CHAPTER 8

グローバル オブジェクトの追加

[Objects] ペインでは、セキュリティ アプライアンスにポリシーを組み込む際に不可欠な再利用コンポーネントの設定、表示、修正がすべてできます。たとえば、セキュリティ ポリシーの対象ホストやネットワークを定義すると、ホストやネットワークを選択するだけで機能を適用でき、適用対象を何度も定義する必要がなくなります。そのため、時間を短縮できると同時に、一貫性のあるセキュリティ ポリシーを高い精度で実現できます。ホストやネットワークの追加、削除が必要な場合、[Objects] ペインを利用して 1 箇所から変更できます。

この章は、次の項で構成されています。

ネットワーク オブジェクトおよびグループの使用

この項では、ネットワーク オブジェクトおよびグループの使用方法について説明します。次の項目を取り上げます。

ネットワーク オブジェクトの概要

ネットワーク オブジェクトを使用すると、ホストおよびネットワークの IP アドレスを事前に定義して、以降の設定を効率よく行えます。アクセス ルールや AAA ルールなどのセキュリティ ポリシーを設定すると、手動で入力する代わりに事前定義済みのアドレスを選択できます。さらに、オブジェクトの定義を変更した場合、変更内容は自動的にそのオブジェクトを使用するすべてのルールに継承されます。

ネットワーク オブジェクトは手動で追加できます。または、ASDM にアクセス ルールや AAA ルールのような既存のコンフィギュレーションからオブジェクトを自動的に作成させることもできます。このような派生したオブジェクトのいずれかを編集した場合、後でそのオブジェクトを使用していたルールを削除してもその編集内容は残ります。編集しない場合、リフレッシュすると、派生したオブジェクトには現在のコンフィギュレーションが反映されるだけです。

ネットワーク オブジェクト グループは、複数のホストとネットワークが一緒に含まれるグループです。ネットワーク オブジェクト グループには、他のネットワーク オブジェクト グループを含めることもできます。このため、ネットワーク オブジェクト グループを送信元アドレスまたは宛先アドレスとしてアクセス ルールに指定できます。

ルールの設定時に、[ASDM] ウィンドウの右側には [Addresses] サイド ペインがあり、使用可能なネットワーク オブジェクトとネットワーク オブジェクト グループが表示されます。[Addresses] ペインで直接オブジェクトを追加、編集、または削除できます。また、追加するネットワーク オブジェクトおよびグループを [Addresses] ペインから選択したアクセス ルールの送信元または宛先にドラッグできます。

ネットワーク オブジェクトの設定

ネットワーク オブジェクトを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Network Objects/Group] ペインで、[Add] > [Network Object] をクリックして新しいオブジェクト グループを追加するか、オブジェクトを選択して [Edit] をクリックします。

ルール ウィンドウの [Addresses] サイド ペインで、またはルールの追加時に、ネットワーク オブジェクトを追加または編集することもできます。

リスト内のオブジェクトを検索するには、[Filter] フィールドに名前または IP アドレスを入力して [Filter] をクリックします。ワイルドカード文字としてアスタリスク（*）や疑問符（?）を使用できます。

[Add/Edit Network Object] ダイアログボックスが表示されます。

ステップ 2　次の値を入力します。

- [Name] :（任意）オブジェクト名。使用できる文字は、a ～ z、A ～ Z、0 ～ 9、ドット（.）、ダッシュ（-）、およびアンダースコア（_）です。名前は 64 文字以下にする必要があります。
- [IP Address] : IP アドレス（ホストまたはネットワーク アドレス）。
- [Netmask] : IP アドレスのサブネット マスク。
- [Description] :（任意）ネットワーク オブジェクトの説明。

ステップ 3　[OK] をクリックします。

これでルールの作成時にこのネットワーク オブジェクトを使用できます。編集したオブジェクトの場合、変更内容は自動的にそのオブジェクトを使用するすべてのルールに継承されます。

（注）　使用中のネットワーク オブジェクトは削除できません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ネットワーク オブジェクト グループの設定

ネットワーク オブジェクト グループを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Network Objects/Group] ペインで、[Add] > [Network Object Group] をクリックして新しいオブジェクト グループを追加するか、オブジェクト グループを選択して [Edit] をクリックします。

ルール ウィンドウの [Addresses] サイド ペインで、またはルールの追加時に、ネットワーク オブジェクト グループを追加または編集できます。

リスト内のオブジェクトを検索するには、[Filter] フィールドに名前または IP アドレスを入力して [Filter] をクリックします。ワイルドカード文字としてアスタリスク（*）や疑問符（?）を使用できます。

