再使用可能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、値を使用する必要がある場合、代わりに名前付きオブジェクトを使用できます。

次のタイプのオブジェクトを作成できます。

- IP アドレスとネットワーク、ポートとプロトコルのペア、セキュリティ ゾーン、および送信側と宛先の国（地理位置情報）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 フィードとリスト、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、非暗号化および復号化されたトラフィックを処理するためのオブジェクト

これらのオブジェクトは、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、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、URL、および公開キー インフラストラクチャ（PKI）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、変更を有効にするために設定の再展開が必要になります。

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（**[Configuration] > [ASA FirePOWER Configuration] > [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、URL、および PKI 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、参照することもできます。

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、PKI、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設定を再展開する必要があります。設定変更の導入を参照してください。

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 **[Configuration] > [ASA FirePOWER Configuration] > [Object Management]** の順に選択します。

ステップ 2 グループ化するオブジェクト タイプ [Network]、[Port]、[URL]、[PKI]、または [Distinguished Name] で、[Object Groups] を選択します。

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

ステップ 4 [Name] に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、[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 と Ctrl を使用するか、右クリックして [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。このフィールドは入力に従って更新され、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にあるリロードアイコン（）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。
- 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 [Store ASA FirePOWER Changes] をクリックします。

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：

1. カラム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：

1. [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。フィールドには、ワイルドカードとして 1 つ以上のアスタリスク（*）を使用できます。

オブジェクトの参照、ソート、およびフィルタ

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：

カラム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：

a) [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 ページ）を参照）は、アクセス コントロール ポリシー、ネットワークの変数、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 **[Configuration]** > **[ASA FirePOWER Configuration]** > **[Object Management]** の順に選択します。

ステップ 2 [Network] で、[Individual Objects] を選択します。

ステップ 3 [Add Network] をクリックします。

ステップ 4 [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 [Add] をクリックします。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入を参照してください。

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制御ルールによって分析される前に、特定の IP アドレスをブロックする（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、アクセス制御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 アドレスをブロックするかどうか決めていない場合は、「モニタのみ」の設定を使用できます。この設定では、システムがアクセス制御ルールを使用して接続を処理でき、接続の一致がセキュリティ インテリジェンスのブロックリストに記録されます。

グローバルホワイトリストと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とブラックリストや、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制約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処理できます。ASA FirePOWER モジュールには、ブラックリストの作成に役立つインテリジェンスフィードがあります。このフィードは、VRT によってレピュテーションが低いと判断された IP アドレスを表します。

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、ポリシーを展開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、シスコでは自動更新を許可することを推奨しています。オンデマンド更新は手動でも実行できますが、システムが定期的にフィードをダウンロードするようにすれば、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 リストは、手動でシステムにアップロードする IP アドレスの単純な静的リストです。フィードやグローバルホワイトリストとブラックリストを増やしたり、微調整したりするには、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、変更を有効にするために設定を再展開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を更新します。

インターネット アクセスおよびハイ 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。

システムでは、カスタム フィードのダウンロード時にピアSSL証明書の検証は行われません。また、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されていません。

フィードとリストの管理

[Security Intelligence] 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 [Security Intelligence] ページを使用して作成および管理します。

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 *1:* セキュリティ インテリジェンス

機能	ブ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のいずれかの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（No）	あり	あり	あり	あり
削除できるか	いいえ（No）	いいえ（No）	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
変更されたときに設定の再展開が必要か	削除する場合は「はい」（IP アドレスを追加する場合は、再展開する必要はありません）	いいえ（No）	いいえ（No）	あり	あり

グローバルホワイトリストと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とブラックリストは、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。ポリシーごとに、これらのグローバル リストを使用しないことを選択できます。

グローバル リストにIPアドレスを追加した後は、設定を再展開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、変更を有効にするために設定を再展開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、[Monitor] または [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、[Source Networks] および [Destination Networks] の [any] のデフォルト値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 [Security Intelligence] 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。

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 IP アドレスを選択し、右クリックして [Delete] を選択します。

ステップ 3 [Store ASA FirePOWER Changes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入を参照してください。

インテリジェンス フィードの操作

ライセンス：Protection

ASA FirePOWER モジュールには、ブラックリストの作成に役立つインテリジェンスフィードがあります。このフィードは、VRT によってレピュテーションが低いと判断された IP アドレスの定期的に更新される複数のリストから成ります。フィードの各リストは、オープンリレー、既知の攻撃者、bogus IP アドレス（bogon）などの、特定のカテゴリを表します。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ロックできます。

