CHAPTER 6

マルチ コンテキスト モードの設定

この章では、ASA 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。次の項目を取り上げます。

セキュリティ コンテキストに関する情報

1 台の ASA を、セキュリティ コンテキストと呼ばれる複数の仮想デバイスに分割できます。各コンテキストは独立したデバイスとして動作し、独自のセキュリティ ポリシー、インターフェイス、および管理者を持ちます。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでサポートされない機能については、「注意事項と制限事項」（P.6-14）を参照してください。

この項では、セキュリティ コンテキストの概要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 コンテキストの一般的な使用方法

マルチセキュリティ コンテキストを使用する状況には次のようなものがあります。

- サービス プロバイダーとして、多数のカスタマーにセキュリティ サービスを販売する。ASA 上でマルチセキュリティ コンテキストをイネーブルにすることによって、費用対効果の高い、省スペース ソリューションを実装できます。このソリューションでは、カスタマーのトラフィックすべての分離とセキュリティが確保され、設定も容易です。
- 大企業または広大な大学の構内で、各部門の完全な独立を維持する必要がある。
- 企業で、部門ごとに個別のセキュリティ ポリシーの提供が求められている。
- 複数の ASA が必要なネットワークを使用している。

コンテキスト コンフィギュレーション ファイル

ここでは、ASA でマルチコンテキスト モードのコンフィギュレーションがどのように実装されるかについて説明します。内容は次のとおりです。

- 「コンテキスト コンフィギュレーション」（P.6-2）
- 「システム設定」（P.6-2）
- 「管理コンテキストの設定」（P.6-2）

コンテキスト コンフィギュレーション

コンテキストごとに、ASA の中に 1 つのコンフィギュレーションがあり、この中ではセキュリティ ポリシーやインターフェイスに加えて、スタンドアロン デバイスで設定できるすべてのオプションが指定されています。コンテキスト コンフィギュレーションはフラッシュ メモリ内に保存することも、TFTP、FTP、または HTTP（S）サーバからダウンロードすることもできます。

システム設定

システム管理者は、各コンテキスト コンフィギュレーションの場所、割り当てられたインターフェイス、およびその他のコンテキスト操作パラメータをシステム コンフィギュレーションに設定することで、コンテキストを追加および管理します。このコンフィギュレーションは、シングル モードのコンフィギュレーション同様、スタートアップ コンフィギュレーションです。システム コンフィギュレーションは、ASA の基本設定を識別します。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。システム コンフィギュレーションに含まれているものに、フェールオーバー トラフィック専用の特殊なフェールオーバー インターフェイスがあります。

管理コンテキストの設定

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。管理コンテキストは、リモートではなくフラッシュ メモリに置く必要があります。

システムがすでにマルチ コンテキスト モードになっている場合、またはシングル モードから変換された場合、管理コンテキストが admin.cfg と呼ばれるファイルとして内部フラッシュ メモリに自動的に作成されます。このコンテキストは「admin」と名付けられます。admin.cfg を管理コンテキストとして使用しない場合は、管理コンテキストを変更できます。

ASA によるパケットの分類方法

ASA に入ってくるパケットはいずれも分類する必要があります。その結果、ASA は、どのコンテキストにパケットを送信するかを決定できます。この項では、次のトピックについて取り上げます。

- 「有効な分類子の基準」（P.6-3）
- 「分類の例」（P.6-4）

（注）　宛先 MAC アドレスがマルチキャストまたはブロードキャスト MAC アドレスの場合、パケットが複製され、各コンテキストに送信されます。

有効な分類子の基準

この項では、分類子で使用される基準について説明します。次の項目を取り上げます。

- 「固有のインターフェイス」（P.6-3）
- 「固有の MAC アドレス」（P.6-3）
- 「NAT コンフィギュレーション」（P.6-4）

（注）　インターフェイス宛の管理トラフィックでは、インターフェイス IP アドレスが分類に使用されます。

ルーティング テーブルはパケット分類には使用されません。

固有のインターフェイス

入力インターフェイスに関連付けられているコンテキストが 1 つだけの場合、ASA はパケットをそのコンテキストに分類します。トランスペアレント ファイアウォール モードでは、各コンテキストに固有のインターフェイスが必要なため、この方法は、常にパケット分類の目的で使用されます。

固有の MAC アドレス

複数のコンテキストが同じインターフェイスを共有している場合は、各コンテキストでそのインターフェイスに割り当てられた一意の MAC アドレスが分類子で使用されます。固有の MAC アドレスがないと、アップストリーム ルータはコンテキストに直接ルーティングできません。デフォルトでは、MAC アドレスの自動生成がイネーブルです。各インターフェイスを設定するときに、手動で MAC アドレスを設定することもできます。