[Add/Edit Network Object Group] ダイアログボックスが表示されます。

ステップ 2　[Group Name] フィールドで、グループ名を入力します。

使用できる文字は、a ～ z、A ～ Z、0 ～ 9、ドット（.）、ダッシュ（-）、およびアンダースコア（_）です。名前は 64 文字以下にする必要があります。

ステップ 3　（任意）[Description] フィールドで、説明を長さ 200 文字以内で入力します。

ステップ 4　既存のオブジェクトまたはグループを新しいグループに追加したり（グループのネストが可能）、新しいアドレスを作成してグループに追加したりできます。

- 既存のネットワーク オブジェクトまたはグループを新しいグループに追加するには、[Existing Network Objects/Groups] ペインでオブジェクトをダブルクリックします。

  または、オブジェクトを選択して、[Add] をクリックします。オブジェクトまたはグループが右側の [Members in Group] ペインに追加されます。
- 新しいアドレスを追加するには、[Create New Network Object Member] 領域で値を入力し、[Add] をクリックします。

  オブジェクトまたはグループが右側の [Members in Group] ペインに追加されます。このアドレスはネットワーク オブジェクト リストにも追加されます。

オブジェクトを削除するには、[Members in Group] ペインでオブジェクトをダブルクリックするか、[Remove] をクリックします。

ステップ 5　すべてのメンバ オブジェクトを追加し終えたら、[OK] をクリックします。

これでルールの作成時にこのネットワーク オブジェクト グループを使用できます。編集したオブジェクト グループの場合、変更内容は自動的にそのグループを使用するすべてのルールに継承されます。

（注）　使用中のネットワーク オブジェクト グループは削除できません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ルールでのネットワーク オブジェクトおよびグループの使用

ルールの作成時には、手動で IP アドレスを入力したり、ルールで使用するネットワーク オブジェクトまたはグループを参照したりできます。

（注）　アクセス ルールのみの場合は、ネットワーク オブジェクトおよびグループを [Addresses] ペインから選択したアクセス ルールの送信元または宛先にドラッグ アンド ドロップできます。

ルールでネットワーク オブジェクトまたはグループを使用するには、次の手順を実行します。

ステップ 1　ルール ダイアログボックスで、送信元または宛先のアドレス フィールドの横にある [...] 参照ボタンをクリックします。

[Browse Source Address] または [Browse Destination Address] ダイアログボックスが表示されます。

ステップ 2　新しいネットワーク オブジェクトまたはグループを追加したり、既存のネットワーク オブジェクトまたはグループをダブルクリックして選択したりできます。

リスト内のオブジェクトを検索するには、[Filter] フィールドに名前または IP アドレスを入力して [Filter] をクリックします。ワイルドカード文字としてアスタリスク（*）や疑問符（?）を使用できます。

- 新しいネットワーク オブジェクトを追加する方法について、「ネットワーク オブジェクトの設定」（P.8-2）を参照してください。
- 新しいネットワーク オブジェクト グループを追加する方法については、「ネットワーク オブジェクト グループの設定」（P.8-3）を参照してください。

新しいオブジェクトを追加するか、既存のオブジェクトをダブルクリックすると、そのオブジェクトが [Selected Source/Destination] フィールドに表示されます。アクセス ルールの場合、このフィールドに複数のオブジェクトをカンマで区切って入力できます。

ステップ 3　[OK] をクリックします。

ルール ダイアログボックスに戻ります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ネットワーク オブジェクトまたはグループの使用状況の表示

ネットワーク オブジェクトまたはグループを使用しているルールを表示するには、[Configuration] > [Firewall] > [Objects] > [Network Objects/Group] ペインで拡大鏡の形をした [Find] アイコンをクリックします。

[Usages] ダイアログボックスが表示され、現在ネットワーク オブジェクトまたはグループを使用しているすべてのルールが一覧表示されます。このダイアログボックスには、そのオブジェクトが含まれるネットワーク オブジェクト グループもすべて一覧表示されます。

サービス グループの設定

この項では、サービス グループを設定する方法について説明します。説明する内容は次のとおりです。

- 「Service Groups」（P.8-5）
- 「Add/Edit Service Group」（P.8-6）
- 「Browse Service Groups」（P.8-7）

Service Groups

[Service Groups] ペインでは、指定したグループに複数のサービスを関連付けられます。1 つのグループに任意のタイプのプロトコルとサービスを指定できます。または、次のタイプごとにサービス グループを作成できます。

- TCP ポート
- UDP ポート
- TCP-UDP ポート
- ICMP タイプ
- IP プロトコル

複数のサービス グループをネストすれば、「グループのグループ」を構成できます。「グループのグループ」は 1 つのグループとして使用できます。

サービス グループは、ポート、ICMP タイプ、プロトコルを識別する必要がある多くのコンフィギュレーションで使用できます。NAT ルールやセキュリティ ポリシー ルールの設定時に、[ASDM] ウィンドウの右側の [Services] ペインにもサービス グループやその他の使用可能なグローバル オブジェクトが表示されます。この [Services] ペインから直接オブジェクトを追加、編集、削除できます。