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処理できます。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展開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 [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。

ステップ 2 [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 [Store ASA FirePOWER Changes] をクリックします。

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やブラックリストによって、インテリジェンスフィードを増やすことができます。また、内部フィードを設定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 でエンコードすることはできません。デフォルトでは、システムは設定された間隔でフィード 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、システムによるチェックサムの再ダウンロードは不要です。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 [Security Intelligence] ページで、[Add Security Intelligence] をクリックします。

ステップ 2 フィードの名前を [Name] に入力します。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 [Type] ドロップダウンリストから、[Feed] を設定することを指定します。

ステップ 4 [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 [Update Frequency] を指定します。

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 [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 [Security Intelligence] ページで、[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可能性があることが警告されます。

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ら、システムはその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ても、そのフィードが組織にとって全体的に有用である場合、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 アドレスだけを含む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 （11 ページ）を参照してください。

新しいセキュリティ インテリジェンスをアップロードする方法：

ステップ 1 オブジェクト マネージャの [Security Intelligence] ページで、[Add Security Intelligence] をクリックします。

ステップ 2 リストの名前を [Name] に入力します。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 [Type] ドロップダウンリストから、[List] をアップロードすることを指定します。

ステップ 4 [Browse] をクリックして list.txt ファイルを参照し、[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、リストで検出された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 [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 [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。

ステップ 2 編集するリストのコピーが必要な場合、[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。

必要に応じてリストを変更します。

ステップ 3 [Security Intelligence] ポップアップ ウィンドウで、[Browse] をクリックして変更されたリストを参照し、[Upload] をクリックします。

ステップ 4 [Store ASA FirePOWER Changes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入を参照してください。

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およびオプションのタイプとコードを表します。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、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 ページ）を参照）は、アクセス コントロール ポリシーやポートの変数など、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、ポート オブジェクトを編集または削除した後に、アクティブ ポリシーがオブジェクトを参照する場合、変更を有効にするには設定を再展開する必要があります。設定変更の導入を参照してください。

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、使用場所のルールはポリシー展開には適用されません。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 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Port] で、[Individual Objects] を選択します。

ステップ 3 [Add Port] をクリックします。

ステップ 4 [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 [Protocol] を選択します。

[TCP]、[UDP]、[IP]、[ICMP]、または [IPv6 ICMP] から選択するか、[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 [All] プロトコルを選択できます。

ステップ 6 オプションで、[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 必要に応じて、[Type] および関連する [Code]（該当する場合）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、タイプおよびコード（該当する場合）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 および
http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml 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、[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。[All] プロトコルを選択した場合は、[Port] フィールドにポート番号を入力します。

ステップ 9 [Store ASA FirePOWER Changes] をクリックします。

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。アクセス コントロール ポリシーでは、URL オブジェクトとグループを使用できます（オブジェクトのグループ化 （2 ページ）を参照）。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、URL オブジェクトを編集または削除した後に、アクティブ ポリシーがオブジェクトを参照する場合、変更を有効にするには設定を再展開する必要があります。設定変更の導入を参照してください。

URL オブジェクトを作成する方法：

ステップ 1 [Configuration] > > [ASA FirePOWER Configuration] > > [Object Management] の順に選択します。

ステップ 2 [URL] で、[Individual Objects] を選択します。

ステップ 3 [Add URL] をクリックします。

ステップ 4 [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 [Store ASA FirePOWER Changes] をクリックします。

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 コントロールの実行には不可欠です。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提供されており、シスコでは頻繁に更新を行い、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追加しています。

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、変更された設定を再展開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。

システム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。ユーザ定義のフィルタでは、システム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。

システム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（[Configuration] > [ASA FirePOWER Configuration] > [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。

[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システム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。

[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の詳細については、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、情報ポップアップにあるいずれかのインターネット検索リンクをクリックします。

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、[All apps matching the filter] を追加することができます。[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 [Application Filters] ページに一覧表示されます。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 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、アプリケーション フィルタ オブジェクトを編集または削除した後に、アクティブ ポリシーがオブジェクトを参照する場合、変更を有効にするには設定を再展開する必要があります。設定変更の導入を参照してください。

アプリケーション フィルタを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Application Filters] をクリックします。