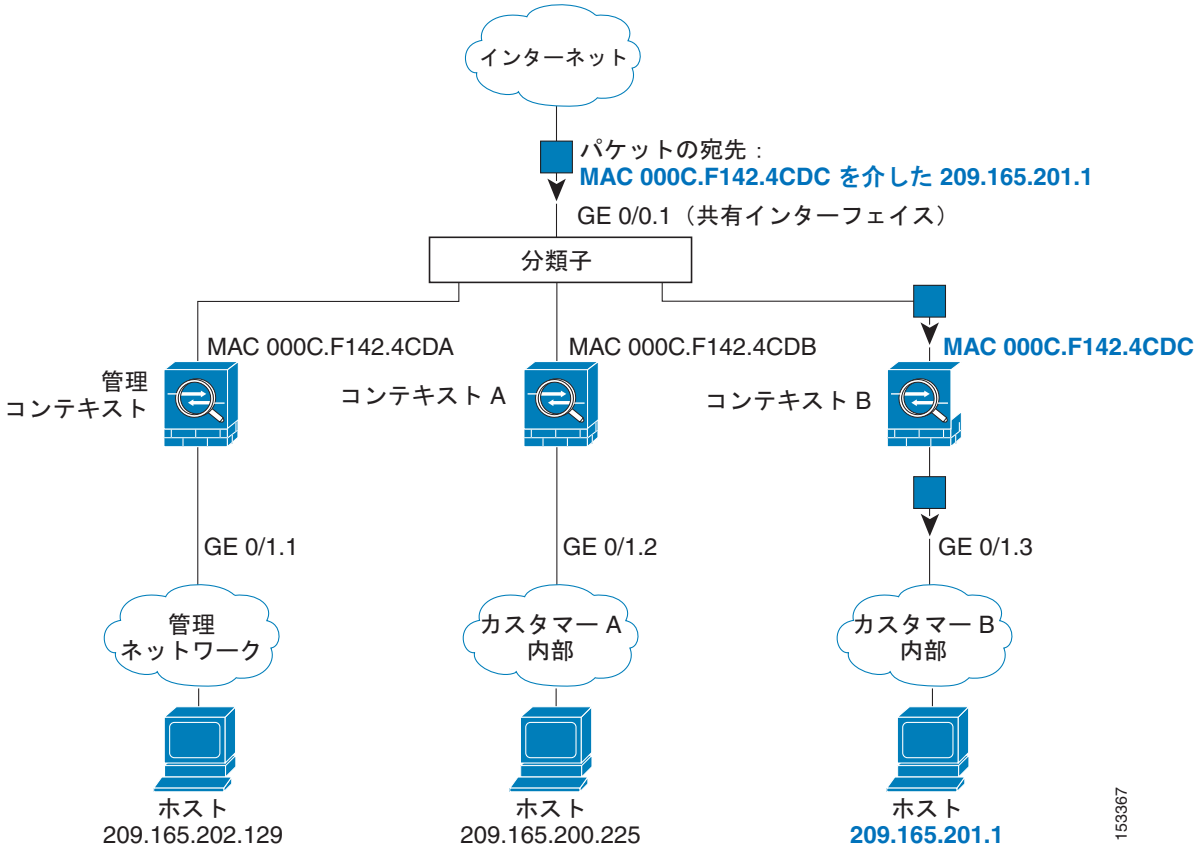
NAT コンフィギュレーション

固有の MAC アドレスの使用をディセーブルにすると、ASA は、NAT コンフィギュレーション内のマッピングされたアドレスを使用してパケットを分類します。NAT コンフィギュレーションの完全性に関係なくトラフィック分類を行うことができるように、NAT ではなく MAC アドレスを使用することをお勧めします。

分類の例

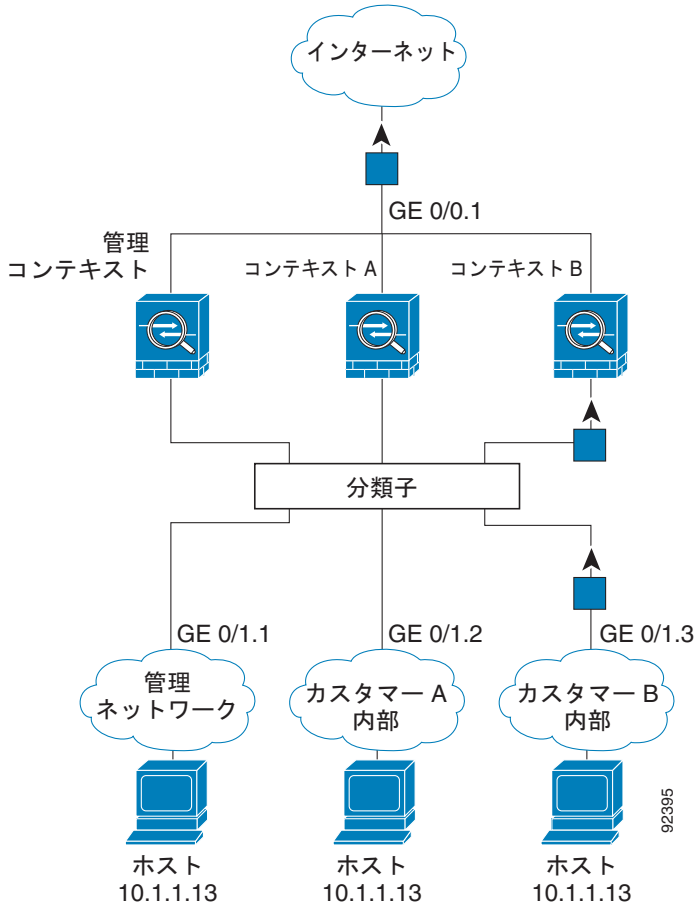
図 6-1 に、外部インターフェイスを共有するマルチ コンテキストを示します。コンテキスト B にはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをコンテキスト B に割り当てます。