フィールド

- [Add]：サービス グループを追加します。追加するサービス グループのタイプをドロップダウンリストから選択します。複数タイプの場合は [Service Group] を選択します。
- [Edit]：サービス グループを編集します。
- [Delete]：サービス グループを削除します。サービス グループを削除すると、使用されているすべてのサービス グループから削除されます。サービス グループがアクセス ルールで使用されている場合は、削除しないでください。アクセス ルールで使用されているサービス グループを空にはできません。
- [Find]：一致する名前だけを表示するように、表示内容をフィルタリングします。[Find] をクリックすると、[Filter]フィールドが開きます。もう一度 [Find] をクリックすると、[Filter] フィールドは非表示になります。
  - [Filter field]：サービス グループの名前を入力します。ワイルドカード文字としてアスタリスク（*）や疑問符（?）を使用できます。
  - [Filter]：フィルタを実行します。
  - [Clear]：[Filter] フィールドをクリアします。
- [Name]：サービス グループ名を一覧表示します。名前の隣にあるプラス（[+]）アイコンをクリックすると、サービス グループが展開され、サービスを確認できます。マイナス（[-]）アイコンをクリックすると、サービス グループが折りたたまれます。
- [Protocol]：サービス グループ プロトコルを一覧表示します。
- [Source Ports]：プロトコルの送信元ポートを一覧表示します。
- [Destination Ports]：プロトコルの宛先ポートを一覧表示します。
- [ICMP Type]：サービス グループの ICMP タイプを一覧表示します。
- [Description]：サービス グループの説明を一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Service Group

[Add/Edit Service Group] ダイアログボックスでは、サービスをサービス グループに割り当てられます。このダイアログボックス名は追加するサービス グループのタイプと同じ名前になります。たとえば、追加するサービス グループが TCP の場合、[Add/Edit TCP Service Group] ダイアログボックスが表示されます。

フィールド

- [Group Name]：グループ名を 64 文字以内で入力します。名前は、すべてのオブジェクト グループで一意であることが必要です。サービス グループの名前にネットワーク オブジェクト グループで使用した名前は使用できません。
- [Description]：サービス グループの説明を 200 文字以内で入力します。
- [Existing Service/Service Group]：サービス グループに追加可能な項目を示します。定義済みのサービス グループから選択するか、よく使用されるポート、タイプ、プロトコルの名前のリストから選択します。
  - [Service Groups]：このテーブルのタイトルは、追加するサービス グループのタイプによって異なります。定義済みサービス グループが含まれます。
  - [Predefined]：事前定義済みのポート、タイプ、またはプロトコルを一覧表示します。
- [Create new member]：新しいサービス グループ メンバを作成できます。
  - [Service Type]：新しいサービス グループ メンバのサービス タイプを選択できます。サービス タイプには、TCP、UDP、TCP-UDP、ICMP、および protocol があります。
  - [Destination Port/Range]：新しい TCP、UDP、または TCP-UDP サービス グループ メンバの宛先ポートまたは範囲を入力できます。
  - [Source Port/Range]：新しい TCP、UDP、または TCP-UDP サービス グループ メンバの送信元ポートまたは範囲を入力できます。
  - [ICMP Type]：新しい ICMP サービス グループ メンバの ICMP タイプを入力できます。
  - [Protocol]：新しい protocol サービス グループ メンバのプロトコルを入力できます。
- [Members in Group]：サービス グループに追加済みのアイテムを示します。
- [Add]：選択したアイテムをサービス グループに追加します。
- [Remove]：選択したアイテムをサービス グループから削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Browse Service Groups

[Browse Service Groups] ダイアログボックスでは、サービス グループを選択できます。このダイアログボックスはさまざまなコンフィギュレーション画面で使用され、その時のタスクに該当する名前で表示されます。たとえば、[Add/Edit Access Rule] ダイアログボックスから使用した場合、このダイアログボックス名は [Browse Source Port] または [Browse Destination Port] になります。

フィールド

- [Add]：サービス グループを追加します。
- [Edit]：選択したサービス グループを編集します。

- [Delete]：選択したサービス グループを削除します。
- [Find]：一致する名前だけを表示するように、表示内容をフィルタリングします。[Find] をクリックすると、[Filter] フィールドが開きます。もう一度 [Find] をクリックすると、[Filter] フィールドは非表示になります。
  - [Filter field]：サービス グループの名前を入力します。ワイルドカード文字としてアスタリスク（*）や疑問符（?）を使用できます。
  - [Filter]：フィルタを実行します。
  - [Clear]：[Filter] フィールドをクリアします。
- [Type]：TCP、UDP、TCP-UDP、ICMP、Protocol など、表示するサービス グループのタイプを選択できます。タイプをすべて表示するには、[All] を選択します。通常、ルールのタイプを設定する場合、使用できるサービス グループのタイプは 1 つだけです。TCP のアクセス ルールに UDP のサービス グループは選択できません。
- [Name]：サービス グループ名を示します。アイテムの名前の隣にあるプラス（[+]）アイコンをクリックすると、アイテムが展開されます。マイナス（[-]）アイコンをクリックすると、アイテムが折りたたまれます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

