CHAPTER 19

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準備

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 1000V でパケット インスペクションを行う必要があります（高速パスの詳細については、「ステートフル インスペクションの概要」（P.1-10）を参照してください）。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 1000V 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。

アプリケーション レイヤ プロトコル インスペクションに関する情報

この項は、次の内容で構成されています。

インスペクション エンジンの動作

図 19-1 に示されているように、ASA 1000V は基本動作に 3 種類のデータベースを使用します。

- アクセス リスト：特定のネットワーク、ホスト、およびサービス（TCP/UDP ポート番号）に基づく接続の認証と認可のために使用されます。
- インスペクション：事前定義済みの一連のスタティックなアプリケーションレベルのインスペクション機能を含みます。

- 接続（XLATE および CONN テーブル）：確立済みの各接続についての状態および他の情報を保持します。この情報は、確立済みのセッション内でトラフィックを効率的に転送するため、アダプティブ セキュリティ アルゴリズムおよびカットスルー プロキシによって使用されます。

図 19-1　　インスペクション エンジンの動作

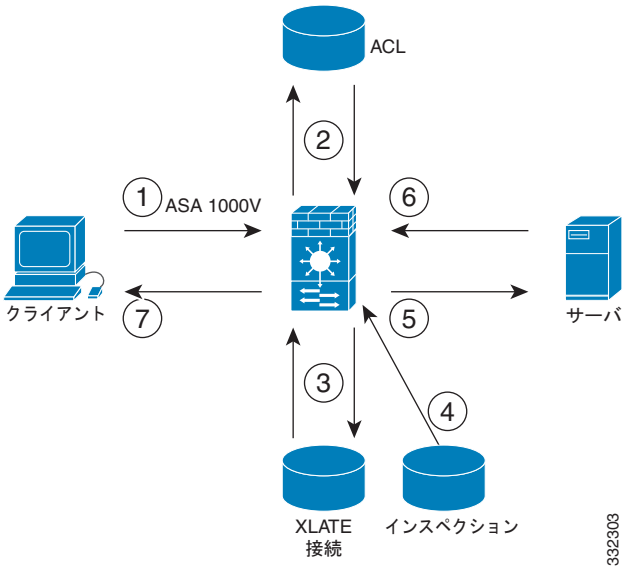

図 19-1 では、動作にはその発生順に番号が付けられており、次でその動作について説明します。

1. TCP SYN パケットが ASA 1000V に到着して、新しい接続を確立します。
2. ASA 1000V はアクセス リスト データベースをチェックして、接続が許可されるかどうかを判定します。
3. ASA 1000V は接続データベース（XLATE および CONN テーブル）に新しいエントリを作成します。
4. ASA 1000V はインスペクション データベースをチェックして、接続にアプリケーションレベルのインスペクションが必要かどうかを判定します。
5. アプリケーション インスペクション エンジンがパケットに必要な処理を完了した後、ASA 1000V はパケットを宛先システムに転送します。
6. 宛先システムは初期要求に応答します。
7. ASA 1000V は応答パケットを受信し、接続データベースで接続を検索して、確立済みのセッションに属しているのでパケットを転送します。

ASA 1000V のデフォルト コンフィギュレーションには、サポートされるプロトコルを特定の TCP または UDP ポート番号と関連付けて、必要とされる特殊な処理を識別する、一連のアプリケーション インスペクション エントリが含まれます。

アプリケーション プロトコル インスペクションを使用するタイミング

ユーザが接続を確立すると、ASA 1000V はアクセス リストと照合してパケットをチェックし、アドレス変換を作成し、高速パスでのセッション用にエントリを作成して、後続のパケットが時間のかかるチェックをバイパスできるようにします。ただし、高速パスは予測可能なポート番号に基づいており、パケット内部のアドレス変換を実行しません。

多くのプロトコルは、セカンダリの TCP ポートまたは UDP ポートを開きます。予約済みポートでの初期セッションは、ダイナミックに割り当てられるポート番号のネゴシエーションに使用されます。

パケットに IP アドレスを埋め込むアプリケーションもあります。この IP アドレスは送信元アドレスと一致する必要があり、通常、ASA 1000V を通過するときに変換されます。

これらのアプリケーションを使用する場合は、アプリケーション インスペクションをイネーブルにする必要があります。

IP アドレスを埋め込むサービスに対してアプリケーション インスペクションをイネーブルにすると、ASA 1000V は埋め込まれたアドレスを変換し、チェックサムや変換の影響を受けたその他のフィールドを更新します。