図 6-1　インターフェイスを共有しているときの MAC アドレスを使用したパケット分類



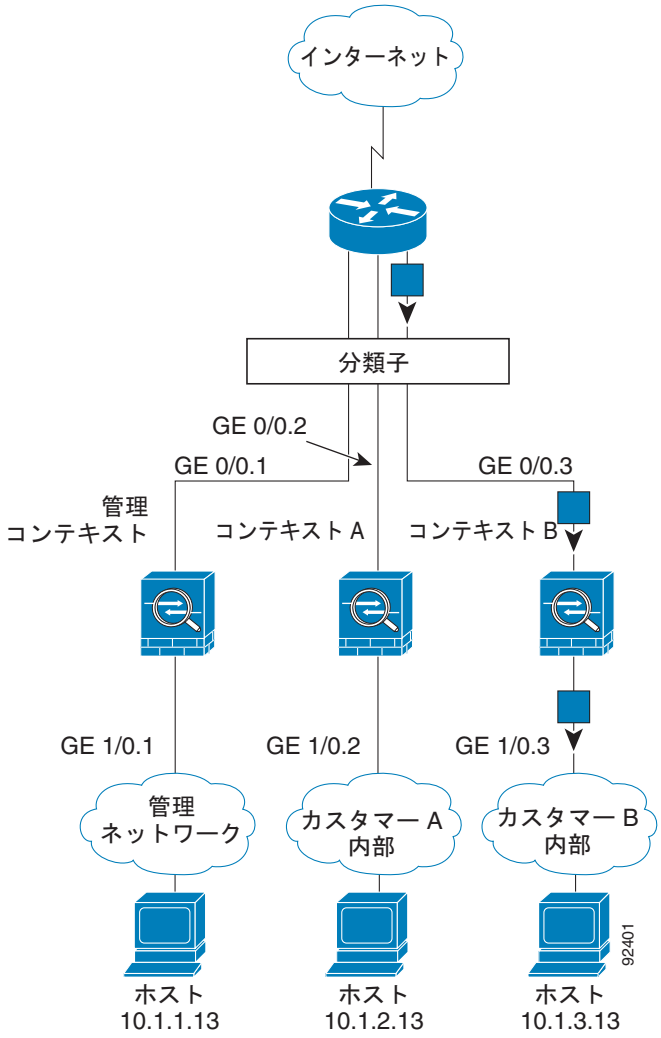
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。図 6-2 に、内部ネットワークのコンテキスト B 上のホストがインターネットにアクセスしている場合を示します。分類子は、パケットをコンテキスト B に割り当てます。これは、入力インターフェイスがギガビット イーサネット 0/1.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 6-2　内部ネットワークからの着信トラフィック



トランスペアレント ファイアウォールでは、固有のインターフェイスを使用する必要があります。図 6-3 に示すパケットは、インターネットから、内部ネットワークのコンテキスト B 上のホスト宛てです。分類子は、パケットをコンテキスト B に割り当てます。これは、入力インターフェイスがギガビット イーサネット 1/0.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 6-3　トランスペアレント ファイアウォールのコンテキスト



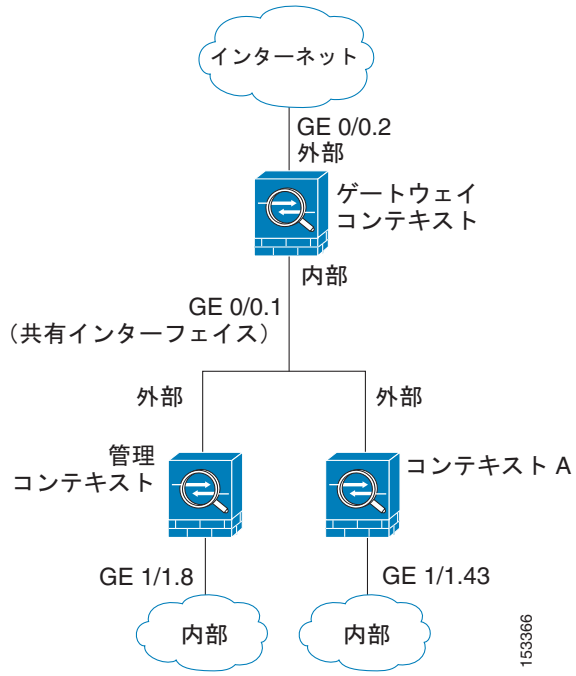
セキュリティ コンテキストのカスケード接続

コンテキストを別のコンテキストのすぐ前に置くことを、「*コンテキストをカスケード接続する*」といいます。一方のコンテキストの外部インターフェイスは、他方のコンテキストの内部インターフェイスと同じインターフェイスです。いくつかのコンテキストのコンフィギュレーションを単純化する場合、最上位のコンテキストの共有パラメータを設定することで、コンテキストをカスケード接続できます。

（注） コンテキストをカスケード接続するには、各コンテキスト インターフェイスに固有の MAC アドレスが必要です（デフォルト設定）。MAC アドレスのない共有インターフェイスのパケットを分類するには限界があるため、固有の MAC アドレスを設定しないでコンテキストのカスケード接続を使用することはお勧めしません。

図 6-4 に、ゲートウェイの背後に 2 つのコンテキストがあるゲートウェイ コンテキストを示します。

図 6-4　コンテキストのカスケード接続



セキュリティ コンテキストへの管理アクセス

ASA では、マルチ コンテキスト モードでのシステム管理アクセスと、各コンテキスト管理者のアクセスを提供します。次の各項では、システム管理者またはコンテキスト管理者としてのログインについて説明します。

- 「システム管理者のアクセス」（P.6-8）
- 「コンテキスト管理者のアクセス」（P.6-8）

システム管理者のアクセス

ASA にシステム管理者としてアクセスするには、次の 2 つの方法があります。

- ASA コンソールにアクセスする

  コンソールから*システム実行スペース*にアクセスします。この場合、入力したコマンドは、システム コンフィギュレーションまたはシステムの実行（run-time コマンド）だけに影響します。