クラス マップの設定

クラス マップの詳細については、「クラス マップのフィールドの説明」（P.24-40）を参照してください。

インスペクション マップの設定

インスペクション マップの詳細については、「インスペクション マップのフィールドの説明」（P.24-61）を参照してください。

正規表現の設定

この項では、正規表現を設定する方法について説明します。説明する内容は次のとおりです。

- 「Add/Edit Regular Expression Class Map」（P.8-14）

正規表現

「クラス マップの設定」や「インスペクション マップの設定」の一部で、パケット内のテキストを照合する正規表現を指定できます。正規表現のクラス マップ内に単独またはグループのいずれかで作成する場合でも、クラス マップまたはインスペクション マップを設定する前に、必ず正規表現を作成してください。

正規表現は、ストリングそのものとしてテキスト ストリングと文字どおりに照合することも、*metacharacters* を使用してテキスト ストリングの複数のバリアントと照合することもできます。正規表現を使用して、特定のアプリケーション トラフィックの内容（HTTP パケット内の本文テキストなど）を照合できます。

フィールド

- [Regular Expressions]：正規表現を示します。
  - [Name]：正規表現の名前を示します。
  - [Value]：正規表現の定義値を示します。
  - [Add]：正規表現を追加します。
  - [Edit]：正規表現を編集します。
  - [Delete]：正規表現を削除します。
- [Regular Expression Classes]：正規表現クラス マップを示します。
  - [Name]：正規表現クラス マップの名前を示します。
  - [Match Conditions]：クラス マップの照合タイプと正規表現を示します。

    [Match Type]：照合タイプを示します。正規表現の場合、常に基準の肯定一致タイプ（等号（=）を表示したアイコン）になります。また、インスペクション クラス マップで否定一致（赤丸を表示したアイコン）の作成もできます。クラス マップに正規表現が複数ある場合は、照合タイプ アイコンの隣にそれぞれ「OR」を表示し、「match any」クラス マップになっていることを示します。正規表現のいずれか 1 つと一致するだけで、トラフィックがクラス マップに一致します。

    [Regular Expression]：クラス マップごとに登録されている正規表現を一覧表示します。
  - [Description]：クラス マップの説明を示します。
  - [Add]：正規表現クラス マップを追加します。
  - [Edit]：正規表現クラス マップを編集します。
  - [Delete]：正規表現クラス マップを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Regular Expression

[Add/Edit Regular Expression] ダイアログボックスでは、正規表現を定義しテストできます。

フィールド

- [Name]：正規表現の名前を 40 文字以内で入力します。
- [Value]：正規表現を 100 文字以内で入力します。表 8-1 に示すメタ文字を使用するか、または [Build] をクリックし、Build Regular Expression のダイアログボックスを利用してテキストを手動で入力します。

（注） 最適化のために、セキュリティ アプライアンスでは、難読化解除された URL が検索されます。難読化解除では、複数のスラッシュ（/）が単一のスラッシュに圧縮されます。「http://」などの、一般的に 2 つのスラッシュが使用されるストリングでは、代わりに「http:/」を検索してください。

表 8-1 に、特別な意味を持つメタ文字の一覧を示します。

表 8-1　regex メタ文字

文字	説明	注意事項
.	ドット	任意の単一文字と一致します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
(*exp*)	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、**d(o|a)g** は dog および dag に一致しますが、**do|ag** は do および ag に一致します。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、**dog|cat** は、dog または cat に一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。たとえば、**lo?se** は、lse または lose に一致します。 **（注）** Ctrl+V を入力してから疑問符を入力しないと、ヘルプ機能が呼び出されます。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示す修飾子。たとえば、**lo*se** は lse、lose、loose、などと一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示す修飾子。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
{*x*} または {*x*,}	最小繰り返し限定作用素	少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
[*abc*]	文字クラス	カッコ内の任意の文字と一致します。たとえば、**[abc]** は、a、b、または c に一致します。

表 8-1　regex メタ文字 （続き）

文字	説明	注意事項
[^*abc*]	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、**[^abc]** は、a、b、c 以外の任意の文字に一致します。**[^A-Z]** は、大文字のアルファベット文字以外の任意の単一の文字に一致します。
[*a-c*]	文字範囲クラス	範囲内の任意の文字と一致します。**[a-z]** は、任意の小文字のアルファベット文字に一致します。文字と範囲を組み合わせて使用することもできます。**[abcq-z]** および **[a-cq-z]** は、a、b、c、q、r、s、t、u、v、w、x、y、z に一致します。 ダッシュ（-）文字は、角カッコ内の最初の文字または最後の文字である場合にのみリテラルとなります（**[abc-]** や **[-abc]**）。
""	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、**" test"** は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
\	エスケープ文字	メタ文字とともに使用すると、リテラル文字と一致します。たとえば、**\[** は左角カッコに一致します。
char	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	Tab	タブ 0x09 と一致します。
\f	改ページ	フォーム フィード 0x0c と一致します。
\x*NN*	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
NNN	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 040 はスペースを表します。

