブラックリスト登録の決定を含む、ブロックされた接続 •	次の操作をする場合 • セッションの期間にわたって収集された情報であらゆる種類の詳細な分析を実行する場合 • グラフ形式で接続データを表示する場合

ASA FirePOWER モジュールまたは外部サーバへの接続のロギング

ライセンス：任意

接続イベントのログは、ASA FirePOWER モジュールの他に、外部 syslog または SNMP トラップ サーバに記録できます。外部サーバに接続データを記録する前に、そのサーバにアラート応答という接続を設定する必要があります。アラート応答の使用（35-2 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 アクションがどのようにロギングに影響を及ぼすかについて

ライセンス：機能によって異なる

すべてのアクセス コントロール ルールにはアクションがあり、それによってシステムがルールに一致するトラフィックを検査および処理する方法だけでなく、一致するトラフィックに関する詳細をユーザがロギングできる時期と方法が決まります。

詳細については、以下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（6-7 ページ）
- モニタされた接続のロギングについて（33-5 ページ）
- 信頼されている接続のロギングについて（33-5 ページ）
- 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（33-5 ページ）
- 許可された接続のロギングについて（33-6 ページ）
- 許可された接続のファイルおよびマルウェア イベント ロギングの無効化（33-7 ページ）

モニタされた接続のロギングについて

ライセンス:機能によって異なる

システムは、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 アクションとは関係なく、次の接続の終了を ASA FirePOWER モジュールに常にロギングします。

- モニタに設定されたセキュリティ インテリジェンスのブラックリストに一致する接続
- アクセス コントロールのモニタ ルールに一致する接続

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 ルールまたはセキュリティ インテリジェンスのモニタ対象ブラックリストに一致すれば、必ず接続がロギングされます。セキュリティ インテリジェンスのフィルタリングの結果、システムが接続イベントをロギングすると、一致するセキュリティ インテリジェンス イベントもロギングされます。そのイベントは特殊なタイプの接続イベントで、個別に表示および分析できます。セキュリティ インテリジェンス(ブラックリスト登録)の決定のロギング(33-8 ページ)を参照してください。

モニタ対象のトラフィックは、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 [モニタ(Monitor)] にはなりません。代わりに、後で接続を処理するルールまたはデフォルト アクションの操作が反映されます。

システムは、1 つの接続が 1 つのアクセス コントロール 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、ASA FirePOWER モジュールにロギングされる各接続イベントには、接続が一致する最初の 8 つのモニタ アクセス コントロール ルールに関する情報を表示することができます。

同様に、外部 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、接続が一致したモニタ ルールの情報が含まれます。

信頼されている接続のロギングについて

ライセンス:機能によって異なる

信頼されている接続は、信頼アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションによって処理される接続です。これらの接続の開始と終了をロギングできますが、信頼されている接続は侵入、または禁止されているファイルおよびマルウェアについて検査されないことに注意してください。したがって、信頼されている接続の接続イベントには、限られた情報が含まれます。

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

ライセンス:機能によって異なる

トラフィックをブロックするアクセス コントロール ルールおよびアクセス コントロール ポリシーのデフォルト アクション(インタラクティブなブロッキング ルールを含む)の場合は、システムは接続開始イベントをロギングします。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拒否されます。

アクセス コントロール ルールでブロックされたセッションの接続イベントには、アクション [ブロック(Block)] または [リセットしてブロック(Block with reset)] があります。

インタラクティブ ブロッキング アクセス コントロール ルール（このルールではユーザが禁止されている Web サイトを参照するとシステムによって警告ページが表示されます）を使用すると、接続の終了をロギングできます。その理由は、警告ページをユーザがクリック スルーすると、その接続は新規の、許可された接続と見なされ、システムによってモニタとロギングができるためです。許可された接続のロギングについて（33-6 ページ）を参照してください。

したがって、[インタラクティブ ブロック（Interactive Block）] ルールまたは [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。

- ユーザの要求が最初にブロックされ警告ページが表示されたときの接続開始イベント。このイベントにはアクション [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] 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 [許可（Allow）] アクションおよび理由 [ユーザ バイパス（User Bypass）] が関連付けられます）

インラ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。

注意　サービス妨害（DoS）攻撃時にブロックされた TCP 接続をロギングすると、複数の同様のイベントによってシステムが過負荷状態にな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。

許可された接続のロギングについて

ライセンス：機能によって異なる

許可アクセス コントロール ルールは、インスペクションおよびトラフィックの処理の次のフェーズに渡せるように一致トラフィックを許可します。

アクセス コントロール ルールで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（またはその両方）を使用して、トラフィックをさらに検査し、トラフィックが最終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ブロックすることができます。

許可アクセス コントロール ルールに一致するトラフィックの接続は次のようにロギングされます。

- アクセス コントロール ルールによって呼び出された侵入ポリシーが侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を ASA FirePOWER モジュールに自動的にロギングします。
- アクセス コントロール ルールによって呼び出されたファイル ポリシーが禁止されたファイル（マルウェアを含む）を検出してファイル イベントまたはマルウェア イベントを生成すると、システムはアクセス コントロール ルールのロギング設定に関係なく、ファイルが検出された接続の終了を ASA FirePOWER モジュールに自動的にロギングします。
- 任意で、システムが安全と見なすトラフィックや、侵入ポリシーまたはファイル ポリシーで検査をしないトラフィックなど、許可されたトラフィックに対して接続の開始および終了のロギングを有効にできます。

結果として生じるすべての接続イベントで、[アクション（Action）] および [理由（Reason）] フィールドにイベントがロギングされた理由が反映されます。次の点に注意してください。

- アクション [許可（Allow）] は、最終宛先に到達した明示的に許可されインタラクティブにユーザがバイパスしたブロックされた接続を表します。
- アクション [ブロック（Block）] は、アクセス コントロール ルールによって初めは許可されたが、侵入、禁止されたファイル、またはマルウェアが検出された接続を表します。

許可された接続のファイルおよびマルウェア イベント ロギングの無効化

ライセンス：Protectionまたはマルウェア

アクセス コントロール ルールでトラフィックを許可すると、関連付けられたファイル ポリシーを使用して、送信されたファイルを検査し、そのトラフィックが宛先に到達する前に禁止されたファイルおよびマルウェアをブロックできます。侵入防御パフォーマンスの調整（10-6 ページ）を参照してください。

システムが禁止されたファイルを検出すると、次のタイプのイベントの 1 つを ASA FirePOWER モジュールに自動的にロギングします。

- 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：検出されたまたはブロックされたマルウェア ファイルのみを表します
- 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 イベントをロギングしない場合は、アクセス コントロール ルール エディタの [ロギング（Logging）] タブの [ログファイル（Log Files）] チェックボックスをオフにすることで、アクセス コントロール ルールごとにこのロギングを無効にできます。

（注）　シスコ では、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を有効のままにすることを推奨しています。

ファイル イベントおよびマルウェア イベントを保存するかどうかにかかわらず、ネットワーク トラフィックがファイル ポリシーに違反すると、呼び出し元のアクセス コントロール ルールのロギング設定に関係なく、システムは関連付けられた接続の終了を ASA FirePOWER モジュールに自動的にロギングします。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（自動）（33-3 ページ）を参照してください。

接続ロギングのライセンス要件

ライセンス：機能によって異なる

アクセス コントロール ポリシーで接続ロギングを設定する前に、これらのポリシーが正常に処理できる任意の接続をロギングできます。

アクセス コントロール ポリシーは、ASA FirePOWER モジュールでのライセンスに関係なく作成できます。ただし、アクセス コントロールのある側面では、ポリシーを適用する前に特定のライセンス交付対象の機能を有効化する必要があります。

次の表では、アクセス コントロールを正常に設定し、アクセス コントロール ポリシーによって処理される接続をロギングするのに必要なライセンスについて説明します。

表 ***33-2***　　アクセス コントロール ポリシーにおける接続ロギングのライセンスの要件

次の接続をロギングするには	ライセンス
ネットワーク、ポートまたはリテラル URL 基準を使用して処理されるトラフィック用	任意
位置情報データを使用して処理されるトラフィック用	任意
関連付ける対象 • レピュテーションが低い IP アドレス（セキュリティ インテリジェンスのフィルタリング） • 侵入または禁止されたファイル	Protection
マルウェアに関連付けられる	マルウェア
ユーザ制御またはアプリケーション制御によって処理されるトラフィック用	Control
URL カテゴリおよびレピュテーション データを使用してシステムがフィルタリングするトラフィック用、およびモニタ対象ホストによって要求される URL の URL カテゴリおよび URL レピュテーション情報を表示するため	URL フィルタリング（URL Filtering）

セキュリティ インテリジェンス(ブラックリスト登録)の決定のロギング

ライセンス:Protection

悪意のあるインターネット コンテンツに対する第一の防衛ラインとして、ASA FirePOWER モジュールにはセキュリティ インテリジェンス機能があります。これを使用することで、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、リソースを集中的に使用する詳細な分析の必要がなくなります。このトラフィック フィルタリングは、他のどのポリシー ベースのインスペクション、分析、またはトラフィック処理よりも先に行われます。

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

セキュリティ インテリジェンスのロギングを有効にすると、アクセス コントロール ポリシーによって処理されるすべてのブロックされた接続およびモニタされた接続がロギングされます。ただし、システムはホワイトリストの一致はロギングしません。ホワイトリストに登録された接続のロギングは、その接続の最終的な傾向によって異なります。

セキュリティ インテリジェンスのフィルタリングの結果、システムが接続イベントをロギングすると、一致するセキュリティ インテリジェンス イベントもロギングされます。そのイベントは特殊なタイプの接続イベントで、個別に表示および分析できます。どちらのタイプのイベントも、[アクション(Action)] および [理由(Reason)] フィールドを使用して、ブラックリストの一致を反映します。さらに、接続でブラックリスト登録された IP アドレスを特定できるように、IP アドレスの横にあるホスト アイコンは、ブラックリスト登録された IP アドレスとモニタされた IP アドレスではイベント ビューアで少々異なる表示になっています。

ブロックされたブラックリスト登録された接続のロギング

ブロックされた接続の場合、システムは接続開始セキュリティ インテリジェンス イベントと接続イベントをロギングします。ブラックリスト登録されたトラフィックは追加のインスペクションなしですぐに拒否されるため、ログに記録できる固有の接続の終了イベントはありません。これらのイベントの場合、アクションは [ブロック(Block)] 、理由は [IP ブロック(IP Block)] です。

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

モニタされブラックリスト登録された接続のロギング

セキュリティ インテリジェンスによってモニタされた(ブロックではなく)接続の場合、システムは接続終了セキュリティ インテリジェンス イベントと接続イベントを ASA FirePOWER モジュールにロギングします。このロギングは、接続が後でアクセス コントロール ルールまたはアクセス コントロールのデフォルト アクションによってどのように処理されるかにかかわらず発生します。

これらの接続イベントの場合、アクションは接続の最終的な傾向によって異なります。[理由(Reason)] フィールドには、[IP モニタ(IP Monitor)] と、接続がロギングされている可能性がある他の理由が含まれています。

ただし、モニタされる接続の場合、以降に接続を処理するアクセス コントロール ルールやデフォルト アクションでのロギング設定によっては、接続開始イベントが生成されることもあります。

ブラックリスト登録された接続をログに記録する方法:

ステップ 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。

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

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。

ステップ 3　[セキュリティ インテリジェンス(Security Intelligence)] タブを選択します。

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

ステップ 4　ロギング アイコン( )をクリックします。

[ブラックリスト オプション(Blacklist Options)] ポップアップ ウィンドウが表示されます。

ステップ 5　[ログ接続(Log Connections)] チェックボックスをオンにします。

ステップ 6　接続イベントとセキュリティ インテリジェンス イベントの送信先を指定します。次の選択肢があります。

- ASA FirePOWER モジュールにイベントを送信するには、[イベント ビューア(Event Viewer)] を選択します。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。オプションで、syslog アラート応答を追加するには、追加アイコン( )をクリックします。Syslog アラート応答の作成(35-4 ページ)を参照してください。
- 接続イベントを SNMP トラップ サーバに送信する場合は、[SNMP トラップ(SNMP Trap)] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン( )をクリックして 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(35-2 ページ)を参照)。

ブラックリスト登録されたオブジェクトをモニタ専用に設定する場合、またはセキュリティ インテリジェンス フィルタリングによって生成された接続イベントで他の ASA FirePOWER モジュール ベースの分析を行う場合は、イベントをイベント ビューアに送信する必要があります。詳細については、ASA FirePOWER モジュールまたは外部サーバへの接続のロギング（33-4 ページ）を参照してください。

ステップ 7　[OK] をクリックしてロギング オプションを設定します。

[セキュリティ インテリジェンス（Security Intelligence）] タブが再表示されます。

ステップ 8　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

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（4-12 ページ）を参照してください。

アクセス コントロールの処理に基づく接続のロギング

ライセンス：任意

アクセス コントロール ポリシー内で、アクセス コントロール ルールはネットワーク トラフィックを処理する詳細な方法を提供しています。クリティカルな接続のみをロギングできるように、アクセス コントロール ルールごとに接続ロギングを有効にします。あるルールに対して接続ロギングを有効にすると、システムはそのルールによって処理されるすべての接続をロギングします。

また、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たトラフィックの接続もロギングできます。デフォルト アクションによって、システムがポリシー内のアクセス コントロール ルールのいずれにも一致しないトラフィックを処理する方法が決まります（トラフィックに一致しロギングするが、処理または検査はしないモニタ ルールを除く）。

すべてのアクセス コントロール ルールおよびデフォルト アクションのロギングを無効にしても、接続がアクセス コントロール ルールに一致し、侵入の試み、禁止されたファイル、またはマルウェアが含まれている場合、接続終了イベントは引き続き ASA FirePOWER モジュールにロギングされる場合があることに注意してください。

ルールまたはデフォルトのポリシー アクション、および設定した関連するインスペクション オプションによって、ロギング オプションは異なります。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 ルールに一致する接続のロギング（33-10 ページ）
- 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た接続のロギング（33-12 ページ）

アクセス コントロール ルールに一致する接続のロギング

ライセンス：任意

クリティカルな接続のみをロギングするには、アクセス コントロール ルールごとに接続ロギングを有効にします。あるルールに対しロギングを有効にすると、システムはそのルールによって処理されたすべての接続をロギングします。

ルール アクションおよびそのルールの侵入およびファイルのインスペクション設定によって、ロギング オプションは異なります。アクセス コントロール ルール アクションがどのようにロギングに影響を及ぼすかについて（33-4 ページ）を参照してください。また、アクセス コントロール ルールに対してロギングを無効にしても、接続が以下の場合は、そのルールに一致する接続の接続終了イベントは引き続き ASA FirePOWER モジュールにロギングされる場合があることに注意してください。

- 侵入の試み、禁止されたファイル、またはマルウェアが含まれている場合
- 以前に少なくとも 1 つのアクセス コントロールのモニタ ルールに一致した場合

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:

ステップ 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。

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。

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)] タブに焦点が置かれています。

ステップ 3　ロギングを設定するルール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 ルール エディタが表示されます。

ステップ 4　[ロギング(Logging)] タブを選択します。

[ロギング(Logging)] タブが表示されます。

ステップ 5　接続の開始および終了時点でロギングを行うか、接続の終了時点でロギングを行うか、または接続のロギングを行わないかを指定します。

単一のブロックされていない接続の場合、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ます。ブロックされたトラフィックは追加のインスペクションなしですぐに拒否されるため、システムはブロック ルールに対する接続開始イベントのみをロギングします。このため、ルール アクションを [ブロック(Block)] または [リセットしてブロック(Block with reset)] に設定すると、接続の開始時点でロギングを行うよう指示するプロンプトが表示されます。

への接続終了ロギングであることに注意してください。

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、[ログ ファイル(Log Files)] チェック ボックスを使用します。

ユーザがファイル ポリシーをルールに関連付けてファイル制御または AMP を実行すると、システムはこのオプションを自動的に有効にします。シスコ は、このオプションを有効のままにすることを推奨します。許可された接続のファイルおよびマルウェア イベント ロギングの無効化(33-7 ページ)を参照してください。

ステップ 7　接続イベントの送信先を指定します。次の選択肢があります。

- ASA FirePOWER モジュールに接続イベントを送信するには、[イベント ビューア(Event Viewer)] を選択します。このオプションは、モニタ ルールに対して無効にできません。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。オプションで、syslog アラート応答を追加するには、追加アイコン( )をクリックします。Syslog アラート応答の作成(35-4 ページ)を参照してください。
- イベントを SNMP トラップ サーバに送信する場合は、[SNMP トラップ(SNMP Trap)] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン( )をクリックして 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(35-2 ページ)を参照)。

接続イベントで ASA FirePOWER モジュール ベースの分析を実行する場合は、イベントをイベント ビューアに送信する必要があります。詳細については、ASA FirePOWER モジュールまたは外部サーバへの接続のロギング(33-4 ページ)を参照してください。

ステップ 8　ルールを保存するために [ASA FirePOWER の変更の保存(Store ASA FirePOWER Changes)] をクリックします。

ルールが保存されます。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。設定変更の展開(4-12 ページ) を参照してください。

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た接続のロギング

ライセンス:任意

アクセス コントロール ポリシーのデフォルト アクションによって処理されたトラフィックの接続をロギングできます。デフォルト アクションによって、システムがポリシー内のアクセス コントロール ルールのいずれにも一致しないトラフィックを処理する方法が決まります(トラフィックに一致しロギングするが、処理または検査はしないモニタ ルールを除く)。デフォルト処理の設定およびネットワーク トラフィックのインスペクション(4-5 ページ)を参照してください。

ポリシーのデフォルト アクションによって処理された接続のメカニズムとオプションは、次の表で示すように、個々のアクセス コントロール ルールによって処理された接続のロギング オプションとほとんど同じです。つまり、ブロックされたトラフィックを除き、システムは接続の開始と終了をロギングし、ユーザは接続イベントを ASA FirePOWER モジュール、または外部 syslog または SNMP トラップ サーバに送信できます。

表 ***33-3***　アクセス コントロールのデフォルト アクションのロギング オプション

デフォルト アクション	比較対象	参照先
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)	ブロック ルール	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(33-5 ページ)
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)	信頼ルール	信頼されている接続のロギングについて(33-5 ページ)
侵入防御(Intrusion Prevention)	関連付けられた侵入ポリシーを持つ許可ルール	許可された接続のロギングについて(33-6 ページ)

しかし、アクセス コントロール ルールによって処理された接続のロギングとデフォルト アクションによって処理された接続のロギングにはいくつかの違いがあります。

- デフォルト アクションにはファイル ロギング オプションはありません。デフォルト アクションを使用して、ファイル制御または AMP を実行できません。
- アクセス コントロールのデフォルト アクションに関連付けられた侵入ポリシーによって侵入イベントが生成された場合、システムは、そのイベントに関連する接続の終了を自動的にログに記録しません。これは、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。

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

デフォルト アクションに対してロギングを無効にしても、接続が以前に少なくとも 1 つのアクセス コントロールのモニタ ルールに一致した場合、そのルールに一致する接続の接続終了イベントは引き続き ASA FirePOWER モジュールにロギングされる場合があることに注意してください。

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たトラフィックの接続をログに記録するには、次の手順を実行します。

ステップ 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。

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。

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）] タブに焦点が置かれています。

ステップ 3　[デフォルトアクション（Default Action）] ドロップダウンリストの横にあるロギング アイコン（ ）をクリックします。

[ロギング（Logging）] ポップアップ ウィンドウが表示されます。

ステップ 4　接続の開始および終了時点でロギングを行うか、接続の終了時点でロギングを行うか、または接続のロギングを行わないかを指定します。

単一のブロックされていない接続の場合、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ます。ブロックされたトラフィックは追加のインスペクションなしですぐに拒否されるため、システムはすべてのトラフィックをブロックする（Block All Traffic）デフォルト アクションに対する接続開始イベントのみをロギングします。このため、デフォルト アクションを [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）] に設定すると、接続の開始時点でロギングを行うよう指示するプロンプトが表示されます。

ステップ 5　接続イベントの送信先を指定します。次の選択肢があります。

- ASA FirePOWER モジュールに接続イベントを送信するには、[イベント ビューア（Event Viewer）] を選択します。このオプションは、モニタ ルールに対して無効にできません。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。オプションで、syslog アラート応答を追加するには、追加アイコン（ ）をクリックします。Syslog アラート応答の作成（35-4 ページ）を参照してください。
- イベントを SNMP トラップ サーバに送信する場合は、[SNMP トラップ（SNMP Trap）] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン（ ）をクリックして 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（35-2 ページ）を参照）。

接続イベントで ASA FirePOWER モジュール ベースの分析を実行する場合は、イベントをイベント ビューアに送信する必要があります。詳細については、ASA FirePOWER モジュールまたは外部サーバへの接続のロギング（33-4 ページ）を参照してください。

ステップ 6　**[Store ASA FirePOWER** の変更の保存（**Store ASA FirePOWER Changes**）**]** をクリックします。

ポリシーが保存されます。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。設定変更の展開（4-12 ページ） を参照してください。

接続で検出された URL のロギング

ライセンス：任意

HTTP トラフィックで、接続終了イベントを ASA FirePOWER モジュールにロギングすると、システムはセッション中にモニタ対象のホストが要求した URL を記録します。

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

URL のロギングを無効にしても、URL フィルタリングには影響しません。アクセス コントロール ルールにより、要求された URL、そのカテゴリ、およびレピュテーションに基づいて、トラフィックが適切にフィルタリングされます。システムが、これらのルールによって処理されたトラフィックで要求された個々の URL を記録しないだけです。詳細については、URL のブロッキング（8-8 ページ）を参照してください。

保存する **URL** の文字数をカスタマイズするには、次の手順を実行します。

ステップ **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。

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

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。

ステップ **3**　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ **4**　[全般設定（General Settings）] の横にある編集アイコン（）をクリックします。

[全般設定（General Settings）] ポップアップ ウィンドウが表示されます。

ステップ **5**　接続イベントで保存する **URL** の最大文字数を入力します。

0 ～ 4096 の値を指定できます。保管する文字数をゼロにすると、URL フィルタリングを無効にすることなく URL の保管が無効になります。

ステップ **6**　[OK] をクリックします。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ **7**　[Store ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

ポリシーが保存されます。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。設定変更の展開（4-12 ページ）を参照してください。

暗号化された接続のロギング

ライセンス:任意

アクセス コントロールの一部として、*SSL* インスペクション機能を使用することで、SSL ポリシーを使用してアクセス コントロール ルールによるさらなる評価のために暗号化されたトラフィックを復号できます。システムがトラフィックを後でどのように処理または検査するかにかかわらず、これらの復号された接続のログを記録するようにシステムに強制できます。また、暗号化されたトラフィックをブロックするとき、または復号せずにトラフィックがアクセス コントロール ルールに渡されることを許可するときに、接続をロギングすることもできます。

暗号化セッションの接続ログには、セッションの暗号化に使用される証明書など、暗号化の詳細が含まれます。クリティカルな接続のみをログに記録するように、SSL ポリシーの暗号化されたセッションの接続ロギングは SSL ルールごとに設定します。

詳細については、次の項を参照してください。

- SSL ルールによる復号可能接続のロギング（33-15 ページ）
- 暗号化された接続および復号できない接続のデフォルトのロギング設定（33-16 ページ）

SSL ルールによる復号可能接続のロギング

ライセンス:任意

SSL ポリシー内では、*SSL* ルールは複数の管理対象デバイス間で暗号化されたトラフィックを処理する詳細な方法を提供します。クリティカルな接続のみをロギングできるように、SSL ルールごとに接続ロギングを有効にします。あるルールに対して接続ロギングを有効にすると、システムはそのルールによって処理されるすべての接続をロギングします。

SSL ポリシーによって検査される暗号化された接続の場合、接続イベントのログは、外部の syslog や SNMP トラップ サーバに記録できます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続（[ブロック（Block）]、[リセットしてブロック（Block with reset）]）の場合、システムは即座にセッションを終了し、イベントを生成します。
- モニタ対象の接続（[モニタ（Monitor）]）およびアクセス コントロール ルールに渡す接続（[復号する（Decrypt）]、[復号しない（Do not decrypt）]）の場合、アクセス コントロール ルールまたはそのセッションを後で処理するデフォルト アクションのロギング設定に関係なく、システムはセッション終了時にイベントを生成します。

詳細については、アクセス コントロール ルール アクションがどのようにロギングに影響を及ぼすかについて（33-4 ページ）を参照してください。

復号できる接続をログに記録するには、次の手順を実行します。

ステップ 1　**[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] >** [ポリシー（Policies）] > [SSL] の順に選択します。

[SSL ポリシー（SSL Policy）] ページが表示されます。

ステップ 2　ロギングを設定するルールの横にある編集アイコン（）をクリックします。

SSL ルール エディタが表示されます。

ステップ 3　[ロギング（Logging）] タブを選択します。

[ロギング（Logging）] タブが表示されます。

ステップ 4　[接続の終了時点でロギングを行う（Log at End of Connection）] を選択します。

ステップ 5　接続イベントの送信先を指定します。次の選択肢があります。

- イベントを外部の 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 アラート応答を選択します。オプションで、syslog アラート応答を追加するには、追加アイコン（ ）をクリックします。Syslog アラート応答の作成（35-4 ページ）を参照してください。
- イベントを SNMP トラップ サーバに送信する場合は、[SNMP トラップ（SNMP Trap）] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン（ ）をクリックして 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（35-2 ページ）を参照）。

ステップ 6　[追加（Add）] をクリックして変更を保存します。

変更を反映させるには、SSL ポリシーが関連付けられているアクセス 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（4-12 ページ）を参照してください。

暗号化された接続および復号できない接続のデフォルトのロギング設定

ライセンス：SSL

SSL 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の接続をログに記録できます。これらのロギング設定では、システムが復号できないセッションをどのようにログに記録するかも管理されます。

SSL ポリシーのデフォルト アクションは、ポリシー内のどの SSL ルール（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）にも一致しない暗号化されたトラフィックをシステムがどのように処理するかを決定します。SSL ポリシーに SSL ルールが含まれていない場合、デフォルト アクションは、ネットワーク上のすべての暗号化セッションがどのようにログに記録されるかを決定します。詳細については、暗号化トラフィックのデフォルトの処理と検査の設定（12-4 ページ）を参照してください。

接続イベントを外部の syslog や SNMP トラップ サーバにロギングするように SSL ポリシーのデフォルト アクションを設定できます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続（[ブロック（Block）]、[リセットしてブロック（Block with reset）]）の場合、システムは即座にセッションを終了し、イベントを生成します。
- 暗号化されていない接続をアクセス コントロール ルールに渡すことを許可する接続の場合（[復号しない（Do not decrypt）]、システムはセッションの終了時にイベントを生成します。

SSL ポリシーのデフォルト アクションのロギングを無効にしても、接続が以前に少なくとも 1 つの SSL モニタ ルールに一致していた場合、または後でアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに一致する場合は、接続終了イベントが引き続きロギングされる可能性があることに注意してください。

暗号化されたトラフィックおよび復号できないトラフィックのデフォルトの処理を設定するには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin/Security Approver

ステップ 1　**[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] >** [ポリシー（Policies）] > [SSL] の順に選択します。

[SSL ポリシー（SSL Policy）] ページが表示されます。

ステップ 2　[デフォルトアクション（Default Action）] ドロップダウンリストの横にあるロギング アイコン（ ）をクリックします。

[ロギング（Logging）] ポップアップ ウィンドウが表示されます。

ステップ 3　[接続の終了時点でロギングを行う（Log at End of Connection）] を選択して、接続イベントのロギングを有効にします。

ステップ 4　接続イベントの送信先を指定します。次の選択肢があります。

- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。オプションで、追加アイコン（ ）をクリックすることで、syslog アラート応答を設定できます。Syslog アラート応答の作成（35-4 ページ）を参照してください。
- イベントを SNMP トラップ サーバに送信する場合は、[SNMP トラップ（SNMP Trap）] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン（ ）をクリックすることで、SNMP アラート応答を設定できます。SNMP アラート応答の作成（35-2 ページ）を参照してください。

ステップ 5　[OK] をクリックして変更を保存します。

変更を反映させるには、SSL ポリシーが関連付けられているアクセス 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（4-12 ページ）を参照してください。

イベントの表示

ASA FirePOWER モジュールによって検査されたトラフィックについてロギングした、リアルタイム イベントを表示できます。

(注) モジュールがメモリにキャッシュするのは、直近の 100 個のイベントのみです。

詳細については、次の項を参照してください。

- ASA FirePOWER リアルタイム イベントへのアクセス(34-1 ページ)
- ASA FirePOWER イベント タイプについて(34-2 ページ)
- ASA FirePOWER イベントのイベント フィールド(34-3 ページ)
- 侵入ルールの分類(34-12 ページ)

ASA FirePOWER リアルタイム イベントへのアクセス

いくつかの定義済みイベント ビューで ASA FirePOWER モジュールによって検出されたイベントを表示できます。または、カスタム イベント ビューを作成して、選択したイベント フィールドを表示できます。

(注) モジュールがメモリにキャッシュするのは、直近の 100 個のイベントのみです。

ASA FirePOWER イベントを表示するには、次の手順を実行します。

ステップ **1** [モニタリング(Monitoring)] > [ASA FirePOWER モニタリング(ASA FirePOWER Monitoring)] > [リアルタイム イベント(Real-time Eventing)] の順に選択します。

ステップ **2** 次の 2 つの選択肢があります。

- 表示するイベント タイプの既存のタブをクリックします。このタイプには、接続イベント、セキュリティ インテリジェンス イベント、侵入イベント、ファイル イベント、またはマルウェア イベントがあります。
- カスタム イベント ビューを作成し、ビューに含めるイベント フィールドを選択するには、[+] アイコンをクリックします。

詳細については、ASA FirePOWER イベント タイプについて(34-2 ページ)および ASA FirePOWER イベントのイベント フィールド(34-3 ページ)を参照してください。

ASA FirePOWER イベント タイプについて

ASA FirePOWER モジュールには、5 つのイベント タイプ（接続イベント、セキュリティ インテリジェンス イベント、侵入イベント、ファイル イベント、およびマルウェア イベント）のイベント フィールドを表示する、リアルタイム イベント ビューがあります。

接続イベント

接続イベントと呼ばれる接続ログには、検出されたセッションに関するデータが含まれています。個々の接続イベントで入手可能な情報はいくつかの要因に応じて異なりますが、一般的には次のものがあります。

- タイムスタンプ、送信元と宛先の IP アドレス、入出力ゾーン、接続を処理したデバイスなど、基本的な接続特性
- アプリケーション、要求される URL、または接続に関連付けられているユーザなど、システムによって検出または推測される追加の接続特性
- どのポリシーのどのアクセス コントロール ルール（または他の設定）がトラフィックを処理したか、接続が許可またはブロックされているかなど、接続がログに記録された理由に関するメタデータ

アクセス コントロールでさまざまな設定を行うことで、ログに記録する接続の種類、接続をログに記録する時期、およびデータを保存する場所をきめ細かく制御できます。アクセス コントロール ポリシーが正常に処理できる接続をログに記録できます。接続のロギングは、次の状況で有効にすることができます。

- 接続がレピュテーション ベースのセキュリティ インテリジェンス機能によってブラックリスト登録（ブロック）またはモニタされた場合
- 接続がアクセス コントロール ルールまたはアクセス 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た場合

設定するロギングに加えて、禁止されたファイル、マルウェア、または侵入の試みをシステムが検出した場合には、ほとんどの接続を自動的にログに記録します。

セキュリティ インテリジェンス イベント

セキュリティ インテリジェンス ロギングを有効にすると、ブラックリストの一致によってセキュリティ インテリジェンス イベントおよび接続イベントが自動的に生成されます。セキュリティ インテリジェンス イベントは特殊なタイプの接続イベントで、単独で表示して分析できます。セキュリティ インテリジェンス ブラックリスト登録の決定を含む、接続ロギングの設定の詳細については、ネットワーク トラフィックの接続のロギング（33-1 ページ）を参照してください。

ヒント　特に断りがない限り、接続イベントに関する一般情報も、セキュリティ インテリジェンス イベントに関係します。セキュリティ インテリジェンスの詳細については、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。

侵入イベント

システムは、ネットワークを通過するパケットを検査し、ホストとそのデータの可用性、整合性、および機密性に影響を与える可能性がある悪意のあるアクティビティについて調べます。システムは、侵入の可能性を特定すると侵入イベントを生成します。これは、エクスプロイトの日付、時刻、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報の記録です。

ファイル イベント

ファイル イベントは、システムがネットワーク トラフィック内で検出した（およびオプションでブロックした）ファイルを表します。

システムは、現在適用されているファイル ポリシーのルールに従って、管理対象デバイスがネットワーク トラフィック内のファイルを検出またはブロックしたときに生成されたファイル イベントを記録します。

マルウェア イベント

マルウェア イベントは、システムがネットワーク トラフィック内で検出した（およびオプションでブロックした）マルウェア ファイルを表します。

マルウェア ライセンスを使用すると、ASA FirePOWER モジュールは全体的なアクセス コントロール設定の一部として、ネットワーク トラフィック内のマルウェアを検出できます。ファイル ポリシーの概要と作成（32-4 ページ）を参照してください。

以下のシナリオでは、マルウェア イベントが生成される可能性があります。

- 管理対象デバイスが一連の特定のファイル タイプのいずれかを検出すると、ASA FirePOWER モジュールはマルウェア クラウド ルックアップを実行します。これにより、ファイル性質として `Malware`、`Clean`、または `Unknown` が ASA FirePOWER モジュールに返されます。
- ASA FirePOWER モジュールがクラウドとの接続を確立できない場合や、その他の理由でクラウドが使用できない場合、ファイル性質は `Unavailable` になります。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。
- クリーン リストに含まれているファイルを管理対象デバイスが検出した場合、ASA FirePOWER モジュールはファイル性質として `Clean` をそのファイルに割り当てます。

ASA FirePOWER モジュールは、ファイルの検出と性質のレコードを、他のコンテキスト データとともにマルウェア イベントとして記録します。

ネットワーク トラフィックで検出され、ASA FirePOWER モジュールによってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。これは、システムがファイル内のマルウェアを検出するために、まずそのファイル自体を検出する必要があるためです。

ASA FirePOWER イベントのイベント フィールド

Action

接続イベントまたはセキュリティ インテリジェンス イベントの場合、接続をロギングしたアクセス コントロール ルールまたはデフォルト アクションに関連付けられたアクション。

- [許可（Allow）] は、明示的に許可されてユーザがバイパスする、インタラクティブにブロックされる接続を表します。
- [信頼（Trust）] は、信頼できる接続を表します。最初のパケットが信頼ルールによって検出された TCP 接続のみ、接続終了イベントを生成します。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。
- [ブロック（Block）] と [リセットしてブロック（Block with reset）] は、ブロックされた接続を表します。さらにシステムは、[ブロック（Block）] アクションを、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に記載された接続、侵入ポリシーによってエクスプロイトが検出された接続、ファイル ポリシーによってファイルがブロックされた接続と関連付けます。

