Cisco ASA シリーズ ファイアウォール CLI コンフィギュレーション ガイド

ソフトウェア バージョン 9.3

リリース：2014 年 7 月 24 日
更新：2014 年 9 月 16 日

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
住所、電話番号、FAX 番号は以下のシスコ Web サイトを
ご覧ください。www.cisco.com/go/offices

文書番号: なし、オンライン専用

CONTENTS

このマニュアルについて

マニュアルの目的

このマニュアルは、コマンドライン インターフェイスを使用して Cisco ASA シリーズのファイアウォール機能を設定する際に役立ちます。このマニュアルは、すべての機能を網羅しているわけではなく、ごく一般的なコンフィギュレーションの事例を紹介しています。

また、Web ベースの GUI アプリケーションである適応型セキュリティ デバイス マネージャ（ASDM）を使用して ASA を設定、監視することもできます。ASDM では、コンフィギュレーション ウィザードを使用して、いくつかの一般的なコンフィギュレーションを設定できます。また、あまり一般的ではない事例には、オンラインのヘルプが用意されています。

このマニュアルを通じて、「ASA」という語は、特に指定がない限り、サポートされているモデルに一般的に適用されます。

関連資料

詳細については、「*Navigating the Cisco ASA Series Documentation*」（http://www.cisco.com/go/asadocs）を参照してください。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。

イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
太字の `courier` フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字の `courier` フォント**で示しています。
イタリック体の `courier` フォント	ユーザが値を指定する引数は、*イタリック体の `courier` フォント*で示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。
http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

PART 1

サービス ポリシーとアクセス コントロール

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

リリース：2014 年 7 月 24 日
更新：2014 年 9 月 16 日

モジュラ ポリシー フレームワークを使用したサービス ポリシーにより、一貫性のある柔軟な方法で ASA の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。サービス ポリシーは、1 つのインターフェイスに適用されるか、またはグローバルに適用される複数のアクションまたはルールで構成されます。

サービス ポリシーについて

次の各トピックでは、サービス ポリシーの仕組みについて説明します。

サービス ポリシーのコンポーネント

サービス ポリシーのポイントは、許可しているトラフィックに高度なサービスを適用することです。アクセス ルールによって許可されるトラフィックにサービスポリシーを適用し、サービス モジュールへのリダイレクトやアプリケーション インスペクションの適用などの特別な処理を実行できます。

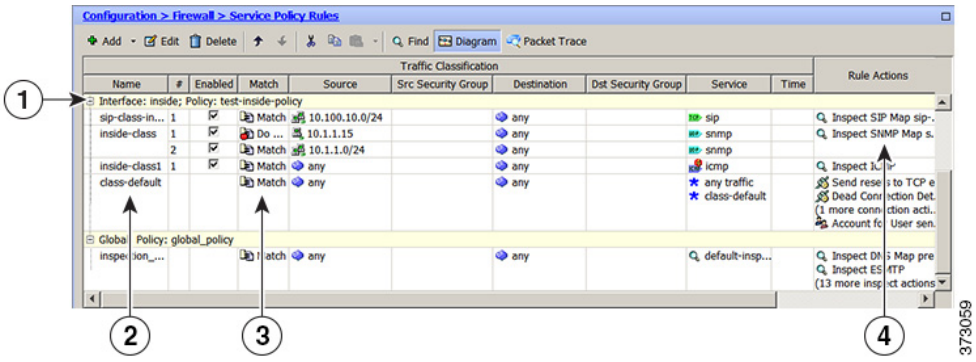
次のタイプのサービス ポリシーを使用できます。

- すべてのインターフェイスに適用される 1 つのグローバル ポリシー。
- インターフェイスごとに適用される 1 つのサービス ポリシー。このポリシーは、デバイスを通過するトラフィックと対象とするクラスと、ASA インターフェイスに向けられた（インターフェイスを通過するのではない）管理トラフィックを対象とするクラスの組み合わせである場合があります。

各サービス ポリシーは、次の要素で構成されます。

1. サービス ポリシー マップ。これはルールの順序セットであり、**service-policy** コマンドで命名されます。ASDM では、ポリシー マップは [Service Policy Rules] ページにフォルダとして表示されます。
2. ルール。各ルールは、サービス ポリシー内の、**class** コマンドと **class** に関連するコマンド群で構成されます。ASDM では、各ルールは個別の行に表示され、ルールの名前はクラス名です。
   a. **class** コマンドは、ルールのトラフィック照合基準を定義します。
   b. **inspect** や **set connection timeout** などの class 関連のコマンドは、一致するトラフィックに適用するサービスと制約を定義します。inspect コマンドは、検査対象トラフィックに適用するアクションを定義するインスペクション ポリシー マップを指す場合があります。インスペクション ポリシー マップとサービス ポリシー マップは同じではないことに注意してください。

次の例では、サービス ポリシーが CLI と ASDM でどのように表示されるかを比較します。図の吹き出しと CLI の行は 1 対 1 で対応しないことに注意してください。



次の CLI は、上の図に示すルールによって生成されます。

```
: Access lists used in class maps.
: In ASDM, these map to call-out 3, from the Match to the Time fields.
access-list inside_mpc line 1 extended permit tcp 10.100.10.0 255.255.255.0 any eq sip
access-list inside_mpc_1 line 1 extended deny udp host 10.1.1.15 any eq snmp
access-list inside_mpc_1 line 2 extended permit udp 10.1.1.0 255.255.255.0 any eq snmp
access-list inside_mpc_2 line 1 extended permit icmp any any
: SNMP map for SNMP inspection.Denies all by v3.
: In ASDM, this maps to call-out 4, rule actions, for the class-inside policy.
```

```
snmp-map snmp-v3only
  deny version 1
  deny version 2
  deny version 2c
: Inspection policy map to define SIP behavior.
: The sip-high inspection policy map must be referred to by an inspect sip command
: in the service policy map.
: In ASDM, this maps to call-out 4, rule actions, for the sip-class-inside policy.
policy-map type inspect sip sip-high
  parameters
    rtp-conformance enforce-payloadtype
    no traffic-non-sip
    software-version action mask log
    uri-non-sip action mask log
    state-checking action drop-connection log
    max-forwards-validation action drop log
    strict-header-validation action drop log
: Class map to define traffic matching for the inside-class rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class
  match access-list inside_mpc_1
: Class map to define traffic matching for the sip-class-inside rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map sip-class-inside
  match access-list inside_mpc
: Class map to define traffic matching for the inside-class1 rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class1
  match access-list inside_mpc_2
: Policy map that actually defines the service policy rule set named test-inside-policy.
: In ASDM, this corresponds to the folder at call-out 1.
policy-map test-inside-policy
: First rule in test-inside-policy, named sip-class-inside.Inspects SIP traffic.
: The sip-class-inside rule applies the sip-high inspection policy map to SIP inspection.
: In ASDM, each rule corresponds to call-out 2.
  class sip-class-inside
    inspect sip sip-high
: Second rule, inside-class.Applies SNMP inspection using an SNMP map.
  class inside-class
    inspect snmp snmp-v3only
: Third rule, inside-class1.Applies ICMP inspection.
  class inside-class1
    inspect icmp
: Fourth rule, class-default.Applies connection settings and enables user statistics.
  class class-default
    set connection timeout embryonic 0:00:30 half-closed 0:10:00 idle 1:00:00
reset dcd 0:15:00 5
    user-statistics accounting
: The service-policy command applies the policy map rule set to the inside interface.
: This command activates the policies.
service-policy test-inside-policy interface inside
```

サービス ポリシーで設定される機能

次の表に、サービス ポリシーを使用して設定する機能を示します。

表 1-1　サービス ポリシーで設定される機能

機能	通過トラフィック用か	管理トラフィック用か	次を参照してください。
アプリケーション インスペクション（複数タイプ）	RADIUS アカウンティングを除く**すべて**	**RADIUS アカウンティング**のみ	• 第 7 章「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」 • 第 8 章「基本インターネット プロトコルのインスペクション」 • 第 9 章「音声とビデオのプロトコルのインスペクション」 • 第 10 章「データベースおよびディレクトリ プロトコルのインスペクション」 • 第 11 章「管理アプリケーション プロトコルのインスペクション」 • 第 15 章「ASA および Cisco Cloud Web Security」
ASA IPS	**はい**	いいえ	第 19 章「ASA IPS モジュール」
ASA CX	**はい**	いいえ	第 18 章「ASA CX モジュール」
ASA FirePOWER（ASA SFR）	**はい**	いいえ	第 17 章「ASA FirePOWER（SFR）モジュール」
NetFlow セキュア イベント ロギングのフィルタリング	**はい**	**はい**	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。
QoS 入出力ポリシング	**はい**	いいえ	第 13 章「QoS」
QoS 標準プライオリティ キュー	**はい**	いいえ	第 13 章「QoS」
TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化	**はい**	**はい**	第 12 章「接続設定」
TCP の正規化	**はい**	いいえ	第 12 章「接続設定」
TCP ステート バイパス	**はい**	いいえ	第 12 章「接続設定」
アイデンティティ ファイアウォールのユーザ統計情報	**はい**	**はい**	コマンド リファレンスの **user-statistics** コマンドを参照してください。

機能の方向

アクションは、機能に応じて双方向または単方向にトラフィックに適用されます。双方向に適用される機能の場合、トラフィックが両方向のクラス マップと一致した場合に、ポリシー マップを適用するインターフェイスを出入り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場合は、すべての機能が単方向です。単一インターフェイスに適用する場合に通常双方向の機能は、グローバルに適用される場合、各インターフェイスの入力にのみ適用されます。ポリシーはすべてのインターフェイスに適用されるため、ポリシーは両方向に適用され、この場合の双方向は冗長になります。

QoS プライオリティ キューなど単方向に適用される機能の場合は、ポリシー マップを適用するインターフェイスに出入りする（機能によって異なります）トラフィックだけが影響を受けます。各機能の方向については、次の表を参照してください。

表 1-2　機能の方向

機能	単一インターフェイスでの方向	グローバルでの方向
アプリケーション インスペクション（複数タイプ）	双方向	入力
ASA CSC	双方向	入力
ASA CX	双方向	入力
ASA CX 認証プロキシ	入力	入力
ASA FirePOWER（ASA SFR）	双方向	入力
ASA IPS	双方向	入力
NetFlow セキュア イベント ロギングのフィルタリング	該当なし	入力
QoS 入力ポリシング	入力	入力
QoS 出力ポリシング	出力	出力
QoS 標準プライオリティ キュー	出力	出力
TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化	双方向	入力
TCP の正規化	双方向	入力
TCP ステート バイパス	双方向	入力
アイデンティティ ファイアウォールのユーザ統計情報	双方向	入力

サービス ポリシー内の機能照合

パケットは、次のルールに従って特定のインターフェイスのポリシー マップのクラス マップに一致します。

1. パケットは、各機能タイプのポリシー マップ ルールで、1 つのクラス マップにだけ一致します。
2. パケットが機能タイプのクラス マップに一致した場合、ASA は、その機能タイプの後続のクラス マップとは照合しません。

3. ただし、パケットが別の機能タイプの後続のクラス マップと一致した場合、ASA は、後続のクラス マップのアクションも適用します（サポートされている場合）。サポートされていない組み合わせの詳細については、「特定の機能アクションの非互換性」（P.1-7）を参照してください。

（注）　アプリケーション インスペクションには、複数のインスペクション タイプが含まれ、ほとんどのタイプは相互に排他的です。組み合わせ可能なインスペクションの場合、各インスペクションは個々の機能と見なされます。

パケット照合の例

次に例を示します。

- パケットが接続制限値のクラス マップ と一致し、アプリケーション インスペクションのクラス マップ とも一致した場合、両方のクラス マップ アクションが適用されます。
- パケットが HTTP インスペクションで 1 つのクラス マップと一致し、HTTP インスペクションを含む別のクラス マップ とも一致した場合、2 番目のクラス マップ のアクションは適用されません。
- パケットが FTP インスペクションで 1 つのクラス マップ と一致し、HTTP インスペクションを含む別のクラス マップ とも一致した場合、HTTP および FTP インスペクションは組み合わせることができないため、2 番目のクラス マップのアクションは適用されません。
- パケットが HTTP インスペクションで 1 つのクラス マップ と一致し、さらに IPv6 インスペクションを含む別のクラス マップ とも一致した場合、IPv6 インスペクションは他のタイプのインスペクションと組み合わせることができるため、両方のアクションが適用されます。

複数の機能アクションが適用される順序

ポリシー マップの各種のアクションが実行される順序は、ポリシー マップ 中に出現する順序とは無関係です。

アクションは次の順序で実行されます。

1. QoS 入力ポリシング
2. TCP の正規化、TCP と UDP の接続制限値とタイムアウト、TCP シーケンス番号のランダム化、および TCP ステート バイパス

（注）　ASA がプロキシ サービス（AAA や CSC など）を実行したり、TCP ペイロード（FTP インスペクション）を変更したりするときは、TCP ノーマライザはデュアル モードで動作します。その場合、サービスを変更するプロキシやペイロードの前後で適用されます。

3. ASA CSC
4. 他のインスペクションと組み合わせることができるアプリケーション インスペクション：
   a. IPv6
   b. IP オプション
   c. WAAS
5. 他のインスペクションと組み合わせることができないアプリケーション インスペクション：詳細については、「特定の機能アクションの非互換性」（P.1-7）を参照してください。

6. ASA IPS
7. ASA CX
8. ASA FirePOWER（ASA SFR）
9. QoS 出力ポリシング
10. QoS 標準プライオリティ キュー

（注）　NetFlow セキュア イベント ロギングのフィルタリングとアイデンティティ ファイアウォールのユーザ統計情報は順番に依存しません。

特定の機能アクションの非互換性

一部の機能は同じトラフィックに対して相互に互換性がありません。次のリストには、すべての非互換性が含まれていない場合があります。各機能の互換性については、機能に関する章または項を参照してください。

- QoS プライオリティ キューイングと QoS ポリシングは同じトラフィックの集合に対して設定できません。
- ほとんどのインスペクションは別のインスペクションと組み合わせられないため、同じトラフィックに複数のインスペクションを設定しても、ASA は 1 つのインスペクションだけを適用します。HTTP インスペクションはクラウド Web セキュリティ インスペクションと組み合わせることができます。他の例外は、「複数の機能アクションが適用される順序」（P.1-6）に記載されています。
- トラフィックを ASA CX および ASA IPS などの複数のモジュールに送信されるように設定することはできません。
- HTTP インスペクションは、ASA CX または ASA FirePOWER と互換性がありません。
- クラウド ネットワーク セキュリティは、ASA CX または ASA FirePOWER と互換性がありません。

（注）　デフォルト グローバル ポリシーで使用される **match default-inspection-traffic** コマンドの は、デフォルト ポートをすべてのインスペクションと照合する特別な CLI ショートカットです。ポリシー マップで使用すると、このクラス マップでは、トラフィックの宛先ポートに基づいて、各パケットに正しいインスペクションが適用されます。たとえば、宛先がポート 69 の UDP トラフィックが ASA に到達すると、ASA は TFTP インスペクションを適用し、宛先がポート 21 の TCP トラフィックが到着すると、ASA は FTP インスペクションを適用します。そのため、この場合に限って同じクラス マップに複数のインスペクションを設定できます。通常、ASA は、ポート番号を使用して適用するインスペクションを決定しないため、標準以外のポートなどにも柔軟にインスペクションを適用できます。

このトラフィック クラスには、クラウド Web セキュリティ インスペクション用のデフォルト ポートは含まれません（80 および 443）。

誤った設定例は、同じポリシー マップに複数のインスペクションを設定しても、default-inspection-traffic ショートカットを使用しないことです。例 1-1 では、ポート 21 宛てのトラフィックが、FTP インスペクションと HTTP インスペクションの両方に誤って設定されています。例 1-2 では、ポート 80 宛てのトラフィックが、FTP インスペクションと HTTP インスペクションの両方に誤って設定されています。どちらの誤った設定例の場合も、FTP インスペクションだけが適用されています。これは、適用されたインスペクションの順序では、FTP が HTTP よりも先になるためです。

例 1-1　　FTP パケットの誤設定（HTTP インスペクションも設定されている）

```
class-map ftp
   match port tcp eq 21
class-map http
   match port tcp eq 21 [80 の誤り]
policy-map test
   class ftp
     inspect ftp
   class http
     inspect http
```

例 1-2　　HTTP パケットの誤設定（FTP インスペクションも設定されている）

```
class-map ftp
   match port tcp eq 80 [21 の誤り]
class-map http
   match port tcp eq 80
policy-map test
   class ftp
     inspect ftp
   class http
     inspect http
```

複数のサービス ポリシーの場合の機能照合

TCP および UDP トラフィック（およびステートフル ICMP インスペクションがイネーブルの場合は ICMP）の場合、サービス ポリシーはトラフィック フローに対して作用し、個々のパケットに限定されません。トラフィックが、1 つのインターフェイスのポリシーで定義されている機能に一致する既存の接続の一部である場合、そのトラフィック フローを別のインターフェイスのポリシーにある同じ機能と照合することはできません。最初のポリシーのみが使用されます。

たとえば、HTTP トラフィックが、HTTP トラフィックを検査する内部インターフェイスのポリシーと一致するときに、HTTP インスペクション用の外部インターフェイスに別のポリシーがある場合、そのトラフィックが外部インターフェイスの出力側でも検査されることはありません。同様に、その接続のリターン トラフィックが外部インターフェイスの入力ポリシーによって検査されたり、内部インターフェイスの出力ポリシーによって検査されたりすることもありません。

ステートフル ICMP インスペクションをイネーブルにしない場合の ICMP のように、フローとして扱われないトラフィックの場合は、リターン トラフィックを戻り側のインターフェイスの別のポリシー マップと照合できます。たとえば、内部および外部のインターフェイスで IPS を設定するとき、内部ポリシーでは仮想センサー 1 を使用するのに対して、外部ポリシーでは仮想センサー 2 を使用する場合、非ステートフル ping は仮想センサー 1 の発信側を照合するだけでなく、仮想センサー 2 の着信側も照合します。

サービス ポリシーのガイドライン

IPv6 のガイドライン

IPv6 は次の機能でサポートされています。

- DNS、FTP、HTTP、ICMP、ScanSafe、SIP、SMTP、IPsec-pass-thru、および IPv6 のアプリケーション インスペクション。
- ASA IPS
- ASA CX
- ASA FirePOWER
- NetFlow セキュア イベント ロギングのフィルタリング
- TCP と UDP の接続制限値とタイムアウト、および TCP シーケンス番号のランダム化
- TCP の正規化
- TCP ステート バイパス
- アイデンティティ ファイアウォールのユーザ統計情報

クラスマップ（トラフィック クラス）のガイドライン

すべてのタイプのクラス マップ（トラフィック クラス）の最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- レイヤ 3/4 クラスマップ（通過トラフィックと管理トラフィック向け）。
- インスペクション クラス マップ
- 正規表現クラス マップ
- インスペクション ポリシー マップ下で直接使用される **match** コマンド

この制限には、すべてのタイプのデフォルト クラス マップも含まれ、ユーザ設定のクラス マップを約 235 に制限します。「デフォルトのクラス マップ（トラフィック クラス）」（P.1-11）を参照してください。

ポリシー マップのガイドライン

ポリシー マップを使用する場合は、次のガイドラインを参考にしてください。

- 各インターフェイスには、ポリシー マップを 1 つだけ割り当てることができます。ただし、設定では最大 64 のポリシー マップを作成できます。
- 同一のポリシー マップを複数のインターフェイスに適用できます。
- 1 つのレイヤ 3/4 ポリシー マップで最大 63 のレイヤ 3/4 クラス マップを識別できます。
- クラス マップごとに、1 つ以上の機能タイプから複数のアクションを割り当てることができます（サポートされている場合）。「特定の機能アクションの非互換性」（P.1-7）を参照してください。

サービス ポリシーのガイドライン

- インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、FTP インスペクションのグローバル ポリシーと、TCP 正規化のインターフェイス ポリシーがある場合、FTP インスペクションと TCP 正規化の両方がインターフェイスに適用されます。これに対し、FTP インスペクションのグローバル ポリシーと、FTP インスペクションのインターフェイス ポリシーがある場合は、インターフェイス ポリシーの FTP インスペクションだけがインターフェイスに適用されます。

- 適用できるグローバル ポリシーは 1 つだけです。たとえば、機能セット 1 が含まれたグローバル ポリシーと、機能セット 2 が含まれた別のグローバル ポリシーを作成することはできません。すべての機能は 1 つのポリシーに含める必要があります。
- コンフィギュレーションに対してサービス ポリシーの変更を加えた場合は、すべての*新しい*接続で新しいサービス ポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。**show** コマンドの出力には、古い接続に関するデータは含まれません。

  たとえばインターフェイスから QoS サービス ポリシーを削除し、変更したバージョンを追加した場合、**show service-policy** コマンドには、新しいサービス ポリシーに一致する新しい接続に関連付けられた QoS カウンタだけが表示されます。古いポリシーの既存の接続はコマンド出力には表示されなくなります。

  すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。**clear conn** または **clear local-host** コマンドを使用してください。

サービス ポリシーのデフォルト

次の各トピックでは、サービス ポリシーとモジュラ ポリシー フレームワークのデフォルト設定について説明します。

- 「デフォルトのサービス ポリシー設定」（P.1-10）
- 「デフォルトのクラス マップ（トラフィック クラス）」（P.1-11）

デフォルトのサービス ポリシー設定

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、特定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）。すべてのインスペクションがデフォルトでイネーブルになっているわけではありません。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場合は、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します。（特定の機能では、グローバル ポリシーはインターフェイス ポリシーより優先されます）。

デフォルト ポリシーには、次のアプリケーション インスペクションが含まれます。

- DNS
- FTP
- H323（H225）
- H323（RAS）
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny（SCCP）
- SunRPC
- XDMCP

- SIP
- NetBios
- TFTP
- IP オプション

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 client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225 _default_h323_map
  inspect h323 ras _default_h323_map
  inspect ip-options _default_ip_options_map
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp _default_esmtp_map
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
service-policy global_policy global
```

（注） デフォルトのクラス マップで使用される特別な **match default-inspection-traffic** コマンドの詳細については、「特定の機能アクションの非互換性」（P.1-7）を参照してください。

デフォルトのクラス マップ（トラフィック クラス）

設定には、ASA が default-inspection-traffic というデフォルト グローバル ポリシーで使用するデフォルトのレイヤ 3/4 クラス マップ（トラフィック クラス）が含まれます。このクラス マップは、デフォルトのインスペクション トラフィックを照合します。デフォルト グローバル ポリシーで使用されるこのクラスは、デフォルト ポートをすべてのインスペクションと照合する特別なショートカットです。

ポリシーで使用すると、このクラスでは、トラフィックの宛先ポートに基づいて、各パケットに正しいインスペクションが適用されます。たとえば、宛先がポート 69 の UDP トラフィックが ASA に到達すると、ASA は TFTP インスペクションを適用し、宛先がポート 21 の TCP トラフィックが到着すると、ASA は FTP インスペクションを適用します。そのため、この場合に限って同じクラス マップに複数のインスペクションを設定できます。通常、ASA は、ポート番号を使用して適用するインスペクションを決定しないため、標準以外のポートなどにも柔軟にインスペクションを適用できます。

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

デフォルト コンフィギュレーションにある別のクラス マップは、class-default と呼ばれ、すべてのトラフィックと一致します。このクラス マップは、すべてのレイヤ 3/4 ポリシー マップの最後に表示され、原則的に、他のすべてのトラフィックでどんなアクションも実行しないように ASA に通知します。必要であれば、独自の **match any** クラス マップを作成する代わりに、class-default クラスを使用できます。実際、一部の機能は class-default でしか使用できません。

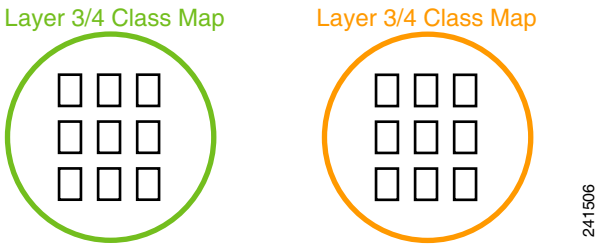
```
class-map class-default
 match any
```

サービス ポリシーの設定

モジュラ ポリシー フレームワークを使用してサービス ポリシーを設定するには、次の手順を実行します。

ステップ 1　「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）の説明に従って、レイヤ 3/4 クラス マップを作成して、操作対象のトラフィックを特定します。

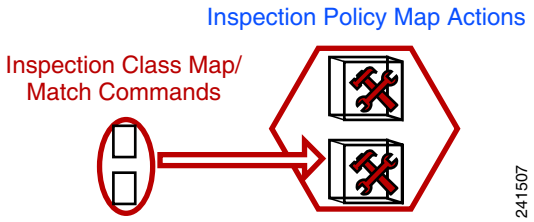
たとえば、ASA を通過するすべてのトラフィックでアクションを実行したり、10.1.1.0/24 から任意の宛先アドレスまでのトラフィックで特定のアクションだけを実行したりできます。



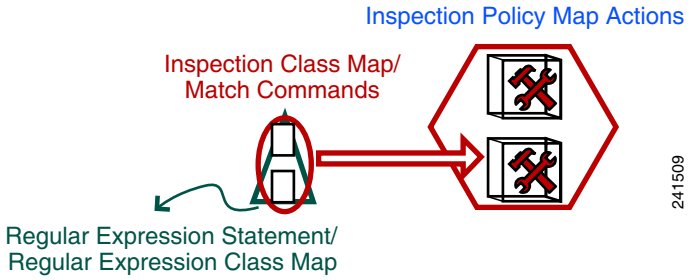
ステップ 2　必要に応じて、あるインスペクション トラフィックで追加のアクションを実行します。

実行するアクションの 1 つがアプリケーション インスペクションであり、あるインスペクション トラフィックで追加のアクションを実行する場合は、検査ポリシーマップを作成します。インスペクション ポリシー マップはトラフィックを特定し、そのトラフィックで何をするかを指定します。

たとえば、本文の長さが 1000 バイトを上回るすべての HTTP 要求をドロップできます。

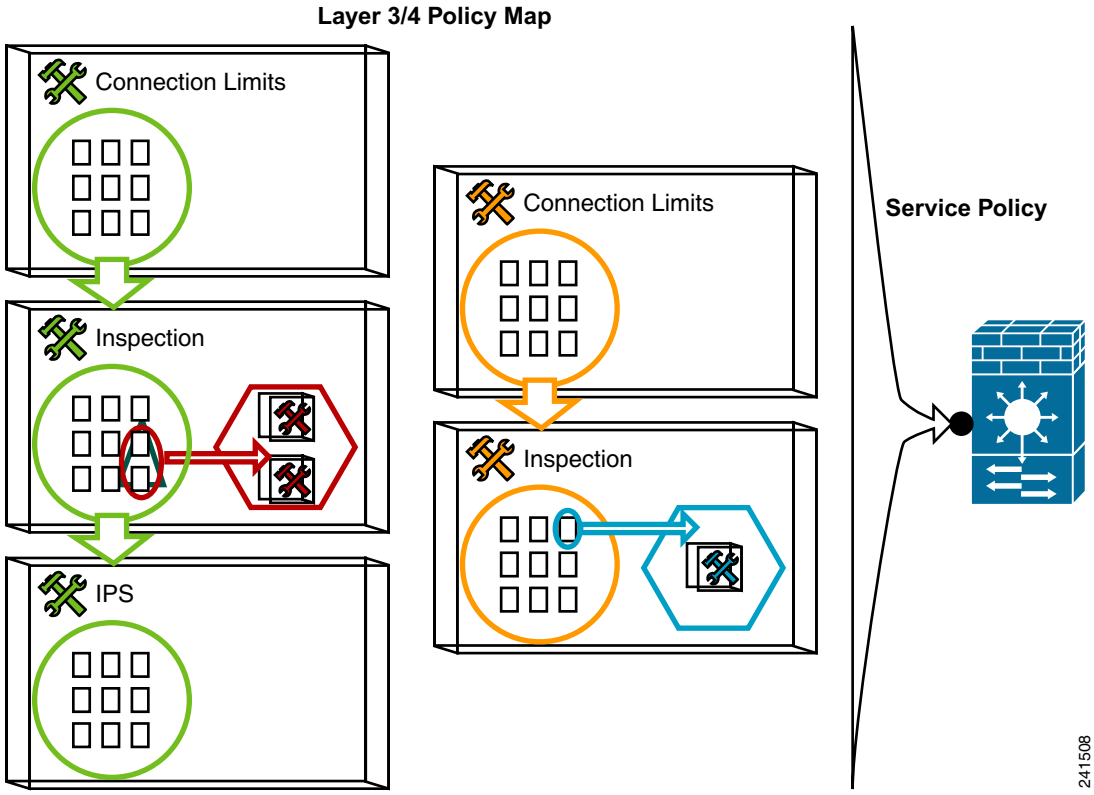


match コマンドでトラフィックを直接特定する独立したインスペクション ポリシー マップを作成したり、再利用のために、またはより複雑な照合のためにインスペクション クラス マップを作成したりできます。たとえば、正規表現または正規表現のグループ（正規表現クラスマップ）を使用して検査対象のパケット内のテキストを照合し、より限定された基準に基づいてアクションの対象を設定できます。たとえば、「example.com」というテキストが含まれた URL を持つすべての HTTP 要求をドロップできます。



「インスペクション ポリシー マップのアクションの定義」（P.2-4）および「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.2-6）を参照してください。

ステップ 3　「アクションの定義（レイヤ 3/4 ポリシー マップ）」（P.1-17）の説明に従って、レイヤ 3/4 ポリシー マップを作成して、各レイヤ 3/4 クラス マップで実行するアクションを定義します。



ステップ 4　「インターフェイス（サービス ポリシー）へのアクションの適用」（P.1-19）の説明に従って、ポリシー マップを適用するインターフェイスを決定するか、ポリシーマップをグローバルに適用します。

トラフィックの特定（レイヤ 3/4 クラス マップ）

レイヤ 3/4 クラス マップにより、アクションを適用するレイヤ 3 および 4 のトラフィックを特定します。1 つのレイヤ 3/4 ポリシー マップに複数のレイヤ 3/4 クラス マップを作成できます。

- 「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.1-14）
- 「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.1-16）

通過トラフィック用のレイヤ 3/4 クラス マップの作成

レイヤ 3/4 クラス マップでは、プロトコル、ポート、IP アドレス、およびレイヤ 3 またはレイヤ 4 の他の属性に基づいてトラフィックを照合します。

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 のパフォーマンスに影響が出る場合があります。

手順

ステップ 1　*class_map_name* が最大 40 文字の文字列であるレイヤ 3/4 クラス マップを作成します。

class-map *class_map_name*

「class-default」という名前は予約されています。すべてのタイプのクラス マップで同じ名前スペースが使用されるため、別のタイプのクラス マップですでに使用されている名前は再度使用できません。CLI はクラスマップ コンフィギュレーション モードに移行します。

例：

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

ステップ 2　（任意）説明をクラス マップに追加します。

description *string*

例：

```
hostname(config-cmap)# description All UDP traffic
```

ステップ 3　次のいずれかのコマンドを使用してトラフィックを照合します。特に指定がない場合、クラス マップに含めることができる **match** コマンドは 1 つだけです。

- **match any**：すべてのトラフィックを照合します。

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

- **match access-list** *access_list_name*：拡張アクセス リストで指定されているトラフィックを照合します。ASA がトランスペアレント ファイアウォール モードで動作している場合は、EtherType ACL を使用できます。

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

- **match port** {**tcp** | **udp**} {**eq** *port_num* | **range** *port_num port_num*}：1 つまたは連続する一定範囲の TCP または UDP ポートを照合します。複数の非連続ポートを使用するアプリケーションに対しては、**match access-list** コマンドを使用して、各ポートと一致する ACE を定義します。

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

- **match default-inspection-traffic**：ASA が検査可能なすべてのアプリケーションによって使用される、デフォルトの TCP および UDP ポートを照合します。

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

デフォルト グローバル ポリシーで使用されるこのコマンドは、ポリシー マップで使用されると、トラフィックの宛先ポートに基づいて各パケットに正しいインスペクションを適用する特別な CLI ショートカットです。たとえば、宛先がポート 69 の UDP トラフィックが ASA に到達すると、ASA は TFTP インスペクションを適用し、宛先がポート 21 の TCP トラフィックが到着すると、ASA は FTP インスペクションを適用します。そのため、この場合に限って同じクラス マップに複数のインスペクションを設定できます（他のインスペクションとともに設定可能な WAAS インスペクションを除きます。アクションの組み合わせの詳細については、「特定の機能アクションの非互換性」（P.1-7）を参照してください）。通常、ASA は、ポート番号を使用して適用するインスペクションを決定しないため、標準以外のポートなどにも柔軟にインスペクションを適用できます。

デフォルト ポートのリストについては、「デフォルト インスペクションと NAT に関する制限事項」（P.7-6）を参照してください。**match default-inspection-traffic** コマンドにポートが含まれているすべてのアプリケーションが、ポリシー マップでデフォルトでイネーブルになっているわけではありません。

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、一致するトラフィックを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とプロトコルが指定されるため、ACL のポートとプロトコルはすべて無視されます。

- **match dscp** *value1* [*value2*] [...] [*value8*]：IP ヘッダーの最大 8 つの DSCP 値を照合します。

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

- **match precedence** *value1* [*value2*] [*value3*] [*value4*]：IP ヘッダーの TOS バイトによって表される、最大 4 つの Precedence 値を照合します。*value1* ～ *value4* には、可能性のある Precedence に対応する 0 ～ 7 を指定できます。

```
hostname(config-cmap)# match precedence 1 4
```

- **match rtp** *starting_port range*：RTP トラフィックを照合します。*starting_port* には、2000 ～ 65534 の間の偶数の UDP 宛先ポートを指定します。*range* には、*starting_port* よりも上の追加 UDP ポートの数を 0 ～ 16383 で指定します。

```
hostname(config-cmap)# match rtp 4004 100
```

- **match tunnel-group** *name*：QoS を適用する VPN トンネル グループ トラフィックを照合します。

トラフィック照合を調整するために、**match** コマンドをもう 1 つ指定できます。上記のコマンドのいずれかを指定できますが、**match any**、**match access-list**、および **match default-inspection-traffic** コマンドは指定できません。または、**match flow ip destination-address** コマンドを入力して、各 IP アドレス宛てのトンネル グループのフローを照合することもできます。

```
hostname(config-cmap)# match tunnel-group group1
hostname(config-cmap)# match flow ip destination-address
```

例

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)# 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)# 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)# 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
```

管理トラフィック用のレイヤ 3/4 クラス マップの作成

ASA への管理トラフィックに対して、この種類のトラフィックに特有のアクションの実行が必要になる場合があります。管理クラス マップを指定して、ACL または TCP や UDP のポートと照合できます。ポリシー マップの管理クラス マップで設定可能なアクションのタイプは、管理トラフィック専用です。「サービス ポリシーで設定される機能」（P.1-4）を参照してください。

手順

ステップ 1　*class_map_name* が最大 40 文字の文字列である管理クラス マップを作成します。

class-map type management *class_map_name*

「class-default」という名前は予約されています。すべてのタイプのクラス マップで同じ名前スペースが使用されるため、別のタイプのクラス マップですでに使用されている名前は再度使用できません。CLI はクラスマップ コンフィギュレーション モードに移行します。

例：

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

ステップ 2　（任意）説明をクラス マップに追加します。

description *string*

例：

```
hostname(config-cmap)# description All UDP traffic
```

ステップ 3　次のいずれかのコマンドを使用してトラフィックを照合します。

- **match access-list** *access_list_name*：拡張アクセス リストで指定されているトラフィックを照合します。ASA がトランスペアレント ファイアウォール モードで動作している場合は、EtherType ACL を使用できます。

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

- **match port** {**tcp** | **udp**} {**eq** *port_num* | **range** *port_num port_num*}：1 つまたは連続する一定範囲の TCP または UDP ポートを照合します。複数の非連続ポートを使用するアプリケーションに対しては、**match access-list** コマンドを使用して、各ポートと一致する ACE を定義します。

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

アクションの定義（レイヤ 3/4 ポリシー マップ）

トラフィックを識別するレイヤ 3/4 クラス マップを設定したら、レイヤ 3/4 ポリシー マップを使用してそれらのクラスにアクションを関連付けます。

ヒント　ポリシー マップの最大数は 64 ですが、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。

手順

ステップ 1　ポリシー マップを追加します。

policy-map *policy_map_name*

policy_map_name 引数は、最大 40 文字のポリシー マップ名です。すべてのタイプのポリシー マップで同じ名前スペースが使用されるため、別のタイプのポリシー マップですでに使用されている名前は再度使用できません。CLI はポリシー マップ コンフィギュレーション モードに入ります。

例：

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

ステップ 2　設定済みのレイヤ 3/4 クラス マップを指定します。*class_map_name* は、クラス マップの名前です。

class *class_map_name*

クラス マップを追加するには、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

（注）　クラス マップに **match default-inspection-traffic** コマンドがない場合、そのクラスに最大 1 つの **inspect** コマンドを設定できます。

class *class_map_name*

例：

```
hostname(config-pmap)# description global policy map
```

ステップ 3　このクラス マップに、1 つ以上のアクションを指定します。

「サービス ポリシーで設定される機能」（P.1-4）を参照してください。

ステップ 4　このポリシー マップに含めるクラス マップごとに、この手順を繰り返します。

例

接続ポリシーの **policy-map** コマンドの例を次に示します。このコマンドは、Web サーバ 10.1.1.1 への接続許可数を制限します。

```
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
```

次の例は、ポリシー マップでの複数の照合の動作を示しています。

```
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 idle 0:10:0
```

次の例は、トラフィックが最初の利用可能なクラス マップと一致した場合に、同じ機能ドメインのアクションが指定されている後続のクラス マップと照合されないことを示しています。

```
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 idle 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 idle 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 idle 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

Telnet 接続は、開始時に **class telnet_traffic** と一致します。同様に FTP 接続は、開始時に **class ftp_traffic** と一致します。Telnet および FTP 以外の TCP 接続の場合は、**class tcp_traffic** と一致します。Telnet 接続または FTP 接続は **class tcp_traffic** と一致しますが、すでに他のクラスと一致しているため、ASA はこの照合を行いません。

インターフェイス（サービス ポリシー）へのアクションの適用

レイヤ 3/4 ポリシー マップをアクティブにするには、1 つ以上のインターフェイスに適用するサービス ポリシー、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。次のコマンドを使用します。

service-policy *policy_map_name* {**global** | **interface** *interface_name*} [**fail-close**]

それぞれの説明は次のとおりです。

- *policy_map_name* は、ポリシー マップの名前です。
- **global** は、特定のポリシーを持たないすべてのインターフェイスに適用するサービス ポリシーを作成します。

  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場合は、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します。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グローバル 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トラフィックにグローバルに適用されます。デフォルト サービス ポリシーには、**service-policy global_policy global** コマンドが含まれます。
- **interface** *interface_name* は、インターフェイスにポリシー マップを関連付けてサービス ポリシーを作成します。
- **fail-close** は、IPv6 トラフィックをサポートしないアプリケーション インスペクションによってドロップされた IPv6 トラフィックの syslog（767001）を生成します。デフォルトでは、syslog が生成されません。IPv6 をサポートするインスペクションのリストについては、「IPv6 のガイドライン」（P.1-9）を参照してください。

例

たとえば、次のコマンドは、外部インターフェイスで inbound_policy ポリシー マップをイネーブルにします。

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

次のコマンドは、デフォルト グローバル ポリシーをディセーブルにし、他のすべての ASA インターフェイスで新しいポリシー new_global_policy 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
```

サービス ポリシーのモニタ

サービス ポリシーをモニタするには、次のコマンドを入力します。

- **show service-policy**

  サービス ポリシーの統計情報を表示します。

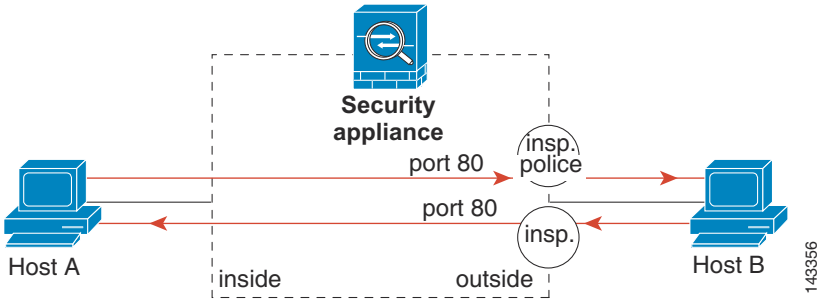
サービス ポリシー（モジュラ ポリシー フレームワーク）の例

このセクションでは、モジュラ ポリシー フレームワークの例をいくつか示します。

HTTP トラフィックへのインスペクションと QoS ポリシングの適用

この例では、外部インターフェイスを通過して ASA を出入りするすべての HTTP 接続（ポート 80 の TCP トラフィック）が HTTP インスペクション対象として分類されます。外部インターフェイスを出るすべての HTTP トラフィックがポリシング対象として分類されます。

図 1-1　HTTP インスペクションと QoS ポリシング



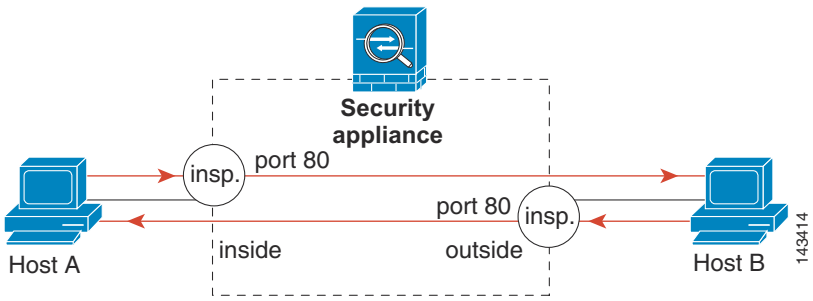
この例について、次のコマンドを参照してください。

```
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-pmap-c)# police output 250000
hostname(config)# service-policy http_traffic_policy interface outside
```

HTTP トラフィックへのインスペクションのグローバルな適用

この例では、任意のインターフェイスを通過して ASA に入るすべての HTTP 接続（ポート 80 の TCP トラフィック）が HTTP インスペクション対象として分類されます。このポリシーはグローバル ポリシーなので、インスペクションが発生するのは各インターフェイスにトラフィックが入ったときだけです。

図 1-2　　グローバル HTTP インスペクション



この例について、次のコマンドを参照してください。

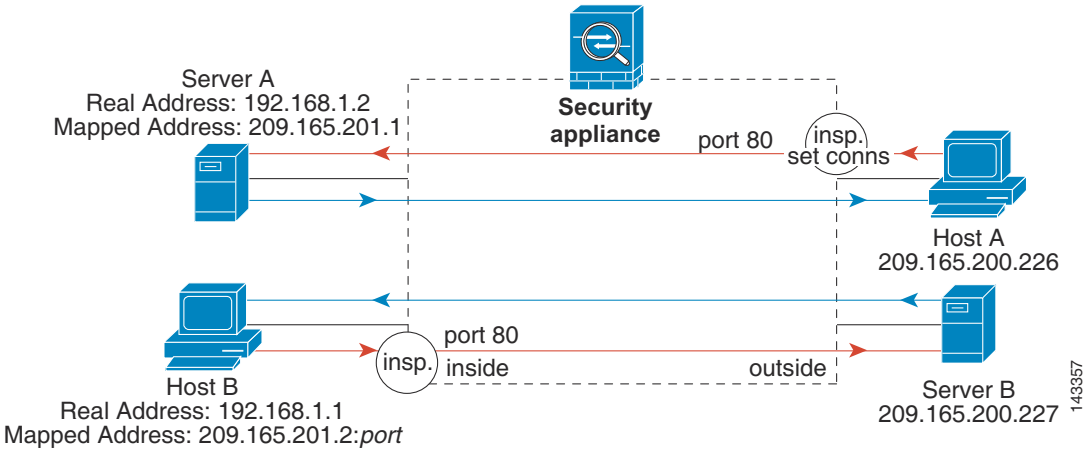
```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

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
```

特定のサーバへの HTTP トラフィックに対するインスペクションと接続制限値の適用

この例では、外部インターフェイスを通過して ASA に入るサーバ A 宛ての HTTP 接続（ポート 80 の TCP トラフィック）が HTTP インスペクションおよび最大接続数制限値の対象として分類されます。サーバ A から発信されたホスト A への接続は、クラスマップの ACL 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を通じて ASA に入るサーバ B 宛てのすべての HTTP 接続は、HTTP インスペクション対象として分類されます。サーバ B から発信されたホスト B への接続は、クラスマップの ACL と一致しないので、影響を受けません。

図 1-3　特定のサーバに対する HTTP インスペクションと接続制限値



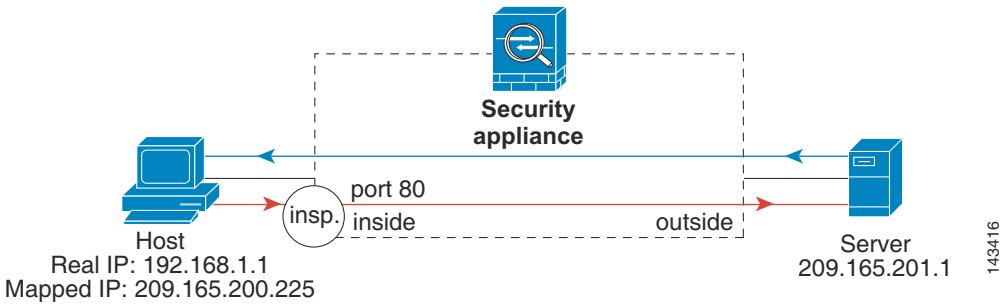
この例について、次のコマンドを参照してください。

```
hostname(config)# object network obj-192.168.1.2
hostname(config-network-object)# host 192.168.1.2
hostname(config-network-object)# nat (inside,outside) static 209.165.201.1
hostname(config)# object network obj-192.168.1.0
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 209.165.201.2
hostname(config)# access-list serverA extended permit tcp any host 209.165.201.1 eq 80
hostname(config)# access-list ServerB extended permit tcp any host 209.165.200.227 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
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

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

NAT による HTTP トラフィックへのインスペクションの適用

この例では、ネットワーク内のホストに 2 つのアドレスがあります。1 つは、実際の IP アドレスの 192.168.1.1 です。もう 1 つは、外部ネットワークで使用するマッピング IP アドレスの 209.165.200.225 です。クラス マップの ACL の実際の IP アドレスを使用する必要があります。outside インターフェイスに適用する場合にも、実際のアドレスを使用します。

図 1-4　NAT による HTTP インスペクション



この例について、次のコマンドを参照してください。

```
hostname(config)# object network obj-192.168.1.1
hostname(config-network-object)# host 192.168.1.1
hostname(config-network-object)# nat (VM1,outside) static 209.165.200.225

hostname(config)# access-list http_client extended permit tcp host 192.168.1.1 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
```

サービス ポリシーの履歴

機能名	リリース	説明
モジュラ ポリシー フレームワーク	7.0(1)	モジュラ ポリシー フレームワークが導入されました。
RADIUS アカウンティング トラフィックで使用する管理クラス マップ	7.2(1)	RADIUS アカウンティング トラフィックで使用する管理クラス マップが導入されました。**class-map type management** コマンドおよび **inspect radius-accounting** コマンドが導入されました。
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。
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。

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。レイヤ 3/4 ポリシー マップ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レイヤ 3/4 クラス マップ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.7-11）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。

- トラフィック照合コマンド：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コマンドを定義して、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コマンドでは、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コマンドが含まれます。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、異なる照合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（**policy-map type inspect http**）を変更する場合、変更を有効にするには、**inspect http** *map* 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、その削除し、サービス ポリシーに再度追加する必要があります。レイヤ 3/4 ポリシーから **inspect http http-map** コマンドを削除して再度追加する必要があります。

```
hostname(config)# policy-map test
hostname(config-pmap)# class http
hostname(config-pmap-c)# no inspect http http-map
hostname(config-pmap-c)# inspect http http-map
```

- 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、**inspect** *protocol map* コマンドを削除し、新しいマップを使用して再度追加します。次に例を示します。

```
hostname(config)# policy-map test
hostname(config-pmap)# class sip
hostname(config-pmap-c)# no inspect sip sip-map1
hostname(config-pmap-c)# inspect sip sip-map2
```

- ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。

  1 つのパケットが複数の異なる **match** コマンドまたは **class** コマンドと一致する場合、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。たとえば、次の match コマンドは任意の順序で入力できますが、**match request method get** コマンドが最初に照合されます。

```
match request header host length gt 100
  reset
match request method get
  log
```

  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 **match** コマンドまたは **class** コマンド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 **match** コマンドまたは **class** コマンドと照合される場合は、ポリシー マップ内での順序に従って照合されます。たとえば、ヘッダーの長さが 1001 のパケットの場合は、次に示す最初のコマンドと照合されてログに記録され、それから 2 番目のコマンドと照合されてリセットされます。2 つの **match** コマンドの順序を逆にすると、2 番目の **match** コマンドとの照合前にパケットのドロップと接続のリセットが行われ、ログには記録されません。

```
match request header length gt 100
  log
match request header length gt 1000
  reset
```

クラス マップは、そのクラス マップ内で重要度が最低の **match** コマンド（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 **match** コマンド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 **match** コマンドがある場合、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。各クラス マップの重要度が最低の照合が異なる場合、重要度が高い **match** コマンドを持つクラス マップが最初に照合されます。たとえば、次の 3 つのクラス マップには、**match request-cmd**（高プライオリティ）と **match filename**（低プライオリティ）という 2 つのタイプの **match** コマンドがあります。ftp3 クラス マップには両方のコマンドが含まれていますが、最低重要度のコマンドである **match filename** に従ってランク付けされています。ftp1 クラス マップには最高重要度のコマンドがあるため、ポリシー マップ内での順序に関係なく最初に照合されます。ftp3 クラス マップは ftp2 クラス マップと同じ重要度としてランク付けされており、**match filename** コマンドも含まれています。これらのクラス マップの場合、ポリシー マップ内での順序に従い、ftp3 が照合されてから ftp2 が照合されます。

```
class-map type inspect ftp match-all ftp1
  match request-cmd get
class-map type inspect ftp match-all ftp2
  match filename regex abc
class-map type inspect ftp match-all ftp3
  match request-cmd get
  match filename regex abc

policy-map type inspect ftp ftp
  class ftp3
    log
  class ftp2
    log
  class ftp1
    log
```

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、次のような 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っています。

- 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。

次のデフォルト コマンドを参照してください。

```
policy-map type inspect dns preset_dns_map
 parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
```

（注） デフォルトのインスペクション ポリシー マップは、**_default_esmtp_map** など、ほかにもあります。たとえば、**inspect esmtp** はポリシー マップ「_default_esmtp_map」を暗黙的に使用します。すべてのデフォルト ポリシー マップは、**show running-config all policy-map** コマンドを使用して表示できます。

インスペクション ポリシー マップのアクションの定義

レイヤ 3/4 ポリシー マップ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

	コマンド	目的
ステップ 1	（任意） インスペクション クラス マップを作成します。	「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.2-6）を参照してください。 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。
ステップ 2	（任意） 正規表現を作成します。	正規表現をサポートするポリシー マップ タイプについては、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。

	コマンド	目的
ステップ 3	**policy-map type inspect** *application policy_map_name* **例：** `hostname(config)# policy-map type inspect http http_policy`	インスペクション ポリシー マップを作成します。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.7-11）を参照してください。 *policy_map_name* 引数は、最大 40 文字のポリシー マップ名です。すべてのタイプのポリシー マップで同じ名前スペースが使用されるため、別のタイプのポリシー マップですでに使用されている名前は再度使用できません。CLI はポリシー マップ コンフィギュレーション モードに入ります。
ステップ 4	次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。	

	class *class_map_name*
	
	例：
	`hostname(config-pmap)# class http_traffic`
	`hostname(config-pmap-c)#`
		「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.2-6）で作成したインスペクション クラス マップを指定します。
		
		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。

	インスペクションの章でアプリケーションごとに説明されている **match** コマンドの 1 つを使用して、ポリシー マップで直接トラフィックを指定します。
	
	例：
	`hostname(config-pmap)# match req-resp content-type mismatch`
	`hostname(config-pmap-c)#`
		match not コマンドを使用すると、**match not** コマンドの基準に一致するすべてのトラフィックにアクションは適用されません。
		
		正規表現をサポートするポリシー マップ タイプについては、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 5	*action*
	
	例：
	`hostname(config-pmap-c)#`
	`drop-connection log`
		一致したトラフィックに対して実行するアクションを指定します。アクションは、インスペクションおよび一致タイプよって異なります。一般的なアクションは、**drop**、**log**、および **drop-connection** です。各一致で使用できるアクションについては、該当するインスペクションの章を参照してください。

ステップ 6	**parameters**
	
	例：
	`hostname(config-pmap)# parameters`
	`hostname(config-pmap-p)#`
		インスペクション エンジンに影響するパラメータを設定します。CLI はパラメータ コンフィギュレーション モードに移行します。各アプリケーションで設定可能なパラメータについては、該当するインスペクションの章を参照してください。

例

次の例では、HTTP インスペクション ポリシー マップとその関連クラス マップを示します。このポリシー マップは、サービス ポリシーがイネーブルにするレイヤ 3/4 ポリシー マップによってアクティブになります。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex url_example
hostname(config-cmap)# match regex url_example2

hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs

hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop-connection log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
hostname(config-pmap-c)# parameters
hostname(config-pmap-p)# protocol-violation action log

hostname(config-pmap-p)# policy-map test
hostname(config-pmap)# class test（レイヤ 3/4 クラス マップは表示されません）
hostname(config-pmap-c)# inspect http http-map1

hostname(config-pmap-c)# service-policy test interface outside
```

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。

制約事項

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。サポートされるアプリケーションのリストについては、**class-map type inspect** の CLI ヘルプを参照してください。

手順の詳細

	コマンド	目的
ステップ 1	（任意） 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 2	**class-map type inspect** *application* [**match-all** | **match-any**] *class_map_name*
	
	例：
	`hostname(config)# class-map type inspect http http_traffic`
	`hostname(config-cmap)#`
		インスペクション クラス マップを作成します。*application* は検査するアプリケーションです。サポートされるアプリケーションのリストについては、CLI ヘルプまたは第 7 章「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」を参照してください。
		
		class_map_name 引数は、最大 40 文字のクラス マップ名です。
		
		match-all キーワードはデフォルトです。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。
		
		match-any キーワードは、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。
		
		CLI がクラスマップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

ステップ 3	（任意） **description** *string* **例：** `hostname(config-cmap)# description All UDP traffic`	クラス マップに説明を追加します。
ステップ 4	アプリケーションで使用可能な 1 つ以上の **match** コマンドを入力して、クラスに含めるトラフィックを定義します。	クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。 各アプリケーションで使用可能な **match** コマンドについては、該当するインスペクションの章を参照してください。

例

次の例では、すべての基準に一致する必要がある HTTP クラス マップを作成します。

```
hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs
```

次の例では、基準のいずれかに一致する必要がある HTTP クラス マップを作成します。

```
hostname(config-cmap)# class-map type inspect http match-any monitor-http
hostname(config-cmap)# match request method get
hostname(config-cmap)# match request method put
hostname(config-cmap)# match request method post
```

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「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」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。
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。

アクセル ルール

この章では、アクセス ルールを使用して ASA へのネットワーク アクセスや ASA を通過するネットワーク アクセスを制御する方法について説明します。ルーテッド ファイアウォール モードの場合もトランスペアレント ファイアウォール モードの場合も、ネットワーク アクセスを制御するには、アクセス ルールを使用します。トランスペアレント モードでは、アクセス ルール（レイヤ 3 トラフィックの場合）と EtherType ルール（レイヤ 2 トラフィックの場合）の両方を使用できます。

（注） また、ASA インターフェイスに管理アクセスの目的でアクセスするには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。一般的な操作のコンフィギュレーション ガイドに従って管理アクセスを設定することだけが必要です。

ネットワーク アクセスの制御

アクセス ルールは、ASA の通過を許可するトラフィックを定義したものです。複数の異なるレイヤのルールを組み合わせてアクセス コントロール ポリシーを実装できます。

- インターフェイスに割り当てられる拡張アクセス ルール（レイヤ 3 以上のトラフィック）：着信方向と発信方向のそれぞれで異なるルール セット（ACL）を適用できます。拡張アクセス ルールでは、送信元と宛先のトラフィックの基準に基づいてトラフィックが許可または拒否されます。
- グローバルに割り当てられる拡張アクセス ルール：デフォルトのアクセス コントロールとして使用する単一のグローバル ルール セットを作成できます。グローバル ルールはインターフェイス ルールの後に適用されます。
- 管理アクセス ルール（レイヤ 3 以上のトラフィック）：インターフェイスに対するトラフィック（通常は管理トラフィック）を制御する単一のルール セットを適用できます。これらのルールは、CLI の「コントロール プレーン」アクセス グループに相当します。デバイスに対する ICMP トラフィックについては、代わりに ICMP ルールを設定できます。

- インターフェイスに割り当てられる EtherType ルール（レイヤ 2 のトラフィック）（トランスペアレント ファイアウォール モードのみ）：着信方向と発信方向のそれぞれで異なるルール セットを適用できます。EtherType ルールは、IP 以外のトラフィックのネットワーク アクセスを制御するルールです。EtherType ルールでは、EtherType に基づいてトラフィックが許可または拒否されます。

トランスペアレント ファイアウォール モードでは、拡張アクセス ルール、管理アクセス ルール、および EtherType ルールを組み合わせて同じインターフェイスに適用できます。

ルールに関する一般情報

この項では、アクセス ルールと EtherType ルールの両方について説明します。次の項目を取り上げます。

インターフェイス アクセス ルールとグローバル アクセス ルール

アクセス ルールを特定のインターフェイスに適用するか、またはアクセス ルールをすべてのインターフェイスにグローバルに適用できます。インターフェイス アクセス ルールと一緒にグローバル アクセス ルールを設定できます。この場合、特定の着信インターフェイス アクセス ルールが常に汎用のグローバル アクセス ルールよりも先に処理されます。グローバル アクセス ルールは、着信トラフィックにだけ適用されます。

着信ルールと発信ルール

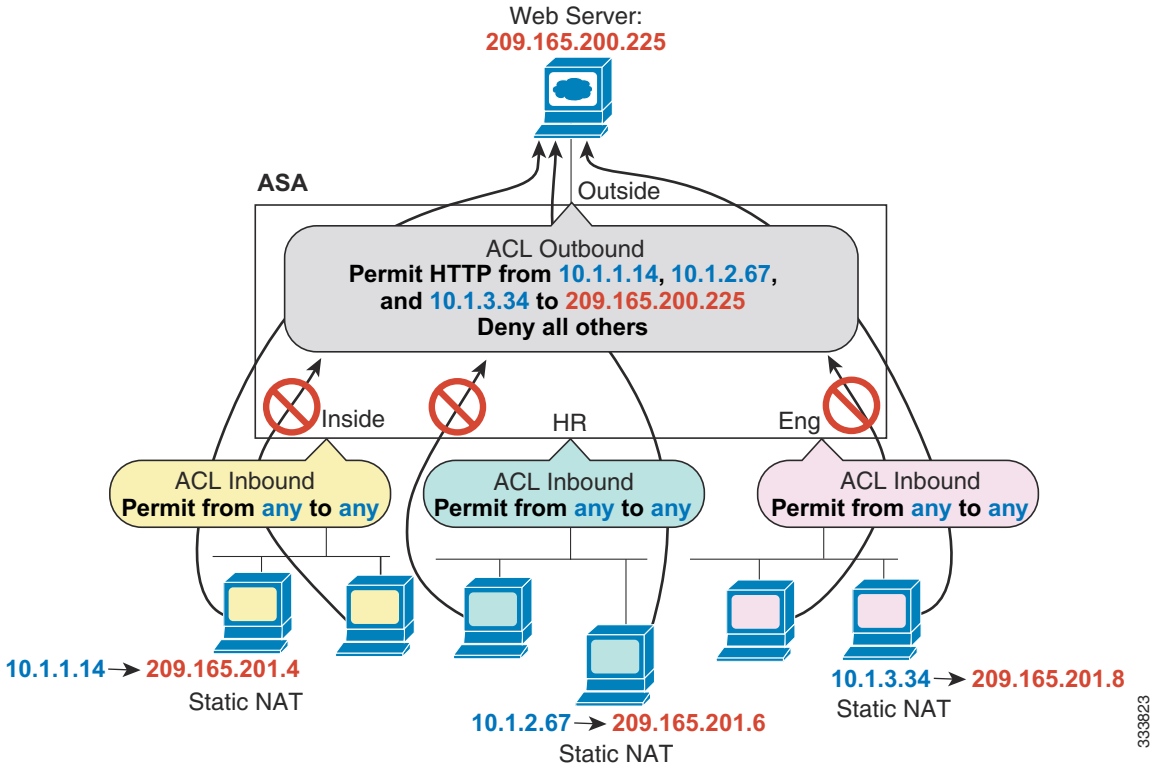
トラフィックの方向に基づいてアクセス ルールを設定できます。

- 着信：着信アクセス ルールは、インターフェイスに入ってくるトラフィックに適用されます。グローバル アクセス ルールおよび管理アクセス ルールは常に着信ルールになります。
- アウトバウンド：アウトバウンド ルールは、インターフェイスから送信されるトラフィックに適用されます。

（注）　「インバウンド」および「アウトバウンド」は、インターフェイスにおける ACL の適用対象を表したもので、前者は、インターフェイスにおいて ASA により受信されるトラフィックに ACL が適用されることを表し、後者はインターフェイスにおいて ASA から送信されるトラフィックに ACL が適用されることを表しています。これらの用語は、一般に着信と呼ばれる、セキュリティの低いインターフェイスから高いインターフェイスへのトラフィックの移動や、一般に発信と呼ばれる、セキュリティの高いインターフェイスから低いインターフェイスへのトラフィックの移動を意味しません。

たとえば、内部ネットワーク上の特定のホストに限って、外部ネットワーク上の Web サーバにアクセスできるようにする場合などには、アウトバウンド ACL が有用です。複数のインバウンド ACL を作成してアクセスを制限することもできますが、指定したホストだけアクセスを許可するアウトバウンド ACL を 1 つだけ作成する方が効率的です（次の図を参照）。このアウトバウンド ACL を使用すれば、その他のホストが外部ネットワークへアクセスすることもできなくなります。

図 3-1　Outbound ACL



この例について、次のコマンドを参照してください。

```
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.1.14
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.2.67
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.3.34
host 209.165.200.225 eq www
hostname(config)# access-group OUTSIDE out interface outside
```

ルールの順序

ルールの順序が重要です。ASA において、パケットを転送するかドロップするかの判断が行われる場合、ASA では、パケットと各ルールとの照合が、適用される ACL におけるそれらのルールの並び順に従って行われます。いずれかのルールに合致した場合、それ以降のルールはチェックされません。たとえば、先頭に作成したアクセス ルールが、インターフェイスに対してすべてのトラフィックを明示的に許可するものであれば、それ以降のルールはチェックされません。

暗黙的な許可

ルーテッド モードの場合、デフォルトでは次のタイプのトラフィックが許可されます。

- 高セキュリティ インターフェイスから低セキュリティ インターフェイスへの IPv4 および IPv6 のユニキャスト トラフィック。

トランスペアレント モードの場合、デフォルトでは次のタイプのトラフィックが許可されます。

- 高セキュリティ インターフェイスから低セキュリティ インターフェイスへの IPv4 および IPv6 のユニキャスト トラフィック。
- 双方向の ARP。ARP トラフィックの制御には ARP インスペクションを使用します。アクセス ルールでは制御できません。
- 双方向の BPDU。

他のトラフィックには、拡張アクセス ルール（IPv4 および IPv6）、または EtherType ルール（非 IP）のいずれかを使用する必要があります。

暗黙的な拒否

ACL の最後で暗黙的な拒否が設定されるため、明示的に許可しない限り、トラフィックは通過できません。たとえば、特定のアドレスを除くすべてのユーザに、ASA を通過してネットワークにアクセスすることを許可する場合、特定のアドレスを拒否したうえで、他のすべてのユーザを許可します。

EtherType ACL の場合、ACL の末尾にある暗黙的な拒否は、IP トラフィックや ARP には影響しません。たとえば、EtherType 8037 を許可する場合、ACL の末尾にある暗黙的な拒否によって、拡張 ACL で以前許可（または高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイスへ暗黙的に許可）した IP トラフィックがブロックされることはありません。ただし、EtherType ルールですべてのトラフィックを明示的に拒否した場合は、IP と ARP のトラフィックが拒否され、物理的なプロトコルのトラフィック（自動ネゴシエーションなど）だけが許可されます。

グローバル アクセス ルールを設定すると、暗黙的な拒否はグローバル ルールが処理された*後*になります。次の動作の順序を参照してください。

1. インターフェイス アクセス ルール。
2. グローバル アクセス ルール。
3. 暗黙的な拒否。

NAT とアクセス ルール

アクセス ルールは、NAT を設定している場合でも、アクセス ルールの一致を決定する際に常に実際の IP アドレスを使用します。たとえば、内部サーバ 10.1.1.5 用の NAT を設定して、パブリックにルーティング可能な外部の IP アドレス 209.165.201.5 をこのサーバに付与する場合は、この内部サーバへのアクセスを外部トラフィックに許可するアクセス ルールの中で、サーバのマッピング アドレス（209.165.201.5）ではなく実際のアドレス（10.1.1.5）を参照する必要があります。

拡張アクセス ルール

この項では、拡張アクセス ルールについて説明します。

リターン トラフィックに対する拡張アクセス ルール

ルーテッド モードとトランスペアレント モードの両方に対する TCP 接続および UDP 接続については、リターン トラフィックを許可するためのアクセス ルールは必要ありません。ASA は、確立された双方向接続のリターン トラフィックをすべて許可します。

ただし、ICMP などのコネクションレス型プロトコルについては、ASA は単方向セッションを確立します。したがって、（ACL を送信元インターフェイスと宛先インターフェイスに適用することで）アクセス ルールで双方向の ICMP を許可するか、ICMP インスペクション エンジンをイネーブルにする必要があります。ICMP インスペクション エンジンは、ICMP セッションを双方向接続として扱います。ping を制御するには、**echo-reply**（**0**）（ASA からホストへ）または **echo**（**8**）（ホストから ASA へ）を指定します。

アクセス ルールを使用したトランスペアレント ファイアウォールを介したブロードキャストとマルチキャスト トラフィックの許可

ルーテッド ファイアウォール モードでは、ブロードキャストとマルチキャスト トラフィックは、アクセス ルールで許可されている場合でもブロックされます。これには、サポートされていないダイナミック ルーティング プロトコルおよび DHCP（DHCP リレーを設定している場合を除く）が含まれます。トランスペアレント ファイアウォール モードでは、すべての IP トラフィックの通過を許可できます。

（注） これらの特殊なタイプのトラフィックはコネクションレス型であるため、アクセス ルールを両方のインターフェイスに適用して、リターン トラフィックの通過を許可する必要があります。

次の表に、トランスペアレント ファイアウォールの通過を許可できる一般的なトラフィック タイプを示します。

表 3-1　トランスペアレント ファイアウォールの特殊トラフィック

トラフィック タイプ	プロトコルまたはポート	注
DHCP	UDP ポート 67 および 68	DHCP サーバがイネーブルの場合、ASA は DHCP パケットの通過を拒否します。
EIGRP	プロトコル 88	—
OSPF	プロトコル 89	—
マルチキャスト ストリーム	UDP ポートは、アプリケーションによって異なります。	マルチキャスト ストリームは、常に Class D アドレス（224.0.0.0 to 239.x.x.x）に送信されます。
RIP（v1 または v2）	UDP ポート 520	—

管理アクセス ルール

ASA 宛ての管理トラフィックを制御するアクセス ルールを設定できます。to-the-box 管理トラフィック（**http**、**ssh**、**telnet** などのコマンドで定義）に対するアクセス コントロール ルールは、**control-plane** オプションを使用して適用される管理アクセス ルールよりも優先されます。したがって、このような許可された管理トラフィックは、to-the-box ACL で明示的に拒否されている場合でも着信が許可されます。

また、デバイスへの ICMP トラフィックは、ICMP ルールを使用して制御できます。デバイスを通過する ICMP トラフィックの制御には、通常の拡張アクセス ルールを使用します。

EtherType ルール

この項では、EtherType ルールについて説明します。

サポートされている EtherType およびその他のトラフィック

EtherType ルールは次を制御します。

- 一般的なタイプの IPX および MPLS ユニキャストまたはマルチキャストを含む、16 ビットの 16 進数値で示された EtherType。
- イーサネット V2 フレーム。
- デフォルトで許可される BPDU。BPDU は、SNAP でカプセル化されており、ASA は特別に BPDU を処理するように設計されています。
- トランク ポート（シスコ専用）BPDU。トランク BPDU のペイロードには VLAN 情報が含まれるので、BPDU を許可すると、ASA により、発信 VLAN を使用してペイロードが修正されます。
- Intermediate System to Intermediate System（IS-IS）。

次のタイプのトラフィックはサポートされていません。

- 802.3 形式フレーム：type フィールドではなく length フィールドが使用されるため、ルールでは処理されません。

リターン トラフィックに対する EtherType ルール

EtherType はコネクションレス型であるため、トラフィックを両方向に通過させる必要がある場合は、両方のインターフェイスにルールを適用する必要があります。

MPLS の許可

MPLS を許可する場合は、ラベル配布プロトコルおよびタグ配布プロトコルの TCP 接続が ASA を経由して確立されるようにしてください。これには、ASA インターフェイス上の IP アドレスを LDP セッションまたは TDP セッションの router-id として使用するように、ASA に接続されている両方の MPLS ルータを設定します（LDP および TDP を使用することにより、MPLS ルータは、転送するパケットに使用するラベル（アドレス）をネゴシエートできるようになります）。

Cisco IOS ルータで、使用プロトコル（LDP または TDP）に適したコマンドを入力します。*interface* は、ASA に接続されているインターフェイスです。

```
hostname(config)# mpls ldp router-id interface force
```

または

```
hostname(config)# tag-switching tdp router-id interface force
```

アクセス コントロールに関するガイドライン

IPv6 のガイドライン

IPv6 をサポートします。送信元アドレスと宛先アドレスには IPv4 アドレスと IPv6 アドレスの組み合わせを含めることができます。

Per-User ACL の注意事項

- ユーザごとの ACL では、**timeout uauth** コマンドの値が使用されますが、この値は AAA のユーザごとのセッション タイムアウト値で上書きできます。
- ユーザごとの ACL のためにトラフィックが拒否された場合、syslog メッセージ 109025 がログに記録されます。トラフィックが許可された場合、syslog メッセージは生成されません。ユーザごとの ACL の **log** オプションの効果はありません。

その他のガイドラインと制限事項

- オブジェクト グループ検索をイネーブルにすると、ルックアップのパフォーマンスは低下しますが、アクセス ルールの検索に必要なメモリを抑えることができます。オブジェクト グループ検索をイネーブルにした場合、ネットワーク オブジェクトは拡張されませんが、それらのグループの定義に基づいて一致するアクセス ルールが検索されます。このオプションを設定するには、**object-group-search access-control** コマンドを使用します。
- アクセス グループにトランザクション コミット モデルを使用することで、システムのパフォーマンスと信頼性を高めることができます。詳細については、一般的な操作のコンフィギュレーション ガイドの基本設定の章を参照してください。**asp rule-engine transactional-commit access-group** コマンドを使用します。
- ASDM では、ACL のルールの前にあるアクセス リストのコメントに基づいてルールの説明が設定されます。ASDM で新しいルールを作成した場合も、関連するルールの前にあるコメントが説明として設定されます。ただし、ASDM のパケット トレーサは、CLI の照合ルール後に設定されたコメントに一致します。

アクセス コントロールの設定

ここでは、アクセス コントロールを設定する方法について説明します。

アクセス グループの設定

アクセス グループを作成するには、まず、ACL を作成します。詳細については、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。

ACL をインターフェイスにバインドするかグローバルに適用するには、次のコマンドを使用します。

```
access-group access_list {
{in | out} interface interface_name [per-user-override | control-plane] |
global}
```

例：

```
hostname(config)# access-group outside_access in interface outside
```

インターフェイス固有のアクセス グループの場合は、次の手順を実行します。

- 拡張または EtherType ACL 名を指定します。ACL タイプ、インターフェイス、方向ごとに 1 つの **access-group** コマンドを設定し、1 つのコントロール プレーン ACL を設定できます。コントロール プレーン ACL は、拡張 ACL である必要があります。
- **in** キーワードは、着信トラフィックに ACL を適用します。**out** キーワードによって、ACL は発信トラフィックに適用されます。
- **interface** 名を指定します。
- **per-user-override** キーワードを使用すると（着信 ACL の場合に限る）、ユーザ許可用にダウンロードしたダイナミック ユーザ ACL により、インターフェイスに割り当てられている ACL を上書きできます。たとえば、インターフェイス ACL が 10.0.0.0 からのトラフィックをすべて拒否し、ダイナミック ACL が 10.0.0.0 からのトラフィックをすべて許可する場合、そのユーザに関しては、ダイナミック ACL によってインターフェイス ACL が上書きされます。

  デフォルトでは、VPN リモート アクセス トラフィックはインターフェイス ACL と照合されません。ただし、**no sysopt connection permit-vpn** コマンドを使用してこのバイパスをオフにした場合は、グループ ポリシーで **vpn-filter** が適用されているかどうか、および **per-user-override** オプションを設定しているかどうかによって動作が異なります。

  - **per-user-override** なし、**vpn-filter** なし：トラフィックはインターフェイス ACL と照合されます。
  - **per-user-override** なし、**vpn-filter**：トラフィックはまずインターフェイス ACL と照合され、次に VPN フィルタと照合されます。
  - **per-user-override**、**vpn-filter**：トラフィックは VPN フィルタのみと照合されます。
- ルールの対象が to-the-box トラフィックである場合、**control-plane** キーワードを指定します。

グローバル アクセス グループの場合は、**global** キーワードを指定して、すべてのインターフェイスの着信方向に拡張 ACL を適用します。

例

次の例は、**access-group** コマンドを使用する方法を示しています。

```
hostname(config)# access-list outside_access permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group outside_access interface outside
```

access-list コマンドでは、任意のホストからポート 80 を使用してホスト アドレスにアクセスできるようにしています。**access-group** コマンドでは、外部インターフェイスに入るトラフィックに **access-list** コマンドを適用するように指定しています。

ICMP アクセス ルールの設定

デフォルトでは、IPv4 または IPv6 を使用して任意の ASA インターフェイスに ICMP パケットを送信できます。ただし、次の例外があります。

- ASA は、ブロードキャスト アドレス宛ての ICMP エコー要求に応答しません。
- ASA は、トラフィックが着信するインターフェイス宛ての ICMP トラフィックにのみ応答します。ICMP トラフィックは、インターフェイス経由で離れたインターフェイスに送信できません。

デバイスを攻撃から保護するために、ICMP ルールを使用して、ASA インターフェイスへの ICMP アクセスを特定のホスト、ネットワーク、または ICMP タイプに限定できます。ICMP ルールにはアクセス ルールと同様に順序があり、パケットに最初に一致したルールの処理が適用されます。

インターフェイスに対して any ICMP ルールを設定すると、ICMP ルールのリストの最後に暗黙の deny ICMP ルールが追加され、デフォルトの動作が変更されます。そのため、一部のメッセージ タイプだけを拒否する場合は、残りのメッセージ タイプを許可するように ICMP ルールのリストの最後に permit any ルールを含める必要があります。

ICMP 到達不能メッセージ タイプ（タイプ 3）の権限を常に付与することを推奨します。ICMP 到達不能メッセージを拒否すると、ICMP パス MTU ディスカバリがディセーブルになって、IPSec および PPTP トラフィックが停止することがあります。また、IPv6 の ICMP パケットは、IPv6 のネイバー探索プロセスに使用されます。パス MTU ディスカバリの詳細については、RFC 1195 および RFC 1435 を参照してください。

手順

ステップ 1　ICMP トラフィックのルールを作成します。

```
icmp {permit | deny} {host ip_address | ip_address mask | any}
[icmp_type] interface_name
```

icmp_type を指定しない場合、すべてのタイプにルールが適用されます。番号または名前を入力できます。ping を制御するには、echo-reply（0）（ASA からホストへ）または echo（8）（ホストから ASA へ）を指定します。

すべてのアドレス（**any**）、単一のホスト（**host**）、またはネットワーク（*ip_address mask*）にルールを適用できます。

ステップ 2　ICMPv6（IPv6）トラフィックのルールを作成します。

ipv6 icmp {**permit** | **deny**} {**host** *ipv6_address* | *ipv6-network/prefix-length* | **any**} [*icmp_type*] *interface_name*

icmp_type を指定しない場合、すべてのタイプにルールが適用されます。

すべてのアドレス（**any**）、単一のホスト（**host**）、またはネットワーク（*ipv6-network/prefix-length*）にルールを適用できます。

ステップ 3　（任意）トレース ルートの出力に ASA が表示されるように、ICMP の到達不能メッセージに対するレート制限を設定します。

icmp unreachable rate-limit *rate* **burst-size** *size*

例

```
hostname(config)# icmp unreachable rate-limit 50 burst-size 1
```

レート制限は 1 ～ 100 の範囲で設定できます。デフォルトは 1 です。バースト サイズは動作には影響しませんが、1 ～ 10 の範囲で設定する必要があります。

ASA をホップの 1 つとして表示するトレース ルートに対して ASA の通過を許可するためには、**set connection decrement-ttl** コマンドをイネーブルにするほか、レート制限を大きくする必要があります。たとえば、次のポリシーでは、ASA を通過するすべてのトラフィックについて、Time-to-Live（TTL; 存続可能時間）の値を小さくしています。

```
class-map global-class
  match any
policy-map global_policy
  class global-class
  set connection decrement-ttl
```

例

次の例は、10.1.1.15 のホストを除くすべてのホストで内部インターフェイスへの ICMP の使用を許可する方法を示しています。

```
hostname(config)# icmp deny host 10.1.1.15 inside
hostname(config)# icmp permit any inside
```

次の例は、10.1.1.15 のアドレスを持つホストに内部インターフェイスへの ping だけを許可する方法を示しています。

```
hostname(config)# icmp permit host 10.1.1.15 inside
```

次に、外部インターフェイスですべての ping 要求を拒否し、すべての packet-too-big メッセージを許可する（パス MTU ディスカバリをサポートするため）方法を示します。

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

次の例は、ホスト 2000:0:0:4::2 またはプレフィックス 2001::/64 上のホストに対して外部インターフェイスへの ping を許可する方法を示しています。

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

アクセス ルールのモニタリング

ネットワーク アクセスをモニタするには、次のコマンドを入力します。

- **clear access-list** *id* **counters**

  アクセス リストのヒット数を消去します。

- **show access-list** [*name*]

  アクセス リストを表示します。ACE ごとに行が表示され、そのヒット数が表示されます。ACL 名を指定しないと、すべてのアクセス リストが表示されます。

- **show running-config access-group**

  インターフェイスにバインドされている現在の ACL を表示します。

アクセス ルールの syslog メッセージの評価

アクセス ルールに関するメッセージは、syslog イベントのビューア（ASDM のビューアなど）を使用して確認できます。

デフォルトのロギングを使用している場合、明示的に拒否されたフローに対する syslog メッセージ 106023 だけが表示されます。ルールのリストの最後にある「暗黙の deny」に一致するトラフィックは記録されません。

ASA が攻撃を受けた場合、拒否されたパケットを示す syslog メッセージの数が非常に大きくなることがあります。代わりに、syslog メッセージ 106100 を使用するロギングをイネーブルにすることをお勧めします。このメッセージは各ルール（許可ルールも含む）の統計情報を示すもので、これを使用することにより、生成される syslog メッセージの数を制限できます。また、特定のルールについて、すべてのロギングをディセーブルにする方法もあります。

メッセージ 106100 のロギングがイネーブルで、パケットが ACE と一致した場合、ASA はフロー エントリを作成して、指定された時間内で受信したパケットの数を追跡します。ASA は、最初のヒットがあったとき、および各間隔の終わりに syslog メッセージを生成し、その間隔におけるヒットの合計数と最後のヒットのタイムスタンプを示します。各間隔の終わりに、ASA はヒット数を 0 にリセットします。1 つの間隔内で ACE と一致するパケットがなかった場合、ASA はそのフロー エントリを削除します。ルールのロギングの設定では、それぞれのルールについて、ログ メッセージの間隔のほか、重大度も制御することができます。

フローは、送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびポートで定義されます。同じ 2 つのホスト間の新しい接続では、送信元ポートが異なる場合があるため、接続のための新しいフローが作成されると、同じフローの増加は示されない場合があります。

確立された接続に属する、許可されたパケットを ACL でチェックする必要はありません。最初のパケットだけがロギングされ、ヒット数に含められます。ICMP などのコネクションレス型プロトコルの場合は、許可されているパケットもすべてロギングされ、拒否されたパケットはすべてロギングされます。

これらのメッセージの詳細については、*syslog メッセージ ガイド*を参照してください。

ヒント　メッセージ 106100 のロギングがイネーブルで、パケットが ACE と一致した場合、ASA はフロー エントリを作成して、指定された時間内で受信したパケットの数を追跡します。ASA では、ACE 用のロギング フローを最大 32 K 保持できます。どの時点でも大量のフローが同時に存在する可能性があります。メモリおよび CPU リソースが無制限に消費されないようにするために、ASA は同時*拒否*フロー数に制限を設定します。この制限は、拒否フローに対してだけ設定されます（許可フローには設定されません）。これは、拒否フローは攻撃を示している可能性があるためです。制限に達すると、ASA は既存の拒否フローが期限切れになるまでロギング用の新しい拒否フローを作成せず、メッセージ 106101 を発行します。このメッセージの頻度は **access-list alert-interval** *secs* コマンドを使用して、拒否フローのキャッシュの最大数は **access-list deny-flow-max** *number* コマンドを使用して制御できます。

ネットワーク アクセスの許可または拒否の設定例

この項では、ネットワーク アクセスの許可または拒否の一般的な設定例を示します。

次の例は、内部サーバ 1 のネットワーク オブジェクトを追加し、サーバに対してスタティック NAT を実行し、内部サーバ 1 への外側からのアクセスをイネーブルにします。

```
hostname(config)# object network inside-server1
hostname(config)# host 10.1.1.1
hostname(config)# nat (inside,outside) static 209.165.201.12

hostname(config)# access-list outside_access extended permit tcp any object inside-server1
eq www
hostname(config)# access-group outside_access in interface outside
```

次の例では、すべてのホストに **inside** ネットワークと **hr** ネットワークの間での通信を許可しますが、外部ネットワークへのアクセスは特定のホストだけに許可されます。

```
hostname(config)# access-list ANY extended permit ip any any
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any

hostname(config)# access-group ANY in interface inside
hostname(config)# access-group ANY in interface hr
hostname(config)# access-group OUT out interface outside
```

たとえば、次のサンプル ACL では、内部インターフェイスで発信される一般的な EtherType が許可されます。

```
hostname(config)# access-list ETHER ethertype permit ipx
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

次の例では、ASA を通過する一部の EtherType が許可されますが、それ以外はすべて拒否されます。

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

次の例では、両方のインターフェイスで EtherType 0x1256 のトラフィックが拒否されますが、他のトラフィックはすべて許可されます。

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

次の例では、オブジェクト グループを使用して内部インターフェイスの特定のトラフィックを許可します。

```
!
hostname (config)# object-group service myaclog
hostname (config-service)# service-object tcp source range 2000 3000
hostname (config-service)# service-object tcp source range 3000 3010 destinatio$
hostname (config-service)# service-object ipsec
hostname (config-service)# service-object udp destination range 1002 1006
hostname (config-service)# service-object icmp echo