- [Build]：Build Regular Expression のダイアログボックスを利用して正規表現を作成できます。
- [Test]：正規表現を適切なサンプル テキストでテストします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Build Regular Expression

[Build Regular Expression] ダイアログボックスでは、文字やメタ文字を構成して正規表現を作成できます。メタ文字の挿入フィールドでは、カッコで囲まれたメタ文字がフィールド名に表示されます。

（注） 最適化のために、セキュリティ アプライアンスでは、難読化解除された URL が検索されます。難読化解除では、複数のスラッシュ（/）が単一のスラッシュに圧縮されます。「http://」などの、一般的に 2 つのスラッシュが使用されるストリングでは、代わりに「http:/」を検索してください。

フィールド

[Build Snippet]：このエリアで、正規表現テキストの部分式を作成したり、メタ文字を [Regular Expression] フィールドに挿入したりできます。

- [Starts at the beginning of the line (^)]：部分式は行頭から開始し、開始場所はメタ文字のカレット（^）で示します。このオプションを使用して作成した部分式は、正規表現の先頭に挿入してください。
- [Specify Character String]：テキスト文字列を手動で入力します。
  - [Character String]：テキスト文字列を入力します。
  - [Escape Special Characters]：テキスト文字列に入力したメタ文字を文字そのものとして扱う場合、このボックスをオンにすると、メタ文字の前にエスケープ文字であるバックスラッシュ（\）が追加されます。たとえば、「example.com」と入力すると「example\.com」に変換されます。
  - [Ignore Case]：大文字と小文字を両方とも照合する場合、このチェックボックスをオンにすると、両方を照合するテキストが自動的に追加されます。たとえば、「cats」と入力すると「[cC][aA][tT][sS]」に変換されます。
- [Specify Character]：正規表現に挿入するメタ文字を指定します。
  - [Negate the character]：識別した文字を照合の対象外に指定します。
  - [Any character (.)]：すべての文字と一致させる、メタ文字のピリオド（.）を挿入します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
  - [Character set]：文字セットを挿入します。テキストをこのセットに含まれるすべての文字と照合します。次のようなセットがあります。

    [0-9A-Za-z]

    [0-9]

    [A-Z]

    [a-z]

    [aeiou]

    [\n\f\r\t]（改行、改ページ、復帰、タブを示す）

    たとえば、[0-9A-Za-z] の場合、部分式は 0 ～ 9 の数字と A ～ Z の大文字および小文字と照合します。
  - [Special character]：エスケープが必要な文字 \、?、*、+、|、.、[、(、^ を挿入します。エスケープ文字はバックスラッシュ（\）で、このオプションを選択すると自動的に入力されます。
  - [Whitespace character]：空白スペースには \n（改行）、\f（改ページ）、\r（復帰）、\t（タブ）があります。

  - [Three digit octal number]：8 進数を使用する ASCII 文字（3 桁まで）と一致します。たとえば、\040 はスペースを意味します。バックスラッシュ（\）は自動的に入力されます。
  - [Two digit hexadecimal number]：16 進数を使用する ASCII 文字（2 桁まで）と一致します。バックスラッシュ（\）は自動的に入力されます。
  - [Specified character]：任意の 1 文字を入力します。
- [Snippet Preview]：*表示専用*。正規表現に入力される部分式を示します。
- [Append Snippet]：部分式を正規表現の最後に追加します。
- [Append Snippet as Alternate]：部分式をパイプ記号（|）で区切って、正規表現の最後に追加します。区切られた表現の一方と照合します。たとえば、**dog|cat** は、dog または cat に一致します。
- [Insert Snippet at Cursor]：部分式をカーソル位置に挿入します。

[Regular Expression]：このエリアには、手動で入力して部分式で作成できる正規表現テキストが含まれます。その後、[Regular Expression] フィールドのテキストを選択して、選択部分に数量詞を適用できます。

- [Selection Occurrences]：[Regular Expression] フィールドのテキストを選択し、次のいずれかのオプションをクリックしてから [Apply to Selection] をクリックします。たとえば、正規表現「test me」の「me」を選択して [One or more times] を適用すると、この正規表現は「test (me)+」になります。
  - [Zero or one times (?)]：この記号よりも前の表現が 0 または 1 つあることを示す数量詞です。たとえば、**lo?se** は、lse または lose に一致します。
  - [One or more times (+)]：この記号よりも前の表現が少なくとも 1 つあることを示す数量詞です。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
  - [Any number of times (*)]：この記号よりも前の表現が 0、1、またはそれ以上あることを示す数量詞です。たとえば、**lo*se** は lse、lose、loose、などと一致します。
  - [At least]：少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は abxyxyz、abxyxyxyz などと一致します。
  - [Exactly]：*x* 回だけ繰り返します。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
  - [Apply to Selection]：数量詞を選択部分に適用します。
- [Test]：正規表現を適切なサンプル テキストでテストします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Test Regular Expression