- Telnet、SSH、または ASDM を使用して管理コンテキストにアクセスする

  Telnet、SSH、および ASDM アクセスをイネーブルにする方法については、第 43 章「管理アクセスの設定」を参照してください。

システム管理者として、すべてのコンテキストにアクセスできます。

管理やシステムのコンテキストから別のコンテキストに変更すると、ユーザ名はデフォルトの「enable_15」に変わります。そのコンテキストでコマンド許可を設定した場合は、「enable_15」というユーザの許可特権を設定する必要があります。または、十分な特権が与えられた別の名前でログインします。新しいユーザ名でログインするには、**login** コマンドを入力します。たとえば、「admin」というユーザ名で管理コンテキストにログインします。管理コンテキストにコマンド許可コンフィギュレーションはありませんが、それ以外のすべてのコンテキストにはコマンド許可があります。便宜を図るために、各コンテキスト コンフィギュレーションには、最大特権を持つ「admin」ユーザが含まれています。管理コンテキストからコンテキスト A に変更したときは、ユーザ名が enable_15 に変更されるので、**login** コマンドを入力して再度「admin」としてログインする必要があります。コンテキスト B に変更したときは、再度 **login** コマンドを入力して「admin」としてログインする必要があります。

システム実行スペースでは AAA コマンドはサポートされていませんが、個別のログインのために、固有のイネーブル パスワードおよびユーザ名をローカル データベースに設定することができます。

コンテキスト管理者のアクセス

Telnet、SSH、または ASDM を使用して、コンテキストにアクセスできます。管理外コンテキストにログインすると、アクセスできるのはそのコンテキストのコンフィギュレーションだけになります。そのコンテキストに個別のログインを付与できます。Telnet、SSH、および ASDM アクセスをイネーブルにする方法、また管理認証を設定する方法については、第 43 章「管理アクセスの設定」を参照してください。

リソース管理に関する情報

デフォルトでは、すべてのセキュリティ コンテキストは ASA のリソースに無制限でアクセスできますが、コンテキストあたりの上限が定められている場合を除きます。唯一の例外は、VPN のリソース（デフォルトでディセーブルになっています）です。特定のコンテキストが使用しているリソースが多すぎることが原因で、他のコンテキストが接続を拒否されるといった現象が発生した場合は、コンテキストあたりのリソースの使用量を制限するようにリソース管理を設定できます。VPN のリソースについては、VPN トンネルを許可するようにリソース管理を設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。

リソース クラス

ASA 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。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。

リソース制限値

個々のリソースの制限値は、パーセンテージ（ハード システム制限がある場合）または絶対値として設定できます。

ほとんどのリソースについては、ASA は、クラスに割り当てられたコンテキストごとにリソースの一部を確保することはしません。代わりに、ASA はコンテキストごとに上限を設定します。リソースをオーバーサブスクライブする場合や、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そのリソースを「使い果たす」ことがあり、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。例外は、VPN リソース タイプです。このリソースはオーバーサブスクライブできないため、各コンテキストに割り当てられたリソースは保証されます 割り当てられた量を超える、VPN セッションの一時的なバーストに対応できるように、ASA は「burst」という VPN リソース タイプをサポートしています。このリソースは、残りの未割り当て VPN セッションに等しくなります。バースト セッションはオーバーサブスクライブでき、コンテキストが先着順で使用できます。

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。

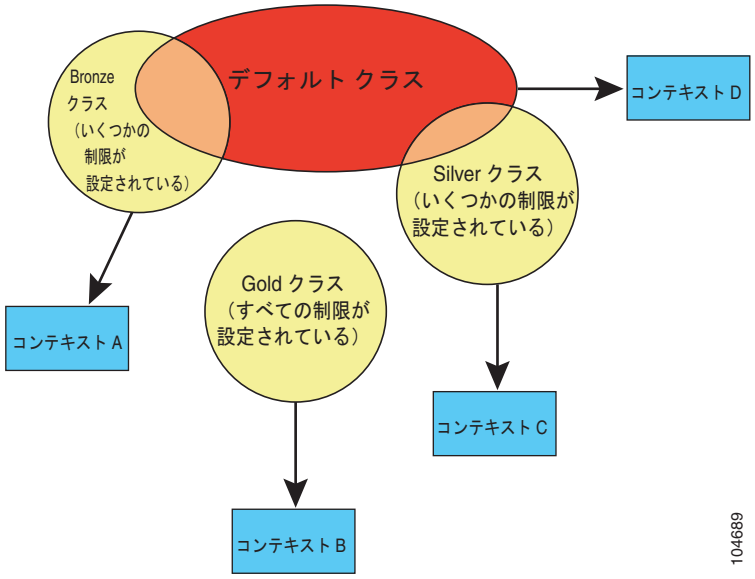
コンテキストがデフォルト クラス以外のクラスに属する場合、それらのクラス設定は常にデフォルト クラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバ コンテキストはそれらの制限にデフォルト クラスを使用します。たとえば、すべての同時接続に 2% の制限を設定したがその他の制限を設定せずにクラスを作成した場合、他のすべての制限はデフォルト クラスから継承されます。これとは逆に、すべてのリソースに対する制限値を設定してクラスを作成すると、そのクラスではデフォルト クラスの設定を何も使用しません。

