CHAPTER 18

モジュラ ポリシー フレームワークの使用

この章では、モジュラ ポリシー フレームワークを使用して、TCP 用のセキュリティ ポリシー、一般的な接続設定、検査を作成する方法について説明します。

この章で説明する内容は、次のとおりです。

- モジュラ ポリシー フレームワークの概要（p.18-2）
- クラス マップを使用したトラフィックの識別（p.18-3）
- ポリシー マップを使用した動作の定義（p.18-5）
- サービス ポリシーを使用したインターフェイスへのポリシーの適用（p.18-8）
- モジュラ ポリシー フレームワークの例（p.18-9）

モジュラ ポリシー フレームワークの概要

モジュラ ポリシー フレームワークは、Cisco IOS ソフトウェア QoS CLI と同様に、FWSM の機能を設定する一貫したフレキシブルな方法を提供します。たとえば、モジュラ ポリシー フレームワークを使用してタイムアウトを設定すると、すべての TCP アプリケーションにではなく、特定の TCP アプリケーションに固有に適用できます。

モジュラ ポリシー フレームワークは、次の機能とともにサポートされます。

- TCP 接続制限およびタイムアウト
- アプリケーション検査

モジュラ ポリシー フレームワークの設定には、3 つのタスクが含まれます。

1. アクションを適用するトラフィックを識別します。「クラス マップを使用したトラフィックの識別」（p.18-3）を参照してください。
2. トラフィックにアクションを適用します。「ポリシー マップを使用した動作の定義」（p.18-5）を参照してください。
3. インターフェイス上でアクションを実行します。「サービス ポリシーを使用したインターフェイスへのポリシーの適用」（p.18-8）を参照してください。

デフォルトのグローバル ポリシー

デフォルトの設定では、すべてのデフォルトのアプリケーション検査トラフィックと一致し、全インターフェイス上のトラフィックに検査を適用するポリシー（グローバル ポリシー）が含まれます。適用できるのは 1 つのグローバル ポリシーだけなので、グローバル ポリシーを変更する場合は、デフォルト ポリシーを編集するか、またはデフォルト ポリシーをディセーブルにして新しいポリシーを適用する必要があります。

デフォルトのポリシー設定には、次のコマンドが含まれます。

```
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect smtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
service-policy global_policy global
```

クラス マップを使用したトラフィックの識別

クラス マップは、アクションを適用するトラフィックを識別します。クラス マップの最大数はシングル モードまたはマルチ モードの各コンテキストで 255 です。設定には、FWSM がデフォルト グローバル ポリシーで使用するデフォルトのクラス マップが含まれます。これは **inspection_default** といい、デフォルトのインスペクション トラフィックに一致します。

```
class-map inspection_default
 match default-inspection-traffic
```

クラス マップを定義する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、クラス マップを作成します。

```
hostname(config)# class-map class_map_name
```

class_map_name は、最大 40 文字の文字列です。

ステップ 2　（任意）次のコマンドを入力して、クラス マップに説明を追加します。

```
hostname(config-cmap)# description string
```

ステップ 3　次の特性のいずれかと一致させて、クラスに含まれるトラフィックを定義します。別途指定のない限り、**match** コマンド 1 つだけをクラス マップに含めることができます。

- 任意のトラフィック — クラスをすべてのトラフィックに一致させます。

  ```
  hostname(config-cmap)# match any
  ```

- アクセス リスト — クラスを拡張アクセス リストで指定されたトラフィックに一致させます。FWSM が透過ファイアウォール モードで稼働している場合、EtherType アクセス リストを使用できます。

  ```
  hostname(config-cmap)# match access-list acl_ID
  ```

  アクセス リストの作成の詳細については、「拡張アクセス リストの追加」（p.10-7）または「EtherType アクセス リストの追加」（p.10-10）を参照してください。

  Network Address Translation（NAT; ネットワーク アドレス変換）を使用したアクセス リストの作成の詳細については、「NAT 使用時のアクセス リスト用 IP アドレス」（p.10-3）を参照してください。

- TCP または UDP 宛先ポート — クラスを単一ポートまたは連続したポート範囲と一致させることができます。

  ```
  hostname(config-cmap)# match port {tcp | udp} {eq port_num | range port_num
  port_num}
  ```

