グローバル オブジェクト

Global 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、Global Objects ペインを利用して 1 箇所から変更できます。

この章には、次の項があります。

ネットワーク オブジェクト グループの設定

この項では、ネットワーク オブジェクト グループを設定する方法について説明します。次の項目を取り上げます。

Network Object Groups

Configuration > Global Objects > Network Object Groups

Network Object Groups ペインで、ネットワーク オブジェクト グループを定義します。ネットワーク オブジェクト グループに、ホストおよびネットワークの IP アドレスをあらかじめ定義しておくと、以後の設定がスムーズになります。アクセスリストや AAA ルールなどのセキュリティ ポリシーを設定するだけで、手動で入力する代わりに事前定義済みのアドレスをクリックすることができます。複数のホストやネットワークをグループ化しておくと、アドレス グループにルールを簡単に適用できます。

ネットワーク オブジェクト グループは、1 つ以上の IP アドレス オブジェクトで構成されています。IP アドレス オブジェクトは、ホストの場合とサブネットの場合があります。ネットワーク オブジェクト グループは、IP アドレス オブジェクトを手動で追加して作成します。また、IP アドレス オブジェクトを、アクセスリストまたは AAA ルールなど他のコンフィギュレーションから取得してグループに追加する方法もあります。

複数のネットワーク オブジェクト グループをネストして「グループのグループ」にすると、単一のグループとして参照できます。

ネットワーク オブジェクト グループは、IP アドレスやネットワークを識別する必要がある、ほとんど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 ルールの設定時は、ASDM ウィンドウの右側のサイド ペインにも IP アドレス オブジェクト、ネットワーク オブジェクト グループなど使用可能なグローバル オブジェクトが表示されます。このサイド 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：ネットワーク オブジェクト グループを追加します。
- Edit：ネットワーク オブジェクト グループを編集します。
- Delete：ネットワーク オブジェクト グループを削除します。ネットワーク オブジェクト グループを削除すると、使用されているすべてのネットワーク オブジェクト グループから削除されます。アクセス ルールで使用されているネットワーク オブジェクト グループは、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ネットワーク オブジェクト グループを空にすることはできません。
- Find：表示されているネットワーク オブジェクト グループと IP アドレスをフィルタし、一致するものだけを表示します。**Find** をクリックすると、Filter field が表示されます。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 フィールド：名前やネットワーク オブジェクト グループに含まれる IP アドレスを入力します。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：ネットワーク オブジェクト グループの名前を示します。名前の隣にあるプラス（+）アイコンをクリックすると、オブジェクト グループが展開され、IP アドレスを確認できます。マイナス（-）アイコンをクリックすると、ネットワーク オブジェクト グループが折りたたまれます。
- IP Address：ネットワーク オブジェクト グループを展開すると IP アドレスが表示されます。
- Netmask：ネットワーク オブジェクト グループを展開するとサブネット マスクが表示されます。
- Description：ネットワーク オブジェクト グループの説明を示します。

モード

次の表に、この機能を使用できるモードを示します。

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 Network Object Group

Configuration > Global Objects > Network Object Groups > Add/Edit Network Object Group

Add/Edit Network Object Group で、ネットワーク オブジェクト グループに IP アドレスや既存のネットワーク オブジェクト グループを割り当てます。

フィールド

- Group Name：グループ名を 64 文字以内で入力します。重複するオブジェクト グループ名は指定できません。ネットワーク オブジェクト グループの名前にサービス グループで使用した名前は使用できません。
- Description：ネットワーク オブジェクト グループの説明を 200 文字以内で入力します。
- Members Not in Group：IP アドレスおよびネットワーク オブジェクト グループを現在のネットワーク オブジェクト グループに割り当てます。
  - Existing Address：定義済みの IP アドレスおよびネットワーク オブジェクト グループから選択できます。既存の IP アドレス オブジェクトを、アクセス ルールや AAA ルールなどのコンフィギュレーションから取得できます。

    Name：定義されている IP アドレスとネットワーク オブジェクト グループを一覧表示します。
  - New Address：新規の IP アドレスを追加できます。

    IP Address：IP アドレスを入力します。

    Netmask：IP アドレスのサブネット マスクを入力します。
- Members in Group：ネットワーク オブジェクト グループにすでに追加されている IP アドレスおよびネットワーク オブジェクト グループを示します。
- Add：選択した IP アドレスをネットワーク オブジェクト グループに追加します。
- Remove：選択した IP アドレスをネットワーク オブジェクト グループから削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 Address

（複数の表示パスがあります。）

Browse Address ダイアログボックスで、IP アドレス オブジェクト、IP 名、ネットワーク オブジェクト グループを選択します。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の場合、このダイアログボックス名は「Browse Source Address」または「Browse Destination Address」になります。

フィールド

- Add：ネットワーク オブジェクト グループや IP 名を追加します。
- Edit：選択したネットワーク オブジェクト グループや IP 名を編集できます。
- Delete：選択したネットワーク オブジェクト グループや IP 名を削除します。
- Find：表示されている名前や IP アドレスをフィルタし、一致するものだけを表示します。**Find** をクリックすると、Filter フィールドが表示されます。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 フィールド：名前やネットワーク オブジェクト グループに含まれる IP アドレスを入力します。ワイルドカード文字としてアスタリスク（*）と疑問符（?）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：IP Address Objects、IP Names、Network Object Groups など、表示するオブジェクト タイプを選択できます。オブジェクトをすべて表示するには、**All** を選択します。
- Name：オブジェクト名を示します。IP アドレス オブジェクトの場合は、IP アドレスが名前になります。ただし、IP アドレス オブジェクトが「any」の場合は例外です。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。
- IP Address：IP アドレスを示します。
- Netmask：サブネット マスクを示します。
- Description：説明を示します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

IP 名の設定

この項では、ホスト IP アドレスと名前を関連付ける方法について説明します。次の項目を取り上げます。

IP Names

Configuration > Global Objects > IP Names

ASDM ではホスト IP アドレスに名前を関連付けることができます。したがって、コンフィギュレーションでは IP アドレスでなく名前を使用できます。IP アドレスはいつでも変更でき、変更によってコンフィギュレーションに問題は起きることはありません。セキュリティ アプライアンスでは、ほとんどの機能が DNS をサポートしていませんが、この方法で同様のことができます。

フィールド

- Add：IP 名を追加します。
- Edit：IP 名を編集します。
- Delete：IP 名を削除します。
- Find：表示されている名前や IP アドレスをフィルタし、一致するものだけを表示します。**Find** をクリックすると、Filter フィールドが表示されます。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 フィールド：名前または IP アドレスを入力します。ワイルドカード文字としてアスタリスク（*）と疑問符（?）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：名前を示します。
- IP Address：IP アドレスを示します。
- Description：説明を示します。

モード

次の表に、この機能を使用できるモードを示します。

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 IP Name

Configuration > Global Objects > IP Names > Add IP Name

Add/Edit IP Name ダイアログボックスで、IP アドレスと名前を関連付けます。

フィールド

- Name：IP アドレスに関連付ける名前を入力します。使用できる文字は、a ～ z、A ～ Z、0 ～ 9、ダッシュ（-）、およびアンダースコア（_）です。63 文字以内で指定します。なお、名前の先頭に数字は使用できません。
- IP Address：IP アドレスを入力します。
- Description：説明を 200 文字以内で入力します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

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。次の項目を取り上げます。

Service Groups

Configuration > Global Objects > Service Groups

Service Groups ペインで、指定したグループに複数のサービスを関連付けます。次のタイプのサービス 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 グループをネストして「グループのグループ」にすると、単一のグループとして参照できます。

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、ほとんど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サイド ペインにもサービス グループなど使用可能なグローバル オブジェクトが表示されます。このサイド 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。
- 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。アクセス ルールで使用しているサービス グループは、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 グループを空にすることはできません。
- Find: フィルタして名前が一致するものだけを表示します。**Find** をクリックすると、Filter フィールドが表示されます。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 フィールド：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（*）と疑問符（?）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。サービス グループをすべて表示するには、**All** を選択します。
- 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。
- Description：サービス グループの説明を一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

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

Configuration > Global Objects > Service Groups > Add/Edit Service Group

Add/Edit Service Group ダイアログボックスで、サービスをサービス グループに割り当てます。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、ダイアログボックス名は「Add/Edit TCP Service Group」になります。

フィールド

- Group Name：グループ名を 64 文字以内で入力します。重複するオブジェクト グループ名は指定できません。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。
- Members Not in Group：サービス グループに追加可能なアイテムです。
  - Service/Service Group, ICMP Type/ICMP Group, or Protocol/Protocol Group：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。

    Name：定義済みのサービス グループ、およびよく使用されるポート、タイプ、プロトコルを一覧表示します。
  - Port #, ICMP #, or Protocol #：このテーブルのタイトルは、追加するサービス グループ タイプによって異なります。アイテムを新規追加するには、番号または名前を入力します。サービス グループが TCP、UDP、TCP-UDP の場合は、ポート番号の範囲を入力できます。
- 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

次の表に、この機能を使用できるモードを示します。

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

（複数の表示パスがあります。）

Browse Service Groups ダイアログボックスで、サービス グループを選択します。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の場合、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: フィルタして名前が一致するものだけを表示します。**Find** をクリックすると、Filter フィールドが表示されます。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 フィールド：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（*）と疑問符（?）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

次の表に、この機能を使用できるモードを示します。

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

検査クラスマップで、アプリケーションのトラフィックを、URL 文字列などアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査マップでトラフィックの照合を直接定義することの違いは、クラスマップでは複雑な照合基準を作成でき、クラスマップを再利用できるという点です。検査クラスマップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

この項では、検査クラスマップを設定する方法について説明します。次の項目を取り上げます。

DNS Class Map

Configuration > Global Objects > Class Maps > DNS

DNS Class Map パネルで、DNS 検査のクラスマップを設定します。

検査クラスマップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査マップでトラフィックの照合を直接定義することの違いは、クラスマップでは複雑な照合基準を作成でき、クラスマップを再利用できるという点です。検査クラスマップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- Name：DNS クラスマップの名前を示します。
- Match Conditions：クラスマップに設定されているタイプ、照合基準、値を示します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：DNS クラスマップの基準を示します。
  - Value：DNS クラスマップで照合する値を示します。
- Description：クラスマップの説明を示します。
- Add：DNS クラスマップの照合条件を追加します。
- Edit：DNS クラスマップの照合条件を編集します。
- Delete：DNS クラスマップの照合条件を削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 DNS Traffic Class Map

Configuration > Global Objects > Class Maps > DNS > Add/Edit DNS Traffic Class Map

Add/Edit DNS Traffic Class Map ダイアログボックスで、DNS クラスマップを定義します。

フィールド

- Name：DNS クラスマップの名前を 40 文字以内で入力します。
- Description：DNS クラスマップの説明を入力します。
- Add：DNS クラスマップを追加します。
- Edit：DNS クラスマップを編集します。
- Delete：DNS クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 DNS Match Criterion

Configuration > Global Objects > Class Maps > DNS > Add/Edit DNS Traffic Class Map > Add/Edit DNS Match Criterion

Add/Edit DNS Match Criterion ダイアログボックスで、DNS クラスマップの照合基準と値を定義します。

フィールド

- Match Type：基準に一致したトラフィックをクラスマップに含めるか、または一致しないトラフィックを含めるか指定します。

  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。
- Criterion：DNS トラフィックに適用する照合基準を指定します。
  - Header Flag：ヘッダーの DNS フラグを照合します。
  - Type：DNS クエリーまたはリソース レコードのタイプを照合します。
  - Class：DNS クエリーまたはリソース レコードのクラスを照合します。
  - Question：DNS の問い合せを照合します。
  - Resource Record：DNS リソース レコードを照合します。
  - Domain Name：DNS クエリーやリソース レコードのドメイン名を照合します。
- Header Flag Criterion Values：DNS ヘッダー フラグの照合値の詳細を指定します。
  - Match Option：完全一致または全ビット一致（ビット マスク一致）のどちらかを指定します。
  - Match Value：ヘッダー フラグについて名前と値のどちらを照合するか指定します。

    Header Flag Name：照合するヘッダー フラグ名を 1 つ以上選択できます。
    AA（authoritative answer）、QR（query）、RA（recursion available）、RD（recursion denied）、TC（truncation）のフラグ ビットがあります。

    Header Flag Value：任意の 16 ビットの値を 16 進数で入力して照合できます。

- Type Criterion Values：DNS タイプの照合値の詳細を指定します。
  - DNS Type Field Name：選択する DNS タイプを一覧表示します。

    A：IPv4 アドレス

    NS：信頼できるネーム サーバ

    CNAME：正規名

    SOA：信頼ゾーンの開始

    TSIG：トランザクション シグニチャ

    IXFR：差分（ゾーン）転送

    AXFR：完全（ゾーン）転送
  - DNS Type Field Value：DNS タイプ フィールドについて値と範囲のどちらを照合するか指定します。

    Value：0 ～ 65535 の範囲の値を入力して照合できます。

    Range：範囲を入力して照合します。両方とも 0 ～ 65535 の範囲の値を指定します。
- Class Criterion Values：DNS クラスの照合値の詳細を指定します。
  - DNS Class Field Name：インターネットで照合する DNS クラス フィールド名を指定します。
  - DNS Class Field Value：DNS クラス フィールドについて値と範囲のどちらを照合するか指定します。

    Value：0 ～ 65535 の範囲の値を入力して照合できます。

    Range：範囲を入力して照合します。両方とも 0 ～ 65535 の範囲の値を指定します。
- Question Criterion Values：DNS の問い合せセクションの照合方法を指定します。
- Resource Record Criterion Values : DNS リソース レコードのセクションの照合方法を指定します。
  - Resource Record：照合対象セクションを一覧表示します。

    Additional：DNS 追加リソース レコード

    Answer：DNS 応答リソース レコード

    Authority：DNS 認証リソース レコード
- Domain Name Criterion Values：DNS ドメイン名の照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Manage Regular Expressions

Configuration > Global Objects > Class Maps > DNS > Add/Edit DNS Traffic Class Map > Add/Edit DNS Match Criterion > Manage Regular Expressions

Manage Regular Expressions ダイアログボックスで Regular Expressions を設定し、パターン照合で使用できます。「_default」で始まる正規表現はデフォルトの正規表現です。変更または削除はできません。

フィールド

- 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。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Manage Regular Expression Class Maps

Configuration > Global Objects > Class Maps > DNS > Add/Edit DNS Traffic Class Map > Add/Edit DNS Match Criterion > Manage Regular Expression Class Maps

Manage Regular Expression Class Maps ダイアログボックスで、正規表現クラスマップを設定します。詳細については、「Regular Expressions」を参照してください。

フィールド

- 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、検査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

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

FTP Class Map

Configuration > Global Objects > Class Maps > FTP

FTP Class Map パネルで FTP 検査のクラスマップを設定します。

検査クラスマップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査マップでトラフィックの照合を直接定義することの違いは、クラスマップでは複雑な照合基準を作成でき、クラスマップを再利用できるという点です。検査クラスマップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- Name：FTP クラスマップの名前を示します。
- Match Conditions：クラスマップに設定されているタイプ、照合基準、値を示します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：FTP クラスマップの基準を示します。
  - Value：FTP クラスマップで照合する値を示します。
- Description：クラスマップの説明を示します。
- Add：FTP クラスマップを追加します。
- Edit：FTP クラスマップを編集します。
- Delete：FTP クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 FTP Traffic Class Map

Configuration > Global Objects > Class Maps > FTP > Add/Edit FTP Traffic Class Map

Add/Edit FTP Traffic Class Map ダイアログボックスで、FTP クラスマップを定義します。

フィールド

- Name：FTP クラスマップの名前を 40 文字以内で入力します。

- Description：FTP クラスマップの説明を入力します。
- Add：FTP クラスマップを追加します。
- Edit：FTP クラスマップを編集します。
- Delete：FTP クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 FTP Match Criterion

Configuration > Global Objects > Class Maps > FTP > Add/Edit FTP Traffic Class Map > Add/Edit FTP Match Criterion

Add/Edit FTP Match Criterion ダイアログボックスで、FTP クラスマップの照合基準と値を定義します。

フィールド

- Match Type：基準に一致したトラフィックをクラスマップに含めるか、または一致しないトラフィックを含めるか指定します。

  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。
- Criterion：FTP トラフィックに適用する照合基準を指定します。
  - Request-Command：FTP 要求コマンドを照合します。
  - File Name：FTP 転送のファイル名を照合します。
  - File Type：FTP 転送のファイル タイプを照合します。
  - Server：FTP サーバを照合します。
  - User Name：FTP ユーザを照合します。
- Request-Command Criterion Values：FTP 要求コマンドの照合値の詳細を指定します。
  - Request Command：照合する要求コマンドを 1 つ以上選択できます。

    APPE：ファイルに追加します。

    CDUP：現在のディレクトリから親ディレクトリへ移動します。

    DELE：サーバ サイトのファイルを削除します。

    GET：retr（retrieve a file）コマンドの FTP クライアント コマンドです。

    HELP：サーバのヘルプ情報です。

    MKD：ディレクトリを作成します。

    PUT：stor（store a file）コマンドの FTP クライアント コマンドです。

    RMD：ディレクトリを削除します。

    RNFR：この名前からリネームします。

    RNTO：この名前にリネームします。

    SITE：サーバ固有のコマンドを指定します。

    STOU：ファイルに一意の名前をつけて保存します。

- File Name Criterion Values：FTP 転送のファイル名の照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- File Type Criterion Values：FTP 転送のファイル タイプの照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Server Criterion Values：FTP サーバの照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- User Name Criterion Values：FTP ユーザの照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

H.323 Class Map

Configuration > Global Objects > Class Maps > H.323

H.323 Class Map パネルで H.323 検査のクラスマップを設定します。

検査クラスマップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査マップでトラフィックの照合を直接定義することの違いは、クラスマップでは複雑な照合基準を作成でき、クラスマップを再利用できるという点です。検査クラスマップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- Name：H.323 クラスマップの名前を示します。

- Match Conditions：クラスマップに設定されているタイプ、照合基準、値を示します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：H.323 クラスマップの基準を示します。
  - Value：H.323 クラスマップで照合する値を示します。
- Description：クラスマップの説明を示します。
- Add：H.323 クラスマップを追加します。
- Edit：H.323 クラスマップを編集します。
- Delete：H.323 クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 H.323 Traffic Class Map

Configuration > Global Objects > Class Maps > H.323 > Add/Edit H.323 Traffic Class Map

Add/Edit H.323 Traffic Class Map ダイアログボックスで、H.323 クラスマップを定義します。

フィールド

- Name：H.323 クラスマップの名前を 40 文字以内で入力します。
- Description：H.323 クラスマップの説明を入力します。
- Add：H.323 クラスマップを追加します。
- Edit：H.323 クラスマップを編集します。
- Delete：H.323 クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 H.323 Match Criterion

Configuration > Global Objects > Class Maps > H.323 > Add/Edit H.323 Traffic Class Map > Add/Edit H.323 Match Criterion

Add/Edit H.323 Match Criterion ダイアログボックスで、H.323 クラスマップの照合基準と値を定義します。

フィールド

- Match Type：基準に一致したトラフィックをクラスマップに含めるか、または一致しないトラフィックを含めるか指定します。

  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。
- Criterion：H.323 トラフィックに適用する照合基準を指定します。
  - Called Party：受信側を照合します。
  - Calling Party：発信元を照合します。
  - Media Type：メディア タイプを照合します。
- Called Party Criterion Values：H.323 受信側の照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Calling Party Criterion Values：H.323 発信元の照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Media Type Criterion Values：照合するメディア タイプを指定します。
  - Audio：音声タイプを照合します。
  - Video：ビデオ タイプを照合します。
  - Data：データ タイプを照合します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

