基本インターネット プロトコルのインスペクションの設定

この章では、アプリケーション レイヤ プロトコル インスペクションを設定する方法について説明します。インスペクション エンジンは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルでは、高速パスでパケットを渡すのではなく、ASA で詳細なパケット インスペクションを行う必要があります。そのため、インスペクション エンジンがスループット全体に影響を与えることがあります。

ASA では、デフォルトでいくつかの一般的なインスペクション エンジンがイネーブルになっていますが、ネットワークによっては他のインスペクション エンジンをイネーブルにしなければならない場合があります。

この章は、次の項で構成されています。

- 「DNS インスペクション」（P.10-1）
- 「FTP インスペクション」（P.10-12）
- 「HTTP インスペクション」（P.10-22）
- 「ICMP インスペクション」（P.10-35）
- 「ICMP エラー インスペクション」（P.10-35）
- 「インスタント メッセージ インスペクション」（P.10-36）
- 「IP オプション インスペクション」（P.10-38）
- 「IPsec パススルー インスペクション」（P.10-42）
- 「IPv6 インスペクション」（P.10-45）
- 「NETBIOS インスペクション」（P.10-47）
- 「PPTP インスペクション」（P.10-49）
- 「SMTP および拡張 SMTP インスペクション」（P.10-49）
- 「TFTP インスペクション」（P.10-58）

DNS インスペクション

この項では、DNS アプリケーション インスペクションについて説明します。この項は、次の内容で構成されています。

- 「DNS アプリケーション インスペクションの動作」（P.10-2）

- 「DNS リライトの動作」（P.10-3）
- 「DNS リライトの設定」（P.10-3）
- 「Select DNS Inspect Map」（P.10-5）
- 「DNS Class Map」（P.10-6）
- 「Add/Edit DNS Traffic Class Map」（P.10-7）
- 「Add/Edit DNS Match Criterion」（P.10-7）
- 「DNS Inspect Map」（P.10-8）
- 「Add/Edit DNS Policy Map（セキュリティ レベル）」（P.10-10）
- 「[Add/Edit DNS Policy Map]（詳細）」（P.10-11）

DNS アプリケーション インスペクションの動作

ASA で DNS 応答が転送されるとすぐに、ASA は DNS クエリーに関連付けられた DNS セッションを切断します。ASA はまた、メッセージ交換をモニタして DNS 応答の ID が DNS クエリーの ID と一致することを確認します。

DNS インスペクションをイネーブルにすると（デフォルト）、ASA は次の追加のタスクを実行します。

- **alias**、**static**、および **nat** コマンドを使用して作成されたコンフィギュレーションに基づいて、DNS レコードを変換します（DNS リライト）。変換は、DNS 応答の A レコードだけに適用されるため、DNS リライトによって PTR レコードを必要とする逆ルックアップが影響を受けることはありません。

（注） 1 つの A レコードには複数の PAT ルールが適用可能で、使用する PAT ルールがあいまいなため、DNS リライトは PAT には適用できません。

- 最大 DNS メッセージ長を指定します（デフォルトは 512 バイト、最大長は 65535 バイト）。ASA は必要に応じてリアセンブリを実行し、パケット長が設定されている最大長よりも短いことを確認します。ASA は、最大長を超えるパケットをドロップします。

（注） **maximum-length** オプションを指定せずに **inspect dns** コマンドを入力した場合、DNS パケット サイズはチェックされません。

- ドメイン名の長さを 255 バイトに制限し、ラベルの長さを 63 バイトに制限します。
- DNS メッセージに圧縮ポインタが出現した場合、ポインタが参照するドメイン名の整合性を確認します。
- 圧縮ポインタのループが終了するかどうかを確認します。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元/宛先 IP アドレス、送信元/宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つだけ作成されます。DNS ID は *app_id* で追跡され、各 app_id のアイドル タイマーは独立して実行されます。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答が ASA を通過できるのは、限られた期間内だけであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力した場合、新しい DNS セッションによってリセットされている DNS 接続のアイドル タイマーが表示されます。これは共有 DNS 接続の性質によるものであり、仕様です。

DNS リライトの動作

DNS インスペクションがイネーブルであるとき、DNS リライトは、任意のインターフェイスから送信された DNS メッセージの NAT を完全にサポートします。

内部のネットワーク上のクライアントが、外部インターフェイス上の DNS サーバから送信される内部アドレスの DNS 解決を要求した場合、DNS A レコードは正しく変換されます。DNS インスペクション エンジンがディセーブルである場合、A レコードは変換されません。

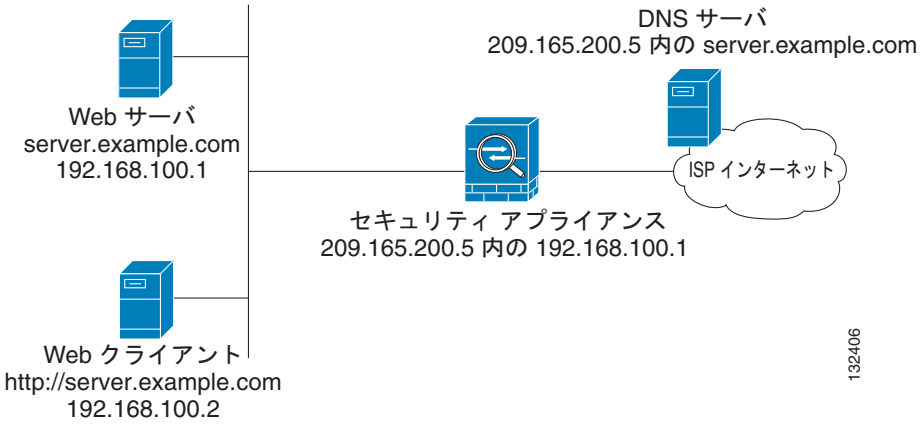
DNS インスペクションがイネーブルであれば、NAT ルールを使用して DNS リライトを設定できます。

DNS リライトは次の 2 つの機能を実行します。

- DNS クライアントがプライベート インターフェイスにある場合、*DNS 応答*のパブリック アドレス（ルーティング可能なアドレスまたは「マッピング」アドレス）をプライベート アドレス（「実際の」アドレス）に変換します。
- DNS クライアントがパブリック インターフェイスにある場合、プライベート アドレスをパブリック アドレスに変換します。

図 10-1 では、DNS サーバは外部（ISP）ネットワークにあります。サーバの実際のアドレス（192.168.100.1）は、**static** コマンドで ISP が割り当てたアドレス（209.165.200.5）にマッピングされています。内部インターフェイスの Web クライアントが http://server.example.com という URL の Web サーバにアクセスしようとすると、Web クライアントが動作するホストが、Web サーバの IP アドレスの解決を求める DNS 要求を DNS サーバに送信します。ASA は、IP ヘッダーに含まれるルーティング不可の送信元アドレスを変換し、外部インターフェイスの ISP ネットワークに要求を転送します。DNS 応答が返されると、ASA はアドレス変換を宛先アドレスだけではなく、DNS 応答の A レコードに含まれる、埋め込まれた Web サーバの IP アドレスにも適用します。結果として、内部ネットワーク上の Web クライアントは、内部ネットワーク上の Web サーバとの接続に使用する正しいアドレスを取得します。

図 10-1　　DNS 応答に含まれるアドレスの変換（DNS リライト）



DNS リライトは、DNS 要求を作成するクライアントが DMZ ネットワークにあり、DNS サーバが内部インターフェイスにある場合にも機能します。

DNS リライトの設定

NAT コンフィギュレーションを使用して DNS リライトを設定します。

図 10-2 では、DNS インスペクションによってどのようにして NAT が最小コンフィギュレーションの DNS サーバと透過的に連携動作するかを示す、より複雑な事例を示します。

図 10-2　　3 つの NAT ゾーンを持つ DNS リライト

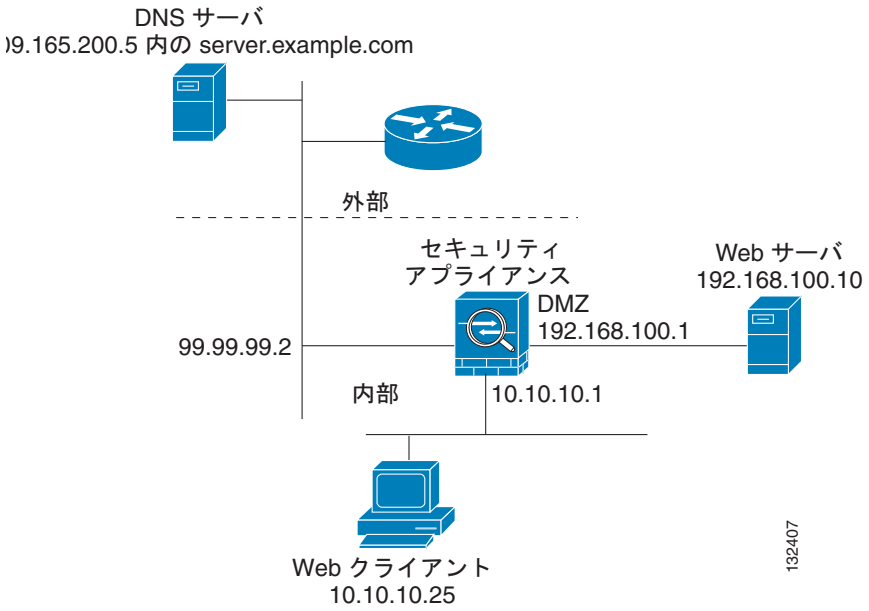


図 10-2 で、Web サーバ server.example.com の実際のアドレスは、ASA の DMZ インターフェイスの 192.168.100.10 です。IP アドレス 10.10.10.25 の Web クライアントが内部インターフェイスにあり、パブリック DNS サーバが外部インターフェイスにあります。サイト NAT ポリシーは次のとおりです。

