CHAPTER 6

セキュリティ コンテキストの追加および管理

この章では、セキュリティ アプライアンスにマルチセキュリティ コンテキストを設定する方法について説明します。次の項で構成されています。

コンテキストの機能およびマルチ コンテキスト モードのイネーブル化については、第 3 章「マルチ コンテキスト モードのイネーブル化」を参照してください。

リソース管理の設定

デフォルトでは、すべてのセキュリティ コンテキストは、コンテキストあたりの最大制限が適用されている場合を除いて、セキュリティ アプライアンスのリソースに無制限にアクセスできます。ただし、1 つ以上のコンテキストがリソースを大量に使用しており、他のコンテキストが接続を拒否されている場合は、リソース管理を設定してコンテキストごとのリソースの使用を制限できます。

この項では、次のトピックについて取り上げます。

クラスおよびクラス メンバーの概要

セキュリティ アプライアンスでは、リソース クラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。この項では、次のトピックについて取り上げます。

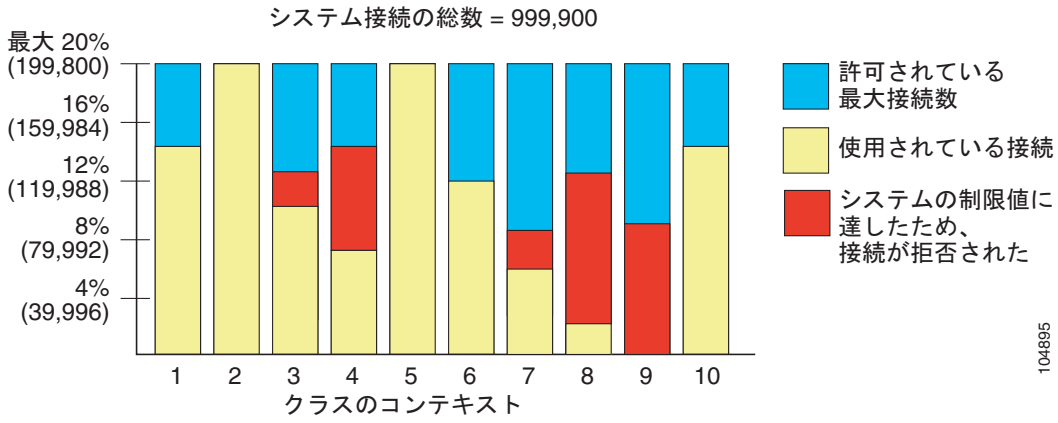
リソース制限値

クラスを作成すると、セキュリティ アプライアンスは、クラスに割り当てられる各コンテキストに対してリソースの一部を確保しなくなります。その代わりに、セキュリティ アプライアンスは、コンテキストの上限を設定します。リソースをオーバーサブスクライブする場合、または一部のリソースを無制限にする場合は、少数のコンテキストがこれらのリソースを「使い果たし」、他のコンテキストへのサービスに影響する可能性があります。

個々のリソースには、割合（ハードウェアのシステム制限がある場合）または絶対値で制限を設定できます。

コンテキスト全体に渡って 100% を超えるリソースを割り当てることにより、セキュリティ アプライアンスをオーバーサブスクライブすることができます。たとえば、接続がコンテキストあたり 20% までに制限されるように Bronze クラスを設定し、それから 10 個のコンテキストをそのクラスに割り当てれば、リソースの合計を 200% にできます。コンテキストがシステム制限を超えて同時に使用する場合、各コンテキストは意図した 20% を下回ります。（図 6-1 を参照）。

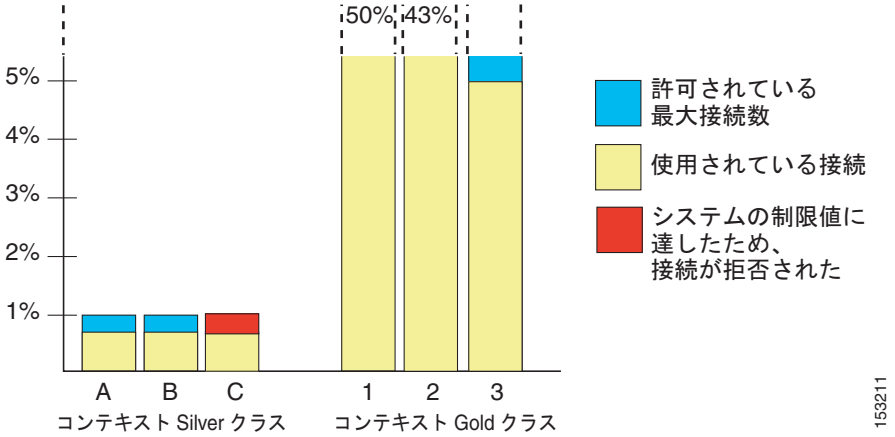
図 6-1　リソースのオーバーサブスクライブ



コンテキスト全体に渡って、セキュリティ アプライアンスの実際の制限を超える絶対値をリソースに割り当てると、セキュリティ アプライアンスのパフォーマンスが低下する場合があります。

セキュリティ アプライアンスでは、割合や絶対値ではなく、クラス内の 1 つ以上のリソースへの無制限アクセスを割り当てることができます。リソースに制限がない場合、コンテキストは、システムに存在する（実際に使用可能な）だけのリソースを使用できます。たとえば、コンテキスト A、B、C が Silver クラスに属しており、クラスの各メンバの使用量が接続の 1% に制限されていて、合計 3% が割り当てられているが、3 つのコンテキストが現在使用しているのは合計 2% だけだとします。Gold クラスは、接続に無制限にアクセスできます。Gold クラスのコンテキストは、「未割り当て」接続のうち 97% を超える分も使用できます。つまり、現在コンテキスト A、B、C で使用されていない、接続の 1% も使用できます。その場合は、コンテキスト A、B、C の使用量が、これらの制限の合計である 3% に達することは不可能になります。（図 6-2 を参照）。無制限アクセスの設定は、システムのオーバーサブスクライブ量を制御する機能が劣る点を除いて、セキュリティ アプライアンスのオーバーサブスクライブに類似しています。

