CHAPTER 3

再利用可能なオブジェクトの管理

柔軟性を高めて、Web インターフェイスを使用しやすくするために、FireSIGHT システムでは、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。

- ネットワークベースのオブジェクト。このオブジェクトによって、IP アドレスとネットワーク、ポート/プロトコルのペア、VLAN タグ、セキュリティ ゾーン、および送信側/宛先の国（地理位置情報）を表します。
- レピュテーションベースのオブジェクト。このオブジェクトによって、セキュリティ インテリジェンスのフィードおよびリスト、大項目およびレピュテーションに基づいたアプリケーション フィルタ、およびファイル リストを表します。
- レピュテーションベース以外のオブジェクト（URL カテゴリなど）
- 侵入ポリシーに関連付ける変数を含む侵入ポリシーの変数セット
- 暗号スイート、公開キー証明書や秘密キーのペア、および証明書の識別名を含む、暗号化トラフィックの処理に役立つオブジェクト。

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、侵入ポリシーやルール、ネットワーク検出ルール、イベント検索、レポート、ダッシュボードなど、システムの Web インターフェイス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、VLAN タグ、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（3-2 ページ）
- ネットワーク オブジェクトの操作（3-4 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（3-5 ページ）
- ポート オブジェクトの操作（3-13 ページ）
- VLAN タグ オブジェクトの操作（3-14 ページ）
- URL オブジェクトの操作（3-15 ページ）

オブジェクト マネージャの使用

ライセンス：任意（Any）

オブジェクト マネージャ（[オブジェクト（Objects）] > [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、VLAN タグ、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。

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

オブジェクトのグループ化

ライセンス：任意（Any）

ネットワーク、ポート、VLAN タグ、URL、および PKI オブジェクトをグループ化できます。システムでは、Web インターフェイスで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。

ヒント　暗号スイートをグループ化するには、暗号スイートのリストを設定します。詳細については、暗号スイート リストの操作（3-45 ページ）を参照してください。

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 VLAN 条件で使用している VLAN タグの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。

アクセス：Admin/Access Admin/Network Admin

手順 1　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

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

手順 2　次の選択肢があります。

- グループ化する [ネットワーク（Network）]、[ポート（Port）]、[VLAN タグ（VLAN Tag）]、[URL（URL）]、または [識別名（Distinguished Name）] オブジェクトのタイプの下で、[オブジェクト グループ（Object Groups）] を選択します。
- [PKI（PKI）] で、グループ化する PKI オブジェクトのタイプとして [内部 CA グループ（Internal CA Groups）]、[信頼できる CA グループ（Trusted CA Groups）]、[内部証明書グループ（Internal Cert Groups）]、または [外部証明書グループ（External Cert 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。

手順 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。

手順 4　グループの**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。

手順 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。

手順 6　[保存（Save）] 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（Any）

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、名前によってフィルタすることもできます。オブジェクトのタイプによっては、同じフィルタが名前または値に一致することがあります。

オブジェクトまたはグループをソートする方法:

アクセス: Admin/Access Admin/Network Admin

手順 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:

アクセス: Admin/Access Admin/Network Admin

手順 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。次のメタ文字を使用できます。

- アスタリスク(*)文字は、ある文字の 0 回以上のオカレンスに一致します。
- キャレット記号(^)は文字列の先頭部分と一致します。
- ドル記号($)は文字列の末尾のコンテンツと一致します。

ネットワーク オブジェクトの操作

ライセンス: 任意(Any)

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 (3-2 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、ネットワーク検出ルール、イベント検索、レポートなど、システムの Web インターフェイス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、ネットワーク検出、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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] を選択します。

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

手順 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。

手順 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。

手順 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。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。

手順 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。

手順 6　[保存(Save)] 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

サポートされるデバイス:すべて（シリーズ 2 を除く）

サポートされる防御センター:DC500 を除くいずれか

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。

（注） デフォルトで、シリーズ 2 デバイスは他のすべての Protection 機能がある場合でも、セキュリティ インテリジェンス フィルタリングを実行できません。

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 Defense Center 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。ブラックリストの作成に役立つように、シスコでは、Cisco VRT によってレピュテーションが低いと判断された IP アドレスを表す*インテリジェンス フィード*（別名 *Sourcefire インテリジェンス フィード*）を提供しています。

Defense Center は、更新されたフィード情報をダウンロードすると、管理対象デバイスを自動的に更新します。フィードの更新が導入環境全体に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） Defense Center 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、Defense Center 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。

Defense Center 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、Defense Center は、認識できるアドレスで管理対象デバイスを更新します。

デフォルトの正常性ポリシーには、セキュリティ インテリジェンス モジュールが含まれています。これは、Defense Center がフィードを更新できない場合や、フィードが破損していたり、認識できない IP アドレスが含まれていたりする場合など、セキュリティ インテリジェンス フィルタリングが関係する一部の状態でアラートを出します。