ほとんどのリソースについては、デフォルト クラスではすべてのコンテキストがリソースに無制限でアクセスできます。ただし、次の制限を除きます。

- Telnet セッション：5 セッション。（コンテキストあたりの最大値）。
- SSH セッション：5 セッション。（コンテキストあたりの最大値）。
- IPsec セッション：5 セッション。（コンテキストあたりの最大値）。
- MAC アドレス：65,535 エントリ。（コンテキストあたりの最大値）。
- VPN サイトツーサイト トンネル：0 セッション。（VPN セッションを許可するようにクラスを手動で設定する必要があります）。

図 6-5 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。

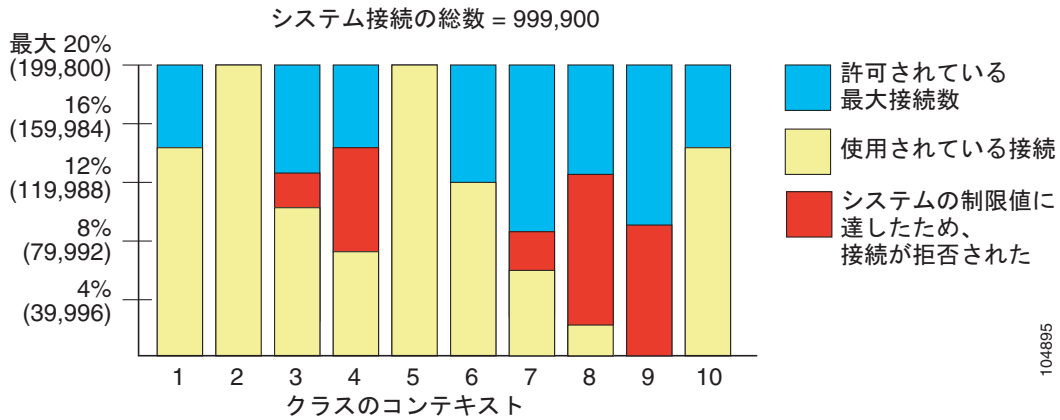
図 6-5　リソース クラス



オーバーサブスクライブ型リソースの使用

ASA をオーバーサブスクライブするには、あるリソースをコンテキストに割り当てた率の合計が 100% を超えるように割り当てます（非バーストの VPN リソースを除く）。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 6-6 を参照）。

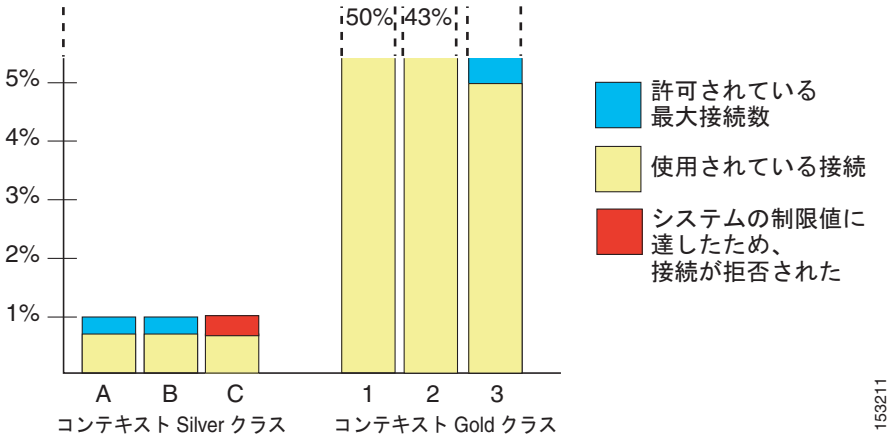
図 6-6　リソースのオーバーサブスクライブ



無制限リソースの使用

ASA 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。リソースが無制限の場合、コンテキストはシステムで使用可能な量まで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、この 3 つ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 6-7 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、ASA のオーバーサブスクライブに類似しています。

図 6-7　　無制限リソース



MAC アドレスに関する情報

コンテキスト間でのインターフェイス共有を許可するには、共有されるコンテキスト インターフェイスそれぞれに固有の MAC アドレスを割り当ててください。

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。あるインターフェイスを共有させる場合に、コンテキストごとにそのインターフェイスの固有 MAC アドレスを設定していなかった場合は、他の分類方法が試行されますが、その方法では十分にカバーされないことがあります。パケットの分類の詳細については、「ASA によるパケットの分類方法」（P.6-3）を参照してください。

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、「MAC アドレスおよび MTU の設定」（P.13-10）を参照してください。

この項では、次のトピックについて取り上げます。

デフォルトの MAC アドレス

MAC アドレスの生成をディセーブルにした場合は、デフォルトの MAC アドレスは次のようになります。

- ASA 5500 シリーズ アプライアンスの場合 : 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、1 つの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。
- ASASM の場合 : すべての VLAN インターフェイスが同じ MAC アドレスを使用します。これは、バックプレーンの MAC アドレスから導出されたものです。

「MAC アドレス形式」（P.6-12）も参照してください。

自動 MAC アドレス生成はイネーブルです。自動生成されたプレフィックスが使用されます。ASA は、インターフェイス（ASA 5500）またはバックプレーン（ASASM）MAC アドレスの最後の 2 バイトに基づいてプレフィックスを自動生成します。レガシーの自動生成方法（プレフィックスなし）は使用できません。