hostname(config)# access-list outsideacl extended permit object-group myaclog interface
inside any
```

アクセス ルールの履歴

機能名	プラットフォーム リリース	説明
インターフェイス アクセス ルール	7.0(1)	ACL を使用した、ASA 経由のネットワーク アクセスの制御。 **access-group** コマンドが導入されました。
グローバル アクセス ルール	8.3(1)	グローバル アクセス ルールが導入されました。 **access-group** コマンドが変更されました。
アイデンティティ ファイアウォールのサポート	8.4(2)	アイデンティティ ファイアウォールのユーザおよびグループを発信元と宛先に使用できるようになりました。アイデンティティ ファイアウォール ACL はアクセス ルールや AAA ルールとともに、および VPN 認証に使用できます。 **access-list extended** コマンドが変更されました。
EtherType ACL が IS-IS トラフィックをサポート	8.4(5)、9.1(2)	トランスペアレント ファイアウォール モードでは、ASA が EtherType ACL を使用して IS-IS トラフィックを渡すことができるようになりました。 **access-list ethertype {permit | deny} isis** コマンドが変更されました。
TrustSec のサポート	9.0(1)	TrustSec セキュリティ グループを送信元と宛先に使用できるようになりました。アイデンティティ ファイアウォール ACL をアクセス ルールとともに使用できます。 **access-list extended** コマンドが変更されました。

機能名	プラットフォーム リリース	説明
IPv4 および IPv6 の統合 ACL	9.0(1)	ACL で IPv4 および IPv6 アドレスがサポートされるようになりました。送信元および宛先に対して IPv4 および IPv6 アドレスの組み合わせも指定できます。**any** キーワードは、IPv4 および IPv6 トラフィックを表すように変更されました。IPv4 のみのトラフィックを表す **any4** キーワードと、IPv6 のみのトラフィックを表す **any6** キーワードが追加されました。IPv6 固有の ACL は非推奨です。既存の IPv6 ACL は拡張 ACL に移行されます。移行の詳細については、リリース ノートを参照してください。 **access-list extended**、**access-list webtype** の各コマンドが変更されました。 **ipv6 access-list**、**ipv6 access-list webtype**、**ipv6-vpn-filter** の各コマンドが削除されました。
ICMP コードによって ICMP トラフィックをフィルタリングするための拡張 ACL とオブジェクト機能拡張	9.0(1)	ICMP コードに基づいて ICMP トラフィックの許可または拒否ができるようになりました。 **access-list extended**、**service-object**、**service** の各コマンドが導入または変更されました。
アクセス グループ ルール エンジンのトランザクション コミット モデル	9.1(5)	イネーブルにすると、ルールのコンパイルの完了後に、ルールの照合パフォーマンスに影響を及ぼすことなくルールの更新が適用されます。 **asp rule-engine transactional-commit**、**show running-config asp rule-engine transactional-commit**、**clear configure asp rule-engine transactional-commit** の各コマンドが導入されました。

PART 2

ネットワーク アドレス変換

ネットワーク アドレス変換（NAT）

この章では、ネットワーク アドレス変換（NAT）が ASA でどのように機能するかについて説明します。

（注） NAT の設定を開始するには、第 5 章「ネットワーク オブジェクト NAT の設定」または第 6 章「Twice NAT」を参照してください。

NAT を使用する理由

IP ネットワーク内の各コンピュータおよびデバイスには、ホストを識別する固有の IP アドレスが割り当てられています。パブリック IPv4 アドレスが不足しているため、これらの IP アドレスの大部分はプライベートであり、プライベートの企業ネットワークの外部にルーティングできません。RFC 1918 では、アドバタイズされない、内部で使用できるプライベート IP アドレスが次のように定義されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

NAT の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。NAT は、プライベート IP アドレスをパブリック IP に置き換え、内部プライベート ネットワーク内のプライベート アドレスをパブリック インターネットで使用可能な正式の、ルーティング可能なアドレスに変換します。このようにして、NAT はパブリック アドレスを節約します。これは、ネットワーク全体に対して 1 つのパブリック アドレスだけを外部に最小限にアドバタイズするように NAT を設定できるからです。

NAT の他の機能には、次のおりです。

- セキュリティ：内部アドレスを隠蔽し、直接攻撃を防止します。
- IP ルーティング ソリューション：NAT を使用する際は、重複 IP アドレスが問題になりません。
- 柔軟性 : 外部で使用可能なパブリック アドレスに影響を与えずに、内部 IP アドレッシング スキームを変更できます。たとえば、インターネットにアクセス可能なサーバの場合、インターネット用に固定 IP アドレスを維持できますが、内部的にはサーバのアドレスを変更できます。
- IPv4 と IPv6（ルーテッド モードのみ）の間の変換：IPv4 ネットワークに IPv6 ネットワークを接続する場合は、NAT を使用すると、2 つのタイプのアドレス間で変換を行うことができます。

（注） NAT は必須ではありません。特定のトラフィック セットに NAT を設定しない場合、そのトラフィックは変換されませんが、セキュリティ ポリシーはすべて通常どおりに適用されます。

NAT の用語

このマニュアルでは、次の用語を使用しています。

- 実際のアドレス/ホスト/ネットワーク/インターフェイス：実際のアドレスとは、ホストで定義されている、変換前のアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、内部ネットワークが「実際の」ネットワークになります。内部ネットワークだけではなく、ASA に接続されている任意のネットワークを変換できます。したがって、外部アドレスを変換するように NAT を設定した場合、「実際の」は、外部ネットワークが内部ネットワークにアクセスしたときの外部ネットワークを指します。
- マッピング アドレス/ホスト/ネットワーク/インターフェイス：マッピング アドレスとは、実際のアドレスが変換されるアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、外部ネットワークが「マッピング」ネットワークになります。

（注） アドレスの変換中、ASA のインターフェイスに存在する IP アドレスは変換されません。

- 双方向の開始：スタティック NAT では、*双方向に*開始できます。つまり、ホストへの接続とホストからの接続の両方を開始できます。
- 送信元および宛先の NAT：任意のパケットについて、送信元 IP アドレスと宛先 IP アドレスの両方を NAT ルールと比較し、1 つまたは両方を変換する、または変換しないことができます。スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。

NAT タイプ

次のトピックで、さまざまなタイプの NAT について説明します。

NAT のタイプの概要

NAT は、次の方法を使用して実装できます。

- スタティック NAT：実際の IP アドレスとマッピング IP アドレスとの間での一貫したマッピング。双方向にトラフィックを開始できます。「スタティック NAT」（P.4-3）を参照してください。
- ダイナミック NAT：実際の IP アドレスのグループが、（通常は、より小さい）マッピング IP アドレスのグループに先着順でマッピングされます。実際のホストだけがトラフィックを開始できます。「ダイナミック NAT」（P.4-8）を参照してください。
- ダイナミック ポート アドレス変換（PAT）：実際の IP アドレスのグループが、1 つの IP アドレスにマッピングされます。この IP アドレスのポートが使用されます。「ダイナミック PAT」（P.4-10）を参照してください。
- アイデンティティ NAT：実際のアドレスが同一アドレスにスタティックに変換され、基本的に NAT をバイパスします。大規模なアドレスのグループを変換するものの、小さいアドレスのサブセットは免除する場合は、NAT をこの方法で設定できます。「アイデンティティ NAT」（P.4-12）を参照してください。

スタティック NAT

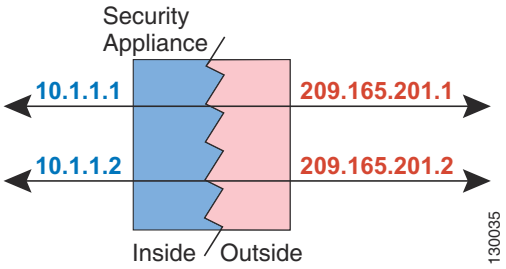
次のトピックでは、スタティック NAT について説明します。

スタティック NAT について

スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。マッピング アドレスは連続する各接続で同じなので、スタティック NAT では、双方向の接続（ホストへの接続とホストから接続の両方）を開始できます（接続を許可するアクセス ルールが存在する場合）。一方、ダイナミック NAT および PAT では、各ホストが以降の各変換に対して異なるアドレスまたはポートを使用するので、双方向の開始はサポートされません。

次の図に、一般的なスタティック NAT のシナリオを示します。この変換は常にアクティブなので、実際のホストとリモート ホストの両方が接続を開始できます。

図 4-1　スタティック NAT



（注）　必要に応じて、双方向をディセーブルにできます。

ポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT では、実際のプロトコルとマッピング プロトコル（TCP または UDP）およびポートを指定できます。

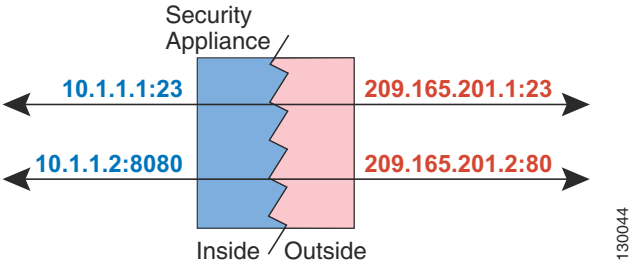
- 「ポート アドレス変換を設定したスタティック NAT について」（P.4-4）
- 「アイデンティティ ポート変換を設定したスタティック NAT」（P.4-5）
- 「標準以外のポートのポート変換を設定したスタティック NAT」（P.4-5）
- 「ポート変換を設定したスタティック インターフェイス NAT」（P.4-6）

ポート アドレス変換を設定したスタティック NAT について

スタティック NAT を使用してポートを指定する場合、ポートまたは IP アドレスを同じ値にマッピングするか、別の値にマッピングするかを選択できます。

次の図に、ポート変換が設定された一般的なスタティック NAT のシナリオを示します。自身にマッピングしたポートと、別の値にマッピングしたポートの両方を示しています。いずれのケースでも、IP アドレスは別の値にマッピングされています。この変換は常にアクティブなので、変換されたホストとリモート ホストの両方が接続を開始できます。

図 4-2　ポート変換を設定したスタティック NAT の一般的なシナリオ

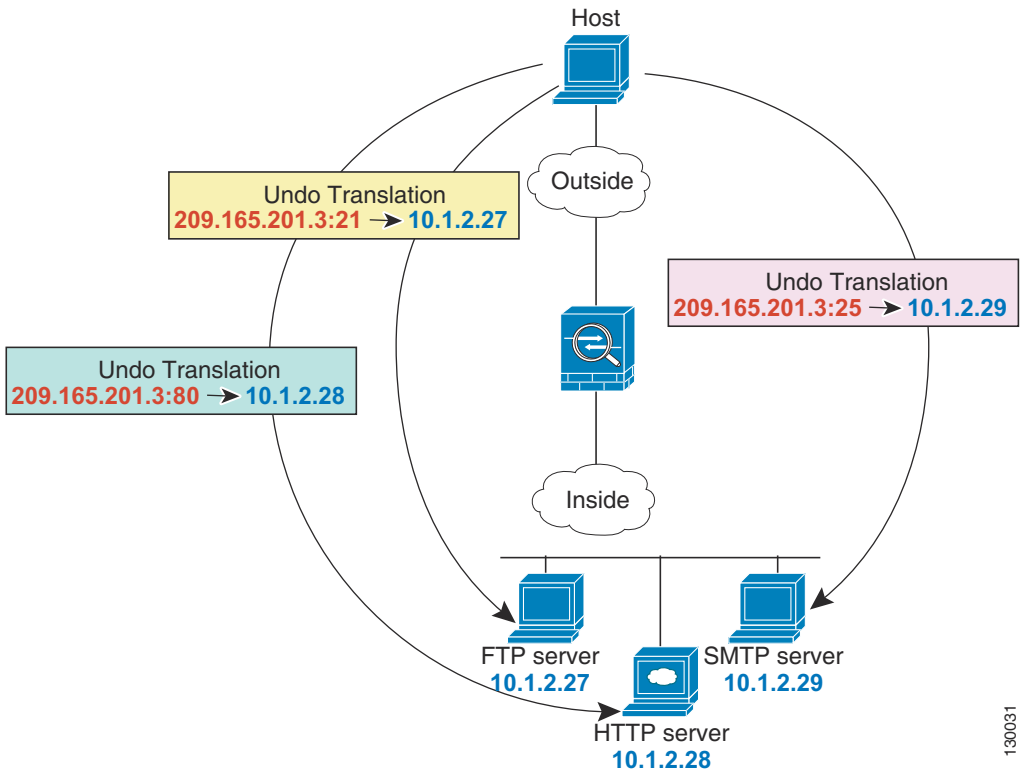


（注）　セカンダリ チャネルのアプリケーション インスペクションが必要なアプリケーション（FTP、VoIP など）を使用する場合は、ASA が自動的にセカンダリ ポートを変換します。

アイデンティティ ポート変換を設定したスタティック NAT

次のポート変換を設定したスタティック NAT の例では、リモート ユーザが FTP、HTTP、および SMTP にアクセスするための単一のアドレスを提供します。実際にはこれらのサーバは、実際のネットワーク上の異なるデバイスですが、各サーバに対して、異なるポートでも同じマッピング IP アドレスを使用するというポート変換ルールを設定したスタティック NAT を指定できます。この例の設定方法については、「FTP、HTTP、および SMTP のための単一アドレス（ポート変換を設定したスタティック NAT）」（P.5-24）を参照してください。

図 4-3　　ポート変換を設定したスタティック NAT



標準以外のポートのポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT を使用すると、予約済みポートから標準以外のポートへの変換や、その逆の変換も実行できます。たとえば、内部 Web サーバがポート 8080 を使用する場合、ポート 80 に接続することを外部ユーザに許可し、その後、変換を元のポート 8080 に戻すことができます。同様に、セキュリティをさらに高めるには、Web ユーザに標準以外のポート 6785 に接続するように指示し、その後、変換をポート 80 に戻すことができます。

ポート変換を設定したスタティック インターフェイス NAT

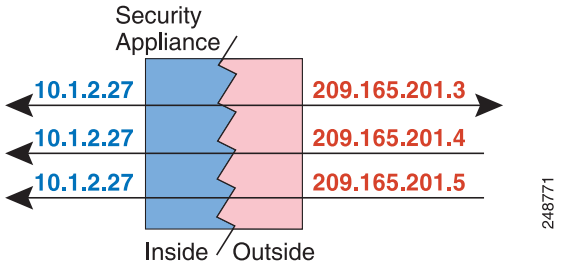
スタティック NAT は、実際のアドレスをインターフェイス アドレスとポートの組み合わせにマッピングするように設定できます。たとえば、ASA の outside インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を ASA のインターフェイス アドレス/ポート 23 にマッピングできます（ASA への Telnet では最低セキュリティのインターフェイスは許可されませんが、インターフェイス ポート変換が設定されたスタティック NAT は、その Telnet セッションを拒否するのではなく、リダイレクトします）。

1 対多のスタティック NAT

通常、スタティック NAT は 1 対 1 のマッピングで設定します。しかし場合によっては、1 つの実際のアドレスを複数のマッピング アドレスに設定することがあります（1 対多）。1 対多のスタティック NAT を設定する場合、実際のホストがトラフィックを開始すると、常に最初のマッピング アドレスが使用されます。しかし、ホストに向けて開始されたトラフィックの場合、任意のマッピング アドレスへのトラフィックを開始でき、1 つの実際のアドレスには変換されません。

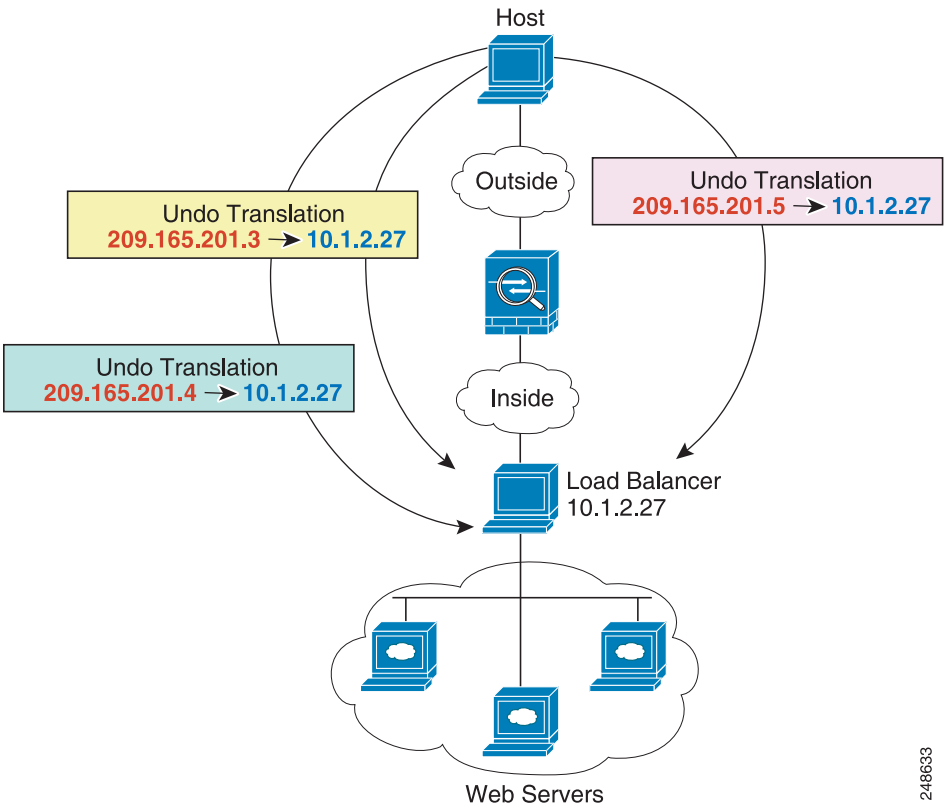
図 4-4 に、一般的な 1 対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピング アドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 4-4　　1 対多のスタティック NAT



たとえば、10.1.2.27 にロード バランサが存在するとします。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。この例の設定方法については、「複数のマッピング アドレス（スタティック NAT、1 対多）を持つ内部ロード バランサ」（P.5-22）を参照してください。

図 4-5　　1 対多のスタティック NAT の例



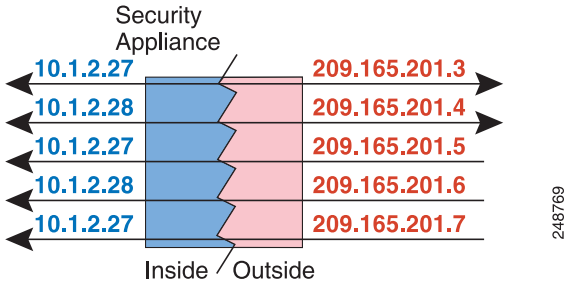
他のマッピング シナリオ（非推奨）

ASA には、1 対 1、1 対多だけではなく、少対多、多対少、多対 1 など任意の種類のスタティック マッピング シナリオを使用できるという柔軟性があります。1 対 1 マッピングまたは 1 対多マッピングだけを使用することをお勧めします。これらの他のマッピング オプションは、予期しない結果が発生する可能性があります。

機能的には、少対多は、1 対多と同じです。しかし、コンフィギュレーションが複雑化して、実際のマッピングが一目では明らかでない場合があるため、必要とする実際の各アドレスに対して 1 対多のコンフィギュレーションを作成することを推奨します。たとえば、少対多のシナリオでは、少数の実際のアドレスが多数のマッピング アドレスに順番にマッピングされます（A は 1、B は 2、C は 3）。すべての実際のアドレスがマッピングされたら、次にマッピングされるアドレスは、最初の実際のアドレスにマッピングされ、すべてのマッピング アドレスがマッピングされるまで続行されます（A は 4、B は 5、C は 6）。この結果、実際の各アドレスに対して複数のマッピング アドレスが存在することになります。1 対多のコンフィギュレーションのように、最初のマッピングだけが双方向であり、以降のマッピングでは、実際のホストへのトラフィックを開始できますが、実際のホストからのすべてのトラフィックは、送信元の最初のマッピング アドレスだけを使用できます。

次の図に、一般的な少対多のスタティック NAT シナリオを示します。

図 4-6　　少対多のスタティック NAT

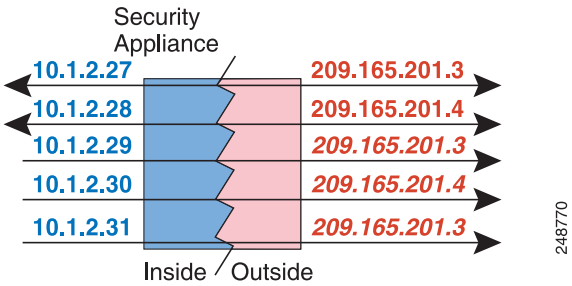


多対少または多対 1 コンフィギュレーションでは、マッピング アドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足するよりも前に、マッピング アドレスが不足します。双方向の開始を実現できるのは、最下位の実際の IP アドレスとマッピングされたプールの間でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターン トラフィックは、接続の固有の 5 つの要素（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。

（注）　多対少または多対 1 の NAT は PAT ではありません。2 つの実際のホストが同じ送信元ポート番号を使用して同じ外部サーバおよび同じ TCP 宛先ポートにアクセスする場合は、両方のホストが同じ IP アドレスに変換されると、アドレスの競合がある（5 つのタプルが一意でない）ため、両方の接続がリセットされます。

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 4-7　　多対少のスタティック NAT



このようにスタティック ルールを使用するのではなく、双方向の開始を必要とするトラフィックに 1 対 1 のルールを作成し、残りのアドレスにダイナミック ルールを作成することをお勧めします。

ダイナミック NAT

次のトピックでは、ダイナミック NAT について説明します。

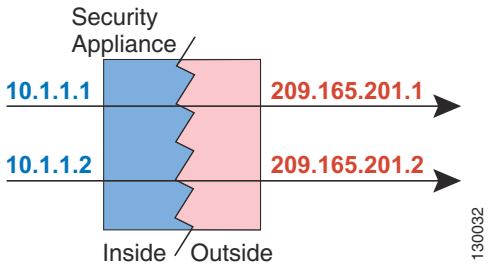
- 「ダイナミック NAT について」（P.4-9）
- 「ダイナミック NAT の欠点と利点」（P.4-10）

ダイナミック NAT について

ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピング アドレスのプールに変換されます。マッピングされたプールにあるアドレスは、通常、実際のグループより少なくなります。変換対象のホストが宛先ネットワークにアクセスすると、ASA は、マッピングされたプールから IP アドレスをそのホストに割り当てます。変換は、実際のホストが接続を開始したときにだけ作成されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセス ルールでその接続が許可されている場合でも、宛先ネットワークのユーザは、ダイナミック NAT を使用するホストへの確実な接続を開始できません。

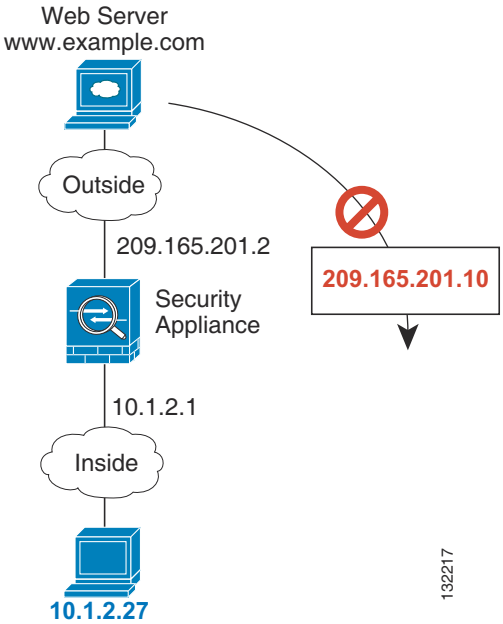
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

図 4-8　ダイナミック NAT



次の図に、マッピング アドレスへの接続開始を試みているリモート ホストを示します。このアドレスは、現時点では変換テーブルにないため、ASA はパケットをドロップしています。

図 4-9　マッピング アドレスへの接続開始を試みているリモート ホスト



（注）　変換が継続している間、アクセス ルールで許可されていれば、リモート ホストは変換済みホストへの接続を開始できます。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。

ダイナミック NAT の欠点と利点

ダイナミック NAT には、次の欠点があります。

- マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。

  PAT では、1 つのアドレスのポートを使用して 64,000 を超える変換を処理できるため、このイベントが頻繁に発生する場合は、PAT または PAT のフォールバック方式を使用します。
- マッピング プールではルーティング可能なアドレスを多数使用する必要があるのに、ルーティング可能なアドレスは多数用意できない場合があります。

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、PAT は次の場合は機能しません。

- GRE バージョン 0 などのように、オーバーロードするためのポートがない IP プロトコルでは機能しません。
- 一部のマルチメディア アプリケーションなどのように、1 つのポート上にデータ ストリームを持ち、別のポート上に制御パスを持ち、公開規格ではないアプリケーションでも機能しません。

NAT および PAT のサポートの詳細については、「デフォルト インスペクションと NAT に関する制限事項」（P.7-6）を参照してください。

ダイナミック PAT

次のトピックでは、ダイナミック PAT について説明します。

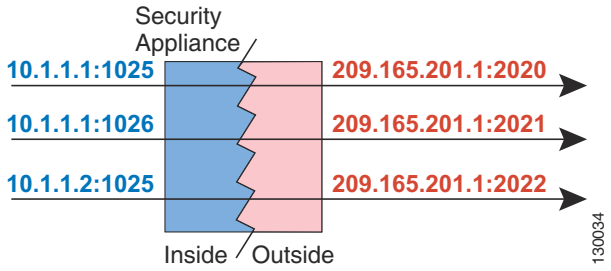
ダイナミック PAT について

ダイナミック PAT では、実際のアドレスおよび送信元ポートが 1 つのマッピング アドレスおよび固有のポートに変換されることによって、複数の実際のアドレスが 1 つのマッピング IP アドレスに変換されます。使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。下位ポート範囲を使用するトラフィックが数多くある場合は、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。

送信元ポートが接続ごとに異なるため、各接続には別の変換セッションが必要です。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

次の図に、一般的なダイナミック PAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。マッピング アドレスはどの変換でも同じですが、ポートがダイナミックに割り当てられます。

図 4-10　　ダイナミック PAT



接続の有効期限が切れると、ポート変換も有効期限切れになります。Multi-Session PAT では、デフォルトで 30 秒の PAT タイムアウトが使用されます。Per-Session PATの場合、xlate が即座に削除されます。宛先ネットワークのユーザは、PAT を使用するホストへの接続を確実には開始できません（アクセス ルールでその接続が許可されている場合も同じです）。

（注） 変換が継続している間、アクセス ルールで許可されていれば、リモート ホストは変換済みホストへの接続を開始できます。実際のポート アドレスおよびマッピング ポート アドレスはどちらも予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。

Per-Session PAT と Multi-Session PAT

Per-Session PAT によって PAT のスケーラビリティが向上し、クラスタリングの場合に各メンバ ユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、マスター ユニットに転送してマスター ユニットを所有者とする必要があります。Per-Session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンド ノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。

HTTP や HTTPS などの「ヒットエンドラン」トラフィックの場合、Per-Session PAT は、1 つのアドレスによってサポートされる接続率を大幅に増やすことができます。Per-Session PAT を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。Per-Session PAT を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/*平均ライフタイム*です。

デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-session PAT xlate を使用します。H.323、SIP、Skinny など、Multi-Session PAT による利点があるトラフィックの場合、Per-Session PAT 拒否ルールを作成して、Per-Session PAT をディセーブルにできます。「Per-Session PAT ルールの設定」（P.5-17）を参照してください。

ダイナミック PAT の欠点と利点

ダイナミック PAT では、1 つのマッピング アドレスを使用できるため、ルーティング可能なアドレスが節約されます。さらに、ASA インターフェイスの IP アドレスを PAT アドレスとして使用できます。

ダイナミック PAT は、制御パスとは異なるデータ ストリームを持つ一部のマルチメディア アプリケーションでは機能しません。NAT および PAT のサポートの詳細については、「デフォルト インスペクションと NAT に関する制限事項」（P.7-6）を参照してください。

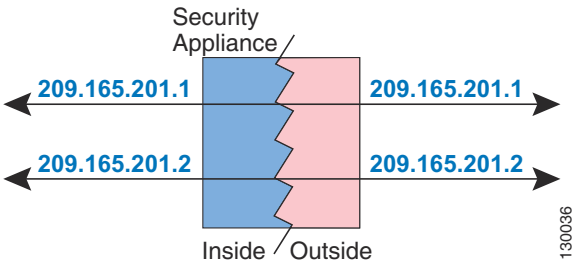
ダイナミック PAT によって、単一の IP アドレスから送信されたように見える数多くの接続が作成されることがあります。この場合、このトラフィックはサーバで DoS 攻撃として解釈される可能性があります。アドレスの PAT プールを設定し、PAT アドレスのラウンドロビン割り当てを使用すると、この状況を緩和できます。

アイデンティティ NAT

IP アドレスを自身に変換する必要のある NAT コンフィギュレーションを設定できます。たとえば、NAT を各ネットワークに適用するものの、1 つのネットワークを NAT から除外するという広範なルールを作成する場合、スタティック NAT ルールを作成して、アドレスを自身に変換することができます。アイデンティティ NAT は、NAT からクライアント トラフィックを除外する必要のある、リモート アクセス VPN で必要です。

次の図に、一般的なアイデンティティ NAT のシナリオを示します。

図 4-11　アイデンティティ NAT



ルーテッド モードとトランスペアレント モードの NAT

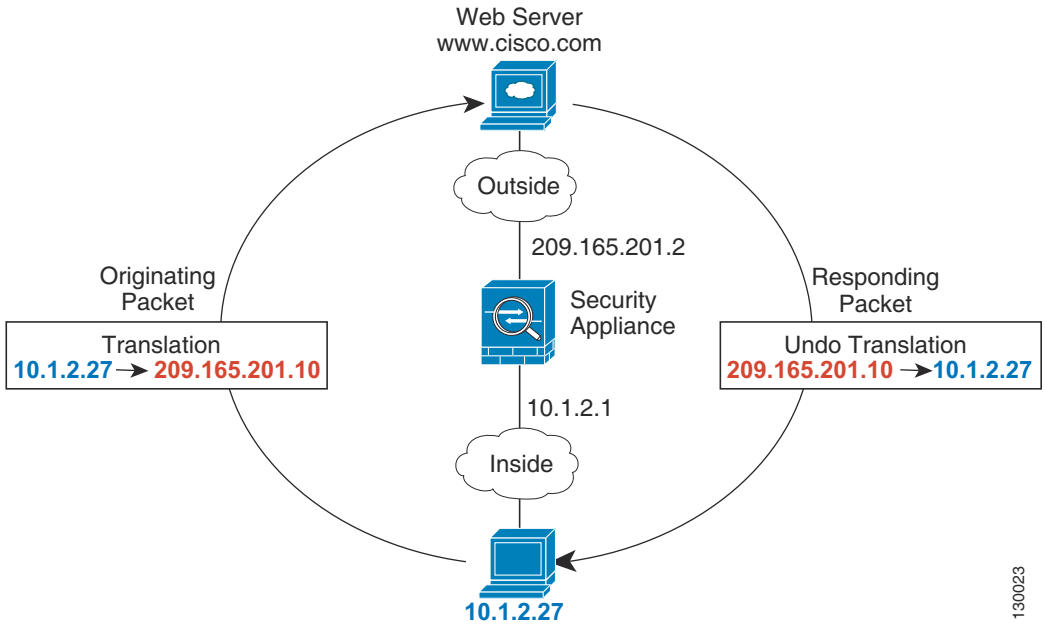
NAT は、ルーテッド モードおよびトランスペアレント ファイアウォール モードの両方に設定できます。この項では、各ファイアウォール モードの一般的な使用方法について説明します。

- 「ルーテッド モードの NAT」（P.4-13）
- 「トランスペアレント モードの NAT」（P.4-13）

ルーテッド モードの NAT

次の図は、内部にプライベート ネットワークを持つ、ルーテッド モードの一般的な NAT の例を示しています。

図 4-12　NAT の例：ルーテッド モード



1. 内部ホスト 10.1.2.27 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.2.27 はマッピング アドレス 209.165.201.10 に変更されます。
2. サーバが応答すると、マッピング アドレス 209.165.201.10 に応答を送信し、ASA がそのパケットを受信します。これは、ASA がプロキシ ARP を実行してパケットを要求するためです。
3. ASA はその後、パケットをホストに送信する前に、マッピング アドレス 209.165.201.10 を変換し、実際のアドレス 10.1.2.27 に戻します。

トランスペアレント モードの NAT

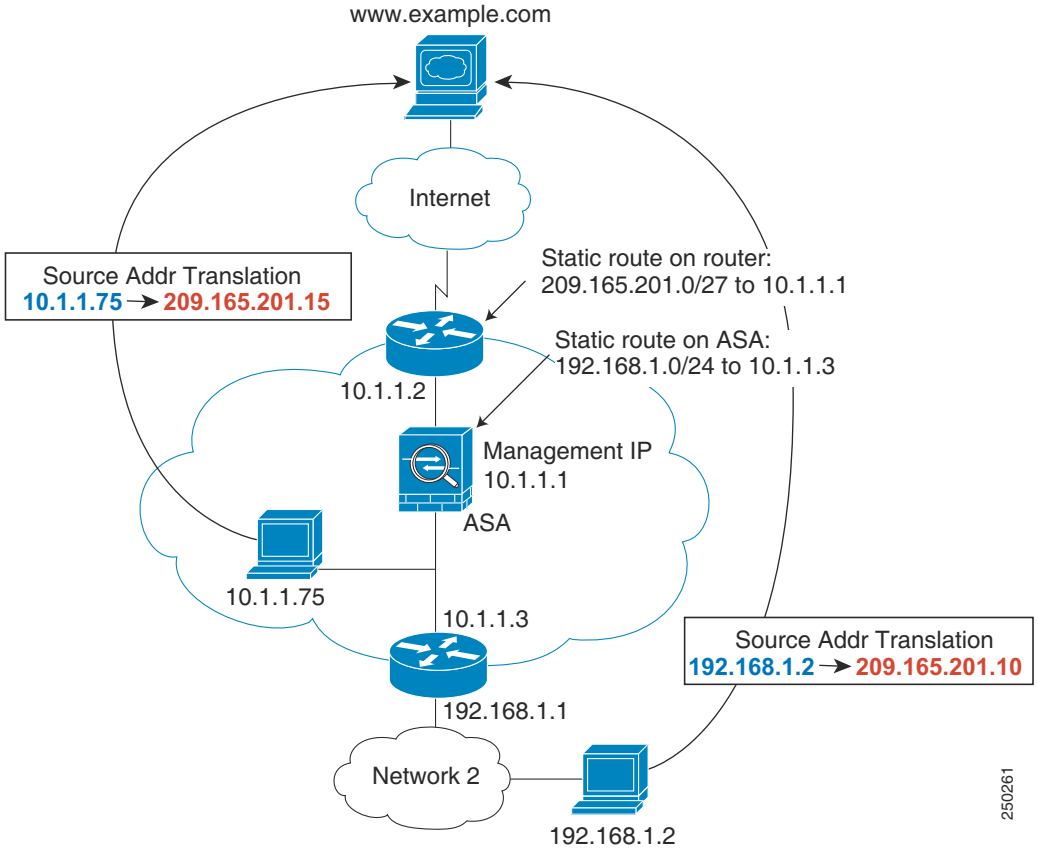
NAT をトランスペアレント モードで使用すると、ネットワークで NAT を実行するためのアップストリーム ルータまたはダウンストリーム ルータが必要なくなります。

トランスペアレント モードの NAT には、次の要件および制限があります。

- トランスペアレント ファイアウォールにはインターフェイス IP アドレスがないため、インターフェイス PAT を使用できません。
- ARP インスペクションはサポートされていません。また、何らかの理由で、一方の ASA のホストがもう一方の ASA のホストに ARP 要求を送信し、開始ホストの実際のアドレスが同じサブネットの別のアドレスにマッピングされる場合、実際のアドレスは ARP 要求で可視のままになります。
- IPv4 および IPv6 ネットワークの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。

次の図に、インターフェイス内部と外部に同じネットワークを持つ、トランスペアレント モードの一般的な NAT のシナリオを示します。このシナリオのトランスペアレント ファイアウォールは NAT サービスを実行しているため、アップストリーム ルータは NAT を実行する必要がありません。

図 4-13　NAT の例：トランスペアレント モード



1. 内部ホスト 10.1.1.75 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.1.75 はマッピング アドレス 209.165.201.15 に変更されます。
2. サーバが応答すると、マッピング アドレス 209.165.201.15 に応答を送信し、ASA がそのパケットを受信します。これは、アップストリーム ルータには、ASA の管理 IP アドレスに転送されるスタティック ルートのこのマッピング ネットワークが含まれるためです。必要なルートの詳細については、「マッピング アドレスとルーティング」（P.4-22）を参照してください。
3. その後、ASA はマッピング アドレス 209.165.201.15 を変換して実際のアドレス 10.1.1.1.75 に戻します。実際のアドレスは直接接続されているため、ASA はそのアドレスを直接ホストに送信します。
4. ホスト 192.168.1.2 の場合も、リターン トラフィックを除き、同じプロセスが発生します。ASA はルーティング テーブルでルートを検索し、192.168.1.0/24 の ASA スタティック ルートに基づいてパケットを 10.1.1.3 にあるダウンストリーム ルータに送信します。必要なルートの詳細については、「リモート ネットワークのトランスペアレント モード ルーティングの要件」（P.4-25）を参照してください。

NAT と IPv6

NAT を使用すると、IPv6 ネットワーク間、さらに IPv4 および IPv6 ネットワークの間で変換できます（ルーテッド モードのみ）。次のベスト プラクティスを推奨します。

- NAT66（IPv6-to-IPv6）：スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（Twice NAT のみ）。
- NAT46（IPv4-to-IPv6）：スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいので、容易にスタティック変換に対応できます。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（Twice NAT のみ）。IPv6 サブネットに変換する場合（/96 以下）、結果のマッピング アドレスはデフォルトで IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます（混合表記で表示）。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。また、任意で、ネット間のアドレスを変換できます。この場合、最初の IPv6 アドレスに最初の IPv4 アドレス、2 番目 IPv6 アドレスに 2 番目の IPv4 アドレス、のようにマッピングします。
- NAT64（IPv6-to-IPv4）：IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

特定の実装のガイドラインおよび制約事項については、設定の章を参照してください。

NAT の実装方法

ASA は、*ネットワーク オブジェクト NAT* および *Twice NAT* という 2 種類の方法でアドレス変換を実装できます。

- 「ネットワーク オブジェクトと Twice NAT の主な違い」（P.4-15）
- 「ネットワーク オブジェクト NAT」（P.4-16）
- 「Twice NAT」（P.4-17）

ネットワーク オブジェクトと Twice NAT の主な違い

これら 2 つの NAT タイプの主な違いは、次のとおりです。

- 実際のアドレスの定義方法
  - ネットワーク オブジェクト NAT：NAT をネットワーク オブジェクトのパラメータとして定義します。ネットワーク オブジェクトは、IP ホスト、範囲、またはサブネットの名前を指定するので、実際の IP アドレスではなく、NAT コンフィギュレーション内のオブジェクトを使用できます。ネットワーク オブジェクトの IP アドレスが実際のアドレスとして機能します。この方法では、ネットワーク オブジェクトがコンフィギュレーションの他の部分ですでに使用されていても、そのネットワーク オブジェクトに NAT を容易に追加できます。

  - Twice NAT：実際のアドレスとマッピング アドレスの両方のネットワーク オブジェクトまたはネットワーク オブジェクト グループを識別します。この場合、NAT はネットワーク オブジェクトのパラメータではありません。ネットワーク オブジェクトまたはグループが、NAT コンフィギュレーションのパラメータです。実際のアドレスのネットワーク オブジェクト *グループ*を使用できることは、Twice NAT がよりスケーラブルであることを意味します。

- 送信元および宛先 NAT の実装方法
  - ネットワーク オブジェクト NAT：各ルールは、パケットの送信元または宛先のいずれかに適用できます。つまり、送信元 IP アドレスに 1 つ、宛先 IP アドレスに 1 つと、2 つのルールが使用されることがあります。これらの 2 つのルールを相互に結び付けて、送信先と宛先の組み合わせに特定の変換を適用することはできません。
  - Twice NAT：1 つのルールが送信元と宛先の両方を変換します。一致するパケットは、1 つのルールだけに一致します。これ以外のルールはチェックされません。Twice NAT にオプションの宛先アドレスを設定しない場合でも、一致するパケットは、1 つの Twice NAT ルールだけに一致します。送信元および宛先は相互に結び付けられるので、送信元と宛先の組み合わせに応じて、異なる変換を適用できます。たとえば、sourceA/destinationA には、sourceA/destinationB とは異なる変換を設定できます。

- NAT ルールの順序
  - ネットワーク オブジェクト NAT：NAT テーブルで自動的に順序付けされます。
  - Twice NAT：NAT テーブルで、手動で順序付けします（ネットワーク オブジェクト NAT ルールの前または後）。

  詳細については、「NAT ルールの順序」（P.4-20）を参照してください。

Twice NAT の追加機能を必要としない場合は、ネットワーク オブジェクト NAT を使用することをお勧めします。ネットワーク オブジェクト NAT は設定が容易で、Voice over IP（VoIP）などの用途では、信頼性が高い場合があります（Twice NAT は 2 つのオブジェクト間だけに適用可能であるため、VoIP では、いずれのオブジェクトにも属さない間接アドレスの変換が失敗することがあります）。

ネットワーク オブジェクト NAT

ネットワーク オブジェクトのパラメータとして設定されているすべての NAT ルールは、*ネットワーク オブジェクト NAT ルール*と見なされます。ネットワーク オブジェクト NAT は、1 つの IP アドレス、アドレスの範囲、またはサブネットであるネットワーク オブジェクトの NAT を設定するための迅速かつ容易な方法です。

ネットワーク オブジェクトを設定すると、このオブジェクトのマッピング アドレスをインライン アドレスとして、または別のネットワーク オブジェクトやネットワーク オブジェクト グループのいずれかとして識別できるようになります。

パケットが ASA に入ると、送信元 IP アドレスと宛先 IP アドレスの両方がネットワーク オブジェクト NAT ルールと照合されます。個別の照合が行われる場合、パケット内の送信元 IP アドレスと宛先 IP アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはないので、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定することはできません。この種の機能には、Twice NAT を使用します（Twice NAT を使用すると、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます）。

ネットワーク オブジェクト NAT の設定を開始するには、第 5 章「ネットワーク オブジェクト NAT の設定」を参照してください。

Twice NAT

Twice NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定できます。

宛先アドレスはオプションです。宛先アドレスを指定する場合、宛先アドレスを自身にマッピングするか（アイデンティティ NAT）、別のアドレスにマッピングできます。宛先マッピングは、常にスタティック マッピングです。

Twice NAT では、ポート変換が設定されたスタティック NAT のサービス オブジェクトを使用できます。ネットワーク オブジェクト NAT は、インライン定義だけを受け入れます。

Twice NAT の設定を開始するには、第 6 章「Twice NAT」を参照してください。

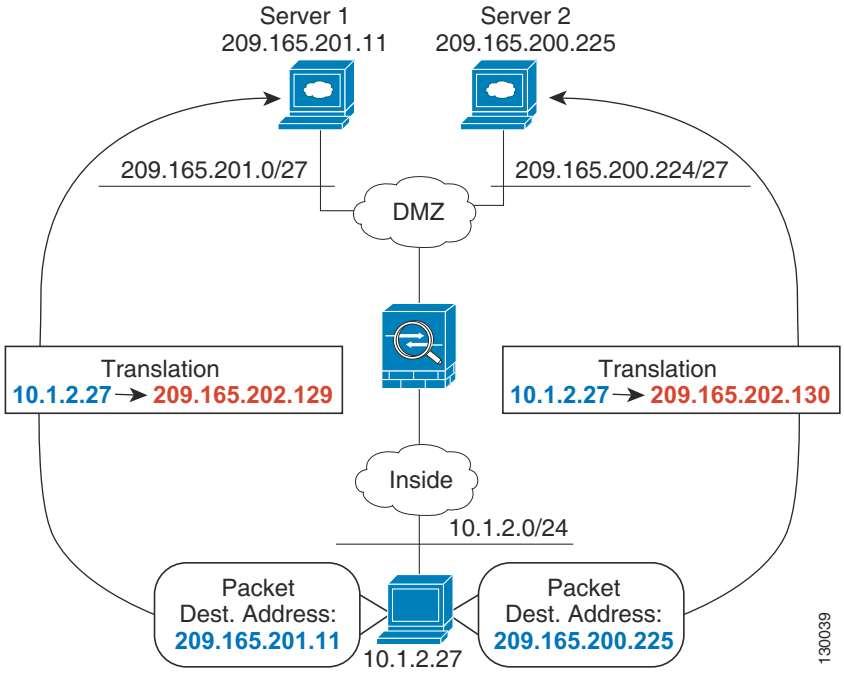
次のトピックで、Twice NAT の例を示します。

- 「例：異なる宛先アドレスを使用する Twice NAT」（P.4-17）
- 「例：異なる宛先ポートを使用する Twice NAT」（P.4-18）
- 「例：宛先アドレス変換が設定された Twice NAT」（P.4-19）

例：異なる宛先アドレスを使用する Twice NAT

次の図に、2 台の異なるサーバにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129 に変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130 に変換されます。この例の設定方法については、「FTP、HTTP、および SMTP のための単一アドレス（ポート変換を設定したスタティック NAT）」（P.5-24）を参照してください。

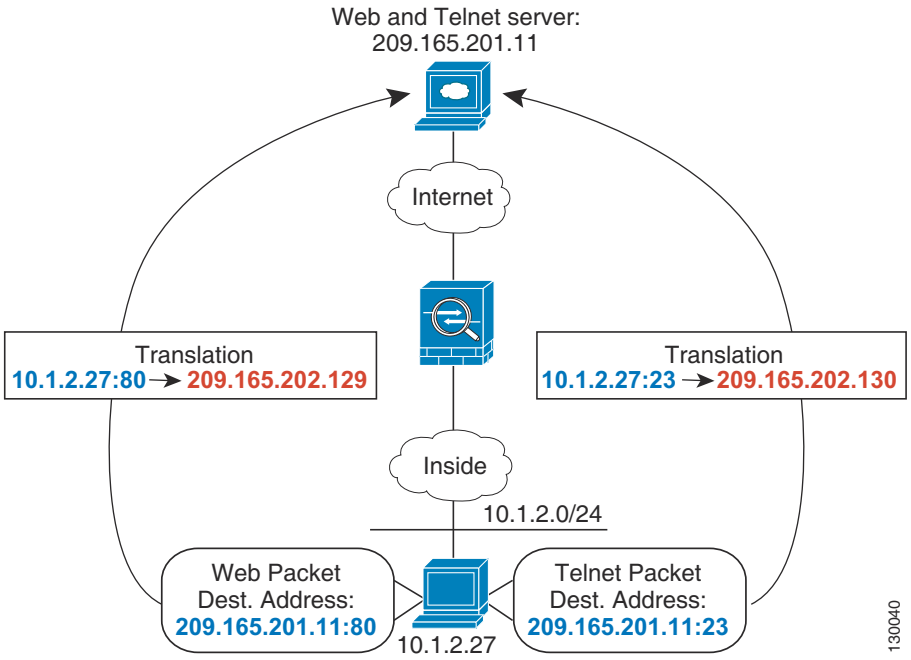
図 4-14　異なる宛先アドレスを使用する Twice NAT



例：異なる宛先ポートを使用する Twice NAT

次の図に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Web サービスを求めてサーバにアクセスすると、実際のアドレスは 209.165.202.129 に変換されます。ホストが Telnet サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130 に変換されます。

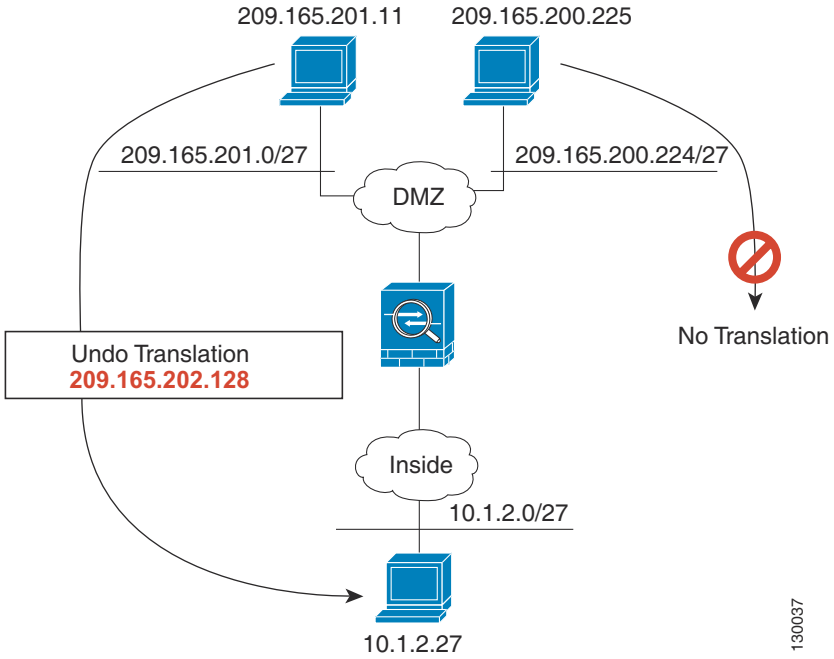
図 4-15　異なる宛先ポートを使用する Twice NAT



例：宛先アドレス変換が設定された Twice NAT

次の図に、マッピングされるホストに接続するリモート ホストを示します。マッピングされるホストには、209.165.201.0/27 ネットワークが起点または終点となるトラフィックに限り実際のアドレスを変換するスタティック Twice NAT 変換が設定されています。209.165.200.224/27 ネットワーク用の変換は存在しません。したがって、変換済みのホストはそのネットワークに接続できず、そのネットワークのホストも変換済みのホストに接続できません。

図 4-16　宛先アドレス変換が設定されたスタティック Twice NAT



NAT ルールの順序

ネットワーク オブジェクト NAT ルールおよび Twice NAT ルールは、3 セクションに分割される 1 つのテーブルに保存されます。最初にセクション 1 のルール、次にセクション 2、最後にセクション 3 というように、一致が見つかるまで順番に適用されます。たとえば、セクション 1 で一致が見つかった場合、セクション 2 とセクション 3 は評価されません。次の表に、各セクション内のルールの順序を示します。

表 4-1　NAT ルール テーブル

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 1	Twice NAT	コンフィギュレーションに登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、固有のルールを期待どおりに適用できない可能性があります。デフォルトでは、Twice NAT ルールはセクション 1 に追加されます。 **（注）** Easy VPN Remote を設定する場合、ASA はこのセクションの末尾に非表示の NAT ルールをダイナミックに追加します。非表示のルールではなく、VPN トラフィックに一致する Twice NAT ルールは、このセクションで設定しないでください。NAT エラーのために VPN が機能しない場合は、このセクションではなく、セクション 3 に NAT ルールを追加することを検討してください。
セクション 2	ネットワーク オブジェクト NAT	セクション 1 で一致が見つからない場合、ASA によって自動的に判断され、セクション 2 のルールが次の順序で適用されます。 1. スタティック ルール 2. ダイナミック ルール **各ルール タイプでは、次の順序ガイドラインが使用されます。** 1. 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。 2. 数量が同じ場合には、アドレス番号（低から高の順）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。 3. 同じ IP アドレスが使用される場合、ネットワーク オブジェクトの名前がアルファベット順で使用されます。たとえば、abracadabra は catwoman よりも先に評価されます。

表 4-1　NAT ルール テーブル（続き）

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 3	Twice NAT	まだ一致が見つからない場合、セクション 3 のルールがコンフィギュレーションに登場する順に、最初の一致ベースで適用されます。このセクションには、最も一般的なルールを含める必要があります。このセクションにおいても、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、一般的なルールが適用されます。Twice NAT ルールを追加するときには、このルールをセクション 3 に追加するかどうかを指定できます。

たとえばセクション 2 のルールでは、ネットワーク オブジェクト内に定義されている次の IP アドレスがあるとします。

192.168.1.0/24（スタティック）

192.168.1.0/24（ダイナミック）

10.1.1.0/24（スタティック）

192.168.1.1/32（ダイナミック）

172.16.1.0/24（ダイナミック）（オブジェクト def）

172.16.1.0/24（ダイナミック）（オブジェクト abc）

この結果、使用される順序は次のとおりです。

192.168.1.1/32（ダイナミック）

10.1.1.0/24（スタティック）

192.168.1.0/24（スタティック）

172.16.1.0/24（ダイナミック）（オブジェクト abc）

172.16.1.0/24（ダイナミック）（オブジェクト def）

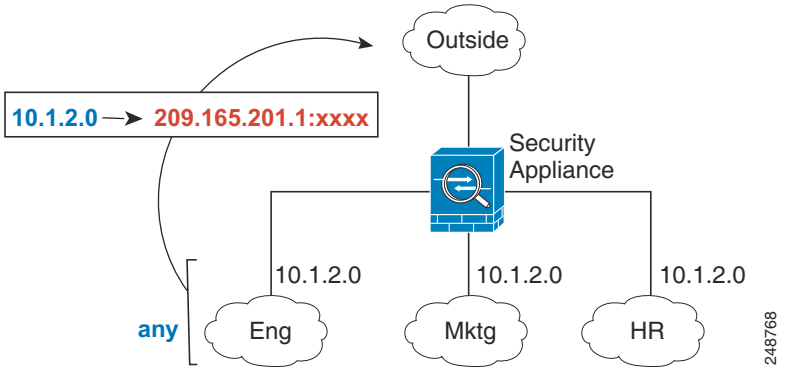
192.168.1.0/24（ダイナミック）

NAT インターフェイス

NAT ルールを設定して任意のインターフェイス（つまり、すべてのインターフェイス）に適用できます。または、特定の実際のインターフェイスおよびマッピング インターフェイスを識別できます。実際のアドレスには任意のインターフェイスを指定できます。マッピング インターフェイスには特定のインターフェイスを指定できます。または、その逆も可能です。

たとえば、複数のインターフェイスで同じプライベート アドレスを使用し、外部へのアクセス時にはすべてのインターフェイスを同じグローバル プールに変換する場合、実際のアドレスに任意のインターフェイスを指定し、マッピング アドレスには outside インターフェイスを指定します。

図 4-17　　任意のインターフェイスの指定



（注）　トランスペアレント モードの場合は、特定の送信元インターフェイスおよび宛先インターフェイスを選択する必要があります。

NAT パケットのルーティング

ASA は、マッピング アドレスに送信されたすべてのパケットの宛先となる必要があります。ASA は、マッピング アドレス宛てに送信されるすべての受信パケットの出力インターフェイスを決定する必要があります。この項では、ASA が NAT を使用してパケットの受信および送信を処理する方法について説明します。

- 「マッピング アドレスとルーティング」（P.4-22）
- 「リモート ネットワークのトランスペアレント モード ルーティングの要件」（P.4-25）
- 「出力インターフェイスの決定」（P.4-26）

マッピング アドレスとルーティング

実際のアドレスをマッピング アドレスに変換する場合は、選択したマッピング アドレスによって、マッピング アドレスのルーティング（必要な場合）を設定する方法が決定されます。

マッピング IP アドレスに関するその他のガイドラインについては、第 5 章「ネットワーク オブジェクト NAT の設定」および第 6 章「Twice NAT」を参照してください。

次のトピックでは、マッピング アドレスのタイプについて説明します。

- 「マッピング インターフェイスと同じネットワーク上のアドレス」（P.4-23）
- 「固有のネットワーク上のアドレス」（P.4-23）
- 「実際のアドレスと同じアドレス（アイデンティティ NAT）」（P.4-23）

マッピング インターフェイスと同じネットワーク上のアドレス

マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、ASA はプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することによって、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法では、ASA がその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。このソリューションは、外部ネットワークに十分な数のフリー アドレスが含まれている場合に最も適しており、ダイナミック NAT またはスタティック NAT などの 1:1 変換を使用している場合は考慮が必要です。ダイナミック PAT ではアドレス数が少なくても使用できる変換の数が大幅に拡張されるので、外部ネットワークで使用できるアドレスが少ししかない場合でも、この方法を使用できます。PAT では、マッピング インターフェイスの IP アドレスも使用できます。

（注）　マッピング インターフェイスを任意のインターフェイスとして設定し、マッピング インターフェイスの 1 つとして同じネットワーク上のマッピング アドレスを指定すると、そのマッピング アドレスの ARP 要求を*別の*インターフェイスで受信する場合、入力インターフェイスでそのネットワークの ARP エントリを手動で設定し、その MAC アドレスを指定する必要があります（**arp** コマンドを参照）。通常、マッピング インターフェイスに任意のインターフェイスを指定して、マッピング アドレスの固有のネットワークを使用すると、この状況は発生しません。

固有のネットワーク上のアドレス

マッピング インターフェイスで使用可能なアドレスより多くのアドレスが必要な場合は、別のサブネット上のアドレスを指定できます。アップストリーム ルータには、ASA を指しているマッピング アドレスのスタティック ルートが必要です。また、ルーテッド モードの場合、宛先ネットワーク上の IP アドレスをゲートウェイとして使用して、マッピング アドレスの ASA にスタティック ルートを設定し、ルーティング プロトコルを使用してルートを再配布することができます。たとえば、内部ネットワーク（10.1.1.0/24）に NAT を使用し、マッピング IP アドレス 209.165.201.5 を使用する場合、次のスタティック ルートを設定して再配布することができます。

```
route inside 209.165.201.5 255.255.255.255 10.1.1.99
```

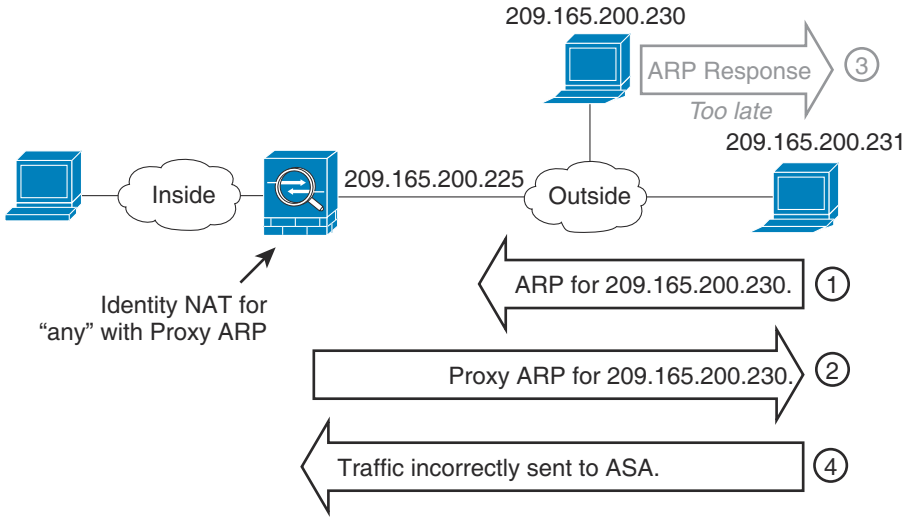
トランスペアレント モードの場合は、実際のホストが直接接続されてる場合は、ASA をポイントするようにアップストリーム ルータのスタティック ルートを設定します。ブリッジ グループの IP アドレスを指定します。トランスペアレント モードのリモート ホストの場合は、アップストリーム ルータのスタティック ルートで、代わりにダウンストリーム ルータの IP アドレスを指定できます。

実際のアドレスと同じアドレス（アイデンティティ NAT）

アイデンティティ NAT のデフォルト動作で、プロキシ ARP はイネーブルにされ、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP をディセーブルにできます。必要に応じて標準スタティック NAT のプロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの適切なルートがあることを確認する必要があります。

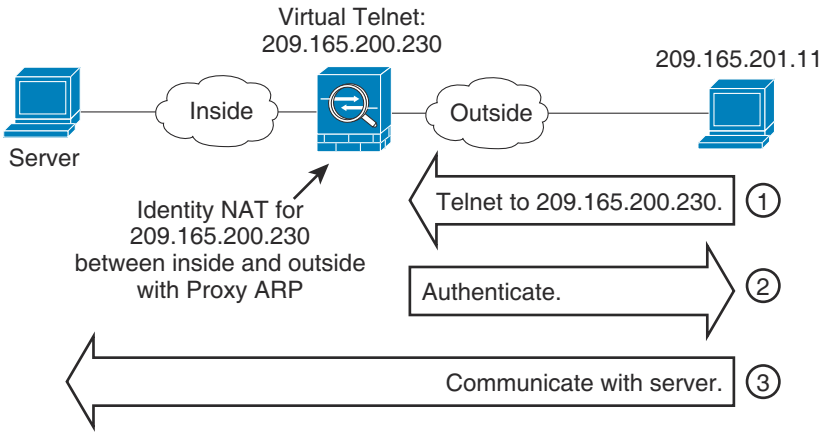
アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。たとえば、任意の IP アドレスの広範なアイデンティティ NAT ルールを設定した場合、プロキシ ARP をイネーブルのままにしておくと、マッピング インターフェイスに直接接続されたネットワーク上のホストの問題を引き起こすことがあります。この場合、マッピング ネットワークのホストが同じネットワークの他のホストと通信すると、ARP 要求内のアドレスは（任意のアドレスと一致する）NAT ルールと一致します。このとき、実際には ASA 向けのパケットでない場合でも、ASA はこのアドレスの ARP をプロキシします（この問題は、Twice NAT ルールが設定されている場合にも発生します。NAT ルールは送信元と宛先のアドレス両方に一致する必要がありますが、プロキシ ARP 判定は「送信元」アドレスに対してのみ行われます）。実際のホストの ARP 応答の前に ASA の ARP 応答を受信した場合、トラフィックは誤って ASA に送信されます（図 4-18 を参照）。

図 4-18　　アイデンティティ NAT に関するプロキシ ARP の問題



まれに、アイデンティティ NAT に対してプロキシ ARP が必要になります（仮想 Telnet など）。ネットワーク アクセスに AAA を使用する場合、ホストは他のトラフィックが通過する前に Telnet のようなサービスを使用して ASA で認証を受ける必要があります。ASA に仮想 Telnet サーバを設定すると、必要なログインを提供できます。仮想 Telnet アドレスに外部からアクセスする場合は、特にプロキシ ARP 機能用のアドレスのアイデンティティ NAT ルールを設定する必要があります。仮想 Telnet の内部プロセスにより、プロキシ ARP を使用すると ASA が NAT ルールに従って送信元インターフェイスからトラフィックを送信せず、トラフィックを仮想 Telnet アドレス宛のままにすることができます（図 4-19 を参照）。

図 4-19　　プロキシ ARP と仮想 Telnet



リモート ネットワークのトランスペアレント モード ルーティングの要件

トランスペアレント モードで NAT を使用する場合、一部のタイプのトラフィックには、スタティック ルートが必要になります。詳細については、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。

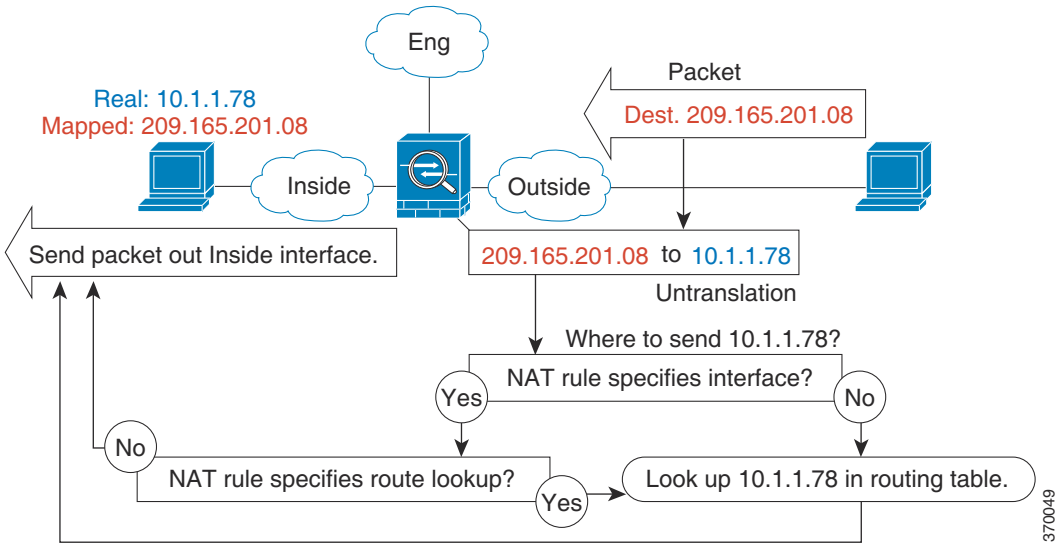
出力インターフェイスの決定

ASA がマッピング アドレスのトラフィックを受信する場合、ASA は NAT ルールに従って宛先アドレスを変換解除し、実際のアドレスにパケットを送信します。ASA は、次の方法でパケットの出力インターフェイスを決定します。

- トランスペアレント モード：ASA は NAT ルールを使用して実際のアドレスの出力インターフェイスを決定します。NAT ルールの一部として送信元インターフェイスと宛先インターフェイスを指定する必要があります。
- ルーテッド モード：ASA は、次のいずれかの方法で出力インターフェイスを決定します。
  - NAT ルールでインターフェイスを設定する：ASA は NAT ルールを使用して出力インターフェイスを決定します。ただし、代わりにオプションとして常にルート ルックアップを使用することもできます。一部のシナリオでは、ルート ルックアップの上書きが必要になる場合があります。たとえば、「NAT および VPN 管理アクセス」（P.4-31）を参照してください。
  - NAT ルールでインターフェイスを設定しない：ASA はルート ルックアップを使用して出力インターフェイスを決定します。

次の図に、ルーテッド モードでの出力インターフェイスの選択方法を示します。ほとんどの場合、ルート ルックアップは NAT ルールのインターフェイスと同じです。ただし、一部のコンフィギュレーションでは、2 つの方法が異なる場合があります。

図 4-20　ルーテッド モードでの出力インターフェイスの選択



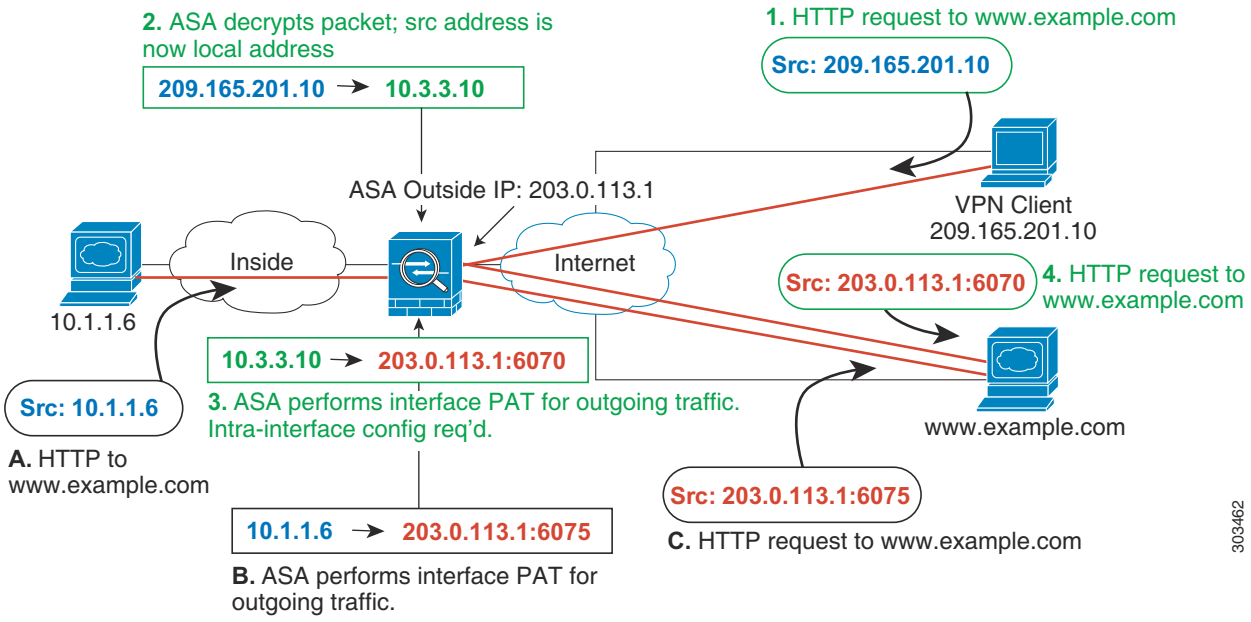
VPN の NAT

次のトピックでは、さまざまなタイプの VPN を用いた NAT の使用例について説明します。

NAT とリモート アクセス VPN

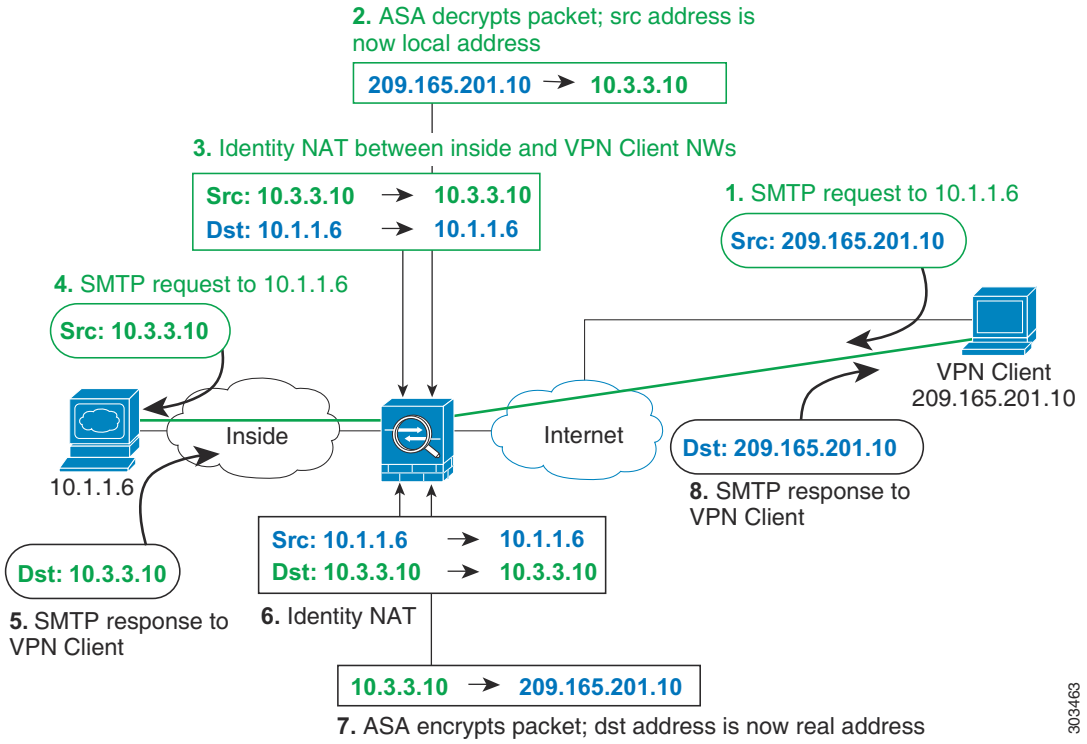
次の図に、内部サーバ（10.1.1.6）とインターネットにアクセスする VPN クライアント（209.165.201.10）の両方を示します。VPN クライアント用のスプリット トンネリング（指定したトラフィックのみが VPN トンネル上でやりとりされる）を設定しない限り、インターネット バインドされた VPN トラフィックも ASA を経由する必要があります。VPN トラフィックが ASA に渡されると、ASA はパケットを復号化し、得られたパケットには送信元として VPN クライアント ローカル アドレス（10.3.3.10）が含まれています。内部ネットワークと VPN クライアント ローカル ネットワークの両方で、インターネットにアクセスするために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。VPN トラフィックが、入ってきたインターフェイスと同じインターフェイスから出て行けるようにするには、インターフェイス内通信（別名「ヘアピン ネットワーキング」）をイネーブルにする必要があります。

図 4-21　インターネット宛 VPN トラフィックのインターフェイス PAT（インターフェイス内）



次の図に、内部のメール サーバにアクセスする VPN クライアントを示します。ASA は、内部ネットワークと外部ネットワークの間のトラフィックが、インターネット アクセス用に設定したインターフェイス PAT ルールに一致することを期待するので、VPN クライアント（10.3.3.10）から SMTP サーバ（10.1.1.6）へのトラフィックは、リバース パス障害が原因で廃棄されます。10.3.3.10 から 10.1.1.6 へのトラフィックは、NAT ルールに一致しませんが、10.1.1.6 から 10.3.3.10 へのリターン トラフィックは、送信トラフィックのインターフェイス PAT ルールに一致する*必要があります*。順方向および逆方向のフローが一致しないため、ASA は受信時にパケットをドロップします。この障害を回避するには、それらのネットワーク間のアイデンティティ NAT ルールを使用して、インターフェイス PAT ルールから VPN クライアント内部のトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスにアドレスを変換します。

図 4-22　　VPN クライアントのアイデンティティ NAT



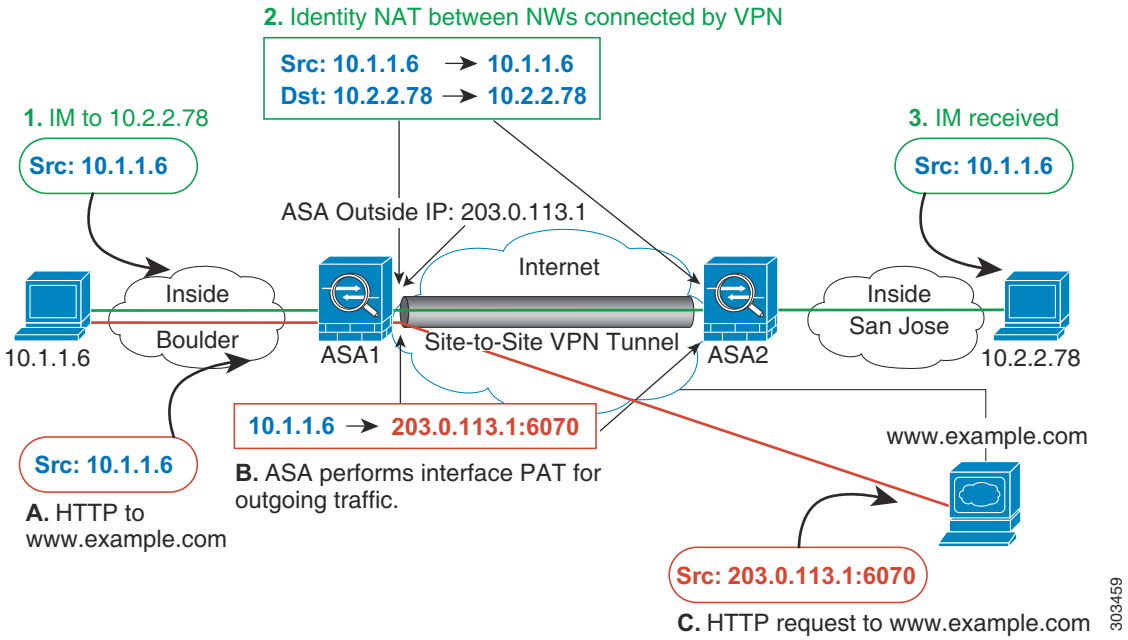
上記のネットワークのための次のサンプル NAT の設定を参照してください。

```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0
    nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
    subnet 10.1.1.0 255.255.255.0
    nat (inside,outside) dynamic interface

! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static inside_nw inside_nw destination static vpn_local
vpn_local
```

NAT およびサイトツーサイト VPN

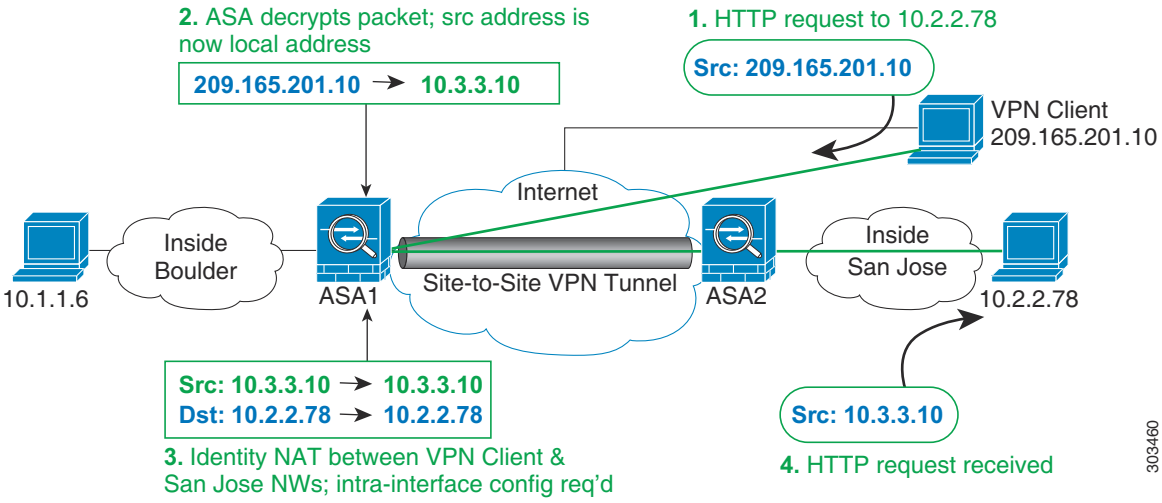
次の図に、ボールダーとサンノゼのオフィスを接続するサイトツーサイト トンネルを示します。インターネットに渡すトラフィックについて（たとえばボールダーの 10.1.1.6 から www.example.com へ）、インターネットへのアクセスのために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。ただし、VPN トンネルを経由するトラフィックについては（たとえば、ボールダーの 10.1.1.6 からサンノゼの 10.2.2.78 へ）、NAT を実行しません。そのため、アイデンティティ NAT ルールを作成して、そのトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスにアドレスを変換します。

図 4-23　サイトツーサイト VPN のためのインターフェイス PAT およびアイデンティティ NAT



次の図に、ASA1（ボールダー）に接続する VPN クライアントと、ASA1 と ASA2（サンノゼ）間のサイトツーサイト トンネル上でアクセス可能なサーバ（10.2.2.78）に対する Telnet 要求を示します。これはヘアピン接続であるため、VPN クライアントからの非スプリット トンネルのインターネット宛トラフィックにも必要な、インターフェイス内通信をイネーブルにする必要があります。発信 NAT ルールからこのトラフィックを除外するため、VPN に接続された各ネットワーク間で行うのと同様に、VPN クライアントとボールダーおよびサンノゼのネットワーク間でアイデンティティ NAT を設定する必要もあります。

図 4-24　サイト ツーサイト VPN への VPN クライアント アクセス



ASA1（ボールダー）については、次の NAT の設定例を参照してください。

```
! Enable hairpin for VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0
    nat (outside,outside) dynamic interface

! Identify inside Boulder network, & perform object interface PAT when going to Internet:
object network boulder_inside
    subnet 10.1.1.0 255.255.255.0
    nat (inside,outside) dynamic interface

! Identify inside San Jose network for use in twice NAT rule:
object network sanjose_inside
    subnet 10.2.2.0 255.255.255.0

! Use twice NAT to pass traffic between the Boulder network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside destination static
vpn_local vpn_local

! Use twice NAT to pass traffic between the Boulder network and San Jose without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside destination static
sanjose_inside sanjose_inside

! Use twice NAT to pass traffic between the VPN client and San Jose without
! address translation (identity NAT):
nat (outside,outside) source static vpn_local vpn_local destination static sanjose_inside
sanjose_inside
```

ASA2（サンノゼ）については、次の NAT の設定例を参照してください。

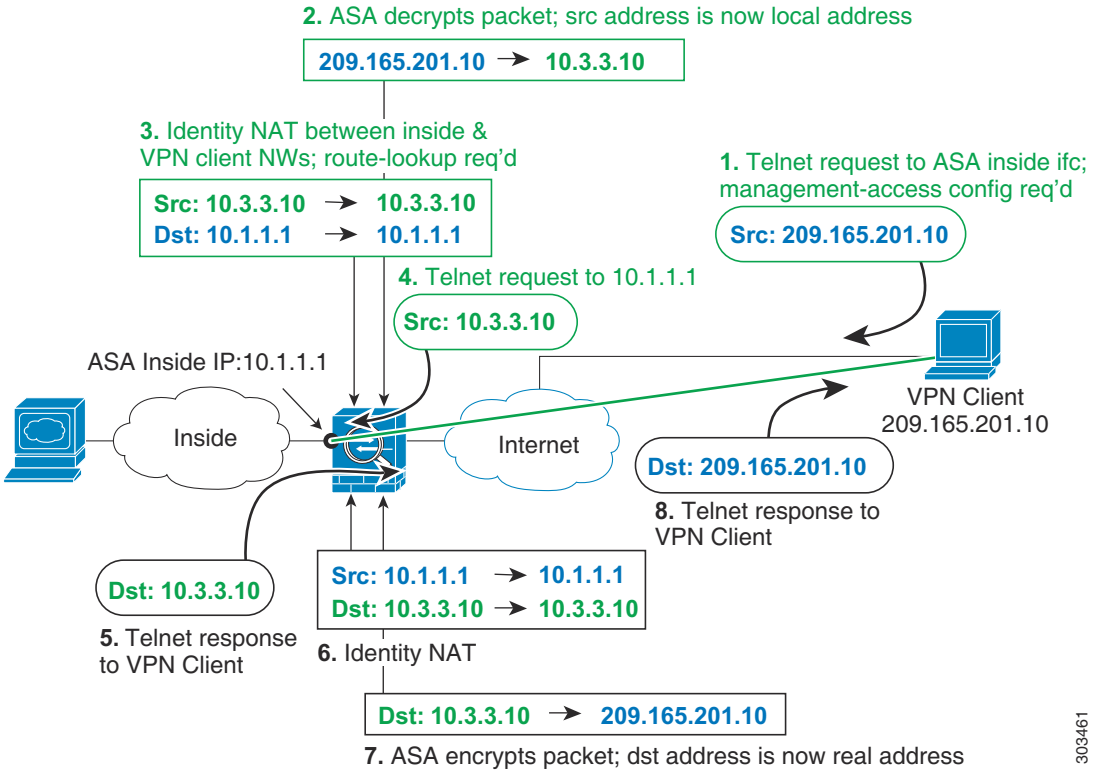
```
! Identify inside San Jose network, & perform object interface PAT when going to Internet:
object network sanjose_inside
    subnet 10.2.2.0 255.255.255.0
    nat (inside,outside) dynamic interface

! Identify inside Boulder network for use in twice NAT rule:
object network boulder_inside
    subnet 10.1.1.0 255.255.255.0

! Identify local VPN network for use in twice NAT rule:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0

! Use twice NAT to pass traffic between the San Jose network and Boulder without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside destination static
boulder_inside boulder_inside

! Use twice NAT to pass traffic between the San Jose network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside destination static
vpn_local vpn_local
```

NAT および VPN 管理アクセス

VPN を使用する場合、ASA を開始したインターフェイス以外のインターフェイスへの管理アクセスを許可することができます（**management-access** コマンドを参照）。たとえば、外部インターフェイスから ASA を開始する場合、管理アクセス機能では、ASDM、SSH、Telnet、または SNMP を使用して内部インターフェイスに接続することが可能です。または、内部インターフェイスに ping を実行できます。

次の図に、ASA の内部インターフェイスに Telnet 接続する VPN クライアントを示します。管理アクセス インターフェイスを使用し、「NAT とリモート アクセス VPN」（P.4-27）または「NAT およびサイトツーサイト VPN」（P.4-29）に従ってアイデンティティ NAT を設定する場合、ルート ルックアップ オプションを使用して NAT を設定する必要があります。ルート ルックアップがない場合、ASA は、ルーティング テーブルの内容に関係なく、NAT コマンドで指定されたインターフェイスからトラフィックを送信します。次の例では、出力インターフェイスは内部インターフェイスです。ASA で、内部ネットワークに管理トラフィックを送信しません。これは、内部インターフェイスの IP アドレスには戻りません。ルート ルックアップ オプションを使用すると、ASA は、内部ネットワークの代わりに内部インターフェイスの IP アドレスに直接トラフィックを送信できます。VPN クライアントから内部ネットワーク上のホストへのトラフィックの場合、ルート ルックアップ オプションがあっても正しい出力インターフェイス（内部）になるため、通常のトラフィック フローは影響を受けません。ルート ルックアップ オプションの詳細については、「出力インターフェイスの決定」（P.4-26）を参照してください。

図 4-25　VPN 管理アクセス



上記のネットワークのための次のサンプル NAT の設定を参照してください。

```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! Enable management access on inside ifc:
management-access inside

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0
    nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
    subnet 10.1.1.0 255.255.255.0
    nat (inside,outside) dynamic interface

! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT), w/route-lookup:
nat (outside,inside) source static vpn_local vpn_local destination static inside_nw
inside_nw route-lookup
```

NAT と VPN のトラブルシューティング

VPN を使用した NAT の問題をトラブルシューティングするためには、次の監視ツールを参照してください。

- パケット トレーサ：正しく使用した場合、パケット トレーサは、パケットが該当している NAT ルールを表示します。
- **show nat detail**：特定の NAT ルールのヒット カウントおよび変換解除されたトラフィックを表示します。
- **show conn all**：ボックス トラフィックとの間の接続を含むアクティブ接続を表示します。

非動作設定と動作設定に習熟するには、次の手順を実行します。

1. アイデンティティ NAT を使用しない VPN を設定します。
2. **show nat detail** と **show conn all** を入力します。
3. アイデンティティ NAT の設定を追加します。
4. **show nat detail** と **show conn all** を繰り返します。

DNS および NAT

応答内のアドレスを NAT コンフィギュレーションと一致するアドレスに置き換えて、DNS 応答を修正するように ASA を設定することが必要になる場合があります。DNS 修正は、各トランスレーション ルールを設定するときに設定できます。

この機能は、NAT ルールに一致する DNS クエリーと応答のアドレスをリライトします（たとえば、IPv4 の A レコード、IPv6 の AAAA レコード、または逆引き DNS クエリーの PTR レコード）。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答では、A レコードはマップされた値から実際の値へリライトされます。逆に、任意のインターフェイスからマッピング インターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へリライトされます。

次に DNS リライトの制限事項を示します。

- 個々の A レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS リライトは PAT には適用されません。
- Twice NAT ルールを設定する場合、送信元アドレスおよび宛先アドレスを指定すると、DNS 修正を設定できません。これらの種類のルールでは、A と B に向かった場合に 1 つのアドレスに対して異なる変換が行われる可能性があります。したがって、ASA は、DNS 応答内の IP アドレスを適切な Twice NAT ルールに一致させることができません。DNS 応答には、DNS 要求を求めたパケット内の送信元アドレスと宛先アドレスの組み合わせに関する情報が含まれません。
- DNS リライトでは、デフォルトでオンになっている DNS 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。詳細については、「DNS インスペクション」（P.8-1）を参照してください。
- 実際には、DNS リライトは NAT ルールではなく xlate エントリで実行されます。したがって、ダイナミック ルールに xlate がない場合、リライトが正しく実行されません。スタティック NAT の場合は、同じような問題が発生しません。

次のトピックで、DNS リライトの例を示します。

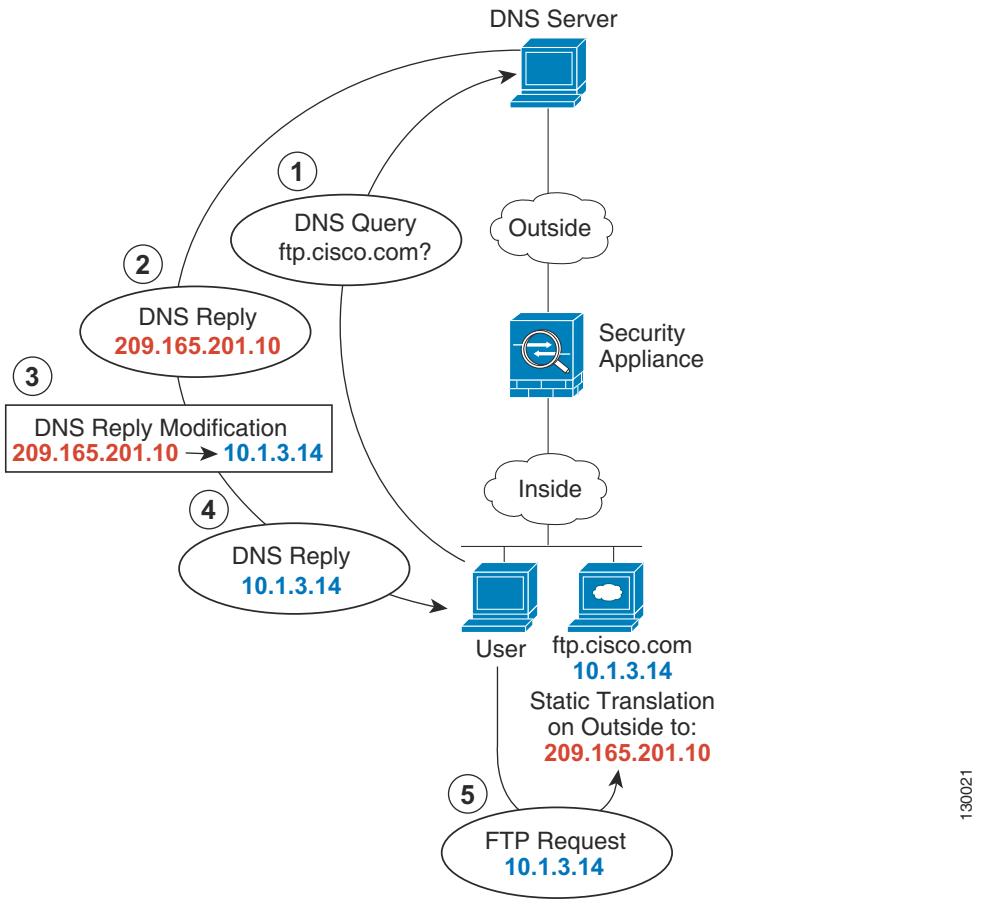
- 「DNS 応答修正：Outside 上の DNS サーバ」（P.4-34）
- 「DNS 応答修正：別々のネットワーク上の DNS サーバ、ホスト、サーバ」（P.4-35）

DNS 応答修正：Outside 上の DNS サーバ

次の図に、外部インターフェイスからアクセス可能な DNS サーバを示します。ftp.cisco.com というサーバが内部インターフェイス上にあります。ftp.cisco.com の実際のアドレス（10.1.3.14）を、外部ネットワーク上で可視のマッピング アドレス（209.165.201.10）にスタティックに変換するように、ASA を設定します。

この場合、このスタティック ルールで DNS 応答修正をイネーブルにする必要があります。これにより、実際のアドレスを使用して ftp.cisco.com にアクセスすることを許可されている内部ユーザは、マッピング アドレスではなく実際のアドレスを DNS サーバから受信できるようになります。内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバは応答でマッピング アドレス（209.165.201.10）を示します。ASA は、内部サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正をイネーブルにしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックを送信することを試みます。

図 4-26　DNS 応答修正：Outside 上の DNS サーバ

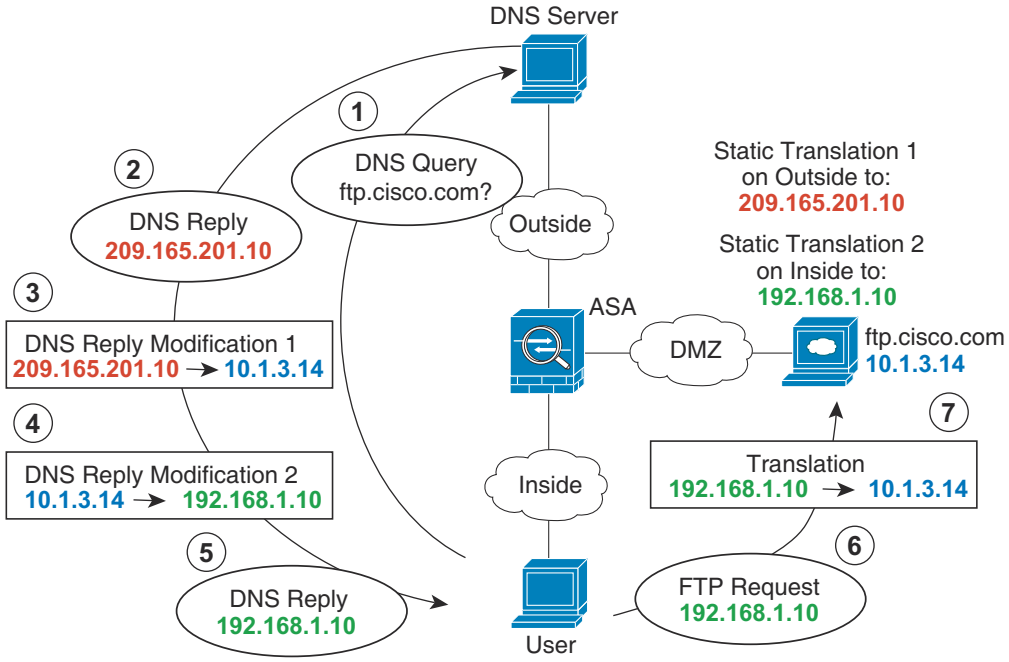


DNS 応答修正：別々のネットワーク上の DNS サーバ、ホスト、サーバ

次の図に、外部 DNS サーバから DMZ ネットワークにある ftp.cisco.com の IP アドレスを要求する内部ネットワークのユーザを示します。DNS サーバは、ユーザが DMZ ネットワーク上に存在しない場合でも、外部と DMZ 間のスタティック ルールに従って応答でマッピング アドレス（209.165.201.10）を示します。ASA は、DNS 応答内のアドレスを 10.1.3.14 に変換します。

ユーザが実際のアドレスを使用して ftp.cisco.com にアクセスする必要がある場合、これ以上の設定は必要ありません。内部と DMZ 間にもスタティック ルールがある場合は、このルールに対して DNS 応答修正もイネーブルにする必要があります。このとき、DNS 応答は 2 回修正されます。この場合、ASA は内部と DMZ 間のスタティック ルールに従って、DNS 応答内のアドレスを再度 192.168.1.10 に変換します。

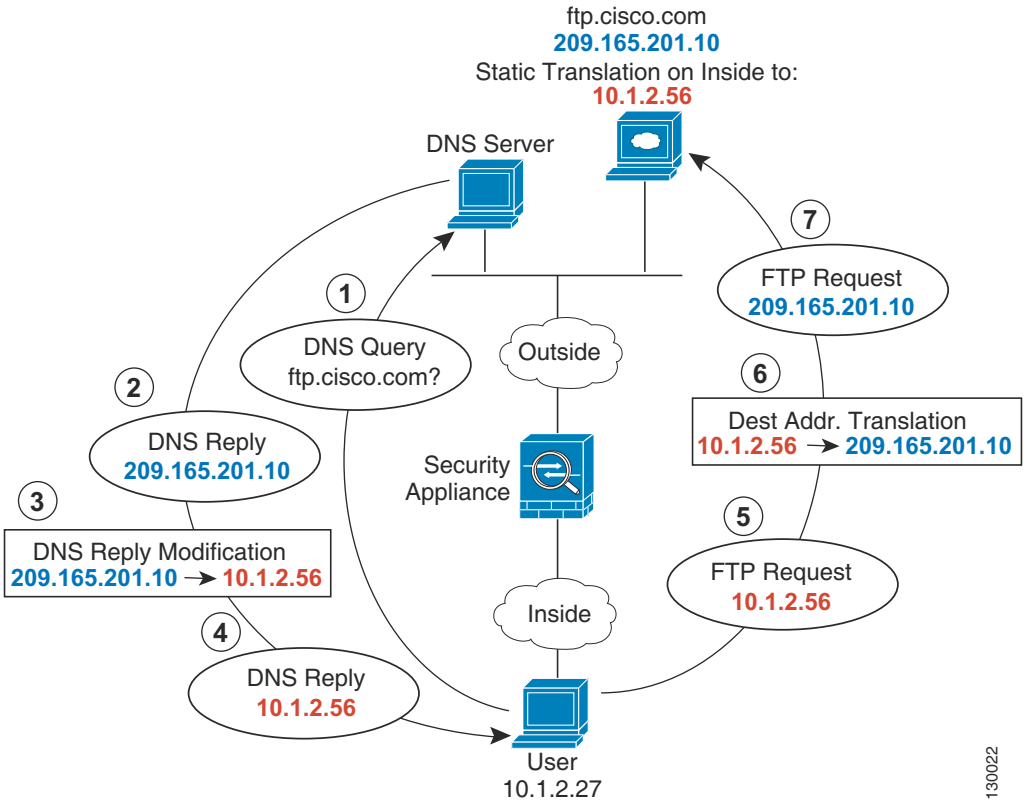
図 4-27　DNS 応答修正：別々のネットワーク上の DNS サーバ、ホスト、サーバ



DNS 応答修正：ホスト ネットワーク上の DNS サーバ

次の図に、外部の FTP サーバと DNS サーバを示します。ASA には、外部サーバ用のスタティック変換があります。この場合、ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答で実際のアドレス 209.165.20.10 を示します。ftp.cisco.com のマッピング アドレス（10.1.2.56）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。

図 4-28　DNS 応答修正：ホスト ネットワーク上の DNS サーバ

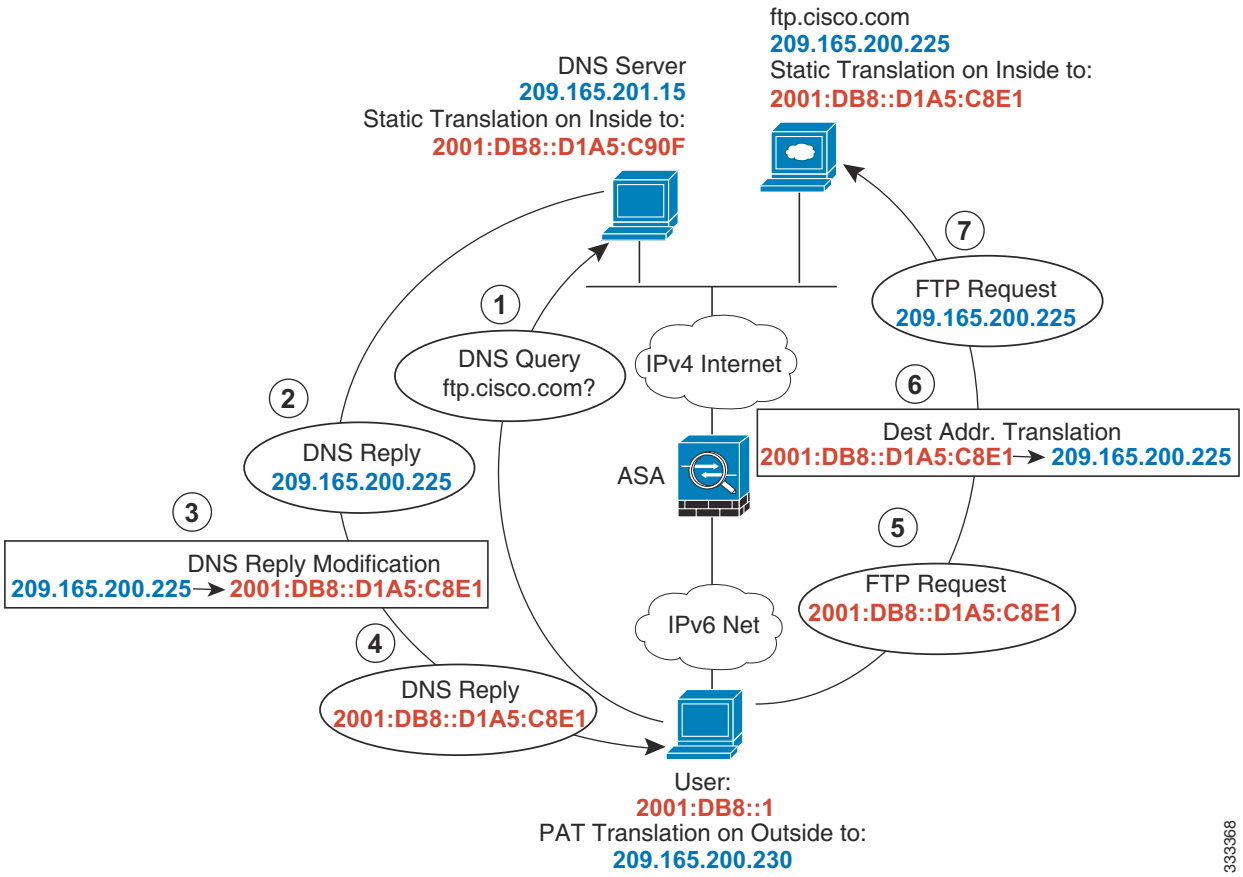


外部 NAT を使用する DNS64 応答修正

次の図に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。ASA には、外部サーバ用のスタティック変換があります。この場合に、内部 IPv6 ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答として実際のアドレス 209.165.200.225 を返します。

ftp.cisco.com のマッピング アドレス（2001:DB8::D1A5:C8E1）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。この例には、DNS サーバのスタティック NAT 変換、および内部 IPv6 ホストの PAT ルールも含まれています。

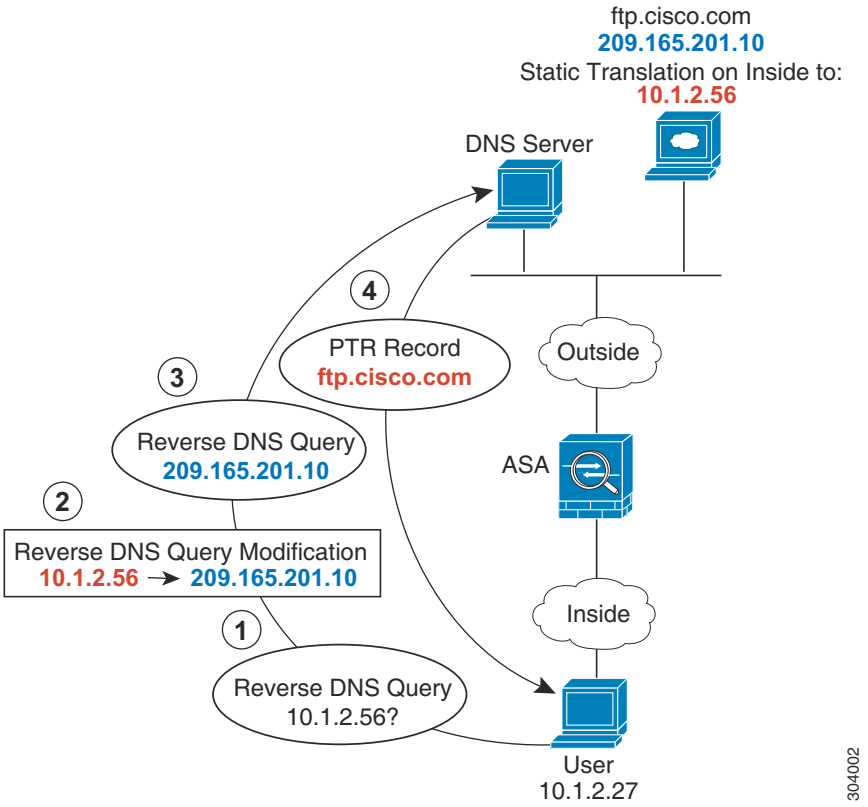
図 4-29　外部 NAT を使用する DNS64 応答修正



PTR の変更、ホスト ネットワークの DNS サーバ

次の図に、外部の FTP サーバと DNS サーバを示します。ASA には、外部サーバ用のスタティック変換があります。この場合、内部のユーザが 10.1.2.56 の逆引き DNS ルックアップを実行する場合、ASA は実際のアドレスを使用して逆引き DNS クエリーを変更し、DNS サーバはサーバ名、ftp.cisco.com を使用して応答します。

図 4-30　PTR の変更、ホスト ネットワークの DNS サーバ



次の作業

ネットワーク オブジェクト NAT を設定するには、第 5 章「ネットワーク オブジェクト NAT の設定」を参照してください。

Twice NAT を設定するには、第 6 章「Twice NAT」を参照してください。

CHAPTER 5

ネットワーク オブジェクト NAT の設定

ネットワーク オブジェクトのパラメータとして設定されているすべての NAT ルールは、*ネットワーク オブジェクト NAT ルール*と見なされます。ネットワーク オブジェクト NAT は、1 つの IP アドレス、アドレスの範囲、またはサブネットに対して NAT を設定するための迅速かつ容易な方法です。ネットワーク オブジェクトを設定したら、このオブジェクトのマッピング アドレスを識別できます。

この章では、ネットワーク オブジェクト NAT を設定する方法について説明します。この章は、次の項で構成されています。

（注） NAT の機能の詳細については、第 4 章「ネットワーク アドレス変換（NAT）」を参照してください。

ネットワーク オブジェクト NAT に関する情報

パケットが ASA に入ると、送信元 IP アドレスと宛先 IP アドレスの両方がネットワーク オブジェクト NAT ルールと照合されます。個別の照合が行われる場合、パケット内の送信元 IP アドレスと宛先 IP アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはありません。したがって、宛先 X に向かう場合は送信元アドレスが A と変換され、宛先 Y に向かう場合は B と変換されるように指定することはできません。この種の機能には、Twice NAT を使用します（Twice NAT を使用すると、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます）。

Twice NAT とネットワーク オブジェクト NAT の違いの詳細については、「NAT の実装方法」（P.4-15）を参照してください。

ネットワーク オブジェクト NAT ルールは、NAT ルール テーブルのセクション 2 に追加されます。NAT の順序の詳細については、「NAT ルールの順序」（P.4-20）を参照してください。

ネットワーク オブジェクト NAT のライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

ネットワーク オブジェクト NAT の前提条件

コンフィギュレーションによっては、必要に応じてマッピング アドレスをインラインで設定したり、マッピング アドレスの別のネットワーク オブジェクトまたはネットワーク オブジェクト グループを作成したりできます（**object network** コマンドまたは **object-group network** コマンド）。ネットワーク オブジェクト グループは、非連続的な IP アドレス範囲または複数のホストやサブネットで構成されるマッピング アドレスを作成する場合に特に便利です。ネットワーク オブジェクトまたはグループを作成するには、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。

オブジェクトおよびグループに関する特定のガイドラインについては、設定する NAT タイプの設定の項を参照してください。「ガイドラインと制限事項」（P.5-2）も参照してください。

ガイドラインと制限事項

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

- ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。
- トランスペアレント モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定する必要があります。**any** は使用できません。
- トランスペアレント モードでは、インターフェイス PAT を設定できません。トランスペアレント モードのインターフェイスには、IP アドレスが設定されていないためです。管理 IP アドレスもマッピング アドレスとして使用できません。
- トランスペアレント モードでは、IPv4 ネットワークと IPv6 ネットワークとの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。

IPv6 のガイドライン

- IPv6 をサポートします。「NAT と IPv6」（P.4-15）も参照してください。
- ルーテッド モードの場合は、IPv4 と IPv6 との間の変換もできます。
- トランスペアレント モードの場合は、IPv4 ネットワークと IPv6 ネットワークとの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。
- トランスペアレント モードの場合は、PAT プールは IPv6 に対してはサポートされません。
- スタティック NAT の場合は、/64 までの IPv6 サブネットを指定できます。これよりも大きいサブネットはサポートされません。
- FTP を NAT46 とともに使用する場合は、IPv4 FTP クライアントが IPv6 FTP サーバに接続するときに、クライアントは拡張パッシブ モード（EPSV）または拡張ポート モード（EPRT）を使用する必要があります。PASV コマンドおよび PORT コマンドは IPv6 ではサポートされません。

その他のガイドライン

- 定義できる NAT ルールは 1 つのオブジェクトに対して 1 つだけです。1 つのオブジェクトに対して複数の NAT ルールを設定する場合は、複数のオブジェクトを作成する必要があります。それぞれに異なる名前を付け、IP アドレスは同じものを指定します。たとえば、**object network obj-10.10.10.1-01**、**object network obj-10.10.10.1-02** などとします。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT コンフィギュレーションが使用されるようにするには、**clear xlate** コマンドを使用して変換テーブルを消去します。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

（注）　ダイナミック NAT または PAT ルールを削除し、次に削除したルールに含まれるアドレスと重複するマッピング アドレスを含む新しいルールを追加すると、新しいルールは、削除されたルールに関連付けられたすべての接続がタイムアウトするか、**clear xlate** コマンドを使用してクリアされるまで使用されません。この予防手段のおかげで、同じアドレスが複数のホストに割り当てられないようにできます。

- NAT で使用されるオブジェクトおよびオブジェクト グループを未定義にすることはできません。IP アドレスを含める必要があります。
- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。
- 同じマッピング オブジェクトやグループを複数の NAT ルールで使用できます。
- マッピング IP アドレス プールは、次のアドレスを含むことができません。
  - マッピング インターフェイスの IP アドレス。ルールに **any** インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT（ルーテッド モードのみ）の場合、IP アドレスの代わりに **interface** キーワードを使用します。
  - （トランスペアレント モード）管理 IP アドレス。
  - （ダイナミック NAT）VPN がイネーブルの場合は、スタンバイ インターフェイスの IP アドレス。
  - 既存の VPN プールのアドレス。

- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- NAT や PAT に伴うアプリケーション インスペクションの制限については、第 7 章「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」の「デフォルト インスペクションと NAT に関する制限事項」（P.7-6）を参照してください。

デフォルト設定

- （ルーテッド モード）デフォルトの実際のインターフェイスおよびマッピング インターフェイスは Any で、すべてのインターフェイスにルールが適用されます。
- アイデンティティ NAT のデフォルト動作で、プロキシ ARP はイネーブルにされ、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP をディセーブルにできます。詳細については、「NAT パケットのルーティング」（P.4-22）を参照してください。
- オプションのインターフェイスを指定する場合、ASA によって NAT コンフィギュレーションが使用されて、出力インターフェイスが決定されます、代わりにルート ルックアップを常に使用するオプションがあります。詳細については、「NAT パケットのルーティング」（P.4-22）を参照してください。

ネットワーク オブジェクト NAT の設定

この項では、ネットワーク オブジェクト NAT を設定する方法について説明します。

- 「マッピング アドレスのネットワーク オブジェクトの追加」（P.5-4）
- 「ダイナミック NAT を使用したダイナミック PAT の設定」（P.5-6）
- 「ダイナミック PAT（隠蔽）の設定」（P.5-9）
- 「スタティック NAT またはポート変換を設定したスタティック NAT の設定」（P.5-13）
- 「アイデンティティ NAT の設定」（P.5-15）
- 「Per-Session PAT ルールの設定」（P.5-17）

マッピング アドレスのネットワーク オブジェクトの追加

ダイナミック NAT の場合は、マッピングされたアドレスに対してオブジェクトまたはグループを使用する必要があります。他のタイプの NAT の場合は、インライン アドレスを使用することも、この項の説明に従ってオブジェクトまたはグループを作成することもできます。ネットワーク オブジェクトまたはグループの設定の詳細については、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。

ガイドライン

- 1 つのネットワーク オブジェクト グループには、IPv4 アドレスと IPv6 アドレスのいずれか一方のオブジェクトやインライン アドレスを入れることができます。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。
- 拒否されるマッピング IP アドレスについては、「ガイドラインと制限事項」（P.5-2）を参照してください。
- ダイナミック NAT：
  - インライン アドレスは使用できません。ネットワーク オブジェクトまたはグループを設定する必要があります。
  - オブジェクトまたはグループには、サブネットを含めることはできません。オブジェクトは、範囲を定義する必要があります。グループには、ホストと範囲を含めることができます。
  - マッピングされたネットワーク オブジェクトに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォール バックとして使用されます。
- ダイナミック PAT（隠蔽）：
  - オブジェクトを使用する代わりに、任意でインライン ホスト アドレスを設定するか、またはインターフェイス アドレスを指定できます。
  - オブジェクトを使用する場合は、オブジェクトまたはグループにサブネットを入れることはできません。オブジェクトは、1 つのホスト、または範囲（PAT プールの場合）を定義する必要があります。グループ（PAT プールの場合）には、複数のホストと範囲を入れることができます。
- スタティック NAT またはポート変換を使用するスタティック NAT：
  - オブジェクトを使用する代わりに、インライン アドレスを設定するか、またはインターフェイス アドレスを指定できます（ポート変換を使用するスタティック NAT の場合）。
  - オブジェクトを使用する場合は、オブジェクトまたはグループにホスト、範囲、またはサブネットを入れることができます。
- アイデンティティ NAT
  - オブジェクトを使用する代わりに、インライン アドレスを設定できます。
  - オブジェクトを使用する場合は、オブジェクトは、変換する実際のアドレスと一致する必要があります。

手順の詳細

コマンド	目的

object network *obj_name* {**host** *ip_address* | **range** *ip_address_1 ip_address_2* | **subnet** *subnet_address netmask*}
 	
例：
`hostname(config)# object network TEST`
`hostname(config-network-object)# range 10.1.1.1 10.1.1.70`
	ネットワーク オブジェクト（IPv4 または IPv6）を追加します。

object-group network *grp_name* {**network-object** {**object** *net_obj_name* | *subnet_address netmask* | **host** *ip_address*} | **group-object** *grp_obj_name*}
 	
例：
`hostname(config)# object network TEST`
`hostname(config-network-object)# range 10.1.1.1 10.1.1.70`
 	
`hostname(config)# object network TEST2`
`hostname(config-network-object)# range 10.1.2.1 10.1.2.70`
 	
`hostname(config-network-object)# object-group network MAPPED_IPS`
`hostname(config-network)# network-object object TEST`
`hostname(config-network)# network-object object TEST2`
`hostname(config-network)# network-object host 10.1.2.79`
	ネットワーク オブジェクト グループ（IPv4 または IPv6）を追加します。

ダイナミック NAT を使用したダイナミック PAT の設定

この項では、ダイナミック NAT のためのネットワーク オブジェクト NAT を設定する方法について説明します。詳細については、「ダイナミック NAT」（P.4-8）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	マッピング アドレスのためのネットワーク オブジェクトまたはグループを作成します。	「マッピング アドレスのネットワーク オブジェクトの追加」（P.5-4）を参照してください。
ステップ 2	**object network** *obj_name* **例：** `hostname(config)# object network my-host-obj1`	NAT を設定するネットワーク オブジェクトを設定するか、既存のネットワーク オブジェクトについてオブジェクト ネットワーク コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **例：** `hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0`	新しいネットワーク オブジェクトを作成する場合は、変換する**実際の** IP アドレス（IPv4 または IPv6）を定義します。
ステップ 4	**nat** [(*real_ifc*,*mapped_ifc*)] **dynamic** *mapped_obj* [**interface** [**ipv6**]] [**dns**] **例：** `hostname(config-network-object)# nat (inside,outside) dynamic MAPPED_IPS interface`	オブジェクト IP アドレスの**ダイナミック NAT** を設定します。 **（注）** 特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。「その他のガイドライン」（P.5-3）を参照してください。 次のガイドラインを参照してください。 • インターフェイス：（トランスペアレント モードの場合に必須）実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。インターフェイスの 1 つまたは両方に **any** キーワードを指定することもできます。 • マッピング IP アドレス：次のものとしてマッピング IP アドレスを指定します。 – 既存のネットワーク オブジェクト（ステップ 1 を参照） – 既存のネットワーク オブジェクト グループ（ステップ 1 を参照） • インターフェイス PAT のフォール バック：（任意）**interface** キーワードは、インターフェイス PAT のフォール バックをイネーブルにします。マッピング IP アドレスを使い果たすと、続いてマッピング インターフェイスの IP アドレスが使用されます。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります（トランスペアレント モードでは、**interface** を指定できません）。 • DNS：（任意）**dns** キーワードは、DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。詳細については、「DNS および NAT」（P.4-33）を参照してください。

例

次の例では、外部アドレス 10.2.2.1 ～ 10.2.2.10 の範囲の背後に 192.168.2.0 ネットワークを隠すダイナミック NAT を設定します。

```
hostname(config)# object network my-range-obj
hostname(config-network-object)# range 10.2.2.1 10.2.2.10
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

次の例では、ダイナミック PAT バックアップを設定したダイナミック NAT を設定します。ネットワーク 10.76.11.0 内のホストは、まず nat-range1 プール（10.10.10.10 ～ 10.10.10.20）にマッピングされます。nat-range1 プール内のすべてのアドレスが割り当てられたら、pat-ip1 アドレス（10.10.10.21）を使用してダイナミック PAT が実行されます。万一、PAT 変換もすべて使用されてしまった場合は、外部インターフェイス アドレスを使用してダイナミック PAT が実行されます。

```
hostname(config)# object network nat-range1
hostname(config-network-object)# range 10.10.10.10 10.10.10.20

hostname(config-network-object)# object network pat-ip1
hostname(config-network-object)# host 10.10.10.21

hostname(config-network-object)# object-group network nat-pat-grp
hostname(config-network-object)# network-object object nat-range1
hostname(config-network-object)# network-object object pat-ip1

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 10.76.11.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

次の例では、ダイナミック NAT とダイナミック PAT バックアップを使用して IPv6 ホストを IPv4 に変換するように設定します。内部ネットワーク 2001:DB8::/96 上のホストは最初に、IPv4_NAT_RANGE プール（209.165.201.30 ～ 209.165.201.1）にマッピングされます。IPv4_NAT_RANGE プール内のすべてのアドレスが割り当てられた後は、IPv4_PAT アドレス（209.165.201.31）を使用してダイナミック PAT が実行されます。PAT 変換もすべて使用されてしまった場合は、外部インターフェイス アドレスを使用してダイナミック PAT が実行されます。

```
hostname(config)# object network IPv4_NAT_RANGE
hostname(config-network-object)# range 209.165.201.1 209.165.201.30

hostname(config-network-object)# object network IPv4_PAT
hostname(config-network-object)# host 209.165.201.31

hostname(config-network-object)# object-group network IPv4_GROUP
hostname(config-network-object)# network-object object IPv4_NAT_RANGE
hostname(config-network-object)# network-object object IPv4_PAT

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface
```

ダイナミック PAT（隠蔽）の設定

この項では、ダイナミック PAT（隠蔽）のためのネットワーク オブジェクト NAT の設定方法について説明します。詳細については、「ダイナミック PAT」（P.4-10）を参照してください。

ガイドライン

PAT プールの場合：

- 使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用 *できない* 場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。（8.4(3) 以降、ただし 8.5(1) と 8.6(1) を除く）下位ポート範囲を使用するトラフィックが数多くある場合は、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます（1024 ～ 65535、または 1 ～ 65535）。
- 同じ PAT プール オブジェクトを 2 つの異なるルールの中で使用する場合は、必ず同じオプションを各ルールに指定してください。たとえば、1 つのルールで拡張 PAT およびフラットな範囲が指定される場合は、もう一方のルールでも拡張 PAT およびフラットな範囲が指定される必要があります。

PAT プールに対する拡張 PAT の場合：

- 多くのアプリケーション インスペクションでは、拡張 PAT はサポートされていません。サポート対象外のインスペクションの完全な一覧については、第 7 章「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」の「デフォルト インスペクションと NAT に関する制限事項」（P.7-6）を参照してください。
- ダイナミック PAT ルールに対して拡張 PAT をイネーブルにする場合は、PAT プール内のアドレスを、ポート変換ルールを設定した別のスタティック NAT の PAT アドレスとしても使用することはできません。たとえば、PAT プールに 10.1.1.1 が含まれている場合、PAT アドレスとして 10.1.1.1 を使用する、ポート変換ルールを設定したスタティック NAT は作成できません。
- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。
- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。

PAT プールのラウンドロビンの場合：

- ホストに既存の接続がある場合は、そのホストからの以降の接続は同じ PAT IP アドレスを使用します（ポートが使用可能である場合）。**注**：この「粘着性」は、フェールオーバーが発生すると失われます。ASA がフェールオーバーすると、ホストからの後続の接続では最初の IP アドレスが使用されない場合があります。
- ラウンドロビンでは、特に拡張 PAT と組み合わせた場合に、大量のメモリが消費されます。NAT プールはマッピングされるプロトコル/IP アドレス/ポート範囲ごとに作成されるため、ラウンドロビンでは数多くの同時 NAT プールが作成され、メモリが使用されます。拡張 PAT では、さらに多くの同時 NAT プールが作成されます。

手順の詳細

	コマンド	目的
ステップ 1	（任意）マッピング アドレスのためのネットワーク オブジェクトまたはグループを作成します。	「マッピング アドレスのネットワーク オブジェクトの追加」（P.5-4）を参照してください。
ステップ 2	**object network** *obj_name* **例：** `hostname(config)# object network my-host-obj1`	NAT を設定するネットワーク オブジェクトを設定するか、既存のネットワーク オブジェクトについてオブジェクト ネットワーク コンフィギュレーション モードを開始します。
ステップ 3	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **例：** `hostname(config-network-object)# range 10.1.1.1 10.1.1.90`	新しいネットワーク オブジェクトを作成する場合は、変換する**実際の** IP アドレス（IPv4 または IPv6）を定義します。

	コマンド	目的
ステップ 4	**nat** [(*real_ifc*,*mapped_ifc*)] **dynamic** {*mapped_inline_host_ip* | *mapped_obj* | **pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] | **interface** [**ipv6**]} [**interface** [**ipv6**]] [**dns**] **例：** hostname(config-network-object)# nat (any,outside) dynamic interface	オブジェクト IP アドレスの**ダイナミック PAT** を設定します。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。「その他のガイドライン」（P.5-3）を参照してください。 次のガイドラインを参照してください。 • インターフェイス：（トランスペアレント モードの場合に必須）実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。インターフェイスの 1 つまたは両方に **any** キーワードを指定することもできます。 • マッピング IP アドレス：マッピング IP アドレスを次のものとして指定できます。 – インライン ホスト アドレス。 – ホスト アドレスとして定義される既存のネットワーク オブジェクト（ステップ 1 を参照）。 – **pat-pool**：複数のアドレスを含む、既存のネットワーク オブジェクトまたはグループ。 – **interface**：（ルーテッド モードのみ）マッピング インターフェイスの IP アドレスは、マッピング アドレスとして使用されます。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。このキーワードは、インターフェイスの IP アドレスを使用するときに使用する必要があります。インラインで、またはオブジェクトとして入力することはできません。 • PAT プールについて、次のオプションの 1 つ以上を指定できます。 – ラウンド ロビン：**round-robin** キーワードは、PAT プールのラウンド ロビン アドレス割り当てをイネーブルにします。ラウンド ロビンを指定しなければ、デフォルトで PAT アドレスのすべてのポートは次の PAT アドレスが使用される前に割り当てられます。ラウンド ロビン方式では、最初のアドレスに戻って再び使用される前に、2 番目のアドレス、またその次と、プール内の各 PAT アドレスからアドレス/ポートが割り当てられます。 （続き）

コマンド	目的
	（続き） – 拡張 PAT：**extended** キーワードは、拡張 PAT をイネーブルにします。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、*サービス*ごとに 65535 個のポートが使用されます。通常は、PAT 変換を作成するときに宛先ポートとアドレスは考慮されないため、PAT アドレスごとに 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。 – フラット範囲：**flat** キーワードを指定すると、ポートを割り当てるときに 1024 ～ 65535 のポート範囲全体を使用できるようになります。変換のマッピング ポート番号を選択するときに、ASA によって、使用可能な場合は実際の送信元ポート番号が使用されます。ただし、このオプションを設定しないと、実際のポートが使用*できない*場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、**include-reserve** キーワードも指定します。 • インターフェイス PAT のフォール バック：（任意）**interface** キーワードは、プライマリ PAT アドレスの後に入力されたときにインターフェイス PAT のフォール バックをイネーブルにします。プライマリ PAT アドレスを使い果たすと、マッピング インターフェイスの IP アドレスが使用されます。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります（トランスペアレント モードでは、**interface** を指定できません）。 • DNS：（任意）**dns** キーワードは、DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。詳細については、「DNS および NAT」（P.4-33）を参照してください。

例

次の例では、アドレス 10.2.2.2 の背後に 192.168.2.0 ネットワークを隠すダイナミック PAT を設定します。

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 10.2.2.2
```

次の例では、外部インターフェイス アドレスの背後に 192.168.2.0 ネットワークを隠蔽するダイナミック PAT を設定します。

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic interface
```

次の例では、ダイナミック PAT と PAT プールを使用して内部 IPv6 ネットワークを外部 IPv4 ネットワークに変換するように設定します。

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 203.0.113.1 203.0.113.254
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

スタティック NAT またはポート変換を設定したスタティック NAT の設定

この項では、ネットワーク オブジェクト NAT を使用してスタティック NAT ルールを設定する方法について説明します。詳細については、「スタティック NAT」（P.4-3）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	（任意）マッピング アドレスのためのネットワーク オブジェクトまたはグループを作成します。	「マッピング アドレスのネットワーク オブジェクトの追加」（P.5-4）を参照してください。
ステップ 2	**object network** *obj_name* **例：** `hostname(config)# object network my-host-obj1`	NAT を設定するネットワーク オブジェクトを設定するか、既存のネットワーク オブジェクトについてオブジェクト ネットワーク コンフィギュレーション モードを開始します。
ステップ 3	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **例：** `hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0`	新しいネットワーク オブジェクトを作成する場合は、変換する**実際の** IP アドレス（IPv4 または IPv6）を定義します。

	コマンド	目的
ステップ 4	**nat** [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj* | **interface** [**ipv6**]} [**net-to-net**] [**dns** | **service** {**tcp** | **udp**} *real_port mapped_port*] [**no-proxy-arp**] **例：** `hostname(config-network-object)# nat (inside,outside) static MAPPED_IPS service tcp 80 8080`	オブジェクト IP アドレスの**スタティック NAT** を設定します。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。 • インターフェイス：（トランスペアレント モードの場合に必須）実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。インターフェイスの 1 つまたは両方に **any** キーワードを指定することもできます。 • マッピング IP アドレス：マッピング IP アドレスを次のものとして指定できます。 – インライン IP アドレス。マッピング ネットワークのネットマスクまたは範囲は、実際のネットワークと同じです。たとえば、実際のネットワークがホストの場合、このアドレスは、ホスト アドレスです。範囲の場合、マッピング アドレスには、実際の範囲と同じ数のアドレスが含まれます。たとえば、実際のアドレスが 10.1.1.1 ～ 10.1.1.6 の範囲として定義され、172.20.1.1 をマッピング アドレスとして指定する場合、マッピング範囲には、172.20.1.1 ～ 172.20.1.6 が含まれます。 – 既存のネットワーク オブジェクトまたはグループ（ステップ 1 を参照）。 – **interface**：（ポート変換を設定したスタティック NAT のみ、ルーテッド モード）このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。**service** キーワードも必ず設定します。 通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。「スタティック NAT」（P.4-3）を参照してください。 • ネットツーネット：（任意）NAT 46 の場合は、**net-to-net** を指定すると、最初の IPv4 アドレスが最初の IPv6 アドレスに、2 番目が 2 番目に、というように変換されます。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このキーワードを使用する必要があります。 • DNS：（任意）**dns** キーワードは、DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。「DNS および NAT」（P.4-33）を参照してください。**service** キーワードを指定した場合、このオプションは使用できません。 • ポート変換：（ポート変換を設定したスタティック NAT のみ）**tcp** または **udp** および実際のポートとマッピング ポートを指定します。ポート番号または予約済みポートの名前（**ftp** など）のいずれかを入力できます。 • No Proxy ARP：（任意）マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。詳細については、「マッピング アドレスとルーティング」（P.4-22）を参照してください。

例

次の例では、内部にある実際のホスト 10.1.1.1 の、DNS リライトがイネーブルに設定された外部にある 10.2.2.2 へのスタティック NAT を設定します。

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.2.2.2 dns
```