- 外部 DNS サーバは server.example.com の信頼できるアドレス レコードを保持しています。
- 外部ネットワークのホストは、ドメイン名が server.example.com の Web サーバに、外部 DNS サーバまたは IP アドレス 209.165.200.5 を使用して接続できます。
- 内部ネットワークのクライアントは、ドメイン名が server.example.com の Web サーバに、外部 DNS サーバまたは IP アドレス 192.168.100.10 を使用してアクセスできます。

いずれかのインターフェイスのホストまたはクライアントは、DMZ Web サーバにアクセスするときに、パブリック DNS サーバに対して server.example.com の A レコードを問い合わせます。DNS サーバは、server.example.com がアドレス 209.165.200.5 にバインドされていることを示す A レコードを返します。

*外部*ネットワークの Web クライアントが http://server.example.com にアクセスを試みたときのイベント シーケンスは次のとおりです。

1. Web クライアントを実行しているホストが DNS サーバに、server.example.com の IP アドレスを求める要求を送信します。
2. DNS サーバが応答で IP アドレス 209.165.200.225 を示します。
3. Web クライアントが HTTP 要求を 209.165.200.225 に送信します。
4. 外部ホストからのパケットが ASA の外部インターフェイスに到達します。
5. スタティック ルールによってアドレス 209.165.200.225 が 192.168.100.10 に変換され、ASA がパケットを DMZ の Web サーバに誘導します。

*内部*ネットワークの Web クライアントが http://server.example.com にアクセスを試みたときのイベント シーケンスは次のとおりです。

1. Web クライアントを実行しているホストが DNS サーバに、server.example.com の IP アドレスを求める要求を送信します。
2. DNS サーバが応答で IP アドレス 209.165.200.225 を示します。
3. ASA が DNS 応答を受信し、その応答を DNS アプリケーション インスペクション エンジンに送信します。
4. DNS アプリケーション インスペクション エンジンは、次の処理を行います。
   a. 埋め込まれた A レコード アドレス「[outside]:209.165.200.5」の変換を元に戻す NAT ルールを検索します。この例では、次のスタティック コンフィギュレーションが検索されます。

```
object network obj-192.168.100.10-01
  host 192.168.100.10
  nat (dmz,outside) static 209.165.200.5 dns
```

   b. **dns** オプションが含まれているため、次のように A レコードをリライトするスタティック ルールを使用します。

```
[outside]:209.165.200.225 --> [dmz]:192.168.100.10
```

   （注）　**nat** コマンドに **dns** オプションが含まれていない場合、DNS リライトは実行されず、他のパケット処理が継続されます。

   c. 内部 Web クライアントと通信するときに、Web サーバ アドレス [dmz]:192.168.100.10 を変換する NAT が検索されます。

      適用可能な NAT ルールがない場合、アプリケーション インスペクションは終了します。

      NAT ルール（nat または static）が適用可能な場合は、**dns** オプションも指定されている必要があります。**dns** オプションが指定されていなかった場合、ステップ b の A レコード リライトは取り消され、他のパケット処理が継続されます。
5. ASA が DMZ インターフェイスの server.example.com に HTTP 要求を送信します。

Select DNS Inspect Map

[Select DNS Map] ダイアログボックスには、次のようにアクセスできます。

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select DNS Inspect Map]

[Select DNS Map] ダイアログボックスでは、DNS マップを選択または新しく作成できます。DNS マップにより、DNS アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select DNS Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default DNS inspection map] : デフォルトの DNS マップの使用を指定します。
- [Select a DNS map for fine control over inspection] : 定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。

- [Enable Botnet traffic filter DNS snooping] : ボットネット トラフィック フィルタ スヌーピングをイネーブルにします。ボットネット トラフィック フィルタ スヌーピングでは、ドメイン名がダイナミック データベースまたはスタティック データベースのドメイン名と比較され、ドメイン名と IP アドレスがボットネット トラフィック フィルタの DNS 逆ルックアップ キャッシュに追加されます。このキャッシュは、疑わしいアドレスへの接続が行われたときにボットネット トラフィック フィルタで使用されます。DNS スヌーピングは、外部 DNS 要求が送信されるインターフェイスでだけイネーブルにすることを推奨します。すべての UDP DNS トラフィック（内部 DNS サーバへの送信トラフィックを含む）に対して DNS スヌーピングをイネーブルにすると、ASA で不要な負荷が発生します。たとえば、DNS サーバが外部インターフェイスに存在する場合は、外部インターフェイスのすべての UDP DNS トラフィックに対して DNS インスペクションとスヌーピングをイネーブルにする必要があります。
- [Add] : そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

DNS Class Map

[DNS Class Map] ダイアログボックスには、次のようにアクセスできます。

[Configuration] > [Global Objects] > [Class Maps] > [DNS]

[DNS Class Map] ペインでは、DNS インスペクションの DNS クラス マップを設定できます。

インスペクション 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 マップをインスペクション 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インスペクション 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。インスペクション 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

次の表は、この機能を使用できるモードを示したものです。

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

Add/Edit DNS Traffic Class Map

[Add/Edit DNS Traffic Class Map] ダイアログボックスには、次のようにアクセスできます。

[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は、DNS クラス マップを定義できます。

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。

Add/Edit DNS Match Criterion

[Add/Edit DNS Match Criterion] ダイアログボックスには、次のようにアクセスできます。

[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は、DNS クラス マップの照合基準と値を定義できます。

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 の問い合わせを照合します。
  - [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]：権限ネーム 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]：増分（ゾーン）転送

    [AXFR]：フル（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 の問い合わ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。

DNS Inspect Map

[DNS Inspect Map] ダイアログボックスには、次のようにアクセスできます。

[Configuration] > [Global Objects] > [Inspect Maps] > [DNS]

[DNS] ペインでは、DNS アプリケーションの事前に設定されたインスペクション マップを表示できます。DNS マップを使用すると、DNS アプリケーション インスペクションに使用するデフォルト設定値を変更できます。

DNS アプリケーション インスペクションは、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 メッセージ制御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できます。

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 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疑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。

不一致の DNS 応答数が過度に増えた場合（キャッシュ ポイズニング攻撃を示している可能性がある）、DNS 不一致のアラートを設定して通知することができます。さらに、すべての DNS メッセージにトランザクション署名（TSIG）を付けるようにチェックする設定も行うことができます。

フィールド

- [DNS Inspect Maps]：定義されている DNS インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい DNS インスペクション マップを設定します。DNS インスペクション マップを編集するには、[DNS Inspect Maps] テーブルで DNS のエントリを選択し、[Customize] をクリックします。
- [Delete]：[DNS Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [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]：[Add/Edit DNS Policy Map] ダイアログボックスを開き、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。

Add/Edit DNS Policy Map（セキュリティ レベル）

[Add/Edit DNS Policy Map] ダイアログボックスには、次のようにアクセスできます。

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

[Add/Edit DNS Policy Map] ペインでは、DNS アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：DNS マップの追加時に DNS マップの名前を入力します。DNS マップの編集時には、事前に設定した DNS マップの名前が表示されます。
- [Description]：DNS 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

- [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。

• [Details]：詳細な設定を行うための [Protocol Conformance] タブ、[Filtering] タブ、[Mismatch Rate] タブ、および [Inspection] タブを表示します。

[Add/Edit DNS Policy Map]（詳細）

[Add/Edit DNS Policy Map] ペインでは、DNS アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：DNS マップの追加時に DNS マップの名前を入力します。DNS マップの編集時には、事前に設定した DNS マップの名前が表示されます。
- [Description]：DNS マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルを表示します。
- [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。クエリーごとに 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。この値を超えると、システム メッセージ ログに出力されます。

    [Time Interval]：監視間隔時間（秒単位）を入力します。
- [Inspections]：このタブで DNS インスペクション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 インスペクションの基準を示します。
  - [Value]：DNS インスペクション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 インスペクションを追加できます。
  - [Edit]：[Edit DNS Inspect] ダイアログボックスが開き、DNS インスペクションを編集できます。
  - [Delete]：DNS インスペクションを削除します。
  - [Move Up]：インスペクションをリストの上に移動します。
  - [Move Down]：インスペクションをリストの下に移動します。

FTP インスペクション

この項では、FTP インスペクション エンジンについて説明します。この項は、次の内容で構成されています。

- 「FTP インスペクションの概要」（P.10-13）

- 「厳密な FTP の使用方法」（P.10-13）
- 「Select FTP Map」（P.10-14）
- 「FTP Class Map」（P.10-14）
- 「Add/Edit FTP Traffic Class Map」（P.10-15）
- 「Add/Edit FTP Match Criterion」（P.10-15）
- 「FTP Inspect Map」（P.10-17）

FTP インスペクションの概要

FTP アプリケーション インスペクションは、FTP セッションを検査し、次の 4 つのタスクを実行します。

- ダイナミックな二次的データ接続の準備
- FTP コマンド応答シーケンスの追跡
- 監査証跡の生成
- 埋め込み IP アドレスの変換

FTP アプリケーション インスペクションによって、FTP データ転送用にセカンダリ チャネルが用意されます。これらのチャネルのポートは、PORT コマンドまたは PASV コマンドを使用してネゴシエートされます。セカンダリ チャネルは、ファイル アップロード、ファイル ダウンロード、またはディレクトリ リスト イベントへの応答で割り当てられます。