図 6-2　無制限リソース



デフォルト クラス

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルト クラスに属します。コンテキストをデフォルト クラスに積極的に割り当てる必要はありません。

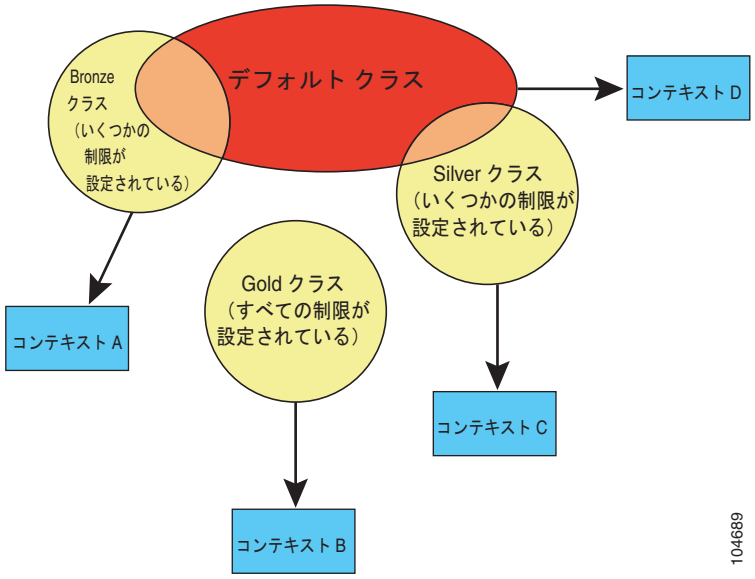
コンテキストがデフォルト クラス以外のクラスに属する場合、それらのクラス設定は常にデフォルト クラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバ コンテキストはそれらの制限にデフォルト クラスを使用します。たとえば、すべての同時接続に 2% の制限を設定したがその他の制限を設定せずにクラスを作成した場合、他のすべての制限はデフォルト クラスから継承されます。これとは逆に、すべてのリソースに対する制限値を設定してクラスを作成すると、そのクラスではデフォルト クラスの設定を何も使用しません。

デフォルトでは、デフォルト クラスは、すべてのコンテキストにリソースへのアクセスを無制限に提供します。ただし、次の制限が適用されます（この制限は、デフォルトではコンテキストあたりの最大許容値が設定されます）。

- Telnet セッション：5 セッション。
- SSH セッション：5 セッション。
- IPSec セッション：5 セッション。
- MAC アドレス：65,535 エントリ。

図 6-3 に、デフォルト クラスと他のクラスの関係を示します。コンテキスト A および C は、いくつかの制限が設定されたクラスに属しており、それ以外の制限はデフォルト クラスから継承します。コンテキスト B は、属している Gold クラスですべての制限が設定されているため、デフォルト クラスから制限値を継承しません。コンテキスト D はクラスに割り当てられなかったため、デフォルトでデフォルト クラスのメンバになります。

図 6-3　　リソース クラス



クラス メンバ

クラスの設定を使用するには、コンテキストを定義するときに、そのコンテキストをクラスに割り当てます。すべてのコンテキストは、別のクラスに割り当てられていなければ、デフォルト クラスに属します。したがって、コンテキストをデフォルト クラスに割り当てる必要は特にありません。コンテキストは 1 つのリソース クラスにだけ割り当てることができます。このルールの例外は、メンバ クラスで未定義の制限はデフォルト クラスから継承されることです。そのため実際には、コンテキストがデフォルト クラスおよび別のクラスのメンバになります。

クラスの設定

システム コンフィギュレーションでクラスを設定するには、次の手順を実行します。新しい値を指定してコマンドを再入力すると、特定のリソース制限値を変更できます。

ステップ 1　クラス名を指定してクラス コンフィギュレーション モードに移行するには、システム実行スペースで次のコマンドを入力します。

```
hostname(config)# class name
```

name は、最大 20 文字の文字列です。デフォルト クラスの制限値を設定するには、名前として **default** と入力します。

ステップ 2　リソースの制限値を設定する場合は、次のオプションを参照してください。

- すべてのリソース制限値を無制限に設定するには（表 6-1 を参照）、次のコマンドを入力します。

```
hostname(config-resmgmt)# limit-resource all 0
```

たとえば、制限のない管理コンテキストを含むクラスを作成するとします。デフォルト クラスでは、デフォルトですべてのリソースが無制限に設定されています。

- 特定のリソース制限値を設定するには、次のコマンドを入力します。

```
hostname(config-resmgmt)# limit-resource [rate] resource_name number[%]
```

この特定のリソースでは、この制限値が **all** に設定された制限値より優先されます。**rate** 引数を入力して、特定のリソースの毎秒あたりのレートを設定します。システム制限が設定されていないリソースの場合は、1 ～ 100 の割合（%）値は設定できず、絶対値だけを設定できます。毎秒あたりのレートを設定可能なリソース、およびシステム制限が設定されていないリソースについては、表 6-1 を参照してください。

表 6-1 に、リソース タイプと制限を示します。**show resource types** コマンドも参照してください。

表 6-1　リソース名と制限

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限[1]	説明
mac-addresses	同時接続数	該当なし	65,535	トランスペアレント ファイアウォール モードでは、MAC アドレス テーブルで許可される MAC アドレス数。
conns	同時またはレート	該当なし	同時接続数：プラットフォームの接続制限については、「サポートされているプラットフォームと機能」（P.A-1）を参照してください。 レート：該当なし	任意の 2 つのホスト間の TCP または UDP 接続（1 つのホストと他の複数のホストとの間の接続を含む）。
inspects	レート	該当なし	該当なし	アプリケーション インスペクション。
hosts	同時接続数	該当なし	該当なし	セキュリティ アプライアンス経由で接続可能なホスト。
asdm	同時接続数	最小 1 最大 5	32	ASDM 管理セッション。 **（注）** ASDM セッションでは、2 つの HTTPS 接続を使用します。1 つは常に存在するモニタリング用の接続、もう 1 つは変更時にのみ存在するコンフィギュレーション変更用の接続です。たとえば、ASDM セッションのシステム制限が 32 の場合、HTTPS セッション数は 64 に制限されます。
ssh	同時接続数	最小 1 最大 5	100	SSH セッション。
syslogs	レート	該当なし	該当なし	システム ログ メッセージ。
telnet	同時接続数	最小 1 最大 5	100	Telnet セッション。
xlates	同時接続数	該当なし	該当なし	アドレス変換。