HTTP Class Map

Configuration > Global Objects > Class Maps > HTTP

HTTP Class Map パネルで HTTP 検査のクラスマップを設定します。

検査クラスマップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査マップでトラフィックの照合を直接定義することの違いは、クラスマップでは複雑な照合基準を作成でき、クラスマップを再利用できるという点です。検査クラスマップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- Name：HTTP クラスマップの名前を示します。
- Match Conditions：クラスマップに設定されているタイプ、照合基準、値を示します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：HTTP クラスマップの基準を示します。
  - Value：HTTP クラスマップで照合する値を示します。
- Description：クラスマップの説明を示します。
- Add：HTTP クラスマップを追加します。
- Edit：HTTP クラスマップを編集します。
- Delete：HTTP クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 HTTP Traffic Class Map

Configuration > Global Objects > Class Maps > HTTP > Add/Edit HTTP Traffic Class Map

Add/Edit HTTP Traffic Class Map ダイアログボックスで、HTTP クラスマップを定義します。

フィールド

- Name：HTTP クラスマップの名前を 40 文字以内で入力します。
- Description：HTTP クラスマップの説明を入力します。
- Add：HTTP クラスマップを追加します。
- Edit：HTTP クラスマップを編集します。
- Delete：HTTP クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 HTTP Match Criterion

Configuration > Global Objects > Class Maps > HTTP > Add/Edit HTTP Traffic Class Map > Add/Edit HTTP Match Criterion

Add/Edit HTTP Match Criterion ダイアログボックスで、HTTP クラスマップの照合基準と値を定義します。

フィールド

- Match Type：基準に一致したトラフィックをクラスマップに含めるか、または一致しないトラフィックを含めるか指定します。

  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。

- Criterion：HTTP トラフィックに適用する照合基準を指定します。
  - Request/Response Content Type Mismatch : 応答のコンテンツ タイプを、要求の accept フィールドの MIME タイプの 1 つに一致させるかどうかを指定します。
  - Request Arguments：要求の引数を正規表現で照合します。

    Regular Expression：照合する定義された正規表現を一覧表示します。

    Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

    Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

    Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
  - Request Body Length：要求の本文に指定したバイト数より長いフィールドがある場合、正規表現で照合します。

    Greater Than Length : 要求フィールドの長さと照合するフィールドの値をバイト単位で入力します。
  - Request Body：要求の本文を正規表現で照合します。

    Regular Expression：照合する定義された正規表現を一覧表示します。

    Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

    Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

    Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
  - Request Header Field Count : 要求ヘッダーのフィールド数が最大値の場合、正規表現で照合します。

    Predefined：要求のヘッダー フィールドを次の中から指定します。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。

    Regular Expression：照合する定義された正規表現を一覧表示します。

Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

Greater Than Count：ヘッダー フィールド数の最大値を入力します。

- Request Header Field Length：要求ヘッダーに指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  Predefined：要求のヘッダー フィールドを次の中から指定します。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Greater Than Length：要求フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- Request Header Field：要求ヘッダーを正規表現で照合します。

  Predefined：要求のヘッダー フィールドを次の中から指定します。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

- Request Header Count：要求ヘッダー数が最大値の場合、正規表現で照合します。

  Greater Than Count：ヘッダー数の最大値を入力します。

- Request Header Length：要求ヘッダーが指定したバイト数より長い場合、正規表現で照合します。

  Greater Than Length：ヘッダーの長さをバイト単位で入力します。

- Request Header non-ASCII：要求ヘッダーに含まれる ASCII 以外の文字を照合します。

- Request Method：要求の方式を正規表現で照合します。

  Method：照合する要求方式を次の中から指定します。bcopy、bdelete、bmove、bpropfind、bproppatch、connect、copy、delete、edit、get、getattribute、getattributenames、getproperties、head、index、lock、mkcol、mkdir、move、notify、options、poll、post、propfind、proppatch、put、revadd、revlabel、revlog、revnum、save、search、setattribute、startrev、stoprev、subscribe、trace、unedit、unlock、unsubscribe。

  Regular Expression：正規表現の照合方法を指定します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

- Request URI Length：要求の URI が指定したバイト数より長い場合、正規表現で照合します。

  Greater Than Length：URI の長さをバイト単位で入力します。

- Request URI：要求の URI を正規表現で照合します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

- Response Body：要求の本文を regex で照合します。

  ActiveX：ActiveX の照合方法を指定します。

  Java Applet：Java アプレットの照合方法を指定します。

  Regular Expression：正規表現の照合方法を指定します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage:Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

- Response Body Length : 応答の本文に指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  Greater Than Length : 応答フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- Response Header Field Count：応答ヘッダーのフィールド数が最大値の場合、正規表現で照合します。

  Predefined : 応答のヘッダー フィールドを次の中から指定します。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage:Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Greater Than Count：ヘッダー フィールド数の最大値を入力します。

- Response Header Field Length : 応答ヘッダーに指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  Predefined : 応答のヘッダー フィールドを次の中から指定します。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage:Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Greater Than Length : 応答フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- Response Header Field：応答ヘッダーを正規表現で照合します。

  Predefined : 応答のヘッダー フィールドを次の中から指定します。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage:Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

- Response Header Count：応答ヘッダー数が最大値の場合、正規表現で照合します。

  Greater Than Count：ヘッダー数の最大値を入力します。

- Response Header Length：応答ヘッダーが指定したバイト数より長い場合、正規表現で照合します。

  Greater Than Length：ヘッダーの長さをバイト単位で入力します。
- Response Header non-ASCII：応答ヘッダーに含まれる ASCII 以外の文字を照合します。
- Response Status Line：ステータス行を正規表現で照合します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

IM Class Map

Configuration > Global Objects > Class Maps > Instant Messaging (IM)

IM Class Map パネルで IM 検査のクラスマップを設定します。

検査クラスマップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査マップでトラフィックの照合を直接定義することの違いは、クラスマップでは複雑な照合基準を作成でき、クラスマップを再利用できるという点です。検査クラスマップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- Name：IM クラスマップの名前を示します。
- Match Conditions：クラスマップに設定されているタイプ、照合基準、値を示します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：IM クラスマップの基準を示します。
  - Value：IM クラスマップで照合する値を示します。
- Description：クラスマップの説明を示します。
- Add：IM クラスマップを追加します。
- Edit：IM クラスマップを編集します。
- Delete：IM クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 IM Traffic Class Map

Configuration > Global Objects > Class Maps > IM > Add/Edit IM Traffic Class Map

Add/Edit IM Traffic Class Map ダイアログボックスで、IM クラスマップを定義します。

フィールド

- Name：IM クラスマップの名前を 40 文字以内で入力します。
- Description：IM クラスマップの説明を入力します。
- Add：IM クラスマップを追加します。
- Edit：IM クラスマップを編集します。
- Delete：IM クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 IM Match Criterion

Configuration > Global Objects > Class Maps > IM > Add/Edit IM Traffic Class Map > Add/Edit IM Match Criterion

Add/Edit IM Match Criterion ダイアログボックスで、IM クラスマップの照合基準と値を定義します。

フィールド

- Match Type：基準に一致したトラフィックをクラスマップに含めるか、または一致しないトラフィックを含めるか指定します。

  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。
- Criterion：IM トラフィックに適用する照合基準を指定します。
  - Protocol：IM プロトコルを照合します。
  - Service：IM サービスを照合します。
  - Version：IM ファイル転送のサービス バージョンを照合します。
  - Client Login Name：IM サービスのクライアント ログイン名を照合します。
  - Client Peer Login Name：IM サービスのクライアントのピア ログイン名を照合します。

  - Source IP Address：送信元 IP アドレスを照合します。
  - Destination IP Address：宛先 IP アドレスを照合します。
  - Filename：IM ファイル転送サービスのファイル名を照合します。
- Protocol Criterion Values：照合する IM プロトコルを指定します。
  - Yahoo! Messenger：Yahoo! Messenger のインスタント メッセージを照合します。
  - MSN Messenger：MSN Messenger のインスタント メッセージを照合します。
- Service Criterion Values：照合する IM サービスを指定します。
  - Chat：IM メッセージ チャット サービスを照合します。
  - Conference：IM コンファレンス サービスを照合します。
  - File Transfer：IM ファイル転送サービスを照合します。
  - Games：IM ゲーム サービスを照合します。
  - Voice Chat：IM 音声チャット サービスを照合します（Yahoo の IM は対象外です）。
  - Web Cam：IM Web カメラ サービスを照合します。
- Version Criterion Values：IM ファイル転送サービスで照合するバージョンを指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Client Login Name Criterion Values：IM サービスで照合するクライアント ログイン名を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Client Peer Login Name Criterion Values：IM サービスで照合するクライアントのピア ログイン名を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Source IP Address Criterion Values：IM サービスで照合する送信元 IP アドレスを指定します。
  - IP Address：IM サービスの送信元 IP アドレスを入力します。
  - IP Mask：送信元 IP アドレスのマスクです。
- Destination IP Address Criterion Values：IM サービスで照合する宛先 IP アドレスを指定します。
  - IP Address：IM サービスの宛先 IP アドレスを入力します。
  - IP Mask：宛先 IP アドレスのマスクです。
- Filename Criterion Values：IM ファイル転送サービスで照合するファイル名を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

— Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

SIP Class Map

Configuration > Global Objects > Class Maps > SIP

SIP Class Map パネルで SIP 検査のクラスマップを設定します。

検査クラスマップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査マップでトラフィックの照合を直接定義することの違いは、クラスマップでは複雑な照合基準を作成でき、クラスマップを再利用できるという点です。検査クラスマップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- Name：SIP クラスマップの名前を示します。
- Match Conditions：クラスマップに設定されているタイプ、照合基準、値を示します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：SIP クラスマップの基準を示します。
  - Value：SIP クラスマップで照合する値を示します。
- Description：クラスマップの説明を示します。
- Add：SIP クラスマップを追加します。
- Edit：SIP クラスマップを編集します。
- Delete：SIP クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 SIP Traffic Class Map

Configuration > Global Objects > Class Maps > SIP > Add/Edit SIP Traffic Class Map

Add/Edit SIP Traffic Class Map ダイアログボックスで、SIP クラスマップを定義します。

フィールド

- Name：SIP クラスマップの名前を 40 文字以内で入力します。
- Description：SIP クラスマップの説明を入力します。
- Add：SIP クラスマップを追加します。
- Edit：SIP クラスマップを編集します。
- Delete：SIP クラスマップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 SIP Match Criterion

Configuration > Global Objects > Class Maps > SIP > Add/Edit SIP Traffic Class Map > Add/Edit SIP Match Criterion

Add/Edit SIP Match Criterion ダイアログボックスで、SIP クラスマップの照合基準と値を定義します。

フィールド

- Match Type：基準に一致したトラフィックをクラスマップに含めるか、または一致しないトラフィックを含めるか指定します。

  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。
- Criterion：SIP トラフィックに適用する照合基準を指定します。
  - Called Party：To ヘッダーに指定された受信側を照合します。
  - Calling Party：From ヘッダーに指定された発信元を照合します。
  - Content Length：ヘッダーのコンテンツの長さを照合します。0 ～ 65536 の範囲の値です。
  - Content Type：ヘッダーのコンテンツ タイプを照合します。
  - IM Subscriber：SIP IM の加入者を照合します。
  - Message Path：SIP の Via ヘッダーを照合します。
  - Request Method：SIP の要求方式を照合します。
  - Third-Party Registration：サード パーティの登録要求者を照合します。
  - URI Length：SIP ヘッダーにある URI を照合します。0 ～ 65536 の範囲の値です。
- Called Party Criterion Values：照合する受信側を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

- Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

- Calling Party Criterion Values：照合する発信元を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Content Length Criterion Values：指定値より長い SIP コンテンツ ヘッダーを照合します。
  - Greater Than Length：ヘッダーの長さをバイト単位で入力します。
- Content Type Criterion Values：照合する SIP コンテンツ ヘッダーのタイプを指定します。
  - SDP：SDP タイプの SIP コンテンツ ヘッダーを照合します。
  - Regular Expression：正規表現を照合します。

    Regular Expression：照合する定義された正規表現を一覧表示します。

    Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

    Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

    Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- IM Subscriber Criterion Values：照合する IM 登録者を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Message Path Criterion Values：照合する SIP の Via ヘッダーを指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Request Method Criterion Values：照合する SIP 要求方式を指定します。
  - Request Method：次の中から要求方式を指定します。ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update。
- Third-Party Registration Criterion Values：照合するサード パーティの登録要求者を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- URI Length Criterion Values：SIP ヘッダーで指定した値より長い、選択したタイプの URI を照合します。
  - URI type：SIP URI または TEL URI を指定して照合します。
  - Greater Than Length：長さをバイト単位で指定します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

検査マップの設定

この項では、検査マップを設定する方法について説明します。次の項目を取り上げます。

セキュリティ アプライアンスのステートフル アプリケーション検査にアルゴリズムを適用して、アプリケーションのセキュリティとサービスを保証します。アプリケーションの中には特別な処理を必要とするものがあり、専用の検査エンジンでそのような場合に対応します。専用の検査エンジンが必要なアプリケーションとは、ユーザのデータ パケットの中に IP アドレッシング情報を埋め込むサービスや、ダイナミック割り当てポートでセカンダリ チャネルを開くサービスなどです。

アプリケーション検査エンジンは NAT と連携し、アドレッシング情報が埋め込まれている場所の識別をサポートします。これによって、このような埋め込みアドレスを NAT で変換したり、変換の影響を受けるチェックサムやその他のフィールドをアップデートしたりすることができます。

各アプリケーション検査エンジンはセッションを監視して、セカンダリ チャネルのポート番号も確認します。多くのプロトコルは、パフォーマンスを向上させるために、TCP または UDP のセカンダリ ポートを開きます。ウェルノウン ポート上の初期セッションは、ダイナミックに割り当てられたポート番号をネゴシエートするために使用されます。アプリケーション検査エンジンは、この初期セッションを監視し、ダイナミックに割り当てられたポートを特定し、所定のセッションの間、それらのポート上でのデータ交換を許可します。

また、ステートフル アプリケーション検査により、検査中のプロトコルの過程で発行されたコマンドと応答の有効性を監査します。セキュリティ アプライアンスは攻撃を確実に防御するため、トラフィックが検査されるプロトコルごとに RFC 仕様に準拠しているかどうかチェックします。

検査マップ機能で、専用のプロトコル検査エンジンを作成できます。検査マップを利用して、プロトコル検査エンジンのコンフィギュレーションを保存します。それから、グローバル セキュリティ ポリシーや特定のインターフェイスのセキュリティ ポリシーを使用して特定のトラフィック タイプにマップを関連付け、検査マップのコンフィギュレーション設定をイネーブルにします。

Security Policy ペインの Service Policy Rules タブから検査マップをトラフィックに適用すると、サービス ポリシーで指定した基準に従って照合が行われます。サービス ポリシーは、セキュリティ アプライアンスの特定のインターフェイスまたはすべてのインターフェイスに適用することができます。

DCERPC	DCERPC 検査で、DCERPC 検査マップを作成、表示、管理します。DCERPC マップでクライアントとエンドポイント マッパーの間で送受される DCERPC メッセージを検査し、必要に応じてセカンダリ接続に NAT を適用します。DCERPC はリモート プロシージャ コール メカニズムの仕様です。
DNS	DNS 検査で、DNS 検査マップを作成、表示、管理します。このマップを使用して DNS メッセージをより詳細に制御し、DNS スプーフィングとキャッシュ ポイズニングを保護できます。DNS は、IP アドレスやメール サーバなどのドメイン名の情報を解決します。
ESMTP	ESMTP 検査で、ESMTP 検査マップを作成、表示、管理します。ESMTP マップを使用してアプリケーションのセキュリティおよびプロトコル準拠性を検査し、攻撃の防御、送信者や受信者のブロック、メール中継のブロックができます。ESMTP（Extended SMTP）は SMTP 規格のプロトコル拡張を定義します。
FTP	FTP 検査で、FTP 検査マップを作成、表示、管理します。インターネットなど、TCP/IP ネットワークを介してファイルを転送する通信プロトコルです。FTP マップを使用して、セキュリティ アプライアンスを通過したり FTP サーバに到達したりする FTP PUT などの、特定の FTP プロトコル方式をブロックできます。
GTP	GTP 検査で、GTP 検査マップを作成、表示、管理します。GTP は比較的新しいプロトコルで、インターネットなど TCP/IP ネットワークと無線接続する場合のセキュリティを提供します。GTP マップを使用して、タイムアウト値、メッセージ サイズ、トンネル数、セキュリティ アプライアンスを通過する GTP バージョンを制御できます。
H.323	H.323 検査で、H.323 検査マップを作成、表示、管理します。H.323 マップを使用して、RAS、H.225、H.245 の VoIP プロトコルを検査し、ステートのトラッキングとフィルタリングができます。
HTTP	HTTP 検査で、HTTP 検査マップを作成、表示、管理します。HTTP はワールドワイド ウェブのクライアントとサーバ間の通信で使用されるプロトコルです。HTTP マップを使用して、RFC 準拠の HTTP ペイロード コンテンツ タイプを設定できます。また、特定の HTTP 方式をブロックし、一部のトンネル アプリケーションによる HTTP 転送を防止できます。
IM	IM 検査で、IM 検査マップを作成、表示、管理します。IM マップを使用してネットワークの使用を制御し、IM アプリケーションによる機密情報の漏洩や他のネットワークの脅威を防止できます。
IPSec パススルー	IPSec パススルー検査で、IPSec パススルーの検査マップを作成、表示、管理します。IPSec パススルー マップを使用すると、アクセスリストを参照しなくても、特定のフローを許可できます。
MGCP	MGCP 検査で、MGCP 検査マップを作成、表示、管理します。MGCP マップを使用して、VoIP デバイスと MGCP コール エージェント間の接続を管理できます。
NetBIOS	NetBIOS 検査で、NetBIOS 検査マップを作成、表示、管理します。NetBIOS マップを使用して、NetBIOS プロトコルに確実に準拠し、フィールドの数と長さの整合性やメッセージなどをチェックできます。
RADIUS Accounting	RADIUS Accounting 検査で、RADIUS Accounting 検査マップを作成、表示、管理します。RADIUS マップを使用すると、過剰請求攻撃を防御できます。
SCCP（Skinny）	SCCP（Skinny）検査で、SCCP（Skinny）の検査マップを作成、表示、管理します。SCCP マップを使用して、プロトコル準拠チェックと基本的なステート トラッキングができます。

SIP	SIP 検査で、SIP の検査マップを作成、表示、管理します。SIP マップを使用して、アプリケーションのセキュリティとプロトコル準拠をチェックし、SIP を利用した攻撃を防御できます。SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、インスタント メッセージ機能で幅広く利用されているプロトコルです。
SNMP	SNMP 検査で、SNMP の検査マップを作成、表示、管理します。SNMP は、ネットワーク管理デバイスとネットワーク管理ステーション間の通信に利用されるプロトコルです。SNMP マップを使用して、SNMP v1、2、2c、3 など特定の SNMP バージョンをブロックできます。

DCERPC Inspect Map

Configuration > Global Objects > Inspect Maps > DCERPC

DCERPC ペインで、DCERPC アプリケーションの事前に設定された検査マップを表示します。DCERPC マップでは、DCERPC アプリケーション検査のデフォルト設定値を変更できます。

DCERPC は、Microsoft のクライアント / サーバ アプリケーションで広く使われているプロトコルです。このプロトコルによって、ソフトウェア クライアントがサーバにあるプログラムをリモートで実行できるようになります。

通常、このプロトコルの接続では、クライアントがウェルノウン ポート番号で接続を受け入れるエンドポイント マッパー（EPM）というサーバに、必要なサービスについてダイナミックに割り当てられるネットワーク情報を問い合せます。次に、クライアントは、サービスを提供しているサーバのインスタンスへのセカンダリ接続を確立します。セキュリティ アプライアンスは、適切なポート番号とネットワーク アドレスへのセカンダリ接続を許可し、必要に応じて NAT を行います。