ステップ 3 [Add Application Filter] をクリックします。

ステップ 4 [Name] 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 必要に応じて、[Application Filters] リストにあるシステム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、[Check All] または [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、[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、[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 [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 [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、[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、[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 アイコンをクリックします。
- 複数の個別のアプリケーションを選択するには、Shift キーおよび Ctrl キーを使用します。現在表示されている個別のアプリケーションをすべて選択するには、右クリックして [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 [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、[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 [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 [Select All] を選択してから、右クリックして [Delete Selected] を選択することもできます。

ステップ 8 [Store ASA FirePOWER Changes] をクリックします。

変数セットの操作

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。いずれのセットでも、定義済みのデフォルトの変数を変更したり、ユーザ定義の変数を追加および変更したりできます。

ASA FirePOWER モジュール提供の共有オブジェクト ルールと標準テキスト ルールの大部分では、定義済みのデフォルト変数を使用してネットワークと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、事前定義されたデフォルト変数の最適化 （17 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 サーバが含まれるようにするには、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監視されます。

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。

事前定義されたデフォルト変数の最適化

デフォルトでは、ASA FirePOWER モジュールには、定義済みのデフォルト変数から成る単一のデフォルト変数セットがあります。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、「ルール更新とローカル ルール ファイルのインポート」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では定義済みのデフォルト変数が使用されるため、そ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、「変数の追加と編集 （26 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、インポートしたデフォルト変数で上書きされます。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、設定のインポートを参照してください。

次の表に、ASA FirePOWER モジュールで提供される変数に関する説明、および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 : ASA FirePOWER* モジュールで提供される変数（続き）

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。
$EXTERNAL_NET	ASA FirePOWER モジュールに非保護ネットワークとして表示され、外部ネットワークを定義するために多くのルールで使用されるネットワークを定義します。	はい。$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。

変数名	説明	変更しますか
$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監視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。
$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。

変数名	説明	変更しますか
$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	後に、バージョン 5.3.0 以降にアップグレードされるバージョン 5.3.0 以前の ASA FirePOWER モジュール ソフトウェア リリースのシステム上に存在する場合にのみ表示されるレガシー拡張変数を特定します。拡張変数について（36 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）。

変数名	説明	変更しますか
$SSH_SERVERS	ネットワーク上で SSH サーバを定義し、SSH をターゲットとしたエクスプロイトを解決するルールで使用されます。	はい。SSH サーバを実行している場合は、$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 （36 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 （36 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。いずれの変数セットでも、ユーザ定義の変数を追加したり、任意の変数の値をカスタマイズしたりできます。

ASA FirePOWER モジュールでは、初めに定義済みのデフォルト値から成る単一のデフォルトの変数セットが提供されます。デフォルト設定では、各変数は最初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。

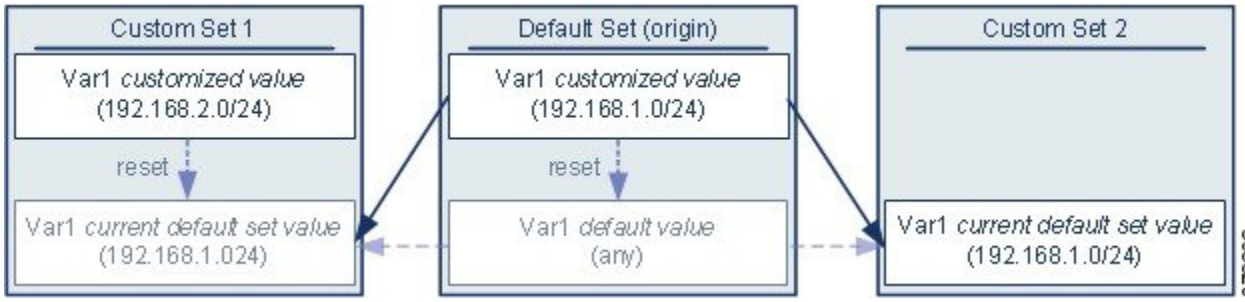
定義済みのデフォルト変数は、デフォルト値のままにすることもできますが、事前定義されたデフォルト変数の最適化 （17 ページ）の説明に従い、定義済みの変数のサブセットを変更することを推奨します。