次の例では、内部にある実際のホスト 10.1.1.1 の、マッピングされたオブジェクトを使用する外部にある 10.2.2.2 へのスタティック NAT を設定します。

```
hostname(config)# object network my-mapped-obj
hostname(config-network-object)# host 10.2.2.2

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-mapped-obj
```

次の例では、10.1.1.1 の TCP ポート 21 の、外部インターフェイスのポート 2121 への、ポート変換を設定したスタティック NAT を設定します。

```
hostname(config)# object network my-ftp-server
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static interface service tcp 21 2121
```

次の例では、内部 IPv4 ネットワークを外部 IPv6 ネットワークにマッピングします。

```
hostname(config)# object network inside_v4_v6
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) static 2001:DB8::/96
```

次の例では、内部 IPv6 ネットワークを外部 IPv6 ネットワークにマッピングします。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96
hostname(config-network-object)# nat (inside,outside) static 2001:DB8:BBBB::/96
```

アイデンティティ NAT の設定

この項では、ネットワーク オブジェクト NAT を使用してアイデンティティ NAT ルールを設定する方法について説明します。詳細については、「アイデンティティ NAT」（P.4-12）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	（任意）マッピング アドレスのためのネットワーク オブジェクトを作成します。	オブジェクトには、変換するアドレスと同じものが含まれている必要があります。「マッピング アドレスのネットワーク オブジェクトの追加」（P.5-4）を参照してください。
ステップ 2	**object network** *obj_name* **例：** `hostname(config)# object network my-host-obj1`	アイデンティティ NAT を実行するネットワーク オブジェクトを設定するか、既存のネットワーク オブジェクトについてオブジェクト ネットワーク コンフィギュレーション モードを開始します。このネットワーク オブジェクトの名前は、マッピングされたネットワーク オブジェクトとは異なります（ステップ 1 を参照）。両方に同じ IP アドレスが含まれていても、このようになります。

	コマンド	目的
ステップ 3	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **例：** hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0	新しいネットワーク オブジェクトを作成する場合は、実行するアイデンティティ NAT の変換先となる実際の IP アドレス（IPv4 または IPv6）を定義します。ステップ 1 でマッピング アドレスのネットワーク オブジェクトを設定した場合、これらのアドレスは一致する必要があります。
ステップ 4	**nat** [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj*} [**no-proxy-arp**] [**route-lookup**] **例：** hostname(config-network-object)# nat (inside,outside) static MAPPED_IPS	オブジェクト IP アドレスの**アイデンティティ NAT** を設定します。 **（注）** 特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。「その他のガイドライン」（P.5-3）を参照してください。 次のガイドラインを参照してください。 • インターフェイス：（トランスペアレント モードの場合に必須）実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。インターフェイスの 1 つまたは両方に **any** キーワードを指定することもできます。 • マッピング IP アドレス：マッピング アドレスと実際のアドレスの両方に同じ IP アドレスを設定するようにしてください。次のいずれかを使用します。 – ネットワーク オブジェクト：実際のオブジェクトと同じ IP アドレスを含めます（ステップ 1 を参照）。 – インライン IP アドレス：マッピング ネットワークのネットマスクまたは範囲は、実際のネットワークと同じです。たとえば、実際のネットワークがホストの場合、このアドレスは、ホスト アドレスです。範囲の場合、マッピング アドレスには、実際の範囲と同じ数のアドレスが含まれます。たとえば、実際のアドレスが 10.1.1.1 ～ 10.1.1.6 の範囲で定義されている場合、マッピング アドレスとして 10.1.1.1 を指定するには、マッピングされた範囲に 10.1.1.1 ～ 10.1.1.6 が含まれます。 • No Proxy ARP：マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。詳細については、「マッピング アドレスとルーティング」（P.4-22）を参照してください。 • ルート ルックアップ：（ルーテッド モードのみ、インターフェイスを指定）NAT コマンドに指定したインターフェイスを使用する代わりに、ルート ルックアップを使用して出力インターフェイスを決定するには、**route-lookup** を指定します。詳細については、「出力インターフェイスの決定」（P.4-26）を参照してください。

例

次の例では、インラインのマッピング アドレスを使用して、ホスト アドレスを自身にマッピングします。

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.1.1.1
```

次の例では、ネットワーク オブジェクトを使用して、ホスト アドレスを自身にマッピングします。

```
hostname(config)# object network my-host-obj1-identity
hostname(config-network-object)# host 10.1.1.1

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

Per-Session PAT ルールの設定

デフォルトでは、すべての TCP PAT トラフィックおよびすべての UDP DNS トラフィックが Per-Session PAT を使用します。トラフィックに Multi-Session PAT を使用するには、Per-Session PAT ルールを設定します。許可ルールで Per-Session PAT を使用し、拒否ルールで Multi-Session PAT を使用します。Per-Session PAT と Multi-Session PAT の詳細については、「Per-Session PAT と Multi-Session PAT」（P.4-11）を参照してください。

デフォルト

デフォルトでは、次のルールがインストールされます。

```
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

（注） これらのルールは削除できません。これらのルールは常に、手動作成されたルールの後に存在します。ルールは順番に評価されるので、デフォルト ルールを無効にすることができます。たとえば、これらのルールを完全に反転させるには、次のものを追加します。

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

手順の詳細

コマンド	目的
xlate per-session {**permit** | **deny**} {**tcp** | **udp**} *source_ip* [*operator src_port*] *destination_ip operator dest_port* **例：** `hostname(config)# xlate per-session deny tcp any4 209.165.201.3 eq 1720`	許可または拒否ルールを作成します。このルールはデフォルト ルールの上に置かれますが、他の手動作成されたルールよりは下です。ルールは必ず、適用する順序で作成してください。 変換元と変換先の IP アドレスについては、次のように設定できます。 • **host** *ip_address*：IPv4 ホスト アドレスを指定します。 • *ip_address mask*：IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。 • *ipv6-address/prefix-length*：IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。 • **any4** および **any6**：**any4** は IPv4 トラフィックだけを指定します。**any6** は any6 トラフィックを指定します。 *operator* では、変換元または変換先で使用されるポート番号の条件を指定します。使用できる演算子は、次のとおりです。 • lt：より小さい • gt：より大きい • eq：等しい • neq：等しくない • range：値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。 `range 100 200`

例

次の例では、H.323 トラフィックのための拒否ルールを作成します。このトラフィックには Multi-Session PAT が使用されるようにするためです。

```
hostname(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
hostname(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719
```

ネットワーク オブジェクト NAT のモニタリング

オブジェクト NAT をモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
show nat	各 NAT ルールのヒットを含む NAT の統計情報を表示します。
show nat pool	割り当てられたアドレスとホスト、および割り当て回数を含む、NAT プールの統計情報を表示します。

show running-config nat	NAT コンフィギュレーションを表示します。
	（注） NAT コンフィギュレーションは、**show running-config object** コマンドを使用して表示できません。**nat** コマンドで作成されていないオブジェクトまたはオブジェクト グループを参照することはできません。**show** コマンド出力での転送または循環参照を回避するために、**show running-config** コマンドは **object** コマンドを 2 回表示します。1 回目は、IP アドレスが定義される場所、2 回目は **nat** コマンドが定義される場所で表示されます。このコマンド出力によって、オブジェクト、オブジェクト グループ、NAT の順に定義されることが保証されます。次に例を示します。
	`hostname# show running-config`
	`...`
	`object network obj1`
	`  range 192.168.49.1 192.150.49.100`
	`object network obj2`
	`  object 192.168.49.100`
	`object network network-1`
	`  subnet <network-1>`
	`object network network-2`
	`  subnet <network-2>`
	`object-group network pool`
	`  network-object object obj1`
	`  network-object object obj2`
	`...`
	`object network network-1`
	`  nat (inside,outside) dynamic pool`
	`object network network-2`
	`  nat (inside,outside) dynamic pool`

show xlate	現在の NAT セッション情報を表示します。

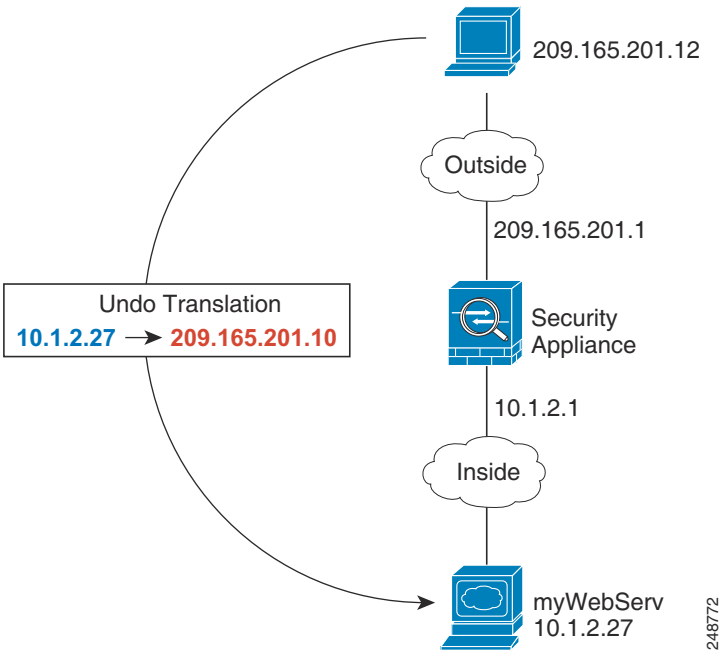
ネットワーク オブジェクト NAT の設定例

ここでは、次の設定例を示します。

内部 Web サーバへのアクセスの提供（スタティック NAT）

次の例では、内部 Web サーバに対してスタティック NAT を実行します。実際のアドレスはプライベート ネットワーク上にあるので、パブリック アドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバへのトラフィックをホストが開始できるようにするために必要です（図 5-1 を参照）。

図 5-1　　内部 Web サーバのスタティック NAT



ステップ 1　内部 Web サーバのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myWebServ
```

ステップ 2　Web サーバのアドレスを定義します。

```
hostname(config-network-object)# host 10.1.2.27
```

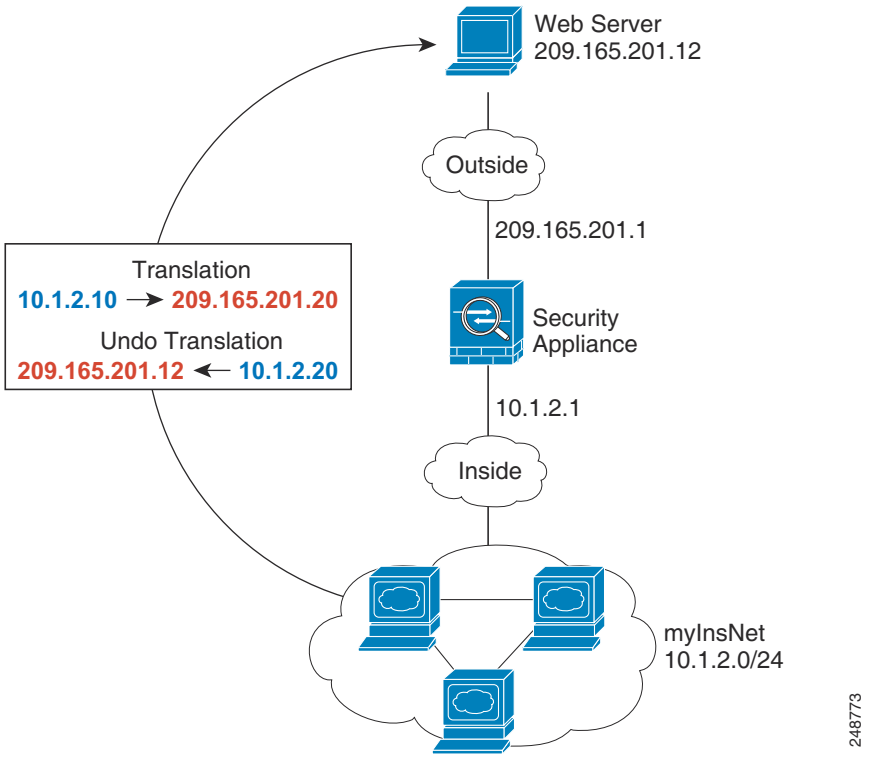
ステップ 3　オブジェクトのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

内部ホストの NAT（ダイナミック NAT）および外部 Web サーバの NAT（スタティック NAT）

次の例では、プライベート ネットワーク上の内部ユーザが外部にアクセスする場合、このユーザにダイナミック NAT を設定します。また、内部ユーザが外部 Web サーバに接続する場合、この Web サーバのアドレスが内部ネットワークに存在するように見えるアドレスに変換されます（図 5-2 を参照）。

図 5-2　内部のダイナミック NAT、外部 Web サーバのスタティック NAT



ステップ 1　内部アドレスに変換するダイナミック NAT プールのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myNatPool
hostname(config-network-object)# range 209.165.201.20 209.165.201.30
```

ステップ 2　内部ネットワークのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myInsNet
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

ステップ 3　内部ネットワークのダイナミック NAT をイネーブルにします。

```
hostname(config-network-object)# nat (inside,outside) dynamic myNatPool
```

ステップ 4　外部 Web サーバのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myWebServ
```

ステップ 5　Web サーバのアドレスを定義します。

```
hostname(config-network-object)# host 209.165.201.12
```

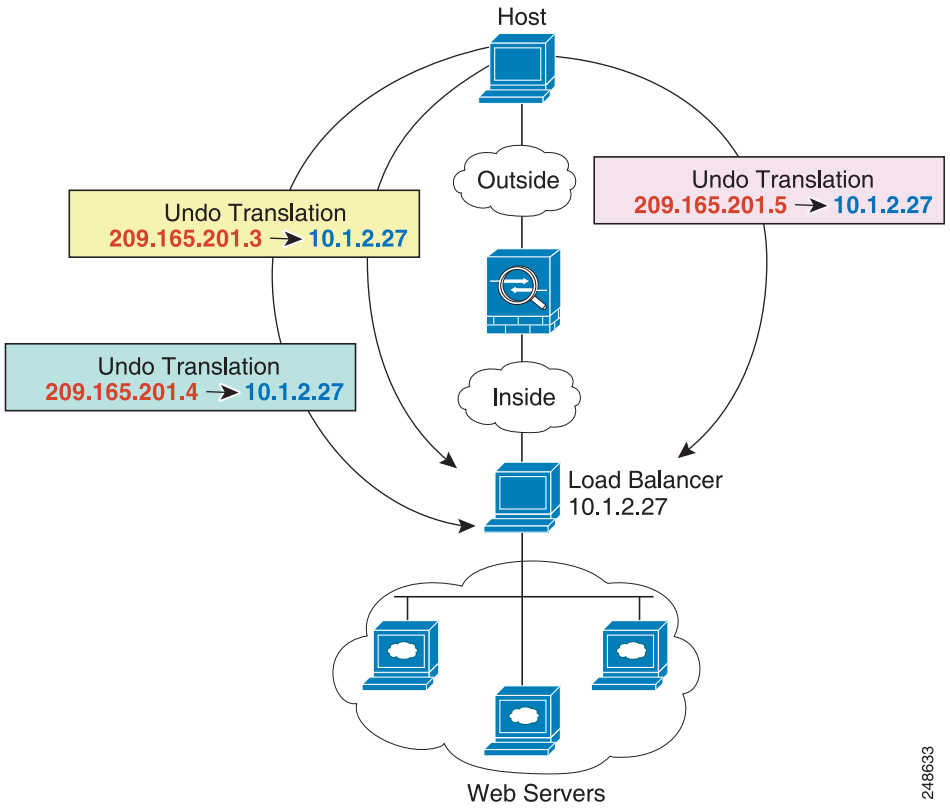
ステップ 6　Web サーバのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.20
```

複数のマッピング アドレス（スタティック NAT、1 対多）を持つ内部ロード バランサ

次の例では、複数の IP アドレスに変換される内部ロード バランサを示しています。外部ホストがマッピング IP アドレスの 1 つにアクセスする場合、1 つのロード バランサのアドレスには変換されません。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします（図 5-3 を参照）。

図 5-3　内部ロード バランサのスタティック NAT（1 対多）



ステップ 1　ロード バランサをマッピングするアドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myPublicIPs
hostname(config-network-object)# range 209.165.201.3 209.265.201.8
```

ステップ 2　ロード バランサのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myLBHost
```

ステップ 3　ロード バランサのアドレスを定義します。

```
hostname(config-network-object)# host 10.1.2.27
```

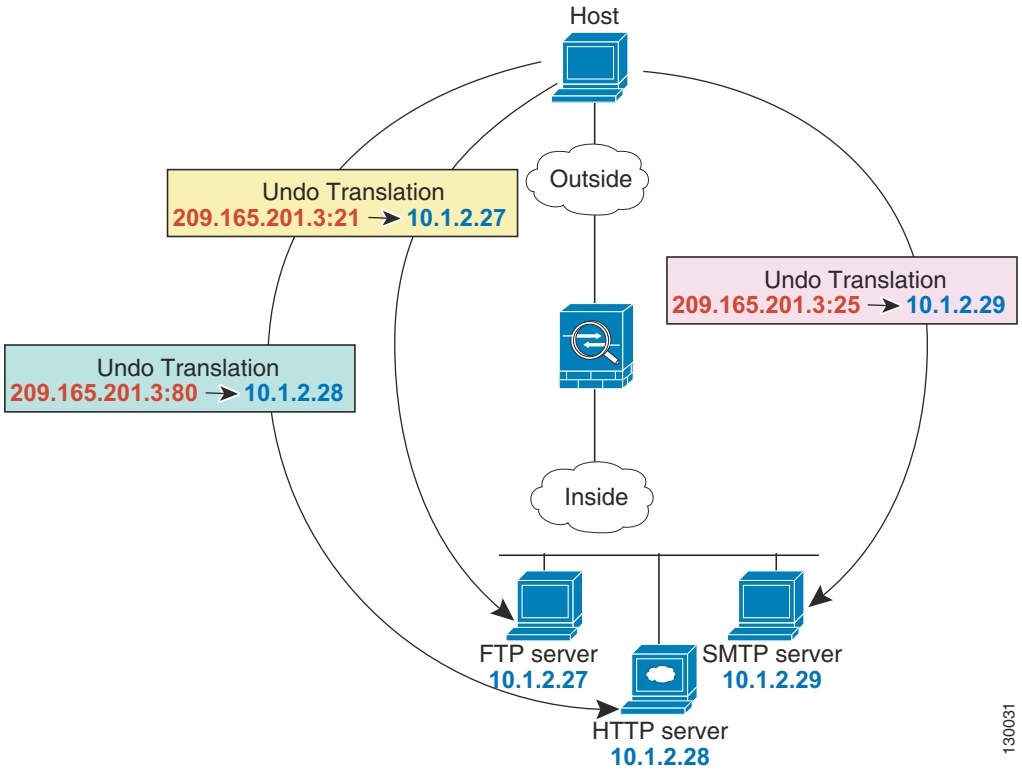
ステップ 4　ロード バランサのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (inside,outside) static myPublicIPs
```

FTP、HTTP、および SMTP のための単一アドレス（ポート変換を設定したスタティック NAT）

次のポート変換を設定したスタティック NAT の例では、リモート ユーザは単一のアドレスで FTP、HTTP、および SMTP にアクセスできるようになります。これらのサーバは実際には、それぞれ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定したスタティック NAT ルールを指定すると、使用するマッピング IP アドレスは同じで、それぞれ別のポートを使用することができます（図 5-4 を参照）。

図 5-4　　ポート変換を設定したスタティック NAT



ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
```

ステップ 2　FTP サーバのアドレスを定義し、アイデンティティ ポート変換を設定したスタティック NAT を FTP サーバに設定します。

```
hostname(config-network-object)# host 10.1.2.27
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp ftp
ftp
```

ステップ 3　HTTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network HTTP_SERVER
```

ステップ 4　HTTP サーバのアドレスを定義し、アイデンティティ ポート変換を設定したスタティック NAT を HTTP サーバに設定します。

```
hostname(config-network-object)# host 10.1.2.28
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp
http http
```

ステップ 5　SMTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network SMTP_SERVER
```

ステップ 6　SMTP サーバのアドレスを定義し、アイデンティティ ポート変換を設定したスタティック NAT を SMTP サーバに設定します。

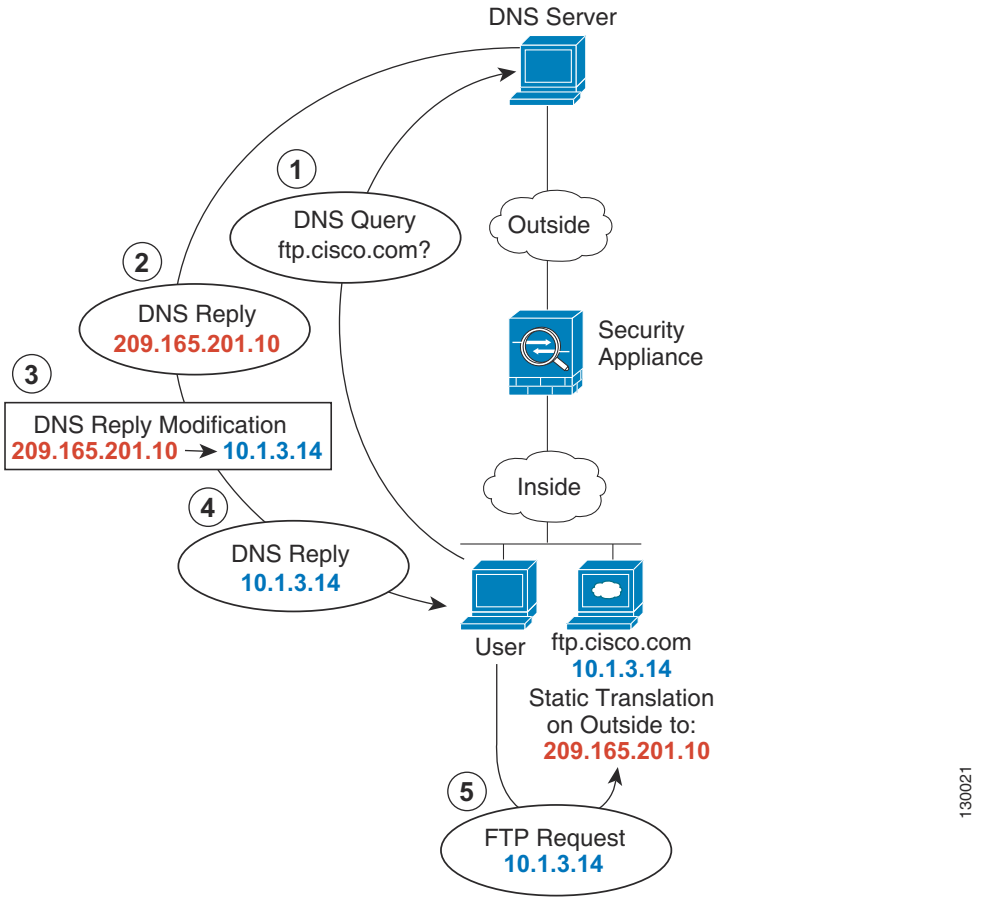
```
hostname(config-network-object)# host 10.1.2.29
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp
smtp smtp
```

マッピング インターフェイス上の DNS サーバ、実際のインターフェイス上の Web サーバ（DNS 修正を設定したスタティック NAT）

たとえば、DNS サーバが外部インターフェイスからアクセス可能であるとします。ftp.cisco.com というサーバが内部インターフェイス上にあります。ftp.cisco.com の実際のアドレス（10.1.3.14）を、外部ネットワーク上で可視のマッピング アドレス（209.165.201.10）にスタティックに変換するように、ASA を設定します（図 5-5 を参照）。この場合、このスタティック ルールで DNS 応答修正をイネーブルにする必要があります。これにより、実際のアドレスを使用して ftp.cisco.com にアクセスすることを許可されている内部ユーザは、マッピング アドレスではなく実際のアドレスを DNS サーバから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバは応答でマッピング アドレス（209.165.201.10）を示します。ASA は、内部サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正をイネーブルにしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックを送信することを試みます。

図 5-5　DNS 応答修正



ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
```

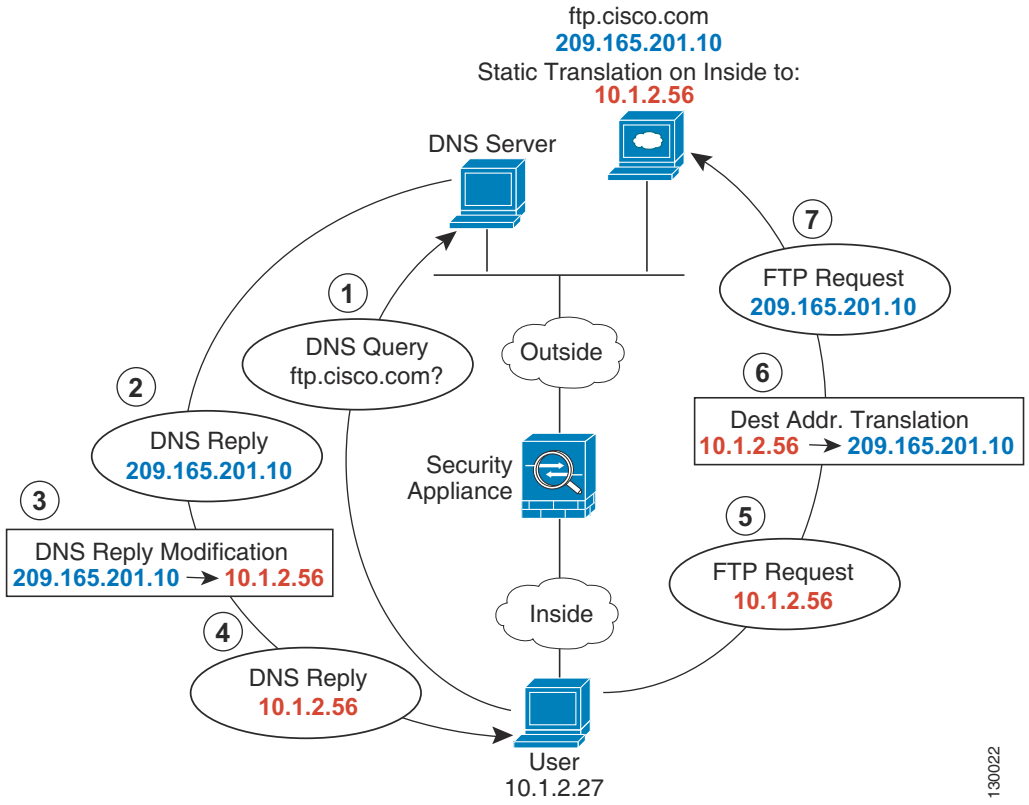
ステップ 2　FTP サーバのアドレスを定義し、DNS 修正を設定したスタティック NAT を設定します。

```
hostname(config-network-object)# host 10.1.3.14
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10 dns
```

マッピング インターフェイス上の DNS サーバおよび FTP サーバ、FTP サーバが変換される（DNS 修正を設定したスタティック NAT）

図 5-6 に、外部の FTP サーバと DNS サーバを示します。ASA には、外部サーバ用のスタティック変換があります。この場合に、内部ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答として実際のアドレス 209.165.201.10 を返します。ftp.cisco.com のマッピング アドレス（10.1.2.56）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。

図 5-6　外部 NAT を使用する DNS 応答修正



ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
```

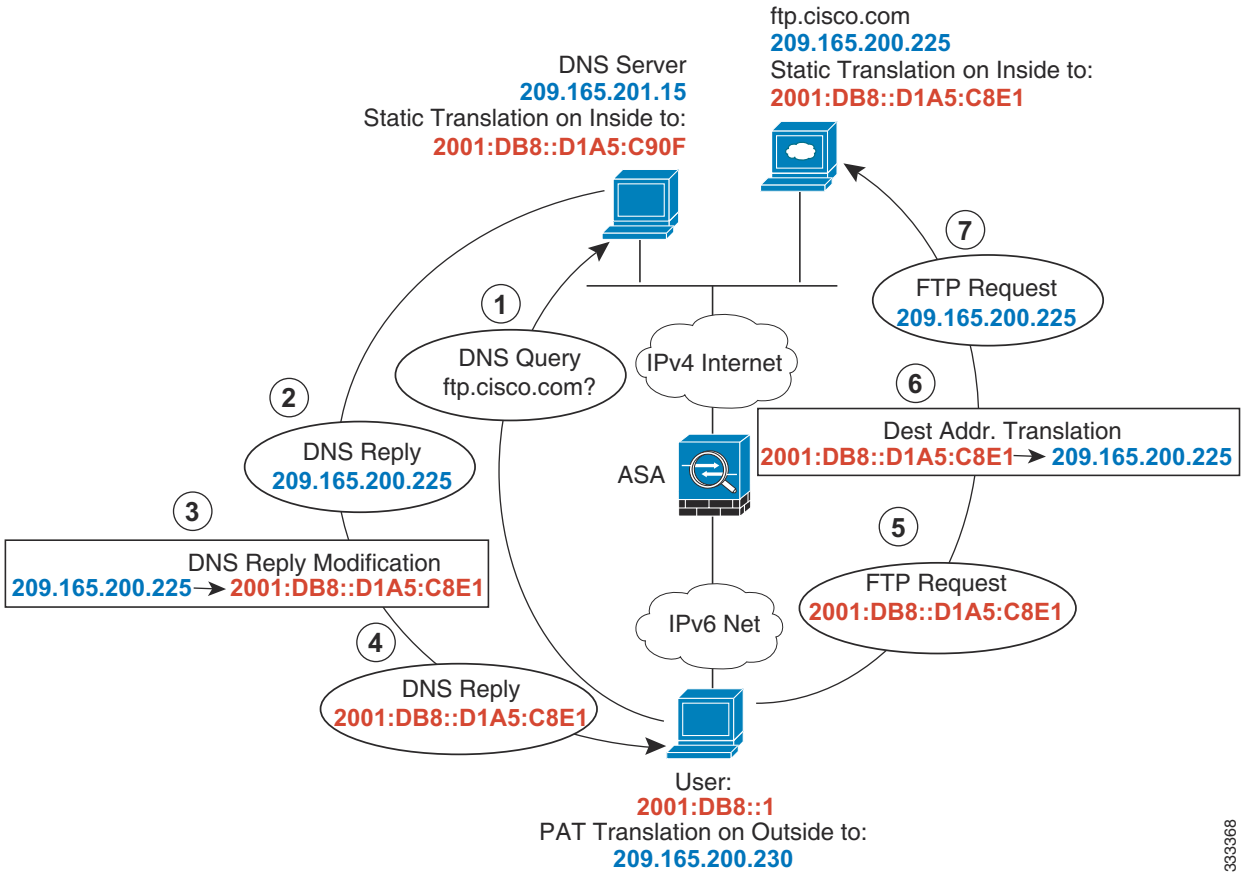
ステップ 2　FTP サーバのアドレスを定義し、DNS 修正を設定したスタティック NAT を設定します。

```
hostname(config-network-object)# host 209.165.201.10
hostname(config-network-object)# nat (outside,inside) static 10.1.2.56 dns
```

マッピング インターフェイス上の IPv4 DNS サーバおよび FTP サーバ、実際のインターフェイス上の IPv6 ホスト（DNS64 修正を設定したスタティック NAT64）

図 5-7 に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。ASA には、外部サーバ用のスタティック変換があります。この場合に、内部 IPv6 ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答として実際のアドレス 209.165.200.225 を返します。ftp.cisco.com のマッピング アドレス（2001:DB8::D1A5:C8E1）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。この例には、DNS サーバのスタティック NAT 変換、および内部 IPv6 ホストの PAT ルールも含まれています。

図 5-7　外部 NAT を使用する DNS 応答修正



ステップ 1　FTP サーバのための、DNS 修正を設定したスタティック NAT を設定します。

a. FTP サーバ アドレスのためのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
```

b. FTP サーバのアドレスを定義し、DNS 修正を設定したスタティック NAT を設定します。これは 1 対 1 変換であるため、NAT46 に対して net-to-net 方式を設定します。

```
hostname(config-network-object)# host 209.165.200.225
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C8E1/128
net-to-net dns
```

ステップ 2　DNS サーバの NAT を設定します。

a. DNS サーバ アドレスのためのネットワーク オブジェクトを作成します。

```
hostname(config)# object network DNS_SERVER
```

b. DNS サーバのアドレスを定義し、net-to-net 方式を使用してスタティック NAT を設定します。

```
hostname(config-network-object)# host 209.165.201.15
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C90F/128
net-to-net
```

ステップ 3　内部 IPv6 ネットワークを変換するための IPv4 PAT プールを設定します。

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 203.0.113.1 203.0.113.254
```

ステップ 4　内部 IPv6 ネットワークのための PAT を設定します。

a. 内部 IPv6 ネットワークのためのネットワーク オブジェクトを作成します。

```
hostname(config)# object network IPv6_INSIDE
```

b. IPv6 ネットワーク アドレスを定義し、PAT プールを使用するダイナミック NAT を設定します。

```
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

ネットワーク オブジェクト NAT の機能履歴

表 5-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 5-1　ネットワーク オブジェクト NAT の機能履歴

機能名	プラットフォーム リリース	機能情報
ネットワーク オブジェクト NAT	8.3(1)	ネットワーク オブジェクトの IP アドレスの NAT を設定します。 **nat**（オブジェクト ネットワーク コンフィギュレーション モード）、**show nat**、**show xlate**、**show nat pool** コマンドが導入または変更されました。
アイデンティティ NAT の設定が可能なプロキシ ARP およびルート ルックアップ	8.4(2)/8.5(1)	アイデンティティ NAT の以前のリリースでは、プロキシ ARP はディセーブルにされ、出力インターフェイスの決定には常にルート ルックアップが使用されていました。これらを設定することはできませんでした。8.4(2) 以降、アイデンティティ NAT のデフォルト動作は他のスタティック NAT コンフィギュレーションの動作に一致するように変更されました。これにより、デフォルトでプロキシ ARP はイネーブルにされ、NAT コンフィギュレーションにより出力インターフェイスが決定されるようになりました（指定されている場合）。これらの設定をそのまま残すこともできますし、個別にイネーブルまたはディセーブルにすることもできます。通常のスタティック NAT のプロキシ ARP をディセーブルにすることもできるようになっています。 8.3(1)、8.3(2)、8.4(1) から 8.4(2) にアップグレードすると、既存機能を保持するため、すべてのアイデンティティ NAT コンフィギュレーションに **no-proxy-arp** キーワードと **route-lookup** キーワードが含まれるようになっています。 **nat static** [**no-proxy-arp**] [**route-lookup**] コマンドが変更されました。
PAT プールおよびラウンド ロビン アドレス割り当て	8.4(2)/8.5(1)	1 つのアドレスの代わりに、PAT アドレスのプールを指定できるようになりました。また、オプションで、PAT アドレスのすべてのポートを使用してからプール内の次のアドレスを使用するのではなく、PAT アドレスのラウンドロビン割り当てをイネーブルにすることもできます。これらの機能は、1 つの PAT アドレスで多数の接続を行っている場合にそれが DoS 攻撃の対象となることを防止するのに役立ちます。またこの機能により、多数の PAT アドレスを簡単に設定できます。 **nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]] コマンドが変更されました。

表 5-1　ネットワーク オブジェクト NAT の機能履歴（続き）

機能名	プラットフォームリリース	機能情報
ラウンドロビン PAT プール割り当てで、既存のホストの同じ IP アドレスを使用する	8.4(3)	ラウンドロビン割り当てで PAT プールを使用するときに、ホストに既存の接続がある場合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT IP アドレスが使用されます。 変更されたコマンドはありません。 *この機能は、8.5(1) または 8.6(1) では使用できません。*
PAT プールの PAT ポートのフラットな範囲	8.4(3)	使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートには、小さい PAT プールのみがあります。 下位ポート範囲を使用するトラフィックが数多くある場合は、PAT プールを使用するときに、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。1024 ～ 65535 または 1 ～ 65535 です。 **nat dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]] コマンドが変更されました。 *この機能は、8.5(1) または 8.6(1) では使用できません。*
PAT プールの拡張 PAT	8.4(3)	各 PAT IP アドレスでは、最大 65535 個のポートを使用できます。65535 個のポートで変換が不十分な場合は、PAT プールに対して拡張 PAT をイネーブルにすることができます。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、*サービス*ごとに 65535 個のポートが使用されます。 **nat dynamic** [**pat-pool** *mapped_object* [**extended**]] コマンドが変更されました。 *この機能は、8.5(1) または 8.6(1) では使用できません。*

表 5-1　ネットワーク オブジェクト NAT の機能履歴（続き）

機能名	プラットフォーム リリース	機能情報
VPN ピアのローカル IP アドレスを変換してピアの実際の IP アドレスに戻す自動 NAT ルール	8.4(3)	まれに、内部ネットワークで、割り当てられたローカル IP アドレスではなく、VPN ピアの実際の IP アドレスを使用する場合があります。VPN では通常、内部ネットワークにアクセスするために、割り当てられたローカル IP アドレスがピアに指定されます。ただし、内部サーバおよびネットワーク セキュリティがピアの実際の IP アドレスに基づく場合などに、ローカル IP アドレスを変換してピアの実際のパブリック IP アドレスに戻す場合があります。 この機能は、トンネル グループごとに 1 つのインターフェイスでイネーブルにすることができます。VPN セッションが確立または切断されると、オブジェクト NAT ルールが動的に追加および削除されます。ルールは **show nat** コマンドを使用して表示できます。 **（注）** ルーティングの問題のため、この機能が必要でない場合は、この機能の使用は推奨しません。ご使用のネットワークとの機能の互換性を確認するには、Cisco TAC にお問い合わせください。次の制限事項を確認してください。 • Cisco IPsec および AnyConnect クライアントのみがサポートされます。 • NAT ポリシーおよび VPN ポリシーが適用されるように、パブリック IP アドレスへのリターン トラフィックは ASA にルーティングされる必要があります。 • ロードバランシングはサポートされません（ルーティングの問題のため）。 • ローミング（パブリック IP 変更）はサポートされません。 **nat-assigned-to-public-ip** *interface* コマンド（トンネル グループ一般属性コンフィギュレーション モード）が導入されました。
IPv6 用の NAT のサポート	9.0(1)	NAT が IPv6 トラフィックをサポートするようになり、IPv4 と IPv6 の間の変換もサポートされます。IPv4 と IPv6 の間の変換は、トランスペアレント モードではサポートされません。 **nat**（オブジェクト ネットワーク コンフィギュレーション モード）、**show nat**、**show nat pool**、**show xlate** の各コマンドが変更されました。

表 5-1　ネットワーク オブジェクト NAT の機能履歴（続き）

機能名	プラットフォーム リリース	機能情報
逆引き DNS ルックアップ用の NAT のサポート	9.0(1)	NAT ルールがイネーブルにされた DNS インスペクションを使用する IPv4 NAT、IPv6 NAT、および NAT64 を使用する場合、NAT は逆引き DNS ルックアップ用の DNS PTR レコードの変換をサポートするようになりました。
Per-Session PAT	9.0(1)	Per-session PAT 機能によって PAT のスケーラビリティが向上し、クラスタリングの場合に各メンバ ユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、マスター ユニットに転送してマスター ユニットを所有者とする必要があります。Per-Session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンド ノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。「ヒットエンドラン」トラフィック、たとえば HTTP や HTTPS の場合は、Per-Session 機能によって、1 アドレスでサポートされる接続率が大幅に増加することがあります。Per-session 機能を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。Per-session 機能を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/平均ライフタイムです。 デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-session PAT xlate を使用します。Multi-Session PAT を必要とするトラフィック、たとえば H.323、SIP、Skinny に対して Per-session PAT をディセーブルにするには、Per-session 拒否ルールを作成します。 **xlate per-session**、**show nat pool** の各コマンドが導入されました。

Twice NAT

Twice NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。この章では、Twice NAT を設定する方法について説明します。

（注） NAT の機能の詳細については、第 4 章「ネットワーク アドレス変換（NAT）」を参照してください。

Twice NAT に関する情報

Twice NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、たとえば送信元アドレスが宛先 X に向かう場合は A に変換され、宛先 Y に向かう場合は B に変換されるように指定できます。

（注） スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。たとえば、ポート アドレス変換を使用するスタティック NAT を設定し、送信元アドレスを Telnet サーバとして指定する場合に、Telnet サーバに向かうすべてのトラフィックのポートを 2323 から 23 に変換するには、このコマンドで、変換する *送信元*ポート（実際：23、マッピング：2323）を指定する必要があります。Telnet サーバ アドレスを送信元アドレスとして指定しているため、その送信元ポートを指定します。

宛先アドレスはオプションです。宛先アドレスを指定する場合、宛先アドレスを自身にマッピングするか（アイデンティティ NAT）、別のアドレスにマッピングできます。宛先マッピングは、常にスタティック マッピングです。

Twice NAT では、ポート変換が設定されたスタティック NAT のサービス オブジェクトも使用できます。ネットワーク オブジェクト NAT は、インライン定義だけを受け入れます。

Twice NAT とネットワーク オブジェクト NAT の違いの詳細については、「NAT の実装方法」（P.4-15）を参照してください。

Twice NAT ルールは、NAT ルール テーブルのセクション 1 に追加されます。指定した場合には、セクション 3 に追加されます。NAT の順序の詳細については、「NAT ルールの順序」（P.4-20）を参照してください。

Twice NAT のライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

Twice NAT の前提条件

- 実際のアドレスとマッピング アドレスの両方について、ネットワーク オブジェクトまたはネットワーク オブジェクト グループを設定します（**object network** コマンドまたは **object-group network** コマンド）。ネットワーク オブジェクト グループは、非連続的な IP アドレスの範囲または複数のホストやサブネットで構成されるマッピング アドレスを作成する場合に特に便利です。ネットワーク オブジェクトまたはグループを作成するには、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。
- ポート変換を設定したスタティック NAT の場合、TCP または UDP サービス オブジェクトを設定します（**object service** コマンド）。サービス オブジェクトを作成するには、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。

オブジェクトおよびグループに関する特定のガイドラインについては、設定する NAT タイプの設定の項を参照してください。「ガイドラインと制限事項」（P.6-2）も参照してください。

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。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

- ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。
- トランスペアレント モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定する必要があります。**any** は使用できません。
- トランスペアレント モードでは、インターフェイス PAT を設定できません。トランスペアレント モードのインターフェイスには、IP アドレスが設定されていないためです。管理 IP アドレスもマッピング アドレスとして使用できません。
- トランスペアレント モードでは、IPv4 ネットワークと IPv6 ネットワークとの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。

IPv6 のガイドライン

- IPv6 をサポートします。
- ルーテッド モードの場合は、IPv4 と IPv6 との間の変換もできます。
- トランスペアレント モードの場合は、IPv4 ネットワークと IPv6 ネットワークとの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。
- トランスペアレント モードの場合は、PAT プールは IPv6 に対してはサポートされません。
- スタティック NAT の場合は、/64 までの IPv6 サブネットを指定できます。これよりも大きいサブネットはサポートされません。
- FTP を NAT46 とともに使用する場合は、IPv4 FTP クライアントが IPv6 FTP サーバに接続するときに、クライアントは拡張パッシブ モード（EPSV）または拡張ポート モード（EPRT）を使用する必要があります。PASV コマンドおよび PORT コマンドは IPv6 ではサポートされません。

その他のガイドライン

- 送信元 IP アドレスがサブネットの場合、FTP 宛先ポート変換を設定できません（セカンダリ接続を使用するその他のアプリケーションも同様）。FTP データ チャネルの確立に失敗します。たとえば、次のような設定は機能しません。

```
object network MyInsNet
 subnet 10.1.2.0 255.255.255.0
object network MapInsNet
 subnet 209.165.202.128 255.255.255.224
object network Server1
 host 209.165.200.225
object network Server1_mapped
 host 10.1.2.67
object service REAL_ftp
 service tcp destination eq ftp
object service MAPPED_ftp
 service tcp destination eq 2021
object network MyOutNet
 subnet 209.165.201.0 255.255.255.224

nat (inside,outside) source static MyInsNet MapInsNet destination static
Server1_mapped Server1 service MAPPED_ftp REAL_ftp
```

- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待機せずに新しい NAT 情報を使用する必要がある場合は、**clear xlate** コマンドを使用して変換テーブルを消去できます。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

（注）　ダイナミック NAT または PAT ルールを削除し、次に削除したルールに含まれるアドレスと重複するマッピング アドレスを含む新しいルールを追加すると、新しいルールは、削除されたルールに関連付けられたすべての接続がタイムアウトするか、**clear xlate** コマンドを使用してクリアされるまで使用されません。この予防手段のおかげで、同じアドレスが複数のホストに割り当てられないようにできます。

- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。
- NAT ルールで **any** キーワードを使用する場合、「any」トラフィック（IPv4 と IPv6）は、ルールによって異なります。ASA がパケットに対して NAT を実行する前に、パケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件では、ASA は、NAT ルールの **any** の値を決定できます。たとえば、「any」から IPv6 サーバへのルールを設定しており、このサーバが IPv4 アドレスからマッピングされている場合、**any** は「任意の IPv6 トラフィック」を意味します。「any」から「any」へのルールを設定しており、送信元をインターフェイス IPv4 アドレスにマッピングする場合、マッピングされたインターフェイス アドレスによって宛先も IPv4 であることが示されるため、**any** は「任意の IPv4 トラフィック」を意味します。
- NAT で使用されるオブジェクトおよびオブジェクト グループを未定義にすることはできません。IP アドレスを含める必要があります。
- 同じオブジェクトを複数のルールで使用できます。
- マッピング IP アドレス プールは、次のアドレスを含むことができません。
  - マッピング インターフェイスの IP アドレス。ルールに **any** インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT（ルーテッド モードのみ）の場合、IP アドレスの代わりに **interface** キーワードを使用します。
  - （トランスペアレント モード）管理 IP アドレス。
  - （ダイナミック NAT）VPN がイネーブルの場合は、スタンバイ インターフェイスの IP アドレス。
  - 既存の VPN プールのアドレス。
- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- NAT のトランザクション コミット モデルを使用すると、システムのパフォーマンスと信頼性を向上させることができます。詳細については、一般的な操作のコンフィギュレーション ガイドの基本設定の章を参照してください。**asp rule-engine transactional-commit nat** コマンドを使用します。

デフォルト設定

- デフォルトでは、NAT テーブルのセクション 1 の最後にルールが追加されます。
- （ルーテッド モード）デフォルトの実際のインターフェイスおよびマッピング インターフェイスは Any で、すべてのインターフェイスにルールが適用されます。
- オプションのインターフェイスを指定する場合、ASA によって NAT コンフィギュレーションが使用されて、出力インターフェイスが決定されますが、代わりにルート ルックアップを常に使用するオプションがあります。

Twice NAT の設定

この項では、Twice NAT の設定方法について説明します。

- 「実際のアドレスおよびマッピング アドレスのネットワーク オブジェクトの追加」（P.6-5）
- 「（任意）実際のポートとマッピング ポートのサービス オブジェクトの追加」（P.6-7）
- 「ダイナミック NAT の設定」（P.6-9）
- 「ダイナミック PAT（隠蔽）の設定」（P.6-13）
- 「スタティック NAT またはポート変換を設定したスタティック NAT の設定」（P.6-19）
- 「アイデンティティ NAT の設定」（P.6-23）
- 「Per-Session PAT ルールの設定」（P.6-26）

実際のアドレスおよびマッピング アドレスのネットワーク オブジェクトの追加

NAT ルールごとに、次に関するネットワーク オブジェクトまたはグループを 4 つまで設定します。

- **送信元の実際のアドレス**
- **送信元のマッピング アドレス**
- **宛先の実際のアドレス**
- **宛先のマッピング アドレス**

すべてのトラフィックを表す **any** キーワード インライン、または一部のタイプの NAT の場合はインターフェイス アドレスを表す **interface** キーワードを指定しない場合は、オブジェクトが必要です。ネットワーク オブジェクトまたはグループの設定の詳細については、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。

ガイドライン

- 1 つのネットワーク オブジェクト グループには、IPv4 アドレスと IPv6 アドレスのいずれか一方のオブジェクトやインライン アドレスを入れることができます。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。
- 拒否されるマッピング IP アドレスについては、「ガイドラインと制限事項」（P.6-2）を参照してください。

- 送信元ダイナミック NAT：
  - 通常は、実際のアドレスの大きいグループが小さいグループにマッピングされるように設定します。
  - マッピングされたオブジェクトまたはグループには、サブネットを含めることはできません。オブジェクトは、範囲を定義する必要があります。グループには、ホストと範囲を含めることができます。
  - マッピングされたネットワーク オブジェクトに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォール バックとして使用されます。
- 送信元ダイナミック PAT（隠蔽）：
  - マッピングされたオブジェクトまたはグループには、サブネットを含めることはできません。ネットワーク オブジェクトはホスト、または PAT プールの場合は範囲を定義する必要があります。ネットワーク オブジェクト グループ（PAT プール用）には、ホストと範囲を含めることができます。
- 送信元スタティック NAT またはポート変換を設定したスタティック NAT：
  - マッピングされたオブジェクトまたはグループには、ホスト、範囲、またはサブネットを含めることができます。
  - スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、「スタティック NAT」（P.4-3）を参照してください。
- 送信元アイデンティティ NAT
  - 実際のオブジェクトおよびマッピングされたオブジェクトが一致する必要があります。両方に同じオブジェクトを使用することも、同じ IP アドレスが含まれる個別のオブジェクトを作成することもできます。
- 宛先スタティック NAT またはポート変換を設定したスタティック NAT（宛先の変換は常にスタティックです）：
  - Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定する場合は、このアドレスにスタティック変換を設定するか、単にアイデンティティ NAT に使用します。宛先アドレスを使用せずに Twice NAT を設定して、実際のアドレスに対するネットワーク オブジェクト グループの使用または手動でのルールの順序付けを含む、Twice NAT の他の特質の一部を活用することができます。詳細については、「ネットワーク オブジェクトと Twice NAT の主な違い」（P.4-15）を参照してください。
  - アイデンティティ NAT では、実際のオブジェクトおよびマッピングされたオブジェクトが一致する必要があります。両方に同じオブジェクトを使用することも、同じ IP アドレスが含まれる個別のオブジェクトを作成することもできます。
  - スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、「スタティック NAT」（P.4-3）を参照してください。
  - ポート変換（ルーテッド モードのみ）が設定されたスタティック インターフェイス NAT では、マッピング アドレスのネットワーク オブジェクト/グループではなく、**interface** キーワードを指定できます。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.4-6）を参照してください。

手順の詳細

コマンド	目的

object network *obj_name*
{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*}
 	
例：
`hostname(config)# object network MyInsNet`
`hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0`
	ネットワーク オブジェクト（IPv4 または IPv6）を追加します。

object-group network *grp_name*
{**network-object** {**object** *net_obj_name* | *subnet_address netmask* | **host** *ip_address*} | **group-object** *grp_obj_name*}
 	
例：
`hostname(config)# object network TEST`
`hostname(config-network-object)# range 10.1.1.1 10.1.1.70`
 	
`hostname(config)# object network TEST2`
`hostname(config-network-object)# range 10.1.2.1 10.1.2.70`
 	
`hostname(config-network-object)# object-group network MAPPED_IPS`
`hostname(config-network)# network-object object TEST`
`hostname(config-network)# network-object object TEST2`
`hostname(config-network)# network-object host 10.1.2.79`
	ネットワーク オブジェクト グループ（IPv4 または IPv6）を追加します。

（任意）実際のポートとマッピング ポートのサービス オブジェクトの追加

次のポートのサービス オブジェクトを設定します。

- 送信元の実際のポート（スタティックのみ）*または*宛先の実際のポート
- 送信元のマッピング ポート（スタティックのみ）*または*宛先のマッピング ポート

サービス オブジェクトの設定の詳細については、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。

ガイドライン

- NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。
- 「not equal（等しくない）」（**neq**）演算子はサポートされていません。

- アイデンティティ ポート変換では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。
- 送信元ダイナミック NAT：送信元ダイナミック NAT では、ポート変換はサポートされません。
- 送信元ダイナミック PAT（隠蔽）：送信元ダイナミック PAT では、ポート変換はサポートされません。
- 送信元スタティック NAT またはポート変換を設定したスタティック NAT：サービス オブジェクトには、送信元ポートと宛先ポートの両方を含めることができます。ただし、両方のサービス オブジェクトに、送信元ポート *または*宛先ポートの*いずれか*を指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバなど）に送信元ポートおよび宛先ポートの*両方*を指定する必要がありますが、固定の送信元ポートはめったに使用されません。たとえば、送信元ホストのポートを変換する場合は、送信元サービスを設定します。
- 送信元アイデンティティ NAT：サービス オブジェクトには、送信元ポートと宛先ポートの両方を含めることができます。ただし、両方のサービス オブジェクトに、送信元ポート *または*宛先ポートの*いずれか*を指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバなど）に送信元ポートおよび宛先ポートの*両方*を指定する必要がありますが、固定の送信元ポートはめったに使用されません。たとえば、送信元ホストのポートを変換する場合は、送信元サービスを設定します。
- 宛先スタティック NAT またはポート変換を設定したスタティック NAT（宛先の変換は常にスタティックです）：非スタティックな送信元 NAT では、宛先でのみポート変換を実行できます。サービス オブジェクトには送信元ポートと宛先ポートの両方を含めることができますが、この場合は、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。

手順の詳細

	コマンド	目的

ステップ 1	**object service** *obj_name*
	　service {**tcp** | **udp**} [**source** *operator port*] [**destination** *operator port*]
	
	例：
	`hostname(config)# object service REAL_SRC_SVC`
	`hostname(config-service-object)# service tcp source eq 80`
	
	`hostname(config)# object service MAPPED_SRC_SVC`
	`hostname(config-service-object)# service tcp source eq 8080`
		サービス オブジェクトを追加します。

ダイナミック NAT の設定

この項では、ダイナミック NAT の Twice NAT を設定する方法について説明します。詳細については、「ダイナミック NAT」（P.4-8）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	次のネットワーク オブジェクトまたはグループを作成します。 • 送信元の実際のアドレス • 送信元のマッピング アドレス • 宛先の実際のアドレス • 宛先のマッピング アドレス	「実際のアドレスおよびマッピングアドレスのネットワーク オブジェクトの追加」（P.6-5）を参照してください。 すべての送信元トラフィックを変換する場合、送信元の実際のアドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **any** キーワードを指定できます。 ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。
ステップ 2	（任意）次のサービス オブジェクトを作成します。 • 宛先の実際のポート • 宛先のマッピング ポート	「（任意）実際のポートとマッピング ポートのサービス オブジェクトの追加」（P.6-7）を参照してください。

	コマンド	目的
ステップ 3	**nat** [**(***real_ifc*,*mapped_ifc***)**] [*line* | {**after-auto** [*line*]}] **source dynamic** {*real_obj* | **any**} {*mapped_obj* [**interface** [**ipv6**]]} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *mapped_dest_svc_obj real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**] [**description** *desc*] **例：** hostname(config)# nat (inside,outside) source dynamic MyInsNet NAT_POOL destination static Server1_mapped Server1 service MAPPED_SVC REAL_SVC	**ダイナミック NAT** を設定します。次のガイドラインを参照してください。 • インターフェイス：（トランスペアレント モードの場合に必須）実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。インターフェイスの 1 つまたは両方に **any** キーワードを指定することもできます。 • セクションおよび行：（任意）デフォルトでは、NAT ルールは、NAT テーブルのセクション 1 の末尾に追加されます（「NAT ルールの順序」（P.4-20）を参照）。セクション 1 ではなく、セクション 3（ネットワーク オブジェクト NAT ルールの後ろ）にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。 • 送信元アドレス： – 実際のアドレス：ネットワーク オブジェクト、グループ、または **any** キーワードを指定します。 – マッピング アドレス：異なるネットワーク オブジェクトまたはグループを指定します。必要に応じて、次のフォールバック方式を設定できます。 インターフェイス PAT のフォール バック：（ルーテッド モードのみ）**interface** キーワードは、インターフェイス PAT のフォール バックをイネーブルにします。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。マッピング IP アドレスを使い果たすと、続いてマッピング インターフェイスの IP アドレスが使用されます。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。

コマンド	目的
	（続き） • 宛先アドレス（任意）： – マッピング アドレス：ネットワーク オブジェクトまたはグループを指定します。ポート変換が設定されたスタティック インターフェイス NAT に限り、**interface** キーワードを指定します。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。**interface** を指定する場合は、必ず **service** キーワードも設定します。このオプションでは、*real_ifc* に特定のインターフェイスを設定する必要があります。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.4-6）を参照してください。 – 実際のアドレス：ネットワーク オブジェクトまたはグループを指定します。アイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。 • 宛先ポート：（任意）マッピングされたサービス オブジェクトおよび実際のサービス オブジェクトとともに、**service** キーワードを指定します。アイデンティティ ポート変換では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用します。 • DNS：（オプション、送信元にのみ適用されるルール）**dns** キーワードは DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。宛先アドレスを設定する場合、**dns** キーワードは設定できません。詳細については、「DNS および NAT」（P.4-33）を参照してください。 • 単方向：（任意）宛先アドレスが送信元アドレスへのトラフィックを開始できないようにするには、**unidirectional** を指定します。 • 非アクティブ：（任意）コマンドを削除する必要がなく、このルールを非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。 • 説明：（オプション）**description** キーワードを使用して、最大 200 文字の説明を入力します。

例

次に、209.165.201.1/27 ネットワークのサーバおよび 203.0.113.0/24 ネットワークのサーバにアクセスする場合の内部ネットワーク 10.1.1.0/24 のダイナミック NAT を設定する例を示します。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1 destination
static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2 destination
static SERVERS_2 SERVERS_2
```

次に、IPv4 209.165.201.1/27 ネットワークのサーバおよび 203.0.113.0/24 ネットワークのサーバにアクセスする場合の IPv6 内部ネットワーク 2001:DB8:AAAA::/96 のダイナミック NAT を設定する例を示します。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1 destination
static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2 destination
static SERVERS_2 SERVERS_2
```

ダイナミック PAT（隠蔽）の設定

この項では、ダイナミック PAT（隠蔽）の Twice NAT の設定方法について説明します。詳細については、「ダイナミック PAT」（P.4-10）を参照してください。

ガイドライン

PAT プールの場合：

- 使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。したがって、1024 未満のポートに使用できるのは、小さな PAT プール 1 つだけです。（8.4(3) 以降、ただし 8.5(1) と 8.6(1) を除く）下位ポート範囲を使用するトラフィックが数多くある場合は、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます（1024 ～ 65535、または 1 ～ 65535）。
- 同じ PAT プール オブジェクトを 2 つの異なるルールの中で使用する場合は、必ず同じオプションを各ルールに指定してください。たとえば、1 つのルールで拡張 PAT およびフラットな範囲が指定される場合は、もう一方のルールでも拡張 PAT およびフラットな範囲が指定される必要があります。

PAT プールに対する拡張 PAT の場合：

- 多くのアプリケーション インスペクションでは、拡張 PAT はサポートされていません。サポート対象外のインスペクションの完全な一覧については、第 7 章「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」の「デフォルト インスペクションと NAT に関する制限事項」（P.7-6）を参照してください。
- ダイナミック PAT ルールに対して拡張 PAT をイネーブルにする場合は、PAT プール内のアドレスを、ポート変換ルールを設定した別のスタティック NAT の PAT アドレスとしても使用することはできません。たとえば、PAT プールに 10.1.1.1 が含まれている場合、PAT アドレスとして 10.1.1.1 を使用する、ポート変換ルールを設定したスタティック NAT は作成できません。
- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。
- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。

PAT プールのラウンドロビンの場合：

- ホストに既存の接続がある場合は、そのホストからの以降の接続は同じ PAT IP アドレスを使用します（ポートが使用可能である場合）。**注**：この「粘着性」は、フェールオーバーが発生すると失われます。ASA がフェールオーバーすると、ホストからの後続の接続では最初の IP アドレスが使用されない場合があります。
- ラウンドロビンでは、特に拡張 PAT と組み合わせた場合に、大量のメモリが消費されます。NAT プールはマッピングされるプロトコル/IP アドレス/ポート範囲ごとに作成されるため、ラウンドロビンでは数多くの同時 NAT プールが作成され、メモリが使用されます。拡張 PAT では、さらに多くの同時 NAT プールが作成されます。

手順の詳細

	コマンド	目的
ステップ 1	次のネットワーク オブジェクトまたはグループを作成します。 • 送信元の実際のアドレス • 送信元のマッピング アドレス • 宛先の実際のアドレス • 宛先のマッピング アドレス	「実際のアドレスおよびマッピング アドレスのネットワーク オブジェクトの追加」（P.6-5）を参照してください。 すべての送信元トラフィックを変換する場合、送信元の実際のアドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **any** キーワードを指定できます。 インターフェイス アドレスをマッピング アドレスとして使用する場合は、送信元のマッピング アドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。 ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。
ステップ 2	（任意）次のサービス オブジェクトを作成します。 • 宛先の実際のポート • 宛先のマッピング ポート	「（任意）実際のポートとマッピング ポートのサービス オブジェクトの追加」（P.6-7）を参照してください。

	コマンド	目的
ステップ 3	**nat** [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-auto** [*line*]}] **source dynamic** {*real-obj* | **any**} {*mapped_obj* [**interface** [**ipv6**]] | [**pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] [**interface** [**ipv6**]] | **interface** [**ipv6**]} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *mapped_dest_svc_obj real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**] [**description** *desc*] **例：** `hostname(config)# nat (inside,outside) source dynamic MyInsNet interface destination static Server1 Server1 description Interface PAT for inside addresses when going to server 1`	**ダイナミック PAT（隠蔽）**を設定します。次のガイドラインを参照してください。 • インターフェイス：（トランスペアレント モードの場合に必須）実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。インターフェイスの 1 つまたは両方に **any** キーワードを指定することもできます。 • セクションおよび行：（任意）デフォルトでは、NAT ルールは、NAT テーブルのセクション 1 の末尾に追加されます（「NAT ルールの順序」（P.4-20）を参照）。セクション 1 ではなく、セクション 3（ネットワーク オブジェクト NAT ルールの後ろ）にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。 • 送信元アドレス： – 実際のアドレス：ネットワーク オブジェクト、グループ、または **any** キーワードを指定します。すべてのトラフィックについて実際のインターフェイスからマッピング インターフェイスに変換する場合は、**any** キーワードを使用します。 – マッピング：次のいずれかを設定します。 - ネットワーク オブジェクト：ホスト アドレスを含むネットワーク オブジェクトを指定します。 - **pat-pool** : **pat-pool** キーワードおよびネットワーク オブジェクトまたは複数のアドレスを含むグループを指定します。 - **interface**：（ルーテッド モードのみ）インターフェイス PAT だけを使用するように **interface** キーワードを単独で指定します。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。PAT プールまたはネットワーク オブジェクトと一緒に指定した場合、**interface** キーワードは、インターフェイス PAT のフォール バックをイネーブルにします。PAT IP アドレスを使い果たすと、マッピング インターフェイスの IP アドレスが使用されます。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。 （続き）

コマンド	目的
	（続き） PAT プールについて、次のオプションの 1 つ以上を指定できます。 -- ラウンド ロビン：**round-robin** キーワードは、PAT プールのラウンド ロビン アドレス割り当てをイネーブルにします。ラウンド ロビンを指定しなければ、デフォルトで PAT アドレスのすべてのポートは次の PAT アドレスが使用される前に割り当てられます。ラウンドロビン方式では、最初のアドレスに戻って再び使用される前に、2 番目のアドレス、またその次と、プール内の各 PAT アドレスからアドレス/ポートが割り当てられます。 -- 拡張 PAT：**extended** キーワードは、拡張 PAT をイネーブルにします。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、*サービス*ごとに 65535 個のポートが使用されます。通常は、PAT 変換を作成するときに宛先ポートとアドレスは考慮されないため、PAT アドレスごとに 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。 -- フラットな範囲：**flat** キーワードは、ポートの割り当て時に 1024 ～ 65535 のポート範囲全体の使用をイネーブルにします。変換のマッピング ポート番号を選択するときに、ASA によって、使用可能な場合は実際の送信元ポート番号が使用されます。ただし、このオプションを設定しないと、実際のポートが使用 *できない* 場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、**include-reserve** キーワードも指定します。 （続き）

コマンド	目的
	（続き） • 宛先アドレス（任意）： – マッピング アドレス：ネットワーク オブジェクトまたはグループを指定します。ポート変換を設定したスタティック インターフェイス NAT に限り（ルーテッド モード）、**interface** キーワードを指定します。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。**interface** を指定する場合は、必ず **service** キーワードも設定します。このオプションでは、*real_ifc* に特定のインターフェイスを設定する必要があります。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.4-6）を参照してください。 – 実際のアドレス：ネットワーク オブジェクトまたはグループを指定します。アイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。 • 宛先ポート：（任意）実際のサービス オブジェクトおよびマッピングされたサービス オブジェクトとともに、**service** キーワードを指定します。アイデンティティ ポート変換では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用します。 • DNS：（オプション、送信元にのみ適用されるルール）**dns** キーワードは DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。**宛先**アドレスを設定する場合、**dns** キーワードは設定できません。詳細については、「DNS および NAT」（P.4-33）を参照してください。 • 単方向：（任意）宛先アドレスが送信元アドレスへのトラフィックを開始できないようにするには、**unidirectional** を指定します。 • 非アクティブ：（任意）コマンドを削除する必要がなく、このルールを非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。 • 説明：（任意）**description** キーワードを使用して、最大 200 文字の説明を入力します。

例

次に、外部 Telnet サーバ 209.165.201.23 へのアクセス時に内部ネットワーク 192.168.1.0/24 のインターフェイス PAT を設定し、203.0.113.0/24 ネットワーク上のサーバへのアクセス時に PAT プールを使用してダイナミック PAT を設定する例を示します。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 209.165.201.23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface destination
static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

次に、外部 IPv6 Telnet サーバ 2001:DB8::23 へのアクセス時に内部ネットワーク 192.168.1.0/24 のインターフェイス PAT を設定し、2001:DB8:AAAA::/96 ネットワーク上のサーバへのアクセス時に PAT プールを使用してダイナミック PAT を設定する例を示します。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 2001:DB8:AAAA::1 2001:DB8:AAAA::200

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 2001:DB8::23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface ipv6 destination
static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

スタティック NAT またはポート変換を設定したスタティック NAT の設定

この項では、Twice NAT を使用してスタティック NAT ルールを設定する方法について説明します。スタティック NAT の詳細については、「スタティック NAT」（P.4-3）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	次のネットワーク オブジェクトまたはグループを作成します。 • 送信元の実際のアドレス • 送信元のマッピング アドレス • 宛先の実際のアドレス • 宛先のマッピング アドレス	「実際のアドレスおよびマッピング アドレスのネットワーク オブジェクトの追加」（P.6-5）を参照してください。 ポート変換を設定した送信元のスタティック インターフェイス NAT のみを設定する場合は、送信元のマッピング アドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。 ポート変換を設定した宛先のスタティックインターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。
ステップ 2	（任意）次のサービス オブジェクトを作成します。 • 送信元 *または* 宛先の実際のポート • 送信元 *または* 宛先のマッピング ポート	「（任意）実際のポートとマッピング ポートのサービス オブジェクトの追加」（P.6-7）を参照してください。

	コマンド	目的
ステップ 3	**nat** [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-object** [*line*]}] **source static** *real_ob* [*mapped_obj* | **interface** [**ipv6**]] [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj*][**net-to-net**] [**dns**] [**unidirectional** | **no-proxy-arp**] [**inactive**] [**description** *desc*] **例：** `hostname(config)# nat (inside,dmz) source static MyInsNet MyInsNet_mapped destination static Server1 Server1 service REAL_SRC_SVC MAPPED_SRC_SVC`	**スタティック NAT** を設定します。次のガイドラインを参照してください。 • インターフェイス：（トランスペアレント モードの場合に必須）実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。インターフェイスの 1 つまたは両方に **any** キーワードを指定することもできます。 • セクションおよび行：（任意）デフォルトでは、NAT ルールは、NAT テーブルのセクション 1 の末尾に追加されます。セクションの詳細については、「NAT ルールの順序」（P.4-20）を参照してください。セクション 1 ではなく、セクション 3（ネットワーク オブジェクト NAT ルールの後ろ）にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。 • 送信元アドレス： – 実際のアドレス：ネットワーク オブジェクトまたはグループを指定します。 – マッピング アドレス：異なるネットワーク オブジェクトまたはグループを指定します。ポート変換を設定したスタティック インターフェイス NAT に限り、**interface** キーワードを指定できます（ルーテッド モードのみ）。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。**interface** を指定する場合、**service** キーワードも設定します（この場合、サービス オブジェクトは送信元ポートだけを含む必要があります）。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.4-6）を参照してください。 • 宛先アドレス（任意）： – マッピング アドレス：ネットワーク オブジェクトまたはグループを指定します。ポート変換が設定されたスタティック インターフェイス NAT に限り、**interface** キーワードを指定します。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。**interface** を指定する場合、必ず **service** キーワードも設定します（この場合、サービス オブジェクトは宛先ポートだけを含む必要があります）。このオプションでは、*real_ifc* に特定のインターフェイスを設定する必要があります。 – 実際のアドレス：ネットワーク オブジェクトまたはグループを指定します。アイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。

コマンド	目的
	（続き） • ポート：（任意）実際のサービス オブジェクトおよびマッピングされたサービス オブジェクトとともに、**service** キーワードを指定します。送信元ポート変換の場合、オブジェクトは送信元サービスを指定する必要があります。送信元ポート変換のコマンド内のサービス オブジェクトの順序は、**service** *real_obj mapped_obj* です。宛先ポート変換の場合、オブジェクトは宛先サービスを指定する必要があります。宛先ポート変換のサービス オブジェクトの順序は、**service** *mapped_obj real_obj* です。オブジェクトで送信元ポートと宛先ポートの両方を指定することはほとんどありませんが、この場合には、最初のサービス オブジェクトに実際の送信元ポート/マッピングされた宛先ポートが含まれます。2 つめのサービス オブジェクトには、マッピングされた送信元ポート/実際の宛先ポートが含まれます。アイデンティティ ポート変換の場合は、実際のポートとマッピング ポートの両方（コンフィギュレーションに応じて、送信元ポート、宛先ポート、またはその両方）に同じサービス オブジェクトを使用するだけです。 • ネットツーネット：（任意）NAT 46 の場合は、**net-to-net** を指定すると、最初の IPv4 アドレスが最初の IPv6 アドレスに、2 番目が 2 番目に、というように変換されます。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このキーワードを使用する必要があります。 • DNS：（オプション、送信元にのみ適用されるルール）**dns** キーワードは DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。**宛先**アドレスを設定する場合、**dns** キーワードは設定できません。詳細については、「DNS および NAT」（P.4-33）を参照してください。 • 単方向：（任意）宛先アドレスが送信元アドレスへのトラフィックを開始できないようにするには、**unidirectional** を指定します。 • No Proxy ARP：（任意）マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。詳細については、「マッピング アドレスとルーティング」（P.4-22）を参照してください。 • 非アクティブ：（任意）コマンドを削除する必要がなく、このルールを非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。 • 説明：（任意）**description** キーワードを使用して、最大 200 文字の説明を入力します。

例

次に、ポート変換を設定したスタティック インターフェイス NAT の使用例を示します。外部にあるホストが、宛先ポート 65000 ～ 65004 を指定して外部インターフェイス IP アドレスに接続することにより、内部にある FTP サーバにアクセスします。トラフィックは、192.168.10.100:6500 ～ :65004 の内部 FTP サーバに変換されません。コマンドで指定した送信元アドレスとポートを変換するため、サービス オブジェクトには送信元ポート範囲（宛先ポートではなく）を指定することに注意してください。宛先ポートは「any」です。スタティック NAT は双方向であるため、「送信元」および「宛先」を使用して一次的にコマンド キーワードを扱うものであり、パケット内の実際の送信元および実際の宛先のアドレスとポートは、パケットを送信するホストによって異なります。この例では、外部から内部への接続が発生しているため、FTP サーバの「送信元」アドレスとポートは、実際には発信元パケット内では宛先アドレスとポートになります。

```
hostname(config)# object service FTP_PASV_PORT_RANGE
hostname(config-service-object)# service tcp source range 65000 65004

hostname(config)# object network HOST_FTP_SERVER
hostname(config-network-object)# host 192.168.10.100

hostname(config)# nat (inside,outside) source static HOST_FTP_SERVER interface service
FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE
```

次に、IPv6 ネットワークへのアクセス時のある IPv6 から別の IPv6 へのスタティック変換、および IPv4 ネットワークへのアクセス時の IPv4 PAT プールへのダイナミック PAT 変換の例を示します。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:BBBB::/96

hostname(config)# object network OUTSIDE_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:CCCC::/96

hostname(config)# object network OUTSIDE_IPv4_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_IPv4_POOL
hostname(config-network-object)# range 10.1.2.1 10.1.2.254

hostname(config)# nat (inside,outside) source static INSIDE_NW MAPPED_IPv6_NW destination
static OUTSIDE_IPv6_NW OUTSIDE_IPv6_NW
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool MAPPED_IPv4_POOL
destination static OUTSIDE_IPv4_NW OUTSIDE_IPv4_NW
```

アイデンティティ NAT の設定

この項では、Twice NAT を使用してアイデンティティ NAT ルールを設定する方法について説明します。アイデンティティ NAT の詳細については、「アイデンティティ NAT」（P.4-12）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	次のネットワーク オブジェクトまたはグループを作成します。 • 送信元の実際のアドレス（通常、送信元のマッピング アドレスと同じオブジェクトを使用します） • 宛先の実際のアドレス • 宛先のマッピング アドレス	「実際のアドレスおよびマッピング アドレスのネットワーク オブジェクトの追加」（P.6-5）を参照してください。 すべてのアドレスに対してアイデンティティ NAT を実行する場合、送信元の実際のアドレスのオブジェクトの作成をスキップして、代わりに、**nat** コマンドで **any any** キーワードを使用できます。 ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。
ステップ 2	（任意）次のサービス オブジェクトを作成します。 • *送信元*または宛先の実際のポート • 送信元 *または*宛先のマッピング ポート	「（任意）実際のポートとマッピング ポートのサービス オブジェクトの追加」（P.6-7）を参照してください。

	コマンド	目的
ステップ 3	**nat** [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-object** [*line*]}] **source static** {*nw_obj nw_obj* | **any any**} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj*] [**no-proxy-arp**] [**route-lookup**] [**inactive**] [**description** *desc*] **例：** `hostname(config)# nat (inside,outside) source static MyInsNet MyInsNet destination static Server1 Server1`	アイデンティティ NAT を設定します。次のガイドラインを参照してください。 • インターフェイス：（トランスペアレント モードの場合に必須）実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。インターフェイスの 1 つまたは両方に **any** キーワードを指定することもできます。 • セクションおよび行：（任意）デフォルトでは、NAT ルールは、NAT テーブルのセクション 1 の末尾に追加されます。セクションの詳細については、「NAT ルールの順序」（P.4-20）を参照してください。セクション 1 ではなく、セクション 3（ネットワーク オブジェクト NAT ルールの後ろ）にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。 • 送信元アドレス：実際のアドレスとマッピング アドレスの両方にネットワーク オブジェクト、グループ、または **any** キーワードを指定します。 • 宛先アドレス（任意）： – マッピング アドレス：ネットワーク オブジェクトまたはグループを指定します。ポート変換が設定されたスタティック インターフェイス NAT に限り、**interface** キーワードを指定します（ルーテッド モードのみ）。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。**interface** を指定する場合、必ず **service** キーワードも設定します（この場合、サービス オブジェクトは宛先ポートだけを含む必要があります）。このオプションでは、*real_ifc* に特定のインターフェイスを設定する必要があります。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.4-6）を参照してください。 – 実際のアドレス：ネットワーク オブジェクトまたはグループを指定します。アイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。

コマンド	目的
	（続き） • ポート：（任意）実際のサービス オブジェクトおよびマッピングされたサービス オブジェクトとともに、**service** キーワードを指定します。送信元ポート変換の場合、オブジェクトは送信元サービスを指定する必要があります。送信元ポート変換のコマンド内のサービス オブジェクトの順序は、**service** *real_obj mapped_obj* です。宛先ポート変換の場合、オブジェクトは宛先サービスを指定する必要があります。宛先ポート変換のサービス オブジェクトの順序は、**service** *mapped_obj real_obj* です。オブジェクトで送信元ポートと宛先ポートの両方を指定することはほとんどありませんが、この場合には、最初のサービス オブジェクトに実際の送信元ポート/マッピングされた宛先ポートが含まれます。2 つめのサービス オブジェクトには、マッピングされた送信元ポート/実際の宛先ポートが含まれます。アイデンティティ ポート変換の場合は、実際のポートとマッピング ポートの両方（コンフィギュレーションに応じて、送信元ポート、宛先ポート、またはその両方）に同じサービス オブジェクトを使用するだけです。 • No Proxy ARP：（任意）マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。詳細については、「マッピング アドレスとルーティング」（P.4-22）を参照してください。 • ルート ルックアップ：（オプション、ルーテッド モードのみ、インターフェイスを指定）NAT コマンドに指定したインターフェイスを使用する代わりに、ルート ルックアップを使用して出力インターフェイスを決定するには、**route-lookup** を指定します。詳細については、「出力インターフェイスの決定」（P.4-26）を参照してください。 • 非アクティブ：（任意）コマンドを削除する必要がなく、このルールを非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。 • 説明：（任意）**description** キーワードを使用して、最大 200 文字の説明を入力します。

Per-Session PAT ルールの設定

デフォルトでは、すべての TCP PAT トラフィックおよびすべての UDP DNS トラフィックが Per-Session PAT を使用します。トラフィックに Multi-Session PAT を使用するには、Per-Session PAT ルールを設定します。許可ルールで Per-Session PAT を使用し、拒否ルールで Multi-Session PAT を使用します。Per-Session PAT と Multi-Session PAT の詳細については、「Per-Session PAT と Multi-Session PAT」（P.4-11）を参照してください。

手順の詳細

Per-Session PAT ルールを設定するには、「Per-Session PAT ルールの設定」（P.5-17）を参照してください。

Twice NAT のモニタリング

Twice NAT をモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
show nat	各 NAT ルールのヒットを含む NAT の統計情報を表示します。
show nat pool	割り当てられたアドレスとホスト、および割り当て回数を含む、NAT プールの統計情報を表示します。
show xlate	現在の NAT セッション情報を表示します。
show nat divert-table	すべての NAT ルールは、NAT 転換テーブルにエントリを構築します。照合ルールにおいて [NAT divert] フィールドが ignore=yes に設定されている場合、ASA は検索を停止し、宛先 IP に基づいてルート ルックアップを行い、出力インターフェイスを決定します。照合ルールにおいて [NAT divert] フィールドが ignore=no に設定されている場合、検出された input_ifc および output_ifc に基づいて NAT テーブルを進み、必要な変換を行います。出力インターフェイスは output_ifc です。

Twice NAT の設定例

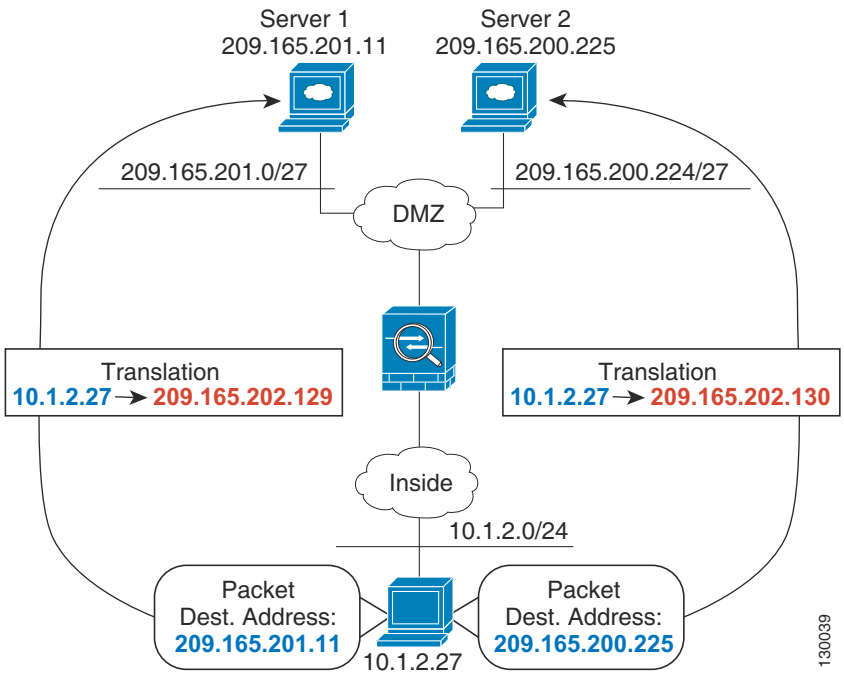
ここでは、次の設定例を示します。

- 「宛先に応じて異なる変換（ダイナミック PAT）」（P.6-27）
- 「宛先アドレスおよびポートに応じて異なる変換（ダイナミック PAT）」（P.6-28）

宛先に応じて異なる変換（ダイナミック PAT）

図 6-1 に、2 台の異なるサーバにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129:*port* に変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130:*port* に変換されます。

図 6-1　異なる宛先アドレスを使用する Twice NAT



ステップ 1　内部ネットワークのネットワーク オブジェクトを追加します。

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

ステップ 2　DMZ ネットワーク 1 のネットワーク オブジェクトを追加します。

```
hostname(config)# object network DMZnetwork1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224
```

ステップ 3　PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

ステップ 4　最初の Twice NAT ルールを設定します。

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1 destination
static DMZnetwork1 DMZnetwork1
```

宛先アドレスは変換しないため、実際の宛先アドレスとマッピング宛先アドレスの両方に同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。

デフォルトでは、NAT ルールは NAT テーブルのセクション 1 の末尾に追加されます。NAT ルールのセクションおよび行番号の指定の詳細については、「ダイナミック PAT（隠蔽）の設定」（P.6-13）を参照してください。

ステップ 5　DMZ ネットワーク 2 のネットワーク オブジェクトを追加します。

```
hostname(config)# object network DMZnetwork2
hostname(config-network-object)# subnet 209.165.200.224 255.255.255.224
```

ステップ 6　PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

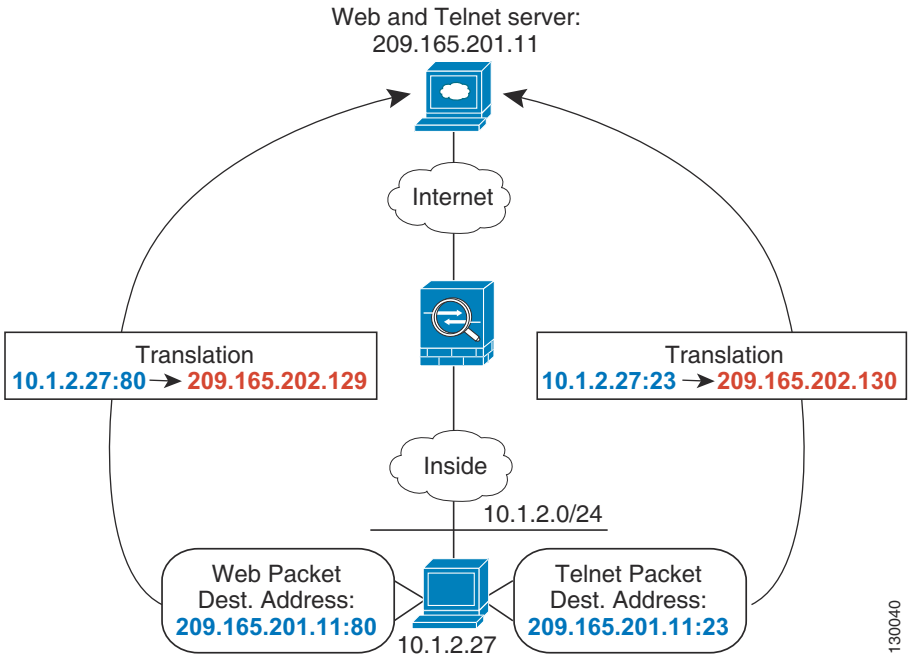
ステップ 7　2 つめの Twice NAT ルールを設定します。

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2 destination
static DMZnetwork2 DMZnetwork2
```

宛先アドレスおよびポートに応じて異なる変換（ダイナミック PAT）

図 6-2 に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Telnet サービスを求めてサーバにアクセスすると、実際のアドレスは 209.165.202.129:*port* に変換されます。ホストが Web サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130:*port* に変換されます。

図 6-2　異なる宛先ポートを使用する Twice NAT



ステップ 1　内部ネットワークのネットワーク オブジェクトを追加します。

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

ステップ 2　Telnet/Web サーバのネットワーク オブジェクトを追加します。

```
hostname(config)# object network TelnetWebServer
hostname(config-network-object)# host 209.165.201.11
```

ステップ 3　Telnet を使用するときの PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

ステップ 4　Telnet のサービス オブジェクトを追加します。

```
hostname(config)# object service TelnetObj
hostname(config-network-object)# service tcp destination eq telnet
```

ステップ 5　最初の Twice NAT ルールを設定します。

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1
destination static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
```

宛先アドレスまたはポートを変換しないため、実際の宛先アドレスとマッピング宛先アドレスに同じアドレスを指定し、実際のサービスとマッピング サービスに同じポートを指定することによって、アイデンティティ NAT を設定する必要があります。

デフォルトでは、NAT ルールは NAT テーブルのセクション 1 の末尾に追加されます。NAT ルールのセクションおよび行番号の指定の詳細については、「ダイナミック PAT（隠蔽）の設定」（P.6-13）を参照してください。

ステップ 6　HTTP を使用するときの PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

ステップ 7　HTTP のサービス オブジェクトを追加します。

```
hostname(config)# object service HTTPObj
hostname(config-network-object)# service tcp destination eq http
```

ステップ 8　2 つめの Twice NAT ルールを設定します。

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress2
destination static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```

Twice NAT の機能履歴

表 6-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 6-1　Twice NAT の機能履歴

機能名	プラットフォーム リリース	機能情報
Twice NAT	8.3(1)	Twice NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。 **nat**、**show nat**、**show xlate**、**show nat pool** コマンドが変更または導入されました。
アイデンティティ NAT の設定が可能なプロキシ ARP およびルート ルックアップ	8.4(2)/8.5(1)	アイデンティティ NAT の以前のリリースでは、プロキシ ARP はディセーブルにされ、出力インターフェイスの決定には常にルート ルックアップが使用されていました。これらを設定することはできませんでした。8.4(2) 以降、アイデンティティ NAT のデフォルト動作は他のスタティック NAT コンフィギュレーションの動作に一致するように変更されました。これにより、デフォルトでプロキシ ARP はイネーブルにされ、NAT コンフィギュレーションにより出力インターフェイスが決定されるようになりました（指定されている場合）。これらの設定をそのまま残すこともできますし、個別にイネーブルまたはディセーブルにすることもできます。通常のスタティック NAT のプロキシ ARP をディセーブルにすることもできるようになっています。 8.3 よりも前の設定の場合、8.4(2) 以降への NAT 免除ルール（**nat 0 access-list** コマンド）の移行には、プロキシ ARP をディセーブルにするキーワード **no-proxy-arp** およびルート ルックアップを使用するキーワード **route-lookup** があります。8.3(2) および 8.4(1) への移行に使用された **unidirectional** キーワードは、移行に使用されなくなりました。8.3(1)、8.3(2)、8.4(1) から 8.4(2) にアップグレードすると、既存機能を保持するため、すべてのアイデンティティ NAT コンフィギュレーションに **no-proxy-arp** キーワードと **route-lookup** キーワードが含まれるようになっています。**unidirectional** キーワードは削除されました。 **nat source static** [**no-proxy-arp**] [**route-lookup**] コマンドが変更されました。

表 6-1　Twice NAT の機能履歴（続き）

機能名	プラットフォームリリース	機能情報
PAT プールおよびラウンド ロビン アドレス割り当て	8.4(2)/8.5(1)	1 つのアドレスの代わりに、PAT アドレスのプールを指定できるようになりました。また、オプションで、PAT アドレスのすべてのポートを使用してからプール内の次のアドレスを使用するのではなく、PAT アドレスのラウンドロビン割り当てをイネーブルにすることもできます。これらの機能は、1 つの PAT アドレスで多数の接続を行っている場合にそれが DoS 攻撃の対象となることを防止するのに役立ちます。またこの機能により、多数の PAT アドレスを簡単に設定できます。 **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]] コマンドが変更されました。
ラウンドロビン PAT プール割り当てで、既存のホストの同じ IP アドレスを使用する	8.4(3)	ラウンドロビン割り当てで PAT プールを使用するときに、ホストに既存の接続がある場合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT IP アドレスが使用されます。 変更されたコマンドはありません。 *この機能は、8.5(1) または 8.6(1) では使用できません。*
PAT プールの PAT ポートのフラットな範囲	8.4(3)	使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートには、小さい PAT プールのみがあります。 下位ポート範囲を使用するトラフィックが数多くある場合は、PAT プールを使用するときに、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。1024 ～ 65535 または 1 ～ 65535 です。 **nat source dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]] コマンドが変更されました。 *この機能は、8.5(1) または 8.6(1) では使用できません。*
PAT プールの拡張 PAT	8.4(3)	各 PAT IP アドレスでは、最大 65535 個のポートを使用できます。65535 個のポートで変換が不十分な場合は、PAT プールに対して拡張 PAT をイネーブルにすることができます。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、*サービス*ごとに 65535 個のポートが使用されます。 **nat source dynamic** [**pat-pool** *mapped_object* [**extended**]] コマンドが変更されました。 *この機能は、8.5(1) または 8.6(1) では使用できません。*

表 6-1　Twice NAT の機能履歴（続き）

機能名	プラットフォームリリース	機能情報
VPN ピアのローカル IP アドレスを変換してピアの実際の IP アドレスに戻す自動 NAT ルール	8.4(3)	まれに、内部ネットワークで、割り当てられたローカル IP アドレスではなく、VPN ピアの実際の IP アドレスを使用する場合があります。VPN では通常、内部ネットワークにアクセスするために、割り当てられたローカル IP アドレスがピアに指定されます。ただし、内部サーバおよびネットワーク セキュリティがピアの実際の IP アドレスに基づく場合などに、ローカル IP アドレスを変換してピアの実際のパブリック IP アドレスに戻す場合があります。 この機能は、トンネル グループごとに 1 つのインターフェイスでイネーブルにすることができます。VPN セッションが確立または切断されると、オブジェクト NAT ルールが動的に追加および削除されます。ルールは **show nat** コマンドを使用して表示できます。 **（注）** ルーティングの問題のため、この機能が必要でない場合は、この機能の使用は推奨しません。ご使用のネットワークとの機能の互換性を確認するには、Cisco TAC にお問い合わせください。次の制限事項を確認してください。 • Cisco IPsec および AnyConnect クライアントのみがサポートされます。 • NAT ポリシーおよび VPN ポリシーが適用されるように、パブリック IP アドレスへのリターン トラフィックは ASA にルーティングされる必要があります。 • ロードバランシングはサポートされません（ルーティングの問題のため）。 • ローミング（パブリック IP 変更）はサポートされません。 **nat-assigned-to-public-ip** *interface* コマンド（トンネル グループ一般属性コンフィギュレーション モード）が導入されました。
IPv6 用の NAT のサポート	9.0(1)	NAT が IPv6 トラフィックをサポートするようになり、IPv4 と IPv6 の間の変換もサポートされます。IPv4 と IPv6 の間の変換は、トランスペアレント モードではサポートされません。 **nat**（グローバル コンフィギュレーション モード）、**show nat**、**show nat pool**、**show xlate** コマンドが変更されました。

表 6-1　Twice NAT の機能履歴（続き）

機能名	プラットフォームリリース	機能情報
逆引き DNS ルックアップ用の NAT のサポート	9.0(1)	NAT ルールがイネーブルにされた DNS インスペクションを使用する IPv4 NAT、IPv6 NAT、および NAT64 を使用する場合、NAT は逆引き DNS ルックアップ用の DNS PTR レコードの変換をサポートするようになりました。
Per-Session PAT	9.0(1)	Per-session PAT 機能によって PAT のスケーラビリティが向上し、クラスタリングの場合に各メンバ ユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、マスター ユニットに転送してマスター ユニットを所有者とする必要があります。Per-Session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンド ノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。「ヒットエンドラン」トラフィック、たとえば HTTP や HTTPS の場合は、Per-Session 機能によって、1 アドレスでサポートされる接続率が大幅に増加することがあります。Per-session 機能を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。Per-session 機能を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/平均ライフタイムです。 デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-session PAT xlate を使用します。Multi-Session PAT を必要とするトラフィック、たとえば H.323、SIP、Skinny に対して Per-session PAT をディセーブルにするには、Per-session 拒否ルールを作成します。 **xlate per-session**、**show nat pool** の各コマンドが導入されました。
NAT ルール エンジンのトランザクション コミット モデル	9.3(1)	イネーブルの場合、NAT ルールの更新はルール コンパイルの完了後に適用され、ルール照合のパフォーマンスに影響を及ぼすことはありません。 **asp rule-engine transactional-commit**、**show running-config asp rule-engine transactional-commit**、**clear configure asp rule-engine transactional-commit** の各コマンドに **nat** キーワードが追加されました。

PART 3

アプリケーション インスペクション

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

次のトピックで、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。

アプリケーション レイヤ プロトコル インスペクション

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（高速パスの詳細については、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）。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。

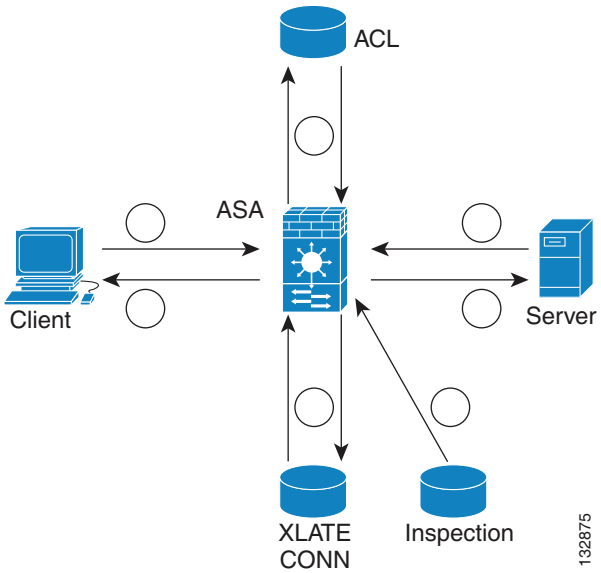
次のトピックで、アプリケーション インスペクションについて詳しく説明します。

インスペクション エンジンの動作

次の図に示すように、ASA は基本動作を行うために 3 つのデータベースを使用します。

- ACL：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許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 7-1　　インスペクション エンジンの動作



この図では、動作の発生順に番号が付けられています。

1. TCP SYN パケットが ASA に到着して、新しい接続を確立します。
2. ASA は ACL 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 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 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 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 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 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 は ACL 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。既知のポートで初期セッションが使用され、動的に割り当てられたポート番号がネゴシエーションされます。

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 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 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 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。

インスペクション ポリシー マップ

*インスペクション ポリシー マップ*を使用して、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。これらのマップはオプションです。インスペクション ポリシー マップをサポートするプロトコルに関しては、マップを設定しなくてもインスペクションをイネーブルにできます。デフォルトのインスペクション アクション以外のことが必要な場合にのみ、これらのマップが必要になります。

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.7-11）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。

- トラフィック照合基準：アプリケーション トラフィックをそのアプリケーションに固有の基準（URL 文字列など）と照合し、その後アクションをイネーブルにできます。

  一部のトラフィック照合基準では、正規表現を使用してパケット内部のテキストを照合します。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：一部のインスペクション ポリシー マップでは、インスペクション クラス マップを使用して複数のトラフィック照合基準を含めることができます。その後、インスペクション ポリシー マップ内でインスペクション クラス マップを指定し、そのクラス全体で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 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、異なる照合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。
- 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。

次のトピックで、詳細に説明します。

- 「使用中のインスペクション ポリシー マップの交換」（P.7-4）
- 「複数のトラフィック クラスの処理方法」（P.7-4）

使用中のインスペクション ポリシー マップの交換

サービス ポリシーですでに使用しているインスペクション ポリシー マップを交換する必要がある場合、次の方法を使用してください。

- 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、**inspect** *protocol map* コマンドを削除し、新しいマップを使用して再度追加します。次に例を示します。

```
hostname(config)# policy-map test
hostname(config-pmap)# class sip
hostname(config-pmap-c)# no inspect sip sip-map1
hostname(config-pmap-c)# inspect sip sip-map2
```

- 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（**policy-map type inspect http**）を変更する場合、変更を有効にするには **inspect http** *map* 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 マップを変更する場合、レイヤ 3/4 ポリシーから **inspect http http-map** コマンドを削除し、再度追加する必要があります。

```
hostname(config)# policy-map test
hostname(config-pmap)# class http
hostname(config-pmap-c)# no inspect http http-map
hostname(config-pmap-c)# inspect http http-map
```

複数のトラフィック クラスの処理方法

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 マップや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 **match** コマンドまたは **class** コマンドと一致する場合、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。たとえば、次の match コマンドは任意の順序で入力できますが、**match request method get** コマンドが最初に照合されます。

```
match request header host length gt 100
  reset
match request method get
  log
```

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、それ以降の照合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 **match** コマンドまたは **class** コマンドと照合される場合は、ポリシー マップ内での順序に従って照合されます。たとえば、ヘッダーの長さが 1001 のパケットの場合は、次に示す最初のコマンドと照合されてログに記録され、それから 2 番目のコマンドと照合されてリセットされます。2 つの **match** コマンドの順序を逆にすると、2 番目の **match** コマンドとの照合前にパケットのドロップと接続のリセットが行われ、ログには記録されません。

```
match request header length gt 100
  log
match request header length gt 1000
  reset
```

クラス マップは、そのクラス マップ内で重要度が最低の **match** コマンド（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 **match** コマンド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 **match** コマンドがある場合、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。各クラス マップの重要度が最低の照合が異なる場合、重要度が高い **match** コマンドを持つクラス マップが最初に照合されます。たとえば、次の 3 つのクラス マップには、**match request-cmd**（高重要度）と **match filename**（低重要度）という 2 つのタイプの **match** コマンドがあります。ftp3 クラス マップには両方のコマンドが含まれていますが、最低重要度のコマンドである **match filename** に従ってランク付けされています。ftp1 クラス マップには最高重要度のコマンドがあるため、ポリシー マップ内での順序に関係なく最初に照合されます。ftp3 クラス マップは ftp2 クラス マップと同じ重要度としてランク付けされており、**match filename** コマンドも含まれています。これらのクラス マップの場合、ポリシー マップ内での順序に従い、ftp3 が照合されてから ftp2 が照合されます。

```
class-map type inspect ftp match-all ftp1
  match request-cmd get
class-map type inspect ftp match-all ftp2
  match filename regex abc
class-map type inspect ftp match-all ftp3
  match request-cmd get
  match filename regex abc

policy-map type inspect ftp ftp
  class ftp3
    log
  class ftp2
    log
  class ftp1
    log
```

アプリケーション インスペクションのガイドライン

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。ステート リンク経由で複製される GTP および SIP は例外です。

IPv6 のガイドライン

IPv6 は次のインスペクションでサポートされています。

- DNS
- FTP
- HTTP
- ICMP
- SCCP（Skinny）
- SIP
- SMTP
- IPSec パススルー
- IPv6

NAT64 は次のインスペクションでサポートされています。

- DNS
- FTP
- HTTP
- ICMP

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 インスペクションと NAT に関する制限事項」（P.7-6）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 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、適応型セキュリティ アプライアンスはシステム 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。スタンバイ装置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。
- ASA（インターフェイス）に送信される TCP/UDP トラフィックはデフォルトで検査されます。ただし、インターフェイスに送信される ICMP トラフィックは、ICMP インスペクションをイネーブルにした場合でも検査されません。したがって、ASA がバックアップ デフォルト ルートを介して到達できる送信元からエコー要求が送信された場合など、特定の状況下では、インターフェイスへの ping（エコー要求）が失敗する可能性があります。

アプリケーション インスペクションのデフォルト

次のトピックで、アプリケーション インスペクションのデフォルトの動作について説明します。

デフォルト インスペクションと NAT に関する制限事項

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。

次の表に、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 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。この表の見方は次のとおりです。

- 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。
- ASA は、これらの指定された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 によってその順序を強制されることはありません。

表 7-1　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	デフォルト ポート	NAT に関する制限事項	標準	注
CTIQBE	TCP/2748	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	—	—
DCERPC	TCP/135	NAT64 なし。	—	—
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	—
FTP	TCP/21	（クラスタリング）スタティック PAT はサポートされません。	RFC 959	—
GTP	UDP/3386 UDP/2123	拡張 PAT はサポートされません。 NAT なし。	—	特別なライセンスが必要です。
H.323 H.225 および **RAS**	TCP/1720 UDP/1718 UDP (RAS) 1718-1719	ダイナミック NAT または PAT はサポートされません。 スタティック PAT は機能しない可能性があります。 （クラスタリング）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。 Per-Session PAT 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。 NAT64 なし。	ITU-T H.323、H.245、H225.0、Q.931、Q.932	—

表 7-1　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	デフォルト ポート	NAT に関する制限事項	標準	注
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	—	—	—	ASA インターフェイスに送信される ICMP トラフィックは検査されません。
ICMP ERROR	—	—	—	—
ILS（LDAP）	TCP/389	拡張 PAT はサポートされません。 NAT64 なし。	—	—
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。 NAT64 なし。	RFC 3860	—
IP オプション	—	NAT64 なし。	RFC 791、RFC 2113	—
IPsec Pass Through	UDP/500	PAT はサポートされません。 NAT64 なし。	—	—
IPv6	—	NAT64 なし。	RFC 2460	—
MGCP	UDP/2427、2727	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック 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。 NAT64 なし。	—	—
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。 NAT64 なし。	—	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	NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	RFC 2637	—
RADIUS アカウンティング	1646	NAT64 なし。	RFC 2865	—

表 7-1　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	デフォルト ポート	NAT に関する制限事項	標準	注
RSH	TCP/514	PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック 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。 NAT64 なし。 （クラスタリング）スタティック PAT 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。
ScanSafe（クラウド Web セキュリティ）	TCP/80 TCP/413	—	—	これらのポートは、ScanSafe インスペクションの default-inspection-traffic クラスには含まれません。
SIP	TCP/5060 UDP/5060	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。 Per-Session PAT はサポートされません。 NAT64 または NAT46 はなし。 （クラスタリング）スタティック PAT はサポートされません。	RFC 2543	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。
SKINNY（SCCP）	TCP/2000	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。 Per-Session PAT はサポートされません。 NAT64、NAT46、または NAT66 はなし。 （クラスタリング）スタティック 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	NAT64 なし。	RFC 821、1123	—

表 7-1　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	デフォルト ポート	NAT に関する制限事項	標準	注
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。 NAT64 なし。 （クラスタリング）スタティック 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。 NAT64 なし。	—	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	NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	RFC 1350	ペイロード IP アドレスは変換されません。
WAAS	TCP/1-65535	拡張 PAT はサポートされません。 NAT64 なし。	—	—
XDMCP	UDP/177	拡張 PAT はサポートされません。 NAT64 なし。 （クラスタリング）スタティック PAT はサポートされません。	—	—

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 client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225 _default_h323_map
  inspect h323 ras _default_h323_map
  inspect ip-options _default_ip_options_map
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp _default_esmtp_map
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

デフォルトのインスペクション ポリシー マップ

一部のインスペクション タイプは、非表示のデフォルト ポリシー マップを使用します。たとえば、マップを指定しないで ESMTP インスペクションをイネーブルにした場合、_default_esmtp_map が使用されます。

デフォルトのインスペクションは、各インスペクション タイプについて説明しているセクションで説明されています。これらのデフォルト マップは、**show running-config all policy-map** コマンドを使用して表示できます。

DNS インスペクションは、明示的に設定されたデフォルト マップ preset_dns_map を使用する唯一のインスペクションです。

アプリケーション レイヤ プロトコル インスペクションの設定

サービス ポリシーにアプリケーション インスペクションを設定します。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 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。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。サービス ポリシーに関する一般的な情報については、第 1 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」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 インスペクションと NAT に関する制限事項」（P.7-6）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

ステップ 1　既存のクラス マップにインスペクションを追加しようとしている場合を除いて、通過トラフィックまたは管理トラフィック向けのレイヤ 3/4 クラス マップでインスペクションを適用したいトラフィックを指定します。

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.1-14）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.1-16）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。

選択するクラス マップに関する重要な関連事項があります。inspection_default クラスにのみ複数のインスペクションを設定できます。また、デフォルトのインスペクションを適用する既存のグローバル ポリシーを編集するだけの場合もあります。選択するクラス マップに関する詳細情報については、「インスペクションの適切なトラフィック クラスの選択」（P.7-17）を参照してください。

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。この手順の後半の表に、インスペクション ポリシー マップを使用できるプロトコルを示します。また、それらの設定手順へのポインタも記載しています。

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 インスペクションと NAT に関する制限事項」（P.7-6）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たいクラス マップを指定します。