[Test Regular Expression] ダイアログボックスでは、入力テキストを正規表現でテストし、意図したとおりに一致するかどうかを確認できます。

フィールド

- [Regular Expression]：テストする正規表現を入力します。デフォルトでは、Add/Edit Regular Expression または Build Regular Expression ダイアログボックスで入力した正規表現が、このフィールドに入力されます。テスト中に正規表現を変更した場合、[OK] をクリックすると [Add/Edit Regular Expression] や [Build Regular Expression] ダイアログボックスにその変更内容が継承されます。[Cancel] をクリックすると、変更内容は失われます。
- [Test String]：正規表現で一致すると想定されたテキスト文字列を入力します。
- [Test]：[Text String] のテキスト文字列を [Regular Expression] の正規表現でテストします。
- [Test Result]：*表示専用*。テストの成功 / 失敗を示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Regular Expression Class Map

[Add/Edit Regular Expression Class Map] ダイアログボックスで、正規表現をグループ化します。正規表現クラス マップは、インスペクション クラス マップとインスペクション ポリシー マップで使用できます。

フィールド

- [Name]：クラス マップの名前を 40 文字以内で入力します。「class-default」という名前は予約されています。すべてのタイプのクラス マップで同じ名前スペースが使用されるため、別のタイプのクラス マップですでに使用されている名前は再度使用できません。
- [Description]：説明を 200 文字以内で入力します。
- [Available Regular Expressions]：クラス マップに割り当てられていない正規表現を一覧表示します。
  - [Edit]：選択した正規表現を編集します。
  - [New]：新しい正規表現を作成します。
- [Add]：選択した正規表現をクラス マップに追加します。
- [Remove]：選択した正規表現をクラス マップから削除します。
- [Configured Match Conditions]：クラス マップの正規表現を照合タイプとともに示します。
  - [Match Type]：照合タイプを示します。正規表現の場合、常に基準の肯定一致タイプ（等号（=）を表示したアイコン）になります。また、インスペクション クラス マップで否定一致（赤丸を表示したアイコン）の作成もできます。クラス マップに正規表現が複数ある場合は、照合タイプ アイコンの隣にそれぞれ「OR」を表示し、「match any」クラス マップになっていることを示します。正規表現のいずれか 1 つと一致するだけで、トラフィックがクラス マップに一致します。
  - [Regular Expression]：このクラス マップに含まれている正規表現の名前を一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

TCP マップの設定

TCP マップの詳細については、「接続設定と TCP 正規化のイネーブル化」（P.27-8）を参照してください。

グローバル プールの設定

グローバル プールの詳細については、「ダイナミック NAT の使用」（P.25-18）を参照してください。

時間範囲の設定

[Time Ranges] オプションで開始時間と終了時間を定義する再利用コンポーネントを作成し、さまざまなセキュリティ機能に適用します。時間範囲を 1 回だけ定義すれば、後は時間範囲を選択して、スケジューリングが必要なさまざまなオプションに適用できます。

時間範囲機能を使用して時間の範囲を定義し、トラフィックのルールやアクションに使用できます。たとえば、アクセス リストに時間範囲を設定すると、セキュリティ アプライアンスのアクセスを制限できます。

時間範囲は、開始時間、終了時間、およびオプションの繰り返しエントリで構成されます。

（注） 時間範囲を作成してもデバイスへのアクセスは制限されません。このペインでは時間範囲だけを定義します。

フィールド

- [Name]：時間範囲の名前を指定します。
- [Start Time]：時間範囲の開始時刻を指定します。
- [End Time]：時間範囲の終了時刻を指定します。
- [Recurring Entries]：指定した開始時刻と停止時刻の範囲内でアクティブな時間の追加制限を指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Time Rnage

[Add/Edit Time Range] ペインでは、特定の日付と時刻を定義し、アクションに設定できます。たとえば、アクセス リストに時間範囲を設定すると、セキュリティ アプライアンスのアクセスを制限できます。時間範囲はセキュリティ アプライアンスのシステム クロックに依存しています。ただし、この機能は、NTP 同期化により最適に動作します。