（注）　**no inspect ftp** コマンドを使用して、FTP インスペクション エンジンをディセーブルにすると、発信ユーザはパッシブ モードだけで接続を開始でき、着信 FTP はすべてディセーブルになります。

厳密な FTP の使用方法

strict オプションにより厳密な FTP を使用すると、Web ブラウザが FTP 要求内の埋め込みコマンドを送信できなくなるため、保護されたネットワークのセキュリティが強化されます。厳密な FTP をイネーブルにするには、[Configuration] > [Firewall] > [Service Policy Rules] > [Edit Service Policy Rule] > [Rule Actions] > [Protocol Inspection] タブで、FTP の横にある [Configure] ボタンをクリックします。

インターフェイスに対して **strict** オプションをオンにすると、FTP インスペクションによって次の動作が適用されます。

- FTP コマンドが確認応答されてからでないと、ASA は新しいコマンドを許可しません。
- ASA は、埋め込みコマンドを送信する接続をドロップします。
- 227 コマンドと PORT コマンドが、エラー文字列に表示されないように確認されます。

注意　**strict** オプションを使用すると、FTP RFC に厳密に準拠していない FTP クライアントは失敗することがあります。

strict オプションがイネーブルの場合、各 FTP コマンドと応答シーケンスが追跡され、次の異常なアクティビティがないか確認されます。

- 切り捨てされたコマンド: PORT コマンドおよび PASV 応答コマンドのカンマの数が 5 であるかどうかが確認されます。カンマの数が 5 でない場合は、PORT コマンドが切り捨てられていると見なされ、TCP 接続は閉じられます。
- 不正なコマンド: FTP コマンドが、RFC の要求どおりに <CR><LF> 文字で終了しているかどうか確認されます。終了していない場合は、接続が閉じられます。
- RETR コマンドと STOR コマンドのサイズ：これらが、固定の定数と比較チェックされます。サイズが定数より大きい場合は、エラー メッセージがロギングされ、接続が閉じられます。
- コマンド スプーフィング: PORT コマンドは、常にクライアントから送信されます。PORT コマンドがサーバから送信される場合、TCP 接続は拒否されます。
- 応答スプーフィング：PASV 応答コマンド（227）は、常にサーバから送信されます。PASV 応答コマンドがクライアントから送信される場合、TCP 接続は拒否されます。これにより、ユーザが「227 xxxxx a1, a2, a3, a4, p1, p2.」を実行する場合のセキュリティ ホールが予防できます。
- TCP ストリーム編集：ASA は、TCP ストリーム編集を検出した場合に接続が閉じられます。
- 無効ポート ネゴシエーション：ネゴシエートされたダイナミック ポート値が、1024 未満であるかどうかが調べられます。1 ～ 1024 の範囲のポート番号は、予約済み接続用に指定されているため、ネゴシエートされたポートがこの範囲内であった場合、TCP 接続は解放されます。
- コマンド パイプライン：PORT コマンドと PASV 応答コマンド内のポート番号の後に続く文字数が、定数の 8 と比べられます。8 より大きい場合は、TCP 接続が閉じられます。
- ASA は、SYST コマンドに対する FTP サーバ応答を X の連続に置き換えることで、FTP クライアントがサーバのシステム タイプを取得できないようにします。このデフォルトの動作を無効にするには、FTP マップで、**no mask-syst-reply** コマンドを使用します。

Select FTP Map

[Select FTP Map] ダイアログボックスには、次のようにアクセスできます。

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select FTP Map]

[Select FTP Map] ダイアログボックスでは、厳密な FTP アプリケーション インスペクションのイネーブル化、FTP マップの選択、または新しい FTP マップの作成を行うことができます。FTP マップにより、FTP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select FTP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [FTP Strict (prevent web browsers from sending embedded commands in FTP requests)]：厳密な FTP アプリケーション インスペクションをイネーブルにします。これによっては、埋め込みコマンドが FTP 要求に含まれている場合、ASA は接続をドロップします。
- [Use the default FTP inspection map]：デフォルトの FTP マップの使用を指定します。
- [Select an FTP map for fine control over inspection]: 定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

FTP Class Map

[FTP Class Map] ダイアログボックスには、次のようにアクセスできます。

[Configuration] > [Global Objects] > [Class Maps] > [FTP]

[FTP Class Map] ペインでは、FTP インスペクションの FTP クラス マップを設定できます。

インスペクション 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 マップをインスペクション 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インスペクション 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。インスペクション 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。

Add/Edit FTP Traffic Class Map

[Add/Edit FTP Traffic Class Map] ダイアログボックスには、次のようにアクセスできます。

[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は、FTP クラス マップを定義できます。

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。

Add/Edit FTP Match Criterion

[Add/Edit FTP Match Criterion] ダイアログボックスには、次のようにアクセスできます。

[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は、FTP クラス マップの照合基準と値を定義できます。

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]：変更元ファイル名

    [RNTO]：変更先ファイル名

    [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。
- [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。

- [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。
- [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。

FTP Inspect Map

[FTP Inspect Map] ダイアログボックスには、次のようにアクセスできます。

[Configuration] > [Global Objects] > [Inspect Maps] > [FTP]

[FTP] ペインでは、FTP アプリケーションの事前に設定されたインスペクション マップを表示できます。FTP マップでは、FTP アプリケーション インスペクションのデフォルト設定値を変更できます。

厳密な FTP インスペクションには、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インスペクションには、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。ファイルのタイプ、サーバ名、および他の属性に基づいて、FTP 接続をブロックできます。インスペクション時に 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

- [FTP Inspect Maps]：定義されている FTP インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい FTP インスペクション マップを設定します。FTP インスペクション マップを編集するには、[FTP Inspect Maps] テーブルで FTP のエントリを選択し、[Customize] をクリックします。
- [Delete]：[FTP Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [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

- [File Type Filtering]：[Type Filtering] ダイアログボックスを開き、ファイル タイプのフィルタを設定します。
- [Customize]：[Add/Edit FTP Policy Map] ダイアログボックスを開き、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

[File Type Filtering] ダイアログボックスには、次のようにアクセスできます。

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

[File Type Filtering] ダイアログボックスでは、ファイル タイプ 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]：インスペクションの基準を示します。
- [Value]：インスペクション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。

[Add/Edit FTP Policy Map]（セキュリティ レベル）

[Add/Edit FTP Policy Map] ダイアログボックスには、次のようにアクセスできます。

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

[Add/Edit FTP Policy Map] ペインでは、FTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：FTP マップの追加時に FTP マップの名前を入力します。FTP マップの編集時には、事前に設定した FTP マップの名前が表示されます。
- [Description]：FTP 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

- [File Type Filtering]：[Type Filtering] ダイアログボックスを開き、ファイル タイプのフィルタを設定します。
- [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。

- [Details]：詳細な設定を行うための [Parameters] タブと [Inspections] タブを表示します。

Add/Edit FTP Policy Map (Details)

[Add/Edit FTP Policy Map (Details)] ダイアログボックスには、次のようにアクセスできます。

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

[Add/Edit FTP Policy Map] ペインでは、FTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：FTP マップの追加時に FTP マップの名前を入力します。FTP マップの編集時には、事前に設定した FTP マップの名前が表示されます。
- [Description]：FTP マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルとファイル タイプ フィルタリング設定を表示します。
- [Parameters]：このタブで FTP インスペクション 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 インスペクション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 インスペクションの基準を示します。
  - [Value]：FTP インスペクション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 インスペクションを追加できます。
  - [Edit]：[Edit FTP Inspect] ダイアログボックスが開き、FTP インスペクションを編集できます。
  - [Delete]：FTP インスペクションを削除します。
  - [Move Up]：インスペクションをリストの上に移動します。

- [Move Down]：インスペクションをリストの下に移動します。

Add/Edit FTP Map

[Add/Edit FTP Map] ダイアログボックスには、次のようにアクセスできます。

[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は、FTP インスペクション マップの照合基準と値を定義できます。

フィールド

- [Single Match]：FTP インスペクションに照合文が 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。
- [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。
- [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。
- [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。
- [Multiple Matches] : FTP インスペクション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] : Reset。
- [Log] : イネーブルまたはディセーブルにします。

FTP 検査の確認とモニタリング

FTP アプリケーション インスペクションでは、次のログ メッセージが生成されます。

- An Audit record 303002 is generated for each file that is retrieved or uploaded.
- The FTP command is checked to see if it is RETR or STOR and the retrieve and store commands are logged.
- The username is obtained by looking up a table providing the IP address.
- The username, source IP address, destination IP address, NAT address, and the file operation are logged.
- Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.