```
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、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　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 7-2　　protocol のキーワード

キーワード	注
ctiqbe	「CTIQBE インスペクション」（P.9-1）を参照してください。
dcerpc [*map_name*]	「DCERPC インスペクション」（P.11-1）を参照してください。 「DCERPC インスペクション ポリシー マップの設定」（P.11-2）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*] [**dynamic-filter-snoop**]	「DNS インスペクション」（P.8-1）を参照してください。 「DNS インスペクション ポリシー マップの設定」（P.8-3）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。デフォルトの DNS インスペクション ポリシー マップの名前は「preset_dns_map」です。 ボットネット トラフィック フィルタの DNS スヌーピングをイネーブルにするには、**dynamic-filter-snoop** キーワードを入力します。
esmtp [*map_name*]	「SMTP および拡張 SMTP インスペクション」（P.8-44）を参照してください。 「ESMTP インスペクション ポリシー マップの設定」（P.8-46）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*]]	「FTP インスペクション」（P.8-9）を参照してください。 **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、「厳密な FTP」（P.8-10）を参照してください。 「FTP インスペクション ポリシー マップの設定」（P.8-11）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。
gtp [*map_name*]	「GTP インスペクション」（P.11-5）を参照してください。 「GTP インスペクション ポリシー マップの設定」（P.11-7）に従って GTP 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。

表 7-2　protocol のキーワード（続き）

キーワード	注
h323 h225 [*map_name*]	「H.323 インスペクション」（P.9-3）を参照してください。 「H.323 インスペクション ポリシー マップの設定」（P.9-7）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*]	「H.323 インスペクション」（P.9-3）を参照してください。 「H.323 インスペクション ポリシー マップの設定」（P.9-7）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 [*map_name*]	「HTTP インスペクション」（P.8-16）を参照してください。 「HTTP インスペクション ポリシー マップの設定」（P.8-17）に従って HTTP 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。
icmp	「ICMP インスペクション」（P.8-23）を参照してください。
icmp error	「ICMP エラー インスペクション」（P.8-23）を参照してください。
ils	「ILS インスペクション」（P.10-1）を参照してください。
im [*map_name*]	「インスタント メッセージ インスペクション」（P.8-24）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 ポリシー マップの設定」（P.8-24）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*]	「IP オプション インスペクション」（P.8-29）を参照してください。 「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.8-31）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。
ipsec-pass-thru [*map_name*]	「IPsec パススルー インスペクション」（P.8-33）を参照してください。 「IPsec パススルー インスペクション」（P.8-33）に従って IPsec パススルー 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。

表 7-2　protocol のキーワード（続き）

キーワード	注
ipv6 [*map_name*]	「IPv6 インスペクション」（P.8-36）を参照してください。 「IPv6 インスペクション ポリシー マップの設定」（P.8-37）に従って IPv6 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*]	「MGCP インスペクション」（P.9-13）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 MGCP インスペクション ポリシー マップの設定」（P.9-15）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*]	「NetBIOS インスペクション」（P.8-40）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 NetBIOS インスペクション ポリシー マップの設定」（P.8-41）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	「PPTP インスペクション」（P.8-43）を参照してください。
radius-accounting *map_name*	「RADIUS アカウンティング インスペクション」（P.11-13）を参照してください。 **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。RADIUS アカウンティング インスペクション ポリシー マップを指定する必要があります。「RADIUS アカウンティング インスペクション ポリシー マップの設定」（P.11-14）を参照してください。
rsh	「RSH インスペクション」（P.11-17）を参照してください。
rtsp [*map_name*]	「RTSP インスペクション」（P.9-19）を参照してください。 「RTSP インスペクション ポリシー マップの設定」（P.9-21）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。
scansafe [*map_name*] [**fail-open** | **fail-closed**]	ScanSafe（クラウド Web セキュリティ）をイネーブルにしたい場合、この手順ではなく、「クラウド Web セキュリティにトラフィックを送信するサービス ポリシーの方法」（P.15-11）で説明している手順を使用してください。前述の手順では、ポリシー インスペクション マップの設定方法を含む、完全なポリシー設定について説明しています。

表 7-2　protocol のキーワード（続き）

キーワード	注
sip [*map_name*] [**tls-proxy** *proxy_name*]	「SIP インスペクション」（P.9-25）を参照してください。 「SIP インスペクション ポリシー マップの設定」（P.9-28）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。暗号化されたトラフィックのインスペクションをイネーブルにするには、TLS プロキシを指定します。
skinny [*map_name*] [**tls-proxy** *proxy_name*]	「Skinny（SCCP）検査」（P.9-34）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 Skinny（SCCP）インスペクション ポリシー マップの設定」（P.9-36）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。暗号化されたトラフィックのインスペクションをイネーブルにするには、TLS プロキシを指定します。
snmp [*map_name*]	「SNMP インスペクション」（P.11-17）を参照してください。 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	「SQL*Net インスペクション」（P.10-2）を参照してください。
sunrpc	「Sun RPC インスペクション」（P.10-3）を参照してください。 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	「TFTP インスペクション」（P.8-50）を参照してください。
waas	TCP オプション 33 解析をイネーブルにします。Cisco Wide Area Application Services 製品を導入するときに使用します。
xdmcp	「XDMCP インスペクション」（P.11-19）を参照してください。

（注） 別のインスペクション ポリシー マップを使用するためにデフォルト グローバル ポリシー（または使用中のポリシー）を編集する場合、**no inspect** *protocol* コマンドを使用して古いインスペクションを削除し、新しいインスペクション ポリシー マップ名でインスペクションを再度追加する必要があります。

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 ポリシー マップの「global_policy」は全体的に適用されます。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。

インスペクションの適切なトラフィック クラスの選択

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。このトラフィック クラスは（インスペクションには通常使用されない **match any** とともに）、IPv6 をサポートするインスペクションについて IPv4 および IPv6 トラフィックの両方を照合します。IPv6 がイネーブルなインスペクションのリストについては、「アプリケーション インスペクションのガイドライン」（P.7-5）を参照してください。

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、ACL 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 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 インスペクションと NAT に関する制限事項」（P.7-6）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、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 ACL 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
```

正規表現の設定

正規表現は、テキスト文字列のパターン照合を定義します。一部のプロトコル インスペクション マップでは、正規表現を使用して、URL や特定のヘッダー フィールドのコンテンツなどの文字列に基づいてパケットを照合できます。

- 「正規表現の作成」（P.7-18）
- 「正規表現クラス マップの作成」（P.7-21）

正規表現の作成

正規表現は、ストリングそのものとしてテキスト ストリングと文字どおりに照合することも、*メタ文字*を使用してテキスト ストリングの複数のバリアントと照合することもできます。正規表現を使用して特定のアプリケーション トラフィックの内容と照合できます。たとえば、HTTP パケット内部の URL 文字列と照合できます。

はじめる前に

Ctrl キーを押した状態で **V** キーを押すと、CLI において、疑問符（?）やタブなどの特殊文字をすべてエスケープできます。たとえば、コンフィギュレーションで **d?g** と入力するには、**d[Ctrl+V]?g** とキー入力します。

正規表現をパケットと照合する場合のパフォーマンスへの影響については、コマンド リファレンスの **regex** コマンドを参照してください。一般的に、長い入力文字列と照合したり、多くの正規表現と照合しようとすると、システム パフォーマンスが低下します。

（注） 最適化のために、ASA では、難読化解除された URL が検索されます。難読化解除では、複数のスラッシュ（/）が単一のスラッシュに圧縮されます。通常、「http://」のようなダブル スラッシュが使用される文字列では、代わりに「http:/」を検索してください。

次の表に、特別な意味を持つメタ文字を示します。

表 7-3　　正規表現のメタ文字

文字	説明	注
.	ドット	任意の単一文字と一致します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
(*exp*)	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、**d(o|a)g** は dog および dag に一致しますが、**do|ag** は do および ag に一致します。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、**dog|cat** は、dog または cat に一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。たとえば、**lo?se** は、lse または lose に一致します。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示す修飾子。たとえば、**lo*se** は、lse、lose、loose などに一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示す修飾子。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
{*x*} または {*x*,}	最小繰り返し限定作用素	少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
[*abc*]	文字クラス	カッコ内の任意の文字と一致します。たとえば、**[abc]** は、a、b、または c に一致します。
[^*abc*]	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、**[^abc]** は、a、b、c 以外の任意の文字に一致します。**[^A-Z]** は、大文字のアルファベット文字以外の任意の単一の文字に一致します。
[*a-c*]	文字範囲クラス	範囲内の任意の文字と一致します。**[a-z]** は、任意の小文字のアルファベット文字に一致します。文字と範囲を組み合わせて使用することもできます。**[abcq-z]** および **[a-cq-z]** は、a、b、c、q、r、s、t、u、v、w、x、y、z に一致します。 ダッシュ（-）文字は、角カッコ内の最初の文字または最後の文字である場合にのみリテラルとなります（**[abc-]** や **[-abc]**）。
“”	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、**" test"** は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
\	エスケープ文字	メタ文字とともに使用すると、リテラル文字と一致します。たとえば、**\[** は左角カッコに一致します。

表 7-3　正規表現のメタ文字（続き）

文字	説明	注
char	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	タブ	タブ 0x09 と一致します。
\f	改ページ	フォーム フィード 0x0c と一致します。
\x*NN*	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
NNN	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 040 はスペースを表します。

手順

ステップ 1　正規表現が一致すべきものと一致するかどうかをテストします。

```
hostname(config)# test regex input_text regular_expression
```

input_text 引数は、正規表現を使用して照合する、長さが最大で 201 文字の文字列です。

regular_expression 引数の長さは、最大 100 文字です。

Ctrl+V を使用して、CLI の特殊文字をすべてエスケープします。たとえば、**test regex** コマンドの入力文字にタブを入力するには、**test regex "test[Ctrl+V Tab]" "test\t"** と入力する必要があります。

正規表現が入力テキストと一致する場合は、次のメッセージが表示されます。

```
INFO: Regular expression match succeeded.
```

正規表現が入力テキストと一致しない場合は、次のメッセージが表示されます。

```
INFO: Regular expression match failed.
```

ステップ 2　テスト後に正規表現を追加するには、次のコマンドを入力します。

```
hostname(config)# regex name regular_expression
```

name 引数の長さは、最大 40 文字です。

regular_expression 引数の長さは、最大 100 文字です。

例

次に、インスペクション ポリシー マップで使用する 2 つの正規表現を作成する例を示します。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
```

正規表現クラス マップの作成

正規表現クラス マップは、1 つ以上の正規表現を特定します。正規表現クラス マップは、正規表現オブジェクトを集めているにすぎません。多くの場合、正規表現オブジェクトの代わりに正規表現クラス マップを使用できます。

手順

ステップ 1　正規表現クラス マップを作成します。

```
hostname(config)# class-map type regex match-any class_map_name
hostname(config-cmap)#
```

class_map_name は、最大 40 文字の文字列です。「class-default」という名前は予約されています。すべてのタイプのクラス マップで同じ名前スペースが使用されるため、別のタイプのクラス マップですでに使用されている名前は再度使用できません。

match-any キーワードにより、トラフィックが少なくとも 1 つの正規表現と一致する場合には、そのトラフィックがクラス マップと一致するように指定します。

ステップ 2　（任意）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　正規表現ごとに次のコマンドを入力して、クラス マップに含める正規表現を指定します。

```
hostname(config-cmap)# match regex regex_name
```

例

次に、2 つの正規表現を作成し、これを正規表現クラス マップに追加する例を示します。文字列「example.com」または「example2.com」が含まれる場合は、トラフィックはクラス マップに一致します。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex url_example
hostname(config-cmap)# match regex url_example2
```

アプリケーション インスペクションの履歴

機能名	リリース	説明
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。
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。

基本インターネット プロトコルのインスペクション

ここでは、基本インターネット プロトコルのアプリケーション インスペクションについて説明します。特定のプロトコルに関してインスペクションを使用する必要がある理由、およびインスペクションを適用する全体的な方法については、「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準備」（P.7-1）を参照してください。

DNS インスペクション

ここでは、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。

DNS インスペクションのアクション

DNS 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。DNS インスペクションをカスタマイズして多くのタスクを実行できます。

- DNS レコードを NAT の設定に基づいて変換します。詳細については、「DNS および NAT」（P.4-33）を参照してください。
- メッセージの長さ、ドメイン名の長さ、ラベルの長さを適用します。
- 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存在するかどうかを確認します。
- DNS のヘッダー、タイプ、クラス、その他に基づいてパケットを検査します。

DNS インスペクションのデフォルト

DNS インスペクションは、次のような 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っています。

- 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。

次のデフォルトの DNS インスペクション コマンドを参照してください。

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
! ...
service-policy global_policy global
```

DNS インスペクションの設定

DNS 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。デフォルト以外の処理が必要な場合にのみ設定する必要があります。DNS インスペクションをカスタマイズする場合は、次のプロセスを使用します。

手順

ステップ 1　「DNS インスペクション ポリシー マップの設定」（P.8-3）。

ステップ 2　「DNS インスペクション サービス ポリシーの設定」（P.8-7）。

DNS インスペクション ポリシー マップの設定

デフォルトのインスペクション動作がネットワークにとって十分でない場合、DNS インスペクション ポリシー マップを作成して DNS インスペクション アクションをカスタマイズできます。

トラフィックの一致基準を定義するときに、クラス マップを作成するか、またはポリシー マップに match ステートメントを直接含めることができます。次の手順では、両方の方法について説明します。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　（任意）次の手順に従って、DNS インスペクションのクラス マップを作成します。

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。代わりに、ポリシー マップで **match** コマンドを直接指定できます。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 マップでトラフィックと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ことです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

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 マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシー マップに直接トラフィックを特定する必要があります。

a. 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 type inspect dns [match-all | match-any] class_map_name
hostname(config-cmap)#
```

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。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。match-any キーワードは、トラフィックが少なくとも 1 つの **match** ステートメントと一致したらクラス マップと一致することを指定します。CLI がクラスマップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b. （任意）クラス マップに説明を追加するには、次のコマンドを使用します。

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

string には、クラス マップの説明を 200 文字以内で指定します。

c. 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **header-flag** [**eq**] {*f_name* [*f_name...*] | *f_value*}：DNS フラグと一致します。*f_name* 引数は DNS フラグ名であり、**AA**（権限応答）、**QR**（クエリー）、**RA**（使用できる再帰）、**RD**（必要な再帰）、**TC**（切り捨て）のいずれかです。*f_value* 引数は、0x で始まる 16 ビットの 16 進値です（0x0 ～ 0xffff）。**eq** キーワードは完全一致を指定します（すべて一致）。**eq** キーワードを指定しないと、パケットは指定されているヘッダーの 1 つと一致するだけで十分です（いずれかと一致）。例：**match header-flag AA QR**。
- **match** [**not**] **dns-type** {**eq** {*t_name* | *t_value*} | **range** *t_value1 t_value2*}：DNS タイプと一致します。*t_name* 引数は DNS タイプ名であり、次のいずれかです。**A**（IPv4 アドレス）、**AXFR**（フル ゾーン転送）、**CNAME**（正規の名前）、**IXFR**（増分ゾーン転送）、**NS**（権限ネーム サーバ）、**SOA**（権限ゾーンの開始）、**TSIG**（トランザクション署名）です。*t_value* 引数には、DNS タイプ フィールドの任意の値（0 ～ 65535）を指定します。**range** キーワードは範囲を指定し、**eq** キーワードは完全一致を指定します。例：**match dns-type eq A**。
- **match** [**not**] **dns-class** {**eq** {**in** | *c_value*} | **range** *c_value1 c_value2*}：DNS クラスと一致します。クラスは **in**（インターネットの場合）または *c_value*（DNS クラス フィールドの 0 ～ 65535 の任意の値）です。**range** キーワードは範囲を指定し、**eq** キーワードは完全一致を指定します。例：**match dns-class eq in**。
- **match** [**not**] {**question** | **resource-record** {**answer** | **authority** | **additional**}}：DNS の質問またはリソース レコードと一致します。**question** キーワードは、DNS メッセージの問い合わせ部分を指定します。**resource-record** キーワードは、リソース レコードのセクション **answer**、**authority**、**additional** のいずれかを指定します。例：**match resource-record answer**。
- **match** [**not**] **domain-name regex** {*regex_name* | **class** *class_name*}：DNS メッセージのドメイン名のリストを、指定された正規表現または正規表現クラスに対して照合します。

d. クラス マップ コンフィギュレーション モードを終了するには、「**exit**」と入力します。

ステップ 2　DNS インスペクション ポリシー マップを作成するには、次のコマンドを入力します。

```
hostname(config)# policy-map type inspect dns policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3　（任意）このポリシー マップに説明を追加するには、次のコマンドを使用します。

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

ステップ 4　一致したトラフィックにアクションを適用するには、次の手順を実行します。

a. 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- DNS クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。

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

- DNS クラス マップで説明されている **match** コマンドのいずれかを使用して、ポリシー マップに直接トラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b. 次のコマンドを入力して、一致したトラフィックに対して実行するアクションを指定します。

```
hostname(config-pmap-c)# {drop [log] | drop-connection [log]|
enforce-tsig {[drop] [log]} | mask [log] | log}
```

各 **match** コマンドまたは **class** コマンドですべてのオプションを使用できるわけではありません。使用できる正確なオプションについては、CLI ヘルプまたはコマンド リファレンスを参照してください。

drop キーワードを指定すると、一致するすべてのパケットをドロップします。

drop-connection キーワードを指定すると、パケットをドロップし、接続を閉じます。

mask キーワードを指定すると、パケットの一致部分をマスクします。このアクションは、ヘッダー フラグの照合だけで利用可能です。

log キーワードを指定すると、システム ログ メッセージを送信します。このキーワードは単独で、または他のキーワードのいずれかと一緒に使用できます。

enforce-tsig {**[drop] [log]**} キーワードは、メッセージに TSIG リソース レコードが存在することを強制します。TSIG リソース レコードがないパケットをドロップ、ログ記録、またはドロップしてログ記録できます。ヘッダー フラグ一致の場合、このオプションをマスク アクションと組み合わせて使用できます。それ以外の場合、このアクションと他のアクションを同時に指定することはできません。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、「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.2-4）を参照してください。

次に例を示します。

```
hostname(config)# policy-map type inspect dns dns-map
hostname(config-pmap)# class dns-class-map
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match header-flag eq aa
hostname(config-pmap-c)# drop log
```

ステップ 5　インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a. パラメータ コンフィギュレーション モードに入るには、次のコマンドを入力します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **dns-guard**：DNS ガードをイネーブルにします。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。

- **id-mismatch count** *number* **duration** *seconds* **action log**：DNS ID の過剰な不一致のロギングをイネーブルにします。**count** *number* **duration** *seconds* 引数は、システム メッセージ ログが送信されるようになる 1 秒間の不一致インスタンスの最大数を指定します。
- **id-randomization**：DNS クエリーの DNS 識別子をランダム化します。
- **message-length maximum** {*length* | **client** {*length* | **auto**} | **server** {*length* | **auto**}}：DNS メッセージの最大長を設定します（512 ～ 65535 バイト）。クライアント メッセージまたはサーバ メッセージの最大長も設定できます。**auto** キーワードは、リソース レコードの値に最大長を設定します。
- **nat-rewrite**：DNS レコードを NAT の設定に基づいて変換します。
- **protocol-enforcement**：DNS メッセージ形式のチェックをイネーブルにします。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。
- **tsig enforced action** {[**drop**] [**log**]}：TSIG リソース レコードの存在を要求します。準拠していないパケットをドロップしたり（**drop**）、パケットをログに記録したり（**log**）できます。両方指定することもできます。

次に例を示します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)# dns-guard
hostname(config-pmap-p)# message-length maximum 1024
hostname(config-pmap-p)# nat-rewrite
hostname(config-pmap-p)# protocol-enforcement
```

例

次の例は、DNS インスペクション ポリシー マップを定義する方法を示しています。

```
regex domain_example "example\.com"
regex domain_foo "foo\.com"

! define the domain names that the server serves
class-map type inspect regex match-any my_domains
    match regex domain_example
    match regex domain_foo

! Define a DNS map for query only
class-map type inspect dns match-all pub_server_map
    match not header-flag QR
    match question
    match not domain-name regex class my_domains

policy-map type inspect dns new_dns_map
    class pub_server_map
        drop log
    match header-flag RD
        mask log
    parameters
        message-length maximum client auto
        message-length maximum 512
        dns-guard
        protocol-enforcement
        nat-rewrite
```

DNS インスペクション サービス ポリシーの設定

ASA のデフォルトの設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの DNS インスペクションが含まれます。インスペクションの設定をカスタマイズする一般的な方法は、デフォルトのグローバル ポリシーをカスタマイズすることです。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

class-map *name*
match *parameter*

例：

```
hostname(config)# class-map dns_class_map
hostname(config-cmap)# match access-list dns
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　DNS インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　DNS インスペクションを設定します。

inspect dns [*dns_policy_map*] [**dynamic-filter-snoop**]

それぞれの説明は次のとおりです。

- *dns_policy_map* は、オプションの DNS インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。DNS インスペクション ポリシー マップの作成の詳細については、「DNS インスペクション ポリシー マップの設定」（P.8-3）を参照してください。
- **dynamic-filter-snoop** は、ボットネット トラフィック フィルタによってのみ使用される動的フィルタの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 フィルタリングを使用する場合に限り、このキーワードを指定します。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。

例：

```
hostname(config-class)# no inspect dns
hostname(config-class)# inspect dns dns-map
```

（注） デフォルトのグローバル ポリシー（または使用中の任意のポリシー）を編集して、異なる DNS インスペクション ポリシー マップを使用する場合は（たとえば、デフォルトの preset_dns_map を置き換える）、**no inspect dns** コマンドで DNS インスペクションを除去した後、新しい DNS インスペクション ポリシー マップ名を指定して再度追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

例

次の例では、グローバル デフォルト設定で新しいインスペクション ポリシー マップを使用する方法を示します。

```
policy-map global_policy
 class inspection_default
  no inspect dns preset_dns_map
  inspect dns new_dns_map
service-policy global_policy global
```

DNS インスペクションのモニタリング

現在の DNS 接続に関する情報を表示するには、次のコマンドを入力します。

```
hostname# show conn
```

DNS サーバを使用する接続の場合、show conn コマンドの出力で、接続の送信元ポートが DNS サーバの IP アドレスに置き換えられることがあります。

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 応答がセキュリティ アプライアンスを通過できるのは、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 アプリケーション インスペクションの統計情報を表示するには、**show service-policy** コマンドを入力します。次に、**show service-policy** コマンドの出力例を示します。

```
hostname# show service-policy
Interface outside:
Service-policy: sample_policy
    Class-map: dns_port
      Inspect: dns maximum-length 1500, packet 0, drop 0, reset-drop 0
```

FTP インスペクション

ここでは、FTP インスペクション エンジンについて説明します。

- 「FTP インスペクションの概要」（P.8-9）
- 「厳密な FTP」（P.8-10）
- 「FTP インスペクションの設定」（P.8-11）
- 「FTP インスペクションの確認とモニタリング」（P.8-15）

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

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、**inspect ftp** コマンドに **strict** オプションを含めます。

厳密な FTP を使用するときは、オプションで FTP インスペクション ポリシー マップを指定して、ASA を通過することが許可されない FTP コマンドを指定できます。

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。

FTP インスペクションの設定

FTP 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。デフォルト以外の処理が必要な場合にのみ設定する必要があります。FTP インスペクションをカスタマイズする場合は、次のプロセスを使用します。

手順

ステップ 1　「FTP インスペクション ポリシー マップの設定」（P.8-11）。

ステップ 2　「FTP インスペクション サービス ポリシーの設定」（P.8-14）。

FTP インスペクション ポリシー マップの設定

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。

FTP インスペクションで FTP サーバがそのシステム タイプを FTP クライアントに公開することを許可し、許可する FTP コマンドを制限する場合、FTP インスペクション ポリシー マップを作成および設定します。作成したマップは、FTP インスペクションをイネーブルにすると適用できます。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　（任意）次の手順に従って、FTP インスペクションのクラス マップを作成します。

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。代わりに、ポリシー マップで **match** コマンドを直接指定できます。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 マップでトラフィックと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ことです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

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 マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシー マップに直接トラフィックを特定する必要があります。

a. 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 type inspect ftp [match-all | match-any] class_map_name
hostname(config-cmap)#
```

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。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。match-any キーワードは、トラフィックが少なくとも 1 つの **match** ステートメントと一致したらクラス マップと一致することを指定します。CLI がクラス マップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b. （任意）クラス マップに説明を追加するには、次のコマンドを使用します。

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

string には、クラス マップの説明を 200 文字以内で指定します。

c. 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **filename regex** {*regex_name* | **class** *class_name*}：FTP 転送のファイル名を、指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **filetype regex** {*regex_name* | **class** *class_name*}：FTP 転送のファイル タイプを、指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **request-command** *ftp_command* [*ftp_command...*]：FTP コマンドを照合します。以下の 1 つ以上です。

  APPE：ファイルに追加します。

  CDUP：現在の作業ディレクトリの親ディレクトリに変更します。

  DELE：サーバのファイルを削除します。

  GET：サーバからファイルを取得します。

  HELP：ヘルプ情報を提供します。

  MKD：サーバにディレクトリを作成します。

  PUT：ファイルをサーバに送信します。

  MKD：サーバのディレクトリを削除します。

  RNFR：「変更前の」ファイル名を指定します。

  RNTO：「変更後の」ファイル名を指定します。

  SITE：サーバ固有のコマンドの指定に使用されます。通常、これはリモート管理に使用されます。

  STOU：一義的なファイル名を使用してファイルを保存します。

- **match** [**not**] **server regex** {*regex_name* | **class** *class_name*}：FTP サーバ名を、指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **username regex** {*regex_name* | **class** *class_name*}：FTP ユーザ名を、指定された正規表現または正規表現クラスに対して照合します。

d. クラス マップ コンフィギュレーション モードを終了するには、「**exit**」と入力します。

ステップ 2　FTP インスペクション ポリシー マップを作成します。

```
hostname(config)# policy-map type inspect ftp policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3　（任意）このポリシー マップに説明を追加するには、次のコマンドを使用します。

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

ステップ 4　一致したトラフィックにアクションを適用するには、次の手順を実行します。

a. 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- FTP クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。

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

- FTP クラス マップで説明されている **match** コマンドのいずれかを使用して、ポリシー マップに直接トラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b. 次のコマンドを入力して、一致したトラフィックに対して実行するアクションを指定します。

```
hostname(config-pmap-c)# reset [log]
```

reset キーワードを指定すると、パケットをドロップして接続を閉じ、サーバまたはクライアントに TCP リセットを送信します。システム ログ メッセージを送信するには、**log** キーワードを追加します。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、「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.2-4）を参照してください。

ステップ 5　インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a. パラメータ コンフィギュレーション モードに入るには、次のコマンドを入力します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **mask-banner**：FTP サーバから接続時バナーをマスクします。
- **mask-syst-reply**：**syst** コマンドに対する応答をマスクします。

例

ユーザ名とパスワードを送信する前に、すべての FTP ユーザに接続時バナーが表示されます。デフォルトでは、このバナーには、ハッカーがシステムの弱点を特定するのに役立つバージョン情報が含まれます。このバナーをマスクする方法を次に示します。

```
hostname(config)# policy-map type inspect ftp mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner
```

```
hostname(config)# class-map match-all ftp-traffic
hostname(config-cmap)# match port tcp eq ftp

hostname(config)# policy-map ftp-policy
hostname(config-pmap)# class ftp-traffic
hostname(config-pmap-c)# inspect ftp strict mymap

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

FTP インスペクション サービス ポリシーの設定

ASA のデフォルトの設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの FTP インスペクションが含まれます。インスペクションの設定をカスタマイズする一般的な方法は、デフォルトのグローバル ポリシーをカスタマイズすることです。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

class-map *name*
match *parameter*

例：

```
hostname(config)# class-map ftp_class_map
hostname(config-cmap)# match access-list ftp
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　FTP インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　FTP インスペクションを設定します。

```
inspect ftp [strict [ftp_policy_map]]
```

それぞれの説明は次のとおりです。

- **strict** は、厳密な FTP を実装します。FTP インスペクション ポリシー マップを指定するには、厳密な FTP を使用する必要があります。
- *ftp_policy_map* は、オプションの FTP インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。FTP インスペクション ポリシー マップの作成の詳細については、「FTP インスペクション ポリシー マップの設定」（P.8-11）を参照してください。

例：

```
hostname(config-class)# no inspect ftp
hostname(config-class)# inspect ftp strict ftp-map
```

（注）　デフォルトのグローバル ポリシー（または使用中の任意のポリシー）を編集して、異なる FTP インスペクション ポリシー マップを使用する場合は、**no inspect ftp** コマンドで FTP インスペクションを除去した後、新しい FTP インスペクション ポリシー マップ名を指定して再度追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

```
service-policy policymap_name {global | interface interface_name}
```

例：

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

global キーワードはポリシー 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。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。

FTP インスペクション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。

- 取得またはアップロードされたファイルごとに監査レコード 303002 が生成されます。
- FTP コマンドが RETR または STOR であるかがチェックされ、取得コマンドおよび保存コマンドがログに記録されます。
- IP アドレスを提供するテーブルを検索してユーザ名が取得されます。

- ユーザ名、接続元の IP アドレス、接続先の IP アドレス、NAT アドレス、およびファイル操作がログに記録されます。
- メモリ不足によって動的なセカンダリ チャネルの準備に失敗した場合は、監査レコード 201005 が生成されます。

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

ここでは、HTTP インスペクション エンジンについて説明します。

HTTP インスペクションの概要

ヒント　アプリケーションおよび URL のフィルタリングを実行するサービス モジュールをインストールできます。これには、ASA CX や ASA FirePOWER などの HTTP インスペクションが含まれます。ASA 上で実行される HTTP インスペクションは、これらのモジュールと互換性がありません。HTTP インスペクション ポリシー マップを使用して ASA 上で手作業による設定を試みるより、専用のモジュールを使用してアプリケーション フィルタリングを設定する方がはるかに簡単であることに注意してください。

HTTP インスペクション エンジンを使用して、HTTP トラフィックに関係する特定の攻撃やその他の脅威から保護します。

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。

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 インスペクション ポリシー 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。

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。

拡張 HTTP インスペクションは、すべての HTTP メッセージについて次の点を確認します。

- 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

HTTP インスペクションの設定

HTTP インスペクションはデフォルトではイネーブルになりません。ASA CX や ASA FirePOWER などの HTTP インスペクションおよびアプリケーション フィルタリングに専用のモジュールを使用していない場合、以下の方法を使用して、ASA に HTTP インスペクションを手動で設定できます。

ヒント　サービス モジュールと ASA の両方で HTTP インスペクションを設定しないでください。インスペクションの互換性はありません。

手順

ステップ 1　「HTTP インスペクション ポリシー マップの設定」（P.8-17）。

ステップ 2　「HTTP インスペクション サービス ポリシーの設定」（P.8-21）。

HTTP インスペクション ポリシー マップの設定

メッセージがパラメータに違反したときのアクションを指定するには、HTTP インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、HTTP インスペクションをイネーブルにすると適用できます。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　（任意）次の手順に従って、HTTP インスペクションのクラス マップを作成します。

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。代わりに、ポリシー マップで **match** コマンドを直接指定できます。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 マップでトラフィックと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ことです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

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 マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシー マップに直接トラフィックを特定する必要があります。

a. 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 type inspect http [match-all | match-any] class_map_name
hostname(config-cmap)#
```

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。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。match-any キーワードは、トラフィックが少なくとも 1 つの **match** ステートメントと一致したらクラス マップと一致することを指定します。CLI がクラス マップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b. （任意）クラス マップに説明を追加するには、次のコマンドを使用します。

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

string には、クラス マップの説明を 200 文字以内で指定します。

c. 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **req-resp content-type mismatch**：HTTP 応答の content-type フィールドが対応する HTTP 要求メッセージの accept フィールドと一致しないトラフィックを照合します。
- **match** [**not**] **request args regex** {*regex_name* | **class** *class_name*}：HTTP 要求メッセージの引数で見つかったテキストを、指定した正規表現または正規表現クラスと照合します。
- **match** [**not**] **request body** {**regex** {*regex_name* | **class** *class_name*} | **length gt** *bytes*}：HTTP 要求メッセージの本文で見つかったテキストを、指定した正規表現または正規表現クラスと照合します。または、要求の本文が指定した長さより長いメッセージを照合します。
- **match** [**not**] **request header** {*field* | **regex** *regex_name*} **regex** {*regex_name* | **class** *class_name*}：HTTP 要求メッセージ ヘッダーのフィールドの内容を、指定した正規表現または正規表現クラスと照合します。フィールド名を明示的に指定することも、フィールド名を正規表現と一致させることもできます。フィールド名は次のとおりです。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。
- **match** [**not**] **request header** {*field* | **regex** {*regex_name* | **class** *class_name*}} {**length gt** *bytes* | **count gt** *number*}：HTTP 要求メッセージ ヘッダーの指定したフィールドの長さ、またはヘッダーのフィールドの総数を照合します。フィールド名を明示的に指定することも、フィールド名を正規表現または正規表現クラスと一致させることもできます。フィールド名は、前の項目の一覧と同じです。
- **match** [**not**] **request header** {**length gt** *bytes* | **count gt** *number* | **non-ascii**}：HTTP 要求メッセージ ヘッダーの全体の長さ、ヘッダーのフィールドの総数、または ASCII 以外の文字を含むヘッダーを照合します。

- **match** [**not**] **request method** {*method* | **regex** {*regex_name* | **class** *class_name*}}：HTTP 要求のメソッドを照合します。メソッドを明示的に指定することも、メソッドを正規表現または正規表現クラスと一致させることもできます。メソッドは次のとおりです。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。
- **match** [**not**] **request uri** {**regex** {*regex_name* | **class** *class_name*} | **length gt** *bytes*}：HTTP 要求メッセージの URI で見つかったテキストを、指定した正規表現または正規表現クラスと照合します。または、要求の URI が指定した長さより長いメッセージを照合します。
- **match** [**not**] **response body** {**active-x** | **java-applet** | **regex** {*regex_name* | **class** *class_name*}}：HTTP 応答メッセージの本文で見つかったテキストを、指定した正規表現または正規表現クラスと照合します。または、Java アプレットおよび Active X オブジェクトをフィルタ処理のためにコメント化します。
- **match** [**not**] **response body length gt** *bytes*：本文が指定した長さより大きい HTTP 応答メッセージを照合します。
- **match** [**not**] **response header** {*field* | **regex** *regex_name*} **regex** {*regex_name* | **class** *class_name*}：HTTP 応答メッセージ ヘッダーのフィールドの内容を、指定した正規表現または正規表現クラスと照合します。フィールド名を明示的に指定することも、フィールド名を正規表現と一致させることもできます。フィールド名は次のとおりです。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。
- **match** [**not**] **response header** {*field* | **regex** {*regex_name* | **class** *class_name*}} {**length gt** *bytes* | **count gt** *number*}：HTTP 応答メッセージ ヘッダーの指定したフィールドの長さ、またはヘッダーのフィールドの総数を照合します。フィールド名を明示的に指定することも、フィールド名を正規表現または正規表現クラスと一致させることもできます。フィールド名は、前の項目の一覧と同じです。
- **match** [**not**] **response header** {**length gt** *bytes* | **count gt** *number* | **non-ascii**}：HTTP 応答メッセージ ヘッダーの全体の長さ、ヘッダーのフィールドの総数、または ASCII 以外の文字を含むヘッダーを照合します。
- **match** [**not**] **response status-line regex** {*regex_name* | **class** *class_name*}：HTTP 応答メッセージのステータス行で見つかったテキストを、指定した正規表現または正規表現クラスと照合します。

d. クラス マップ コンフィギュレーション モードを終了するには、「**exit**」と入力します。

ステップ 2　HTTP インスペクション ポリシー マップを作成します。

```
hostname(config)# policy-map type inspect http policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3　（任意）このポリシー マップに説明を追加するには、次のコマンドを使用します。

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

ステップ 4　一致したトラフィックにアクションを適用するには、次の手順を実行します。

a. 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- HTTP クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。

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

- HTTP クラス マップで説明されている **match** コマンドのいずれかを使用して、ポリシー マップに直接トラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b. 次のコマンドを入力して、一致したトラフィックに対して実行するアクションを指定します。

```
hostname(config-pmap-c)# {drop-connection [log]| reset [log] | log}
```

drop-connection キーワードを指定すると、パケットをドロップし、接続を閉じます。

reset キーワードを指定すると、パケットをドロップして接続を閉じ、サーバまたはクライアントに TCP リセットを送信します。

log キーワードを指定すると、システム ログ メッセージを送信します。このキーワードは単独で、または他のキーワードのいずれかと一緒に使用できます。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、「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.2-4）を参照してください。

ステップ 5　インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a. パラメータ コンフィギュレーション モードに入るには、次のコマンドを入力します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **body-match-maximum** *number*：HTTP メッセージの本文照合時に検索する本文の最大文字数を設定します。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。
- **protocol-violation action {drop-connection [log] | reset [log] | log}**：HTTP メッセージの本文照合時に検索する本文の最大文字数を設定します。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。HTTP プロトコル違反を検査します。違反に対して実行するアクション（切断、リセット、ログ記録）、およびロギングをイネーブルまたはディセーブルにするかどうかも選択する必要があります。
- **spoof-server** *string*：サーバ ヘッダー フィールドの文字列を置き換えます。WebVPN ストリームは **spoof-server** コマンドの対象ではありません。

例

次に、「GET」メソッドまたは「PUT」メソッドで「www\.xyz.com/.*\.asp」または「www\.xyz[0-9][0-9]\.com」にアクセスしようとしている HTTP 接続を許可し、ロギングする HTTP インスペクション ポリシー マップを定義する例を示します。それ以外の URL/メソッドの組み合わせは、サイレントに許可されます。

```
hostname(config)# regex url1 "www\.xyz.com/.*\.asp"
hostname(config)# regex url2 "www\.xyz[0-9][0-9]\.com"
hostname(config)# regex get "GET"
hostname(config)# regex put "PUT"

hostname(config)# class-map type regex match-any url_to_log
hostname(config-cmap)# match regex url1
hostname(config-cmap)# match regex url2
hostname(config-cmap)# exit

hostname(config)# class-map type regex match-any methods_to_log
hostname(config-cmap)# match regex get
hostname(config-cmap)# match regex put
hostname(config-cmap)# exit

hostname(config)# class-map type inspect http http_url_policy
hostname(config-cmap)# match request uri regex class url_to_log
hostname(config-cmap)# match request method regex class methods_to_log
hostname(config-cmap)# exit

hostname(config)# policy-map type inspect http http_policy
hostname(config-pmap)# class http_url_policy
hostname(config-pmap-c)# log
```

HTTP インスペクション サービス ポリシーの設定

HTTP インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの HTTP ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで HTTP インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

```
class-map name
match parameter
```

例：

```
hostname(config)# class-map http_class_map
hostname(config-cmap)# match access-list http
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　HTTP インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　HTTP インスペクションを設定します。

inspect http [*http_policy_map*]

http_policy_map は、オプションの HTTP インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。HTTP インスペクション ポリシー マップの作成の詳細については、「HTTP インスペクション ポリシー マップの設定」（P.8-17）を参照してください。

例：

```
hostname(config-class)# no inspect http
hostname(config-class)# inspect http http-map
```

（注）　デフォルトのグローバル ポリシー（または使用中の任意のポリシー）を編集して、異なる HTTP インスペクション ポリシー マップを使用する場合は、**no inspect http** コマンドで HTTP インスペクションを除去した後、新しい HTTP インスペクション ポリシー マップ名を指定して再度追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

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 が ASA を通過するの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。

ただし、ASA インターフェイスに送られる ICMP トラフィックは、ICMP インスペクションをイネーブルにした場合でも、検査されません。したがって、ASA がバックアップ デフォルト ルートを介して到達できる送信元からエコー要求が送信された場合など、特定の状況下では、インターフェイスへの ping（エコー要求）が失敗する可能性があります。

ICMP インスペクションをイネーブルにする方法については、「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.7-11）を参照してください。

ICMP エラー インスペクション

ICMP エラー インスペクションをイネーブルにすると、ASA は NAT の設定に基づいて、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。

ICMP エラー インスペクションをイネーブルにする方法については、「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.7-11）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

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 のネットワーク使用を制御し、機密情報の漏洩、ワームの送信、および企業ネットワークへのその他の脅威を停止できます。

IM インスペクションはデフォルトではイネーブルになりません。IM インスペクションが必要な場合は設定する必要があります。

手順

ステップ 1　「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.8-24）。

ステップ 2　「IM インスペクション サービス ポリシーの設定」（P.8-27）。

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

メッセージがパラメータに違反したときのアクションを指定するには、IM インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、IM インスペクションをイネーブルにすると適用できます。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　（任意）次の手順に従って、IM インスペクションのクラス マップを作成します。

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。代わりに、ポリシー マップで **match** コマンドを直接指定できます。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 マップでトラフィックと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ことです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

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 マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシー マップに直接トラフィックを特定する必要があります。

a. 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 type inspect im [match-all | match-any] class_map_name
hostname(config-cmap)#
```

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。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。match-any キーワードは、トラフィックが少なくとも 1 つの **match** ステートメントと一致したらクラス マップと一致することを指定します。CLI がクラスマップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b. （任意）クラス マップに説明を追加するには、次のコマンドを使用します。

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

string には、クラス マップの説明を 200 文字以内で指定します。

c. 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **protocol {im-yahoo | im-msn}**：特定の IM プロトコル（Yahoo または MSN）を照合します。
- **match** [**not**] **service {chat | file-transfer | webcam | voice-chat | conference | games}**：特定の IM サービスを照合します。
- **match** [**not**] **login-name regex** {*regex_name* | **class** *class_name*}：IM メッセージの送信元クライアント ログイン名を、指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **peer-login-name regex** {*regex_name* | **class** *class_name*}：IM メッセージの宛先ピア ログイン名を、指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **ip-address** *ip_address mask*}：IM メッセージの送信元 IP アドレスとマスクを照合します。
- **match** [**not**] **peer-ip-address** *ip_address mask*}：IM メッセージの宛先 IP アドレスとマスクを照合します。
- **match** [**not**] **version regex** {*regex_name* | **class** *class_name*}：IM メッセージのバージョンを、指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **filename regex** {*regex_name* | **class** *class_name*}：IM メッセージのファイル名を、指定された正規表現または正規表現クラスに対して照合します。この照合は MSN IM プロトコルに対してはサポートされません。

d. クラス マップ コンフィギュレーション モードを終了するには、「**exit**」と入力します。

ステップ 2　IM インスペクション ポリシー マップを作成します。

```
hostname(config)# policy-map type inspect im policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3　（任意）このポリシー マップに説明を追加するには、次のコマンドを使用します。

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

ステップ 4　一致したトラフィックにアクションを適用するには、次の手順を実行します。

a. 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- IM クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。

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

- IM クラス マップで説明されている **match** コマンドのいずれかを使用して、ポリシー マップに直接トラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b. 次のコマンドを入力して、一致したトラフィックに対して実行するアクションを指定します。

```
hostname(config-pmap-c)# {drop-connection [log]| reset [log] | log}
```

drop-connection キーワードを指定すると、パケットをドロップし、接続を閉じます。

reset キーワードを指定すると、パケットをドロップして接続を閉じ、サーバまたはクライアントに TCP リセットを送信します。

log キーワードを指定すると、システム ログ メッセージを送信します。このキーワードは単独で、または他のキーワードのいずれかと一緒に使用できます。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、「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.2-4）を参照してください。

例

次の例は、IM インスペクション ポリシー マップを定義する方法を示しています。

```
hostname(config)# regex loginname1 "ying\@yahoo.com"
hostname(config)# regex loginname2 "Kevin\@yahoo.com"
hostname(config)# regex loginname3 "rahul\@yahoo.com"
hostname(config)# regex loginname4 "darshant\@yahoo.com"
hostname(config)# regex yahoo_version_regex "1\.0"
hostname(config)# regex gif_files ".*\.gif"
hostname(config)# regex exe_files ".*\.exe"

hostname(config)# class-map type regex match-any yahoo_src_login_name_regex
hostname(config-cmap)# match regex loginname1
hostname(config-cmap)# match regex loginname2

hostname(config)# class-map type regex match-any yahoo_dst_login_name_regex
hostname(config-cmap)# match regex loginname3
hostname(config-cmap)# match regex loginname4

hostname(config)# class-map type inspect im match-any yahoo_file_block_list
hostname(config-cmap)# match filename regex gif_files
hostname(config-cmap)# match filename regex exe_files

hostname(config)# class-map type inspect im match-all yahoo_im_policy
hostname(config-cmap)# match login-name regex class yahoo_src_login_name_regex
hostname(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex

hostname(config)# class-map type inspect im match-all yahoo_im_policy2
hostname(config-cmap)# match version regex yahoo_version_regex

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

```
hostname(config)# policy-map type inspect im im_policy_all
hostname(config-pmap)# class yahoo_file_block_list
hostname(config-pmap-c)# match service file-transfer
hostname(config-pmap)# class yahoo_im_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yahoo_im_policy2
hostname(config-pmap-c)# reset
hostname(config)# policy-map global_policy_name
hostname(config-pmap)# class im_inspect_class_map
hostname(config-pmap-c)# inspect im im_policy_all
```

IM インスペクション サービス ポリシーの設定

IM インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの IM ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで IM インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

class-map *name*
match *parameter*

例：

```
hostname(config)# class-map im_class_map
hostname(config-cmap)# match access-list im
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　IM インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　IM インスペクションを設定します。

inspect im [*im_policy_map*]

im_policy_map は、オプションの IM インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。IM インスペクション ポリシー マップの作成の詳細については、「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.8-24）を参照してください。

例：

```
hostname(config-class)# no inspect im
hostname(config-class)# inspect im im-map
```

（注）　デフォルトのグローバル ポリシー（または使用中の任意のポリシー）を編集して、異なる IM インスペクション ポリシー マップを使用する場合は、**no inspect im** コマンドで IM インスペクションを除去した後、新しい IM インスペクション ポリシー マップ名を指定して再度追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

IP オプション インスペクション

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 オプションをクリアしたうえでのパケットの転送許可を ASA に指示します。

ここでは、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。

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 オプションおよび関連する RFC の参照のリストについては、IANA のページ（http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml）を参照してください。

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 オプションをクリアしたうえでのパケットの転送許可を ASA に指示します。

オプションをクリアしたときの結果

IP オプション インスペクション ポリシー マップを設定する場合、各オプション タイプを許可またはクリアするかどうかを指定できます。オプション タイプを指定しないと、そのオプションを含むパケットはドロップされます。

オプションを単に許可すると、そのオプションを含むパケットは未変更で渡されます。

IP ヘッダーからオプションをクリアするように指定すると、IP ヘッダーは次のように変更されます。

- オプションがヘッダーから除去されます。
- 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。
- パケット内のインターネット ヘッダー長（IHL）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。

インスペクションでサポートされる IP オプション

IP オプション インスペクションでは、パケット内の次の IP オプションをチェックできます。IP ヘッダーにこれら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。

- 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。すべてのオプションのビット数が 32 ビットの倍数でない場合、NOP オプションは、オプションを 32 ビット境界上に揃えるために、「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、パケットの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。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 オプション インスペクションのデフォルト

IP オプション インスペクションは、_default_ip_options_map インスペクション ポリシー マップを使用して、デフォルトで有効になります。

- Router Alert オプションは許可されます。
- その他のオプションを含むパケットはドロップされます。これには、サポートされていないオプションを含むパケットが含まれます。

ポリシー マップのコンフィギュレーションは次のとおりです。

```
policy-map type inspect ip-options _default_ip_options_map
 description Default IP-OPTIONS policy-map
 parameters
  router-alert action allow
```

IP オプション インスペクションの設定

IP オプション 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。デフォルト マップで許可されているもの以外の追加オプションが必要な場合にのみ、設定する必要があります。

手順

ステップ 1　「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.8-31）。

ステップ 2　「IP オプション インスペクション サービス ポリシーの設定」（P.8-31）。

IP オプション インスペクション ポリシー マップの設定

デフォルト以外の IP オプション インスペクションを実行する場合は、IP オプション インスペクション ポリシー マップを作成して、サポートされる各オプション タイプの処理方法を指定します。

手順

ステップ 1　IP オプション インスペクション ポリシー マップを設定します。

```
hostname(config)# policy-map type inspect ip-options policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2　（任意）このポリシー マップに説明を追加するには、次のコマンドを使用します。

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

ステップ 3　インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a.　パラメータ コンフィギュレーション モードに入るには、次のコマンドを入力します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b.　1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。いずれの場合も、**allow** アクションはそのオプションを含むパケットを変更なしで許可し、**clear** アクションはパケットを許可しますがヘッダーからそのオプションを除去します。マップで指定されていないオプションを含むパケットはすべてドロップされます。オプションの詳細については、「インスペクションでサポートされる IP オプション」（P.8-30）を参照してください。

- **eool action** {**allow** | **clear**}：End of Options List オプションを許可またはクリアします。
- **nop action** {**allow** | **clear**}：No Operation オプションを許可またはクリアします。
- **router-alert action** {**allow** | **clear**}：Router Alert（RTRALT）オプションを許可またはクリアします。

IP オプション インスペクション サービス ポリシーの設定

ASA のデフォルトのコンフィギュレーションには、すべてのインターフェイスにグローバルに適用される IP オプション インスペクションが含まれます。インスペクションの設定をカスタマイズする一般的な方法は、デフォルトのグローバル ポリシーをカスタマイズすることです。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

```
class-map name
match parameter
```

例：

```
hostname(config)# class-map ip_options_class_map
hostname(config-cmap)# match access-list ipoptions
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　IP オプション インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　IP オプション インスペクションを設定します。

inspect ip-options [*ip_options_policy_map*]

ip_options_policy_map は、オプションの IP オプション インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。IP オプション インスペクション ポリシー マップの作成の詳細については、「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.8-31）を参照してください。

例：

```
hostname(config-class)# no inspect ip-options
hostname(config-class)# inspect ip-options ip-options-map
```

（注）　デフォルトのグローバル ポリシー（または使用中の任意のポリシー）を編集して、異なる IP オプション インスペクション ポリシー マップを使用する場合は、**no inspect ip-options** コマンドで IP オプション インスペクションを除去した後、新しい IP オプション インスペクション ポリシー マップ名を指定して再度追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

IP オプション インスペクションのモニタリング

以下の方法を使用して IP オプション インスペクションの結果をモニタリングできます。

- インスペクションによってパケットがドロップされるたびに、syslog 106012 が発行されます。メッセージではドロップの原因になったオプションが示されます。
- **show service-policy inspect ip-options** コマンドを使用して、各オプションの統計情報を表示します。

IPsec パススルー インスペクション

ここでは、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。

- 「IPsec パススルー インスペクションの概要」（P.8-33）
- 「IPsec パススルー インスペクションの設定」（P.8-34）

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検査できます。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。

ESP または AH トラフィックの制限を指定するには、IPsec パススルーのポリシー マップを設定します。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。

IPsec パススルー インスペクションの設定

IPsec パススルー インスペクションはデフォルトではイネーブルになりません。IPsec パススルー インスペクションが必要な場合は設定する必要があります。

手順

ステップ 1　「IPsec パススルー インスペクション ポリシー マップの設定」（P.8-34）。

ステップ 2　「IPsec パススルー インスペクション サービス ポリシーの設定」（P.8-35）。

IPsec パススルー インスペクション ポリシー マップの設定

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。

コンフィギュレーションに含まれるデフォルト マップ _default_ipsec_passthru_map では、ESP 接続に対するクライアントごとの最大数は制限なしに設定され、ESP アイドル タイムアウトは 10 分に設定されます。異なる値が必要な場合、または AH 値を設定する必要がある場合にのみ、インスペクション ポリシー マップを設定する必要があります。

手順

ステップ 1　IPsec パススルー インスペクション ポリシー マップを作成します。

```
hostname(config)# policy-map type inspect ipsec-pass-thru policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2　（任意）このポリシー マップに説明を追加するには、次のコマンドを使用します。

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

ステップ 3　インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a.　パラメータ コンフィギュレーション モードに入るには、次のコマンドを入力します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b.　1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **esp per-client-max** *number* **timeout** *time* : ESP トンネルを許可し、クライアントごとに許可される最大接続数およびアイドル タイムアウト（hh:mm:ss の形式）を設定します。接続の数を無制限に設定するには、値を 0 に指定します。
- **ah per-client-max** *number* **timeout** *time* : AH トンネルを許可します。パラメータの意味は esp コマンドと同じです。

例

次に、ACL を使用して IKE トラフィックを識別し、IPsec Pass Thru パラメータ マップを定義して、ポリシーを定義し、外部インターフェイスにポリシーを適用する例を示します。

```
hostname(config)# access-list ipsecpassthruacl permit udp any any eq 500
hostname(config)# class-map ipsecpassthru-traffic
hostname(config-cmap)# match access-list ipsecpassthruacl
hostname(config)# policy-map type inspect ipsec-pass-thru iptmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
hostname(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class ipsecpassthru-traffic
hostname(config-pmap-c)# inspect ipsec-pass-thru iptmap
hostname(config)# service-policy inspection_policy interface outside
```

IPsec パススルー インスペクション サービス ポリシーの設定

IPsec パススルー インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの IPsec ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで IPsec インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

class-map *name*
match *parameter*

例：

```
hostname(config)# class-map ipsec_class_map
hostname(config-cmap)# match access-list ipsec
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　IPsec パススルー オプション インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　IPsec パススルー インスペクションを設定します。

inspect ipsec-pass-thru [*ipsec_policy_map*]

ipsec_policy_map は、オプションの IPsec パススルー インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。インスペクション ポリシー マップの作成の詳細については、「IPsec パススルー インスペクション ポリシー マップの設定」（P.8-34）を参照してください。

例：

```
hostname(config-class)# no inspect ipsec-pass-thru
hostname(config-class)# inspect ipsec-pass-thru ipsec-map
```

（注）　デフォルトのグローバル ポリシー（または使用中の任意のポリシー）を編集して、異なる IPsec パススルー インスペクション ポリシー マップを使用する場合は、**no inspect ipsec-pass-thru** コマンドで IPsec パススルー インスペクションを除去した後、新しい IPsec パススルー インスペクション ポリシー マップ名を指定して再度追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

IPv6 インスペクション

IPv6 インスペクションを使用すると、拡張ヘッダーに基づいて IPv6 トラフィックを選択的にログに記録したりドロップしたりできます。さらに、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も確認できます。

- 「IPv6 インスペクションのデフォルト」（P.8-37）
- 「IPv6 インスペクションの設定」（P.8-37）

IPv6 インスペクションのデフォルト

IPv6 インスペクションをイネーブルにし、インスペクション ポリシー マップを指定しないと、デフォルトの IPv6 インスペクション ポリシー マップが使用され、次のアクションが実行されます。

- 既知の IPv6 拡張ヘッダーのみを許可します。準拠しないパケットはドロップされ、ログに記録されます。
- RFC 2460 仕様で定義されている IPv6 拡張ヘッダーの順序を適用します。準拠しないパケットはドロップされ、ログに記録されます。
- ルーティング タイプ ヘッダーを含むパケットをドロップします。

ポリシー マップのコンフィギュレーションは次のとおりです。

```
policy-map type inspect ipv6 _default_ipv6_map
 description Default IPV6 policy-map
 parameters
  verify-header type
  verify-header order
 match header routing-type range 0 255
  drop log
```

IPv6 インスペクションの設定

IPv6 インスペクションはデフォルトではイネーブルになりません。IPv6 インスペクションが必要な場合は設定する必要があります。

手順

ステップ 1　「IPv6 インスペクション ポリシー マップの設定」（P.8-37）。

ステップ 2　「IPv6 インスペクション サービス ポリシーの設定」（P.8-39）。

IPv6 インスペクション ポリシー マップの設定

ドロップまたはロギングする拡張ヘッダーを指定するには、またはパケットの検証をディセーブルにするには、サービス ポリシーで使用される IPv6 インスペクション ポリシー マップを作成します。

手順

ステップ 1　IPv6 インスペクション ポリシー マップを作成します。

```
hostname(config)# policy-map type inspect ipv6 policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2　（任意）説明をポリシー マップに追加します。

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

ステップ 3　（任意）IPv6 メッセージのヘッダーに基づいてトラフィックをドロップまたはロギングします。

a. IPv6 ヘッダーに基づいてトラフィックを識別します。

```
hostname(config-pmap)# match header type
```

type は次のいずれかです。

- **ah**：IPv6 認証拡張ヘッダーと一致します。
- **count gt** *number*：IPv6 拡張ヘッダーの最大数を指定します（0 ～ 255）。
- **destination-option**：IPv6 の宛先オプション拡張ヘッダーと一致します。
- **esp**：IPv6 のカプセル化セキュリティ ペイロード（ESP）拡張ヘッダーと一致します。
- **fragment**：IPv6 のフラグメント拡張ヘッダーと一致します。
- **hop-by-hop**：IPv6 のホップバイホップ拡張ヘッダーと一致します。
- **routing-address count gt** *number*：IPv6 ルーティング ヘッダー タイプ 0 アドレスの最大数を設定します（0 ～ 255）。
- **routing-type** {**eq** | **range**} *number*：IPv6 ルーティング ヘッダー タイプと一致します（0 ～ 255）。範囲を指定するには、値をスペースで区切ります（例：**30 40**）。

b. 一致したパケットに対して実行するアクションを指定します。パケットをドロップし、必要に応じてログに記録できます。または、ログへの記録だけを行うこともできます。アクションを入力しない場合、パケットがログに記録されます。

```
hostname(config-pmap)# {drop [log] | log}
```

c. ドロップまたはロギングするすべてのヘッダーを識別するまで、プロセスを繰り返します。

ステップ 4　インスペクション エンジンに影響するパラメータを設定します。

a. パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **verify-header type**：既知の IPv6 拡張ヘッダーだけを許可します。
- **verify-header order**：RFC 2460 で定義されている IPv6 拡張ヘッダーの順序を適用します。

例

次の例では、ホップバイホップ、宛先オプション、ルーティング アドレス、およびルーティング タイプ 0 の各ヘッダーを含むすべての IPv6 パケットをドロップし、ログに記録するインスペクション ポリシー マップを作成します。また、ヘッダーの順序とタイプを適用します。

```
policy-map type inspect ipv6 ipv6-pm
 parameters
  verify-header type
  verify-header order
 match header hop-by-hop
  drop log
 match header destination-option
  drop log
 match header routing-address count gt 0
  drop log
```

```
 match header routing-type eq 0
  drop log

policy-map global_policy
 class class-default
  inspect ipv6 ipv6-pm
!
service-policy global_policy global
```

IPv6 インスペクション サービス ポリシーの設定

IPv6 インスペクションはデフォルトのインスペクション ポリシーではイネーブルにされないため、このインスペクションが必要な場合はイネーブルにする必要があります。デフォルトのグローバル インスペクション ポリシーを編集して IPv6 インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

class-map *name*
match *parameter*

例：

```
hostname(config)# class-map ipv6_class_map
hostname(config-cmap)# match access-list ipv6
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　IPv6 インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　IPv6 インスペクションを設定します。

```
inspect ipv6 [ipv6_policy_map]
```

ipv6_policy_map は、オプションの IPv6 インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。インスペクション ポリシー マップの作成の詳細については、「IPv6 インスペクション ポリシー マップの設定」（P.8-37）を参照してください。

例：

```
hostname(config-class)# no inspect ipv6
hostname(config-class)# inspect ipv6 ipv6-map
```

（注）　デフォルトのグローバル ポリシー（または使用中の任意のポリシー）を編集して、異なる IPv6 インスペクション ポリシー マップを使用する場合は、**no inspect ipv6** コマンドで IPv6 インスペクションを除去した後、新しい IPv6 インスペクション ポリシー マップ名を指定して再度追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

```
service-policy policymap_name {global | interface interface_name}
```

例：

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

global キーワードはポリシー 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。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。

NetBIOS インスペクション

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 ネーム サービス（NBNS）パケット内の IP アドレスを変換します。必要に応じて、NetBIOS プロトコル違反をドロップまたはログに記録するポリシー マップを作成できます。

手順

ステップ 1　「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.8-41）。

ステップ 2　「NetBIOS インスペクション サービス ポリシーの設定」（P.8-41）。

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

プロトコル違反のアクションを指定するには、NetBIOS インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、NETBIOS インスペクションをイネーブルにすると適用できます。

手順

ステップ 1　NetBIOS インスペクション ポリシー マップを作成します。

```
hostname(config)# policy-map type inspect netbios policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2　（任意）このポリシー マップに説明を追加するには、次のコマンドを使用します。

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

ステップ 3　パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

ステップ 4　NetBIOS プロトコル違反に対して実行するアクションを指定します。

```
hostname(config-pmap-p)# protocol-violation action {drop [log] | log}
```

drop アクションはパケットをドロップします。**log** アクションを指定すると、ポリシー マップがトラフィックに一致したときにシステム ログ メッセージを送信します。

例

```
hostname(config)# policy-map type inspect netbios netbios_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation drop log

hostname(config)# policy-map netbios_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect netbios netbios_map
```

NetBIOS インスペクション サービス ポリシーの設定

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。

ASA のデフォルトの設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの NetBIOS インスペクションが含まれます。インスペクションの設定をカスタマイズする一般的な方法は、デフォルトのグローバル ポリシーをカスタマイズすることです。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

```
class-map name
match parameter
```

例：

```
hostname(config)# class-map netbios_class_map
hostname(config-cmap)# match access-list netbios
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

```
policy-map name
```

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　NetBIOS インスペクションに使用する L3/L4 クラス マップを指定します。

```
class name
```

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　NetBIOS インスペクションを設定します。

```
inspect netbios [netbios_policy_map]
```

netbios_policy_map は、オプションの NetBIOS インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。NetBIOS インスペクション ポリシー マップの作成の詳細については、「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.8-41）を参照してください。

例：

```
hostname(config-class)# no inspect netbios
hostname(config-class)# inspect netbios netbios-map
```

（注）　デフォルトのグローバル ポリシー（または使用中の任意のポリシー）を編集して、異なる NetBIOS インスペクション ポリシー マップを使用する場合は、**no inspect skinny** コマンドで NetBIOS インスペクションを除去した後、新しい NetBIOS インスペクション ポリシー マップ名を指定して再度追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

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。

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。

PPTP インスペクションをイネーブルにする方法については、「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.7-11）を参照してください。

SMTP および拡張 SMTP インスペクション

ESMTP インスペクションは、スパム、フィッシング、不正な形式のメッセージによる攻撃、バッファ オーバーフロー /アンダーフロー攻撃を検出します。また、アプリケーション セキュリティとプロトコル準拠により、正常な ESMTP メッセージだけを通し、各種の攻撃の検出や送受信者およびメール中継のブロックも行います。

ここでは、ESMTP インスペクション エンジンについて説明します。

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。復帰（CR）、および改行（LF）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、次の異常なシグニチャがないかどうか、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。縦棒（|）は削除され（ブランクに変更されます）、「<」および「>」はメール アドレスを定義する場合にのみ許可されます（「>」より前に「<」がある必要があります）。
- 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るため、TCP チェックサムの再計算または調整が必要になります。
- TCP ストリーム編集
- コマンド パイプライン

ESMTP インスペクションのデフォルト

ESMTP インスペクションは、_default_esmtp_map インスペクション ポリシー マップを使用して、デフォルトで有効になります。

- サーバ バナーはマスクされます。
- 暗号化されたトラフィックが検査されます。
- 送信側と受信側のアドレスの特殊文字は認識されず、アクションは実行されません。
- コマンド行の長さが 512 より大きい接続は、ドロップされてログに記録されます。
- 受信者が 100 より多い接続は、ドロップされてログに記録されます。
- 本文の長さが 998 バイトより大きいメッセージはログに記録されます。
- ヘッダー行の長さが 998 より大きい接続は、ドロップされてログに記録されます。
- MIME ファイル名が 255 文字より長いメッセージは、ドロップされてログに記録されます。
- 「others」に一致する EHLO 応答パラメータはマスクされます。

ポリシー マップのコンフィギュレーションは次のとおりです。

```
policy-map type inspect esmtp _default_esmtp_map
 description Default ESMTP policy-map
 parameters
  mask-banner
  no mail-relay
  no special-character
  no allow-tls
 match cmd line length gt 512
  drop-connection log
 match cmd RCPT count gt 100
  drop-connection log
 match body line length gt 998
  log
 match header line length gt 998
  drop-connection log
 match sender-address length gt 320
  drop-connection log
```

```
match MIME filename length gt 255
 drop-connection log
match ehlo-reply-parameter others
 mask
```

ESMTP インスペクションの設定

ESMTP 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。デフォルト インスペクション マップとは異なるプロセスが必要な場合にのみ、設定する必要があります。

手順

ステップ 1　「ESMTP インスペクション ポリシー マップの設定」（P.8-46）。

ステップ 2　「ESMTP インスペクション サービス ポリシーの設定」（P.8-48）。

ESMTP インスペクション ポリシー マップの設定

メッセージがパラメータに違反したときのアクションを指定するには、ESMTP インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、ESMTP インスペクションをイネーブルにすると適用できます。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　ESMTP インスペクション ポリシー マップを作成するには、次のコマンドを入力します。

```
hostname(config)# policy-map type inspect esmtp policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2　（任意）このポリシー マップに説明を追加するには、次のコマンドを使用します。

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

ステップ 3　一致したトラフィックにアクションを適用するには、次の手順を実行します。

a. 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **body** {**length** | **line length**} **gt** *bytes*：ESMTP 本文メッセージの長さまたは行の長さが指定したバイト数より大きいメッセージと一致します。
- **match** [**not**] **cmd verb** *verb1* [*verb2...*]：メッセージ内のコマンド動詞と一致します。次のコマンドの 1 つまたは複数を指定できます。auth、data、ehlo、etrn、helo、help、mail、noop、quit、rcpt、rset、saml、soml、vrfy。

- **match** [**not**] **cmd line length gt** *bytes*：コマンド動詞の行の長さが指定したバイト数より大きいメッセージと一致します。
- **match** [**not**] **cmd rcpt count gt** *count*：受信者の数が指定した値より大きいメッセージと一致します。
- **match** [**not**] **ehlo-reply-parameter** *parameter* [*parameter2...*]：ESMTP EHLO 応答パラメータと一致します。次のパラメータの 1 つまたは複数を指定できます。8bitmime、auth、binaryname、checkpoint、dsn、etrn、others、pipelining、size、vrfy。
- **match** [**not**] **header** {**length** | **line length**} **gt** *bytes*：ESMTP ヘッダーの長さまたは行の長さが指定したバイト数より大きいメッセージと一致します。
- **match** [**not**] **header to-fields count gt** *count*：ヘッダーの To フィールドの数が指定した値より大きいメッセージと一致します。
- **match** [**not**] **invalid-recipients count gt** *number*：無効な受信者の数が指定した値より大きいメッセージと一致します。
- **match** [**not**] **mime filetype regex** {*regex_name* | **class** *class_name*}：MIME またはメディア ファイル タイプを、指定した正規表現または正規表現クラスと照合します。
- **match** [**not**] **mime filename length gt** *bytes*：ファイル名が指定したバイト数より大きいメッセージと一致します。
- **match** [**not**] **mime encoding** *type* [*type2...*]：MIME エンコーディング タイプと一致します。次のタイプの 1 つまたは複数を指定できます。7bit、8bit、base64、binary、others、quoted-printable。
- **match** [**not**] **sender-address regex** {*regex_name* | **class** *class_name*}：送信者の電子メール アドレスを、指定した正規表現または正規表現クラスと照合します。
- **match** [**not**] **sender-address length gt** *bytes*：送信者のアドレスが指定したバイト数より大きいメッセージと一致します。

b. 次のコマンドを入力して、一致したトラフィックに対して実行するアクションを指定します。

```
hostname(config-pmap-c)# {drop-connection [log]| mask [log] | reset [log] | log |
rate-limit message_rate}
```

各 **match** コマンドですべてのオプションを使用できるわけではありません。使用できる正確なオプションについては、CLI ヘルプまたはコマンド リファレンスを参照してください。

- **drop-connection** キーワードを指定すると、パケットをドロップし、接続を閉じます。
- **mask** キーワードを指定すると、パケットの一致部分をマスクします。このアクションは、**ehlo-reply-parameter** および **cmd verb** に対してのみ使用できます。
- **reset** キーワードを指定すると、パケットをドロップして接続を閉じ、サーバとクライアントの両方またはいずれかに TCP リセットを送信します。
- **log** キーワードを指定すると、システム ログ メッセージを送信します。このキーワードは単独で、または他のキーワードのいずれかと一緒に使用できます。
- **rate-limit** *message_rate* 引数では、メッセージのレートを制限します。このオプションは、**cmd verb** のみで使用できます。唯一のアクションとして使用することも、**mask** アクションと組み合わせて使用することもできます。

ポリシー マップでは、複数の **match** コマンドを指定できます。**match** コマンドの順序については、「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.2-4）を参照してください。

ステップ 4　インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a. パラメータ コンフィギュレーション モードに入るには、次のコマンドを入力します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **mail-relay** *domain-name* **action** {**drop-connection** [**log**] | **log**}：メール中継のドメイン名を指定します。接続をドロップし、必要に応じてログに記録できます。または、ログへの記録だけを行うこともできます。
- **mask-banner**：ESMTP サーバからのバナーをマスクします。
- **special-character action** {**drop-connection** [**log**] | **log**}：電子メールの送信者または受信者アドレスに特殊文字パイプ（|）、バック クォート、NUL が含まれるメッセージに対して実行するアクションを指定します。接続をドロップし、必要に応じてログに記録できます。または、ログへの記録だけを行うこともできます。
- **allow-tls** [**action log**]：インスペクションなしで ESMTP over TLS（暗号化された接続）を許可するかどうか。必要に応じて、暗号化された接続をログに記録できます。

例

次の例は、ESMTP インスペクション ポリシー マップを定義する方法を示しています。

```
hostname(config)# regex user1 "user1@cisco.com"
hostname(config)# regex user2 "user2@cisco.com"
hostname(config)# regex user3 "user3@cisco.com"
hostname(config)# class-map type regex senders_black_list
hostname(config-cmap)# description "Regular expressions to filter out undesired senders"
hostname(config-cmap)# match regex user1
hostname(config-cmap)# match regex user2
hostname(config-cmap)# match regex user3

hostname(config)# policy-map type inspect esmtp advanced_esmtp_map
hostname(config-pmap)# match sender-address regex class senders_black_list
hostname(config-pmap-c)# drop-connection log

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect esmtp advanced_esmtp_map

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

ESMTP インスペクション サービス ポリシーの設定

ASA のデフォルトのコンフィギュレーションには、すべてのインターフェイスにグローバルに適用される ESMTP インスペクションが含まれます。インスペクションの設定をカスタマイズする一般的な方法は、デフォルトのグローバル ポリシーをカスタマイズすることです。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

class-map *name*
match *parameter*

例：

```
hostname(config)# class-map esmtp_class_map
hostname(config-cmap)# match access-list esmtp
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　IP オプション インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　ESMTP インスペクションを設定します。

inspect esmtp [*esmtp_policy_map*]

esmtp_policy_map は、オプションの ESMTP インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。ESMTP インスペクション ポリシー マップの作成の詳細については、「ESMTP インスペクション サービス ポリシーの設定」（P.8-48）を参照してください。

例：

```
hostname(config-class)# no inspect esmtp
hostname(config-class)# inspect esmtp esmtp-map
```

（注）　デフォルトのグローバル ポリシー（または使用中の任意のポリシー）を編集して、異なるインスペクション ポリシー マップを使用する場合は、**no inspect esmtp** コマンドで ESMTP インスペクションを除去した後、新しいインスペクション ポリシー マップ名を指定して再度追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

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 読み取り要求（RRQ）、書き込み要求（WRQ）、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。

TFTP インスペクションをイネーブルにする方法については、「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.7-11）を参照してください。

CHAPTER 9

音声とビデオのプロトコルのインスペクション

ここでは、音声とビデオのプロトコルのアプリケーション インスペクションについて説明します。特定のプロトコルに関してインスペクションを使用する必要がある理由、およびインスペクションを適用する全体的な方法については、「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準備」（P.7-1）を参照してください。

CTIQBE インスペクション

CTIQBE プロトコル インスペクションは、NAT、PAT、および双方向 NAT をサポートします。これによって、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが Cisco CallManager と連動し、ASA を越えてコール セットアップを行えるようになります。

TAPI と JTAPI は、多くの Cisco VoIP アプリケーションで使用されます。CTIQBE は、Cisco TSP が Cisco CallManager と通信するために使用されます。

CTIQBE インスペクションをイネーブルにする方法については、「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.7-11）を参照してください。

CTIQBE インスペクションの制限事項

CTIQBE アプリケーション インスペクションの使用時に適用される制限を次にまとめます。

- CTIQBE アプリケーション インスペクションは、**alias** コマンドを使用するコンフィギュレーションをサポートしません。
- CTIQBE コールのステートフル フェールオーバーはサポートされていません。
- **debug ctiqbe** コマンドを入力すると、メッセージの伝送が遅れ、リアルタイム環境のパフォーマンスに影響を与える場合があります。このデバッグまたはログをイネーブルにし、ASA を介して Cisco IP SoftPhone でコール セットアップを完了できない場合は、Cisco IP SoftPhone の動作するシステムで Cisco TSP 設定のタイムアウト値を増やしてください。

次に、CTIQBE アプリケーション インスペクションを特定の事例で使用する際に、特別に注意が必要な事項をまとめます。

- 2 つの Cisco IP SoftPhone が異なる Cisco CallManager に登録されていて、各 CallManager が ASA の異なるインターフェイスに接続されている場合、これら 2 つの電話間のコールは失敗します。
- Cisco IP SoftPhone と比較して Cisco CallManager の方がセキュリティの高いインターフェイス上に配置されている状態で、NAT または外部 NAT が Cisco CallManager IP アドレスに必要な場合、マッピングはスタティックである必要があります。Cisco IP SoftPhone では Cisco CallManager IP アドレスを PC 上の Cisco TSP コンフィギュレーションで明示的に指定することが必要なためです。
- PAT または外部 PAT の使用時に Cisco CallManager IP アドレスを変換する場合、Cisco IP SoftPhone を正常に登録させるには、TCP ポート 2748 を PAT（インターフェイス）アドレスと同じポートにスタティックにマッピングする必要があります。CTIQBE 受信ポート（TCP 2748）は固定されていて、Cisco CallManager、Cisco IP SoftPhone、Cisco TSP のいずれにおいてもユーザによる設定はできません。

CTIQBE インスペクションの確認とモニタリング

show ctiqbe コマンドは、ASA を越えて確立されている CTIQBE セッションに関する情報を表示します。CTIQBE インスペクション エンジンで割り当てられたメディア接続に関する情報が表示されます。

次の条件における **show ctiqbe** コマンドの出力例を示します。ASA を越えてセットアップされているアクティブ CTIQBE セッションは 1 つだけです。そのセッションは、ローカル アドレス 10.0.0.99 の内部 CTI デバイス（たとえば、Cisco IP SoftPhone）と 172.29.1.77 の外部 Cisco CallManager の間で確立されています。ここで、TCP ポート 2748 は、Cisco CallManager です。このセッションのハートビート間隔は 120 秒です。

```
hostname# # show ctiqbe

Total: 1
        LOCAL           FOREIGN         STATE   HEARTBEAT
-----------------------------------------------------------------
1       10.0.0.99/1117  172.29.1.77/2748        1       120
        -----------------------------------------------------------------
        RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 - 1029)
        -----------------------------------------------------------------
        MEDIA: Device ID 27     Call ID 0
               Foreign 172.29.1.99      (1028 - 1029)
               Local   172.29.1.88      (26822 - 26823)
        -----------------------------------------------------------------
```

CTI デバイスは、すでに CallManager に登録されています。デバイスの内部アドレスおよび RTP 受信ポートは 172.29.1.99 の UDP ポート 1028 に PAT 変換されています。RTCP 受信ポートは UDP 1029 に PAT 変換されています。

`RTP/RTCP: PAT xlates:` で始まる行は、内部 CTI デバイスが外部 CallManager に登録され、CTI デバイスのアドレスとポートがその外部インターフェイスに PAT 変換されている場合に限り表示されます。この行は、CallManager が内部インターフェイス上にある場合、または内部 CTI デバイスのアドレスとポートが、CallManager が使用しているのと同じ外部インターフェイスに変換されている場合は、表示されません。

この出力は、コールがこの CTI デバイスと 172.29.1.88 にある別の電話機の間に確立されていることを示します。他の電話機の RTP および RTCP 受信ポートは、UDP 26822 および 26823 です。ASA は 2 番目の電話機と CallManager に関連する CTIQBE セッション レコードを維持できないので、他の電話機は、CallManager と同じインターフェイス上にあります。CTI デバイス側のアクティブ コール レッグは、Device ID 27 および Call ID 0 で確認できます。

これらの CTIQBE 接続の **show xlate debug** コマンドの出力例を示します。

```
hostname# show xlate debug
3 in use, 3 most used
Flags:  D - DNS, d - dump, I - identity, i - inside, n - no random,
        r - portmap, s - static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
```

show conn state ctiqbe コマンドは、CTIQBE 接続のステータスを表示します。出力には、CTIQBE インスペクション エンジンによって割り当てられたメディア接続が「C」フラグで示されます。次に、**show conn state ctiqbe** コマンドの出力例を示します。

```
hostname# show conn state ctiqbe
1 in use, 10 most used
hostname# show conn state ctiqbe detail
1 in use, 10 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, k - Skinny media,
       M - SMTP data, m - SIP media, O - outbound data, P - inside back connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
```

H.323 インスペクション

ここでは、H.323 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。

H.323 インスペクションの概要

H.323 インスペクションは、Cisco CallManager や VocalTec Gatekeeper など、H.323 準拠のアプリケーションをサポートします。H.323 は、国際電気通信連合によって定義されている、LAN を介したマルチメディア会議用のプロトコル群です。ASA は、H.323 v3 機能の同一コール シグナリング チャネルでの複数コールを含めて、H.323 を Version 6 までサポートします。

H.323 インスペクションをイネーブルにした場合、ASA は、H.323 Version 3 で導入された機能である同一コール シグナリング チャネルでの複数コールをサポートします。この機能によってセットアップ時間が短縮され、ASA でのポート使用が減少します。

H.323 インスペクションの 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化形式で符号化されているため、ASA では ASN.1 デコーダを使用して H.323 メッセージを復号化します。
- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。RAS を使用すると、H.225 接続もダイナミックに割り当てることができます。

H.323 の動作

H.323 のプロトコルのコレクションは、合計で最大 2 つの TCP 接続と 4 ～ 8 つの UDP 接続を使用できます。FastConnect は 1 つの TCP 接続だけを使用し、RAS は登録、アドミッション、およびステータス用に 1 つの UDP 接続を使用します。

H.323 クライアントは、最初に TCP ポート 1720 を使用して、H.323 サーバへの TCP 接続を確立し、Q.931 コール セットアップを要求します。H.323 端末は、コール セットアップ プロセスの一部として、H.245 TCP 接続に使用するため、クライアントに 1 つのポート番号を供給します。H.323 ゲートキーパーが使用されている環境では、初期パケットは UDP を使用して送信されます。

H.323 インスペクションは、Q.931 TCP 接続をモニタして、H.245 ポート番号を決定します。H.323 端末が、FastConnect を使用していない場合は、ASA が H.225 メッセージのインスペクションに基づいて、H.245 接続をダイナミックに割り当てます。

（注） RAS を使用すると、H.225 接続もダイナミックに割り当てることができます。

各 H.245 メッセージ内で、H.323 エンドポイントが、後続の UDP データ ストリームに使用するポート番号を交換します。H.323 インスペクションは、H.245 メッセージを調査して、ポート番号を識別し、メディア交換用の接続をダイナミックに作成します。RTP はネゴシエートされたポート番号を使用し、RTCP はその次に高いポート番号を使用します。

H.323 制御チャネルは、H.225、H.245、および H.323 RAS を処理します。H.323 インスペクションでは、次のポートが使用されます。

- 1718：ゲートキーパー検出 UDP ポート
- 1719：RAS UDP ポート
- 1720：TCP 制御ポート

RAS シグナリング用に予約済み H.323 ポート 1719 のトラフィックを許可する必要があります。さらに、H.225 コール シグナリング用に、予約済み H.323 ポート 1720 のトラフィックを許可する必要があります。ただし、H.245 シグナリング ポートは、H.225 シグナリングのエンドポイント間でネゴシエートされます。H.323 ゲートキーパーの使用時、ASA は、ACF メッセージと RCF メッセージのインスペクションに基づいて H.225 接続を開きます。

H.225 メッセージを検査した後、ASA は H.245 チャネルを開き、H.245 チャネルで送信されるトラフィックも検査します。ASA を通過するすべての H.245 メッセージは、H.245 アプリケーション インスペクションを受けます。このインスペクションでは、埋め込み IP アドレスが変換され、H.245 メッセージでネゴシエートされたメディア チャネルが開かれます。

H.323 ITU 規準では、メッセージ長を定義する TPKT ヘッダーが最初に送信されてから、H.225 と H.245 が信頼できる接続上を送信されることが要求されています。TPKT ヘッダーは、必ずしも H.225 メッセージや H.245 メッセージと同一の TCP パケットで送信される必要はないため、ASA は、メッセージを正しく処理して復号化するために TPKT 長を記憶しておく必要があります。ASA は、次のメッセージに備えて、TPKT 長が含まれるレコードを接続ごとに保持します。

ASA でメッセージ内の IP アドレスに NAT を行う必要がある場合、チェックサム、UUIE 長、および TPKT（H.225 メッセージが入っている TCP パケットに含まれている場合）は変更されます。TPKT が別の TCP パケットで送信される場合、ASA がその TPKT へのプロキシ ACK を実行し、新しい TPKT を新しい長さで H.245 メッセージに追加します。

（注） ASA は、TPKT に対する ACK の代理処理では TCP オプションをサポートしていません。

H.323 インスペクションを通過するパケットが通る各 UDP 接続は、H.323 接続としてマークされ、**timeout** コマンドで設定された H.323 タイムアウト値でタイムアウトします。

（注） ゲートキーパーがネットワーク内にある場合は、H.323 エンドポイント間のコール セットアップをイネーブルにできます。ASA には、RegistrationRequest/RegistrationConfirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開くオプションが含まれています。これらの RRQ/RCF メッセージは ゲートキーパーとの間で送受信されるので、発信側エンドポイントの IP アドレスは不明で、ASA は発信元 IP アドレス/ポート 0/0 を通じてピンホールを開きます。デフォルトでは、このオプションは無効になっています。H.323 エンドポイント間のコール セットアップをイネーブルにするには、H.323 インスペクション ポリシー マップの作成時に、パラメータ コンフィギュレーション モードで **ras-rcf-pinholes enable** コマンドを入力します。「H.323 インスペクション ポリシー マップの設定」（P.9-7）を参照してください。

H.245 メッセージでの H.239 サポート

ASA は、2 つの H.323 エンドポイントの間に存在します。2 つの H.323 エンドポイントが、スプレッドシート データなどのデータ プレゼンテーションを送受信できるようにテレプレゼンテーション セッションをセットアップするとき、ASA はエンドポイント間で H.239 ネゴシエーションが成功することを保証します。

H.239 は、H.300 シリーズ エンドポイントが 1 回のコールで追加ビデオ チャネルを開くことができる機能を提供する規格です。コールで、エンドポイント（ビデオ電話など）はビデオ用チャネルとデータ プレゼンテーション用チャネルを送信します。H.239 ネゴシエーションは H.245 チャネルで発生します。

ASA が追加メディア チャネル用とメディア制御チャネル用のピンホールを開きます。エンドポイントは、オープン論理チャネル メッセージ（OLC）を使用して新しいチャネルの作成を通知します。メッセージ拡張は H.245 バージョン 13 の一部です。

テレプレゼンテーション セッションの復号化と符号化は、デフォルトでイネーブルにされています。H.239 の符号化と復号化は ASN.1 コーダによって実行されます。

H.323 インスペクションの制限事項

H.323 インスペクションは、Cisco Unified Communications Manager (CUCM) 7.0 でテストおよびサポートされています。CUCM 8.0 以降ではサポートされません。H.323 インスペクションは、他のリリースや製品で機能する場合があります。

H.323 アプリケーション インスペクションの使用に関して、次の既知の問題および制限があります。

- 完全にサポートされているのは、スタティック NAT だけです。スタティック PAT は、H.323 メッセージのオプション フィールドに埋め込まれた IP アドレスを正しく変換できないことがあります。この問題が発生した場合は、H.323 でスタティック PAT を使用しないでください。
- ダイナミック NAT または PAT ではサポートされません。
- 拡張 PAT ではサポートされません。
- セキュリティ レベルが同一のインターフェイス間の NAT ではサポートされません。
- 外部 NAT ではサポートされません。
- NAT64 ではサポートされません。
- NetMeeting クライアントが H.323 ゲートキーパーに登録し、同じく H.323 ゲートキーパーに登録されている H.323 ゲートウェイを呼び出そうとすると、接続は確立されますが、どちらの方向でも音声が聞こえません。この問題は、ASA の問題ではありません。
- ネットワーク スタティック アドレスを設定した場合、このネットワーク スタティック アドレスが第三者のネットマスクおよびアドレスと同じであると、すべての発信 H.323 接続が失敗します。

H.323 インスペクションの設定

H.323 インスペクションは RAS、H.225、H.245 をサポートし、埋め込まれた IP アドレスとポートをすべて変換する機能を備えています。ステートのトラッキングとフィルタリングを実行し、インスペクション機能のアクティベーションをカスケードできます。H.323 インスペクションは、電話番号のフィルタリング、T.120 のダイナミック制御、H.245 のトンネル機能制御、HSI グループ、プロトコルのステート トラッキング、H.323 通話時間制限の適用、音声/ビデオ制御をサポートします。

H.323 検査はデフォルトではイネーブルです。デフォルト以外の処理が必要な場合にのみ設定する必要があります。H.323 インスペクションをカスタマイズする場合は、次のプロセスを使用します。

手順

ステップ 1　「H.323 インスペクション ポリシー マップの設定」（P.9-7）

ステップ 2　「H.323 インスペクション サービス ポリシーの設定」（P.9-10）

H.323 インスペクション ポリシー マップの設定

ネットワークに対してデフォルトのインスペクション動作が十分でない場合は、H.323 インスペクション ポリシー マップを作成して H.323 インスペクションのアクションをカスタマイズできます。

トラフィックの一致基準を定義するときに、クラス マップを作成するか、またはポリシー マップに match ステートメントを直接含めることができます。次の手順では、両方の方法について説明します。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　（任意）次の手順に従って、H.323 インスペクションのクラス マップを作成します。

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。代わりに、ポリシー マップで **match** コマンドを直接指定できます。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 マップでトラフィックと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ことです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

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 マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシー マップに直接トラフィックを特定する必要があります。

a. 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 type inspect h323 [match-all | match-any] class_map_name
hostname(config-cmap)#
```

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。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。**match-any** キーワードは、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。CLI がクラスマップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b. （任意）クラス マップに説明を追加するには、次のコマンドを使用します。

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

string には、クラス マップの説明を 200 文字以内で指定します。

c. 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **called-party regex** {*regex_name* | **class** *class_name*}：指定した正規表現または正規表現クラスに対して着信側を照合します。
- **match** [**not**] **calling-party regex** {*regex_name* | **class** *class_name*}：指定した正規表現または正規表現クラスに対して発信側を照合します。
- **match** [**not**] **media-type** {**audio** | **data** | **video**}：メディア タイプを照合します。

ステップ 2　H.323 インスペクション ポリシー マップを作成します。

```
hostname(config)# policy-map type inspect h323 policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3　（任意）このポリシー マップに説明を追加するには、次のコマンドを使用します。

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

ステップ 4　一致したトラフィックにアクションを適用するには、次の手順を実行します。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、「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.2-4）を参照してください。

a.　次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- H.323 クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。

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

- H.323 クラス マップで記述された **match** コマンドの 1 つを使用して、ポリシー マップでトラフィックを直接指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b.　次のコマンドを入力して、一致したトラフィックに対して実行するアクションを指定します。

```
hostname(config-pmap-c)# {drop [log] | drop-connection | reset}
```

drop キーワードはパケットをドロップします。メディア タイプの照合の場合、**log** キーワードを含めてシステム ログ メッセージを送信できます。

drop-connection キーワードを指定すると、パケットをドロップし、接続を閉じます。このオプションは、着信側または発信側の照合に使用できます。

reset キーワードを指定すると、パケットをドロップして接続を閉じ、サーバとクライアントの両方またはいずれかに TCP リセットを送信します。このオプションは、着信側または発信側の照合に使用できます。

ステップ 5　インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a.　パラメータ コンフィギュレーション モードに入るには、次のコマンドを入力します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b.　1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **ras-rcf-pinholes enable**：H.323 エンドポイント間のコール セットアップをイネーブルにします。ゲートキーパーがネットワーク内にある場合は、H.323 エンドポイント間のコール セットアップをイネーブルにできます。RegistrationRequest/RegistrationConfirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開くには、このオプションを使用します。これらの RRQ/RCF メッセージは ゲートキーパーとの間で送受信されるので、発信側エンドポイントの IP アドレスは不明で、ASA は発信元 IP アドレス/ポート 0/0 を通じてピンホールを開きます。デフォルトでは、このオプションは無効になっています。

- **timeout users** *time*：H.323 コールの制限時間（hh: mm: ss 形式）を設定します。タイムアウトを付けない場合は、00:00:00 を指定してください。範囲は、0:0:0 ～ 1193:0:0 です。
- **call-party-number**：コール設定時に発信側の番号を強制的に送信します。
- **h245-tunnel-block action {drop-connection | log}**：H.245 トンネル ブロッキングを適用します。接続をドロップするか、単にログに記録するだけかを選択します。
- **rtp-conformance [enforce-payloadtype]**：ピンホール上を流れる RTP パケットのプロトコル準拠をチェックします。オプションの **enforce-payloadtype** キーワードを指定すると、シグナリング交換に基づいてペイロード タイプを強制的に音声やビデオにします。
- **state-checking {h225 | ras}**：ステート チェック検証をイネーブルにします。個別にコマンドを入力して、H.225 および RAS のステート チェックをイネーブルにすることができます。

ステップ 6　パラメータ コンフィギュレーション モードのままで、HSI グループを設定できます。

a. HSI グループを定義し、HSI グループ コンフィギュレーション モードを開始します。

```
hostname(config-pmap-p)# hsi-group id
```

id には、HSI グループ ID を指定します。範囲は 0 ～ 2147483647 です。

b. IP アドレスを使用して HSI を HSI グループに追加します。HSI グループあたり最大 5 つのホストを追加できます。

```
hostname(config-h225-map-hsi-grp)# hsi ip_address
```

c. HSI グループにエンドポイントを追加します。

```
hostname(config-h225-map-hsi-grp)# endpoint ip_address if_name
```

ip_address には追加するエンドポイント、*if_name* にはエンドポイントを ASA に接続するときに使用するインターフェイスを指定します。HSI グループあたり最大 10 個のエンドポイントを追加できます。

例

次の例は、電話番号のフィルタリングを設定する方法を示しています。

```
hostname(config)# regex caller 1 "5551234567"
hostname(config)# regex caller 2 "5552345678"
hostname(config)# regex caller 3 "5553456789"

hostname(config)# class-map type inspect h323 match-all h323_traffic
hostname(config-pmap-c)# match called-party regex caller1
hostname(config-pmap-c)# match calling-party regex caller2

hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# class h323_traffic
hostname(config-pmap-c)# drop
```

H.323 インスペクション サービス ポリシーの設定

デフォルトの ASA 設定には、すべてのインターフェイスでグローバルに適用されるデフォルト ポートでの H.323 H.255、および RAS のインスペクションが含まれます。インスペクションの設定をカスタマイズする一般的な方法は、デフォルトのグローバル ポリシーをカスタマイズすることです。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

class-map *name*
match *parameter*

例：

```
hostname(config)# class-map h323_class_map
hostname(config-cmap)# match access-list h323
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　H.323 インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　H.323 インスペクションを設定します。

inspect h323 {**h255** | **ras**} [*h323_policy_map*]

h323_policy_map は、オプションの H.323 インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。H.323 インスペクション ポリシー マップの作成の詳細については、「H.323 インスペクション ポリシー マップの設定」（P.9-7）を参照してください。

例：

```
hostname(config-class)# no inspect h323 h225
hostname(config-class)# no inspect h323 ras
hostname(config-class)# inspect h255 h323-map
hostname(config-class)# inspect ras h323-map
```

（注）　デフォルトのグローバル ポリシー（または使用中の任意のポリシー）を編集して、異なる H.323 インスペクション ポリシー マップを使用する場合は、**no inspect h323** コマンドで H.323 インスペクションを除去した後、新しい H.323 インスペクション ポリシー マップ名を指定して再度追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

H.323 および H.225 タイムアウト値の設定

[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ページで H.323/H.255 グローバル タイムアウト値を設定できます。H.255 シグナリング接続を閉じるまでの非アクティブ状態の間隔（デフォルトは 1 時間）または H.323 制御接続を閉じるまでの非アクティブ状態間隔（デフォルトは 5 分）を設定できます。

H.225 シグナリング接続を閉じるまでのアイドル時間を設定するには、**timeout h225** コマンドを使用します。H.225 タイムアウトのデフォルトは 1 時間です。

H.323 制御接続を閉じるまでのアイドル時間を設定するには、**timeout h323** コマンドを使用します。デフォルトは 5 分です。

H.323 インスペクションの確認とモニタリング

ここでは、H.323 セッションに関する情報を表示する方法について説明します。

- 「H.225 セッションのモニタリング」（P.9-12）
- 「H.245 セッションのモニタリング」（P.9-12）
- 「H.323 RAS セッションのモニタリング」（P.9-13）

H.225 セッションのモニタリング

show h225 コマンドは、ASA を越えて確立されている H.225 セッションの情報を表示します。このコマンドは、**debug h323 h225 event**、**debug h323 h245 event**、および **show local-host** コマンドとともに、H.323 インスペクション エンジンの問題のトラブルシューティングに使用されます。

異常なほど多くの接続が存在する場合は、デフォルトのタイムアウト値または設定した値に基づいてセッションがタイムアウトしているかどうか確認します。タイムアウトしていなければ問題があるので、調査が必要です。

次に、**show h225** コマンドの出力例を示します。

```
hostname# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
    1. CRV 9861
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
    Local:   10.130.56.4/1050   Foreign: 172.30.254.205/1720
```

この出力は、現在 ASA を通過しているアクティブ H.323 コールが 1 つ、ローカル エンドポイント 10.130.56.3 と外部のホスト 172.30.254.203 の間にあることを示しています。また、これらの特定のエンドポイントの間に、同時コールが 1 つあり、そのコールの CRV が 9861 であることを示しています。

ローカル エンドポイント 10.130.56.4 と外部ホスト 172.30.254.205 に対して、同時コールは 0 です。つまり H.225 セッションがまだ存在しているものの、このエンドポイント間にはアクティブ コールがないことを意味します。この状況は、**show h225** コマンドを実行したときに、コールはすでに終了しているが、H.225 セッションがまだ削除されていない場合に発生する可能性があります。または、2 つのエンドポイントが、「maintainConnection」を TRUE に設定しているため、TCP 接続をまだ開いたままにしていることを意味する可能性もあります。したがって、「maintainConnection」を再度 FALSE に設定するまで、またはコンフィギュレーション内の H.225 タイムアウト値に基づくセッションのタイムアウトが起こるまで、セッションは開いたままになります。

H.245 セッションのモニタリング

show h245 コマンドは、スロー スタートを使用しているエンドポイントが ASA を越えて確立した H.245 セッションの情報を表示します。スロー スタートは、コールの 2 つのエンドポイントが H.245 用の別の TCP コントロール チャネルを開いた場合です。ファスト スタートは、H.245 メッセージが H.225 コントロール チャネルで H.225 メッセージの一部として交換された場合です。

次に、**show h245** コマンドの出力例を示します。

```
hostname# show h245
Total: 1
        LOCAL            TPKT    FOREIGN          TPKT
1       10.130.56.3/1041         0       172.30.254.203/1245    0
        MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
                       Local   10.130.56.3 RTP 49608 RTCP 49609
        MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
                       Local   10.130.56.3 RTP 49606 RTCP 49607
```

ASAでアクティブな H.245 コントロール セッションが、現在 1 つあります。ローカル エンドポイントは、10.130.56.3 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します。TKTP ヘッダーは、各 H.225/H.245 メッセージの前に送られる 4 バイトのヘッダーです。このヘッダーで、この 4 バイトのヘッダーを含むメッセージの長さがわかります。外部のホストのエンドポイントは、172.30.254.203 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します。

これらのエンドポイント間でネゴシエートされたメディアには、258 という LCN があり、外部に 172.30.254.203/49608 という RTP IP アドレス/ポート ペアと 172.30.254.203/49609 という RTCP IP アドレス/ポート ペアを持ち、ローカルに 10.130.56.3/49608 という RTP IP アドレス/ポート ペアと 49609 という RTCP ポートを持っています。

259 という 2 番目の LCN には、外部に 172.30.254.203/49606 という RTP IP アドレス/ポート ペアと 172.30.254.203/49607 という RTCP IP アドレス/ポート ペアがあり、ローカルに 10.130.56.3/49606 という RTP IP アドレス/ポート ペアと 49607 という RTCP ポートを持っています。

H.323 RAS セッションのモニタリング

show h323-ras コマンドは、ASA を越えてゲートキーパーとその H.323 エンドポイントの間に確立されている H.323 RAS セッションの接続情報を表示します。このコマンドは、**debug h323 ras event** および **show local-host** コマンドとともに、H.323 RAS インスペクション エンジンの問題のトラブルシューティングに使用されます。

次に、**show h323-ras** コマンドの出力例を示します。

```
hostname# show h323-ras
Total: 1
        GK                      Caller
        172.30.254.214 10.130.56.14
```

この出力は、ゲートキーパー 172.30.254.214 とそのクライアント 10.130.56.14 の間にアクティブな登録が 1 つあることを示しています。

MGCP インスペクション

ここでは、MGCP 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。

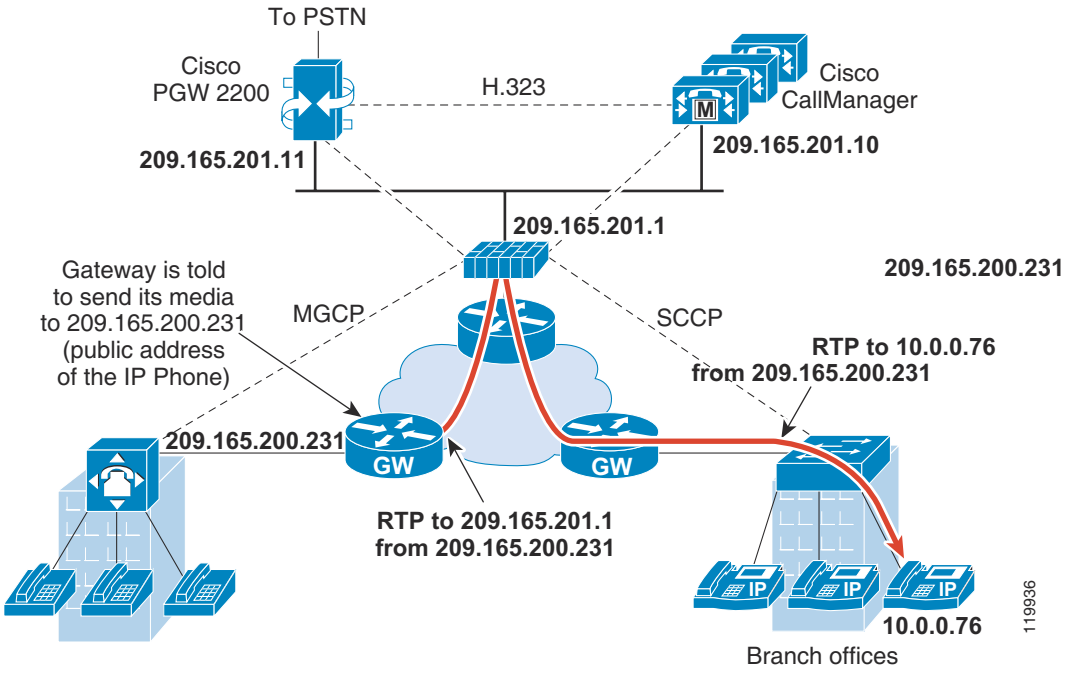
MGCP インスペクションの概要

MGCP は、メディア ゲートウェイ コントローラまたはコール エージェントと呼ばれる外部のコール制御要素からメディア ゲートウェイを制御するために使用するマスター /スレーブ プロトコルです。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。NAT および PAT を MGCP とともに使用すると、限られた外部（グローバル）アドレスのセットで、内部ネットワークの多数のデバイスをサポートできます。メディア ゲートウェイの例は次のとおりです。

- トランキング ゲートウェイ。電話ネットワークと Voice over IP ネットワークとの間のインターフェイスです。このようなゲートウェイは通常、大量のデジタル回線を管理します。
- 住宅用ゲートウェイ。従来のアナログ（RJ11）インターフェイスを Voice over IP ネットワークに提供します。住宅用ゲートウェイの例としては、ケーブル モデムやケーブル セットトップ ボックス、xDSL デバイス、ブロードバンド ワイヤレス デバイスなどがあります。
- ビジネス ゲートウェイ。従来のデジタル PBX（構内交換機）インターフェイスまたは統合 soft PBX インターフェイスを Voice over IP ネットワークに提供します。

MGCP メッセージは UDP を介して送信されます。応答はコマンドの送信元アドレス（IP アドレスと UDP ポート番号）に返送されますが、コマンド送信先と同じアドレスからの応答は到達しない場合があります。これは、複数のコール エージェントがフェールオーバー コンフィギュレーションで使用されているときに、コマンドを受信したコール エージェントが制御をバックアップ コール エージェントに引き渡し、バックアップ コール エージェントが応答を送信する場合に起こる可能性があります。次の図は、NAT と MGCP を使用する方法を示しています。

図 9-1　NAT と MGCP の使用



MGCP エンドポイントは、物理または仮想のデータ送信元および宛先です。メディア ゲートウェイには、他のマルチメディア エンドポイントとのメディア セッションを確立して制御するために、コール エージェントが接続を作成、変更、および削除できるエンドポイントが含まれています。また、コール エージェントは、特定のイベントを検出してシグナルを生成するようにエンドポイントに指示できます。エンドポイントは、サービス状態の変化を自動的にコール エージェントに伝達します。

- 通常、ゲートウェイは UDP ポート 2427 をリッスンしてコール エージェントからのコマンドを受信します。
- コール エージェントがゲートウェイからのコマンドを受信するポート。通常、コール エージェントは UDP ポート 2727 をリッスンしてゲートウェイからコマンドを受信します。

（注） MGCP インスペクションでは、MGCP シグナリングと RTP データで異なる IP アドレスを使用することはサポートされていません。一般的かつ推奨される方法は、ループバック IP アドレスや仮想 IP アドレスなどの復元力のある IP アドレスから RTP データを送信することです。ただし、ASA は、MGCP シグナリングと同じアドレスから RTP データを受信する必要があります。

MGCP インスペクションの設定

MGCP インスペクションをイネーブルにするには、次のプロセスを使用します。

手順

ステップ 1　「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.9-15）。

ステップ 2　「MGCP インスペクション サービス ポリシーの設定」（P.9-16）。

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

ASA がピンホールを開く必要のあるコール エージェントとゲートウェイがネットワークに複数ある場合、MGCP マップを作成します。作成した MGCP マップは、MGCP インスペクションをイネーブルにすると適用できます。

手順

ステップ 1　MGCP インスペクション ポリシー マップを作成するには、次のコマンドを入力します。