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、Defense Center でインバウンドとアウトバウンド両方の適切なポートを開く必要があります。フィード サイトへのダイレクト アクセスを持っていない場合、Defense Center はプロキシ サーバを使用できます（管理インターフェイスの構成（64-9 ページ）を参照してください）。

（注）　Defense Center 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。

ハイ アベイラビリティの導入環境では、セキュリティ インテリジェンス オブジェクトは Defense Center 間で同期されますが、プライマリ Defense Center だけがフィードの更新をダウンロードします。プライマリ Defense Center が失敗した場合、セカンダリ Defense Center がフィード サイトへのアクセス権を持っていることを確認するだけでなく、セカンダリ Defense Center の Web インターフェイスを使用してアクセス権のレベルを [アクティブ（Active）] に昇格する必要があります。詳細については、ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）を参照してください。

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（3-4 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 3-1　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（Capability）	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	No	Yes	Yes	Yes	Yes
削除できるか	No	No	Yes（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（コンテキスト メニューを使用して IP アドレスを追加する）	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）	No	No	Yes	Yes

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（3-7 ページ）
- インテリジェンス フィードの操作（3-9 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（3-10 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（3-11 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（3-11 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（13-1 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

サポートされるデバイス：すべて（シリーズ 2 を除く）

サポートされる防御センター：DC500 を除くいずれか

分析の過程で、イベント ビュー、Context Explorer、またはダッシュボードで IP アドレスのコンテキスト メニューを使用し、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* を作成できます。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 アドレスを即時にブラックリストに入れることができます。また、同じ方法で *グローバル ホワイトリスト* も作成できます。

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 アドレスを追加すると、Defense Center は自動的に管理対象デバイスを更新します。導入環境全体で変更を反映するには数分かかる場合がありますが、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に追加すると、アクセス コントロールに影響を与えるため、次のいずれかを持っている必要があります。

- 管理者アクセス権
- デフォルト ロールの組み合わせ：Network Admin または Access Admin に加えて Security Analyst および Security Approver
- Modify Access Control Policy と Apply Access Control Policy の両方の権限を持つカスタム ロール。カスタム ユーザ ロールによる展開の管理（12-4 ページ）を参照してください。

コンテキスト メニューを使用して 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に追加する方法：

アクセス：Admin/Custom

手順 1　イベント ビュー、パケット ビュー、Context Explorer、またはダッシュボードでは、ポインタを IP アドレスのホットスポットの上に移動します。

ヒント　イベント ビューまたはダッシュボードで、ポインタを左側のホスト アイコン（）ではなく、IP アドレスの上に移動します。

手順 2　コンテキスト メニューを起動します。

- イベント ビューまたはダッシュボードの場合は、右クリックします。
- Context Explorer またはパケット ビューの場合は、左クリックします。

手順 3　コンテキスト メニューから、[今すぐホワイトリスト（Whitelist Now）] または [今すぐブラックリスト（Blacklist Now）] を選択します。

コンテキスト メニューの他のオプションの詳細については、コンテキスト メニューの使用（2-5 ページ）を参照してください。

手順 4　IP アドレスをホワイトリストまたはブラックリストに登録することを確認します。

Defense Center がユーザの追加を管理対象デバイスに通信すると、導入環境ではその変更に従ってトラフィックのフィルタリングが開始されます。

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:

アクセス: Admin/Network Admin

手順 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。

手順 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。

手順 3　[保存(Save)] 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

サポートされるデバイス: すべて(シリーズ 2 を除く)

サポートされる防御センター: DC500 を除くいずれか

ブラックリストの作成に役立つように、シスコ では*インテリジェンス フィード*(別名 *Sourcefire インテリジェンス フィード*)を提供しています。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 アドレスの複数のリストから構成されており、リストは定期的に更新されます。インテリジェンス 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)を表しています。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の変更方法:

アクセス: Admin/Network Admin

手順 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、[Sourcefire インテリジェンス フィード(Sourcefire Intelligence Feed)] の横にある編集アイコン( )をクリックします。

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

手順 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。

手順 3　[保存(Save)] 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

サポートされるデバイス:すべて(シリーズ 2 を除く)

サポートされる防御センター:DC500 を除くいずれか

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。これは、1 つのソース リストを使用して導入環境で複数の Defense Center を更新する場合に役立ちます。

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、Defense Center 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、管理対象デバイスを自動更新します。

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。Defense Center 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は、システムによってフィードを再ダウンロードする必要はありません。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:

アクセス: Admin/Intrusion Admin

手順 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。

手順 2　[名前(Name)] にフィード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。

手順 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。

手順 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。

手順 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。

手順 6　[保存(Save)] 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、Defense Center 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

サポートされるデバイス:すべて（シリーズ 2 を除く）

サポートされる防御センター:DC500 を除くいずれか

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:

アクセス: Admin/Access Admin/Network Admin

手順 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。

手順 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。

手順 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、Defense Center はすべての変更内容を管理対象デバイスに通知します。導入環境では、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が開始されます。

