CHAPTER 2

# 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

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、またはロギング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。**class-map type inspect** 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。**class-map type regex** コマンド、**regex** コマンド、および**match regex** 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 **match any** 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、**match all** だけが使用可能でした。 |

## インスペクション ポリシー マップの機能履歴