```
hostname(config)# policy-map type inspect mgcp map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2　（任意）このポリシー マップに説明を追加するには、次のコマンドを使用します。

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

ステップ 3　パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

ステップ 4　1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **call-agent** *ip_address group_id*：1 つ以上のゲートウェイを管理できるコール エージェント グループを設定します。コール エージェントのグループ情報は、どのコール エージェントも応答を送信できるように、グループ内の（ゲートウェイがコマンドを送信する先以外の）コール エージェントに接続を開くために使用されます。同じ *group_id* を持つコール エージェントは、同じグループに属します。1 つのコール エージェントは複数のグループに所属できます。*group_id* オプションには、0 ～ 4294967295 の数字を指定します。*ip_address* オプションには、コール エージェントの IP アドレスを指定します。

  （注）　MGCP コール エージェントは、AUEP メッセージを送信して、MGCP エンドポイントが存在するかどうかを判定します。これによって、ASA を通過するフローが確立され、MGCP エンドポイントをコール エージェントに登録できます。

- **gateway** *ip_address group_id*：特定のゲートウェイを管理しているコール エージェントのグループを指定します。*ip_address* オプションを使用して、ゲートウェイの IP アドレスを指定します。*group_id* オプションには 0 ～ 4294967295 の数字を指定します。この数字は、ゲートウェイを管理しているコール エージェントの *group_id* に対応している必要があります。1 つのゲートウェイは 1 つのグループだけに所属できます。
- **command-queue** *command_limit*：MGCP コマンド キューで許容されるコマンドの最大数（1 ～ 2147483647）を設定します。デフォルトは 200 です。

例

次の例は、MGCP マップを定義する方法を示しています。

```
hostname(config)# policy-map type inspect mgcp sample_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-agent 10.10.11.5 101
hostname(config-pmap-p)# call-agent 10.10.11.6 101
hostname(config-pmap-p)# call-agent 10.10.11.7 102
hostname(config-pmap-p)# call-agent 10.10.11.8 102
hostname(config-pmap-p)# gateway 10.10.10.115 101
hostname(config-pmap-p)# gateway 10.10.10.116 102
hostname(config-pmap-p)# gateway 10.10.10.117 102
hostname(config-pmap-p)# command-queue 150
```

MGCP インスペクション サービス ポリシーの設定

MGCP インスペクションは、デフォルトのインスペクション ポリシーでイネーブルになっていないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの MGCP ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで MGCP インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

```
class-map name
match parameter
```

例：

```
hostname(config)# class-map mgcp_class_map
hostname(config-cmap)# match access-list mgcp
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

```
policy-map name
```

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　MGCP インスペクションに使用する L3/L4 クラス マップを指定します。

```
class name
```

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　MGCP インスペクションを設定します。

```
inspect mgcp [mgcp_policy_map]
```

mgcp_policy_map は、オプションの MGCP インスペクション ポリシー マップです。MGCP インスペクション ポリシー マップの作成の詳細については、「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.9-15）を参照してください。

例：

```
hostname(config-class)# no inspect mgcp
hostname(config-class)# inspect mgcp mgcp-map
```

（注）　デフォルトのグローバル ポリシー（または使用中の任意のポリシー）を編集して、異なる MGCP インスペクション ポリシー マップを使用する場合は、**no inspect mgcp** コマンドで MGCP インスペクションを除去した後、新しい MGCP インスペクション ポリシー マップ名を指定して再度追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

MGCP タイムアウト値の設定

[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ページで複数の MGCP グローバル タイムアウト値を設定できます。MGCP メディア接続を閉じるまでの非アクティブ状態の間隔を設定できます（デフォルトは 5 分）。PAT xlate のタイムアウトを設定することもできます（30 秒）。

timeout mgcp コマンドを使用して、MGCP メディア接続を閉じるまでの非アクティブ状態の間隔を設定できます。デフォルトは 5 分です。

timeout mgcp-pat コマンドを使用して、PAT xlate のタイムアウトを設定できます。MGCP にはキープアライブ メカニズムがないため、Cisco 以外の MGCP ゲートウェイ（コール エージェント）を使用すると、デフォルトのタイムアウト間隔（30 秒）の後で PAT xlate は切断されます。

MGCP インスペクションの確認とモニタリング

show mgcp commands コマンドは、コマンド キュー内の MGCP コマンド数を表示します。**show mgcp sessions** コマンドは、既存の MGCP セッション数を表示します。**detail** オプションは、各コマンド（またはセッション）に関する追加情報を出力に含めます。次に、**show mgcp commands** コマンドの出力例を示します。

```
hostname# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
```

次に、**show mgcp detail** コマンドの出力例を示します。

```
hostname# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
        Gateway IP      host-pc-2
        Transaction ID  2052
        Endpoint name   aaln/1
```

```
        Call ID         9876543210abcdef
        Connection ID
        Media IP        192.168.5.7
        Media port      6058
```

次に、**show mgcp sessions** コマンドの出力例を示します。

```
hostname# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
```

次に、**show mgcp sessions detail** コマンドの出力例を示します。

```
hostname# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
        Gateway IP      host-pc-2
        Call ID         9876543210abcdef
        Connection ID   6789af54c9
        Endpoint name   aaln/1
        Media lcl port  6166
        Media rmt IP    192.168.5.7
        Media rmt port  6058
```

RTSP インスペクション

ここでは、RTSP 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。

RTSP インスペクションの概要

RTSP インスペクション エンジンを使用することにより、ASA は RTSP パケットを通過させることができます。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV の各接続で使用されます。

（注）　Cisco IP/TV では、RTSP TCP ポート 554 および 8554 を使用します。

RTSP アプリケーションは、制御チャネルとしての TCP（例外的に UDP）とともに予約済みポート 554 を使用します。ASA は、RFC 2326 に準拠して、TCP だけをサポートします。この TCP 制御チャネルは、クライアント上で設定されているトランスポート モードに応じて、音声/ビデオ トラフィックの送信に使用されるデータ チャネルのネゴシエーションに使用されます。

サポートされている RDT トランスポートは、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、x-pn-tng/udp です。

ASA は、ステータス コード 200 の SETUP 応答メッセージを解析します。SETUP 応答メッセージが、着信方向に移動している場合、サーバは ASA との相対位置関係で外部に存在することになるため、サーバから着信する接続に対してダイナミック チャネルを開くことが必要になります。この応答メッセージが発信方向である場合、ASA は、ダイナミック チャネルを開く必要はありません。

RFC 2326 では、クライアント ポートとサーバ ポートが、SETUP 応答メッセージ内に含まれていることは必要でないため、ASA では、状態を維持し、SETUP メッセージ内のクライアント ポートを記憶します。QuickTime が、SETUP メッセージ内にクライアント ポートを設定すると、サーバは、サーバ ポートだけで応答します。

RTSP インスペクションは、PAT またはデュアル NAT をサポートしていません。また、ASA は、RTSP メッセージが HTTP メッセージ内に隠される HTTP クローキングを認識できません。

RealPlayer 設定要件

RealPlayer を使用するときは、転送モードを正しく設定することが重要です。ASA では、サーバからクライアントに、またはその逆に **access-list** コマンドを追加します。RealPlayer の場合、[Options] > [Preferences] > [Transport] > [RTSP] [Settings] をクリックして転送モードを変更します。

RealPlayer で TCP モードを使用する場合は、[Use TCP to Connect to Server] チェックボックスおよび [Attempt to use TCP for all content] チェックボックスをオンにします。ASA で、インスペクション エンジンを設定する必要はありません。

RealPlayer で UDP モードを使用する場合、[Use TCP to Connect to Server] および [Attempt to use UDP for static content] チェックボックスをオンにします。マルチキャストでの使用ができないライブ コンテンツについては、ASA で、**inspect rtsp** *port* コマンドを追加します。

RSTP インスペクションの制限事項

RSTP インスペクションには次の制限が適用されます。

- ASA は、マルチキャスト RTSP または UDP による RTSP メッセージをサポートしません。
- ASA には、RTSP メッセージが HTTP メッセージ内に隠されている HTTP クローキングを認識する機能はありません。
- 埋め込み IP アドレスが HTTP メッセージまたは RTSP メッセージの一部として SDP ファイル内に含まれているため、ASA は、RTSP メッセージに NAT を実行できません。パケットはフラグメント化できますが、ASA ではフラグメント化されたパケットに対して NAT を実行することはできません。
- Cisco IP/TV では、メッセージの SDP 部分に対して ASA が実行する変換の数は、Content Manager にあるプログラム リストの数に比例します（各プログラム リストには、少なくとも 6 個の埋め込み IP アドレスを含めることができます）。
- Apple QuickTime 4 または RealPlayer 用の NAT を設定できます。Cisco IP/TV は、ビューアと Content Manager が外部ネットワークにあり、サーバが内部ネットワークにあるときにだけ NAT を使用できます。

RTSP インスペクションの設定

RTSP 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。デフォルト以外の処理が必要な場合にのみ設定する必要があります。RTSP インスペクションをカスタマイズする場合は、次のプロセスを使用します。

手順

ステップ 1　「RTSP インスペクション ポリシー マップの設定」（P.9-21）

ステップ 2　「RTSP インスペクション サービス ポリシーの設定」（P.9-23）

RTSP インスペクション ポリシー マップの設定

ネットワークに対してデフォルトのインスペクション動作が十分でない場合は、RTSP インスペクション ポリシー マップを作成して RTSP インスペクションのアクションをカスタマイズできます。

トラフィックの一致基準を定義するときに、クラス マップを作成するか、またはポリシー マップに match ステートメントを直接含めることができます。次の手順では、両方の方法について説明します。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　（任意）次の手順に従って、RTSP インスペクションのクラス マップを作成します。

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。代わりに、ポリシー マップで **match** コマンドを直接指定できます。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 マップでトラフィックと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ことです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

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 マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシー マップに直接トラフィックを特定する必要があります。

a. 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 type inspect rtsp [match-all | match-any] class_map_name
hostname(config-cmap)#
```

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。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。**match-any** キーワードは、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。CLI がクラスマップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b. （任意）クラス マップに説明を追加するには、次のコマンドを使用します。

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

c. 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **request-method** *method*：RTSP 要求方式を照合します。要求方式は、announce、describe、get_parameter、options、pause、play、record、redirect、setup、set_parameter、teardown です。
- **match** [**not**] **url-filter regex** {*regex_name* | **class** *class_name*}：指定した正規表現または正規表現クラスに対して URL を照合します。

ステップ 2　RTSP インスペクション ポリシー マップを作成するには、次のコマンドを入力します。

```
hostname(config)# policy-map type inspect rtsp policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3　（任意）このポリシー マップに説明を追加するには、次のコマンドを使用します。

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

ステップ 4　一致したトラフィックにアクションを適用するには、次の手順を実行します。

a. 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- RTSP クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。

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

- RTSP クラス マップで記述された **match** コマンドの 1 つかを使用して、ポリシー マップでトラフィックを直接指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b. 次のコマンドを入力して、一致したトラフィックに対して実行するアクションを指定します。

```
hostname(config-pmap-c)# {drop-connection [log] | log | rate-limit message_rate}
```

drop-connection キーワードを指定すると、パケットをドロップし、接続を閉じます。このオプションは、URL のマッチングに使用できます。

単独または **drop-connection** と一緒に使用できる **log** キーワードからシステム ログ メッセージが送信されます。

rate-limit *message_rate* 引数では、1 秒あたりのメッセージのレートを制限します。このオプションは、要求方式の照合に使用できます。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、「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.2-4）を参照してください。

ステップ 5　インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a. パラメータ コンフィギュレーション モードに入るには、次のコマンドを入力します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **reserve-port-protect**：メディア ネゴシエーション中の予約ポートの使用を制限します。
- **url-length-limit** *bytes*：メッセージで使用できる URL の長さを 0 ～ 6000 バイトで設定します。

例

次の例は、RTSP インスペクション ポリシー マップを定義する方法を示しています。

```
hostname(config)# regex badurl1 www.url1.com/rtsp.avi
hostname(config)# regex badurl2 www.url2.com/rtsp.rm
hostname(config)# regex badurl3 www.url3.com/rtsp.asp

hostname(config)# class-map type regex match-any badurl-list
hostname(config-cmap)# match regex badurl1
hostname(config-cmap)# match regex badurl2
hostname(config-cmap)# match regex badurl3

hostname(config)# policy-map type inspect rtsp rtsp-filter-map
hostname(config-pmap)# match url-filter regex class badurl-list
hostname(config-pmap-p)# drop-connection

hostname(config)# class-map rtsp-traffic-class
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map rtsp-traffic-policy
hostname(config-pmap)# class rtsp-traffic-class
hostname(config-pmap-c)# inspect rtsp rtsp-filter-map

hostname(config)# service-policy rtsp-traffic-policy global
```

RTSP インスペクション サービス ポリシーの設定

ASA のデフォルトの設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの RTSP インスペクションが含まれます。インスペクションの設定をカスタマイズする一般的な方法は、デフォルトのグローバル ポリシーをカスタマイズすることです。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

class-map *name*
match *parameter*

例：

```
hostname(config)# class-map rtsp_class_map
hostname(config-cmap)# match access-list rtsp
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　RTSP インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　RTSP インスペクションを設定します。

inspect rtsp [*rtsp_policy_map*]

rtsp_policy_map は、オプションの RTSP インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。RTSP インスペクション ポリシー マップの作成の詳細については、「RTSP インスペクション ポリシー マップの設定」（P.9-21）を参照してください。

例：

```
hostname(config-class)# no inspect rtsp
hostname(config-class)# inspect rtsp rtsp-map
```

（注）　デフォルトのグローバル ポリシー（または使用中の任意のポリシー）を編集して、異なる RTSP インスペクション ポリシー マップを使用する場合は、**no inspect rtsp** コマンドで RTSP インスペクションを除去した後、新しい RTSP インスペクション ポリシー マップ名を指定して再度追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

SIP インスペクション

SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、およびインスタント メッセージングに広く使用されているプロトコルです。テキストベースの性質とその柔軟性により、SIP ネットワークは数多くのセキュリティ脅威にさらされます。

SIP アプリケーション インスペクションでは、メッセージ ヘッダーおよび本文のアドレス変換、ポートの動的なオープン、および基本的な健全性チェックが行われます。SIP メッセージの健全性を実現するアプリケーション セキュリティおよびプロトコルへの準拠と、SIP ベースの攻撃の検出もサポートされます。

SIP 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。SCCP インスペクションは、デフォルト以外の処理が必要な場合、または暗号化されたトラフィックのインスペクションをイネーブルにするために TLS プロキシを設定する場合にのみ設定する必要があります。ここでは、SIP インスペクションについてより詳細に説明します。

SIP インスペクションの概要

IETF で定義されている SIP により、特に 2 者間の音声会議などのコール処理セッションまたは「コール」が使用可能になります。SIP は、コール シグナリング用の SDP で動作します。SDP は、メディア ストリーム用のポートを指定します。SIP を使用することにより、ASA は SIP VoIP ゲートウェイおよび VoIP プロキシ サーバをサポートできます。SIP と SDP の定義は、次の RFC に記載されています。

- SIP：Session Initiation Protocol、RFC 3261
- SDP：Session Description Protocol、RFC 2327

ASA 経由の SIP コールをサポートする場合は、シグナリング メッセージは予約済みの宛先ポート（UDP/TCP 5060）経由で送信され、メディア ストリームはダイナミックに割り当てられるため、メディア接続アドレスのシグナリング メッセージ、メディア ポート、およびメディアの初期接続を検査する必要があります。また、SIP は、IP パケットのユーザデータ部分に IP アドレスを埋め込みます。ASA がサポートする SIP 要求 URI の最大長は 255 であることに注意してください。

SIP インスペクションの制限事項

SIP インスペクションは、埋め込まれた IP アドレスに NAT を適用します。ただし、送信元と宛先両方のアドレスを変換するように NAT を設定している場合、外部アドレス（「trying」応答メッセージの SIP ヘッダー内の「from」）は書き換えられません。そのため、宛先アドレスの変換を回避するように SIP トラフィックを使用している場合は、オブジェクト NAT を使用する必要があります。

PAT を SIP で使用する場合、次の制限事項が適用されます。

- ASA で保護されているネットワークの SIP プロキシにリモート エンドポイントを登録しようとすると、次のような一定の条件下で登録が失敗します。
  - PAT がリモート エンドポイント用に設定されている。
  - SIP レジストラ サーバが外部ネットワークにある。
  - エンドポイントからプロキシ サーバに送信された REGISTER メッセージの接続先フィールドにポートが設定されていない。
- SDP 部分の所有者/作成者フィールド（o=）の IP アドレスが接続フィールド（c=）の IP アドレスと異なるパケットを SIP デバイスが送信すると、o= フィールドの IP アドレスが正しく変換されない場合があります。これは、o= フィールドでポート値を提供しない SIP プロトコルの制限によるものです。
- PAT を使用する場合は、ポートを持たない内部 IP アドレスを含む SIP ヘッダー フィールドは変換されない可能性があるため、内部 IP アドレスが外部に漏れます。この漏出を避けるには、PAT の代わりに NAT を設定します。

SIP インスタント メッセージ

インスタント メッセージとは、ほぼリアルタイムにユーザ間でメッセージを転送することです。SIP は、Windows Messenger RTC Client バージョン 4.7.0105 を使用する Windows XP のチャット機能のみをサポートします。次の RFC で定義されているように、MESSAGE/INFO 方式および 202 Accept 応答を使用して IM をサポートします。

- Session Initiation Protocol（SIP）Specific Event Notification、RFC 3265
- Session Initiation Protocol（SIP）Extension for Instant Messaging、RFC 3428

MESSAGE/INFO 要求は、登録または加入の後、任意の時点で着信する可能性があります。たとえば、2 人のユーザはいつでもオンラインになる可能性がありますが、何時間もチャットをすることはありません。そのため、SIP インスペクション エンジンは、設定されている SIP タイムアウト値に従ってタイムアウトするピンホールを開きます。この値は、登録継続時間よりも 5 分以上長く設定する必要があります。登録継続時間は Contact Expires 値で定義し、通常 30 分です。

MESSAGE/INFO 要求は、通常、ポート 5060 以外の動的に割り当てられたポートを使用して送信されるため、SIP インスペクション エンジンを通過する必要があります。

（注）　チャット機能のみがサポートされています。ホワイトボード、ファイル転送、アプリケーション共有はサポートされていません。RTC Client 5.0 はサポートされていません。

SIP インスペクションは、テキストベースの SIP メッセージを変換し、メッセージの SDP 部分の内容長を再計算した後、パケット長とチェックサムを再計算します。また、エンドポイントが受信すべきアドレスまたはポートとして、SIP メッセージの SDP 部分に指定されたポートに対するメディア接続をダイナミックに開きます。

SIP インスペクションでは、SIP ペイロードから取得したインデックス CALL_ID/FROM/TO を持つデータベースが使用されます。これらのインデックスにより、コール、送信元、宛先が識別されます。このデータベースには、SDP のメディア情報フィールド内で見つかったメディア アドレスとメディア ポート、およびメディア タイプが格納されます。1 つのセッションに対して、複数のメディア アドレスとポートが存在することが可能です。ASA は、これらのメディア アドレス/ポートを使用して、2 つのエンドポイント間に RTP/RTCP 接続を開きます。

初期コール セットアップ（INVITE）メッセージでは、予約済みポート 5060 を使用する必要があります。ただし、後続のメッセージにはこのポート番号がない場合もあります。SIP インスペクション エンジンはシグナリング接続のピンホールを開き、それらの接続を SIP 接続としてマークします。これは、SIP アプリケーションに到達した変換対象のメッセージに対して行われます。

コールのセットアップ時に、SIP セッションは、着信側エンドポイントから応答メッセージでメディア アドレスとメディア ポートを受信し、着信側エンドポイントがどの RTP ポートで受信するかを知らされるまで「一時的な」状態にあります。1 分以内に、応答メッセージの受信に障害があった場合は、シグナリング接続は切断されます。

最終的なハンドシェイクが行われると、コール状態はアクティブに移行し、シグナリング接続は、BYE メッセージの受信まで継続されます。

内部エンドポイントが、外部エンドポイントに発呼した場合、メディア ホールが、外部インターフェイスに対して開き、内部エンドポイントから送信された INVITE メッセージで指定された内部エンドポイントのメディア アドレスとメディア ポートに、RTP/RTCP UDP パケットが流れることが許可されます。内部インターフェイスに対する要求外の RTP/RTCP UDP パケットは、ASA のコンフィギュレーションで特別に許可されない限り、ASA を通過できません。

デフォルトの SIP インスペクション

SIP インスペクションはデフォルトでイネーブルになっており、次を含むデフォルトのインスペクション ポリシー マップを使用します。

- SIP インスタント メッセージ（IM）の拡張機能：イネーブル
- SIP トラフィック以外の SIP ポート使用：許可
- サーバとエンドポイントの IP アドレスの非表示：ディセーブル
- ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル
- 1 以上の宛先ホップ カウントを保証：イネーブル
- RTP 準拠：適用強制しない
- SIP 準拠：ステート チェックとヘッダー検証を実行しない

暗号化されたトラフィックのインスペクションがイネーブルになっていないことにも注意してください。暗号化されたトラフィックを検査するには、TLS プロキシを設定する必要があります。

SIP インスペクションの設定

SIP アプリケーション インスペクションでは、メッセージ ヘッダーおよび本文のアドレス変換、ポートの動的なオープン、および基本的な健全性チェックが行われます。SIP メッセージの健全性を実現するアプリケーション セキュリティおよびプロトコルへの準拠と、SIP ベースの攻撃の検出もサポートされます。

SIP 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。SCCP インスペクションは、デフォルト以外の処理が必要な場合、または暗号化されたトラフィックのインスペクションをイネーブルにするために TLS プロキシを設定する場合にのみ設定する必要があります。SIP インスペクションをカスタマイズする場合は、次のプロセスを使用します。

手順

ステップ 1　「SIP インスペクション ポリシー マップの設定」（P.9-28）

ステップ 2　「SIP インスペクション サービス ポリシーの設定」（P.9-32）

SIP インスペクション ポリシー マップの設定

ネットワークに対してデフォルトのインスペクション動作が十分でない場合は、SIP インスペクション ポリシー マップを作成して SIP インスペクションのアクションをカスタマイズできます。

トラフィックの一致基準を定義するときに、クラス マップを作成するか、またはポリシー マップに match ステートメントを直接含めることができます。次の手順では、両方の方法について説明します。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　（任意）次の手順に従って、SIP インスペクションのクラス マップを作成します。

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。代わりに、ポリシー マップで **match** コマンドを直接指定できます。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 マップでトラフィックと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ことです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

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 マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシー マップに直接トラフィックを特定する必要があります。

a. 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 type inspect sip [match-all | match-any] class_map_name
hostname(config-cmap)#
```

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。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。match-any キーワードは、トラフィックが少なくとも 1 つの **match** ステートメントと一致したらクラス マップと一致することを指定します。CLI がクラス マップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b. （任意）クラス マップに説明を追加するには、次のコマンドを使用します。

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

string には、クラス マップの説明を 200 文字以内で指定します。

c. 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **called-party regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対して、To ヘッダーで指定された着信側を照合します。
- **match** [**not**] **calling-party regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対して、From ヘッダーで指定された発信側を照合します。
- **match** [**not**] **content length gt** *bytes*：SIP ヘッダーのコンテンツの長さが指定されたバイト数（0 ～ 65536）を超えているメッセージを照合します。
- **match** [**not**] **content type** {**sdp** | **regex** {*regex_name* | **class** *class_name*}：コンテンツ タイプを SDP として、または指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **im-subscriber regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対して SIP IM サブスクライバを照合します。
- **match** [**not**] **message-path regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対して SIP via ヘッダーを照合します。
- **match** [**not**] **request-method** *method*：ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update の SIP 要求方式を照合します。

- **match [not] third-party-registration regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対してサードパーティ登録の要求者を照合します。
- **match [not] uri {sip | tel} length gt** *bytes*：指定された長さ（0 ～ 65536 バイト）を超えている、選択したタイプ（SIP または TEL）の SIP ヘッダーの URI を照合します。

d. クラス マップ コンフィギュレーション モードを終了するには、「**exit**」と入力します。

ステップ 2　SIP インスペクション ポリシー マップを作成するには、次のコマンドを入力します。

```
hostname(config)# policy-map type inspect sip policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3　（任意）このポリシー マップに説明を追加するには、次のコマンドを使用します。

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

ステップ 4　一致したトラフィックにアクションを適用するには、次の手順を実行します。

a. 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- SIP クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。

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

- SIP クラス マップで記述された **match** コマンドの 1 つを使用して、ポリシー マップでトラフィックを直接指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b. 次のコマンドを入力して、一致したトラフィックに対して実行するアクションを指定します。

```
hostname(config-pmap-c)# {[drop | drop-connection | reset] [log] |
rate-limit message_rate}
```

各 **match** コマンドまたは **class** コマンドですべてのオプションを使用できるわけではありません。使用できる正確なオプションについては、CLI ヘルプまたはコマンド リファレンスを参照してください。

drop キーワードを指定すると、一致するすべてのパケットをドロップします。

drop-connection キーワードを指定すると、パケットをドロップし、接続を閉じます。

reset キーワードを指定すると、パケットをドロップして接続を閉じ、サーバとクライアントの両方またはいずれかに TCP リセットを送信します。

log キーワードを指定すると、システム ログ メッセージを送信します。このキーワードは単独で、または他のキーワードのいずれかと一緒に使用できます。

rate-limit *message_rate* 引数では、メッセージのレートを制限します。レート制限は、「invite」および「register」に一致する要求方式の場合にのみ使用できます。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、「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.2-4）を参照してください。

ステップ 5　インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a. パラメータ コンフィギュレーション モードに入るには、次のコマンドを入力します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **im**：インスタント メッセージングをイネーブルにします。
- **ip-address-privacy**：IP アドレスのプライバシーをイネーブルにし、サーバとエンドポイントの IP アドレスを非表示にします。
- **max-forwards-validation action** {**drop** | **drop-connection** | **reset** | **log**} [**log**]：これにより、宛先に到達するまで 0 にすることができない Max-Forwards ヘッダーの値がチェックされます。また、不適合なトラフィックに対して実行するアクション（パケットのドロップ、接続のドロップ、リセット、またはログ）と、ロギングをイネーブルまたはディセーブルのどちらにするかを選択する必要もあります。
- **rtp-conformance** [**enforce-payloadtype**]：ピンホール上を流れる RTP パケットのプロトコル準拠をチェックします。オプションの **enforce-payloadtype** キーワードを指定すると、シグナリング交換に基づいてペイロード タイプを強制的に音声やビデオにします。
- **software-version action** {**mask** [**log**] | **log**}：Server および User-Agent（エンドポイント）ヘッダー フィールドを使用するソフトウェア バージョンを識別します。SIP メッセージのソフトウェア バージョンをマスクしてオプションでロギングするか、単にロギングのみ実行することができます。
- **state-checking action** {**drop** | **drop-connection** | **reset** | **log**} [**log**]：状態遷移チェックをイネーブルにします。また、不適合なトラフィックに対して実行するアクション（パケットのドロップ、接続のドロップ、リセット、またはログ）と、ロギングをイネーブルまたはディセーブルのどちらにするかを選択する必要もあります。
- **strict-header-validation action** {**drop** | **drop-connection** | **reset** | **log**} [**log**]：RFC 3261 に従って SIP メッセージのヘッダー フィールドの厳密な検証をイネーブルにします。また、不適合なトラフィックに対して実行するアクション（パケットのドロップ、接続のドロップ、リセット、またはログ）と、ロギングをイネーブルまたはディセーブルのどちらにするかを選択する必要もあります。
- **traffic-non-sip**：既知の SIP シグナリング ポートで SIP 以外のトラフィックを許可します。
- **uri-non-sip action** {**mask** [**log**] | **log**}：Alert-Info および Call-Info ヘッダー フィールドにある SIP 以外の URI を識別します。SIP メッセージの情報をマスクしてオプションでロギングするか、単にロギングのみ実行することができます。

例

次の例は、SIP を使用したインスタント メッセージをディセーブルにする方法を示しています。

```
hostname(config)# policy-map type inspect sip mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# no im

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect sip mymap

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

SIP インスペクション サービス ポリシーの設定

ASA のデフォルトの設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの SIP インスペクションが含まれます。インスペクションの設定をカスタマイズする一般的な方法は、デフォルトのグローバル ポリシーをカスタマイズすることです。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

class-map *name*
match *parameter*

例：

```
hostname(config)# class-map sip_class_map
hostname(config-cmap)# match access-list sip
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　SIP インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　SIP インスペクションを設定します。

```
inspect sip [sip_policy_map] [tls-proxy proxy_name]
```

それぞれの説明は次のとおりです。

- *sip_policy_map* は、オプションの SIP インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。SIP インスペクション ポリシー マップの作成の詳細については、「SIP インスペクション ポリシー マップの設定」（P.9-28）を参照してください。
- **tls-proxy** *proxy_name* には、このインスペクションに使用する TLS プロキシを指定します。TLS プロキシは、暗号化されたトラフィックのインスペクションをイネーブルにする場合にのみ必要です。

例：

```
hostname(config-class)# no inspect sip
hostname(config-class)# inspect sip sip-map
```

（注）　デフォルトのグローバル ポリシー（または使用中の任意のポリシー）を編集して、異なる SIP インスペクション ポリシー マップを使用する場合は、**no inspect sip** コマンドで SIP インスペクションを除去した後、新しい SIP インスペクション ポリシー マップ名を指定して再度追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

```
service-policy policymap_name {global | interface interface_name}
```

例：

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

global キーワードはポリシー 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。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。

SIP タイムアウト値の設定

メディア接続は、接続がアイドル状態になってから 2 分以内に切断されます。ただし、これは設定可能なタイムアウトであり、時間間隔は変更することが可能です。

[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ページで複数の SIP グローバル タイムアウト値を設定できます。

SIP 制御接続のタイムアウトを設定するには、次のコマンドを入力します。

```
hostname(config)# timeout sip hh:mm:ss
```

このコマンドは、SIP 制御接続を閉じるまでのアイドル タイムアウトを設定します。

SIP メディア接続のタイムアウトを設定するには、次のコマンドを入力します。

```
hostname(config)# timeout sip_media hh:mm:ss
```

このコマンドは、SIP メディア接続を閉じるまでのアイドル タイムアウトを設定します。

SIP インスペクションの確認とモニタリング

show sip コマンドは、ASA を越えて確立されている SIP セッションの情報を表示します。このコマンドは、**debug sip** および **show local-host** コマンドとともに、SIP インスペクション エンジンの問題のトラブルシューティングに使用されます。

次に、**show sip** コマンドの出力例を示します。

```
hostname# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
    state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
    state Active, idle 0:00:06
```

この例は、ASA 上の 2 つのアクティブな SIP セッションを示しています（Total フィールドで示されているように）。各 call-id は、コールを表しています。

最初のセッションは call-id c3943000-960ca-2e43-228f@10.130.56.44 で、Call Init 状態にあります。これは、このセッションがまだコール設定中であることを示しています。コール セットアップは、コールへの最後の応答が受信されるまでは完了しません。たとえば、発信者はすでに INVITE を送信して、100 Response を受信した可能性がありますが、200 OK はまだ受信していません。したがって、コール セットアップはまだ完了していません。1xx で始まっていない応答メッセージは最後の応答と考えられます。このセッションは、1 秒間アイドル状態でした。

2 番めのセッションは Active 状態です。この状態ではコール設定が完了し、エンドポイントがメディアを交換しています。このセッションは、6 秒間アイドル状態でした。

Skinny（SCCP）検査

ここでは、SCCP 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。

- 「SCCP インスペクションの概要」（P.9-34）
- 「Cisco IP Phone のサポート」（P.9-35）
- 「SCCP インスペクションの制限事項」（P.9-35）
- 「デフォルトのSCCP インスペクション」（P.9-36）
- 「SCCP（Skinny）インスペクションの設定」（P.9-36）
- 「SIP インスペクションの確認とモニタリング」（P.9-34）

SCCP インスペクションの概要

Skinny（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境でも使用できます。Cisco CallManager と併用すると、SCCP クライアントは、H.323 準拠端末と同時使用できます。

ASA は、SCCP に対して PAT と NAT をサポートします。IP 電話で使用できるグローバル IP アドレスよりも IP 電話が多い場合は、PAT が必要です。Skinny アプリケーション インスペクションは、SCCP シグナリング パケットの NAT と PAT をサポートすることで、すべての SCCP シグナリング パケットとメディア パケットが ASA を通過できるようにします。

Cisco CallManager と Cisco IP Phones 間の通常のトラフィックは SCCP を使用しており、特別な設定をしなくても SCCP インスペクションによって処理されます。ASA は、TFTP サーバの場所を Cisco IP Phone とその他の DHCP クライアントに送信することで、DHCP オプション 150 および 66 もサポートします。Cisco IP Phone では、デフォルト ルートを設定する DHCP オプション 3 を要求に含めることもできます。

（注）　ASA は、SCCP プロトコル バージョン 22 以前が稼働している Cisco IP Phone からのトラフィックのインスペクションをサポートします。

Cisco IP Phone のサポート

Cisco CallManager が Cisco IP Phone と比べてセキュリティの高いインターフェイスにあるトポロジでは、NAT が Cisco CallManager の IP アドレスに必要な場合、マッピングは**スタティック**である必要があります。これは、Cisco IP Phone では Cisco CallManager の IP アドレスをコンフィギュレーションで明示的に指定する必要があるためです。スタティック アイデンティティ エントリを使用すると、セキュリティが高いインターフェイス上にある Cisco CallManager が Cisco IP Phone からの登録を受け付けるようにできます。

Cisco IP Phone では、TFTP サーバにアクセスして、Cisco CallManager サーバに接続するために必要な設定情報をダウンロードする必要があります。

TFTP サーバと比較して Cisco IP Phone の方がセキュリティの低いインターフェイス上にある場合は、ACL を使用して UDP ポート 69 の保護された TFTP サーバに接続する必要があります。TFTP サーバに対してはスタティック エントリが必要ですが、識別スタティック エントリにする必要はありません。NAT を使用する場合、識別スタティック エントリは同じ IP アドレスにマッピングされます。PAT を使用する場合は、同じ IP アドレスとポートにマッピングされます。

Cisco IP Phone が TFTP サーバおよび Cisco CallManager と比べてセキュリティの*高い*インターフェイス上にある場合、Cisco IP Phone が接続を開始できるようにするために、ACL やスタティック エントリは必要ありません。

SCCP インスペクションの制限事項

内部の Cisco CallManager のアドレスが NAT または PAT 用に別の IP アドレスかポートを設定している場合、ASA は現在のところ TFTP を経由して転送するファイルの内容に対して NAT または PAT をサポートしていないため、外部の Cisco IP Phone 用の登録は失敗します。ASA は TFTP メッセージの NAT をサポートし、TFTP ファイル用にピンホールを開きますが、ASA は電話の登録中に TFTP によって転送された Cisco IP Phone のコンフィギュレーション ファイルに埋め込まれた Cisco CallManager の IP アドレスとポートを変換することはできません。

（注）　ASA では、コール セットアップ中であるコール以外の SCCP コールのステートフル フェールオーバーはサポートされていません。

デフォルトのSCCP インスペクション

SCCP インスペクションは、次のデフォルト値を使用してデフォルトでイネーブルになっています。

- 登録：適用強制しない
- メッセージの最大 ID：0x181
- プレフィックスの長さの最小値：4
- メディア タイムアウト：00:05:00
- シグナリング タイムアウト：01:00:00
- RTP 準拠：適用強制しない

暗号化されたトラフィックのインスペクションがイネーブルになっていないことにも注意してください。暗号化されたトラフィックを検査するには、TLS プロキシを設定する必要があります。

SCCP（Skinny）インスペクションの設定

SCCP（Skinny）アプリケーション インスペクションでは、パケット データ、ピンホールの動的開放に埋め込まれている IP アドレスとポート番号を変換します。また、追加のプロトコル準拠チェックと基本的なステート トラッキングも行います。

SCCP インスペクションはデフォルトではイネーブルです。SCCP インスペクションは、デフォルト以外の処理が必要な場合、または暗号化されたトラフィックのインスペクションをイネーブルにするために TLS プロキシを設定する場合にのみ設定する必要があります。SCCP インスペクションをカスタマイズする場合は、次のプロセスを使用します。

手順

ステップ 1　「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.9-36）。

ステップ 2　「SCCP インスペクション サービス ポリシーの設定」（P.9-38）。

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

メッセージがパラメータに違反したときのアクションを指定するには、SCCP インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、SCCP インスペクションをイネーブルにすると適用できます。

手順

ステップ 1　SCCP インスペクション ポリシー マップを作成します。

```
hostname(config)# policy-map type inspect skinny policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2　（任意）説明をポリシー マップに追加します。

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

ステップ 3　（任意）SCCP メッセージのステーション メッセージ ID フィールドに基づいてトラフィックをドロップします。

a. 0x0 ～ 0xffff の 16 進数のステーション メッセージ ID の値に基づいてトラフィックを識別します。**match [not] message-id** コマンドを使用して、単一の ID または ID の範囲を指定できます。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

```
hostname(config-pmap)# match message-id value
hostname(config-pmap)# match message-id range start_value end_value
```

例：

```
hostname(config-pmap)# match message-id 0x181

hostname(config-pmap)# match message-id range 0x200 0xffff
```

b. 一致したパケットに対して実行するアクションを指定します。パケットをドロップし、必要に応じてロギングできます。

```
hostname(config-pmap)# drop [log]
```

c. ドロップするすべてのメッセージ ID を指定するまで、このプロセスを繰り返します。

ステップ 4　インスペクション エンジンに影響するパラメータを設定します。

a. パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **enforce-registration**：コールを発信する前に強制的に登録を実行します。
- **message-ID max** *hex_value*：許可される最大 SCCP ステーション メッセージ ID を設定します。メッセージ ID は 16 進数で指定します。デフォルトの最大値は 0x181 です。
- **rtp-conformance** [**enforce-payloadtype**]：ピンホール上を流れる RTP パケットのプロトコル準拠をチェックします。オプションの **enforce-payloadtype** キーワードを指定すると、シグナリング交換に基づいてペイロード タイプを強制的に音声やビデオにします。
- **sccp-prefix-len** {**max** | **min**} *length*：許可される最大または最小の SCCP プレフィックスの長さを設定します。最小値と最大値の両方を設定するには、このコマンドを 2 回入力します。デフォルトの最小値は 4 で、デフォルトの最大値はありません。
- **timeout** {**media** | **signaling**} *time*：メディアおよびシグナリング接続のタイムアウトを設定します（hh: mm: ss 形式）。タイムアウトを設定しない場合は、番号に 0 を指定します。デフォルトのメディア タイムアウトは 5 分、デフォルトのシグナリング タイムアウトは 1 時間です。

例

次の例は、SCCP インスペクション ポリシー マップを定義する方法を示しています。

```
hostname(config)# policy-map type inspect skinny skinny-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enforce-registration
hostname(config-pmap-p)# match message-id range 200 300
hostname(config-pmap-p)# drop log
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect skinny skinny-map
hostname(config)# service-policy global_policy global
```

SCCP インスペクション サービス ポリシーの設定

ASA のデフォルトの設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの SCCP インスペクションが含まれます。インスペクションの設定をカスタマイズする一般的な方法は、デフォルトのグローバル ポリシーをカスタマイズすることです。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

class-map *name*
match *parameter*

例：

```
hostname(config)# class-map sccp_class_map
hostname(config-cmap)# match access-list sccp
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　SCCP インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　SCCP インスペクションを設定します。

inspect skinny [*sccp_policy_map*] [**tls-proxy** *proxy_name*]

それぞれの説明は次のとおりです。

- *sccp_policy_map* は、オプションの SCCP インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。SCCP インスペクション ポリシー マップの作成の詳細については、「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.9-36）を参照してください。
- **tls-proxy** *proxy_name* には、このインスペクションに使用する TLS プロキシを指定します。TLS プロキシは、暗号化されたトラフィックのインスペクションをイネーブルにする場合にのみ必要です。

例：

```
hostname(config-class)# no inspect skinny
hostname(config-class)# inspect skinny sccp-map
```

（注）　デフォルトのグローバル ポリシー（または使用中の任意のポリシー）を編集して、異なる SCCP インスペクション ポリシー マップを使用する場合は、**no inspect skinny** コマンドで SCCP インスペクションを除去した後、新しい SCCP インスペクション ポリシー マップ名を指定して再度追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

SCCP インスペクションの確認およびモニタ

show skinny コマンドは、SCCP（Skinny）インスペクション エンジンの問題のトラブルシューティングに役立ちます。次の条件での **show skinny** コマンドの出力例を示します。ASA を越えて 2 つのアクティブな Skinny セッションがセットアップされています。最初の Skinny セッションは、ローカル アドレス 10.0.0.11 にある内部 Cisco IP Phone と 172.18.1.33 にある外部 Cisco CallManager の間に確立されています。TCP ポート 2000 は、CallManager です。2 番目の Skinny セッションは、ローカル アドレス 10.0.0.22 にある別の内部 Cisco IP Phone と同じ Cisco CallManager の間に確立されています。

```
hostname# show skinny
        LOCAL                   FOREIGN                 STATE
-----------------------------------------------------------------
1       10.0.0.11/52238         172.18.1.33/2000                1
  MEDIA 10.0.0.11/22948         172.18.1.22/20798
2       10.0.0.22/52232         172.18.1.33/2000                1
  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

この出力は、2 つの内部 Cisco IP Phone 間でコールが確立されていることを示します。最初と 2 番目の電話機の RTP リスン ポートは、それぞれ UDP 22948 と 20798 です。

次に、これらの Skinny 接続の **show xlate debug** コマンドの出力例を示します。

```
hostname# show xlate debug
2 in use, 2 most used
Flags:  D - DNS, d - dump, I - identity, i - inside, n - no random,
        r - portmap, s - static
NAT from inside:10.0.0.11 to outside:172.18.1.11 flags si idle 0:00:16 timeout 0:05:00
NAT from inside:10.0.0.22 to outside:172.18.1.22 flags si idle 0:00:14 timeout 0:05:00
```

音声とビデオのプロトコル インスペクションの履歴

機能名	リリース	機能情報
SIP、SCCP、および TLS プロキシでの IPv6 のサポート	9.3(1)	SIP、SCCP、および TLS プロキシ（SIP または SCCP を使用）を使用している場合、IPv6 トラフィックを検査できるようになりました。 変更されたコマンドはありません。

CHAPTER 10

データベースおよびディレクトリ プロトコルのインスペクション

ここでは、データベースとディレクトリのプロトコルのアプリケーション インスペクションについて説明します。特定のプロトコルに関してインスペクションを使用する必要がある理由、およびインスペクションを適用する全体的な方法については、「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準備」（P.7-1）を参照してください。

ILS インスペクション

ILS インスペクション エンジンは、LDAP を使用してディレクトリ情報を ILS サーバと交換する Microsoft NetMeeting、SiteServer、および Active Directory の各製品に対して NAT をサポートします。

ASA は ILS に対して NAT をサポートします。NAT は、ILS または SiteServer Directory のエンドポイントの登録および検索で使用されます。LDAP データベースには IP アドレスだけが保存されるため、PAT はサポートされません。

LDAP サーバが外部にある場合、内部ピアが外部 LDAP サーバに登録された状態でローカルに通信できるように、検索応答に対して NAT を行うことを検討してください。このような検索応答では、最初に xlate が検索され、次に DNAT エントリが検索されて正しいアドレスが取得されます。これらの検索が両方とも失敗した場合、アドレスは変更されません。NAT 0（NAT なし）を使用していて、DNAT の相互作用を想定していないサイトの場合は、パフォーマンスを向上させるためにインスペクション エンジンをオフにすることをお勧めします。

ILS サーバが ASA 境界の内部にある場合は、さらに設定が必要なことがあります。この場合、外部クライアントが指定されたポート（通常は TCP 389）の LDAP サーバにアクセスするためのホールが必要となります。

（注） ILS トラフィック（H225 コール シグナリング）はセカンダリ UDP チャネルだけで発生するため、TCP 接続は TCP 非アクティブ間隔の後に切断されます。デフォルトでは、この間隔は 60 分です。この値は、TCP **timeout** コマンドを使用して調整できます。ASDM では、これは [Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインにあります。

ILS/LDAP はクライアント/サーバ モデルに従っており、セッションは 1 つの TCP 接続で処理されます。クライアントのアクションに応じて、このようなセッションがいくつか作成されることがあります。

接続ネゴシエーション時間中、クライアントからサーバに BIND PDU が送信されます。サーバから成功を示す BIND RESPONSE を受信すると、ILS Directory に対する操作を実行するためのその他の操作メッセージ（ADD、DEL、SEARCH、MODIFY など）が交換される場合があります。ADD REQUEST PDU および SEARCH RESPONSE PDU には、NetMeeting セッションを確立するために H.323（SETUP および CONNECT メッセージ）によって使用される、NetMeeting ピアの IP アドレスが含まれている場合があります。Microsoft NetMeeting v2.X および v3.X は、ILS をサポートしています。

ILS インスペクションでは、次の操作が実行されます。

- BER 復号化機能を使用して LDAP REQUEST PDU/RESPONSE PDU を復号化する。
- LDAP パケットを解析する。
- IP アドレスを抽出する。
- 必要に応じて IP アドレスを変換する。
- BER 符号化機能を使用して、変換後のアドレスが含まれる PDU を符号化する。
- 新しく符号化された PDU を元の TCP パケットにコピーする。
- TCP チェックサムとシーケンス番号の増分を調整する。

ILS インスペクションには、次の制限事項があります。

- 照会要求や応答はサポートされません。
- 複数のディレクトリのユーザは統合されません。
- 複数のディレクトリに複数の ID を持っている単一のユーザは NAT には認識されません。

ILS インスペクションをイネーブルにする方法については、「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.7-11）を参照してください。

SQL*Net インスペクション

SQL*Net 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。

SQL*Net プロトコルは、さまざまなパケット タイプで構成されています。ASA はこれらのパケットを処理して、ASA のどちらの側の Oracle アプリケーションにも一貫性のあるデータ ストリームが表示されるようにします。

SQL*Net のデフォルトのポート割り当ては 1521 です。これは、Oracle が SQL*Net 用に使用している値ですが、構造化照会言語（SQL）の IANA ポート割り当てとは一致しません。SQL*Net インスペクションを一連のポート番号に適用するには、**class-map** コマンドを使用します。

（注）　SQL 制御 TCP ポート 1521 と同じポートで SQL データ転送が行われる場合は、SQL*Net のインスペクションをディセーブルにします。SQL*Net インスペクションがイネーブルになっていると、セキュリティ アプライアンスはプロキシとして機能し、クライアントのウィンドウ サイズを 65000 から約 16000 に減らすため、データ転送の問題が発生します。

ASA は、すべてのアドレスを変換し、SQL*Net バージョン 1 用に開いたすべての埋め込みポートのパケットを調べます。

SQL*Net バージョン 2 の場合、データ長ゼロの REDIRECT パケットの直後に続くすべての DATA パケットまたは REDIRECT パケットはフィックスアップされます。

フィックスアップが必要なパケットには、埋め込みホスト アドレスおよびポート アドレスが次の形式で含まれています。

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL*Net バージョン 2 の各 TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker）は、NAT 対象のアドレスがあるかどうかがスキャンされません。また、インスペクションがパケット内に埋め込まれたポートにダイナミック接続を開くこともありません。

SQL*Net バージョン 2 の TNSFrame、Redirect パケット、および Data パケットは、ペイロードのデータ長がゼロの REDIRECT TNSFrame タイプの後に続く場合、開くポートおよび NAT 対象のアドレスがあるかどうかスキャンされます。データ長ゼロの Redirect メッセージが ASA を通過すると、後に続く Data メッセージまたは Redirect メッセージは変換対象であり、ポートはダイナミックに開かれると想定するフラグが、接続データ構造に設定されます。先行するパラグラフの TNS フレームのいずれかが Redirect メッセージの後に到着した場合、フラグはリセットされます。

SQL*Net インスペクション エンジンは、チェックサムを再計算し、IP および TCP の長さを変更し、新旧のメッセージの長さの差を使用してシーケンス番号と確認応答番号を再調整します。

SQL*Net バージョン 1 では、その他のすべての場合を想定しています。TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker、Redirect、Data）とすべてのパケットは、ポートおよびアドレスがあるかどうかスキャンされます。アドレスが変換され、ポート接続が開かれます。

SQL*Net インスペクションをイネーブルにする方法については、「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.7-11）を参照してください。

Sun RPC インスペクション

この項では、Sun RPC 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。

Sun RPC インスペクションの概要

Sun RPC インスペクション エンジンは、Sun RPC プロトコルのアプリケーション インスペクションをイネーブルまたはディセーブルにします。Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスはどのポート上でも実行できます。サーバ上の Sun RPC サービスにアクセスしようとするクライアントは、そのサービスが実行されているポートを知る必要があります。そのためには、予約済みポート 111 でポート マッパー プロセス（通常は rpcbind）に照会します。

クライアントがサービスの Sun RPC プログラム番号を送信すると、ポート マッパー プロセスはサービスのポート番号を応答します。クライアントは、ポート マッパー プロセスによって特定されたポートを指定して、Sun RPC クエリーをサーバに送信します。サーバが応答すると、ASA はこのパケットを代行受信し、そのポートで TCP と UDP の両方の初期接続を開きます。

ヒント　Sun RPC インスペクションはデフォルトではイネーブルです。Sun RPC サーバ テーブルを管理するだけで、ファイアウォールの通過を許可されているサービスを識別できます。Sun RPC インスペクションをイネーブルにする方法については、「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.7-11）を参照してください。

Sun RPC インスペクションには、次の制限事項が適用されます。

- Sun RPC ペイロード情報の NAT または PAT はサポートされていません。
- Sun RPC インスペクションは着信 ACL のみをサポートします。Sun RPC インスペクションは発信 ACL はサポートしません。これは、インスペクション エンジンでセカンダリ接続でなくダイナミック ACL が使用されるためです。ダイナミック ACL は常に入力方向に追加され、出力方向には追加されません。したがって、このインスペクション エンジンは発信 ACL をサポートしません。ASA に設定されているダイナミック ACL を表示するには、**show asp table classify domain permit** コマンドを使用します。

Sun RPC サービスの管理

Sun RPC サービス テーブルを使用して、確立された Sun RPC セッションに基づいて ASA を経由する Sun RPC トラフィックを制御します。Sun RPC サービス テーブルのエントリを作成するには、グローバル コンフィギュレーション モードで **sunrpc-server** コマンドを使用します。

```
hostname(config)# sunrpc-server interface_name ip_address mask service service_type
protocol {tcp | udp} port[-port] timeout hh:mm:ss
```

このコマンドを使用して、Sun RPC アプリケーション インスペクションで開いたピンホールを閉じるまでのタイムアウトを指定できます。たとえば、IP アドレスが 192.168.100.2 の Sun RPC サーバに対して 30 分のタイムアウトを作成するには、次のコマンドを入力します。

```
hostname(config)# sunrpc-server inside 192.168.100.2 255.255.255.255 service 100003
protocol tcp 111 timeout 00:30:00
```

このコマンドは、Sun RPC アプリケーション インスペクションで開いたピンホールが 30 分後に閉じるように指定します。この例では、Sun RPC サーバは TCP ポート 111 を使用する内部インターフェイスにあります。UDP、別のポート番号、ポート範囲を指定することもできます。ポート範囲を指定するには、範囲の開始ポート番号と終了ポート番号をハイフンで区切ります（111-113 など）。

サービス タイプは、特定のサービス タイプとそのサービスに使用するポート番号の間のマッピングを特定します。サービス タイプ（この例では 100003）を判定するには、Sun RPC サーバ マシンの UNIX または Linux コマンドラインで、**sunrpcinfo** コマンドを使用します。

Sun RPC コンフィギュレーションを消去するには、次のコマンドを入力します。

```
hostname(config)# clear configure sunrpc-server
```

これによって、**sunrpc-server** コマンドを使用して実行されるコンフィギュレーションが削除されます。**sunrpc-server** コマンドを使用して、指定したタイムアウト値を持つピンホールを作成できます。

アクティブな Sun RPC サービスを消去するには、次のコマンドを入力します。

```
hostname(config)# clear sunrpc-server active
```

これによって、そのサービス（NFS、NIS など）で Sun RPC アプリケーション インスペクションが開いたピンホールが消去されます。

Sun RPC インスペクションの確認とモニタリング

この項の出力例では、Sun RPC サーバの IP アドレスは 192.168.100.2 で内部インターフェイスにあり、Sun RPC クライアントの IP アドレスは 209.168.200.5 で外部インターフェイスにあるものとします。

現在の Sun RPC 接続に関する情報を表示するには、**show conn** コマンドを入力します。次に、**show conn** コマンドの出力例を示します。

```
hostname# show conn
15 in use, 21 most used
UDP out 209.165.200.5:800 in 192.168.100.2:2049 idle 0:00:04 flags -
UDP out 209.165.200.5:714 in 192.168.100.2:111 idle 0:00:04 flags -
UDP out 209.165.200.5:712 in 192.168.100.2:647 idle 0:00:05 flags -
UDP out 192.168.100.2:0 in 209.165.200.5:714 idle 0:00:05 flags i
hostname(config)#
```

Sun RPC サービス テーブル コンフィギュレーションに関する情報を表示するには、**show running-config sunrpc-server** コマンドを入力します。次に、**show running-config sunrpc-server** コマンドの出力例を示します。

```
hostname(config)# show running-config sunrpc-server
sunrpc-server inside 192.168.100.2 255.255.255.255 service 100003 protocol UDP port 111
timeout 0:30:00
sunrpc-server inside 192.168.100.2 255.255.255.255 service 100005 protocol UDP port 111
timeout 0:30:00
```

この出力では、IP アドレスが 192.168.100.2 で内部インターフェイスにある Sun RPC サーバの UDP ポート 111 で、タイムアウト間隔が 30 分に設定されていることが示されています。

Sun RPC サービスで開かれているピンホールを表示するには、**show sunrpc-server active** コマンドを入力します。次に、**show sunrpc-server active** コマンドの出力例を示します。

```
hostname# show sunrpc-server active
LOCAL FOREIGN SERVICE TIMEOUT
-----------------------------------------------
1 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
2 209.165.200.5/0 192.168.100.2/2049 100003 0:30:0
3 209.165.200.5/0 192.168.100.2/647 100005 0:30:00
4 209.165.200.5/0 192.168.100.2/650 100005 0:30:00
```

LOCAL カラムのエントリは、内部インターフェイスのクライアントまたはサーバの IP アドレスを示します。FOREIGN カラムの値は、外部インターフェイスのクライアントまたはサーバの IP アドレスを示します。

Sun RPC サーバで実行されている Sun RPC サービスに関する情報を表示するには、Linux または UNIX サーバのコマンドラインから **rpcinfo -p** コマンドを入力します。次に、**rpcinfo -p** コマンドの出力例を示します。

```
sunrpcserver:~ # rpcinfo -p
program vers proto port
100000 2 tcp 111 portmapper
100000 2 udp 111 portmapper
100024 1 udp 632 status
100024 1 tcp 635 status
100003 2 udp 2049 nfs
100003 3 udp 2049 nfs
100003 2 tcp 2049 nfs
100003 3 tcp 2049 nfs
100021 1 udp 32771 nlockmgr
100021 3 udp 32771 nlockmgr
100021 4 udp 32771 nlockmgr
100021 1 tcp 32852 nlockmgr
```

```
100021 3 tcp 32852 nlockmgr
100021 4 tcp 32852 nlockmgr
100005 1 udp 647 mountd
100005 1 tcp 650 mountd
100005 2 udp 647 mountd
100005 2 tcp 650 mountd
100005 3 udp 647 mountd
100005 3 tcp 650 mountd
```

この出力では、ポート 647 が UDP 上で実行されている mountd デーモンに対応しています。mountd プロセスは、通常、ポート 32780 を使用します。この例では、TCP 上で実行されている mountd プロセスがポート 650 を使用しています。

管理アプリケーション プロトコルのインスペクション

ここでは、管理アプリケーション プロトコルのアプリケーション インスペクションについて説明します。特定のプロトコルに関してインスペクションを使用する必要がある理由、およびインスペクションを適用する全体的な方法については、「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準備」（P.7-1）を参照してください。

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。

DCERPC インスペクション

次の項では、DCERPC インスペクション エンジンについて説明します。

DCERPC の概要

DCERPC は、Microsoft 社の分散クライアント/サーバ アプリケーションで広く使われているプロトコルです。このプロトコルによって、ソフトウェア クライアントがサーバにあるプログラムをリモートで実行できるようになります。

通常、このプロトコルの接続では、クライアントが予約済みポート番号で接続を受け入れるエンドポイント マッパーというサーバに、必要なサービスについてダイナミックに割り当てられるネットワーク情報を問い合わせます。次に、クライアントは、サービスを提供しているサーバのインスタンスへのセカンダリ接続をセットアップします。セキュリティ アプライアンスは、適切なポート番号とネットワーク アドレスへのセカンダリ接続を許可し、必要に応じて NAT を適用します。

DCERPC インスペクション マップは、EPM とウェルノウン TCP ポート 135 上のクライアントとの間のネイティブ TCP 接続を検査します。クライアント用に EPM のマッピングとルックアップがサポートされています。クライアントとサーバは、どのセキュリティ ゾーンにあってもかまいません。埋め込まれたサーバの IP アドレスとポート番号は、EPM からの応答メッセージで受け取ります。クライアントが EPM から返されたサーバのポートに対して複数の接続を試みる可能性があるので、ピンホールが複数使用でき、ユーザがそのタイムアウトを設定できるようになっています。

（注）　DCERPC の検査は、ASA にピンホールを開くための EPM とクライアント間の通信だけがサポートされます。EPM を使用しない RPC 通信を使用するクライアントは、DCERPC インスペクションではサポートされません。

DCERPC インスペクションの設定

DCERPC インスペクションはデフォルトではイネーブルになっていません。DCERPC インスペクションが必要な場合は設定してください。

手順

ステップ 1　「DCERPC インスペクション ポリシー マップの設定」（P.11-2）。

ステップ 2　「DCERPC インスペクションのサービス ポリシーの設定」（P.11-3）。

DCERPC インスペクション ポリシー マップの設定

DCERPC インスペクションの追加のパラメータを指定するには、DCERPC インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、DCERPC インスペクションをイネーブルにすると適用できます。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　DCERPC インスペクション ポリシー マップを作成するには、次のコマンドを入力します。

```
hostname(config)# policy-map type inspect dcerpc policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2　（任意）このポリシー マップに説明を追加するには、次のコマンドを使用します。

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

ステップ 3　インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a. パラメータ コンフィギュレーション モードに入るには、次のコマンドを入力します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **timeout pinhole** *hh: mm: ss* : DCERPC ピンホールのタイムアウトを設定し、2 分のグローバル システム ピンホール タイムアウトを上書きします。タイムアウトは 00:00:01 ～ 119:00:00 まで指定できます。
- **endpoint-mapper** [**epm-service-only**] [**lookup-operation** [**timeout** *hh:mm:ss*]] : エンドポイント マッパー トラフィックのオプションを設定します。**epm-service-only** キーワードを指定すると、バインド中にエンドポイント マッパー サービスを実行し、このサービスのトラフィックだけが処理されるようにします。**lookup-operation** キーワードを指定すると、エンドポイント マッパー サービスのルックアップ操作をイネーブルにします。ルックアップ操作で生成されたピンホールのタイムアウトを設定できます。ルックアップ操作にタイムアウトが設定されていない場合は、timeout pinhole コマンドで指定した値かデフォルトの値が使用されます。

例

次の例は、DCERPC インスペクション ポリシー マップを定義し、DCERPC のピンホールのタイムアウトを設定する方法を示しています。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# timeout pinhole 0:10:00

hostname(config)# class-map dcerpc
hostname(config-cmap)# match port tcp eq 135

hostname(config)# policy-map global-policy
hostname(config-pmap)# class dcerpc
hostname(config-pmap-c)# inspect dcerpc dcerpc-map

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

DCERPC インスペクションのサービス ポリシーの設定

デフォルトのインスペクション ポリシーでは、DCERPC インスペクションがイネーブルにされていないため、この検査が必要な場合はイネーブルにします。デフォルトのグローバル インスペクション ポリシーを編集するだけで、DCERPC インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

```
class-map name
match parameter
```

例：

```
hostname(config)# class-map dcerpc_class_map
hostname(config-cmap)# match access-list dcerpc
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　DCERPC インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　DCERPC インスペクションを設定します。

inspect dcerpc [*dcerpc_policy_map*]

dcerpc_policy_map が任意の DCERPC インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。インスペクション ポリシー マップの作成の詳細については、「DCERPC インスペクション ポリシー マップの設定」（P.11-2）を参照してください。

例：

```
hostname(config-class)# no inspect dcerpc
hostname(config-class)# inspect dcerpc dcerpc-map
```

（注）　別のインスペクション ポリシー マップを使用するためにデフォルト グローバル ポリシー（または使用中のポリシー）を編集する場合は、**no inspect dcerpc** コマンドで DCERPC インスペクションを削除し、新しいインスペクション ポリシー マップの名前で再追加してください。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

GTP インスペクション

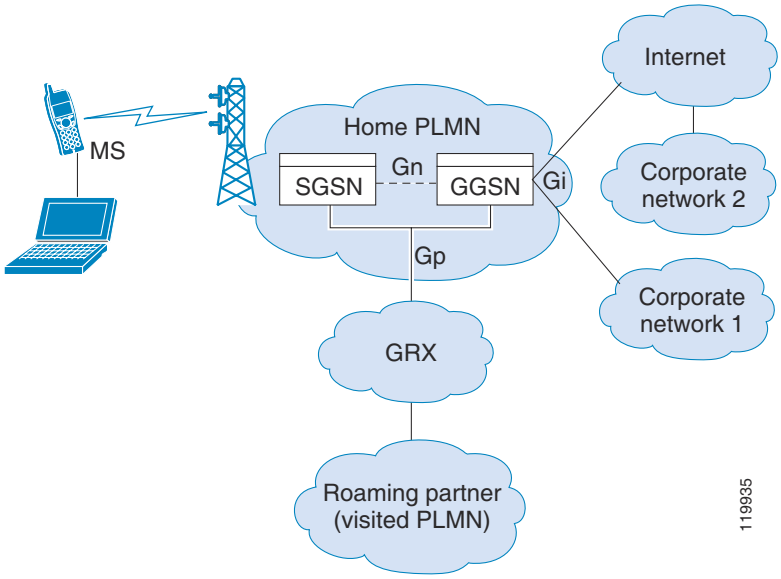
次の項では、GTP インスペクション エンジンについて説明します。

（注）　GTP インスペクションには、特別なライセンスが必要です。

GTP インスペクションの概要

GPRS は、モバイル ユーザに対して、GSM ネットワークと企業ネットワークまたはインターネットとの間で中断しない接続を提供します。GGSN は、GPRS 無線データ ネットワークと他のネットワークとの間のインターフェイスです。SGSN は、モビリティ、データ セッション管理、およびデータ圧縮を実行します。

図 11-1　　GPRS トンネリング プロトコル



UMTS は、固定回線テレフォニー、モバイル、インターネット、コンピュータ テクノロジーの商用コンバージェンスです。UTRAN は、このシステムで無線ネットワークを実装するためのネットワーキング プロトコルです。GTP を使用すると、GGSN、SGSN、および UTRAN 間の UMTS/GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。

GTP には固有のセキュリティやユーザ データの暗号化は含まれていませんが、ASA で GTP を使用することによって、これらの危険性からネットワークを保護できます。

SGSN は、GTP を使用する GGSN に論理的に接続されます。GTP を使用すると、GSN 間の GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによって、SGSN は、トンネルの作成、変更、および削除を行い、モバイル ステーションに GPRS ネットワーク アクセスを提供できます。GTP は、トンネリング メカニズムを使用して、ユーザ データ パケットを伝送するためのサービスを提供します。

（注） GTP をフェールオーバーと同時に使用しているとき、GTP 接続が確立され、データがトンネルを超えて伝送される前にアクティブ装置に障害が発生した場合、GTP データ接続（「j」フラグが設定されています）は、スタンバイ装置に複製されません。これは、アクティブ装置が初期接続をスタンバイ装置に複製しないためです。

GTP インスペクションのデフォルト

GTP インスペクションはデフォルトではイネーブルになっていません。ただし、ユーザ自身のインスペクション マップを指定せずにイネーブルにすると、次の処理を行うデフォルト マップが使用されます。マップを設定する必要があるのは、異なる値が必要な場合のみです。

- エラーは許可されません。
- 要求の最大数は 200 です。
- トンネルの最大数は 500 です。
- GSN タイムアウトは 30 分です。

- PDP コンテキストのタイムアウトは 30 分です。
- 要求のタイムアウトは 1 分です。
- シグナリング タイムアウトは 30 分です。
- トンネリングのタイムアウトは 1 時間です。
- T3 応答タイムアウトは 20 秒です。
- 未知のメッセージ ID はドロップされ、ログに記録されます。

GTP インスペクションの設定

GTP インスペクションはデフォルトではイネーブルになっていません。GTP インスペクションが必要な場合は設定してください。

手順

ステップ 1　「GTP インスペクション ポリシー マップの設定」（P.11-7）。

ステップ 2　「GTP インスペクションのサービス ポリシーの設定」（P.11-10）。

ステップ 3　（任意）過剰請求攻撃から保護するために RADIUS アカウンティング インスペクションを設定します。「RADIUS アカウンティング インスペクション」（P.11-13）を参照してください。

GTP インスペクション ポリシー マップの設定

GTP トラフィックで追加のパラメーターを実行する際にデフォルト マップがニーズを満たさない場合は、GTP マップを作成し、設定します。

はじめる前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1　GTP インスペクション ポリシー マップの作成

```
hostname(config)# policy-map type inspect gtp policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2　（任意）このポリシー マップに説明を追加するには、次のコマンドを使用します。

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

ステップ 3　一致したトラフィックにアクションを適用するには、次の手順を実行します。

a. 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **apn regex** {*regex_name* | **class** *class_name*}：指定した正規表現または正規表現クラスに対する Access Point Name (APN) に一致します。
- **match** [**not**] **message id** {*message_id* | **range** *message_id_1 message_id_2*}：1 ～ 255 のいずれかのメッセージ ID に一致します。1 つの ID または ID の範囲を指定できます。
- **match** [**not**] **message length min** *bytes* **max** *bytes*：UDP ペイロード（GTP ヘッダーと残りのメッセージ）の長さが最小値と最大値の間である、1 ～ 65536 のメッセージに一致します。
- **match** [**not**] **version** {*version_id* | **range** *version_id_1 version_id_2*}：0 ～ 255 のいずれかの GTP バージョンに一致します。1 つのバージョンまたはバージョンの範囲を指定できます。

b. 次のコマンドを入力して、一致したトラフィックに対して実行するアクションを指定します。

```
hostname(config-pmap-c)# {drop [log]| log | rate-limit message_rate}
```

各 **match** コマンドですべてのオプションを使用できるわけではありません。

- **drop** キーワードはパケットをドロップします。
- 単独または **drop** と一緒に使用できる **log** キーワードからシステム ログ メッセージが送信されます。
- **rate-limit** *message_rate* 引数では、メッセージのレートを制限します。このオプションでは、**message id** のみ使用できます。

ポリシー マップでは、複数の **match** コマンドを指定できます。**match** コマンドの順序については、「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.2-4）を参照してください。

ステップ 4　インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a. パラメータ コンフィギュレーション モードに入るには、次のコマンドを入力します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **permit errors**：無効な GTP パケットや別の方法で解析されるとドロップされるパケットを許可します。
- **request-queue** *max_requests*：キューで応答待ちができる GTP 要求数の最大値を設定します。デフォルトは 200 です。この上限に達した後に新しい要求が到着すると、最も長い時間キューに入っていた要求が削除されます。「Error Indication」、「Version Not Supported」および「SGSN Context Acknowledge」というメッセージは、要求と見なされないため、応答待ち要求のキューに入れられません。
- **tunnel-limit** *max_tunnels*：ASA 上でアクティブになることができる GTP トンネルの最大数を設定します。デフォルト値は 500 です。このコマンドで指定したトンネル数に達すると、新しい要求はドロップされます。
- **timeout** {**gsn** | **pdp-context** | **request** | **signaling** | **tunnel**} *time*：指定したサービスのアイドル タイムアウトを設定します（hh: mm: ss 形式）。タイムアウトを設定しない場合は、番号に 0 を指定します。このコマンドは、タイムアウトごとに別々に入力します。

  gsn キーワードで指定した時間、非アクティブ状態が続くと、GSN が削除されます。

  pdp-context キーワードでは、PDP コンテキストの受信を開始するまでの最大許容時間を指定します。

request キーワードでは、GTP メッセージの受信を開始するまでの最大許容時間を指定します。

signaling キーワードで指定した時間、非アクティブ状態が続くと、GTP シグナリングが削除されます。

tunnel キーワードで指定した時間、非アクティブ状態が続くと、GTP トンネルが切断されます。

ステップ 5　必要に応じて、パラメータ コンフィギュレーション モードに入っている間に、IMSI プレフィックス フィルタリングを設定します。

```
hostname(config-pmap-p)# mcc country_code mnc network_code
```

デフォルトでは、セキュリティ アプライアンスは、有効なモバイル カントリ コード（MCC）とモバイル ネットワーク コード（MNC）の組み合わせをチェックしません。IMSI プレフィックス フィルタリングを設定すると、受信パケットの IMSI の MCC と MNC が、設定された MCC と MNC の組み合わせと比較され、一致しないものはドロップされます。

モバイル カントリ コードは 0 以外の 3 桁の数字で、1 桁または 2 桁の値のプレフィックスとして 0 が追加されます。モバイル ネットワーク コードは 2 桁または 3 桁の数字です。

割り当てられたすべての MCC と MNC の組み合わせを追加します。デフォルトでは、ASA は MNC と MCC の組み合わせが有効であるかどうかをチェックしないため、設定した組み合わせが有効であるかどうかを確認する必要があります。MCC および MNC コードの詳細については、ITU E.212 勧告『*Identification Plan for Land Mobile Stations*』を参照してください。

ステップ 6　必要に応じて、パラメータ コンフィギュレーション モードに入っている間に、GSN プーリングを設定します。

```
hostname(config-pmap-p)# permit response to-object-group SGSN_name
from-object-group GSN_pool
```

ASA が GTP インスペクションを実行する場合、デフォルトで ASA は、GTP 要求で指定されていない GSN からの GTP 応答をドロップします。これは、GSN のプール間でロードバランシングを使用して、GPRS の効率とスケーラビリティを高めているときに発生します。

GSN プーリングを設定し、ロード バランシングをサポートするために、GSN を指定するネットワーク オブジェクト グループを作成し、これを **from-object-group** パラメータで指定します。同様に、SGSN のためにネットワーク オブジェクト グループを作成し、**to-object-group** パラメータとして選択します。応答している GSN が GTP 要求の送信先の GSN と同じオブジェクト グループに属している場合、および応答している GSN による GTP 応答の送信が許可されている先のオブジェクト グループに SGSN がある場合、ASA はその応答を許可します。

ネットワーク オブジェクト グループは、GSN または SGSN をホスト アドレスまたは GSN や SGSN を含むサブネットから識別できます。

例

次の例では、GSN プールと SGSN のネットワーク オブジェクトを定義して GSN プーリングをサポートする方法を示します。クラス C ネットワーク全体が GSN プールとして定義されていますが、ネットワーク全体を指定する代わりに、複数の個別の IP アドレスを **network-object** コマンドで 1 つずつ指定できます。この例では、次に、GSN プールから SGSN への応答を許可するように、GTP インスペクション マップを変更します。

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.100.0 255.255.255.0
hostname(config)# object-group network sgsn32
hostname(config-network)# network-object host 192.168.50.100
```

```
hostname(config)# policy-map type inspect gtp gtp-policy
hostname(config)# gtp-map gtp-policy
hostname(config-pmap)# parameters
hostname(config-pmap-p)# permit response to-object-group sgsn32
from-object-group gsnpool32
```

例

次の例は、ネットワークのトンネル数を制限する方法を示しています。

```
hostname(config)# policy-map type inspect gtp gmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# tunnel-limit 3000

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect gtp gmap

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

GTP インスペクションのサービス ポリシーの設定

デフォルトのインスペクション ポリシーでは、GTP インスペクションがイネーブルにされていないため、この検査が必要な場合はイネーブルにします。デフォルトのグローバル インスペクション ポリシーを編集するだけで、GTP インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

class-map *name*
match *parameter*

例：

```
hostname(config)# class-map gtp_class_map
hostname(config-cmap)# match access-list gtp
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　GTP インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 4　GTP インスペクションの設定

inspect gtp [*gtp_policy_map*]

gtp_policy_map は任意の GTP インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。インスペクション ポリシー マップの作成の詳細については、「GTP インスペクション ポリシー マップの設定」（P.11-7）を参照してください。

例：

```
hostname(config-class)# no inspect gtp
hostname(config-class)# inspect gtp gtp-map
```

（注）　別のインスペクション ポリシー マップを使用するためにデフォルト グローバル ポリシー（または使用中のポリシー）を編集する場合は、**no inspect gtp** コマンドで GTP インスペクションを削除してから、新しいインスペクション ポリシー マップの名前で再追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

GTP インスペクションの確認とモニタリング

GTP コンフィギュレーションを表示するには、特権 EXEC モードで **show service-policy inspect gtp** コマンドを入力します。

show service-policy inspect gtp statistics コマンドを使用して、GTP インスペクションの統計情報を表示します。次に、**show service-policy inspect gtp statistics** コマンドの出力例を示します。

```
hostname# show service-policy inspect gtp statistics
GPRS GTP Statistics:
version_not_support                 0     msg_too_short             0
  unknown_msg                       0     unexpected_sig_msg        0
  unexpected_data_msg               0     ie_duplicated             0
  mandatory_ie_missing              0     mandatory_ie_incorrect    0
  optional_ie_incorrect             0     ie_unknown                0
  ie_out_of_order                   0     ie_unexpected             0
  total_forwarded                   0     total_dropped             0
  signalling_msg_dropped            0     data_msg_dropped          0
  signalling_msg_forwarded          0     data_msg_forwarded        0
  total created_pdp                 0     total deleted_pdp         0
  total created_pdpmcb              0     total deleted_pdpmcb      0
  pdp_non_existent                  0
```

次に、**show service-policy inspect gtp statistics gsn** コマンドの GSN 出力例を示します。

```
hostname# show service-policy inspect gtp statistics gsn 10.9.9.9
1 in use, 1 most used, timeout 0:00:00

GTP GSN Statistics for 10.9.9.9, Idle 0:00:00, restart counter 0
    Tunnels Active 0Tunnels Created 0
    Tunnels Destroyed 0
    Total Messages Received 2
    Signaling Messages Data Messages
    total received 2 0
    dropped 0 0
    forwarded 2 0
```

show service-policy inspect gtp pdp-context コマンドを使用して、PDP コンテキストに関する情報を表示します。次に例を示します。

```
hostname# show service-policy inspect gtp pdp-context detail
1 in use, 1 most used, timeout 0:00:00

Version TID                 MS Addr         SGSN Addr    Idle      APN
v1      1234567890123425         10.0.1.1        10.0.0.2 0:00:13  gprs.cisco.com

    user_name (IMSI): 214365870921435    MS address:         1.1.1.1
    primary pdp: Y                       nsapi: 2
    sgsn_addr_signal:        10.0.0.2    sgsn_addr_data:          10.0.0.2
    ggsn_addr_signal:        10.1.1.1    ggsn_addr_data:          10.1.1.1
    sgsn control teid:     0x000001d1    sgsn data teid:        0x000001d3
    ggsn control teid:     0x6306ffa0    ggsn data teid:        0x6305f9fc
    seq_tpdu_up:                  0    seq_tpdu_down:                  0
    signal_sequence:              0
    upstream_signal_flow:         0     upstream_data_flow:          0
    downstream_signal_flow:       0     downstream_data_flow:        0
    RAupdate_flow:                0
```

PDP コンテキストは、IMSI と NSAPI の値の組み合わせであるトンネル ID によって識別されます。GTP トンネルは、それぞれ別個の GSN ノードにある、2 つの関連する PDP コンテキストによって定義され、トンネル ID によって識別されます。GTP トンネルは、パケットを外部パケット データ ネットワークと MS ユーザの間で転送するために必要です。

RADIUS アカウンティング インスペクション

次の項では、RADIUS アカウンティング インスペクション エンジンについて説明します。

RADIUS アカウンティング インスペクションの概要

RADIUS アカウンティング インスペクションの目的は、RADIUS サーバを使用した GPRS ネットワークの過剰請求攻撃を防ぐことです。RADIUS アカウンティング インスペクションを実行するには、GTP/GPRS ライセンスは必要ありませんが、GTP インスペクションを実行し、GPRS セットアップをセットアップしない限り、意味がありません。

GPRS ネットワークの過剰請求攻撃は、コンシューマに対して、利用していないサービスの請求を行います。この場合、悪意のある攻撃者は、サーバへの接続をセットアップし、SGSN から IP アドレスを取得します。攻撃者がコールを終了しても、攻撃者のサーバはパケットの送信を続けます。このパケットは GGSN によってドロップされますが、サーバからの接続はアクティブなままです。攻撃者に割り当てられていた IP アドレスが解放され、正規ユーザに再割り当てされるので、正規ユーザは、攻撃者が利用するサービスの分まで請求されることになります。

RADIUS アカウンティング インスペクションは、GGSN へのトラフィックが正規のものかどうかを確認することにより、このような攻撃を防ぎます。RADIUS アカウンティングの機能を正しく設定しておくと、ASA は、RADIUS アカウンティング要求の開始メッセージと終了メッセージに含まれる Framed IP 属性との照合結果に基づいて接続を切断します。終了メッセージの Framed IP 属性の IP アドレスが一致している場合、ASA は、一致する IP アドレスを持つ送信元との接続をすべて検索します。

ASA でメッセージを検証できるように、RADIUS サーバとの事前共有秘密キーを設定することもできます。共有秘密が設定されていない場合、ASA は、ソース IP アドレスが RADIUS メッセージを送信できるよう設定された IP アドレスであるということだけをチェックします。

（注）　GPRS をイネーブルにして RADIUS アカウンティング インスペクションを使用すると、ASA はアカウンティング要求の STOP メッセージで 3GPP-Session-Stop-Indicator をチェックして、セカンダリ PDP コンテキストを正しく処理します。具体的には、ASA では、アカウンティング要求の終了メッセージがユーザ セッションおよび関連するすべての接続を終了する前に、メッセージに 3GPP-SGSN-Address 属性が含まれる必要があります。一部のサードパーティの GGSN は、この属性をデフォルトでは送信しない場合があります。

RADIUS アカウンティング インスペクションの設定

RADIUS アカウンティング インスペクションはデフォルトではイネーブルになっていません。RADIUS アカウンティング インスペクションが必要な場合は設定してください。

手順

ステップ 1　「RADIUS アカウンティング インスペクション ポリシー マップの設定」（P.11-14）。

ステップ 2　「RADIUS アカウンティング インスペクションのサービス ポリシーの設定」（P.11-15）。

RADIUS アカウンティング インスペクション ポリシー マップの設定

検査に必要な属性を設定する RADIUS アカウンティング インスペクション ポリシー マップを作成します。

手順

ステップ 1　RADIUS アカウンティング インスペクション ポリシー マップを作成します。

```
hostname(config)# policy-map type inspect radius-accounting policy_map_name
hostname(config-pmap)#
```

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2　（任意）説明をポリシー マップに追加します。

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

ステップ 3　パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

ステップ 4　1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **send response**：Accounting-Request の Start および Stop メッセージを、それらのメッセージの送信元（**host** コマンド内で識別されています）へ送信するよう ASA に指示します。
- **enable gprs**：GPRS 過剰請求の保護を実装します。セカンダリ PDP コンテキストを適切に処理するため、ASA は、Accounting-Request の Stop および Disconnect メッセージの 3GPP VSA 26-10415 属性をチェックします。この属性が存在する場合、ASA は、設定インターフェイスのユーザ IP アドレスに一致するソース IP を持つすべての接続を切断します。
- **validate-attribute** *number*：Accounting-Request Start メッセージを受信する際、ユーザ アカウントのテーブルを作成する場合に使用する追加基準。これらの属性は、ASA が接続を切断するかどうかを決定する場合に役立ちます。

  検証する追加属性を指定しない場合は、Framed IP アドレス属性の IP アドレスのみに基づいて決定されます。追加属性を設定し、ASA が現在追跡されているアドレスを含むが、その他の検証する属性が異なるアカウンティング開始メッセージを受信すると、古い属性を使用して開始するすべての接続は、IP アドレスが新しいユーザに再割り当てされたという前提で、切断されます。

値の範囲は 1 ～ 191 で、このコマンドは複数回入力できます。属性番号および説明のリストについては、http://www.iana.org/assignments/radius-types を参照してください。

- **host** *ip_address* [**key** *secret*] : RADIUS サーバまたは GGSN の IP アドレスです。ASA がメッセージを許可できるよう、任意で秘密キーを含めることができます。キーがない場合、IP アドレスだけがチェックされます。複数の RADIUS と GGSN のホストを識別するため、このコマンドは繰り返し実行できます。ASA は、これらのホストから RADIUS アカウンティング メッセージのコピーを受信します。
- **timeout users** *time* : ユーザのアイドル タイムアウトを設定します（hh: mm: ss 形式）。タイムアウトを付けない場合は、00:00:00 を指定してください。デフォルトは 1 時間です。

例

```
policy-map タイプは radius-accounting radius-acct-pmap を検査します
  parameters
    send response
    enable gprs
    validate-attribute 31
    host 10.2.2.2 key 123456789
    host 10.1.1.1 key 12345
class-map type management radius-class
  match port udp eq radius-acct
policy-map global_policy
  class radius-class
    inspect radius-accounting radius-acct-pmap
```

RADIUS アカウンティング インスペクションのサービス ポリシーの設定

デフォルトのインスペクション ポリシーでは、RADIUS アカウンティング インスペクションはイネーブルにされてないため、この検査が必要な場合はイネーブルにします。RADIUS アカウンティング インスペクションは ASA のトラフィック用に指示されますので、標準ルールではなく、管理インスペクション ルールとして設定してください。

手順

ステップ 1　検査を適用するトラフィックを識別するため L3/L4 マネジメント クラス マップを作成し、一致するトラフィックを識別します。

class-map type management *name*
match {port | access-list} *parameter*

例：

```
hostname(config)# class-map type management radius-class-map
hostname(config-cmap)# match port udp eq radius-acct
```

この例では、一致は radius acct UDP ポート（1646）です。ポートの範囲（**match port udp range** *number1 number2*）または **match access-list** *acl_name* と ACL を使って異なるポートを指定できます。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　RADIUS アカウンティング インスペクションに使用する L3/L4 管理クラス マップを指定します。

class *name*

例：

```
hostname(config-pmap)# class radius-class-map
```

ステップ 4　RADIUS アカウンティング インスペクションを設定します。

inspect radius-accounting *radius_accounting_policy_map*

radius_accounting_policy_map は「RADIUS アカウンティング インスペクション ポリシー マップの設定」（P.11-14）で作成した RADIUS アカウンティング インスペクション ポリシー マップです。

例：

```
hostname(config-class)# no inspect radius-accounting
hostname(config-class)# inspect radius-accounting radius-class-map
```

（注）　別のインスペクション ポリシー マップを使用するために使用中のポリシーを編集する場合、**no inspect radius-accounting** コマンドで RADIUS アカウンティング インスペクションを削除してから、新しいインスペクション ポリシー マップの名前で再追加します。

ステップ 5　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

RSH インスペクション

RSH 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。RSH プロトコルは、TCP ポート 514 で RSH クライアントから RSH サーバへの TCP 接続を使用します。クライアントとサーバは、クライアントが STDERR 出力ストリームを受信する TCP ポート番号をネゴシエートします。RSH インスペクションは、必要に応じて、ネゴシエートされたポート番号の NAT をサポートします。

RSH インスペクションのイネーブル化の詳細については、「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.7-11）を参照してください。

SNMP インスペクション

SNMP アプリケーション インスペクションでは、SNMP トラフィックを特定のバージョンの SNMP に制限できます。以前のバージョンの SNMP は安全性が低いため、セキュリティ ポリシーを使用して特定の SNMP バージョンを拒否する必要が生じる場合もあります。ASA は、SNMP バージョン 1、2、2c、または 3 を拒否できます。許可するバージョンは、SNMP マップを作成して制御します。

デフォルトのインスペクション ポリシーでは、SNMP インスペクションがイネーブルにされていないため、この検査が必要な場合はイネーブルにします。デフォルトのグローバル インスペクション ポリシーを編集するだけで、SNMP インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

手順

ステップ 1　SNMP マップを作成します。

snmp-map *map_name* コマンドを使ってマップを作成して SNMP マップ 設定モードに入り、次に **deny version** *version* コマンドで拒否するバージョンを識別します。バージョンは 1、2、2c、3 があります。

例：

次の例では、SNMP バージョン 1 および 2 を拒否しています。

```
hostname(config)# snmp-map sample_map
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# deny version 2
```

ステップ 2　必要な場合は、L3/L4 クラス マップを作成して、インスペクションを適用するトラフィックを識別します。

```
class-map name
match parameter
```

例：

```
hostname(config)# class-map snmp_class_map
hostname(config-cmap)# match access-list snmp
```

デフォルト グローバル ポリシーの inspection_default クラス マップは、すべてのインスペクション タイプのデフォルト ポートを含む特別なクラス マップです（**match default-inspection-traffic**）。このマップをデフォルト ポリシーまたは新しいサービス ポリシーで使用する場合は、このステップを省略できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 4　SNMP インスペクションに使用する L3/L4 クラス マップを指定します。

class *name*

例：

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

デフォルト ポリシーを編集する場合、または新しいポリシーで特別な inspection_default クラス マップを使用する場合は、*name* として **inspection_default** を指定します。それ以外の場合は、この手順ですでに作成したクラスを指定します。

ステップ 5　SNMP インスペクションを設定します。

inspect snmp [*snmp_map*]

snmp_map が任意の SNMP インスペクション ポリシー マップです。デフォルト以外のインスペクション処理が必要な場合にのみマップが必要です。

例：

```
hostname(config-class)# no inspect snmp
hostname(config-class)# inspect snmp snmp-map
```

（注）　別のインスペクション ポリシー マップを使用するためにデフォルト グローバル ポリシー（または使用中のポリシー）を編集する場合は、**no inspect dcerpc** コマンドで SNMP インスペクションを削除してから、新しいインスペクション ポリシー マップの名前で再追加します。

ステップ 6　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

XDMCP インスペクション

XDMCP 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が、XDMCP インスペクション エンジンは、**established** コマンドが適切に構成されていないと使用できません。

XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションは確立時に TCP を使用します。

XWindows セッションを正常にネゴシエートして開始するために、ASA は、Xhosted コンピュータからの TCP 戻り接続を許可する必要があります。戻り接続を許可するには、ASA で **established** コマンドを使用します。XDMCP がディスプレイを送信するポートをネゴシエートすると、**established** コマンドが参照され、この戻り接続を許可すべきかどうかが確認されます。

XWindows セッション中、マネージャは予約済みポート 6000 l n 上でディスプレイ Xserver と通信します。次の端末設定を行うと、各ディスプレイは別々に Xserver と接続します。

```
setenv DISPLAY Xserver: n
```

n はディスプレイ番号です。

XDMCP が使用されている場合、ディスプレイは IP アドレスを使用してネゴシエートされます。IP アドレスは、ASAが必要に応じて NAT を行うことができます。XDCMP インスペクションでは、PAT はサポートされません。

XDMCP インスペクションのイネーブル化の詳細については、「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.7-11）を参照してください。

PART 4

接続設定とサービスの品質

接続設定

この章では、ASA を経由する接続用、または、ASA を宛先とする管理接続用の接続を設定する方法について説明します。接続の設定には、次のものが含まれます。

- 最大接続数（TCP および UDP 接続、初期接続、クライアントあたりの接続）
- 接続タイムアウト
- デッド接続検出
- TCP シーケンスのランダム化
- TCP 正規化カスタマイゼーション
- TCP ステート バイパス
- グローバル タイムアウト
- 「接続の設定に関する情報」（P.12-1）
- 「接続設定のライセンス要件」（P.12-5）
- 「ガイドラインと制限事項」（P.12-5）
- 「デフォルト設定」（P.12-6）
- 「接続の設定」（P.12-6）
- 「接続設定のモニタリング」（P.12-14）
- 「接続設定の設定例」（P.12-14）
- 「接続設定の機能履歴」（P.12-16）

接続の設定に関する情報

この項では、接続の制限が必要になる理由を示します。

- 「TCP 代行受信および初期接続の制限」（P.12-2）
- 「クライアントレス SSL 互換での管理パケットの TCP 代行受信のディセーブル化」（P.12-2）
- 「デッド接続検出（DCD）」（P.12-2）
- 「TCP シーケンスのランダム化」（P.12-3）
- 「TCP の正規化」（P.12-3）
- 「TCP ステート バイパス」（P.12-4）

TCP 代行受信および初期接続の制限

初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA では、クライアントあたりの制限値と初期接続の制限を利用して TCP 代行受信を開始します。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。TCP 代行受信では、SYN クッキー アルゴリズムを使用して TCP SYN フラッディング攻撃を防ぎます。SYN フラッディング攻撃は、通常はスプーフィングされた IP アドレスから送信されてくる一連の SYN パケットで構成されています。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、接続要求に対してサービスを提供できなくなります。接続の初期接続しきい値を超えると、ASA はサーバのプロキシとして動作し、クライアント SYN 要求に対する SYN-ACK 応答を生成します。ASA がクライアントから ACK を受信すると、クライアントを認証し、サーバへの接続を許可できます。

（注）　TCP SYN クッキー保護を使用して SYN 攻撃からサーバを保護する場合、保護するサーバの TCP SYN バックログ キューより低い初期接続制限を設定する必要があります。これより高い初期接続制限を設定すると、有効なクライアントが、SYN 攻撃中にサーバにアクセスできなくなります。

TCP 代行受信に関する統計情報（攻撃を受けた上位 10 サーバなど）を表示する方法については、第 16 章「脅威の検出」を参照してください。

クライアントレス SSL 互換での管理パケットの TCP 代行受信のディセーブル化

デフォルトでは、TCP 管理接続では TCP 代行受信が常にイネーブルになっています。TCP 代行受信をイネーブルにすると、3 ウェイ TCP 接続確立のハンドシェイク パケットが代行受信されるため、ASA ではクライアントレス SSL のパケットを処理できなくなります。クライアントレス SSL では、クライアントレス SSL 接続で selective-ack や他の TCP オプションを提供するために、3 ウェイ ハンドシェイク パケットを処理する機能が必要になります。管理トラフィックの TCP 代行受信をディセーブルにするには、初期接続制限を設定します。初期接続制限に達した後にだけ TCP 代行受信をイネーブルにできます。

デッド接続検出（DCD）

DCD では、デッド接続を検出して、トラフィックをまだ処理できる接続を期限切れにすることなく、そのデッド接続を期限切れにすることができます。DCD は、アイドル状態でも有効な接続を維持する場合に設定します。

DCD をイネーブルにすると、アイドル タイムアウト動作が変化します。アイドル タイムアウトになると、DCD プローブが 2 つのエンドホストそれぞれに送信され、接続の有効性が判断されます。設定された間隔でプローブが送信された後にエンドホストが応答を返さないと、その接続は解放され、リセット値が設定されていれば各エンドホストに送信されます。両方のエンドホストが応答して接続の有効性が確認されると、アクティビティ タイムアウトは現在時刻に更新され、それに応じてアイドル タイムアウトが再スケジュールされます。

DCD をイネーブルにすると、TCP ノーマライザでのアイドルタイムアウト処理の動作が変更されます。DCD プローブにより、**show conn** コマンドで表示される接続でのアイドル タイムアウトがリセットされます。タイムアウト コマンドで設定したタイムアウト値を超過していても、DCD プローブのために存続している接続を判別するため、**show service-policy** コマンドには、DCD からのアクティビティ数を示すカウンタが含まれています。

TCP シーケンスのランダム化

それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。ASA は、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

- 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
- ASA で eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
- ASA で接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

TCP の正規化

TCP 正規化機能は、検出時に ASA が対処できる異常なパケットを識別します。ASA は、パケットを許可、ドロップ、またはクリアできます。TCP 正規化は、攻撃から ASA を保護するのに役立ちます。TCP 正規化は常にイネーブルになっていますが、機能の一部の動作をカスタマイズできます。

TCP 正規化には、設定できないアクションと設定できるアクションが含まれます。通常、接続をドロップまたはクリアする設定できないアクションは、どのような場合でも不良なパケットに適用されます。設定できるアクション（「TCP マップを使用した TCP ノーマライザのカスタマイズ」（P.12-6）を参照）は、ネットワークのニーズに応じたカスタマイズが必要な場合があります。

TCP 正規化に関する次のガイドラインを参考にしてください。

- ノーマライザは、SYN フラッドからの保護は行いません。ASA には、他の方法による SYN フラッド保護機能が組み込まれています。
- ノーマライザは、ASA がフェールオーバーのためにルーズ モードになっていない限り、SYN パケットを最初のパケットと見なします。

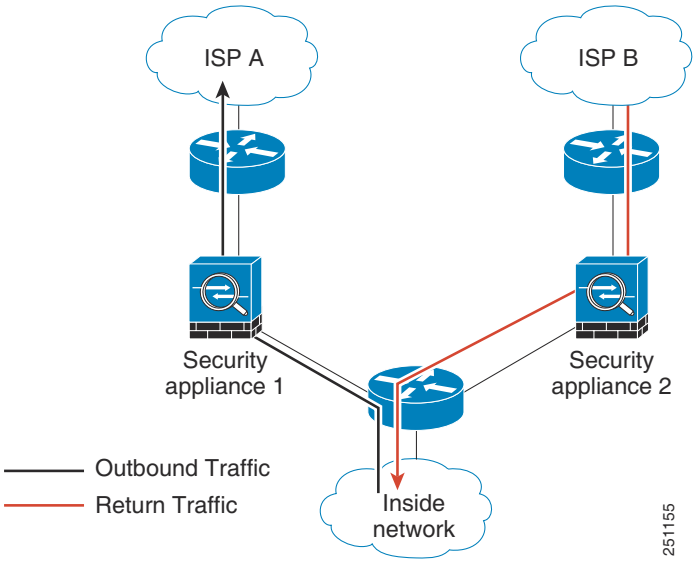
TCP ステート バイパス

デフォルトでは、ASA を通過するトラフィックはすべて、アダプティブ セキュリティ アルゴリズムを使用して検査され、セキュリティ ポリシーに基づいて、通過を許可されるか、またはドロップされます。ASA では、各パケットの状態（新規接続であるか、または確立済み接続であるか）がチェックされ、そのパケットをセッション管理パス（新規接続の SYN パケット）、ファスト パス（確立済みの接続）、またはコントロール プレーン パス（高度なインスペクション）に割り当てることによって、ファイアウォールのパフォーマンスが最大化されます。ステートフル ファイアウォールの詳細については、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。

高速パスの既存の接続に一致する TCP パケットは、セキュリティ ポリシーのあらゆる面の再検査を受けることなく ASA を通過できます。この機能によってパフォーマンスは最大になります。ただし、SYN パケットを使用してファスト パスにセッションを確立する方法、およびファスト パスで行われるチェック（TCP シーケンス番号など）が、非対称ルーティング ソリューションの障害となる場合があります。これは、接続の発信フローと着信フローの両方が同じ ASA を通過する必要があるためです。

たとえば、ある新しい接続が ASA 1 に開始されるとします。SYN パケットはセッション管理パスを通過し、接続のエントリが高速パス テーブルに追加されます。この接続の後続のパケットが ASA 1 を通過する場合、パケットは高速パスのエントリと一致して、通過します。しかし、後続のパケットが ASA 2 に到着すると、SYN パケットがセッション管理パスを通過していないために、高速パスにはその接続のエントリがなく、パケットはドロップされます。図 12-1 は非対称ルーティングの例を示したもので、アウトバウンド トラフィックはインバウンド トラフィックとは異なる ASA を通過しています。

図 12-1　非対称ルーティング



アップストリーム ルータに設定された非対称ルーティングがあり、トラフィックが 2 つの ASA の間で切り替わる場合は、特定のトラフィックに対して TCP ステート バイパスを設定できます。TCP ステート バイパスは、高速パスでのセッションの確立方法を変更し、高速パスのインスペクションをディセーブルにします。この機能は、TCP トラフィックを UDP 接続と同じように処理します。指定されているネットワークに一致する非 SYN パケットが ASA に到着し、高速パスのエントリがない場合は、パケットはセッション管理パスを通過して、高速パスの接続を確立します。いったん高速パスに入ると、トラフィックは高速パスのインスペクションをバイパスします。

接続設定のライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

ガイドラインと制限事項

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド モードとトランスペアレント モードでサポートされます。

フェールオーバーのガイドライン

フェールオーバーはサポートされます。

TCP ステート バイパスでサポートされない機能

TCP ステート バイパスを使用するときは、次の機能はサポートされません。

- アプリケーション インスペクション：アプリケーション インスペクションではインバウンド トラフィックとアウトバウンド トラフィックの両方が同じ ASA を通過する必要があるので、アプリケーション インスペクションは TCP ステート バイパスではサポートされません。
- AAA 認証済みセッション：ユーザが 1 つの ASA で認証するとき、他の ASA を介して返されるトラフィックは、ユーザがその ASA で認証を受けていないので拒否されます。
- TCP 代行受信、最大初期接続制限、TCP シーケンス番号のランダム化：ASA は接続のステートを追跡しないので、これらの機能は適用されません。
- TCP 正規化：TCP ノーマライザはディセーブルになります。
- SSM および SSC 機能：TCP ステート バイパスおよび IPS や CSC などの SSM または SSC 上で実行するアプリケーションは使用できません。

TCP ステート バイパスの NAT のガイドライン

変換セッションは ASA ごとに個別に確立されるので、TCP ステート バイパス トラフィック用に両方のASAでスタティック NAT を設定してください。ダイナミック NAT を使用すると、ASA 1 でのセッションに選択されるアドレスが、ASA 2 でのセッションに選択されるアドレスと異なります。

最大同時接続および初期接続のガイドライン

ASA モデル上の CPU コア数によっては、同時接続および初期接続の最大数が、各コアによる接続の管理方法が原因で、設定されている数を超える場合があります。最悪の場合、ASA は最大 *n*-1 の追加接続および初期接続を許可します。ここで、*n* はコアの数です。たとえば、モデルに 4 つのコアがあり、6 つの同時接続および 4 つの初期接続を設定した場合は、各タイプで 3 つの追加接続を使用できます。ご使用のモデルのコア数を確認するには、**show cpu core** コマンドを入力します。

デフォルト設定

TCP ステート バイパス

TCP ステート バイパスは、デフォルトでディセーブルになっています。

TCP ノーマライザ

デフォルト コンフィギュレーションには、次の設定が含まれます。

```
no check-retransmission
no checksum-verification
exceed-mss allow
queue-limit 0 timeout 4
reserved-bits allow
syn-data allow
synack-data drop
invalid-ack drop
seq-past-window drop
tcp-options range 6 7 clear
tcp-options range 9 255 clear
tcp-options selective-ack allow
tcp-options timestamp allow
tcp-options window-scale allow
ttl-evasion-protection
urgent-flag clear
window-variation allow-connection
```

接続の設定

接続の設定のタスク フロー

ステップ 1　TCP 正規化カスタマイゼーションについては、「TCP マップを使用した TCP ノーマライザのカスタマイズ」（P.12-6）に従って TCP マップを作成します。

ステップ 2　すべての接続設定については、第 1 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」に従ってサービス ポリシーを設定します。

ステップ 3　「接続の設定」（P.12-11）に従って接続を設定します。

TCP マップを使用した TCP ノーマライザのカスタマイズ

TCP ノーマライザをカスタマイズするには、まず、TCP マップを使用する設定を定義します。

手順の詳細

ステップ 1　検索する TCP 正規化基準を指定するには、次のコマンドを入力して TCP マップを作成します。