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。



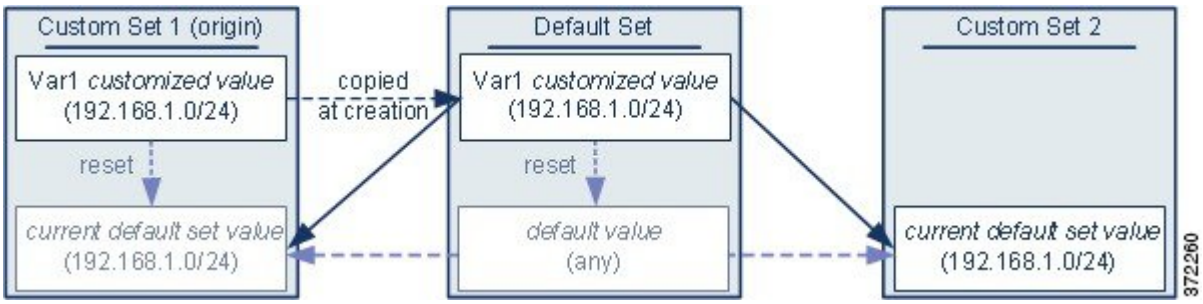
オプションで、任意のセットの Var1 値をカスタマイズできます。Var1 がカスタマイズされていない Custom Set 2 では、この値は 192.168.1.0/24 です。Custom Set 1 では、Var1 のカスタマイズ値 192.168.2.0/24 はデフォルト値をオーバーライドします。デフォルト セット内のユーザ定義変数をリセットすると、すべてのセットのデフォルト値が any にリセットされます。

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。

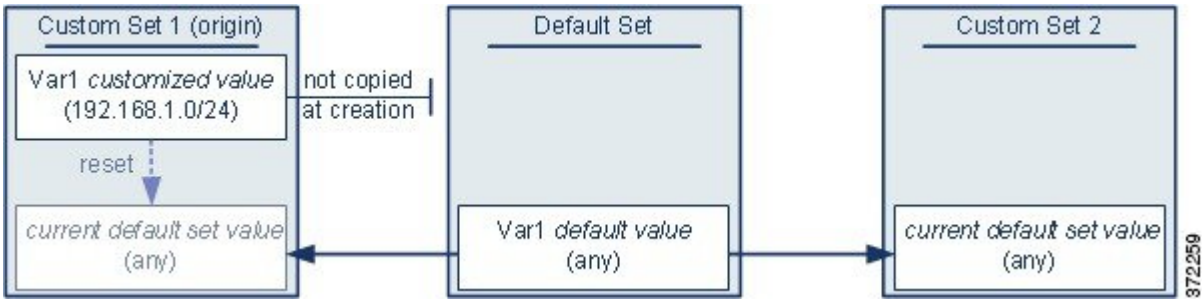
例：カスタム セットにユーザ定義変数を追加する

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を示しています。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**

[Object Manager] ページ（[Configuration] > > [ASA FirePOWER Configuration] > > [Object Management] > ）で [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は、デフォルトの変数セットは、デフォルトのシステム提供変数だけで構成されます。

各変数セットには、システム提供のデフォルト変数と、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 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	[Configuration] > [ASA FirePOWER Configuration] > [Object Management] を選択し、[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	[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。 変数セットの行内で右クリックし、[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、[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。 変数セットの行内で右クリックし、[Delete] を選択してから、[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 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Variable Set] を選択します。

ステップ 3 変数セットを作成したり、既存のセットを編集したりするには、以下の手順に従います。

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

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、変数の追加と編集 （26 ページ）を参照してください。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入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 [Customized Variables] ページ領域と [Default Variables] ページ領域に分かれています。

デフォルト変数は、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、その変数は [Default Variables] 領域から [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した場合、その変数は [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 *4*: 変数の管理アクション（続き）

目的	操作
変数のページを表示する	変数セット ページで、[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	[Name] および [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	[Add] をクリックします。 詳細については、「変数の追加と編集 （26 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、「変数の追加と編集 （26 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	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、[Yes] をクリックして変数の削除を確認します。 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 [Store ASA FirePOWER Changes] をクリックしてから、[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 [Configuration] > > [ASA FirePOWER Configuration] > > [Object Management] の順に選択します。

ステップ 2 [Variable Set] を選択します。

ステップ 3 変数セットを作成したり、既存のセットを編集したりするには、以下の手順に従います。

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

ステップ 4 変数を作成したり、既存の変数を編集したりするには、以下の手順に従います。

- 変数を作成するには、[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。

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、変数の追加と編集 （26 ページ）を参照してください。