- [インタラクティブ ブロック（Interactive Block）] と [リセットしてインタラクティブ ブロック（Interactive Block with reset）] は、システムがインタラクティブ ブロック ルールを使用して最初にユーザの HTTP 要求をブロックしたときにロギングできる接続開始イベントをマークします。システムが表示する警告ページでユーザがクリック操作をすると、そのセッションについてロギングするその他の接続イベントは、アクションが [許可（Allow）] になります。
- [デフォルト アクション（Default Action）] は、デフォルト アクションによって接続が処理されたことを示します。
- セキュリティ インテリジェンスによってモニタされている接続の場合、そのアクションは、接続によってトリガーされる最初の（モニタ以外の）アクセス コントロール ルールのアクションであるか、またはデフォルト アクションです。同様に、モニタ ルールに一致するトラフィックは常に後続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 ルールによってロギングされた接続と関連付けられたアクションが [モニタ（Monitor）] になることはありません。

ファイル イベントまたはマルウェア イベントの場合、ファイルが一致したルールのルール アクションに関連付けられているファイル ルール アクションと、関連するファイル ルール アクションのオプション。

許可された接続（**Allowed Connection**）

システムがイベントのトラフィック フローを許可したかどうか。

Application

接続で検出されたアプリケーション。

アプリケーションのビジネスとの関連性（**Application Business Relevance**）

接続で検出されたアプリケーション トラフィックに関連するビジネス関連性：`Very High`、`High`、`Medium`、`Low`、または `Very Low`。接続で検出されたアプリケーションのタイプごとに、関連するビジネス関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

アプリケーション カテゴリ（**Application Categories**）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示すカテゴリ。

アプリケーションのリスク（**Application Risk**）

接続で検出されたアプリケーション トラフィックに関連するリスク：`Very High`、`High`、`Medium`、`Low`、または `Very Low`。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

アプリケーションタグ（**Application Tag**）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示すタグ。

ブロック タイプ（**Block Type**）

イベントのトラフィック フローと一致するアクセス コントロール ルールで指定されたブロックのタイプ。ブロックまたはインタラクティブ ブロック。

クライアント（**Client**）

接続で検出されたクライアント アプリケーション。

接続に使用されている特定のクライアントをシステムが特定できなかった場合、このフィールドは汎用的な名称としてアプリケーション プロトコル名の後に `client` を付加して `FTP client` などと表示します。

クライアントのビジネスとの関連性（**Client Business Relevance**）

接続で検出されたクライアント トラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたクライアントのタイプごとに、ビジネスとの関連性が関連付けられています。このフィールドは、最も低いもの（関連性が最も低い）を表示します。

クライアント カテゴリ（**Client Categories**）

クライアントの機能を理解するのに役立つ、トラフィックで検出されたクライアントの特性を示すカテゴリ。

クライアント リスク（**Client Risk**）

接続で検出されたクライアント トラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出されたクライアントのタイプごとに、リスクが関連付けられています。このフィールドは、最も高いものを表示します。

クライアント タグ（**Client Tag**）

クライアントの機能を理解するのに役立つ、トラフィックで検出されたクライアントの特性を示すタグ。

クライアント バージョン（**Client Version**）

接続で検出されたクライアントのバージョン。

Connection

内部的に生成されたトラフィック フローの固有 ID。

接続ブロックタイプ インジケータ（**Connection Blocktype Indicator**）

イベントのトラフィック フローと一致するアクセス コントロール ルールで指定されたブロックのタイプ。ブロックまたはインタラクティブ ブロック。

接続バイト（**Connection Bytes**）

接続の合計バイト数。

接続時間（**Connection Time**）

接続の開始時刻。

接続タイムスタンプ（**Connection Timestamp**）

接続が検出された時刻。

コンテキスト

トラフィックが通過したセキュリティ コンテキストを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチコンテキスト モードの デバイスだけです。

拒否された接続（**Denied Connection**）

システムがイベントのトラフィック フローを拒否したかどうか。

宛先の国または大陸（**Destination Country and Continent**）

受信ホストの国および大陸。

宛先 **IP**（**Destination IP**）

受信ホストが使用する IP アドレス。

宛先ポート、宛先ポート コード、宛先ポート/ICMP コード（**Destination Port, Destination Port Icode, Destination Port/ICMP Code**）

セッション レスポンダが使用する宛先ポートまたは ICMP コード。

方向（**Direction**）

ファイルの送信方向。

傾向（**Disposition**）

以下のファイル性質のいずれかです。

- マルウェア（Malware）：クラウドでそのファイルがマルウェアとして分類されていることを示します。
- クリーン（Clean）：クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。
- 不明（Unknown）：クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。ファイルは分類されていません。
- カスタム検出（Custom Detection）：ユーザがカスタム検出リストにファイルを追加したことを示します。
- 使用不可（Unavailable）：ASA FirePOWER モジュールがマルウェア クラウド ルックアップを実行できなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。
- N/A：[ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] ルールがファイルを処理し、ASA FirePOWER モジュールがマルウェア クラウド ルックアップを行わなかったことを示します。

出力インターフェイス（**Egress Interface**）

接続に関連付けられた出力インターフェイス。展開環境に非同期のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインターフェイス セットに属する場合があることに注意してください。

出力セキュリティ ゾーン（**Egress Security Zone**）

接続に関連付けられた出力セキュリティ ゾーン。

イベント

イベントのタイプ。

イベント（マイクロ秒）（**Event Microseconds**）

イベントが検出された時刻（マイクロ秒単位）。

イベント（秒）（**Event Seconds**）

イベントが検出された時刻（秒単位）。

イベント タイプ（**Event Type**）

イベントのタイプ。

ファイル カテゴリ（**File Category**）

ファイル タイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイル など）。

ファイル イベント タイムスタンプ（**File Event Timestamp**）
ファイルまたはマルウェア ファイルが作成された日時。

ファイル名（**File Name**）
ファイルまたはマルウェア ファイルの名前。

ファイル **SHA256**（**File SHA256**）
ファイルの SHA-256 ハッシュ値。

ファイル サイズ（**File size**）
ファイルまたはマルウェア ファイルのサイズ（KB 単位）。

ファイル タイプ（**File Type**）
ファイルまたはマルウェア ファイルのファイル タイプ（`HTML` や `MSEXE` など）。

ファイル**/**マルウェア ポリシー（**File/Malware Policy**）
イベントの生成に関連付けられているファイル ポリシー。

ファイルログ ブロックタイプ インジケータ（**Filelog Blocktype Indicator**）
イベントのトラフィック フローと一致するファイル ルールで指定されたブロックのタイプ。ブロックまたはインタラクティブ ブロック。

ファイアウォール ポリシー ルール**/SI** カテゴリ（**Firewall Policy Rules/SI Category**）
接続でブラックリストに記載された IP アドレスを表すか、もしくはそれを含む、ブラックリストに記載されたオブジェクトの名前。セキュリティ インテリジェンスのカテゴリは、ネットワーク オブジェクトまたはグループ、グローバル ブラックリスト、カスタム セキュリティ インテリジェンスのリストまたはフィード、またはインテリジェンス フィードのカテゴリのいずれかの名前にすることができます。[理由（Reason）] が [IP ブロック（IP Block）] または [IP モニタ（IP Monitor）] の場合にのみ、このフィールドに値が入力されることに注意してください。セキュリティ インテリジェンス イベントのビューでは、エントリに必ず理由が表示されます。

ファイアウォール ルール（**Firewall Rule**）
接続を処理したアクセス コントロール ルールまたはデフォルト アクションと、その接続に一致した最大 8 つのモニタ ルール。

最初のパケット（**First Packet**）
セッションの最初のパケットが検出された日時。

HTTP リファラ（**HTTP Referrer**）
接続で検出された HTTP トラフィックの要求 URL のリファラを示す HTTP リファラ（他の URL へのリンクを提供した Web サイト、他の URL からリンクをインポートした Web サイトなど）。

IDS の分類（**IDS Classification**）
イベントを生成したルールが属する分類。ルールの分類名と番号のリストについては、ルールの分類の表を参照してください。

影響（**Impact**）
このフィールドの影響レベルは、侵入データ、ネットワーク検出データ、脆弱性情報との関係を示します。

影響フラグ（**Impact Flag**）

「影響（Impact）」を参照してください。

入力インターフェイス（**Ingress Interface**）

接続に関連付けられた入力インターフェイス。展開環境に非同期のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインターフェイス セットに属する場合があることに注意してください。

入力セキュリティ ゾーン（**Ingress Security Zone**）

接続に関連付けられた入力セキュリティ ゾーン。

イニシエータ バイト数（**Initiator Bytes**）

セッション イニシエータが送信した合計バイト数。

イニシエータの国または大陸（**Initiator Country and Continent**）

ルーティング可能な IP が検出された場合の、セッションを開始したホスト IP アドレスに関連付けられた国および大陸。

イニシエータ **IP**（**Initiator IP**）

セッション レスポンダを開始したホスト IP アドレス（および DNS 解決が有効化されている場合はホスト名）。

イニシエータ パケット（**Initiator Packets**）

セッション イニシエータが送信した合計パケット数。

インライン結果（**Inline Result**）

次のいずれかです。

- 黒い下矢印。ルールをトリガーとして使用したパケットをシステムがドロップしたことを示します
- 灰色の下矢印。[インライン時にドロップ（Drop when Inline）] 侵入ポリシー オプション（インライン展開環境）を有効にした場合、またはシステムがプルーニングしている間に [ドロップしてイベントを生成する（Drop and Generate）] ルールがイベントを生成した場合、IPS がパケットをドロップしたことを示します
- ブランク。トリガーとして使用されたルールが [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていないことを示します
- 侵入ポリシーのルールの状態またはインライン ドロップ動作にかかわらず、インライン インターフェイスがタップ モードになっている場合を含め、パッシブ展開環境ではシステムはパケットをドロップしないことに注意してください。

IPS ブロックタイプ インジケータ（**IPS Blocktype Indicator**）

イベントのトラフィック フローと一致する侵入ルールのアクション。

最後のパケット（**Last Packet**）

セッションの最後のパケットが検出された日時。

MPLS ラベル（**MPLS Label**）

この侵入イベントをトリガーしたパケットと関連付けられているマルチプロトコル ラベル スイッチング ラベル。

マルウェア ブロックタイプ インジケータ（**Malware Blocktype Indicator**）

イベントのトラフィック フローと一致するファイル ルールで指定されたブロックのタイプ。ブロックまたはインタラクティブ ブロック。

メッセージ（**Message**）

イベントを説明するテキスト。

ルールベースの侵入イベントの場合、イベント メッセージはルールから取得されます。デコーダベースおよびプリプロセッサベースのイベントの場合は、イベント メッセージはハード コーディングされています。

マルウェア イベントの場合は、マルウェア イベントに関連付けられている追加情報。ネットワークベースのマルウェア イベントの場合、このフィールドにデータが入れられるのは、性質が変更されたファイルだけです。

モニタ ルール（**Monitor Rules**）

その接続で一致する 8 つまでのモニタ ルール。

Netbios ドメイン（**Netbios Domain**）

セッションで使用された NetBIOS ドメイン。

ポリシー

イベントの生成に関連付けられているアクセス コントロール ポリシー、侵入ポリシー、またはネットワーク分析ポリシー（NAP）（ある場合）。

ポリシー リビジョン（**Policy Revision**）

イベントの生成に関連付けられているアクセス コントロール ポリシー、ファイル ポリシー、侵入ポリシー、またはネットワーク分析ポリシー（NAP）（ある場合）のリビジョン。

[プライオリティ（**Priority**）**]**

シスコ VRT で指定されたイベントの優先度。

プロトコル

接続で検出されたプロトコル。

理由（**Reason**）

次の場合に接続がロギングされた 1 つまたは複数の原因。

- [ユーザ バイパス（User Bypass）] は、システムが最初はユーザの HTTP 要求をブロックしたが、ユーザが警告ページでクリック操作をして、最初に要求していたサイトへ進むのを選択したことを示します。[ユーザ バイパス（User Bypass）] の原因は必ず [許可（Allow）] のアクションと対として組み合わされます。
- [IP ブロック（IP Block）] は、システムがセキュリティ インテリジェンス データに基づいて、インスペクションなしで接続を拒否したことを示します。[IP ブロック（IP Block）] の原因は必ず [ブロック（Block）] のアクションと対として組み合わされます。
- [IP モニタ（IP Monitor）] は、システムがセキュリティ インテリジェンス データに基づいて接続を拒否するはずでしたが、ユーザが接続を拒否せずモニタするように設定したことを示します。
- [ファイル モニタ（File Monitor）] は、システムが接続において特定のファイルの種類を検出したことを示します。

- [ファイル ブロック（File Block）] は、ファイルまたはマルウェア ファイルが接続に含まれており、システムがその送信を防いだことを示します。[ファイル ブロック（File Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
- [ファイル カスタム検出（File Custom Detection）] は、カスタム検出リストにあるファイルが接続に含まれており、システムがその送信を防いだことを示します。
- [ファイル復帰許可（File Resume Allow）] は、ファイル送信がはじめに [ファイル ブロック（Block Files）] または [マルウェア ブロック（Block Malware）] ファイル ルールによってブロックされたことを示します。ファイルを許可する新しいアクセス コントロール ポリシーが適用された後、HTTP セッションが自動的に再開しました。この原因は、インライン構成のみで表示されることに注意してください。
- [ファイル復帰ブロック（File Resume Block）] は、ファイル送信がはじめに [ファイル検出（Detect Files）] または [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] ファイル ルールによって許可されたことを示します。ファイルをブロックする新しいアクセス コントロール ポリシーが適用された後、HTTP セッションが自動的に停止しました。この原因は、インライン構成のみで表示されることに注意してください。
- [侵入ブロック（Intrusion Block）] は、接続で検出されたエクスプロイト（侵入ポリシー違反）をシステムがブロックしたか、ブロックするはずだったことを示します。[侵入ブロック（Intrusion Block）] の原因は、ブロックされたエクスプロイトの場合は [ブロック（Block）]、ブロックされるはずだったエクスプロイトの場合は [許可（Allow）] のアクションと対として組み合わされます。
- [侵入モニタ（Intrusion Monitor）] は、接続で検出されたエクスプロイトをシステムが検出したものの、ブロックしなかったことを示します。これは、トリガーされた侵入ルールの状態が [イベントを生成する（Generate Events）] に設定されている場合に発生します。

受信時間（**Receive Times**）

宛先ホストまたはレスポンダがイベントに応答した時刻。

参照ホスト（**Referenced Host**）

接続のプロトコルが DNS、HTTP、または HTTPS の場合、このフィールドにはそれぞれのプロトコルが使用していたホスト名が表示されます。

レスポンダ バイト数（**Responder Bytes**）

セッション レスポンダが送信した合計バイト数。

レスポンダの国または大陸（**Responder Country and Continent**）

ルーティング可能な IP が検出された場合の、セッション レスポンダのホスト IP アドレスに関連付けられた国および大陸。

レスポンダ パケット（**Responder Packets**）

セッション レスポンダが送信した合計パケット数。

レスポンダ **IP**（**Responder IP**）

セッション イニシエータに応答したホスト IP アドレス（および DNS 解決が有効化されている場合はホスト名）。

シグネチャ（**Signature**）

イベントのトラフィックと一致する侵入ルールのシグネチャ ID。

ソースの国または大陸（**Source Country and Continent**）
送信元ホストの国および大陸。

ソース **IP**
侵入イベントで送信元ホストが使用する IP アドレス。

送信元または宛先（**Source or Destination**）
イベントの接続を送信元/宛先とするホスト。

送信元ポート、送信元ポート タイプ、送信元ポート**/ICMP** タイプ（**Source Port, Source Port Type, Source Port/ICMP Type**）
セッション イニシエータが使用する送信元ポートまたは ICMP タイプ。

TCP フラグ（**TCP Flags**）
接続で検出された TCP フラグ。

URL
セッション中にモニタ対象のホストによって要求された URL。

URL カテゴリ（**URL Category**）
セッション中にモニタ対象のホストによって要求された URL に関連付けられているカテゴリ（使用可能な場合）。

URL レピュテーション（**URL Reputation**）
セッション中にモニタ対象のホストによって要求された URL に関連付けられているレピュテーション（使用可能な場合）。

URL レピュテーション スコア（**URL Reputation Score**）
セッション中にモニタ対象のホストによって要求された URL に関連付けられているレピュテーション スコア（使用可能な場合）。

ユーザ（**User**）
イベントが発生したホスト（受信 **IP**）のユーザ

ユーザ エージェント（**User Agent**）
接続で検出された HTTP トラフィックから取得したユーザ エージェント アプリケーションの情報。

VLAN
イベントをトリガーしたパケットに関連付けられている最内部 VLAN ID。

Web アプリケーションのビジネスとの関連性（**Web App Business Relevance**）
接続で検出された Web アプリケーション トラフィックに関連するビジネス関連性: `Very High`、`High`、`Medium`、`Low`、または `Very Low`。接続で検出された Web アプリケーションのタイプごとに、ビジネスとの関連性が関連付けられています。このフィールドは、最も低いもの（関連性が最も低い）を表示します。

Web アプリケーションのカテゴリ（**Web App Categories**）

Web アプリケーションの機能を理解するのに役立つ、トラフィックで検出された Web アプリケーションの特性を示すカテゴリ。

Web アプリケーションのリスク（**Web App Risk**）

接続で検出された Web アプリケーション トラフィックに関連するリスク：`Very High`、`High`、`Medium`、`Low`、または `Very Low`。接続で検出された Web アプリケーションのタイプごとに、リスクが関連付けられています。このフィールドは、最も高いものを表示します。

Web アプリケーションのタグ（**Web App Tag**）

Web アプリケーションの機能を理解するのに役立つ、トラフィックで検出された Web アプリケーションの特性を示すタグ。

Web アプリケーション（**Web Application**）

トラフィックで検出された Web アプリケーション。

侵入ルールの分類

侵入ルールには、攻撃の分類が含まれています。次の表に、それぞれの分類の名前と番号を示します。

表 ***34-1***　　ルールの分類

番号	分類名	説明
1	not-suspicious	不審ではないトラフィック
2	unknown	不明なトラフィック
3	bad-unknown	有害な可能性のあるトラフィック
4	attempted-recon	情報漏えいが試行された
5	successful-recon-limited	情報漏えいが発生
6	successful-recon-largescale	大規模な情報漏えい
7	attempted-dos	サービス妨害が試行された
8	successful-dos	サービス妨害（DoS）
9	attempted-user	ユーザ特権の獲得が試行された
10	unsuccessful-user	ユーザ特権の獲得が失敗した
11	successful-user	ユーザ特権の獲得に成功
12	attempted-admin	管理者特権の獲得が試行された
13	successful-admin	管理者特権の獲得に成功
18	rpc-portmap-decode	RPC クエリのデコード
15	shellcode-detect	実行可能コードが検出された
16	string-detect	疑わしい文字列が検出された
17	suspicious-filename-detect	疑わしいファイル名が検出された
18	suspicious-login	疑わしいユーザ名を使用したログイン試行が検出された

表 **34-1**　ルールの分類

番号	分類名	説明
19	system-call-detect	システム コールが検出された
20	tcp-connection	TCP 接続が検出された
21	trojan-activity	ネットワーク トロイの木馬が検出された
22	unusual-client-port-connection	通常とは異なるポートをクライアントが使用していた
23	network-scan	ネットワーク スキャンの検出
24	denial-of-service	サービス妨害攻撃の検出
25	non-standard-protocol	非標準プロトコルまたはイベントの検出
26	protocol-command-decode	一般的なプロトコル コマンド デコード
27	web-application-activity	脆弱な可能性のある Web アプリケーションへのアクセス
36	web-application-attack	Web アプリケーション攻撃
29	misc-activity	その他のアクティビティ
30	misc-attack	その他の攻撃
31	icmp-event	一般的な ICMP イベント
32	inappropriate-content	不適切な内容が検出された
33	policy-violation	企業プライバシー侵害の可能性
34	default-login-attempt	デフォルトのユーザ名とパスワードによるログイン試行
35	sdf	機密データ
36	malware-cnc	既知のマルウェア コマンドと制御トラフィック
37	client-side-exploit	既知のクライアント側エクスプロイト試行
38	file-format	既知の悪意のあるファイルまたはファイル ベースのエクスプロイト

外部アラートの設定

ASA FirePOWER モジュールではイベントのさまざまなビューをモジュール インターフェイス内で提供しますが、重要なシステムの継続的なモニタリングを容易にするために外部イベント通知を設定することもできます。次のいずれかが発生した場合にアラートを生成して、SNMP トラップまたは syslog により通知するように、モジュールを設定できます。

- ネットワークベースのマルウェア イベントまたはレトロスペクティブ マルウェア イベント
- 特定のアクセス コントロール ルールによってトリガーとして使用される接続イベント

ASA FirePOWER モジュールでこれらのアラートが送信されるようにするには、まずアラート応答を作成する必要があります。アラート応答は、アラート送信を計画している外部システムとモジュールが連携できるようにする一連の設定です。それらの設定では、たとえば、SNMP アラート パラメータ、または syslog ファシリティおよびプライオリティを指定する場合があります。

アラート応答を作成した後、アラートをトリガーとして使用するために使用するイベントに関連付けます。アラート応答とイベントを関連付けるための処理は、次のように、イベントのタイプによって異なることに注意してください。

- アラート応答をマルウェア イベントと関連付ける場合は、独自の設定ページを使用します。
- SNMP および syslog アラート応答を接続のログ記録と関連付ける場合は、アクセス コントロール ルールとポリシーを使用します。

ASA FirePOWER モジュールには、実行可能なもう 1 つのタイプのアラートがあります。この場合は、個々の侵入イベントに対して、SNMP、および syslog による侵入イベント通知を設定します。これらの通知は侵入ポリシーで設定します。侵入ルールの外部アラートの設定（36-1 ページ）および SNMP アラートの追加（24-34 ページ）を参照してください。次の表では、アラート生成に必要なライセンスについて説明します。

表 **35-1**　　アラートを生成するためのライセンス要件

アラートを生成する条件	必要なライセンス
侵入イベント	Protection
ネットワークベースのマルウェア イベント	マルウェア
接続イベント	接続をログに記録するために必要なライセンス

詳細については、以下を参照してください。

- アラート応答の使用（35-2 ページ）
- ネットワーク トラフィックの接続のロギング（33-1 ページ）

アラート応答の使用

ライセンス：任意

外部アラートを設定する際の最初の手順はまずアラート応答を作成することです。アラート応答は、アラート送信を計画している外部システムと ASA FirePOWER モジュールが連携できるようにする一連の設定です。アラート応答を作成して、Simple Network Management Protocol（SNMP）トラップまたはシステム ログ（syslog）によりアラートを送信できます。

アラートで受け取る情報は、アラートをトリガーしたイベントのタイプによって異なります。

作成したアラート応答は自動的に有効になります。有効なアラート応答のみがアラートを生成できます。アラートの生成を停止するには、設定を削除する代わりに、一時的にアラート応答を無効にすることができます。

アラート応答は [アラート（Alerts）] ページ（[ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アクション アラート（Actions Alerts）]）で管理します。各アラート応答の横のスライダは有効かどうかを示します。有効なアラート応答のみがアラートを生成できます。このページは、たとえば、アクセス コントロール ルールの接続をログに記録するための設定でアラート応答が使用されているかどうかも示します。該当する列見出しをクリックして、名前、タイプ、使用中ステータス、および有効または無効のステータスでアラート応答をソートできます。列見出しを再度クリックすると、順序が反転します。

詳細については、以下を参照してください。

- SNMP アラート応答の作成（35-2 ページ）
- Syslog アラート応答の作成（35-4 ページ）
- アラート応答の変更（35-6 ページ）
- アラート応答の削除（35-6 ページ）
- アラート応答の有効化と無効化（35-7 ページ）

SNMP アラート応答の作成

ライセンス：任意

SNMPv1、SNMPv2、または SNMPv3 を使用して SNMP アラート応答を作成できます。

（注）　SNMP で 64 ビット値をモニタする場合は、SNMPv2 または SNMPv3 を使用する必要があります。SNMPv1 は 64 ビットのモニタリングをサポートしていません。

SNMP アラート応答を作成する方法：

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アクション アラート（Actions Alerts）] の順に選択します。

[アラート（Alerts）] ページが表示されます。

ステップ **2**　[アラートの作成（Create Alert）] ドロップダウン メニューから、[SNMP アラートの作成（Create SNMP Alert）] を選択します。

[SNMP アラート作成の設定（Create SNMP Alert Configuration）] ポップアップ ウィンドウが表示されます。

ステップ 3　[名前(Name)] フィールドに、SNMP 応答を識別するために使用する名前を入力します。

ステップ 4　[トラップサーバ(Trap Server)] フィールドに、英数字を使用して SNMP トラップ サーバのホスト名または IP アドレスを入力します。

このフィールドに無効な IPv4 アドレス(192.169.1.456 など)を入力した場合でも、システムからの警告がないことに注意してください。無効なアドレスはホスト名として扱われます。

ステップ 5　[バージョン(Version)] ドロップダウンリストから、使用する SNMP バージョンを選択します。

SNMP v3 がデフォルトです。SNMP v1 または SNMP v2 を選択すると、異なるオプションが表示されます。

(注)　SNMPv2 は読み取り専用コミュニティのみをサポートし、SNMPv3 は読み取り専用ユーザのみをサポートしています。

ステップ 6　どのバージョンの SNMP を選択したかに応じて、以下のようにします。

- SNMP v1 または SNMP v2 の場合、英数字または特殊文字(* または $)を使用して、[コミュニティ ストリング(Community String)] フィールドに SNMP コミュニティの名前を入力し、ステップ 12 に進みます。
- SNMP v3 の場合、[ユーザ名(User Name)] フィールドに SNMP サーバで認証するユーザの名前を入力し、次のステップに進みます。

ステップ 7　[認証プロトコル(Authentication Protocol)] ドロップダウンリストから、認証に使用するプロトコルを選択します。

ステップ 8　[認証パスワード(Authentication Password)] フィールドに、SNMP サーバの認証に必要なパスワードを入力します。

ステップ 9　[プライバシー プロトコル(Privacy Protocol)] リストから、[なし(None)] を選択してプライバシー プロトコルを使用しないか、または [DES] を選択してプライバシー プロトコルにデータ暗号規格を使用します。

ステップ 10　[プライバシー パスワード(Privacy Password)] フィールドに、SNMP サーバに必要なプライバシー パスワードを入力します。

ステップ 11　[エンジン ID(Engine ID)] フィールドに、SNMP エンジンの識別子を偶数桁の 16 進表記で入力します。

SNMPv3 を使用する場合、メッセージの符号化には エンジン ID 値が使用されます。SNMP サーバでは、メッセージをデコードするためにこの値が必要です。

シスコは、ASA FirePOWER モジュールの IP アドレスの 16 進数バージョンを使用することを推奨します。たとえば、ASA FirePOWER モジュールの IP アドレスが `10.1.1.77` である場合、`0a01014D0` を使用します。

ステップ 12　[ASA FirePOWER の変更の保存(Store ASA FirePOWER Changes)] をクリックします。

アラート応答が保存され、自動的に有効になります。

Syslog アラート応答の作成

ライセンス:任意

syslog アラート応答を設定する際、syslog サーバで確実に正しく処理されるようにするために、syslog メッセージに関連付けられる重大度とファシリティを指定できます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。ファシリティと重大度は syslog に示される実際のメッセージには表示されませんが、syslog メッセージを受信するシステムに対して、メッセージの分類方法を指示するために使用されます。

ヒント　syslog の機能とその設定方法の詳細については、ご使用のシステムのマニュアルを参照してください。UNIX システムでは、`syslog` および `syslog.conf` の `man` ページで概念情報および設定手順が説明されています。

syslog アラート応答の作成時に任意のタイプのファシリティを選択できますが、syslog サーバに基づいて意味のあるものを選択する必要があります。すべての syslog サーバがすべてのファシリティをサポートしているわけではありません。UNIX syslog サーバの場合、`syslog.conf` ファイルで、どのファシリティがサーバ上のどのログ ファイルに保存されるかを示す必要があります。

次の表に、選択可能な syslog ファシリティを示します。

表 ***35-2***　使用可能な ***syslog*** ファシリティ

ファシリティ	説明
ALERT	アラート メッセージ。
AUDIT	監査サブシステムによって生成されるメッセージ。
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CLOCK	クロック デーモンによって生成されるメッセージ。 Windows オペレーティング システムを実行している syslog サーバは `CLOCK` ファシリティを使用することに注意してください。
CRON	クロック デーモンによって生成されるメッセージ。 Linux オペレーティング システムを実行している syslog サーバは `CRON` ファシリティを使用することに注意してください。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージは表示されるときにコンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。
NTP	NTP デーモンによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザ レベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

次の表に、選択可能な標準の syslog 重大度レベルを示します。

表 **35-3**　***syslog*** 重大度レベル

レベル	説明
ALERT	ただちに修正する必要がある状態。
CRIT	クリティカルな状態。
DEBUG	デバッグ情報を含むメッセージ。
EMERG	すべてのユーザに配信されるパニック状態。
ERR	エラー状態。
INFO	情報メッセージ。
NOTICE	エラー状態ではないが、注意が必要な状態。
WARNING	警告メッセージ。

syslog アラートの送信を開始する前に、syslog サーバがリモート メッセージを受信できることを確認してください。

syslog アラートを作成する方法:

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アクション アラート（Actions Alerts）] の順に選択します。

[アラート（Alerts）] ページが表示されます。[アラートの作成（Create Alert）] ドロップダウン メニューから、[Syslog アラートの作成（Create Syslog Alert）] を選択します。

[Syslog アラート作成の設定（Create Syslog Alert Configuration）] ポップアップ ウィンドウが表示されます。

ステップ **2**　[名前（Name）] フィールドに、保存される応答を識別するために使用する名前を入力します。

ステップ **3**　[ホスト（Host）] フィールドに、syslogサーバのホスト名またはIPアドレスを入力します。

このフィールドに無効な IPv4 アドレス（192.168.1.456 など）を入力した場合でも、システムからの警告がないことに注意してください。無効なアドレスはホスト名として扱われます。

ステップ **4**　[ポート（Port）] フィールドに、サーバが syslog メッセージに使用するポートを入力します。

この値はデフォルトで 514 です。

ステップ **5**　[ファシリティ（Facility）] リストから、ファシリティを選択します。

使用可能なファシリティの一覧については、使用可能な syslog ファシリティの表を参照してください。

ステップ **6**　[重大度（Severity）] リストから、重大度を選択します。

使用可能な重大度の一覧については、syslog 重大度レベルの表を参照してください。

ステップ **7**　[タグ（Tag）] フィールドに、syslog メッセージとともに表示するタグ名を入力します。

タグ名には英数字のみを使用します。スペースまたは下線は使用できません。

例として、syslog に送信されるすべてのメッセージの前に `FromDC` を付ける場合、フィールドに `FromDC` と入力します。

ステップ **8**　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

アラート応答が保存され、自動的に有効になります。

アラート応答の変更

ライセンス:任意

ほとんどのタイプのアラートについて、アラート応答が有効で使用中の場合、アラート応答への変更はすぐに反映されます。ただし、接続イベントをログに記録するアクセス コントロール ルールで使用されるアラート応答の場合、アクセス コントロール ポリシーを再適用するまで変更は有効になりません。

アラート応答を編集する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [アクション アラート(Actions Alerts)] の順に選択します。

[アラート(Alerts)] ページが表示されます。

ステップ 2　編集するアラート応答の横にある編集アイコン( )をクリックします。

そのアラート応答の設定ポップアップ ウィンドウが表示されます。

ステップ 3　必要に応じて変更を加えます。

ステップ 4　[ASA FirePOWER の変更の保存(Store ASA FirePOWER Changes)] をクリックします。

アラート応答が保存されます。

アラート応答の削除

ライセンス:任意

使用中でない任意のアラート応答を削除できます。

アラート応答を削除する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [アクション アラート(Actions Alerts)] の順に選択します。

[アラート(Alerts)] ページが表示されます。

ステップ 2　削除するアラート応答の横にある削除アイコン( )をクリックします。

ステップ 3　アラート応答を削除することを確認します。

アラート応答が削除されます。

アラート応答の有効化と無効化

ライセンス:任意

有効なアラート応答のみがアラートを生成できます。アラートの生成を停止するには、設定を削除する代わりに、一時的にアラート応答を無効にすることができます。無効化するときにアラートが使用中の場合は、無効にしても使用中とみなされることに注意してください。

アラート応答を有効または無効にする方法:

ステップ **1** [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [アクション アラート(Actions Alerts)] の順に選択します。

[アラート(Alerts)] ページが表示されます。

ステップ **2** 有効または無効にするアラート応答の横の有効または無効のスライダをクリックします。

アラート応答が有効だった場合は、無効になります。無効だった場合は、有効になります。

侵入ルールの外部アラートの設定

ASA FirePOWER モジュールでは、ユーザ インターフェイスで侵入イベントのさまざまな側面を表示できますが、重要なシステムを継続的にモニタリングできるように、外部侵入イベント通知を定義することを望んでいる企業もあります。syslog ファシリティへのロギングを有効にしたり、SNMP トラップ サーバにイベント データを送信したりできます。

各侵入ポリシー内では、侵入イベントの通知制限を指定し、外部ロギング ファシリティへの侵入イベント通知をセットアップし、侵入イベントへの外部応答を設定できます。

ヒント アナリストによっては、同じ侵入イベントに対して複数のアラートを受信することは望まないものの、特定の侵入イベントの発生については、頻度を制限したうえで通知を受信したいと考えています。詳細については、ポリシー単位の侵入イベント通知のフィルタリング（24-23 ページ）を参照してください。

侵入ポリシー以外にも、ASA FirePOWER モジュールで実行可能な別のタイプのアラートがあります。特定のアクセス コントロール ルールによって記録された接続イベントなど、他のタイプのイベントに対して SNMP、syslog アラートによる応答を設定できます。詳細については、外部アラートの設定（35-1 ページ）を参照してください。

外部侵入イベント通知の詳細情報については、次の項を参照してください。

- SNMP 応答の使用（36-1 ページ）では、指定された SNMP トラップ サーバにイベント データを送信する場合に設定可能なオプションや、SNMP アラート オプションを指定する手順について説明します。
- Syslog 応答の使用（36-4 ページ）では、外部 syslog にイベント データを送信する場合に設定可能なオプションや、syslog アラート オプションを指定する手順について説明します。

SNMP 応答の使用

ライセンス：Protection

SNMP トラップは、ネットワーク管理に関する通知です。侵入イベントに関する通知を SNMP トラップ（*SNMP* アラートとも呼ばれる）として送信するようにデバイスを設定できます。各 SNMP アラートには次のものが含まれます。

- トラップを生成するサーバの名前
- アラートを検出したデバイスの IP アドレス
- アラートを検出したデバイスの名前
- イベント データ

さまざまな SNMP アラート パラメータを設定できます。使用可能なパラメータは、使用する SNMP のバージョンによって異なります。SNMP アラートを有効化および無効化する方法の詳細については、侵入ポリシーの詳細設定の設定（23-7 ページ）を参照してください。

ヒント　ネットワーク管理システムで Management Information Base（MIB）ファイルが必要な場合は、ASA FirePOWER モジュールの `/etc/sf/DCEALERT.MIB` から取得できます。

SNMPv2 のオプション

SNMPv2 の場合は、次の表で説明しているオプションを指定できます。

表 ***36-1***　***SNMPv2*** のオプション

オプション	説明
トラップ タイプ	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[バイナリとして（as Binary）] を選択できます。そうでない場合は、[文字列として（as String）] を選択します。たとえば、HP Openview では String タイプが必要になります。
トラップ サーバ（Trap Server）	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。
コミュニティ ストリング（Community String）	コミュニティ名。