```
hostname(config)# tcp-map tcp-map-name
```

TCP マップごとに 1 つまたは複数の設定値をカスタマイズできます。

ステップ 2　（任意）次の 1 つ以上のコマンド（表 12-1 を参照）を入力して TCP マップ基準を設定します。一部の設定をカスタマイズする場合、入力しないコマンドにはデフォルトが使用されます。

表 12-1　tcp-map コマンド

コマンド	注
check-retransmission	一貫性のない TCP 再送信を防止します。
checksum-verification	チェックサムを確認します。
exceed-mss {**allow** | **drop**}	データ長が TCP 最大セグメント サイズを超えるパケットに対するアクションを設定します。 （デフォルト）**allow** キーワードは、データ長が TCP 最大セグメント サイズを超えるパケットを許可します。 **drop** キーワードは、データ長が TCP 最大セグメント サイズを超えるパケットをドロップします。
invalid-ack {**allow** | **drop**}	無効な ACK を含むパケットに対するアクションを設定します。次のような場合に無効な ACK が検出される可能性があります。 • TCP 接続が SYN-ACK-received ステータスでは、受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号と同じでない場合、その ACK は無効です。 • 受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号より大きい場合は常に、その ACK は無効です。 **allow** キーワードは、無効な ACK を含むパケットを許可します。 （デフォルト）**drop** キーワードは、無効な ACK を含むパケットをドロップします。 **（注）**　無効な ACK を含む TCP パケットは、WAAS 接続で自動的に許可されます。

表 12-1　tcp-map コマンド（続き）

コマンド	注
queue-limit *pkt_num* [**timeout** *seconds*]	バッファに格納して TCP 接続の正しい順序に設定できる、異常なパケットの最大数を設定します。1 ～ 250 パケットです。デフォルト値の 0 は、この設定がディセーブルであり、トラフィックのタイプに応じたデフォルトのシステム キュー制限が使用されることを意味します。 • アプリケーション インスペクション（**inspect** コマンド）、IPS（**ips** コマンド）、および TCP インスペクション再送信（TCP マップ **check-retransmission** コマンド）のための接続のキュー制限は、3 パケットです。ASA が異なるウィンドウ サイズの TCP パケットを受信した場合は、アドバタイズされた設定と一致するようにキュー制限がダイナミックに変更されます。 • 他の TCP 接続の場合は、異常なパケットはそのまま通過します。 **queue-limit** コマンドを 1 以上に設定した場合、すべての TCP トラフィックに対して許可される異常なパケットの数は、この設定と一致します。たとえば、アプリケーション インスペクション、IPS、および TCP check-retransmission のトラフィックの場合、TCP パケットからアドバタイズされたすべての設定が**キュー制限**設定を優先して、無視されます。その他の TCP トラフィックについては、異常なパケットはバッファに格納されて、そのまま通過するのではなく、正しい順序に設定されます。 **timeout** *seconds* 引数は、異常なパケットがバッファ内に留まることができる最大時間を設定します。設定できる値は 1 ～ 20 秒です。タイムアウト期間内に正しい順序に設定されて渡されなかったパケットはドロップされます。デフォルトは 4 秒です。*pkt_num* 引数を 0 に設定した場合は、どのトラフィックのタイムアウトも変更できません。**timeout** キーワードを有効にするには、制限を 1 以上に設定する必要があります。
reserved-bits {**allow** | **clear** | **drop**}	TCP ヘッダーの予約ビットに対するアクションを設定します。 （デフォルト）**allow** キーワードは、TCP ヘッダーの予約ビットが設定されているパケットを許可します。 **clear** キーワードは、TCP ヘッダーの予約ビットを消去して、パケットを許可します。 **drop** キーワードは、TCP ヘッダーの予約ビットが設定されているパケットをドロップします。

表 12-1　tcp-map コマンド（続き）

コマンド	注
seq-past-window {**allow** | **drop**}	パストウィンドウ シーケンス番号を含むパケットに対するアクションを設定します。つまり、受信した TCP パケットのシーケンス番号が、TCP 受信ウィンドウの右端より大きい場合です。 **allow** キーワードは、パストウィンドウ シーケンス番号を含むパケットを許可します。このアクションは、**queue-limit** コマンドが 0（ディセーブル）に設定されている場合に限り許可されます。 （デフォルト）**drop** キーワードは、パストウィンドウ シーケンス番号を含むパケットをドロップします。
synack-data {**allow** | **drop**}	データを含む TCP SYNACK パケットに対するアクションを設定します。 **allow** キーワードは、データを含む TCP SYNACK パケットを許可します。 （デフォルト）**drop** キーワードは、データを含む TCP SYNACK パケットをドロップします。
syn-data {**allow** | **drop**}	データを含む SYN パケットに対するアクションを設定します。 （デフォルト）**allow** キーワードは、データを含む SYN パケットを許可します。 **drop** キーワードは、データを含む SYN パケットをドロップします。
tcp-options {**selective-ack** | **timestamp** | **window-scale**} {**allow** | **clear**} または **tcp-options range** *lower upper* {**allow** | **clear** | **drop**}	selective-ack、timestamp、window-scale などの TCP オプションを含むパケットに対するアクションを設定します。 （デフォルト）**allow** キーワードは、指定したオプションを含むパケットを許可します。 （**range** の場合のデフォルト）**clear** キーワードは、オプションを消去して、パケットを許可します。 **drop** キーワードは、指定したオプションを含むパケットをドロップします。 **selective-ack** キーワードは、SACK オプションに対するアクションを設定します。 **timestamp** キーワードは、タイムスタンプ オプションに対するアクションを設定します。タイムスタンプ オプションを消去すると、PAWS と RTT がディセーブルになります。 **widow-scale** キーワードは、ウィンドウ スケール メカニズム オプションに対するアクションを設定します。 **range** キーワードは、オプションの範囲を指定します。*lower* 引数は、範囲の下限を設定します。6、7、または 9 ～ 255 です。 *upper* 引数は、範囲の上限を設定します。6、7、または 9 ～ 255 です。

表 12-1　tcp-map コマンド（続き）

コマンド	注
ttl-evasion-protection	TTL 回避保護をディセーブルにします。セキュリティ ポリシーを回避しようとする攻撃を防ぐ場合は、このコマンドを入力しないでください。 たとえば、攻撃者は TTL を非常に短くしてポリシーを通過するパケットを送信できます。TTL がゼロになると、ASA とエンドポイントの間のルータはパケットをドロップします。この時点で、攻撃者は TTL を長くした悪意のあるパケットを送信できます。このパケットは、ASA にとって再送信のように見えるため、通過します。一方、エンドポイント ホストにとっては、このパケットが攻撃者によって受信された最初のパケットになります。この場合、攻撃者はセキュリティによる攻撃の防止を受けず、攻撃に成功します。
urgent-flag {**allow** | **clear**}	URG フラグを含むパケットに対するアクションを設定します。URG フラグは、ストリーム中の他のデータよりもプライオリティの高い情報がこのパケットに含まれていることを示すために使用します。TCP RFC では、URG フラグの正確な解釈が明確にされていません。そのため、エンド システムは緊急オフセットをさまざまな方法で処理しており、これが攻撃に対する脆弱性になることがあります。 **allow** キーワードは、URG フラグを含むパケットを許可します。 （デフォルト）**clear** キーワードは、URG フラグを消去してパケットを許可します。
window-variation {**allow** | **drop**}	予想外のウィンドウ サイズの変更が発生した接続に対するアクションを設定します。ウィンドウ サイズ メカニズムによって、TCP は大きなウィンドウをアドバタイズでき、続いて、過剰な量のデータを受け入れずに、はるかに小さなウィンドウをアドバタイズできます。TCP 仕様により、「ウィンドウの縮小」は極力避けることが推奨されています。この条件が検出された場合に、接続をドロップできます。 （デフォルト）**allow** キーワードは、ウィンドウが変化した接続を許可します。 **drop** キーワードは、ウィンドウが変化した接続をドロップします。

接続の設定

接続を設定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**class-map** *name* **例：** hostname(config)# class-map bypass_traffic	ステートフル ファイアウォール インスペクションをディセーブルにするトラフィックを識別するためのクラス マップを作成します。
ステップ 2	**match** *parameter* **例：** hostname(config-cmap)# match access-list bypass	クラス マップのトラフィックを指定します。詳細については、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。
ステップ 3	**policy-map** *name* **例：** hostname(config)# policy-map tcp_bypass_policy	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ポリシー マップを追加または編集します。
ステップ 4	**class** *name* **例：** hostname(config-pmap)# class bypass_traffic	ステップ 1 で作成したクラス マップを識別します。
ステップ 5	次のいずれかまたは複数の作業を実行します。	

コマンド	目的
set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]} **例：** `hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable`	最大接続数を設定するか、TCP シーケンスのランダム化をイネーブルにするかどうかを設定します。 **conn-max** *n* 引数には、許可される同時 TCP/UDP 接続の最大数を 0 ～ 2000000 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。 TCP または UDP の同時接続を許可するように 2 つのサーバが設定されている場合、接続制限数は、設定されている各サーバに別々に適用されます。 クラスに設定された場合、この引数では、クラス全体で許可される同時接続最大数が制限されます。この場合、1 つの攻撃ホストがすべての接続を使い果たし、クラスにおいて ACL に一致する他のホストが使用できる接続がなくなる可能性があります。 **embryonic-conn-max** *n* 引数には、許可される同時初期接続の最大数を 0 ～ 2000000 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。 **per-client-embryonic-max** *n* 引数には、クライアントごとに許可される同時初期接続の最大数を 0 ～ 2000000 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。 **per-client-max** *n* 引数には、クライアントごとに許可される同時接続の最大数を 0 ～ 2000000 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。クラスに設定された場合、この引数では、クラスにおいて ACL に一致する各ホストに許可される同時接続最大数が制限されます。 **random-sequence-number** {**enable** | **disable**} キーワードで、TCP シーケンス番号のランダム化をイネーブルまたはディセーブルにします。詳細については、「TCP シーケンスのランダム化」（P.12-3）を参照してください。 このコマンドを 1 行ですべて入力することも（順序は任意）、各属性を別々のコマンドとして入力することもできます。ASA は、コマンドを実行コンフィギュレーション内で 1 行に結合します。 **（注）** 管理トラフィックの場合は、**conn-max** キーワードと **embryonic-conn-max** キーワードだけを設定できます。

コマンド	目的
set connection timeout {[**embryonic** *hh*:*mm*:*ss*] {**idle** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [dcd *hh*:*mm*:*ss* [*max_retries*]]} **例：** hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0 half-closed 0:20:0 dcd	接続タイムアウトを設定します。グローバル タイムアウトについては、コマンド リファレンスの **timeout** コマンドを参照してください。次に説明するデフォルト値は、これらの動作のグローバルのデフォルト値を変更していないことを前提としています。グローバルのデフォルト値はここで説明する値を上書きします。 **embryonic** *hh*:*mm*:*ss* キーワードには、TCP 初期（ハーフオープン）接続が閉じられるまでのタイムアウトを 0:0:5 ～ 1193:00:00 の間で設定します。デフォルトは 0:0:30 です。この値を 0 に設置することもでき、この場合は接続がタイムアウトしないことを意味します。 **idle** *hh*:*mm*:*ss* キーワードは、いずれかのプロトコルの確立された接続が閉じてからのアイドル タイムアウト期間を 0:0:1 から 1193:0:0 の間で設定します。デフォルトは 1:0:0 です。この値を 0 に設置することもでき、この場合は接続がタイムアウトしないことを意味します。TCP トラフィックの場合、**reset** キーワードを指定すると、接続のタイムアウト時にリセット パケットが TCP エンドポイントに送信されます。 The **half-closed** *hh*:*mm*:*ss* キーワードは、ハーフ クローズ接続が閉じられるまでのアイドル タイムアウト期間を 0:5:0（9.1(1) 以前の場合）または 0:0:30（9.1(2) 以降の場合）から 1193:0:0 の間で設定します。デフォルトは 0:10:0 です。ハーフクローズの接続は DCD の影響を受けません。また、ASA は、ハーフクローズ接続を切断するときにリセット パケットを送信しません。 **dcd** キーワードは、DCD をイネーブルにします。DCD では、デッド接続を検出して、トラフィックをまだ処理できる接続を期限切れにすることなく、そのデッド接続を期限切れにすることができます。DCD は、アイドル状態でも有効な接続を維持する場合に設定します。TCP 接続がタイムアウトすると、ASA は、エンドホストに DCD プローブを送信して接続の有効性を判断します。最大再試行回数を超えてもエンドホストの一方が応答しない場合、ASA はその接続を解放します。両方のエンドホストが応答して接続の有効性が確認されると、ASA はアクティビティ タイムアウトを現在時刻に更新し、それに応じてアイドル タイムアウトを再スケジュールします。*retry-interval* には、DCD プローブに応答がない場合に別のプローブを送信するまで待機する時間を、*hh*:*mm*:*ss* 形式で、0:0:1 から 24:0:0 の範囲で設定します。デフォルトは 0:0:15 です。*max-retries* には、接続が無活動状態であると宣言するまでに失敗する DCD の連続再試行回数を設定します。最小値は 1、最大値は 255 です。デフォルトは 5 です。 デフォルトの **udp** アイドル タイムアウトは 2 分です。 デフォルトの **icmp** アイドル タイムアウトは 2 秒です。 デフォルトの **esp** および **ha** アイドル タイムアウトは 30 秒です。 その他すべてのプロトコルでは、デフォルトのアイドル タイムアウトは 2 分です。 タイムアウトにならないようにするには、0:0:0 を入力します。 このコマンドを 1 行ですべて入力することも（順序は任意）、各属性を別々のコマンドとして入力することもできます。コマンドは実行コンフィギュレーションで 1 行に結合されます。このコマンドは、管理トラフィックでは使用できません。

	コマンド	目的
	set connection advanced-options *tcp-map-name* **例：** hostname(config-pmap-c)# set connection advanced-options tcp_map1	TCP ノーマライザをカスタマイズします。TCP マップを作成するには、「TCP マップを使用した TCP ノーマライザのカスタマイズ」（P.12-6）を参照してください。
	set connection advanced-options tcp-state-bypass **例：** hostname(config-pmap-c)# set connection advanced-options tcp-state-bypass	TCP ステート バイパスをイネーブルにします。
ステップ 6	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} **例：** hostname(config)# service-policy tcp_bypass_policy outside	1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。**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。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。

接続設定のモニタリング

TCP ステート バイパスをモニタするには、次のいずれかのタスクを実行します。

コマンド	目的
show conn	**show conn** コマンドを使用した場合、TCP ステート バイパスを使用する接続にはフラグ「b」が表示されます。

接続設定の設定例

- 「接続の制限値とタイムアウトの設定例」（P.12-15）
- 「TCP ステート バイパスの設定例」（P.12-15）
- 「TCP 正規化の設定例」（P.12-15）

接続の制限値とタイムアウトの設定例

次の例では、すべてのトラフィックに対して接続の制限値とタイムアウトを設定しています。

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname(config-pmap-c)# set connection conn-max 1000 embryonic-conn-max 3000
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0 half-closed
0:20:0 dcd
hostname(config-pmap-c)# service-policy CONNS interface outside
```

複数のパラメータを使用して **set connection** コマンドを入力するか、各パラメータを別々のコマンドとして入力できます。ASA は、コマンドを実行コンフィギュレーション内で 1 行に結合します。たとえば、クラス コンフィギュレーション モードで次の 2 つのコマンドを入力するとします。

```
hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50
```

show running-config policy-map コマンドの出力には、2 つのコマンドの結果が単一の結合コマンドとして表示されます。

```
set connection conn-max 600 embryonic-conn-max 50
```

TCP ステート バイパスの設定例

TCP ステート バイパスの設定例を次に示します。

```
hostname(config)# access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224 any

hostname(config)# class-map tcp_bypass
hostname(config-cmap)# description "TCP traffic that bypasses stateful firewall"
hostname(config-cmap)# match access-list tcp_bypass

hostname(config-cmap)# policy-map tcp_bypass_policy
hostname(config-pmap)# class tcp_bypass
hostname(config-pmap-c)# set connection advanced-options tcp-state-bypass

hostname(config-pmap-c)# service-policy tcp_bypass_policy outside

hostname(config-pmap-c)# static (inside,outside) 209.165.200.224 10.1.1.0 netmask
255.255.255.224
```

TCP 正規化の設定例

たとえば、既知の FTP データ ポートと Telnet ポートの間の TCP ポート範囲に送信されるすべてのトラフィックで緊急フラグと緊急オフセット パケットを許可するには、次のコマンドを入力します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config-tcp-map)# class-map urg-class
hostname(config-cmap)# match port tcp range ftp-data telnet
hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap
hostname(config-pmap-c)# service-policy pmap global
```

接続設定の機能履歴

表 12-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 12-2　　接続設定の機能履歴

機能名	プラットフォーム リリース	機能情報
TCP ステート バイパス	8.2(1)	この機能が導入されました。**set connection advanced-options tcp-state-bypass** コマンドが導入されました。
すべてのプロトコルの接続タイムアウト	8.2(2)	アイドル タイムアウトは、TCP だけでなく、すべてのプロトコルに適用するように変更されました。 **set connection timeout** コマンドが変更されました。
バックアップ スタティック ルートを使用する接続のタイムアウト	8.2(5)/8.4(2)	同じネットワークへの複数のスタティック ルートが存在しており、それぞれメトリックが異なる場合は、ASA は接続確立時点でメトリックが最良のルートを使用します。より適切なルートが使用可能になった場合は、このタイムアウトによって接続が閉じられるので、その適切なルートを使用して接続を再確立できます。デフォルトは 0 です（接続はタイムアウトしません）。この機能を使用するには、タイムアウトを新しい値に変更します。 **timeout floating-conn** コマンドが変更されました。
PAT xlate に対する設定可能なタイムアウト	8.4(3)	PAT xlate がタイムアウトし（デフォルトでは 30 秒後）、ASA が新しい変換用にポートを再使用すると、一部のアップストリーム ルータは、前の接続がアップストリーム デバイスで依然として開いている可能性があるため、この新しい接続を拒否する場合があります。PAT xlate のタイムアウトを、30 秒～ 5 分の範囲内の値に設定できるようになりました。 **timeout pat-xlate** コマンドが導入されました。 *この機能は、8.5(1) または 8.6(1) では使用できません。*

表 12-2　接続設定の機能履歴（続き）

機能名	プラットフォームリリース	機能情報
サービス ポリシー ルールの最大接続数の引き上げ	9.0(1)	サービス ポリシー ルールの最大接続数が 65535 から 2000000 に引き上げられました。 **set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max**、**set connection per-client-max** の各コマンドが変更されました。
ハーフ クローズ タイムアウト最小値を 30 秒に削減	9.1(2)	グローバル タイムアウトおよび接続タイムアウトの両方のハーフ クローズド タイムアウトの最小値は、より優れた DoS 保護を提供するために 5 分から 30 秒に短縮されました。 **set connection timeout half-closed**、**timeout half-closed** の各コマンドが変更されました。

CHAPTER 13

QoS

衛星接続を使用した長距離電話では、会話が、短い間ですが認識できる程度に割り込みされ、不定期に中断されることがあります。このような中断は、ネットワークで送信されるパケットが到着する間隔の時間で、遅延と呼ばれます。音声やビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。Quality of Service（QoS）機能を使用すると、重要なトラフィックのプライオリティを高くし、帯域幅の過剰な使用を防ぎ、ネットワーク ボトルネックを管理してパケットのドロップを防止できます。

（注） ASASM については、ASASM の代わりにスイッチで QoS を実行することを推奨します。スイッチの方が、この領域においては多機能です。一般的に、QoS は、ASA よりも広範な機能を持つ傾向がある、ネットワーク内のルータおよびスイッチで実行するのが最適です。

この章では、QoS ポリシーの適用方法について説明します。

QoS について

常に変化するネットワーク環境では、QoS は 1 回限りの構成ではなく、ネットワーク設計の継続的で不可欠な要素であることを考慮する必要があります。

この項では、ASA で使用できる QoS 機能について説明します。

サポートされる QoS 機能

ASA は、次の QoS の機能をサポートしています。

- ポリシング：分類されたフローがネットワーク帯域幅を大量に使用するのを防ぐため、クラスごとの最大使用帯域幅を制限できます。詳細については、「ポリシング」（P.13-2）を参照してください。
- プライオリティ キューイング：Voice over IP（VoIP）のような遅延を許されない重要なトラフィックについて、トラフィックを低遅延キューイング（LLQ）に指定することで、常に他のトラフィックより先に送信できます。「プライオリティ キューイング」（P.13-3）を参照してください。

トークン バケットとは

トークン バケットは、フロー内のデータを規制するデバイス（トラフィック ポリサーなど）の管理に使用されます。トークン バケット自体には、廃棄ポリシーまたはプライオリティ ポリシーはありません。むしろ、トークン バケットは、フローによって規制機能が過剰に働く場合に、トークンを廃棄し、送信キューの管理の問題はフローに任せます。

トークン バケットは、転送レートの正式な定義です。トークン バケットには、バースト サイズ、平均レート、時間間隔という 3 つのコンポーネントがあります。平均レートは通常 1 秒間のビット数で表されますが、次のような関係によって、任意の 2 つの値を 3 番目の値から求めることができます。

平均レート = バースト サイズ / 時間間隔

これらの用語の定義は次のとおりです。

- 平均レート：認定情報レート（CIR）とも呼ばれ、単位時間に送信または転送できるデータ量の平均値を指定します。
- バースト サイズ：認定バースト（Bc）サイズとも呼ばれ、スケジューリングに関する問題を発生させることなく単位時間内に送信できるトラフィックの量を、バーストあたりのバイト数で指定します。
- 時間間隔：測定間隔とも呼ばれ、バーストごとの時間を秒単位で指定します。

トークン バケットのたとえで言えば、トークンは特定のレートでバケットに入れられます。バケット自体には指定された容量があります。バケットがいっぱいになると、新しく到着するトークンは廃棄されます。各トークンは、送信元が一定の数のビットをネットワークに送信するための権限です。パケットを送信するため、規制機能はパケット サイズに等しい数のトークンをバケットから削除する必要があります。

パケットを送信するための十分なトークンがバケットにない場合、パケットは、パケットが廃棄されるか、ダウン状態とマークされるまで待機します。バケットがすでにトークンで満たされている場合、着信トークンはオーバーフローし、以降のパケットには使用できません。したがって、いつでも、送信元がネットワークに送信できる最大のバーストは、バケットのサイズにほぼ比例します。

ポリシング

ポリシングは、設定した最大レート（ビット/秒単位）を超えるトラフィックが発生しないようにして、1 つのトラフィック クラスが全体のリソースを占有しないようにする方法です。トラフィックが最大レートを超えると、ASA は超過した分のトラフィックをドロップします。また、ポリシングでは、許可されるトラフィックの最大単一バーストも設定されます。

プライオリティ キューイング

LLQ プライオリティ キューイングを使用すると、特定のトラフィック フロー（音声やビデオのような遅延の影響を受けやすいトラフィックなど）をその他のトラフィックよりも優先できます。プライオリティ キューイングでは、インターフェイスで LLQ プライオリティ キューが使用されます（「インターフェイスのプライオリティ キューの設定」（P.13-6）を参照してください）。一方、他のトラフィックはすべて「ベストエフォート」キューに入ります。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これは*テール ドロップ*と呼ばれます。キューがいっぱいになることを避けるには、キューのバッファ サイズを大きくします。送信キューに入れることのできるパケットの最大数も微調整できます。これらのオプションを使用して、プライオリティ キューイングの遅延と強固さを制御できます。LLQ キュー内のパケットは、常に、ベストエフォート キュー内のパケットよりも前に送信されます。

QoS 機能の相互作用のしくみ

ASA で必要な場合は、個々の QoS 機能を単独で設定できます。ただし、普通は、たとえば一部のトラフィックを優先させて、他のトラフィックによって帯域幅の問題が発生しないようにするために、複数の QoS 機能を ASA に設定します。次のことを設定できます。

プライオリティ キューイング（特定のトラフィックについて）+ ポリシング（その他のトラフィックについて）

同じトラフィックのセットに対して、プライオリティ キューイングとポリシングを両方設定することはできません。

DSCP（DiffServ）の保存

DSCP（DiffServ）のマーキングは、ASA を通過するすべてのトラフィックで維持されます。ASA は、分類されたトラフィックをローカルにマーク/再マークすることはありません。たとえば、すべてのパケットの完全優先転送（EF）DSCP ビットを受け取り、「プライオリティ」処理が必要かどうかを判断し、ASA にそれらのパケットを LLQ に入れさせることができます。

QoS のガイドライン

コンテキスト モードのガイドライン

シングル コンテキスト モードでだけサポートされます。マルチ コンテキスト モードをサポートしません。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

IPv6 のガイドライン

IPv6 はサポートされません。

モデルのガイドライン

- （ASA 5512-X ～ ASA 5555-X）プライオリティ キューイングは、Management 0/0 インターフェイスでサポートされていません。
- （ASASM）ポリシングだけがサポートされます。

その他のガイドラインと制限事項

- QoS は単方向に適用されます。ポリシー マップを適用するインターフェイスに出入りする（QoS 機能によって異なります）トラフィックだけが影響を受けます。詳細については、「機能の方向」（P.1-4）を参照してください。
- プライオリティ トラフィックに対しては、**class-default** クラス マップは使用できません。
- プライオリティ キューイングの場合、プライオリティ キューは物理インターフェイス用または ASASM の場合には VLAN 用に設定する必要があります。
- ポリシングでは、to-the-box トラフィックはサポートされません。
- ポリシングでは、VPN トンネルとの間で送受信されるトラフィックはインターフェイスのポリシングをバイパスします。
- ポリシングでは、トンネル グループ クラス マップを照合する場合、出力ポリシングのみがサポートされます。

QoS の設定

ASA に QoS を実装するには、次の手順を使用します。

ステップ 1　「プライオリティ キューのプライオリティ キューおよび TX リング制限の決定」（P.13-4）。

ステップ 2　「インターフェイスのプライオリティ キューの設定」（P.13-6）。

ステップ 3　「プライオリティ キューイングとポリシング用のサービス ルールの設定」（P.13-7）。

プライオリティ キューのプライオリティ キューおよび TX リング制限の決定

プライオリティ キューおよび TX リング制限を決定するには、次のワークシートを使用します。

- 「キュー制限のワークシート」（P.13-5）
- 「TX リング制限のワークシート」（P.13-5）

キュー制限のワークシート

次のワークシートは、プライオリティ キューのサイズを計算する方法を示しています。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます（*テール ドロップ*と呼ばれます）。キューがいっぱいになることを避けるには、「インターフェイスのプライオリティ キューの設定」（P.13-6）に従ってキューのバッファ サイズを調節します。

ワークシートに関するヒント:

- アウトバウンド帯域幅：たとえば、DSL のアップリンク速度は 768 Kbps などです。プロバイダーに確認してください。
- 平均パケット サイズ：この値は、コーデックまたはサンプリング サイズから決定します。たとえば、VoIP over VPN の場合は、160 バイトなどを使用します。使用するサイズがわからない場合は、256 バイトにすることをお勧めします。
- 遅延：遅延はアプリケーションによって決まります。たとえば、VoIP の場合の推奨される最大遅延は 200 ミリ秒です。使用する遅延がわからない場合は、500 ミリ秒にすることをお勧めします。

表 13-1　　キュー制限のワークシート

1	_____ *アウトバウンド帯域幅（Mbps または Kbps）*	Mbps	**x 125**	**=**	_____ *バイト数/ミリ秒*		
		Kbps	**x .125**	**=**	_____ *バイト数/ミリ秒*		
2	_____ *ステップ 1 からのバイト数/ミリ秒*		**÷** _____ *平均パケット サイズ（バイト）*	**x**	_____ *遅延（ミリ秒）*	**=**	_____ *キュー制限（パケット数）*

TX リング制限のワークシート

次のワークシートは、TX リング制限の計算方法を示しています。この制限により、イーサネット送信ドライバが受け入れるパケットの最大数が決まります。この制限に達すると、ドライバはパケットをインターフェイスのキューに差し戻し、輻輳が解消されるまでパケットをバッファに格納できるようにします。この設定により、ハードウェアベースの送信リングがプライオリティの高いパケットに対して制限以上の余分な遅延を発生させないことが保証されます。

ワークシートに関するヒント:

- アウトバウンド帯域幅：たとえば、DSL のアップリンク速度は 768 Kbps などです。プロバイダーに確認してください。
- 最大パケット サイズ：通常、最大サイズは 1538 バイト、またはタグ付きイーサネットの場合は 1542 バイトです。ジャンボ フレームを許可する場合（プラットフォームでサポートされている場合）、パケット サイズはさらに大きくなる場合があります。
- 遅延：遅延はアプリケーションによって決まります。たとえば、VoIP のジッタを制御するには、20 ミリ秒を使用します。

表 13-2　TX リング制限のワークシート

1	_____	Mbps	**x 125**	**=**	_____	
	アウトバウンド帯域幅（Mbps または Kbps）				*バイト数/ミリ秒*	
		Kbps	**x 0.125**	**=**	_____	
					バイト数/ミリ秒	
2	_____	**÷**	_____	**x**	_____	**=** _____
	ステップ 1 からのバイト数/ミリ秒		*最大パケット サイズ（バイト）*		*遅延（ミリ秒）*	*TX リング制限（パケット数）*

インターフェイスのプライオリティ キューの設定

物理インターフェイスでトラフィックに対するプライオリティ キューイングをイネーブルにする場合は、各インターフェイスでプライオリティ キューを作成する必要もあります。各物理インターフェイスは、プライオリティ トラフィック用と、他のすべてのトラフィック用に、2 つのキューを使用します。他のトラフィックについては、必要に応じてポリシングを設定できます。

はじめる前に

- （ASASM）ASASM では、プライオリティ キューイングはサポートされません。
- （ASA 5512-X ～ ASA 5555-X）プライオリティ キューイングは、Management 0/0 インターフェイスでサポートされていません。

手順

ステップ 1　インターフェイスのプライオリティ キューを作成します。

priority-queue *interface_name*

例：

```
hostname(config)# priority-queue inside
```

interface_name 引数には、プライオリティキューをイネーブルにする物理インターフェイスの名前、または ASASM の場合は VLAN インターフェイス名を指定します。

ステップ 2　プライオリティ キューのサイズを変更します。

queue-limit *number_of_packets*

例：

```
hostname(config-priority-queue)# queue-limit 260
```

デフォルトのキューの制限は 1024 パケットです。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます（*テール ドロップ*と呼ばれます）。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。

queue-limit コマンドの値の範囲の上限は、実行時に動的に決まります。この制限を表示するには、コマンドラインで **queue-limit ?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。

指定した **queue-limit** は、プライオリティの高い低遅延キューとベストエフォート キューの両方に適用されます。

ステップ 3　プライオリティ キューの深さを指定します。

tx-ring-limit *number_of_packets*

例：

```
hostname(config-priority-queue)# tx-ring-limit 3
```

デフォルトの tx-ring-limit は 128 パケットです。このコマンドは、イーサネット送信ドライバが受け入れる低遅延パケットまたは通常プライオリティ パケットの最大数を設定します。この制限に達すると、ドライバはパケットをインターフェイスのキューに差し戻し、輻輳が解消されるまでパケットをバッファに格納できるようにします。この設定により、ハードウェアベースの送信リングがプライオリティの高いパケットに対して制限以上の余分な遅延を発生させないことが保証されます。

tx-ring-limit コマンドの値の範囲の上限は、実行時に動的に決まります。この制限を表示するには、コマンドラインで **tx-ring-limit ?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。

指定した **tx-ring-limit** は、プライオリティの高い低遅延キューとベストエフォート キューの両方に適用されます。

例

次の例は、デフォルトの queue-limit と tx-ring-limit を使用して、インターフェイス「outside」（GigabitEthernet0/1 インターフェイス）にプライオリティ キューを構築します。

```
hostname(config)# priority-queue outside
```

次の例は、queue-limit を 260 パケット、tx-ring-limit を 3 に設定して、インターフェイス「outside」（GigabitEthernet0/1 インターフェイス）にプライオリティ キューを構築します。

```
hostname(config)# priority-queue outside
hostname(config-priority-queue)# queue-limit 260
hostname(config-priority-queue)# tx-ring-limit 3
```

プライオリティ キューイングとポリシング用のサービス ルールの設定

同じポリシー マップ内の異なるクラス マップに対し、プライオリティ キューイングとポリシングを設定できます。有効な QoS 設定については、「QoS 機能の相互作用のしくみ」（P.13-3）を参照してください。

はじめる前に

- プライオリティ トラフィックに対しては、**class-default** クラス マップは使用できません。
- （ASASM）ASASM はポリシングだけをサポートします。
- ポリシングでは、to-the-box トラフィックはサポートされません。
- ポリシングでは、VPN トンネルとの間で送受信されるトラフィックはインターフェイスのポリシングをバイパスします。
- ポリシングでは、トンネル グループ クラス マップを照合する場合、出力ポリシングのみがサポートされます。
- プライオリティ トラフィックの場合は、遅延が問題になるトラフィックだけを指定します。
- ポリシング トラフィックの場合は、他のすべてのトラフィックをポリシングすることも、トラフィックを特定のタイプに制限することもできます。

手順

ステップ 1　プライオリティ キューイングを実行するトラフィックを識別するためのクラス マップを作成します。

class-map *priority_map_name*

例：

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

ステップ 2　クラス マップにトラフィックを指定します。

match *parameter*

例：

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

詳細については、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 3　ポリシングを実行するトラフィックを識別するためのクラス マップを作成します。

class-map *policing_map_name*

例：

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

ステップ 4　クラス マップにトラフィックを指定します。

match *parameter*

例：

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

詳細については、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ヒント　トラフィック照合に ACL を使用する場合、ポリシングは ACL で指定された方向にのみ適用されます。つまり、送信元から宛先に向かうトラフィックがポリシングされ、宛先から送信元に向かうトラフィックはポリシングされません。

ステップ 5　ポリシー マップを追加または編集します。

policy-map *name*

例：

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

ステップ 6　優先されるトラフィック用に作成したクラス マップを指定します。

class *priority_map_name*

例：

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

ステップ 7　クラスのプライオリティ キューイングを設定します。

priority

例：

```
hostname(config-pmap-c)# priority
```

ステップ 8　ポリシングされるトラフィック用に作成したクラス マップを指定します。

class *policing_map_name*

例：

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

ステップ 9　クラスのポリシングを設定します。

police {**output** | **input**} *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**]] [**exceed-action** [**drop** | **transmit**]]

例：

```
hostname(config-pmap-c)# police output 56000 10500
```

次のオプションがあります。

- *conform-burst argument*：適合レート値にスロットリングするまでに、持続したバーストで許可された最大瞬間バイト数を 1000 ～ 512000000 バイトの範囲で指定します。
- **conform-action**：レートが *conform_burst* 値を下回ったときに実行するアクションを設定します。
- *conform-rate*：このトラフィック クラスのレート制限を 8000 ～ 2000000000 ビット/秒の範囲で設定します。
- **drop**：パケットをドロップします。
- **exceed-action**：レートが *conform-rate* 値～ *conform-burst* 値の範囲にあるときに実行するアクションを設定します。
- **input**：入力方向のトラフィック フローのポリシングをイネーブルにします。
- **output**：出力方向のトラフィック フローのポリシングをイネーブルにします。
- **transmit**：パケットを送信します。

ステップ 10　1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global オプションはポリシー 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。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。

QoS のモニタ

QoS ポリシーの統計情報

トラフィック ポリシングの QoS 統計情報を表示するには、**show service-policy police** コマンドを使用します。

```
hostname# show service-policy police

Global policy:
    Service-policy: global_fw_policy

Interface outside:
    Service-policy: qos
        Class-map: browse
            police Interface outside:
                cir 56000 bps, bc 10500 bytes
                conformed 10065 packets, 12621510 bytes; actions: transmit
                exceeded 499 packets, 625146 bytes; actions: drop
                conformed 5600 bps, exceed 5016 bps
        Class-map: cmap2
            police Interface outside:
                cir 200000 bps, bc 37500 bytes
                conformed 17179 packets, 20614800 bytes; actions: transmit
                exceeded 617 packets, 770718 bytes; actions: drop
                conformed 198785 bps, exceed 2303 bps
```

QoS プライオリティの統計情報

priority コマンドを実装するサービス ポリシーの統計情報を表示するには、**show service-policy priority** コマンドを使用します。

```
hostname# show service-policy priority
Global policy:
    Service-policy: global_fw_policy
Interface outside:
    Service-policy: qos
        Class-map: TG1-voice
            Priority:
                Interface outside: aggregate drop 0, aggregate transmit 9383
```

「Aggregate drop」は、このインターフェイスでの合計ドロップ数を示しています。「aggregate transmit」は、このインターフェイスで送信されたパケットの合計数を示しています。

QoS プライオリティ キューの統計情報

インターフェイスのプライオリティ キュー統計情報を表示するには、**show priority-queue statistics** コマンドを使用します。ベストエフォート（BE）キューと低遅延キュー（LLQ）の両方の統計情報が表示されます。次の例に、test という名前のインターフェイスに対する **show priority-queue statistics** コマンドの使用方法を示します。

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type         = BE
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0

Queue Type         = LLQ
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0
hostname#
```

この統計情報レポートの内容は次のとおりです。

- 「Packets Dropped」は、このキューでドロップされたパケットの合計数を示します。
- 「Packets Transmit」は、このキューで送信されたパケットの合計数を示します。
- 「Packets Enqueued」は、このキューでキューイングされたパケットの合計数を示します。
- 「Current Q Length」は、このキューの現在の深さを示します。
- 「Max Q Length」は、このキューで発生した最大の深さを示します。

プライオリティ キューイングとポリシングの設定例

次の項では、プライオリティ キューイングとポリシングを設定する例を示します。

VPN トラフィックのクラス マップの例

次の例で、**class-map** コマンドは tcp_traffic という ACL を使用して、すべての非トンネル TCP トラフィックを分類します。

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic
```

次の例では、より限定的な一致基準を使用して、特定のセキュリティ関連のトンネル グループにトラフィックを分類します。これらの特定の一致基準では、トラフィックが特定のトンネルに分類されるために、最初の一致特性としてトンネルグループ（この例では、すでに定義されている Tunnel-Group-1）に一致する必要があります。次に、別の照合行でトラフィックを分類できます（IP DiffServ コード ポイント、緊急転送）。

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef
```

次の例では、**class-map** コマンドはトンネル トラフィックと非トンネル トラフィックの両方をトラフィック タイプに従って分類します。

```
hostname(config)# access-list tunneled extended permit ip 10.10.34.0 255.255.255.0
192.168.10.0 255.255.255.0
hostname(config)# access-list non-tunneled extended permit tcp any any
hostname(config)# tunnel-group tunnel-grp1 type IPsec_L2L

hostname(config)# class-map browse
hostname(config-cmap)# description "This class-map matches all non-tunneled tcp traffic."
hostname(config-cmap)# match access-list non-tunneled

hostname(config-cmap)# class-map TG1-voice
hostname(config-cmap)# description "This class-map matches all dscp ef traffic for
tunnel-grp 1."
hostname(config-cmap)# match dscp ef
hostname(config-cmap)# match tunnel-group tunnel-grp1

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# description "This class-map matches all best-effort traffic for
tunnel-grp1."
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address
```

次の例は、クラス トラフィックがトンネルとして指定されておらず、トンネルを*通過する*場合に、トンネル内のトラフィックをポリシングする方法を示します。この例では、192.168.10.10 がリモート トンネルのプライベート側のホスト マシンのアドレスで、ACL の名前は「host-over-l2l」です。クラスマップ（名前は「host-specific」）を作成すると、LAN-to-LAN 接続によるトンネルのポリシングの前に、「host-specific」クラスをポリシングできます。この例では、トンネルの前で「host-specific」トラフィックのレートが制限され、次にトンネルのレートが制限されます。

```
hostname(config)# access-list host-over-l2l extended permit ip any host 192.168.10.10
hostname(config)# class-map host-specific
hostname(config-cmap)# match access-list host-over-l2l
```

プライオリティとポリシングの例

次の例は、前の項で作成したコンフィギュレーションで構築されています。前の例と同様に、tcp_traffic と TG1-voice という 2 つのクラスマップがあります。

```
hostname(config)# class-map TG1-best-effort
hostname(config-cmap)# match tunnel-group Tunnel-Group-1
hostname(config-cmap)# match flow ip destination-address
```

第 3 のクラス マップを追加することで、次のように、トンネルおよび非トンネル QoS ポリシーを定義する基本が提供されます。トンネルおよび非トンネル トラフィックに対する単純な QoS ポリシーが作成され、クラス TG1-voice のパケットが低遅延キューに割り当てられ、tcp_traffic および TG1-best-effort フローにレート制限が設定されます。

この例では、tcp_traffic クラスのトラフィックの最大レートは 56,000 ビット/秒で、最大バースト サイズは 10,500 バイト/秒です。TC1-BestEffort クラスの最大レートは 200,000 ビット/秒で、最大バーストは 37,500 バイト/秒です。TC1-voice クラスのトラフィックは、プライオリティ クラスに属しているため、最大速度またはバースト レートでポリシングされません。

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic

hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address

hostname(config)# policy-map qos
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# police output 56000 10500

hostname(config-pmap-c)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# class TG1-best-effort
hostname(config-pmap-c)# police output 200000 37500

hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)# police output 1000000 37500

hostname(config-pmap-c)# service-policy qos global
```

QoS の履歴

機能名	プラットフォームリリース	説明
プライオリティ キューイングとポリシング	7.0(1)	QoS プライオリティ キューイングとポリシングが導入されました。 **priority-queue**、**queue-limit**、**tx-ring-limit**、**priority**、**police**、**show priority-queue statistics**、**show service-policy police**、**show service-policy priority**、**show running-config priority-queue**、**clear configure priority-queue** の各コマンドが導入されました。
シェーピングおよび階層型プライオリティ キューイング	7.2(4)/8.0(4)	QoS シェーピングおよび階層型プライオリティ キューイングが導入されました。 **shape**、**show service-policy shape** の各コマンドが導入されました。
ASA 5585-X での 10 ギガビット イーサネットによる標準プライオリティ キューのサポート	8.2(3)/8.4(1)	ASA 5585-X の 10 ギガビット イーサネット インターフェイスでの標準プライオリティ キューのサポートが追加されました。

接続のトラブルシューティングおよびリソース

この章では、ASA のトラブルシューティング方法について説明します。

コンフィギュレーションのテスト

この項では、シングル モード ASAまたは各セキュリティ コンテキストの接続性のテスト方法、ASA インターフェイスを ping する方法、およびあるインターフェイスにあるホストが他のインターフェイスのホストに ping できるようにする方法について説明します。

ping メッセージおよびデバッグ メッセージはトラブルシューティング時に限りイネーブルにしてください。ASA のテストが終了したら、「テスト設定のディセーブル化」（P.14-6）の手順に従ってください。

ICMP デバッグ メッセージと Syslog メッセージのイネーブル化

デバッグ メッセージと syslog メッセージは、ping が成功しない理由をトラブルシューティングするのに役立ちます。ASA では、ASA インターフェイスへの ping に対する ICMP デバッグ メッセージだけが表示されます。ASA を経由する他のホストへの ping に対する ICMP デバッグ メッセージは表示されません。

デバッグ メッセージと syslog メッセージをイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	**debug icmp trace** **例：** `hostname(config)# debug icmp trace`	ASA インターフェイスへの ping の ICMP パケット情報を表示します。
ステップ 2	**logging monitor debug** **例：** `hostname(config)# logging monitor debug`	Telnet セッションまたは SSH セッションに送信する syslog メッセージを設定します。 **（注）** あるいは、**logging buffer debug** コマンドを使用してログ メッセージをバッファに送信してから、**show logging** コマンドを使用してそれらを表示することもできます。
ステップ 3	**terminal monitor** **例：** `hostname(config)# terminal monitor`	Telnet セッションまたは SSH セッションに syslog メッセージを送信します。
ステップ 4	**logging on** **例：** `hostname(config)# logging on`	syslog メッセージの生成をイネーブルにします。

例

次に、外部ホスト（209.165.201.2）から ASA の外部インターフェイス（209.165.201.1）への ping が成功した例を示します。

```
hostname(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

この出力では、ICMP パケット長（32 バイト）、ICMP パケット識別子（1）、および ICMP シーケンス番号（ICMP シーケンス番号は 0 から始まり、要求が送信されるたびに増分されます）が示されています。

ASA のインターフェイスへの ping の実行

ASA インターフェイスが起動して動作しているかどうか、および ASA と接続ルータが正しく動作しているかどうかをテストするには、ASA インターフェイスを ping します。

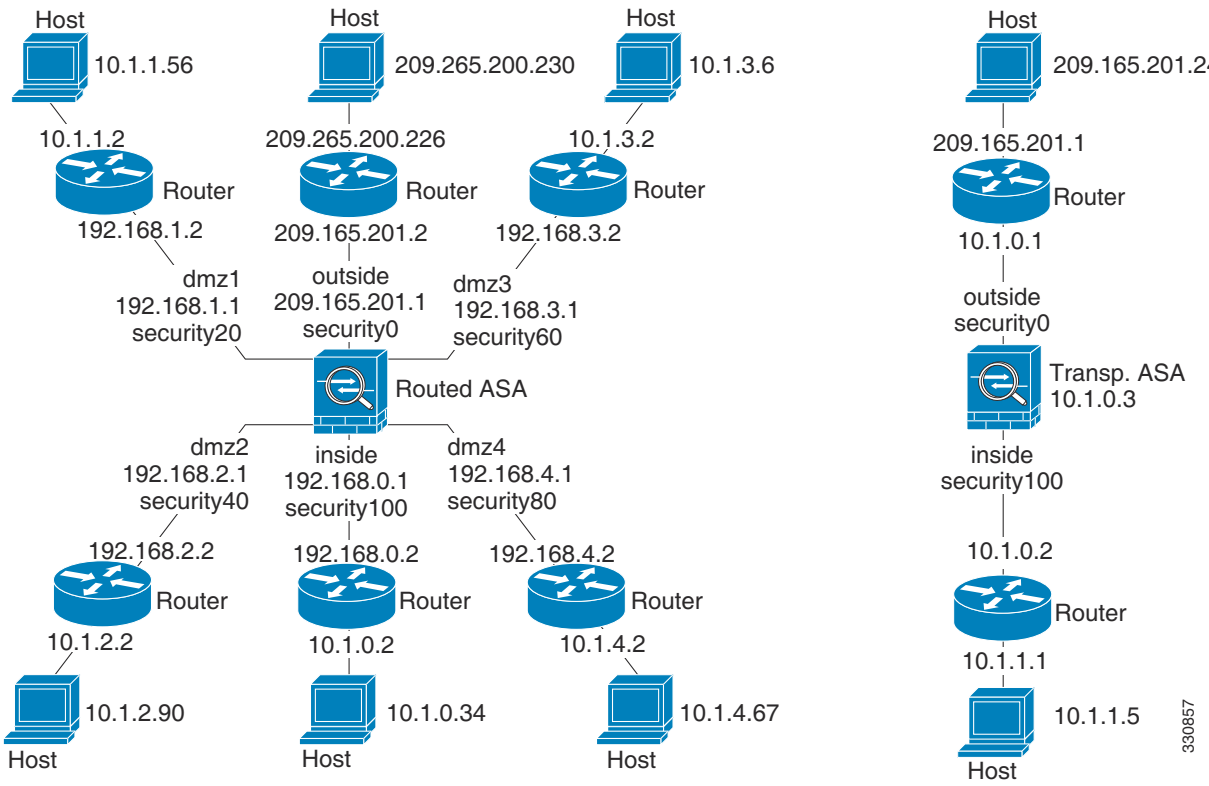
ASA インターフェイスを ping するには、次の手順を実行します。

ステップ 1　インターフェイス名、セキュリティ レベル、および IP アドレスを示すシングル モードの ASA またはセキュリティ コンテキストの図を作成します。

（注）　この手順では IP アドレスを使用しますが、**ping** コマンドでは、DNS 名および **name** コマンドを使用してローカル IP アドレスに割り当てられた名前もサポートされます。

図には、直接接続されたすべてのルータ、および ASA を ping するルータの反対側にあるホストも含める必要があります。この情報はこの手順と「トラフィックの ASA の通過」（P.14-5）の手順で使用します（図 14-1 を参照）。

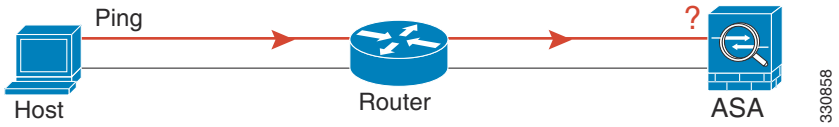
図 14-1　インターフェイス、ルータ、およびホストを含むネットワーク図



ステップ 2　直接接続されたルータから各ASA インターフェイスを ping します。トランスペアレント モードでは、管理 IP アドレスを ping します。このテストは、ASA インターフェイスがアクティブであること、およびインターフェイス コンフィギュレーションが正しいことを確認します。

ASA インターフェイスがアクティブではない場合、インターフェイス コンフィギュレーションが正しくない場合、または ASA とルータの間でスイッチがダウンしている場合、ping は失敗する可能性があります（図 14-2を参照）。この場合は、パケットが ASA に到達しないので、デバッグ メッセージや syslog メッセージは表示されません。

図 14-2　ASA のインターフェイスへの ping の失敗

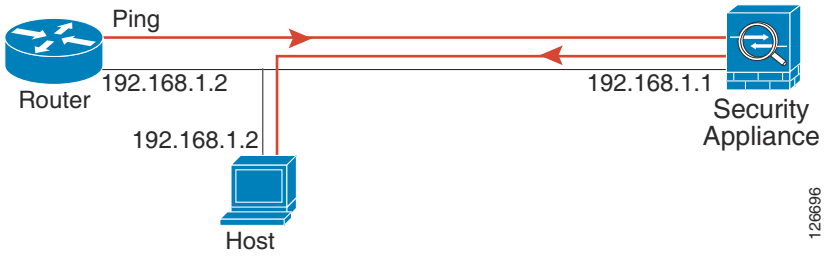


ping が ASA に到達し、応答があると、次のようなデバッグ メッセージが表示されます。

```
ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
```

ping 応答がルータに戻されない場合は、スイッチ ループまたは冗長 IP アドレスが存在する可能性があります（図 14-3 を参照）。

図 14-3　IP アドレッシングの問題による ping の失敗



ステップ 3　リモート ホストから各 ASA インターフェイスを ping します。トランスペアレント モードでは、管理 IP アドレスを ping します。このテストは、直接接続されたルータがホストと ASA の間でパケットをルーティングできるかどうか、および ASA がパケットを正確にルーティングしてホストに戻せるかどうかを確認します。

中間ルータを通ってホストに戻るルートが ASA にない場合、ping は失敗する可能性があります（図 14-4 を参照）。この場合は、デバッグ メッセージは ping が成功したことを示しますが、ルーティングの失敗を示す syslog メッセージ 110001 が表示されます。

図 14-4　ASA の戻りルート未設定による ping の失敗

トラフィックの ASA の通過

ASA インターフェイスを正常に ping した後で、トラフィックが ASA を正常に通過できることを確認します。デフォルトでは、セキュリティの高いインターフェイスからセキュリティの低いインターフェイスへの ping を実行できます。リターン トラフィックを通過させるように ICMP インスペクションをイネーブルにすることだけが必要です。高位から低位に ping するには、トラフィックを許可する ACL を適用する必要があります。NAT を使用する場合は、このテストを行うと NAT が正しく動作していることがわかります。

ホストまたはルータから発信元インターフェイスを介して別のインターフェイス上の別のホストまたはルータに ping します。確認が必要なすべてのインターフェイス ペアに対して、このステップを繰り返します。

ping が成功すると、ルーテッド モードのアドレス変換（305009 または 305011）と ICMP 接続が確立されたこと（302020）を確認する syslog メッセージが表示されます。**show xlate** コマンドまたは **show conns** コマンドを入力してこの情報を表示することもできます。

NAT が正しく設定されていないことが原因で、ping に失敗することもあります。この場合、NAT が失敗したことを示す syslog メッセージが表示されます（305005 または 305006）。外部ホストから内部ホストに ping し、スタティック変換がない場合は、次の syslog メッセージが表示されます。

```
%ASA-3-106010: deny inbound icmp.
```

（注）　ASA によって ICMP デバッグ メッセージが表示されるのは、ASA インターフェイスへの ping に対してのみであり、ASA 経由の他のホストへの ping に対しては表示されません。

図 14-5　ASA のアドレス変換の問題による ping の失敗

手順の詳細

	コマンド	目的
ステップ 1	`policy-map global_policy`	デフォルト グローバル ポリシーを編集し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 2	`class inspection_default`	デフォルトのクラス マップを編集します。これには、標準のプロトコルとポートのアプリケーション トラフィックが一致します。ICMP の場合は、このクラスには、すべての ICMP トラフィックが一致します。
ステップ 3	`inspect icmp`	ICMP インスペクション エンジンをイネーブルにします。ICMP 応答が発信元ホストに戻されるようになります。

ステップ 4	（任意、低セキュリティ インターフェイスの場合） **access-list ICMPACL extended permit icmp any any**	発信元ホストから ICMP トラフィックを許可する ACL を追加します。
ステップ 5	**access-group ICMPACL in interface outside**	ACL を外部インターフェイスに割り当てます。「outside」を実際のインターフェイス名で置き換えます（これとは異なる場合）。高位から低位への ICMP トラフィックを許可するインターフェイスごとに、このコマンドを繰り返します。 **（注）** セキュリティが最低ではないインターフェイスにこの ACL を適用すると、ICMP トラフィックだけが許可されます。つまり、高位から低位への暗黙的な許可が削除されます。たとえば、DMZ インターフェイス（レベル 50）から内部インターフェイス（レベル 100）に ping できるようにするには、この ACL を適用する必要があります。ただし、この時点では、DMZ から外部（レベル 0）へのトラフィックは ICMP トラフィックのみに制限されます。適用前は、暗黙的な許可によってすべてのトラフィックが許可されていました。ping のテストの後は、必ずこの ACL をインターフェイスから削除してください。特に、暗黙的な許可を復元したいインターフェイスです（**no access-list ICMPACL**）。

テスト設定のディセーブル化

テストの完了後、ICMP の ASA への送信および通過を許可し、デバッグ メッセージを表示するテスト コンフィギュレーションをディセーブルにします。このコンフィギュレーションをそのままにしておくと、深刻なセキュリティ リスクが生じる可能性があります。また、デバッグ メッセージを表示すると、ASA のパフォーマンスが低下します。

テスト コンフィギュレーションをディセーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	**no debug icmp trace**	ICMP デバッグ メッセージをディセーブルにします。
ステップ 2	**no logging on**	ロギングをディセーブルにします。
ステップ 3	**no access-list ICMPACL**	ICMPACL ACL を削除し、関連する **access-group** コマンドを削除します。
ステップ 4	**policy-map global_policy** ** class inspection_default** ** no inspect icmp**	（任意）ICMP インスペクション エンジンをディセーブルにします。

トレースルートによるパケット ルーティングの決定

パケットのルートは、トレースルート機能を使用してトレースできます。この機能には、**traceroute** コマンドでアクセスできます。トレースルートは、無効なポート上の宛先に UDP パケットを送信することで機能します。ポートが有効ではないため、宛先までの間にあるルータから ICMP Time Exceeded メッセージが返され、ASA にエラーが報告されます。

パケット トレーサによるパケットの追跡

パケット トレーサ ツールは、パケット スニフィングとネットワーク障害箇所特定のためのパケット追跡を実現するとともに、パケットに関する詳細情報と ASA によるパケットの処理方法を示します。コンフィギュレーション コマンドがパケット ドロップの原因ではない場合は、パケット トレーサ ツールを実行すると、その原因に関する情報が読みやすい形式で表示されます。

パケット トレーサ ツールでは次のことができます。

- ASA を通過するパケットの寿命をトレースして、パケットが正しく動作しているかどうかを確認する。
- ネットワーク内にドロップするすべてのパケットをデバッグする。
- コンフィギュレーションが意図したとおりに機能しているかを確認する。
- パケットに適用可能なすべてのルール、およびルールが追加される原因となった CLI コマンドを表示する。
- データ パス内でのパケット変化を時系列で表示する。
- データ パスにトレーサ パケットを挿入する。
- ユーザ アイデンティティおよび FQDN に基づいて IPv4 アドレスまたは IPv6 アドレスを検索する。
- 特定のセッションが許可または拒否された原因をデバッグする。
- どのセキュリティ グループ タグ（SGT）の値が使用されているか（つまり、パケットの SGT、IP-SGT Manager、またはインターフェイスに対して設定されている **policy static sgt** コマンドのいずれから取得したものか）を特定する。
- 適用されているセキュリティ グループ ベースのセキュリティ ポリシーを特定する。

パケットを追跡するには、次のコマンドを入力します。

コマンド	目的
packet-tracer input [*ifc_name*] [**icmp** [**inline-tag** *tag*] [*sip* | **user** *username* | **security-group** [**name** *name* | **tag** *tag*]| **fqdn** *fqdn-string*] *type code ident* [*dip* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*]] | [**tcp** [**inline-tag** *tag*] [*sip* | **user** *username* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] *sport* [*dip* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] *dport*] | [**udp** [**inline-tag** *tag*] [*sip* | **user** *username* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] *sport* [*dip* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] *dport*] | [**rawip** [**inline-tag** *tag*] [*sip* | **user** *username* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] [*dip* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] | **security-group** [**name** *name* | **tag** *tag*] [**detailed**] [**xml**] **例：** `hostname# packet-tracer input inside tcp 10.2.25.3 www 209.165.202.158 aol detailed`	パケットに関する詳細情報と ASA によるパケットの処理方法を示します。詳細情報を出力し、内部ホスト 10.2.25.3 から外部ホスト 209.165.202.158 にパケット トレーシングをイネーブルにする例を示します。

プロセスごとの CPU 使用率のモニタリング

CPU で実行されているプロセスをモニタできます。特定のプロセスで使用される CPU の使用率に関する情報を取得できます。CPU 使用率の統計情報は降順で並べられ、使用率の最も高いプロセスが先頭に表示されます。また、プロセスごとの CPU に対する負荷に関する情報（記録時間の 5 秒前、1 分前、および 5 分前の情報）も含まれています。この情報は 5 秒おきに自動的に更新され、リアルタイムの統計情報が表示されます。

show process cpu-usage sorted コマンドを使用すると、設定済みコンテキストで消費されるプロセス関連の CPU 負荷の内訳がわかります。

PART 5

高度なネットワーク保護

CHAPTER 15

ASA および Cisco Cloud Web Security

Cisco クラウド Web セキュリティ では、Software as a Service（SaaS）による Web セキュリティおよび Web フィルタリング サービスが提供されます。ネットワークで ASA を使用している企業は、追加ハードウェアをインストールせずにクラウド Web セキュリティ サービスを使用できます。

ASA でクラウド Web セキュリティがイネーブルになっている場合、ASA は、選択された HTTP および HTTPS トラフィックをクラウド Web セキュリティ プロキシ サーバに透過的にリダイレクトします。クラウド Web セキュリティ プロキシ サーバは、コンテンツをスキャンし、Cisco ScanCenter で設定されたポリシーに基づいてトラフィックに関する警告を許可、ブロック、または送信して、許容範囲での使用を促進し、マルウェアからユーザを保護します。

ASA は、任意でアイデンティティ ファイアウォール（IDFW）および AAA ルールによりユーザを認証および識別できます。ASA は、ユーザ クレデンシャル（ユーザ名またはユーザ グループ、あるいはその両方を含む）を暗号化して、クラウド Web セキュリティにリダイレクトするトラフィックに含めます。クラウド Web セキュリティ サービスは、このユーザ クレデンシャルを使用して、ポリシーとトラフィックを照合します。また、ユーザベースのレポーティングでもこのクレデンシャルを使用します。ASA は、ユーザ認証を行わずに（オプションの）デフォルトのユーザ名またはグループ、あるいはその両方を指定できます。ただし、クラウド Web セキュリティ サービスがポリシーを適用するために、ユーザ名とグループは必要ありません。

サービス ポリシー ルールを作成するときに、クラウド Web セキュリティに送信するトラフィックをカスタマイズできます。また、サービス ポリシー ルールに一致する Web トラフィックのサブセットが最初に要求された Web サーバに代わりに直接移動し、クラウド Web セキュリティにスキャンされないように、「ホワイトリスト」を設定できます。

プライマリおよびバックアップ クラウド Web セキュリティ プロキシ サーバを設定できます。ASA は各サーバを定期的にポーリングして、可用性を確認します。

（注） この機能は「ScanSafe」とも呼ばれていますので、ScanSafe という名前が表示されるコマンドがあります。

Cisco クラウド Web セキュリティについて

クラウド Web セキュリティへの Web トラフィックのリダイレクト

エンド ユーザが HTTP または HTTPS 要求を送信すると、ASA はその要求を受信し、オプションでユーザやグループの情報を取得します。トラフィックがクラウド Web セキュリティの ASA サービス ポリシー ルールと一致した場合、ASA は要求をクラウド Web セキュリティ プロキシ サーバにリダイレクトします。ASA は、プロキシ サーバへの接続のリダイレクトによって、エンド ユーザとクラウド Web セキュリティ プロキシ サーバの間の仲介役として機能します。ASA は、クライアント要求の宛先 IP アドレスおよびポートを変更し、クラウド Web セキュリティに固有の HTTP ヘッダーを追加して、クラウド Web セキュリティ プロキシ サーバに変更された要求を送信します。クラウド Web セキュリティ HTTP ヘッダーには、ユーザ名、ユーザ グループなど、さまざまな種類の情報が含まれています（使用可能な場合）。

ユーザ認証およびクラウド Web セキュリティ

ユーザ アイデンティティは、クラウド Web セキュリティでポリシーを適用するために使用できます。また、ユーザ アイデンティティは、クラウド Web セキュリティ レポーティングにも役立ちます。クラウド Web セキュリティを使用するには、ユーザ アイデンティティは必要はありません。クラウド Web セキュリティ ポリシーのトラフィックを識別する他の方法があります。

ASA は、ユーザのアイデンティティを決定したり、デフォルト アイデンティティを提供したりする次の方式をサポートします。

- AAA ルール：ASA が AAA ルールを使用してユーザ認証を実行すると、ユーザ名が AAA サーバまたはローカル データベースから取得されます。AAA ルールによるアイデンティティには、グループ情報が含まれていません。設定されている場合は、デフォルトのグループが使用されます。AAA ルールの設定については、従来の機能ガイドを参照してください。
- IDFW：ASA が Active Directory（AD）で IDFW を使用すると、アクセス ルールなどの機能またはサービス ポリシーで ACL を使用するか、ユーザ アイデンティティ モニタを設定してユーザ アイデンティティ情報を直接ダウンロードして、ユーザやグループをアクティブ化したときに、AD エージェントからユーザ名およびグループが取得されます。

  IDFW の設定方法については、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。
- デフォルトのユーザ名とグループ：ASA は、ユーザ認証を使用せずに、クラウド Web セキュリティ サービス ポリシー ルールと一致するすべてのユーザのオプションのデフォルトのユーザ名やグループを使用します。

認証キー

各 ASA は、クラウド Web セキュリティから取得した認証キーを使用する必要があります。認証キーを使用して、クラウド Web セキュリティは、Web 要求に関連付けられた会社を識別し、ASA が有効なカスタマーに関連付けられていることを確認できます。

ASA では、2 つの認証キー（企業キーおよびグループ キー）のいずれか 1 つを使用できます。

- 「企業認証キー」（P.15-3）
- 「グループ認証キー」（P.15-3）

企業認証キー

企業認証キーは、企業内の複数の ASA で使用できます。このキーは、単に ASA のクラウド Web セキュリティ サービスをイネーブルにします。管理者は ScanCenter（https://scancenter.scansafe.com/portal/admin/login.jsp）でこのキーを生成します。後で使用するためにこのキーを電子メールで送信できます。ScanCenter では、後でこのキーを検索できません。ScanCenter には、最後の 4 桁だけが表示されます。詳細については、クラウド Web セキュリティのマニュアルを参照してください。マニュアルは、http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html から入手できます。

グループ認証キー

グループ認証キーは 2 つの機能を実行する各 ASA に固有の特別なキーです。

- 1 つの ASA のクラウド Web セキュリティ サービスをイネーブルにします。
- ASA からのすべてのトラフィックが識別されるため、ASA ごとに ScanCenter ポリシーを作成できます。

ポリシーにグループ認証キーを使用する方法については、「ScanCenter ポリシー」（P.15-4）を参照してください。

管理者は ScanCenter（https://scancenter.scansafe.com/portal/admin/login.jsp）でこのキーを生成します。後で使用するためにこのキーを電子メールで送信できます。ScanCenter では、後でこのキーを検索できません。ScanCenter には、最後の 4 桁だけが表示されます。詳細については、クラウド Web セキュリティのマニュアルを参照してください。マニュアルは、http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html から入手できます。

ScanCenter ポリシー

ScanCenter では、トラフィックは、ルールに一致するまで順にルールに照合されます。その後、クラウド Web セキュリティがルールの設定済みのアクションを適用します。ユーザ トラフィックはグループの関連付け（*ディレクトリ グループ*または*カスタム グループ*）に基づいて ScanCenter ポリシー ルールと照合できます。

- 「ディレクトリ グループ」（P.15-4）
- 「カスタム グループ」（P.15-4）
- 「グループおよび認証キーの相互運用の仕組み」（P.15-5）

ディレクトリ グループ

ディレクトリ グループはトラフィックが属するグループを定義します。グループが存在する場合、グループは、クライアント要求の HTTP ヘッダーに含まれています。ASA は、IDFW を設定すると HTTP ヘッダーにグループを含めます。IDFW を使用しない場合は、クラウド Web セキュリティ インスペクションの ASA ルールに一致するトラフィックのデフォルト グループを設定できます。

ディレクトリ グループを設定する場合、グループ名を正確に入力する必要があります。

- IDFW グループ名は次の形式で送信されます。

  *domain-name**group-name*

  ASA が IDFW グループ名を学習すると、ASA での形式は *domain-name**group-name* となります。ただし、一般的な ScanCenter 表記に準拠させるため、ASA はバックスラッシュ（\）を 1 つだけ使用するように名前を変更します。

- デフォルト グループ名は次の形式で送信されます。

  [*domain*\]*group-name*

  ASA では、オプションのドメイン名を 2 つのバックスラッシュ（\\）が続くように設定する必要があります。ただし、一般的な ScanCenter 表記に準拠させるため、ASA はバックスラッシュ（\）を 1 つだけ使用するように名前を変更します。たとえば、「Cisco\\Boulder1」と指定すると、ASA は、グループ名をクラウド Web セキュリティに送信するときに、バックスラッシュ（\）を 1 つのみ使用する「Cisco\Boulder1」に変更します。

カスタム グループ

カスタム グループは、次の 1 つ以上の基準を使用して定義されます。

- ScanCenter グループ認証キー：カスタム グループのグループ認証キーを生成できます。その後、ASA を設定するときにこのグループ キーを識別すると、ASA からのすべてのトラフィックがグループ キーでタグ付けされます。
- 送信元 IP アドレス：カスタム グループの送信元 IP アドレスを特定できます。ASA サービス ポリシーが送信元 IP アドレスに基づくため、代わりに ASA で IP アドレスベースのポリシーを設定することもできます。

- ユーザ名：カスタム グループのユーザ名を識別できます。
  - IDFW ユーザ名は次の形式で送信されます。
    domain-name\username
  - RADIUS または TACACS+ を使用する場合、AAA ユーザ名は次の形式で送信されます。
    LOCAL*username*
  - LDAP を使用する場合、AAA ユーザ名は次の形式で送信されます。
    domain-name\username
  - デフォルトのユーザ名は、次の形式で送信されます。
    [*domain-name*\]*username*
    たとえば「ゲスト」としてデフォルトのユーザ名を設定する場合、ASA は「ゲスト」を送信します。「Cisco \ゲスト」としてデフォルトのユーザ名を設定する場合は、ASA は「Cisco \ゲスト」を送信します。

グループおよび認証キーの相互運用の仕組み

カスタム group+group キーが提供する ASA ごとのポリシーが必要ない場合は、企業キーを使用します。すべてのカスタム グループがグループ キーに関連付けられているわけではありません。キーを使用しないカスタム グループを使用して、IP アドレスまたはユーザ名を識別できます。また、キーを使用しないカスタム グループは、ディレクトリ グループを使用するルールとともにポリシー内で使用できます。

ASA ごとのポリシーが必要であり、グループ キーを使用している場合でも、ディレクトリ グループおよびキーを使用しないカスタム グループによって提供される照合機能を使用できます。この場合、グループ メンバーシップ、IP アドレス、またはユーザ名に基づいていくつかの例外を除いて ASA ベースのポリシーが必要になる場合があります。たとえば、すべての ASA 間で America\Management グループのユーザを除外する場合は、次の手順を実行します。

1. America\Management 用のディレクトリ グループを追加します。
2. このグループに対する免除ルールを追加します。
3. 免除ルールの後に各カスタム group+group キーのルールを追加して、ASA ごとのポリシーを適用します。
4. America\Management のユーザからのトラフィックは免除ルールに一致し、その他すべてのトラフィックは発信元の ASA のルールに一致します。

キー、グループ、およびポリシー ルールの組み合わせが可能です。

クラウド Web セキュリティのアクション

設定されたポリシーの適用後、クラウド Web セキュリティは、ユーザ要求をブロック、許可、またはユーザ要求に関する警告を送信します。

- 許可：クラウド Web セキュリティは、クライアント要求を許可する場合、最初の要求先サーバにアクセスし、データを取得します。サーバ応答が ASA に転送され、ここからユーザに転送されます。
- ブロック：クラウド Web セキュリティは、クライアント要求をブロックする場合、アクセスがブロックされたことをユーザに通知します。HTTP 302「Moved Temporarily」応答が、クライアント アプリケーションをクラウド Web セキュリティ プロキシ サーバでホストされている Web ページに送信され、ブロック エラー メッセージが表示されます。ASA はクライアントに 302 応答を転送します。

- 警告：サイトにアクセプタブル ユース ポリシー違反があることをクラウド Web セキュリティ プロキシ サーバが決定すると、サイトに関する警告ページが表示されます。警告を挿入し、接続要求をドロップすることも、警告をクリックし、要求されたサイトに進むこともできます。

ASA がプライマリまたはバックアップ クラウド Web セキュリティ プロキシ サーバに到達できない場合の、ASA による Web トラフィックの処理方法を選択できます。これにより、すべての Web トラフィックがブロックされたり、許可されたりする可能性があります。デフォルトでは、Web トラフィックをブロックします。

ホワイトリストを使用したスキャンのバイパス

AAA ルールまたは IDFW を使用する場合、その他の場合にはサービス ポリシー ルールに一致する特定のユーザまたはグループからの Web トラフィックがスキャンのためクラウド Web セキュリティ プロキシ サーバにリダイレクトされないように ASA を設定できます。クラウド Web セキュリティ スキャンをバイパスすると、ASA はプロキシ サーバに接続せず、最初に要求された Web サーバからコンテンツを直接取得します。Web サーバから応答を受け取ると、データをクライアントに送信します。このプロセスはトラフィックの「ホワイトリスト」といいます。

ACL を使用してクラウド Web セキュリティに送信するトラフィックのクラスを設定すると、ユーザまたはグループに基づいてトラフィックを免除する同じ結果を得ることができますが、ホワイトリストを使用した方がより簡単です。ホワイトリスト機能は、ユーザおよびグループだけに基づき、IP アドレスには基づかないことに注意してください。

IPv4 および IPv6 のサポート

クラウド Web セキュリティは、現在 IPv4 アドレスだけをサポートしています。IPv6 を内部的に使用する場合は、クラウド Web セキュリティに送信する必要がある IPv6 フローに対して NAT 64 を実行する必要があります。

次の表に、クラウド Web セキュリティ リダイレクションでサポートされるクラス マップ トラフィックを示します。

クラス マップ トラフィック	クラウド Web セキュリティ インスペクション
IPv4 から IPv4	サポートあり
IPv6 から IPv4（NAT64 を使用）	サポートあり
IPv4 から IPv6	未サポート
IPv6 から IPv6	未サポート

プライマリ プロキシ サーバからバックアップ プロキシ サーバへのフェールオーバー

Cisco クラウド Web セキュリティ サービスに登録すると、プライマリ クラウド Web セキュリティ プロキシ サーバとバックアップ プロキシ サーバが割り当てられます。

クライアントがプライマリ サーバに到達できない場合、ASA は可用性を判定するためにタワーのポーリングを開始します（クライアントのアクティビティが存在しない場合、ASA は 15 秒ごとにポーリングします）。設定された回数だけ再試行してもプロキシ サーバが使用できない場合（デフォルトは 5 回。この設定は設定可能）、サーバは到達不能として宣言され、バックアップ プロキシ サーバがアクティブになります。

クライアントまたは ASA が、再試行回数に到達する前に少なくとも 2 回連続してサーバに到達できる場合、ポーリングは停止し、タワーはアクセス可能であると判定されます。

バックアップ サーバへのフェールオーバー後、ASA はプライマリ サーバをポーリングし続けます。プライマリ サーバが到達可能になると、ASA はプライマリ サーバの使用に戻ります。

Cisco クラウド Web セキュリティのライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

クラウド Web セキュリティ側では、Cisco クラウド Web セキュリティ ライセンスを購入し、ASA が処理するユーザの数を特定する必要があります。その後、ScanCenter にログインし、認証キーを生成します。

クラウド Web セキュリティの前提条件

（任意）ユーザ認証の前提条件

クラウド Web セキュリティにユーザ アイデンティティ情報を送信するには、ASA で次のいずれかを設定します。

- AAA ルール（ユーザ名のみ）：従来の機能ガイドを参照してください。
- IDFW（ユーザ名およびグループ）：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。

（任意）完全修飾ドメイン名の前提条件

サービス ポリシー ルールまたはクラウド Web セキュリティ サーバに対して ACL で FQDN を使用する場合は、一般的な操作のコンフィギュレーション ガイドに従って ASA の DNS サーバを設定する必要があります。

ガイドラインと制限事項

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

マルチ コンテキスト モードでは、サーバ設定はシステム内だけで使用でき、サービス ポリシー ルールの設定はセキュリティ コンテキスト内だけで使用できます。

各コンテキストには、必要に応じて独自の認証キーを設定できます。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

IPv6 のガイドライン

IPv6 はサポートされません。「IPv4 および IPv6 のサポート」（P.15-6）を参照してください。

その他のガイドライン

- クラウド Web セキュリティは、ASA クラスタリングではサポートされません。
- クライアントレス SSL VPN はクラウド Web セキュリティではサポートされません。クラウド Web セキュリティの ASA サービス ポリシーからクライアントレス SSL VPN トラフィックを免除してください。
- クラウド Web セキュリティ プロキシ サーバへのインターフェイスがダウンすると、**show scansafe server** コマンドは、約 15 ～ 25 分間、両方のサーバを示します。この状態が発生する原因は、ポーリング メカニズムがアクティブな接続に基づいていること、また、そのインターフェイスがダウンしており、ゼロ接続を示し、ポーリング時間が最も長い方法が使用されることなどです。
- クラウド Web セキュリティは、ASA CX モジュールではサポートされません。同じトラフィックに対して ASA CX アクションおよびクラウド Web セキュリティ インスペクションの両方を設定した場合、ASA は ASA CX アクションのみを実行します。
- クラウド Web セキュリティ インスペクションは同じトラフィックの HTTP インスペクションと互換性があります。HTTP インスペクションは、デフォルト グローバル ポリシーの一部としてデフォルトでイネーブルになっています。
- クラウド Web セキュリティは、別の接続に対して同じ送信元ポートおよび IP アドレスを使用できる可能性がある拡張 PAT またはアプリケーションではサポートされません。たとえば、2 つの異なる接続（別個のサーバへの接続）が拡張 PAT を使用する場合、これらの接続は別個の宛先によって区別されているため、ASA は、両方の接続変換に同じ送信元 IP および送信元ポートを再利用する可能性があります。ASA がこれらの接続をクラウド Web セキュリティ サーバにリダイレクトすると、宛先がクラウド Web セキュリティ サーバの IP アドレスおよびポート（デフォルトは 8080）に置き換えられます。その結果、接続は両方とも、同じフロー（同じ送信元 IP/ポートおよび宛先 IP/ポート）に属しているように見え、リターン トラフィックが適切に変換解除されません。
- この **match default-inspection-traffic** コマンドには、クラウド Web セキュリティ インスペクションのデフォルト ポートは含まれません（80 および 443）。

デフォルト設定

デフォルトでは、Cisco クラウド Web セキュリティはイネーブルになりません。

Cisco クラウド Web セキュリティの設定

クラウド Web セキュリティ プロキシ サーバとの通信の設定

ガイドライン

公開キーは ASA ソフトウェアに組み込まれているため、設定する必要がありません。

手順の詳細

	コマンド	目的
ステップ 1	**scansafe general-options** **例：** hostname(config)# scansafe general-options	scansafe 汎用オプション コンフィギュレーション モードを開始します。
ステップ 2	**server primary** {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*] **例：** hostname(cfg-scansafe)# server primary ip 192.168.43.10	プライマリ クラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。 デフォルトでは、クラウド Web セキュリティ プロキシ サーバは HTTP と HTTPS の両方のトラフィックにポート 8080 を使用します。指示されている場合以外は、この値を変更しないでください。
ステップ 3	**server backup** {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*] **例：** hostname(cfg-scansafe)# server backup fqdn server.example.com	（任意）バックアップ クラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。 デフォルトでは、クラウド Web セキュリティ プロキシ サーバは HTTP と HTTPS の両方のトラフィックにポート 8080 を使用します。指示されている場合以外は、この値を変更しないでください。

	コマンド	目的
ステップ 4	**retry-count** *value* **例：** hostname(cfg-scansafe)# retry-count 2	（任意）サーバが到達不能であると判定する前に、クラウド Web セキュリティ プロキシ サーバに対するポーリングに連続して失敗した回数を示す値を入力します。ポーリングは、30 秒ごとに実行されます。有効な値は 2 ～ 100 で、デフォルトは 5 です。 「プライマリ プロキシ サーバからバックアップ プロキシ サーバへのフェールオーバー」（P.15-7）を参照してください。
ステップ 5	**license** *hex_key* **例：** hostname(cfg-scansafe)# ライセンス F12A588FE5A0A4AE86C10D222FC658F3	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。認証キーは 16 バイトの 16 進数です。 「認証キー」（P.15-3）を参照してください。

例

次に、プライマリ サーバとバックアップ サーバを設定する例を示します。

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

（マルチ コンテキスト モード）セキュリティ コンテキストごとのクラウド Web セキュリティの許可

マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可する必要があります。詳細については、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。

（注） 管理コンテキストおよび特定のコンテキスト両方の Scansafe タワーに対応するルートを設定する必要があります。これは Scansafe タワーがアクティブ/アクティブ フェールオーバーのシナリオで到達不能にならないことを保障します。

次に、デフォルトのライセンスを使用してコンテキスト 1 でクラウド Web セキュリティをイネーブルにし、ライセンス キーの上書きを使用してコンテキスト 2 でクラウド Web セキュリティをイネーブルにする設定の例を示します。

```
! System Context
!
scansafe general-options
server primary ip 180.24.0.62 port 8080
retry-count 5
license 366C1D3F5CE67D33D3E9ACEC265261E5
!
context one
 allocate-interface GigabitEthernet0/0.1
 allocate-interface GigabitEthernet0/1.1
 allocate-interface GigabitEthernet0/3.1
```

```
 scansafe
 config-url disk0:/one_ctx.cfg
!
context two
 allocate-interface GigabitEthernet0/0.2
 allocate-interface GigabitEthernet0/1.2
 allocate-interface GigabitEthernet0/3.2
 scansafe license 366C1D3F5CE67D33D3E9ACEC26789534
 config-url disk0:/two_ctx.cfg
!
```

クラウド Web セキュリティにトラフィックを送信するサービス ポリシーの方法

サービス ポリシー ルールの詳細については、第 1 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」を参照してください。

前提条件

（任意）ホワイトリストを使用して一部のトラフィックをクラウド Web セキュリティへの送信から免除する必要がある場合は、サービス ポリシー ルールでホワイトリストを参照できるように、最初に「（任意）ホワイトリストに記載されたトラフィックを設定します」（P.15-16）に従ってホワイトリストを作成します。

手順の詳細

	コマンド	目的
ステップ 1	**policy-map type inspect scansafe** *name1* **例：** `hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1`	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。クラウド Web セキュリティに送信するトラフィックのクラスごとにインスペクション ポリシー マップが必要です。 *policy_map_name* 引数の長さは、最大 40 文字です。 ポリシーマップ コンフィギュレーション モードを開始します。

ステップ 2	`parameters`
	
	例：
	`hostname(config-pmap)# parameters`
		パラメータを使用すると、プロトコルおよびデフォルト ユーザまたはグループを設定できます。パラメータ コンフィギュレーション モードを開始します。

ステップ 3	**{http | https}** **例：** `hostname(config-pmap-p)# http`	このインスペクション ポリシー マップには、**http** または **https** のいずれか 1 つのサービス タイプのみを指定できます。

	コマンド	目的
ステップ 4	（任意） **default** {**[user** *username*] [**group** *groupname*]} **例：** hostname(config-pmap-p)# default group default_group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合にデフォルトのユーザやグループが HTTP ヘッダーに含まれることを指定します。
ステップ 5	（任意。ホワイトリスト用） **class** *whitelist_name* **例：** hostname(config-pmap-p)# class whitelist1	「（任意）ホワイトリストに記載されたトラフィックを設定します」（P.15-16）で作成したホワイトリスト クラス マップ名を識別します。
ステップ 6	whitelist **例：** hostname(config-pmap-p)# class whitelist1 hostname(config-pmap-c)# whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。
ステップ 7	**policy-map type inspect scansafe** *name2* parameters **default** {**[user** *user*] [**group** *group*]} **class** *whitelist_name2* whitelist **例：** hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2 hostname(config-pmap)# parameters hostname(config-pmap-p)# default group2 default_group2 hostname(config-pmap-p)# class whitelist2 hostname(config-pmap-c)# whitelist	ステップ 1 ～ ステップ 6 を繰り返して、HTTPS トラフィックの各クラス マップを作成します（例）。クラウド Web セキュリティに送信するトラフィックのクラスごとにインスペクション クラス マップを作成できます。必要に応じて、トラフィックの複数のクラスに対してインスペクション クラス マップを再利用できます。

	コマンド	目的
ステップ 8	**access-list** *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} **tcp** [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] *dest_address_argument* [*port_argument*] **例：** hostname(config)# object network cisco1 hostname(config-object-network)# fqdn www.cisco.com hostname(config)# object network cisco2 hostname(config-object-network)# fqdn tools.cisco.com hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80 hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80 hostname(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80	クラウド Web セキュリティに送信するトラフィックのクラスを識別します。1 つまたは複数のアクセス コントロール エントリ（ACE）で構成される ACL を作成します。ACL の設定の詳細については、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。 クラウド Web セキュリティは HTTP および HTTPS トラフィックだけで動作します。各トラフィックのタイプは、ASA によって個別に処理されます。したがって、HTTP のみの ACL および HTTPS のみの ACL を作成する必要があります。ポリシーに必要な数の ACL を作成します。 **許可** ACE は、クラウド Web セキュリティに一致したトラフィックを送信します。**拒否** ACE は、クラウド Web セキュリティに送信されないように、トラフィックをサービス ポリシー ルールから免除します。 ACL を作成する場合は、インターネット宛ての適切なトラフィックを照合し、他のインターネット ネットワーク宛てのトラフィックを照合しないようにする方法を考慮します。たとえば、宛先が DMZ の内部サーバである場合に内部トラフィックがクラウド Web セキュリティに送信されないようにするには、DMZ へのトラフィックを免除する ACL に拒否 ACE を追加します。 FQDN ネットワーク オブジェクトは、特定のサーバへのトラフィックを免除するのに役立つ場合があります。 *user_argument* を使用すると、インラインまたはオブジェクト グループを参照することにより、IDFW のユーザ名またはグループを指定できます。 *security_group_argument* を使用すると、インラインまたはオブジェクト グループを参照することにより、TrustSec セキュリティ グループを指定できます。セキュリティ グループによってクラウド Web セキュリティに送信するトラフィックを照合できますが、ASA はクラウド Web セキュリティの HTTP ヘッダーにセキュリティ グループ情報を送信しないことに注意してください。クラウド Web セキュリティはセキュリティ グループに基づいてポリシーを作成できません。
ステップ 9	**class-map** *name1* **例：** hostname(config)# class-map cws_class1	クラウド Web セキュリティ フィルテリングをイネーブルにするトラフィックを識別するためのクラス マップを作成します。
ステップ 10	**match access-list** *acl1* **例：** hostname(config-cmap)# match access-list SCANSAFE_HTTP	ステップ 8 で作成した ACL を指定します。 このルールには別の照合ステートメントを使用できますが、HTTP または HTTPS のみのトラフィックを識別する最も汎用的なコマンドである **match access-list** コマンドを使用することを推奨します。詳細については、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

	コマンド	目的
ステップ 11	**class-map** *name2* 　**match access-list** *acl2* **例：** hostname(config)# class-map cws_class2 hostname(config-cmap)# match access-list SCANSAFE_HTTPS	（任意）HTTPS トラフィックなどのクラス マップを作成します。このサービス ポリシー ルールに必要な数のクラスを作成できます。
ステップ 12	**policy-map** *name* **例：** hostname(config)# policy-map cws_policy	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ポリシー マップを追加または編集します。デフォルトのグローバル ポリシーのグローバル マップは global_policy と呼ばれます。このポリシーを編集するか、または新しいポリシーを作成できます。各インターフェイスにポリシー マップを 1 つだけ適用するか、またはグローバルに適用できます。
ステップ 13	**class** *name1* **例：** hostname(config-pmap)# class cws_class1	ステップ 9 で作成したクラス マップを識別します。
ステップ 14	**inspect scansafe** *scansafe_policy_name1* [**fail-open** | **fail-close**] **例：** hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。ステップ 1 で作成したインスペクション クラス マップの名前を指定します。 **fail-open** を指定すると、クラウド Web セキュリティ サーバを使用できない場合にトラフィックが ASA を通過できます。 **fail-close** を指定すると、クラウド Web セキュリティ サーバを使用できない場合にすべてのトラフィックがドロップされます。**fail-close** がデフォルトです。
ステップ 15	**class** *name2* 　**inspect scansafe** *scansafe_policy_name2* [**fail-open** | **fail-close**] **例：** hostname(config-pmap)# class cws_class2 hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open	（任意）ステップ 11 で作成した 2 番目のクラス マップを識別し、そのマップに対するクラウド Web セキュリティ インスペクションをイネーブルにします。 必要に応じて複数のクラス マップを設定できます。
ステップ 16	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} **例：** hostname(config)# service-policy cws_policy inside	1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。**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。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。詳細については、「インターフェイス（サービス ポリシー）へのアクションの適用」（P.1-19）を参照してください。

例

次に、2 つのクラス（HTTP に 1 つ、HTTPS に 1 つ）を設定する例を示します。各 ACL は www.cisco.com と tools.cisco.com、DMZ ネットワーク、および HTTP と HTTPS の両方に対するトラフィックを免除します。他のすべてのトラフィックは、複数のホワイトリストに記載されたユーザおよびグループを除き、クラウド Web セキュリティに送信されます。ポリシーは、内部インターフェイスに適用されます。

```
hostname(config)# class-map type inspect scansafe match-any whitelist1
hostname(config-cmap)# match user user1 group cisco
hostname(config-cmap)# match user user2
hostname(config-cmap)# match group group1
hostname(config-cmap)# match user user3 group group3

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap)# parameters
hostname(config-pmap-p)# http
hostname(config-pmap-p)# default group default_group
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2
hostname(config-pmap)# parameters
hostname(config-pmap-p)# https
hostname(config-pmap-p)# default group2 default_group2
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# object network cisco1
hostname(config-object-network)# fqdn www.cisco.com
hostname(config)# object network cisco2
hostname(config-object-network)# fqdn tools.cisco.com
hostname(config)# object network dmz_network
hostname(config-object-network)# subnet 10.1.1.0 255.255.255.0

hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq
80
hostname(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80

hostname(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco1 eq 443
hostname(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco2 eq 443
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq
443
hostname(config)# access-list SCANSAFE_HTTPS extended permit tcp any4 any4 eq 443

hostname(config)# class-map cws_class1
hostname(config-cmap)# match access-list SCANSAFE_HTTP
hostname(config)# class-map cws_class2
hostname(config-cmap)# match access-list SCANSAFE_HTTPS

hostname(config)# policy-map cws_policy
hostname(config-pmap)# class cws_class1
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
hostname(config-pmap)# class cws_class2
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open
hostname(config)# service-policy cws_policy inside
```

（任意）ホワイトリストに記載されたトラフィックを設定します

ユーザ認証を使用する場合は、ユーザ名やグループ名に基づいて一部のトラフィックをクラウド Web セキュリティによるフィルタリングから免除できます。クラウド Web セキュリティ サービス ポリシー ルールを設定する場合は、ホワイトリスト インスペクション クラス マップを参照できます。IDFW および AAA のユーザ クレデンシャルをこの機能とともに使用できます。

サービス ポリシー ルールを設定すると、ユーザまたはグループに基づいてトラフィックを免除する同じ結果を得ることができますが、ホワイトリストを使用した方がより簡単です。ホワイトリスト機能は、ユーザおよびグループだけに基づき、IP アドレスには基づかないことに注意してください。

手順の詳細

	コマンド	目的
ステップ 1	**class-map type inspect scansafe** [**match-all** | **match-any**] *name* **例：** `hostname(config)# class-map type inspect scansafe match-any whitelist1`	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。 *class_map_name* 引数は、最大 40 文字のクラス マップ名です。 **match-all** キーワードはデフォルトです。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。 **match-any** キーワードは、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。 CLI がクラスマップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。
ステップ 2	**match** [**not**] {[**user** *username*] [**group** *groupname*]} **例：** `hostname(config-cmap)# match`	**match** キーワードには、特定のユーザ名またはグループ名が続きます。このキーワードは、ホワイトリストにユーザまたはグループを指定します。 **match not** キーワードはユーザやグループがクラウド Web セキュリティを使用してフィルタリングされる必要があることを指定します。たとえばグループ「cisco」をホワイトリストに記載し、ユーザ「johncrichton」および「aerynsun」からのトラフィックをスキャンする場合、これらのユーザに **match not** を指定できます。このコマンドを繰り返して、必要な数のユーザおよびグループを追加します。

例

次に、HTTP および HTTPS インスペクション ポリシー マップの同じユーザおよびグループをホワイトリストに記載する例を示します。

```
hostname(config)# class-map type inspect scansafe match-any whitelist1
hostname(config-cmap)# match user user1 group cisco
hostname(config-cmap)# match user user2
hostname(config-cmap)# match group group1
hostname(config-cmap)# match user user3 group group3

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap)# parameters
hostname(config-pmap-p)# http
hostname(config-pmap-p)# default group default_group
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2
hostname(config-pmap)# parameters
hostname(config-pmap-p)# https
hostname(config-pmap-p)# default group2 default_group2
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist
```

（任意）ユーザ アイデンティティ モニタを設定します

IDFW を使用する場合、ASA は、アクティブな ACL に含まれるユーザおよびグループの AD サーバからのユーザ アイデンティティ情報のみをダウンロードします。ACL は、アクセス ルール、AAA ルール、サービス ポリシー ルール、またはアクティブと見なされるその他の機能で使用する必要があります。クラウド Web セキュリティでは、そのポリシーがユーザ アイデンティティに基づくことができるため、すべてのユーザに対する完全な IDFW カバレッジを取得するには、アクティブな ACL の一部ではないグループをダウンロードする必要があります。たとえば、ユーザおよびグループとともに ACL を使用するクラウド Web セキュリティ サービス ポリシー ルールを設定して、関連グループをアクティブ化できますが、これは必須ではありません。IP アドレスのみに基づく ACL を使用できます。ユーザ アイデンティティ モニタ機能を使用すると、AD エージェントからグループ情報を直接ダウンロードできます。

制限事項

ASA は、ユーザ アイデンティティ モニタ用に設定されたグループ、アクティブな ACL によってモニタされているグループも含めて 512 以下のグループモニタできます。

手順の詳細

コマンド	目的
user-identity monitor {**user-group** [*domain-name*\\]*group-name* | **object-group-user** *object-group-name*} **例：** `hostname(config)# user-identity monitor user-group CISCO\\Engineering`	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。 • **user-group**：グループ名インラインを指定します。ドメインとグループの間に 2 つのバックスラッシュ（\\）を指定しますが、ASA は、クラウド Web セキュリティへの送信時に、クラウド Web セキュリティの表記規則に準拠するようにバックスラッシュが 1 つのみ含まれるように名前を変更します。 • **object-group-user**：**object-group user** 名を指定します。このグループには、複数のグループを含めることができます。

クラウド Web セキュリティ ポリシーの設定

ASA サービス ポリシー ルールを設定した後は、ScanCenter ポータルを起動して、Web コンテンツ スキャン、フィルタリング、マルウェア保護サービスおよびレポートを設定します。

手順の詳細

https://scancenter.scansafe.com/portal/admin/login.jsp に移動します。

詳細については、『Cisco ScanSafe Cloud Web Security Configuration Guides』を参照してください。

http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html

クラウド Web セキュリティのモニタ

コマンド	目的
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
show scansafe statistics	合計と現在の HTTP 接続を表示します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show service policy inspect scansafe	特定のポリシーによってリダイレクトまたはホワイトリストに記載された接続の数を表示します。
次の URL を参照してください。 http://Whoami.scansafe.net	トラフィックがクラウド Web セキュリティ サーバに移動するかどうかを確認するには、クライアントからこの Web サイトにアクセスします。

show scansafe server コマンドは、クラウド Web セキュリティ プロキシ サーバが到達可能かどうかを示します。

```
hostname# show scansafe server
hostname# Primary: proxy197.scansafe.net (72.37.244.115) (REACHABLE)*
hostname# Backup: proxy137.scansafe.net (80.254.152.99)
```

show scansafe statistics コマンドは、プロキシ サーバにリダイレクトされる接続数、現在リダイレクトされている接続数、ホワイトリストに記載されている接続数などのクラウド Web セキュリティ アクティビティに関する情報を示します。

```
hostname# show scansafe statistics
Current HTTP sessions : 0
Current HTTPS sessions : 0
Total HTTP Sessions : 0
Total HTTPS Sessions : 0
Total Fail HTTP sessions : 0
Total Fail HTTPS sessions : 0
Total Bytes In : 0 Bytes
Total Bytes Out : 0 Bytes
HTTP session Connect Latency in ms(min/max/avg) : 0/0/0
HTTPS session Connect Latency in ms(min/max/avg) : 0/0/0
```

show service policy inspect scansafe コマンドは、特定のポリシーによってリダイレクトまたはホワイトリストに記載された接続数を表示します。

```
hostname(config)# show service-policy inspect scansafe
Global policy:
Service-policy: global_policy
    Class-map: inspection_default
Interface inside:
Service-policy: scansafe-pmap
    Class-map: scansafe-cmap
      Inspect: scansafe p-scansafe fail-open, packet 0, drop 0, reset-drop 0,
v6-fail-close 0
Number of whitelisted connections: 0
Number of connections allowed without scansafe inspection because of "fail-open" config: 0
Number of connections dropped because of "fail-close" config: 0
Number of HTTP connections inspected: 0
Number of HTTPS connections inspected: 0
Number of HTTP connections dropped because of errors: 0
Number of HTTPS connections dropped because of errors: 0
```

Cisco クラウド Web セキュリティの設定例

シングル モードの例

次に、Cisco クラウド Web セキュリティの完全な設定の例を示します。

ACL の設定

通過した HTTP および HTTPS パケットの数を確認できるように、個別の HTTP および HTTPS クラス マップを作成して、トラフィックを分割することを推奨します。

その後、トラブルシューティングする必要がある場合、デバッグ コマンドを実行して、各クラス マップを通過したパケットの数を識別し、HTTP または HTTPS トラフィックをさらに通過させているかを確認できます。

```
hostname(config)# access-list web extended permit tcp any any eq www
hostname(config)# access-list https extended permit tcp any any eq https
```

クラス マップの設定

```
hostname(config)# class-map cmap-http
hostname(config-cmap)# match access-list web

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

インスペクション ポリシー マップの設定

```
hostname(config)# policy-map type inspect scansafe http-pmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# default group httptraffic
hostname(config-pmap-p)# http

hostname(config)# policy-map type inspect scansafe https-pmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# default group httpstraffic
hostname(config-pmap-p)# https
```

ポリシー マップの設定

```
hostname(config)# policy-map pmap-webtraffic
hostname(config-pmap)# class cmap-http
hostname(config-pmap-c)# inspect scansafe http-pmap fail-close

hostname(config-pmap)# class cmap-https
hostname(config-pmap-c)# inspect scansafe https-pmap fail-close
```

サービス ポリシーの設定

```
hostname(config)# service-policy pmap-webtraffic interface inside
```

ASA でのクラウド Web セキュリティの設定

```
hostname(config)# scansafe general-options
hostname(cfg-scansafe)# server primary ip 192.168.115.225 web 8080
hostname(cfg-scansafe)# retry-count 5
hostname(cfg-scansafe)# license 366C1D3F5CE67D33D3E9ACEC265261E5
```

マルチ モードの例

次に、デフォルトのライセンスを使用してコンテキスト 1 でクラウド Web セキュリティをイネーブルにし、認証キーの上書きを使用してコンテキスト 2 でクラウド Web セキュリティをイネーブルにする例を示します。

```
! System Context
!
hostname(config)#scansafe general-options
hostname(cfg-scansafe)#server primary ip 180.24.0.62 port 8080
hostname(cfg-scansafe)#retry-count 5
hostname(cfg-scansafe)#license FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
hostname(cfg-scansafe)#publickey <path to public key>
!
context one
 allocate-interface GigabitEthernet0/0.1
 allocate-interface GigabitEthernet0/1.1
 allocate-interface GigabitEthernet0/3.1
 scansafe
 config-url disk0:/one_ctx.cfg
!
context two
 allocate-interface GigabitEthernet0/0.2
 allocate-interface GigabitEthernet0/1.2
 allocate-interface GigabitEthernet0/3.2
 scansafe license 366C1D3F5CE67D33D3E9ACEC265261E5
!
config-url disk0:/two_ctx.cfg
!
```

ホワイトリストの例

どのアクセス リスト トラフィックをクラウド Web セキュリティに送信する必要があるかを設定します。

```
access-list 101 extended permit tcp any4 any4 eq www
access-list 102 extended permit tcp any4 any4 eq https

class-map web
 match access-list 101
class-map https
 match access-list 102
```

user1 がこのアクセス リストの範囲内であることを確認するホワイト リストを設定して、クラウド Web セキュリティをバイパスするには、次を実行します。

```
class-map type inspect scansafe match-any whiteListCmap
 match user LOCAL\user1
```

クラウド Web セキュリティ ポリシー マップにクラス マップを添付するには、次を実行します。

```
policy-map type inspect scansafe ss
 parameters
  default user user1 group group1
  http
 class whiteListCmap
  whitelist
```

```
policy-map type inspect scansafe ss2
 parameters
  default user user1 group group1
  https
 class whiteListCmap
  whitelist
```

このインスペクション ポリシーを作成したら、サービス グループに割り当てられるポリシー マップに添付します。

```
policy-map pmap
 class web
  inspect scansafe ss fail-close
class https
  inspect scansafe ss2 fail-close
```

次に、ポリシー マップをサービス ポリシーに添付して、グローバルに有効にするか、または ASA インターフェイスごとに有効にします。

```
service-policy pmap interface inside
```

ディレクトリの統合の例

この項では、ディレクトリの統合のさまざまな設定例を示します。

- 「LDAP を使用する Active Directory サーバの設定」（P.15-22）
- 「RADIUS を使用する Active Directory エージェントの設定」（P.15-23）
- 「AD エージェント サーバのクライアントとしての ASA の作成」（P.15-23）
- 「AD エージェントと DC の間のリンクの作成」（P.15-23）
- 「AD エージェントのテスト」（P.15-23）
- 「ASA のアイデンティティ オプションの設定」（P.15-23）
- 「ユーザ アイデンティティ オプションの設定および詳細なレポートのイネーブル化」（P.15-24）
- 「Active Directory グループのモニタリング」（P.15-24）
- 「Active Directory サーバからのアクティブ ユーザ データベース全体のダウンロード」（P.15-24）
- 「AD エージェントからのデータベースのダウンロード」（P.15-24）
- 「アクティブ ユーザのリストの表示」（P.15-24）

LDAP を使用する Active Directory サーバの設定

次に、LDAP を使用して ASA で Active Directory サーバを設定する例を示します。

```
hostname(config)# aaa-server AD protocol ldap
hostname(config-aaa-server-group)# aaa-server AD (inside) host 192.168.116.220
hostname(config-aaa-server-host)# ldap-base-dn DC=ASASCANLAB,DC=local
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# server-type microsoft
hostname(config-aaa-server-host)# server-port 389
hostname(config-aaa-server-host)# ldap-login-dn
cn=administrator,cn=Users,dc=asascanlab,dc=local
hostname(config-aaa-server-host)# ldap-login-password Password1
```

RADIUS を使用する Active Directory エージェントの設定

次に、RADIUS を使用して ASA で Active Directory エージェントを設定する例を示します。

```
hostname(config)# aaa-server adagent protocol radius
hostname(config-aaa-server-group)# ad-agent-mode
hostname(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.116.220
hostname(config-aaa-server-host)# key cisco123
hostname(config-aaa-server-host)# user-identity ad-agent aaa-server adagent
```

AD エージェント サーバのクライアントとしての ASA の作成

次に、Active Directory エージェント サーバのクライアントとして ASA を作成する例を示します。

```
c:\IBF\CLI\adacfg client create -name ASA5520DEVICE -ip 192.168.116.90 -secret cisco123
```

AD エージェントと DC の間のリンクの作成

次に、ログオン/ログオフ イベントをモニタする Active Directory エージェントとすべての DC の間にリンクを作成する例を示します。

```
c:\IBF\CLI\adacfg.exe dc create -name DCSERVER1 -host W2K3DC -domain
W2K3DC.asascanlab.local -user administrator -password Password1
c:\IBF\CLI\adacfg.exe dc list
```

最後のコマンドを実行すると、ステータス「UP」が表示されます。

AD_Agent がログオン/ログオフ イベントをモニタするには、アクティブにモニタされているすべての DC でこれらのイベントがログに記録されていることを確認する必要があります。これを行うには、次を選択します。

[Start] > [Administrative Tools] > [Domain Controller Security Policy]

[Local policies] > [Audit Policy] > [Audit account logon events (success and failure)]

AD エージェントのテスト

次に、ASA と通信できるようにテスト Active Directory エージェントを設定する例を示します。

```
hostname# test aaa-server ad-agent adagent
Server IP Address or name: 192.168.116.220
INFO: Attempting Ad-agent test to IP address <192.168.116.220> (timeout: 12 seconds)
INFO: Ad-agent Successful
```

コマンド「**show user-identity ad-agent**」も参照してください。

ASA のアイデンティティ オプションの設定

次に、ASA でアイデンティティ オプションを設定する例を示します。

```
hostname(config)# user-identity domain ASASCANLAB aaa-server AD
hostname(config)# user-identity default-domain ASASCANLAB
```

ユーザ アイデンティティ オプションの設定および詳細なレポートのイネーブル化

次に、ASA にユーザ クレデンシャルを送信し、プロキシ サーバからの詳細なユーザ レポートをイネーブルにするユーザ アイデンティティ オプションを設定する例を示します。

```
hostname(config)# user-identity inactive-user-timer minutes 60
hostname(config)# user-identity action netbios-response-fail remove-user-ip
hostname(config)# user-identity user-not-found enable
hostname(config)# user-identity action mac-address-mismatch remove-user-ip
hostname(config)# user-identity ad-agent active-user-database full-download
```

複数のドメインを使用する場合は、次のコマンドを入力します。

```
hostname(config)# user-identity domain OTHERDOMAINNAME
```

Active Directory グループのモニタリング

次に、Active Directory グループをモニタするように設定する例を示します。

```
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME1
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME2
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME3
```

注意　完了後に設定を保存するようにしてください。

Active Directory サーバからのアクティブ ユーザ データベース全体のダウンロード

次のコマンドは、ポーリング インポート ユーザ グループ タイマーの満了を待たずに即時に Active Directory サーバを照会して、指定されたインポート ユーザ グループ データベースを更新します。

```
hostname(config)# user-identity update import-user
```

AD エージェントからのデータベースのダウンロード

次に、ユーザ データベースが Active Directory と同期していないと思われる場合に、Active Directory エージェントからのデータベースのダウンロードを手動で開始する例を示します。

```
hostname(config)# user-identity update active-user-database
```

アクティブ ユーザのリストの表示

次に、アクティブなユーザを表示する例を示します。

```
hostname# show user-identity user active list detail
```

アイデンティティ ファイアウォールには、フル ダウンロードおよびオンデマンドの 2 つのダウンロード モードがあります。

- フル ダウンロード：ユーザがネットワークにログインするたびに、IDFW は即時に ASA にユーザ アイデンティティを通知します（ASA 5512-X 以降で推奨）。
- オンデマンド：ユーザがネットワークにログインするたびに、ASA が AD（ADHOC）からユーザ アイデンティティを要求します。

アイデンティティ ファイアウォールを使用したクラウド Web セキュリティの例

次に、ASA でアイデンティティ ファイアウォールを使用するクラウド Web セキュリティを設定する例を示します。

```
hostname# sh run
ASA Version 100.8(24)32
!
hostname QFW-201-QASS
domain-name uk.scansafe.net
enable password liqhNWIOSfzvir2g encrypted
passwd liqhNWIOSfzvir2g encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 192.168.116.90 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 192.168.114.90 255.255.254.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
boot system disk0:/asa100824-32-k8.bin
ftp mode passive
dns server-group DefaultDNS
 domain-name uk.scansafe.net
object network obj0192.168.116.x
 subnet 192.168.116.0 255.255.255.0
access-list 101 extended permit tcp any any eq www
access-list 101 extended permit tcp any any eq https
access-list web extended permit tcp any any eq www
access-list icmp extended permit icmp any any
access-list https extended permit tcp any any eq https
!
scansafe general-options
 server primary ip 192.168.115.225 web 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC26789534f
!
pager lines 24
logging buffered debugging
```

```
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
!
object network obj0192.168.116.x
 nat (inside,outside) dynamic interface
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.114.19 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AD protocol ldap
aaa-server AD (inside) host 192.168.116.220
 server-port 389
 ldap-base-dn DC=ASASCANLAB,DC=local
 ldap-scope subtree
 ldap-login-password *****
 ldap-login-dn cn=administrator,cn=Users,dc=asascanlab,dc=local
 server-type microsoft
aaa-server adagent protocol radius
 ad-agent-mode
aaa-server adagent (inside) host 192.168.116.220
 key *****
user-identity domain ASASCANLAB aaa-server AD
user-identity default-domain ASASCANLAB
user-identity action netbios-response-fail remove-user-ip
user-identity poll-import-user-group-timer hours 1
user-identity ad-agent aaa-server adagent
user-identity user-not-found enable
user-identity monitor user-group ASASCANLAB\\GROUP1
user-identity monitor user-group ASASCANLAB\\GROUPNAME
no snmp-server location
no snmp-server contact
crypto ca trustpool policy
telnet timeout 5
ssh 192.168.0.0 255.255.255.0 inside
ssh 192.168.21.0 255.255.255.0 inside
ssh timeout 30
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map cmap-https
 match access-list https
class-map inspection_default
 match default-inspection-traffic
class-map cmap-http
 match access-list web
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
```