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

サポートされるデバイス:すべて（シリーズ 2 を除く）

サポートされる防御センター:DC500 を除くいずれか

セキュリティ インテリジェンスのリストは、Defense Center に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、単一の Defense Center の管理対象デバイスで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（3-12 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 Defense Center にアップロードする方法:

アクセス: Admin/Access Admin/Network Admin

手順 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。

手順 2　[名前(Name)] に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。

手順 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。

手順 4　[参照(Browse)] をクリックしてリストの `.txt` ファイルを参照し、[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。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。

手順 5　[保存(Save)] 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

サポートされるデバイス: すべて(シリーズ 2 を除く)

サポートされる防御センター: DC500 を除くいずれか

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。Defense Center の Web インターフェイス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、Defense Center から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:

アクセス: Admin/Access Admin/Network Admin

手順 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。

手順 2　編集するリストのコピーが必要な場合、[ダウンロード(Download)] をクリックして、ブラウザの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。

手順 3　必要に応じてリストを変更します。

手順 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。

手順 5　[保存(Save)] 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(Any)

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。

シスコ がウェルノウン 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(3-2 ページ)を参照)を、アクセス コントロール ポリシー、ネットワーク検出ルール、ポート変数、およびイベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、特定のポート範囲を使用するカスタム クライアントを組織で使用することが原因で、システムによって過剰なイベントや誤解を与えるイベントが生成される場合、それらのポートのモニタリングを除外するようネットワーク検出ポリシーを設定できます。

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 ポリシーまたはネットワーク検出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中の管理対象デバイス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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] を選択します。

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

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

手順 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。

手順 4　[名前(Name)] にポート 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。

手順 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。

手順 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。

手順 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、次の URL を参照してください。

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

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。

手順 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。

手順 9　[保存(Save)] をクリックします。

ポート オブジェクトが追加されます。

VLAN タグ オブジェクトの操作

ライセンス: 任意(Any)

設定した各 VLAN タグ オブジェクトは、VLAN タグまたはタグの範囲を表します。VLAN タグ 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(3-2 ページ)を参照)を、アクセス コントロール ポリシーおよびイベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、特定の VLAN 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。

使用中の VLAN タグ 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 VLAN タグ 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。

VLAN タグ オブジェクトを追加する方法:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] を選択します。

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

手順 2　[VLAN タグ(VLAN Tag)] で、[個々のオブジェクト(Individual Objects)] を選択します。

手順 3　[VLAN タグの追加(Add VLAN Tag)] をクリックします。

[VLAN タグ(VLAN Tag)] ポップアップ ウィンドウが表示されます。

手順 4　[名前(Name)] に、VLAN タグ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。

手順 5　[VLAN タグ(VLAN Tag)] フィールドに VLAN タグの値を入力します。

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

手順 6　[保存(Save)] をクリックします。

VLAN タグ 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(Any)

サポートされるデバイス: すべて(シリーズ 2 を除く)

サポートされる防御センター: DC500 を除くいずれか

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(3-2 ページ)を参照)を、アクセス コントロール ポリシーおよびイベント検索など、システムの Web インターフェイスのさまざまな場所で使用できます。たとえば、特定の Web サイト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。

URL オブジェクトを作成する際に、特に暗号化トラフィックを復号またはブロックする SSL インスペクションを設定しない場合は、次の事項に留意してください。

- アクセス コントロール ルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は含めないでください。たとえば、www.example.com ではなく、example.com を使用します。
- URL 条件を含むアクセス コントロール ルールを使用して Web トラフィックを照合する場合、システムは暗号化プロトコル(HTTP 対 HTTPS)を無視します。つまり、アプリケーション条件を使用してルールを調整しない限り、Web サイトをブロックすると、その Web サイトへの HTTP と HTTPS の両方のトラフィックがブロックされます。URL オブジェクトを作成する場合は、オブジェクトの作成時にプロトコルを指定する必要はありません。たとえば、`http://example.com/` ではなく、`example.com` を使用します。

詳細については、トラフィック復号の概要(19-1 ページ)および URL のブロッキング(16-10 ページ)を参照してください。

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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] を選択します。

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

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

手順 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。

手順 4　[名前(Name)] に URL 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。

手順 5　URL オブジェクトの [URL] または IP アドレスを入力します。このフィールドでは、ワイルドカード(*)は使用**できません**。

手順 6　[保存(Save)] 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: FireSIGHT

サポートされるデバイス:すべて(シリーズ 2 を除く)

FireSIGHT システムは 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。また、独自のアプリケーション プロトコル ディテクタを作成して、システムの検出機能を強化することもできます。

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(表 45-2(45-12 ページ)を参照)。アプリケーション プロトコル ディテクタを作成する場合、これらの基準を使用してアプリケーションを特徴付ける必要もあります。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(16-4 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、シスコ 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、システム 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。

シスコ 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。また、ユーザ定義フィルタを次の方法でも使用できます。