（注）　SNMPv2 は、読み込み専用コミュニティのみをサポートしています。

SNMPv3 のオプション

SNMPv3 の場合は、次の表で説明しているオプションを指定できます。

（注）　SNMPv3 を使用する場合、アプライアンスは Engine ID 値を使用してメッセージをエンコードします。SNMP サーバでは、メッセージをデコードするためにこの値が必要です。現在、この Engine ID 値は常に、文字列の末尾に `01` が付く、アプライアンスの IP アドレスの 16 進数バージョンになります。たとえば、SNMP アラートを送信するアプライアンスの IP アドレスが `172.16.1.50` である場合、Engine ID は `0xAC10013201` になります。また、アプライアンスの IP アドレスが `10.1.1.77` である場合、Engine ID `0x0a01014D01` が使用されます。

表 ***36-2***　***SNMPv3*** のオプション

オプション	説明
トラップ タイプ	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[バイナリとして（as Binary）] を選択できます。そうでない場合は、[文字列として（as String）] を選択します。たとえば、HP Openview では String タイプが必要になります。
トラップ サーバ（Trap Server）	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。

表 *36-2*　*SNMPv3* のオプション（続き）

オプション	説明
認証パスワード（Authentication Password）	認証に必要なパスワード。SNMPv3 は、設定に応じて Message Digest 5（MD5）ハッシュ関数またはセキュア ハッシュ アルゴリズム（SHA）ハッシュ関数のいずれかを使用し、このパスワードを暗号化します。 認証パスワードを指定すると、認証が有効になります。
プライベート パスワード（Private Password）	プライバシー用の SNMP キー。SNMPv3 は Data Encryption Standard（DES）ブロック暗号を使用して、このパスワードを暗号化します。 プライベート パスワードを指定すると、プライバシーが有効になります。プライベート パスワードを指定する場合は、認証パスワードも指定する必要があります。
ユーザ名（User Name）	SNMP ユーザ名。

（注）　SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

SNMP アラートの設定の詳細については、SNMP 応答の設定（36-3 ページ）を参照してください。

SNMP 応答の設定

ライセンス：Protection

侵入ポリシーで SNMP アラートを設定できます。アクセス コントロール ポリシーの一部としてポリシーを適用すると、システムは SNMP トラップで検出した侵入イベントをすべて通知するようになります。SNMP アラートの詳細については、SNMP 応答の使用（36-1 ページ）を参照してください。

SNMP アラート オプションの設定方法：

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ **2**　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ **3**　左側のナビゲーション パネルの [詳細設定（Advanced Settings）] をクリックします。

[詳細設定（Advanced Settings）] ページが表示されます。

ステップ **4**　外部応答の [SNMP アラート（SNMP Alerting）] が有効かどうかに応じて、次の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[SNMP アラート（SNMP Alerting）] ページが表示されます。

ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 5　IP アドレスに使用するトラップ タイプの形式を [バイナリとして（as Binary）] または [文字列として（as String）] のいずれかに指定します。

（注）　ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[バイナリとして（as Binary）] オプションを使用できます。正常にレンダリングされなかった場合は、[文字列として（as String）] オプションを使用します。たとえば、HP OpenView では [文字列として（as String）] オプションが必要になります。

ステップ 6　SNMPv2 または SNMPv3 を選択します。

- SNMPv2 を設定するには、使用するトラップ サーバの IP アドレスとコミュニティ名を対応するフィールドに入力します。SNMPv2 のオプション（36-2 ページ）を参照してください。
- SNMPv3 を設定するには、使用するトラップ サーバの IP アドレス、認証パスワード、プライベート パスワード、およびユーザ名を対応するフィールドに入力します。詳細については、SNMPv3 のオプション（36-2 ページ）を参照してください。

（注）　SNMPv2 または SNMPv3 を選択する必要があります。SNMPv2 は読み取り専用コミュニティのみをサポートし、SNMPv3 は読み取り専用ユーザのみをサポートしています。

（注）　SNMPv3 パスワードを入力すると、パスワードは、初期設定時にはプレーン テキストで表示されますが、暗号化形式で保存されます。

ステップ 7　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

Syslog 応答の使用

ライセンス：Protection

システム ログ、つまり *syslog* は、ネットワーク イベント ロギングの標準ロギング メカニズムです。侵入イベントの通知である *syslog* アラートをアプライアンスの syslog に送信できます。syslog では、syslog 内の情報を優先度別およびファシリティ別に分類することができます。優先度はアラートの重大度を反映し、ファシリティはアラートを生成したサブシステムを示します。ファシリティおよび優先度は syslog の実際のメッセージに表示されませんが、その代わりに、syslog メッセージを受信するシステムにそれを分類する方法を指示するために使用されます。

syslog アラートには次の情報が含まれます。

- アラート生成の日時
- イベント メッセージ
- イベント データ
- トリガー イベントのジェネレータ ID
- トリガー イベントの Snort ID
- 改訂

侵入ポリシーでは、syslog アラートを有効にして、syslog の侵入イベントの通知に関連付けられている syslog の優先度およびファシリティを指定できます。アクセス コントロール ポリシーの一部として侵入ポリシーを適用した場合、システムは、検出した侵入イベントの syslog アラートをローカル ホストまたはポリシーで指定されたロギング ホストの syslog ファシリティに送信します。アラートを受信したホストは、syslog アラートの設定時に設定されたファシリティおよび優先度に関する情報を使用して、アラートを分類します。

次の表には、syslog アラートを設定する場合に選択できるファシリティを示します。使用するリモート syslog サーバの設定に基づいて、効果のあるファシリティの設定を行ってください。リモート システムにある `syslog.conf` ファイル（UNIX または Linux ベースのシステムに syslog メッセージをロギングしている場合）は、サーバのどのログ ファイルにどのファシリティが保存されるかを示します。

表 ***36-3***　使用可能な ***syslog*** ファシリティ

ファシリティ	説明
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CRON	クロック デーモンによって生成されるメッセージ。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージは表示されるときにコンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザ レベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

このアラートで生成されるすべての通知を表示するには、次の標準的な syslog の優先度レベルのいずれかを選択します。

表 ***36-4***　***syslog*** の優先度レベル

レベル	説明
EMERG	すべてのユーザにブロードキャストするパニック状態
ALERT	すぐに修正する必要がある状態
CRIT	重大な状態
ERR	エラー状態
WARNING	警告メッセージ
NOTICE	エラー状態ではないが、注意が必要な状態
INFO	通知メッセージ
DEBUG	デバッグ情報を含むメッセージ

syslog の動作とその設定方法の詳細については、システムに付属の資料を参照してください。UNIX または Linux ベースのシステムの syslog にログインしている場合、`syslog.conf` man ファイル（コマンドラインで `man syslog.conf` と入力）および syslog man ファイル（コマンドラインで `man syslog` と入力）に、syslog の動作とその設定方法に関する情報が示されます。

syslog 応答の設定

ライセンス：Protection

侵入ポリシーで syslog アラートを設定できます。アクセス コントロール ポリシーの一部としてポリシーを適用すると、システムは syslog で検出した侵入イベントをすべて通知するようになります。syslog アラートの詳細については、Syslog 応答の使用（36-4 ページ）を参照してください。

syslog アラート オプションの設定方法：

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ **2**　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ **3**　左側のナビゲーション パネルの [詳細設定（Advanced Settings）] をクリックします。

[詳細設定（Advanced Settings）] ページが表示されます。

ステップ **4**　外部応答の [Syslog アラート（Syslog Alerting）] が有効かどうかに応じて、次の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[Syslog アラート（Syslog Alerting）] ページが表示されます。

ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ **5**　オプションで、[ロギング ホスト（Logging Hosts）] フィールドに、ロギング ホストとして指定するリモート アクセス IP アドレスを入力します。複数のホストを指定する場合は、カンマで区切ります。

ステップ **6**　ドロップダウン リストからファシリティおよび優先度のレベルを選択します。

ファシリティおよび優先度オプションの詳細については、Syslog 応答の使用（36-4 ページ）を参照してください。

ステップ **7**　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

ASA FirePOWER ダッシュボードの使用

ASA FirePOWER モジュール ダッシュボードでは、現在のシステム ステータスが一目で確認できます。ダッシュボードには 3 列のレイアウトで ウィジェットを表示できます。ウィジェットは、ASA FirePOWER モジュールのさまざまな側面を理解するための、自己完結型の小さいコンポーネントです。システムには、事前定義された複数のウィジェットが付属しています。たとえば、[アプライアンス情報（Appliance Information）] ウィジェットは、アプライアンスの名前、モデル、および ASA FirePOWER モジュール ソフトウェアの実行中のバージョンを通知します。

ダッシュボードには、ウィジェットを制約する時間範囲があります。最短で 1 時間前から、最長では 1 年前からの期間を反映するように時間範囲を変更できます。

各アプライアンスには、サマリ ダッシュボードというデフォルトのダッシュボードが付属しています。このダッシュボードは、一時ユーザに対して、ご利用の ASA FirePOWER モジュールの展開についての汎用的なシステム ステータスの情報を提供します。

ダッシュボードおよびその内容の詳細については、次の項を参照してください。

- ダッシュボード ウィジェットについて（37-1 ページ）
- 事前定義されたウィジェットについて（37-2 ページ）
- ダッシュボードの操作（37-7 ページ）

ダッシュボード ウィジェットについて

ライセンス：任意

ダッシュボードには 3 列のレイアウトで複数のウィジェットを表示できます。ASA FirePOWER モジュールには、事前定義された複数のダッシュボード ウィジェットが付属しています。それぞれのウィジェットはシステムのさまざまな側面を理解するうえで役に立ちます。ユーザは、ウィジェットを最小化および最大化する、ウィジェットを再配置する、といったことができます。

詳細については、以下を参照してください。

- ウィジェットのプリファレンスについて（37-2 ページ）
- 事前定義されたウィジェットについて（37-2 ページ）
- ダッシュボードの操作（37-7 ページ）

ウィジェットのプリファレンスについて

ライセンス:任意

各ウィジェットには、動作を決定する一連のプリファレンスがあります。

ウィジェットのプリファレンスは単純なものにすることもできます。たとえば、[現在のインターフェイス ステータス(Current Interface Status)] ウィジェットのプリファレンスを設定できます。これは、内部ネットワークで有効になっているすべてのインターフェイスについて現在のステータスを表示します。このウィジェットでは、更新頻度のみを設定します。

ウィジェットのプリファレンスを変更する方法:

ステップ 1　プリファレンスを変更するウィジェットのタイトル バーで、プリファレンスの表示アイコン( )をクリックします。

そのウィジェットのプリファレンス セクションが表示されます。

ステップ 2　必要に応じて変更を加えます。

変更はすぐに反映されます。ユーザが個々のウィジェットに指定できるプリファレンスについては、事前定義されたウィジェットについて(37-2 ページ)を参照してください。

ステップ 3　プリファレンスのセクションを非表示にするには、ウィジェットのタイトル バーで、プリファレンスの非表示アイコン( )をクリックします。

事前定義されたウィジェットについて

ライセンス:任意

ASA FirePOWER モジュールにはいくつかの事前定義されたウィジェットが付属しています。このウィジェットでは、現在のシステム ステータスの概要的なビューが提供されます。

ウィジェットの詳細については、次の項を参照してください。

- [アプライアンス情報(Appliance Information)] ウィジェットについて(37-3 ページ)
- [現在のインターフェイス ステータス(Current Interface Status)] ウィジェットについて(37-3 ページ)
- [ディスク使用率(Disk Usage)] ウィジェットについて(37-4 ページ)
- [製品ライセンス(Product Licensing)] ウィジェットについて(37-4 ページ)
- [製品アップデート(Product Updates)] ウィジェットについて(37-5 ページ)
- [システム負荷(System Load)] ウィジェットについて(37-6 ページ)
- [システム時刻(System Time)] ウィジェットについて(37-6 ページ)

[アプライアンス情報（Appliance Information）] ウィジェットについて

ライセンス：任意

[アプライアンス情報（Appliance Information）] ウィジェットは、次の情報を提供します。

- アプライアンスの名前、IPv4 アドレス、IPv6 アドレス、およびモデル
- アプライアンスにインストールされている、ASA FirePOWER モジュール ソフトウェア、ルール アップデート、および位置情報アップデートのバージョン

単純なビューまたは高度なビューを表示するようにウィジェットのプリファレンスを変更することで、ウィジェットで表示する情報量を調整できます。プリファレンスでは、ウィジェットをアップデートする頻度を調整することもできます。詳細については、ウィジェットのプリファレンスについて（37-2 ページ）を参照してください。

[現在のインターフェイス ステータス（Current Interface Status）] ウィジェットについて

ライセンス：任意

[現在のインターフェイス ステータス（Current Interface Status）] ウィジェットは、有効になっているか未使用のアプライアンスのすべてのインターフェイスのステータスを示します。ウィジェットは、各インターフェイスに対して次の情報を提供します。

- インターフェイスの名前
- インターフェイスのリンク状態
- インターフェイスのリンク モード（100Mb 全二重、または 10Mb 半二重など）
- インターフェイスのタイプ（銅線または光ファイバ）
- インターフェイスで受け取ったデータ量（Rx）および送信したデータ量（Tx）

リンク状態を表すボールの色は、次のように現在のステータスを示します。

- 緑色：リンクがフル スピードでアップ状態になっています
- 黄色：リンクはアップ状態ですがフル スピードではありません
- 赤色：リンクはアップ状態ではありません
- 灰色：リンクは管理上無効になっています
- 青色：リンク ステート情報は使用できません（たとえば ASA）

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。詳細については、ウィジェットのプリファレンスについて（37-2 ページ）を参照してください。

[ディスク使用率(Disk Usage)] ウィジェットについて

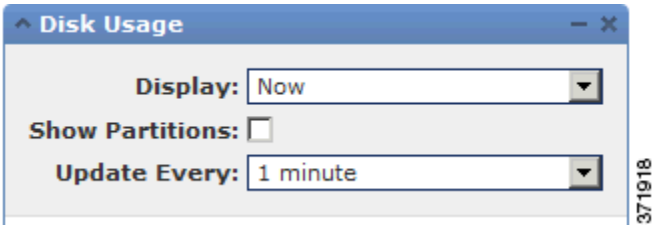
ライセンス:任意

[ディスク使用率(Disk Usage)] ウィジェットは、ディスク使用率のカテゴリに基づいて、ハードドライブで使用される領域を表示します。また、アプライアンスのハード ドライブの各パーティションで使用される領域および容量も示します。[カテゴリ別(By Category)] スタック バーは、各ディスク使用率のカテゴリを、使用可能な合計ディスク領域に対する使用量の割合として表示します。次の表で、使用可能なカテゴリについて説明します。

表 *37-1*　ディスク使用率のカテゴリ

ディスク使用率のカテゴリ	説明
イベント	システムで記録されたすべてのイベント
ファイル	システムに格納されたすべてのファイル
バックアップ(Backups)	すべてのバックアップ ファイル
変更点	ルールのアップデートやシステムのアップデートなど、アップデートに関連するすべてのファイル
その他	システムのトラブルシューティング ファイルおよびその他のファイル
未使用(Free)	アプライアンス上の残りの空き領域

マルウェア ストレージ パックがインストールされている場合は、ウィジェットのプリファレンスを変更して、[カテゴリ別(By Category)] スタック バーのみを表示したり、スタック バーと admin(/)、/Volume、および /boot パーティションの使用率、および /var/storage パーティションを表示したりするようにウィジェットを設定できます。



ウィジェットのプリファレンスは、ウィジェットのアップデート頻度、およびダッシュボードの時間範囲で現在のディスク使用率または収集したディスク使用率の統計のいずれかを表示するかも制御します。詳細については、ウィジェットのプリファレンスについて(37-2 ページ)を参照してください。

[製品ライセンス(Product Licensing)] ウィジェットについて

ライセンス:任意

[製品ライセンス(Product Licensing)] ウィジェットは、現在インストールされているデバイスおよび機能のライセンスを示します。また、ライセンス契約されているアイテム(ホストやユーザ)の数、許可される残りのライセンス契約アイテム数も示します。

このウィジェットの上部のセクションには、一時的なライセンスも含めて、インストールされているすべてのデバイスおよび機能のライセンスが表示されますが、[期限の切れたライセンス（Expiring Licenses）] セクションには、一時的なライセンスおよび期限の切れたライセンスのみが表示されます。

ウィジェットの背景のバーは、使用中のライセンスのそれぞれのタイプの割合を示しています。このバーは右から左へ読みます。期限の切れたライセンスには、取り消し線が付けられています。

ウィジェットのプリファレンスを変更して、現在ライセンス契約されている機能を表示するか、またはライセンス契約が可能なすべての機能を表示するようにウィジェットを設定することができます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて（37-2 ページ）を参照してください。

任意のライセンス タイプをクリックすると、ローカル設定の [ライセンス（License）] ページに移動して、機能ライセンスを追加または削除することができます。詳細については、ASA FirePOWER モジュールのライセンス（42-1 ページ）を参照してください。

[製品アップデート（Product Updates）] ウィジェットについて

ライセンス：任意

[製品アップデート（Product Updates）] ウィジェットは、アプライアンスに現在インストールされているソフトウェア（ASA FirePOWER モジュール ソフトウェアおよびルール アップデート）の概要、およびそのソフトウェアについてダウンロードしたが、まだインストールしていないアップデートの情報を提供します。

このウィジェットは、ユーザがソフトウェアのアップデートをダウンロード、プッシュ、またはインストールするスケジュールされたタスクを設定していない場合、ソフトウェアの最新バージョンを [不明（Unknown）] と表示します。ウィジェットではスケジュールされたタスクを使用して、最新のバージョンを決定するためです。詳細については、タスクのスケジュール（39-1 ページ）を参照してください。

ウィジェットは、ソフトウェアをアップデートできるページへのリンクも提供します。

ウィジェットのプリファレンスを変更して、最新のバージョンを非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて（37-2 ページ）を参照してください。

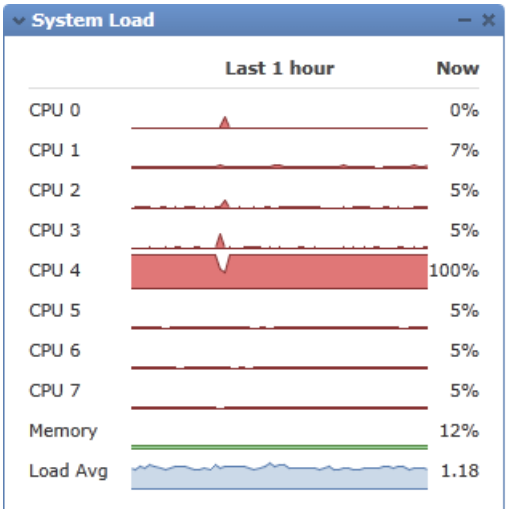
製品アップデート ウィジェットでは、次のことができます。

- ASA FirePOWER モジュール ソフトウェア、ルール アップデート、または位置情報アップデートの現在のバージョンをクリックして、アプライアンスを手動でアップデートします。
- システム ソフトウェア、または位置情報データベースを更新するには、ASA FirePOWER モジュール ソフトウェアの更新（43-1 ページ）を参照してください。
- 最新のルール アップデートをインポートするには、ルールの更新とローカル ルール ファイルのインポート（43-10 ページ）を参照してください。
- 最新バージョンをクリックして、ASA FirePOWER モジュール ソフトウェアまたはルール アップデートの最新バージョンをダウンロードするためのスケジュールされたタスクを作成します。タスクのスケジュール（39-1 ページ）を参照してください。

[システム負荷(System Load)] ウィジェットについて

ライセンス:任意

[システム負荷(System Load)] ウィジェットは、アプライアンス上の(各 CPU についての)CPU の使用率、メモリ(RAM)の使用率、およびシステムの負荷(実行を待機しているプロセスの数によって測定され、負荷平均とも呼ばれる)を現在、およびダッシュボードの時間範囲について表示します。

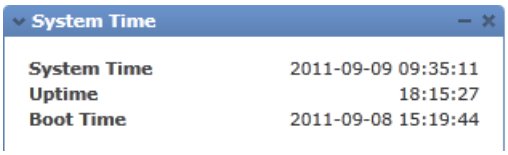


ウィジェットのプリファレンスを変更して、負荷平均を表示または非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて(37-2 ページ)を参照してください。

[システム時刻(System Time)] ウィジェットについて

ライセンス:任意

[システム時刻(System Time)] ウィジェットは、アプライアンスのローカル システム時間、稼動時間、およびブート時間を表示します。



ウィジェットのプリファレンスを変更して、ブート時間を非表示にするようウィジェットを設定できます。プリファレンスは、ウィジェットがアプライアンスの時計と同期する頻度も調整します。詳細については、ウィジェットのプリファレンスについて(37-2 ページ)を参照してください。

ダッシュボードの操作

ライセンス:任意

ダッシュボードに示されるウィジェットを表示および変更できます。

ダッシュボードの操作の詳細については、以下を参照してください。

- ダッシュボードの表示(37-7 ページ)
- ダッシュボードの変更(37-8 ページ)
- 設定のエクスポート(B-1 ページ)

ダッシュボードの表示

ライセンス:任意

いつでも、[ホーム(Home)] > [ASA FirePOWER ダッシュボード(ASA FirePOWER Dashboard)] ASA FirePOWER モジュールのダッシュボードを表示できます。使用可能なすべてのダッシュボードの詳細を表示する場合は、[概要(Overview)] > [ダッシュボード(Dashboards)] > [管理(Management)] を選択します。

ダッシュボードには、ウィジェットを制約する時間範囲があります。最短で 1 時間前(デフォルト)から、最長では 1 年前からの期間を反映するように時間範囲を変更できます。時間範囲を変更する場合は、時間によって制約される可能性のあるウィジェットが自動でアップデートされ、新しい時間範囲が反映されます。

すべてのウィジェットを時間で制約できるわけではないことに注意してください。たとえば、ダッシュボードの時間範囲は [アプライアンス情報(Appliance Information)] ウィジェットには影響を与えません。このウィジェットは、アプライアンスの名前、モデル、および ASA FirePOWER モジュール ソフトウェアの現在のバージョンが含まれている情報を提供します。

ダッシュボードを表示するには、次の手順を実行します。

ステップ 1　[ホーム(Home)] > [ASA FirePOWER ダッシュボード(ASA FirePOWER Dashboard)] の順の選択します。

ASA FirePOWER ダッシュボードが表示されます。

ダッシュボードの時間範囲を変更するには、次のようにします。

ステップ 1　[リストを表示(Show the Last)] ドロップダウンリストから、ダッシュボードの時間範囲を選択します。

ページ上で該当するすべてのウィジェットがアップデートされ、最新の時間範囲が反映されます。

ダッシュボードの変更

ライセンス:任意

ダッシュボードには、3 列のレイアウトでウィジェットが表示されます。ユーザは、ウィジェットを最小化および最大化する、ウィジェットを再配置する、といったことができます。

詳細については、次の項を参照してください。

- ウィジェットの再配置（37-8 ページ）
- ウィジェットの最小化および最大化（37-8 ページ）

ウィジェットの再配置

ライセンス:任意

任意のウィジェットの場所を変更できます。

ウィジェットを移動するには、次のようにします。

ステップ 1　移動するウィジェットのタイトル バーをクリックし、新しい場所へドラッグします。

ウィジェットの最小化および最大化

ライセンス:任意

ウィジェットを最小化してビューを単純化したり、その後で最大化してもう一度表示したりできます。

ウィジェットを最小化するには、次のようにします。

ステップ 1　ウィジェットのタイトル バーで、最小化のアイコン（ − ）をクリックします。

ウィジェットを最大化するには、次のようにします。

ステップ 1　ウィジェットのタイトル バーで、最大化のアイコン（ □ ）をクリックします。

ASA FirePOWER レポートの使用

ネットワーク上のトラフィックを分析するため、さまざまな期間のレポートを表示できます。レポートは、ネットワーク トラフィックのさまざまな面の情報を集約します。ほとんどの場合、一般情報から特定の情報にドリルダウンできます。たとえば、すべてのユーザのレポートを表示し、次に特定のユーザの詳細を表示できます。

概要レポートと詳細レポートには、トップ ポリシーや Web カテゴリなど、複数のレポート コンポーネントがあります。これらのレポートには、表示しているレポートのそのタイプで最も発生頻度の高い項目が示されます。たとえば、特定のユーザの詳細レポートを表示している場合、トップ ポリシーにはそのユーザに最も関連付けられたポリシー ヒットが表示されます。

詳細については、以下を参照してください。

- 使用可能なレポートについて（38-1 ページ）
- レポートの基礎（38-3 ページ）

使用可能なレポートについて

ライセンス：任意

使用可能なレポートには、ASA FirePOWER モジュールで使用可能なメイン レポートが含まれます。[ASA FirePOWER レポート（ASA FirePOWER Reporting）] メニューからこれらのレポートを表示できます。

一般に、名前や [詳細情報（View More）] リンクなど、多くの項目をクリックして、個々の項目またはモニタするカテゴリ全体に関する詳細な情報を取得できます。

ネットワークの概要（**Network Overview**）

このレポートには、ネットワークのトラフィックに関するサマリー情報が表示されます。この情報は、詳細な分析を必要とするエリアの識別、またはネットワークが一般的な予測の範囲内で動作していることの確認に使用します。

ユーザ（**Users**）

このレポートには、ネットワークの上位ユーザが表示されます。この情報は、ユーザの異常活動の識別に役立ちます。

ヒント　ユーザ名は、ユーザの ID 情報がトラフィック フローに関連付けられている場合に限り使用できます。ユーザ ID が大多数のトラフィックのレポートで使用できるようにする場合は、アクセス コントロール ポリシーでアクティブ認証を使用する必要があります。

アプリケーション

このレポートには、侵入イベントをトリガーしたトラフィックで検出された HTTP トラフィックの内容または要求された URL を表すアプリケーションが表示されます。モジュールが HTTP のアプリケーション プロトコルを検出し、特定の Web アプリケーションを検出できなかった場合、モジュールはここで一般的な Web ブラウジング指定を提供することに注意してください。

Web カテゴリ（**Web categories**）

このレポートには、訪問する Web サイトのカテゴリに基づいて、ネットワークで使用されている Web サイトのカテゴリ（ギャンブル、広告、検索エンジン、ポータルなど）が表示されます。この情報は、ユーザが訪問する上位カテゴリを識別し、アクセス コントロール ポリシーによって望ましくないカテゴリが十分にブロックされているかどうかを判別するために使用します。

ポリシー（**Policies**）

このレポートには、アクセス コントロール ポリシーがネットワークのトラフィックにどのように適用されたかが表示されます。この情報を使用すると、ポリシーの効果の評価に役立ちます。

入力ゾーン（**Ingress zones**）

このレポートには、イベントをトリガーしたパケットの入力セキュリティ ゾーンが表示されます。

出力ゾーン（**Egress zones**）

このレポートには、イベントをトリガーとして使用したパケットの出力セキュリティ ゾーンが表示されます。

接続先（**Destinations**）

このレポートには、ネットワーク トラフィックの分析に基づいて、ネットワークで使用中のアプリケーション（Facebook など）が表示されます。この情報を使用すると、ネットワークで使用された上位アプリケーションの識別に役立ち、不要なアプリケーションの使用量を減らすために追加のアクセス コントロール ポリシーが必要かどうかを判断できます。

攻撃者（**Attackers**）

このレポートには、イベントをトリガーした送信元ホストが使用する送信元 IP アドレスが表示されます。

ターゲット（**Targets**）

このレポートには、イベントをトリガーした受信ホストが使用する宛先 IP アドレスが表示されます。

脅威（**Threats**）

このレポートには、ネットワークに対し検出された各脅威に割り当てられた固有の識別番号と説明のテキストが表示されます。

ファイル ログ（**Files logs**）

このレポートには、検出されたファイルのタイプ（たとえば HTML や MSEXE）が表示されます。

レポートの基礎

ライセンス:任意

ここでは、レポート使用の基本を説明します。続く各トピックは、いずれか 1 つの特定のレポートではなく、レポート全般に適用されます。

詳細については、以下を参照してください。

レポート データについて

ライセンス:任意

レポート データはデバイスからすぐに収集されるため、レポートに反映されるデータとネットワーク活動の間に時差はほとんどありません。ただし、データを分析するときは次の点に注意してください。

- データは、ASA FirePOWER モジュールに適用されたアクセス コントロール ポリシーに一致するトラフィックについて収集されます。
- データは 5 分バケットで集約されるため、30 分グラフと 1 時間グラフではデータ ポイントは 5 分刻みで表示されます。1 時間の終了時に、5 分バケットが 1 時間バケットに集約され、さらにこれらが日バケットおよび週バケットに集約されます。5 分バケットは 7 日間保持され、1 時間バケットは 31 日間、日バケットは最大 365 日間保持されます。前にさかのぼるほど、データはさらに集約されます。古いデータを照会する場合、これらのデータ バケットが利用できる状態に合わせてクエリーを実行すると最良の結果が得られます。

（注）　たとえば、5 分間よりも長い間デバイスが到達不能になったなどの理由により、データ ポイントが欠けている場合は、折れ線グラフが途切れます。

レポートのドリルダウン

ライセンス:任意

レポートには、必要な情報にドリルダウンするための多くのリンクが含まれます。項目の上にマウスを置くと、どの項目でその詳細に進めるかがわかります。

たとえば、一般的なレポート項目において、[詳細情報（View More）] リンクをクリックすると、その項目のサマリー レポートに移動できます。

サマリー レポートの項目をクリックして、特定の項目の詳細レポートに移動することもできます。たとえば、アプリケーション サマリー レポートで Hypertext Transfer Protocol（HTTP）をクリックすると、HTTP のアプリケーション詳細レポートに進みます。

レポート時間範囲の変更

ライセンス：任意

レポートを表示するときは、[時間範囲（Time Range）] リストを使用して、レポートに含める情報を定義する時間範囲を変更できます。時間範囲のリストは各レポートの上部に表示され、これを使用して最近 1 時間または 1 週間などの定義済みの時間範囲を選択したり、特定の開始時刻と終了時刻でカスタムの時間範囲を定義したりできます。選択した時間範囲は、選択を変更するまで、表示する他のすべてのレポートに引き継がれます。

レポートは 10 分ごとに自動的に更新されます。

次の表に、時間範囲オプションの説明を示します。

表 ***38-1***　レポートの時間範囲

時間範囲	戻されるデータ
直近の 30 分（Last 5 minutes）	5 分間隔で 30 分間と、追加で最大 5 分間。
過去 1 時間（Last hour）	5 分間隔で 60 分間と、追加で最大 5 分間。
直近の 24 時間（Last 3 hours）	直前の時間境界に丸めた、1 時間間隔で直近の 24 時間。たとえば、現在時刻が 13:45 の場合、[最近の 24 時間（Last 24 Hour）] は昨日の 13:00 から今日の 13:00 までの期間になります。
過去 7 日（Last 7 days）	直前の時間境界に丸めた、1 時間間隔で直近の 7 日間。
過去 30 日（Last 7 days）	直前の午前 0 時から始まり、1 日間隔で最近の 30 日間。
カスタム範囲（Custom Range）	ユーザ定義の時間範囲。開始日、開始時刻、終了日、および終了時刻用に [編集（Edit）] ボックスが表示されます。各ボックスをクリックして、目的の値を選択します。作業が完了したら、[適用（Apply）] をクリックしてレポートを更新します。 カスタム時間範囲を作成する際、その範囲をデータ バケットの利用可能な範囲に揃える必要があります。過去 7～31 日の範囲の場合、クエリーを時に合わせます。古い範囲の場合は、その日に合わせます。1 年を超える範囲の場合は、週に合わせます。

レポートに表示されるデータの制御

ライセンス：任意

概要レポートと詳細レポートには、トップ ポリシーや Web カテゴリなど、複数の下位レポートがあります。各レポート パネルにあるコントロールを使用すると、データのさまざまな側面を表示できます。次のコントロールを使用できます。

[トランザクション（Transactions）] または **[データ使用量（Data Usage）]**

これらのリンクをクリックすると、トランザクション数またはトランザクションのデータ量に基づいたグラフが表示されます。

[すべて（All）]、**[拒否（Denied）]**、**[許可（Allowed）]**

各レポートの右上にあるラベルのないドロップダウンリストに、これらのオプションがあります。これらを使用して、拒否接続のみ、許可接続のみ、あるいは拒否または許可にかかわらずすべての接続の表示に変更します。

詳細情報（**View More**）

表示する項目のレポートに移動するには、[詳細情報（View More）] リンクをクリックします。たとえば、[接続先（Destinations）] レポートの [Web カテゴリ（Web Categories）] グラフで [詳細情報（View More）] をクリックすると、[Web カテゴリ（Web Categories）] レポートに進みます。詳細レポートのレポートを表示している場合は、詳細を表示している項目の詳細な [Web カテゴリ（Web Categories）] レポートに移動します。

レポート カラムについて

ライセンス：任意

通常、レポートにはグラフ形式で表示される情報の加えて、情報を提供する 1 つ以上のテーブルが含まれています。

- 多くのカラムの意味は、そのカラムを含むレポートによって変わります。たとえば、トランザクションのカラムには、レポートの基準になる項目タイプのトランザクション数が示されます。[値（Values）] または [割合（Percentages）] をクリックすることで、未処理の数値で行うか、項目に報告されたすべての未処理値の比率で行うか、値の切り替えを行うこともできます。
- カラム ヘッダーをクリックすると、カラムのソート順を変更できます。

次の表に、各種レポートで使用される標準のカラムの説明を示します。

表 ***38-2***　レポート カラム

カラム	説明
トランザクション（Transactions）	報告された項目のトランザクション総数。
許可されたトランザクション（Transactions allowed）	報告された項目で許可されたトランザクションの数。
拒否されたトランザクション（Transactions denied）	報告された項目で（ポリシーに基づいて）ブロックされたトランザクションの数。
合計バイト数（Total Bytes）	報告された項目の送受信バイト数の合計。
受信バイト数（Bytes received）	報告された項目の受信バイト数。
送信バイト数（Total Bytes Sent）	報告された項目の送信バイト数。

タスクのスケジュール

さまざまな種類の管理タスクを、指定した回数（1 度または繰り返し）実行するようにスケジュールを設定できます。

（注） タスクによっては、低帯域幅のネットワークに非常に負荷をかけることがあります（ソフトウェアの自動更新が含まれるタスクなど）。ネットワーク使用率が低い時間帯にこのようなタスクを実行するよう、スケジュールしてください。

詳細については、次の各項を参照してください。

- 定期タスクの設定（39-1 ページ）：スケジュール済みタスクが定期的に実行されるようセットアップする方法について説明します。
- バックアップ ジョブの自動化（39-3 ページ）：バックアップ ジョブをスケジュールする手順を示します。
- 証明書失効リストのダウンロードの自動化（39-4 ページ）：アプライアンスの証明書失効リスト（CRL）を自動的に更新する手順を示します。
- 侵入ポリシーの適用の自動化（39-5 ページ）：侵入ポリシーの適用をキューイングする手順を示します。
- 位置情報データベースの更新の自動化（39-6 ページ）：位置情報データベース（GeoDB）の自動更新をスケジュールする手順を示します。
- ソフトウェア更新の自動化（39-7 ページ）：ソフトウェア更新のダウンロード、プッシュ、インストールをスケジュールする手順について示します。
- URL フィルタリング更新の自動化（39-9 ページ）：URL フィルタリング データの更新を自動化する手順を示します。
- タスクの表示（39-10 ページ）：スケジュールした後のタスクを表示したり管理したりする方法について説明します。
- スケジュール済みタスクの編集（39-12 ページ）：既存のタスクを編集する方法について説明します。
- スケジュール済みタスクの削除（39-12 ページ）：ワンタイム タスクや、定期タスクのすべてのインスタンスを削除する方法について説明します。