1. このカラムに「該当なし」と記述されている場合、そのリソースにはハード システム制限がないため、リソースのパーセンテージを設定できません。

たとえば、接続のデフォルト クラス制限を、無制限ではなく 10% に設定するには、次のコマンドを入力します。

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
```

他のリソースはすべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

```
hostname(config)# class gold
```

```
hostname(config-class)# limit-resource mac-addresses 10000
hostname(config-class)# limit-resource conns 15%
hostname(config-class)# limit-resource rate conns 1000
hostname(config-class)# limit-resource rate inspects 500
hostname(config-class)# limit-resource hosts 9000
hostname(config-class)# limit-resource asdm 5
hostname(config-class)# limit-resource ssh 5
hostname(config-class)# limit-resource rate syslogs 5000
hostname(config-class)# limit-resource telnet 5
hostname(config-class)# limit-resource xlates 36000
```

セキュリティ コンテキストの設定

システム コンフィギュレーション内のセキュリティ コンテキストの定義によって、コンテキストの名前、コンフィギュレーション ファイルの URL、コンテキストが使用できるインターフェイスが識別されます。

（注） 管理コンテキストがない場合（コンフィギュレーションをクリアした場合など）は、最初に次のコマンドを入力して管理コンテキスト名を指定する必要があります。

```
hostname(config)# admin-context name
```

このコンテキスト名はコンフィギュレーションにまだ存在しませんが、続いて **context** *name* コマンドを入力すると、指定した名前との照合が行われて、管理コンテキスト コンフィギュレーションを続行できます。

システム コンフィギュレーションにコンテキストを追加する場合、または既存のコンテキストを変更する場合は、次の手順を実行します。

ステップ 1　コンテキストを追加または修正するには、システム実行スペースで次のコマンドを入力します。

```
hostname(config)# context name
```

name は最大 32 文字の文字列です。コンテキスト名は、大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という名前の 2 つのコンテキストを保持できます。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンは使用できません。

「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。

ステップ 2　（任意）このコンテキストに説明を追加するには、次のコマンドを使用します。

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

ステップ 3　コンテキストで使用するインターフェイスを指定するには、1 つの物理インターフェイス、あるいは 1 つまたは複数のサブインターフェイスに該当するコマンドを入力します。

- 物理インターフェイスを割り当てるには、次のコマンドを入力します。

  ```
  hostname(config-ctx)# allocate-interface physical_interface [map_name]
  [visible | invisible]
  ```

- 1 つまたは複数のサブインターフェイスを割り当てるには、次のコマンドを入力します。

  ```
  hostname(config-ctx)# allocate-interface
  physical_interface.subinterface[-physical_interface.subinterface]
  [map_name[-map_name]] [visible | invisible]
  ```

これらのコマンドを複数回入力して複数の範囲を指定できます。このコマンドの **no** 形式を使用して割り当てを削除すると、このインターフェイスを含むコンテキスト コマンドすべてが実行コンフィギュレーションから削除されます。

トランスペアレント ファイアウォール モードでは、2 つのインターフェイスのみがトラフィックを通過させることができます。ただし、ASA 適応型セキュリティ アプライアンスでは、専用の管理インターフェイス Management 0/0（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第 3 のインターフェイスとして使用できます。

（注） トランスペアレント モードの管理インターフェイスは、MAC アドレス テーブルにないパケットをインターフェイスにフラッディングしません。

ルーテッド モードでは、必要に応じて同じインターフェイスを複数のコンテキストに割り当てることができます。トランスペアレント モードでは、インターフェイスを共有できません。

map_name は、インターフェイス ID の代わりにコンテキスト内で使用できるインターフェイスの英数字のエイリアスです。マッピング名を指定しない場合、インターフェイス ID 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インターフェイスをコンテキスト管理者に知らせない場合があります。

マッピング名はアルファベットで始まり、アルファベットまたは数字で終わる必要があります。その間の文字には、アルファベット、数字、または下線のみを使用できます。たとえば、次の名前を使用できます。

int0

inta

int_0

サブインターフェイスの場合は、マッピング名の範囲を指定できます。

サブインターフェイスの範囲を指定する場合は、マッピング名の一致範囲を指定できます。範囲については、次のガイドラインに従ってください。

- マッピング名は、アルファベット部分と、それに続く数値部分で構成する必要があります。マッピング名のアルファベット部分は、範囲の両端で一致している必要があります。たとえば、次のような範囲を入力します。

  int0-int10

  たとえば、**gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5** と入力した場合、コマンドは失敗します。

- マッピング名の数値部分には、サブインターフェイスの範囲と同じ個数の数値を含める必要があります。たとえば、次の例では、両方の範囲に 100 個のインターフェイスが含まれています。

  gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100

  たとえば、**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15** と入力した場合、コマンドは失敗します。

visible と指定することで、マッピング名を設定した場合でも、**show interface** コマンドで物理インターフェイスのプロパティが表示されるようにします。デフォルトの **invisible** は、マッピング名だけが表示されるように指定するキーワードです。

次に、gigabitethernet0/1.100、gigabitethernet0/1.200、および gigabitethernet0/2.300 ～ gigabitethernet0/1.305 をコンテキストに割り当てる例を示します。マッピング名は、int1 ～ int8 です。

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
```

```
hostname(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

ステップ 4　システムがコンテキスト コンフィギュレーションをダウンロードする URL を識別するには、次のコマンドを入力します。

