



## アプリケーションインスペクションの特別なアクション (インスペクションポリシーマップ)

モジュラポリシーフレームワークでは、多くのアプリケーションインスペクションで実行される特別なアクションを設定できます。サービスポリシーでインスペクションエンジンをイネーブルにする場合は、インスペクションポリシーマップで定義されるアクションを必要に応じてイネーブルにすることもできます。インスペクションポリシーマップが、インスペクションアクションを定義したサービスポリシー内のトラフィックと一致すると、トラフィックのそのサブセットが指定したとおりに動作します (たとえば、ドロップやレート制限など)。

- 「インスペクションポリシーマップに関する情報」 (P.2-1)
- 「ガイドラインと制限事項」 (P.2-2)
- 「デフォルトのインスペクションポリシーマップ」 (P.2-3)
- 「インスペクションポリシーマップのアクションの定義」 (P.2-3)
- 「インスペクションクラスマップ内のトラフィックの特定」 (P.2-4)
- 「次の作業」 (P.2-4)
- 「インスペクションポリシーマップの機能履歴」 (P.2-4)

## インスペクションポリシーマップに関する情報

インスペクションポリシーマップをサポートするアプリケーションのリストについては、「[アプリケーションレイヤプロトコルインスペクションの設定](#)」 (P.8-10) を参照してください。

インスペクションポリシーマップは、次に示す要素の1つ以上で構成されています。インスペクションポリシーマップで使用可能な実際のオプションは、アプリケーションに応じて決まります。

- **トラフィック照合オプション**：インスペクションポリシーマップで直接トラフィック照合オプションを定義して、アプリケーションのトラフィックを、URL 文字列などのアプリケーションに固有の基準と照合できます。一致した場合にはアクションをイネーブルにします。
  - 一部のトラフィック照合オプションでは、正規表現を指定してパケット内部のテキストを照合できます。ポリシーマップを設定する前に、正規表現クラスマップ内で、正規表現を単独またはグループで作成およびテストしておいてください。

- **インスペクションクラスマップ**：インスペクションクラスマップには、複数のトラフィック照合オプションが含まれます。その後、ポリシーマップでクラスマップを指定し、クラスマップのアクションを全体としてイネーブルにします。クラスマップを作成することと、インスペクションポリシーマップ内で直接トラフィック照合を定義することの違いは、より複雑な一致基準を作成できる点と、クラスマップを再使用できる点です。ただし、異なる一致基準に対して異なるアクションを設定することはできません。**注**：すべてのアプリケーションがインスペクションクラスマップをサポートするわけではありません。
- **パラメータ**：パラメータは、インスペクションエンジンの動作に影響します。

## ガイドラインと制限事項

- **HTTP インスペクションポリシーマップ**：使用中の HTTP インスペクションポリシーマップを変更する場合、変更を有効にするには、インスペクションポリシーマップのアクションを削除し、再適用する必要があります。たとえば、「`http-map`」インスペクションポリシーマップを修正する場合は、そのインスペクションポリシーマップを削除し、変更を適用して、サービスポリシーに再度追加する必要があります。
- **すべてのインスペクションポリシーマップ**：使用中のインスペクションポリシーマップを別のマップ名と交換する場合は、そのインスペクションポリシーマップを削除し、変更を適用して、新しいインスペクションポリシーマップをサービスポリシーに再度追加する必要があります。
- **インスペクションポリシーマップ**には、複数のインスペクションクラスマップまたは直接照合を指定できます。

1つのパケットが複数の異なる照合と一致する場合、ASA がアクションを適用する順序は、インスペクションポリシーマップにアクションが追加された順序ではなく、ASA の内部ルールによって決まります。内部ルールは、アプリケーションのタイプとパケット解析の論理的進捗によって決まり、ユーザが設定することはできません。HTTP トラフィックの場合、Request Method フィールドの解析が Header Host Length フィールドの解析よりも先に行われ、Request Method フィールドに対するアクションは Header Host Length フィールドに対するアクションより先に行われます。

アクションがパケットをドロップすると、インスペクションポリシーマップではそれ以降のアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合、それ以降の一致基準との照合は行われません。最初のアクションがパケットのログへの記録である場合、接続のリセットなどの2番目のアクションは実行されます。

パケットが、同じ複数の一致基準と照合される場合は、ポリシーマップ内のそれらのコマンドの順序に従って照合されます。

クラスマップは、そのクラスマップ内で重要度が最低の照合オプション（重要度は、内部ルールに基づきます）に基づいて、別のクラスマップまたは直接照合のと同じタイプであると判断されます。クラスマップに、別のクラスマップと同じタイプの重要度が最低の照合オプションがある場合、それらのクラスマップはポリシーマップに追加された順序で照合されます。クラスマップごとに最低重要度の照合が異なる場合は、最高重要度の照合オプションを持つクラスマップが最初に照合されます。