定期タスクの設定

ライセンス：任意

定期タスクの頻度を設定する際には、すべてのタイプのタスクで同じ手順に従います。

ユーザ インターフェイスのほとんどのページに表示される時間はローカル時刻であり、ローカル設定で指定したタイム ゾーンに従ってそれが決定されます。さらに、ASA FirePOWER モジュールは、該当する場合にはローカル時刻の表示を夏時間（DST）に合わせて自動的に調整します。ただし、DST から標準時への移行日および元に戻る移行日をまたがる定期タスクは、移行を考慮して調整されません。つまり、標準時の午前 2:00 にタスク スケジュールを作成すると、DST 期間中は午前 3:00 に実行されます。同様に、DST の午前 2:00 にタスク スケジュールを作成すると、標準時には午前 1:00 に実行されます。

定期タスクを設定するには、次の手順を実行します。

ステップ 1　ASDM で、[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ツール（Tools）] > [スケジューリング（Scheduling）] の順に選択します。

[スケジューリング（Scheduling）] ページが表示されます。

ステップ 2　[タスクの追加（Add Task）] をクリックします。

[新しいタスク（New Task）] ページが表示されます。

ステップ 3　[ジョブ タイプ（Job Type）] リストから、スケジュールするタスクのタイプを選択します。

スケジュールできるタスク タイプについては、それぞれ該当する項で説明します。

ステップ 4　[実行するタスクのスケジュール（Schedule task to run）] オプションで、[定期（Recurring）] を選択します。

ページがリロードされ、定期タスクのオプションが示されます。

ステップ 5　[開始日付（Start On）] フィールドに、定期タスクを開始する日付を指定します。ドロップダウンリストを使用して月、日、年を選択できます。

ステップ 6　[繰り返し設定（Repeat Every）] フィールドに、タスクを繰り返す頻度を指定します。時間、日、週、または月の数値を指定できます。

ヒント　数値を入力するか、上矢印（▲）および下矢印（▼）アイコンをクリックして、間隔を指定できます。たとえば、2 日おきにタスクを実行するには、2 を入力して [日（Days）] を選択します。

ステップ 7　[実行時刻（Run At）] フィールドで、定期タスクを開始する時刻を指定します。

ステップ 8　[繰り返し設定（Repeat Every）] で [週（Weeks）] を選択した場合は、[繰り返し単位（Repeat On）] フィールドが表示されます。タスクを実行する曜日の横にあるチェック ボックスを選択してください。

ステップ 9　[繰り返し設定（Repeat Every）] に [月（Months）] を選択した場合は、[繰り返し単位（Repeat On）] フィールドが表示されます。ドロップダウンリストを使用して、タスクを実行する各月の日を選択します。

[新しいタスク（New Task）] ページ上のその他のオプションは、作成中のタスクに応じて異なります。詳細については、次の各項を参照してください。

- バックアップ ジョブの自動化（39-3 ページ）
- 証明書失効リストのダウンロードの自動化（39-4 ページ）
- 侵入ポリシーの適用の自動化（39-5 ページ）
- ソフトウェア更新の自動化（39-7 ページ）
- URL フィルタリング更新の自動化（39-9 ページ）

バックアップ ジョブの自動化

スケジューラを使用して、ASA FirePOWER モジュールのバックアップを自動化できます。バックアップをスケジュール済みタスクとして設定するには、その前にバックアップ プロファイルを設計する必要があります。詳細については、バックアップ プロファイルの作成（45-3 ページ）を参照してください。

バックアップ タスクを自動化するには、次の手順を実行します。

ステップ 1　ASDM で、[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ツール（Tools）] > [スケジューリング（Scheduling）] の順に選択します。

[スケジューリング（Scheduling）] ページが表示されます。

ステップ 2　[タスクの追加（Add Task）] をクリックします。

[新しいタスク（New Task）] ページが表示されます。

ステップ 3　[ジョブ タイプ（Job Type）] リストから、[バックアップ（Backup）] を選択します。

ページがリロードされ、バックアップのオプションが表示されます。

ステップ 4　バックアップをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[現在時刻（Current Time）] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（39-1 ページ）を参照してください。

ステップ 5　[ジョブ名（Job Name）] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　[バックアップ プロファイル（Backup Profile）] リストから、適切なバックアップ プロファイルを選択します。

新しいバックアップ プロファイルの作成の詳細については、バックアップ プロファイルの作成（45-3 ページ）を参照してください。

ステップ 7　オプションで、[コメント（Comment）] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [タスクの表示（View Tasks）] セクションに表示されるので、ある程度短くしてください。

ステップ 8　オプションで、[ステータスの送信先：（Email Status To:）] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（40-7 ページ）を参照してください。

ステップ 9　[保存（Save）] をクリックします。

タスクが追加されます。[タスクのステータス（Task Status）] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

証明書失効リストのダウンロードの自動化

スケジューラを使用すると、ユーザ証明書を有効にするアプライアンス上でアプライアンス Web サーバの証明書失効リスト（CRL）を自動的に更新できます。ローカル アプライアンス設定で CRL の取得を有効にすると、CRL のダウンロード タスクが自動的に作成されるため、以下の手順では、スケジュール済みタスクを開いて頻度を設定する方法について説明します。

ヒント　このタスクをスケジュールする前に、ユーザ証明書を有効化して設定し、CRL ダウンロード URL を設定する必要があります。ユーザ証明書の設定については、ユーザ証明書の要求（41-5 ページ）を参照してください。

証明書失効リストのダウンロードを自動化するには、次の手順を実行します。

ステップ 1　ASDM で、[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ツール（Tools）] > [スケジューリング（Scheduling）] の順に選択します。

[スケジューリング（Scheduling）] ページが表示されます。

ステップ 2　[タスクの詳細（Task Details）] で **Download CRL** タスクを見つけ、編集アイコン（  ）をクリックします。

[タスクの編集（Edit Task）] ページが表示され、ダウンロード オプションが示されます。

ステップ 3　CRL ダウンロードをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[現在時刻（Current Time）] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（39-1 ページ）を参照してください。

ステップ 4　オプションで、[コメント（Comment）] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [タスクの表示（View Tasks）] セクションに表示されるので、ある程度短くしてください。

ステップ 5　オプションで、[ステータスの送信先：（Email Status To:）] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、ASA FirePOWER モジュールで有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（40-7 ページ）を参照してください。

ステップ 6　[保存（Save）] をクリックします。

タスクが追加されます。[タスクのステータス（Task Status）] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

侵入ポリシーの適用の自動化

ライセンス：Protection

ASA FirePOWER モジュールへの侵入ポリシーの適用をキューイングすることができます。このタスクの実行時点で、侵入ポリシーを参照するアクセス コントロール ポリシーが、ASA FirePOWER モジュールに対して適用されている場合に限り、このタスクは侵入ポリシーを適用します。それ以外の場合、このタスクは完了せずに終了します。

このタスクをスケジュールする前に、侵入ポリシーをアクセス コントロール ポリシーに関連付けて、アクセス コントロール ポリシーをデバイスに適用する必要があります。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（10-1 ページ）を参照してください。

ポリシー適用をキューイングするには、次の手順を実行します。

ステップ 1　ASDM で、[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ツール（Tools）] > [スケジューリング（Scheduling）] の順に選択します。

現在の月のスケジュール カレンダー ページが表示されます。

ステップ 2　[タスクの追加（Add Task）] をクリックします。

[新しいタスク（New Task）] ページが表示されます。

ステップ 3　[ジョブ タイプ（Job Type）] リストから、[侵入ポリシー適用のキューイング（Queue Intrusion Policy Apply）] を選択します。

ページがリロードされ、ポリシー適用のキューイングに関するオプションが表示されます。

ステップ 4　タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[現在時刻（Current Time）] フィールドには、ASA FirePOWER モジュールの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（39-1 ページ）を参照してください。

ステップ 5　[ジョブ名（Job Name）] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　[侵入ポリシー（Intrusion Policy）] フィールドには、次のオプションがあります。

- ASA FirePOWER モジュールに適用する侵入ポリシーを 1 つ選択します。
- [すべての侵入ポリシー（All intrusion policies）] を選択すると、ASA FirePOWER モジュールで選択したデバイスにすでに適用されているすべての侵入ポリシーが適用されます。

ステップ 7　オプションで、[コメント（Comment）] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　スケジュール カレンダー ページの下部の [タスクの詳細（Task Details）] セクションにコメント フィールドが表示されるため、コメントの長さを制限してください。

ステップ 8　オプションで、[ステータスの送信先：（Email Status To:）] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（40-7 ページ）を参照してください。

ステップ 9　[保存(Save)] をクリックします。

タスクが追加されます。カレンダー ページの [タスクの詳細(Task Details)] セクションで、実行中のタスクの状態を確認できます(実行時間が長いタスクのステータスの表示(C-1 ページ)を参照)。

ステップ 10　保存済みのタスクを編集するには、スケジュール カレンダー ページに表示されているタスクをクリックします。

[タスクの詳細(Task Details)] セクションがページの下部に表示されます。変更を行うには、編集アイコン( )をクリックします。

位置情報データベースの更新の自動化

ライセンス:任意

スケジューラを使用して、位置情報データベース(GeoDB)の定期更新を自動化できます。GeoDB の定期更新は 7 日ごとに 1 度(週 1 回)実行されます。週ごとに更新が繰り返される時刻を設定できます。GeoDB 更新の詳細については、位置情報データベースの更新(43-21 ページ)を参照してください。

位置情報データベースの更新を自動化するには、次の手順を実行します。

ステップ 1　ASDM で、[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > **[**更新(**Updates**)**]** の順に選択します。

[製品アップデート(Product Updates)] ページが表示されます。

ステップ 2　[位置情報の更新(Geolocation Updates)] タブをクリックします。

[位置情報の更新(Geolocation Updates)] ページが表示されます。

ステップ 3　[位置情報の定期更新(Recurring Geolocation Updates)] の下で、[週ごとの定期更新を有効にする(Enable Recurring Weekly Updates)] チェック ボックスを選択します。

[更新の開始時刻(Update Start Time)] フィールドが表示されます。

ステップ 4　[更新の開始時刻(Update Start Time)] フィールドで、週ごとに GeoDB 更新を行う曜日と時刻を指定します。

ステップ 5　[保存(Save)] をクリックします。

タスクが追加されます。[タスクのステータス(Task Status)] ページで、実行中のタスクの状態を確認できます(実行時間が長いタスクのステータスの表示(C-1 ページ)を参照)。

ソフトウェア更新の自動化

ほとんどのパッチや機能リリースを自動的にダウンロードして ASA FirePOWER モジュールに適用することができます。

（注）　手動で更新をアップロードしてインストールする必要が生じる状況が 2 つあります。まず、ASA FirePOWER モジュールのメジャー アップデート（主要な更新）をスケジュールすることはできません。次に、サポート サイトにアクセスできないアプライアンスの更新や、そのアプライアンスからのプッシュをスケジュールすることはできません。ASA FirePOWER モジュールの手動更新について詳しくは、ASA FirePOWER モジュール ソフトウェアの更新（43-1 ページ）を参照してください。

このプロセスをより確実に制御するには、更新がリリースされたことがわかった後、[1 回（Once）] オプションを使用してオフピーク時間帯に更新をダウンロード/インストールできます。

詳細については、次の各項を参照してください。

- ソフトウェア ダウンロードの自動化（39-7 ページ）
- ソフトウェア インストールの自動化（39-8 ページ）

ソフトウェア ダウンロードの自動化

シスコから最新のソフトウェア更新を自動的にダウンロードするスケジュール済みタスクを作成することができます。このタスクを使用すると、手動でインストールする予定の更新のダウンロードをスケジュールできます。

ソフトウェア更新のダウンロードを自動化するには、次の手順を実行します。

ステップ 1　ASDM で、[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ツール（Tools）] > [スケジューリング（Scheduling）] の順に選択します。

[スケジューリング（Scheduling）] ページが表示されます。

ステップ 2　[タスクの追加（Add Task）] をクリックします。

[新しいタスク（New Task）] ページが表示されます。

ステップ 3　[ジョブ タイプ（Job Type）] リストから、[最新の更新のダウンロード（Download Latest Update）] を選択します。

[新しいタスク（New Task）] ページがリロードされ、更新オプションが示されます。

ステップ 4　タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[現在時刻（Current Time）] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（39-1 ページ）を参照してください。

ステップ 5　[ジョブ名（Job Name）] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　[更新項目（Update Items）] セクションで、[ソフトウェア（Software）] を選択します。

ステップ 7　オプションで、[コメント（Comment）] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [タスクの表示（View Tasks）] セクションに表示されるので、ある程度短くしてください。

ステップ 8　オプションで、[ステータスの送信先：（Email Status To:）] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（40-7 ページ）を参照してください。

ステップ 9　[保存（Save）] をクリックします。

タスクが追加されます。[タスクのステータス（Task Status）] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

ソフトウェア インストールの自動化

注意　インストールする更新によっては、ソフトウェアのインストール後にアプライアンスがリブートする場合があります。

ソフトウェア インストール タスクをスケジュールするには、次の手順を実行します。

ステップ 1　ASDM で、[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ツール（Tools）] > [スケジューリング（Scheduling）] の順に選択します。

[スケジューリング（Scheduling）] ページが表示されます。

ステップ 2　[タスクの追加（Add Task）] をクリックします。

[新しいタスク（New Task）] ページが表示されます。

ステップ 3　[ジョブ タイプ（Job Type）] リストから、[最新の更新のインストール（Install Latest Update）] を選択します。

ページがリロードされ、更新をインストールするためのオプションが表示されます。

ステップ 4　タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[現在時刻（Current Time）] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（39-1 ページ）を参照してください。

ステップ 5　[ジョブ名（Job Name）] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　オプションで、[コメント（Comment）] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [タスクの表示（View Tasks）] セクションに表示されるので、ある程度短くしてください。

ステップ 7　オプションで、[ステータスの送信先：（Email Status To:）] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（40-7 ページ）を参照してください。

ステップ 8　[保存（Save）] をクリックします。

タスクが追加されます。[タスクのステータス（Task Status）] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

URL フィルタリング更新の自動化

ライセンス：URL フィルタリング（URL Filtering）

スケジューラを使用して、Collective Security Intelligence クラウドからの URL フィルタリング データの更新を自動化できます。URL フィルタリングを更新するタスクが正しく実行されるには：

- ASA FirePOWER モジュールがインターネットにアクセスできる必要があります。アクセスできない場合は、クラウドと通信できません。
- クラウド通信の有効化（41-2 ページ）の説明に従って、URL フィルタリングを有効にする必要があります。

また、URL フィルタリングを有効にする際に、自動更新を有効にできることに注意してください。その場合、URL フィルタリング データの更新を確認するためにASA FirePOWER モジュールは必ず 30 分ごとにクラウドと通信します。自動更新がすでに有効になっている場合は、URL フィルタリング データを更新するスケジュール済みタスクを作成しないでください。

通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL フィルタリング データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

URL フィルタリング データのタスクを自動化するには、次の手順を実行します。

ステップ 1　ASDM で、[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ツール（Tools）] > [スケジューリング（Scheduling）] の順に選択します。

[スケジューリング（Scheduling）] ページが表示されます。

ステップ 2　[タスクの追加（Add Task）] をクリックします。

[新しいタスク（New Task）] ページが表示されます。

ステップ 3　[ジョブ タイプ（Job Type）] リストから、[URL フィルタリング データベースの更新（Update URL Filtering Database）] を選択します。

ページがリロードされ、URL フィルタリング更新のオプションが示されます。

ステップ 4　更新をスケジュールする頻度として、ワンタイム更新を示す [1 回（Once）] または定期更新を示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。[現在時刻（Current Time）] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定（39-1 ページ）を参照してください。

ステップ 5　[ジョブ名（Job Name）] フィールドに、255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6　オプションで、[コメント（Comment）] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント　コメント フィールドはページの [タスクの表示（View Tasks）] セクションに表示されるので、ある程度短くしてください。

ステップ 7　オプションで、[ステータスの送信先（Email Status To）] フィールドに、ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定（40-7 ページ）を参照してください。

ステップ 8　[保存（Save）] をクリックします。

タスクが追加されます。[タスクのステータス（Task Status）] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示（C-1 ページ）を参照）。

タスクの表示

スケジュール済みタスクを追加した後、それらのタスクを表示したり、状態を評価したりできます。ページの [表示オプション（View Options）] セクションで、カレンダーやスケジュール済みタスク リストを使用してスケジュール済みタスクを表示できます。

詳細については、次の各項を参照してください。

- カレンダーの使用法（39-10 ページ）
- タスク リストの使用法（39-11 ページ）

カレンダーの使用法

カレンダー表示オプションを使用すると、どの日にどのスケジュール済みタスクが行われるかを表示できます。

カレンダーを使用してスケジュール済みタスクを表示するには、次の手順を実行します。

ステップ 1　ASDM で、[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ツール（Tools）] > [スケジューリング（Scheduling）] の順に選択します。

[スケジューリング（Scheduling）] ページが表示されます。

ステップ 2　カレンダー ビューを使用して、次のタスクを実行できます。

- 二重左矢印アイコン（）をクリックすると、1 年戻ります。
- 単一の左矢印アイコン（）をクリックすると、1 ヵ月戻ります。
- 単一の右矢印アイコン（）をクリックすると、1 ヵ月進みます。
- 二重右矢印アイコン（）をクリックすると、1 年進みます。
- [今日（Today）] をクリックすると、現在の年月に戻ります。
- [タスクの追加（Add Task）] をクリックすると、新しいタスクをスケジュールできます。
- 1 つの日付をクリックすると、カレンダーの下にあるタスク リスト表に、特定の日付のスケジュール済みタスクがすべて表示されます。
- ある日付の特定のタスクをクリックすると、カレンダーの下にあるタスク リスト表にそのタスクが表示されます。

（注）　タスク リストの使用方法の詳細については、タスク リストの使用法を参照してください。

タスク リストの使用法

タスク リストには、タスクとその状態のリストが表示されます。タスク リストは、カレンダーを開いたときにカレンダーの下に表示されます。また、カレンダーで 1 つの日付またはタスクを選択してアクセスすることもできます。詳細については、カレンダーの使用法（39-10 ページ）を参照してください。

表 ***39-1***　　タスク リストのカラム

カラム	説明
名前（Name）	スケジュール済みタスクの名前と、関連付けられているコメントを表示します。
タイプ（Type）	スケジュール済みタスクのタイプを表示します。
開始時刻（Start Time）	スケジュールされている開始日時を表示します。
頻度（Frequency）	タスクの実行頻度を表示します。
ステータス（Status）	スケジュール済みタスクの現在の状態を次のように示します。 • チェック マーク アイコン（  ）は、タスクが正常に実行されたことを示します。 • 疑問符アイコン（  ）は、タスクの状態が不明であることを示します。 • 感嘆符アイコン（  ）は、タスクが失敗したことを示します。
作成者（Creator）	スケジュール済みタスクを作成したユーザの名前を表示します。
編集（Edit）	スケジュール済みタスクを編集します。
削除（Delete）	スケジュール済みタスクを削除します。

スケジュール済みタスクの編集

以前に作成したスケジュール済みタスクを編集できます。この機能は、パラメータが正しいことを確認するために、スケジュール済みタスクを 1 度テストする場合に特に役立ちます。タスクが正常に完了したら、後で定期タスクに変更できます。

既存のスケジュール済みタスクを編集するには、次の手順を実行します。

ステップ 1　[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] を選択します。

[スケジューリング（Scheduling）] ページが表示されます。

ステップ 2　編集するタスク、またはタスクが表示されている日付をクリックします。

[タスクの詳細（Task Details）] 表に、選択した 1 つ以上のタスクが示されます。

ステップ 3　この表で、編集するタスクを見つけて編集アイコン（  ）をクリックします。

[タスクの編集（Edit Task）] ページが表示され、選択したタスクの詳細が示されます。

ステップ 4　必要に応じて、タスクの開始時間、ジョブ名、コメント、実行頻度（1 度または繰り返し）などを編集します。ジョブのタイプを変更することはできません。

残りのオプションは、編集中のタスクに応じて異なります。詳細については、次の各項を参照してください。

- バックアップ ジョブの自動化（39-3 ページ）
- 証明書失効リストのダウンロードの自動化（39-4 ページ）
- ソフトウェア更新の自動化（39-7 ページ）
- URL フィルタリング更新の自動化（39-9 ページ）

ステップ 5　[保存（Save）] をクリックして編集内容を保存します。

変更が保存され、[スケジューリング（Scheduling）] ページが再び表示されます。

スケジュール済みタスクの削除

[スケジュール表示（Schedule View）] ページから 2 種類の削除操作を実行できます。まだ実行されていない特定のワンタイム タスク、または定期タスクのすべてのインスタンスを削除できます。定期タスクの 1 つのインスタンスを削除すると、そのタスクのすべてのインスタンスが削除されます。1 度だけ実行するようスケジュールされているタスクを削除すると、そのタスクだけが削除されます。

以下の項では、タスクを削除する方法について説明します。

- タスクのすべてのインスタンスを削除するには、定期タスクの削除（39-13 ページ）を参照してください。
- タスクの 1 つのインスタンスを削除するには、ワンタイム タスクの削除（39-13 ページ）を参照してください。

定期タスクの削除

定期タスクの 1 つのインスタンスを削除すると、そのタスクのすべてのインスタンスが自動的に削除されます。

定期タスクを削除するには、次の手順を実行します。

ステップ 1　ASDM で、[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ツール（Tools）] > [スケジューリング（Scheduling）] の順に選択します。

[スケジューリング（Scheduling）] ページが表示されます。

ステップ 2　カレンダーで、削除する定期タスクのインスタンスを 1 つ選択します。

ページがリロードされ、カレンダーの下にタスクの表が表示されます。

ステップ 3　この表で、削除する定期タスクのインスタンスを見つけて、削除アイコン（ ）をクリックします。

その定期タスクのすべてのインスタンスが削除されます。

ワンタイム タスクの削除

タスク リストを使用して、スケジュール済みのワンタイム タスクを削除したり、以前に実行されたスケジュール済みタスクのレコードを削除したりできます。

1 つのタスク（そのタスクがすでに実行済みの場合はタスク レコード）を削除するには、次の手順を実行します。

ステップ 1　ASDM で、[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > **[** ツール（**Tools**）**] > [**スケジューリング（**Scheduling**）**]** の順に選択します。

[スケジューリング（Scheduling）] ページが表示されます。

ステップ 2　削除するタスク、またはタスクが表示されている日付をクリックします。

選択した 1 つ以上のタスクを含む表が表示されます。

ステップ 3　この表で、削除するタスクを見つけて削除アイコン（ ）をクリックします。

選択したタスクのインスタンスが削除されます。

システム ポリシーの管理

システム ポリシーを使用して、ASA FirePOWER モジュール で次のものを管理できます。

- 監査ログ設定
- メール リレー ホストおよび通知アドレス
- SNMP ポーリング設定
- STIG コンプライアンス

詳細については、次の各項を参照してください。

システム ポリシーの作成

ライセンス：任意

システム ポリシーを作成したら、それに名前と説明を割り当てます。次に、ポリシーのさまざまな側面（それぞれの項の説明を参照）を設定します。

新しいポリシーを作成する代わりに、別の ASA FirePOWER モジュール からシステム ポリシーをエクスポートし、ASA FirePOWER モジュール にインポートすることができます。ニーズに合わせて、インポートされたポリシーを編集してから適用することができます。詳細については、設定のインポートおよびエクスポート（B-1 ページ）を参照してください。

システム ポリシーを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ローカル（Local）] > [システム ポリシー（System Policy）] の順に選択します。

[システム ポリシー（System Policy）] ページが表示されます。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。

[ポリシーの作成（Create Policy）] ページが表示されます。

ステップ 3 ドロップダウン リストから、新しいシステム ポリシーのテンプレートとして使用する既存のポリシーを選択します。

ステップ 4　新規ポリシーの名前を [新しいポリシー名（New Policy Name）] フィールドに入力します。

ステップ 5　新規ポリシーの説明を [新しいポリシーの説明（New Policy Description）] フィールドに入力します。

ステップ 6　[作成（Create）] をクリックします。

システム ポリシーが保存され、[システム ポリシーの編集（Edit System Policy）] ページが表示されます。システム ポリシーのそれぞれの側面の設定については、次の項のいずれかを参照してください。

- 監査ログの設定（40-5 ページ）
- メール リレー ホストおよび通知アドレスの設定（40-7 ページ）
- SNMP ポーリングの設定（40-8 ページ）
- STIG コンプライアンスの有効化（40-9 ページ）

システム ポリシーの編集

ライセンス：任意

既存のシステム ポリシーを編集できます。ASA FirePOWER モジュール に現在適用されているシステム ポリシーを編集する場合は、変更を保存してからポリシーを再適用してください。詳細については、システム ポリシーの適用（40-3 ページ）を参照してください。

既存のシステム ポリシーを編集するには、次の手順を実行します。

ステップ 1　**[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ローカル（Local）] > [システム ポリシー（System Policy）]** の順に選択します。

既存のシステム ポリシーのリストを含む、[システム ポリシー（System Policy）] ページが表示されます。

ステップ 2　編集するシステム ポリシーの横にある編集アイコン（ ）をクリックします。

[ポリシーの編集（Edit Policy）] ページが表示されます。ポリシー名とポリシーの説明を変更できます。システム ポリシーのそれぞれの側面の設定については、次の項のいずれかを参照してください。

- 監査ログの設定（40-5 ページ）
- メール リレー ホストおよび通知アドレスの設定（40-7 ページ）
- SNMP ポーリングの設定（40-8 ページ）
- STIG コンプライアンスの有効化（40-9 ページ）

（注）　ASA FirePOWER モジュール に適用されているシステム ポリシーを編集する場合は、編集が完了したら、更新したポリシーを再適用してください。システム ポリシーの適用（40-3 ページ）を参照してください。

ステップ 3　[ポリシーを保存して終了（Save Policy and Exit）] をクリックして変更を保存します。変更が保存され、[システム ポリシー（System Policy）] ページが表示されます。

システム ポリシーの適用

ライセンス:任意

ASA FirePOWER モジュール にシステム ポリシーを適用できます。システム ポリシーがすでに適用されている場合、再適用するまで、ポリシーに加えた変更は有効になりません。

システム ポリシーを適用するには、次の手順を実行します。

ステップ 1　**[**設定(**Configuration**)**] > [ASA FirePOWER** 設定(**ASA FirePOWER Configuration**)**] > [**ローカル(**Local**)**] > [**システム ポリシー(**System Policy**)**]** の順に選択します。

[システム ポリシー(System Policy)] ページが表示されます。

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

ステップ 3　[適用(Apply)] をクリックします。

[システム ポリシー(System Policy)] ページが表示されます。メッセージはシステム ポリシーの適用のステータスを示します。

システム ポリシーの削除

ライセンス:任意

システム ポリシーは、使用中でも削除できます。使用中の場合は、新しいポリシーが適用されるまで現在のポリシーが使用されます。デフォルトのシステム ポリシーは削除できません。

システム ポリシーを削除するには、次の手順を実行します。

ステップ 1　**[**設定(**Configuration**)**] > [ASA FirePOWER** 設定(**ASA FirePOWER Configuration**)**] > [**ローカル(**Local**)**] > [**システム ポリシー(**System Policy**)**]** の順に選択します。

[システム ポリシー(System Policy)] ページが表示されます。

ステップ 2　削除するシステム ポリシーの横にある削除アイコン( )をクリックします。ポリシーを削除するには、[OK] をクリックします。

[システム ポリシー(System Policy)] ページが表示されます。ポリシーの削除について確認を求めるポップアップ メッセージが表示されます。

システム ポリシーの設定

ライセンス:任意

さまざまなシステム ポリシーの設定を行うことができます。システム ポリシーのそれぞれの側面の設定については、次の項のいずれかを参照してください。

- アプライアンスのアクセス リストの設定(40-4 ページ)
- 監査ログの設定(40-5 ページ)

- メール リレー ホストおよび通知アドレスの設定（40-7 ページ）
- SNMP ポーリングの設定（40-8 ページ）
- STIG コンプライアンスの有効化（40-9 ページ）

アプライアンスのアクセス リストの設定

ライセンス：任意

[アクセスリスト（Access List）] ページを使用して、特定ポートのアプライアンスにどのコンピュータがアクセス可能かを制御できます。デフォルトでは、Web インターフェイスへのアクセスに使用されるポート 443（Hypertext Transfer Protocol Secure（HTTPS））と、コマンド ラインへのアクセスに使用されるポート 22（Secure Shell（SSH））は、あらゆる IP アドレスに対して有効です。ポート 161 を介した SNMP アクセスを追加することもできます。SNMP 情報をポーリングするには、使用する任意のコンピュータで SNMP アクセスを追加する必要があることに注意してください。

注意　デフォルトでは、アプライアンスへのアクセスは制限されません。よりセキュアな環境でアプライアンスを稼動させるために、特定の IP アドレスに対してアプライアンスへのアクセスを追加してから、デフォルトの任意のオプションを削除することを検討してください。

アクセス リストは、システム ポリシーの一部です。新しいシステム ポリシーを作成するか、既存のシステム ポリシーを編集することによって、アクセス リストを指定できます。いずれの場合も、システム ポリシーを適用するまでアクセス リストは有効になりません。

このアクセス リストは、外部データベース アクセスを制御しないので注意してください。外部データベースのアクセス リストの詳細については、クラウド通信の有効化（41-2 ページ）を参照してください。

アクセス リストを設定するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ローカル（Local）] > [システム ポリシー（System Policy）] の順に選択します。

[システム ポリシー（System Policy）] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーのアクセス リストを変更するには、システム ポリシーの横にある編集アイコン（  ）をクリックします。
- 新しいシステム ポリシーの一部としてアクセス リストを設定するには、[ポリシーの作成（Create Policy）] をクリックします。

  システム ポリシーの作成（40-1 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[保存（Save）] をクリックします。

いずれの場合も、[アクセスリスト（Access List）] ページが表示されます。

ステップ 3　現在の設定の 1 つを削除するために、削除アイコン（）をクリックすることもできます。

設定が削除されます。

注意　アプライアンスのインターフェイスへの接続に現在使用されている IP アドレスへのアクセスを削除し、「`IP=any port=443`」のエントリが存在しない場合、ポリシーを適用した時点でシステムへのアクセスは失われます。

ステップ 4　1 つ以上の IP アドレスへのアクセスを追加するために、[ルールの追加（Add Rules）] をクリックすることもできます。

[IP アドレスの追加（Add IP Address）] ページが表示されます。

ステップ 5　[IP アドレス（IP Address）] フィールドでは、追加する IP アドレスに応じて次のオプションがあります。

- 厳密な IP アドレス（192.168.1.101 など）
- CIDR 表記を使用した IP アドレス ブロック（192.168.1.1/24 など）

  FireSIGHT システム での CIDR の使用方法については、IP アドレスの表記規則（1-4 ページ）を参照してください。
- `any`（任意の IP アドレスを指定）

ステップ 6　[SSH]、[HTTPS]、[SNMP]、またはこれらのオプションの組み合わせを選択して、これらの IP アドレスで有効にするポートを指定します。

ステップ 7　[追加（Add）] をクリックします。

[アクセスリスト（Access List）] ページが再度表示され、ユーザが行った変更が反映されます。

ステップ 8　[ポリシーを保存して終了（Save Policy and Exit）] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、システム ポリシーの適用（40-3 ページ）を参照してください。

監査ログの設定

ライセンス：任意

ASA FirePOWER モジュール が外部ホストに監査ログをストリーミングするように、システム ポリシーを設定できます。

（注）　外部ホストが機能しており、監査ログを送信する ASA FirePOWER モジュール からアクセスできることを確認する必要があります。

送信元ホスト名は送信される情報の一部です。ファシリティ、重大度、およびオプションのタグを使用して監査ログ ストリームをより詳細に識別できます。ASA FirePOWER モジュール は、システム ポリシーが適用されるまで監査ログを送信しません。

この機能を有効にしてポリシーを適用し、監査ログを受け入れるように宛先ホストを設定した後で、syslog メッセージが送信されます。次に、出力構造の例を示します。

```
Date Time Host [Tag] Sender: [User_Name]@[User_IP], [Subsystem], [Action]
```