NAT と連携することにより、FTP アプリケーション インスペクションでは、アプリケーション ペイロード内の IP アドレスが変換されます。これは、RFC 959 に詳細に記述されています。

HTTP インスペクション

この項では、HTTP インスペクション エンジンについて説明します。この項は、次の内容で構成されています。

- 「HTTP インスペクションの概要」（P.10-22）
- 「Select HTTP Map」（P.10-22）
- 「HTTP Class Map」（P.10-23）
- 「Add/Edit HTTP Traffic Class Map」（P.10-23）
- 「Add/Edit HTTP Match Criterion」（P.10-24）
- 「HTTP Inspect Map」（P.10-28）
- 「URI Filtering」（P.10-29）
- 「Add/Edit HTTP Policy Map (Security Level)」（P.10-29）
- 「Add/Edit HTTP Policy Map（詳細）」（P.10-30）
- 「Add/Edit HTTP Map」（P.10-31）

HTTP インスペクションの概要

HTTP インスペクション エンジンを使用して、特定の攻撃、および HTTP トラフィックに関係するその他の脅威から保護します。HTTP インスペクションは、次のようないくつかの機能を実行します。

- 拡張 HTTP インスペクション
- N2H2 または Websense を使用する URL のスクリーニング

  詳細については、「URL フィルタリングに関する情報」（P.28-2）を参照してください。
- Java と ActiveX のフィルタリング

2 つ目と 3 つ目の機能は、フィルタ ルールと共に設定します。

拡張 HTTP インスペクション機能はアプリケーション ファイアウォールとも呼ばれ、HTTP マップを設定するときに使用できます。これによって、攻撃者がネットワーク セキュリティ ポリシーに従わない HTTP メッセージを使用できないようにします。この機能は、すべての HTTP メッセージについて次のことを確認します。

- RFC 2616 への準拠
- RFC で定義された方式だけを使用していること
- 追加の基準への準拠

Select HTTP Map

[Select HTTP Map] ダイアログボックスには、次のようにアクセスできます。

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select HTTP Map]

[Select HTTP Map] ダイアログボックスでは、HTTP マップを選択または新しく作成できます。HTTP マップにより、HTTP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select HTTP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default HTTP inspection map]：デフォルトの HTTP マップの使用を指定します。
- [Select an HTTP map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

HTTP Class Map

[HTTP Class Map] ダイアログボックスには、次のようにアクセスできます。

[Configuration] > [Global Objects] > [Class Maps] > [HTTP]

[HTTP Class Map] ペインでは、HTTP インスペクションの HTTP クラス マップを設定できます。

インスペクション 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 マップをインスペクション 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インスペクション 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。インスペクション 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。

Add/Edit HTTP Traffic Class Map

[Add/Edit HTTP Traffic Class Map] ダイアログボックスには、次のようにアクセスできます。

[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は、HTTP クラス マップを定義できます。

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。

Add/Edit HTTP Match Criterion

[Add/Edit HTTP Match Criterion] ダイアログボックスには、次のようにアクセスできます。

[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は、HTTP クラス マップの照合基準と値を定義できます。

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 タイプが要求の accept フィールドの MIME タイプの 1 つと一致する必要があることを指定します。
  - [Request Arguments]：要求の引数に正規表現照合を適用します。

    [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 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]：要求の本文に正規表現照合を適用します。

    [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 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、正規表現を設定できます。

[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、正規表現を設定できます。

  [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]：要求のヘッダーに正規表現照合を適用します。

  [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 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 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 に正規表現照合を適用します。

  [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。

- [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。

- [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、正規表現を設定できます。

[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、正規表現を設定できます。

  [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]：応答のヘッダーに正規表現照合を適用します。

  [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。

- [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。

HTTP Inspect Map

[HTTP Inspect Map] ダイアログボックスには、次のようにアクセスできます。

[Configuration] > [Global Objects] > [Inspect Maps] > [HTTP]

[HTTP] ペインでは、HTTP アプリケーションの事前に設定されたインスペクション マップを表示できます。HTTP マップでは、HTTP アプリケーション インスペクション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 インスペクションで 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 インスペクションでトンネル 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

- [HTTP Inspect Maps] : 定義されている HTTP インスペクション マップを一覧表示するテーブルです。
- [Add] : 新しい HTTP インスペクション マップを設定します。HTTP インスペクション マップを編集するには、[HTTP Inspect Maps] テーブルで HTTP のエントリを選択し、[Customize] をクリックします。
- [Delete] : [HTTP Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [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

    高度なインスペクション : 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

    高度なインスペクション : 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

高度なインスペクション：設定しない

- [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。
- [Customize]：[Edit HTTP Policy Map] ダイアログボックスを開き、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には、次のようにアクセスできます。

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

[URI Filtering] ダイアログボックスでは、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]：インスペクションの基準を示します。
- [Value]：インスペクション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。

Add/Edit HTTP Policy Map (Security Level)

[Add/Edit HTTP Policy Map (Security Level)] ダイアログボックスには、次のようにアクセスできます。

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

[Add/Edit HTTP Policy Map] ペインでは、HTTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：HTTP マップの追加時に HTTP マップの名前を入力します。HTTP マップの編集時には、事前に設定した HTTP マップの名前が表示されます。
- [Description]：HTTP 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

高度なインスペクション：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

高度なインスペクション：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

高度なインスペクション：設定しない

- [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。
- [Default Level]：セキュリティ レベルをデフォルトに戻します。

- [Details]：詳細な設定を行うための [Parameters] タブと [Inspections] タブを表示します。

Add/Edit HTTP Policy Map（詳細）

[Add/Edit HTTP Policy Map]（詳細）ダイアログボックスには、次のようにアクセスできます。

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

[Add/Edit HTTP Policy Map] ペインでは、HTTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：HTTP マップの追加時に HTTP マップの名前を入力します。HTTP マップの編集時には、事前に設定した HTTP マップの名前が表示されます。
- [Description]：HTTP マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルと URI フィルタリング設定を表示します。
- [Parameters]：このタブで HTTP インスペクション 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 インスペクション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 インスペクションの基準を示します。
  - [Value]：HTTP インスペクション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 インスペクションを追加できます。
  - [Edit]：[Edit HTTP Inspect] ダイアログボックスが開き、HTTP インスペクションを編集できます。
  - [Delete]：HTTP インスペクションを削除します。
  - [Move Up]：インスペクションをリストの上に移動します。
  - [Move Down]：インスペクションをリストの下に移動します。

Add/Edit HTTP Map

[Add/Edit HTTP Map] ダイアログボックスには、次のようにアクセスできます。

[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は、HTTP インスペクション マップの照合基準と値を定義できます。

フィールド

- [Single Match]：HTTP インスペクションに照合文が 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 タイプが要求の accept フィールドの MIME タイプの 1 つと一致する必要があることを指定します。
  - [Request Arguments]：要求の引数に正規表現照合を適用します。

    [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 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]：要求の本文に正規表現照合を適用します。

  [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 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、正規表現を設定できます。

  [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、正規表現を設定できます。

  [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]：要求のヘッダーに正規表現照合を適用します。

  [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 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 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 に正規表現照合を適用します。

  [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。

- [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。

- [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、正規表現を設定できます。

  [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、正規表現を設定できます。

  [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] : 応答のヘッダーに正規表現照合を適用します。

  [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。

- [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。

- [Multiple Matches]：HTTP インスペクション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、または Log。
- [Log]：イネーブルまたはディセーブルにします。

ICMP インスペクション

ICMP インスペクション エンジンを使用すると、ICMP トラフィックが「セッション」を持つようになるため、TCP トラフィックや UDP トラフィックのように検査することが可能になります。ICMP インスペクション エンジンを使用しない場合は、ACL で ICMP による ASA の通過を禁止することを推奨します。ステートフル インスペクションを実行しないと、ICMP がネットワーク攻撃に利用される可能性があります。ICMP インスペクション エンジンは、要求ごとに応答が 1 つだけであること、シーケンス番号が正しいことを確認します。

ICMP エラー インスペクション

この機能がイネーブルの場合、ASA は、NAT コンフィギュレーションに基づいて ICMP エラー メッセージを送信する中間ホップ用の変換セッションを作成します。ASA は、変換後の IP アドレスでパケットを上書きします。

ディセーブルの場合、ASA は、ICMP エラー メッセージを生成する中間ノード用の変換セッションを作成しません。内部ホストと ASA の間にある中間ノードによって生成された ICMP エラー メッセージは、NAT リソースをそれ以上消費することなく、外部ホストに到達します。外部ホストが traceroute コマンドを使用して ASA の内部にある宛先までのホップをトレースする場合、これは適切ではありません。ASA が中間ホップを変換しない場合、すべての中間ホップは、マッピングされた宛先 IP アドレスとともに表示されます。

ICMP ペイロードがスキャンされて、元のパケットから 5 つのタプルが取得されます。取得した 5 つのタプルを使用してルックアップを実行し、クライアントの元のアドレスを判別します。ICMP エラー インスペクション エンジンは、ICMP パケットに対して次の変更を加えます。

- IP ヘッダー内のマッピング IP を実際の IP（宛先アドレス）に変更し、IP チェックサムを修正する。
- ICMP パケットに変更を加えたため、ICMP ヘッダー内の ICMP チェックサムを修正する。
- ペイロードに次の変更を加える。
  - 元のパケットのマッピング IP を実際の IP に変更する。
  - 元のパケットのマッピング ポートを実際のポートに変更する。
  - 元のパケットの IP チェックサムを再計算する。

インスタント メッセージ インスペクション

この項では、IM インスペクション エンジンについて説明します。この項は、次の内容で構成されています。

- 「インスタント メッセージ インスペクションの概要」（P.10-36）
- 「Select IM Map」（P.10-37）

インスタント メッセージ インスペクションの概要

インスタント メッセージ（IM）インスペクション エンジンを使用すると、IM アプリケーションの制御を細かく調整して、ネットワークの使用を制御し、機密情報の漏洩やワームの繁殖などの企業のネットワークへの脅威を阻止できます。

IM インスペクション クラス マップ デスクリプションの追加

[Add Service Policy Rule Wizard - Rule Actions] ダイアログボックスを使用して IP プロトコル インスペクションを設定します。

このウィザードは [Configuration] > [Firewall] > [Service Policy Rules] > [Add] > [Add Service Policy Rule Wizard - Rule Actions] ダイアログボックスから使用できます。

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Class Maps] > [Instant Messaging (IM)] の順に選択します。インスタント メッセージ インスペクションの設定済みクラス マップを表示するテーブルが表示されます。