（注） 時間範囲を作成してもデバイスへのアクセスは制限されません。このペインでは時間範囲だけを定義します。

フィールド

- [Time Range Name]：時間範囲の名前を指定します。スペースや引用符は使用できません。また、先頭にはアルファベットか数字を使用します。
- [Start now/Started]：時間範囲がただちに開始するか、または時間範囲がすでに始まっているかを指定します。このボタンのラベルは、追加/編集する時間範囲の設定状態によって変わります。時間範囲を新規追加する場合または固定の開始時間が定義された時間範囲を編集する場合、ボタンは [Start Now] になります。開始時間が非固定の時間範囲を編集する場合は、ボタンが [Started] になります。
- [Start Time]：時間範囲の開始時刻を指定します。
  - [Month]：月を 1 月～ 12 月の範囲で指定します。
  - [Day]：日を 01 ～ 31 の範囲で指定します。
  - [Year]：年を 1993 ～ 2035 の範囲で指定します。
  - [Hour]：時間を 00 ～ 23 の範囲で指定します。
  - [Minute]：分を 00 ～ 59 の範囲で指定します。
- [Never end]：時間範囲が終了しない場合に指定します。
- [End at (inclusive)]：時間範囲の終了時刻を指定します。指定した終了時刻も範囲に含まれます。たとえば、指定した時間範囲が 11:30 で終了する場合、11 時 30 分 59 秒まで有効です。この場合、時間範囲は 11:31 になったとき終了します。
  - [Month]：月を 1 月～ 12 月の範囲で指定します。
  - [Day]：日を 01 ～ 31 の範囲で指定します。
  - [Year]：年を 1993 ～ 2035 の範囲で指定します。
  - [Hour]：時間を 00 ～ 23 の範囲で指定します。
  - [Minute]：分を 00 ～ 59 の範囲で指定します。

- [Recurring Time Ranges]：時間範囲を日単位または週単位で設定します。
  - [Add]：繰り返し時間範囲を追加します。
  - [Edit]：選択した繰り返し時間範囲を編集します。
  - [Delete]：選択した繰り返し時間範囲を削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Recurring Time Range

[Add/Edit Recurring Time Range] ペインでは、日単位または週単位で時間範囲を詳細に指定できます。

（注）　時間範囲を作成してもデバイスへのアクセスは制限されません。このペインでは時間範囲だけを定義します。

フィールド

- Days of the week
  - [Every day]：週の毎日を指定します。
  - [Weekdays]：月曜日～金曜日を指定します。
  - [Weekends]：土曜日と日曜日を指定します。
  - [On these days of the week]：特定の曜日を指定します。
  - [Daily Start Time]：時間範囲が開始する時間と分を指定します。
  - [Daily End Time (inclusive)] エリア：時間範囲が終了する時間と分を指定します。指定した終了時刻も範囲に含まれます。
- Weekly Interval
  - [From]：月曜日～日曜日までの曜日を一覧表示します。
  - [Through]：月曜日～日曜日までの曜日を一覧表示します。
  - [Hour]：時間を 00 ～ 23 の範囲で一覧表示します。
  - [Minute]：分を 00 ～ 59 の範囲で一覧表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

暗号化トラフィック インスペクション

この項では、暗号化トラフィック インスペクションを設定する方法について説明します。説明する内容は次のとおりです。

TLS プロキシ

[TLS Proxy] オプションを使用して、Cisco CallManager と対話する SSL 暗号化 VoIP シグナリング（Skinny および SIP）の検査をイネーブルにします。

[TLS Proxy] ペインでは、Transaction Layer Security（TLS）Proxy を定義および設定して暗号化トラフィック インスペクションをイネーブルにできます。

フィールド

- [TLS Proxy Name]：TLS Proxy 名を一覧表示します。
- [Server]：トラストポイントを一覧表示します。自己署名または証明書サーバに登録済みのいずれかになります。
- [Local Dynamic Certificate Issuer]：クライアント ダイナミック証明書またはサーバ ダイナミック証明書を発行するローカル認証局を一覧表示します。
- [Local Dynamic Certificate Key Pair]：クライアント ダイナミック証明書またはサーバ ダイナミック証明書が使用する RSA キー ペアを一覧表示します。
- [Add]：TLS Proxy を追加します。
- [Edit]：TLS Proxy を編集します。
- [Delete]：TLS Proxy を削除します。
- [Maximum Sessions]：サポートする TLS Proxy の最大セッション数を指定できます。
  - ASA がサポートする必要がある TLS Proxy の最大セッション数を指定します。デフォルトでは、ASA がサポートするセッション数は 300 です。[Maximum number of sessions] オプションをイネーブルにします。
  - セッションの最大数：最小数は 1 です。最大値は、プラットフォームによって異なります。デフォルトは 300 です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit TLS Proxy

[Add/Edit TLS Proxy] ダイアログボックスでは、TLS Proxy のパラメータを定義できます。

フィールド

- [TLS Proxy Name]：TLS Proxy 名を指定します。
- [Server Configuration]：プロキシ証明書名を指定します。
  - [Server]：TLS ハンドシェイク中に提示するトラストポイントを指定します。トラストポイントは自己署名の場合と、ローカルでプロキシの証明書サービスに登録済みの場合があります。
- [Client Configuration]：ローカル ダイナミック証明書の発行者とキー ペアを指定します。
  - [Local Dynamic Certificate Issuer]：クライアント ダイナミック証明書またはサーバ ダイナミック証明書を発行するローカル認証局を一覧表示します。