ダイナミックに割り当てられたポートを使用するサービスに対してアプリケーション インスペクションをイネーブルにすると、ASA 1000V はセッションをモニタしてダイナミックに割り当てられたポートを特定し、所定のセッションの間、それらのポートでのデータ交換を許可します。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

フェールオーバーのガイドライン

インスペクションが必要なマルチメディア セッションのステート情報は、ステートフル フェールオーバーのステート リンク経由では渡されません。

その他のガイドラインと制限事項

一部のインスペクション エンジンは、PAT、NAT、外部 NAT、または同一セキュリティ インターフェイス間の NAT をサポートしません。NAT サポートの詳細については、「デフォルト設定」を参照してください。

すべてのアプリケーション インスペクションについて、ASA 1000V はアクティブな同時データ接続の数を 200 接続に制限します。たとえば、FTP クライアントが複数のセカンダリ接続を開く場合、FTP インスペクション エンジンはアクティブな接続を 200 だけ許可して 201 番目の接続からはドロップし、ASA 1000V はシステム エラー メッセージを生成します。

検査対象のプロトコルは高度な TCP ステート トラッキングの対象となり、これらの接続の TCP ステートは自動的には複製されません。スタンバイ ASA 1000V への接続は複製されますが、TCP ステートを再確立するベスト エフォート型の試行が行われます。

デフォルト設定

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーがコンフィギュレーションに含まれ、すべてのインスペクションがすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。デフォルト アプリケーション インスペクション トラフィックには、各プロトコルのデフォルト ポートへのトラフィックが含まれます。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する（標準以外のポートにインスペクションを適用する場合や、デフォルトでイネーブルになっていないインスペクションを追加する場合など）には、デフォルトのポリシーを編集するか、デフォルトの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。

表 19-1 にサポートされているすべてのインスペクション、デフォルトのクラス マップで使用されるデフォルトのポート、およびデフォルトでオンになっているインスペクション エンジン（太字）を示します。この表には、NAT に関する制限事項も含まれています。

表 19-1　サポートされているアプリケーション インスペクション エンジン

アプリケーション[1]	デフォルト ポート	NAT に関する制限事項	標準[2]	コメント
CTIQBE	TCP/2748	拡張 PAT はサポートされません。	—	—
DCERPC	TCP/135	—	—	—
DNS over UDP	UDP/53	NAT サポートは、WINS 経由の名前解決では使用できません。	RFC 1123	PTR レコードは変更されません。
FTP	TCP/21	—	RFC 959	—
H.323 H.225 および **RAS**	TCP/1720 UDP/1718 UDP (RAS) 1718-1719	同一セキュリティのインターフェイス上の NAT はサポートされません。 スタティック PAT はサポートされません。 拡張 PAT はサポートされません。	ITU-T H.323、H.245、H225.0、Q.931、Q.932	—
HTTP	TCP/80	—	RFC 2616	ActiveX と Java を除去する場合の MTU 制限に注意してください。MTU が小さすぎて Java タグまたは ActiveX タグを 1 つのパケットに納められない場合は、除去の処理は行われません。
ICMP	—	—	—	すべての ICMP トラフィックは、デフォルトのクラス マップで照合されます。
ICMP ERROR	—	—	—	すべての ICMP トラフィックは、デフォルトのクラス マップで照合されます。
ILS（LDAP）	TCP/389	拡張 PAT はサポートされません。	—	—
Instant Messaging（IM; インスタント メッセージ）	クライアントにより異なる	拡張 PAT はサポートされません。	RFC 3860	—
IP オプション	—	—	RFC 791、RFC 2113	すべての IP オプション トラフィックは、デフォルトのクラス マップで照合されます。
MGCP	UDP/2427、2727	拡張 PAT はサポートされません。	RFC 2705bis-05	—
MMP	TCP 5443	拡張 PAT はサポートされません。	—	—