ステップ 2　新しいクラス マップを追加するには、[Add] をクリックします。[Add Instant Messaging (IM) Traffic Class Map] ダイアログボックスが表示されます。

ステップ 3　クラス マップの名前を入力します。

ステップ 4　（任意）クラス マップの説明を入力します。説明を 200 文字以内で入力できます。

ステップ 5　[Match Option] フィールドで、クラス マップの次のオプションをクリックします。

- [Match All]：トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。デフォルトでは、[Match All] オプションが選択されています。
- [Match Any]：トラフィックが少なくとも基準の 1 つに一致したらクラス マップと一致することを指定します。

ステップ 6　[Add] をクリックして、クラス マップの一致基準を追加します。[Add Instant Messaging (IM) Match Criterion] ダイアログボックスが表示されます。

ステップ 7　[Match Type] フィールドで、[Match] または [No Match] オプション ボタンをクリックします。

ステップ 8　[Criterion] ドロップダウン リストで、次のオプションのいずれかを選択し、基準の値を指定します。選択したオプションに応じて、[Value] フィールドが動的にリフレッシュされ、その基準の適切な値が表示されます。

- [Protocol] : 特定の IM プロトコル（Yahoo Messenger や MSN Messenger など）のトラフィックを照合する場合に選択します。
- [Service] : 特定の IM サービス（チャット、ファイル転送、Web カメラ、音声チャット、会議、ゲームなど）を照合する場合に選択します。
- [Version] : IM メッセージのバージョンを照合する場合に選択します。[Value] フィールドで、[Regular Expression] または [Regular Expression Class] オプションをクリックし、ドロップダウン リストから式を選択します。

  一般的な操作のコンフィギュレーション ガイドの Configuring Regular Expressions, page 15-20 を参照してください。
- [Client Login Name] : IM メッセージの送信元のログイン名を照合する場合に選択します。[Value] フィールドで、[Regular Expression] または [Regular Expression Class] オプションをクリックし、ドロップダウン リストから式を選択します。

  一般的な操作のコンフィギュレーション ガイドの Configuring Regular Expressions, page 15-20 を参照してください。
- [Client Peer Login Name] : IM メッセージの宛先のログイン名を照合する場合に選択します。[Value] フィールドで、[Regular Expression] または [Regular Expression Class] オプションをクリックし、ドロップダウン リストから式を選択します。

  一般的な操作のコンフィギュレーション ガイドの Configuring Regular Expressions, page 15-20 を参照してください。
- [Source IP Address] : IM メッセージの送信元の IP アドレスを照合する場合に選択します。[Value] フィールドに、メッセージの送信元の IP アドレスおよびネットマスクを入力します。
- [Destination IP Address] : IM メッセージの宛先の IP アドレスを照合する場合に選択します。[Value] フィールドに、メッセージの宛先の IP アドレスおよびネットマスクを入力します。
- [Filename] : IM メッセージのファイル名を照合する場合に選択します。[Value] フィールドで、[Regular Expression] または [Regular Expression Class] オプションをクリックし、ドロップダウン リストから式を選択します。

  一般的な操作のコンフィギュレーション ガイドの Configuring Regular Expressions, page 15-20 を参照してください。

ステップ 9　[OK] をクリックして、基準を保存します。[Add Instant Messaging (IM) Match Criterion] ダイアログボックスが閉じ、[Match Criterion] テーブルに基準が表示されます。

ステップ 10　[OK] をクリックしてクラス マップを保存します。

Select IM Map

[Select IM Map] ダイアログボックスには、次のようにアクセスできます。

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select IM Map]

[Select IM Map] ダイアログボックスでは、IM マップを選択または新しく作成できます。IM マップにより、IM アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select IM Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

IP オプション インスペクション

この項では、IP オプション インスペクション エンジンについて説明します。この項は、次の内容で構成されています。

- 「IP オプション インスペクションの概要」（P.10-38）
- 「IP オプション インスペクションの設定」（P.10-39）
- 「Select IP Options Inspect Map」（P.10-40）
- 「IP Options Inspect Map」（P.10-41）
- 「Add/Edit IP Options Inspect Map」（P.10-41）

IP オプション インスペクションの概要

各 IP パケットには、Options フィールドのある IP ヘッダーが含まれています。Options フィールドは、通常は IP オプションと呼ばれ、制御機能を提供します。特定の状況で必要になりますが、一般的な通信では必要ありません。具体的には、IP オプションにはタイムスタンプ、セキュリティ、および特殊なルーティングの規定が含まれています。IP オプションの使用は任意であり、このフィールドにはオプションを 0 個、1 個、またはそれ以上含めることができます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。このインスペクションを設定することで、パケットの転送許可や、指定した IP オプションのクリアが ASA に指示され、パケットの転送が可能になります。

IP オプション インスペクションでは、パケット内の次の 3 つの IP オプションをチェックできます。

- End of Options List（EOOL）または IP Option 0：このオプションにはゼロ バイトが 1 つだけ含まれており、オプションのリストの終わりを示すために、すべてのオプションの末尾に表示されます。これは、ヘッダー長に基づくヘッダーの末尾とは一致しない場合があります。
- No Operation（NOP）または IP Option 1：IP ヘッダーの Options フィールドには、オプションを 0 個、1 個、またはそれ以上含めることができ、これがフィールド変数全体の長さになります。ただし、IP ヘッダーは 32 ビットの倍数である必要があります。全オプションのビット数が 32 ビットの倍数でない場合、32 ビット境界上のオプションと位置合わせするために、NOP オプションは「内部パディング」として使用されます。
- Router Alert（RTRALT）または IP Option 20：このオプションは、中継ルータに対し、パケットの宛先がそのルータでない場合でも、パケットのコンテンツを検査するよう通知します。このインスペクションは、RSVP を実装している場合に役に立ちます。同様のプロトコルは、パケット配信パス上にあるルータでの比較的複雑な処理を必要とします。

（注）　IP オプション インスペクションは、グローバル インスペクション ポリシーにデフォルトで含まれています。したがって、ASA がルーテッド モードの場合、その ASA はパケットに Router Alert オプション（option 20）が含まれた RSVP トラフィックを許可します。

Router Alert オプションが含まれた RSVP パケットをドロップすると、VoIP の実装で問題が生じることがあります。

IP ヘッダーから Router Alert オプションをクリアするように ASA を設定すると、その IP ヘッダーは次のように変更されます。

- Options フィールドは、32 ビット境界で終了するようにパディングされます。
- Internet header length（IHL; インターネット ヘッダーの長さ）が変更されます。
- パケット全体の長さが変更されます。
- チェックサムが再計算されます。

IP ヘッダーに EOOL、NOP、または RTRALT 以外のオプションがさらに含まれている場合、これらのオプションを許可するように ASA が設定されているかどうかに関係なく、ASA はそのパケットをドロップします。

IP オプション インスペクションの設定

[Add Service Policy Rule Wizard - Rule Actions] ダイアログボックスを使用して IP プロトコル インスペクションを設定します。

このウィザードは [Configuration] > [Firewall] > [Service Policy Rules] > [Add] > [Add Service Policy Rule Wizard - Rule Actions] ダイアログボックスから使用できます。

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] > [Add] の順に選択して、[Add Service Policy Rule Wizard] を開きます。

ウィザードの [Service Policy]、[Traffic Classification Criteria]、および [Traffic Match - Destination Port] の各ページを完了するには、次の手順を実行します。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-9）を参照してください。

[Add Service Policy Rule Wizard - Rule Actions] ダイアログボックスが開きます。

ステップ 2　[IP-Options] チェックボックスをオンにします。

ステップ 3　[Configure] をクリックします。

[Select IP Options Inspect Map] ダイアログボックスが開きます。

ステップ 4　次のいずれかの操作を行います。

- [Use the default IP-Options inspection map] オプション ボタンをクリックして、デフォルトの IP オプション マップを使用します。デフォルト マップは、すべての検査済み IP オプション、つまり [End of Options List (EOOL)]、[No Operation (NOP)]、および [Router Alert (RTRALT)] を含むパケットをドロップします。
- [Select an IP-Options inspect map for fine control over inspection] オプション ボタンをクリックして、定義済みのアプリケーション インスペクション マップを選択します。
- [Add] をクリックして、[Add IP-Options Inspect Map] ダイアログボックスを開き、新しいインスペクション マップを作成します。

ステップ 5　（任意）[Add] をクリックして新しいインスペクション マップを作成した場合、IP オプション インスペクションの次の値を定義します。

a. インスペクション マップの名前を入力します。

b. インスペクション マップの説明を 200 文字以内で入力します。

c. [Parameters] 領域で、ASA 経由で転送する、またはクリアしてから ASA 経由で転送する IP オプションを選択します。

– [Allow packets with the End of Options List (EOOL)] オプション

ゼロ バイトが 1 つだけ含まれたこのオプションは、オプションのリストの終わりを示すために、すべてのオプションの末尾に表示されます。これは、ヘッダー長に基づくヘッダーの末尾とは一致しない場合があります。

– [Allow packets with the No Operation (NOP)] オプション

IP ヘッダーの Options フィールドには、オプションを 0 個、1 個、またはそれ以上含めることができ、これがフィールド変数全体の長さになります。ただし、IP ヘッダーは 32 ビットの倍数である必要があります。全オプションのビット数が 32 ビットの倍数でない場合、32 ビット境界上のオプションと位置合わせするために、NOP オプションは「内部パディング」として使用されます。

– [Allow packets with the Router Alert (RTRALT)] オプション

このオプションは、中継ルータに対し、パケットの宛先がそのルータでない場合でも、パケットのコンテンツを検査するよう通知します。このインスペクションは、RSVP を実装している場合に役に立ちます。同様のプロトコルは、パケット配信パス上にあるルータでの比較的複雑な処理を必要とします。