- イベント ビューアを使用してアプリケーションを検索する場合は、検索でのオブジェクトとアプリケーション フィルタの使用（60-5 ページ）を参照してください
- レポート テンプレートでテーブル ビューを抑制する場合は、レポート テンプレート セクションの検索設定の操作（57-19 ページ）を参照してください
- [カスタム分析（Custom Analysis）] ダッシュボード ウィジェットでアプリケーション統計情報をフィルタする場合は、Custom Analysis ウィジェットの設定（55-17 ページ）を参照してください

アプリケーション フィルタを作成および管理する場合は、オブジェクト マネージャ（[オブジェクト（Objects）] > [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 シスコ 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（3-2 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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

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

手順 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。

手順 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。

手順 4　[名前（Name）] にフィルタの名前を指定します。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。

手順 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 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。

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。

手順 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。

手順 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。

手順 8　[保存（Save）] 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、適応型プロファイル、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。シスコ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 FireSIGHT システムが提供する 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（3-20 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（3-20 ページ）
- 変数セットについて（3-22 ページ）
- 変数セットの管理（3-24 ページ）
- 変数の管理（3-26 ページ）
- 変数の追加および編集（3-27 ページ）
- 変数のリセット（3-34 ページ）
- 変数のネスト（3-35 ページ）
- 変数セットを侵入ポリシーにリンクさせる（3-37 ページ）
- 拡張変数について（3-37 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

FireSIGHT システムはデフォルトで、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。シスコの脆弱性調査チーム（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（66-16 ページ）を参照してください。

シスコ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（3-27 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（A-5 ページ）を参照してください。

以下の表は、シスコ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 3-2　シスコ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。
$EXTERNAL_NET	保護されていないネットワークとして FireSIGHT システムが表示するネットワークを定義し、外部ネットワークを定義するために多くのルールで使用されます。	はい。$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（Web 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（Web 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。
$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。

表 3-2　シスコによって提供される変数（続き）

変数名	説明	変更しますか
$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 FireSIGHT システム 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（3-37 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（Web 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 Web 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（3-37 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（3-37 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。

FireSIGHT システムは初めに、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。

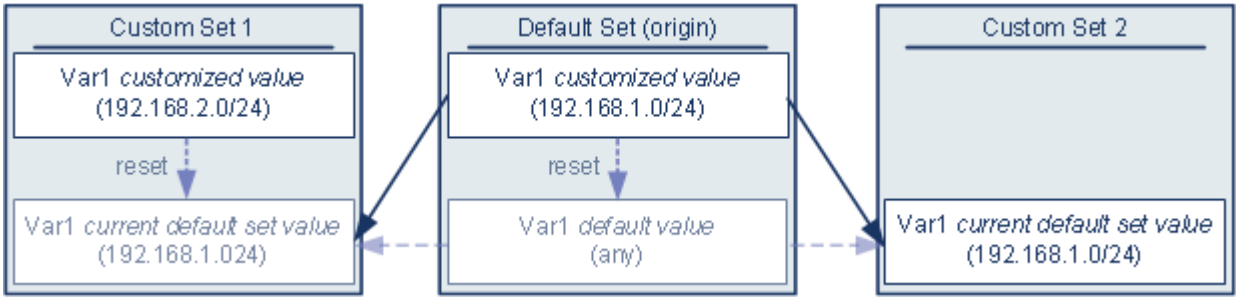
定義済みのデフォルト変数は、デフォルト値のままにすることもできますが、シスコは定義済みのデフォルトの変数の最適化（3-20 ページ）で説明されているように、定義済みの変数のサブセットを変更することを推奨します。

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。



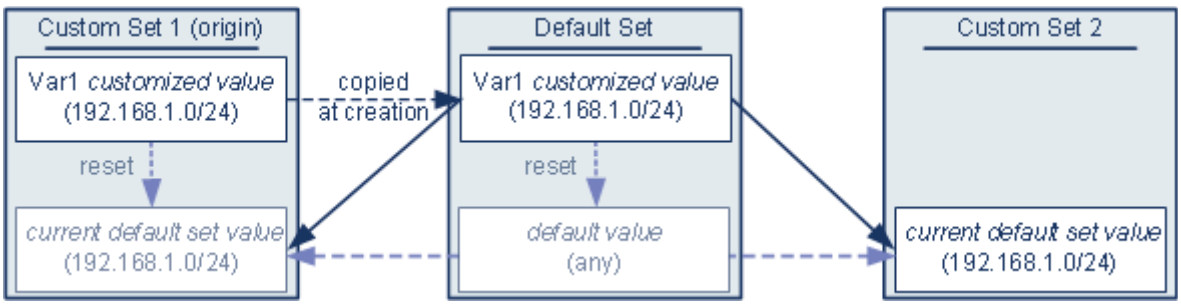
オプションで、任意のセットの `Var1` 値をカスタマイズできます。`Var1` がカスタマイズされていない Custom Set 2 では、この値は `192.168.1.0/24` です。Custom Set 1 では、`Var1` のカスタマイズ値 `192.168.2.0/24` はデフォルト値をオーバーライドします。デフォルト設定では、ユーザ定義変数をリセットすると、すべてのセットのデフォルト値が `any` にリセットされます。