表 19-1　サポートされているアプリケーション インスペクション エンジン （続き）

アプリケーション[1]	デフォルト ポート	NAT に関する制限事項	標準[2]	コメント
NetBIOS Name Server over IP	UDP/137、138（送信元ポート）	拡張 PAT はサポートされません。	—	NetBIOS は、NBNS UDP ポート 137 および NBDS UDP ポート 138 に対してパケットの NAT 処理を実行することでサポートされます。
PPTP	TCP/1723	—	RFC 2637	—
RADIUS Accounting	1646	—	RFC 2865	—
RSH	TCP/514	PAT はサポートされません。	Berkeley UNIX	—
RTSP	TCP/554	拡張 PAT はサポートされません。 外部 NAT はサポートされません。	RFC 2326、2327、1889	HTTP クローキングは処理しません。
SIP	TCP/5060 UDP/5060	外部 NAT はサポートされません。 同一セキュリティのインターフェイス上の NAT はサポートされません。 拡張 PAT はサポートされません。	RFC 2543	—
SKINNY（SCCP）	TCP/2000	外部 NAT はサポートされません。 同一セキュリティのインターフェイス上の NAT はサポートされません。 拡張 PAT はサポートされません。	—	一定の条件下で、Cisco IP Phone 設定をアップロード済みの TFTP は処理しません。
SMTP および **ESMTP**	TCP/25	—	RFC 821、1123	—
SNMP	UDP/161、162	NAT および PAT はサポートされません。	RFC 1155、1157、1212、1213、1215	v.2 RFC 1902 ～ 1908、v.3 RFC 2570 ～ 2580
SQL*Net	TCP/1521	拡張 PAT はサポートされません。	—	v.1 および v.2
Sun RPC over UDP および TCP	UDP/111	拡張 PAT はサポートされません。	—	デフォルトのルールには UDP ポート 111 が含まれています。TCP ポート 111 の Sun RPC インスペクションをイネーブルにする場合は、TCP ポート 111 を照合する新しいルールを作成し、Sun RPC インスペクションを実行する必要があります。
TFTP	UDP/69	—	RFC 1350	ペイロード IP アドレスは変換されません。

表 19-1　サポートされているアプリケーション インスペクション エンジン （続き）

アプリケーション[1]	デフォルト ポート	NAT に関する制限事項	標準[2]	コメント
WAAS	—	拡張 PAT はサポートされません。	—	—
XDCMP	UDP/177	拡張 PAT はサポートされません。	—	—

1. デフォルト ポートに対してデフォルトでイネーブルになっているインスペクション エンジンは太字で表記されています。
2. ASA 1000V は、これらの標準に準拠していますが、検査対象のパケットには準拠を強制しません。たとえば、各 FTP コマンドは特定の順序である必要がありますが、ASA 1000V によってその順序を強制されることはありません。

デフォルト ポリシー コンフィギュレーションには、次のコマンドが含まれます。

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

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

この機能は、モジュラ ポリシー フレームワークを使用してサービス ポリシーを作成します。サービス ポリシーでは、一貫性と柔軟性を備えた方法で ASA 1000V 機能を設定できます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。詳細については、第 14 章「モジュラ ポリシー フレームワークを使用したサービス ポリシーの設定」を参照してください。アプリケーションによっては、インスペクションをイネーブルにすると特別なアクションを実行できるものがあります。詳細については、第 14 章「モジュラ ポリシー フレームワークを使用したサービス ポリシーの設定」を参照してください。

一部のアプリケーションでは、デフォルトでインスペクションがイネーブルになっています。詳細については、「デフォルト設定」を参照してください。この項を参照してインスペクション ポリシーを変更してください。

手順の詳細

ステップ 1　検査するトラフィックを特定するには、通過トラフィック用または管理トラフィック用のレイヤ 3/4 クラス マップを追加します。詳細については、「通過トラフィック用のレイヤ 3/4 クラス マップの作成」（P.14-11）および「管理トラフィック用のレイヤ 3/4 クラス マップの作成」（P.14-13）を参照してください。管理レイヤ 3/4 クラス マップは、RADIUS アカウンティングのインスペクションだけで使用できます。

通過トラフィックのデフォルトのレイヤ 3/4 クラス マップの名前は「inspection_default」です。このクラス マップは、特殊な **match** コマンド（**match default-inspection-traffic**）を使用して、トラフィックを各アプリケーション プロトコルのデフォルト ポートと照合します。

match access-list コマンドを **match default-inspection-traffic** コマンドとともに指定すると、照合するトラフィックを特定の IP アドレスに絞り込むことができます。**match default-inspection-traffic** コマンドによって照合するポートが指定されるため、アクセス リストのポートはすべて無視されます。

ヒント　トラフィック インスペクションは、アプリケーション トラフィックが発生するポートだけで行うことをお勧めします。**match any** などを使用してすべてのトラフィックを検査すると、ASA 1000V のパフォーマンスに影響が出る場合があります。

標準以外のポートを照合する場合は、標準以外のポート用に新しいクラス マップを作成してください。各インスペクション エンジンの標準ポートについては、「デフォルト設定」（P.19-3）を参照してください。必要に応じて同じポリシー内に複数のクラス マップを組み合わせることができるため、照合するトラフィックに応じたクラス マップを作成することができます。ただし、トラフィックがインスペクション コマンドを含むクラス マップと一致し、その後同様にインスペクション コマンドを含む別のクラス マップとも一致した場合、最初に一致したクラスだけが使用されます。たとえば、SNMP では inspection_default クラスを照合します。SNMP インスペクションをイネーブルにするには、ステップ 5 に従って、デフォルト クラスの SNMP インスペクションをイネーブルにします。SNMP を照合する他のクラスを追加しないでください。