変数の追加と編集

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 を作成する場合はさらに、独自のユーザ定義変数を作成して、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場合は、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選択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 （21 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 [New Variable] ページで行い、既存の変数の編集は [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作業 （31 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 （33 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、[Include] または [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 5: 変数の編集アクション（続き）

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、[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	[Name] フィールドに、下線文字（_）以外の特殊文字を含まない、大文字と小文字を区別した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	[Type] ドロップダウンリストから [Network] または [Port] を選択します。 ネットワーク変数およびポート変数の使用および設定方法の詳細については、ネットワーク変数の作業 （31 ページ）およびポート変数の操作 （33 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	[Type] ドロップダウンリストから [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 （4 ページ） を参照してください。
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	[Type] ドロップダウンリストから [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 （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に名前を入力します。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、[Include] または [Excluede] 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 [literal Network] または [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入力して、[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 [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	[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、[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、[No] をクリックするとデフォルト値 any が使用されます。

変数を編集した後に、アクティブ ポリシーがオブジェクトを参照する場合、変更を有効にするには設定を再展開する必要があります。設定変更の導入を参照してください。

変数を作成または編集する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Variable Set] を選択します。

ステップ 3 変数セットを作成したり、既存のセットを編集したりするには、以下の手順に従います。

- 変数セットを作成するには、[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。

ステップ 4 新しい変数を作成したり、既存の変数を編集したりするには、以下の手順に従います。

- 新しい変数を作成するには、[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。

ステップ 5 新しい変数を作成するには、以下の手順に従います。

- [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 [Type] として [Network] または [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、[Include] または [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 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、[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 [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。

- [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。
- [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 [Store ASA FirePOWER Changes] をクリックして、[Yes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入を参照してください。

ネットワーク変数の作業

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。ネットワーク変数はネットワーク オブジェクトやネットワーク オブジェクト グループとは異なります。ネットワーク変数は、侵入ポリシーや侵入ルールに固有のものですが、ネットワーク オブジェクトおよびグループは、アクセス コントロール ポリシー、ネットワーク変数、レポートなど、ASA FirePOWER モジュールのさまざまな場所で IP アドレスを表すために使用できます。詳細については、「ネットワーク オブジェクトの操作 （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 [Source IPs] および [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。

- 抑制

送信元または宛先の侵入ルール抑制の [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。侵入ポリシーごとの抑制の設定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 [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 [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。ルールを使用した侵入ポリシーの調整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 （4 ページ）を参照してください。

- [New Variable] または [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、他の既存の変数、今後の変数に追加可能）
- 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 でも、192.168.1.5 でもない」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、変数の追加と編集 （26 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 [Source Port] および [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 および UDP 以外のプロトコル用にポート オブジェクトを作成して、ポート変数とアクセス 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 （11 ページ）」を参照してください。

侵入ルールの [Source Port] および [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、システムによりアクセス 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 （11 ページ）を参照してください。

- [New Variable] または [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、他の既存の変数、今後の変数に追加可能）

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、変数の追加と編集 （26 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 *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際は、リンクされたカスタム セットの変数を使用している侵入ポリシーが、その変更によってどのような影響を受けるかを評価することをお勧めします（特に、カスタム セット内の変数値をまだ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

侵入ポリシーへの変数セットのリンク

ライセンス：Control

デフォルトでは、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 ポリシーを展開すると、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用されるカスタム変数セットを変更すると、[Access Control] ページに、そのポリシーのステータスが「失効」と表示されます。変数セットの変更を実装するには、設定を展開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」と表示され、変更を実装するには設定を再展開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」（144 ページ）の手順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
- 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、デフォルトの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展開するには、設定変更の導入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あり、USER_CONF 拡張変数のみ編集できます。

USER_CONF

USER_CONFは、モジュールインターフェイスで通常設定できない1つ以上の機能を設定するための汎用ツールです。

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 オブジェクトの操作

ライセンス：Protection

シンクホール オブジェクトは、シンクホール内のすべてのドメイン名にルーティング不可アドレスを付与する DNS サーバ、またはサーバに解決しない IP アドレスのいずれかを表します。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できます。このオブジェクトには 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に、変更を有効にするには、設定を再展開する必要があります。設定変更の導入を参照してください。

シンクホール オブジェクトを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 オブジェクト タイプのリストから [Sinkhole] を選択します。