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、セット間の相互作用は、ユーザ定義変数およびデフォルト変数に対して同じです。ただし、デフォルト セットのデフォルト変数をリセットした場合、デフォルト変数は、現在のルール アップデートでシスコによって設定された値にリセットされます。

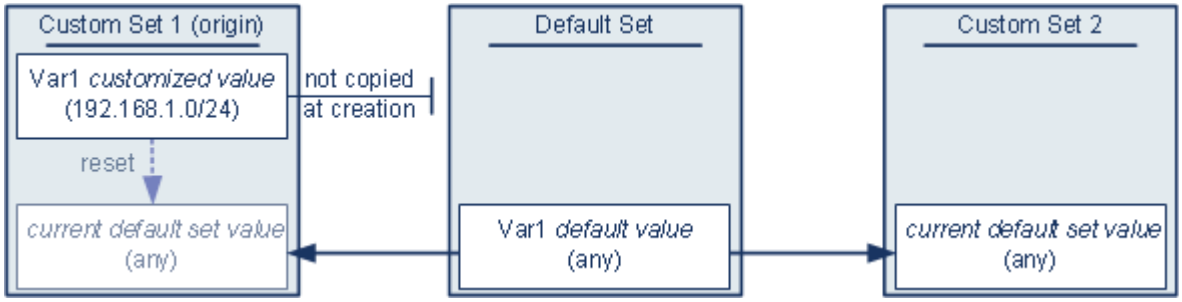
例:カスタム セットにユーザ定義変数を追加する

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（[オブジェクト（Objects）] > [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、シスコ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。

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（A-5 ページ）を参照してください。

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 3-3　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	[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] を選択し、[変数セット(Variable Sets)] 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。 **(注)** 変数セット名には、縦線(|)または中カッコ({})を除き、印字可能な任意の標準 ASCII 文字を使用できます。
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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] を選択します。

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

手順 2　[変数セット(Variable Set)] を選択します。

手順 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。変数セットの命名には、縦線(|)または中カッコ({})を除き、印字可能な任意の標準 ASCII 文字を使用できます。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(3-27 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、シスコ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 3-4　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。 **（注）** 変数セット名には、縦線（|）または中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。
変数の完全な値を表示する	変数の横にある [値（Value）] 列の値にポインタを移動します。 **（注）** 変数値には最大で 8192 文字まで格納できます。ただし、この制限は変数の拡張値のサイズに適用されることに注意してください。1 つ以上の変数を使用して別の変数を定義する場合、すべての変数値の文字やスペースの合計数は 8192 文字を超えてはいけません。
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（3-27 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（3-27 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。 **ヒント** アクティブなリセット アイコンの上にポインタを移動して、デフォルト値を表示します。

表 3-4　変数の管理アクション（続き）

目的	操作
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 [保存（Save）] 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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

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

手順 2　[変数セット（Variable Set）] を選択します。

手順 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。変数セットの命名には、縦線（|）または中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

手順 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（3-27 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（3-22 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（3-31 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（3-33 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、[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 3-5　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。 変数名では大文字と小文字が区別されるので注意してください。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(3-31 ページ)およびポート変数の操作(3-33 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	[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(3-4 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	[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(3-13 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。

表 3-5　変数の編集アクション(続き)

目的	操作
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 [保存(Save)] をクリックします。 **(注)** 変数名は一意の英数字文字列でなければなりません。この文字列では、大文字と小文字が区別され、下線文字(_)以外の特殊文字は使用できません。
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	[保存(Save)] 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(3-31 ページ)
- ポート変数の操作(3-33 ページ)

変数を追加または編集する方法:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] を選択します。

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

手順 2　[変数セット(Variable Set)] を選択します。

手順 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。変数セットの命名には、縦線(|)または中カッコ({})を除き、印字可能な任意の標準 ASCII 文字を使用できます。

手順 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。

ヒント　変数ページで、右クリックのコンテキスト メニューを使用して項目を選択または削除できます(コンテキスト メニューの使用(2-5 ページ)を参照)。

手順 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。

手順 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。

手順 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。

手順 8　[保存(Save)] 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。

手順 9　変更を終えたら、変数セットを保存するために [保存(Save)] 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(アクセス コントロール ポリシーの適用(12-17 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、ネットワーク検出ルール、イベント検索、レポートなど、システムの Web 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(3-4 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（36-5 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（32-31 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（32-34 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 ストリームのリアセンブルを改善させる必要がある、ネットワーク マップ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（30-1 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（3-4 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 です。これは「ネットワークなし」を意味します。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 ブロックが除外されます。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（3-27 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、アクセス コントロール ポリシー、ネットワーク検出ルール、イベント検索など、システムの Web インターフェイスのさまざまな場所でポート 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（3-13 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（3-13 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除外されます。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(3-27 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 3-6　　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)。