DCERPC 検査マップは、TCP のウェルノウン ポート 135 を経由した、EPM とクライアント間のネイティブ TCP の通信を検査します。クライアント用に EPM のマッピングとルックアップがサポートされています。クライアントとサーバは、どのセキュリティ ゾーンにあってもかまいません。サーバの埋め込まれた IP アドレスとポート番号は、EPM からの応答メッセージで受け取ります。クライアントが EPM から返されたサーバのポート番号で複数の接続を確立する可能性があるので、ピンホールを複数使用でき、ユーザがそのタイムアウトを設定できるようになっています。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low

    ピンホールのタイムアウト：00:02:00

    エンドポイント マッパー サービス：適用強制しない

    エンドポイント マッパー サービス ルックアップ：イネーブル

    エンドポイント マッパー サービス ルックアップのタイムアウト：00:05:00
  - Medium：デフォルト

    ピンホールのタイムアウト：00:01:00

    エンドポイント マッパー サービス：適用強制しない

    エンドポイント マッパー サービス ルックアップ：ディセーブル
  - High

    ピンホールのタイムアウト：00:01:00

    エンドポイント マッパー サービス：適用強制する

エンドポイント マッパー サービス ルックアップ：ディセーブル

- Customize：Customize Security Level ダイアログボックスが開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトの Medium レベルに戻します。

- DCERPC Inspect Maps：定義されている DCERPC 検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの DCERPC エリアにもリストされます。
- Add：新規の DCERPC 検査マップを、DCERPC Inspect Maps テーブルの定義リストと Inspect Maps ツリーの DCERPC エリアに追加します。DCERPC マップを新たに設定するには、Inspect Maps ツリーで DCERPC のエントリを選択します。
- Delete：DCERPC Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの DCERPC エリアからも削除されます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Customize Security Level

Configuration > Global Objects > Inspect Maps > DCERPC > Customize Security Level

Customize Security Level ダイアログボックスで、DCERPC アプリケーションの事前に設定された検査マップにセキュリティ設定を行います。

フィールド

- Settings：ピンホール タイムアウトとエンドポイント マッパーのセキュリティ データを設定します。
  - Pinhole Timeout：ピンホール タイムアウトを設定します。クライアントが使用するサーバ情報は、複数の接続のエンドポイント マッパーから返される場合があるため、タイムアウト値はクライアントのアプリケーション環境を考慮して設定します。0:0:1 ～ 1193:0:0 の範囲で指定します。デフォルト値は 2 分です。
  - Enforce endpoint-mapper service：バインディング中はエンドポイント マッパー サービスの適用を強制します。
  - Enforce endpoint-mapper service lookup：エンドポイント マッパー サービスのルックアップをイネーブルにします。ディセーブルの場合、ピンホール タイムアウトが適用されます。

    Service Lookup Timeout：ルックアップでピンホールした場合のタイムアウトを設定します。
- Reset to Predefined Security Level：セキュリティ レベルの設定を、あらかじめ定義された High、Medium、または Low のレベルにリセットします。
  - Reset To：セキュリティ レベルを High、Medium、または Low にリセットします。
- Reset：すべてのセキュリティ設定をデフォルトにリセットします。デフォルトのピンホール タイムアウトは 1 分です。エンドポイント マッパーのデフォルト設定値はありません。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

DCERPC Inspect Map Basic/Advanced View

Configuration > Global Objects > Inspect Maps > DCERPC > DCERPC Inspect Map > Basic/Advanced View

DCERPC map ペインで、DCERPC アプリケーションの事前に設定された検査マップに基本設定や詳細設定を行います。

フィールド

- Name：すでに設定されている DCERPC マップの名前を示します。
- Description：DCERPC マップの説明を 200 文字以内で入力します。
- Basic View：現在のセキュリティ設定を表示します。
  - Customize：Customize Security Level ダイアログボックスが開き、セキュリティ データを設定できます。
  - Default Level：セキュリティ レベルをデフォルトの Medium レベルに戻します。
- Advanced View：セキュリティ設定を行います。
  - Pinhole Timeout：ピンホール タイムアウトを設定します。クライアントが使用するサーバ情報は、複数の接続のエンドポイント マッパーから返される場合があるため、タイムアウト値はクライアントのアプリケーション環境を考慮して設定します。0:0:1 ～ 1193:0:0 の範囲で指定します。デフォルト値は 2 分です。
  - Enforce endpoint-mapper service：バインディング中はエンドポイント マッパー サービスの適用を強制します。
  - Enforce endpoint-mapper service lookup：エンドポイント マッパー サービスのルックアップをイネーブルにします。ディセーブルの場合、ピンホール タイムアウトが適用されます。

    Service Lookup Timeout : ルックアップでピンホールした場合のタイムアウトを設定します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

DNS Inspect Map

Configuration > Global Objects > Inspect Maps > DNS

DNS ペインで、DNS アプリケーションの事前に設定された検査マップを表示します。DNS マップでは、DNS アプリケーション検査のデフォルト設定値を変更できます。

DNS アプリケーション検査は、DNS スプーフィングとキャッシュ ポイズニングを防ぐための DNS メッセージの管理機能をサポートしています。ユーザが設定できるルールを使用して、特定の DNS タイプを許可、ドロップ、ロギングし、他の DNS タイプをブロックすることができます。たとえば、ゾーン転送をこの機能のあるサーバ間だけに制限します。

公開サーバが特定の内部ゾーンだけをサポートしている場合に、DNS パケットのヘッダーにある Recursion Desired フラグと Recursion Available フラグをマスクして、サーバを攻撃から守ることができます。また、DNS のランダム化をイネーブルにすると、ランダム化をサポートしていないサーバや強度の低い擬似乱数ジェネレータを使用するサーバのスプーフィングやキャッシュ ポイズニングを回避できます。照会できるドメイン名を制限することにより、公開サーバの保護がさらに確実になります。

DNS の不一致の応答数が増える（キャッシュ ポイズニング攻撃を示す可能性があります）と、DNS の不一致のアラートを設定して通知されるようします。さらに、DNS のすべてのメッセージに Transaction Signature（TSIG; トランザクション シグニチャ）を付け、メッセージをチェックする設定も行えます。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    DNS Guard：イネーブル

    NAT のリライト：イネーブル

    プロトコル適用：イネーブル

    ID のランダム化：ディセーブル

    メッセージの長さのチェック：イネーブル

    メッセージの最大長：512

    不一致レートのロギング：ディセーブル

    TSIG リソース レコード：適用強制しない
  - Medium

    DNS Guard：イネーブル

    NAT のリライト：イネーブル

    プロトコル適用：イネーブル

    ID のランダム化：イネーブル

    メッセージの長さのチェック：イネーブル

    メッセージの最大長：512

    不一致レートのロギング：イネーブル

    TSIG リソース レコード：適用強制しない
  - High

    DNS Guard：イネーブル

    NAT のリライト：イネーブル

    プロトコル適用：イネーブル

ID のランダム化：イネーブル

メッセージの長さのチェック：イネーブル

メッセージの最大長：512

不一致レートのロギング：イネーブル

TSIG リソース レコード：適用強制する

- Customize：Customize Security Level ダイアログボックスが開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトの Low レベルに戻します。

- DNS Inspect Maps：定義されている DNS 検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの DNS エリアにもリストされます。
- Add：新規の DNS 検査マップを、DNS Inspect Maps テーブルの定義リストと Inspect Maps ツリーの DNS エリアに追加します。DNS マップを新たに設定するには、Inspect Maps ツリーで DNS のエントリを選択します。
- Delete：DNS Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの DNS エリアからも削除されます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Customize Security Level

Configuration > Global Objects > Inspect Maps > DNS > Customize Security Level

Customize Security Level ダイアログボックスで、DNS アプリケーションの事前に設定された検査マップにセキュリティ設定を行います。

フィールド

- Settings：DNS のセキュリティ設定とアクションを指定します。
  - Enable DNS guard function：プロトコル準拠では、DNS ヘッダーの識別フィールドを使用して、DNS クエリーと応答の不一致のチェックを行います。1 つのクエリーに対して 1 つの応答がセキュリティ アプライアンスを通過できます。
  - Enable NAT rewrite function：プロトコル準拠では、DNS 応答の A レコードにある IP アドレスの変換をイネーブルにします。
  - Enable protocol enforcement：プロトコル準拠では、DNS メッセージの形式チェックをイネーブルにします。ドメイン名、ラベルの長さ、圧縮、ループしたポインタなどをチェックします。
  - Randomize the DNS identifier for DNS query：プロトコル準拠では、DNS クエリー メッセージの DNS 識別子をランダム化します。
  - Drop packets that exceed specified maximum length：フィルタリングでは、最大長（バイト）を超えるパケットをドロップします。

    Maximum Packet Length：パケットの最大長をバイト単位で入力します。
  - Enable Logging when DNS ID mismatch rate exceeds specified rate：DNS 識別子の不一致が多く発生した場合にレポートを表示します。

    Mismatch Instance Threshold：不一致のインスタンスの最大数を入力します。この値を超えない場合、システム メッセージ ログに出力されません。

Time Interval：監視間隔時間（秒単位）を入力します。

- Enforce TSIG record source to be present in DNS message : プロトコル準拠では、このオプションを選択すると TSIG リソース レコードが DNS トランザクションに存在する必要があります。TSIG を強制的に適用すると、次のアクションが実行されます。

  Drop packet：パケットをドロップします（ロギングはイネーブルまたはディセーブルに指定できます）。

  Log：ロギングをイネーブルにします。

- Reset to predefined security level : セキュリティ レベルの設定を、あらかじめ定義された High、Medium、または Low のレベルにリセットします。デフォルトは Low です。
  - Reset to：セキュリティ設定（High、Medium、Low）を指定します。
  - Reset：選択したレベルに設定をリセットします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

DNS Inspect Map Basic View

Configuration > Global Objects > Inspect Maps > DNS > DNS Inspect Map > Basic View

DNS Inspect Map Basic View ペインで、DNS 検査マップの設定済みデータを表示します。Advanced View から設定できます。

フィールド

- Name：すでに設定されている DNS マップの名前を示します。
- Description：DNS マップの説明を 200 文字以内で入力します。
- Security Level：現在のセキュリティ設定を表示します。
  - Customize：Customize Security Level ダイアログボックスが開き、セキュリティ設定を行います。
  - Default Level：セキュリティ レベルをデフォルトに戻します。
- Advanced View：セキュリティ設定を行います。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

DNS Inspect Map Advanced View

Configuration > Global Objects > Inspect Maps > DNS > DNS Inspect Map > Advanced View

DNS Inspect Map Advanced View ペインで、検査マップを設定できます。

フィールド

- Name：すでに設定されている DNS マップの名前を示します。
- Description：DNS マップの説明を 200 文字以内で入力します。
- Protocol Conformance：このタブで DNS のプロトコル準拠を設定します。
  - Enable DNS guard function：DNS ヘッダーの識別フィールドを使用して、DNS クエリーと応答の不一致のチェックを行います。1 つのクエリーに対して 1 つの応答がセキュリティアプライアンスを通過できます。
  - Enable NAT re-write function：DNS 応答の A レコードにある IP アドレスの変換をイネーブルにします。
  - Enable protocol enforcement：DNS メッセージの形式チェックをイネーブルにします。ドメイン名、ラベルの長さ、圧縮、ループしたポインタなどをチェックします。
  - Randomize the DNS identifier for DNS query：DNS クエリー メッセージの DNS 識別子をランダム化します。
  - Enforce TSIG resource record to be present in DNS message：TSIG リソース レコードが DNS トランザクションに存在する必要があります。TSIG を強制的に適用すると、次のアクションが実行されます。

    Drop packet：パケットをドロップします（ロギングはイネーブルまたはディセーブルに指定できます）。

    Log：ロギングをイネーブルにします。
- Filtering：このタブで DNS のフィルタリングを設定します。
  - Global Settings：設定がグローバルに適用されます。

    Drop packets that exceed specified maximum length (global)：最大長（バイト）を超えるパケットをドロップします。

    Maximum Packet Length：パケットの最大長をバイト単位で入力します。
  - Server Settings：サーバの設定だけを適用します。

    Drop packets that exceed specified maximum length：最大長（バイト）を超えるパケットをドロップします。

    Maximum Packet Length：パケットの最大長をバイト単位で入力します。

    Drop packets sent to server that exceed length indicated by the RR：Resource Record で指定された長さを超えるパケットがサーバに送信された場合はドロップします。
  - Client Settings：クライアントの設定だけを適用します。

    Drop packets that exceed specified maximum length：最大長（バイト）を超えるパケットをドロップします。

    Maximum Packet Length：パケットの最大長をバイト単位で入力します。

    Drop packets sent to client that exceed length indicated by the RR：Resource Record で指定された長さを超えるパケットがクライアントに送信された場合はドロップします。
- Mismatch Rate：このタブで DNS の ID 不一致レートを設定します。
  - Enable Logging when DNS ID mismatch rate exceeds specified rate：DNS 識別子の不一致が多く発生した場合にレポートを表示します。

    Mismatch Instance Threshold：不一致のインスタンスの最大数を入力します。この値を超えない場合、システム メッセージ ログに出力されません。

    Time Interval：監視間隔時間（秒単位）を入力します。

- Inspections：このタブで DNS 検査のコンフィギュレーションを表示して、追加や編集ができます。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：DNS 検査の基準を示します。
  - Value：DNS 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add DNS Inspect ダイアログボックスが開き、DNS 検査を追加できます。
  - Edit：Edit DNS Inspect ダイアログボックスが開き、DNS 検査を編集できます。
  - Delete：DNS 検査を削除します。
  - Move Up：検査をリストの上に移動します。
  - Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

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 DNS Inspect

Configuration > Global Objects > Inspect Maps > DNS > DNS Inspect Map > Advanced View > Add/Edit DNS Inspect

Add/Edit DNS Inspect ダイアログボックスで DNS 検査マップの照合基準と値を定義します。

フィールド

- Single Match：DNS 検査に照合文が 1 つだけの場合に指定します。
- Match Type：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。
- Criterion：DNS トラフィックに適用する照合基準を指定します。
  - Header Flag：ヘッダーの DNS フラグを照合します。
  - Type：DNS クエリーまたはリソース レコードのタイプを照合します。
  - Class：DNS クエリーまたはリソース レコードのクラスを照合します。
  - Question：DNS の問い合せを照合します。
  - Resource Record：DNS リソース レコードを照合します。
  - Domain Name：DNS クエリーやリソース レコードのドメイン名を照合します。
- Header Flag Criterion Values：DNS ヘッダー フラグの照合値の詳細を指定します。
  - Match Option：完全一致または全ビット一致（ビット マスク一致）のどちらかを指定します。
  - Match Value：ヘッダー フラグについて名前と値のどちらを照合するか指定します。

    Header Flag Name：照合するヘッダー フラグ名を 1 つ以上選択できます。AA（authoritative answer）、QR（query）、RA（recursion available）、RD（recursion denied）、TC（truncation）のフラグ ビットがあります。

Header Flag Value：任意の 16 ビットの値を 16 進数で入力して照合できます。

- Type Criterion Values：DNS タイプの照合値の詳細を指定します。
  - DNS Type Field Name：選択する DNS タイプを一覧表示します。

    A：IPv4 アドレス

    NS：信頼できるネーム サーバ

    CNAME：正規名

    SOA：信頼ゾーンの開始

    TSIG：トランザクション シグニチャ

    IXFR：差分（ゾーン）転送

    AXFR：完全（ゾーン）転送
  - DNS Type Field Value：DNS タイプ フィールドについて値と範囲のどちらを照合するか指定します。

    Value：0 ～ 65535 の範囲の値を入力して照合できます。

    Range：範囲を入力して照合します。両方とも 0 ～ 65535 の範囲の値を指定します。
- Class Criterion Values：DNS クラスの照合値の詳細を指定します。
  - DNS Class Field Name : インターネットで照合する DNS クラス フィールド名を指定します。
  - DNS Class Field Value：DNS クラス フィールドについて値と範囲のどちらを照合するか指定します。

    Value：0 ～ 65535 の範囲の値を入力して照合できます。

    Range：範囲を入力して照合します。両方とも 0 ～ 65535 の範囲の値を指定します。
- Question Criterion Values：DNS の問い合せセクションの照合方法を指定します。
- Resource Record Criterion Values : DNS リソース レコードのセクションの照合方法を指定します。
  - Resource Record：照合対象セクションを一覧表示します。

    Additional：DNS 追加リソース レコード

    Answer：DNS 応答リソース レコード

    Authority：DNS 認証リソース レコード
- Domain Name Criterion Values：DNS ドメイン名の照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Multiple Matches：DNS 検査の複数の照合文を指定します。
  - DNS Traffic Class：DNS トラフィック クラスを照合します。
  - Manage：Manage DNS Class Maps ダイアログボックスが開き、DNS クラスマップの追加、編集、削除ができます。
- Actions：プライマリ アクションおよびログを設定します。
  - Primary Action：マスク、パケットをドロップ、接続をドロップ、なし。
  - Log：イネーブルまたはディセーブル
  - Enforce TSIG：適用強制しない、パケットをドロップ、ログに出力、パケットをドロップしてログに出力。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Manage Class Maps

Configuration > Global Objects > Inspect Maps > DNS > DNS Inspect Map > Advanced View > Add DNS Inspect > Multiple Matches > Manage DNS Class Maps

Manage Class Map ダイアログボックスで、検査のクラスマップを設定します。

検査クラスマップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラスマップを検査マップから特定して、アクションをイネーブルにします。クラスマップを作成することと検査マップでトラフィックの照合を直接定義することの違いは、クラスマップでは複雑な照合基準を作成でき、クラスマップを再利用できるという点です。検査クラスマップは DNS、FTP、H.323、HTTP、インスタント メッセージ（IM）、SIP のアプリケーションでサポートされます。

フィールド

- Name：クラスマップの名前を示します。
- Match Conditions：クラスマップに設定されているタイプ、照合基準、値を示します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：クラスマップの基準を示します。
  - Value：クラスマップで照合する値を示します。
- Description：クラスマップの説明を示します。
- Add：クラスマップの照合条件を追加します。
- Edit：クラスマップの照合条件を編集します。
- Delete：クラスマップの照合条件を削除します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

ESMTP Inspect Map

Configuration > Global Objects > Inspect Maps > ESMTP

ESMTP ペインで、ESMTP アプリケーションの事前に設定された検査マップを表示します。ESMTP マップでは、ESMTP アプリケーション検査のデフォルト設定値を変更できます。

スパム、フィッシング、不正な形式のメッセージ、バッファ オーバーフロー / アンダーフローなどの攻撃の大部分は ESMTP トラフィックから発生するので、ESMTP トラフィックのパケットを詳細に検査して制御します。アプリケーション セキュリティとプロトコルで正常な ESMTP メッセージだけを通し、各種の攻撃の検出、送受信者およびメール中継のブロックも行います。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    コマンドラインの長さが 512 を超える場合、ログを出力

    コマンドの宛先の数が 100 を超える場合、ログを出力

    本文の行の長さが 1000 を超える場合、ログを出力

    送信者のアドレスの長さが 320 を超える場合、ログを出力

    MIME ファイル名の長さが 255 を超える場合、ログを出力
  - Medium

    サーバ バナーを難読化

    コマンドラインの長さが 512 を超える場合、接続をドロップ

    コマンドの宛先の数が 100 を超える場合、接続をドロップ

    本文の行の長さが 1000 を超える場合、接続をドロップ

    送信者のアドレスの長さが 320 を超える場合、接続をドロップ

    MIME ファイル名の長さが 255 を超える場合、接続をドロップ
  - High

    サーバ バナーを難読化

    コマンドラインの長さが 512 を超える場合、接続をドロップ

    コマンドの宛先の数が 100 を超える場合、接続をドロップ

    本文の行の長さが 1000 を超える場合、接続をドロップ

    送信者のアドレスの長さが 320 を超える場合、接続をドロップしてログを出力

    MIME ファイル名の長さが 255 を超える場合、接続をドロップしてログを出力
  - Customize：Customize Security Level ダイアログボックスが開き、追加の設定を行います。
  - Default Level：セキュリティ レベルをデフォルトの Low レベルに戻します。
  - MIME File Type Filtering : MIME Type Filtering ダイアログボックスが開き、MIME ファイル タイプのフィルタを設定できます。
- ESMTP Inspect Maps：定義されている ESMTP 検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの ESMTP エリアにもリストされます。
- Add：新規の ESMTP 検査マップを、ESMTP Inspect Maps テーブルの定義リストと Inspect Maps ツリーの ESMTP エリアに追加します。ESMTP マップを新たに設定するには、Inspect Maps ツリーで ESMTP のエントリを選択します。
- Delete：ESMTP Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの ESMTP エリアからも削除されます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Customize Security Level