現地の日付、時刻、およびホスト名の後に、角括弧で囲まれたオプション タグが続き、送信側デバイス名の後に監査ログ メッセージが続きます。

次に例を示します。

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3000: admin@10.1.1.2, Operations > Monitoring, Page View
```

監査ログの設定を行うには、次の手順を実行します。

ステップ 1　**[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ローカル（Local）] > [システム ポリシー（System Policy）]** の順に選択します。

[システム ポリシー（System Policy）] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーの監査ログの設定を変更するには、システム ポリシーの横にある編集アイコン（）をクリックします。
- 新しいシステム ポリシーの一部として監査ログ設定を設定するには、[ポリシーの作成（Create Policy）] をクリックします。

  システム ポリシーの作成（40-1 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[保存（Save）] をクリックします。

ステップ 3　[監査ログ設定（Audit Log Settings）] をクリックします。

[監査ログ設定（Audit Log Settings）] ページが表示されます。

ステップ 4　[監査ログを Syslog に送信（Send Audit Log to Syslog）] ドロップダウン メニューから、[有効（Enabled）] を選択します。（デフォルト設定では [無効（Disabled）] になっています。）

ステップ 5　[ホスト（Host）] フィールドにあるホストの IP アドレスまたは完全修飾名を使用して、監査情報の宛先ホストを指定します。デフォルト ポート（514）が使用されます。

注意　監査ログを受け入れるように設定しているコンピュータが、リモート メッセージを受け入れるようにセットアップされていない場合、ホストは監査ログを受け入れません。

ステップ 6　[ファシリティ（Facility）] フィールドから syslog ファシリティを選択します。

ステップ 7　[重大度（Severity）] フィールドから重大度を選択します。

ステップ 8　必要に応じて、[タグ（オプション）（Tag (optional)）] フィールドで参照タグを挿入します。

ステップ 9　定期的な監査ログの更新を外部 HTTP サーバに送信するには、[監査ログを HTTP サーバに送信（Send Audit Log to HTTP Server）] ドロップダウン リストから [有効（Enabled）] を選択します。デフォルト設定では [無効（Disabled）] になっています。

ステップ 10　[監査情報を送信する URL（URL to Post Audit）] フィールドに、監査情報の送信先 URL を指定します。次にリストされている HTTP POST 変数を要求するリスナー プログラムに対応する URL を入力する必要があります。

- `subsystem`
- `actor`
- `event_type`
- `message`
- `action_source_ip`
- `action_destination_ip`
- 結果
- 時刻
- `tag`（上記のように定義されている場合）

注意　暗号化されたポストを許可するには、HTTPS URL を使用する必要があります。外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があるので注意してください。

ステップ 11　[ポリシーを保存して終了（Save Policy and Exit）] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで、変更は有効になりません。詳細については、システム ポリシーの適用（40-3 ページ）を参照してください。

メール リレー ホストおよび通知アドレスの設定

ライセンス:任意

次の処理を行う場合、メール ホストを設定する必要があります。

- イベント ベースのレポートの電子メール送信
- スケジュールされたタスクのステータス レポートの電子メール送信
- 変更調整レポートの電子メール送信
- データ切り捨て通知の電子メール送信

アプライアンスとメール リレー ホスト間の通信に使用する暗号化方式を選択し、必要に応じて、メール サーバの認証資格情報を指定できます。設定を行った後、指定された設定を使用してアプライアンスとメール サーバとの間の接続をテストできます。

メール リレー ホストを設定するには、次の手順を実行します。

ステップ 1　**[**設定(**Configuration**)**] > [ASA FirePOWER** 設定(**ASA FirePOWER Configuration**)**] > [**ローカル(**Local**)**] > [**システム ポリシー(**System Policy**)**]** の順に選択します。

[システム ポリシー(System Policy)] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーの電子メールの設定を変更するには、システム ポリシーの横にある編集アイコン( )をクリックします。
- 新しいシステム ポリシーの一部として電子メールの設定を行うには、[ポリシーの作成(Create Policy)] をクリックします。

  システム ポリシーの作成(40-1 ページ)で説明されているように、システム ポリシーの名前および説明を入力し、[保存(Save)] をクリックします。

ステップ 3　[電子メール通知(Email Notification)] をクリックします。

[電子メール通知の設定(Configure Email Notification)] ページが表示されます。

ステップ 4　[メール リレー ホスト(Mail Relay Host)] フィールドで、使用するメール サーバのホスト名または IP アドレスを入力します。

(注)　入力したメール ホストはアプライアンスからのアクセスを許可している必要があります。

ステップ 5　[ポート番号(Port Number)] フィールドに、電子メール サーバで使用するポート番号を入力します。ポートは通常、暗号化を使用しない場合は 25、SSLv3 を使用する場合は 465、TLS を使用する場合は 587 です。

ステップ 6　暗号化方式を選択するには、次のオプションがあります。

- Transport Layer Security を使用してアプライアンスとメール サーバ間の通信を暗号化するには、[暗号化方式(Encryption Method)] ドロップダウン リストから [TLS] を選択します。
- セキュア ソケット レイヤを使用してアプライアンスとメール サーバ間の通信を暗号化するには、[暗号化方式(Encryption Method)] ドロップダウン リストから [SSLv3] を選択します。
- アプライアンスとメール サーバ間の非暗号化通信を許可するには、[暗号化方式(Encryption Method)] ドロップダウン リストから [なし(None)] を選択します。

アプライアンスとメール サーバとの間の暗号化された通信では、証明書の検証は不要であることに注意してください。

ステップ 7　アプライアンスによって送信されるメッセージの送信元の電子メール アドレスとして使用する有効な電子メール アドレスを、[送信元アドレス（From Address）] フィールドに入力します。

ステップ 8　必要に応じて、メール サーバに接続する際にユーザ名とパスワードを指定するには、[認証を使用（Use Authentication）] を選択します。[ユーザ名（Username）] フィールドにユーザ名を入力します。パスワードを [パスワード（Password）] フィールドに入力します。

ステップ 9　設定したメール サーバを使用してテスト メールを送信するには、[テスト メールのサーバ設定（Test Mail Server Settings）] をクリックします。

テストの成功または失敗を示すメッセージがボタンの横に表示されます。

ステップ 10　[ポリシーを保存して終了（Save Policy and Exit）] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、システム ポリシーの適用（40-3 ページ）を参照してください。

SNMP ポーリングの設定

ライセンス：任意

システム ポリシーを使用して、アプライアンスの Simple Network Management Protocol（SNMP）ポーリングを有効化できます。SNMP 機能は、SNMP プロトコルのバージョン 1、2、および 3 をサポートします。

システム ポリシー SNMP 機能を有効にすると、アプライアンスで SNMP トラップを送信できなくなり、MIB の情報はネットワーク管理システムによるポーリングでのみ使用可能になることに注意してください。

（注）　アプライアンスをポーリングするには、使用する任意のコンピュータで SNMP アクセスを追加する必要があります。詳細については、アプライアンスのアクセス リストの設定（40-4 ページ）を参照してください。SNMP MIB にはアプライアンスの攻撃に使用される可能性がある情報も含まれているので注意してください。シスコ では、SNMP アクセスのアクセス リストを MIB のポーリングに使用される特定のホストに制限することを推奨しています。シスコ では、SNMPv3 を使用し、ネットワーク管理アクセスには強力なパスワードを使用することも推奨しています。

SNMP ポーリングを設定するには、次の手順を実行します。

ステップ 1　**[**設定（**Configuration**）**] > [ASA FirePOWER** 設定（**ASA FirePOWER Configuration**）**] > [**ローカル（**Local**）**] > [**システム ポリシー（**System Policy**）**]** の順に選択します。

[システム ポリシー（System Policy）] ページが表示されます。

ステップ 2　次の選択肢があります。

- 既存のシステム ポリシーの SNMP ポーリングの設定を変更するには、システム ポリシーの横にある編集アイコン（ ）をクリックします。
- 新しいシステム ポリシーの一部として SNMP ポーリングの設定を行うには、[ポリシーの作成（Create Policy）] をクリックします。

  システム ポリシーの作成（40-1 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[作成（Create）] をクリックします。

ステップ 3　アプライアンスのポーリングに使用する各コンピュータに SNMP アクセスを追加していない場合は、ここで追加してください。詳細については、アプライアンスのアクセス リストの設定（40-4 ページ）を参照してください。

ステップ 4　[SNMP] をクリックします。

[SNMP] ページが表示されます。

ステップ 5　[SNMP バージョン（SNMP Version）] ドロップダウン リストから、使用する SNMP バージョンを選択します。

ドロップダウン リストに選択したバージョンが表示されます。

ステップ 6　次の選択肢があります。

- [バージョン 1（Version 1）] または [バージョン 2（Version 2）] を選択した場合は、[コミュニティ ストリング（Community String）] フィールドに SNMP コミュニティ名を入力します。ステップ 15 に進みます。
- [Version 3] を選択した場合、[ユーザを追加（Add User）] をクリックするとユーザ定義ページが表示されます。

ステップ 7　[ユーザ名（Username）] フィールドにユーザ名を入力します。

ステップ 8　[認証プロトコル（Authentication Protocol）] ドロップダウン リストから、認証に使用するプロトコルを選択します。

ステップ 9　[認証パスワード（Authentication Password）] フィールドに SNMP サーバの認証に必要なパスワードを入力します。

ステップ 10　[認証パスワード（Authentication Password）] フィールドのすぐ下にある [パスワードの確認（Verify Password）] フィールドに認証パスワードを再入力します。

ステップ 11　使用するプライバシー プロトコルを [プライバシー プロトコル（Privacy Protocol）] リストから選択するか、プライバシー プロトコルを使用しない場合は [なし（None）] を選択します。

ステップ 12　[プライバシー パスワード（Privacy Password）] フィールドに SNMP サーバで必要な SNMP プライバシー キーを入力します。

ステップ 13　[プライバシー パスワード（Privacy Password）] フィールドのすぐ下にある [パスワードの確認（Verify Password）] フィールドにプライバシー パスワードを再入力します。

ステップ 14　[追加（Add）] をクリックします。

ユーザが追加されます。ステップ 6 ～ 13 までを繰り返して、さらにユーザを追加できます。ユーザを削除するには、削除アイコン（ ）をクリックします。

ステップ 15　[ポリシーを保存して終了（Save Policy and Exit）] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、システム ポリシーの適用（40-3 ページ）を参照してください。

STIG コンプライアンスの有効化

ライセンス：任意

米国連邦政府内の組織は、Security Technical Implementation Guides（STIG）に示されている一連のセキュリティ チェックリストに準拠しなければならない場合があります。STIG コンプライアンス オプションは、米国国防総省によって定められた特定の要件に準拠することを目的とした設定を有効にします。

展開内の ASA FirePOWER モジュール で STIG コンプライアンスを有効にする場合は、すべての ASA FirePOWER モジュール で有効にする必要があります。

STIG コンプライアンスを有効にした場合、適用可能なすべての STIG に厳格なコンプライアンスが保証されるわけではありません。

STIG コンプライアンスを有効にすると、ローカル シェル アクセス アカウントのパスワードの複雑さや維持に関するルールが変わります。さらに、STIG コンプライアンス モードでは、ssh のリモート ストレージを使用できません。

STIG コンプライアンスが有効なシステム ポリシーを適用すると、アプライアンスが強制的に再起動されるので注意してください。すでに STIG が有効になっているアプライアンスに STIG が有効なシステム ポリシーを適用した場合、アプライアンスは再起動しません。STIG が無効なシステム ポリシーを STIG が有効になっているアプライアンスに適用した場合、STIG は引き続き有効であり、アプライアンスはリブートしません。

注意　サポートからの支援なしでこの設定を無効にすることはできません。また、この設定はシステムのパフォーマンスに大きく影響する可能性があります。シスコ では、米国国防総省のセキュリティ要件に準拠する以外の目的で、STIG コンプライアンスを有効化することを推奨しません。

STIG コンプライアンスを有効にするには、次の手順を実行します。

ステップ **1**　**[**設定（**Configuration**）**] > [ASA FirePOWER** 設定（**ASA FirePOWER Configuration**）**] > [**ローカル（**Local**）**] > [**システム ポリシー（**System Policy**）**]** の順に選択します。

[システム ポリシー（System Policy）] ページが表示されます。

ステップ **2**　次の選択肢があります。

- 既存のシステム ポリシーの時間の設定を変更するには、システム ポリシーの横にある編集アイコン（）をクリックします。
- 新しいシステム ポリシーの一部として時間の設定を行うには、[ポリシーの作成（Create Policy）] をクリックします。

  システム ポリシーの作成（40-1 ページ）で説明されているように、システム ポリシーの名前および説明を入力し、[保存（Save）] をクリックします。

ステップ **3**　[STIG コンプライアンス（STIG Compliance）] をクリックします。

[STIG コンプライアンス（STIG Compliance）] ページが表示されます。

ステップ **4**　STIG コンプライアンスをアプライアンスで永続的に有効にする場合は、[STIG コンプライアンスを有効化（Enable STIG Compliance）] を選択します。

注意　STIG コンプライアンスが有効なポリシーを適用した後、アプライアンスで STIG コンプライアンスを無効にすることはできません。コンプライアンスを無効にする必要がある場合は、サポートに連絡してください。

ステップ **5**　[ポリシーを保存して終了（Save Policy and Exit）] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、システム ポリシーの適用（40-3 ページ）を参照してください。

STIG コンプライアンスを有効にするシステム ポリシーをアプライアンスに適用すると、アプライアンスが再起動するので注意してください。STIG が有効なシステム ポリシーをすでに STIG が有効になっているアプライアンスに適用した場合は、アプライアンスはリブートしないことに注意してください。

ASA FirePOWER モジュールの設定

次の表は、ASA FirePOWER モジュール のローカル設定をまとめたものです。

表 **41-1** ローカル設定のオプション

オプション	説明	詳細
情報	アプライアンスに関する現在の情報が表示されます。アプライアンスの名前を変更することもできます。	アプライアンス情報の表示と変更（41-1 ページ）
HTTPS 証明書（HTTPS Certificate）	信頼できる機関の HTTPS サーバ証明書を要求し（必要な場合）、証明書をアプライアンスにアップロードできます。	カスタム HTTPS 証明書の使用（41-3 ページ）
クラウド サービス（Cloud Services）	Collective Security Intelligence クラウドから URL フィルタリング データをダウンロードしたり、未分類の URL を検索したり、検出されたファイルの診断情報を シスコ に送信したりできます。	クラウド通信の有効化（41-2 ページ）

アプライアンス情報の表示と変更

ライセンス：任意

[情報（Information）] ページには、ASA FirePOWER モジュール に関する情報が表示されます。これには、製品名とモデル番号、オペレーティング システムとバージョン、現在のシステム ポリシーなどの読み取り専用情報が含まれます。このページには、アプライアンスの名前を変更するオプションも用意されています。

次の表で、各フィールドについて説明します。

表 **41-2** アプライアンス情報

フィールド	説明
[名前（Name）]	アプライアンスに割り当てられた名前。この名前は ASA FirePOWER モジュール のコンテキスト内でのみ使用されることに注意してください。ホスト名をアプライアンスの名前として使用できますが、このフィールドに別の名前を入力しても、ホスト名は変更されません。
製品モデル（Product Model）	アプライアンスのモデル名。
シリアル番号（Serial Number）	アプライアンスのシャーシのシリアル番号。
ソフトウェア バージョン（Software Version）	現在インストールされているソフトウェアのバージョン。

表 41-2　アプライアンス情報（続き）

フィールド	説明
オペレーティング システム（Operating System）	アプライアンス上で現在実行されているオペレーティング システム。
オペレーティング システム バージョン（Operating System Version）	アプライアンス上で現在実行されているオペレーティング システムのバージョン。
IPv4 アドレス（IPv4 Address）	アプライアンスのデフォルトの管理インターフェイス（eth0）の IPv4 アドレス。アプライアンスで IPv4 の管理が無効になっている場合は、このフィールドにそのことが示されます。
IPv6 アドレス（IPv6 Address）	アプライアンスのデフォルトの管理インターフェイス（eth0）の IPv6 アドレス。アプライアンスで IPv6 の管理が無効になっている場合は、このフィールドにそのことが示されます。
現在のポリシー（Current Policies）	現在適用されているアプライアンスレベルのポリシー。ポリシーが最後に適用された後で更新されていると、ポリシーの名前がイタリック体で表示されます。
モデル番号（Model Number）	アプライアンスのモデル番号。この番号は、トラブルシューティングで重要になる場合があります。

アプライアンスの情報を変更するには、次の手順を実行します。

ステップ 1　**[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ローカル（Local）] > [設定（Configuration）]** の順に選択します。

[情報（Information）] ページが表示されます。

ステップ 2　アプライアンス名を変更するには、[名前（Name）] フィールドに新しい名前を入力します。

名前は、英数字である必要があり、数字だけで構成することはできません。

ステップ 3　変更を保存するには、[保存（Save）] をクリックします。

ページが更新され、変更が保存されます。

クラウド通信の有効化

ライセンス：URL フィルタリング（URL Filtering）またはマルウェア

ASA FirePOWER モジュール は、シスコ の Collective Security Intelligence クラウド に接続してさまざまなタイプの情報を取得します。

- アクセス コントロール ルールに関連付けられているファイル ポリシーにより、デバイスはネットワーク トラフィックで送信されるファイルを検出できます。ASA FirePOWER モジュール は、シスコ クラウドからのデータを使用して、ファイルがマルウェアに相当するかどうかを判定します。ファイル ポリシーの概要と作成（32-4 ページ）を参照してください。
- URL フィルタリングを有効にすると、ASA FirePOWER モジュール は、一般的にアクセスされる多数の URL のカテゴリとレピュテーション データを取得し、さらに未分類 URL の検索も実行します。その後、アクセス コントロール ルールの URL 条件をすばやく作成できます。レピュテーション ベースの URL ブロッキングの実行（8-9 ページ）を参照してください。

ASA FirePOWER モジュール のローカル構成を使用して、次のオプションを指定します。

URL フィルタリングを有効にする（**Enable URL Filtering**）

カテゴリおよびレピュテーションベースの URL フィルタリングを実行するには、このオプションを有効にする必要があります。

不明 **URL** のクエリ クラウド（**Query Cloud for Unknown URL**）

監視対象ネットワーク上で誰かがローカル データ セットに存在しない URL を参照しようとしたときに、システムがクラウドを照会できるようにします。

クラウドが URL のカテゴリまたはレピュテーションを識別できない場合や、ASA FirePOWER モジュール がクラウドに接続できない場合、その URL は、カテゴリまたはレピュテーション ベースの URL 条件を含むアクセス コントロール ルールと一致しません。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

プライバシー上の理由などで、未分類の URL を シスコ クラウドでカタログ化したくない場合は、このオプションを無効にします。

自動アップデートを有効にする（**Enable Automatic Updates**）

システムが定期的にクラウドに接続して、アプライアンスのローカル データ セットに含まれる URL データの更新を取得できるようにします。通常、クラウドはそのデータを 1 日に 1 回更新しますが、自動更新を有効にすると、ASA FirePOWER モジュール によるチェックが 30 分ごとに強制的に行われ、常に最新の情報が保持されるようになります。

通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL フィルタリング データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

システムがクラウドに接続するタイミングを厳密に制御する必要がある場合は、URL フィルタリング更新の自動化（39-9 ページ）で説明しているように、自動更新を無効にして、代わりにスケジューラを使用できます。

（注）　シスコ では、自動更新を有効にするか、またはスケジューラを使用して更新をスケジュールすることを推奨しています。手動でオンデマンド更新を実行することもできますが、定期的にクラウドに接続するようにシステムを自動化することで、最も関連性の高い最新の URL データを取得できます。

ライセンス

カテゴリおよびレピュテーションベースの URL フィルタリングとデバイスベースのマルウェア検出を実行するには、ASA FirePOWER モジュール で適切なライセンスを有効にする必要があります（ASA FirePOWER モジュールのライセンス（42-1 ページ）を参照）。

ASA FirePOWER モジュールに URL フィルタリング（URL Filtering）のライセンスがない場合は、クラウド接続オプションを設定できません。[クラウド サービス（Cloud Services）] ローカル設定ページには、ライセンスが付与されているオプションのみが表示されます。ライセンスが期限切れになっている ASA FirePOWER モジュール では、クラウドに接続できません。

ASA FirePOWER モジュールに URL フィルタリング（URL Filtering）ライセンスを追加すると、URL フィルタリングの設定オプションが表示されることに加えて、[URL フィルタリングを有効にする（Enable URL Filtering）] と [自動アップデートを有効にする（Enable Automatic Updates）] が自動的に有効になります。必要な場合は、手動でこれらのオプションを無効にすることができます。

インターネット アクセス

システムは、シスコ クラウドへの接続にポート 80/HTTP および 443/HTTPS を使用します。

次の手順は、シスコ クラウドとの通信を有効にする方法、および URL データのオンデマンド更新を実行する方法を示しています。更新がすでに進行中である場合は、オンデマンド更新を開始できません。

クラウドとの通信を有効にするには、次の手順を実行します。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ローカル（Local）] > [設定（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

ステップ 2　[クラウド サービス（Cloud Services）] をクリックします。

[クラウド サービス（Cloud Services）] ページが表示されます。URL フィルタリング（URL Filtering）ライセンスがある場合は、このページに URL データの最終更新時間が表示されます。

ステップ 3　上記の説明に従って、クラウド接続のオプションを構成します。

[自動アップデートを有効にする（Enable Automatic Updates）] または [不明 URL のクエリ クラウド（Query Cloud for Unknown URL）] を有効にするには、あらかじめ [URL フィルタリングを有効にする（Enable URL Filtering）] を有効にする必要があります。

ステップ 4　[保存（Save）] をクリックします。

設定が保存されます。URL フィルタリングを有効化すると、URL フィルタリングが最後に有効化されてから経過した時間、または URL フィルタリングが今回初めて有効化されたかどうかに応じて、ASA FirePOWER モジュールがクラウドから URL フィルタリング データを取得します。

システムの **URL** データのオンデマンド更新を実行するには、次の手順を実行します。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [統合（Integration）] > [Cisco CSI] の順に選択します。

[情報（Information）] ページが表示されます。

ステップ 2　[URL フィルタリング（URL Filtering）] をクリックします。

[URL フィルタリング（URL Filtering）] ページが表示されます。

ステップ 3　[今すぐ更新（Update Now）] をクリックします。

ASA FirePOWER モジュール がクラウドに接続し、更新が使用可能な場合はその URL フィルタリング データを更新します。

時刻（Time）

[時刻（Time）] ページを使用して、現在の時刻と時刻源をASA FirePOWER モジュールに表示できます。

ASA FirePOWER モジュールのライセンス

組織に対して ASA FirePOWER の最適な展開を実現するために、さまざまな機能についてライセンスを取得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。

ライセンスについて

ライセンス：任意

組織に対して ASA FirePOWER の最適な展開を実現するために、さまざまな機能についてライセンスを取得することができます。

ライセンスにより、デバイスは次のようなさまざまな機能を実行できます。

- 侵入検知と防御
- セキュリティ インテリジェンス フィルタリング
- ファイル制御および高度なマルウェア防御
- アプリケーション、ユーザ、および URL 制御

ASA FirePOWER モジュール のライセンス付き機能にアクセスできなくなる状況がいくつかあります。ライセンス付き機能を削除できます。また、一部のライセンスには有効期限が設定されています。いくつかの例外がありますが、期限切れライセンスまたは削除済みライセンスに関連付けられている機能は使用できません。

ここでは、ASA FirePOWER モジュール 展開環境で使用可能なライセンスのタイプについて説明します。アプライアンスで有効にできるライセンスは、他の有効なライセンスに応じて異なる場合があります。

次の表に、ASA FirePOWER モジュール ライセンスの要約を示します。

表 *42-1*　*ASA FirePOWER* モジュール ライセンス

ライセンス	付与される機能	要件
保護	侵入検知と防御 ファイル制御 セキュリティ インテリジェンス フィルタリング	なし
Control	ユーザおよびアプリケーション制御	保護
マルウェア	高度なマルウェア防御(ネットワークベースのマルウェアの検出とブロッキング)	保護
URL フィルタリング	カテゴリとレピュテーションに基づく URL フィルタリング	保護

詳細については、以下を参照してください。

- 保護(42-2 ページ)
- Control(42-3 ページ)
- マルウェア(42-3 ページ)
- URL フィルタリング(42-3 ページ)

保護

ライセンス:保護

保護 ライセンスでは、侵入検知および防御、ファイル制御、およびセキュリティ インテリジェンスのフィルタリングを実行できます。

- 侵入検知および防御により、侵入とエクスプロイトを検出するためネットワーク トラフィックを分析できます。またオプションで違反パケットをドロップできます。
- ファイル制御により、特定のアプリケーション プロトコルを介した特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード(送信)またはダウンロード(受信)をブロックできます。マルウェア ライセンス(マルウェア(42-3 ページ)を参照)では、マルウェアの性質に基づいて限られたファイル タイプを検査およびブロックすることもできます。
- *Security Intelligence* フィルタリングにより、トラフィックをアクセス コントロール ルールによる分析対象にする前に、特定の IP アドレスをブラックリストに追加(その IP アドレスとの間のトラフィックを拒否)できます。ダイナミック フィードにより、最新の情報に基づいて接続をただちにブラックリストに追加できます。オプションで、セキュリティ インテリジェンス フィルタリングに「モニタのみ」設定を使用できます。

ライセンスがない状態で 保護 関連の検査を実行するようにアクセス コントロール ポリシーを設定できますが、保護 ライセンスを最初に ASA FirePOWER モジュール に追加するまではポリシーを適用できません。

保護 ライセンスを ASA FirePOWER モジュール から削除すると、ASA FirePOWER モジュールは侵入イベントとファイル イベントを検出しなくなります。また、ASA FirePOWER モジュールは シスコ によって提供される情報またはサードパーティのセキュリティ インテリジェンス情報を取得するためにインターネットに接続しなくなります。保護 を再度有効にするまでは、既存のポリシーを再適用できません。

保護 ライセンスは URL フィルタリング、マルウェア、およびControl ライセンスに必要であるため、保護 ライセンスを削除または無効にすると、URL フィルタリング、マルウェア、または Control ライセンスを削除または無効にすることと同じ効果があります。

Control

ライセンス:Control

Control ライセンスでは、アクセス コントロール ルールにユーザとアプリケーションの条件を追加することで、ユーザとアプリケーションの制御を実装できます。Control を有効にするには、保護 も有効にする必要があります。

Control ライセンスがない状態でアクセス コントロール ルールにユーザ条件とアプリケーション条件を追加できますが、ポリシーを適用するには、最初に Control ライセンスを ASA FirePOWER モジュール に追加します。

Controlライセンスを削除すると、既存のアクセス コントロール ポリシーにユーザまたはアプリケーションの条件が含まれている場合はそのポリシーを再適用できません。

URL フィルタリング

ライセンス:URL フィルタリング

URL フィルタリングにより、モニタ対象ホストにより要求される URL に基づいて、ネットワークを移動可能なトラフィックを判別するアクセス コントロール ルールを作成し、ASA FirePOWER モジュール が シスコ クラウドから取得する URL に関する情報に関連付けることができます。URL フィルタリング を有効にするには、保護 ライセンスも有効にする必要があります。

ヒント　URL フィルタリング ライセンスがない状態で、許可またはブロックする個別 URL または URL グループを指定できます。これにより、Web トラフィックをカスタムできめ細かく制御できますが、URL カテゴリおよびレピュテーション データをネットワーク トラフィックのフィルタリングに使用することはできません。

URL フィルタリングにはサブスクリプション ベースの URL フィルタリング ライセンスが必要です。URL フィルタリング ライセンスがない状態でも、アクセス コントロール ルールにカテゴリ ベースの URL 条件およびレピュテーション ベースの URL 条件を追加できますが、ASA FirePOWER モジュール は URL 情報を取得するためにクラウドに接続しません。最初に URL フィルタリング ライセンスを ASA FirePOWER モジュール に追加するまでは、アクセス コントロール ポリシーを適用できません。

ASA FirePOWER モジュール からライセンスを削除すると、URL フィルタリングにアクセスできなくなることがあります。また、URL フィルタリング ライセンスが期限切れになることがあります。ライセンスが期限切れになるか、ライセンスを削除すると、URL 条件が含まれているアクセス コントロール ルールは URL フィルタリングをただちに停止し、ASA FirePOWER モジュール はクラウドにアクセスできなくなります。既存のアクセス コントロール ポリシーに、カテゴリ ベースまたはレピュテーション ベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再適用することができません。

マルウェア

ライセンス:マルウェア

マルウェア ライセンスでは、高度なマルウェア防御を実行できます。つまり、デバイスを使用して、ネットワーク上で送信されるファイルからマルウェアを検出してブロックできます。デバイス上で マルウェア を有効にするには、保護 も有効にする必要があります。

ファイル ポリシーの一部としてマルウェア検出を設定し、その後 1 つ以上のアクセス コントロール ルールを関連付けます。ファイル ポリシーは、特定のアプリケーション プロトコルを使用して特定のファイルをアップロードまたはダウンロードするユーザを検出できます。マルウェア ライセンスでは、限られたファイル タイプのセットを調べてマルウェアが存在するかどうかを確認します。マルウェア ライセンスでは、ファイル リストに特定のファイルを追加し、そのファイル リストをファイル ポリシー内で有効にすることもできます。これにより、検出時にこれらのファイルを自動的に許可またはブロックできます。

マルウェア ライセンスがなくてもアクセス コントロール ルールにマルウェア検出ファイル ポリシーを追加できますが、アクセス コントロール ルール エディタでこのファイル ポリシーに警告アイコン( )が付きます。ファイル ポリシー内でも、マルウェア クラウド ルックアップ ルールに警告アイコンが付きます。マルウェア検出ファイル ポリシーを含むアクセス コントロール ポリシーを適用する前に、マルウェア ライセンスを追加する必要があります。後からライセンスを削除すると、マルウェア検出を実行するファイル ポリシーが含まれている既存のアクセス コントロール ポリシーをこれらのデバイスに対して再適用することはできません。

マルウェア ライセンスを削除するか、期限切れになると、ASA FirePOWER モジュール はマルウェア クラウド ルックアップの実行と、シスコ クラウドから送信される遡及的イベントの認識を停止します。既存のアクセス コントロール ポリシーにマルウェア検出を実行するファイル ポリシーが含まれている場合、このアクセス コントロール ポリシーを再適用することはできません。マルウェア ライセンスの期限切れまたは削除後のごく短い時間内は、マルウェア クラウド ルックアップ ファイル ルールで検出されたファイルのキャッシュされた性質を、システムが使用できることに注意してください。この時間枠の経過後は、システムは検索を実行せず `Unavailable` という性質をこれらのファイルに割り当てます。

ライセンスの表示

ライセンス:任意

[ライセンス(Licenses)] ページで、ASA FirePOWER モジュール のライセンスを表示します。

[ラインセス(Licenses)] ページ以外にも、ライセンスとライセンス制限を確認できる方法がいくつかあります。

- [製品ライセンス(Product Licensing)] ダッシュボード ウィジェットはライセンスの概要を示します。
- [デバイス(Device)] ページ([設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [デバイス管理(Device Management)] > [デバイス(Device)])には、ライセンスがリストされます。

ライセンスを確認するには、次の手順を実行します。

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ライセンス(Licenses)] の順に選択します。

[ライセンス(Licenses)] ページが表示されます。

ASA FirePOWER モジュールへのライセンスの追加

ライセンス:任意

ASA FirePOWER モジュールにライセンスを追加する前に、ライセンスの購入時にシスコから提供されたアクティベーション キーがあることを確認してください。ライセンス付き機能を使用する前に、ライセンスを追加する必要があります。

(注)　バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを(それらが使用されている場所をメモした上で)削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。

ライセンスを追加するには、次の手順を実行します。

ステップ **1**　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ライセンス(Licenses)] の順に選択します。

[ライセンス(Licenses)] ページが表示されます。

ステップ **2**　[新規ライセンスの追加(Add New License)] をクリックします。

[ライセンスの追加(Add License)] ページが表示されます。

ステップ **3**　ライセンスを電子メールで受信しましたか?

- 電子メールで受信した場合は電子メールからライセンスをコピーし、[ライセンス(License)] フィールドに貼り付け、[ライセンスの送信(Submit License)] をクリックします。

  ライセンスが正しい場合、ライセンスが追加されます。残りの手順は省略します。

- 電子メールで受信していない場合は、[ライセンスの取得(Get License)] をクリックします。

  [製品ライセンス登録(Product License Registration)] ポータルが表示されます。インターネットにアクセスできない場合は、インターネットにアクセスできるコンピュータに切り替えてください。ページ下部に表示されるライセンス キーを書きとめ、https://www.cisco.com/go/license [英語] を参照します。

ステップ **4**　画面の指示に従ってライセンスを取得します。ライセンスは電子メールで送信されます。

ヒント　サポート サイトにログインした後で、[ライセンス(Licenses)] タブでライセンスを要求することもできます。

ステップ **5**　電子メールからライセンスをコピーし、ASA FirePOWER モジュール の Web ユーザ インターフェイスの [ライセンス(License)] フィールドに貼り付け、[ライセンスの送信(Submit License)] をクリックします。

ライセンスが有効な場合、ライセンスが追加されます。

ライセンスの削除

ライセンス：任意

何らかの理由でライセンスを削除する必要がある場合は、次の手順を使用します。シスコ は各 ASA FirePOWER モジュール の固有ライセンス キーに基づいてライセンスを生成するため、ある ASA FirePOWER モジュール からライセンスを削除し、この削除したライセンスを別の ASA FirePOWER モジュール で再利用することはできないことに注意してください。

ほとんどの場合、ライセンスを削除すると、そのライセンスによって有効になる機能を使用することができなくなります。詳細については、ライセンスについて（42-1 ページ）を参照してください。

ライセンスを削除するには：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ライセンス（Licenses）] の順に選択します。

[ライセンス（Licenses）] ページが表示されます。

ステップ 2　削除するライセンスの横にある削除アイコン（ ）をクリックします。

ステップ 3　ライセンスを削除することを確認します。

ライセンスが削除されます。

ASA FirePOWER モジュール ソフトウェアの更新

シスコでは、ルールの更新や位置情報データベース（GeoDB）の更新、脆弱性データベース（VDB）の更新だけでなく、ASA FirePOWER モジュール ソフトウェア本体のメジャーおよびマイナーの更新など、さまざまなタイプの更新を電子的に配布しています。

注意 この項では、ASA FirePOWER モジュール の更新に関する全般的な情報について説明します。VDB、GeoDB、侵入ルールなどを更新する前に、更新に付随しているリリース ノートまたはアドバイザリ テキストを読んでおく必要があります。リリース ノートには、前提条件、警告、および特定のインストールとアンインストールの手順などの重要な情報が記載されています。

リリース ノートまたはアドバイザリ テキストに特に記載されていない限り、を更新しても設定は変更されず、設定はそのまま保持されます。

詳細については、次の各項を参照してください。

- 更新のタイプについて（43-1 ページ）
- ソフトウェア更新の実行（43-2 ページ）
- ソフトウェア アップデートのアンインストール（43-7 ページ）
- 脆弱性データベースの更新（43-8 ページ）