```
hostname(config-ctx)# config-url url
```

コンテキストの URL を追加すると、そのコンテキストをただちにロードし、コンフィギュレーションが使用可能であればコンテキストを実行できるようにします。

（注）　**config-url** コマンドを入力する前に、**allocate-interface** コマンドを入力します。セキュリティ アプライアンスは、コンテキスト コンフィギュレーションをロードする前に、コンテキストにインターフェイスを割り当てる必要があります。コンテキスト コンフィギュレーションには、インターフェイス（**interface**、**nat**、**global** など）を示すコマンドが含まれている場合があります。最初に **config-url** コマンドを入力した場合、セキュリティ アプライアンスはただちにコンテキスト コンフィギュレーションをロードします。インターフェイスを示すコマンドがコンテキストに含まれている場合、それらのコマンドは失敗します。

次の URL 構文を参照してください。

- **disk:/**[*path*/]*filename*

  この URL は内部フラッシュ メモリを示します。ファイル名のファイル拡張子は必須ではありませんが、「.cfg」を使用することを推奨します。コンフィギュレーション ファイルが存在しない場合は、次のメッセージが表示されます。

  ```
  WARNING: Could not fetch the URL disk:/url
  INFO: Creating context with default config
  ```

  次に、コンテキストを変更し、CLI で設定を行い、**write memory** コマンドを入力してフラッシュ メモリにファイルを書き込むことができます。

  （注）　管理コンテキスト ファイルは、内部フラッシュ メモリに保存する必要があります。

- **ftp://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*]

  type には次のキーワードのいずれかを指定できます。

  - **ap**：ASCII 受動モード
  - **an**：ASCII 通常モード
  - **ip**：（デフォルト）バイナリ受動モード
  - **in**：バイナリ通常モード

  管理コンテキストからサーバにアクセス可能である必要があります。ファイル名のファイル拡張子は必須ではありませんが、「.cfg」を使用することを推奨します。コンフィギュレーション ファイルが存在しない場合は、次のメッセージが表示されます。

  ```
  WARNING: Could not fetch the URL ftp://url
  INFO: Creating context with default config
  ```

  次に、コンテキストを変更し、CLI で設定を行い、**write memory** コマンドを入力して FTP サーバにファイルを書き込むことができます。

- **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*

管理コンテキストからサーバにアクセス可能である必要があります。ファイル名のファイル拡張子は必須ではありませんが、「.cfg」を使用することを推奨します。コンフィギュレーション ファイルが存在しない場合は、次のメッセージが表示されます。

```
WARNING: Could not fetch the URL http://url
INFO: Creating context with default config
```

コンテキストに変更を加え、CLI でコンテキストを設定する場合は、**write memory** コマンドを使用して HTTP または HTTPS サーバに変更を保存することはできません。ただし、**copy tftp** コマンドを使用して実行コンフィギュレーションを TFTP サーバにコピーできます。

- **tftp://**[*user*[**:***password*]**@**]*server*[**:***port*]/[*path*/]*filename*[**;int=***interface_name*]

  管理コンテキストからサーバにアクセス可能である必要があります。サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。ファイル名のファイル拡張子は必須ではありませんが、「.cfg」を使用することを推奨します。コンフィギュレーション ファイルが存在しない場合は、次のメッセージが表示されます。

  ```
  WARNING: Could not fetch the URL tftp://url
  INFO: Creating context with default config
  ```

  次に、コンテキストを変更し、CLI で設定を行い、**write memory** コマンドを入力して TFTP サーバにファイルを書き込むことができます。

URL を変更するには、新しい URL で **config-url** コマンドを再入力します。

URL の変更の詳細については、「セキュリティ コンテキスト URL の変更」（P.6-14）を参照してください。

たとえば、次のコマンドを入力します。

```
hostname(config-ctx)# config-url ftp://joe:passw0rd1@10.1.1.1/configlets/test.cfg
```

ステップ 5　（任意）コンテキストをリソース クラスに割り当てるには、次のコマンドを入力します。

```
hostname(config-ctx)# member class_name
```

クラスを指定しない場合、コンテキストはデフォルト クラスに属します。コンテキストは 1 つのリソース クラスにだけ割り当てることができます。

たとえば、コンテキストを gold クラスに割り当てるには、次のコマンドを入力します。

```
hostname(config-ctx)# member gold
```

ステップ 6　コンテキスト情報を表示するには、『*Cisco Security Appliance Command Reference*』の **show context** コマンドを参照してください。

次に、管理コンテキストに「administrator」を設定し、内部フラッシュ メモリに「administrator」というコンテキストを作成してから、FTP サーバから 2 つのコンテキストを追加する例を示します。

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
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)# 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)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver
```

コンテキスト インターフェイスへの MAC アドレスの自動割り当て

コンテキストでインターフェイスを共有するには、一意の MAC アドレスを各コンテキストのインターフェイスに割り当てることをお勧めします。MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。インターフェイスを共有するものの、各コンテキストにインターフェイスの固有の MAC アドレスがない場合は、宛先 IP アドレスがパケットの分類に使用されます。宛先アドレスは、コンテキスト NAT コンフィギュレーションと照合されます。この方法には、MAC アドレスの方法に比べるといくつか制限があります。パケットの分類の詳細については、「セキュリティ アプライアンスによるパケットの分類方法」（P.3-3）を参照してください。

デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

次のコマンドをシステム コンフィギュレーションに入力することにより、MAC アドレスを各共有コンテキスト インターフェイスに自動的に割り当てることができます。

```
hostname(config)# mac-address auto
```

フェールオーバーで使用できるように、セキュリティ アプライアンスはインターフェイスごとにアクティブとスタンバイの両方の MAC アドレスを生成します。アクティブ ユニットがフェールオーバーしてスタンバイ ユニットがアクティブになると、その新規アクティブ ユニットがアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。

インターフェイスをコンテキストに割り当てると、新しい MAC アドレスがただちに生成されます。コンテキスト インターフェイスを生成した後にこのコマンドをイネーブルにした場合、このコマンドを入力するとただちに MAC アドレスがすべてのインターフェイスに生成されます。**no mac-address auto** コマンドを使用すると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。

MAC アドレスは、次の形式を使用して生成されます。

- アクティブ ユニットの MAC アドレス：12*_slot.port_subid.contextid*.
- スタンバイ ユニットの MAC アドレス：02*_slot.port_subid.contextid*.