Configuration > Global Objects > Inspect Maps > ESMTP > Customize Security Level

Customize Security Level ダイアログボックスで、ESMTP アプリケーションの事前に設定された検査マップにセキュリティ設定を行います。

フィールド

- Settings：ESMTP のセキュリティ設定とアクションを指定します。
  - Mask server banner：バナーを難読化します。
  - Configure Mail Relay：ESMTP のメール中継をイネーブルにします。

    Domain Name：ローカル ドメインを指定します。

    Action：接続をドロップまたはログに出力します。

    Log：イネーブルまたはディセーブルにします。
  - Check for command line length：コマンドラインの長さと指定した長さの照合をイネーブルにします。

    Minimum Length：設定されている最低限必要な長さを示します。

    Action：リセット、接続をドロップ、またはログに出力します。

    Log：イネーブルまたはディセーブルにします。
  - Check for command recipient count：コマンドの宛先の数を指定した数に照合します。

    Minimum Count：設定されている最低限必要な数を示します。

    Action：リセット、接続をドロップ、またはログに出力します。

    Log：イネーブルまたはディセーブルにします。
  - Check for body line length：本文の行の長さと指定した長さの照合をイネーブルにします。

    Minimum Length：設定されている最低限必要な長さを示します。

    Action：リセット、接続をドロップ、またはログに出力します。

    Log：イネーブルまたはディセーブルにします。
  - Check for sender address length：送信者のアドレスの長さと指定した長さの照合をイネーブルにします。

    Minimum Length：設定されている最低限必要な長さを示します。

    Action：リセット、接続をドロップ、またはログに出力します。

    Log：イネーブルまたはディセーブルにします。
  - Check for MIME file name length：MIME ファイル名の長さと指定した長さの照合をイネーブルにします。

    Minimum Length：設定されている最低限必要な長さを示します。

    Action：リセット、接続をドロップ、またはログに出力します。

    Log：イネーブルまたはディセーブルにします。

- Reset to predefined security level：セキュリティ レベルの設定を、あらかじめ定義された High、Medium、または Low のレベルにリセットします。デフォルトは Low です。
  - Reset to：セキュリティ設定（High、Medium、Low）を指定します。
  - Reset：選択したレベルに設定をリセットします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

MIME File Type Filtering

Configuration > Global Objects > Inspect Maps > ESMTP > MIME File Type Filtering

MIME File Type Filtering ダイアログボックスで、MIME ファイル タイプのフィルタを設定します。

フィールド

- Match Type：一致タイプを示します。肯定一致と否定一致があります。
- Criterion：検査の基準を示します。
- Value：検査で照合する値を示します。
- Action：照合条件が一致したときのアクションを示します。
- Log：ログの状態を示します。
- Add : Add MIME File Type Filter ダイアログボックスが開き、MIME ファイル タイプのフィルタを追加できます。
- Edit : Edit MIME File Type Filter ダイアログボックスが開き、MIME ファイル タイプのフィルタを編集できます。
- Delete：MIME ファイル タイプのフィルタを削除します。
- Move Up：エントリをリストの上に移動します。
- Move Down：エントリをリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

ESMTP Inspect Map Basic View

Configuration > Global Objects > Inspect Maps > ESMTP > ESMTP Inspect Map > Basic View

ESMTP Inspect Map Basic View ペインで、ESMTP 検査マップの設定済みデータを表示します。Advanced View から設定できます。

フィールド

- Name：すでに設定されている ESMTP マップの名前を示します。
- Description：ESMTP マップの説明を 200 文字以内で入力します。
- Security Level：現在のセキュリティ設定を表示します。
  - Customize：Customize Security Level ダイアログボックスが開き、セキュリティ設定を行います。
  - Default Level：セキュリティ レベルをデフォルトに戻します。
- MIME File Type Filtering：MIME Type Filtering ダイアログボックスが開き、MIME ファイル タイプのフィルタを設定できます。
- Advanced View：セキュリティ設定を行います。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

ESMTP Inspect Map Advanced View

Configuration > Global Objects > Inspect Maps > ESMTP > ESMTP Inspect Map > Advanced View

ESMTP Inspect Map Advanced View ペインで、検査マップを設定できます。

フィールド

- Name：すでに設定されている ESMTP マップの名前を示します。
- Description：ESMTP マップの説明を 200 文字以内で入力します。
- Parameters：このタブで ESMTP 検査マップのパラメータを設定します。
  - Mask server banner：バナーを難読化します。
  - Configure Mail Relay：ESMTP のメール中継をイネーブルにします。
    Domain Name：ローカル ドメインを指定します。
    Action：接続をドロップまたはログに出力します。
    Log：イネーブルまたはディセーブルにします。
- Inspections：このタブで ESMTP 検査のコンフィギュレーションを表示して、追加や編集ができます。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：ESMTP 検査の基準を示します。
  - Value：ESMTP 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。

- Add：Add ESMTP Inspect ダイアログボックスが開き、ESMTP 検査を追加できます。
- Edit：Edit ESMTP Inspect ダイアログボックスが開き、ESMTP 検査を編集できます。
- Delete：ESMTP 検査を削除します。
- Move Up：検査をリストの上に移動します。
- Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

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 ESMTP Inspect

Configuration > Global Objects > Inspect Maps > ESMTP > ESMTP Inspect Map > Advanced View > Add/Edit ESMTP Inspect

Add/Edit ESMTP Inspect ダイアログボックスで、ESMTP 検査マップの照合基準と値を定義します。

フィールド

- Match Type：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。
- Criterion：ESMTP トラフィックに適用する照合基準を指定します。
  - Body Length：本文の長さと指定した長さをバイト単位で照合します。
  - Body Line Length：本文の行の長さと指定した長さをバイト単位で照合します。
  - Commands：ESMTP プロトコルで交換されるコマンドを照合します。
  - Command Recipient Count：コマンド宛先の数が指定した数より大きい場合に照合します。
  - Command Line Length：コマンドラインが指定した長さより長い場合に、バイト単位で照合します。
  - EHLO Reply Parameters：ESMTP の EHLO 応答パラメータを照合します。
  - Header Length：ヘッダーの長さと指定した長さをバイト単位で照合します。
  - Header To Fields Count：ヘッダーの To フィールドの数が指定した数より大きい場合に照合します。
  - Invalid Recipients Count：無効な宛先の数が指定した数より大きい場合に照合します。
  - MIME File Type：MIME ファイル タイプを照合します。
  - MIME Filename Length：MIME ファイル名を照合します。
  - MIME Encoding：MIME の符号化を照合します。
  - Sender Address：送信者の電子メール アドレスを照合します。
  - Sender Address Length：送信者の電子メール アドレスの長さを照合します。
- Body Length Criterion Values：本文の長さの照合値に関する詳細を指定します。
  - Greater Than Length：本文の長さをバイト単位で指定します。
  - Action：リセット、接続をドロップ、またはログに出力します。
  - Log：イネーブルまたはディセーブルにします。

- Body Line Length Criterion Values：本文の行の長さの照合値に関する詳細を指定します。
  - Greater Than Length：本文の行の長さをバイト単位で指定します。
  - Action：リセット、接続をドロップ、またはログに出力します。
  - Log：イネーブルまたはディセーブルにします。
- Commands Criterion Values：コマンドの照合値の詳細を指定します。
  - Available Commands テーブル

    AUTH
    DATA
    EHLO
    ETRN
    HELO
    HELP
    MAIL
    NOOP
    QUIT
    RCPT
    RSET
    SAML
    SOML
    VRFY
  - Add : Available Commands テーブルで選択したコマンドを Selected Commands テーブルに追加します。
  - Remove：選択したコマンドを Selected Commands テーブルから削除します。
  - Primary Action：Mask、Reset、Drop Connection、None、Limit Rate (pps)。
  - Log：イネーブルまたはディセーブルにします。
  - Rate Limit：Do not limit rate、Limit Rate (pps)。
- Command Recipient Count Criterion Values : コマンド宛先の数の照合値に関する詳細を指定します。
  - Greater Than Count：コマンド宛先の数を指定します。
  - Action：リセット、接続をドロップ、またはログに出力します。
  - Log：イネーブルまたはディセーブルにします。
- Command Line Length Criterion Values：コマンドラインの長さの値に関する詳細を指定します。
  - Greater Than Length：コマンドラインの長さをバイト単位で指定します。
  - Action：リセット、接続をドロップ、またはログに出力します。
  - Log：イネーブルまたはディセーブルにします。
- EHLO Reply Parameters Criterion Values：EHLO 応答パラメータの照合値の詳細を指定します。
  - Available Parameters テーブル

    8bitmime
    auth
    binarymime
    checkpoint
    dsn
    ecode
    etrn
    others

pipelining

size

vrfy

- Add：Available Parameters テーブルで選択したパラメータを Selected Parameters テーブルに追加します。
- Remove：選択したパラメータを Selected Parameters テーブルから削除します。
- Action：Reset、Drop Connection、Mask、Log。
- Log：イネーブルまたはディセーブルにします。

- Header Length Criterion Values：ヘッダーの長さの照合値に関する詳細を指定します。
  - Greater Than Length：ヘッダーの長さをバイト単位で指定します。
  - Action：Reset、Drop Connection、Mask、Log。
  - Log：イネーブルまたはディセーブルにします。
- Header To Fields Count Criterion Values：ヘッダーの To フィールド数の照合値に関する詳細を指定します。
  - Greater Than Count：ヘッダーの To フィールド数を指定します。
  - Action：リセット、接続をドロップ、またはログに出力します。
  - Log：イネーブルまたはディセーブルにします。
- Invalid Recipients Count Criterion Values：無効な宛先の数の照合値に関する詳細を指定します。
  - Greater Than Count：無効な宛先の数を指定します。
  - Action：リセット、接続をドロップ、またはログに出力します。
  - Log：イネーブルまたはディセーブルにします。
- MIME File Type Criterion Values：MIME ファイル タイプの照合値の詳細を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
  - Action：リセット、接続をドロップ、またはログに出力します。
  - Log：イネーブルまたはディセーブルにします。
- MIME Filename Length Criterion Values：MIME ファイル名の長さの照合値に関する詳細を指定します。
  - Greater Than Length：MIME ファイル名の長さをバイト単位で指定します。
  - Action：Reset、Drop Connection、Log。
  - Log：イネーブルまたはディセーブルにします。
- MIME Encoding Criterion Values：MIME の符号化の照合値に関する詳細を指定します。
  - Available Encodings テーブル

    7bit

    8bit

    base64

    binary

    others

    quoted-printable
  - Add：Available Encodings テーブルで選択したパラメータを Selected Encodings テーブルに追加します。
  - Remove：選択したパラメータを Selected Encodings テーブルから削除します。

- Action：Reset、Drop Connection、Log。
- Log：イネーブルまたはディセーブルにします。

- Sender Address Criterion Values：送信者アドレスの照合値の詳細を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
  - Action：Reset、Drop Connection、Log。
  - Log：イネーブルまたはディセーブルにします。
- Sender Address Length Criterion Values：送信者アドレスの長さの照合値に関する詳細を指定します。
  - Greater Than Length：送信者アドレスの長さをバイト単位で指定します。
  - Action：Reset、Drop Connection、Log。
  - Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

FTP Inspect Map

Configuration > Global Objects > Inspect Maps > FTP

FTP ペインで、FTP アプリケーションの事前に設定された検査マップを表示します。FTP マップでは、FTP アプリケーション検査のデフォルト設定値を変更できます。

厳密な FTP 検査には、セキュリティと制御を向上させるためのコマンド フィルタリングとセキュリティ チェック機能が用意されています。プロトコルとの適合性の検査には、パケットの長さのチェック、デリミタとパケットの形式のチェック、コマンドのターミネータのチェック、およびコマンドの検証が含まれます。

また、ユーザの値に基づいて FTP 接続をブロックできるので、FTP サイトにダウンロード用のファイルを置き、アクセスを特定のユーザだけに制限できます。ファイル名、サーバ名、および他のアトリビュートに基づいて、FTP 接続をブロックできます。検査時に FTP 接続が拒否されると、システム メッセージのログが作成されます。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（Medium または Low）を選択します。
  - Low

    Mask Banner：ディセーブル

    Mask Reply：ディセーブル

- Medium：デフォルト

  Mask Banner：イネーブル

  Mask Reply：イネーブル
- Customize：Customize Security Level ダイアログボックスが開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトの Medium レベルに戻します。
- File Type Filtering：Type Filtering ダイアログボックスが開き、ファイル タイプのフィルタを設定できます。

- FTP Inspect Maps：定義されている FTP 検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの FTP エリアにもリストされます。
- Add：新規の FTP 検査マップを、FTP Inspect Maps テーブルの定義リストと Inspect Maps ツリーの FTP エリアに追加します。FTP マップを新たに設定するには、Inspect Maps ツリーで FTP のエントリを選択します。
- Delete：FTP Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの FTP エリアからも削除されます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Customize Security Level

Configuration > Global Objects > Inspect Maps > FTP > Customize Security Level

Customize Security Level ダイアログボックスで、FTP アプリケーションの事前に設定された検査マップにセキュリティ設定を行います。

フィールド

- Settings：FTP のセキュリティ設定とアクションを指定します。
  - Mask greeting banner from the server：FTP サーバとの接続時に表示されるバナーをマスクし、クライアントに対するサーバ情報の公開を防止します。
  - Mask reply to SYST command：syst コマンドに対する応答をマスクし、クライアントに対するサーバ情報の公開を防止します。
- Reset to predefined security level：セキュリティ レベルの設定を、あらかじめ定義された High、Medium、または Low のレベルにリセットします。デフォルトは Medium です。
  - Reset to：セキュリティ設定（High、Medium、Low）を指定します。
  - Reset：選択したレベルに設定をリセットします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

File Type Filtering

Configuration > Global Objects > Inspect Maps > FTP > MIME File Type Filtering

File Type Filtering ダイアログボックスで、ファイル タイプ フィルタを設定します。

フィールド

- Match Type：一致タイプを示します。肯定一致と否定一致があります。
- Criterion：検査の基準を示します。
- Value：検査で照合する値を示します。
- Action：照合条件が一致したときのアクションを示します。
- Log：ログの状態を示します。
- Add：Add File Type Filter ダイアログボックスが開き、ファイル タイプのフィルタを追加できます。
- Edit：Edit File Type Filter ダイアログボックスが開き、ファイル タイプのフィルタを編集できます。
- Delete：ファイル タイプのフィルタを削除します。
- Move Up：エントリをリストの上に移動します。
- Move Down：エントリをリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

FTP Inspect Map Basic View

Configuration > Global Objects > Inspect Maps > FTP > FTP Inspect Map > Basic View

FTP Inspect Map Basic View ペインで、FTP 検査マップの設定済みデータを表示します。Advanced View から設定できます。

フィールド

- Name：すでに設定されている FTP マップの名前を示します。
- Description：FTP マップの説明を 200 文字以内で入力します。
- Security Level：現在のセキュリティ設定を表示します。
  - Customize：Customize Security Level ダイアログボックスが開き、セキュリティ設定を行います。
  - Default Level：セキュリティ レベルをデフォルトに戻します。
- File Type Filtering：Type Filtering ダイアログボックスが開き、ファイル タイプのフィルタを設定できます。
- Advanced View：セキュリティ設定を行います。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

FTP Inspect Map Advanced View

Configuration > Global Objects > Inspect Maps > FTP > FTP Inspect Map > Advanced View

FTP Inspect Map Advanced View ペインで、検査マップを設定できます。

フィールド

- Name：すでに設定されている FTP マップの名前を示します。
- Description：FTP マップの説明を 200 文字以内で入力します。
- Parameters：このタブで FTP 検査マップのパラメータを設定します。
  - Mask greeting banner from the server：FTP サーバとの接続時に表示されるバナーをマスクし、クライアントに対するサーバ情報の公開を防止します。
  - Mask reply to SYST command : syst コマンドに対する応答をマスクし、クライアントに対するサーバ情報の公開を防止します。
- Inspections：このタブで FTP 検査のコンフィギュレーションを表示して、追加や編集ができます。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：FTP 検査の基準を示します。
  - Value：FTP 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add FTP Inspect ダイアログボックスが開き、FTP 検査を追加できます。
  - Edit：Edit FTP Inspect ダイアログボックスが開き、FTP 検査を編集できます。
  - Delete：FTP 検査を削除します。
  - Move Up：検査をリストの上に移動します。
  - Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

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 FTP Map

Configuration > Global Objects > Inspect Maps > FTP > FTP Inspect Map > Advanced View > Add/Edit FTP Inspect

Add/Edit FTP Inspect ダイアログボックスで、FTP 検査マップの照合基準と値を定義します。

フィールド

- Single Match：FTP 検査に照合文が 1 つだけの場合に指定します。
- Match Type：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。
- Criterion：FTP トラフィックに適用する照合基準を指定します。
  - Request Command：FTP 要求コマンドを照合します。
  - File Name：FTP 転送のファイル名を照合します。
  - File Type：FTP 転送のファイル タイプを照合します。
  - Server：FTP サーバを照合します。
  - User Name：FTP ユーザを照合します。
- Request Command Criterion Values：FTP 要求コマンドの照合値の詳細を指定します。
  - 要求コマンド

    APPE：ファイルに追加するコマンド

    CDUP：現在の作業ディレクトリの親ディレクトリに移動するコマンド

    DELE：ファイルを削除するコマンド

    GET：ファイルを取得するコマンド

    HELP：ヘルプ情報を提供するコマンド

    MKD：ディレクトリを作成するコマンド

    PUT：ファイルを送信するコマンド

    RMD：ディレクトリを削除するコマンド

    RNFR：変更元ファイル名を指定するコマンド

    RNTO：変更先ファイル名を指定するコマンド

    SITE：サーバ システム固有のコマンド。通常、リモート管理に使用します。

    STOU：一意のファイル名を使用してファイル名を保存するコマンド
- File Name Criterion Values：FTP ファイル名の照合値の詳細を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- File Type Criterion Values：FTP ファイル タイプの照合値の詳細を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Server Criterion Values：FTP サーバの照合値の詳細を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。

  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- User Name Criterion Values：FTP ユーザ名の照合値の詳細を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Multiple Matches：FTP 検査の複数の照合文を指定します。
  - FTP Traffic Class：FTP トラフィック クラスを照合します。
  - Manage：Manage FTP Class Maps ダイアログボックスが開き、FTP クラスマップの追加、編集、削除ができます。
- Action：リセットします。
- Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

GTP Inspect Map

Configuration > Global Objects > Inspect Maps > GTP

GTP ペインで、GTP アプリケーションの事前に設定された検査マップを表示します。GTP マップでは、GTP アプリケーション検査のデフォルト設定値を変更できます。

GTP は比較的新しいプロトコルで、インターネットなど TCP/IP ネットワークと無線接続する場合のセキュリティを提供します。GTP マップを使用して、タイムアウト値、メッセージ サイズ、トンネル数、セキュリティ アプライアンスを通過する GTP バージョンを制御できます。