変数セット内のリセット アイコン( )の上にポインタを置くと、リセット値を確認できます。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

変数のネスト

ネストが循環でない限り変数をネストできます。ネストされ、拒否された変数はサポートされていません。

例:有効なネストされた変数

次の例では、SMTP_SERVERS、HTTP_SERVERS、および OTHER_SERVERS は有効なネストされた変数です。

表 3-7　例:有効なネストされた変数

変数	タイプ(Type)	含まれるネットワーク	除外されるネットワーク
SMTP_SERVERS	カスタマイズされたデフォルト	10.1.1.1	—
HTTP_SERVERS	カスタマイズされたデフォルト	10.1.1.2	—
OTHER_SERVERS	ユーザ定義	10.2.2.0/24	—
HOME_NET	カスタマイズされたデフォルト	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

次の例の HOME_NET は、HOME_NET のネストが循環であるため、つまり、OTHER_SERVERS の定義に HOME_NET が含まれているため、無効なネストされた変数です。HOME_NET をそれ自体にネストしています。

表 3-8　例:無効なネストされた変数

変数	タイプ(Type)	含まれるネットワーク	除外されるネットワーク
SMTP_SERVERS	カスタマイズされたデフォルト	10.1.1.1	—
HTTP_SERVERS	カスタマイズされたデフォルト	10.1.1.2	—
OTHER_SERVERS	ユーザ定義	10.2.2.0/24 HOME_NET	—
HOME_NET	カスタマイズされたデフォルト	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

ネストされ、拒否された変数はサポートされていないため、次の例に示すように、変数 NONCORE_NET を使用して、保護されたネットワークの外にある IP アドレスを表すことはできません。

表 3-9　例:サポートされないネストおよび拒否された変数

変数	タイプ(Type)	含まれるネットワーク	除外されるネットワーク
HOME_NET	カスタマイズされたデフォルト	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
EXTERNAL_NET	カスタマイズされたデフォルト	—	HOME_NET
DMZ_NET	ユーザ定義	10.4.0.0/16	—
NOTDMZ_NET	ユーザ定義	—	DMZ_NET
NONCORE_NET	ユーザ定義	EXTERNAL_NET NOTDMZ_NET	—

上記の例の代わりに、次の例に示すように、変数 NONCORE_NET を作成することにより、保護されたネットワークの外にある IP アドレスを表すことができます。

表 3-10　例:サポートされないネストおよび拒否された変数の代替

変数	タイプ(Type)	含まれるネットワーク	除外されるネットワーク
HOME_NET	カスタマイズされたデフォルト	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
DMZ_NET	ユーザ定義	10.4.0.0/16	—
NONCORE_NET	ユーザ定義	—	HOME_NET DMZ_NET

変数セットを侵入ポリシーにリンクさせる

ライセンス：Protection

デフォルトは、FireSIGHT システムは、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、[アクセス コントロール ポリシー（Access Control Policy）] ページにそのポリシーのステータスが失効として示されます。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（18-8 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、ネットワーク トラフィックに対するデフォルトの処理とインスペクションの設定（12-8 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、アクセス コントロール ポリシーの適用（12-17 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 Web 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、FireSIGHT システムには 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、Web 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。

SNORT_BPF

SNORT_BPF はレガシー拡張変数です。バージョン 5.3.0 以降にアップグレードされる前の旧バージョンの FireSIGHT システム ソフトウェア リリースのときにシステムでこの変数が設定された場合にのみ、これが表示されます。この変数を表示または削除することだけが可能です。削除後に、編集または復元することはできません。

この変数を使用すると、Berkeley Packet Filter（BPF）を適用して、システムに到達する前のトラフィックをフィルタできました。SNORT_BPF に備わっていたフィルタリング機能を今後も適用するには、この変数の代わりにアクセス コントロール ルールを使用してください。この変数は、システム アップグレード前に存在していた設定でのみ表示されます。

ファイル リストの操作

ライセンス：Malware

サポートされるデバイス：すべて（シリーズ 2 または X-シリーズ を除く）

サポートされる防御センター：DC500 を除くいずれか

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（37-20 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。

- イベント ビューアのコンテキスト メニューを使用して SHA-256 値を追加する。
- 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 リストにファイルを追加するとアクセス コントロールに影響を与えるため、ユーザは、ファイル リストのすべての側面を管理する次のいずれかを持っている必要があります。

- 管理者アクセス権
- Network Admin または Access Admin アクセス権（ファイル リストを編集する場合）、Security Approver アクセス権（アクセス コントロール ポリシーを再適用する場合）、および Security Analyst または Security Analyst（RO）アクセス権（イベント ビューから SHA-256 値を使用してファイルを追加する場合）の組み合わせ
- Modify Access Control Policy および Object Manager（ファイル リストを編集する場合）、Apply Access Control Policy（アクセス コントロール ポリシーを再適用する場合）、および Modify File Events（イベント ビューから SHA-256 値を使用してファイルを追加する場合）権限を持つカスタム ロール。カスタム ユーザ ロールによる展開の管理（12-4 ページ）を参照してください。