ヒント　連続しない複数のポートを使用するアプリケーションの場合、**match access-list** コマンドを使用して、各ポートと一致するよう Access Control Entry（ACE; アクセス制御エントリ）を定義します。

ポートのリストについては、「TCP ポートおよび UDP ポート」（p.D-14）を参照してください。

たとえば、次のコマンドを入力して、ポート 80（HTTP）上の TCP パケットを一致させます。

```
hostname(config-cmap)# match tcp eq 80
```

- 検査用のデフォルトのトラフィック — デフォルトで FWSM が検査するトラフィックにクラスを一致させます。

  ```
  hostname(config-cmap)# match default-inspection-traffic
  ```

  match default-inspection-traffic コマンドは、デフォルトで検査されるプロトコルやポートを指定します。デフォルトのインスペクション トラフィックについては、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』のコマンドを参照してください。FWSM には、デフォルト インスペクション トラフィックと一致し、すべてのインターフェイス上のトラフィックに検査を適用するデフォルト グローバル ポリシーが含まれます。

  match default-inspection-traffic コマンドと一緒に **match access-list** コマンドを指定すると、一致したトラフィックを絞り込むことができます。クラスは、**match default-inspection-traffic** コマンドにすでに含まれている **match access-list** コマンド内で指定されたプロトコルまたはポート情報を除外します。

- IP ヘッダーの DSCP 値 — クラスを最大 8 つの DSCP 値に一致させることができます。

  ```
  hostname(config-cmap)# match dscp value1 [value2] [...] [value8]
  ```

  次に、入力例を示します。

  ```
  hostname(config-cmap)# match dscp af43 cs1 ef
  ```

- 優先 — クラスを最大で 4 つの優先値に一致できます。値は IP ヘッダーの TOS バイトで示されます。

  ```
  hostname(config-cmap)# match precedence value1 [value2] [value3] [value4]
  ```

  value1 ～ *value4* は、優先順位に相当する 0 ～ 7 です。

- RTP トラフィック — クラスを RTP トラフィックに一致させることができます。

  ```
  hostname(config-cmap)# match rtp starting_port range
  ```

  starting_port は 2000 ～ 65,534 の間の偶数の UDP 宛先ポートを指定します。*range* は、上述の *starting_port* と一致した追加の UDP ポートの番号を指定します。範囲は 0 ～ 16,383 です。

次に、**class-map** コマンドの例を示します。

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255
hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp
hostname(config-cmap)# exit
hostname(config)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp
hostname(config-cmap)# exit
hostname(config)# class-map all_http
hostname(config-cmap)# description "This class-map matches all HTTP traffic"
hostname(config-cmap)# match port tcp eq http
hostname(config-cmap)# exit
hostname(config)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server
10.1.1.1"
hostname(config-cmap)# match access-list host_foo
hostname(config-cmap)# exit
```

ポリシー マップを使用した動作の定義

ここでは、ポリシー マップを作成してアクションとクラス マップを対応付ける手順について説明します。次の内容について説明します。

- ポリシー マップの概要（p.18-5）
- デフォルトのポリシー マップ（p.18-6）
- ポリシー マップの追加（p.18-6）

ポリシー マップの概要

ポリシー マップで複数のクラス マップを指定できます。1 つまたは複数の機能タイプの複数のアクションを各クラス マップに割り当てることができます。機能タイプには次が含まれます。

- TCP 接続制限およびタイムアウト
- アプリケーション検査

1 つのパケットは、各機能タイプのポリシー マップのクラス マップ 1 つと一致させることができます。パケットが各機能タイプのクラス マップと一致すると、FWSM はパケットをその機能タイプの以降のクラス マップに一致させようとはしません。ただし、パケットが別の機能タイプの以降のクラス マップと一致すると、FWSM は以降のクラス マップのアクションを適用します。

たとえば、パケットが接続制限のクラス マップと一致し、アプリケーション検査のクラス マップとも一致した場合、両方のクラス マップのアクションが適用されます。パケットがアプリケーション検査のクラス マップと一致し、アプリケーション検査の別のクラス マップとも一致した場合、2 番めのクラス マップのアクションは適用されません。

動作はトラフィックに双方向に適用されます。トラフィックが双方向のクラス マップと一致すると、ポリシー マップの適用先であるインターフェイスに発着するすべてのトラフィックが影響を受けます。

（注）　グローバル　ポリシーを使用すると、すべての機能は単一方向になります。単一インターフェイスに適用されると通常は双方向である機能が、グローバルに適用された場合は、各インターフェイスの入力方向のみに適用されます。ポリシーはすべてのインターフェイスに適用されるので、ポリシーは双方向に適用されます。したがって、この場合の双方向性は冗長になります。

ポリシー マップの異なるアクション タイプが実行される順番は、ポリシー マップで動作が表示される順番とは関係ありません。実行される動作は、次の順番で行われます。

- TCP 接続制限およびタイムアウト
- アプリケーション検査

ポリシー マップはインターフェイスごとに 1 つしか割り当てることができませんが、同じポリシー マップを複数のインターフェイスに適用することができます。

デフォルトのポリシー マップ

設定には、FWSM がデフォルト グローバル ポリシーで使用するデフォルトのポリシー マップが含まれます。これは **global_policy** といい、デフォルトのインスペクション トラフィック上の検査で実行されます。適用できるのは 1 つのグローバル ポリシーだけなので、グローバル ポリシーを変更する場合は、デフォルト ポリシーを編集するか、またはデフォルト ポリシーをディセーブルにして新しいポリシーを適用する必要があります。

デフォルトのポリシー マップ設定には、次のコマンドが含まれます。