ステップ 3 [Add Sinkhole] をクリックします。

ステップ 4 [Name] 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、[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、[Block and Log Connections to Sinkhole] を選択します。

ステップ 7 [Indication of Compromise (IoC)] タイプをシンクホールに割り当てる場合は、[Type] ドロップダウンからいずれかを選択します。

ステップ 8 [Store ASA FirePOWER Changes] をクリックします。

ファイル リストの操作

ライセンス：Malware

ネットワークベースの高度なマルウェア防御（AMP）を使用していて、Collective Security Intelligence クラウドによってファイルの性質が誤って識別される場合は、SHA256 ハッシュ値を使用してそのファイルをファイル リストに追加し、以降のファイル検出精度を向上できます。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 アクションとブロック マルウェア アクションのいずれか、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ります。詳細については、「ファイル ルールの操作」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。クラウドによってファイルのマルウェアの性質が割り当てられている場合、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、システムはそれらのファイル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 SHA256 値を計算して追加できます。
- 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 値を削除したりする場合、変更を有効にするには、設定を再展開する必要があります。設定変更の導入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

ライセンス：**Malware**

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で、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、新たにアップロードし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 ファイルに同じ SHA-256 値のエントリが含まれている場合は、最新の値が使用されます。
- 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 （41 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 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [File List] をクリックします。

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。

ステップ 4 [Add by] フィールドから [List of SHAs] を選択します。

ステップ 5 オプションで、[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 [Browse] をクリックしてソース ファイルを参照してから、[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 値の数が表示されます。

ステップ 7 [Store ASA FirePOWER Changes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入を参照してください。

設定が展開されると、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：**Malware**

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 値を計算して、ファイルをリストに追加します。SHA-256 を計算する場合、ファイル サイズは制限されません。

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 [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にある編集アイコン（  ）をクリックします。

ステップ 2 [Add by] フィールドから [Calculate SHA] を選択します。

ステップ 3 オプションで、[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 [Browse] をクリックしてソース ファイルを参照してから、[Calculate and Add SHA] をクリックしてリストを追加します。

ステップ 5 [Store ASA FirePOWER Changes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入を参照してください。

設定が展開されると、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：Malware

ファイルの SHA-256 値を送信して、その値をファイル 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 値を手動で入力し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 [File List] ページで、ファイルの追加先となるクリーン リストまたはカスタム検出リストの横にある編集アイコン（  ）をクリックします。

ステップ 2 [Add by] フィールドから [Enter SHA Value] を選択します。

ステップ 3 [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、[Add] をクリックします。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入を参照してください。

設定の展開後には、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：**Malware**

ファイル リストの個々の SHA-256 値を編集または削除できます。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 （41 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 [File List] ページで、変更するファイルがあるクリーン リストまたはカスタム検出リストの横にある編集アイコン（  ）をクリックします。

ステップ 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。

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（  ）をクリックします。

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

ステップ 4 [**Save**] をクリックします。

ステップ 5 [Store ASA FirePOWER Changes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入を参照してください。

設定の展開後には、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：**Malware**

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 （38 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 [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にある編集アイコン（  ）をクリックします。

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。

ステップ 3 [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。

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。単一のデバイス上に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でき、システムによりさまざまなポリシーを適用できるようになります。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、ゾーンはアクセス コントロール ポリシーでも使用できます。たとえば、特定の送信元または宛先ゾーンだけに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もできます。

オブジェクト マネージャの [Security Zones] ページには、ASA FirePOWER モジュールで設定されたゾーンが一覧表示されます。

使用中のセキュリティ ゾーンは削除できません。ゾーンでのインターフェイスの追加または削除の後に、アクティブ ポリシーがオブジェクトを参照する場合は、変更を有効にするために設定を展開する必要があります。設定変更の導入を参照してください。

セキュリティ ゾーンを作成する手順：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Security Zones] を選択します。

ステップ 3 [Add Security Zone] をクリックします。

ステップ 4 [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 [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 [Add] をクリックします。

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、手順 6 から 8 までを繰り返します。

ステップ 9 [Store ASA FirePOWER Changes] をクリックします。

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。定義済みの各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用さ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、暗号スイート リストを編集した後に、アクティブ ポリシーがオブジェクトを参照する場合、変更を有効にするには設定を再展開する必要があります。設定変更の導入を参照してください。

暗号スイート リストを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Cipher Suite List] を選択します。