– [Clear the option value from the packets]

オプションをオンにした場合、[Clear the option value from the packets] チェックボックスからそのオプションで利用できるようになります。[Clear the option value from the packets] チェックボックスをオンにして、ASA でのパケットの通過を許可する前に、そのパケットからそのオプションをクリアします。

d. [OK] をクリックします。

ステップ 6　[OK] をクリックします。

ステップ 7　[Finish] をクリックします。

Select IP Options Inspect Map

[Select IP Options Inspect Map] ダイアログボックスには、次のようにアクセスできます。

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select IM Map]

[Select IP-Options Inspect Map] ダイアログボックスでは、IP オプション インスペクション マップを選択または新しく作成できます。このインスペクション マップを使用して、IP オプション（[End of Options List]、[No Operations]、および [Router Alert]）を含む IP パケットを ASA がドロップ、転送、またはクリアするかを制御します。

フィールド

- [Use the default IP-Options inspection map]：デフォルトの IP オプション マップの使用を指定します。デフォルト マップは、すべての検査済み IP オプション、つまり [End of Options List (EOOL)]、[No Operation (NOP)]、および [Router Alert (RTRALT)] を含むパケットをドロップします。
- [Select an IP-Options map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add IP Options Inspect Map] ダイアログボックスを開きます。

IP Options Inspect Map

[IP Options Inspect Maps] ペインでは、事前に設定された IP オプション インスペクション マップを表示できます。IP オプション インスペクション マップを使用すると、IP オプション インスペクションに使用するデフォルト設定値を変更できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、セキュリティ アプライアンスを通過できるかを制御できます。このインスペクションを設定することで、パケットの転送許可や、指定した IP オプションのクリアがセキュリティ アプライアンスに指示され、パケットの転送が可能になります。

特に、Router Alert（RTRALT）オプションが含まれたパケットをセキュリティ アプライアンスがドロップ、クリア、または転送するかを制御できます。Router Alert オプションが含まれた RSVP パケットをドロップすると、VoIP の実装で問題が生じることがあります。このため、IP オプション インスペクション マップを作成して、RTRALT オプションが含まれたパケットを転送できます。

フィールド

[IP Options Inspect Maps]：定義されている IP オプション インスペクション マップを一覧表示するテーブルです。

[Add]：新しい IP オプション インスペクション マップを設定します。

[Edit]：既存の IP オプション インスペクション マップを編集します。IP オプション インスペクション マップを編集するには、テーブルでエントリを選択し、[Edit] をクリックします。

[Delete]：[IP Options Inspect Maps] テーブルで選択したインスペクション マップを削除します。

Add/Edit IP Options Inspect Map

[Add/Edit IP Options Inspect Map] では、IP オプション インスペクション マップの設定値を設定できます。

フィールド

- [Name]：IP オプション インスペクション マップの追加時に、そのマップの名前を入力します。マップの編集時には、事前に設定したマップの名前が表示されます。
- [Description]：IP オプション インスペクション マップの説明を 200 文字以内で入力します。

- [Parameters] : ASA 経由で転送する、またはクリアしてから ASA 経由で転送する IP オプションを選択します。
  - [Allow packets with the End of Options List (EOOL)] オプション

    ゼロ バイトが 1 つだけ含まれたこのオプションは、オプションのリストの終わりを示すために、すべてのオプションの末尾に表示されます。これは、ヘッダー長に基づくヘッダーの末尾とは一致しない場合があります。
  - [Allow packets with the No Operation (NOP)] オプション

    IP ヘッダーの Options フィールドには、オプションを 0 個、1 個、またはそれ以上含めることができ、これがフィールド変数全体の長さになります。ただし、IP ヘッダーは 32 ビットの倍数である必要があります。全オプションのビット数が 32 ビットの倍数でない場合、32 ビット境界上のオプションと位置合わせするために、NOP オプションは「内部パディング」として使用されます。
  - [Allow packets with the Router Alert (RTRALT)] オプション

    このオプションは、中継ルータに対し、パケットの宛先がそのルータでない場合でも、パケットのコンテンツを検査するよう通知します。このインスペクションは、RSVP を実装している場合に役に立ちます。同様のプロトコルは、パケット配信パス上にあるルータでの比較的複雑な処理を必要とします。
  - [Clear the option value from the packets]

    オプションをオンにした場合、[Clear the option value from the packets] チェックボックスからそのオプションで利用できるようになります。[Clear the option value from the packets] チェックボックスをオンにして、ASA でのパケットの通過を許可する前に、そのパケットからそのオプションをクリアします。

IPsec パススルー インスペクション

この項では、IPSec パススルー インスペクション エンジンについて説明します。この項は、次の内容で構成されています。

- 「IPsec パススルー インスペクションの概要」（P.10-42）
- 「Select IPsec-Pass-Thru Map」（P.10-43）
- 「IPsec Pass Through Inspect Map」（P.10-43）
- 「Add/Edit IPsec Pass Thru Policy Map (Security Level)」（P.10-44）
- 「Add/Edit IPsec Pass Thru Policy Map (Details)」（P.10-45）

IPsec パススルー インスペクションの概要

Internet Protocol Security（IPsec）は、データ ストリームの各 IP パケットを認証および暗号化することによって、IP 通信をセキュリティで保護するためのプロトコル スイートです。IPSec には、セッションの開始時、およびセッション中に使用される暗号キーのネゴシエーションの開始時に、エージェント間の相互認証を確立するためのプロトコルも含まれています。IPSec を使用して、ホスト（コンピュータ ユーザまたはサーバなど）のペア間、セキュリティ ゲートウェイ（ルータやファイアウォールなど）のペア間、またはセキュリティ ゲートウェイとホスト間のデータ フローを保護できます。

IPsec パススルー アプリケーション インスペクションは、IKE UDP ポート 500 接続に関連付けられた ESP（IP プロトコル 50）および AH（IP プロトコル 51）トラフィックを簡単に横断できます。このインスペクションは、冗長な ACL コンフィギュレーションを回避して ESP および AH トラフィックを許可し、タイムアウトと最大接続数を使用してセキュリティも確保します。

インスペクション用パラメータの定義に使用する特定のマップを識別するには、IPsec パススルー インスペクション パラメータを指定します。所定の IPSec パススルー検査のポリシーマップを設定し、パラメータ コンフィギュレーションにアクセスします。このコンフィギュレーションでは、ESP または AH トラフィックの制限を指定できます。パラメータ コンフィギュレーションでは、クライアントあたりの最大接続数と、アイドル タイムアウトを設定できます。

NAT および非 NAT トラフィックは許可されます。ただし、PAT はサポートされません。

Select IPsec-Pass-Thru Map

[Select IPsec-Pass-Thru Map] ダイアログボックスには、次のようにアクセスできます。

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select IPsec-Pass-Thru Map]

[Select IPsec-Pass-Thru] ダイアログボックスでは、IPsec マップを選択または新しく作成できます。IPsec マップにより、IPsec アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select IPsec Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default IPsec inspection map] : デフォルトの IPsec マップの使用を指定します。
- [Select an IPsec map for fine control over inspection] : 定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add] : そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

IPsec Pass Through Inspect Map

[IPsec Pass Through Inspect Map] ダイアログボックスには、次のようにアクセスできます。

[Configuration] > [Global Objects] > [Inspect Maps] > [IPsec Pass Through]

[IPsec Pass Through] ペインでは、IPsec パススルー アプリケーションの事前に設定されたインスペクション マップを表示できます。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 インスペクション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、アクセスリストを使用しなくても、特定のフローを許可できます。

フィールド

- [IPsec Pass Through Inspect Maps] : 定義されている IPsec パススルー インスペクション マップを一覧表示するテーブルです。
- [Add] : 新しい IPsec パススルー インスペクション マップを設定します。IPsec パススルー インスペクション マップを編集するには、[IPsec Pass Through Inspect Maps] テーブルで IPsec パススルーのエントリを選択し、[Customize] をクリックします。
- [Delete] : [IPsec Pass Through Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [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]：[Add/Edit IPsec Pass Thru Policy Map] ダイアログボックスを開き、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。

Add/Edit IPsec Pass Thru Policy Map (Security Level)

[Add/Edit IPsec Pass Thru Policy Map (Security Level)] ダイアログボックスには、次のようにアクセスできます。

[Configuration] > [Global Objects] > [Inspect Maps] > [IPsec Pass Through] > [IPsec Pass Through Inspect Map] > [Basic View]

[Add/Edit IPSec Pass Thru Policy Map] ペインでは、IPSec パススルー アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：IPSec パススルー マップの追加時に IPSec パススルー マップの名前を入力します。IPSec パススルー マップの編集時には、事前に設定した IPSec パススルー マップの名前が表示されます。
- [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

  – [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。
- [Details]：追加の設定を行うパラメータを表示します。

Add/Edit IPsec Pass Thru Policy Map (Details)

[Add/Edit IPsec Pass Thru Policy Map (Details)] ダイアログボックスには、次のようにアクセスできます。

[Configuration] > [Global Objects] > [Inspect Maps] > [IPsec Pass Through] > [IPsec Pass Through Inspect Map] > [Advanced View]

[Add/Edit IPSec Pass Thru Policy Map] ペインでは、IPSec パススルー アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：IPSec パススルー マップの追加時に IPSec パススルー マップの名前を入力します。IPSec パススルー マップの編集時には、事前に設定した IPSec パススルー マップの名前が表示されます。
- [Description]：IPsec パススルー インスペクション マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルを表示します。
- [Parameters]：ESP および AH パラメータを設定します。
  - [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。