```
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect smtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
```

ポリシー マップの追加

ポリシー マップを作成する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、ポリシー マップを追加します。

```
hostname(config)# policy-map policy_map_name
```

ステップ 2　（任意）ポリシー マップの説明を指定します。

```
hostname(config-pmap)# description text
```

ステップ 3　次のコマンドを使用して、すでに設定済みのクラス マップを指定します。

```
hostname(config-pmap)# class class_map_name
```

クラス マップを追加するには、「クラス マップを使用したトラフィックの識別」（p.18-3）を参照してください。

ステップ 4　クラス マップに 1 つまたは複数のアクションを指定します。

- 接続制限。「接続制限とタイムアウトの設定」（p.19-2）を参照してください。
- アプリケーション検査。第 20 章「アプリケーション レイヤ プロトコル検査の適用」を参照してください。

（注）　**match default_inspection_traffic** コマンドがクラス マップにない場合、**inspect** コマンドを 1 つだけ、クラスの下に設定できます。

ステップ 5　このポリシー マップに指定する各クラス マップについて、ステップ 4 を繰り返します。

次に、接続ポリシー用の **policy-map** コマンドの例を示します。このコマンドは、Web サーバ 10.1.1.1 への接続を許可する数を制限します。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning
connection to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

次に、複数の一致がポリシー マップ内で動作する例を示します。

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

次に、トラフィックが最初に利用可能なクラス マップと一致し、同一の機能ドメイン内でアクションを指定する以降のクラス マップとは一致しない例を示します。

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

Telnet 接続が開始されると、トラフィックは **class telnet_traffic** と一致します。同様に、FTP 接続が開始されると、トラフィックは **class ftp_traffic** と一致します。Telnet および FTP 以外の TCP 接続の場合、トラフィックは **class tcp_traffic** と一致します。Telnet または FTP 接続が **class tcp_traffic** と一致できても、この接続は他のクラスと以前に一致しているので FWSM ではこの一致は行われません。

サービス ポリシーを使用したインターフェイスへのポリシーの適用

ポリシー マップを実行するには、ポリシー マップを 1 つまたは複数のインターフェイスに適用するか、またはすべてのインターフェイスにグローバルに適用するサービス ポリシーを作成します。インターフェイス サービス ポリシーは、グローバル サービス ポリシーより優先されます。

- ポリシー マップとインターフェイスを対応付けてサービス ポリシーを作成するには、次のコマンドを入力します。

  ```
  hostname(config)# service-policy policy_map_name interface interface_name
  ```

- 特定のポリシーを持たないインターフェイスすべてに適用するサービス　ポリシーを作成するには、次のコマンドを入力します。

  ```
  hostname(config)# service-policy policy_map_name global
  ```

  デフォルトの設定では、すべてのデフォルトのアプリケーション検査トラフィックと一致し、検査をトラフィックにグローバルに適用するグローバル ポリシーが含まれます。適用できるのは 1 つのグローバル ポリシーだけなので、グローバル ポリシーを変更する場合は、デフォルト ポリシーを編集するか、またはデフォルト ポリシーをディセーブルにして新しいポリシーを適用する必要があります。

  デフォルトのサービス ポリシーには、次のコマンドが含まれます。