ステップ 3 [Add Cipher Suites] をクリックします。

ステップ 4 [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、[Add] をクリックします。

- Shift および Ctrl を使用して複数の暗号スイートを選択するか、右クリックして [Select All] を選択します。
- 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（🔍）を使用します。このフィールドは入力に従って更新され、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

ルドの上にあるリロードアイコン（）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。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

識別名オブジェクトの操作

ライセンス：任意

各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の識別名リストを表します。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 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=」を含まない共通名を追加すると、オブジェクトを保存する前に「CN=」が名前の前に追加されます。

さらに、次の表にリストされている、コンマで区切られた属性を含む識別名を追加することもできます。

表 7: 識別名の属性

属性	説明	使用可能な値
C	国番号	2 つの英字
CN	共通名	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	組織	
OU	組織単位	

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 *8*: 共通名属性のワイルドカードの例

属性	一致する	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	mail.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、識別名オブジェクトを編集した後に、アクティブポリシーがオブジェクトを参照する場合、変更を有効にするには設定を展開する必要があります。設定変更の導入を参照してください。

識別名オブジェクトを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Distinguished Name] の下で、[Individual Objects] を選択します。

ステップ 3 [Add Distinguished Name] をクリックします。

ステップ 4 [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、[Distinguished Name Attributes] テーブルにリストされている、コンマで区切られた属性を含める必要があります。
- 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 [Store ASA FirePOWER Changes] をクリックします。

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、次のものを復号化できます。

- 発信トラフィック：内部 CA オブジェクトを使用してサーバ証明書を再署名することで復号化します
- 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化します

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、証明書のサブジェクト識別名がオブジェクト値として表示されます。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。その他の証明書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キーを、ランダムに生成されたキーを使用して暗号化してから保存します。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用して秘密キーを復号化し、ランダムに生成されたキーを使用して再暗号化してから保存します。

内部認証局オブジェクトの操作

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 ページ）を参照）を使用すると、内部CAでサーバ証明書を再署名することで、発信される暗号化トラフィックを復号化できます。

（注） [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。

- 既存のRSAベースまたは楕円曲線ベースの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。

システム生成の場合でも、ユーザ作成の場合でも、内部CAオブジェクトの名前は変更できますが、オブジェクトの他の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、内部CAオブジェクトを編集した後に、アクティブポリシーがオブジェクトを参照する場合、変更を有効にするには設定を展開する必要があります。設定変更の導入を参照してください。

CA証明書および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、復号化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 [Decrypt - Resign] アクションを設定すると、そのルールでは、設定されているすべての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化するには、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、「復号化アクション：さらに検査するためにトラフィックを復号化」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 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [PKI] で、[Internal CAs] を選択します。

ステップ 3 [Import CA] をクリックします。

ステップ 4 [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 [Certificate Data] フィールドの上部にある [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 [Key] フィールドの上部にある [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、[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 [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で、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 *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	2 つの英字
州または地域、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）		
組織単位（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。[Valid From] の日付は生成の一週間前です。

自己署名 CA 証明書を生成するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [PKI] で、[Internal CAs] を選択します。

ステップ 3 [Generate CA] をクリックします。

ステップ 4 [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「生成される内部 CA 属性」の説明に従い、識別属性を入力します。

ステップ 6 [Generate self-signed CA] をクリックします。

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 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。

a) [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。
b) [PKI] で、[Internal CAs] を選択します。
c) [Generate CA] をクリックします。
d) [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。
e) 新しい CA 証明書と秘密キーの生成 （48 ページ）の説明に従い、識別属性を入力します。
f) [Generate CSR] をクリックします。
g) CA に送信するために CSR をコピーします。
h) [Store ASA FirePOWER Changes] をクリックします。

ステップ 2 CA から署名証明書をアップロードします。

a) [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。
b) [PKI] で、[Internal CAs] を選択します。
c) CSR を待機している未署名の証明書を含む CA オブジェクトの横にある編集アイコン（✏）をクリックします。
d) [Install Certificate] をクリックします。
e) [Certificate Data] フィールドの上部にある [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。
f) 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、[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。
g) [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 証明書および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化してから、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、復号化されてから、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 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [PKI] で、[Internal CAs] を選択します。

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

ステップ 4 [Download] をクリックします。

ステップ 5 [Password] および [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 [Store ASA FirePOWER Changes] をクリックします。