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。

- コンテキスト メニューの使用（2-5 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（3-39 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（3-41 ページ）
- ファイル リストに SHA-256 値を追加する（3-41 ページ）
- ファイル リスト上のファイルの変更（3-42 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（3-43 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：Malware

サポートされるデバイス：すべて（シリーズ 2 または X-シリーズ を除く）

サポートされる防御センター：DC500 を除くいずれか

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。Defense Center 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（3-43 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:

アクセス: Admin/Any Security Analyst

手順 1　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

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

手順 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。

手順 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。

手順 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。

手順 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。

手順 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。

手順 7　[保存（Save）] をクリックします。

手順 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: Malware

サポートされるデバイス:すべて(シリーズ 2 または X-シリーズ を除く)

サポートされる防御センター:DC500 を除くいずれか

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 Defense Center 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。

Defense Center 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方法:

アクセス: Admin/Network Admin

手順 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。

手順 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。

手順 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。

手順 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。

手順 5 [保存(Save)] をクリックします。

手順 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: Malware

サポートされるデバイス:すべて(シリーズ 2 または X-シリーズ を除く)

サポートされる防御センター:DC500 を除くいずれか

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。

ヒント イベント ビューからファイルまたはマルウェア イベントを右クリックし、コンテキスト メニューで [フル テキストの表示(Show Full Text)] を選択し、ファイルの SHA-256 値全体を表示してコピーします。

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:

アクセス: Admin/Network Admin

手順 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。

手順 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。

手順 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。

手順 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。

手順 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。

手順 6　[保存(Save)] をクリックします。

手順 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: Malware

サポートされるデバイス:すべて(シリーズ 2 または X-シリーズ を除く)

サポートされる防御センター:DC500 を除くいずれか

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 (3-43 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:

アクセス: Admin/Network Admin

手順 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。

手順 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。

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

手順 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。

手順 5　[保存(Save)] をクリックします。

手順 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: Malware

サポートされるデバイス: すべて(シリーズ 2 または X-シリーズ を除く)

サポートされる防御センター: DC500 を除くいずれか

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 (3-39 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:

アクセス: Admin/Network Admin

手順 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。

手順 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。

手順 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。

手順 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（Any）

*セキュリティ ゾーン*は、1 つ以上のインライン、パッシブ、スイッチド、ルーテッド、または 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 つのゾーン内のインターフェイスは、複数デバイスにまたがる場合があります。また、1 つのデバイスで複数のゾーンを設定することもできます。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、ネットワーク検出ルール、イベント検索など、システムの Web インターフェイスのさまざまな場所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 ルールを作成したり、ネットワーク検出を、特定のゾーンに送受信されるトラフィックに限定したりすることができます。

セキュリティ ゾーン オブジェクトを更新すると、システムはそのオブジェクトの新しいリビジョンを保存します。この結果、同じセキュリティ ゾーン内に、いくつかの異なるリビジョンのセキュリティ ゾーン オブジェクトを含む管理対象デバイスが存在する場合は、接続の重複と思われる項目をログに記録できます。接続の重複が報告されていることに気づいた場合、同じリビジョンのオブジェクトを使用するよう、すべての管理対象デバイスを更新できます。オブジェクト マネージャでセキュリティ ゾーンを編集して、すべての管理対象デバイスを削除し、オブジェクトを保存し、管理対象デバイスを再び追加して、オブジェクトを再び保存します。次に、影響を受けるすべてのデバイス ポリシーを再適用します。デバイス ポリシーの適用の詳細については、デバイスへの変更の適用（4-27 ページ）を参照してください。

次のいずれかの方法でセキュリティ ゾーンを作成します。

- 初期設定時にデバイスで選択した検出モードに応じて、デバイス登録時にシステムがセキュリティ ゾーンを作成します。たとえば、パッシブ展開ではシステムはパッシブ ゾーンを作成し、インライン展開では外部ゾーンと内部ゾーンを作成します。
- 管理対象デバイスでインターフェイスを設定するときに、その場でセキュリティ ゾーンを作成できます。
- オブジェクト マネージャを使用してセキュリティ ゾーンを作成できます（[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]）。

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、管理対象デバイスで設定されたゾーンがリストされます。また、このページには、各ゾーンのインターフェイスのタイプも表示され、各ゾーンを展開すると、どのデバイスのどのインターフェイスが各ゾーンに属するかを表示できます。

（注） 1 つのセキュリティ ゾーン内のすべてのインターフェイスは同じタイプ（つまり、すべてインライン、パッシブ、スイッチド、ルーテッド、または ASA）でなければなりません。さらに、セキュリティ ゾーンを作成した後、それに含まれるインターフェイスのタイプを変更することはできません。

ASA セキュリティ コンテキストを変更して、シングル コンテキスト モードからマルチコンテキスト モード（またはその逆）に切り替えると、セキュリティ ゾーンの設定からすべてのインターフェイスが削除されます。