- ルールの更新とローカル ルール ファイルのインポート（43-10 ページ）
- 位置情報データベースの更新（43-21 ページ）

更新のタイプについて

ライセンス：任意

シスコ では、侵入ルールの更新や VDB の更新だけでなく、ASA FirePOWER モジュールソフトウェア本体のメジャーおよびマイナーの更新など、さまざまなタイプの更新を電子的に配布しています。

次の表で、シスコ が提供している更新のタイプについて説明します。ほとんどのタイプの更新では、ダウンロードとインストールをスケジュールすることができます。タスクのスケジュール（39-1 ページ）および 再帰的なルール更新の使用（43-14 ページ）を参照してください。

表 *43-1*　*ASA FirePOWER* モジュールの更新タイプ

更新のタイプ	説明	スケジュールを行うか	アンインストールをするか
パッチの適用	パッチには、限定された範囲の修正が含まれています（また通常は、5.4.0.1 のようにバージョン番号の 4 桁目が変更されます）。	はい	はい
機能の更新	機能の更新はパッチよりも包括的であり、通常は新しい機能が含まれています（また通常は、5.4.1 のようにバージョン番号の 3 桁目が変更されます）。	はい	はい
メジャーな更新（メジャーおよびマイナー バージョンのリリース）	メジャーな更新は「アップグレード」と呼ばれることもあります。この更新には新しい機能が含まれており、大規模な変更が含まれることがあります（通常は、5.3 または 5.4 のようにバージョン番号の 1 桁目または 2 桁目が変更されます）。	いいえ	いいえ
VDB	VDB の更新は、ホストが影響を受ける可能性がある既知の脆弱性データベースに影響します。	はい	いいえ
侵入ルール	侵入ルールの更新には、新規および更新された侵入ルールとプリプロセッサ ルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が含まれています。ルールの更新では、ルールが削除されたり、新しいルール カテゴリとデフォルトの変数が提供されたり、デフォルトの変数値が変更されたりすることもあります。	はい	いいえ
位置情報データベース（GeoDB）	GeoDB の更新には、物理的な場所や接続タイプなど、検出されたルート可能な IP アドレスにシステムが関連付けることができるものに関する更新情報が含まれています。位置情報データは、アクセス コントロール ルールとして使用できます。位置情報の詳細を表示するには、GeoDB をインストールする必要があります。	はい	いいえ

ただし、パッチや他のマイナーな更新はアンインストールできますが、VDB、GeoDB、または侵入ルールに対するメジャーな更新をアンインストールしたり、前のバージョンに戻したりすることはできません。を、FireSIGHT システム の新しいメジャー バージョン および古いバージョンに戻す必要がある場合は、サポートに連絡してください。

ソフトウェア更新の実行

ライセンス：任意

更新するには、いくつかの基本的な手順があります。最初にリリース ノートを参照し、必要な更新前のタスクをすべて完了することで更新の準備を整えておく必要があります。その後に更新を開始することができます。更新が正常に終了したことを確認する必要があります。最後に、更新後の必要な手順を完了させます。

詳細については、次の項を参照してください。

- 更新の計画（43-3 ページ）
- 更新プロセスについて（43-3 ページ）
- ASA FirePOWER モジュール ソフトウェアの更新（43-5 ページ）
- メジャーな更新のステータスのモニタリング（43-7 ページ）

更新の計画

ライセンス:任意

更新を開始する前に、リリース ノートをよく読んで理解する必要があります。リリース ノートはサポート サイトからダウンロードすることができます。リリース ノートには、新しい機能、および既知の問題と解決済みの問題が記載されています。また、リリース ノートには前提条件、警告、および特別なのインストールおよびアンインストールの手順についての重要な情報が含まれています。

以降の項では、更新の計画で検討しなければならない要素の概要を提供します。

ソフトウェア バージョンの要件

適切なソフトウェア バージョンを実行していることを確認してください。リリース ノートには必要なバージョンが示されています。古いバージョンを実行している場合は、サポート サイトから更新を取得することができます。

時間とディスク スペース要件

十分な空きディスク領域があることを確認し、更新のために十分な時間を確保しておく必要があります。リリース ノートには、ディスク領域と時間の要件が示されています。

設定のバックアップのガイドライン

シスコでは、メジャーな更新を開始する前に、ASA FirePOWER モジュールに残っているバックアップを外部の場所にコピーしてから、それらのバックアップを削除することを推奨しています。更新のタイプに関係なく、現行の設定データを外部の場所にバックアップしておく必要もあります。バックアップと復元の使用（45-1 ページ）を参照してください。

更新を実行するタイミング

更新プロセスはトラフィックの調査 およびトラフィック フロー、および更新を行っている間は Data Correlator が無効になっていることにより、シスコ では、保守を行っている間、または中断が及ぼす影響が最も少ない時間に更新を行うことを推奨しています。

更新プロセスについて

ライセンス:任意

ASA FirePOWER モジュール を更新するには ASA FirePOWER モジュール インターフェイスを使用します。

[製品アップデート（Product Updates）] ページ（**[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [更新（Updates）]**）には、それぞれの更新のバージョン、およびその更新が生成された日時が表示されます。また、ソフトウェアの再起動が更新の一環として必要です。サポートから取得した更新をアップロードすると、更新がページに示されます。パッチ機能および機能の更新のアンインストーラも表示されます。ソフトウェア アップデートのアンインストール（43-7 ページ）を参照してください。このページには VDB の更新も一覧表示されます。

ヒント　パッチおよび機能の更新では、自動更新機能を利用することができます。ソフトウェア更新の自動化（39-7 ページ） を参照してください。

トラフィック フローとインスペクション

更新をインストールまたはアンインストールすると、次の機能に影響を及ぼすことがあります。

- トラフィックのインスペクション（アプリケーションおよびユーザの認識とコントロール、URL フィルタリング、セキュリティ インテリジェンス フィルタリング、侵入検出と防御、接続のロギングなど）
- トラフィック フロー

Data Correlator は、システムの更新中は動作しません。更新が完了すると再開します。

ネットワーク トラフィック中断の動作と期間は、ASA FirePOWER モジュール の設定方法と展開方法、およびASA FirePOWER モジュール が再起動されるかどうかに応じて異なります。特定の更新に対してネットワーク トラフィックがいつ、どのように影響を受けるかについての情報は、リリース ノートを参照してください。

更新時の **ASA FirePOWER** モジュールの使用

更新のタイプに関係なく、ASA FirePOWER モジュール を使用して、更新のモニタリング以外のタスクを実行しないでください。

メジャーな更新中にユーザが ASA FirePOWER モジュール を使用するのを阻止するとともに、メジャーな更新の進捗をユーザが簡単にモニタできるようにするために、ASA FirePOWER モジュール インターフェイスは合理化されています。タスク キュー（[モニタリング（Monitoring）] > [ASA FirePOWER モニタリング（ASA FirePOWER Monitoring）] > [タスクのステータス（Task Status）]）で、マイナーな更新の進行状況をモニタできます。マイナーな更新中に ASA FirePOWER モジュール を使用することは禁止されていませんが、シスコでは推奨していません。

マイナーな更新であっても、更新プロセス中は ASA FirePOWER モジュール を使用できなくなることがあります。これは想定されている動作です。そのような場合は、再び ASA FirePOWER モジュール にアクセスできるようになるまで待機します。まだ更新が実行中の場合は、更新が完了するまで ASA FirePOWER モジュール を使用しないでください。更新中は、ASA FirePOWER モジュール が 2 回リブートされることがありますが、これは予想される動作です。

注意　（更新に失敗した場合や、[更新ステータス（Update Status）] ページを手動更新しても進捗が表示されない場合など）更新で問題が発生した場合には、更新を再開しないでください。代わりに、サポートに連絡してください。

更新後

リリース ノートに記載されている更新後のタスクをすべて完了し、展開が正常に実行されていることを確認する必要があります。

更新後に行う最も重要なタスクは、アクセス コントロール ポリシーを再適用することです。アクセス コントロール ポリシーを適用すると、トラフィック フローと処理が一時的に停止することがあります。また、いくつかのパケットが検査されない場合があります。設定変更の展開（4-12 ページ）を参照してください。

また、次の作業を実行する必要があります。

- 更新が正常に終了したことを確認する
- 必要に応じて侵入ルール、VDB、および GeoDB を更新する
- リリース ノートの情報に基づいて、必要な設定変更を行う
- リリース ノートに記載されている、更新後の追加タスクを実行する

ASA FirePOWER モジュール ソフトウェアの更新

ライセンス：任意

更新のタイプ、および ASA FirePOWER モジュール がインターネットへアクセスできるかどうかに応じて、ASA FirePOWER モジュール ソフトウェアを次のいずれかの方法で更新します。

- ASA FirePOWER モジュール がインターネットにアクセスできる場合は、サポート サイトから直接更新を取得できます。このオプションは、メジャーな更新ではサポートされていません。
- サポート サイトから更新を手動でダウンロードして、ASA FirePOWER モジュール へアップロードすることもできます。ASA FirePOWER モジュール がインターネットにアクセスできない場合や、メジャーな更新を実行している場合は、このオプションを選択します。

メジャーな更新の場合は、ASA FirePOWER モジュール を更新すると以前の更新のアンインストーラが削除されます。

ASA FirePOWER モジュール ソフトウェアを更新するには、次の手順を実行します。

ステップ **1**　リリース ノートを読んで、更新前の必要なタスクを完了させます。

更新前のタスクには、たとえば、次のような項目の確認が含まれます。ASA FirePOWER モジュール がシスコ ソフトウェアの正しいバージョンを実行しているか、更新を実行するための十分な空きディスク領域があるか、更新を実行するために十分な時間を確保しているか、設定データをバックアップしたか。

ステップ **2**　更新をアップロードします。更新のタイプ、および ASA FirePOWER モジュール がインターネットにアクセスできるかどうかに応じて、2 つのオプションがあります。

- メジャーな更新を除くすべての更新において、ASA FirePOWER モジュール がインターネットにアクセスできる場合は、**[**設定（**Configuration**）**] > [ASA FirePOWER**の設定（**ASA FirePOWER Configuration**）**] > [**更新（**Updates**）**]** を選択し、[アップデートのダウンロード（Download Updates）] をクリックして、次のサポート サイトのいずれかで最新の更新を確認します。
  - **Sourcefire**：（https://support.sourcefire.com/）
  - シスコ：（http://www.cisco.com/cisco/web/support/index.html）
- メジャーな更新の場合、またはASA FirePOWER モジュール がインターネットにアクセスできない場合は、最初に次のいずれかのサポート サイトから更新を手動でダウンロードする必要があります。
  - **Sourcefire**：（https://support.sourcefire.com/）
  - シスコ：（http://www.cisco.com/cisco/web/support/index.html）
- **[**設定（**Configuration**）**] > [ASA FirePOWER**設定（**ASA FirePOWER Configuration**）**] > [**更新（**Updates**）**]** の順に選択し、**[**アップデートのアップロード（**Upload Update**）**]** をクリックします。[ファイルの選択（Choose File）] をクリックし、更新を選択して [アップロード（Upload）] をクリックします。

（注）　[製品アップデート（Product Updates）] タブで [アップデートのダウンロード（Download Updates）] をクリックするか、または手動で、サポート サイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、破損する可能性があります。

更新がアップロードされます。

ステップ 3　[モニタリング（**Monitoring**）] > [**ASA FirePOWER**モニタリング（**ASA FirePOWER Monitoring**）] > [タスクのステータス（**Task Status**）] を選択してタスク キューを表示し、進行中のジョブがないことを確認します。

更新の開始時に実行中だったタスクは停止され、再開できません。これらのタスクは更新の完了後にタスク キューから手動で削除する必要があります。タスク キューは 10 秒ごとに自動的にリフレッシュされます。実行時間の長いタスクがある場合は、それらが完了するまで待ってから、更新を開始する必要があります。

ステップ 4　[設定（**Configuration**）] > [**ASA FirePOWER** 設定（**ASA FirePOWER Configuration**）] > [更新（**Updates**）] を選択します。

[製品アップデート（Product Updates）] ページが表示されます。

ステップ 5　アップロードした更新の横にあるインストール アイコンをクリックします。

更新プロセスが開始されます。更新をモニタする方法は、更新がメジャーかマイナーかによって異なります。更新のタイプを判断するには、ASA FirePOWER モジュールの更新タイプの表およびリリース ノートを参照してください。

- マイナーな更新の場合は、タスク キュー（[モニタリング（Monitoring）] > [ASA FirePOWERモニタリング（ASA FirePOWER Monitoring）] > [タスクのステータス（Task Status）]）で、更新の進行状況をモニタできます。
- メジャーな更新の場合は、タスク キューで更新の進捗のモニタリングを開始できます。ただし、ASA FirePOWER モジュール による更新前のチェックが完了すると、ユーザはモジュール インターフェイスからロックアウトされます。再度アクセスすると、[アップグレードステータス（Upgrade Status）] ページが表示されます。詳細については、メジャーな更新のステータスのモニタリング（43-7 ページ）を参照してください。

注意　更新のタイプに関係なく、更新が完了するまで、更新のモニタリング以外のタスクを実行するために ASA FirePOWER モジュール を使用しないでください。必要な場合は、ASA FirePOWER モジュール を再起動してください。詳細については、更新時の ASA FirePOWER モジュールの使用（43-4 ページ）を参照してください。

ステップ 6　更新が完了したら、ASA FirePOWER モジュール インターフェイスにアクセスし、ページを更新します。そうしない場合、インターフェイスが予期しない動作を示すことがあります。メジャーな更新の後、最初にインターフェイスにアクセスしたユーザに対してエンド ユーザ ライセンス契約（EULA）が表示されることがあります。EULA を確認して承認し、処理を続行します。

ステップ 7　サポート サイトの利用可能なルール更新が、ASA FirePOWER モジュールで使用しているルールよりも新しい場合は、新しいルールをインポートします。

詳細については、ルールの更新とローカル ルール ファイルのインポート（43-10 ページ）を参照してください。

ステップ 8　アクセス コントロール ポリシーを再適用します。

アクセス コントロール ポリシーを適用すると、トラフィック フローと処理が一時的に停止することがあります。また、いくつかのパケットが検査されずに通過する可能性があります。詳細については、設定変更の展開（4-12 ページ）を参照してください。

ステップ 9　サポート サイトの利用可能な VDB が、最も新たにインスールした VDB よりも新しい場合は、最新の VDB をインストールします。

VDB の更新をインストールすると、トラフィック フローと処理が一時的に停止することがあります。また、いくつかのパケットが検査されずに通過する可能性があります。詳細については、脆弱性データベースの更新（43-8 ページ）を参照してください。

メジャーな更新のステータスのモニタリング

ライセンス:任意

メジャーな更新では、ASA FirePOWER モジュール は、更新プロセスを簡単にモニタできるように、簡潔なインターフェイスが提供されます。この簡潔なインターフェイスでは、更新のモニタリング以外のタスクを実行するためにASA FirePOWER モジュール を使用することはできません。更新の進行状況のモニタリングは、タスク キュー([モニタリング(Monitoring)] > [ASA FirePOWER モニタリング(ASA FirePOWER Monitoring)] > [タスクのステータス(Task Status)])で開始できます。ただし、ASA FirePOWER モジュール が更新前の必要なチェックを完了すると、ユーザはユーザ インターフェイスからロックアウトされます(簡潔な更新ページが表示されます。

簡潔なインターフェイスには、更新前のバージョン、更新後のバージョン、および更新を開始してからの経過時間が表示されます。また進捗バーが表示され、現在実行中のスクリプトに関する詳細が示されます。

ヒント　更新ログを表示するには、[現在のスクリプトのログを表示する(show log for current script)] をクリックします。ログをもう一度非表示にするには、[現在のスクリプトのログを非表示する(hide log for current script)] をクリックします。

何らかの理由で更新に失敗した場合は、このページにエラー メッセージが表示され、失敗した日時、更新が失敗したときに実行していたスクリプト、およびサポートへの連絡方法が示されます。更新は再開しないでください。

注意　更新で他の問題が生じた場合(ページを手動更新しても長時間にわたって進捗が表示されない場合など)には、更新を再開しないでください。代わりに、サポートに連絡してください。

更新が完了すると、ASA FirePOWER モジュール は正常終了メッセージを表示し、再起動します。ASA FirePOWER モジュール の再起動が完了したら、更新後の必須手順を完了させます。

ソフトウェア アップデートのアンインストール

ライセンス:任意

パッチまたは機能の更新を適用すると、更新プロセスによってアンインストーラが作成されます。これにより、更新を削除することができます。

更新をアンインストールした場合、結果として保持されるシスコ ソフトウェアのバージョンは、更新パスに応じて異なります。たとえば、バージョン 5.0 からバージョン 5.0.0.2 に直接更新した場合について考えてみます。バージョン 5.0.0.2 のパッチをアンインストールすると、バージョン 5.0.0.1 の更新をインストールしていなくても、バージョン 5.0.0.1 が残ります。更新をアンインストールしたときに結果として生成される シスコ ソフトウェアのバージョンの詳細については、リリース ノートを参照してください。

(注)　メジャーな更新では、アンインストールはサポートされていません。新しいメジャー バージョンに更新して、古いバージョンに戻す必要がある場合は、サポートに連絡してください。

トラフィック フローとインスペクション

更新をアンインストールすると、トラフィックのインスペクションとトラフィック フローに影響を及ぼすことがあります。特定の更新に対してネットワーク トラフィックがいつ、どのように影響を受けるかについての情報は、リリース ノートを参照してください。

アンインストール後

更新をアンインストールした後、アンインストールが成功したことを確認します。それぞれの更新に特定の情報については、リリース ノートを参照してください。

パッチまたは機能の更新をアンインストールするには、次の手順を実行します。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [更新（Updates）] の順に選択します。

[製品アップデート（Product Updates）] ページが表示されます。

ステップ 2　削除する更新のアンインストーラの隣にあるインストール アイコンをクリックします。

プロンプトが表示されたら、更新をアンインストールすることを確認してASA FirePOWER モジュール を再起動します。

アンインストール プロセスが開始されます。タスク キュー（[モニタリング（Monitoring）] > [ASA FirePOWER モニタリング（ASA FirePOWER Monitoring）] > [タスクのステータス（Task Status）]）で、進行状況をモニタできます。

注意　アンインストールが完了するまで、タスクを実行するために ASA FirePOWER モジュール インターフェイスを使用しないでください。必要な場合は、ASA FirePOWER モジュール を起動してください。詳細については、更新時の ASA FirePOWER モジュールの使用（43-4 ページ）を参照してください。

ステップ 3　ページを更新します。そうしない場合、インターフェイスが予期しない動作を示すことがあります。

脆弱性データベースの更新

ライセンス：任意

シスコ脆弱性データベース（VDB）は、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。シスコ脆弱性調査チーム（VRT）は、VDB を定期的に更新します。VDB を更新するには、[製品アップデート（Product Updates）] ページを使用します。

（注）　検出の更新とともに VDB アップデートをインストールすると、トラフィック フローと処理が一時的に停止し、いくつかのパケットが検査なしで通過する場合があります。システムのダウンタイムの影響を最小限に抑えるために、システムの使用率が低い時間に合わせて更新をスケジュールすることもできます。

（注）　VDB の更新完了後に、古くなったすべてのアクセス コントロール ポリシーを再適用します。VDB のインストールまたはアクセス コントロール ポリシーの再適用を行うと、トラフィック フローと処理が一時的に停止することがあり、また、いくつかのパケットが検査されずに通過する場合があるので注意してください。詳細については、設定変更の展開（4-12 ページ）を参照してください。

この項では、手動による VDB 更新を計画および実行する方法について説明します。

脆弱性データベースを更新するには、次の手順を実行します。

ステップ 1　更新用の VDB 更新アドバイザリ テキストを読みます。

このアドバイザリ テキストには、更新でが含まれています。

ステップ 2　**[**設定（**Configuration**）**] > [ASA FirePOWER** 設定（**ASA FirePOWER Configuration**）**] > [**更新（**Updates**）**]** の順に選択します。

[製品アップデート（Product Updates）] ページが表示されます。

ステップ 3　更新をアップロードします。

- ASA FirePOWER モジュール がインターネットにアクセスできる場合は、[アップデートのダウンロード（Download Updates）] をクリックして、次のいずれかのサポート サイトで最新の更新を確認します。
  - **Sourcefire**：（https://support.sourcefire.com/）
  - シスコ：（http://www.cisco.com/cisco/web/support/index.html）
- ASA FirePOWER モジュール がインターネットにアクセスできない場合は、次のいずれかのサポート サイトから更新を手動でダウンロードして [アップデートのアップロード（Upload Update）] をクリックします。[ファイルの選択（Choose File）] をクリックして、その更新に移動して選択し、[アップロード（Upload）] をクリックします。
  - **Sourcefire**：（https://support.sourcefire.com/）
  - シスコ：（http://www.cisco.com/cisco/web/support/index.html）

（注）　手動でまたは [アップデートのダウンロード（Download Updates）] をクリックして、サポート サイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、破損する可能性があります。

更新がアップロードされます。

ステップ 4　VDB 更新の隣にあるインストール アイコンをクリックします。

[アップデートをインストール（Install Update）] ページが表示されます。

ステップ 5　[インストール（Install）] をクリックします。

注意　更新プロセスが開始されます。タスク キュー（[モニタリング（Monitoring）] > [ASA FirePOWER モニタリング（ASA FirePOWER Monitoring）] > [タスクのステータス（Task Status）]）で、更新の進行状況をモニタできます。更新で問題が発生した場合（更新に失敗したことがタスク キューに示されている場合など）には、更新を再開しないでください。代わりに、サポートに連絡してください。

VDB の更新を有効にするには、失効したアクセス コントロール ポリシーを再適用する必要があります。設定変更の展開（4-12 ページ）を参照してください。

ルールの更新とローカル ルール ファイルのインポート

ライセンス:任意

新しい脆弱性が判明すると、シスコ脆弱性調査チーム(VRT)からルール更新がリリースされます。ルール更新を実装するには、最初にそれを ASA FirePOWER モジュール にインポートしてから、影響を受けるアクセス コントロール ポリシー、ネットワーク分析ポリシー、侵入ポリシーを適用します。

ルール更新は累積されていくので、シスコでは常に最新の更新をインポートすることを推奨しています。現在インストールされているルールのバージョンに一致するルール更新、またはそれより前のバージョンのルール更新をインポートすることはできません。

(注)　ルール更新には新しいバイナリが含まれていることがあるので、ルール更新をダウンロードしてインストールするプロセスが、各自のセキュリティ ポリシーに合致していることを確認してください。また、ルールの更新は量が多くなることがあるため、ルールのインポートはネットワークの使用量が少ないときに行うようにしてください。

ルールの更新によって以下が提供される場合があります。

- 新規または変更されたルールおよびルール ステータス:ルール更新は、新規および更新された侵入ルールとプリプロセッサ ルールを提供します。新規ルールの場合は、システム付属の各侵入ポリシーでルール ステータスが異なることがあります。たとえば、新規ルールが、Security over Connectivity 侵入ポリシーでは有効になっており、Connectivity over Security 侵入ポリシーでは無効になっていることがあります。ルールの更新では、既存のルールのデフォルトの状態が変更されたり、既存のルールが完全に削除されることもあります。
- 新しいルール カテゴリ:ルール更新には、常に追加される新しいルール カテゴリが含まれている場合があります。
- 変更されたプリプロセッサおよび詳細設定:ルール更新によって、システム付属侵入ポリシーの詳細設定、およびシステム付属ネットワーク分析ポリシーのプリプロセッサ設定が変更されることがあります。また、アクセス コントロール ポリシーの高度な前処理およびパフォーマンスのオプションのデフォルト値も変更される場合があります。
- 新規および変更された変数:ルール更新によって、既存のデフォルト変数のデフォルト値が変更されることがありますが、ユーザによる変更は上書きされません。新しい変数が常に追加されます。

ルールの更新がポリシーを変更するタイミングについて

ルールの更新は、システムが提供するネットワーク分析ポリシーとカスタム ネットワーク分析ポリシーの両方だけでなく、すべてのアクセス コントロール ポリシーにも影響する場合があります。

- システム付属:システム付属のネットワーク分析ポリシーと侵入ポリシーへの変更、およびアクセス コントロールの詳細設定への変更は、更新後にポリシーを再適用すると自動的に有効になります。
- カスタム:すべてのカスタム ネットワーク分析ポリシーと侵入ポリシーは、システム付属ポリシーをそのベースとして、またはポリシー チェーンの根本的ベースとして使用しているので、ルール更新によってカスタム ネットワーク分析ポリシーと侵入ポリシーが影響を受けることがあります。ただし、ルール更新によるこれらの自動的な変更は回避することができます。これにより、ルール更新のインポートとは関係ないスケジュールで、システムによって提供される基本ポリシーを手動で更新できます。ユーザによる選択(カスタム ポリシーごとに実装)とは関係なく、システム付属ポリシーに対する更新によって、カスタマイズ済みの設定が上書きされることはありません。詳細については、ルール更新がシステムによって提供される基本ポリシーを変更することを許可する(16-4 ページ)を参照してください。

ルール更新をインポートすると、ネットワーク分析ポリシーと侵入ポリシーのキャッシュされていた変更がすべて廃棄されるので注意してください。便宜のために、[ルールの更新（Rule Updates）] ページには、ポリシーとキャッシュされている変更が表示されます。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

ポリシーの再適用

ルール更新による変更を反映させるには、変更されたすべてのポリシーを再適用する必要があります。ルール更新をインポートする際には、侵入またはアクセス コントロール ポリシーを自動的に再適用するように、システムを設定できます。これは、ルールの更新によってシステムにより提供される基本ポリシーが変更されることを許可する場合に特に役立ちます。

- アクセス コントロール ポリシーを再適用すると、関連する ネットワーク分析ポリシーとファイル ポリシーも再適用されますが、侵入ポリシーは再適用されません。また、変更された詳細設定のデフォルト値も更新されます。ネットワーク分析ポリシーを単独で適用することはできないため、ネットワーク分析ポリシーでプリプロセッサ設定を更新する場合は、アクセス コントロール ポリシーを再適用する必要があります。
- 侵入ポリシーを再適用すると、ルールおよびその他の変更された侵入ポリシーの設定も更新することができます。侵入ポリシーをアクセス コントロール ポリシーとともに再適用することができます。または、侵入ポリシーのみを適用して、他のアクセス コントロールの設定を更新することなく侵入ルールを更新することができます。

ルールの更新に共有オブジェクトのルールが含まれている場合は、インポート後に初めてアクセス コントロールまたは侵入ポリシーを適用したときに、トラフィック フローと処理が一時的に停止し、いくつかのパケットが検査されずに通過することがあります。要件、他の影響、および推奨事項など、アクセス コントロール ポリシーおよび侵入ポリシーの適用の詳細については、設定変更の展開（4-12 ページ）を参照してください。

ルール更新のインポートの詳細については、以下を参照してください。

- ワンタイム ルール更新の使用（43-11 ページ）では、サポート サイトから 1 つのルール更新をインポートする方法について説明しています。
- 再帰的なルール更新の使用（43-14 ページ）では、自動機能を使用して、サポート サイトからルールの更新をダウンロードしてインストールする方法について説明しています。
- ローカル ルール ファイルのインポート（43-16 ページ）では、ローカル マシンで作成した 標準テキスト ルール ファイルのコピーをインポートする方法について説明しています。
- ルール更新ログの表示（43-17 ページ）では、ルール更新のログについて説明しています。

ワンタイム ルール更新の使用

ライセンス：任意

ワンタイム ルール更新では次の 2 つの方法を使用することができます。

- 手動によるワンタイム ルール更新の使用（43-12 ページ）では、サポート サイトから手動でルール更新をダウンロードし、それを手動でインストールする方法について説明しています。
- 自動ワンタイム ルール更新の使用（43-13 ページ）では、自動機能を使用してサポート サイトで新しいルール更新を検索し、それをアップロードする方法について説明しています。

手動によるワンタイム ルール更新の使用

ライセンス:任意

次の手順では、新しいルール更新を手動でインポートする方法について説明します。この手順は、ASA FirePOWER モジュール がインターネットにアクセスできない場合に特に役立ちます。

手動でルール更新をインポートするには、次の手順を実行します。

ステップ 1　インターネットにアクセスできるコンピュータから、次のサイトのいずれかへアクセスします。

- **Sourcefire**:（https://support.sourcefire.com/）
- シスコ:（http://www.cisco.com/cisco/web/support/index.html）

ステップ 2　[ダウンロード(Download)] をクリックし、[ルール（Rules）] をクリックします。

ステップ 3　最新のルール更新へ移動します。

ルールの更新は累積されます。現在インストールされているルールのバージョンに一致するルール更新、またはそれより前のバージョンのルール更新をインポートすることはできません。

ステップ 4　ダウンロードするルール更新ファイルをクリックし、そのファイルをコンピュータに保存します。

ステップ 5　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [更新（Updates）] の順に選択し、[ルールの更新（Rule Updates）] タブを選択します。の順に選択します。

[ルールのアップデート（Rule Updates）] ページが表示されます。

ヒント　[ルール エディタ（Rule Editor）] ページ（[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] > [ルール エディタ（Rule Editor）]）で [ルールのインポート（**Import Rules**）] をクリックすることもできます。

ステップ 6　必要に応じて、[すべてのローカル ルールを削除（Delete All Local Rules）] をクリックして、[OK] をクリックし、作成またはインポートしたすべてのユーザ定義ルールを削除済みフォルダに移動します。詳細については、カスタム ルールの削除（27-109 ページ）を参照してください。

ステップ 7　[アップロードおよびインストールするルール アップデートまたはテキスト ルール ファイル（Rule Update or text rule file to upload and install）] を選択し、[ファイルの選択（Choose File）] をクリックして、ルール更新ファイルに移動して選択します。

ステップ 8　必要に応じて、更新の完了後にポリシーを再適用します。

- 侵入ポリシーを自動的に再適用するには、[ルール更新のインポート完了後に侵入ポリシーを再適用する（Reapply intrusion policies after the rule update import completes）] を選択します。他のアクセス コントロールの設定を更新せずに、ルールとその他の変更された侵入ポリシーの設定を更新する場合は、このオプションだけを選択します。侵入ポリシーをアクセス コントロール ポリシーとともに再適用するには、このオプションを選択する必要があります。この場合、アクセス コントロール ポリシーを再適用しても、完全な適用は実行されません。
- アクセス コントロール ポリシーとそれに関連するネットワーク分析ポリシーおよびファイル ポリシーを自動的に再適用し、侵入ポリシーを再適用しない場合は、[ルール更新のインポート完了後にアクセス コントロール ポリシーを再適用する（Reapply access control policies after the rule update import completes）] を選択します。このオプションを選択すると、変更されたアクセス コントロールの詳細設定のデフォルト値もすべて更新されます。ネットワーク分析ポリシーを親のアクセス コントロール ポリシーから切り離して適用することはできないため、ネットワーク分析ポリシーでプリプロセッサ設定を更新する場合は、アクセス コントロール ポリシーを再適用する必要があります。

ステップ 9　[インポート（Import）] をクリックします。

ルールの更新がインストールされ、[ルール アップデート ログ（Rule Update Log）] 詳細ビューが表示されます。[ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューについて（43-20 ページ）を参照してください。また、システムは前の手順で指定した通りにポリシーを適用します。設定変更の展開（4-12 ページ）および 侵入ポリシーの適用（23-8 ページ）を参照してください。

（注）　ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

自動ワンタイム ルール更新の使用

ライセンス：任意

次の手順では、サポート サイトに自動的に接続して、新しいルール更新をインポートする方法について説明します。この手順は、ASA FirePOWER モジュール がインターネットにアクセスできる場合のみ使用できます。

自動でルール更新をインポートするには、次の手順を実行します。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [更新（Updates）] の順に選択し、[ルールの更新（Rule Updates）] タブを選択します。の順に選択します。

[ルールのアップデート（Rule Updates）] ページが表示されます。

ヒント　[ルール エディタ（Rule Editor）] ページ（[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] > [ルール エディタ（Rule Editor）]）で **[**ルールのインポート（**Import Rules**）**]** をクリックすることもできます。

ステップ 2　必要に応じて、[すべてのローカル ルールを削除（Delete All Local Rules）] をクリックして、[OK] をクリックし、作成またはインポートしたすべてのユーザ定義ルールを削除済みフォルダに移動します。詳細については、カスタム ルールの削除（27-109 ページ）を参照してください。

ステップ 3　[サポート サイトから新しいルール アップデートをダウンロードする（Download new Rule Update from the Support Site）] を選択します。

ステップ 4　必要に応じて、更新の完了後にポリシーを再適用します。

- 侵入ポリシーを自動的に再適用するには、[ルール更新のインポート完了後に侵入ポリシーを再適用する（Reapply intrusion policies after the rule update import completes）] を選択します。他のアクセス コントロールの設定を更新せずに、ルールとその他の変更された侵入ポリシーの設定を更新する場合は、このオプションだけを選択します。侵入ポリシーをアクセス コントロール ポリシーとともに再適用するには、このオプションを選択する必要があります。この場合、アクセス コントロール ポリシーを再適用しても、完全な適用は実行されません。
- アクセス コントロール ポリシー、ネットワーク分析ポリシー、およびファイル ポリシーを自動的に再適用し、侵入ポリシーを再適用しない場合は、[ルール更新のインポート完了後にアクセス コントロール ポリシーを再適用する（Reapply access control policies after the rule update import completes）] を選択します。このオプションを選択すると、変更されたアクセス コントロールの詳細設定のデフォルト値もすべて更新されます。ネットワーク分析ポリシー

を親のアクセス コントロール ポリシーから切り離して適用することはできないため、ネットワーク分析ポリシーでプリプロセッサ設定を更新する場合は、アクセス コントロール ポリシーを再適用する必要があります。

ステップ 5　[インポート（Import）] をクリックします。

ルールの更新がインストールされ、[ルール アップデート ログ（Rule Update Log）] 詳細ビューが表示されます。[ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューについて（43-20 ページ）を参照してください。また、システムは前の手順で指定した通りにポリシーを適用します。設定変更の展開（4-12 ページ）および侵入ポリシーの適用（23-8 ページ）を参照してください。

（注）　ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

再帰的なルール更新の使用

ライセンス：任意

[ルールのアップデート（Rule Updates）] ページを使用して、ルール更新を日次、週次、または月次ベースでインポートすることができます。

ルール更新のインポートに該当するサブタスクは、ダウンロード、インストール、ベース ポリシーの更新、ポリシーの再適用の順序で実行されます。1 つのサブタスクが完了すると、次のサブタスクが開始されます。適用できるのは、再帰的インポートが設定されている ASA FirePOWER モジュールで以前に適用されたポリシーだけであることに注意してください。

再帰的なルール更新をスケジュールするには、次の手順を実行します。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [更新（Updates）] の順に選択し、[ルールの更新（Rule Updates）] タブを選択します。の順に選択します。

[ルールのアップデート（Rule Updates）] ページが表示されます。

ヒント　[ルール エディタ（Rule Editor）] ページ（[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] > [ルール エディタ（Rule Editor）]）で [ルールのインポート（**Import Rules**）] をクリックすることもできます。

ステップ 2　必要に応じて、[すべてのローカル ルールを削除（Delete All Local Rules）] をクリックして、[OK] をクリックし、作成またはインポートしたすべてのユーザ定義ルールを削除済みフォルダに移動します。詳細については、カスタム ルールの削除（27-109 ページ）を参照してください。

ステップ 3　[ルール アップデートの再帰的なインポートを有効にする（Enable Recurring Rule Update Imports）] を選択します。

ページが展開され、再帰的なインポートを設定するためのオプションが表示されます。[ルール アップデートの再帰的なインポート（Recurring Rule Update Imports）] セクションの見出しの下に、インポート ステータスに関するメッセージが表示されます。設定を保存すると、再帰的なインポートが有効になります。

ヒント　再帰的なインポートを無効にするには、[ルール アップデートの再帰的なインポートを有効にする（Enable Recurring Rule Update Imports）] チェック ボックスをオフにして [保存（Save）] をクリックします。

ステップ 4　[インポート頻度（Import Frequency）] フィールドで、ドロップダウンリストから [日次（Daily）]、[週次（Weekly）]、または [月次（Monthly）] を選択します。

インポート間隔として週次または月次を選択した場合は、表示されるドロップダウン リストで、ルールの更新をインポートする曜日または日付を選択します。選択項目をクリックするか、または選択項目の最初の文字または数字を 1 回以上入力して Enter を押すことで、再帰タスクのドロップダウン リストから選択できます。