インターフェイス スロットがないプラットフォームの場合、スロットは常に 0 です。*port* はインターフェイス ポートです。*subid* は、表示不可能なサブインターフェイスの内部 ID です。*contextid* は、**show context detail** コマンドで表示可能なコンテキストの内部 ID です。たとえば、ID 1 のコンテキスト内のインターフェイス GigabitEthernet 0/1.200 には、次の生成済み MAC アドレスがあります。サブインターフェイス 200 の内部 ID は 31 です。

- アクティブ：1200.0131.0001
- スタンバイ：0200.0131.0001

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、コンテキスト内のインターフェイスの MAC アドレスを手動で設定できます。MAC アドレスの手動設定の詳細については、「インターフェイスの設定」（P.7-2）を参照してください。

コンテキストとシステム実行スペースの切り替え

システム実行スペースにログインした場合（または Telnet や SSH を使用して管理コンテキストにログインした場合）は、コンテキスト間の切り替えが可能であり、各コンテキスト内でコンフィギュレーション タスクやモニタリング タスクを実行できます。実行コンフィギュレーションが、コンフィギュレーション モードで編集するか、**copy** コマンドまたは **write** コマンドに使用されるかは、ログインした場所で決まります。システム実行スペースにログインした場合、実行コンフィギュレーションはシステム コンフィギュレーションのみで構成され、コンテキストにログインした場合は、実行コンフィギュレーションはそのコンテキストのみで構成されます。たとえば、**show running-config** コマンドを入力しても、すべての実行コンフィギュレーション（システム コンテキストとすべてのコンテキスト）を表示することはできません。現在のコンフィギュレーションだけが表示されます。

システム実行スペースとコンテキスト間の切り替え、またはコンテキスト間の切り替えを行うには、次のコマンドを使用します。

- あるコンテキストに切り替えるには、次のコマンドを入力します。

  ```
  hostname# changeto context name
  ```

  プロンプトが次のように変化します。

  ```
  hostname/name#
  ```

- システム実行スペースに切り替えるには、次のコマンドを入力します。

  ```
  hostname/admin# changeto system
  ```

  プロンプトが次のように変化します。

  ```
  hostname#
  ```

セキュリティ コンテキストの管理

この項では、セキュリティ コンテキストを管理する方法について説明します。次の項目を取り上げます。

セキュリティ コンテキストの削除

コンテキストは、システム コンフィギュレーションを編集することによってのみ削除できます。現在の管理コンテキストは、**clear context** コマンドを実行してすべてのコンテキストを削除しない限り、削除できません。

（注） フェールオーバーを使用すると、アクティブ装置でコンテキストを削除した時刻と、スタンバイ装置でコンテキストが削除された時刻との間で遅延が生じます。アクティブ装置とスタンバイ装置の間でインターフェイス数が一致していないことを示すエラー メッセージが表示される場合があります。このエラーは一時的に表示されるもので、無視できます。

コンテキストの削除には、次のコマンドを使用します。

- 1 つのコンテキストを削除するには、システム実行スペースで次のコマンドを入力します。

  ```
  hostname(config)# no context name
  ```

  すべてのコンテキスト コマンドを削除することもできます。

- すべてのコンテキスト（管理コンテキストを含む）を削除するには、システム実行スペースで次のコマンドを入力します。

  ```
  hostname(config)# clear context
  ```

管理コンテキストの変更

システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザに制限する必要があります。

コンフィギュレーション ファイルが内部フラッシュ メモリに保存されている限り、任意のコンテキストを管理コンテキストとして設定できます。管理コンテキストを設定するには、システム実行スペースで次のコマンドを入力します。

```
hostname(config)# admin-context context_name
```

Telnet、SSH、HTTPS など、管理コンテキストに接続しているリモート管理セッションはすべて終了します。新しい管理コンテキストに再接続する必要があります。

（注） **ntp server** を含むいくつかのシステム コマンドは、管理コンテキストに所属するインターフェイス名を識別します。管理コンテキストを変更した場合に、そのインターフェイス名が新しい管理コンテキストに存在しないときは、そのインターフェイスを参照するシステム コマンドはすべて、アップデートしてください。

セキュリティ コンテキスト URL の変更

セキュリティ コンテキスト URL は、新しい URL からコンフィギュレーションをリロードしないと変更できません。

セキュリティ アプライアンスは、新しいコンフィギュレーションを現在の実行コンフィギュレーションにマージします。同じ URL を再入力した場合でも、保存されたコンフィギュレーションが実行コンフィギュレーションにマージされます。マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。実行コンフィギュレーションが空白の場合（たとえば、サーバが使用不可でコンフィギュレーションがダウンロードされなかった場合）は、新しいコンフィギュレーションが使用されます。コンフィギュレーションをマージしない場合は、コンテキストを経由する通信を妨げる実行コンフィギュレーションをクリアしてから、新しい URL からコンフィギュレーションをリロードすることができます。

コンテキストの URL を変更するには、次の手順を実行します。

ステップ 1　コンフィギュレーションをマージしない場合、コンテキストに切り替えてそのコンフィギュレーションをクリアするには、次のコマンドを入力します。マージを実行する場合は、ステップ 2 にスキップします。

```
hostname# changeto context name
hostname/name# configure terminal
hostname/name(config)# clear configure all
```

ステップ 2　必要な場合は、次のコマンドを入力してシステム実行スペースに切り替えます。

```
hostname/name(config)# changeto system
```

ステップ 3　切り替えたコンテキストに対応するコンテキスト 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)# context name
```

ステップ 4　新しい URL を入力するには、次のコマンドを入力します。

```
hostname(config)# config-url new_url
```

システムは、動作中になるように、ただちにコンテキストをロードします。

セキュリティ コンテキストのリロード

セキュリティ コンテキストは、次の 2 つの方法でリロードできます。

- 実行コンフィギュレーションをクリアしてからスタートアップ コンフィギュレーションをインポートする。

  このアクションでは、セキュリティ コンテキストに関連付けられている接続や NAT テーブルなどの属性の大部分がクリアされます。

- セキュリティ コンテキストをシステム コンフィギュレーションから削除する。

  このアクションでは、トラブルシューティングに役立つ可能性のあるメモリ割り当てなど補足的な属性がクリアされます。しかし、コンテキストをシステムに戻して追加するには、URL とインターフェイスを再指定する必要があります。

この項では、次のトピックについて取り上げます。

- 「コンフィギュレーションのクリアによるリロード」（P.6-15）
- 「コンテキストの削除および再追加によるリロード」（P.6-15）

コンフィギュレーションのクリアによるリロード

コンテキスト コンフィギュレーションをクリアし、URL からコンフィギュレーションをリロードすることによってコンテキストをリロードするには、次の手順を実行します。

ステップ 1　リロードするコンテキストに切り替えるには、次のコマンドを入力します。