たとえば、デフォルトのクラス マップを使用して、インスペクションを 10.1.1.0 から 192.168.1.0 へのトラフィックに限定するには、次のコマンドを入力します。

```
hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
hostname(config)# class-map inspection_default
hostname(config-cmap)# match access-list inspect
```

次のコマンドを使用して、クラス マップ全体を表示します。

```
hostname(config-cmap)# show running-config class-map inspection_default
!
class-map inspection_default
 match default-inspection-traffic
 match access-list inspect
!
```

ポート 21 とポート 1056（標準以外のポート）の FTP トラフィックを検査するには、それらのポートを指定するアクセス リストを作成し、新しいクラス マップに割り当てます。

```
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 21
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 1056
hostname(config)# class-map new_inspection
hostname(config-cmap)# match access-list ftp_inspect
```

ステップ 2　（任意）一部のインスペクション エンジンでは、トラフィックにインスペクションを適用するときの追加パラメータを制御できます。アプリケーションのインスペクション ポリシー マップを設定する方法については、次の項を参照してください。

- DCERPC：「インスペクション制御を追加するための DCERPC インスペクション ポリシー マップの設定」（P.23-2）を参照してください。
- DNS：「インスペクション制御を追加するための DNS インスペクション ポリシー マップの設定」（P.20-7）を参照してください。
- ESMTP：「インスペクション制御を追加するための ESMTP インスペクション ポリシー マップの設定」（P.20-28）を参照してください。
- FTP：「インスペクション制御を追加するための FTP インスペクション ポリシー マップの設定」（P.20-13）を参照してください。
- H323：「インスペクション制御を追加するための H.323 インスペクション ポリシー マップの設定」（P.21-6）を参照してください。
- インスタント メッセージ：「インスペクション制御を追加するためのインスタント メッセージ インスペクション ポリシー マップの設定」（P.20-18）を参照してください。
- IP オプション：「インスペクション制御を追加するための IP オプション インスペクション ポリシー マップの設定」（P.20-22）を参照してください。
- MGCP：「インスペクション制御を追加するための MGCP インスペクション ポリシー マップの設定」（P.21-13）を参照してください。
- NetBIOS：「インスペクション制御を追加するための NetBIOS インスペクション ポリシー マップの設定」（P.20-24）を参照してください。
- RADIUS アカウンティング：「インスペクション制御を追加するための RADIUS インスペクション ポリシー マップの設定」（P.23-4）を参照してください。
- RTSP：「インスペクション制御を追加するための RTSP インスペクション ポリシー マップの設定」（P.21-17）を参照してください。
- SIP：「インスペクション制御を追加するための SIP インスペクション ポリシー マップの設定」（P.21-21）を参照してください。
- Skinny：「インスペクション制御を追加するための Skinny（SCCP）インスペクション ポリシー マップの設定」（P.21-28）を参照してください。
- SNMP：「インスペクション制御を追加するための SNMP インスペクション ポリシー マップの設定」（P.23-5）を参照してください。

ステップ 3　クラス マップ トラフィックで実行するアクションを設定するレイヤ 3/4 ポリシー マップを追加または編集するには、次のコマンドを入力します。

```
hostname(config)# policy-map name
hostname(config-pmap)#
```

デフォルトのポリシー マップの名前は「global_policy」です。このポリシー マップには、「デフォルト設定」（P.19-3）で示されているデフォルトのインスペクションが含まれています。デフォルトのポリシーを変更する場合（インスペクションを追加または削除する場合や、追加のクラス マップを特定してアクションを割り当てる場合など）は、**global_policy** を名前として入力します。

ステップ 4　アクションを割り当てるステップ 1 のクラス マップを特定するには、次のコマンドを入力します。

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

デフォルトのポリシー マップを編集する場合、デフォルトのポリシー マップには inspection_default クラス マップが含まれています。このクラスのアクションを編集する場合は、**inspection_default** を名前として入力します。このポリシー マップに別のクラス マップを追加する場合は、異なる名前を指定してください。必要に応じて同じポリシー内に複数のクラス マップを組み合わせることができるため、照合するトラフィックに応じたクラス マップを作成することができます。ただし、トラフィックがインスペクション コマンドを含むクラス マップと一致し、その後同様にインスペクション コマンド