（注） GTP 検査には、特別なライセンスが必要です。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベルは常に Low です。
  - エラーを許可しない
  - トンネルの最大数：500
  - GSN タイムアウト：00:30:00
  - PDP コンテキスト タイムアウト：00:30:00
  - 要求タイムアウト：00:01:00
  - シグナリング タイムアウト：00:30:00
  - トンネル タイムアウト：01:00:00
  - T3 応答タイムアウト：00:00:20
  - 未知のメッセージ ID をドロップしてログを出力
- Customize：Customize Security Level ダイアログボックスが開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトに戻します。
- IMSI Prefix Filtering：IMSI Prefix Filtering ダイアログボックスが開き、IMSI プレフィックス フィルタを設定できます。
- GTP Inspect Maps：定義されている GTP 検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの GTP エリアにも表示されます。
- Add：新規の GTP 検査マップを、GTP Inspect Maps テーブルの定義リストと Inspect Maps ツリーの GTP エリアに追加します。GTP マップを新たに設定するには、Inspect Maps ツリーで GTP のエントリを選択します。
- Delete：GTP Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの GTP エリアからも削除されます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Customize Security Level

Configuration > Global Objects > Inspect Maps > GTP > Customize Security Level

Customize Security Level ダイアログボックスで、GTP アプリケーションの事前に設定された検査マップにセキュリティ設定を行います。

フィールド

- Permit Errors : 無効なパケットや検査時にエラーが見つかったパケットを、ドロップしないでセキュリティ アプライアンスから送信します。デフォルトでは、無効なパケットや解析中に失敗したパケットはドロップされます。
- Drop and Log unknown message IDs : 未知のメッセージ ID は、すべてドロップしてログを出力します。
- Maximum Number of Requests：許容される要求キュー サイズのデフォルト最大値を変更できます。要求キュー サイズのデフォルト最大値は 200 です。キューで応答待ちができる GTP 要求数の最大値を指定します。1 ～ 9999999 の範囲で指定できます。
- Maximum Number of Tunnels : 許容されるトンネル数のデフォルト最大値を変更できます。デフォルトのトンネル制限値は 500 です。許容するトンネル数の最大値を指定します。グローバルなトンネル全体の制限値を 1 ～ 9999999 の範囲で指定できます。
- Timeouts
  - GSN timeout : GSN を削除するまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。
  - PDP-Context timeout : GTP セッションで PDP コンテキストを受け取るまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。
  - Request Queue : GTP セッション中に GTP メッセージを受け取るまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 1 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。
  - Signaling : GTP シグナリングを削除するまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。
  - Tunnel : GTP トンネルの非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 1 時間です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は切断しないことを意味します。
  - Request timeout：GTP 要求のアイドル タイムアウト値を指定します。
  - T3-Response timeout：接続を削除するまでの、応答待ち時間の最大値を指定します。
- Reset to：セキュリティの設定を Low に指定します。
- Reset：選択したレベルに設定をリセットします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

IMSI Prefix Filtering

Configuration > Global Objects > Inspect Maps > GTP > IMSI Prefix Filtering

IMSI Prefix タブで、GTP 要求の中で使用できるように IMSI プレフィックスを定義します。

フィールド

- Mobile Country Code：0 以外の 3 桁の値でモバイル カントリ コードを定義します。1 桁または 2 桁の値を指定すると、先頭に 0 が付加されて 3 桁になります。
- Mobile Network Code：2 桁または 3 桁の数字でネットワーク コードを定義します。
- Add：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルに追加します。
- Delete：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

GTP Inspect Map Basic View

Configuration > Global Objects > Inspect Maps > GTP > GTP Inspect Map > Basic View

GTP Inspect Map Basic View ペインで、GTP 検査マップの設定済みデータを表示します。Advanced View から設定できます。

フィールド

- Name：すでに設定されている GTP マップの名前を示します。
- Description：GTP マップの説明を 200 文字以内で入力します。
- Security Level：現在のセキュリティ設定を表示します。
  - Customize：Customize Security Level ダイアログボックスが開き、セキュリティ設定を行います。
  - Default Level：セキュリティ レベルをデフォルトに戻します。
- IMSI Prefix Filtering：IMSI Prefix Filtering ダイアログボックスが開き、IMSI プレフィックス フィルタを設定できます。
- Advanced View：セキュリティ設定を行います。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

GTP Inspect Map Advanced View

Configuration > Global Objects > Inspect Maps > GTP > GTP Inspect Map > Advanced View

GTP Inspect Map Advanced View ペインで、検査マップを設定できます。

フィールド

- Name：すでに設定されている GTP マップの名前を示します。
- Description：GTP マップの説明を 200 文字以内で入力します。
- Permit Parameters：このタブで GTP 検査マップの許可パラメータを設定します。
  - Object Groups to Add

    From object group：オブジェクト グループを指定して、または Browse ボタンをクリックして、Add Network Object Group ダイアログボックスを開きます。

    To object group：オブジェクト グループを指定して、または Browse ボタンをクリックして、Add Network Object Group ダイアログボックスを開きます。
  - Add：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルに追加します。
  - Delete：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルから削除します。
  - Permit Errors：無効なパケットまたは検査時にエラーが見つかったパケットを、ドロップしないでセキュリティ アプライアンスから送信します。デフォルトでは、無効なパケットや解析中に失敗したパケットはドロップされます。
- General Parameters：このタブで GTP 検査マップの一般パラメータを設定します。
  - Maximum Number of Requests：許容される要求キュー サイズのデフォルト最大値を変更できます。要求キュー サイズのデフォルト最大値は 200 です。キューで応答待ちができる GTP 要求数の最大値を指定します。1 ～ 9999999 の範囲で指定できます。
  - Maximum Number of Tunnels：許容されるトンネル数のデフォルト最大値を変更できます。デフォルトのトンネル制限値は 500 です。許容するトンネル数の最大値を指定します。グローバルなトンネル全体の制限値を 1 ～ 9999999 の範囲で指定できます。
  - Timeouts

    GSN timeout：GSN を削除するまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

    PDP-Context timeout：GTP セッションで PDP コンテキストを受け取るまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

    Request Queue：GTP セッション中に GTP メッセージを受け取るまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 1 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

Signaling：GTP シグナリングを削除するまでの、非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 30 分です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は、切断しないことを意味します。

Tunnel：GTP トンネルの非アクティブ期間のデフォルト最大値を変更できます。デフォルトは 1 時間です。タイムアウト値を *hh*:*mm*:*ss* 形式で指定します。ここで *hh* は時間、*mm* は分、*ss* は秒です。値 0 は切断しないことを意味します。

Request timeout：GTP 要求のアイドル タイムアウト値を指定します。

T3-Response timeout：接続を削除するまでの、応答待ち時間の最大値を指定します。

- IMSI Prefix Filtering：このタブで GTP 検査マップの IMSI プレフィックス フィルタリングを設定します。
  - Mobile Country Code：0 以外の 3 桁の値でモバイル カントリ コードを定義します。1 桁または 2 桁の値を指定すると、先頭に 0 が付加されて 3 桁になります。
  - Mobile Network Code：2 桁または 3 桁の数字でネットワーク コードを定義します。
  - Add：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルに追加します。
  - Delete：指定したカントリ コードとネットワーク コードを IMSI Prefix テーブルから削除します。
- Inspections：このタブで GTP 検査マップを設定します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：GTP 検査の基準を示します。
  - Value：GTP 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add GTP Inspect ダイアログボックスが開き、GTP 検査を追加できます。
  - Edit：Edit GTP Inspect ダイアログボックスが開き、GTP 検査を編集できます。
  - Delete：GTP 検査を削除します。
  - Move Up：検査をリストの上に移動します。
  - Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

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 GTP Map

Configuration > Global Objects > Inspect Maps > GTP > GTP Inspect Map > Add/Edit GTP Map

Add/Edit GTP Inspect ダイアログボックスで、GTP 検査マップの照合基準と値を定義します。

フィールド

- Match Type：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。
- Criterion：GTP トラフィックに適用する照合基準を指定します。

- Access Point Name：アクセス ポイント名を照合します。
- Message ID：メッセージ ID を照合します。
- Message Length：メッセージの長さを照合します。
- Version：バージョンを照合します。

- Access Point Name Criterion Values：照合するアクセス ポイント名を指定します。デフォルトでは、有効な APN のメッセージをすべて検査します。すべての APN が指定できます。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
  - Action：Drop。
  - Log：イネーブルまたはディセーブルにします。
- Message ID Criterion Values：照合するメッセージの数値識別子を指定します。有効な指定範囲は 1 ～ 255 です。デフォルトでは、すべての有効なメッセージ ID が対象です。
  - Value：値を完全一致で照合するか、範囲で照合するかを指定します。

    Equals：値を入力します。

    Range：値の範囲を入力します。
  - Action：Drop packet または limit rate (pps)。
  - Log：イネーブルまたはディセーブルにします。
- Message Length Criterion Values：許可される UDP ペイロードの、メッセージの長さのデフォルト最大値を変更できます。
  - Minimum value : UDP ペイロードの最小バイト数を指定します。1 ～ 65536 の範囲の値を指定できます。
  - Maximum value：UDP ペイロードの最大バイト数を指定します。1 ～ 65536 の範囲の値を指定できます。
  - Action：Drop packet。
  - Log：イネーブルまたはディセーブルにします。
- Version Criterion Values : 照合するメッセージの GTP バージョンを指定します。有効な指定範囲は 0 ～ 255 です。0 は Version 0、1 は Version 1 を示します。GTP の Version 0 はポート 3386 を使用し、Version 1 はポート 2123 を使用します。デフォルトでは、すべての GTP バージョンが対象です。
  - Value：値を完全一致で照合するか、範囲で照合するかを指定します。

    Equals：値を入力します。

    Range：値の範囲を入力します。
  - Action：Drop packet。
  - Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

H.323 Inspect Map

Configuration > Global Objects > Inspect Maps > H.323

H.323 ペインで、H.323 アプリケーションの事前に設定された検査マップを表示します。H.323 マップでは、H.323 アプリケーション検査のデフォルト設定値を変更できます。

H.323 検査は RAS、H.225、H.245 をサポートし、埋め込まれた IP アドレスとポートをすべて変換する機能を備えています。ステートのトラッキングとフィルタリングを実行し、検査機能のアクティベーションをカスケードできます。H.323 検査は、電話番号のフィルタリング、T.120 のダイナミック制御、H.245 のトンネル機能制御、プロトコルのステート トラッキング、H.323 通話時間制限の適用、音声 / ビデオ制御をサポートします。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    H.225 状態確認：ディセーブル

    RAS 状態確認：ディセーブル

    発信側の番号：ディセーブル

    通話制限時間：ディセーブル

    RTP 準拠：適用強制しない
  - Medium

    H.225 状態確認：イネーブル

    RAS 状態確認：イネーブル

    発信側の番号：ディセーブル

    通話制限時間：ディセーブル

    RTP 準拠：適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用：しない
  - High

    H.225 状態確認：イネーブル

    RAS 状態確認：イネーブル

    発信側の番号：イネーブル

    通話制限時間：1:00:00

    RTP 準拠：適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用：する
  - Customize：Customize Security Level ダイアログボックスが開き、追加の設定を行います。
  - Default Level：セキュリティ レベルをデフォルトの Medium レベルに戻します。
  - Phone Number Filtering：Phone Number Filtering ダイアログボックスが開き、電話番号フィルタを設定できます。
- H.323 Inspect Maps：定義されている H.323 検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの H.323 エリアにもリストされます。
- Add：新規の H.323 検査マップを、H.323 Inspect Maps テーブルの定義リストと Inspect Maps ツリーの H.323 エリアに追加します。H.323 マップを新たに設定するには、Inspect Maps ツリーで H.323 のエントリを選択します。
- Delete：H.323 Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの H.323 エリアからも削除されます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Customize Security Level

Configuration > Global Objects > Inspect Maps > H323 > Customize Security Level

Customize Security Level ダイアログボックスで、H.323 アプリケーションの事前に設定された検査マップにセキュリティ設定を行います。

フィールド

- Settings：H.323 のセキュリティ設定とアクションを指定します。
  - Check state transition of H.225 messages : H.323 の状態確認を H.225 メッセージに適用します。
  - Check state transition of RAS messages：H.323 の状態確認を RAS メッセージに適用します。
  - Enforce call duration limit：通話を一定の時間で制限します。

    Call Duration Limit：通話制限時間（hh:mm:ss）。
  - Enforce presence of calling and called party numbers : 通話設定時に、強制的に発信側の番号を送信します。
  - Check RTP packets for protocol conformance : ピンホールの RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。

    Limit payload to audio or video, based on the signaling exchange : ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。
- Reset to predefined security level : セキュリティ レベルの設定を、あらかじめ定義された High、Medium、または Low のレベルにリセットします。デフォルトは Low です。
  - Reset to：セキュリティ設定（High、Medium、Low）を指定します。
  - Reset：選択したレベルに設定をリセットします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Phone Number Filtering

Configuration > Global Objects > Inspect Maps > H323 > Phone Number Filtering

Phone Number Filtering ダイアログボックスで、電話番号のフィルタを設定します。

フィールド

- Match Type：一致タイプを示します。肯定一致と否定一致があります。
- Criterion：検査の基準を示します。
- Value：検査で照合する値を示します。
- Action：照合条件が一致したときのアクションを示します。
- Log：ログの状態を示します。
- Add : Add Phone Number Filter ダイアログボックスが開き、電話番号のフィルタを追加できます。
- Edit：Edit Phone Number Filter ダイアログボックスが開き、電話番号を編集できます。
- Delete：電話番号のフィルタを削除します。
- Move Up：エントリをリストの上に移動します。
- Move Down：エントリをリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

H.323 Inspect Map Basic View

Configuration > Global Objects > Inspect Maps > H323 > H323 Inspect Map > Basic View

H323 Inspect Map Basic View ペインで、H.323 検査マップの設定済みデータを表示します。Advanced View から設定できます。

フィールド

- Name：すでに設定されている H.323 マップの名前を示します。
- Description：H.323 マップの説明を 200 文字以内で入力します。
- Security Level：現在のセキュリティ設定を表示します。
  - Customize：Customize Security Level ダイアログボックスが開き、セキュリティ設定を行います。
  - Default Level：セキュリティ レベルをデフォルトに戻します。
- Phone Number Filtering：Phone Number Filtering ダイアログボックスが開き、電話番号のフィルタを設定できます。
- Advanced View：セキュリティ設定を行います。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

H.323 Inspect Map Advanced View

Configuration > Global Objects > Inspect Maps > H323 > H323 Inspect Map > Advanced View

H.323 Inspect Map Advanced View ペインで、検査マップを設定できます。

フィールド

- Name：すでに設定されている H.323 マップの名前を示します。
- Description：H.323 マップの説明を 200 文字以内で入力します。
- State Checking：このタブで H.323 検査マップの状態確認パラメータを設定します。
  - Check state transition of H.225 messages : H.323 の状態確認を H.225 メッセージに適用します。
  - Check state transition of RAS messages：H.323 の状態確認を RAS メッセージに適用します。
- Call Attributes：このタブで H.323 検査マップのコール アトリビュート パラメータを設定します。
  - Enforce call duration limit：通話を一定の時間で制限します。

    Call Duration Limit：通話制限時間（hh:mm:ss）。
  - Enforce presence of calling and called party numbers：通話設定時に、強制的に発信側の番号を送信します。
- Tunneling and Protocol Conformance：このタブで H.323 検査マップのトンネリングとプロトコル準拠パラメータを設定します。
  - Check for H.245 tunneling：H.245 のトンネリングを許可します。

    Action：Drop Connection または Log。
  - Check RTP packets for protocol conformance : ピンホールの RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。

    Limit payload to audio or video, based on the signaling exchange : ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。
- HSI Group Parameters：このタブで HSI グループを設定します。
  - HSI Group ID：HSI グループの ID を示します。
  - IP Address：HSI グループの IP アドレスを示します。
  - Endpoints：HSI グループのエンドポイントを示します。
  - Add：Add HSI Group ダイアログボックスが開き、HSI グループを追加できます。
  - Edit：Edit HSI Group ダイアログボックスが開き、HSI グループを編集できます。
  - Delete：HSI グループを削除します。
- Inspections：このタブで H.323 検査のコンフィギュレーションを表示して、追加や編集ができます。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：H.323 検査の基準を示します。
  - Value：H.323 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。

- Log：ログの状態を示します。
- Add：Add H.323 Inspect ダイアログボックスが開き、H.323 検査を追加できます。
- Edit：Edit H.323 Inspect ダイアログボックスが開き、H.323 検査を編集できます。
- Delete：H.323 検査を削除します。
- Move Up：検査をリストの上に移動します。
- Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

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 HSI Group

Configuration > Global Objects > Inspect Maps > H323 > H323 Inspect Map > Advanced View > Add/Edit HSI Group

Add/Edit HSI Group ダイアログボックスで、HSI グループを設定できます。

フィールド

- Group ID：HSI のグループ ID を入力します。
- IP Address：HSI の IP アドレスを入力します。
- Endpoints：エンドポイントの IP アドレスとインターフェイスを設定します。
  - IP Address：エンドポイントの IP アドレスを入力します。
  - Interface：エンドポイントのインターフェイスを指定します。
- Add：定義された HSI グループを追加します。
- Delete：選択した HSI グループを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 H.323 Map

Configuration > Global Objects > Inspect Maps > H323 > H323 Inspect Map > Advanced View > Add/Edit H323 Inspect

Add/Edit H.323 Inspect ダイアログボックスで H.323 検査マップの照合基準と値を定義します。

フィールド

- Single Match：H.323 検査に照合文が 1 つだけの場合に指定します。
- Match Type：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。
- Criterion：H.323 トラフィックに適用する照合基準を指定します。
  - Called Party：受信側を照合します。
  - Calling Party：発信元を照合します。
  - Media Type：メディア タイプを照合します。
- Called Party Criterion Values：H.323 受信側の照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Calling Party Criterion Values：H.323 発信元の照合方法を指定します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Media Type Criterion Values：照合するメディア タイプを指定します。
  - Audio：音声タイプを照合します。
  - Video：ビデオ タイプを照合します。
  - Data：データ タイプを照合します。
- Multiple Matches：H.323 検査の複数の照合文を指定します。
  - H323 Traffic Class：H.323 トラフィック クラスを照合します。
  - Manage : Manage H.323 Class Maps ダイアログボックスが開き、H.323 クラスマップの追加、編集、削除ができます。
- Action：Drop Packet、Drop Connection、Reset。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

HTTP Inspect Map

Configuration > Global Objects > Inspect Maps > HTTP

HTTP ペインで、HTTP アプリケーションの事前に設定された検査マップを表示します。HTTP マップでは、HTTP アプリケーション検査のデフォルト設定値を変更できます。

HTTP アプリケーション検査で HTTP のヘッダーと本文をスキャンし、さまざまなデータ チェックができます。これらのチェックで、HTTP 構築、コンテンツ タイプ、トンネル プロトコル、メッセージ プロトコルなどがセキュリティ アプライアンスを通過することを防止します。

HTTP アプリケーション検査でトンネル アプリケーションと ASCII 以外の文字を含む HTTP 要求や応答をブロックして、悪意のあるコンテンツが Web サーバに到達することを防ぎます。HTTP 要求や応答ヘッダーのさまざまな要素のサイズ制限、URL のブロッキング、HTTP サーバ ヘッダー タイプのスプーフィングもサポートされています。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    プロトコル違反時のアクション：Drop Connection

    安全でない方式の接続ドロップ：ディセーブル

    要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ：ディセーブル

    URI フィルタリング：設定しない

    高度な検査：設定しない
  - Medium

    プロトコル違反時のアクション：Drop Connection

    安全でない方式の接続ドロップ：GET、HEAD、POST だけを許可

    要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ：ディセーブル

    URI フィルタリング：設定しない

    高度な検査：設定しない
  - High

    プロトコル違反時のアクション：Drop Connection と Log

    安全でない方式の接続ドロップ：GET、HEAD だけを許可

    要求のヘッダーに ASCII 以外の文字が含まれる場合の接続ドロップ：イネーブル

    URI フィルタリング：設定しない

    高度な検査：設定しない
  - Customize：Customize Security Level ダイアログボックスが開き、追加の設定を行います。
  - Default Level：セキュリティ レベルをデフォルトの Medium レベルに戻します。
  - URI Filtering：URI Filtering ダイアログボックスが開き、URI フィルタを設定できます。
- HTTP Inspect Maps：定義されている HTTP 検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの HTTP エリアにも表示されます。
- Add：新規の HTTP 検査マップを、HTTP Inspect Maps テーブルの定義リストと Inspect Maps ツリーの HTTP エリアに追加します。HTTP マップを新たに設定するには、Inspect Maps ツリーで HTTP のエントリを選択します。
- Delete：HTTP Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの HTTP エリアからも削除されます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Customize Security Level