```
hostname# changeto context name
```

ステップ 2　コンフィギュレーション モードにアクセスするには、次のコマンドを入力します。

```
hostname/name# configure terminal
```

ステップ 3　実行コンフィギュレーションをクリアするには、次のコマンドを入力します。

```
hostname/name(config)# clear configure all
```

このコマンドを実行するとすべての接続がクリアされます。

ステップ 4　コンフィギュレーションをリロードするには、次のコマンドを入力します。

```
hostname/name(config)# copy startup-config running-config
```

セキュリティ アプライアンスは、システム コンフィギュレーションに指定された URL からコンフィギュレーションをコピーします。コンテキスト内で URL を変更することはできません。

コンテキストの削除および再追加によるリロード

コンテキストを削除し、その後再追加することによってコンテキストをリロードするには、次の各項で説明してある手順を実行してください。

1. 「コンテキスト インターフェイスへの MAC アドレスの自動割り当て」（P.6-11）
2. 「セキュリティ コンテキストの設定」（P.6-7）

セキュリティ コンテキストのモニタリング

この項では、コンテキスト情報の表示およびモニタの方法について説明します。次の項目を取り上げます。

- 「コンテキスト情報の表示」（P.6-16）
- 「リソース割り当ての表示」（P.6-17）
- 「リソースの使用状況の表示」（P.6-19）
- 「コンテキストでの SYN 攻撃のモニタリング」（P.6-21）

コンテキスト情報の表示

システム実行スペースから、名前、割り当てられているインターフェイス、コンフィギュレーション ファイル URL を含むコンテキストのリストを表示できます。

システム実行スペースから次のコマンドを入力すると、すべてのコンテキストが表示されます。

```
hostname# show context [name | detail| count]
```

detail オプションを指定すると、追加情報が表示されます。詳細については、次の出力例を参照してください。

特定のコンテキストの情報を表示する場合は、*name* にコンテキスト名を指定します。

count オプションを指定すると、コンテキストの合計数が表示されます。

次に、**show context** コマンドの出力例を示します。この例では、3 つのコンテキストが表示されています。

```
hostname# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      disk0:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      disk0:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      disk0:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

表 6-2 に、各フィールドの説明を示します。

表 6-2　show context のフィールド

フィールド	説明
Context Name	すべてのコンテキスト名が表示されます。アスタリスク（*）の付いているコンテキスト名は、管理コンテキストです。
Interfaces	このコンテキストに割り当てられたインターフェイス。
URL	セキュリティ アプライアンスがコンテキストのコンフィギュレーションをロードする URL。

次に、**show context detail** コマンドの出力例を示します。

```
hostname# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk0:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
```

```
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

detail の出力の詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。

次に、**show context count** コマンドの出力例を示します。

```
hostname# show context count
Total active contexts: 2
```

リソース割り当ての表示

システム実行スペースから、すべてのクラスおよびクラス メンバーに渡るリソースごとの割り当て状況を表示できます。

リソース割り当てを表示するには、次のコマンドを入力します。

```
hostname# show resource allocation [detail]
```

このコマンドは、リソース割り当てを表示しますが、実際に使用されているリソースは表示しません。実際のリソース使用状況の詳細については、「リソースの使用状況の表示」（P.6-19）を参照してください。

detail 引数を指定すると、追加情報が表示されます。詳細については、次の出力例を参照してください。

次の出力例には、各リソースの合計割り当て量が絶対値および使用可能なシステム リソースの割合として示されています。

```
hostname# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]              35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000           30.50%
 Hosts                      78842           N/A
 SSH                           35           35.00%
 Telnet                        35           35.00%
 Xlates                     91749           N/A
 All                    unlimited
```

表 6-3 に、各フィールドの説明を示します。

表 6-3　show resource allocation のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。

表 6-3　show resource allocation のフィールド （続き）

フィールド	説明
Total	すべてのコンテキストで割り当てられるリソースの総量。この数量は、同時発生インスタンスまたは 1 秒あたりのインスタンスの絶対量です。クラス定義でパーセンテージを指定した場合、セキュリティ アプライアンスはこの表示のためにパーセンテージを絶対数に変換します。
% of Avail	リソースにハードウェア システム制限がある場合に、コンテキスト全体に渡って割り当てられている合計システム リソースの割合。リソースにシステム制限がない場合、このカラムには N/A と表示されます。

次に、**show resource allocation detail** コマンドの出力例を示します。

```
hostname# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource          Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]      default          all      CA  unlimited
                  gold               1       C      34000      34000     N/A
                  silver             1      CA      17000      17000     N/A
                  bronze             0      CA       8500
                  All Contexts:      3                         51000     N/A

Inspects [rate]   default          all      CA  unlimited
                  gold               1      DA  unlimited
                  silver             1      CA      10000      10000     N/A
                  bronze             0      CA       5000
                  All Contexts:      3                         10000     N/A

Syslogs [rate]    default          all      CA  unlimited
                  gold               1       C       6000       6000     N/A
                  silver             1      CA       3000       3000     N/A
                  bronze             0      CA       1500
                  All Contexts:      3                          9000     N/A

Conns             default          all      CA  unlimited
                  gold               1       C     200000     200000     20.00%
                  silver             1      CA     100000     100000     10.00%
                  bronze             0      CA      50000
                  All Contexts:      3                        300000     30.00%

Hosts             default          all      CA  unlimited
                  gold               1      DA  unlimited
                  silver             1      CA      26214      26214      N/A
                  bronze             0      CA      13107
                  All Contexts:      3                         26214      N/A

SSH               default          all       C          5
                  gold               1       D          5          5      5.00%
                  silver             1      CA         10         10     10.00%
                  bronze             0      CA          5
                  All Contexts:      3                            20     20.00%