    [Certificate Authority Server]：認証局サーバを指定します。

    [Certificate]：証明書を指定します。

    [Manage]：ローカル認証局を設定します。初期設定の終了後にコンフィギュレーションを変更する場合は、ローカル認証局をディセーブルにします。
  - [Local Dynamic Certificate Key Pair]：クライアント ダイナミック証明書が使用する RSA キー ペアを一覧表示します。

    [Key-Pair Name]：定義済みキー ペアを指定します。

    [Show]：生成時刻、使用方法、係数サイズ、キー データなど、キー ペアの詳細を表示します。

    [New]：新しいキー ペアを定義できます。
- [More Options]：TLS ハンドシェイク中に通知または照合する使用可能でアクティブなアルゴリズムを指定します。
  - [Available Algorithms]：TLS ハンドシェイク中に通知または照合する使用可能なアルゴリズム（des-sha1、3des-sha1、aes128-sha1、aes256-sha1、null-sha1）を一覧表示します。

    [Add]：選択したアルゴリズムをアクティブ リストに追加します。

    [Remove]：選択したアルゴリズムをアクティブ リストから削除します。
  - [Active Algorithms]：TLS ハンドシェイク中に通知または照合するアクティブなアルゴリズム（des-sha1、3des-sha1、aes128-sha1、aes256-sha1、null-sha1）を一覧表示します。クライアント プロキシ（サーバに対する TLS クライアントとして機能）の場合、2 つの TLS レッグ間の非対称暗号化方式のために、ユーザ定義のアルゴリズムで hello メッセージの元のアルゴリズムが置き換えられます。たとえば、CallManager をオフロードするために、プロキシと CallManager の間のレッグにはヌル暗号化が使用される場合があります。

    [Move Up]：アルゴリズムをリストの上に移動します。

    [Move Down]：アルゴリズムをリストの下に移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CTL Provider

[CTL Provider] オプションは、Certificate Trust List（CTL）プロバイダー サービスを設定するために使用します。

[CTL Provider] ペインでは、Certificate Trust List プロバイダー サービスを定義および設定して、暗号化トラフィック インスペクションをイネーブルにできます。

フィールド

- [CTL Provider Name]：CTL プロバイダー名を一覧表示します。
- [Client Details]：クライアントの名前と IP アドレスを一覧表示します。
  - [Interface Name]：定義されているインターフェイス名を一覧表示します。
  - [IP Address]：定義されているインターフェイス IP アドレスを一覧表示します。
- [Certificate Name]：エクスポートする証明書を一覧表示します。
- [Add]：CTL プロバイダーを追加します。
- [Edit]：CTL プロバイダーを編集します。
- [Delete]：CTL プロバイダーを削除します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit CTL Provider

[Add/Edit CTL Provider] ダイアログボックスでは、CTL プロバイダーのパラメータを定義できます。

フィールド

- [CTL Provider Name]：CTL プロバイダー名を指定します。
- [Certificate to be Exported]：クライアントにエクスポートする証明書を指定します。

  - [Certificate Name]：クライアントにエクスポートする証明書の名前を指定します。
  - [Manage]：ID 証明書を管理します。
- [Client Details]：接続を許可するクライアントを指定します。
  - [Client to be Added]：クライアント リストに追加するクライアント インターフェイスと IP アドレスを指定します。

    [Interface]：クライアント インターフェイスを指定します。

    [IP Address]：クライアント IP アドレスを指定します。

    [Add]：クライアント リストに新しいクライアントを追加します。

    [Delete]：クライアント リストから選択したクライアントを削除します。
- [More Options]：TLS ハンドシェイク中に通知または照合する使用可能でアクティブなアルゴリズムを指定します。
  - [Parse the CTL file provided by the CTL Client and install trustpoints]：このオプションでインストールされたトラストポイントの名前には「_internal_CTL_」というプレフィックスがつきます。ディセーブルにした場合、各 CallManager サーバと CAPF 証明書を手動でインポートおよびインストールする必要があります。
  - [Port Number]：CTL プロバイダーがリッスンするポートを指定します。ポートは、クラスタの CallManager サーバがリッスンするポート（[CallManager administration] ページの [Enterprise Parameters] で設定されたもの）と同じである必要があります。デフォルト値は 2444 です。
  - [Authentication]：クライアントがプロバイダーの認証を受けるためのユーザ名とパスワードを指定します。

    [Username]：クライアントのユーザ名。

    [Password]：クライアントのパスワード。

    [Confirm Password]：クライアントのパスワード。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—