Configuration > Global Objects > Inspect Maps > HTTP > Customize Security Level

Customize Security Level ダイアログボックスで、HTTP アプリケーションの事前に設定された検査マップにセキュリティ設定を行います。

フィールド

- Settings：HTTP のセキュリティ設定とアクションを指定します。
  - Check for protocol violations：HTTP プロトコル違反の有無をチェックします。

    Action：Drop Connection、Reset、Log。

    Log：イネーブルまたはディセーブルにします。
  - Drop connections for unsafe methods：安全でない方式の有無をチェックし、接続をドロップします。

    Allow Only：GET、HEAD、GET、HEAD、POST を許可します。
  - Drop connections for requests with non-ASCII headers : メッセージ ヘッダーに ASCII 以外の文字が含まれているかどうかをチェックします。
- Reset to predefined security level : セキュリティ レベルの設定を、あらかじめ定義された High、Medium、または Low のレベルにリセットします。デフォルトは Low です。
  - Reset to：セキュリティ設定（High、Medium、Low）を指定します。
  - Reset：選択したレベルに設定をリセットします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

URI Filtering

Configuration > Global Objects > Inspect Maps > HTTP > URI Filtering

URI Filtering ダイアログボックスで、URI フィルタを設定できます。

フィールド

- Match Type：一致タイプを示します。肯定一致と否定一致があります。
- Criterion：検査の基準を示します。

- Value：検査で照合する値を示します。
- Action：照合条件が一致したときのアクションを示します。
- Log：ログの状態を示します。
- Add：Add URI Filtering ダイアログボックスが開き、URI フィルタを追加できます。
- Edit：Edit URI Filtering ダイアログボックスが開き、URI フィルタを編集できます。
- Delete：URI フィルタを削除します。
- Move Up：エントリをリストの上に移動します。
- Move Down：エントリをリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

HTTP Inspect Map Basic View

Configuration > Global Objects > Inspect Maps > HTTP > HTTP Inspect Map > Basic View

HTTP Inspect Map Basic View ペインで、HTTP 検査マップの設定済みデータを表示します。Advanced View から設定できます。

フィールド

- Name：すでに設定されている HTTP マップの名前を示します。
- Description：HTTP マップの説明を 200 文字以内で入力します。
- Security Level：現在のセキュリティ設定を表示します。
  - Customize：Customize Security Level ダイアログボックスが開き、セキュリティ設定を行います。
  - Default Level：セキュリティ レベルをデフォルトに戻します。
- URI Filtering：URI Filtering ダイアログボックスが開き、URI フィルタを設定します。
- Advanced View：セキュリティ設定を行います。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

HTTP Inspect Map Advanced View

Configuration > Global Objects > Inspect Maps > HTTP > HTTP Inspect Map > Advanced View

HTTP Inspect Map Advanced View ペインで、検査マップを設定できます。

フィールド

- Name：すでに設定されている HTTP マップの名前を示します。
- Description：HTTP マップの説明を 200 文字以内で入力します。
- Parameters：このタブで HTTP 検査マップのパラメータを設定します。
  - Check for protocol violations：HTTP プロトコル違反の有無をチェックします。

    Action：Drop Connection、Reset、Log。

    Log：イネーブルまたはディセーブルにします。
  - Spoof server string：サーバの HTTP ヘッダーの値を指定の文字列で置き換えます。

    Spoof String：サーバのヘッダー フィールドと置き換える文字列を入力します。最大 82 文字まで入力できます。
  - Body Match Maximum：HTTP メッセージの本文照合時に検索される、最大文字数です。デフォルトは 200 バイトです。大きな値を指定すると、パフォーマンスに大きな影響を与えます。
- Inspections：このタブで HTTP 検査のコンフィギュレーションを表示して、追加や編集ができます。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：HTTP 検査の基準を示します。
  - Value：HTTP 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add HTTP Inspect ダイアログボックスが開き、HTTP 検査を追加できます。
  - Edit：Edit HTTP Inspect ダイアログボックスが開き、HTTP 検査を編集できます。
  - Delete：HTTP 検査を削除します。
  - Move Up：検査をリストの上に移動します。
  - Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

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 HTTP Map

Configuration > Global Objects > Inspect Maps > HTTP > HTTP Inspect Map > Advanced View > Add/Edit HTTP Inspect

Add/Edit HTTP Inspect ダイアログボックスで、HTTP 検査マップの照合基準と値を定義します。

フィールド

- Single Match：HTTP 検査に照合文が 1 つだけの場合に指定します。
- Match Type：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。
- Criterion：HTTP トラフィックに適用する照合基準を指定します。
  - Request/Response Content Type Mismatch : 応答のコンテンツ タイプを、要求の accept フィールドの MIME タイプの 1 つに一致させるかどうかを指定します。
  - Request Arguments：要求の引数を正規表現で照合します。

    Regular Expression：照合する定義された正規表現を一覧表示します。

    Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

    Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

    Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
  - Request Body Length：要求の本文に指定したバイト数より長いフィールドがある場合、正規表現で照合します。

    Greater Than Length : 要求フィールドの長さと照合するフィールドの値をバイト単位で入力します。
  - Request Body：要求の本文を正規表現で照合します。

    Regular Expression：照合する定義された正規表現を一覧表示します。

    Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

    Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

    Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
  - Request Header Field Count：要求ヘッダーのフィールド数が最大値の場合、正規表現で照合します。

    Predefined：要求のヘッダー フィールドを次の中から指定します。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。

    Regular Expression：照合する定義された正規表現を一覧表示します。

    Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

    Greater Than Count：ヘッダー フィールド数の最大値を入力します。
  - Request Header Field Length：要求ヘッダーに指定したバイト数より長いフィールドがある場合、正規表現で照合します。

    Predefined：要求のヘッダー フィールドを次の中から指定します。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。

    Regular Expression：照合する定義された正規表現を一覧表示します。

Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

Greater Than Length：要求フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- Request Header Field：要求ヘッダーを正規表現で照合します。

  Predefined：要求のヘッダー フィールドを次の中から指定します。accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

- Request Header Count：要求ヘッダー数が最大値の場合、正規表現で照合します。

  Greater Than Count：ヘッダー数の最大値を入力します。

- Request Header Length：要求ヘッダーが指定したバイト数より長い場合、正規表現で照合します。

  Greater Than Length：ヘッダーの長さをバイト単位で入力します。

- Request Header non-ASCII：要求ヘッダーに含まれる ASCII 以外の文字を照合します。

- Request Method：要求の方式を正規表現で照合します。

  Method：照合する要求方式を次の中から指定します。bcopy、bdelete、bmove、bpropfind、bproppatch、connect、copy、delete、edit、get、getattribute、getattributenames、getproperties、head、index、lock、mkcol、mkdir、move、notify、options、poll、post、propfind、proppatch、put、revadd、revlabel、revlog、revnum、save、search、setattribute、startrev、stoprev、subscribe、trace、unedit、unlock、unsubscribe。

  Regular Expression：正規表現の照合方法を指定します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

- Request URI Length：要求の URI が指定したバイト数より長い場合、正規表現で照合します。

  Greater Than Length：URI の長さをバイト単位で入力します。

- Request URI：要求の URI を正規表現で照合します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

- Response Body：要求の本文を regex で照合します。

  ActiveX：ActiveX の照合方法を指定します。

  Java Applet：Java アプレットの照合方法を指定します。

  Regular Expression：正規表現の照合方法を指定します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

- Response Body Length : 応答の本文に指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  Greater Than Length : 応答フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- Response Header Field Count：応答ヘッダーのフィールド数が最大値の場合、正規表現で照合します。

  Predefined : 応答のヘッダー フィールドを次の中から指定します。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、 www-authenticate。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Greater Than Count：ヘッダー フィールド数の最大値を入力します。

- Response Header Field Length : 応答ヘッダーに指定したバイト数より長いフィールドがある場合、正規表現で照合します。

  Predefined : 応答のヘッダー フィールドを次の中から指定します。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、 www-authenticate。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Greater Than Length : 応答フィールドの長さと照合するフィールドの値をバイト単位で入力します。

- Response Header Field：応答ヘッダーを正規表現で照合します。

  Predefined : 応答のヘッダー フィールドを次の中から指定します。accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、 www-authenticate。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

- Response Header Count：応答ヘッダー数が最大値の場合、正規表現で照合します。

  Greater Than Count：ヘッダー数の最大値を入力します。

- Response Header Length：応答ヘッダーが指定したバイト数より長い場合、正規表現で照合します。

  Greater Than Length：ヘッダーの長さをバイト単位で入力します。

- Response Header non-ASCII：応答ヘッダーに含まれる ASCII 以外の文字を照合します。

- Response Status Line：ステータス行を正規表現で照合します。

  Regular Expression：照合する定義された正規表現を一覧表示します。

  Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。

  Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。

- Multiple Matches：HTTP 検査の複数の照合文を指定します。
  - H323 Traffic Class：HTTP トラフィック クラスを照合します。
  - Manage : Manage HTTP Class Maps ダイアログボックスが開き、HTTP クラスマップの追加、編集、削除ができます。
- Action：Drop Connection、Reset、Log。
- Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Instant Messaging (IM) Inspect Map

Configuration > Global Objects > Inspect Maps > IM

IM ペインで、インスタント メッセージ（IM）アプリケーションの事前に設定された検査マップを表示します。インスタント メッセージ（IM）マップでは、インスタント メッセージ（IM）アプリケーション検査のデフォルト設定値を変更できます。

インスタント メッセージ（IM）アプリケーション検査で、ネットワーク アクセスの使用量を詳細に制御できます。また、機密情報の漏洩やその他の攻撃からネットワークを守ります。正規表現データベースのさまざまな検索パターンを使って、インスタント メッセージ（IM）をフィルタできます。フローが認識されない場合は、syslog が生成されます。

スコープを限定するには、アクセスリストから検査するトラフィック ストリームを指定します。UDP メッセージの場合、対応する UDP ポート番号も設定できます。Yahoo! Messenger および MSN Messenger のインスタント メッセージの検査もサポートされています。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- IM Inspect Maps：定義されている IM 検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの IM エリアにも表示されます。
- Add : 新規の IM 検査マップを、IM Inspect Maps テーブルの定義リストと Inspect Maps ツリーの IM エリアに追加します。IM マップを新たに設定するには、Inspect Maps ツリーで IM のエントリを選択します。
- Delete : IM Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの IM エリアからも削除されます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Instant Messaging (IM) Inspect Map View

Configuration > Global Objects > Inspect Maps > IM > IM Inspect Map > View

IM Inspect Map View ペインで、検査マップを設定できます。

フィールド

- Name：すでに設定されている IM マップの名前を示します。
- Description：IM マップの説明を 200 文字以内で入力します。
- Match Type：一致タイプを示します。肯定一致と否定一致があります。
- Criterion：IM 検査の基準を示します。
- Value：IM 検査で照合する値を示します。
- Action：照合条件が一致したときのアクションを示します。
- Log：ログの状態を示します。
- Add：Add IM Inspect ダイアログボックスが開き、IM 検査を追加できます。
- Edit：Edit IM Inspect ダイアログボックスが開き、IM 検査を編集できます。
- Delete：IM 検査を削除します。
- Move Up：検査をリストの上に移動します。
- Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

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 IM Map

Configuration > Global Objects > Inspect Maps > IM > IM Inspect Map > View > Add/Edit IM Inspect

Add/Edit IM Inspect ダイアログボックスで、IM 検査マップの照合基準と値を定義します。

フィールド

- Single Match：IM 検査に照合文が 1 つだけの場合に指定します。
- Match Type：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。

- Criterion：IM トラフィックに適用する照合基準を指定します。
  - Protocol：IM プロトコルを照合します。
  - Service：IM サービスを照合します。
  - Source IP Address：送信元 IP アドレスを照合します。
  - Destination IP Address：宛先 IP アドレスを照合します。
  - Version：IM ファイル転送のサービス バージョンを照合します。
  - Client Login Name：IM サービスのクライアント ログイン名を照合します。
  - Client Peer Login Name：IM サービスのクライアントのピア ログイン名を照合します。
  - Filename：IM ファイル転送サービスのファイル名を照合します。
- Protocol Criterion Values：照合する IM プロトコルを指定します。
  - Yahoo! Messenger：Yahoo! Messenger のインスタント メッセージを照合します。
  - MSN Messenger：MSN Messenger のインスタント メッセージを照合します。
- Service Criterion Values：照合する IM サービスを指定します。
  - Chat：IM メッセージ チャット サービスを照合します。
  - Conference：IM コンファレンス サービスを照合します。
  - File Transfer：IM ファイル転送サービスを照合します。
  - Games：IM ゲーム サービスを照合します。
  - Voice Chat：IM 音声チャット サービスを照合します（Yahoo の IM は対象外です）。
  - Web Cam：IM Web カメラ サービスを照合します。
- Source IP Address Criterion Values：IM サービスで照合する送信元 IP アドレスを指定します。
  - IP Address：IM サービスの送信元 IP アドレスを入力します。
  - IP Mask：送信元 IP アドレスのマスクです。
- Destination IP Address Criterion Values：IM サービスで照合する宛先 IP アドレスを指定します。
  - IP Address：IM サービスの宛先 IP アドレスを入力します。
  - IP Mask：宛先 IP アドレスのマスクです。
- Version Criterion Values：IM ファイル転送サービスで照合するバージョンを指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Client Login Name Criterion Values：IM サービスで照合するクライアント ログイン名を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Client Peer Login Name Criterion Values：IM サービスで照合するクライアントのピア ログイン名を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Filename Criterion Values：IM ファイル転送サービスで照合するファイル名を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現の設定を行います。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップの設定を行います。
- Multiple Matches：IM 検査の複数の照合文を指定します。
  - IM Traffic Class：IM トラフィック クラスを照合します。
  - Manage：Manage IM Class Maps ダイアログボックスが開き、IM クラスマップの追加、編集、削除ができます。
- Action：Drop Connection、Reset、Log。
- Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

IPSec Pass Through Inspect Map

Configuration > Global Objects > Inspect Maps > IPSec Pass Through

IPSec Pass Through ペインで、IPSec パススルーの事前に設定された検査マップを表示します。IPSec パススルー マップでは、IPSec パススルー アプリケーション検査のデフォルト設定値を変更できます。IPSec パススルー マップを使用すると、アクセスリストを参照しなくても、特定のフローを許可できます。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト

    クライアントごとの最大 ESP フロー：制限なし

    ESP アイドル タイムアウト：00:10:00

    クライアントごとの最大 AH フロー：制限なし

    AH アイドル タイムアウト：00:10:00
  - High

    クライアントごとの最大 ESP フロー：10

    ESP アイドル タイムアウト：00:00:30

    クライアントごとの最大 AH フロー：10

    AH アイドル タイムアウト：00:00:30

- Customize：Customize Security Level ダイアログボックスが開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトの Low レベルに戻します。

- IPSec Pass Through Inspect Maps：定義されている IPSec パススルー検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの IPSec Pass Through エリアにも表示されます。
- Add : 新規の IPSec パススルー検査マップを、IPSec Pass Through Inspect Maps テーブルの定義リストと Inspect Maps ツリーの IPSec Pass Through エリアに追加します。IPSec パススルー マップを新たに設定するには、Inspect Maps ツリーで IPSec Pass Through のエントリを選択します。
- Delete：IPSec Pass Through Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの IPSec Pass Through エリアからも削除されます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Customize Security Level

Configuration > Global Objects > Inspect Maps > IPSec Pass Through > Customize Security Level

Customize Security Level ダイアログボックスで、IPSec パススルー アプリケーションの事前に設定された検査マップにセキュリティ設定を行います。

フィールド

- Settings：IPSec パススルーのセキュリティ設定とアクションを指定します。
  - Limit ESP flows per client：クライアントごとの ESP フローを制限します。
    Maximum：最大限度を指定します。
  - Apply ESP idle timeout：ESP アイドル タイムアウトを適用します。
    Timeout：タイムアウト値を指定します。
  - Limit AH flows per client：クライアントごとの AH フローを制限します。
    Maximum：最大限度を指定します。
  - Apply AH idle timeout：AH アイドル タイムアウトを適用します。
    Timeout：タイムアウト値を指定します。
- Reset to predefined security level：セキュリティ レベルの設定を、あらかじめ定義された High、Medium、または Low のレベルにリセットします。デフォルトは Low です。
  - Reset to：セキュリティ設定（High、Medium、Low）を指定します。
  - Reset：選択したレベルに設定をリセットします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

IPSec Pass Through Inspect Map Basic View

Configuration > Global Objects > Inspect Maps > IPSec Pass Through > IPSec Pass Through Inspect Map > Basic View

IPSec Pass Through Inspect Map Basic View ペインで、検査マップの基本設定を行います。

フィールド

- Description：検査マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト
    クライアントごとの最大 ESP フロー：制限なし
    ESP アイドル タイムアウト：00:10:00
    クライアントごとの最大 AH フロー：制限なし
    AH アイドル タイムアウト：00:10:00
  - High
    クライアントごとの最大 ESP フロー：10
    ESP アイドル タイムアウト：00:00:30
    クライアントごとの最大 AH フロー：10
    AH アイドル タイムアウト：00:00:30
  - Customize：Customize Security Level ダイアログボックスが開き、追加の設定を行います。
  - Default Level：セキュリティ レベルをデフォルトの Low レベルに戻します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

IPSec Pass Through Inspect Map Advanced View

Configuration > Global Objects > Inspect Maps > IPSec Pass Through > IPSec Pass Through Inspect Map > Advanced View

IPSec Pass Through Inspect Map Advanced View ペインで、検査マップの詳細設定を行います。

フィールド

- Name：すでに設定されている IPSec パススルー マップの名前を示します。
- Description：IPSec パススルー検査マップの説明を 200 文字以内で入力します。
- Limit ESP flows per client：クライアントごとの ESP フローを制限します。
  - Maximum：最大限度を指定します。
- Apply ESP idle timeout：ESP アイドル タイムアウトを適用します。
  - Timeout：タイムアウト値を指定します。
- Limit AH flows per client：クライアントごとの AH フローを制限します。
  - Maximum：最大限度を指定します。
- Apply AH idle timeout：AH アイドル タイムアウトを適用します。
  - Timeout：タイムアウト値を指定します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

MGCP Inspect Map

Configuration > Global Objects > Inspect Maps > MGCP

MGCP ペインで、MGCP アプリケーションの事前に設定された検査マップを表示します。MGCP マップでは、MGCP アプリケーション検査のデフォルト設定値を変更できます。MGCP マップを使用して、VoIP デバイスと MGCP コール エージェント間の接続を管理できます。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- Command Queue Size：キューに入れるコマンドの最大数を指定します。1 ～ 2147483647 の範囲の値を指定できます。
- Gateways and Call Agents：Gateways and Call Agents ダイアログボックスが開き、MGCP マップを追加できます。
- MGCP Inspect Maps：定義されている MGCP 検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの MGCP エリアにも表示されます。
- Add：新規の MGCP 検査マップを、MGCP Inspect Maps テーブルの定義リストと Inspect Maps ツリーの MGCP エリアに追加します。MGCP マップを新たに設定するには、Inspect Maps ツリーで MGCP のエントリを選択します。
- Delete：MGCP Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの MGCP エリアからも削除されます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Gateways and Call Agents

Configuration > Global Objects > Inspect Maps > MGCP > Gateways and Call Agents

Gateways and Call Agents ダイアログボックスで、ゲートウェイとコール エージェントのグループをマップに設定します。

フィールド

- Group ID：コール エージェント グループの ID を識別します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。ゲートウェイの IP アドレスは、1 つのグループ ID だけに関連付けできます。同じゲートウェイを別のグループ ID で使用できません。1 ～ 2147483647 の範囲の値を指定できます。
- Criterion：検査の基準を示します。
- Gateways：関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスを識別します。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。
- Call Agents：コール エージェント グループの MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを識別します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
- Add：Add MGCP ダイアログボックスが表示され、新規のアプリケーション検査マップを定義できます。
- Edit：Edit MGCP ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