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、インターフェイスが存在するデバイスに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 ポリシーおよびネットワーク検出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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

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

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

手順 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。

手順 4　[名前（Name）] に、ゾーンの名前を入力します。中カッコ（{}）、縦線（|）、セミコロン（;）、ポンド記号（#）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

手順 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。

手順 6　[デバイス（Device）] > [インターフェイス（Interfaces）] ドロップダウン リストから、ゾーンに追加するインターフェイスを含んでいるデバイスを選択します。

手順 7　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。管理対象デバイスで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 10 に進みます。

手順 8　[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。

手順 9　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。

手順 10　[保存（Save）] 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（Any）

サポートされるデバイス: シリーズ 3

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)　Web 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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] を選択します。

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

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

手順 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。

手順 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。

手順 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。

手順 6　[保存(Save)] 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(Any)

サポートされるデバイス: シリーズ 3

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 (3-2 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 3-11　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 3-12　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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] を選択します。

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

手順 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。

手順 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。

手順 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。

手順 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 3-11(3-47 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。

手順 6　[保存(Save)] 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(Any)

サポートされるデバイス:シリーズ 3

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)　Defense Center および管理対象デバイスは、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、保存前にランダムに生成されたキー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（3-49 ページ）
- 信頼できる認証局オブジェクトの使用（3-54 ページ）
- 外部証明書オブジェクトの使用（3-56 ページ）
- 内部証明書オブジェクトの使用（3-57 ページ）

内部認証局オブジェクトの使用

ライセンス：任意（Any）

サポートされるデバイス：シリーズ 3

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（3-2 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（3-50 ページ）
- 新しい CA 証明書と秘密キーの生成（3-51 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（3-52 ページ）
- CA 証明書と秘密キーのダウンロード（3-53 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（Any）

サポートされるデバイス：シリーズ 3

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（Decrypt）] アクション：さらに検査するためにトラフィックを復号（21-11 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：

アクセス：Admin/Access Admin/Network Admin

手順 1　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

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

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

手順 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。

手順 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。

手順 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。

手順 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。

手順 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。

手順 8　[保存（Save）] 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（Any）

サポートされるデバイス: シリーズ 3

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 3-13　生成される内部 CA の属性

フィールド	使用可能な値	必須（Required）
国名（Country Name）（2 文字コード）	2 つの英字	Yes
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	No
市区町村（Locality or City）		
Organization		
組織		
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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

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

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

手順 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。

手順 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。

手順 5　表 3-13（3-51 ページ）の説明に従って、識別属性を入力します。

手順 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（Any）

サポートされるデバイス: シリーズ 3

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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

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

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

手順 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。

手順 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。

手順 5　表 3-13（3-51 ページ）の説明に従って、識別属性を入力します。

手順 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。

手順 7　CA に送信するために CSR をコピーします。

手順 8　[OK] 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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

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

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

手順 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。

手順 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。

手順 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。

手順 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。

手順 7　[保存（Save）] 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（Any）

サポートされるデバイス：シリーズ 3

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（70-2 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：

アクセス：Admin/Access Admin/Network Admin

手順 1　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

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

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

手順 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。

手順 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。

手順 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。

手順 6　[OK] 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(Any)

サポートされるデバイス: シリーズ 3

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(3-2 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。

- 信頼できる CA オブジェクトの追加(3-54 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(3-55 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(Any)

サポートされるデバイス: シリーズ 3

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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] を選択します。

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

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

手順 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。

手順 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。

手順 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。

手順 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。

手順 7　[OK] 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(Any)

サポートされるデバイス: シリーズ 3

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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] を選択します。

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

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

手順 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。

手順 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。

手順 5　[OK] 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（Any）

サポートされるデバイス：シリーズ 3

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（3-2 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：

アクセス：Admin/Access Admin/Network Admin

手順 1　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

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

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

手順 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。

手順 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。

手順 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。

手順 6　[保存（Save）] 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（Any）

サポートされるデバイス：シリーズ 3

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（3-2 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：

アクセス：Admin/Access Admin/Network Admin

手順 1　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

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

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

手順 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。

手順 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。

手順 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。

手順 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。

手順 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。

手順 8　[保存(Save)] 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。

地理位置情報オブジェクトの操作

ライセンス: FireSIGHT

サポートされるデバイス: シリーズ 3、仮想、ASA FirePOWER

サポートされる防御センター: すべて(DC500 を除く)

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。アクセス コントロール ポリシー、SSL ポリシー、イベント検索など、システムの Web インターフェイスのさまざまな場所で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(15-4 ページ)を参照してください。地理的な場所による暗号化トラフィックのフィルタリングの詳細については、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(22-4 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(66-32 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:

アクセス: Admin/Access Admin/Network Admin

手順 1　[オブジェクト(Objects)] > [オブジェクト管理(Object Management)] を選択します。

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

手順 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。

手順 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。

手順 4　[名前(Name)] に、位置情報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。

手順 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。

手順 6　[保存(Save)] 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。