  ```
  service-policy global_policy global
  ```

たとえば、次のコマンドを使用すると、inbound_policy ポリシー マップを外部インターフェイス上でイネーブルにします。

```
hostname(config)# service-policy inbound_policy interface outside
```

次のコマンドを使用すると、デフォルトのグローバル ポリシーをディセーブルにし、その他すべての FWSM インターフェイス上で new_global_policy という新しいポリシーをイネーブルにします。

```
hostname(config)# no service-policy global_policy global
hostname(config)# service-policy new_global_policy global
```

モジュラ ポリシー フレームワークの例

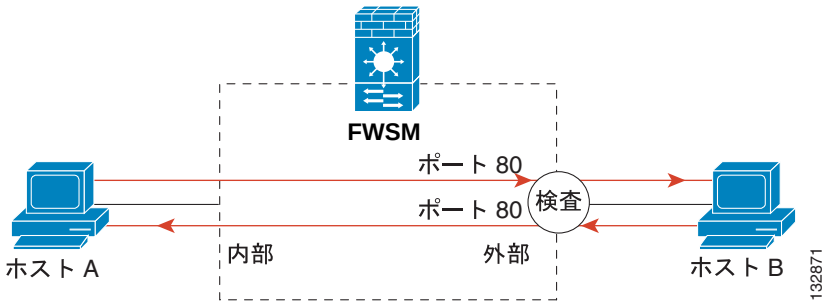
ここでは、モジュラ ポリシー フレームワークの例について説明します。内容は次のとおりです。

- HTTP トラフィックへの検査の適用（p.18-9）
- HTTP トラフィックへの検査のグローバルな適用（p.18-10）
- 特定のサーバに対する HTTP トラフィックの検査および接続制限の適用（p.18-11）
- NAT を使用した HTTP トラフィックへの検査の適用（p.18-12）

HTTP トラフィックへの検査の適用

この例では（図 18-1 を参照）、外部インターフェイス経由で FWSM に発着する HTTP 接続（ポート 80 上の TCP トラフィック）は HTTP 検査用に分類されます。

図 18-1　HTTP 検査



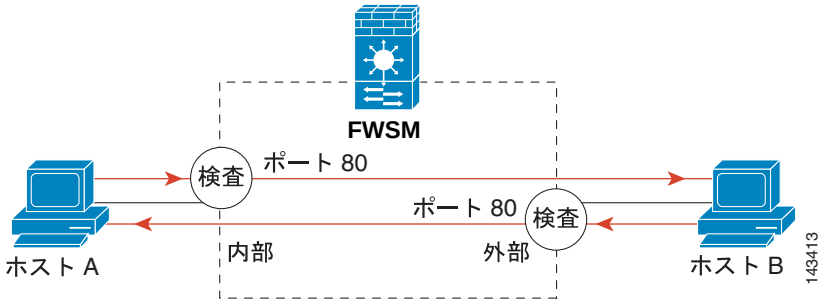
この例に対応するコマンドは、次のとおりです。