MGCP Inspect Map View

Configuration > Global Objects > Inspect Maps > MGCP > MGCP Inspect Map > View

MGCP Inspect Map View ペインで、検査マップを設定できます。

フィールド

- Name：すでに設定されている MGCP マップの名前を示します。
- Description：MGCP マップの説明を 200 文字以内で入力します。
- Command Queue：このタブで MGCP コマンドの許容キュー サイズを指定します。
  - Command Queue Size：キューに入れるコマンドの最大数を指定します。1 ～ 2147483647 の範囲の値を指定できます。
- Gateways and Call Agents : このタブでゲートウェイとコール エージェント グループをマップに設定します。
  - Group ID : コール エージェント グループの ID を識別します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。ゲートウェイの IP アドレスは、1 つのグループ ID だけに関連付けできます。同じゲートウェイを別のグループ ID で使用できません。1 ～ 2147483647 の範囲の値を指定できます。
  - Criterion：検査の基準を示します。
  - Gateways : 関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスを識別します。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。
  - Call Agents : コール エージェント グループの MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを識別します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
  - Add：Add MGCP Group ダイアログボックスが表示され、ゲートウェイとコール エージェントの新規の MGCP グループを定義できます。
  - Edit : Edit MGCP ダイアログボックスが表示され、Gateways and Call Agents テーブルで選択した MGCP グループを修正できます。
  - Delete：Gateways and Call Agents テーブルで選択した MGCP グループを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 MGCP Group

Configuration > Global Objects > Inspect Maps > MGCP > Add/Edit MGCP Group

Add/Edit MGCP Group ダイアログボックスで、MGCP アプリケーション検査がイネーブルのときに使用される MGCP グループのコンフィギュレーションを定義します。

フィールド

- Group ID：コール エージェント グループの ID を指定します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。0 ～ 2147483647 の範囲の値を指定できます。
- Gateways エリア
  - Gateway to Be Added：関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスを指定します。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。
  - Add：指定した IP アドレスを IP アドレス テーブルに追加します。
  - Delete：選択した IP アドレスを IP アドレス テーブルから削除します。
  - IP Address：コール エージェント グループに設定されているゲートウェイの IP アドレスを一覧表示します。
- Call Agents
  - Call Agent to Be Added：コール エージェント グループの MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを指定します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
  - Add：指定した IP アドレスを IP アドレス テーブルに追加します。
  - Delete：選択した IP アドレスを IP アドレス テーブルから削除します。
  - IP Address：コール エージェント グループに設定されているコール エージェントの IP アドレスを一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

NetBIOS Inspect Map

Configuration > Global Objects > Inspect Maps > NetBIOS

NetBIOS ペインで、NetBIOS アプリケーションの事前に設定された検査マップを表示します。NetBIOS マップでは、NetBIOS アプリケーション検査のデフォルト設定値を変更できます。

NetBIOS アプリケーション検査では、NetBIOS ネーム サービス パケットおよび NetBIOS データグラム サービス パケットに埋め込まれている IP アドレスで NAT を実行します。また、プロトコル準拠チェックを行って、さまざまなフィールドの数や長さの整合性を確認します。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。

- Description：検査マップの説明を 200 文字以内で入力します。
- Check for protocol violations：プロトコル違反の有無をチェックして、指定したアクションを実行します。
  - Action：Drop packet または Log。
  - Log：イネーブルまたはディセーブルにします。
- NetBIOS Inspect Maps：定義されている NetBIOS 検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの NetBIOS エリアにも表示されます。
- Add：新規の NetBIOS 検査マップを、NetBIOS Inspect Maps テーブルの定義リストと Inspect Maps ツリーの NetBIOS エリアに追加します。NetBIOS マップを新たに設定するには、Inspect Maps ツリーで NetBIOS のエントリを選択します。
- Delete：NetBIOS Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの NetBIOS エリアからも削除されます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

NetBIOS Inspect Map View

Configuration > Global Objects > Inspect Maps > NetBIOS > NetBIOS Inspect Map > View

NetBIOS Inspect Map View ペインで、検査マップを設定できます。

フィールド

- Name：すでに設定されている NetBIOS マップの名前を示します。
- Description：NetBIOS マップの説明を 200 文字以内で入力します。
- Check for protocol violations：プロトコル違反の有無をチェックして、指定したアクションを実行します。
  - Action：Drop packet または Log。
  - Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

RADIUS Inspect Map

Configuration > Global Objects > Inspect Maps > RADIUS

RADIUS ペインで、RADIUS アプリケーションの事前に設定された検査マップを表示します。RADIUS マップで、RADIUS アプリケーション検査に使用されるデフォルト設定値を変更することができます。また、過剰請求攻撃の防御にも利用されます。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- RADIUS Inspect Maps：定義されている RADIUS 検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの RADIUS エリアにも表示されます。
- Add:新規の RADIUS 検査マップを、RADIUS Inspect Maps テーブルの定義リストと Inspect Maps ツリーの RADIUS エリアに追加します。RADIUS マップを新たに設定するには、Inspect Maps ツリーで RADIUS のエントリを選択します。
- Delete：RADIUS Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの RADIUS エリアからも削除されます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

RADIUS Inspect Map Host

Configuration > Global Objects > Inspect Maps > RADIUS > RADIUS Inspect Map > Host

RADIUS Inspect Map Host Parameters ペインで、検査マップのホスト パラメータを設定できます。

フィールド

- Name：すでに設定されている RADIUS アカウンティング マップの名前を示します。
- Description：RADIUS アカウンティング マップの説明を 200 文字以内で入力します。
- Host Parameters：ホストのパラメータを設定できます。
  - Host IP Address：RADIUS メッセージを送信するホストの IP アドレスを指定します。
  - Key：（オプション）キーを指定します。
- Add：ホスト エントリを Host テーブルに追加します。
- Delete：ホスト エントリを Host テーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

RADIUS Inspect Map Other

Configuration > Global Objects > Inspect Maps > RADIUS > RADIUS Inspect Map > Other

RADIUS Inspect Map Other Parameters ペインで、検査マップに追加するパラメータを設定できます。

フィールド

- Name：すでに設定されている RADIUS アカウンティング マップの名前を示します。
- Description：RADIUS アカウンティング マップの説明を 200 文字以内で入力します。
- Other Parameters：追加するパラメータを設定できます。
  - Attribute Number：Accounting Start を受信したときに検証するアトリビュート番号を指定します。
- Add：エントリを Attribute テーブルに追加します。
- Delete：エントリを Attribute テーブルから削除します。
- Send response to the originator of the RADIUS message：RADIUS メッセージを送信したホストに、メッセージを送り返します。
- Enforce timeout：ユーザのタイムアウトをイネーブルにします。
  - Users Timeout：データベースのユーザ タイムアウト値（hh:mm:ss）です。
- Enable detection of GPRS accounting：GPRS アカウンティングの検出をイネーブルにします。このオプションは、GTP/GPRS ライセンスがイネーブルの場合にのみ使用できます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

SCCP (Skinny) Inspect Map

Configuration > Global Objects > Inspect Maps > SCCP (Skinny)

SCCP (Skinny) ペインで、SCCP（Skinny）アプリケーションの事前に設定された検査マップを表示します。SCCP (Skinny) マップでは、SCCP (Skinny) アプリケーション検査のデフォルト設定値を変更できます。

Skinny アプリケーション検査では、パケット データ、ピンホールの動的開放に埋め込まれている IP アドレスとポート番号を変換します。また、追加のプロトコル準拠チェックと基本的なステートフル トラッキングも行います。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High、Midium、Low）を選択します。
  - Low：デフォルト

    登録：適用強制しない

    メッセージの最大 ID：0x181

    プレフィックスの長さの最小値：4

メディア タイムアウト：00:05:00
シグナリング タイムアウト：01:00:00
RTP 準拠：適用強制しない

- Medium

登録：適用強制しない
メッセージの最大 ID：0x141
プレフィックスの長さの最小値：4
メディア タイムアウト：00:01:00
シグナリング タイムアウト：00:05:00
RTP 準拠：適用強制する
ペイロードを音声またはビデオに限定してシグナリング交換を適用：しない

- High

登録：適用強制する
メッセージの最大 ID：0x141
プレフィックスの長さの最小値：4
プレフィックスの長さの最大値：65536
メディア タイムアウト：00:01:00
シグナリング タイムアウト：00:05:00
RTP 準拠：適用強制する
ペイロードを音声またはビデオに限定してシグナリング交換を適用：する

- Customize：Customize Security Level ダイアログボックスが開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトの Low レベルに戻します。

- Message ID Filtering：Messaging ID Filtering ダイアログボックスが開き、メッセージ ID フィルタを設定できます。
- SCCP (Skinny) Inspect Maps：定義されている SCCP (Skinny) 検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの SCCP (Skinny) エリアにも表示されます。
- Add：新規の SCCP (Skinny) 検査マップを、SCCP (Skinny) Inspect Maps テーブルの定義リストと Inspect Maps ツリーの SCCP (Skinny) エリアに追加します。SCCP (Skinny) マップを新たに設定するには、Inspect Maps ツリーで SCCP (Skinny) のエントリを選択します。
- Delete：SCCP (Skinny) Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの SCCP (Skinny) エリアからも削除されます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Customize Security Level

Configuration > Global Objects > Inspect Maps > SCCP (Skinny) > Customize Security Level

Customize Security Level ダイアログボックスで、SCCP (Skinny) アプリケーションの事前に設定された検査マップにセキュリティ設定を行います。

フィールド

- Settings：SCCP (Skinny) のセキュリティ設定とアクションを指定します。
  - Enforce endpoint registration：Skinny エンドポイントを登録してから通話を受発信します。

    Maximum Message ID : SCCP メッセージ ID に使用できる最大値を（0x0 ～ 0xffff の範囲で）指定します。
  - SCCP Prefix Length : Skinny メッセージのプレフィックスの長さを（4 ～ 4,294,967,295 の範囲で）指定します。

    Minimum Prefix Length：SCCP プレフィックスの長さの許容最小値を指定します。

    Maximum Prefix Length：SCCP プレフィックスの長さの許容最大値を指定します。
  - Enable media timeout：メディア タイムアウトをイネーブルにします。

    Media Timeout: メディア接続のタイムアウト値を（0:0:01 ～ 1993:0:0 の範囲で）指定します。
  - Enable signaling timeout：シグナリング タイムアウトをイネーブルにします。

    Signaling Timeout : シグナリング接続のタイムアウト値を（0:0:01 ～ 1993:0:0 の範囲で）指定します。
  - Check RTP packets for protocol conformance : ピンホールをフローする RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。

    Limit payload to audio or video, based on the signaling exchange : ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。
- Reset to predefined security level : セキュリティ レベルの設定を、あらかじめ定義された High、Medium、または Low のレベルにリセットします。デフォルトは Low です。
  - Reset to：セキュリティ設定（High、Medium、Low）を指定します。
  - Reset：選択したレベルに設定をリセットします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Message ID Filtering

Configuration > Global Objects > Inspect Maps > SCCP (Skinny) > Message ID Filtering

Message ID Filtering ダイアログボックスで、メッセージ ID のフィルタを設定します。

フィールド

- Match Type：一致タイプを示します。肯定一致と否定一致があります。
- Criterion：検査の基準を示します。
- Value：検査で照合する値を示します。
- Action：照合条件が一致したときのアクションを示します。

- Log：ログの状態を示します。
- Add：Add Message ID Filtering ダイアログボックスが開き、メッセージ ID のフィルタを追加できます。
- Edit：Edit Message ID Filtering ダイアログボックスが開き、メッセージ ID のフィルタを編集できます。
- Delete：メッセージ ID のフィルタを削除します。
- Move Up：エントリをリストの上に移動します。
- Move Down：エントリをリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

SCCP (Skinny) Inspect Map Basic View

Configuration > Global Objects > Inspect Maps > SCCP (Skinny) > SCCP (Skinny) Inspect Map > Basic View

SCCP (Skinny) Inspect Map Basic View ペインで、SCCP (Skinny) 検査マップの設定済みデータを表示します。Advanced View から設定できます。

フィールド

- Name：すでに設定されている SCCP (Skinny) マップの名前を示します。
- Description：SCCP (Skinny) マップの説明を 200 文字以内で入力します。
- Security Level：現在のセキュリティ設定を示します。
  - Customize：Customize Security Level ダイアログボックスが開き、セキュリティ設定を行います。
  - Default Level：セキュリティ レベルをデフォルトに戻します。
  - Message ID Filtering : Messaging ID Filtering ダイアログボックスが開き、メッセージ ID フィルタを設定できます。
- Advanced View：セキュリティ設定を行います。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

SCCP (Skinny) Inspect Map Advanced View

Configuration > Global Objects > Inspect Maps > SCCP (Skinny) > SCCP (Skinny) Inspect Map > Advanced View

SCCP (Skinny) Inspect Map Advanced View ペインで、検査マップを設定できます。

フィールド

- Name：すでに設定されている SCCP (Skinny) マップの名前を示します。
- Description：SCCP (Skinny) マップの説明を 200 文字以内で入力します。
- Parameters：このタブで SCCP (Skinny) のパラメータを設定します。
  - Enforce endpoint registration：Skinny エンドポイントを登録してから通話を受発信します。
    Maximum Message ID：SCCP メッセージ ID に使用できる最大値を指定します。
  - SCCP Prefix Length：Skinny メッセージのプレフィックスの長さを指定します。
    Minimum Prefix Length：SCCP プレフィックスの長さの許容最小値を指定します。
    Maximum Prefix Length：SCCP プレフィックスの長さの許容最大値を指定します。
  - Media Timeout：メディア接続時のタイムアウト値を指定します。
  - Signaling Timeout：シグナリング接続時のタイムアウト値を指定します。
- RTP Conformance：このタブで SCCP (Skinny) の RTP 準拠を設定します。
  - Check RTP packets for protocol conformance : ピンホールをフローする RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。
    Limit payload to audio or video, based on the signaling exchange : ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。
- Message ID Filtering : このタブで SCCP (Skinny) のメッセージ ID フィルタリングを設定します。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：検査の基準を示します。
  - Value：検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add Message ID Filtering ダイアログボックスが開き、メッセージ ID のフィルタを追加できます。
  - Edit：Edit Message ID Filtering ダイアログボックスが開き、メッセージ ID のフィルタを編集できます。
  - Delete：メッセージ ID のフィルタを削除します。
  - Move Up：エントリをリストの上に移動します。
  - Move Down：エントリをリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

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 Message ID Filter

Configuration > Global Objects > Inspect Maps > SCCP (Skinny) > SCCP (Skinny) Inspect Map > Advanced View > Add/Edit Message ID Filter

Add Message ID Filter ダイアログボックスで、メッセージ ID のフィルタを設定します。

フィールド

- Match Type：トラフィックと値を一致させるかどうかを指定します。
  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。
- Criterion：SCCP (Skinny) トラフィックに適用する照合基準を指定します。
  - Message ID：指定したメッセージ ID を照合します。
    Message ID：SCCP メッセージ ID に使用できる最大値を指定します。
  - Message ID Range：指定範囲のメッセージ ID を照合します。
    Lower Message ID：SCCP メッセージ ID に使用できる下限値を指定します。
    Upper Message ID：SCCP メッセージ ID に使用できる上限値を指定します。
- Action：Drop packet。
- Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

SIP Inspect Map

Configuration > Global Objects > Inspect Maps > SIP

SIP ペインで、SIP アプリケーションの事前に設定された検査マップを表示します。SIP マップでは、SIP アプリケーション検査のデフォルト設定値を変更できます。

SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、インスタント メッセージ機能で幅広く利用されているプロトコルです。もともとテキスト ベースで自由に操作できるこのプロトコルに原因の一端があり、SIP ネットワークのセキュリティは数多くの脅威にさらされています。

SIP アプリケーション検査では、メッセージのヘッダーと本文、ポートの動的開放でアドレス変換を行い、基本的な正常性チェックを行います。また、アプリケーションのセキュリティとプロトコル準拠をサポートし、SIP メッセージの正常性を保つと同時に SIP 関連の脅威を検出します。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- Security Level：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト
    SIP インスタント メッセージ（IM）の拡張機能：イネーブル

SIP トラフィック以外の SIP ポート使用：許可
サーバとエンドポイントの IP アドレスを非表示：ディセーブル
ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル
1 以上の宛先ホップ数を保証：イネーブル
RTP 準拠：適用強制しない
SIP 準拠：ステート チェックとヘッダー検証を実行しない

- Medium

SIP インスタント メッセージ（IM）の拡張機能：イネーブル
SIP トラフィック以外の SIP ポート使用：許可
サーバとエンドポイントの IP アドレスを非表示：ディセーブル
ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル
1 以上の宛先ホップ数を保証：イネーブル
RTP 準拠：適用強制する
ペイロードを音声やビデオに限定してシグナリング交換を適用：しない
SIP 準拠：ステート チェックで失敗したパケットをドロップ

- High

SIP インスタント メッセージ（IM）の拡張機能：イネーブル
SIP トラフィック以外の SIP ポート使用：禁止
サーバとエンドポイントの IP アドレスを非表示：ディセーブル
ソフトウェアのバージョンと SIP 以外の URI をマスク：イネーブル
1 以上の宛先ホップ数を保証：イネーブル
RTP 準拠：適用強制する
ペイロードを音声やビデオに限定してシグナリング交換を適用：する
SIP 準拠：ステート チェックとヘッダー検証で失敗したパケットをドロップ

- Customize：Customize Security Level ダイアログボックスが開き、追加の設定を行います。
- Default Level：セキュリティ レベルをデフォルトの Low レベルに戻します。

- SIP Inspect Maps：定義されている SIP 検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの SIP エリアにも表示されます。
- Add：新規の SIP 検査マップを、SIP Inspect Maps テーブルの定義リストと Inspect Maps ツリーの SIP エリアに追加します。SIP マップを新たに設定するには、Inspect Maps ツリーで SIP のエントリを選択します。
- Delete：SIP Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの SIP エリアからも削除されます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Customize Security Level

Configuration > Global Objects > Inspect Maps > SIP > Customize Security Level

Customize Security Level ダイアログボックスで、SIP アプリケーションの事前に設定された検査マップにセキュリティ設定を行います。

フィールド

- Settings：RTP や SIP 準拠など、SIP の追加設定を行います。
  - Enable SIP instant messaging (IM) extensions：インスタント メッセージの拡張機能をイネーブルにします。デフォルトはイネーブルです。
  - Permit non-SIP traffic on SIP port：SIP トラフィック以外に SIP ポートの使用を許可します。デフォルトは許可です。
  - Hide server's and endpoint's IP addresses：IP アドレスのプライバシーをイネーブルにします。デフォルトはディセーブルです。
  - Mask software version and non-SIP URIs：Alert-Info と Call-Info ヘッダーで SIP 以外の URI 検査をイネーブルにします。
  - Ensure that number of hops to destination is greater than 0：Max-Forwards ヘッダーの値が 0 かどうかのチェックをイネーブルにします。
- RTP Conformance
  - Check RTP packets for protocol conformance：ピンホールをフローする RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。

    Limit payload to audio or video, based on the signaling exchange：ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。
- SIP Conformance
  - Do not perform state checking and header validation：SIP ステート チェックをディセーブルにします。
  - Drop packets that fail state checking：ステート チェックで失敗したパケットをドロップします。
  - Drop connections that fail state checking and packets that fail header validation：ステート チェックで失敗した接続と、SIP メッセージのヘッダー検証で失敗したパケットをドロップします。
- Reset to Predefined Security Level：セキュリティ レベルの設定を、あらかじめ定義された High、Medium、または Low のレベルにリセットします。
  - Reset To：セキュリティ レベルを High、Medium、または Low にリセットします。
- Reset：すべてのセキュリティ設定をデフォルトにリセットします。デフォルトのピンホール タイムアウトは 1 分です。エンドポイント マッパーのデフォルト設定値はありません。
- Criterion：SIP トラフィックに適用する照合基準を指定します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