## デフォルトのインスペクションポリシーマップ

DNS インスペクションは、`preset_dns_map` インスペクションクラス マップを使用して、デフォルトでイネーブルになります。

- 最大 DNS メッセージ長は、512 バイトです。
- 最大クライアント DNS メッセージ長は、リソース レコードに一致するように自動的に設定されます。
- DNS ガードはイネーブルになり、ASA によって 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ている 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。
- NAT の設定に基づく DNS レコードの変換はイネーブルです。
- プロトコルの強制はイネーブルであり、DNS メッセージ形式チェックが行われます。ドメイン名の長さが 255 文字以下、ラベルの長さが 63 文字、圧縮、ループ ポインタのチェックなどです。



(注)

`_default_esmtp_map` など、デフォルトのインスペクションポリシーマップはほかにもあります。たとえば、ESMTP インスペクションルールはポリシーマップ「`_default_esmtp_map`」を暗黙的に使用します。

## インスペクションポリシーマップのアクションの定義

サービス ポリシーでインスペクションエンジンをイネーブルにする場合は、インスペクションポリシーマップで定義されるアクションを必要に応じてイネーブルにすることもできます。

### 手順の詳細

- ステップ 1 (オプション) インスペクションクラス マップを作成します。または、ポリシーマップ内でトラフィックを直接特定できます。「[インスペクションクラスマップ内のトラフィックの特定 \(P.2-4\)](#)」を参照してください。
- ステップ 2 (オプション) 正規表現をサポートするポリシーマップタイプの場合は、正規表現を作成します。『一般的な操作のコンフィギュレーションガイド』を参照してください。
- ステップ 3 [Configuration] > [Firewall] > [Objects] > [Inspect Maps] を選択します。
- ステップ 4 設定するインスペクションタイプを選択します。
- ステップ 5 [Add] をクリックして、新しいインスペクションポリシーマップを追加します。
- ステップ 6 インスペクションの章の該当するインスペクションタイプの手順に従います。

## インスペクションクラスマップ内のトラフィックの特定

このタイプのクラスマップを使用して、アプリケーション固有の基準と照合できます。たとえば DNS トラフィックの場合は、DNS クエリー内のドメイン名と照合可能です。

クラスマップは、複数のトラフィック照合をグループ化します (**match-all** クラスマップ)。あるいはクラスマップで、照合リストのいずれかを照合できます (**match-any** クラスマップ)。クラスマップを作成することと、インスペクションポリシーマップ内で直接トラフィック照合を定義することの違いは、クラスマップを使用して複数の **match** コマンドをグループ化できる点と、クラスマップを再使用できる点です。このクラスマップで指定するトラフィックに対しては、インスペクションポリシーマップで、接続のドロップ、リセット、またはログインなどのアクションを指定できます。タイプの異なるトラフィックで異なるアクションを実行する場合は、ポリシーマップで直接トラフィックを指定してください。

### 制限事項

すべてのアプリケーションがインスペクションクラスマップをサポートするわけではありません。

### 手順の詳細

- 
- ステップ 1 [Configuration] > [Firewall] > [Objects] > [Class Maps] を選択します。
  - ステップ 2 設定するインスペクションタイプを選択します。
  - ステップ 3 [Add] をクリックして、新しいインスペクションクラスマップを追加します。
  - ステップ 4 インスペクションの章の該当するインスペクションタイプの手順に従います。
- 

## 次の作業

インスペクションポリシーを使用するには、第1章「サービスポリシー」を参照してください。

## インスペクションポリシーマップの機能履歴

表 2-1 に、この機能のリリース履歴を示します。

表 2-1 サービスポリシーの機能履歴

機能名	リリース	機能情報
インスペクションポリシーマップ	7.2(1)	インスペクションポリシーマップが導入されました。 <b>class-map type inspect</b> コマンドが導入されました。
正規表現およびポリシーマップ	7.2(1)	インスペクションポリシーマップで使用される正規表現およびポリシーマップが導入されました。 <b>class-map type regex</b> コマンド、 <b>regex</b> コマンド、および <b>match regex</b> コマンドが導入されました。

表 2-1 サービスポリシーの機能履歴 (続き)

機能名	リリース	機能情報
インスペクションポリシーマップの match any	8.0(2)	インスペクションポリシーマップで使用される <b>match any</b> キーワードが導入されました。トラフィックを1つ以上の基準に照合してクラスマップに一致させることができます。以前は、 <b>match all</b> だけが使用可能でした。