```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config)# service-policy http_traffic_policy interface outside
```

HTTP トラフィックへの検査のグローバルな適用

この例では（図 18-2 を参照）、任意のインターフェイス経由で FWSM に入る HTTP 接続（ポート 80 上の TCP トラフィック）は HTTP 検査用に分類されます。ポリシーはグローバル ポリシーなので、トラフィックがインターフェイスに入ったときのみ検査が実行されます。

図 18-2　グローバル HTTP 検査



この例に対応するコマンドは、次のとおりです。

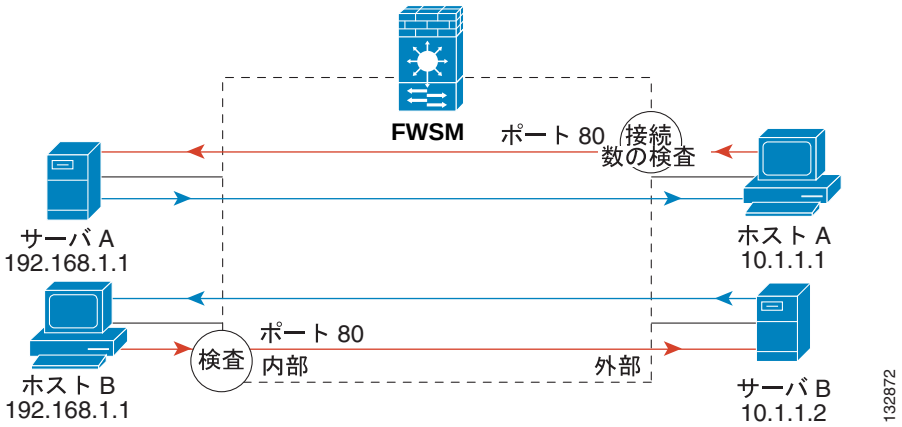
```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config)# service-policy http_traffic_policy global
```

特定のサーバに対する HTTP トラフィックの検査および接続制限の適用

この例では（図 18-3 を参照）、外部インターフェイス経由で FWSM に入り、宛先がサーバ A の HTTP 接続（ポート 80 上の TCP トラフィック）は HTTP 検査用に分類され、最大接続が制限されます。サーバ A からホスト A に開始された接続は、クラス マップのアクセス リストと一致しないので、影響を受けません。

内部インターフェイス経由で FWSM に入り、宛先がサーバ B である HTTP 接続は、HTTP 検査用に分類されます。サーバ B からホスト B に開始された接続は、クラス マップのアクセス リストと一致しないので、影響を受けません。

図 18-3　特定のサーバの HTTP 検査および接続制限



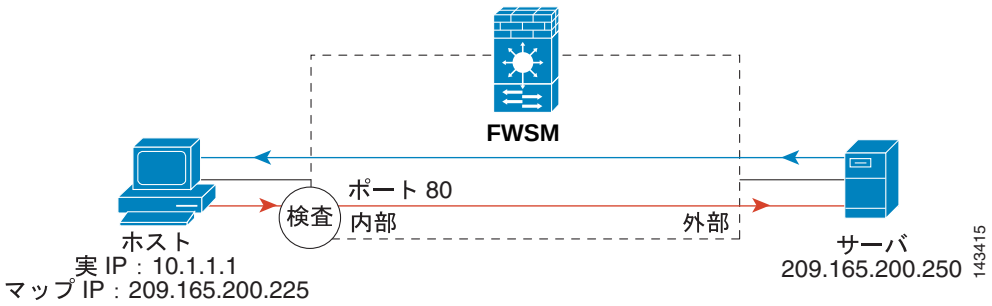
この例に対応するコマンドは、次のとおりです。

```
hostname(config)# access-list serverA extended permit tcp any host 192.168.1.1 eq 80
hostname(config)# access-list ServerB extended permit tcp any host 10.1.1.2 eq 80

hostname(config)# class-map http_serverA
hostname(config-cmap)# match access-list serverA
hostname(config)# class-map http_serverB
hostname(config-cmap)# match access-list serverB

hostname(config)# policy-map policy_serverA
hostname(config-pmap)# class http_serverA
hostname(config-pmap-c)# inspect http http_map_serverA
hostname(config-pmap-c)# set connection conn-max 100
hostname(config)# policy-map policy_serverB
hostname(config-pmap)# class http_serverB
hostname(config-pmap-c)# inspect http http_map_serverB

hostname(config)# service-policy policy_serverB interface inside
hostname(config)# service-policy policy_serverA interface outside
```

NAT を使用した HTTP トラフィックへの検査の適用

この例では、内部ネットワーク上のホストには、実 IP アドレス 10.1.1.1 と、外部ネットワークで使用されるマップされた IP アドレス 209.165.200.225 があります。ポリシーは内部インターフェイスに適用されているので、実アドレスが使用されている場合、実 IP アドレスをクラス マップのアクセス リストで使用する必要があります。ポリシーを外部インターフェイスに適用する場合、マップされたアドレスを使用してください。

図 18-4　NAT を使用した HTTP 検査



この例に対応するコマンドは、次のとおりです。

```
hostname(config)# static (inside,outside) 209.165.200.225 10.1.1.1
hostname(config)# access-list http_client extended permit tcp host 10.1.1.1 any eq 80

hostname(config)# class-map http_client
hostname(config-cmap)# match access-list http_client

hostname(config)# policy-map http_client
hostname(config-pmap)# class http_client
hostname(config-pmap-c)# inspect http

hostname(config)# service-policy http_client interface inside
```