（注）　フェールオーバーがイネーブルの場合、フェールオーバー ペアのヒットレス アップグレードを維持するために、ASA はリロード時に既存の自動生成コンフィギュレーションを変換しません。ただし、フェールオーバーを使用するときは、プレフィックスによる生成方式に手動で変更することを強く推奨します（特に ASASM の場合）。プレフィックス方式を使用しない場合、異なるスロット番号にインストールされた ASASM では、フェールオーバーが発生した場合に MAC アドレスの変更が行われ、トラフィックの中断が発生することがあります。アップグレード後に、プレフィックス方式での MAC アドレス生成を使用するには、MAC アドレス自動生成を再度イネーブルにすると、プレフィックスが使用されるようになります。

手動 MAC アドレスとの通信

MAC アドレスを手動で割り当てた場合、自動生成がイネーブルになっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます。

自動生成されたアドレス（プレフィックスを使用するとき）は A2 で始まるため、自動生成も使用する予定のときは手動 MAC アドレスを A2 で始めることはできません。

フェールオーバー用の MAC アドレス

フェールオーバーで使用できるように、ASA 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。詳細については、「MAC アドレス形式」（P.6-12）を参照してください。

MAC アドレス形式

プレフィックスのない MAC アドレス形式はレガシー バージョンであり、新しいバージョンの ASA ではサポートされません。

ASA は、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

xx.yy はユーザ定義プレフィックスまたはインターフェイス（ASA 5500）またはバックプレーン（ASASM）MAC アドレスの最後の 2 バイトに基づいて自動生成されたプレフィックス、*zz.zzzz* は ASA によって生成される内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、ASA は 77 を 16 進数値 004D（*yyxx*）に変換します。MAC アドレスで使用すると、プレフィックスは ASA ネイティブ形式に一致するように逆にされます（*xxyy*）。

A2**4D.00***zz.zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03***zz.zzzz*

マルチ コンテキスト モードのライセンス要件

モデル	ライセンス要件
ASA 5505	サポートしない
ASA 5510	Security Plus ライセンス：2 コンテキスト *オプション ライセンス：5 コンテキスト*
ASA 5520	基本ライセンス：2 コンテキスト *オプション ライセンス：5、10、または 20 コンテキスト*
ASA 5540	基本ライセンス：2 コンテキスト *オプション ライセンス：5、10、20、または 50 コンテキスト*
ASA 5550	基本ライセンス：2 コンテキスト *オプション ライセンス：5、10、20、50、または 100 コンテキスト。*
ASA 5580	基本ライセンス：2 コンテキスト *オプション ライセンス:5、10、20、50、100、または 250 コンテキスト。*
ASA 5512-X	サポートしない
ASA 5515-X	Security Plus ライセンス：2 コンテキスト *オプション ライセンス：5 コンテキスト*
ASA 5525-X	基本ライセンス：2 コンテキスト *オプション ライセンス：5、10、または 20 コンテキスト*
ASA 5545-X	基本ライセンス：2 コンテキスト *オプション ライセンス：5、10、20、または 50 コンテキスト*
ASA 5555-X	基本ライセンス：2 コンテキスト *オプション ライセンス：5、10、20、50、または 100 コンテキスト。*
ASA 5585-X（SSP-10）	基本ライセンス：2 コンテキスト *オプション ライセンス：5、10、20、50、または 100 コンテキスト。*

モデル	ライセンス要件
ASA 5585-X（SSP-20、-40、および -60）	基本ライセンス：2 コンテキスト *オプション ライセンス:5、10、20、50、100、または 250 コンテキスト。*
ASASM	基本ライセンス：2 コンテキスト *オプション ライセンス:5、10、20、50、100、または 250 コンテキスト。*

前提条件

マルチ コンテキスト モードに切り替えた後で、システム コンフィギュレーションにアクセスするためにシステムまたは管理コンテキストに接続します。管理以外のコンテキストからシステムを設定することはできません。デフォルトでは、マルチ コンテキスト モードをイネーブルにした後はデフォルトの管理 IP アドレスを使用して管理コンテキストに接続できます。ASA に接続する方法の詳細については、第 3 章「スタートアップ ガイド」を参照してください。

注意事項と制限事項

この項では、この機能のガイドラインと制限事項について説明します。

ファイアウォール モードのガイドライン

ルーテッドおよび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ます。コンテキストごとにファイアウォール モードを設定します。

フェールオーバーのガイドライン

アクティブ/アクティブ モード フェールオーバーは、マルチ コンテキスト モードでのみサポートされます。

IPv6 のガイドライン

IPv6 をサポートします。

モデルのガイドライン

ASA 5505 および 5512-X をサポートしません。

サポートされていない機能

マルチ コンテキスト モードでサポートされていない機能は、次のとおりです。

- RIP
- OSPFv3。（OSPFv2 がサポートされます）。
- マルチキャスト ルーティング
- 脅威の検出
- ユニファイド コミュニケーション
- QoS
- リモート アクセス VPN。（サイトツーサイト VPN がサポートされます）。

その他のガイドライン

コンテキスト モード（シングルまたはマルチ）は、リブートされても持続されますが、コンフィギュレーション ファイルには保存されません。コンフィギュレーションを別のデバイスにコピーする必要がある場合は、新規デバイスのモードを match に設定します。

デフォルト設定

- デフォルトで、ASA はシングル コンテキスト モードになります。
- 「デフォルト クラス」（P.6-9）を参照してください。
- 「デフォルトの MAC アドレス」（P.6-12）を参照してください。

マルチ コンテキストの設定

この項では、マルチ コンテキスト モードを設定する方法について説明します。次の項目を取り上げます。

- 「マルチ コンテキスト モードの設定のタスク フロー」（P.6-15）
- 「マルチ コンテキスト モードのイネーブル化とディセーブル化」（P.6-16）
- 「リソース管理のクラスの設定」（P.6-17）
- 「セキュリティ コンテキストの設定」（P.6-20）
- 「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.6-24）