Telnet            default          all       C          5
                  gold               1       D          5          5      5.00%
                  silver             1      CA         10         10     10.00%
                  bronze             0      CA          5
                  All Contexts:      3                            20     20.00%
```

```
Xlates          default          all      CA  unlimited
                gold               1      DA  unlimited
                silver             1      CA      23040      23040     N/A
                bronze             0      CA      11520
                All Contexts:      3                         23040     N/A

mac-addresses   default          all       C      65535
                gold               1       D      65535      65535    100.00%
                silver             1      CA       6553       6553      9.99%
                bronze             0      CA       3276
                All Contexts:      3                        137623    209.99%
```

表 6-4 に、各フィールドの説明を示します。

表 6-4　show resource allocation detail のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
Class	デフォルト クラスを含む、各クラスの名前。 すべてのコンテキスト フィールドには、すべてのクラス全体での合計値が表示されます。
Mmbrs	各クラスに割り当てられるコンテキストの数。
Origin	リソース制限の生成元。値は次のとおりです。 • A：この制限を個々のリソースとしてではなく、**all** オプションを使用して設定します。 • C：この制限はメンバー クラスから生成されます。 • D：この制限はメンバー クラスでは定義されたのではなく、デフォルト クラスから生成されました。デフォルト クラスに割り当てられたコンテキストの場合、値は「D」ではなく「C」になります。 セキュリティ アプライアンスでは、「A」を「C」または「D」と組み合わせることができます。
Limit	コンテキストごとのリソース制限（絶対数として）。クラス定義でパーセンテージを指定した場合、セキュリティ アプライアンスはこの表示のためにパーセンテージを絶対数に変換します。
Total	クラス内のすべてのコンテキストにわたって割り当てられているリソースの合計数。この数量は、同時発生インスタンスまたは 1 秒あたりのインスタンスの絶対量です。リソースが無制限の場合、この表示は空白です。
% of Avail	クラス内のコンテキスト全体に渡って割り当てられている合計システム リソースの割合。リソースが無制限の場合、この表示は空白です。リソースにシステム制限がない場合、このカラムの表示は N/A になります。

リソースの使用状況の表示

システム実行スペースで、コンテキストごとのリソースの使用状況やシステム リソースの使用状況を表示できます。

システム実行スペースでコンテキストごとのリソースの使用状況を表示するには、次のコマンドを入力します。

```
hostname# show resource usage [context context_name | top n | all | summary | system]
[resource {resource_name | all} | detail] [counter counter_name [count_threshold]]
```

デフォルトでは、**all**（すべての）コンテキストの使用状況が表示されます。各コンテキストは個別にリスト表示されます。

指定したリソースの上位 *n* 人のユーザとなっているコンテキストを表示するには、**top** *n* キーワードを入力します。このオプションでは、**resource all** ではなく、リソース タイプを 1 つのみ指定する必要があります。

summary オプションを指定すると、すべてのコンテキストの使用状況が組み合されて表示されます。

system オプションでは、すべてのコンテキストの使用状況が組み合されて表示されますが、組み合されたコンテキスト制限ではなく、リソースに対するシステムの制限が表示されます。

resource *resource_name* で使用可能なリソース名については、表 6-1 を参照してください。**show resource type** コマンドも参照してください。すべてのタイプを表示するには **all**（デフォルト）を指定します。

detail オプションを指定すると、管理できないリソースを含むすべてのリソースの使用状況が表示されます。たとえば、TCP 代行受信の数を表示できます。

counter *counter_name* には、次のいずれかのキーワードを指定します。

- **current**：リソースのアクティブな同時発生インスタンス数、またはリソースの現在のレートを表示します。
- **denied**：Limit カラムに示されるリソース制限を超えたため拒否されたインスタンスの数を表示します。
- **peak**：ピーク時のリソースの同時発生インスタンス数、またはピーク時のリソースのレートを表示します。これは、統計情報が **clear resource usage** コマンドまたはデバイスのリブートによって最後にクリアされた時点から計測されます。
- **all**：（デフォルト）すべての統計情報を表示します。

count_threshold は、表示するリソースの下限を設定します。デフォルトは 1 です。リソースの使用状況がここで設定する回数を下回っている場合、そのリソースは表示されません。カウンタ名に **all** を指定した場合、*count_threshold* は現在の使用状況に適用されます。

（注） すべてのリソースを表示するには、*count_threshold* を **0** に設定します。

次に、**show resource usage context** コマンドの出力例を示します。ここでは、admin コンテキストのリソース使用状況を表示する例を示しています。

```
hostname# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

次に、**show resource usage summary** コマンドの出力例を示します。ここでは、すべてのコンテキストとすべてのリソースのリソース使用状況を表示する例を示しています。ここでは、6 コンテキスト分の制限値が表示されています。

```
hostname# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      N/A            0 Summary
Conns                     584          763      280000(S)      0 Summary
Xlates                   8526         8966      N/A            0 Summary
Hosts                     254          254      N/A            0 Summary
Conns [rate]              270          535      N/A         1704 Summary
Inspects [rate]           270          535      N/A            0 Summary
```

```
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

次に、**show resource usage summary** コマンドの出力例を示します。このコマンドでは、25 コンテキストの制限が示されます。Telnet 接続および SSH 接続のコンテキストの限界がコンテキストごとに 5 であるため、合計の限界は 125 です。システムの限界が単に 100 であるため、システムの限界が表示されています。

```
hostname# show resource usage summary

Resource              Current         Peak      Limit    Denied   Context
Telnet                      1            1        100[S]      0   Summary
SSH                         2            2        100[S]      0   Summary
Conns                      56           90        N/A         0   Summary
Hosts                      89          102        N/A         0   Summary
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

次に、**show resource usage system** コマンドの出力例を示します。このコマンドは、すべてのコンテキストのリソース使用状況を表示しますが、組み合わせたコンテキストの限界ではなく、システムの限界を表示しています。現在使用中でないリソースを表示するには、**counter all 0** オプションを指定します。Denied の統計情報は、システム制限がある場合に、その制限によってリソースが拒否された回数を示します。

```
hostname# show resource usage system counter all 0

Resource              Current         Peak      Limit        Denied    Context
Telnet                      0            0        100             0    System
SSH                         0            0        100             0    System
ASDM                        0            0         32             0    System
Syslogs [rate]              1           18        N/A             0    System
Conns                       0            1     280000             0    System
Xlates                      0            0        N/A             0    System
Hosts                       0            2        N/A             0    System
Conns [rate]                1            1        N/A             0    System
Inspects [rate]             0            0        N/A             0    System
```