ファイルを保存するように指示するメッセージが表示されます。

信頼できる認証局オブジェクトの操作

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 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、信頼できる CA オブジェクトを編集した後に、アクティブポリシーがオブジェクトを参照する場合、変更を有効にするには設定を展開する必要があります。設定変更の導入を参照してください。

信頼できる CA オブジェクトの追加

ライセンス：任意

外部 CA オブジェクトは、X.509 v3 CA 証明書をアップロードすることによって設定できます。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、復号化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 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [PKI] で、[Trusted CAs] を選択します。

ステップ 3 [Add Trusted CAs] をクリックします。

ステップ 4 [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 [Certificate Data] フィールドの上部にある [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、[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 [Store ASA FirePOWER Changes] をクリックします。

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 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。
ステップ 2 [PKI] で、[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。
ステップ 4 [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 [Store ASA FirePOWER Changes] をクリックします。

外部証明書オブジェクトの操作

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 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はアップロードできますが、信頼できる CA 証明書を使用し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、外部証明書オブジェクトを編集した後に、アクティブ ポリシーがオブジェクトを参照する場合、変更を有効にするには設定を展開する必要があります。設定変更の導入を参照してください。

外部証明書オブジェクトを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。
ステップ 2 [PKI] で、[External Certs] を選択します。

ステップ 3 [Add External Cert] をクリックします。

ステップ 4 [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 [Certificate Data] フィールドの上部にある [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 [Store ASA FirePOWER Changes] をクリックします。

内部証明書オブジェクトの操作

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 ページ）を参照）を使用すると、既知の秘密キー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化できます。

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で、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、復号化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、内部証明書オブジェクトを編集した後に、アクティブポリシーがオブジェクトを参照する場合、変更を有効にするには設定を展開する必要があります。設定変更の導入を参照してください。

内部証明書オブジェクトを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [PKI] で、[Internal Certs] を選択します。

ステップ 3 [Add Internal Cert] をクリックします。

ステップ 4 [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 [Certificate Data] フィールドの上部にある [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 [Key] フィールドの上部にある [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 アップロードした秘密キー ファイルがパスワード保護されている場合は、[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 [Store ASA FirePOWER Changes] をクリックします。

次のタスク

- CA 証明書および秘密キーのインポート （47 ページ）
新しい CA 証明書と秘密キーの生成 （48 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 （49 ページ）
CA 証明書および秘密キーのダウンロード （50 ページ）

地理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、管理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。アクセス コントロール ポリシーまたは SSL ポリシーでは、地理位置情報オブジェクトを使用できます。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、地理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、地理情報データベースについて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 ポリシーまたは SSL ポリシーで使用される地理位置情報オブジェクトを編集した後、変更を有効にするには、ポリシーを再適用する必要があります。

地理位置情報オブジェクトを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Geolocation] を選択します。

ステップ 3 [Add Geolocation] をクリックします。

ステップ 4 [Name] に、地理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 [Store ASA FirePOWER Changes] をクリックします。

セキュリティ グループ タグ オブジェクトの操作

ライセンス：任意

セキュリティ グループ タグ（SGT）オブジェクトは、単一の SGT 値を指定します。この値はアクセス コントロール ルールでカスタム SGT 条件として使用できます。SGT オブジェクトをグループ化することはできません。

ISE/ISE-PIC をアイデンティティ ソースとして設定すると、システムはオブジェクト マネージャの [セキュリティ グループ タグ（Security Group Tag）] オプションを自動的に無効にします。ISE/ISE-PIC 接続を無効にしない限り、新規 SGT オブジェクトの追加、既存 SGT オブジェクトの編集、またはルール条件としての SGT オブジェクトの使用はできません。カスタム SGT と ISE SGT の違いの詳細については、ISE SGT およびカスタム SGT ルール条件を参照してください。

SGT オブジェクトを編集または削除した後に、アクティブ ポリシーがオブジェクトを参照する場合、変更を有効にするには設定を再展開する必要があります。設定変更の導入を参照してください。

SGT オブジェクトを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Security Group] タグを選択します。

ステップ 3 [Add Security Group Tag] をクリックします。

ステップ 4 [Name] を入力します。

ステップ 5 （任意）[Description] に説明を入力します。

ステップ 6 [Tag] フィールドに、単一の SGT を入力します。

ステップ 7 [Store ASA FirePOWER Changes] をクリックします。