IPv6 インスペクション

MPF ルールを使用して IPv6 インスペクションを設定し、拡張ヘッダーに基づいて IPv6 トラフィックを選択的にブロックできます。IPv6 パケットに対しては、早期セキュリティ チェックが実行されます。ASA は、ルータ ヘッダーとノー ネクスト ヘッダーをブロックする一方で、常に、ホップバイホップと宛先オプション タイプの拡張ヘッダーを通過させます。

デフォルトの IPv6 インスペクションをイネーブルにする、または IPv6 インスペクションを定義することができます。IPv6 インスペクションの MPF ポリシー マップを定義することで、IPv6 パケットにある拡張ヘッダーに含まれる、次に示すタイプに基づいて、選択的に IPv6 パケットをドロップするように ASA を設定できます。

- ホップバイホップ オプション
- ルーティング（タイプ 0）
- フラグメント
- 宛先オプション
- 認証
- 暗号ペイロード

デフォルト IPv6 インスペクションでは、IPv6 パケット内の拡張ヘッダーのタイプと順序が RFC 2460 に準拠しているかどうかについてのチェックも実行されます。

- IPv6 ヘッダー
- Hop-by-Hop オプション ヘッダー（0）
- 宛先オプション ヘッダー（60）
- ルーティング ヘッダー（43）
- フラグメント ヘッダー（44）
- 認証（51）
- カプセル化セキュリティ ペイロード ヘッダー（50）
- 宛先オプション ヘッダー（60）
- ノー ネクスト ヘッダー（59）

ポリシー マップが IPv6 インスペクション用に設定されていないか、または設定済みのポリシー マップがインターフェイスに関連付けられていない場合、ASA は、任意のモビリティ タイプで、ルーティング タイプの IPv6 拡張ヘッダーのある、インターフェイスに到着したパケットをドロップします。

IPv6 インスペクション ポリシー マップの作成時に、ASA は、0 ～ 255 の範囲のヘッダー ルーティング タイプに一致するパケットをドロップする設定を自動的に生成します。

IPv6 インスペクション ポリシー マップの設定

IPv6 拡張ヘッダーを処理する IPv6 インスペクション ポリシー マップを設定できます。IPv6 ポリシー マップは、指定された方向の分類された IPv6 パケットごとに適用されます。現在、IPv6 トラフィックのみを検査できます。

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [IPv6] を選択します。[Configure IPv6 Maps] ペインが表示されます。

ステップ 2　[Add] をクリックします。[Add IPv6 Inspection Map] ダイアログボックスが表示されます。

ステップ 3　インスペクション マップの名前と説明を入力します。

デフォルトでは、[Enforcement] タブが選択され、次のオプションが選択されています。

- Permit only known extension headers
- Enforce extension header order

[Permit only known extension headers] が選択されている場合、ASA は IPv6 拡張ヘッダーを検証します。

[Enforce extension header order] が選択されている場合は、RFC 2460 仕様で定義されている IPv6 拡張ヘッダーの順序が適用されます。

これらのオプションが指定されている場合にエラーが検出されると、ASA はパケットをドロップし、アクションをログに記録します。

ステップ 4　拡張ヘッダーでの一致を設定するには、[Header Matches] タブをクリックします。

ステップ 5　[Add] をクリックして、一致を追加します。[Add IPv6 Inspect] ダイアログボックスが表示されます。

ステップ 6　一致の基準を選択します。

次のいずれかの基準を選択した場合は、到着した IPv6 パケットが基準に一致した場合にドロップまたはログに記録するように ASA を設定できます。

- 認証（AH）認証ヘッダー
- 宛先オプション ヘッダー
- カプセル化セキュリティ ペイロード（ESP）ヘッダー
- フラグメント ヘッダー
- ホップバイホップ オプション ヘッダー

ルーティング ヘッダーが選択されており、IPv6 ルーティング拡張ヘッダーが検出された場合、ASA は、ルーティング タイプが一致したか、または指定したルーティング タイプ範囲の数値が一致したときに、指定のアクションを実行します。

ヘッダー カウントが選択されており、IPv6 ルーティング拡張ヘッダーが検出された場合、ASA は、パケット内の IPv6 拡張ヘッダーの数が指定した値を超えると、指定のアクションを実行します。

ルーティング ヘッダー アドレス カウントが選択されており、IPv6 ルーティング拡張ヘッダーが検出された場合、ASA は、タイプ 0 ルーティング ヘッダー内のアドレスの数が設定した値を超えると、指定のアクションを実行します。

ステップ 7　[OK] をクリックして一致基準を保存します。

ステップ 8　[OK] をクリックして IPv6 インスペクション マップを保存します。

NETBIOS インスペクション

この項では、IM インスペクション エンジンについて説明します。この項は、次の内容で構成されています。

- 「NETBIOS インスペクションの概要」（P.10-47）
- 「Select NETBIOS Map」（P.10-47）
- 「NetBIOS Inspect Map」（P.10-48）
- 「Add/Edit NetBIOS Policy Map」（P.10-48）

NETBIOS インスペクションの概要

NETBIOS インスペクションはデフォルトでイネーブルになっています。NetBios インスペクション エンジンは、ASA の NAT コンフィギュレーションに基づいて、NetBios Name Service（NBNS; NetBios ネーム サービス）パケット内の IP アドレスを変換します。

Select NETBIOS Map

[Select NETBIOS Map] ダイアログボックスには、次のようにアクセスできます。

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select NetBIOS Map]

[Select NETBIOS Map] ダイアログボックスでは、NetBIOS マップを選択または新しく作成できます。NetBIOS マップにより、NetBIOS アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select NetBIOS Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default IM inspection map]：デフォルトの NetBIOS マップの使用を指定します。
- [Select a NetBIOS map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

NetBIOS Inspect Map

[NetBIOS Inspect Map] ダイアログボックスには、次のようにアクセスできます。

[Configuration] > [Global Objects] > [Inspect Maps] > [NetBIOS]

[NetBIOS] ペインでは、NetBIOS アプリケーションの事前に設定されたインスペクション マップを表示できます。NetBIOS マップでは、NetBIOS アプリケーション インスペクション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 インスペクションでは、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

- [NetBIOS Inspect Maps]：定義されている NetBIOS インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい NetBIOS インスペクション マップを設定します。
- [Edit]：[NetBIOS Inspect Maps] テーブルで選択した NetBIOS のエントリを編集します。
- [Delete]：[NetBIOS Inspect Maps] テーブルで選択したインスペクション マップを削除します。

Add/Edit NetBIOS Policy Map

[Add/Edit NetBIOS Policy Map] ダイアログボックスには、次のようにアクセスできます。

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

[Add/Edit NetBIOS Policy Map] ペインでは、NetBIOS アプリケーション インスペクション マップのプロトコル違反の設定値を設定できます。

フィールド

- [Name]：NetBIOS マップの追加時に NetBIOS マップの名前を入力します。NetBIOS マップの編集時には、事前に設定した NetBIOS マップの名前が表示されます。
- [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。

PPTP インスペクション

PPTP は、PPP トラフィックのトンネリングに使用されるプロトコルです。PPTP セッションは、1 つの TCP チャネルと通常 2 つの PPTP GRE トンネルで構成されます。TCP チャネルは、PPTP GRE トンネルのネゴシエートと管理に使用される制御チャネルです。GRE トンネルは、2 つのホスト間の PPP セッションを伝送します。

PPTP アプリケーション インスペクションは、イネーブルになると、PPTP プロトコル パケットを検査し、PPTP トラフィックを許可するために必要な GRE 接続と xlate をダイナミックに作成します。RFC 2637 で定義されているバージョン 1 だけがサポートされます。

PAT は、PPTP TCP 制御チャネル上で修正バージョンの GRE（RFC 2637）がネゴシエートされたときに、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE（RFC 1701、RFC 1702）には実行*されません*。

具体的には、ASA は、PPTP のバージョン通知と発信コールの要求/応答シーケンスを検査します。RFC 2637 で定義されている PPTP バージョン 1 だけが検査されます。どちらかの側から通知されたバージョンがバージョン 1 でない場合、TCP 制御チャネルでのそれ以降のインスペクションはディセーブルになります。また、発信コールの要求と応答のシーケンスは追跡されます。接続と xlate は、後続のセカンダリ GRE データ トラフィックを許可するために、必要に応じてダイナミックに割り当てられます。

PPTP インスペクション エンジンは、PPTP トラフィックを PAT で変換できるように、イネーブルにする必要があります。また、PAT は、PPTP TCP 制御チャネルで修正バージョンの GRE（RFC 2637）がネゴシエートされた場合に限り、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE（RFC 1701、RFC 1702）には実行されません。

RFC 2637 で定義されているように、PPTP プロトコルは、主に、モデム バンク PPTP Access Concentrator（PAC; PPTP アクセス コンセントレータ）から開始されたヘッドエンド PPTP Network Server（PNS; PPTP ネットワーク サーバ）への PPP セッションのトンネリングに使用されます。このように使用された場合、PAC がリモート クライアントで PNS がサーバです。

ただし、Windows によって VPN で使用された場合、この関係は逆になります。PNS は、中央のネットワークにアクセスするためにヘッドエンド PAC への接続を開始するリモートのシングル ユーザ PC です。

SMTP および拡張 SMTP インスペクション

この項では、IM インスペクション エンジンについて説明します。この項は、次の内容で構成されています。

- 「SMTP および拡張 SMTP（ESMTP）のインスペクションの概要」（P.10-50）
- 「Select ESMTP Map」（P.10-51）
- 「ESMTP Inspect Map」（P.10-51）
- 「MIME File Type Filtering」（P.10-52）
- 「Add/Edit ESMTP Policy Map（セキュリティ レベル）」（P.10-53）
- 「Add/Edit ESMTP Policy Map（詳細）」（P.10-54）
- 「Add/Edit ESMTP Inspect」（P.10-54）