コンテキストでの SYN 攻撃のモニタリング

セキュリティ アプライアンス は TCP 代行受信を使用して SYN 攻撃を阻止します。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、セキュリティ アプライアンス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。セキュリティ アプライアンス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。

show perfmon コマンドを使用して、個々のコンテキストの攻撃レートをモニタできます。**show resource usage detail** コマンドを使用すれば、個々のコンテキストの TCP 代行受信で使用されるリソース量をモニタできます。システム全体での TCP 代行受信で使用されるリソースをモニタするには、**show resource usage summary detail** コマンドを使用します。

次に、**show perfmon** コマンドの出力例を示します。このコマンドは、admin というコンテキストの TCP 代行受信レートを表示します。

```
hostname/admin# show perfmon

Context:admin
PERFMON STATS:   Current      Average
Xlates               0/s          0/s
```

```
Connections              0/s           0/s
TCP Conns                0/s           0/s
UDP Conns                0/s           0/s
URL Access               0/s           0/s
URL Server Req           0/s           0/s
WebSns Req               0/s           0/s
TCP Fixup                0/s           0/s
HTTP Fixup               0/s           0/s
FTP Fixup                0/s           0/s
AAA Authen               0/s           0/s
AAA Author               0/s           0/s
AAA Account              0/s           0/s
TCP Intercept       322779/s      322779/s
```

次に、**show resource usage detail** コマンドの出力例を示します。このコマンドは、個々のコンテキストの TCP 代行受信で使用されるリソース量を表示します（イタリック体のサンプル テキストは、TCP 代行受信情報を示します）。

```
hostname(config)# show resource usage detail
Resource                Current         Peak      Limit        Denied Context
memory                   843732       847288  unlimited             0 admin
chunk:channels               14           15  unlimited             0 admin
chunk:fixup                  15           15  unlimited             0 admin
chunk:hole                    1            1  unlimited             0 admin
chunk:ip-users               10           10  unlimited             0 admin
chunk:list-elem              21           21  unlimited             0 admin
chunk:list-hdr                3            4  unlimited             0 admin
chunk:route                   2            2  unlimited             0 admin
chunk:static                  1            1  unlimited             0 admin
tcp-intercepts           328787       803610  unlimited             0 admin
np-statics                    3            3  unlimited             0 admin
statics                       1            1  unlimited             0 admin
ace-rules                     1            1  unlimited             0 admin
console-access-rul            2            2  unlimited             0 admin
fixup-rules                  14           15  unlimited             0 admin
memory                   959872       960000  unlimited             0 c1
chunk:channels               15           16  unlimited             0 c1
chunk:dbgtrace                1            1  unlimited             0 c1
chunk:fixup                  15           15  unlimited             0 c1
chunk:global                  1            1  unlimited             0 c1
chunk:hole                    2            2  unlimited             0 c1
chunk:ip-users               10           10  unlimited             0 c1
chunk:udp-ctrl-blk            1            1  unlimited             0 c1
chunk:list-elem              24           24  unlimited             0 c1
chunk:list-hdr                5            6  unlimited             0 c1
chunk:nat                     1            1  unlimited             0 c1
chunk:route                   2            2  unlimited             0 c1
chunk:static                  1            1  unlimited             0 c1
tcp-intercept-rate        16056        16254  unlimited             0 c1
globals                       1            1  unlimited             0 c1
np-statics                    3            3  unlimited             0 c1
statics                       1            1  unlimited             0 c1
nats                          1            1  unlimited             0 c1
ace-rules                     2            2  unlimited             0 c1
console-access-rul            2            2  unlimited             0 c1
fixup-rules                  14           15  unlimited             0 c1
memory                232695716    232020648  unlimited             0 system
chunk:channels               17           20  unlimited             0 system
chunk:dbgtrace                3            3  unlimited             0 system
chunk:fixup                  15           15  unlimited             0 system
chunk:ip-users                4            4  unlimited             0 system
chunk:list-elem            1014         1014  unlimited             0 system
chunk:list-hdr                1            1  unlimited             0 system
chunk:route                   1            1  unlimited             0 system
```

```
block:16384               510          885  unlimited             0 system
block:2048                 32           34  unlimited             0 system
```

次の出力例は、システム全体の TCP 代行受信で使用されるリソースを示します （イタリック体のサンプル テキストは、TCP 代行受信情報を示します)。

```
hostname(config)# show resource usage summary detail
Resource              Current         Peak      Limit        Denied Context
memory             238421312    238434336  unlimited             0 Summary
chunk:channels             46           48  unlimited             0 Summary
chunk:dbgtrace              4            4  unlimited             0 Summary
chunk:fixup                45           45  unlimited             0 Summary
chunk:global                1            1  unlimited             0 Summary
chunk:hole                  3            3  unlimited             0 Summary
chunk:ip-users             24           24  unlimited             0 Summary
chunk:udp-ctrl-blk          1            1  unlimited             0 Summary
chunk:list-elem          1059         1059  unlimited             0 Summary
chunk:list-hdr             10           11  unlimited             0 Summary
chunk:nat                   1            1  unlimited             0 Summary
chunk:route                 5            5  unlimited             0 Summary
chunk:static                2            2  unlimited             0 Summary
block:16384               510          885  unlimited             0 Summary
block:2048                 32           35  unlimited             0 Summary
tcp-intercept-rate     341306       811579  unlimited             0 Summary
globals                     1            1  unlimited             0 Summary
np-statics                  6            6  unlimited             0 Summary
statics                     2            2        N/A             0 Summary
nats                        1            1        N/A             0 Summary
ace-rules                   3            3        N/A             0 Summary
console-access-rul          4            4        N/A             0 Summary
fixup-rules                43           44        N/A             0 Summary
```