```
policy-map type inspect scansafe ss
 parameters
  default user john group qa
  http
policy-map type inspect scansafe https-pmap
 parameters
  https
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
policy-map type inspect scansafe http-pmap
 parameters
  default group http-scansafe
  http
policy-map pmap-http
 class cmap-http
  inspect scansafe http-pmap fail-open
 class cmap-https
  inspect scansafe https-pmap fail-open
!
service-policy pmap-http global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:667ba936945b370c394806a63548e7a0
: end
QFW-201-QASS#
```

関連資料

関連資料	URL
『Cisco ScanSafe Cloud Web Security Configuration Guides』	http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html

Cisco クラウド Web セキュリティの機能の履歴

表 15-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 15-1　クラウド Web セキュリティの機能の履歴

機能名	プラットフォーム リリース	機能情報
クラウド Web セキュリティ	9.0(1)	この機能が導入されました。 Cisco クラウド Web セキュリティは、Web トラフィックに対するコンテンツ スキャンおよびその他のマルウェア保護サービスを提供します。また、ユーザ アイデンティティに基づいて Web トラフィックのリダイレクトと報告を行うこともできます。 **class-map type inspect scansafe**、**default user group**、**http[s]**（パラメータ）、**inspect scansafe**、**license**、**match user group**、**policy-map type inspect scansafe**、**retry-count**、**scansafe**、**scansafe general-options**、**server {primary | backup}**、**show conn scansafe**、**show scansafe server**、**show scansafe statistics**、**user-identity monitor**、**whitelist** の各コマンドが導入または変更されました。

脅威の検出

この章では、脅威検出の統計情報およびスキャン脅威検出を設定する方法について説明します。

脅威の検出

ASA の脅威検出は、攻撃に対して最前線で防御する機能です。脅威検出は、パケット ドロップの統計を分析し、トラフィック パターンに基づいた「トップ」レポートを蓄積することで、レイヤ 3 と 4 にトラフィックのベースラインを作成します。一方、IPS または次世代 IPS サービスを提供するモジュールは、ASA が許可したトラフィックの攻撃ベクトルをレイヤ 7 まで識別して軽減させますが、すでに ASA がドロップしたトラフィックは認識できません。そのため、脅威検出と IPS を一緒に使用することで、より総合的な脅威に対する防御を可能にします。

脅威検出は次の要素から構成されています。

- さまざまな脅威を収集する複数レベルの統計情報

  脅威検出統計情報は、ASA に対する脅威の管理に役立ちます。たとえば、スキャン脅威検出をイネーブルにすると、統計情報を見ることで脅威を分析できます。次の 2 種類の脅威検出統計情報を設定できます。

  - 基本脅威検出統計情報：システムに対する攻撃アクティビティについての全体的な情報を含みます。基本脅威検出統計情報はデフォルトでイネーブルになっており、パフォーマンスに対する影響はありません。
  - 拡張脅威検出統計情報：オブジェクト レベルでアクティビティを追跡するので、ASA は個別のホスト、ポート、プロトコル、または ACL についてのアクティビティを報告できます。拡張脅威検出統計情報は、収集される統計情報によってはパフォーマンスに大きく影響するので、デフォルトでは ACL の統計情報だけがイネーブルになっています。

- ホストからスキャンが実行されていることを検出するスキャン脅威検出機能 オプションとして、スキャン脅威であることが特定されたホストを排除できます。

基本脅威検出統計情報

ASA は、基本脅威検出統計情報を使用して、次の理由でドロップしたパケットおよびセキュリティ イベントの割合をモニタします。

- ACL による拒否。
- 不正なパケット形式（invalid-ip-header や invalid-tcp-hdr-length など）。
- 接続制限の超過（システム全体のリソース制限とコンフィギュレーションで設定されている制限の両方）。
- DoS 攻撃の検出（無効な SPI、ステートフル ファイアウォール検査の不合格など）。
- 基本ファイアウォール検査に不合格。このオプションは、このリストのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません。
- 疑わしい ICMP パケットの検出。
- アプリケーション インスペクションに不合格のパケット。
- インターフェイスの過負荷。
- スキャン攻撃の検出。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニタします。フル スキャン脅威検出では、このスキャン攻撃レート情報を収集し、ホストを攻撃者として分類して自動的に排除することによって対処します。
- 不完全セッションの検出（TCP SYN 攻撃の検出やデータなし UDP セッション攻撃の検出など）。

ASA は、脅威を検出するとただちにシステム ログ メッセージ（733100）を送信します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト レート間隔は、平均レート間隔の 1/30 または 10 秒のうち、どちらか大きいほうです。ASA は、受信するイベントごとに平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、ASA は、バースト期間におけるレート タイプごとに最大 1 つのメッセージの割合で 2 つの別々のシステム メッセージを送信します。

基本脅威検出は、ドロップや潜在的な脅威があった場合に限りパフォーマンスに影響を与えます。この状況でも、パフォーマンスへの影響は大きくありません。

拡張脅威検出統計情報

拡張脅威検出統計情報は、ホスト、ポート、プロトコル、ACL などの個別のオブジェクトについて、許可されたトラフィック レートとドロップされたトラフィック レートの両方を表示します。

注意　拡張統計情報をイネーブルにすると、イネーブルにする統計情報のタイプに応じて、ASA のパフォーマンスが影響を受けます。**threat-detection statistics host** コマンドは、パフォーマンスに大幅に影響を与えます。トラフィックの負荷が高い場合、このタイプの統計情報は一時的にイネーブルにすることを検討できます。一方、**threat-detection statistics port** コマンドは大きな影響を与えません。

スキャン脅威検出

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、ホストからスキャンが実行されていることを検出します。トラフィック シグニチャに基づく IPS スキャン検出とは異なり、ASA の脅威検出スキャンでは、広範なデータベースが保持され、これに含まれるホスト統計情報をスキャン アクティビティに関する分析に使用できます。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

スキャン脅威レートを超過すると、ASA は syslog メッセージ（733101）を送信し、必要に応じて攻撃者を排除します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト イベント レートは、平均レート間隔の 1/30 または 10 秒のうち、どちらか大きいほうです。スキャン攻撃の一部と見なされるイベントが検出されるたびに、ASA は平均レート制限とバースト レート制限をチェックします。ホストから送信されるトラフィックがどちらかのレートを超えると、そのホストは攻撃者と見なされます。ホストが受信したトラフィックがどちらかのレートを超えると、そのホストはターゲットと見なされます。

次の表に、スキャン脅威検出のデフォルトのレート制限を示します。

表 16-1　　スキャン脅威検出のデフォルトのレート制限

平均レート	バースト レート
直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
直前の 3600 秒間で 5 ドロップ/秒。	直近の 120 秒間で 10 ドロップ/秒。

注意　スキャン脅威検出機能は、ホストおよびサブネットベースのデータ構造を作成し情報を収集する間、ASA のパフォーマンスとメモリに大きく影響することがあります。

脅威検出のガイドライン

セキュリティ コンテキストのガイドライン

高度な脅威統計を除き、脅威検出はシングル モードのみでサポートされます。マルチ モードでは、TCP 代行受信の統計情報が唯一サポートされている統計情報です。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

モニタ対象トラフィックのタイプ

- through-the-box トラフィックだけがモニタされます。to-the-box トラフィックは、脅威検出に含まれません。
- ACL によって拒否されたトラフィックは、スキャン脅威検出をトリガーしません。ASA から許可され、フローを作成したトラフィックだけがスキャン脅威検出の影響を受けます。

脅威検出のデフォルト

基本脅威検出統計情報は、デフォルトでイネーブルになっています。

次の表に、デフォルト設定を示します。これらのデフォルト設定すべてを表示するには、**show running-config all threat-detection** コマンドを使用します。

高度な統計情報では、ACL の統計情報はデフォルトでイネーブルになっています。

表 16-2　基本脅威検出のデフォルト設定

	トリガー設定	
パケット ドロップの理由	**平均レート**	**バースト レート**
• DoS 攻撃の検出 • 不正なパケット形式 • 接続制限の超過 • 疑わしい ICMP パケットの検出	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 400 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 120 秒間で 320 ドロップ/秒。
スキャン攻撃の検出	直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
	直前の 3600 秒間で 4 ドロップ/秒。	直近の 120 秒間で 8 ドロップ/秒。
不完全セッションの検出（TCP SYN 攻撃の検出やデータなし UDP セッション攻撃の検出など）（複合）	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 200 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 120 秒間で 160 ドロップ/秒。
ACL による拒否	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 800 ドロップ/秒。
	直前の 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 640 ドロップ/秒。
• 基本ファイアウォール検査に不合格 • アプリケーション インスペクションに不合格のパケット	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 1600 ドロップ/秒。
	直前の 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 1280 ドロップ/秒。
インターフェイスの過負荷	直前の 600 秒間で 2000 ドロップ/秒。	直近の 20 秒間で 8000 ドロップ/秒。
	直前の 3600 秒間で 1600 ドロップ/秒。	直近の 120 秒間で 6400 ドロップ/秒。

脅威検出の設定

基本脅威検出統計情報はデフォルトでイネーブルになっており、ユーザが必要とする唯一の脅威検出サービスである場合があります。さらに脅威検出サービスを実行する場合は、次の手順を使用します。

手順

ステップ 1　「基本脅威検出統計情報の設定」（P.16-5）。

基本脅威検出統計情報には、DoS 攻撃（サービス拒絶攻撃）などの攻撃に関連している可能性があるアクティビティが含まれます。

ステップ 2　「拡張脅威検出統計情報の設定」（P.16-6）。

ステップ 3　「スキャン脅威検出の設定」（P.16-7）。

基本脅威検出統計情報の設定

基本脅威検出統計情報は、デフォルトでイネーブルになっています。ディセーブルにすることも、一度ディセーブルにしたあと再度イネーブルにすることもできます。

手順

ステップ 1　基本脅威検出統計情報をイネーブルにします（ディセーブルになっている場合）。

threat-detection basic-threat

例：

```
hostname(config)# threat-detection basic-threat
```

基本脅威検出は、デフォルトでイネーブルになっています。これをディセーブルにするには **no threat-detection basic-threat** を使用します。

ステップ 2　（任意）各イベント タイプのデフォルト設定を変更します。

threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

例：

```
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

各イベント タイプの説明については、「基本脅威検出統計情報」（P.16-2）を参照してください。

scanning-threat キーワードを指定してこのコマンドを使用すると、スキャン脅威検出機能でもこのコマンドが使用されます。基本脅威検出を設定しない場合でも、**scanning-threat** キーワードを指定してこのコマンドを使用し、スキャン脅威検出でのレート制限を設定できます。

イベント タイプごとに、異なるレート間隔を 3 つまで設定できます。

拡張脅威検出統計情報の設定

広範な統計情報を収集するように ASA を設定することができます。デフォルトでは、ACL の統計情報はイネーブルになっています。他の統計情報をイネーブルにするには、次の手順を実行します。

手順

ステップ 1　（任意）*すべての*統計情報をイネーブルにします。

threat-detection statistics

例：

```
hostname(config)# threat-detection statistics
```

特定の統計情報だけをイネーブルにするには、（この表で示す）各統計情報タイプに対してこのコマンドを入力し、オプションを指定しないでコマンドを入力しないようにします。**threat-detection statistics** を（何もオプションを指定しないで）入力した後、統計情報固有のオプション（たとえば **threat-detection statistics host number-of-rate 2**）を指定してコマンドを入力することで、特定の統計情報をカスタマイズできます。**threat-detection statistics** を（何もオプションを指定しないで）入力した後、特定の統計情報のコマンドを、統計情報固有のオプションを指定しないで入力した場合は、すでにイネーブルになっているので、そのコマンドによる効果は何もありません。

このコマンドの **no** 形式を入力すると、すべての **threat-detection statistics** コマンドが削除されます。これには、デフォルトでイネーブルになる **threat-detection statistics access-list** コマンドも含まれます。

ステップ 2　（任意）ACL の統計情報をイネーブルにします（ディセーブルになっている場合）。

threat-detection statistics access-list

例：

```
hostname(config)# threat-detection statistics access-list
```

ACL の統計情報は、デフォルトでイネーブルになっています。ACL 統計情報は、**show threat-detection top access-list** コマンドを使用した場合にだけ表示されます。このコマンドは、デフォルトでイネーブルになっています。

ステップ 3　（任意）ホスト（**host** キーワード）、TCP および UDP ポート（**port** キーワード）、または非 TCP/UDP IP プロトコル（**protocol キーワード**）の統計情報を設定します。

threat-detection statistics {**host** | **port** | **protocol**} [**number-of-rate** {**1** | **2** | **3**}]

例：

```
hostname(config)# threat-detection statistics host number-of-rate 2

hostname(config)# threat-detection statistics port number-of-rate 2

hostname(config)# threat-detection statistics protocol number-of-rate 3
```

number-of-rate キーワードは、統計情報で保持するレート間隔の数を設定します。デフォルトのレート間隔の数は **1** です。メモリの使用量を低く抑えます。より多くのレート間隔を表示するには、値を **2** または **3** に設定します。たとえば、値を **3** に設定すると、直前の 1 時間、8 時間、および 24 時間のデータが表示されます。このキーワードを **1** に設定した場合（デフォルト）、最も短いレート間隔統計情報だけが保持されます。値を **2** に設定すると、短い方から 2 つの間隔が保持されます。

ホストがアクティブで、スキャン脅威ホスト データベース内に存在する限り、ホスト統計情報は累積されます。ホストは、非アクティブになってから 10 分後にデータベースから削除されます（統計情報もクリアされます）。

ステップ 4　（任意）TCP 代行受信によって代行受信された攻撃の統計情報を設定します（TCP 代行受信をイネーブルにする方法については第 12 章「接続設定」を参照してください）。

threat-detection statistics tcp-intercept [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]

例：

```
hostname(config)# threat-detection statistics tcp-intercept rate-interval 60 burst-rate
800 average-rate 600
```

rate-interval キーワードは、履歴モニタリング ウィンドウのサイズを、1 ～ 1440 分の範囲で設定します。デフォルトは 30 分です。この間隔の間に、ASA は攻撃の数を 30 回サンプリングします。

burst-rate キーワードは、syslog メッセージ生成のしきい値を、25 ～ 2147483647 の範囲で設定します。デフォルトは 1 秒間に 400 です。バースト レートがこれを超えると、syslog メッセージ 733104 が生成されます。

average-rate キーワードは、syslog メッセージ生成の平均レートしきい値を、25 ～ 2147483647 の範囲で設定します。デフォルトは 1 秒間に 200 回です。平均レートがこれを超えると、syslog メッセージ 733105 が生成されます。

（注）　このコマンドは、他の threat-detection コマンドとは異なり、マルチ コンテキスト モードで用意されています。

スキャン脅威検出の設定

攻撃者を識別し、必要に応じて排除するため、スキャン脅威検出を設定できます。

手順

ステップ 1　スキャン脅威検出をイネーブルにします。

threat-detection scanning-threat [**shun** [**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*}]]

例：

```
hostname(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
```

デフォルトでは、ホストが攻撃者であると識別されると、システム ログ メッセージ 733101 が生成されます。このコマンドを複数回入力し、複数の IP アドレスまたはネットワーク オブジェクト グループを特定して遮断対象から除外できます。

ステップ 2　（任意）攻撃元のホストを遮断する期間を設定します。

threat-detection scanning-threat shun duration *seconds*

例：

```
hostname(config)# threat-detection scanning-threat shun duration 2000
```

ステップ 3　（任意）ASA がホストを攻撃者またはターゲットとして識別する場合のデフォルト イベント制限を変更します。

threat-detection rate scanning-threat rate-interval *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

例：

```
hostname(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 10
burst-rate 20

hostname(config)# threat-detection rate scanning-threat rate-interval 2400 average-rate 10
burst-rate 20
```

このコマンドが基本脅威検出コンフィギュレーションの一部としてすでに設定されている場合、それらの設定はスキャン脅威検出機能でも共有され、基本脅威検出とスキャン脅威検出で個別にレートを設定することはできません。このコマンドを使用してレートを設定しない場合は、基本脅威検出機能とスキャン脅威検出機能の両方でデフォルト値が使用されます。個別にコマンドを入力することで、異なるレート間隔を 3 つまで設定できます。

脅威検出のモニタリング

次のトピックでは、脅威検出のモニタリングとトラフィック統計情報を表示する方法を説明します。

- 「基本脅威検出統計情報のモニタリング」（P.16-8）
- 「拡張脅威検出統計情報のモニタリング」（P.16-9）
- 「ホストの脅威検出統計情報の評価」（P.16-11）
- 「遮断されたホスト、攻撃者、ターゲットのモニタリング」（P.16-13）

基本脅威検出統計情報のモニタリング

次のコマンドを使用して、基本脅威検出統計情報を表示します。

show threat-detection rate [**min-display-rate** *min_display_rate*]
[**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** |
icmp-drop | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**]

min-display-rate *min_display_rate* 引数により、毎秒あたりの最小表示レートを超過する統計情報に表示内容を限定します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。

他の引数を使用すると、特定のカテゴリに表示を制限できます。各イベント タイプの説明については、「基本脅威検出統計情報」（P.16-2）を参照してください。

出力には、直前の 10 分と直前の 1 時間の固定された 2 期間における平均レート（イベント数/秒）が表示されます。また、最後に終了したバースト間隔（平均レート間隔の 1/30 または 10 秒のうち、どちらか大きいほう）における現在のバースト レート（イベント数/秒）、レートが超過した回数（トリガーした回数）、およびその期間の合計イベント数も表示されます。

ASA は、各バースト期間の終わりにカウント数を保存します。合計で 30 回分のバースト間隔を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

clear threat-detection rate コマンドを使用して統計情報を消去できます。

次に、**show threat-detection rate** コマンドの出力例を示します。

```
hostname# show threat-detection rate

                      Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:              0              0       0                   16
  1-hour ACL  drop:              0              0       0                  112
  1-hour SYN attck:              5              0       2                21438
  10-min  Scanning:              0              0      29                  193
  1-hour  Scanning:            106              0      10               384776
  1-hour Bad  pkts:             76              0       2               274690
  10-min  Firewall:              0              0       3                   22
  1-hour  Firewall:             76              0       2               274844
  10-min DoS attck:              0              0       0                    6
  1-hour DoS attck:              0              0       0                   42
  10-min Interface:              0              0       0                  204
  1-hour Interface:             88              0       0               318225
```

拡張脅威検出統計情報のモニタリング

ボタンをクリックする拡張脅威検出統計情報をモニタするには、次の表に示すコマンドを使用します。ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

ASA は、各バースト期間の終わりにカウント数を保存します。合計で 30 回分のバースト間隔を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

コマンド	目的
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**] | **tcp-intercept** [**all**] **detail**]]	上位 10 件の統計情報を表示します。オプションを入力しない場合は、カテゴリ全体での上位 10 件の統計情報が表示されます。 **min-display-rate** *min_display_rate* 引数により、毎秒あたりの最小表示レートを超過する統計情報に表示内容を限定します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。 次の行は、オプション キーワードを示します。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top access-list** [**rate-1** | **rate-2** | **rate-3**]	許可 ACE と拒否 ACE の両方を含め、パケットに一致する上位 10 件の ACE を表示するには、**access-list** キーワードを使用します。この表示では許可されたトラフィックと拒否されたトラフィックが区別されません。**threat-detection basic-threat** コマンドを使用して基本脅威検出をイネーブルにする場合は、**show threat-detection rate acl-drop** コマンドを使用して、ACL による拒否を追跡できます。 **rate-1** キーワードを指定すると、表示できる最小固定レート間隔の統計情報が表示され、**rate-2** を指定すると次に大きなレート間隔の統計情報が表示されます。3 つの間隔が定義されている場合には、**rate-3** を指定すると最大レート間隔の統計情報が表示されます。たとえば、ディスプレイに直前の 1 時間、8 時間、および 24 時間の統計情報が表示されるとします。**rate-1** キーワードを設定すると、ASA は 1 時間の統計情報だけを表示します。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top host** [**rate-1** | **rate-2** | **rate-3**]	ホスト統計情報だけを表示するには、**host** キーワードを使用します。**注**：脅威検出アルゴリズムに起因して、フェールオーバー リンクとステート リンクの組み合わせとして使用されるインターフェイスは上位 10 個のホストに表示されることがあります。これは予期された動作であり、表示される IP アドレスは無視できます。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top port-protocol** [**rate-1** | **rate-2** | **rate-3**]	ポートおよびプロトコルの統計情報を表示するには、**port-protocol** キーワードを使用します。**port-protocol** キーワードを指定すると、ポートとプロトコルの両方の統計情報が表示され（表示するには、両方がイネーブルに設定されている必要があります）、TCP/UDP ポートと IP プロトコル タイプを組み合わせた統計情報が表示されます。TCP（プロトコル 6）と UDP（プロトコル 17）は、IP プロトコルの表示には含まれていませんが、TCP ポートと UDP ポートはポートの表示に含まれています。これらのタイプ（ポートまたはプロトコル）の 1 つの統計情報だけをイネーブルにすると、イネーブルにされた統計情報だけが表示されます。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top tcp-intercept** [**all**] **detail**]]	TCP 代行受信の統計情報だけを表示するには、**tcp-intercept** キーワードを使用します。表示には、攻撃を受けて保護された上位 10 サーバが含まれます。**all** キーワードは、トレースされているすべてのサーバの履歴データを表示します。**detail** キーワードは、履歴サンプリング データを表示します。ASA はレート間隔の間に攻撃の数を 30 回サンプリングするので、デフォルトの 30 分間隔では、60 秒ごとに統計情報が収集されます。

コマンド	目的
show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]	すべてのホスト、特定のホスト、または特定のサブネットの統計情報を表示します。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **port** [*start_port*[**-***end_port*]]	すべてのポート、特定のポート、または特定のポート範囲の統計情報を表示します。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | **ah** | **eigrp** | **esp** | **gre** | **icmp** | **icmp6** | **igmp** | **igrp** | **ip** | **ipinip** | **ipsec** | **nos** | **ospf** | **pcp** | **pim** | **pptp** | **snp** | **tcp** | **udp**]	すべての IP プロトコルまたは特定のプロトコルの統計情報を表示します。 *protocol_number* 引数は、0 ～ 255 の整数です。

ホストの脅威検出統計情報の評価

次に、**show threat-detection statistics host** コマンドの出力例を示します。

```
hostname# show threat-detection statistics host

                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:               2938               0       0             10580308
  8-hour Sent byte:                367               0       0             10580308
 24-hour Sent byte:                122               0       0             10580308
  1-hour Sent pkts:                 28               0       0               104043
  8-hour Sent pkts:                  3               0       0               104043
 24-hour Sent pkts:                  1               0       0               104043
  20-min Sent drop:                  9               0       1                10851
  1-hour Sent drop:                  3               0       1                10851
  1-hour Recv byte:               2697               0       0              9712670
  8-hour Recv byte:                337               0       0              9712670
 24-hour Recv byte:                112               0       0              9712670
  1-hour Recv pkts:                 29               0       0               104846
  8-hour Recv pkts:                  3               0       0               104846
 24-hour Recv pkts:                  1               0       0               104846
  20-min Recv drop:                 42               0       3                50567
  1-hour Recv drop:                 14               0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                  0               0       0                  614
  8-hour Sent byte:                  0               0       0                  614
 24-hour Sent byte:                  0               0       0                  614
  1-hour Sent pkts:                  0               0       0                    6
  8-hour Sent pkts:                  0               0       0                    6
 24-hour Sent pkts:                  0               0       0                    6
  20-min Sent drop:                  0               0       0                    4
  1-hour Sent drop:                  0               0       0                    4
  1-hour Recv byte:                  0               0       0                  706
  8-hour Recv byte:                  0               0       0                  706
 24-hour Recv byte:                  0               0       0                  706
  1-hour Recv pkts:                  0               0       0                    7
```

次の表は出力について示しています。

表 16-3　show threat-detection statistics host

フィールド	説明
Host	ホストの IP アドレス。
tot-ses	ホストがデータベースに追加されて以降の、このホストでの合計セッション数。
act-ses	ホストが現在関係しているアクティブなセッションの合計数。
fw-drop	ファイアウォール ドロップの数。ファイアウォール ドロップは、基本脅威検出で追跡されたすべてのファイアウォール関連のパケット ドロップを含む組み合わせレートです。これには、ACL での拒否、不良パケット、接続制限の超過、DoS 攻撃パケット、疑わしい ICMP パケット、TCP SYN 攻撃パケット、およびデータなし UDP 攻撃パケットなどが含まれます。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません。
insp-drop	アプリケーション インスペクションに不合格になったためにドロップされたパケット数。
null-ses	ヌル セッションの数。ヌル セッションは、3 秒間のタイムアウト内に完了しなかった TCP SYN セッション、およびセッション開始の 3 秒後までにサーバからデータが送信されなかった UDP セッションです。
bad-acc	閉じられた状態のホストのポートに対する不正なアクセスの試行回数。ポートがヌル セッションと判断されると（null-ses フィールドの説明を参照）、ホストのポートの状態は HOST_PORT_CLOSE に設定されます。そのホストのポートにアクセスしようとするクライアントはすべて、タイムアウトを待たずにすぐ不正アクセスとして分類されます。
Average(eps)	各間隔における平均レート（イベント数/秒）。 ASA は、各バースト期間の終わりにカウント数を保存します。合計で 30 回分のバースト間隔を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。
Trigger	ドロップされたパケット レートの制限値を超過した回数。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。

表 16-3　show threat-detection statistics host（続き）

フィールド	説明
Total events	各レート間隔におけるイベントの合計数。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASA は、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
20-min、1-hour、8-hour、および 24-hour	これらの固定レート間隔の統計情報。各インターバルごとに、以下を示します。 • [Sent byte]：ホストから正常に送信されたバイト数。 • [Sent pkts]：ホストから正常に送信されたパケット数。 • [Sent drop]：ホストから送信された、スキャン攻撃の一部であったためにドロップされたパケット数。 • [Recv byte]：ホストが受信した正常なバイト数。 • [Recv pkts]：ホストが受信した正常なパケット数。 • [Recv drop]：ホストが受信したパケットの中で、スキャン攻撃の一部であったためにドロップされたパケット数。

遮断されたホスト、攻撃者、ターゲットのモニタリング

遮断されたホスト、攻撃者、ターゲットをモニタおよび管理するには、次のコマンドを使用します。

- **show threat-detection shun**

  現在遮断されているホストを表示します。次に例を示します。

```
hostname# show threat-detection shun
Shunned Host List:
10.1.1.6
192.168.6.7
```

- **clear threat-detection shun** [*ip_address* [*mask*]]

  ホストを回避対象から解除します。IP アドレスを指定しない場合は、すべてのホストが遮断リストからクリアされます。

  たとえば、10.1.1.6 のホストを解除するには、次のコマンドを入力します。

```
hostname# clear threat-detection shun 10.1.1.6
```

- **show threat-detection scanning-threat** [**attacker** | **target**]

  ASA が攻撃者（遮断リストのホストを含む）と判断したホスト、および攻撃のターゲットにされたホストを表示します。オプションを入力しない場合は、攻撃者とターゲットの両方のホストが表示されます。次に例を示します。

```
hostname# show threat-detection scanning-threat attacker
10.1.2.3
10.8.3.6
209.165.200.225
```

脅威検出の例

次の例では、基本脅威検出統計情報を設定し、DoS 攻撃レートの設定を変更しています。すべての拡張脅威検出統計情報はイネーブルであり、ホスト統計情報のレート間隔数は 2 に減らされています。TCP 代行受信のレート間隔もカスタマイズされています。スキャン脅威検出はイネーブルで、10.1.1.0/24 を除くすべてのアドレスを自動遮断します。スキャン脅威レート間隔はカスタマイズされています。

```
threat-detection basic-threat
threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate 100
threat-detection statistics
threat-detection statistics host number-of-rate 2
threat-detection statistics tcp-intercept rate-interval 60 burst-rate 800 average-rate 600
threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0
threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20
threat-detection rate scanning-threat rate-interval 2400 average-rate 10 burst-rate 20
```

脅威検出の履歴

機能名	プラットフォームリリース	説明
基本および拡張脅威検出統計情報、スキャン脅威検出	8.0(2)	基本および拡張脅威検出統計情報、スキャン脅威検出が導入されました。 次のコマンドが導入されました。**threat-detection basic-threat**、**threat-detection rate**、**show threat-detection rate**、**clear threat-detection rate**、**threat-detection statistics**、**show threat-detection statistics**、**threat-detection scanning-threat**、**threat-detection rate scanning-threat**、**show threat-detection scanning-threat**、**show threat-detection shun**、**clear threat-detection shun**。
排除期間	8.0(4)/8.1(2)	排除期間を設定できるようになりました。 **threat-detection scanning-threat shun duration** コマンドが導入されました。
TCP 代行受信の統計情報	8.0(4)/8.1(2)	TCP 代行受信の統計情報が導入されました。 **threat-detection statistics tcp-intercept**、**show threat-detection statistics top tcp-intercept**、**clear threat-detection statistics** コマンドが変更または導入されました。

機能名	プラットフォームリリース	説明
ホスト統計情報レート間隔のカスタマイズ	8.1(2)	統計情報が収集されるレート間隔の数をカスタマイズできるようになりました。デフォルトのレート数は、3 から 1 に変更されました。 **threat-detection statistics host number-of-rates** コマンドが変更されました。
バースト レート間隔が平均レートの 1/30 に変更されました。	8.2(1)	以前のリリースでは、平均レートの 1/60 でした。メモリを最大限に使用するため、サンプリング間隔が平均レートの間に 30 回に減らされました。
ポートおよびプロトコル統計情報レート間隔のカスタマイズ	8.3(1)	統計情報が収集されるレート間隔の数をカスタマイズできるようになりました。デフォルトのレート数は、3 から 1 に変更されました。 **threat-detection statistics port number-of-rates**、**threat-detection statistics protocol number-of-rates** コマンドが変更されました。
メモリ使用率の向上	8.3(1)	脅威検出のメモリ使用率が向上しました。 **show threat-detection memory** コマンドが導入されました。

PART 6

ASA モジュール

ASA FirePOWER（SFR）モジュール

この章では、ASA で実行される ASA FirePOWER モジュールを設定する方法について説明します。

ASA FirePOWER モジュール

ASA FirePOWER モジュールは、次世代 IPS（NGIPS）、アプリケーションの可視性とコントロール（AVC）、URL フィルタリング、高度なマルウェア保護（AMP）などの次世代ファイアウォール サービスを提供します。このモジュールは、シングルまたはマルチ コンテキスト モードとルーテッドまたはトランスペアレント モードで使用できます。

このモジュールは ASA SFR とも呼ばれます。

このモジュールには、初期設定およびトラブルシューティングのための基本的なコマンド ライン インターフェイス（CLI）が用意されていますが、デバイスのセキュリティ ポリシーは、独立したアプリケーションである FireSIGHT 管理センター を使用して設定できます。このアプリケーションは、独立した FireSIGHT 管理センター アプライアンスで、または VMware サーバ上で実行される仮想アプライアンスとしてホストできます（FireSIGHT 管理センター は防御センターとも呼ばれます）。

ASA FirePOWER モジュールを ASA と連携させる方法

ASA FirePOWER モジュールは、ASA と別のアプリケーションを実行します。このモジュールは、ハードウェア モジュール（ASA 5585-X 上）か、ソフトウェア モジュール（5512-X ～ 5555-X）です。ハードウェア モジュールには、独立した管理およびコンソール ポートと、モジュール自体ではなく ASA によって直接使用される追加のデータ インターフェイスがあります。

デバイスは、パッシブ（「モニタ専用」）展開またはインライン展開のいずれかで設定できます。

- パッシブ展開では、トラフィックのコピーがデバイスに送信されますが、ASA には返されません。パッシブ モードでは、デバイスがトラフィックに対して実行したであろう処理を表示し、ネットワークに影響を与えずにトラフィックの内容を評価することができます。
- インライン展開では、実際のトラフィックがデバイスに送信され、デバイスのポリシーがトラフィックに対する処理に影響します。不要なトラフィックがドロップされ、ポリシーによって適用されるその他のアクションが実行された後、トラフィックはさらなる処理と最終的な送信のために ASA に返されます。

次の各セクションでは、これらのモードについて詳しく説明します。

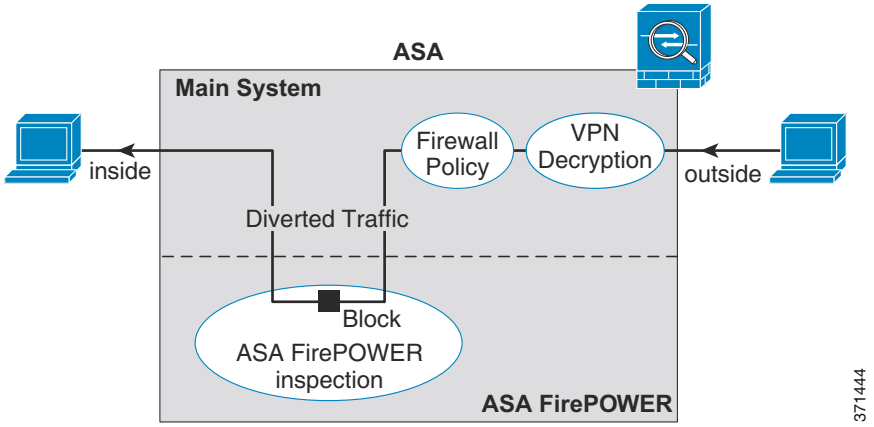
ASA FirePOWER インライン モード

インライン モードでは、トラフィックはファイアウォール検査を通過してから ASA FirePOWER モジュールへ転送されます。ASA で ASA FirePOWER インスペクションのトラフィックを識別する場合、トラフィックは次のように ASA およびモジュールを通過します。

1. トラフィックは ASA に入ります。
2. 着信 VPN トラフィックが復号化されます。
3. ファイアウォール ポリシーが適用されます。
4. トラフィックが ASA FirePOWER モジュールに送信されます。
5. ASA FirePOWER モジュールは、セキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
6. 有効なトラフィックが ASA に返送されます。ASA FirePOWER モジュールは、セキュリティ ポリシーに従ってトラフィックをブロックすることがあり、ブロックされたトラフィックは渡されません。
7. 発信 VPN トラフィックが暗号化されます。
8. トラフィックが ASA から出ます。

次の図に、ASA FirePOWER モジュールをインライン モードで使用する場合のトラフィック フローを示します。この例では、特定のアプリケーションに対して許可されていないトラフィックがモジュールによってブロックされます。それ以外のトラフィックは、ASA を通って転送されます。

図 17-1　ASA での ASA FirePOWER モジュールのトラフィック フロー



（注）　2 つの ASA インターフェイス上でホスト間が接続されており、ASA FirePOWER のサービス ポリシーがインターフェイスの一方のみについて設定されている場合は、これらのホスト間のすべてのトラフィックが ASA FirePOWER モジュールに送信されます。これには、ASA FirePOWER インターフェイス以外からのトラフィックも含まれます（この機能は双方向であるため）。

ASA FirePOWER パッシブ（モニタ専用）モード

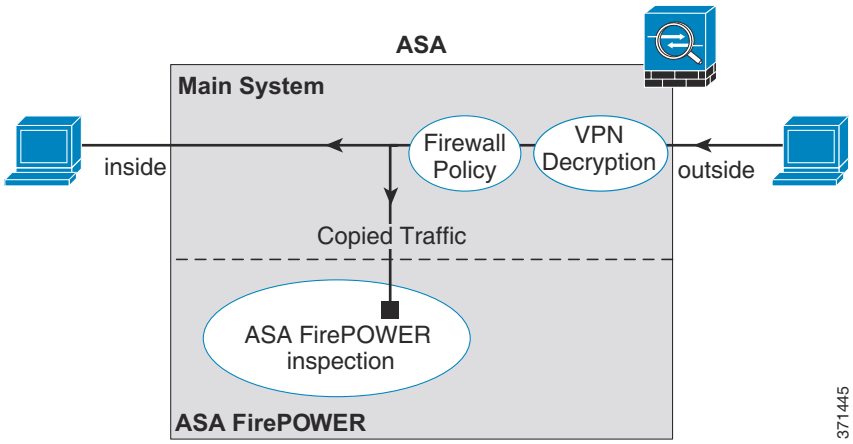
モニタ専用モードのトラフィック フローは、インライン モードのトラフィック フローと同じです。唯一の違いは、ASA FirePOWER モジュールが ASA に戻るトラフィックを通過させないことです。代わりに、モジュールはトラフィックにセキュリティ ポリシーを適用し、インライン モードで動作していた場合に実行したであろう処理をユーザに通知します。たとえば、トラフィックはイベントで「ドロップされていたはず」とマークされる場合があります。この情報をトラフィック分析に使用し、インライン モードが望ましいかどうかを判断するのに役立てることができます。

パッシブ モードを設定するには、モジュールにトラフィックをリダイレクトするサービス ポリシーに monitor-only という指示を追加します。

（注）　ASA 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。マルチ コンテキスト モードで、あるコンテキストについてモニタ専用モードを設定し、それ以外のコンテキストについて通常のインライン モードを設定することはできません。

次の図に、パッシブ モードで動作している場合のトラフィック フローを示します。

図 17-2　ASA FirePOWER パッシブ（モニタ専用）モード



ASA FirePOWER 管理アクセス

ASA FirePOWER モジュールは、初期設定（およびそれ以降のトラブルシューティング）とポリシー管理の 2 つの独立したアクセス レイヤを使用して管理できます。

- 「初期設定」（P.17-4）
- 「ポリシー設定および管理」（P.17-5）

初期設定

初期設定には、ASA FirePOWER モジュールの CLI を使用する必要があります。デフォルトの管理アドレスの詳細については、「ASA FirePOWER のデフォルト」（P.17-7）を参照してください。

CLI にアクセスするには、次の方法を使用します。

- ASA 5585-X
  - ASA FirePOWER コンソール ポート：コンソール ポートは、独立した外部コンソール ポートです。
  - ASA FirePOWER Management 1/0 インターフェイス（SSH を使用）：デフォルトの IP アドレスに接続することも、ASDM を使用して管理 IP アドレスを変更してから SSH を使用して接続することもできます。モジュールの管理インターフェイスは、独立した外部ギガビット イーサネット インターフェイスです。

（注）　**session** コマンドを使用して ASA バックプレーンを介して ASA FirePOWER ハードウェア モジュール CLI にアクセスすることはできません。

- ASA 5512-X ～ ASA 5555-X
  - バックプレーンを経由した ASA セッション：ASA に CLI アクセスが可能な場合は、モジュールにセッション接続し、そのモジュール CLI にアクセスできます。
  - ASA FirePOWER Management 0/0 インターフェイス（SSH を使用）：デフォルトの IP アドレスに接続することも、ASDM を使用して管理 IP アドレスを変更してから SSH を使用して接続することもできます。これらのモデルは、ASA FirePOWER モジュールをソフトウェア モジュールとして実行します。ASA FirePOWER 管理インターフェイスは、Management 0/0 インターフェイスを ASA と共有します。ASA と ASA FirePOWER モジュールのそれぞれに別の MAC アドレスと IP アドレスがサポートされます。ASA FirePOWER IP アドレスの設定は、ASA FirePOWER オペレーティング システム内で（CLI または ASDM を使用して）実行する必要があります。ただし、物理特性（インターフェイスのイネーブル化など）は、ASA 上で設定されます。ASA インターフェイス コンフィギュレーションを削除して（特にインターフェイス名）、このインターフェイスを ASA FirePOWER 専用インターフェイスとすることができます。このインターフェイスは管理専用です。

ポリシー設定および管理

初期設定を実行した後で、FireSIGHT 管理センター を使用して ASA FirePOWER セキュリティ ポリシーを設定します。次に、ASDM または Cisco Security Manager を使用して、ASA FirePOWER モジュールにトラフィックを送信するための ASA ポリシーを設定します。

ASA の機能との互換性

ASA には、多数の高度なアプリケーション インスペクション機能があり、HTTP インスペクションもその一つです。ただし、ASA FirePOWER モジュールには ASA よりも高度な HTTP インスペクション機能があり、その他のアプリケーションについても機能が追加されています。たとえば、アプリケーション使用状況のモニタリングと制御です。

ASA FirePOWER モジュールの機能を最大限に活用するには、ASA FirePOWER モジュールに送信するトラフィックに関する次のガイドラインを参照してください。

- HTTP トラフィックに対して ASA インスペクションを設定しないでください。
- クラウド Web セキュリティ（ScanSafe）インスペクションを設定しないでください。同じトラフィックに対して ASA FirePOWER CX インスペクションおよびクラウド Web セキュリティ インスペクションの両方を設定した場合、ASA は ASA FirePOWER インスペクションのみを実行します。
- ASA 上の他のアプリケーション インスペクションは ASA FirePOWER モジュールと互換性があり、これにはデフォルト インスペクションも含まれます。
- Mobile User Security（MUS）サーバをイネーブルにしないでください。これは、ASA FirePOWER モジュールとの間に互換性がありません。
- フェールオーバーをイネーブルにしている場合、ASA がフェールオーバーすると、既存の ASA FirePOWER フローは新しい ASA に転送されます。新しい ASA の ASA FirePOWER モジュールがその時点からトラフィックのインスペクションを開始します。古いインスペクションの状態は転送されません。

ASA FirePOWER モジュールのライセンス要件

ASA FirePOWER モジュールと FireSIGHT 管理センター には、追加のライセンスが必要です。これらのライセンスは、ASA のコンテキストではなく、モジュール自体にインストールする必要があります。ASA 自体には、追加ライセンスは必要ありません。

詳細については、『*FireSIGHT System User Guide*』または FireSIGHT 管理センター のオンラインヘルプの「Licensing」の章を参照してください。

ASA FirePOWER のガイドライン

フェールオーバーのガイドライン

フェールオーバーを直接サポートしていません。ASA がフェールオーバーすると、既存の ASA FirePOWER フローは新しい ASA に転送されます。新しい ASA の ASA FirePOWER モジュールがその時点からトラフィックのインスペクションを開始します。古いインスペクションの状態は転送されません。

フェールオーバーの動作の一貫性を確保するために、高可用性 ASA ペアの ASA FirePOWER モジュールで一貫性のあるポリシーを維持する必要があります（FireSIGHT 管理センター を使用）。

ASA クラスタリングのガイドライン

このモジュールは、クラスタリングは直接サポートしていませんが、クラスタで使用できます。FireSIGHT 管理センター を使用して、クラスタの ASA FirePOWER モジュールで一貫性のあるポリシーを維持する必要があります。クラスタ内のデバイスに異なる ASA インターフェイス ベースのゾーン定義を使用しないでください。

モデルのガイドライン

- ASA 5585-X（ハードウェア モジュールとして）および 5512-X ～ ASA 5555-X（ソフトウェア モジュールとして）でサポートされています。詳細については、『*Cisco ASA Compatibility Matrix*』を参照してください。

  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

- 5512-X ～ ASA 5555-X の場合は、シスコのソリッド ステート ドライブ（SSD）を実装する必要があります。詳細については、ASA 5500-X のハードウェア ガイドを参照してください。

その他のガイドラインと制限事項

- 「ASA の機能との互換性」（P.17-5）を参照してください。
- ハードウェア モジュールにインストールされているソフトウェアのタイプの変更はできません。つまり、購入した ASA FirePOWER モジュールに、後で別のソフトウェアをインストールすることはできません。
- ASA 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。マルチ コンテキスト モードで、あるコンテキストについてモニタ専用モードを設定し、それ以外のコンテキストについて通常のインライン モードを設定することはできません。

ASA FirePOWER のデフォルト

次の表に、ASA FirePOWER モジュールのデフォルト設定を示します。

表 17-1　ASA FirePOWER のデフォルトのネットワーク パラメータ

パラメータ	デフォルト
管理 IP アドレス	• システム ソフトウェア イメージ：192.168.45.45/24 • ブート イメージ： – ASA 5585-X：Management 1/0 192.168.8.8/24 – ASA 5512-X ～ ASA 5555-X：Management 0/0 192.168.1.2/24
ゲートウェイ	• システム ソフトウェア イメージ：なし • ブート イメージ： – ASA 5585-X：192.168.8.1/24 – ASA 5512-X ～ ASA 5555-X：192.168.1.1/24
SSH またはセッションのユーザ名	admin
パスワード	• システム ソフトウェア イメージ：**Sourcefire** • ブート イメージ：**Admin123**

ASA FirePOWER モジュールの設定

ASA FirePOWER モジュールの設定は、トラフィックを ASA FirePOWER モジュールに送信するための ASA FirePOWER モジュールでの ASA FirePOWER セキュリティ ポリシーの設定、およびその後の ASA の設定を含むプロセスです。ASA FirePOWER モジュールを設定するには、次の手順に従います。

ステップ 1　「ASA FirePOWER 管理インターフェイスの接続」（P.17-8）。ケーブルで ASA FirePOWER 管理インターフェイスに接続します（任意でコンソール インターフェイスにも）。

ステップ 2　「（ASA 5512-X ～ 5555-X）ソフトウェア モジュールのインストールまたはイメージの再作成」（P.17-11）。

ステップ 3　必要に応じて、「ASA FirePOWER 管理 IP アドレスの変更」（P.17-15）。これは最初の SSH アクセスに必要になる場合があります。

ステップ 4　「ASA FirePOWER CLI での基本的な ASA FirePOWER 設定値の設定」（P.17-15）。これは ASA FirePOWER モジュールで行います。

ステップ 5　「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.17-17）。これはデバイスを管理する FireSIGHT 管理センター を指定します。

ステップ 6　「ASA FirePOWER モジュールへのセキュリティ ポリシーの設定」（P.17-18）。

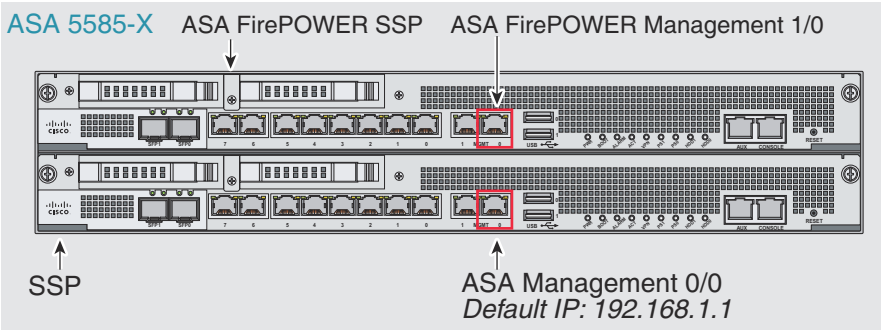
ステップ 7　「ASA FirePOWER モジュールへのトラフィックのリダイレクト」（P.17-18）。

ASA FirePOWER 管理インターフェイスの接続

ASA FirePOWER モジュールへの管理アクセスを提供する以外に、ASA FirePOWER 管理インターフェイスは、HTTP プロキシ サーバまたは DNS サーバおよびインターネットへのアクセスを必要とします。これは、シグニチャ アップデートなどのためです。この項では、推奨されるネットワーク コンフィギュレーションを示します。実際のネットワークでは、異なる可能性があります。

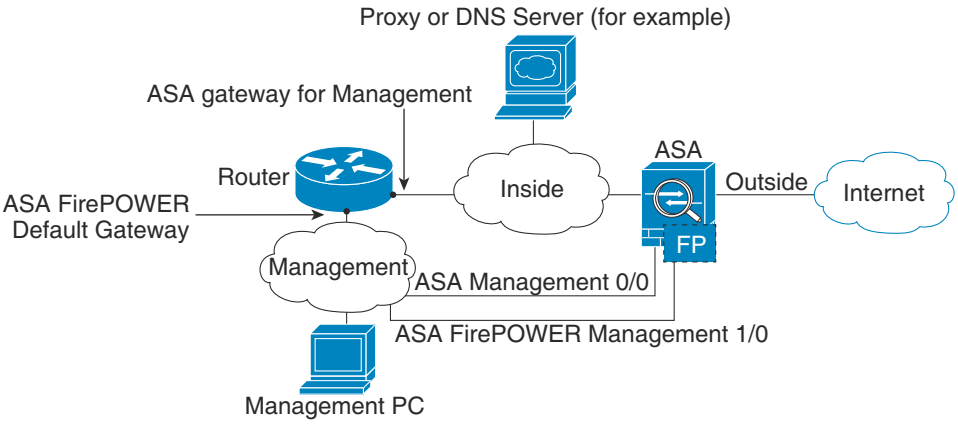
ASA 5585-X（ハードウェア モジュール）

ASA FirePOWER モジュールには、ASA とは別の管理およびコンソール インターフェイスが含まれます。初期設定を行うには、デフォルト IP アドレスを使用して ASA FirePOWER Management 1/0 インターフェイスに SSH で接続できます。デフォルト IP アドレスを使用できない場合は、コンソール ポートを使用するか、ASDM を使用して SSH を使用できるように管理 IP アドレスを変更します（「ASA FirePOWER 管理 IP アドレスの変更」（P.17-15）を参照）。



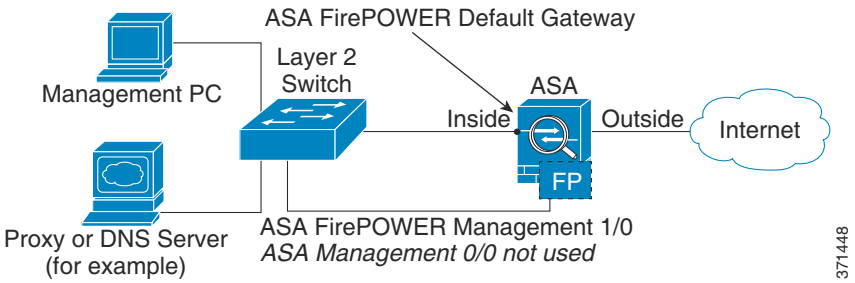
内部ルータがある場合

内部ルータがある場合は、管理ネットワーク（これには ASA Management 0/0 インターフェイスおよび ASA FirePOWER Management 1/0 インターフェイスの両方を含めることができます）と ASA 内部ネットワークとの間でルーティングできます（インターネット アクセス用）。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



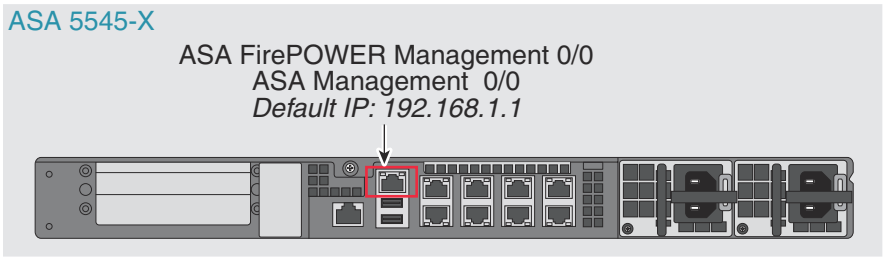
内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません（仮に持つとすれば、内部ルータがネットワーク間のルーティングを行う必要があります）。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA FirePOWER モジュールは ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に ASA FirePOWER Management 1/0 アドレスを設定できます。



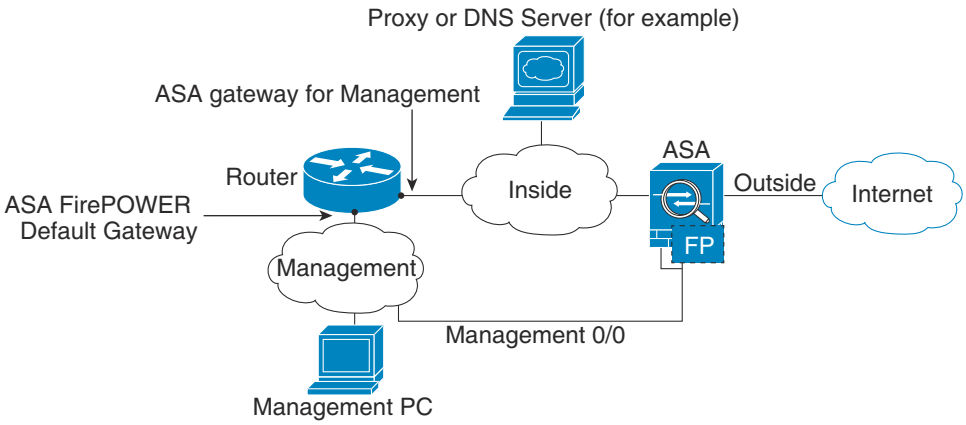
ASA 5512-X ～ ASA 5555-X（ソフトウェア モジュール）

これらのモデルは、ASA FirePOWER モジュールをソフトウェア モジュールとして実行し、ASA FirePOWER 管理インターフェイスは Management 0/0 インターフェイスを ASA と共有します。初期設定を行うには、デフォルト IP アドレスを使用して ASA FirePOWER に SSH で接続できます。デフォルト IP アドレスを使用できない場合は、バックプレーンを経由して ASA FirePOWER にセッション接続するか、ASDM を使用して SSH を使用できるように管理 IP アドレスを変更します。



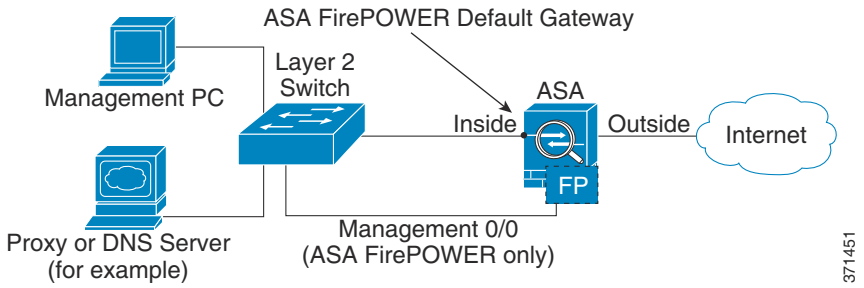
内部ルータがある場合

内部ルータがある場合、Management 0/0 ネットワーク間でルーティングできます。これには、ASA および ASA FirePOWER の両方の管理 IP アドレス、およびインターネット アクセス用の内部ネットワークが含まれます。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA で設定された名前を Management 0/0 インターフェイスから削除した場合も、そのインターフェイスの ASA FirePOWER IP アドレスを設定できます。ASA FirePOWER モジュールは実質的に ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に ASA FirePOWER 管理アドレスを設定できます。



（注）　Management 0/0 に対して ASA で設定された名前を削除する必要があります。この名前が ASA 上で設定されている場合は、ASA FirePOWER のアドレスは ASA と同じネットワーク上にあることが必要になり、その結果、他の ASA インターフェイス上ですでに設定されたネットワークが除外されます。名前が設定されていない場合は、ASA FirePOWER のアドレスが存在するのはどのネットワークでも、たとえば、ASA 内部ネットワークでもかまいません。

（ASA 5512-X ～ 5555-X）ソフトウェア モジュールのインストールまたはイメージの再作成

ASA FirePOWER モジュールとともに ASA を購入した場合、モジュール ソフトウェアおよび必要なソリッド ステート ドライブ（SSD）は事前にインストールされており、すぐに設定できます。既存の ASA に ASA FirePOWER ソフトウェア モジュールを追加する場合、または SSD を交換する必要がある場合は、この手順に従って ASA FirePOWER ブート ソフトウェアをインストールし、SSD を分割して、システム ソフトウェアをインストールする必要があります。

モジュールのイメージを再作成する手順は、最初に ASA FirePOWER モジュールをアンインストールする必要があることを除いてこれと同じです。システムのイメージの再作成は、SSD を交換する場合に行います。

物理的に SSD を取り付ける方法の詳細については、『ASA Hardware Guide』を参照してください。

はじめる前に

- フラッシュ（disk0）の空き領域には、少なくとも、ブート ソフトウェアのサイズに 3 GB を加えた大きさが必要です。
- マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。
- 実行している可能性があるその他のソフトウェア モジュールをシャットダウンする必要があります。デバイスでは、一度に 1 つのソフトウェア モジュールを実行できます。これは ASA CLI から実行する必要があります。たとえば、次のコマンドはIPS モジュール ソフトウェアをシャット ダウンしてアンインストールし、ASA をリロードします。CX モジュールを削除するコマンドは、**ips** の代わりに **cxsc** キーワードを使用することを除いてこのコマンドと同じです。

```
hostname# sw-module module ips shutdown
hostname# sw-module module ips uninstall
hostname# reload
```

（注）　IPS または CX モジュールにトラフィックをリダイレクトするアクティブ サービス ポリシーがある場合、そのポリシーを削除する必要があります。たとえば、ポリシーがグローバル ポリシーの場合、**noservice-policy** *ips_policy* **global** を使用します。ポリシーは、CLI または ASDM を使用して削除できます。

- モジュールのイメージを再作成する場合は、同じシャットダウン/アンインストール コマンドを使用して古いイメージを削除します。たとえば、**sw-module module sfr uninstall** を使用します。
- ASA FirePOWER のブート イメージとシステム ソフトウェア パッケージの両方を Cisco.com から取得します。

手順

ステップ 1　ブート イメージをデバイスにダウンロードします。システム ソフトウェアは転送しないでください。これは後で SSD にダウンロードされます。次の選択肢があります。

- ASDM：まず、ブート イメージをワークステーションにダウンロードするか、FTP、TFTP、HTTP、HTTPS、SMB、または SCP サーバに配置します。次に、ASDM で [Tools] > [File Management] の順に選択し、[Between Local PC and Flash] または [Between Remote Server and Flashnd] のいずれか該当する [File Transfer] コマンドを選択します。ブート ソフトウェアを ASA 上の disk0 に転送します。
- ASA CLI：まず、ブート イメージを TFTP、FTP、HTTP、または HTTPS サーバに配置し、**copy** コマンドを使用してそのブート イメージをフラッシュにダウンロードします。次の例では TFTP を使用しています。<TFTP Server> をお使いのサーバの IP アドレスまたはホスト名に置き換えてください。

```
ciscoasa# copy tftp://<TFTP SERVER>/asasfr-5500x-boot-5.3.1-58.img
disk0:/asasfr-5500x-boot-5.3.1-58.img
```

ステップ 2　ASA FirePOWER 管理インターフェイスからアクセス可能な HTTP、HTTPS、または FTP サーバに、Cisco.com から ASA FirePOWER システム ソフトウェアをダウンロードします。

ステップ 3　次のコマンドを入力して、ASA disk0 で ASA FirePOWER モジュール ブート イメージの場所を設定します。

```
hostname# sw-module module sfr recover configure image disk0:file_path
```

（注）　「ERROR: Another service (cxsc) is running, only one service is allowed to run at any time」というメッセージが表示される場合は、すでに別のソフトウェア モジュールが設定されています。このソフトウェア モジュールをシャットダウンして削除し、上の前提条件セクションの説明に従って新しいモジュールをインストールする必要があります。

例：

```
hostname# sw-module module sfr recover configure image
disk0:asasfr-5500x-boot-5.3.1-58.img
```

ステップ 4　次のコマンドを入力して、ASA FirePOWER ブート イメージをロードします。

```
hostname# sw-module module sfr recover boot
```

ステップ 5　ASA FirePOWER モジュールが起動するまで約 5 分待ってから、現在実行中の ASA FirePOWER ブート イメージへのコンソール セッションを開きます。ログイン プロンプトを表示するには、セッションを開いた後に Enter キーを押さなければならない場合があります。デフォルトのユーザ名は **admin** で、デフォルトのパスワードは **Admin123** です。

```
hostname# session sfr console
Opening console session with module sfr.
Connected to module sfr.Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

ヒント　モジュールのブートが完了していない場合は、**session** コマンドが失敗し、ttyS1 経由で接続できないことに関するメッセージが表示されます。しばらく待ってから再試行してください。

ステップ 6　システム ソフトウェア パッケージをインストールできるように、**setup** コマンドを使用してシステムを設定します。

```
asasfr-boot> setup


                Welcome to SFR Setup
                 [hit Ctrl-C to abort]
               Default values are inside []
```

次の項目を指定するように求められます。主な設定項目は、管理アドレスとゲートウェイ、および DNS 情報です。

- ホスト名：65 文字までの英数字で、スペースは使用できません。ハイフンを使用できます。
- ネットワーク アドレス：スタティック IPv4 または IPv6 アドレスを設定するか、または DHCP （IPv4 の場合）または IPv6 ステートレス自動設定を使用することができます。
- DNS 情報：少なくとも 1 つの DNS サーバを指定する必要があります。ドメイン名と検索ドメインを設定することもできます。
- NTP 情報：システム時刻を設定するために、NTP をイネーブルにして NTP サーバを設定することができます。

ステップ 7　**system install** コマンドを使用してシステム ソフトウェア イメージをインストールします。

system install [**noconfirm**] *url*

確認メッセージに応答したくない場合は、**noconfirm** オプションを指定します。HTTP、HTTPS、または FTP URL を使用してください。ユーザ名とパスワードが必要な場合は、それらを指定するように求められます。

インストールが完了すると、システムが再起動します。アプリケーション コンポーネントのインストールと ASA FirePOWER サービスの起動には 10 分以上かかります（**show module sfr** の出力で、すべてのプロセスがアクティブであると表示される必要があります）。

次に例を示します。

```
asasfr-boot> system install http://asasfr-sys-5.3.1-44.pkg
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA-FirePOWER 5.3.1-44 System Install
        Requires reboot:                Yes

Do you want to continue with upgrade?[y]: y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade.Press 'Enter' to reboot the system.
(Enter キーを押します)
Broadcast message from root (ttyS1) (Mon Feb 17 19:28:38 2014):

The system is going down for reboot NOW!
Console session with module sfr terminated.
```

ステップ 8　ASA FirePOWER モジュールへのセッションを開きます。フル機能のモジュールにログインしようとしているため、別のログイン プロンプトが表示されます。

```
asa3# session sfr
Opening command session with module sfr.
Connected to module sfr.Escape character sequence is 'CTRL-^X'.

Sourcefire ASA5555 v5.3.1 (build 44)
Sourcefire3D login:
```

ステップ 9　ユーザ名 **admin** およびパスワード **Sourcefire** を使用してログインします。

ステップ 10　プロンプトに従ってシステム設定を完了します。

まず、エンド ユーザ ライセンス契約（EULA）を読み、これに同意する必要があります。次に、プロンプトに従って管理者パスワードを変更し、管理アドレスと DNS 設定を設定します。IPv4 と IPv6 の両方の管理アドレスを設定できます。次に例を示します。

```
System initialization in progress.Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <新しいパスワード>
Confirm new password: <パスワードの再入力>
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4?(y/n) [y]: y
Do you want to configure IPv6?(y/n) [n]:
Configure IPv4 via DHCP or manually?(dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.86.118.3
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
10.120.10.14
Enter a comma-separated list of search domains or 'none' [example.net]: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
(システムが自動的に再設定されるまで待機します)

This sensor must be managed by a Defense Center.A unique alphanumeric
registration key is always required.In most cases, to register a sensor
to a Defense Center, you must provide the hostname or the IP address along
with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Defense Center are separated by a NAT device,
you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.
```

ステップ 11　**configure manager add** コマンドを使用して、このデバイスを管理する FireSIGHT 管理センター アプライアンスを指定します。

登録キーを考え出します。このキーは、デバイスをインベントリに追加するときに FireSIGHT 管理センター で使用します。次に、簡単な例を示します。NAT 境界がある場合は、コマンドが異なります。「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.17-17）を参照してください。

```
> configure manager add 10.89.133.202 123456
Manager successfully configured.
```

ステップ 12　上で入力したホスト名またはアドレスを使用し、ブラウザで HTTPS 接続を使用して FireSIGHT 管理センター にログインします。たとえば、https://DC.example.com などです。

[Device Management]（[Devices] > [Device Management]）ページでデバイスを追加します。詳細については、オンライン ヘルプまたは『*FireSIGHT System User Guide*』の「Managing Devices」の章を参照してください。

ヒント　また、FireSIGHT 管理センター で NTP と時刻設定も設定します。時刻同期設定は、[System] > [Local] > [System Policy] ページからローカル ポリシーを編集する場合に使用します。

ASA FirePOWER 管理 IP アドレスの変更

デフォルトの管理 IP アドレスを使用できない場合、ASA から管理 IP アドレスを設定できます。管理 IP アドレスを設定した後は、追加設定を実行するために SSH を使用して ASA FirePOWER モジュールにアクセスできます。

システムの初期設定時に「ASA FirePOWER CLI での基本的な ASA FirePOWER 設定値の設定」（P.17-15）の説明に従って ASA FirePOWER CLI で管理アドレスをすでに設定している場合は、ASA CLI または ASDM で管理アドレスを設定する必要はありません。

（注）　ソフトウェア モジュールの場合、ASA FirePOWER CLI にアクセスして、ASA CLI からのセッション接続によって設定を実行できます。その後、設定の一部として ASA FirePOWER 管理 IP アドレスを設定できます。ハードウェア モジュールの場合は、コンソール ポートを使用して初期設定を完了できます。

ASA で管理 IP アドレスを変更するには、次のいずれかを実行します。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

- CLI で、ASA FirePOWER 管理 IP アドレス、マスク、およびゲートウェイを設定するには、次のコマンドを使用します。ハードウェア モジュールの場合は **1**、ソフトウェア モジュールの場合は **sfr** を使用します。

  ```
  session {1 | sfr} do setup host ip ip_address/mask,gateway_ip
  ```

  たとえば、**session 1 do setup host ip 10.1.1.2/24,10.1.1.1** と指定します。

- ASDM で、[Wizards] > [Startup Wizard] の順に選択し、ウィザードで [ASA FirePOWER Basic Configuration] に進みます。このページでは、IP アドレス、マスク、およびデフォルト ゲートウェイを設定できます。

ASA FirePOWER CLI での基本的な ASA FirePOWER 設定値の設定

セキュリティ ポリシーを設定する前に、基本的なネットワーク設定およびその他のパラメータを ASA FirePOWER モジュール上で設定する必要があります。この手順では、完全なシステム ソフトウェア（ブート イメージだけでなく）がインストールされていること（直接インストールしたか、ハードウェア モジュールにインストール済みであること）を前提としています。

ヒント　この手順では、初期設定を実行していることも前提としています。初期設定時に、これらの設定を行うように求められます。これらの設定を後で変更する必要がある場合は、各種の **configure network** コマンドを使用して個々の設定を変更します。**configure network** コマンドの詳細については、**?** コマンドを使用してヘルプを表示し、『*FireSIGHT System User Guide*』または FireSIGHT 管理センター のオンライン ヘルプを参照してください。

手順

ステップ 1　次のどちらかを実行します。

- （すべてのモデル）SSH を使用して ASA FirePOWER 管理 IP アドレスに接続します。
- （ASA 5512-X ～ ASA 5555-X）ASA CLI からモジュールへのセッションを開きます（ASA CLI にアクセスするには、一般的な操作のコンフィギュレーション ガイドの「Getting Started」の章を参照してください）。マルチ コンテキスト モードでは、システム実行スペースからセッションを開きます。

  ```
  hostname# session sfr
  ```

ステップ 2　ユーザ名 **admin** およびパスワード **Sourcefire** を使用してログインします。

ステップ 3　プロンプトに従ってシステム設定を完了します。

まず、エンド ユーザ ライセンス契約（EULA）を読み、これに同意する必要があります。次に、プロンプトに従って管理者パスワードを変更し、管理アドレスと DNS 設定を設定します。IPv4 と IPv6 の両方の管理アドレスを設定できます。センサーは FireSIGHT 管理センター で管理する必要があるというメッセージが表示されたら、設定は完了です。

次に例を示します。

```
System initialization in progress.Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <新しいパスワード>
Confirm new password: <パスワードの再入力>
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually?(dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.86.118.3
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
10.120.10.14
Enter a comma-separated list of search domains or 'none' [example.net]: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
(システムが自動的に再設定されるまで待機します)

This sensor must be managed by a Defense Center.A unique alphanumeric
registration key is always required.In most cases, to register a sensor
to a Defense Center, you must provide the hostname or the IP address along
with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Defense Center are separated by a NAT device,
you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

```
Later, using the web interface on the Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.
```

ステップ 4　ここで、「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.17-17）の説明に従って、このデバイスを管理する FireSIGHT 管理センター を指定する必要があります。

FireSIGHT 管理センター への ASA FirePOWER の追加

モジュールにポリシーを設定するためのアプリケーションである ASA FirePOWER に FireSIGHT 管理センター モジュールを登録する必要があります。FireSIGHT 管理センター は防御センターとも呼ばれます。

デバイスを登録するには、**configure manager add** コマンドを使用します。FireSIGHT 管理センター にデバイスを登録するには、一意の英数字の登録キーが常に必要です。これはユーザが指定する簡単なキーで、ライセンス キーと同じではありません。

ほとんどの場合、FireSIGHT 管理センター のホスト名または IP アドレスを登録キーと一緒に指定する必要があります。次に例を示します。

```
configure manager add DC.example.com my_reg_key
```

ただし、デバイスと FireSIGHT 管理センター が NAT デバイスによって分離されている場合、一意の NAT ID を登録キーと一緒に入力し、ホスト名の代わりに DONTRESOLVE を指定します。次に例を示します。

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

手順

ステップ 1　次のどちらかを実行します。

- （すべてのモデル）SSH を使用して ASA FirePOWER 管理 IP アドレスに接続します。
- （ASA 5512-X ～ ASA 5555-X）ASA CLI からモジュールへのセッションを開きます（ASA CLI にアクセスするには、一般的な操作のコンフィギュレーション ガイドの「Getting Started」の章を参照してください）。マルチ コンテキスト モードでは、システム実行スペースからセッションを開きます。

  ```
  hostname# session sfr
  ```

ステップ 2　ユーザ名 **admin** または CLI コンフィギュレーション（管理者）アクセス レベルを持つ別のユーザ名でログインします。

ステップ 3　プロンプトで、**configure manager add** コマンドを使用して FireSIGHT 管理センター にデバイスを登録します。このコマンドの構文は次のとおりです。

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

それぞれの説明は次のとおりです。

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} では、FireSIGHT 管理センター の完全修飾名または IP アドレスを指定します。FireSIGHT 管理センター のアドレスを直接指定できない場合は、DONTRESOLVE を使用します。

- *reg_key* は、FireSIGHT 管理センター にデバイスを登録するために必要な一意の英数字の登録キーです。
- *nat_id* は、FireSIGHT 管理センター とデバイス間の登録プロセス中に使用されるオプションの英数字の文字列です。これは、ホスト名が DONTRESOLVE に設定されている場合に必要です。

ステップ 4　上で入力したホスト名またはアドレスを使用し、ブラウザで HTTPS 接続を使用して FireSIGHT 管理センター にログインします。たとえば、https://DC.example.com などです。

[Device Management]（[Devices] > [Device Management]）ページでデバイスを追加します。詳細については、オンライン ヘルプまたは『*FireSIGHT System User Guide*』の「Managing Devices」の章を参照してください。

ASA FirePOWER モジュールへのセキュリティ ポリシーの設定

ASA FirePOWER モジュールにセキュリティ ポリシーを設定するには、FireSIGHT 管理センター を使用します。セキュリティ ポリシーは、次世代 IPS フィルタリングやアプリケーション フィルタリングなど、モジュールによって提供されるサービスを制御します。ASA FirePOWER CLI、ASA CLI、または ASDM を使用してポリシーを設定することはできません。

FireSIGHT 管理センター を開くには、Web ブラウザを使用して次の URL を開きます。

https://*DC_address*

DC_address は、「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.17-17）で定義したマネージャの DNS 名または IP アドレスです。たとえば、https://DC.example.com などです。

セキュリティ ポリシーの設定方法については、『*FireSIGHT System User Guide*』または FireSIGHT 管理センター のオンライン ヘルプを参照してください。

ヒント　FireSIGHT 管理センター は、ASDM の [ASA FirePOWER Status] ダッシュボードから開くこともできます。[Home] > [ASA FirePOWER Status] を選択して、ダッシュボードの下部にあるリンクをクリックします。

ASA FirePOWER モジュールへのトラフィックのリダイレクト

特定のトラフィックを識別するサービス ポリシーを作成して、ASA FirePOWER モジュールへのトラフィックをリダイレクトします。

デバイスは、パッシブ（「モニタ専用」）展開またはインライン展開のいずれかで設定できます。

- パッシブ展開では、トラフィックのコピーがデバイスに送信されますが、ASA には返されません。パッシブ モードでは、デバイスがトラフィックに対して実行したであろう処理を表示し、ネットワークに影響を与えずにトラフィックの内容を評価することができます。
- インライン展開では、実際のトラフィックがデバイスに送信され、デバイスのポリシーがトラフィックに対する処理に影響します。不要なトラフィックがドロップされ、ポリシーによって適用されるその他のアクションが実行された後、トラフィックはさらなる処理と最終的な送信のために ASA に返されます。

（注）　ASA 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。マルチ コンテキスト モードで、あるコンテキストについてモニタ専用モードを設定し、それ以外のコンテキストについて通常のインライン モードを設定することはできません。

はじめる前に

- （ASA FirePOWER と交換した）IPS または CX モジュールにトラフィックをリダイレクトするアクティブ サービス ポリシーがある場合は、ASA FirePOWER サービス ポリシーを設定する前にそのポリシーを削除する必要があります。
- ASA および ASA FirePOWER には、必ず一貫性のあるポリシーを設定してください（FireSIGHT 管理センター を使用）。両方のポリシーに、トラフィックのパッシブ モードまたはインライン モードを反映させる必要があります。
- マルチコンテキスト モードでは、各セキュリティ コンテキストでこの手順を実行します。

手順

ステップ 1　モジュールに送信するトラフィックを L3/L4 指定するためのクラス マップを作成します。

class-map *name*
match *parameter*

例：

```
hostname(config)# class-map firepower_class_map
hostname(config-cmap)# match access-list firepower
```

モジュールに複数のトラフィック クラスを送信する場合は、セキュリティ ポリシーで使用するための複数のクラス マップを作成できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

policy-map *name*

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　この手順の最初に作成したクラス マップを指定します。

class *name*

例：

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

ステップ 4　ASA FirePOWER モジュールにトラフィックを送信します。

```
sfr {fail-close | fail-open} [monitor-only]
```

それぞれの説明は次のとおりです。

- **fail-close** キーワードを指定すると、ASA FirePOWER モジュールが使用できない場合はすべてのトラフィックをブロックするように ASA が設定されます。
- **fail-open** キーワードを指定すると、モジュールが使用できない場合はすべてのトラフィックを検査なしで通過させるように ASA が設定されます。
- トラフィックの読み取り専用コピーをモジュールに送信するには、**monitor-only** を指定します（パッシブ モード）。キーワードを指定しない場合、トラフィックはインライン モードで送信されます。詳細については、「ASA FirePOWER パッシブ（モニタ専用）モード」（P.17-3）を参照してください。

例：

```
hostname(config-pmap-c)# sfr fail-close
```

ステップ 5　ASA FirePOWER トラフィックに複数のクラス マップを作成した場合、ポリシーに対して別のクラスを指定し、**sfr** リダイレクト処理を適用できます。

ポリシー マップ内でのクラスの順番が重要であることの詳細については、「サービス ポリシー内の機能照合」（P.1-5）を参照してください。トラフィックを同じアクション タイプの複数のクラス マップに一致させることはできません。

ステップ 6　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

```
service-policy policymap_name {global | interface interface_name}
```

例：

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

global キーワードはポリシー 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。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。

ASA FirePOWER モジュールの管理

この項には、モジュールの管理に役立つ手順が含まれます。

パスワードのリセット

管理ユーザのパスワードを忘れた場合は、CLI 設定権限を持つ別のユーザがログインして、パスワードを変更できます。

必要な権限を持つ別のユーザが存在しない場合は、**session do** コマンドを使用して ASA から管理者パスワードをリセットできます。

ヒント　ASA hw-module および sw-module コマンドの password-reset オプションは、ASA FirePOWER では機能しません。

ユーザ **admin** のモジュール パスワードをデフォルトの **Sourcefire** にリセットするには、次のコマンドを使用します。ハードウェア モジュールの場合は **1**、ソフトウェア モジュールの場合は **sfr** を使用します。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

```
session {1 | sfr} do password-reset
```

たとえば、**session sfr do password-reset** を使用します。

モジュールのリロードまたはリセット

モジュールをリロード、またはリセットしてからリロードするには、ASA CLI で次のいずれかのコマンドを入力します。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

- ハードウェア モジュール（ASA 5585-X）：

  ```
  hw-module module 1 {reload | reset}
  ```

- ソフトウェア モジュール（ASA 5512-X ～ ASA 5555-X）：

  ```
  sw-module module sfr {reload | reset}
  ```

モジュールのシャットダウン

モジュール ソフトウェアをシャットダウンするのは、コンフィギュレーション データを失うことなく安全にモジュールの電源をオフにできるように準備するためです。モジュールをグレースフル シャットダウンするには、ASA CLI で次のいずれかのコマンドを入力します。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

（注）　ASA をリロードする場合は、モジュールは自動的にはシャットダウンされないので、ASA のリロード前にモジュールをシャットダウンすることを推奨します。

- ハードウェア モジュール（ASA 5585-X）：

  ```
  hw-module module 1 shutdown
  ```

- ソフトウェア モジュール（ASA 5512-X ～ ASA 5555-X）：

  ```
  sw-module module sfr shutdown
  ```

（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュール イメージのアンインストール

ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールできます。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

手順

ステップ 1　ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールします。

```
hostname# sw-module module sfr uninstall

Module sfr will be uninstalled.This will completely remove the disk image
associated with the sw-module including any configuration that existed within it.

Uninstall module sfr?[confirm]
```

ステップ 2　ASA をリロードします。新しいモジュールをインストールする前に、ASA をリロードする必要があります。

```
hostname# reload
```

（ASA 5512-X ～ ASA 5555-X）ASA からモジュールへのセッション

基本的なネットワーク設定を構成し、モジュールをトラブルシューティングするには、ASA FirePOWER CLI を使用します。

ASA FirePOWER ソフトウェア モジュール CLI に ASA からアクセスするには、ASA からセッションを開始します。モジュールへのセッションを開始することも（Telnet を使用）、仮想コンソール セッションを作成することもできます。コンソール セッションは、コントロール プレーンがダウンし、Telnet セッションを確立できない場合に便利です。マルチ コンテキスト モードでは、システム実行スペースからセッションを開きます。

Telnet またはコンソール セッションでは、ユーザ名とパスワードの入力を求められます。ASA FirePOWER に設定されている任意のユーザ名とパスワードでログインできます。最初は、**admin** が唯一の設定済みユーザ名です（このユーザ名は常に使用可能です）。最初のデフォルトのユーザ名は、フル イメージの場合は **Sourcefire**、ブート イメージの場合は **Admin123** です。

- Telnet セッション：

  session sfr

  ASA FirePOWER CLI にいるときに ASA CLI に戻るには、モジュールからログアウトするコマンド（**logout** や **exit** など）を入力するか、**Ctrl+Shift+6、x** を押します。

- コンソール セッション：

  session sfr console

  コンソール セッションからログアウトする唯一の方法は、**Ctrl+Shift+6、x** を押すことです。モジュールからログアウトすると、モジュールのログイン プロンプトに戻ります。

（注）　**session sfr console** コマンドは、**Ctrl+Shift+6、x** がターミナル サーバのプロンプトに戻るエスケープ シーケンスであるターミナル サーバとともに使用しないでください。**Ctrl+Shift+6、x** は、ASA FirePOWER コンソールをエスケープして、ASA プロンプトに戻るためのシーケンスでもあります。したがって、この状況で、ASA FirePOWER コンソールを終了しようとすると、ターミナル サーバ プロンプトまで終了することになります。ASA にターミナル サーバを再接続すると、ASA FirePOWER コンソール セッションがまだアクティブなままであり、ASA プロンプトに戻ることができません。ASA プロンプトにコンソールを戻すには、直接シリアル接続を使用する必要があります。この状況が発生した場合は、console コマンドの代わりに **session sfr** コマンドを使用します。

5585-X ASA FirePOWER ハードウェア モジュールのイメージの再作成

何らかの理由で ASA FirePOWER ASA 5585-X アプライアンスのハードウェア モジュールのイメージを再作成する必要がある場合は、ブート イメージとシステム ソフトウェア パッケージの両方をこの順序でインストールする必要があります。システムが機能するには、両方のパッケージをインストールする必要があります。通常の状況では、アップグレード パッケージをインストールするために、システムのイメージを再作成する必要はありません。

ブート イメージをインストールするには、モジュールのコンソール ポートにログインして、ASA FirePOWER SSP の Management-0 ポートからイメージを TFTP ブートする必要があります。Management-0 ポートは SSP の最初のスロットにあるため、Management1/0 とも呼ばれますが、ROMmon では Management-0 または Management0/1 として認識されます。

TFTP ブートを行うには、次の手順を実行します。

- ソフトウェア イメージを、ASA FirePOWER の Management1/0 インターフェイスからアクセス可能な TFTP サーバに配置する。
- Management1/0 をネットワークに接続する。このインターフェイスを使用して、ブート イメージを TFTP ブートする必要があります。
- ROMmon 変数を設定する。ROMmon 変数を設定するには、Esc キーを押して自動ブート プロセスを中断します。

ブート イメージがインストールされたら、システム ソフトウェア パッケージをインストールします。ASA FirePOWER からアクセス可能な HTTP、HTTPS、または FTP サーバに、パッケージを配置する必要があります。

次の手順では、ブート イメージをインストールしてからシステム ソフトウェア パッケージをインストールする方法を説明します。

手順

ステップ 1　コンソール ポートに接続します。ASA 製品に付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナル エミュレータを用いて PC をコンソールに接続します。コンソール ケーブルの詳細については、ASA のハードウェア ガイドを参照してください。

ステップ 2　**system reboot** コマンドを入力してシステムをリロードします。

ステップ 3　プロンプトが表示されたら、Esc キーを押してブートから抜け出します。GRUB がシステムをブートするために起動するのが表示された場合は、待ちすぎです。

これにより、ROMmon プロンプトに切り替わります。

ステップ 4　ROMmon プロンプトで、**set** を入力して次のパラメータを設定します。

- ADDRESS：モジュールの管理 IP アドレス。
- SERVER：TFTP サーバの IP アドレス。
- GATEWAY：TFTP サーバのゲートウェイ アドレス。TFTP サーバが Management1/0 に直接接続されている場合は、TFTP サーバの IP アドレスを使用します。TFTP サーバおよび管理アドレスが同じサブネット上にある場合は、ゲートウェイを設定しないでください。設定すると、TFTP ブートが失敗します。
- IMAGE：TFTP サーバ上のブート イメージのパスとイメージ名。たとえば、TFTP サーバの /tftpboot/images/filename.img にファイルを置いた場合、IMAGE の値は images/filename.img となります。

次に例を示します。

```
ADDRESS=10.5.190.199
SERVER=10.5.11.170
GATEWAY=10.5.1.1
IMAGE=asasfr-boot-5.3.1-26-54.img
```

ステップ 5　**sync** を入力して設定を保存します。

ステップ 6　**tftp** を入力してダウンロードおよびブート プロセスを開始します。

進行状況を示す！ マークが表示されます。数分後にブートが完了すると、ログイン プロンプトが表示されます。

ステップ 7　パスワード **Admin123** を使用して **admin** としてログインします。

ステップ 8　システム ソフトウェア パッケージをインストールできるように、**setup** コマンドを使用してシステムを設定します。

次の項目を指定するように求められます。主な設定項目は、管理アドレスとゲートウェイ、および DNS 情報です。

- ホスト名：65 文字までの英数字で、スペースは使用できません。ハイフンを使用できます。
- ネットワーク アドレス：スタティック IPv4 または IPv6 アドレスを設定するか、または DHCP （IPv4 の場合）または IPv6 ステートレス自動設定を使用することができます。
- DNS 情報：少なくとも 1 つの DNS サーバを指定する必要があります。ドメイン名と検索ドメインを設定することもできます。
- NTP 情報：システム時刻を設定するために、NTP をイネーブルにして NTP サーバを設定することができます。

ステップ 9　**system install** コマンドを使用してシステム ソフトウェア イメージをインストールします。

system install [**noconfirm**] *url*

確認メッセージに応答したくない場合は、**noconfirm** オプションを指定します。

インストールが完了すると、システムが再起動します。アプリケーション コンポーネントのインストールと ASA FirePOWER サービスの起動には 10 分以上かかります次に例を示します。

```
asasfr-boot> system install http://asasfr-sys-5.3.1-54.pkg
```

ステップ 10　ブートが完了したら、パスワード **Sourcefire** を使用して **admin** としてログインします。

プロンプトに従ってシステム設定を完了します。

まず、エンド ユーザ ライセンス契約（EULA）を読み、これに同意する必要があります。次に、プロンプトに従って管理者パスワードを変更し、管理アドレスと DNS 設定を設定します。IPv4 と IPv6 の両方の管理アドレスを設定できます。

ステップ 11　**configure manager add** コマンドを使用して、このデバイスを管理する FireSIGHT 管理センター アプライアンスを指定します。

登録キーを考え出します。このキーは、デバイスをインベントリに追加するときに FireSIGHT 管理センター で使用します。次に、簡単な例を示します。NAT 境界がある場合は、コマンドが異なります。「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.17-17）を参照してください。

```
> configure manager add 10.89.133.202 123456
Manager successfully configured.
```

ステップ 12　上で入力したホスト名またはアドレスを使用し、ブラウザで HTTPS 接続を使用して FireSIGHT 管理センター にログインします。たとえば、https://DC.example.com などです。

[Device Management]（[Devices] > [Device Management]）ページでデバイスを追加します。詳細については、『*FireSIGHT System User Guide*』または FireSIGHT 管理センター のオンライン ヘルプの「Managing Devices」の章を参照してください。

システム ソフトウェアのアップグレード

FireSIGHT 管理センター を使用して ASA FirePOWER モジュールにアップグレード イメージを適用します。アップグレードを適用する前に、ASA が新しいバージョンに最小限必要なリリースを実行していることを確認します。場合によっては、モジュールをアップグレードする前に ASA をアップグレードする必要があります。

アップグレードの適用の詳細については、『*FireSIGHT System User Guide*』または FireSIGHT 管理センター のオンライン ヘルプを参照してください。

ASA FirePOWER モジュールのモニタリング

次の各トピックでは、モジュールのモニタリングに関するガイダンスを示します。ASA FirePOWER 関連の syslog メッセージについては、syslog メッセージ ガイドを参照してください。ASA FirePOWER の syslog メッセージは、メッセージ番号 434001 から始まります。

- 「モジュール ステータスの表示」（P.17-25）
- 「モジュールの統計情報の表示」（P.17-27）
- 「モジュール接続のモニタリング」（P.17-27）

モジュール ステータスの表示

モジュールのステータスを確認するには、次のいずれかのコマンドを入力します。

- **show module** [**1** | **sfr**] [**details**]

  モジュールのステータスを表示します。ASA FirePOWER モジュールに固有のステータスを表示するには、1（ハードウェア モジュールの場合）または sfr（ソフトウェア モジュールの場合）キーワードを指定します。モジュールを管理するデバイスのアドレスなどの追加情報を取得するには、details キーワードを指定します。

- **show module sfr recover**

  モジュールのインストール時に使用されたブート イメージの場所を表示します。

ASA 5585-X に ASA FirePOWER ハードウェア モジュールがインストールされている場合の **show module** コマンドの出力例を次に示します。

```
hostname# show module
Mod  Card Type                                    Model              Serial No.
---- -------------------------------------------- ------------------ -----------
   0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10     JAF1507AMKE
   1 ASA 5585-X FirePOWER Security Services Proce ASA5585-SSP-SFR10  JAF1510BLSA

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 5475.d05b.1100 to 5475.d05b.110b  1.0          2.0(7)0      100.10(0)8
   1 5475.d05b.2450 to 5475.d05b.245b  1.0          2.0(13)0     5.3.1-44

Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
   1 FirePOWER                      Up               5.3.1-44

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
   1 Up                 Up
```

次に、ソフトウェア モジュールの詳細を表示する例を示します。DC Addr は、このデバイスを管理する FireSIGHT 管理センター のアドレスを示しています。

```
hostname# show module sfr details
Getting details from the Service Module, please wait...

Card Type:          FirePOWER Services Software Module
Model:              ASA5555
Hardware version:   N/A
Serial Number:      FCH1714J6HP
Firmware version:   N/A
Software version:   5.3.1-100
MAC Address Range:  bc16.6520.1dcb to bc16.6520.1dcb
App.name:           ASA FirePOWER
App.Status:         Up
App.Status Desc:    Normal Operation
App.version:        5.3.1-100
Data Plane Status:  Up
Status:             Up
DC addr:            10.89.133.202
Mgmt IP addr:       10.86.118.7
Mgmt Network mask:  255.255.252.0
Mgmt Gateway:       10.86.116.1
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

次に、モジュールのインストール時に **sw-module module sfr recover** コマンドで使用された ASA FirePOWER ブート イメージの場所を表示する例を示します。

```
hostname# show module sfr recover
Module sfr recover parameters...
Boot Recovery Image: No
Image File Path:     disk0:/asasfr-5500x-boot-5.3.1-44.img
```

モジュールの統計情報の表示

sfr コマンドを含む各サービス ポリシーの統計情報およびステータスを表示するには、show service-policy sfr コマンドを使用します。カウンタをクリアするには、**clear service-policy** を使用します。

次に、ASA FirePOWER サービス ポリシーと現在の統計情報およびモジュールのステータスを表示する例を示します。

```
ciscoasa# show service-policy sfr

Global policy:
Service-policy: global_policy
    Class-map: my-sfr-class
      SFR: card status Up, mode fail-close
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

次に、モニタ専用ポリシーを表示する例を示します。この場合、パケット入力カウンタは増加しますが、ASA に戻されるトラフィックはないので、パケット出力カウンタはゼロのままです。

```
hostname# show service-policy sfr
Global policy:
Service-policy: global_policy
    Class-map: bypass
      SFR: card status Up, mode fail-open, monitor-only
        packet input 2626422041, packet output 0, drop 0, reset-drop 0, proxied 0
```

モジュール接続のモニタリング

ASA FirePOWER モジュールを通過する接続を表示するには、次のいずれかのコマンドを入力します。

- **show asp table classify domain sfr**

  トラフィックを ASA FirePOWER モジュールに送信するために作成された NP ルールを表示します。

- **show asp drop**

  ドロップされたパケットを表示します。ドロップのタイプについては、以下で説明します。

- **show conn**

  「X - inspected by service module」フラグを表示することにより、接続がモジュールに転送されているかどうかを示します。

show asp drop コマンドには、ASA FirePOWER モジュールに関連する次のドロップの理由を含めることができます。

フレーム ドロップ：

- sfr-bad-tlv-received：これが発生するのは、ASA が FirePOWER から受信したパケットにポリシー ID TLV がないときです。非制御パケットのアクション フィールドで Standy/Active ビットが設定されていない場合は、この TLV が存在している必要があります。
- sfr-request：FirePOWER 上のポリシーが理由で、フレームをドロップするよう FirePOWER から要求されました。このポリシーによって、FirePOWER はアクションを Deny Source、Deny Destination、または Deny Pkt に設定します。フレームがドロップべきでなかった場合は、フローを拒否しているモジュールのポリシーを確認します。

- sfr-fail-close：パケットがドロップされたのは、カードが動作中ではなく、設定済みのポリシーが「fail-close」であったからです（対照的に、「fail-open」の場合は、カードがダウンしていてもパケットの通過が許可されます）。カードのステータスを確認し、サービスを再開するか、再起動します。
- sfr-fail：既存のフローに対する FirePOWER コンフィギュレーションが削除されており、FirePOWER で処理できないため、ドロップされます。これが発生することは、ほとんどありません。
- sfr-malformed-packet：FirePOWER からのパケットに無効なヘッダーが含まれます。たとえば、ヘッダー長が正しくない可能性があります。
- sfr-ha-request：セキュリティ アプライアンスが FirePOWER HA 要求パケットを受信し、それを処理できなかった場合、このカウンタが増加し、パケットがドロップされます。
- sfr-invalid-encap：セキュリティ アプライアンスが無効なメッセージ ヘッダーを持つ FirePOWER パケットを受信すると、このカウンタが増加し、パケットがドロップされます。
- sfr-bad-handle-received：FirePOWER モジュールからパケットで不正フロー ハンドルを受信し、フローをドロップしました。FirePOWER フローのハンドルがフロー期間中に変更されると、このカウンタが増加し、フローとパケットが ASA でドロップされます。
- sfr-rx-monitor-only：セキュリティ アプライアンスがモニタ専用モードのときに FirePOWER パケットを受信すると、このカウンタが増加し、パケットがドロップされます。

フロードロップ：

- sfr-request：フローを終了させることを FirePOWER が要求しました。アクション ビット 0 が設定されます。
- reset-by-sfr：フローの終了とリセットを FirePOWER が要求しました。アクション ビット 1 が設定されます。
- sfr-fail-close：フローが終了させられたのは、カードがダウン状態であり、設定済みのポリシーが「fail-close」であったからです。

ASA FirePOWER モジュールの例

次に、すべての HTTP トラフィックを ASA FirePOWER モジュールに迂回させ、何らかの理由でモジュールで障害が発生した場合にはすべての HTTP トラフィックをブロックする例を示します。

```
hostname(config)# access-list ASASFR permit tcp any any eq 80
hostname(config)# class-map my-sfr-class
hostname(config-cmap)# match access-list ASASFR
hostname(config-cmap)# policy-map my-sfr-policy
hostname(config-pmap)# class my-sfr-class
hostname(config-pmap-c)# sfr fail-close
hostname(config-pmap-c)# service-policy my-sfr-policy global
```

次に、10.1.1.0 ネットワークおよび 10.2.1.0 ネットワーク宛てのすべての IP トラフィックを ASA FirePOWER モジュールに迂回させ、何らかの理由でモジュールに障害が発生してもすべてのトラフィックを許可する例を示します。

```
hostname(config)# access-list my-sfr-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-sfr-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-sfr-class
hostname(config-cmap)# match access-list my-sfr-acl
hostname(config)# class-map my-sfr-class2
hostname(config-cmap)# match access-list my-sfr-acl2
hostname(config-cmap)# policy-map my-sfr-policy
hostname(config-pmap)# class my-sfr-class
hostname(config-pmap-c)# sfr fail-open
hostname(config-pmap)# class my-sfr-class2
hostname(config-pmap-c)# sfr fail-open
hostname(config-pmap-c)# service-policy my-sfr-policy interface outside
```

ASA FirePOWER モジュールの履歴

機能名	プラットフォームリリース	機能情報
ASA 5585-X（すべてのモデル）で適合する ASA FirePOWER SSP ハードウェア モジュールをサポート。 ASA 5512-X ～ ASA 5555-X で ASA FirePOWER ソフトウェア モジュールをサポート。	ASA 9.2(2.4) ASA FirePOWER 5.3.1	ASA FirePOWER モジュールは、次世代 IPS（NGIPS）、アプリケーションの可視性とコントロール（AVC）、URL フィルタリング、高度なマルウェア保護（AMP）などの次世代ファイアウォール サービスを提供します。このモジュールは、シングルまたはマルチ コンテキスト モードとルーテッドまたはトランスペアレント モードで使用できます。 **capture interface asa_dataplane**、**debug sfr**、**hw-module module 1 reload**、**hw-module module 1 reset**、**hw-module module 1 shutdown**、**session do setup host ip**、**session do get-config**、**session do password-reset**、**session sfr**、**sfr**、**show asp table classify domain sfr**、**show capture**、**show conn**、**show module sfr**、**show service-policy**、**sw-module sfr** の各コマンドが導入または変更されました。

ASA CX モジュール

この章では、ASA で実行される ASA CX モジュールを設定する方法について説明します。

ASA CX モジュール

ASA CX モジュールを使用すると、特定の状況の完全なコンテキストに基づいてセキュリティを強制することができます。このコンテキストには、ユーザのアイデンティティ（誰が）、ユーザがアクセスを試みているアプリケーションまたは Web サイト（何を）、アクセス試行の発生元（どこで）、アクセス試行の時間（いつ）、およびアクセスに使用されているデバイスのプロパティ（どのように）が含まれます。ASA CX モジュールを使用すると、フローの完全なコンテキストを抽出して、細分化したポリシーを適用することができます。たとえば、Facebook へのアクセスを許可するが Facebook でのゲームへのアクセスは禁止する、あるいは企業の機密データベースへのアクセスを財務担当者に許可するが他の社員には禁止するといったことが可能です。

ASA CX モジュールがどのように ASA と連携するか

ASA CX モジュールは、ASA とは別のアプリケーションを実行します。このモジュールは、ハードウェア モジュール（ASA 5585-X 上）か、ソフトウェア モジュール（5512-X ～ 5555-X）です。ハードウェア モジュールには、独立した管理およびコンソール ポートと、モジュール自体ではなく ASA によって直接使用される追加のデータ インターフェイスがあります。

ご使用のデバイスをデモンストレーション用に、通常のインライン モードまたはモニタ専用モードのいずれかに設定できます。

- インライン展開では、実際のトラフィックがデバイスに送信され、デバイスのポリシーがトラフィックに対する処理に影響します。不要なトラフィックがドロップされ、ポリシーによって適用されるその他のアクションが実行された後、トラフィックはさらなる処理と最終的な送信のために ASA に返されます。
- モニタ専用配置では、トラフィックのコピーがデバイスに送信されますが、ASA に戻されることはありません。モニタ専用モードでは、ネットワークに影響を与えることなくデバイスがトラフィックへの処理を行うことがわかります。モニタ専用のサービス ポリシーまたはトラフィック転送インターフェイスを使用してこのモードを設定できます。モニタ専用モードに関するガイドラインと制限事項については、「ASA CX のガイドライン」（P.18-6）を参照してください。

次の各セクションでは、これらのモードについて詳しく説明します。

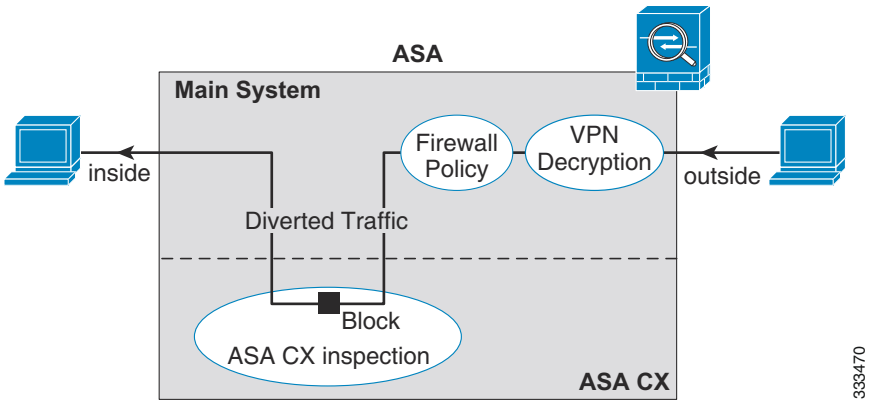
ASA CX の通常のインライン モード

通常のインライン モードでは、トラフィックは、ファイアウォール検査を通過してから ASA CX モジュールへ転送されます。ASA で ASA CX インスペクション対象として指定されたトラフィックは、次に示すように ASA および ASA CX モジュールを通過します。

1. トラフィックは ASA に入ります。
2. 着信 VPN トラフィックが復号化されます。
3. ファイアウォール ポリシーが適用されます。
4. トラフィックが ASA CX モジュールに送信されます。
5. ASA CX モジュールはセキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
6. 有効なトラフィックが ASA に返送されます。ASA CX モジュールは、セキュリティ ポリシーに従ってトラフィックをブロックすることがあり、ブロックされたトラフィックは渡されません。
7. 発信 VPN トラフィックが暗号化されます。
8. トラフィックが ASA から出ます。

次の図は、ASA CX モジュールを使用する場合のトラフィック フローを示します。この例では、特定のアプリケーションに対して許可されていないトラフィックを ASA CX モジュールが自動的にブロックします。それ以外のトラフィックは、ASA を通って転送されます。

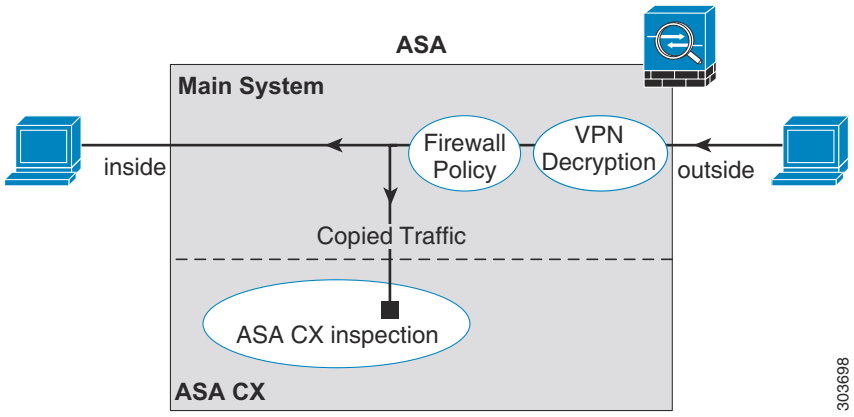
図 18-1　ASA での ASA CX モジュールのトラフィック フロー



モニタ専用モードでのサービス ポリシー

テストおよびデモンストレーション用に、ASA CX モジュールに読み取り専用トラフィックの重複ストリームを送信するように ASA を設定できるので、モジュールが ASA トラフィック フローに影響を与えることなく、どのようにトラフィックをインスペクションするかを確認できます。このモードでは、ASA CX モジュールが通常どおりトラフィックをインスペクションし、ポリシーを決定し、イベントを生成します。ただし、パケットが読み取り専用コピーであるため、モジュールのアクションは実際のトラフィックには影響しません。代わりに、モジュールはインスペクション後コピーをドロップします。次の図は、モニタ専用モードの ASA CX モジュールを示します。

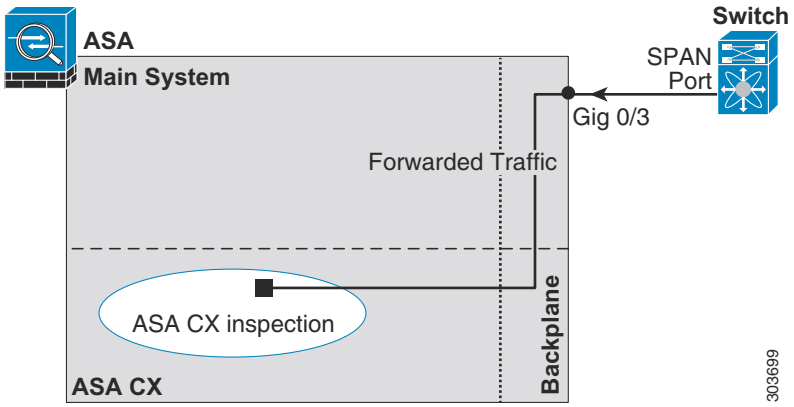
図 18-2　ASA CX モニタ専用モード



モニタ専用モードでのトラフィック転送インターフェイス

または、ASA インターフェイスを転送インターフェイスに設定し、ASA 処理を行わずに受信したすべてのトラフィックを直接 ASA CX モジュールに転送できます。テストおよびデモンストレーション用に、トラフィック転送では ASA 処理の余分な複雑性を取り除きます。トラフィック転送はモニタ専用モードでのみサポートされるので、ASA CX モジュールはインスペクション後トラフィックをドロップします。次の図は、トラフィック転送が設定されている ASA GigabitEthernet 0/3 インターフェイスを示します。このインターフェイスは、ASA CX モジュールがすべてのネットワーク トラフィックをインスペクションできるように、スイッチの SPAN ポートに接続されます。

図 18-3　ASA CX トラフィック転送



ASA CX の管理アクセス

ASA CX モジュールの管理には、初期設定（とその後のトラブルシューティング）およびポリシー管理の 2 つの異なるアクセスのレイヤがあります。

- 「初期設定」（P.18-4）
- 「ポリシー設定および管理」（P.18-5）

初期設定

初期設定を行うには、ASA CX モジュールの CLI を使用して **setup** コマンドを実行し、その他の任意の設定値を設定する必要があります。

CLI にアクセスするには、次の方法を使用します。

- ASA 5585-X
  - ASA CX コンソール ポート：ASA CX コンソール ポートは、独立した外部コンソール ポートです。
  - ASA CX Management 1/0 インターフェイス（SSH を使用）：デフォルトの IP アドレス（192.168.8.8）に接続することも、ASDM を使用して管理 IP アドレスを変更してから SSH を使用して接続することもできます。ASA CX 管理インターフェイスは、独立した外部ギガビット イーサネット インターフェイスです。

（注）　**session** コマンドを使用して ASA バックプレーンを介して ASA CX ハードウェア モジュール CLI にアクセスすることはできません。

- ASA 5512-X ～ ASA 5555-X
  - バックプレーンを経由した ASA セッション：ASA に CLI アクセスが可能な場合は、モジュールにセッション接続し、そのモジュール CLI にアクセスできます。
  - ASA CX Management 0/0 インターフェイス（SSH を使用）：デフォルトの IP アドレス（192.168.1.2）に接続することも、ASDM を使用して管理 IP アドレスを変更してから SSH を使用して接続することもできます。これらのモデルは、ASA CX モジュールをソフトウェア モジュールとして実行します。ASA CX 管理インターフェイスは、Management 0/0 インターフェイスを ASA と共有します。ASA と ASA CX モジュールのそれぞれに別の MAC アドレスと IP アドレスがサポートされます。ASA CX IP アドレスの設定は、ASA CX オペレーティング システム内で（CLI または ASDM を使用して）実行する必要があります。ただし、物理特性（インターフェイスのイネーブル化など）は、ASA 上で設定されます。ASA インターフェイス コンフィギュレーションを削除して（特にインターフェイス名）、このインターフェイスを ASA CX 専用インターフェイスとすることができます。このインターフェイスは管理専用です。