SMTP および拡張 SMTP（ESMTP）のインスペクションの概要

ESMTP アプリケーション インスペクションを使用すると、ASA を通過できる SMTP コマンドの種類を制限し、モニタ機能を追加することによって、SMTP ベースの攻撃からより強固に保護できます。

ESMTP は SMTP プロトコルの拡張で、ほとんどの観点で SMTP に似ています。便宜上、このマニュアルでは、SMTP という用語を SMTP と ESMTP の両方に使用します。拡張 SMTP に対するアプリケーション インスペクション処理は、SMTP アプリケーション インスペクションに似ており、SMTP セッションのサポートが含まれています。拡張 SMTP セッションで使用するほとんどのコマンドは、SMTP セッションで使用するコマンドと同じですが、ESMTP セッションの方が大幅に高速で、配信ステータス通知など信頼性およびセキュリティに関するオプションが増えています。

拡張 SMTP アプリケーション インスペクションでは、AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS、および VRFY を含む拡張 SMTP コマンドに対するサポートが追加されています。ASA は、7 つの RFC 821 コマンド（DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET）をサポートするとともに、合計 15 の SMTP コマンドをサポートします。

その他の拡張 SMTP コマンド（ATRN、ONEX、VERB、CHUNKING など）、およびプライベート拡張はサポートされません。サポートされないコマンドは、内部サーバにより拒否される X に変換されます。この結果は、「500 Command unknown: 'XXX'」のようなメッセージで表示されます。不完全なコマンドは、廃棄されます。

ESMTP インスペクション エンジンは、文字「2」、「0」、「0」を除くサーバの SMTP バナーの文字をアスタリスクに変更します。Carriage Return（CR; 復帰）、および Linefeed（LF; 改行）は無視されます。

SMTP インスペクションをイネーブルにする場合、次のルールに従わないと、対話型の SMTP に使用する Telnet セッションが停止することがあります。SMTP コマンドの長さは 4 文字以上にする必要があります。復帰と改行で終了する必要があります。次の応答を発行する前に現在の応答を待機する必要があります。

SMTP サーバは、数値の応答コード、およびオプションの可読文字列でクライアント要求に応答します。SMTP アプリケーション インスペクションは、ユーザが使用できるコマンドとサーバが返送するメッセージを制御し、その数を減らします。SMTP インスペクションは、次の 3 つの主要なタスクを実行します。

- SMTP 要求を 7 つの基本 SMTP コマンドと 8 つの拡張コマンドに制限します。
- SMTP コマンド応答シーケンスをモニタします。
- 監査証跡の生成：メール アドレス内に埋め込まれている無効な文字が置き換えられたときに、監査レコード 108002 を生成します。詳細については、RFC 821 を参照してください。

SMTP インスペクションでは、次の異常な署名がないかどうか、コマンドと応答のシーケンスをモニタします。

- 切り捨てられたコマンド
- 不正なコマンド終端（<CR><LR> で終了していない）
- MAIL コマンドと RCPT コマンドでは、メールの送信者と受信者が指定されます。異常な文字がないか、メール アドレスがスキャンされます。パイプ（|）が削除（空白スペースに変更）され、「<」および「>」については、メール アドレスの定義に使用される場合だけ許可されます（「<」の後には、必ず「>」が使用されている必要があります）。
- SMTP サーバによる不意の移行
- 未知のコマンドに対しては、ASA はパケット内のすべての文字を X に変更します。この場合、サーバがクライアントに対してエラー コードを生成します。パケット内が変更されているため、TCP チェックサムは、再計算または調節する必要があります。
- TCP ストリーム編集
- コマンド パイプライン

Select ESMTP Map

[Select ESMTP Map] ダイアログボックスには、次のようにアクセスできます。

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select ESMTP Map]

[Select ESMTP Map] ダイアログボックスでは、ESMTP マップを選択または新しく作成できます。ESMTP マップにより、ESMTP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select ESMTP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default ESMTP inspection map]：デフォルトの ESMTP マップの使用を指定します。
- [Select an ESMTP map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

ESMTP Inspect Map

[ESMTP Inspect Map] ダイアログボックスには、次のようにアクセスできます。

[Configuration] > [Global Objects] > [Inspect Maps] > [ESMTP]

[ESMTP] ペインでは、ESMTP アプリケーションの事前に設定されたインスペクション マップを表示できます。ESMTP マップでは、ESMTP アプリケーション インスペクション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

- [ESMTP Inspect Maps]：定義されている ESMTP インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい ESMTP インスペクション マップを設定します。ESMTP インスペクション マップを編集するには、[ESMTP Inspect Maps] テーブルで ESMTP のエントリを選択し、[Customize] をクリックします。
- [Delete]：[ESMTP Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [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

– [MIME File Type Filtering] : [MIME Type Filtering] ダイアログボックスを開き、MIME ファイル タイプのフィルタを設定します。
– [Customize] : [Add/Edit ESMTP Policy Map] ダイアログボックスを開き、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 File Type Filtering] ダイアログボックスには、次のようにアクセスできます。

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

[MIME File Type Filtering] ダイアログボックスでは、MIME ファイル タイプの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] : インスペクションの基準を示します。
- [Value] : インスペクション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。

Add/Edit ESMTP Policy Map（セキュリティ レベル）

[Add/Edit ESMTP Policy Map]（セキュリティ レベル）ダイアログボックスには、次のようにアクセスできます。

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

[Add/Edit ESMTP Policy Map] ペインでは、ESMTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：ESMTP マップの追加時に ESMTP マップの名前を入力します。ESMTP マップの編集時には、事前に設定した ESMTP マップの名前が表示されます。
- [Description]：ESMTP 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
  - [MIME File Type Filtering]：[MIME Type Filtering] ダイアログボックスを開き、MIME ファイル タイプのフィルタを設定します。
  - [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。
- [Details]：詳細な設定を行うための [Parameters] タブと [Inspections] タブを表示します。

Add/Edit ESMTP Policy Map（詳細）

[Add/Edit ESMTP Policy Map]（詳細）ダイアログボックスには、次のようにアクセスできます。

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

[Add/Edit ESMTP Policy Map] ペインでは、ESMTP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：ESMTP マップの追加時に ESMTP マップの名前を入力します。ESMTP マップの編集時には、事前に設定した ESMTP マップの名前が表示されます。
- [Description]：ESMTP マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルと MIME ファイル タイプ フィルタリング設定を表示します。
- [Parameters]：このタブで ESMTP インスペクション 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]：Drop connection 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 ESMTP インスペクション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 インスペクションの基準を示します。
  - [Value]：ESMTP インスペクション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 インスペクションを追加できます。
  - [Edit]：Edit [ESMTP Inspect] ダイアログボックスが開き、ESMTP インスペクションを編集できます。
  - [Delete]：ESMTP インスペクションを削除します。
  - [Move Up]：インスペクションをリストの上に移動します。
  - [Move Down]：インスペクションをリストの下に移動します。

Add/Edit ESMTP Inspect

[Add/Edit ESMTP Inspect] ダイアログボックスには、次のようにアクセスできます。

[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は、ESMTP インスペクション マップの照合基準と値を定義できます。

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]：Reset、Drop connection、または Log。
  - [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]：Reset、Drop connection、または Log。
  - [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、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。
  - [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] : Reset、Drop connection、または Log。
  - [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] : Reset、Drop connection、または Log。
  - [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] : 選択したコマンドを [Selected Commands] テーブルから削除します。
  - [Action] : Reset、Drop Connection、Mask、または 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、または 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] : コマンド宛先の数を指定します。
  - [Action] : Reset、Drop connection、または Log。
  - [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] : コマンド宛先の数を指定します。
  - [Action] : Reset、Drop connection、または Log。
  - [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。
  - [Action] : Reset、Drop connection、または Log。
  - [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、または 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]：選択したコマンドを [Selected Commands] テーブルから削除します。
- [Action]：Reset、Drop Connection、または 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。
  - [Action]：Reset、Drop Connection、または 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、または Log。
  - [Log]：イネーブルまたはディセーブルにします。

TFTP インスペクション

TFTP インスペクションはデフォルトでイネーブルになっています。

TFTP は、RFC 1350 に記述されているように、TFTP サーバとクライアントの間のファイルの読み書きを行うための簡易プロトコルです。

ASA は、TFTP トラフィックを検査し、必要に応じてダイナミックに接続と変換を作成し、TFTP クライアントとサーバの間のファイル転送を許可します。具体的には、インスペクション エンジンは TFTP Read Request（RRQ; 読み取り要求）、Write Request（WRQ; 書き込み要求）、およびエラー通知（ERROR）を検査します。

有効な読み取り要求（RRQ）または書き込み要求（WRQ）を受信すると、必要に応じて、ダイナミックなセカンダリ チャネルと PAT 変換が割り当てられます。このセカンダリ チャネルは、これ以降 TFTP によってファイル転送またはエラー通知用に使用されます。

TFTP サーバだけがセカンダリ チャネル経由のトラフィックを開始できます。また、TFTP クライアントとサーバの間に存在できる不完全なセカンダリ チャネルは 1 つまでです。サーバからのエラー通知があると、セカンダリ チャネルは閉じます。

TFTP トラフィックのリダイレクトにスタティック PAT が使用されている場合は、TFTP インスペクションをイネーブルにする必要があります。