マルチ コンテキスト モードの設定のタスク フロー

マルチ コンテキスト モードを設定するには、次の手順を実行します。

ステップ 1　マルチ コンテキスト モードをイネーブルにします。「マルチ コンテキスト モードのイネーブル化とディセーブル化」（P.6-16）を参照してください。

ステップ 2　（任意）リソース管理のクラスを設定します。「リソース管理のクラスの設定」（P.6-17）を参照してください。

ステップ 3　システム実行スペースでインターフェイスを設定します。

- ASA 5500：第 11 章「インターフェイス コンフィギュレーションの開始（ASA 5510 以降）」
- ASASM：第 2 章「ASA サービス モジュール を使用するためのスイッチの設定」

ステップ 4　セキュリティ コンテキストを設定します。「セキュリティ コンテキストの設定」（P.6-20）を参照してください。

ステップ 5　（任意）MAC アドレス割り当てをカスタマイズします。「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.6-24）を参照してください。

ステップ 6　コンテキストのインターフェイス コンフィギュレーションを完成させます。第 13 章「インターフェイス コンフィギュレーションの実行（ルーテッド モード）」または第 14 章「インターフェイス コンフィギュレーションの実行（トランスペアレント モード）」を参照してください。

マルチ コンテキスト モードのイネーブル化とディセーブル化

シスコへの発注方法によっては、ASA がすでにマルチセキュリティ コンテキスト用に設定されている場合があります。シングル モードからマルチ モードに変換する必要がある場合は、この項の手順に従ってください。

この項では、次のトピックについて取り上げます。

マルチ コンテキスト モードのイネーブル化

シングル モードからマルチ モードに変換すると、ASA は実行コンフィギュレーションを 2 つのファイルに変換します。システム コンフィギュレーションで構成される新規スタートアップ コンフィギュレーションと、（内部フラッシュ メモリのルート ディレクトリの）管理コンテキストで構成される admin.cfg です。元の実行コンフィギュレーションは、old_running.cfg として（内部フラッシュ メモリのルート ディレクトリに）保存されます。元のスタートアップ コンフィギュレーションは保存されません。ASA は、管理コンテキストのエントリをシステム コンフィギュレーションに「admin」という名前で自動的に追加します。

前提条件

スタートアップ コンフィギュレーションをバックアップします。シングル モードからマルチ モードに変換すると、ASA は実行コンフィギュレーションを 2 つのファイルに変換します。元のスタートアップ コンフィギュレーションは保存されません。「コンフィギュレーションまたはその他のファイルのバックアップ」（P.85-18）を参照してください。

手順の詳細

コマンド	目的
mode multiple **例：** `hostname(config)# mode multiple`	マルチ コンテキスト モードに変更します。ASA をリブートするよう求められます。

シングルコンテキスト モードの復元

以前の実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてモードをシングル モードに変更するには、次の手順を実行します。

前提条件

この手順はシステム実行スペースで実行します。

手順の詳細

	コマンド	目的
ステップ 1	**copy disk0:old_running.cfg startup-config** **例：** `hostname(config)# copy disk0:old_running.cfg startup-config`	元の実行コンフィギュレーションのバックアップ バージョンを現在のスタートアップ コンフィギュレーションにコピーします。
ステップ 2	**mode single** **例：** `hostname(config)# mode single`	モードを single mode に設定します。ASA をリブートするよう求められます。

リソース管理のクラスの設定

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。

前提条件

この手順はシステム実行スペースで実行します。

ガイドライン

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
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。
conns	同時またはレート	N/A	同時接続数：モデルごとの接続制限については、「モデルごとにサポートされている機能のライセンス」（P.4-1）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）。

表 6-1　リソース名と制限 （続き）

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
hosts	同時接続数	N/A	N/A	ASA 経由で接続可能なホスト。
inspects	レート	N/A	N/A	アプリケーション インスペクション数/秒。
mac-addresses	同時接続数	N/A	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。
routes	同時接続数	N/A	N/A	ダイナミック ルート。
vpn burst other	同時接続数	N/A	モデルに応じた Other VPN セッション数から、**vpn other** 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。	**vpn other** でコンテキストに割り当てられた数を超えて許可されるサイトツーサイト VPN セッションの数。たとえば、使用するモデルで 5000 セッションがサポートされており、**vpn other** で割り当てたセッション数の合計が全コンテキストで 4000 の場合は、残りの 1000 セッションが **vpn burst other** に使用可能です。**vpn other** ではセッション数がコンテキストに対して保証されますが、対照的に **vpn burst other** ではオーバーサブスクライブが可能です。バースト プールをすべてのコンテキストが、先着順に使用できます。
vpn other	同時接続数	N/A	モデルごとの使用可能な Other VPN セッション数については、「モデルごとにサポートされている機能のライセンス」（P.4-1）を参照してください。	サイトツーサイト VPN セッション。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたセッションは、そのコンテキストに対して保証されます。
ssh	同時接続数	最小 1 最大 5	100	SSH セッション
syslogs	レート	N/A	N/A	Syslog メッセージ数/秒。
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	N/A	N/A	ネットワーク 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。