SIP Inspect Map Basic View

Configuration > Global Objects > Inspect Maps > SIP > SIP Inspect Map > Basic View

SIP Inspect Map Basic View ペインで、SIP 検査マップの設定済みデータを表示します。Advanced View から設定できます。

フィールド

- Name：すでに設定されている SIP マップの名前を示します。
- Description：SIP マップの説明を 200 文字以内で入力します。
- Security Level：現在のセキュリティ設定を示します。
  - Customize：Customize Security Level ダイアログボックスが開き、セキュリティ設定を行います。
  - Default Level：セキュリティ レベルをデフォルトに戻します。
- Advanced View：セキュリティ設定を行います。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

SIP Inspect Map Advanced View

Configuration > Global Objects > Inspect Maps > SIP > SIP Inspect Map > Advanced View

SIP Inspect Map Advanced View ペインで、検査マップを設定できます。

フィールド

- Name：すでに設定されている SIP マップの名前を示します。
- Description：SIP マップの説明を 200 文字以内で入力します。
- Filtering：このタブで SIP のフィルタリングを設定します。
  - Enable SIP instant messaging (IM) extensions：インスタント メッセージの拡張機能をイネーブルにします。デフォルトはイネーブルです。
  - Permit non-SIP traffic on SIP port：SIP トラフィック以外に SIP ポートの使用を許可します。デフォルトは許可です。
- IP Address Privacy：このタブで SIP の IP アドレスのプライバシーを設定します。
  - Hide server's and endpoint's IP addresses：IP アドレスのプライバシーをイネーブルにします。デフォルトはディセーブルです。
- Hop Count：このタブで SIP のホップ数を設定します。
  - Ensure that number of hops to destination is greater than 0：Max-Forwards ヘッダーの値が 0 かどうかのチェックをイネーブルにします。

    Action：Drop packet、Drop Connection、Reset、Log。

    Log：イネーブルまたはディセーブルにします。
- RTP Conformance：このタブで SIP の RTP 準拠を設定します。
  - Check RTP packets for protocol conformance：ピンホールをフローする RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。

    Limit payload to audio or video, based on the signaling exchange：ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。
- SIP Conformance：このタブで SIP の SIP 準拠を設定します。
  - Enable state transition checking：SIP のステート チェックをイネーブルにします。

    Action：Drop packet、Drop Connection、Reset、Log。

Log：イネーブルまたはディセーブルにします。

- Enable strict validation of header fields : SIP ヘッダー フィールドの検証をイネーブルにします。

  Action：Drop packet、Drop Connection、Reset、Log。

  Log：イネーブルまたはディセーブルにします。

- Field Masking：このタブで SIP のフィールド マスクを設定します。
  - Inspect non-SIP URIs：Alert-Info と Call-Info ヘッダーに含まれる SIP 以外の URI 検査をイネーブルにします。

    Action：Mask または Log。

    Log：イネーブルまたはディセーブルにします。
  - Inspect server's and endpoint's software version：User-Agent と Server ヘッダーに含まれる SIP エンドポイントのソフトウェア バージョンを検査します。

    Action：Mask または Log。

    Log：イネーブルまたはディセーブルにします。
- Inspections : このタブで SIP 検査のコンフィギュレーションを表示して、追加や編集ができます。
  - Match Type：一致タイプを示します。肯定一致と否定一致があります。
  - Criterion：SIP 検査の基準を示します。
  - Value：SIP 検査で照合する値を示します。
  - Action：照合条件が一致したときのアクションを示します。
  - Log：ログの状態を示します。
  - Add：Add SIP Inspect ダイアログボックスが開き、SIP 検査を追加できます。
  - Edit：Edit SIP Inspect ダイアログボックスが開き、SIP 検査を編集できます。
  - Delete：SIP 検査を削除します。
  - Move Up：検査をリストの上に移動します。
  - Move Down：検査をリストの下に移動します。

モード

次の表に、この機能を使用できるモードを示します。

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 SIP Inspect

Configuration > Global Objects > Inspect Maps > SIP > SIP Inspect Map > Advanced View > Add/Edit SIP Inspect

Add/Edit SIP Inspect ダイアログボックスで、SIP 検査マップの照合基準と値を定義します。

フィールド

- Single Match：SIP 検査に照合文が 1 つだけの場合に指定します。
- Match Type：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で「No Match」を選択した場合、「example.com」を含むトラフィックはすべてクラスマップの対象外になります。
- Criterion：SIP トラフィックに適用する照合基準を指定します。

- Called Party：To ヘッダーに指定された受信側を照合します。
- Calling Party：From ヘッダーに指定された発信元を照合します。
- Content Length：ヘッダーのコンテンツの長さを照合します。
- Content Type：ヘッダーのコンテンツ タイプを照合します。
- IM Subscriber：SIP IM の加入者を照合します。
- Message Path：SIP の Via ヘッダーを照合します。
- Request Method：SIP の要求方式を照合します。
- Third-Party Registration：サード パーティの登録要求者を照合します。
- URI Length：SIP ヘッダーの URI を照合します。

• Called Party Criterion Values：照合する受信側を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
• Calling Party Criterion Values：照合する発信元を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
• Content Length Criterion Values : 指定値より長い、照合する SIP コンテンツ ヘッダーを指定します。
  - Greater Than Length：ヘッダーの長さをバイト単位で入力します。
• Content Type Criterion Values：照合する SIP コンテンツ ヘッダーのタイプを指定します。
  - SDP：SDP タイプの SIP コンテンツ ヘッダーを照合します。
  - Regular Expression：正規表現を照合します。

    Regular Expression：照合する定義された正規表現を一覧表示します。

    Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。

    Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。

    Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
• IM Subscriber Criterion Values：照合する IM 登録者を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
• Message Path Criterion Values : 照合する SIP の Via ヘッダーを指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage：Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。

- Request Method Criterion Values：照合する SIP 要求方式を指定します。
  - Request Method : 次の中から要求方式を指定します。ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update。
- Third-Party Registration Criterion Values：照合するサード パーティの登録要求者を指定します。正規表現で照合します。
  - Regular Expression：照合する定義された正規表現を一覧表示します。
  - Manage : Manage Regular Expressions ダイアログボックスが開き、正規表現を設定できます。
  - Regular Expression Class：照合する定義された正規表現クラスを一覧表示します。
  - Manage：Manage Regular Expression Class ダイアログボックスが開き、正規表現クラスマップを設定できます。
- URI Length Criterion Values：指定値より長い SIP ヘッダーの URI を指定して照合します。
  - URI type：SIP URI または TEL URI を指定して照合します。
  - Greater Than Length：長さをバイト単位で指定します。
- Multiple Matches：SIP 検査の複数の照合文を指定します。
  - SIP Traffic Class：SIP トラフィック クラスを照合します。
  - Manage：Manage SIP Class Maps ダイアログボックスが開き、SIP クラスマップの追加、編集、削除ができます。
- Actions：プライマリ アクションおよびログを設定します。
  - Action：Drop Packet、Drop Connection、Reset、Log。注：要求方式が invite か register の場合は、Limit rate (pps) アクションを使用できます。
  - Log：イネーブルまたはディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

SNMP Inspect Map

Configuration > Global Objects > Inspect Maps > SNMP

SNMP ペインで、SNMP アプリケーションの事前に設定された検査マップを表示します。SNMP マップでは、SNMP アプリケーション検査のデフォルト設定値を変更できます。

フィールド

- Map Name：すでに設定されているアプリケーション検査マップを一覧表示します。マップのチェックボックスをオンにし、**Edit** をクリックして、既存のマップの表示または変更ができます。
- Disallowed SNMP Versions：特定の SNMP アプリケーション検査マップで拒否される SNMP バージョンを識別します。
- Add：Add SNMP ダイアログボックスが表示され、新規のアプリケーション検査マップを定義できます。
- Edit：Edit SNMP ダイアログボックスが表示され、アプリケーション検査マップ テーブルで選択した検査マップを修正できます。
- Delete：アプリケーション検査マップ テーブルで選択した検査マップを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 SNMP Map

Configuration > Global Objects > Inspect Maps > SNMP > Add/Edit SNMP Map（このダイアログボックスに移動するパスは数種類あります。）

Add/Edit SNMP Map ダイアログボックスで、SNMP のアプリケーション検査を制御する SNMP マップを新規作成できます。

フィールド

- SNMP Map Name：アプリケーション検査マップの名前を定義します。
- SNMP version 1：SNMP バージョン 1 のアプリケーション検査をイネーブルにします。
- SNMP version 2 (party based) : SNMP バージョン 2 のアプリケーション検査をイネーブルにします。
- SNMP version 2c (community based)：SNMP バージョン 2c のアプリケーション検査をイネーブルにします。
- SNMP version 3：SNMP バージョン 3 のアプリケーション検査をイネーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

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。次の項目を取り上げます。

Regular Expressions

Configuration > Global Objects > Regular Expressions

クラスマップの設定や検査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検査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、文字通り正確な文字列として、またはメタ文字を使用してテキスト文字列を照合するので、テキスト文字列の複数のバリアントを照合できます。正規表現を使用すると、特定のアプリケーション トラフィックの内容を照合できます。たとえば、HTTP パケット内部の本文テキストを照合できます。

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の名前を示します。
  - 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、検査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 アイコンの隣りにそれぞれ「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

次の表に、この機能を使用できるモードを示します。

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

Configuration > Global Objects > Regular Expressions > Add/Edit a Regular Expression

Add/Edit Regular Expression ダイアログボックスで、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 6-1 に示すメタ文字を使用するか、または **Build** をクリックして Build Regular Expression 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。

  表 6-1 には特殊な意味を持つメタ文字を一覧表示しています。

表 6-1　regex コマンドのメタ文字

文字	説明	注意
.	ドット	1 個の文字と照合します。たとえば、**d.g** は、doggonnit など、これらの文字を含む単語、dog、dag、dtg と一致します。
(*exp*)	サブ表現	サブ表現はカッコと文字を分離するので、サブ表現の他のメタ文字を使用できます。たとえば、**d(o|a)g** は dog と dag と一致し、**do|ag** は do と ag と一致します。サブ表現は繰り返しの数量詞とともに使用され、繰り返し用の文字を区別します。たとえば、**ab(xy){3}z** は abxyxyxyz と一致します。
|	二者択一	この記号により分けられるいずれかの表現と照合します。たとえば、**dog|cat** は dog または cat のいずれかと一致します。
?	疑問符	この記号より前の表現が 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 と一致します。 **（注）** **Ctrl+V** キー、疑問符の順に押してください。そのように操作しないと、ヘルプ機能が起動します。
*	アスタリスク	この記号より前の表現が 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。
+	プラス記号	この記号より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 と一致しますが、lse とは一致しません。
{*x*}	繰り返しの数量詞です。	*x* 回だけ繰り返します。たとえば、**ab(xy){3}z** は abxyxyxyz と一致します。

表 6-1　regex コマンドのメタ文字（続き）

文字	説明	注意
{*x*,}	最小の繰り返しの数量詞です。	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。
[*abc*]	文字クラス	カッコ内の文字と照合します。たとえば、**[abc]** は、a、b、または c と一致します。
[^*abc*]	否定の文字クラスです。	カッコ内に含まれない 1 個の文字と照合します。たとえば、**[^abc]** は a、b、または c 以外の文字と一致します。**[^A-Z]** は、大文字でない 1 個の文字と一致します。
[*a-c*]	文字の範囲クラス	指定された範囲内の文字と照合します。**[a-z]** は小文字の文字と一致します。文字と範囲を混合させることができます。**[abcq-z]** は a、b、c、q、r、s、t、u、v、w、x、y、z と一致し、**[a-cq-z]** も同じように一致します。 ダッシュ（-）は、**[abc-]** または **[-abc]** などのように、カッコ内の最後または最初の文字である場合にのみ、ダッシュを示します。
""	引用符	文字列内の末尾または冒頭にスペースを維持します。たとえば、**" test"** は照合する際に冒頭のスペースを維持します。
^	カレット	行の冒頭を指定します。
\	エスケープ文字	メタ文字と併用されている場合は、文字通りの文字と一致します。たとえば、**\[** は、左角カッコと一致します。
char	文字	文字がメタ文字でない場合、文字通りの文字と一致します。
\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	タブ	タブ 0x09 と一致します。
\f	改ページ	改ページ 0x0c と一致します。
\x*NN*	エスケープされた 16 進数値	16 進数を使用する ASCII 文字（2 桁のみ）と一致します。
NNN	エスケープされた 8 進数値	8 進数を使用する ASCII 文字（3 桁のみ）と一致します。たとえば、040 はスペースを表します。

- Build：Build Regular Expression 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

次の表に、この機能を使用できるモードを示します。

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

Configuration > Global Objects > Regular Expressions > Add/Edit a Regular Expression > Build Regular Expression

Build Regular Expression ダイアログボックスで、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。

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、このチェック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（\）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、doggonnit など、これらの文字を含む単語、dog、dag、dtg と一致します。
  - 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 桁のみ）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：表示のみ。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 のいずれかと一致します。
- 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 Occurrances：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 と一致します。
  - One or more times (+) : この記号より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 と一致しますが、lse とは一致しません。
  - Any number of times (*)：この記号より前の表現が 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 と一致します。
  - 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

次の表に、この機能を使用できるモードを示します。

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

Configuration > Global Objects > Regular Expressions > Add/Edit a Regular Expression > Test Regular Expression

Test Regular Expression ダイアログボックスで、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から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：*表示のみ*。テストの成功 / 失敗を示します。

モード

次の表に、この機能を使用できるモードを示します。

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

Configuration > Global Objects > Regular Expressions > 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、検査クラスマップと検査ポリシー 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は同じネーム スペースを使用しています。そのため、すでに別のタイプのクラスマップで使用されている名前を再利用できません。
- 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、検査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 アイコンの隣りにそれぞれ「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

次の表に、この機能を使用できるモードを示します。

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 Maps

Configuration > Global Objects > TCP Maps（このペインに移動するパスは数種類あります。）

TCP Maps オプションを使用して、異なるトラフィック フローの TCP 接続の設定を定義する、再利用コンポーネントを作成します。TCP マップの作成後、セキュリティ ポリシーを利用して、接続設定を特定のトラフィック タイプに関連付けます。Security Policy ペインの Service Policy Rules オプションでトラフィック基準を定義し、サービス ポリシー ルールに特定のインターフェイスを関連付けるか、セキュリティ アプライアンスのすべてのインターフェイスを適用します。

TCP Maps ペインでは、TCP フロー検査をカスタマイズして、通過トラフィックと内部トラフィックに適用できます。

フィールド

- Map Name：TCP マップの名前を一覧表示します。
- Urgent Flag：セキュリティ アプライアンスを通過する URG ポインタをクリアするか許可するかを示します。
- Window Variation：予想外のウィンドウ サイズの変更が発生した接続を許可するかドロップするかを示します。
- SYN Data：SYN パケットにデータがある場合、許可するかドロップするかを示します。
- TTL Evasion Protection：セキュリティ アプライアンスの TTL 回避保護をイネーブルにするかディセーブルにするかを示します。
- Exceed MSS：パケットがピアで設定した MSS を超過した場合、許可するかドロップするかを示します。
- Check Retransmission：再送信データ チェックをイネーブルにするかディセーブルにするかを示します。
- Verify Checksum：チェックサム検証をイネーブルにするかディセーブルにするかを示します。
- Reserved Bits：予約済みフラグ ポリシーのステータスを一覧表示します。
- TCP Option：TCP オプションの値が設定されたパケットの動作を一覧表示します。デフォルトのアクションでは、オプションをクリアしてパケットを許可します。
  - Clear Selective Ack：selective-ack TCP オプションを許可するかクリアするかを示します。
  - Clear TCP Timestamp：TCP タイムスタンプ オプションを許可するかクリアするかを示します。
  - Clear Window Scale：ウィンドウ スケール タイムスタンプ オプションを許可するかクリアするかを示します。
  - Range：有効な TCP オプションの範囲を示します。正しい範囲は 6 ～ 7 と 9 ～ 255 です。下限境界値は上限境界値以下でなければなりません。
- Queue Size：TCP 接続のキューに格納できる異常なパケットの最大数を一覧表示します。デフォルトは 0 です。

モード

次の表に、この機能を使用できるモードを示します。

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 TCP Map

Configuration > Global Objects > TCP Maps > Add/Edit TCP Map
（このダイアログボックスに移動するパスは数種類あります。）

Add/Edit TCP Maps ダイアログボックスで、トラフィック クラスを定義し、TCP マップを利用して TCP 検査をカスタマイズします。TCP マップを適用するにはポリシー マップを利用します。TCP 検査を実行するにはサービス ポリシーを利用します。

フィールド

- TCP Map Name：TCP マップの名前を指定します。
- Clear Urgent Flag：セキュリティ アプライアンスを通過する URG ポインタを許可またはクリアします。
- Drop SYN Packets With Data：データのある SYN パケットを許可またはドロップします。
- Drop Connection on Window Variation：予想外のウィンドウ サイズの変更が発生した接続をドロップします。
- Enable TTL Evasion Protection：セキュリティ アプライアンスの TTL 回避保護をイネーブルまたはディセーブルにします。
- Drop Packets that Exceed Maximum Segment Size：ピアで設定した MSS を超過したパケットを許可またはドロップします。
- Verify TCP Checksum：チェックサム検証をイネーブルまたはディセーブルにします。
- Check if transmitted data is the same as original：再送信データ チェックをイネーブルまたはディセーブルにします。
- Reserved Bits：予約済みフラグ ポリシーをセキュリティ アプライアンスに設定します。
  - Clear and allow
  - Allow only
  - Drop
- TCP Option：TCP オプションの値が設定されたパケットの動作を設定します。デフォルトのアクションでは、オプションをクリアしてパケットを許可します。
  - Clear Selective Ack：selective-ack TCP オプションを許可またはクリアします。
  - Clear TCP Timestamp：TCP タイムスタンプ オプションを許可またはクリアします。
  - Clear Window Scale：ウィンドウ スケール タイムスタンプ オプションを許可またはクリアします。
- Range：有効な TCP オプションの値を 6 ～ 7 と 9 ～ 255 の範囲で指定します。下限境界値は上限境界値以下でなければなりません。
- Action：Allow または drop。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

時間範囲の設定

Configuration > Global Objects > Time Ranges（このペインに移動するパスは数種類あります。）

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、および定期的な時間範囲エントリ（オプション）で構成されます。

（注）　時間範囲を作成しても、デバイス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：時間範囲の開始を指定します。
- End Time：時間範囲の終了を指定します。
- Periodic Entries : 指定された開始時間と終了時間の間で、時間範囲を有効にする詳細条件を指定します。

モード

次の表に、この機能を使用できるモードを示します。

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 Range

Configuration > Global Objects > Time Ranges > Add/Edit Time Range
（このダイアログボックスに移動するパスは数種類あります。）

Add/Edit Time Range ペインで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 クロックに依存します。ただし、最適に動作するのは NPT 同期を適用した場合です。

（注）　時間範囲を作成しても、デバイス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 at：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。
- Periodic Time Ranges：時間範囲を日単位または週単位で設定します。
  - Add：定期的な時間範囲を追加します。
  - Edit：選択した定期的な時間範囲を編集します。
  - Delete：選択した定期的な時間範囲を削除します。

モード

次の表に、この機能を使用できるモードを示します。

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 Periodic Time Range

Configuration > Global Objects > Time Ranges > Add/Edit Time Range > Add/Edit Periodic Time Range（このダイアログボックスに移動するパスは数種類あります。）

Add/Edit Periodic Time Range ペインで時間範囲を詳細に指定し、日単位または週単位の設定を行います。

（注） 時間範囲を作成しても、デバイス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 まで一覧表示します。
  - Minute：分を 00 ～ 59 まで一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—