ポリシー設定および管理

初期設定を実行した後で、Cisco Prime Security Manager（PRSM）を使用して ASA CX ポリシーを設定します。PRSM は ASA CX 設定インターフェイスの名前であり、それとは別に ASA CX デバイス、Cisco Prime Security Manager を設定する製品の名前でもあります。

その後、ASDM、ASA CLI、またはマルチ デバイス モードで PRISM を使用して、ASA CX モジュールにトラフィックを送信するために ASA ポリシーを設定します。

アクティブ認証用の認証プロキシ

アイデンティティ ポリシーを ASA CX に設定して、アクセス ポリシーで使用するユーザ アイデンティティ情報を収集できます。システムは、ユーザ アイデンティティをアクティブに（ユーザ名およびパスワードのクレデンシャルの入力を求めるプロンプトを表示する）またはパッシブに（AD エージェントまたは Cisco Context Directory Agent（CDA）が収集した情報を取得する）収集できます。

アクティブ認証を使用する場合は、認証プロキシとして動作するように ASA を設定する必要があります。ASA CX モジュールは認証要求を ASA インターフェイスの IP アドレス/プロキシ ポートにリダイレクトします。デフォルト ポートは 885 ですが、別のポートを設定することもできます。

アクティブ認証をイネーブルにするには、「ASA CX サービス ポリシーの作成」（P.18-18）で説明するように、トラフィックを ASA CX にリダイレクトするサービス ポリシーの一部として認証プロキシをイネーブルにします。

ASA の機能との互換性

ASA には、多数の高度なアプリケーション インスペクション機能があり、HTTP インスペクションもその一つです。ただし、ASA CX モジュールには ASA よりも高度な HTTP インスペクション機能があり、その他のアプリケーションについても機能が追加されています。たとえば、アプリケーション使用状況のモニタリングと制御です。

ASA CX モジュールの機能を最大限に活用するには、ASA CX モジュールに送信するトラフィックに関する次のガイドラインを参照してください。

- HTTP トラフィックに対して ASA インスペクションを設定しないでください。
- クラウド Web セキュリティ（ScanSafe）インスペクションを設定しないでください。同じトラフィックに対して ASA CX のアクションとクラウド Web セキュリティ インスペクションの両方が設定されている場合に、ASA が実行するのは ASA CX のアクションのみです。
- ASA 上の他のアプリケーション インスペクションは ASA CX モジュールと互換性があり、これにはデフォルト インスペクションも含まれます。
- Mobile User Security（MUS）サーバをイネーブルにしないでください。これは、ASA CX モジュールとの間に互換性がありません。
- ASA クラスタリングをイネーブルにしないでください。これは、ASA CX モジュールとの間に互換性がありません。

ASA CX モジュールのライセンス要件

ASA CX モジュールと PRSM には追加のライセンスが必要です。このライセンスは ASA との関連でインストールするのではなく、モジュール自体にインストールする必要があります。ASA 自体には、追加ライセンスは必要ありません。詳細については、ASA CX のマニュアルを参照してください。

ASA CX の前提条件

PRSM を使用して ASA を設定するには、セキュアな通信を行うために ASA に証明書をインストールする必要があります。デフォルトでは、ASA は自己署名証明書を生成します。ただし、この証明書のパブリッシャが不明であるため、ブラウザに証明書の検証を求めるプロンプトが表示されます。これらのブラウザのプロンプトが表示されないようにするには、代わりに既知の認証局（CA）からの証明書をインストールします。CA からの証明書を要求する場合、証明書タイプがサーバ認証証明書とクライアント認証証明書の両方であることを確認します。詳細については、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。

ASA CX のガイドライン

コンテキスト モードのガイドライン

ASA CX 9.1(3) を始めに、複数のマルチ コンテキスト モードがサポートされます。

ただし、（PRSM で設定されている）ASA CX モジュール自体はシングル コンテキスト モードのデバイスです。つまり、ASA から着信するコンテキスト固有のトラフィックは共通の ASA CX ポリシーと照合されます。したがって、複数のコンテキストで同じ IP アドレスを使用できず、各コンテキストに独自のネットワークを含める必要があります。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。トラフィック転送インターフェイスは、トランスペアレント モードでのみサポートされます。

フェールオーバーのガイドライン

フェールオーバーを直接にはサポートしていません。ASA がフェールオーバーしたときに、既存の ASA CX フローは新しい ASA に転送されますが、トラフィックは ASA CX によるインスペクションを受けることなく ASA の通過を許可されます。新しい ASA が受信した新しいフローだけが、ASA CX モジュールによる処理の対象となります。

ASA クラスタリングのガイドライン

クラスタリングはサポートされません。

IPv6 のガイドライン

- IPv6 をサポートします。
- （9.1(1) 以前）NAT 64 はサポートされません。9.1(2) 以降では、NAT 64 がサポートされます。

モデルのガイドライン

- ASA 5585-X および 5512-X ～ ASA 5555-X でのみサポートされています。詳細については、『*Cisco ASA Compatibility Matrix*』を参照してください。

  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

- 5512-X ～ ASA 5555-X の場合は、シスコのソリッド ステート ドライブ（SSD）を実装する必要があります。詳細については、ASA 5500-X のハードウェア ガイドを参照してください。

モニタ専用モードのガイドライン

モニタ専用モードは厳密にデモンストレーション用であり、モジュールの通常の動作モードではありません。

- ASA 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。マルチ コンテキスト モードで、あるコンテキストについてモニタ専用モードを設定し、それ以外のコンテキストについて通常のインライン モードを設定することはできません。
- 次の機能は、モニタ専用モードではサポートされません。
  - 拒否ポリシー
  - アクティブ認証
  - 復号ポリシー
- ASA CX は、モニタ専用モードでパケット バッファリングを実行せず、イベントはベストエフォート方式で生成されます。たとえば、長い URL がパケット境界にまたがっている一部のイベントは、バッファリングの欠如の影響を受ける可能性があります。
- ASA ポリシーと ASA CX の両方で必ずモードが一致するように設定する必要があります（両方ともモニタ専用モード、または両方とも通常のインライン モード）。

上記のほか、トラフィック転送インターフェイスには次のガイドラインがあります。

- ASA はトランスペアレント モードにする必要があります。
- 最大 4 つのインターフェイスを、トラフィック転送インターフェイスとして設定できます。その他の ASA インターフェイスは、通常どおり使用できます。
- トラフィック転送インターフェイスは、VLAN または BVI ではなく、物理インターフェイスである必要があります。また、物理インターフェイスには、それに関連付けられた VLAN を設定することはできません。
- トラフィック転送インターフェイスは、ASA トラフィックには使用できません。これらに名前を付けたり、フェールオーバーや管理専用を含む ASA 機能向けに設定できません。
- トラフィック転送インターフェイスとサービス ポリシーの両方を ASA CX トラフィック用に設定できません。

その他のガイドラインと制限事項

- 「ASA の機能との互換性」（P.18-6）を参照してください。
- ハードウェア モジュールにインストールされているソフトウェアのタイプの変更はできません。つまり、購入した ASA CX モジュールに、後で別のソフトウェアをインストールすることはできません。

ASA CX のデフォルト設定

次の表に、ASA CX モジュールのデフォルト設定を示します。

表 18-1　デフォルトのネットワーク パラメータ

パラメータ	デフォルト
管理 IP アドレス	ASA 5585-X：Management 1/0 192.168.8.8/24 ASA 5512-X ～ ASA 5555-X：Management 0/0 192.168.1.2/24
ゲートウェイ	ASA 5585-X：192.168.8.1/24 ASA 5512-X ～ ASA 5555-X：192.168.1.1/24
SSH またはセッションのユーザ名	admin
パスワード	Admin123

ASA CX モジュールの設定

ASA CX モジュールの設定プロセスでは、ASA CX セキュリティ ポリシーを ASA CX モジュール上で設定してから、トラフィックを ASA CX モジュールに送信するように ASA を設定します。ASA CX モジュールを設定するには、次の手順に従います。

ステップ 1　「ASA CX 管理インターフェイスの接続」（P.18-9）。ケーブルで ASA CX 管理インターフェイスに接続します（任意でコンソール インターフェイスにも）。

ステップ 2　「（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールのインストールまたはイメージの再作成」（P.18-12）。

ステップ 3　「(ASA 5585-X) ASA CX 管理 IP アドレスの変更」(P.18-14)（必要な場合）。これは最初の SSH アクセスに必要になる場合があります。

ステップ 4　「基本的な ASA CX 設定値の設定」(P.18-15)。この設定は ASA CX モジュールで行います。

ステップ 5　「ASA CX モジュールでのセキュリティ ポリシーの設定」(P.18-17)。

ステップ 6　（任意）「認証プロキシ ポートの設定」(P.18-17)。

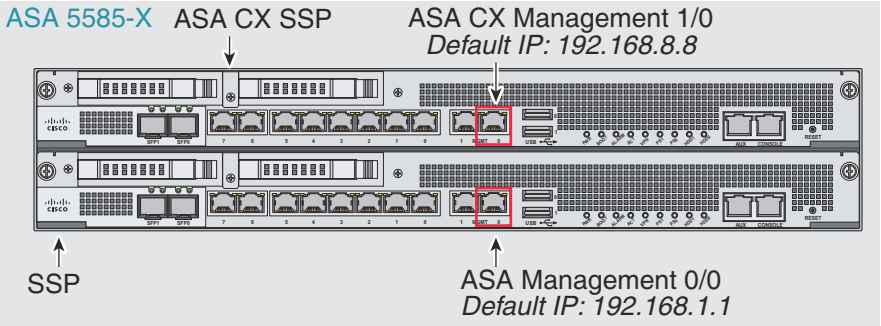
ステップ 7　「ASA CX モジュールへのトラフィックのリダイレクト」(P.18-17)。

ASA CX 管理インターフェイスの接続

ASA CX モジュールへの管理アクセスを提供する以外に、ASA CX 管理インターフェイスは、HTTP プロキシ サーバまたは DNS サーバおよびインターネットへのアクセスを必要とします。これは、シグニチャ アップデートなどのためです。この項では、推奨されるネットワーク コンフィギュレーションを示します。実際のネットワークでは、異なる可能性があります。

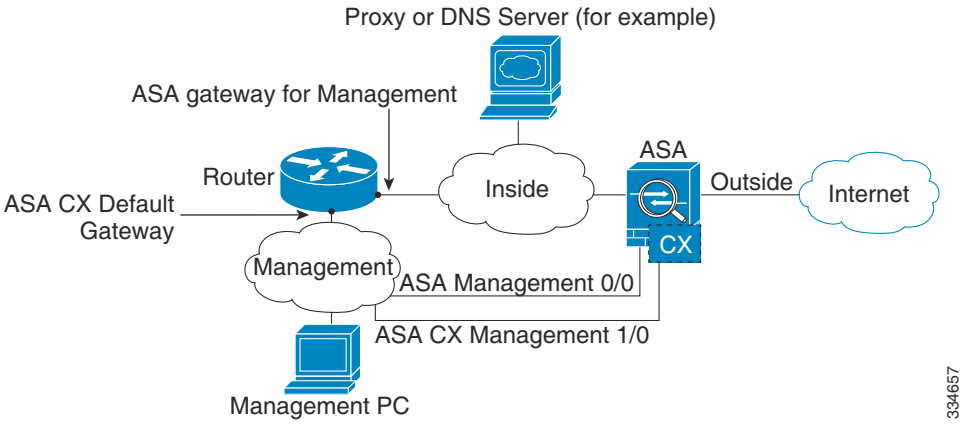
ASA 5585-X（ハードウェア モジュール）

ASA CX モジュールには、ASA とは別の管理およびコンソール インターフェイスが含まれます。初期設定を行うには、デフォルト IP アドレス（192.168.8.8/24）を使用して ASA CX Management 1/0 インターフェイスに SSH で接続できます。デフォルト IP アドレスを使用できない場合は、コンソール ポートを使用するか、ASDM を使用して SSH を使用できるように管理 IP アドレスを変更します。



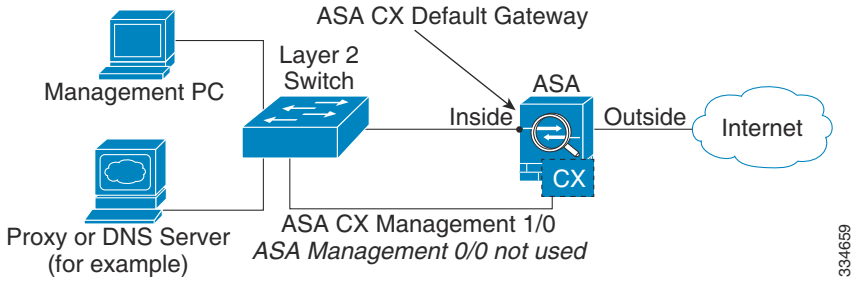
内部ルータがある場合

内部ルータがある場合は、管理ネットワーク（これには ASA Management 0/0 インターフェイスおよび ASA CX Management 1/0 インターフェイスの両方を含めることができます）と ASA 内部ネットワークとの間でルーティングできます（インターネット アクセス用）。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



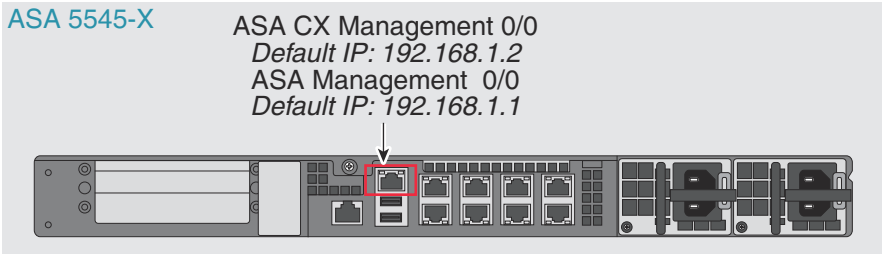
内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません（仮に持つとすれば、内部ルータがネットワーク間のルーティングを行う必要があります）。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA CX モジュールは ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に ASA CX Management 1/0 アドレスを設定できます。



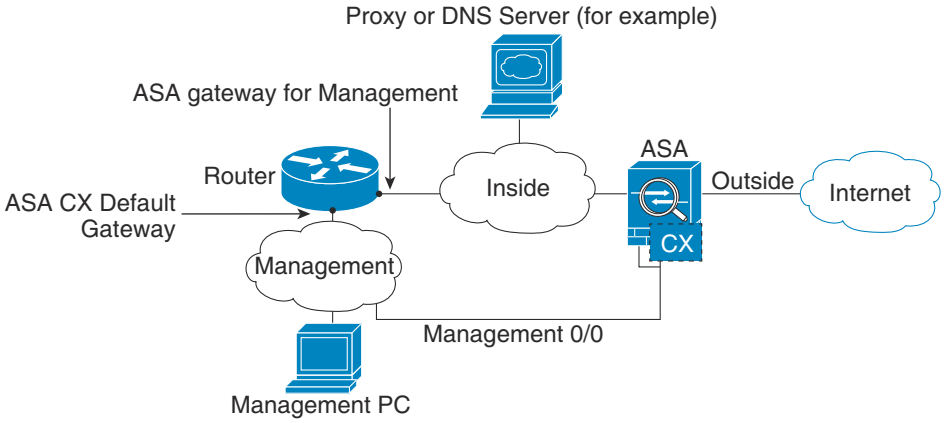
ASA 5512-X ～ ASA 5555-X（ソフトウェア モジュール）

これらのモデルは、ASA CX モジュールをソフトウェア モジュールとして実行し、ASA CX 管理インターフェイスは Management 0/0 インターフェイスを ASA と共有します。初期設定を行うには、SSH で ASA CX のデフォルト IP アドレス（192.168.1.2/24）に接続できます。デフォルト IP アドレスを使用できない場合は、バックプレーンを経由して ASA CX にセッション接続するか、ASDM を使用して SSH を使用できるように管理 IP アドレスを変更します。



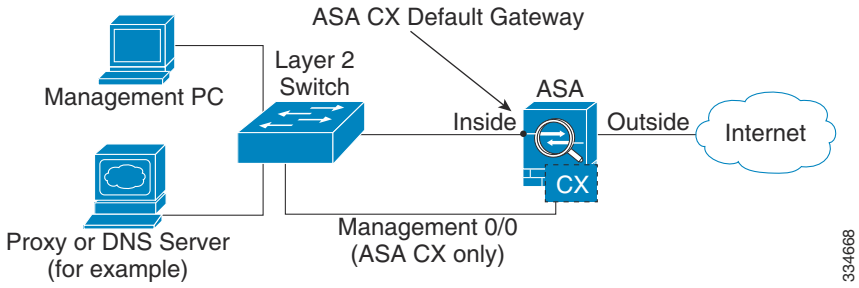
内部ルータがある場合

内部ルータがある場合、Management 0/0 ネットワーク間でルーティングできます。これには、ASA および ASA CX の両方の管理 IP アドレス、およびインターネット アクセス用の内部ネットワークが含まれます。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA 設定の名前を Management 0/0 インターフェイスから削除する場合、そのインターフェイスの ASA CX IP アドレスを引き続き設定できます。ASA CX モジュールは基本的には ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上にあるように ASA CX 管理アドレスを設定 できます。



（注）　Management 0/0 に対して ASA が設定した名前を削除する必要があります。これが ASA で設定されている場合、ASA CX アドレスは、ASA と同じネットワーク上に存在する必要があり、これによって、その他の ASA インターフェイス上ですでに設定されたネットワークはすべて除外されます。名前が設定されていない場合、ASA CX は、任意のネットワーク上（たとえば、ASA 内部ネットワーク）に存在することができます。

（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールのインストールまたはイメージの再作成

ASA CX モジュールとともに ASA を購入した場合、モジュール ソフトウェアおよび必要なソリッド ステート ドライブ（SSD）は事前にインストールされており、すぐに使用できます。既存の ASA に ASA CX を追加する場合、または SSD を交換する必要がある場合は、この手順に従って ASA CX ブート ソフトウェアをインストールし、SSD を分割する必要があります。物理的に SSD を取り付けるには、『ASA Hardware Guide』を参照してください。

最初に ASA CX モジュールをアンインストールする必要がある点を除いて、モジュールのイメージの再作成はこれと同じ手順です。システムのイメージの再作成は、SSD を交換する場合に行います。

（注）　ASA 5585-X ハードウェア モジュールの場合、ASA CX モジュールからイメージをインストールまたはアップグレードする必要があります。詳細は、ASA CX モジュールのマニュアルを参照してください。

はじめる前に

- フラッシュ（disk0）の空き領域には、少なくとも、ブート ソフトウェアのサイズに 3 GB を加えた大きさが必要です。
- マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。
- 実行している可能性があるその他のソフトウェア モジュールをシャットダウンする必要があります。デバイスでは、一度に 1 つのソフトウェア モジュールを実行できます。これは ASA CLI から実行する必要があります。たとえば、次のコマンドは IPS ソフトウェア モジュールをシャットダウンしてアンインストールし、ASA をリロードします。

```
hostname# sw-module module ips shutdown
hostname# sw-module module ips uninstall
hostname# reload
```

（注）　IPS モジュールにトラフィックをリダイレクトするアクティブ サービス ポリシーがある場合、そのポリシーを削除する必要があります。たとえば、ポリシーがグローバル ポリシーの場合、**noservice-policy** *ips_policy* **global** を使用します。ポリシーは、CLI または ASDM を使用して削除できます。

- モジュールのイメージを再作成する場合は、同じシャットダウン/アンインストール コマンドを使用して古いイメージを削除します。たとえば、**sw-module module cxsc uninstall** などです。
- Cisco.com（http://software.cisco.com/download/type.html?mdfid=284325223&flowid=34503）から、ASA CX のブート イメージおよびシステム ソフトウェア パッケージの両方を取得します。

手順

ステップ 1　ブート イメージをデバイスにダウンロードします。システム ソフトウェアは転送しないでください。これは後で SSD にダウンロードされます。次の選択肢があります。

- ASDM：まず、ブート イメージをワークステーションにダウンロードするか、FTP、TFTP、HTTP、HTTPS、SMB、または SCP サーバに配置します。次に、ASDM で [Tools] > [File Management] の順に選択し、[Between Local PC and Flash] または [Between Remote Server and Flashnd] のいずれか該当する [File Transfer] コマンドを選択します。ブート ソフトウェアを ASA 上の disk0 に転送します。
- ASA CLI：まず、ブート イメージを TFTP、FTP、HTTP、または HTTPS サーバに配置し、**copy** コマンドを使用してそのブート イメージをフラッシュにダウンロードします。次の例では TFTP を使用しています。<TFTP Server> をお使いのサーバの IP アドレスまたはホスト名に置き換えてください。

```
ciscoasa# copy tftp://<TFTP SERVER>/asacx-5500x-boot-9.3.1.1-112.img
disk0:/asacx-5500x-boot-9.3.1.1-112.img
```

ステップ 2　ASA CX 管理インターフェイスからアクセス可能な HTTP、HTTPS、または FTP サーバに、Cisco.com から ASA CX システム ソフトウェアをダウンロードします。

ステップ 3　次のコマンドを入力して、ASA disk0 で ASA CX モジュール ブート イメージの場所を設定します。

```
hostname# sw-module module cxsc recover configure image disk0:file_path
```

（注）　「ERROR: Another service (ips) is running, only one service is allowed to run at any time」のようなメッセージが表示される場合、別のソフトウェア モジュールがすでに設定されていることを意味します。このソフトウェア モジュールをシャットダウンして削除し、上の前提条件セクションの説明に従って新しいモジュールをインストールする必要があります。

例：

```
hostname# sw-module module cxsc recover configure image
disk0:asacx-5500x-boot-9.3.1.1-112.img
```

ステップ 4　次のコマンドを入力して、ASA CX ブート イメージをロードします。

```
hostname# sw-module module cxsc recover boot
```

ステップ 5　ASA CX モジュールが起動するまで約 5 分待ってから、現在実行中の ASA CX ブート イメージへのコンソール セッションを開きます。デフォルトのユーザ名は **admin** で、デフォルトのパスワードは **Admin123** です。

```
hostname# session cxsc console
Establishing console session with slot 1
Opening console session with module cxsc.
Connected to module cxsc.Escape character sequence is 'CTRL-SHIFT-6 then x'.
cxsc login: admin
Password: Admin123
```

ヒント　モジュールのブートが完了していない場合は、**session** コマンドが失敗し、ttyS1 経由で接続できないことに関するメッセージが表示されます。しばらく待ってから再試行してください。

ステップ 6　SSD を分割します。

```
asacx-boot> partition
....
Partition Successfully Completed
```

ステップ 7　「基本的な ASA CX 設定値の設定」（P.18-15）に従って、**setup** コマンドを使用して基本的なネットワーク設定を実行し（ASA CX CLI を終了しないでください）、この手順に戻ってソフトウェア イメージをインストールします。

ステップ 8　**system install** コマンドを使用してシステム ソフトウェア イメージをインストールします。

system install [**noconfirm**] *url*

確認メッセージに応答したくない場合は、**noconfirm** オプションを指定します。HTTP、HTTPS、または FTP URL を使用してください。ユーザ名とパスワードが必要な場合は、それらを指定するように求められます。

インストールの終了時にシステムが再起動して、コンソール セッションが閉じられます。アプリケーション コンポーネントのインストールと ASA CX サービスの起動には 10 分以上かかります（**show module cxsc** の出力には、すべてのプロセスが Up と表示されます）。

次のコマンドは asacx-sys-9.3.1.1-112.pkg システム ソフトウェアをインストールします。

```
asacx-boot> system install https://upgrades.example.com/packages/asacx-sys-9.3.1.1-112.pkg

Username: buffy
Password: angelforever
Verifying
Downloading
Extracting
Package Detail
        Description:                 Cisco ASA CX 9.3.1.1-112 System Install
        Requires reboot:             Yes

Do you want to continue with upgrade?[n]: Y
Warning: Please do not interrupt the process or turn off the system.Doing so might leave
system in unusable state.
Upgrading
Stopping all the services ...
Starting upgrade process ...
Reboot is required to complete the upgrade.Press Enter to reboot the system.
```

（ASA 5585-X）ASA CX 管理 IP アドレスの変更

デフォルトの管理 IP アドレス（192.168.8.8）を使用できない場合は、管理 IP アドレスを ASA から設定できます。管理 IP アドレスを設定した後は、初期設定を実行するために SSH を使用して ASA CX モジュールにアクセスできます。

（注）　ソフトウェア モジュールの場合、ASA CX CLI にアクセスして、ASA CLI からのセッション接続によって設定を実行できます。その後、設定の一部として ASA CX 管理 IP アドレスを設定できます。「基本的な ASA CX 設定値の設定」（P.18-15）を参照してください。

ASA で管理 IP アドレスを変更するには、次のいずれかを実行します。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

- CLI で、次のコマンドを使用して ASA CX の管理 IP アドレス、マスク、およびゲートウェイを設定します。

  session 1 do setup host ip *ip_address*/*mask*,*gateway_ip*

  たとえば、**session 1 do setup host ip 10.1.1.2/24,10.1.1.1** と指定します。

- （シングルコンテキスト モードのみ）ASDM で、[Wizards] > [Startup Wizard] を選択して、ウィザードの [ASA CX Basic Configuration] まで進めます。ここで IP アドレス、マスク、およびデフォルト ゲートウェイを設定できます。デフォルトが適していない場合は、他の認証プロキシのポートを設定することもできます。

基本的な ASA CX 設定値の設定

セキュリティ ポリシーを設定する前に、基本的なネットワーク設定およびその他のパラメータを ASA CX モジュール上で設定する必要があります。ASA CX CLI は、これらの設定を行う唯一の方法です。

手順

ステップ 1　次のどちらかを実行します。

- （すべてのモデル）SSH を使用して ASA CX 管理 IP アドレスに接続します。
- （ASA 5512-X ～ ASA 5555-X）ASA からモジュールへのコンソール セッションを開きます。マルチ コンテキスト モードでは、システム実行スペースからセッションを開きます。

  ```
  hostname# session cxsc console
  ```

ステップ 2　ユーザ名 **admin** およびパスワード **Admin123** を使用してログインします。この手順の中で、パスワードを変更します。

ステップ 3　次のコマンドを入力します。

```
asacx> setup
```

例：

```
asacx> setup
Welcome to Cisco Prime Security Manager Setup
[hit Ctrl-C to abort]
Default values are inside [ ]
```

セットアップ ウィザードでは入力が求められます。次の例は、ウィザードでの一般的な順序を示しています。プロンプトで **N** ではなく **Y** を入力した場合は、追加の設定を行うことができます。次に、IPv4 および IPv6 両方のスタティック アドレスの設定例を示します。IPv6 ステートレス自動設定を設定するには、スタティック IPv6 アドレスを設定するかどうかを尋ねるプロンプトで **N** と応答します。

```
Enter a hostname [asacx]: asa-cx-host
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n)[N]: N
Enter an IPv4 address [192.168.8.8]: 10.89.31.65
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 10.89.31.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: Y
Enter an IPv6 address: 2001:DB8:0:CD30::1234/64
```

```
Enter the gateway: 2001:DB8:0:CD30::1
Enter the primary DNS server IP address [ ]: 10.89.47.11
Do you want to configure Secondary DNS Server?(y/n) [N]: N
Do you want to configure Local Domain Name?(y/n) [N] Y
Enter the local domain name: example.com
Do you want to configure Search domains?(y/n) [N] Y
Enter the comma separated list for search domains: example.com
Do you want to enable the NTP service?(y/n) [N]: Y
Enter the NTP servers separated by commas: 1.ntp.example.com, 2.ntp.example.com
```

ステップ 4　最後のプロンプトが完了すると、設定のサマリーが示されます。サマリーに目を通して値が正しいことを確認し、変更した設定を適用するには **Y** を入力します。変更をキャンセルするには **N** を入力します。

例：

```
Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
Done.
Generating self-signed certificate, the web server will be restarted after that
...
Done.
Press ENTER to continue...
asacx>
```

（注）　ホスト名を変更した場合は、ログアウトして再びログインするまでプロンプトに新しい名前は表示されません。

ステップ 5　NTP を使用しない場合は、時刻を設定します。デフォルトのタイム ゾーンは UTC タイム ゾーンです。現在の設定を表示するには、**show time** コマンドを使用します。時間設定を変更するには、次のコマンドを使用できます。

```
asacx> config timezone
asacx> config time
```

ステップ 6　次のコマンドを入力して、admin のパスワードを変更します。

```
asacx> config passwd
```

例：

```
asacx> config passwd
The password must be at least 8 characters long and must contain
at least one uppercase letter (A-Z), at least one lowercase letter
(a-z) and at least one digit (0-9).
Enter password: Farscape1
Confirm password: Farscape1
SUCCESS: Password changed for user admin
```

ステップ 7　**exit** コマンドを入力してログアウトします。

ASA CX モジュールでのセキュリティ ポリシーの設定

ASA CX モジュールでセキュリティ ポリシーを設定するには PRSM を使用します。セキュリティ ポリシーは、モジュールが提供するサービスを制御します。ASA CX CLI、ASA CLI、または ASDM を使用してポリシーを設定できません。

PRSM は ASA CX 設定インターフェイスの名前であり、それとは別に ASA CX デバイス、Cisco Prime Security Manager を設定する製品の名前でもあります。設定インターフェイスへのアクセス方法とその使用方法は同じです。PRSM を使用して ASA CX/PRSM セキュリティ ポリシーを設定する方法の詳細については、ASA CX ユーザ ガイドまたはオンライン ヘルプを参照してください。

PRSM を開くには、Web ブラウザを使用して次の URL を開きます。

https://*management_address*

management_address は ASA CX 管理インターフェイスまたは PRSM サーバの DNS 名または IP アドレスです。たとえば、https://asacx.example.com などです。

認証プロキシ ポートの設定

ASA CX ポリシーでアクティブ認証を使用する場合、ASA は、認証プロキシのポートとしてポート 885 を使用します。885 が許可されない場合は別のポートを設定できますが、デフォルト以外のポートは 1024 より大きい必要があります。認証プロキシの詳細については、「アクティブ認証用の認証プロキシ」（P.18-5）を参照してください。

マルチコンテキスト モードでは、各セキュリティ コンテキスト内のポートを変更します。

認証プロキシ ポートを変更するには、次のコマンドを入力します。

```
cxsc auth-proxy port port
```

たとえば、**cxsc auth-proxy port 5000** などです。

ASA CX モジュールへのトラフィックのリダイレクト

特定のトラフィックを識別するサービス ポリシーを作成して、ASA CX モジュールへのトラフィックをリダイレクトできます。デモンストレーション用にのみ、元のトラフィックが影響を受けることなく、ASA CX モジュールへのトラフィックのコピーを転送するサービス ポリシーに対するモニタ専用モードもイネーブルにできます。

デモンストレーション用のもう 1 つのオプションは、サービス ポリシーの代わりにトラフィック転送をモニタ専用モードで設定することです。トラフィック転送インターフェイスは、ASA をバイパスすることにより、すべてのトラフィックを ASA CX モジュールに直接送信します。

- 「ASA CX サービス ポリシーの作成」（P.18-18）
- 「トラフィック転送インターフェイスの設定（モニタ専用モード）」（P.18-20）

ASA CX サービス ポリシーの作成

特定のトラフィックを識別するサービス ポリシーを作成して、ASA CX モジュールへのトラフィックをリダイレクトします。

（注）　ASA CX は双方向にリダイレクトを行います。したがって、1 つのインターフェイスにサービス ポリシーを設定し、そのインターフェイス上のホストとリダイレクションが設定されていないインターフェイス上のホストが接続されている場合、それらのホスト間の ASA CX ではないインターフェイスから発信されるトラフィックを含めたすべてのトラフィックは ASA CX モジュールに送信されます。ただし、認証プロキシは入力トラフィックのみに適用されるため、ASA は、サービス ポリシーが適用されているインターフェイス上の認証プロキシに対してのみ処理を行います。

はじめる前に

- この手順を使用して ASA で認証プロキシをイネーブルにする場合は、必ず ASA CX モジュールで認証用のディレクトリ レルムも設定してください。詳細については、ASA CX ユーザ ガイドを参照してください。
- （ASA CX と交換した）IPS モジュールにトラフィックをリダイレクトするアクティブ サービス ポリシーがある場合は、ASA CX サービス ポリシーを設定する前にそのポリシーを削除する必要があります。
- ASA ポリシーと ASA CX の両方で必ずモードが一致するように設定する必要があります（両方ともモニタ専用モード、または両方とも通常のインライン モード）。
- マルチコンテキスト モードでは、各セキュリティ コンテキストでこの手順を実行します。
- PRSM をマルチ デバイス モードで使用するときは、以下で説明するようにトラフィックを ASA CX モジュールに送信するための ASA ポリシーの設定を、ASDM または ASA CLI を使用する代わりに PRSM の中で行うことができます。ただし、PRSM では、ASA サービス ポリシーを設定するときにいくつかの制限があります。詳細については、ASA CX のユーザ ガイドを参照してください。

手順

ステップ 1　モジュールに送信するトラフィックを L3/L4 指定するためのクラス マップを作成します。

```
class-map name
match parameter
```

例：

```
hostname(config)# class-map cx_class
hostname(config-cmap)# match access-list cx_traffic
```

モジュールに複数のトラフィック クラスを送信する場合は、セキュリティ ポリシーで使用するための複数のクラス マップを作成できます。

照合ステートメントについては、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。

ステップ 2　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ポリシー マップを追加または編集します。

```
policy-map name
```

例：

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

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3　この手順の最初に作成したクラス マップを指定します。

class *name*

例：

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

ステップ 4　ASA CX モジュールにトラフィックを送信します。

cxsc {**fail-close** | **fail-open**} [**auth-proxy** | **monitor-only**]

それぞれの説明は次のとおりです。

- **fail-close** キーワードを指定すると、ASA CX モジュールが使用できない場合はすべてのトラフィックをブロックするように ASA が設定されます。
- **fail-open** キーワードを指定すると、モジュールが使用できない場合はすべてのトラフィックを検査なしで通過させるように ASA が設定されます。
- **auth-proxy** キーワードを任意で指定すると、アクティブ認証に必要な認証プロキシがイネーブルになります。
- デモンストレーション用にのみ、**monitor-only** を指定して、トラフィックの読み取り専用のコピーを ASA CX モジュールに送信します。すべてのクラスとポリシーは、モニタ専用モード、または通常のインライン モードのいずれか設定する必要があります。同じ ASA で両方のモードを混在させることはできません。

例：

```
hostname(config-pmap-c)# cxsc fail-close auth-proxy
```

ステップ 5　ASA CX トラフィックに複数のクラス マップを作成した場合、ポリシーに別のクラスを指定して **cxsc** リダイレクト アクションを適用できます。

ポリシー マップ内でのクラスの順番が重要であることの詳細については、「サービス ポリシー内の機能照合」（P.1-5）を参照してください。トラフィックを同じアクション タイプの複数のクラス マップに一致させることはできません。

ステップ 6　既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

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

global キーワードはポリシー 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。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。

トラフィック転送インターフェイスの設定（モニタ専用モード）

デモンストレーション用にのみ、すべてのトラフィックが ASA CX モジュールに直接転送されるトラフィック転送インターフェイスを設定できます。正常な ASA CX の動作については、「ASA CX サービス ポリシーの作成」（P.18-18）を参照してください。

詳細については、「モニタ専用モードでのトラフィック転送インターフェイス」（P.18-4）を参照してください。トラフィック転送インターフェイスに固有のガイドラインと制限については「ASA CX のガイドライン」（P.18-6）も参照してください。

はじめる前に

- ASA ポリシーと ASA CX の両方で必ずモードが一致するように設定する必要があります（両方ともモニタ専用モード）。
- マルチコンテキスト モードでは、各セキュリティ コンテキストでこの手順を実行します。

手順

ステップ 1　トラフィック転送に使用する物理インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

interface *physical_interface*

例：

```
hostname(config)# interface gigabitethernet 0/5
```

ステップ 2　インターフェイスに設定された名前を削除します。このインターフェイスがいずれかの ASA 設定で使用されると、その設定は削除されます。指定したインターフェイス上でトラフィック転送を設定できません。

no nameif

ステップ 3　トラフィック転送をイネーブルにします。

traffic-forward cxsc monitor-only

ステップ 4　インターフェイスをイネーブルにします。

no shutdown

追加のインターフェイスについて、この手順を繰り返します。

例

次の例は、GigabitEthernet 0/5 のトラフィック転送インターフェイスを作成します。

```
interface gigabitethernet 0/5
  no nameif
  traffic-forward cxsc monitor-only
  no shutdown
```

ASA CX モジュールの管理

この項には、モジュールの管理に役立つ手順が含まれます。

パスワードのリセット

モジュールのパスワードをデフォルトにリセットできます。ユーザ **admin** のデフォルトのパスワードは **Admin123** です。パスワードをリセットした後は、モジュール アプリケーションを使用してパスワードを独自の値に変更する必要があります。

モジュールのパスワードをリセットすると、モジュールがリブートします。モジュールのリブート中は、サービスを使用できません。

モジュール パスワードをデフォルトにリセットするには、次のいずれかの方法を使用します。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

- （CLI）ハードウェア モジュール（ASA 5585-X）

  hw-module module 1 password-reset

- （CLI）ソフトウェア モジュール（ASA 5512-X ～ ASA 5555-X）

  sw-module module cxsc password-reset

モジュールのリロードまたはリセット

モジュールをリロード、またはリセットしてからリロードするには、ASA CLI で次のいずれかのコマンドを入力します。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

- ハードウェア モジュール（ASA 5585-X）：

  hw-module module 1 {**reload** | **reset**}

- ソフトウェア モジュール（ASA 5512-X ～ ASA 5555-X）：

  sw-module module cxsc {**reload** | **reset**}

モジュールのシャットダウン

モジュール ソフトウェアをシャットダウンするのは、コンフィギュレーション データを失うことなく安全にモジュールの電源をオフにできるように準備するためです。モジュールをグレースフル シャットダウンするには、ASA CLI で次のいずれかのコマンドを入力します。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

（注） ASA をリロードする場合は、モジュールは自動的にはシャットダウンされないので、ASA のリロード前にモジュールをシャットダウンすることを推奨します。

- ハードウェア モジュール（ASA 5585-X）：

  hw-module module 1 shutdown

- ソフトウェア モジュール（ASA 5512-X ～ ASA 5555-X）：

  sw-module module cxsc shutdown

（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュール イメージのアンインストール

ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールできます。マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

手順

ステップ 1　ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールします。

```
hostname# sw-module module cxsc uninstall

Module cxsc will be uninstalled.This will completely remove the disk image
associated with the sw-module including any configuration that existed within it.

Uninstall module cxsc?[confirm]
```

ステップ 2　ASA をリロードします。新しいモジュールをインストールする前に、ASA をリロードする必要があります。

```
hostname# reload
```

（ASA 5512-X ～ ASA 5555-X）ASA からモジュールへのセッション

ASA CX CLI を使用して、基本的なネットワーク設定を構成し、モジュールのトラブルシューティングを行います。

ASA から ASA CX ソフトウェア モジュール CLI にアクセスするには、ASA からセッション接続できます。モジュールへのセッションを開始することも（Telnet を使用）、仮想コンソール セッションを作成することもできます。コンソール セッションは、コントロール プレーンがダウンし、Telnet セッションを確立できない場合に便利です。マルチ コンテキスト モードでは、システム実行スペースからセッションを開きます。

Telnet またはコンソール セッションでは、ユーザ名とパスワードの入力を求められます。**admin** ユーザ名とパスワード（デフォルトは **Admin123**）を入力します。

- Telnet セッション：

  ```
  session cxsc
  ```

  CX ASA CLI で、終了して ASA CLI に戻るには、**exit** コマンドを使用するか **Ctrl+Shift+6、x** を押します。

- コンソール セッション：

  ```
  session cxsc console
  ```

  コンソール セッションからログアウトする唯一の方法は、**Ctrl+Shift+6、x** を押すことです。モジュールからログアウトすると、モジュールのログイン プロンプトに戻ります。

（注）　**session cxsc console** コマンドは、**Ctrl+Shift+6、x** がターミナル サーバのプロンプトに戻るエスケープ シーケンスであるターミナル サーバとともに使用しないでください。**Ctrl+Shift+6、x** は、ASA CX コンソールをエスケープし ASA プロンプトに戻るシーケンスでもあります。したがって、この状況で ASA CX を終了しようとすると、代わりにターミナル サーバ プロンプトに戻ります。ASA にターミナル サーバを再接続すると、ASA CX コンソール セッションがまだアクティブなままであり、ASA プロンプトに戻ることができません。ASA プロンプトにコンソールを戻すには、直接シリアル接続を使用する必要があります。この状況が発生した場合は、コンソール コマンドの代わりに **session cxsc** コマンドを使用します。

ASA CX モジュールのモニタリング

次の各トピックでは、モジュールのモニタリングに関するガイダンスを示します。ASA CX 関連の syslog メッセージについては、syslog メッセージ ガイドを参照してください。ASA CX の syslog メッセージは、メッセージ番号 429001 から始まります。

- 「モジュール ステータスの表示」（P.18-24）
- 「モジュールの統計情報の表示」（P.18-24）
- 「モジュール接続のモニタリング」（P.18-25）

モジュール ステータスの表示

モジュールのステータスを確認するには、次のいずれかのコマンドを入力します。

- **show module** [**1** | **cxsc**] [**details**]

  モジュールのステータスを表示します。ASA CX モジュールに固有のステータスを確認するには、1（ハードウェア モジュールの場合）または cxsc（ソフトウェア モジュールの場合）キーワードを指定します。モジュールを管理するデバイスのアドレスなどの追加情報を取得するには、details キーワードを指定します。

- **show module cxsc recover**

  モジュールのインストール時に使用されたブート イメージの場所を表示します。

次に、ASA CX SSP がインストールされている ASA での **show module** コマンドの出力例を示します。

```
hostname# show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10     JAF1507AMKE
  1 ASA 5585-X CX Security Services Processor-10 ASA5585-SSP-CX10   JAF1510BLSA

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 5475.d05b.1100 to 5475.d05b.110b  1.0          2.0(7)0      100.7(6)78
  1 5475.d05b.2450 to 5475.d05b.245b  1.0          2.0(13)0     0.6.1

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 ASA CX Security Module         Up               0.6.1

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

モジュールの統計情報の表示

cxsc コマンドを含む各サービス ポリシーの統計情報およびステータスを表示するには、**show service-policy cxsc** コマンドを使用します。カウンタをクリアするには、**clear service-policy** を使用します。

次に示す **show service-policy** コマンドの出力例では、認証プロキシがディセーブルになっているときの、ASA CX ポリシーと現在の統計情報およびモジュールのステータスが表示されています。

```
hostname# show service-policy cxsc
Global policy:
Service-policy: global_policy
    Class-map: bypass
      CXSC: card status Up, mode fail-open, auth-proxy disabled
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

次に示す **show service-policy** コマンドの出力例では、認証プロキシがイネーブルになっているときの、ASA CX ポリシーと現在の統計情報およびモジュールのステータスが表示されています。この場合は、proxied カウンタもインクリメントされます。

```
hostname# show service-policy cxsc
Global policy:
Service-policy: pmap
    Class-map: class-default
      Default Queueing      Set connection policy: random-sequence-number disable
        drop 0
      CXSC: card status Up, mode fail-open, auth-proxy enabled
        packet input 7724, packet output 7701, drop 0, reset-drop 0, proxied 10
```

モジュール接続のモニタリング

ASA CX モジュールを通過する接続を表示するには、次のいずれかのコマンドを入力します。

- **show asp table classify domain cxsc**

  トラフィックを ASA CX モジュールに送信するために作成された NP ルールを表示します。

- **show asp table classify domain cxsc-auth-proxy**

  ASA CX モジュールの認証プロキシ用に作成された NP ルールを表示します。次に、コマンドの出力例を示します。ここでは、宛先「port=2000」は **cxsc auth-proxy port 2000** コマンドによって設定された認証プロキシのポートであり、宛先「ip/id=192.168.0.100」は ASA インターフェイスの IP アドレスである 1 つのルールを示します。

  ```
  hostname# show asp table classify domain cxsc-auth-proxy
  Input Table
  in  id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
      hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
      src ip/id=0.0.0.0, mask=0.0.0.0, port=0
      dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
      input_ifc=inside, output_ifc=identity
  ```

- **show asp drop**

  ドロップされたパケットを表示します。ドロップのタイプについては、以下で説明します。

- **show asp event dp-cp cxsc-msg**

  この出力には、dp-cp キューにある ASA CX モジュール メッセージの数が表示されます。ASA CX モジュールからの VPN クエリーのみが dp-cp に送信されます。

- **show conn**

  「X - inspected by service module」フラグを表示することにより、接続がモジュールに転送されているかどうかを示します。

show asp drop コマンドは、ASA CX モジュールに関連する次のドロップ理由を含めることができます。

フレーム ドロップ：

- cxsc-bad-tlv-received：これが発生するのは、ASA が CXSC から受信したパケットにポリシー ID TLV がないときです。非制御パケットのアクション フィールドで Standby Active ビットが設定されていない場合は、この TLV が存在している必要があります。
- cxsc-request：CXSC 上のポリシーが理由で、フレームをドロップするよう CXSC から要求されました。このポリシーによって、CXSC はアクションを Deny Source、Deny Destination、または Deny Pkt に設定します。

- cxsc-fail-close：パケットがドロップされたのは、カードが動作中ではなく、設定済みのポリシーが「fail-close」であったからです（対照的に、「fail-open」の場合は、カードがダウンしていてもパケットの通過が許可されます）。
- cxsc-fail：既存のフローに対する CXSC コンフィギュレーションが削除されており、CXSC で処理できないため、ドロップされます。これが発生することは、ほとんどありません。
- cxsc-malformed-packet：CXSC からのパケットに無効なヘッダーが含まれます。たとえば、ヘッダー長が正しくない可能性があります。

フロードロップ：

- cxsc-request：フローを終了させることを CXSC が要求しました。アクション ビット 0 が設定されます。
- reset-by-cxsc：フローの終了とリセットを CXSC が要求しました。アクション ビット 1 が設定されます。
- cxsc-fail-close：フローが終了させられたのは、カードがダウン状態であり、設定済みのポリシーが「fail-close」であったからです。

認証プロキシでの問題のトラブルシューティング

認証プロキシ機能を使用するときに問題が発生した場合は、次の手順に従って設定および接続のトラブルシューティングを行います。

（注） 2 つの ASA インターフェイス上でホスト間が接続されており、ASA CX のサービス ポリシーがインターフェイスの一方のみについて設定されている場合は、これらのホスト間のすべてのトラフィックが ASA CX モジュールに送信されます。これには、ASA CX インターフェイス以外からのトラフィックも含まれます（この機能は双方向です）。ただし、ASA が認証プロキシを実行するのは、サービス ポリシーが適用されているインターフェイス上のみです。これは、入力のみの機能であるからです。

手順

ステップ 1　コンフィギュレーションを確認します。

- ASA で、**show asp table classify domain cxsc-auth-proxy** コマンドの出力を調べて、ルールがインストールされていて正しいことを確認します。
- PRSM で、ディレクトリのレルムが作成されていて正しいクレデンシャルが指定されていることを確認するとともに、接続をテストして、認証サーバに到達可能であることを確認します。また、認証用のポリシー オブジェクトが設定されていることを確認します。

ステップ 2　**show service-policy cxsc** コマンドの出力を見て、プロキシされたパケットがあるかどうかを調べます。

ステップ 3　バックプレーンに対してパケット キャプチャを実行します（**capture** *name* **interface asa_dataplane**）。そしてトラフィックが正しく設定されたポートにリダイレクトされているかどうかを確認します。**show running-config cxsc** コマンドまたは **show asp table classify domain cxsc-auth-proxy** コマンドを使用して設定されたポートを確認できます。

例

ポート 2000 が一貫して使用されていることの確認

1. 認証プロキシのポートを確認します。

```
hostname# show running-config cxsc
cxsc auth-proxy port 2000
```

2. 認証プロキシ ルールを確認します。

```
hostname# show asp table classify domain cxsc-auth-proxy

Input Table
in  id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=inside, output_ifc=identity
```

3. パケット キャプチャでは、リダイレクト要求が宛先ポート 2000 に送られる必要があります。

ASA CX モジュールの設定例

次の例では、すべての HTTP トラフィックが ASA CX モジュールに誘導され、何らかの理由で ASA CX モジュールに障害が発生した場合はすべての HTTP トラフィックがブロックされます。

```
hostname(config)# access-list ASACX permit tcp any any eq port 80
hostname(config)# class-map my-cx-class
hostname(config-cmap)# match access-list ASACX
hostname(config-cmap)# policy-map my-cx-policy
hostname(config-pmap)# class my-cx-class
hostname(config-pmap-c)# cxsc fail-close auth-proxy
hostname(config-pmap-c)# service-policy my-cx-policy global
```

次の例では、10.1.1.0 ネットワークと 10.2.1.0 ネットワーク宛てのすべての IP トラフィックが ASA CX モジュールに誘導され、何らかの理由で ASA CX モジュールに障害が発生した場合は、すべてのトラフィックの通過が許可されます。

```
hostname(config)# access-list my-cx-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-cx-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-cx-class
hostname(config-cmap)# match access-list my-cx-acl
hostname(config)# class-map my-cx-class2
hostname(config-cmap)# match access-list my-cx-acl2
hostname(config-cmap)# policy-map my-cx-policy
hostname(config-pmap)# class my-cx-class
hostname(config-pmap-c)# cxsc fail-open auth-proxy
hostname(config-pmap)# class my-cx-class2
hostname(config-pmap-c)# cxsc fail-open auth-proxy
hostname(config-pmap-c)# service-policy my-cx-policy interface outside
```

ASA CX モジュールの履歴

機能名	プラットフォームリリース	説明
ASA CX SSP-10 および -20 用の ASA 5585-X（SSP-10 および -20 搭載）サポート	ASA 8.4(4.1) ASA CX 9.0(1)	ASA CX モジュールを使用すると、特定の状況の完全なコンテキストに基づいてセキュリティを強制することができます。このコンテキストには、ユーザのアイデンティティ（誰が）、ユーザがアクセスを試みているアプリケーションまたは Web サイト（何を）、アクセス試行の発生元（どこで）、アクセス試行の時間（いつ）、およびアクセスに使用されているデバイスのプロパティ（どのように）が含まれます。ASA CX モジュールを使用すると、フローの完全なコンテキストを抽出して、細分化したポリシーを適用することができます。たとえば、Facebook へのアクセスを許可するが Facebook でのゲームへのアクセスは禁止する、あるいは企業の機密データベースへのアクセスを財務担当者に許可するが他の社員には禁止するといったことが可能です。 **capture**、**cxsc**、**cxsc auth-proxy**、**debug cxsc**、**hw-module module password-reset**、**hw-module module reload**、**hw-module module reset**、**hw-module module shutdown**、**session do setup host ip**、**session do get-config**、**session do password-reset**、**show asp table classify domain cxsc**、**show asp table classify domain cxsc-auth-proxy**、**show capture**、**show conn**、**show module**、**show service-policy** の各コマンドが導入または変更されました。
ASA CX SSP 用 ASA 5512-X ～ ASA 5555-X サポート	ASA 9.1(1) ASA CX 9.1(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X に対する ASA CX SSP ソフトウェア モジュールのサポートが導入されました。 **session cxsc**、**show module cxsc**、**sw-module cxsc** の各コマンドが変更されました。

機能名	プラットフォームリリース	説明
デモンストレーション用モニタ専用モード	ASA 9.1(2) ASA CX 9.1(2)	デモンストレーション目的でのみ、サービス ポリシー用のモニタリング専用モードをイネーブルにすることができ、元のトラフィックに影響を与えずに、トラフィックのコピーを ASA CX モジュールに転送することができます。 デモンストレーション用のもう 1 つのオプションは、サービス ポリシーの代わりにトラフィック転送をモニタ専用モードで設定することです。トラフィック転送インターフェイスは、ASA をバイパスすることにより、すべてのトラフィックを ASA CX モジュールに直接送信します。 **cxsc {fail-close | fail-open} monitor-only**、**traffic-forward cxsc monitor-only** の各コマンドが変更または導入されました。
ASA CX モジュールに対する NAT 64 のサポート	ASA 9.1(2) ASA CX 9.1(2)	ASA CX モジュールとともに NAT 64 を使用できるようになりました。 変更されたコマンドはありません。
ASA CX SSP-40 および -60 用の ASA 5585-X（SSP-40 および -60 搭載）サポート	ASA 9.1(3) ASA CX 9.2(1)	ASA CX SSP-40 および -60 モジュールは、SSP-40 および -60 搭載の ASA 5585-X と一致するレベルで使用できます。 変更されたコマンドはありません。
ASA CX モジュールのマルチ コンテキスト モードのサポート	ASA 9.1(3) ASA CX 9.2(1)	ASA でコンテキストごとに ASA CX サービス ポリシーを設定できます。 **（注）** コンテキストごとに ASA サービス ポリシーを設定できますが、（PRSM で設定されている）ASA CX モジュール自体はシングル コンテキスト モードのデバイスです。つまり、ASA から着信するコンテキスト固有のトラフィックは共通の ASA CX ポリシーと照合されます。 変更されたコマンドはありません。

機能名	プラットフォームリリース	説明
ASA CX バックプレーンでキャプチャされたパケットのフィルタリング	ASA 9.1(3) ASA CX 9.2(1)	**match** または **access-list** キーワードを **capture interface asa_dataplane** コマンドと共に使用して、ASA CX バックプレーンでキャプチャされたパケットをフィルタリングできます。 ASA CX モジュールに固有の制御トラフィックは、access-list または match フィルタリングの影響を受けません。ASA はすべての制御トラフィックをキャプチャします。 マルチ コンテキスト モードでは、コンテキストごとにパケット キャプチャを設定します。マルチ コンテキスト モードのすべての制御トラフィックが送信されるのはシステム実行スペースだけであることに注意してください。access-list または match を使用して制御トラフィックのフィルタリングを行うことができないため、これらのオプションはシステム実行スペースでは使用できません。 **capture interface asa_dataplane** コマンドが変更されました。

ASA IPS モジュール

この章では、ASA IPS モジュールを設定する方法について説明します。ASA IPS モジュールは、ご使用の ASA モデルに応じて、ハードウェア モジュールである場合とソフトウェア モジュールである場合があります。ASA モデルごとにサポートされている ASA IPS モジュールのリストについては、次の URL にある『*Cisco ASA Compatibility Matrix*』を参照してください。

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

ASA IPS モジュールに関する情報

ASA IPS モジュールは、高度な IPS ソフトウェアを実行します。このソフトウェアによる、予防的なフル機能の侵入防御サービスは、ワームやネットワーク ウイルスなどの悪意のあるトラフィックがネットワークに影響を与える前に、これらを阻止します。

ASA IPS モジュールがどのように ASA と連携するか

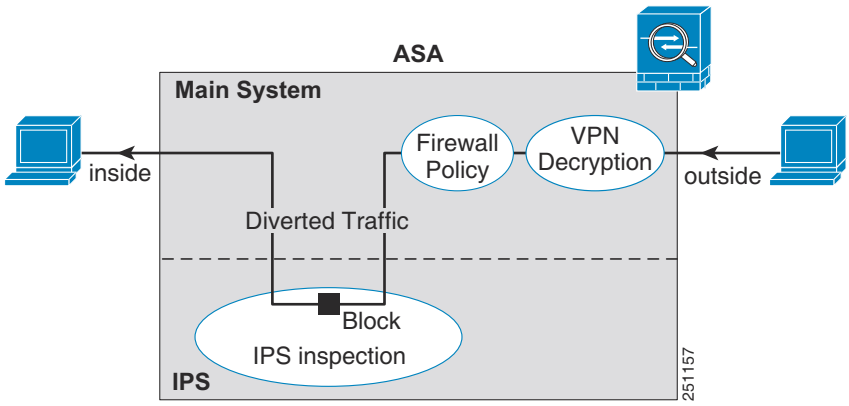
ASA IPS モジュールは、ASA とは別のアプリケーションを実行します。ASA IPS モジュールに外部管理インターフェイスが搭載されている場合は、ASA IPS モジュールに直接接続することができます。管理インターフェイスが搭載されていない場合は、ASA インターフェイスを介して ASA IPS モジュールに接続できます。ASA 5585-X 上の ASA IPS SSP にはデータ インターフェイスが含まれます。このインターフェイスによって、ASA のポート密度が増加します。ただし、ASA の全体的なスループットは増加しません。

トラフィックは、ファイアウォール検査を通過してから ASA IPS モジュールへ転送されます。ASA で IPS インスペクション対象として指定されたトラフィックは、次に示すように ASA および ASA IPS モジュールを通過します。**注**：この例は「インライン モード」の場合です。ASA がトラフィックのコピーを ASA IPS モジュールに送信するだけである「無差別モード」については、「動作モード」（P.19-3）を参照してください。

1. トラフィックは ASA に入ります。
2. 着信 VPN トラフィックが復号化されます。
3. ファイアウォール ポリシーが適用されます。
4. トラフィックが ASA IPS モジュールに送信されます。
5. ASA IPS モジュールはセキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
6. 有効なトラフィックが ASA に返送されます。ASA IPS モジュールは、セキュリティ ポリシーに従ってトラフィックをブロックすることがあり、ブロックされたトラフィックは渡されません。
7. 発信 VPN トラフィックが暗号化されます。
8. トラフィックが ASA から出ます。

図 19-1 は、ASA IPS モジュールをインライン モードで実行している場合のトラフィック フローを示します。この例では、ASA IPS モジュールが攻撃と見なしたトラフィックは自動的にブロックされます。それ以外のトラフィックは、ASA を通って転送されます。

図 19-1　ASA での ASA IPS モジュールのトラフィック フロー：インライン モード

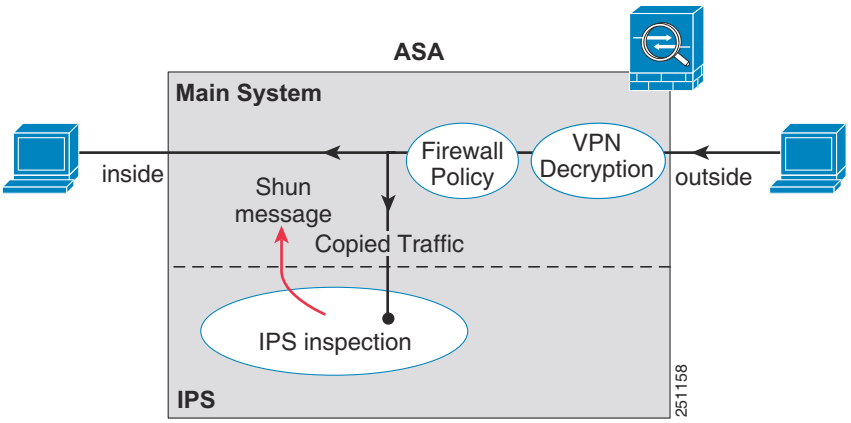


動作モード

次のいずれかのモードを使用して、トラフィックを ASA IPS モジュールに送信できます。

- インライン モード：このモードでは、ASA IPS モジュールはトラフィック フローの中に直接配置されます（図 19-1 を参照）。IPS インスペクション対象として指定されたトラフィックは、ASA IPS モジュールに渡されて検査を受けてからでなければ、ASA を通過することはできません。インスペクション対象と識別されたすべてのパケットは通過する前に分析されるため、このモードは最もセキュアです。また、ASA IPS モジュールはパケット単位でブロッキング ポリシーを実装できます。ただし、このモードは、スループットに影響を与えることがあります。
- 無差別モード：このモードでは、トラフィックの複製ストリームが ASA IPS モジュールに送信されます。このモードは安全性では劣りますが、トラフィックのスループットにほとんど影響を与えません。インライン モードとは異なり、無差別モードでは、ASA IPS モジュールがトラフィックをブロックできるのは、ASA にトラフィックの排除を指示するか、ASA 上の接続をリセットした場合だけです。また、ASA IPS モジュールがトラフィックを分析している間は、ASA IPS モジュールがそのトラフィックを排除できるようになる前に、少量のトラフィックが ASA を通過することがあります。図 19-2 は、無差別モードでの ASA IPS モジュールを示します。この例では、ASA IPS モジュールは脅威と見なしたトラフィックについての排除メッセージを ASA に送信します。

図 19-2　ASA での ASA IPS モジュールのトラフィック フロー：無差別モード



仮想センサーの使用

IPS ソフトウェアのバージョン 6.0 以降を実行している ASA IPS モジュールでは、複数の仮想センサーを実行できます。つまり、ASA IPS モジュールで複数のセキュリティ ポリシーを設定することができます。各 ASA セキュリティ コンテキストまたはシングル モードの ASA を 1 つまたは複数の仮想センサーに割り当てる、または複数のセキュリティ コンテキストを同じ仮想センサーに割り当てることができます。仮想センターの詳細（サポートされている最大センサー数など）については、IPS のマニュアルを参照してください。

図 19-3 では、1 つのセキュリティ コンテキストと 1 つの仮想センター（インライン モード）がペアになり、2 つのセキュリティ コンテキストが同じ仮想センサーを共有しています。

図 19-3　セキュリティ コンテキストと仮想センサー

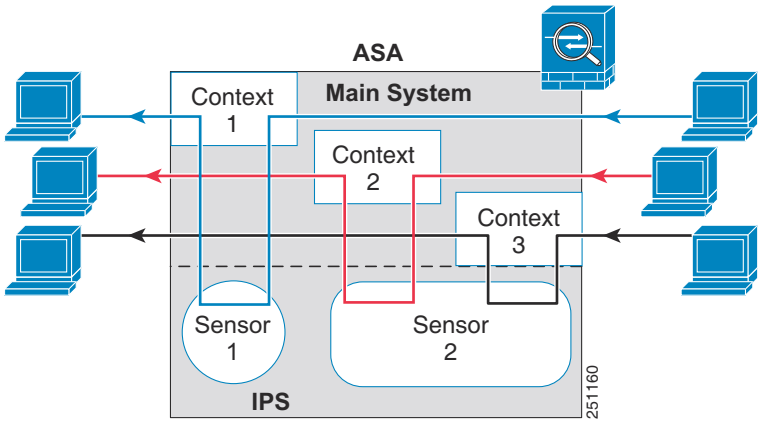
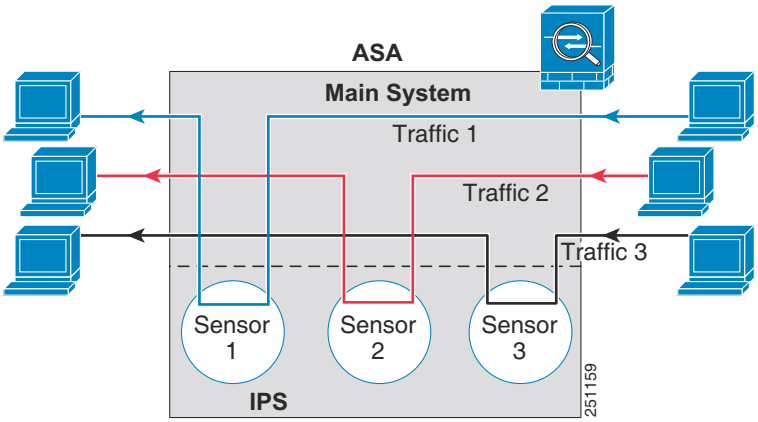


図 19-4 では、シングル モードの ASA が複数の仮想センサー（インライン モード）とペアになっています。定義されている各トラフィック フローは異なるセンサーに進みます。

図 19-4　複数の仮想センサーがあるシングル モードの ASA



管理アクセスに関する情報

次の方法を使用して、IPS アプリケーションを管理できます。

- ASA からモジュールへのセッション接続：ASA に CLI アクセスが可能な場合は、モジュールにセッション接続し、そのモジュール CLI にアクセスできます。「ASA からモジュールへのセッションの開始」（P.19-10）を参照してください。
- ASDM または SSH を使用して IPS 管理インターフェイスに接続する：ASDM を ASA から起動すると、IPS アプリケーションを設定するために管理ステーションがモジュール管理インターフェイスに接続します。SSH の場合、モジュール管理インターフェイスでモジュール CLI に直接アクセスできます（Telnet アクセスでは、モジュール アプリケーションで追加の設定が必要になります）。モジュール管理インターフェイスは、syslog メッセージの送信や、シグニチャ データベースの更新などのモジュール アプリケーションの更新に使用できます。

管理インターフェイスについては、次の情報を参照してください。

- ASA 5585-X：IPS 管理インターフェイスは、独立した外部ギガビット イーサネット インターフェイスです。
- ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X：これらのモデルは、ASA IPS モジュールをソフトウェア モジュールとして実行します。IPS 管理インターフェイスは、Management 0/0 インターフェイスを ASA と共有します。ASA と ASA IPS モジュールのそれぞれに別の MAC アドレスと IP アドレスがサポートされます。IPS IP アドレスの設定は、IPS オペレーティング システム内で（CLI または ASDM を使用して）実行する必要があります。ただし、物理特性（インターフェイスのイネーブル化など）は、ASA 上で設定されます。ASA インターフェイス コンフィギュレーションを削除して（特にインターフェイス名）、このインターフェイスを IPS 専用インターフェイスとすることができます。このインターフェイスは管理専用です。

ASA IPS モジュールのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
ASA 5512-X、 ASA 5515-X、 ASA 5525-X、 ASA 5545-X、 ASA 5555-X	IPS モジュールのライセンス **（注）** IPS モジュール ライセンスがあると、ASA で IPS ソフトウェア モジュールを実行することができます。別の IPS シグニチャ サブスクリプションを購入する必要があります。フェールオーバー用に、各ユニットのサブスクリプションを購入します。IPS シグニチャのサポートを受けるには、IPS が事前インストールされた ASA を購入する必要があります（製品番号に「IPS」が含まれている必要があります）。結合されたフェールオーバー クラスタ ライセンスでは、非 IPS ユニットと IPS ユニットをペアにすることはできません。たとえば ASA 5515-X の IPS 版（製品番号 ASA5515-IPS-K9）を購入し、非 IPS 版（製品番号 ASA5515-K9）を使用してフェールオーバー ペアを作成しようとしている場合は、他のユニットから IPS モジュール ライセンスを継承した場合であっても、ASA5515-K9 ユニットの IPS シグニチャ アップデートを取得できません。
ASA 5585-X	基本ライセンス
他のすべてのモデル	サポートしない

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。

モデルのガイドライン

- どのモデルがどのモジュールをサポートするかの詳細については、次の URL にある『*Cisco ASA Compatibility Matrix*』を参照してください。

  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

その他のガイドライン

- ASA と IPS モジュールの総スループットは、ASA 単独のスループットよりも低くなります。
  - ASA 5512-X ～ ASA 5555-X：http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/qa_c67-700608.html を参照
  - ASA 5585-X：http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/qa_c67-617018.html を参照
- モジュールにインストールされているソフトウェアのタイプの変更はできません。つまり、購入した ASA IPS モジュールに、後で別のソフトウェアをインストールすることはできません。

デフォルト設定

表 19-1 に、ASA IPS モジュールのデフォルト設定値を示します。

表 19-1　デフォルトのネットワーク パラメータ

パラメータ	デフォルト
管理 IP アドレス	192.168.1.2/24
ゲートウェイ	192.168.1.1/24（デフォルトの ASA 管理 IP アドレス）
ユーザ名	cisco
パスワード	cisco

（注）　ASA のデフォルトの管理 IP アドレスは 192.168.1.1/24 です。

ASA IPS モジュールの設定

この項では、ASA IPS モジュールを設定する方法について説明します。

- 「ASA IPS モジュールのタスク フロー」（P.19-7）
- 「ASA IPS 管理インターフェイスの接続」（P.19-7）
- 「ASA からモジュールへのセッションの開始」（P.19-10）
- 「IPS モジュールの基本的なネットワーク設定値の設定」（P.19-13）
- 「（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールの起動」（P.19-11）
- 「ASA IPS モジュールでのセキュリティ ポリシーの設定」（P.19-13）
- 「セキュリティ コンテキストへの仮想センサーの割り当て」（P.19-14）
- 「ASA IPS モジュールへのトラフィックの誘導」（P.19-16）

ASA IPS モジュールのタスク フロー

ASA IPS モジュールの設定プロセスでは、IPS セキュリティ ポリシーを ASA IPS モジュール上で設定してから、トラフィックを ASA IPS モジュールに送信するように ASA を設定します。ASA IPS モジュールを設定するには、次の手順に従います。

ステップ 1　ASA IPS 管理インターフェイスにケーブル接続します。「ASA IPS 管理インターフェイスの接続」（P.19-7）を参照してください。

ステップ 2　モジュールへのセッションを開始します。バックプレーンを介して IPS CLI にアクセスします。「ASA からモジュールへのセッションの開始」（P.19-10）を参照してください。

ステップ 3　（ASA 5512-X ～ ASA 5555-X、必須の可能性があります）ソフトウェア モジュールをインストールします。「（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールの起動」（P.19-11）を参照してください。

ステップ 4　ASA は、IPS モジュールの基本的なネットワーク設定を設定します。「IPS モジュールの基本的なネットワーク設定値の設定」（P.19-13）を参照してください。

ステップ 5　モジュール上で、インスペクションと保護のポリシーを設定します。このポリシーによって、トラフィックの検査方法と侵入検出時の処理が決まります。「ASA IPS モジュールでのセキュリティ ポリシーの設定」（P.19-13）を参照してください。

ステップ 6　（任意）マルチ コンテキスト モードの ASA で、各コンテキストで使用可能な IPS 仮想センサーを指定します（仮想センサーが設定されている場合）。「セキュリティ コンテキストへの仮想センサーの割り当て」（P.19-14）を参照してください。

ステップ 7　ASA で、ASA IPS モジュールに誘導するトラフィックを指定します。「ASA IPS モジュールへのトラフィックの誘導」（P.19-16）を参照してください。

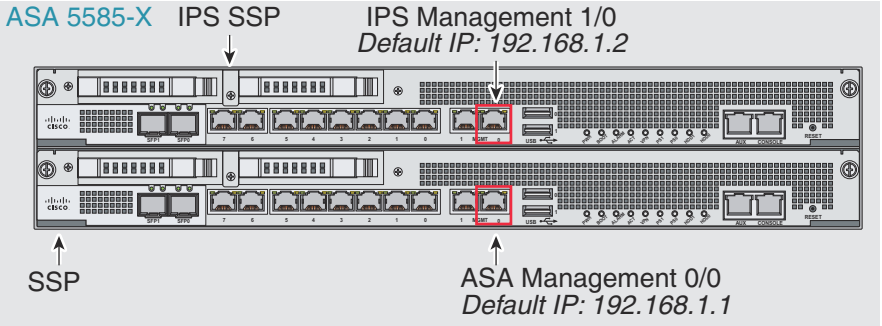
ASA IPS 管理インターフェイスの接続

IPS モジュールへの管理アクセスを提供する以外に、IPS 管理インターフェイスは、HTTP プロキシ サーバまたは DNS サーバおよびインターネットへのアクセスを必要とします。グローバル相関、シグニチャ アップデートおよびライセンス要求をダウンロードできるようにするためです。この項では、推奨されるネットワーク コンフィギュレーションを示します。実際のネットワークでは、異なる可能性があります。

- 「ASA 5585-X（ハードウェア モジュール）」（P.19-8）
- 「ASA 5512-X ～ ASA 5555-X（ソフトウェア モジュール）」（P.19-9）

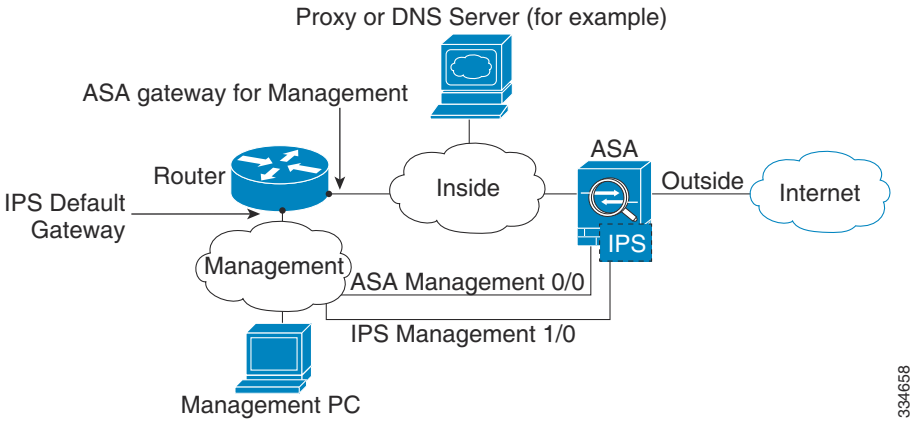
ASA 5585-X（ハードウェア モジュール）

IPS モジュールには、ASA とは別の管理インターフェイスが含まれます。



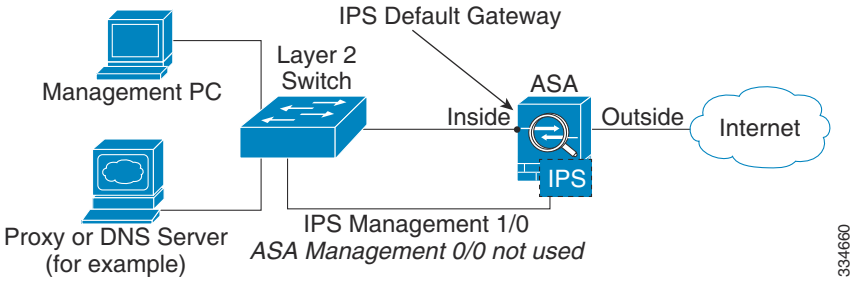
内部ルータがある場合

内部ルータがある場合は、管理ネットワーク（これには ASA Management 0/0 インターフェイスおよび IPS Management 1/0 インターフェイスの両方を含めることができます）と ASA 内部ネットワークとの間でルーティングできます。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



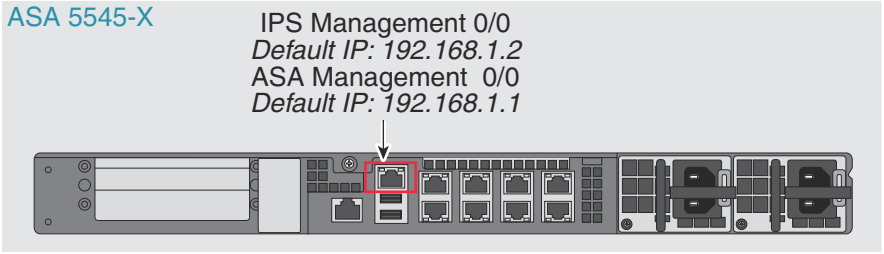
内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません（仮に持つとすれば、内部ルータがネットワーク間のルーティングを行う必要があります）。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。IPS モジュールは ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に IPS Management 1/0 アドレスを設定できます。



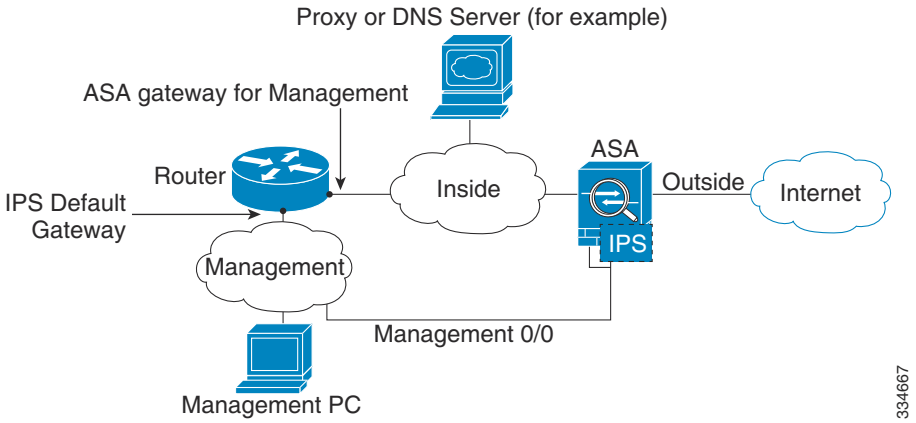
ASA 5512-X ～ ASA 5555-X（ソフトウェア モジュール）

これらのモデルは、IPS モジュールをソフトウェア モジュールとして実行し、IPS 管理インターフェイスは Management 0/0 インターフェイスを ASA と共有します。



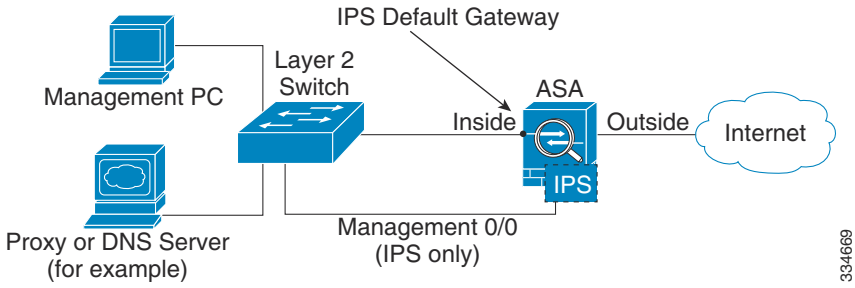
内部ルータがある場合

内部ルータがある場合は、Management 0/0 ネットワーク（これには ASA および IPS の両方の管理 IP アドレスとが含まれます）と内部ネットワークとの間でルーティングできます。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA で設定された名前を Management 0/0 インターフェイスから削除した場合も、そのインターフェイスの IPS IP アドレスを設定できます。IPS モジュールは実質的に ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に IPS 管理アドレスを設定できます。



（注）　Management 0/0 に対して ASA で設定された名前を削除する必要があります。この名前が ASA 上で設定されている場合は、IPS のアドレスは ASA と同じネットワーク上にあることが必要になり、その結果、他の ASA インターフェイス上ですでに設定されたネットワークが除外されます。名前が設定されていない場合は、IPS のアドレスが存在するのはどのネットワークでも、たとえば、ASA 内部ネットワークでもかまいません。

次の作業

- 基本的なネットワーク設定を設定します。「IPS モジュールの基本的なネットワーク設定値の設定」（P.19-13）を参照してください。

ASA からモジュールへのセッションの開始

IPS モジュール CLI に ASA からアクセスするには、ASA からセッションを開始します。ソフトウェア モジュールの場合は、モジュールへのセッションを開始することも（Telnet を使用）、仮想コンソール セッションを作成することもできます。コンソール セッションは、コントロール プレーンがダウンし、Telnet セッションを確立できない場合に便利です。

手順の詳細

コマンド	目的

Telnet セッション。
ハードウェア モジュール（例：ASA 5585-X）の場合：
session 1
ソフトウェア モジュール（例：ASA 5545-X）の場合：
session ips
 	
例：
`hostname# session 1`
 	
`Opening command session with slot 1.`
`Connected to slot 1.Escape character sequence is 'CTRL-^X'.`
 	
`sensor login: cisco`
`Password: cisco`
	Telnet を使用してモジュールにアクセスします。ユーザ名とパスワードの入力を求められます。デフォルトのユーザ名は **cisco**、デフォルトのパスワードは **cisco** です。
	（注） 初めてモジュールにログインしたときに、デフォルトのパスワードの変更を要求するプロンプトが表示されます。パスワードは 8 文字以上で、辞書に載っていない単語にする必要があります。

コンソール セッション（ソフトウェア モジュールのみ）。
session ips console
 	
例：
`hostname# session ips console`
 	
`Establishing console session with slot 1`
`Opening console session with module ips.`
`Connected to module ips.Escape character sequence is 'CTRL-SHIFT-6 then x'.`
 	
`sensor login: cisco`
`Password: cisco`
	モジュール コンソールにアクセスします。ユーザ名とパスワードの入力を求められます。デフォルトのユーザ名は **cisco**、デフォルトのパスワードは **cisco** です。
	（注） このコマンドは、Ctrl+Shift+6、x がターミナル サーバのプロンプトに戻るエスケープ シーケンスであるターミナル サーバとともに使用しないでください。Ctrl+Shift+6、x は、IPS コンソールをエスケープし ASA プロンプトに戻るシーケンスでもあります。したがって、この状況で IPS を終了しようとすると、代わりにターミナル サーバ プロンプトに戻ります。ASA にターミナル サーバを再接続すると、IPS コンソール セッションがまだアクティブなままであり、ASA プロンプトに戻ることができません。ASA プロンプトにコンソールを戻すには、直接シリアル接続を使用する必要があります。
	
	代わりに **session ips** コマンドを使用します。

（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールの起動

ASA には一般的に、IPS モジュール ソフトウェアが付属しており、Disk0 に収録されています。このモジュールが実行されていない場合や、IPS モジュールを既存の ASA に追加する場合は、モジュール ソフトウェアを起動する必要があります。モジュールが実行中か不明な場合は、セッションを開始できません。

手順の詳細

ステップ 1　次のどちらかを実行します。

- プリインストール済みの IPS を搭載する新しい ASA : フラッシュ メモリで IPS モジュール ソフトウェアのファイル名を表示するには、次のコマンドを入力します。

  ```
  hostname# dir disk0:
  ```

  たとえば、IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip のようなファイル名を検索します。ファイル名をメモしておきます。このファイル名は、この手順で後ほど必要になります。

- 既存の ASA に新しい IPS をインストールする場合 : IPS ソフトウェアを Cisco.com から TFTP サーバ にダウンロードします。Cisco.com のログインをお持ちの場合は、次の Web サイトからソフトウェアを入手できます。

  http://www.cisco.com/cisco/software/navigator.html?mdfid=282164240

  ASA にソフトウェアをコピーします。

  ```
  hostname# copy tftp://server/file_path disk0:/file_path
  ```

  他のダウンロード サーバ タイプの場合は、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。

  ファイル名をメモしておきます。このファイル名は、この手順で後ほど必要になります。

ステップ 2　disk0 の IPS モジュール ソフトウェアの場所を設定するには、次のコマンドを入力します。

```
hostname# sw-module module ips recover configure image disk0:file_path
```

たとえば、この例のステップ 1 のファイル名を使用するには、次のとおりに入力します。

```
hostname# sw-module module ips recover configure image
disk0:IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip
```

ステップ 3　IPS モジュール ソフトウェアをインストールし、ロードするには、次のコマンドを入力します。

```
hostname# sw-module module ips recover boot
```

ステップ 4　イメージ転送とモジュール再起動プロセスの進行状況を確認するには、次のコマンドを入力します。

```
hostname# show module ips details
```

出力の [Status] フィールドが、モジュールの動作ステータスを示します。モジュールの動作ステータスは、通常は「Up」と表示されます。ASA によってアプリケーション イメージがモジュールに転送されているときは、出力の [Status] フィールドには [Recover] と表示されます。ASA によるイメージの転送が完了してモジュールが再起動されると、新たに転送されたイメージが実行されます。

IPS モジュールの基本的なネットワーク設定値の設定

マルチ コンテキスト モードでは、ASA からモジュールへのセッションを開始し、**setup** コマンドを使用して基本設定を行います。

（注）（ASA 5512-X ～ ASA 5555-X）モジュールへのセッションを開始できない場合は、IPS モジュールが動作していません。「（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールの起動」（P.19-11）を参照し、モジュールをインストールした後でこの手順をもう一度実行してください。

手順の詳細

	コマンド	目的
ステップ 1	「ASA からモジュールへのセッションの開始」（P.19-10）に従って、IPS モジュールへのセッションを開始します。	
ステップ 2	セットアップ **例：** `sensor# setup`	ASA IPS モジュールの初期設定用のセットアップ ユーティリティを実行します。基本設定を求めるプロンプトが表示されます。デフォルト ゲートウェイについては、アップストリーム ルータの IP アドレスを指定します。ネットワークの要件については、「ASA IPS 管理インターフェイスの接続」（P.19-7）を参照してください。ASA の管理 IP アドレスのデフォルト設定は機能しません。

ASA IPS モジュールでのセキュリティ ポリシーの設定

この項では、ASA IPS モジュール アプリケーションを設定する方法について説明します。

手順の詳細

ステップ 1　次のいずれかの方法を使用して ASA IPS モジュール CLI にアクセスします。

- ASA から ASA IPS モジュールへのセッションを開始します。「ASA からモジュールへのセッションの開始」（P.19-10）を参照してください。
- SSH を使用して IPS 管理インターフェイスに接続します。変更していなければ、デフォルトの管理 IP アドレスは 192.168.1.2 です。デフォルトのユーザ名は **cisco**、デフォルトのパスワードは **cisco** です。管理インターフェイスの詳細については、「管理アクセスに関する情報」（P.19-4）を参照してください。

ステップ 2　IPS のマニュアルに従って IPS セキュリティ ポリシーを設定します。

IPS に関連するすべてのドキュメントを利用するには、http://www.cisco.com/c/en/us/support/security/ips-4200-series-sensors/products-documentation-roadmaps-list.html にアクセスします。

ステップ 3　仮想センサーを設定する場合は、センサーの 1 つをデフォルトとして指定します。ASA のコンフィギュレーションで仮想センサー名が指定されていない場合は、デフォルト センサーが使用されます。

ステップ 4　ASA IPS モジュールの設定が完了したら、次のコマンドを入力して IPS ソフトウェアを終了します。

```
sensor# exit
```

ASA IPS モジュールへのセッションを ASA から開始した場合は、ASA のプロンプトに戻ります。

次の作業

- マルチ コンテキスト モードの ASA の場合は、「セキュリティ コンテキストへの仮想センサーの割り当て」（P.19-14）を参照してください。
- シングル コンテキスト モードの ASA の場合は、「ASA IPS モジュールへのトラフィックの誘導」（P.19-16）を参照してください。

セキュリティ コンテキストへの仮想センサーの割り当て

ASA がマルチ コンテキスト モードにある場合、1 つまたは複数の IPS 仮想センサーを各コンテキストに割り当てることができます。このようにすると、トラフィックを ASA IPS モジュールに送信するようにコンテキストを設定するときに、そのコンテキストに割り当てられているセンサーを指定できます。そのコンテキストに割り当てられていないセンサーを指定することはできません。コンテキストにセンサーを割り当てない場合は、ASA IPS モジュール上で設定されているデフォルト センサーが使用されます。同じセンサーを複数のコンテキストに割り当てることができます。

（注）　仮想センサーを使用するためにマルチ コンテキスト モードを開始する必要はありません。シングル モードでトラフィック フローごとに異なるセンサーを使用できます。

前提条件

コンテキストの設定の詳細については、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。

手順の詳細

	コマンド	目的
ステップ1	**context** *name* **例：** hostname(config)# context admin hostname(config-ctx)#	設定するコンテキストを識別します。システム実行スペースにこのコマンドを入力します。
ステップ2	**allocate-ips** *sensor_name* [*mapped_name*] [**default**] **例：** hostname(config-ctx)# allocate-ips sensor1 highsec	コンテキストに割り当てるセンサーごとに、このコマンドを入力します。 *sensor _name* 引数は、ASA IPS モジュール上で設定されているセンサー名です。ASA IPS モジュール上で設定されているセンサーを表示するには、**allocate-ips ?** と入力します。使用可能なすべてのセンサーが表示されます。**show ips** コマンドを入力することもできます。システム実行スペースで **show ips** コマンドを入力すると、使用可能なすべてのセンサーが表示されます。このコマンドをコンテキストで入力すると、そのコンテキストにすでに割り当てられているセンサーが表示されます。ASA IPS モジュールにまだ存在しないセンサー名を指定すると、エラーになりますが、**allocate-ips** コマンドはそのまま入力されます。その名前のセンサーが ASA IPS モジュール上で作成されるまで、コンテキストはセンサーがダウンしていると見なします。 *mapped_name* 引数を、実際のセンサー名の代わりにコンテキストで使用可能なセンサー名のエイリアスとして使用します。マッピング名を指定しない場合、センサー名がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているセンサーをコンテキスト管理者に知らせない場合があります。または、コンテキスト コンフィギュレーションを一般化する場合もあります。たとえば、すべてのコンテキストで「sensor1」と「sensor2」という名前のセンサーが使用されるようにする場合に、コンテキスト A ではセンサー「highsec」と「lowsec」を sensor1 と sensor2 にマッピングし、コンテキスト B ではセンサー「medsec」と「lowsec」を sensor1 と sensor2 にマッピングします。 **default** キーワードは、コンテキストごとに 1 つのセンサーをデフォルトのセンサーとして設定します。コンテキスト コンフィギュレーションでセンサー名を指定しない場合、コンテキストではこのデフォルト センサーが使用されます。コンテキストごとに設定できるデフォルト センサーは 1 つのみです。デフォルト センサーを変更する場合は、**no allocate-ips** *sensor_name* コマンドを入力して現在のデフォルト センサーを削除してから、新しいデフォルト センサーを割り当てます。デフォルトとして指定されたセンサーがなく、コンテキスト コンフィギュレーションにもセンサー名が含まれていない場合は、ASA IPS モジュールで指定されたデフォルト センサーがトラフィックに使用されます。
ステップ3	**changeto context** *context_name* **例：** hostname# changeto context customer1 hostname/customer1#	「ASA IPS モジュールへのトラフィックの誘導」（P.19-16）での説明に従って、IPS セキュリティ ポリシーを設定するには各コンテキストに切り替えます。

例

次に、sensor1 と sensor2 をコンテキスト A に、sensor1 と sensor3 をコンテキスト B に割り当てる例を示します。両方のコンテキストで、センサー名を「ips1」と「ips2」にマッピングしています。コンテキスト A では、sensor1 がデフォルト センサーとして設定されていますが、コンテキスト B ではデフォルトは設定されていないため、ASA IPS モジュールで設定されているデフォルトが使用されます。

```
hostname(config-ctx)# context A
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1 default
hostname(config-ctx)# allocate-ips sensor2 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1
hostname(config-ctx)# allocate-ips sensor3 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver

hostname(config-ctx)# changeto context A
...
```

次の作業

IPS セキュリティ ポリシーを設定するには各コンテキストに切り替えます（「ASA IPS モジュールへのトラフィックの誘導」（P.19-16）で説明されています）。

ASA IPS モジュールへのトラフィックの誘導

この項では、ASA から ASA IPS モジュールに誘導するトラフィックを指定します。

前提条件

マルチ コンテキスト モードでは、各コンテキスト実行スペースでこれらの手順を実行します。コンテキストに変更するには、**changeto context** *context_name* コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	**class-map** *name* **例：** `hostname(config)# class-map ips_class`	ASA IPS モジュールに送信するトラフィックを指定するためのクラス マップを作成します。 ASA IPS モジュールに複数のトラフィック クラスを送信する場合は、セキュリティ ポリシーで使用するための複数のクラス マップを作成できます。
ステップ 2	**match** *parameter* **例：** `hostname(config-cmap)# match access-list ips_traffic`	クラス マップのトラフィックを指定します。詳細については、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。
ステップ 3	**policy-map** *name* **例：** `hostname(config)# policy-map ips_policy`	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ポリシー マップを追加または編集します。
ステップ 4	**class** *name* **例：** `hostname(config-pmap)# class ips_class`	ステップ 1 で作成したクラス マップを識別します。

	コマンド	目的
ステップ 5	**ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}] **例：** `hostname(config-pmap-c)# ips promiscuous fail-close`	トラフィックが ASA IPS モジュールに送信されるように指定します。 **inline** キーワードと **promiscuous** キーワードは、ASA IPS モジュールの動作モードを制御します。詳細については、「動作モード」（P.19-3）を参照してください。 **fail-close** キーワードを指定すると、ASA IPS モジュールが使用できない場合はすべてのトラフィックをブロックするように ASA が設定されます。 **fail-open** キーワードを指定すると、ASA IPS モジュールが使用できない場合はすべてのトラフィックを検査なしで通過させるように ASA が設定されます。 仮想センサーを使用する場合、**sensor** *sensor_name* 引数を使用してセンサー名を指定できます。使用可能なセンサー名を表示するには、**ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} **sensor ?**コマンドを使用します。使用可能なセンサーの一覧が表示されます。また、**show ips** コマンドを使用することもできます。ASA でマルチ コンテキスト モードを使用する場合、コンテキストに割り当てたセンサーだけを指定できます（「セキュリティ コンテキストへの仮想センサーの割り当て」（P.19-14）を参照）。コンテキストで設定する場合は、*mapped_name* を使用します。センサー名を指定しないと、トラフィックはデフォルトのセンサーを使用します。マルチ コンテキスト モードでは、コンテキストのデフォルトのセンサーを指定できます。シングル モードの場合や、マルチ モードでデフォルト センサーが指定されていない場合は、ASA IPS モジュールで設定されているデフォルト センサーがトラフィックに使用されます。入力した名前がまだ ASA IPS モジュール上に存在しない場合は、エラーとなり、コマンドは拒否されます。
ステップ 6	（任意） **class** *name2* **例：** `hostname(config-pmap)# class ips_class2`	IPS トラフィックに複数のクラス マップを作成した場合、ポリシーに対して別のクラスを指定できます。 ポリシー マップ内でのクラスの順番が重要であることの詳細については、「サービス ポリシー内の機能照合」（P.1-5）を参照してください。トラフィックを同じアクション タイプの複数のクラス マップに一致させることはできません。そのため、ネットワーク A を sensorA に進ませ、それ以外のすべてのトラフィックを sensorB に進ませる場合、まずネットワーク A に対して **class** コマンドを入力してから、すべてのトラフィックに対して **class** コマンドを入力する必要があります。このようにしないと、ネットワーク A を含むすべてのトラフィックが最初の **class** コマンドに一致して、sensorB に送信されます。

	コマンド	目的
ステップ 7	（任意） **ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}] **例：** hostname(config-pmap-c)# ips promiscuous fail-close	トラフィックの 2 番目のクラスが ASA IPS モジュールに送信されるように指定します。 これらのステップを繰り返して、必要な数のクラスを追加します。
ステップ 8	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} **例：** hostname(config)# service-policy tcp_bypass_policy outside	1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。**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。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。

ASA IPS モジュールの管理

この項には、モジュールのリカバリやトラブルシューティングに役立つ手順が含まれます。

モジュール上でのイメージのインストールおよび起動

モジュールに障害が発生して、モジュール アプリケーション イメージを実行できない場合は、TFTP サーバから（ハードウェア モジュールの場合）、またはローカル ディスク（ソフトウェア モジュールの場合）から、モジュール上に新しいイメージを再インストールできます。

（注） モジュール ソフトウェア内部では、イメージをインストールするために **upgrade** コマンドを使用しないでください。

前提条件

- ハードウェア モジュール：指定する TFTP サーバが、最大 60 MB のファイルを転送できることを確認してください。

（注） ネットワークとイメージのサイズに応じて、このプロセスは完了までに約 15 分間かかることがあります。

- ソフトウェア モジュール：この手順を実行する前に、イメージを ASA 内部フラッシュ（disk0）にコピーします。

（注）　IPS ソフトウェアを disk0 にダウンロードする前に、フラッシュ メモリの最低 50% が空いていることを確認します。IPS をインストールするときに、IPS のファイル システム用に内部フラッシュ メモリの 50% が予約されます。

手順の詳細

	コマンド	目的

ステップ 1	ハードウェア モジュール（例：ASA 5585-X）の場合：
	hw-module module 1 recover configure
	ソフトウェア モジュール（例：ASA 5545-X）の場合：
	sw-module module ips recover configure image disk0:*file_path*
	例：
	`hostname# hw-module module 1 recover configure`
	`Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg`
	`Port IP Address [127.0.0.2]: 10.1.2.10`
	`Port Mask [255.255.255.254]: 255.255.255.0`
	`Gateway IP Address [1.1.2.10]: 10.1.2.254`
	`VLAN ID [0]: 100`
		新しいイメージの場所を指定します。
		ハードウェア モジュールの場合：このコマンドを実行すると、TFTP サーバの URL、管理インターフェイスの IP アドレスとネットマスク、ゲートウェイ アドレスの入力を求めるプロンプトが表示されます。これらのネットワーク パラメータは ROMMON で設定されます。モジュール アプリケーション コンフィギュレーションで設定したネットワーク パラメータは ROMMON には使用できないため、ここで別個に設定する必要があります。
		ソフトウェア モジュールの場合：ローカル ディスク上のイメージの場所を指定します。
		リカバリ コンフィギュレーションを表示するには、**show module {1 | ips} recover** コマンドを使用します。
		マルチ コンテキスト モードでは、システム実行スペースでこのコマンドを入力します。

ステップ 2	ハードウェア モジュールの場合： **hw-module module 1 recover boot** ソフトウェア モジュールの場合： **sw-module module ips recover boot** **例：** `hostname# hw-module module 1 recover boot`	IPS モジュール ソフトウェアをインストールして起動します。
ステップ 3	ハードウェア モジュールの場合： **show module 1 details** ソフトウェア モジュールの場合： **show module ips details** **例：** `hostname# show module 1 details`	イメージ転送とモジュール再起動のプロセスの進捗を確認します。 出力の [Status] フィールドが、モジュールの動作ステータスを示します。モジュールの動作ステータスは、通常は「Up」と表示されます。ASA によってアプリケーション イメージがモジュールに転送されているときは、出力の [Status] フィールドには [Recover] と表示されます。ASA によるイメージの転送が完了してモジュールが再起動されると、新たに転送されたイメージが実行されます。

モジュールのシャットダウン

モジュール ソフトウェアをシャットダウンするのは、コンフィギュレーション データを失うことなく安全にモジュールの電源をオフにできるように準備するためです。**注**：ASA をリロードする場合は、モジュールは自動的にはシャットダウンされないので、ASA のリロード前にモジュールをシャットダウンすることを推奨します。モジュールをグレースフル シャットダウンするには、ASA CLI で次の手順を実行します。

手順の詳細

コマンド	目的
ハードウェア モジュール（例：ASA 5585-X）の場合： **hw-module module 1 shutdown** ソフトウェア モジュール（例：ASA 5545-X）の場合： **sw-module module ips shutdown** **例：** `hostname# hw-module module 1 shutdown`	モジュールをシャットダウンします。

ソフトウェア モジュール イメージのアンインストール

ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールするには、次の手順を実行します。

手順の詳細

	コマンド	目的

ステップ 1	**sw-module module ips uninstall**
	
	例：
	`hostname# sw-module module ips uninstall`
	`Module ips will be uninstalled.This will completely remove the`
	`disk image associated with the sw-module including any configuration`
	`that existed within it.`
	
	`Uninstall module <id>?[confirm]`
		ソフトウェア モジュール イメージおよび関連するコンフィギュレーションを永続的にアンインストールします。

ステップ 2	**reload** **例：** `hostname# reload`	ASA をリロードします。新しいモジュール タイプをインストールする前に、ASA をリロードする必要があります。

パスワードのリセット

モジュールのパスワードをデフォルトにリセットできます。ユーザ **cisco** のデフォルトのパスワードは **cisco** です。パスワードをリセットした後は、モジュール アプリケーションを使用してパスワードを独自の値に変更する必要があります。

モジュールのパスワードをリセットすると、モジュールがリブートします。モジュールのリブート中は、サービスを使用できません。

モジュールのパスワードをデフォルトの「cisco」にリセットするには、次の手順を実行します。

手順の詳細

コマンド	目的
ハードウェア モジュール（例：ASA 5585-X）の場合： **hw-module module 1 password-reset** ソフトウェア モジュール（例：ASA 5545-X）の場合： **sw-module module ips password-reset** **例：** `hostname# hw-module module 1 password-reset`	ユーザ **cisco** のモジュール パスワードを **cisco** にリセットします。

モジュールのリロードまたはリセット

モジュールをリロードまたはリセットするには、ASA CLI で次のいずれかのコマンドを入力します。

手順の詳細

コマンド	目的
ハードウェア モジュール（例：ASA 5585-X）の場合： **hw-module module 1 reload** ソフトウェア モジュール（例：ASA 5545-X）の場合： **sw-module module ips reload** **例：** `hostname# hw-module module 1 reload`	モジュール ソフトウェアをリロードします。
ハードウェア モジュールの場合： **hw-module module 1 reset** ソフトウェア モジュールの場合： **sw-module module ips reset** **例：** `hostname# hw-module module 1 reset`	リセットを実行してから、モジュールをリロードします。

ASA IPS モジュールのモニタリング

モジュールのステータスを確認するには、次のいずれかのコマンドを入力します。

コマンド	目的
show module	ステータスを表示します。
show module {**1** | **ips**} **details**	ステータスの追加情報を表示します。ハードウェア モジュールの場合は **1**、ソフトウェア モジュールの場合は **ips** を指定します。
show module {**1** | **ips**} **recover**	イメージをモジュールに転送するためのネットワーク パラメータを表示します。ハードウェア モジュールの場合は **1**、ソフトウェア モジュールの場合は **ips** を指定します。

例

次に、**show module details** コマンドの出力例を示します。この出力の内容は、SSC がインストールされている ASA に関する追加情報です。

```
hostname# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Card-5
Hardware version: 0.1
Serial Number: JAB11370240
Firmware version: 1.0(14)3
Software version: 6.2(1)E2
MAC Address Range: 001d.45c2.e832 to 001d.45c2.e832
App.Name: IPS
App.Status: Up
App.Status Desc: Not Applicable
App.Version: 6.2(1)E2
Data plane Status: Up
Status: Up
Mgmt IP Addr: 209.165.201.29
Mgmt Network Mask: 255.255.224.0
Mgmt Gateway: 209.165.201.30
Mgmt Access List: 209.165.201.31/32
                  209.165.202.158/32
                  209.165.200.254/24
Mgmt Vlan: 20
```

ASA 5525-X に IPS SSP ソフトウェア モジュールがインストールされている場合の **show module ips** コマンドの出力例を次に示します。

```
hostname# show module ips
Mod Card Type                                    Model           Serial No.
--- -------------------------------------------- --------------------------
ips IPS 5525 Intrusion Protection System         IPS5525         FCH1504V03P

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ---------------------------
ips 503d.e59c.6f89 to 503d.e59c.6f89  N/A          N/A          7.1(1.160)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------------------------------------
ips IPS                            Up               7.1(1.160)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
ips Up                 Up
```

```
Mod License Name      License Status  Time Remaining
--- ----------------- --------------- ---------------
ips IPS Module        Enabled         7 days
```

ASA IPS モジュールの設定例

次の例では、すべての IP トラフィックが ASA IPS モジュールに無差別モードで誘導され、何らかの理由で ASA IPS モジュール カードに障害が発生した場合はすべての IP トラフィックがブロックされます。

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

次の例では、10.1.1.0 ネットワークと 10.2.1.0 ネットワーク宛てのすべての IP トラフィックが AIP SSM にインライン モードで誘導され、何らかの理由で AIP SSM に障害が発生した場合は、すべてのトラフィックの通過が許可されます。my-ips-class トラフィックにはセンサー 1 が使用され、my-ips-class2 トラフィックにはセンサー 2 が使用されます。

```
hostname(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list my-ips-acl
hostname(config)# class-map my-ips-class2
hostname(config-cmap)# match access-list my-ips-acl2
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips inline fail-open sensor sensor1
hostname(config-pmap)# class my-ips-class2
hostname(config-pmap-c)# ips inline fail-open sensor sensor2
hostname(config-pmap-c)# service-policy my-ips-policy interface outside
```

ASA IPS モジュールの機能履歴

表 19-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 19-2　ASA IPS モジュールの機能履歴

機能名	プラットフォーム リリース	機能情報
AIP SSM	7.0(1)	ASA 5510、5520、および 5540 対応の AIP SSM のサポートが導入されました。 **ips** コマンドが導入されました。
仮想センサー（ASA 5510 以降）	8.0(2)	仮想センサーのサポートが導入されました。仮想センサーを使用すると ASA IPS モジュール上で複数のセキュリティ ポリシーを設定できます。 **allocate-ips** コマンドが導入されました。
ASA 5505 用 AIP SSC	8.2(1)	ASA 5505 対応の AIP SSC のサポートが導入されました。 **allow-ssc-mgmt**、**hw-module module ip**、および **hw-module module allow-ip** コマンドが導入されました。
ASA 5585-X 対応の ASA IPS SSP-10、-20、-40、および -60 のサポート	8.2(5)/ 8.4(2)	ASA 5585-X 対応の ASA IPS SSP-10、-20、-40、および -60 のサポートが導入されました。ASA IPS SSP をインストールできるのは、SSP のレベルが一致する場合だけです（たとえば、SSP-10 と ASA IPS SSP-10）。 **（注）** ASA 5585-X はバージョン 8.3 ではサポートされていません。

表 19-2　ASA IPS モジュールの機能履歴（続き）

機能名	プラットフォームリリース	機能情報
SSP-40 および SSP-60 対応のデュアル SSP のサポート	8.4(2)	SSP-40 および SSP-60 の場合、同じシャーシでレベルが同じ 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-40 と SSP-60 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。 （注）　2 個の SSP をシャーシで使用する場合、VPN はサポートされません。しかし、VPN がディセーブルになっていないことに注意してください。 **show module**、**show inventory**、**show environment** の各コマンドが変更されました。
ASA 5512-X ～ ASA 5555-X に対する ASA IPS SSP のサポート	8.6(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X に対する ASA IPS SSP ソフトウェア モジュールのサポートが導入されました。 **session**、**show module**、**sw-module** の各コマンドが導入または変更されました。