ステップ 5　[インポート頻度（Import Frequency）] フィールドで、再帰的なルール更新のインポートを開始するタイミングを指定します。

ステップ 6　必要に応じて、更新の完了後にポリシーを再適用します。

- 侵入ポリシーを自動的に再適用するには、[ルール更新のインポート完了後に侵入ポリシーを再適用する（Reapply intrusion policies after the rule update import completes）] を選択します。他のアクセス コントロールの設定を更新せずに、ルールとその他の変更された侵入ポリシーの設定を更新する場合は、このオプションだけを選択します。侵入ポリシーをアクセス コントロール ポリシーとともに再適用するには、このオプションを選択する必要があります。この場合、アクセス コントロール ポリシーを再適用しても、完全な適用は実行されません。
- アクセス コントロール ポリシーとネットワーク分析ポリシーおよびファイル ポリシーを自動的に再適用し、侵入ポリシーを再適用しない場合は、[ルール更新のインポート完了後にアクセス コントロール ポリシーを再適用する（Reapply access control policies after the rule update import completes）] を選択します。このオプションを選択すると、変更されたアクセス コントロールの詳細設定のデフォルト値もすべて更新されます。ネットワーク分析ポリシーを親のアクセス コントロール ポリシーから切り離して適用することはできないため、ネットワーク分析ポリシーでプリプロセッサ設定を更新する場合は、アクセス コントロール ポリシーを再適用する必要があります。

ステップ 7　[保存（Save）] をクリックし、設定を使用した再帰的なルール更新のインポートを有効にします。

[ルール アップデートの再帰的なインポート（Recurring Rule Update Imports）] セクションの見出しの下のステータス メッセージが変わり、ルールの更新がまだ実行されていないことが示されます。予定時刻になると、前の手順で指定した通りにシステムはルールの更新をインストールし、ポリシーを適用します。設定変更の展開（4-12 ページ） および 侵入ポリシーの適用（23-8 ページ） を参照してください。

インポート前やインポート中は、ログオフすることも、他のタスクを実行することもできます。インポート中に [ルール アップデート ログ（Rule Update Log）] にアクセスすると、赤色のステータス アイコン（  ）が表示され、[ルール アップデート ログ（Rule Update Log）] 詳細ビューに表示されるメッセージを確認できます。ルール更新のサイズと内容によっては、ステータス メッセージが表示されるまでに数分かかることがあります。詳細については、ルール更新ログの表示（43-17 ページ） を参照してください。

（注）　ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

ローカル ルール ファイルのインポート

ライセンス：任意

ローカル ルールは、ASCII または UTF-8 エンコードのプレーン テキスト ファイルとしてローカル マシンからインポートされるカスタムの 標準テキスト ルールです。Snort ユーザ マニュアル（http://www.snort.org で入手可能）の指示に従って、ローカル ルールを作成することができます。

ローカル ルールのインポートについて、次の点に注意してください。

- テキスト ファイル名には英数字とスペースを使用できますが、下線（_）、ピリオド（.）、ダッシュ（-）以外の特殊記号は使用できません。
- ジェネレータ ID（GID）を指定する必要はありません。GID を指定する場合は、標準テキスト ルール に対しては GID 1、機密データ ルールに対しては 138 のみ指定できます。
- 初めてルールをインポートするときには、Snort ID（SID）またはリビジョン番号を指定しないでください。これにより、削除されたルールを含む、他のルールの SID との競合が回避されます。

  システムはルールに対して、1000000 以上の次に使用できるカスタム ルール SID 、およびリビジョン番号 の 1 を自動的に割り当てます。
- 以前にインポートしたローカル ルールの更新バージョンをインポートする場合には、システムによって割り当てられた SID、および現在のリビジョン番号よりも大きいリビジョン番号を含める必要があります。

  現行のローカル ルールのリビジョン番号を表示するには、[ルール エディタ（Rule Editor）] ページを表示し、ローカル ルールのカテゴリをクリックしてフォルダを展開し、ルールの横にある [編集（Edit）] をクリックします。
- システムによって割り当てられた SID と現行のリビジョン番号よりも大きいリビジョン番号を使用してルールをインポートすることで、削除したローカル ルールを元に戻すことができます。ローカル ルールを削除すると、システムは自動的にリビジョン番号を増やすことに注意してください。これは、ローカル ルールを元に戻すための方法です。

  削除したローカル ルールのリビジョン番号を表示するには、[ルール エディタ（Rule Editor）] ページを表示し、削除したルールのカテゴリをクリックしてフォルダを展開し、ルールの横にある [編集（Edit）] をクリックします。
- 2147483647 よりも大きい SID を持つルールが含まれているルール ファイルはインポートできません。この場合、インポートが失敗します。
- 64 文字を超える送信元または宛先のポートのリストが含まれているルールをインポートすると、そのインポートは失敗します。
- インポートしたローカル ルールのステータスは常に無効に設定されます。これらのローカル ルールを侵入ポリシーで使用するには、事前に手動でそのステータスを設定する必要があります。詳細については、ルール状態の設定（24-21 ページ）を参照してください。
- ファイル内のルールに、エスケープ文字が含まれていないことを確認する必要があります。
- ルール インポータでは、すべてのカスタム ルールを ASCII または UTF-8 エンコードでインポートする必要があります。
- インポートされたすべてのローカル ルールは、ローカル ルール カテゴリに自動的に保存されます。
- 削除されたすべてのローカル ルールは、ローカル ルール カテゴリから、削除されたルール カテゴリへ移動されます。
- システムは、単一のシャープ文字（#）で始まるローカル ルールをインポートします。
- また、二重のシャープ文字（##）で始まるローカル ルールは無視し、インポートしません。
- 非推奨の `threshold` キーワードと侵入イベントしきい値機能を組み合わせて使用しているローカル ルールをインポートして、侵入ポリシーで有効にすると、ポリシーの検証に失敗します。詳細については、イベントしきい値の設定（24-23 ページ）を参照してください。

ローカル ルール ファイルをインポートするには、次の手順を実行します。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [更新（Updates）] の順に選択し、[ルールの更新（Rule Updates）] タブを選択します。

[ルールのアップデート（Rule Updates）] ページが表示されます。

ステップ 2　[アップロードおよびインストールするルール アップデートまたはテキスト ルール ファイル（Rule Update or text rule file to upload and install）] を選択し、[ファイルの選択（Choose File）] をクリックして、ルール ファイルに移動します。この方法でアップロードされたすべてのルールは、ローカル ルール カテゴリに保存されることに注意してください。

ヒント　ASCII または UTF-8 エンコーディングによるプレーン テキスト ファイルのみをインポートできます。

ステップ 3　[インポート（Import）] をクリックします。

ルール ファイルがインポートされます。侵入ポリシーで、適切なルールが有効になっていることを確認してください。影響を受けるポリシーが次に適用されるまで、ルールはアクティブにはなりません。

（注）　システムは、ユーザの侵入ポリシーが適用されるまでインスペクションに対して新しいルール セットを使用しません。手順については、設定変更の展開（4-12 ページ）を参照してください。

ルール更新ログの表示

ライセンス：任意

ASA FirePOWER モジュールは、インポートされたルール更新とローカル ルール ファイルごとに 1 つのレコードを生成します。

各レコードにはタイム スタンプ、ファイルをインポートしたユーザの名前、およびインポートが正常に終了したか失敗したかを示すステータス アイコンが含まれています。ユーザは、インポートしたすべてのルール更新とローカル ルール ファイルのリストを管理したり、リストからレコードを削除したり、インポートしたすべてのルールとルール更新コンポーネントに関する詳細レコードにアクセスすることができます。[ルール アップデート ログ（Rule Update Log）] で実行できる操作を次の表で説明します。

表 ***43-2***　　***[ルール アップデート ログ（Rule Update Log）]*** のアクション

目的	操作
テーブルのカラムの内容について詳しく調べる	[ルール アップデート ログ（Rule Update Log）] の表について（43-18 ページ）で詳細を参照してください。
インポート ログからインポート ファイル レコード（ファイルに含まれているすべてのオブジェクトについて削除されたレコードも含めて）を削除する	インポート ファイルでファイル名の隣にある削除アイコン（ ）をクリックします。 （注）　ログからファイルを削除しても、インポート ファイルにインポートされているオブジェクトはいずれも削除されませんが、インポート ログ レコードのみは削除されます。

表 *43-2*　*[ルール アップデート ログ（**Rule Update Log**）]* のアクション（続き）

目的	操作
ルール更新またはローカル ルール ファイルにインポートされている各オブジェクトの詳細を表示する	インポート ファイルでファイル名の隣にある表示アイコン（  ）をクリックします。

詳細については、次の各項を参照してください。

- [ルール アップデート ログ（Rule Update Log）] の表について（43-18 ページ）では、インポートするルール更新およびローカル ルール ファイルのリスト内のフィールドについて説明します。
- [ルール アップデートのインポート ログ（Rule Update Import Log）] の詳細の表示（43-19 ページ）では、ルール更新またはローカル ルール ファイルにインポートされた各オブジェクトの詳細レコードについて説明します。
- [ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューについて（43-20 ページ）では、[ルール アップデート ログ（Rule Update Log）] 詳細ビューの各フィールドについて説明します。

[ルール アップデート ログ（Rule Update Log）] を表示するには、次の手順を実行します。

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [更新（Updates）] の順に選択し、[ルールの更新（Rule Updates）] タブを選択します。の順に選択します。

[ルールのアップデート（Rule Updates）] ページが表示されます。

ヒント　[ルール エディタ（Rule Editor）] ページ（[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] > [ルール エディタ（Rule Editor）]）で **[ルールのインポート（Import Rules）]** をクリックすることもできます。

ステップ **2**　[ルール アップデート ログ（Rule Update Log）] をクリックします。

[ルール アップデート ログ（Rule Update Log）] ページが表示されます。このページには、インポートされた各ルール更新とローカル ルール ファイルが示されています。

[ルール アップデート ログ（Rule Update Log）] の表について

ライセンス：任意

次の表で、ユーザがインポートするルール更新およびローカル ルール ファイルのリストのフィールドについて説明します。

表 *43-3*　*[ルール アップデート ログ（**Rule Update Log**）]* のフィールド

フィールド	説明
要約	インポート ファイルの名前。インポートが失敗した場合は、ファイル名の下に、失敗した理由の簡単な説明が表示されます。
時刻（Time）	インポートが開始された日時。
ユーザ ID（User ID）	インポートをトリガーとして使用したユーザ名。

表 *43-3*　*[ルール アップデート ログ（**Rule Update Log**）]* のフィールド（続き）

フィールド	説明
ステータス（Status）	インポートの状態を表します • 正常終了（） • 失敗、または実行中（） ヒント　インポート中には [ルール アップデート ログ（Rule Update Log）] ページで、正常終了しなかった、または完了していないことを示す赤いステータス アイコンが表示され、インポートが正常終了した場合のみこれが緑色のアイコンに変わります。

ルール更新またはファイル名の隣にある表示アイコン（）をクリックして、ルール更新またはローカル ルール ファイルの [ルール アップデート ログ（Rule Update Log）] 詳細ページを表示するか、または削除アイコン（）をクリックして、ファイル レコード、およびファイルと一緒にインポートされたすべての詳細オブジェクト レコードを削除します。

ヒント　ルール更新のインポートの進行中に示される、インポートの詳細を表示することができます。

[ルール アップデートのインポート ログ（**Rule Update Import Log**）] の詳細の表示

ライセンス：任意

[ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューには、ルール更新またはローカル ルール ファイルにインポートされた各オブジェクトの詳細レコードが表示されます。表示されるレコードのうち、自分のニーズに合う情報のみを含むカスタム ワークフローまたはレポートを作成することもできます。

次の表では、[ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューので実行できる特定のアクションについて説明します。

表 *43-4*　*[ルール アップデートのインポート ログ（**Rule Update Import Log**）]* 詳細ビューのアクション

目的	操作
テーブルのカラムの内容について詳しく調べる	[ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューについて（43-20 ページ） で詳細を参照してください。

[ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューを表示するには、次の手順を実行します。

ステップ **1**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [更新（Updates）] の順に選択し、[ルールの更新（Rule Updates）] タブを選択します。の順に選択します。

[ルールのアップデート（Rule Updates）] ページが表示されます。

ヒント　[ルール エディタ（Rule Editor）] ページ（[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] > [ルール エディタ（Rule Editor）]）で **[ルールのインポート（Import Rules）]** をクリックすることもできます。

ステップ 2　[ルール アップデート ログ（Rule Update Log）] をクリックします。

[ルール アップデート ログ（Rule Update Log）] ページが表示されます。

ステップ 3　表示する詳細レコードが含まれているファイルの隣にある表示アイコン（ ）をクリックします。

詳細レコードのテーブル ビューが表示されます。

[ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューについて

ライセンス：任意

ルール更新またはローカル ルール ファイルにインポートされた各オブジェクトの詳細レコードを表示することができます。以下の表で、[ルール アップデート ログ（Rule Update Log）] 詳細ビューのフィールドについて説明します。

表 *43-5*　*[ルール アップデートのインポート ログ（Rule Update Import Log）]* 詳細ビューのフィールド

フィールド	説明
時刻（Time）	インポートが開始された日時。
[名前（Name）]	インポートされたオブジェクトの名前。ルールの場合はルールの [メッセージ（Message）] フィールドに対応した名前で、ルール更新コンポーネントの場合はコンポーネント名です。
タイプ（Type）	インポートされたオブジェクトのタイプで、有効な値は次のいずれかです。 • [ルール更新コンポーネント（rule update component）]（ルール パックやポリシー パックなどのインポートされたコンポーネント） • [ルール（rule）]（ルール用。新しいルールまたは更新されたルール。バージョン 5.0.1 では、廃止された `update` 値の代わりにこの値が使用されます）。 • [ポリシー適用（policy apply）]（インポートに対して [ルール更新のインポート完了後に侵入ポリシーを再適用する（Reapply intrusion policies after the rule update import completes）] オプションが有効だった場合）
アクション（Action）	オブジェクト タイプについて、次のいずれかが発生していることを示します。 • [新規（new）]（ルール用。この ASA FirePOWER モジュール にルールが初めて格納された場合） • [変更済み（changed）]（ルール更新コンポーネントまたはルール用。ルール更新コンポーネントが変更された場合、またはルールのリビジョン番号が大きく、GID と SID が同じ場合） • [競合（collision）]（ルール更新コンポーネントまたはルール用。既存のコンポーネントまたはルールとリビジョンが競合しているため、インポートがスキップされた場合） • [削除済み（deleted）]（ルール用。ルール更新からルールが削除された場合） • [有効（enabled）]（ルール更新の編集用。プリプロセッサ、ルール、またはその他の機能がシステム付属ポリシーで有効になっている場合） • [無効（disabled）]（ルール用。システム付属ポリシーでルールが無効になっている場合） • [ドロップ（drop）]（ルール用。システム付属ポリシーで、ルールが [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されている場合） • [エラー（error）]（ルール更新またはローカル ルール ファイル用。インポートに失敗した場合） • [適用（apply）]（インポートに対して [ルール更新のインポート完了後に侵入ポリシーを再適用する（Reapply intrusion policies after the Rule Update import completes）] オプションが有効だった場合）

表 *43-5*　*[ルール アップデートのインポート ログ(Rule Update Import Log)]* 詳細ビューのフィールド(続き)

フィールド	説明
デフォルト アクション(Default Action)	ルールの更新によって定義されたデフォルトのアクション。インポートされたオブジェクトのタイプが [ルール(rule)] の場合、デフォルトのアクションは [通過(Pass)]、[アラート(Alert)]、または [ドロップ(Drop)] になります。インポートされた他のすべてのオブジェクト タイプには、デフォルトのアクションはありません。
GID	ルールのジェネレータ ID。例:1(標準テキスト ルール)、3(共有オブジェクトのルール)。
SID	ルールの SID。
Rev	ルールのリビジョン番号。
ポリシー(Policy)	インポートされたルールの場合、このフィールドには [すべて(All)] が表示されます。これは、そのルールがすべてのシステム付属侵入ポリシーに含まれていたことを示しています。インポートされた他のタイプのオブジェクトについては、このフィールドは空白です。
詳細(Details)	コンポーネントまたはルールに対する一意の文字列。ルールの場合、変更されたルールの GID、SID、および旧リビジョン番号は、`previously (GID:SID:Rev)` と表示されます。変更されていないルールについては、このフィールドは空白です。
メンバー数(Count)	各レコードのカウント(1)。テーブルが制限されており、[ルール アップデート ログ(Rule Update Log)] 詳細ビューがデフォルトでルール更新レコードに制限されている場合は、テーブル ビューに [Count] フィールドが表示されます。

位置情報データベースの更新

ライセンス:任意

シスコ位置情報データベース(GeoDB)は、ルート可能な IP アドレスに関連する位置情報データのデータベースです。ASA FirePOWER モジュールでは、国および大陸を使用できます。検出された IP アドレスと一致する GeoDB 情報が検出された場合は、その IP アドレスに関連付けられている位置情報を表示できます。シスコでは、GeoDB の定期的な更新を提供しています。

GeoDB を更新するには、[位置情報の更新(Geolocation Updates)] ページを使用します(**[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [更新(Updates)] > [位置情報の更新(Geolocation Updates)]**)。GeoDB の更新をアップロードすると、それらがこのページに表示されます。

インストールには通常、30 ～ 40 分かかります。GeoDB の更新によって他のシステム機能(進行中の位置情報収集など)が中断されることはありませんが、更新が完了するまでシステム リソースが消費されます。更新を計画する場合には、この点について考慮してください。

この項では、手動による GeoDB の更新を計画および実行する方法について説明します。自動更新機能を利用して GeoDB の更新をスケジュールすることもできます。詳細については、位置情報データベースの更新の自動化(39-6 ページ)を参照してください。

位置情報データベースを更新するには、次の手順を実行します。

ステップ **1**　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [更新(Updates)] の順に選択します。

[製品アップデート(Product Updates)] ページが表示されます。

ステップ **2**　[位置情報の更新(Geolocation Updates)] タブをクリックします。

[位置情報の更新(Geolocation Updates)] ページが表示されます。

ステップ 3　更新をアップロードします。

- ASA FirePOWER モジュール がインターネットにアクセスできる場合は、[位置情報の更新をサポート サイトからダウンロードおよびインストールする（Download and install geolocation update from the Support Site）] をクリックして、以下のサポート サイトのいずれかで最新の更新を確認します。
  - **Sourcefire**：（https://support.sourcefire.com/）
  - シスコ：（http://www.cisco.com/cisco/web/support/index.html）
- ASA FirePOWER モジュール がインターネットにアクセスできない場合は、以下のサポート サイトのいずれかから更新を手動でダウンロードして、[位置情報の更新をアップロードおよびインストールする（Upload and install geolocation update）] をクリックします。[ファイルの選択（Choose File）] をクリックして、その更新に移動して選択し、[インポート（Import）] をクリックします。
  - **Sourcefire**：（https://support.sourcefire.com/）
  - シスコ：（http://www.cisco.com/cisco/web/support/index.html）

（注）　[位置情報の更新（Geolocation Updates）] ページで [位置情報の更新をサポート サイトからダウンロードおよびインストールする（Download and install geolocation update from the Support Site）] をクリックするか、または手動で、サポート サイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、破損する可能性があります。

更新プロセスが開始されます。更新のインストールには、平均で 30 ～ 40 分かかります。タスク キュー（[モニタリング（Monitoring）] > [ASA FirePOWER モニタリング（ASA FirePOWER Monitoring）] > [タスクのステータス（Task Status）]）で、更新の進行状況をモニタできます。

ステップ 4　更新が終了したら [位置情報の更新（Geolocation Updates）] ページに戻り、GeoDB のビルド番号がインストールした更新と一致していることを確認します。

GeoDB を更新すると、GeoDB の以前のバージョンが上書きされ、すぐに有効になります。展開全体で GeoDB の更新が有効になるには数分かかることがありますが、更新後にアクセス コントロール ポリシーを再適用する必要はありません。

システムのモニタリング

ASA FirePOWER モジュール ASA FirePOWER モジュールは、日常のシステム管理をサポートする多くの便利なモニタリング機能を、単一のページ上で提供します。たとえば、[ホスト統計(Host Statistics)] ページでは、基本的なホスト統計情報をモニタできます。次の各項では、システムに備わっているモニタリング機能について詳しく説明します。

- ホスト統計情報の表示(44-1 ページ)では、次のようなホスト情報の表示方法について説明します。
- システム稼働時間
- ディスクおよびメモリの使用状況
- システム プロセス
- 侵入イベント情報
- システム ステータスとディスク領域使用率のモニタ(44-2 ページ)では、基本的なイベントおよびディスク パーティションの情報を表示する方法について説明します。
- システム プロセス ステータスの表示(44-3 ページ)では、基本プロセスのステータスを表示する方法について説明します。
- 実行中のプロセスについて(44-4 ページ)では、アプライアンスで実行する基本システム プロセスについて説明します。

ホスト統計情報の表示

ライセンス:任意

[統計情報(Statistics)] ページには、次の内容の現在のステータスが表示されます。

- 一般的なホスト統計情報。詳細については、ホスト統計情報の表を参照してください
- 侵入イベント情報(Protection が必要)。詳細については、イベントの表示(34-1 ページ)を参照してください

次の表に、[統計情報(Statistics)] ページにリストされるホスト統計情報を示します。

表 **44-1** ホスト統計情報

カテゴリ	説明
時刻(Time)	システムの現在の時刻。
Uptime(アップタイム)	システムが前回起動してから経過した日数(該当する場合)、時間数、および分数。

表 *44-1*　ホスト統計情報（続き）

カテゴリ	説明
メモリ使用率（Memory Usage）	使用中のシステム メモリの割合。
負荷平均（Load Average）	直前の 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数。
ディスク使用量（Disk Usage）	使用中のディスクの割合。詳細なホスト統計情報を表示するには、矢印をクリックします。詳細については、システム ステータスとディスク領域使用率のモニタ（44-2 ページ）を参照してください。
プロセス（Processes）	システムで実行されているプロセスの概要。詳細については、システム プロセス ステータスの表示（44-3 ページ）を参照してください。

[統計情報（**Statistics**）**]** ページを表示するには、次の手順を実行します。

ステップ **1**　[モニタリング（Monitoring）] > [ASA FirePOWER モニタリング（ASA FirePOWER Monitoring）] > [統計情報（Statistics）] の順に選択します。

[統計情報（Statistics）] ページが表示されます。

システム ステータスとディスク領域使用率のモニタ

ライセンス：任意

[統計情報（Statistics）] ページの [ディスク使用量（Disk Usage）] セクションは、カテゴリ別およびパーティション ステータス別に、ディスク使用量のクイック概要を示します。マルウェア ストレージ パックがデバイスにインストールされている場合、そのパーティション ステータスも確認できます。このページを定期的にモニタして、システム プロセスおよびデータベースで十分なディスク領域が使用可能であることを確認できます。

ディスク使用量情報にアクセスするには、次の手順に従います。

ステップ **1**　[モニタリング（Monitoring）] > [ASA FirePOWER モニタリング（ASA FirePOWER Monitoring）] > [統計情報（Statistics）] の順に選択します。

[統計情報（Statistics）] ページが表示されます。

ディスク使用量カテゴリの詳細については、[ディスク使用率（Disk Usage）] ウィジェットについて（37-4 ページ）を参照してください。

ステップ **2**　展開するには、[合計（Total）] の横にある下矢印をクリックします。

[ディスク使用量（Disk Usage）] セクションが展開され、パーティションの使用状況が表示されます。マルウェア ストレージ パックがインストールされている場合は、`/var/storage` パーティションの使用状況も表示されます。

システム プロセス ステータスの表示

ライセンス:任意

[ホスト統計情報(Host Statistics)] ページの [プロセス(Processes)] セクションでは、アプライアンスで現在実行中のプロセスを表示できます。これは、一般的なプロセス情報と、実行中の各プロセスに固有の情報を提供します。

次の表に、プロセス リストに表示される各列を示します。

表 **44-2**　プロセス ステータス

カラム	説明
Pid	プロセス ID 番号
ユーザ名(Username)	プロセスを実行しているユーザまたはグループの名前
Pri	プロセスの優先度
Nice	*nice* 値。プロセスのスケジューリング優先度を示す値です。値は 20(最も高い優先度)から 19(最も低い優先度)までの範囲になります
Size	プロセスで使用されるメモリ サイズ(値の後ろにメガバイトを表す m がない場合はキロバイト単位)
Res	メモリ内の常駐ページング ファイルの量(値の後ろにメガバイトを表す m がない場合はキロバイト単位)
状態(State)	プロセスの状態: • D:プロセスが中断不能スリープ状態(通常は入出力)にある • N:プロセスの nice 値が正の値 • R:プロセスが実行可能である(実行するキュー上で) • S:プロセスがスリープ モードにある • T:プロセスがトレースまたは停止されている • W:プロセスがページングしている • X:プロセスがデッド状態である • Z:プロセスが機能していない • <:プロセスの nice 値が負の値
時刻(Time)	プロセスが実行されてきた時間の長さ(時間数:分数:秒数)
Cpu	プロセスが使用している CPU の割合
コマンド(Command)	プロセスの実行可能ファイル名

プロセス リストを展開するには、次の手順に従います。

ステップ **1**　[モニタリング(Monitoring)] > [ASA FirePOWER モニタリング(ASA FirePOWER Monitoring)] > [統計情報(Statistics)] の順に選択します。

[統計情報(Statistics)] ページが表示されます。

ステップ **2**　[プロセス(Processes)] の横にある下矢印をクリックします。

プロセス リストが展開され、実行中のタスクの数やタイプ、現在の時刻、現在のシステム稼働時間、システムの負荷平均、CPU、メモリ、およびスワップ情報などの、一般的なプロセス ステータス情報と、実行中の各プロセスに関する固有の情報がリストされます。

[CPU（Cpu(s)）] には、以下の CPU 使用状況情報がリストされます。

- ユーザ プロセスの使用状況の割合
- システム プロセスの使用状況の割合
- nice 使用状況の割合（高い優先度を示す、負の nice 値を持つプロセスの CPU 使用状況）

  nice 値は、システム プロセスのスケジュールされた優先度を示しており、20（最も高い優先度）から 19（最も低い優先度）の範囲の値になります。
- アイドル状態の使用状況の割合

[メモリ（Mem）] には、以下のメモリ使用状況情報がリストされます。

- メモリ内の合計キロバイト数
- メモリ内の使用キロバイト数の合計
- メモリ内の空きキロバイト数の合計
- メモリ内のバッファに書き出されたキロバイト数の合計

[スワップ（Swap）] には、以下のスワップ使用状況情報がリストされます。

- スワップ内の合計キロバイト数
- スワップ内の使用キロバイト数の合計
- スワップ内の空きキロバイト数の合計
- スワップ内のキャッシュされたキロバイト数の合計

（注）　アプライアンスで実行されるプロセスのタイプの詳細については、実行中のプロセスについて（44-4 ページ）を参照してください。

プロセス リストを折りたたむには、次の手順に従います。

ステップ 1　[プロセス（Processes）] の横にある上矢印をクリックします。

プロセス リストが折りたたまれます。

実行中のプロセスについて

ライセンス：任意

アプライアンスで実行されるプロセスには、デーモンと実行可能ファイルの 2 種類があります。デーモンは常に実行され、実行可能ファイルは必要に応じて実行されます。

詳細については、次の各項を参照してください。

- システム デーモンについて（44-5 ページ）
- 実行可能ファイルおよびシステム ユーティリティについて（44-6 ページ）

システム デーモンについて

ライセンス:任意

デーモンは、アプライアンスで継続的に実行されます。これにより、サービスが使用可能になり、必要に応じてプロセスが生成されるようになります。次の表では、[プロセスのステータス(Process Status)] ページに表示されるデーモンをリストし、その機能について簡単に説明しています。

(注)　次の表は、アプライアンスで実行される可能性があるすべてのプロセスの包括的なリストではありません。

表 ***44-3***　システム デーモン

デーモン	説明
crond	スケジュールされたコマンド(cron ジョブ)の実行を管理します
dhclient	ダイナミック ホスト IP アドレッシングを管理します
httpd	HTTP(Apache Web サーバ)プロセスを管理します
httpsd	HTTPS(SSL を使用した Apache Web サーバ)サービスを管理し、SSL および有効な証明書の認証が機能しているかチェックし、アプライアンスへの安全な Web アクセスを提供するためにバックグラウンドで実行します
keventd	Linux カーネルのイベント通知メッセージを管理します
klogd	Linux カーネル メッセージのインターセプションおよびロギングを管理します
kswapd	Linux カーネルのスワップ メモリを管理します
kupdated	ディスクの同期を実行する、Linux カーネルの更新プロセスを管理します
mysqld	ASA FirePOWER モジュール データベース プロセスを管理します
ntpd	Network Time Protocol(NTP)プロセスを管理します
pm	すべてのCiscoプロセスを管理し、必要なプロセスを始動し、予期せずに失敗したプロセスをすべて再始動します
reportd	レポートを管理します
safe_mysqld	データベースのセーフ モード運用を管理し、エラーが発生した場合にはデータベース デーモンを再始動し、ランタイム情報をファイルに記録します
sfmgr	アプライアンスへの sftunnel 接続を使用して、リモートでアプライアンスを管理および設定するための RPC サービスを提供します
sftroughd	着信ソケットで接続をリッスンしてから、正しい実行可能ファイル(通常は、Cisco メッセージ ブローカ sfmb)を呼び出して要求を処理します
sftunnel	リモート アプライアンスとの通信を必要とするすべてのプロセスに対し、安全な通信チャネルを提供します。
sshd	セキュア シェル(SSH)プロセスを管理し、アプライアンスへの SSH アクセスを提供するためにバックグラウンドで実行します
syslogd	システム ロギング(syslog)プロセスを管理します

実行可能ファイルおよびシステム ユーティリティについて

ライセンス:任意

システム上には、他のプロセスまたはユーザ操作によって実行される実行可能ファイルが数多く存在します。次の表に、[プロセス ステータス(Process Status)] ページで表示される実行可能ファイルについて説明します。

表 **44-4**　システムの実行可能ファイルおよびユーティリティ

実行可能ファイル	説明
awk	awk プログラミング言語で作成されたプログラムを実行するユーティリティ
bash	GNU Bourne-Again シェル
cat	ファイルを読み取り、コンテンツを標準出力に書き込むユーティリティ
chown	ユーザおよびグループのファイル権限を変更するユーティリティ
chsh	デフォルトのログイン シェルを変更するユーティリティ
cp	ファイルをコピーするユーティリティ
df	アプライアンスの空き領域の量をリストするユーティリティ
echo	コンテンツを標準出力に書き込むユーティリティ
egrep	指定された入力を、ファイルおよびフォルダで検索するユーティリティ。標準 grep でサポートされていない正規表現の拡張セットをサポートします
find	指定された入力のディレクトリを再帰的に検索するユーティリティ
grep	指定された入力をファイルとディレクトリで検索するユーティリティ
halt	サーバを停止するユーティリティ
httpsdctl	セキュアな Apache Web プロセスを処理する
hwclock	ハードウェア クロックへのアクセスを許可するユーティリティ
ifconfig	ネットワーク構成実行可能ファイルを示します。MAC アドレスが常に一定になるようにします
iptables	[アクセス権の設定(Access Configuration)] ページに加えられた変更に基づいてアクセス制限を処理します。アクセス権の設定の詳細については、アプライアンスのアクセス リストの設定(40-4 ページ)を参照してください。
iptables-restore	iptables ファイルの復元を処理します
iptables-save	iptables に対する保存済みの変更を処理します
kill	セッションおよびプロセスを終了するために使用できるユーティリティ
killall	すべてのセッションおよびプロセスを終了するために使用できるユーティリティ
ksh	Korn シェルのパブリック ドメイン バージョン
logger	コマンドラインから syslog デーモンにアクセスする方法を提供するユーティリティ
md5sum	指定したファイルのチェックサムとブロック数を印刷するユーティリティ

表 **44-4**　システムの実行可能ファイルおよびユーティリティ（続き）

実行可能ファイル	説明
mv	ファイルを移動（名前変更）するユーティリティ
myisamchk	データベース テーブルの検査および修復を示します
mysql	データベース プロセスを示します。複数のインスタンスが表示されることがあります
openssl	認証証明書の作成を示します
perl	perl プロセスを示します
ps	標準出力にプロセス情報を書き込むユーティリティ
sed	1 つ以上のテキスト ファイルの編集に使用されるユーティリティ
sh	Korn シェルのパブリック ドメイン バージョン
shutdown	アプライアンスをシャットダウンするユーティリティ
sleep	指定された秒数のあいだプロセスを中断するユーティリティ
smtpclient	電子メール イベント通知機能が有効な場合に、電子メール送信を処理するメール クライアント
snmptrap	SNMP 通知機能が有効な場合に、指定された SNMP トラップ サーバに SNMP トラップ データを転送します
snort（Protection が必要）	Snort が動作していることを示します
ssh	アプライアンスへのセキュア シェル（SSH）接続を示します
sudo	sudo プロセスを示します。これにより、admin 以外のユーザが実行可能ファイルを実行できるようになります
top	上位の CPU プロセスに関する情報を表示するユーティリティ
touch	指定したファイルへのアクセス時刻や変更時刻を変更するために使用できるユーティリティ
vim	テキスト ファイルの編集に使用されるユーティリティ
wc	指定したファイルの行、ワード、バイトのカウントを実行するユーティリティ

バックアップと復元の使用

バックアップと復元は、システム保守プランの重要な部分です。各組織のバックアップ計画は高度に個別化されていますが、ASA FirePOWER モジュール には、障害発生時に データを復元できるようにデータをアーカイブするメカニズムが備わっています。

バックアップと復元に関する次の制限事項に注意してください。

- バックアップは、バックアップを作成する製品バージョンに対してのみ有効です。
- バックアップの作成に使用された ASA FirePOWER モジュール ソフトウェアと同じバージョンを実行している場合にのみ、バックアップを復元できます。

注意 ASA FirePOWER モジュール の間でコンフィギュレーション ファイルをコピーするためにバックアップと復元のプロセスを使用しないでください。コンフィギュレーション ファイルには ASA FirePOWER モジュール を一意的に識別する情報が含まれており、このファイルを共有することはできません。

注意 侵入ルールのアップデートを適用した場合、それらのアップデートはバックアップされません。復元後に、最新のルールのアップデートを適用する必要があります。

アプライアンスまたはローカル コンピュータにバックアップ ファイルを保存できます。

詳細については、次の各項を参照してください。

- バックアップ ファイルの作成については、バックアップ ファイルの作成（45-1 ページ）を参照してください。
- バックアップ作成のテンプレートとして後で使用できるバックアップ プロファイルを作成する方法については、バックアップ プロファイルの作成（45-3 ページ）を参照してください。
- ローカル ホストからバックアップ ファイルをアップロードする方法については、ローカル ホストからのバックアップのアップロード（45-4 ページ）を参照してください。
- アプライアンスにバックアップ ファイルを復元する方法については、バックアップ ファイルからのアプライアンスの復元（45-5 ページ）を参照してください。

バックアップ ファイルの作成

ライセンス：任意

モジュール インターフェイスを使用して、ASA FirePOWER モジュール のバックアップを実行できます。既存のシステム バックアップを表示して使用するには、[バックアップ管理（Backup

Management）] ページに移動します。イベント データに加えて、アプライアンスの復元に必要なすべてのコンフィギュレーション ファイルを含むバックアップ ファイルを定期的に保存する必要があります。設定の変更をテストする際にもシステムをバックアップして、必要に応じて保存されている設定に戻すことができます。バックアップ ファイルを、アプライアンスに保存するか、ローカル コンピュータに保存するかを選択できます。

アプライアンスに十分なディスク スペースがない場合は、バックアップ ファイルを作成できません。バックアップ プロセスの使用スペースが使用可能なディスク スペースの 90% を超えると、バックアップに失敗することがあります。必要に応じて、古いバックアップ ファイルを削除するか、古いバックアップ ファイルをアプライアンスを使用してください。

あるいは、バックアップ ファイルが 4GB を超える場合は、SCP 経由でリモート ホストにコピーします。4 GB

注意　セキュリティ ゾーンとのインターフェイス アソシエーションが設定されている場合、それらのアソシエーションはバックアップされません。それらは、復元後に再設定する必要があります。詳細については、セキュリティ ゾーンの操作（2-37 ページ）を参照してください。

ASA FirePOWER モジュール のバックアップ ファイルを作成するには、次の手順を実行します。