を含む別のクラス マップとも一致した場合、最初に一致したクラスだけが使用されます。たとえば、SNMP では inspection_default クラス マップを照合します。SNMP インスペクションをイネーブルにするには、ステップ 5 に従って、デフォルト クラスの SNMP インスペクションをイネーブルにします。SNMP を照合する他のクラスを追加しないでください。

ステップ 5　次のコマンドを入力して、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。

```
hostname(config-pmap-c)# inspect protocol
```

protocol には、次のいずれかの値を指定します。

表 19-2　protocol のキーワード

キーワード	注釈
ctiqbe	—
dcerpc [*map_name*]	「インスペクション制御を追加するための DCERPC インスペクション ポリシー マップの設定」（P.23-2）に従って DCERPC インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
dns [*map_name*]	「インスペクション制御を追加するための DNS インスペクション ポリシー マップの設定」（P.20-7）に従って DNS インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。DNS インスペクションのデフォルトのポリシー マップの名前は「preset_dns_map」です。このデフォルトのインスペクション ポリシー マップでは、DNS パケットの最大長が 512 バイトに設定されています。
esmtp [*map_name*]	「インスペクション制御を追加するための ESMTP インスペクション ポリシー マップの設定」（P.20-28）に従って ESMTP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
ftp [**strict** [*map_name*]]	**strict** キーワードを使用して、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いようにすることで、保護されたネットワークのセキュリティを強化できます。詳細については、「strict オプションの使用」（P.20-12）を参照してください。 「インスペクション制御を追加するための FTP インスペクション ポリシー マップの設定」（P.20-13）に従って FTP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
h323 h225 [*map_name*]	「インスペクション制御を追加するための H.323 インスペクション ポリシー マップの設定」（P.21-6）に従って H323 インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
h323 ras [*map_name*]	「インスペクション制御を追加するための H.323 インスペクション ポリシー マップの設定」（P.21-6）に従って H323 インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
http	—
icmp	—
icmp error	—

表 19-2　protocol のキーワード （続き）

キーワード	注釈
ils	—
im [*map_name*]	「インスペクション制御を追加するためのインスタント メッセージ インスペクション ポリシー マップの設定」（P.20-18）に従ってインスタント メッセージ インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
ip-options [*map_name*]	「インスペクション制御を追加するための IP オプション インスペクション ポリシー マップの設定」（P.20-22）に従って IP オプション インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
mgcp [*map_name*]	「インスペクション制御を追加するための MGCP インスペクション ポリシー マップの設定」（P.21-13）に従って MGCP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
netbios [*map_name*]	「インスペクション制御を追加するための NetBIOS インスペクション ポリシー マップの設定」（P.20-24）に従って NetBIOS インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
pptp	—
radius-accounting [*map_name*]	**radius-accounting** キーワードは、管理クラス マップだけで使用できます。管理クラス マップの作成の詳細については、「管理トラフィック用のレイヤ 3/4 クラス マップの作成」（P.14-13）を参照してください。 「インスペクション制御を追加するための RADIUS インスペクション ポリシー マップの設定」（P.23-4）に従って RADIUS アカウンティング インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
rsh	—
rtsp [*map_name*]	「インスペクション制御を追加するための RTSP インスペクション ポリシー マップの設定」（P.21-17）に従って RTSP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
sip [*map_name*]	「インスペクション制御を追加するための SIP インスペクション ポリシー マップの設定」（P.21-21）に従って SIP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
skinny [*map_name*]	「インスペクション制御を追加するための Skinny（SCCP）インスペクション ポリシー マップの設定」（P.21-28）に従って Skinny インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
snmp [*map_name*]	「インスペクション制御を追加するための SNMP インスペクション ポリシー マップの設定」（P.23-5）に従って SNMP インスペクション ポリシー マップを追加した場合は、このコマンドでマップ名を特定します。
sqlnet	—

表 19-2　protocol のキーワード（続き）

キーワード	注釈
sunrpc	デフォルトのクラス マップには UDP ポート 111 が含まれています。TCP ポート 111 の Sun RPC インスペクションをイネーブルにするには、TCP ポート 111 を照合する新しいクラス マップを作成し、クラスをポリシーに追加してから、そのクラスに **inspect sunrpc** コマンドを適用する必要があります。
tftp	—
waas	—
xdmcp	—

ステップ 6　1 つ以上のインターフェイスでポリシー マップをアクティブにするには、次のコマンドを入力します。

```
hostname(config)# service-policy policymap_name {global | interface interface_name}
```

ここで、**global** はポリシー マップをすべてのインターフェイスに適用し、**interface** は 1 つのインターフェイスに適用します。デフォルトでは、デフォルトのポリシー マップ「global_policy」がグローバルに適用されます。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシー マップを 1 つだけ適用できます。