ステップ 1　**[**設定（**Configuration**）**] > [ASA FirePOWER** 設定（**ASA FirePOWER Configuration**）**] > [**ツール（**Tools**）**] > [**バックアップ**/**復元（**Backup/Restore**）**]** の順に選択します。

[バックアップ管理（Backup Management）] ページが表示されます。

ステップ 2　[デバイスのバックアップ（Device Backup）] をクリックします。

[バックアップの作成（Create Backup）] ページが表示されます。

ステップ 3　[名前（Name）] フィールドに、バックアップ ファイルの名前を入力します。英数字、句読記号、およびスペースを使用できます。

ステップ 4　オプションで、バックアップの完了時に通知を受けるためには、[電子メール（Email）] チェックボックスをオンにして、用意されているテキスト ボックスに電子メール アドレスを入力します。

（注）　電子メール通知を受信するには、メール リレー ホストおよび通知アドレスの設定（40-7 ページ）で説明されているように、リレー ホストを設定する必要があります。

ステップ 5　オプションで、セキュアなコピー（SCP）を使用してバックアップ アーカイブを異なるマシンにコピーするには、[完了時にコピー（Copy when complete）] チェック ボックスをオンにしてから、用意されているテキスト ボックスに以下の情報を入力します。

- [ホスト（Host）] フィールドに、バックアップのコピー先となるマシンのホスト名または IP アドレス
- [パス（Path）] フィールドに、バックアップのコピー先となるディレクトリへのパス
- [ユーザ（User）] フィールドに、リモート マシンへのログインに使用するユーザ名
- [パスワード（Password）] フィールドに、そのユーザ名のパスワード
  パスワードの代わりに SSH 公開キーを使用してリモート マシンにアクセスする場合は、そのマシンの指定ユーザの `authorized_keys` ファイルに、[SSH 公開キー（SSH Public Key）] フィールドの内容をコピーします。

このオプションをオフにする場合、バックアップ中に使用された一時ファイルがシステムによってリモート サーバに保存されます。このオプションをオンにする場合は、一時ファイルはリモート サーバに保存されません。

ヒント　シスコ は、システム障害が発生した場合にアプライアンスを復元できるように、バックアップをリモート ロケーションに定期的に保存することを推奨します。

ステップ 6　次の選択肢があります。

- バックアップ ファイルをアプライアンスに保存するには、[バックアップを開始(Start Backup)] をクリックします。

  バックアップ ファイルは `/var/sf/backup` ディレクトリに保存されます。

  バックアップ プロセスが完了すると、[復元データベース(Restoration Database)] ページでファイルを参照できます。バックアップ ファイルを復元する方法については、バックアップ ファイルからのアプライアンスの復元(45-5 ページ)を参照してください。
- この設定を後で使用できるバックアップ プロファイルとして保存するには、[新規保存(Save As New)] をクリックします。

  [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ツール(Tools)] > [バックアップ/復元(Backup/Restore)] を選択し、次に [バックアップ プロファイル(Backup Profiles)] をクリックすることにより、バックアップ プロファイルを変更または削除できます。詳細については、バックアップ プロファイルの作成(45-3 ページ)を参照してください。

バックアップ プロファイルの作成

ライセンス:任意

[バックアップ プロファイル(Backup Profiles)] ページを使用して、さまざまな種類のバックアップに使用する設定値を含むバックアップ プロファイルを作成できます。後にアプライアンスのファイルをバックアップするときに、これらのプロファイルの 1 つを選択できます。

ヒント　バックアップ ファイルの作成(45-1 ページ)で説明されているようにバックアップ ファイルを作成すると、バックアップ プロファイルが自動的に作成されます。

バックアップ プロファイルを作成するには、次の手順を実行します。

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ツール(Tools)] > [バックアップ/復元(Backup/Restore)] の順に選択します。

[バックアップ管理(Backup Management)] ページが表示されます。

ステップ 2　[バックアップ プロファイル(Backup Profiles)] タブをクリックします。

[バックアップ プロファイル(Backup Profiles)] ページが表示されて、既存のバックアップ プロファイルのリストが示されます。

ヒント　編集アイコン( )をクリックして既存のプロファイルを変更するか、または削除アイコン( )をクリックしてリストからプロファイルを削除することができます。

ステップ 3　[プロファイルを作成（Create Profile）] をクリックします。

[バックアップの作成（Create Backup）] ページが表示されます。

ステップ 4　バックアップ プロファイルの名前を入力します。英数字、句読記号、およびスペースを使用できます。

ステップ 5　バックアップ プロファイルを必要に合わせて設定します。

このページのオプションについては、バックアップ ファイルの作成（45-1 ページ）を参照してください。

ステップ 6　バックアップ プロファイルを保存するには、[新規保存（Save As New）] をクリックします。

[バックアップ プロファイル（Backup Profiles）] ページが表示されて、新しいプロファイルがリストに示されます。

ローカル ホストからのバックアップのアップロード

ライセンス：任意

バックアップ管理（Backup Management）の表で説明されているダウンロード機能を使用してローカル ホストにバックアップ ファイルをダウンロードした場合、それを ASA FirePOWER モジュール にアップロードできます。

バックアップ ファイルに PKI オブジェクトが含まれている場合、内部 CA と内部証明書オブジェクトに関連付けられた秘密キーは、アップロードの際にランダムに生成されるキーによって再暗号化されます。

ヒント　4 GB よりも大きなサイズのバックアップをローカル コンピュータからアップロードすることはできません。代わりに、バックアップを SCP 経由でリモート ホストにコピーし、そこから取得することができます。

ローカル ホストからバックアップをアップロードするには、次の手順を実行します。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] の順に選択します。

[バックアップ管理（Backup Management）] ページが表示されます。

ステップ 2　[バックアップのアップロード（Upload Backup）] をクリックします。

[バックアップのアップロード（Upload Backup）] ページが表示されます。

ステップ 3　[ファイルの選択（Choose File）] をクリックして、アップロードするバックアップ ファイルに移動します。

アップロードするファイルを選択した後に、[バックアップのアップロード（Upload Backup）] をクリックします。

ステップ 4　[バックアップ管理（Backup Management）] をクリックして、[バックアップ管理（Backup Management）] ページに戻ります。

バックアップ ファイルがアップロードされ、バックアップ リストに表示されます。ASA FirePOWER モジュール によってファイルの整合性が検証された後に、[バックアップ管理（Backup Management）] ページを更新して、詳細なファイル システム情報を確認します。

バックアップ ファイルからのアプライアンスの復元

ライセンス:任意

[バックアップ管理(Backup Management)] ページを使用して、バックアップ ファイルからアプライアンスを復元できます。バックアップを復元するには、バックアップ ファイル内の VDB のバージョンが、アプライアンスの現在の VDB のバージョンと一致している必要があります。復元プロセスが完了した後、最新の シスコ ルール アップデートを適用する必要があります。

ローカル ストレージを使用する場合、バックアップ ファイルは `/var/sf/backup` に保存され、`/var` パーティションで使用されるディスク容量と共に [バックアップ管理(Backup Management)] ページの下部に一覧表示されます。

(注)　バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを(それらが使用されている場所をメモした上で)削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。

次の表では、[バックアップ管理(Backup Management)] ページの各列とアイコンについて説明します。

表 ***45-1***　　バックアップ管理(***Backup Management***)

機能	説明
システム情報(System Information)	元のアプライアンスの名前、タイプ、バージョン。バックアップを復元できるのは、同一のアプライアンス タイプとバージョンに対してだけであることに注意してください。
作成日	バックアップ ファイルが作成された日時
ファイル名(File Name)	バックアップ ファイルのフルネーム
VDB バージョン(VDB Version)	バックアップ時にアプライアンスで実行されている脆弱性データベース(VDB)のビルド。
参照先	バックアップ ファイルの場所
サイズ(MB)(Size (MB))	バックアップ ファイルのサイズ(メガバイト)
表示(View)	バックアップ ファイルの名前をクリックすると、圧縮されたバックアップ ファイルに含まれるファイルのリストが表示されます。
復元(Restore)	バックアップ ファイルを選択した状態でクリックすると、そのバックアップ ファイルがアプライアンスに復元されます。VDB バージョンがバックアップ ファイルの VDB のバージョンと一致しない場合、このオプションは無効になります。
ダウンロード(Download)	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルがローカル コンピュータに保存されます。
削除(Delete)	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルが削除されます。
移動(Move)	作成済みのローカル バックアップを選択した状態でクリックすると、そのバックアップが指定したリモート バックアップ ロケーションに送信されます。

バックアップ ファイルからのアプライアンスを復元するには、次の手順を実行します。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] の順に選択します。

[バックアップ管理（Backup Management）] ページが表示されます。

ステップ 2　バック アップ ファイルの内容を確認するには、ファイルの名前をクリックします。

マニフェストが表示され、各ファイルの名前、所有者と権限、およびファイル サイズと日付がリストされます。

ステップ 3　[バックアップ管理（Backup Management）] をクリックして、[バックアップ管理（Backup Management）] ページに戻ります。

ステップ 4　復元するバックアップ ファイルを選択して、[復元（Restore）] をクリックします。

[バックアップの復元（Restore Backup）] ページが表示されます。

バックアップの VDB バージョンがアプライアンスに現在インストールされている VDB のバージョンと一致しない場合、[復元（Restore）] ボタンはグレー表示されることに注意してください。

注意　この手順により、すべてのコンフィギュレーション ファイルおよびすべてのイベント データが上書きされます。

ステップ 5　ファイルを復元するには、次のいずれかまたは両方を選択します。

- **Replace Configuration Data**
- **Restore Event Data**

ステップ 6　[復元（Restore）] をクリックして、復元を開始します。

アプライアンスが、指定したバックアップ ファイルを使用して復元されます。

ステップ 7　アプライアンスを再起動します。

ステップ 8　最新の シスコ ルール アップデートを適用して、ルールのアップデートを再適用します。

ステップ 9　復元されたシステムにアクセス コントロール ポリシー、侵入ポリシー、およびシステム ポリシーを再適用します。

トラブルシューティング ファイルの生成

アプライアンスで問題が発生したときに、問題の診断に役立つように、サポートからトラブルシューティング ファイルを生成するように依頼されることがあります。次の表に示すオプションのいずれかを選択して、ASA FirePOWER モジュールから報告されるトラブルシューティング データをカスタマイズすることができます。

表 ***A-1*** 選択可能なトラブルシュート オプション

オプション	報告内容
Snort のパフォーマンスと設定（Snort Performance and Configuration）	アプライアンス上の Snort に関連するデータと構成設定
ハードウェア パフォーマンスとログ（Hardware Performance and Logs）	アプライアンス ハードウェアのパフォーマンスに関連するデータとログ
システムの設定、ポリシー、ログ（System Configuration, Policy, and Logs）	アプライアンスの現在のシステム設定に関連する構成設定、データ、およびログ
検知機能の構成、ポリシー、ログ（Detection Configuration, Policy, and Logs）	アプライアンス上の検知機能に関連する構成設定、データ、およびログ
インターフェイスとネットワーク関連データ（Interface and Network Related Data）	アプライアンスのインライン セットとネットワーク設定に関連する構成設定、データ、およびログ
検知、認識、VDB データ、およびログ（Discovery, Awareness, VDB Data, and Logs）	アプライアンス上の現在の検出設定と認識設定に関連する構成設定、データ、およびログ
データおよびログのアップグレード（Upgrade Data and Logs）	アプライアンスの以前のアップグレードに関連するデータおよびログ
全データベースのデータ（All Database Data）	トラブルシュート レポートに含まれるすべてのデータベース関連データ
全ログのデータ（All Log Data）	アプライアンス データベースによって収集されたすべてのログ
ネットワーク マップ情報（Network Map Information）	現在のネットワーク トポロジ データ

一部のオプションは報告対象のデータの点で重複していますが、トラブルシューティング ファイルには、オプションの選択に関係なく冗長コピーは含まれません。

詳細については、次の項を参照してください。

- アプライアンス トラブルシューティング ファイルの生成（A-2 ページ）
- トラブルシューティング ファイルのダウンロード（A-2 ページ）

アプライアンス トラブルシューティング ファイルの生成

ライセンス:任意

次の手順を使用して、サポートに送信できる、カスタマイズされたトラブルシューティング ファイルを生成できます。

トラブルシューティング ファイルを生成するには、次の手順を実行します。

ステップ 1　ASDM で、[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ツール(Tools)] > [トラブルシューティング(Troubleshooting)] の順に選択します。

ステップ 2　[トラブルシューティング ファイルの生成(Generate Troubleshooting Files)] をクリックします。

[トラブルシューティング オプション(Troubleshooting Options)] ポップアップ ウィンドウが表示されます。

ステップ 3　[全データ(All Data)] を選択して入手可能なすべてのトラブルシューティング データを生成することも、個別のチェック ボックスをオンにしてレポートをカスタマイズすることもできます。詳細については、選択可能なトラブルシュート オプションの表を参照してください。

ステップ 4　[OK] をクリックします。

ASA FirePOWER モジュールがトラブルシューティング ファイルを生成します。タスク キュー([モニタリング(Monitoring)] > [ASA FirePOWER モニタリング(ASA FirePOWER Monitoring)] > [タスクのステータス(Task Status)])でファイル生成プロセスをモニタできます。

ステップ 5　次の項(トラブルシューティング ファイルのダウンロード)の手順に進みます。

トラブルシューティング ファイルのダウンロード

ライセンス:任意

次の手順を使用して、生成されたトラブルシューティング ファイルのコピーをダウンロードします。

トラブルシューティング ファイルをダウンロードする方法には、次の手順を実行します。

ステップ 1　ASDM で、[モニタリング(Monitoring)] > [ASA FirePOWER モニタリング(ASA FirePOWER Monitoring)] > [タスクのステータス(Task Status)] の順に選択します。

[タスク ステータス(Task Status)] ページが表示されます。

ステップ 2　生成されたトラブルシューティング ファイルに対応するタスクを探します。

ステップ 3　アプライアンスがトラブルシューティング ファイルを生成し、タスク ステータスが [完了(Completed)] に変ったら、[クリックして生成されたファイルを取得(Click to retrieve generated files)] をクリックします。

ステップ 4　ブラウザのプロンプトに従ってファイルをダウンロードします。

ファイルは単一の `.tar.gz` ファイルとしてダウンロードされます。

ステップ 5　サポートの指示に従って、トラブルシューティング ファイルをシスコに送信してください。

設定のインポートおよびエクスポート

インポート/エクスポート機能を使用して、ポリシーを含む複数のタイプの設定を、1 つのアプライアンスから同じタイプの別のアプライアンスにコピーにできます。設定のインポートやエクスポートはバックアップ ツールとして設計されてはいませんが、ASA FirePOWER モジュールに新しい追加するプロセスを簡易化するために使用できます。

以下の設定をインポートおよびエクスポートできます。

- アクセス コントロール ポリシーおよび関連するネットワーク分析およびファイル ポリシー
- 侵入ポリシー
- システム ポリシー
- アラート応答

エクスポートされた設定をインポートするには、両方の ASA FirePOWER モジュールで同じソフトウェア バージョンが稼動していなければなりません。エクスポートされた侵入ポリシーまたはアクセス コントロール ポリシーをインポートするには、両方のアプライアンスでルール更新のバージョンも一致している必要があります。

詳細については、次の項を参照してください。

- 設定のエクスポート（B-1 ページ）
- 設定のインポート（B-3 ページ）

設定のエクスポート

ライセンス：任意

単一の設定をエクスポートすることや、（同じタイプまたは異なるタイプの）一連の設定を同時にエクスポートすることができます。後に別のアプライアンスにパッケージをインポートするとき、パッケージ内のどの設定をインポートするかを選択できます。

設定をエクスポートするとき、アプライアンスは、その設定のリビジョン情報もエクスポートします。ASA FirePOWER モジュールはその情報を使用して、別のアプライアンスにその設定をインポートできるかどうかを判別します。アプライアンスにすでに存在する設定リビジョンをインポートすることはできません。

また、設定をエクスポートするとき、その設定が依存するシステム設定も、アプライアンスによってエクスポートされます。

ヒント

ASA FirePOWER モジュール の多くのリスト ページには、リスト項目の横にエクスポート アイコン（）があります。このアイコンがある場合は、それを使用することにより、その後のエクスポート操作を簡単に代行させることができます。

以下の設定をエクスポートできます。

- アラート応答:アラート応答は、アラートの送信先とする予定の外部システムと ASA FirePOWER モジュールが対話できるようにするための一連の設定です。
- アクセス コントロール ポリシー:アクセス コントロール ポリシーには、システムがネットワーク トラフィックをどのように管理するかを指定するために設定できる、さまざまなコンポーネントが含まれます。これらのコンポーネントには、アクセス コントロール ルール、関連する侵入ポリシー、ファイル ポリシー、およびネットワーク分析ポリシー、および侵入の変数セットを含むルールとポリシーが使用するオブジェクトが含まれています。アクセス コントロール ポリシーをエクスポートすると、そのポリシーのすべての設定とコンポーネントもエクスポートされます。ただし、複数のアプライアンスで同等であり、ユーザが変更できない URL レピュテーションとカテゴリは(それらが存在しても)エクスポートされません。アクセス コントロール ポリシーをインポートするには、エクスポート元とインポート先の ASA FirePOWER モジュールでルール更新のバージョンが一致している必要があります。

  エクスポートするアクセス コントロール ポリシーには、位置情報データを参照するルールが含まれている場合、インポート先のモジュールの位置情報データベース(GeoDB)の更新バージョンが使用されます。
- 侵入ポリシー:侵入ポリシーには、ネットワーク トラフィックを検査して侵入やポリシー違反を見つけるように設定できる、さまざまなコンポーネントが組み込まれています。これらのコンポーネントは、プロトコル ヘッダー値、ペイロード コンテンツ、および特定のパケット サイズの特性および他の詳細設定を検査する侵入ルールです。

  侵入ポリシーをエクスポートすると、そのポリシーのすべての設定もエクスポートされます。たとえば、イベントを生成するルールを設定するように選択した場合、ルールの SNMP アラートを設定した場合、またはポリシーでセンシティブ データ プリプロセッサをオンにした場合は、エクスポートされるポリシー内にそれらの設定値が保持されます。カスタム ルール、カスタム ルールの分類、およびユーザ定義変数も、ポリシーとともにエクスポートされます。

  レイヤを使用する侵入ポリシーをエクスポートする場合、そのレイヤが 2 番目の侵入ポリシーによって共有されているときは、エクスポートするポリシーにその共有レイヤがコピーされて、共有関係はなくなることに注意してください。侵入ポリシーを別のアプライアンスにインポートするときは、インポートするポリシーをニーズに合うように編集できます。レイヤの削除、追加、共有などができます。

  1 つの ASA FirePOWER モジュールから別の Defense Center に侵入ポリシーをエクスポートする場合、2 つ目の ASA FirePOWER モジュールでデフォルト変数が別の設定になっている場合は、インポートされたポリシーの動作が異なる可能性があります。

  (注)　インポート/エクスポート機能を使用して、脆弱性調査チーム(VRT)が作成したルールを更新することはできません。代わりに、最新バージョンのルール更新をダウンロードして適用します。ルールの更新とローカル ルール ファイルのインポート (43-10 ページ)を参照してください。

- システム ポリシー:システム ポリシーは、時間設定、SNMP 設定など、展開内の他の ASA FirePOWER モジュールに類似する可能性のあるASA FirePOWER モジュールの側面を制御します。

(注)　エクスポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、エクスポート プロセスに数分かかる場合があります。

1 つ以上の設定をエクスポートする方法:

ステップ **1**　設定のエクスポート元の ASA FirePOWER モジュールと設定のインポート先の ASA FirePOWER モジュールで、同じバージョンが稼働していることを確認します。侵入ポリシーまたはアクセス コントロール ポリシーをエクスポートする場合は、ルール更新のバージョンが一致することを確認します。

ASA FirePOWER モジュールのバージョン（および該当する場合はルール更新のバージョン）が一致しない場合、インポートは失敗します。

ステップ **2**　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ツール（Tools）] > [インポート エクスポート（Import Export）] の順に選択します。

[インポート/エクスポート（Import/Export）] ページが表示され、ASA FirePOWER モジュール上の設定のリストが示されます。エクスポートする設定がない設定カテゴリは、このリストに表示されないことに注意してください。

ヒント　設定のリストは、設定タイプの横にある折りたたみアイコン（）をクリックして折りたたむことができます。設定を確認するには、設定タイプの横にあるフォルダ展開アイコン（）をクリックします。

ステップ **3**　エクスポートする設定の横にあるチェック ボックスを選択して、[エクスポート（Export）] をクリックします。

ステップ **4**　プロンプトに従って、エクスポートされたパッケージをコンピュータに保存します。

設定のインポート

ライセンス:任意

アプライアンスから設定をエクスポートした後に、その設定が別のアプライアンスでもサポートされていれば、そのアプライアンスにインポートできます。

インポートしている設定のタイプに応じて、以下の点に注意する必要があります。

- 設定をインポートする ASA FirePOWER モジュールが、設定のエクスポートに使用した ASA FirePOWER モジュールと同じバージョンで実行していることを確認します。侵入ポリシーまたはアクセス コントロール ポリシーをインポートする場合は、両方のアプライアンスでルール更新のバージョンも一致している必要があります。バージョンが一致しない場合、インポートは失敗します。
- ゾーンに基づいてトラフィックを評価するアクセス コントロール ポリシーをインポートする場合は、インポートされたポリシー内のゾーンを、インポート先の ASA FirePOWER モジュールのゾーンにマッピングする必要があります。ゾーンをマッピングするときは、それらのタイプが一致している必要があります。したがって、インポートを開始する前に、インポート先の ASA FirePOWER モジュールで必要となるゾーン タイプを作成する必要があります。セキュリティ ゾーンの詳細については、セキュリティ ゾーンの操作（2-37 ページ）を参照してください。
- 既存のオブジェクトやグループと同一の名前を持つオブジェクトやオブジェクト グループを含むアクセス コントロール ポリシーをインポートする場合は、オブジェクトやグループの名前を変更する必要があります。

- アクセス コントロール ポリシーや侵入ポリシーをインポートする場合、インポート プロセスによって、デフォルト変数セットに含まれる既存のデフォルト変数が、インポートされたデフォルト変数に置換されます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。
- 侵入ポリシーをインポートするとき、その侵入ポリシーが 2 番目の侵入ポリシーの共有レイヤを使用していた場合は、エクスポート プロセスによって共有関係が切断されて、それまで共有されていたレイヤがパッケージにコピーされます。つまり、インポートされた侵入ポリシーに共有レイヤは含まれません。

（注）　インポート/エクスポート機能を使用して、脆弱性調査チーム（VRT）が作成したルールを更新することはできません。代わりに、最新バージョンのルール更新をダウンロードして適用します。ルールの更新とローカル ルール ファイルのインポート（43-10 ページ）を参照してください。

ASA FirePOWER モジュール1 つのパッケージで複数の設定をエクスポートできるため、パッケージのインポート時に、パッケージ内のどの設定をインポートするかを選択する必要があります。

設定をインポートしようとすると、ASA FirePOWER モジュールは、その設定がアプライアンスにすでに存在しているかどうかを判別します。競合がある場合は、以下の操作が可能です。

- 既存の設定を維持する、
- 既存の設定を新しい設定に置き換える、
- 最新の設定を維持する、または
- 設定を新しい設定としてインポートする。

設定をインポートした後に、宛先システムで設定を変更してその設定を再インポートすると、保持する設定のバージョンを選択する必要があります。

インポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、インポート プロセスに数分かかる場合があります。

1 つ以上の設定をインポートする方法:

ステップ **1**　設定のエクスポート元の ASA FirePOWER モジュールと設定のインポート先のモジュールで、同じバージョンが稼働していることを確認します。侵入ポリシーまたはアクセス コントロール ポリシーをインポートする場合は、ルール更新のバージョンが一致することも確認する必要があります。

ASA FirePOWER モジュールのバージョン（および該当する場合はルール更新のバージョン）が一致しない場合、インポートは失敗します。

ステップ **2**　インポートする設定をエクスポートします。設定のエクスポート（B-1 ページ）を参照してください。

ステップ **3**　設定をインポートするアプライアンスで、[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ツール（Tools）] > [インポート エクスポート（Import Export）] を選択します。

[インポート エクスポート（Import Export）] ページが表示されます。

ヒント　設定のリストを折りたたむには、設定タイプの横にある折りたたみアイコン（）をクリックします。設定を確認するには、設定タイプの横にあるフォルダ展開アイコン（）をクリックします。

ステップ 4　[パッケージのアップロード(Upload Package)] をクリックします。

[パッケージのアップロード(Upload Package)] ページが表示されます。

ステップ 5　次の 2 つの対処法があります。

- アップロードするパッケージへのパスを入力します。
- [ファイルのアップロード(Upload File)] をクリックしてパッケージを見つけます。

ステップ 6　[アップロード(Upload)] をクリックします。

アップロードの結果は、パッケージの内容によって異なります。

- パッケージ内の設定が、アプライアンスにすでに存在するバージョンと正確に一致する場合、そのバージョンが存在することを示すメッセージが表示されます。アプライアンスに最新の設定が存在するので、それらをインポートする必要はありません。
- 使用するアプライアンスとパッケージのエクスポート元のアプライアンスとの間に、ASA FirePOWER モジュールまたは(該当する場合)ルール更新のバージョンの不一致がある場合、パッケージをインポートできないことを示すメッセージが表示されます。ASA FirePOWER モジュールまたはルール更新のバージョンを更新して、プロセスを再試行します。
- アプライアンスに存在しない設定やルールのバージョンがパッケージに含まれている場合、[パッケージのインポート(Package Import)] ページが表示されます。次の手順に進みます。

ステップ 7　インポートする設定を選択して、[インポート(Import)] をクリックします。

インポート プロセスが解決されて、以下のような結果になります。

- ASA FirePOWER モジュールに、インポートする設定の以前のリビジョンが存在しない場合、インポートは自動的に完了し、成功メッセージが表示されます。残りの手順は省略します。
- セキュリティ ゾーンを含むアクセス コントロール ポリシーをインポートする場合、[アクセス コントロール インポートの解決(Access Control Import Resolution)] ページが表示されます。ステップ 8 に進みます。
- インポートする設定に対してアプライアンスに以前のリビジョンが存在する場合、[インポートの解決(Import Resolution)] ページが表示されます。ステップ 9 に進みます。

ステップ 8　取り込まれる各セキュリティ ゾーンの横で、同じタイプの既存のローカル セキュリティ ゾーンをマップ先として選択し、[インポート(Import)] をクリックします。

ステップ 7 に戻ります。

ステップ 9　各設定を展開して、以下の該当するオプションを選択します。

- アプライアンスの設定を保持するには、[既存の保持(Keep existing)] を選択します。
- アプライアンスの設定をインポートした設定に置き換えるには、[既存の置換(Replace existing)] を選択します。
- 最新の設定を保持するには、[最新の保持(Keep newest)] を選択します。
- インポートした設定を新しい設定として保存するには、[新規としてインポート(Import as new)] を選択し、オプションとして設定名を編集します。

  クリーン リストまたはカスタム検出リストが有効になっているファイル ポリシーを含むアクセス コントロール ポリシーをインポートする場合、[新規としてインポート(Import as new)] オプションは使用できません。
- 従属オブジェクトを含むアクセス コントロール ポリシーや保存済み検索をインポートする場合、提案された名前を受け入れるか、またはオブジェクトの名前を変更します。システムは常にこれらの従属オブジェクトを新規としてインポートします。既存のオブジェクトを保存したり置き換えたりするオプションはありません。システムではオブジェクトもオブジェクト グループも同様に処理されることに注意してください。

ステップ 10 [インポート(Import)] をクリックします。

設定がインポートされます。

実行時間が長いタスクのステータスの表示

ASA FirePOWER モジュール で実行できるタスクの中には、ポリシーの適用やアップデートのインストールなど、すぐには完了せず実行に時間がかかるものがあります。このように実行時間が長いタスクの進捗状況を、タスク キューで確認できます。また、これらのタスクが正常に終了したり、異常終了したりした場合にも、タスク キューで報告されます。

詳細については、次の項を参照してください。

- タスク キューの表示（C-1 ページ）
- タスク キューの管理（C-2 ページ）

タスク キューの表示

ライセンス：任意

ポリシーの適用やアップデートのインストールなど、実行時間が長いタスクを実行すると、これらのタスクのステータスがタスク キューで報告されます。タスク キューは複雑なタスクに関する情報を示し、そのようなタスクが完了したときに報告します。

[タスク ステータス（Task Status）] ページでタスク キューを表示します。これは 10 秒ごとに自動的に更新されます。

[ジョブ サマリ（Job Summary）] セクションには、次の表に記載するように、ページに示されているタスクの状態が表示されます。

表 ***C-1*** タスク キューのタスク タイプ

タスク タイプ	説明
実行中（Running）	現在進行中のタスクの数。
待機中（Waiting）	進行中のタスクが完了するまで待機している、実行前のタスクの数。
完了	正常に完了したタスクの数。
再試行中（Retrying）	自動的に再試行されるタスクの数。なお、すべてのタスクの再試行が許可されるわけではありません。
停止（Stopped）	システムの更新のために中断されたタスクの数。停止したタスクは再開できません。タスク キューから手動で削除する必要があります。
失敗しました（Failed）	正常に終了しなかったタスクの数。

[ジョブ(Jobs)] セクションには、各タスクの情報(簡単な説明、タスクがいつ起動されたか、タスクの現在のステータス、ステータスが最後に変更されたのはいつかなど)が示されます。同じタイプの複数のタスクは 1 つのタスク グループにまとめて表示されます。

[タスクのステータス(Task Status)] ページがすばやくロードされるように、ASA FirePOWER モジュール では、1 カ月より前に完了/失敗/停止したすべてのタスクが 1 週間に一度キューから削除されます。さらに、1000 個を超えるタスクを含んでいるタスク グループ内の古いタスクも同じ頻度で削除されます。なお、手動でキューからタスクを削除することもできます(タスク キューの管理 の説明を参照してください)。

タスク キューを表示するには、次の手順を実行します。

ステップ 1　次の 2 つの対処法があります。

- 手動でタスクを起動した場合は、タスク起動時に表示された通知ボックスの [タスク ステータス(Task Status)] リンクをクリックします。

  ポップアップ ウィンドウに [タスクのステータス(Task Status)] ページが表示されます。

- タスクをスケジュールした場合、または表示されていないページからタスクが起動された場合は、**[モニタリング(Monitoring)] > [ASA FirePOWER モニタリング(ASA FirePOWER Monitoring)] > [タスクのステータス(Task Status)]** を選択します。

  [タスク ステータス(Task Status)] ページが表示されます。

[タスク ステータス(Task Status)] ページで実行できる操作については、タスク キューの管理を参照してください。

タスク キューの管理

ライセンス:任意

ユーザ ロールが割り当てられている場合は、次の表に示すように、タスク キューを表示(タスク キューの表示(C-1 ページ)を参照)しているときにいくつかの操作を実行できます。

表 C-2　タスク キューの操作

目的	操作
完了したすべてのタスクをタスク キューから削除する	[完了したジョブを削除する(Remove Completed Jobs)] をクリックします。
失敗したすべてのタスクをタスク キューから削除する	[失敗したジョブを削除する(Remove Failed Jobs)] をクリックします。
タスク キューから 1 つのタスクを削除する	削除するタスクの横にある削除アイコン( )をクリックします。 実行中のタスクは削除できないので注意してください。実行中のタスクを削除する必要がある場合(例えばタスクが何度も失敗する場合)は、サポート担当にお問い合わせください。
タスク グループを縮小し、タスクを非表示にする	展開されたタスク グループの横にあるオープン フォルダ アイコン( )をクリックします。
タスク グループを展開し、タスクを表示する	縮小されたタスク グループの横にあるクローズド フォルダ アイコン( )をクリックします。

セキュリティ、インターネット アクセス、および通信ポート

ASA FirePOWER モジュールを保護するには、保護された内部ネットワークにそれをインストールしてください。ASA FirePOWER モジュールは必要なサービスとポートだけを使用するよう設定されますが、ファイアウォール外部からの攻撃がそこまで決して到達できないようにする必要があります。

また、ASA FirePOWER モジュール の機能によってはインターネット接続が必要となることにも注意してください。デフォルトで、ASA FirePOWER モジュールはインターネットに直接接続するよう設定されます。加えて、システムで特定のポートを開いたままにしておく必要があります。その目的はセキュアなアプライアンス アクセスおよび特定のシステム機能を正しく動作させるためにローカル/インターネット リソースへのアクセスを可能にすることです。

詳細については、以下を参照してください。

- インターネット アクセス要件（D-1 ページ）
- 通信ポートの要件（D-2 ページ）

インターネット アクセス要件

デフォルトで、ASA FirePOWER モジュールはポート 443/tcp（HTTPS）および 80/tcp（HTTP）でインターネットに直接接続するよう設定されます。これらのポートは、ASA FirePOWER モジュール上でデフォルトでオープンになっています（通信ポートの要件（D-2 ページ）を参照）。

次の表に、ASA FirePOWER モジュールの特定の機能におけるインターネット アクセス要件を示します。

表 ***D-1*** ***ASA FirePOWER*** モジュール機能のインターネット アクセス要件

機能	インターネット アクセスの用途
侵入ルール、VDB、および GeoDB の更新	侵入ルール、GeoDB、または VDB の更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。
ネットワークベースの AMP	マルウェア クラウド検索を実行します。
セキュリティ インテリジェンス フィルタリング	インテリジェンス フィードを含む、外部ソースからのセキュリティ インテリジェンス フィード データをダウンロードします。
システム ソフトウェアの更新	システム更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。

表 *D-1*　*ASA FirePOWER* モジュール機能のインターネット アクセス要件（続き）

機能	インターネット アクセスの用途
URL フィルタリング	クラウドベースの URL カテゴリおよびレピュテーション データをアクセス コントロール用にダウンロードし、カテゴライズされていない URL に対してルックアップを実行します。
whois	外部ホストの whois 情報を要求します。

通信ポートの要件

オープン ポートは以下を許可します。

- アプライアンスのユーザ インターフェイスにアクセスする
- アプライアンスへのリモート接続を保護する
- 特定のシステム機能を正しく動作させるために必要なローカル/インターネット リソースへのアクセスを可能にする

一般に、機能関連のポートは、該当する機能を有効化または設定する時点まで、閉じたままになります。

注意　開いたポートを閉じると展開にどのような影響が及ぶか理解するまでは、開いたポートを閉じないでください。

たとえば、管理デバイス上のポート 25/tcp（SMTP）アウトバウンドを閉じた場合、個別の侵入イベントに関する電子メール通知をデバイスから送信できなくなります（侵入ルールの外部アラートの設定（36-1 ページ）を参照）。

次の表は、ASA FirePOWER モジュールの機能を最大限に活用できるように、必要なオープン ポートを示しています。

表 *D-2*　*ASA FirePOWER* モジュールの機能と運用のためのデフォルト通信ポート

ポート	説明	方向	開く目的
22/tcp	SSH/SSL	双方向	アプライアンスへのセキュアなリモート接続を許可します。
25/tcp	SMTP	発信	アプライアンスから電子メール通知とアラートを送信します。
53/tcp	DNS	発信	DNS を使用します。
67/udp 68/udp	DHCP	発信	DHCP を使用します。 （注）　これらのポートはデフォルトで閉じられています。
		双方向	HTTP 経由でカスタムおよびサードパーティのセキュリティ インテリジェンス フィードを更新します。 URL カテゴリおよびレピュテーション データをダウンロードします（さらにポート 443 も必要）。

表 *D-2*　*ASA FirePOWER* モジュールの機能と運用のためのデフォルト通信ポート（続き）

ポート	説明	方向	開く目的
161/udp	SNMP	双方向	SNMP ポーリング経由でアプライアンスの MIB にアクセスできるようにします。
162/udp	SNMP	発信	リモート トラップ サーバに SNMP アラートを送信します。
389/tcp 636/tcp	LDAP	発信	外部認証用に LDAP サーバと通信します。
389/tcp 636/tcp	LDAP	発信	検出された LDAP ユーザに関するメタデータを取得します。
443/tcp	HTTPS	着信	アプライアンスのユーザ インターフェイスにアクセスします。
443/tcp	HTTPS クラウド通信	双方向	次のものを取得します。 • ソフトウェア、侵入ルール、VDB、および GeoDB の更新 • URL カテゴリおよびレピュテーション データ（さらにポート 80 も必要） • インテリジェンス フィードおよび他のセキュアなセキュリティ インテリジェンス フィード • ファイルに関してネットワーク トラフィックで検出されたマルウェアの性質
			デバイスのローカル ユーザ インターフェイスを使用してソフトウェア更新をダウンロードします。
514/udp	syslog	発信	リモート syslog サーバにアラートを送信します。
8305/tcp	アプライアンス通信	双方向	展開におけるアプライアンス間で安全に通信します。必須作業です。
8307/tcp	ホスト入力クライアント	双方向	ホスト入力クライアントと通信します。