手順の詳細

	コマンド	目的
ステップ 1	**class** *name* **例：** hostname(config)# class gold	クラス名を指定して、クラス コンフィギュレーション モードを開始します。*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	**limit-resource** [**rate**] *resource_name number*[**%**] **例：** hostname(config-class)# limit-resource rate inspects 10	リソース タイプのリソース制限を設定します。リソース タイプのリストについては、表 6-1 を参照してください。**all** を指定すると、すべてのリソースが同じ値に設定されます。特定のリソースの値も指定した場合は、その制限は **all** に対して設定された制限よりも優先されます。 **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。 ほとんどのリソースについては、**0** を *number* に対して設定すると、そのリソースは無制限となるか、システム制限を上限とする（システム制限がある場合）ことになります。VPN のリソースについては、**0** を指定すると制限なしと設定されます。 システム制限がないリソースの場合は、パーセンテージ（**%**）を設定できません。絶対値のみを設定できます。

例

たとえば、conns のデフォルト クラス制限を無制限ではなく 10% に設定し、サイトツーサイト VPN トンネル 5 本と VPN バースト用のトンネル 2 本を許可するには、次のコマンドを入力します。

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
hostname(config-class)# limit-resource vpn other 5
hostname(config-class)# limit-resource vpn burst other 2
```

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
hostname(config-class)# limit-resource routes 5000
hostname(config-class)# limit-resource vpn other 10
hostname(config-class)# limit-resource vpn burst other 5
```

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のセキュリティ コンテキスト定義では、コンテキスト名、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、およびその他の設定値を指定します。

前提条件

- この手順はシステム実行スペースで実行します。
- ASASM では、第 2 章「ASA サービス モジュール を使用するためのスイッチの設定」に従ってスイッチ上の ASASM に VLAN を割り当てます。
- ASA 5500 では、物理インターフェイス パラメータ、VLAN サブインターフェイス、EtherChannel、および冗長インターフェイスを第 11 章「インターフェイス コンフィギュレーションの開始（ASA 5510 以降）」に従って設定します。
- 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
```

このコンテキストはコンフィギュレーション内にまだ存在しませんが、続いて **context** *name* コマンドを入力して管理コンテキスト コンフィギュレーションに進むことができます。

手順の詳細

	コマンド	目的
ステップ 1	**context** *name* **例：** `hostname(config)# context administrator`	コンテキストを追加または編集します。*name* は最大 32 文字の文字列です。この名前で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 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） **description** *text* **例：** `hostname(config-ctx)# description Administrator Context`	このコンテキストの説明を追加します。

コマンド	目的
ステップ 3　インターフェイスを割り当てるには： **allocate-interface** *interface_id* [*mapped_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： **allocate-interface** *interface_id.subinterface*[**-***interface_id.subinterface*] [*mapped_name*[**-***mapped_name*]] [**visible** | **invisible**] **例：** 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	コンテキストで使用できるインターフェイスを指定します。インターフェイス タイプとポート番号の間にスペースを含めないでください。 これらのコマンドを複数回入力して複数の範囲を指定します。 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、限られた数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、専用の管理インターフェイスである管理スロット/ポート（物理、サブインターフェイス、冗長、または EtherChannel）を管理トラフィック用の追加インターフェイスとして使用できます。独立した管理インターフェイスは、ASASM では使用できません。 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。 *mapped_name* は、インターフェイスの英数字のエイリアスで、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ます。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。セキュリティ目的で、コンテキストがどのインターフェイスを使用しているかをコンテキスト管理者には知らせないようにすることができます。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、gig0/1.1-gig0/1.5 **happy**1-**sad**5 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、gig0/0.**100**-gig0/0.**199** int**1**-int**15** と入力した場合、コマンドは失敗します。 マッピング名を設定している場合に **show interface** コマンドで実際のインターフェイス ID を参照するには、**visible** を指定します。デフォルトの **invisible** キーワードでは、マッピング名のみが表示されます。

	コマンド	目的

ステップ 4	**config-url** *url*
	
	例：
	`hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg`
		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 を識別します。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。最初に **config-url** コマンドを入力した場合、ASA 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。そのコンテキストが（未設定）インターフェイスを参照するコマンドを含んでいる場合、それらのコマンドは失敗します。
		
		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。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。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 url`
		`INFO: Creating context with default config`
		
		HTTP（S）以外の URL の場合、対象 URL にファイルを書き込むには、URL を指定した後、そのコンテキストに変更し、CLI に設定して、**write memory** コマンドを入力します。（HTTP（S）は読み取り専用です）。
		
		（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。
		
		使用可能な URL は次のタイプがあります。**disk***number*（フラッシュ メモリ用）、**ftp**、**http**、**https**、または **tftp**。
		
		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.6-27）を参照してください。

ステップ 5	（任意） **member** *class_name* **例：** `hostname(config-ctx)# member gold`	コンテキストをリソース クラスに割り当てます。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。
ステップ 6	（任意） **allocate-ips** *sensor_name* [*mapped_name*] [**default**] **例：** `hostname(config-ctx)# allocate-ips sensor1 highsec`	このコンテキストに IPS 仮想センサーを割り当てます（IPS モジュールがインストールされている場合）。 仮想センサーの詳細については、「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（ASA 5510 以降）」（P.65-16）を参照してください。

	コマンド	目的
ステップ 7	（任意） **join-failover-group** {**1** | **2**) **例：** hostname(config-ctx)# join-failover-group 2	アクティブ/アクティブ フェールオーバーのフェールオーバー グループにコンテキストを割り当てます。デフォルトでは、コンテキストはグループ 1 にあります。管理コンテキストは常にグループ 1 に置く必要があります。 フェールオーバー グループに関する詳細については、「プライマリ フェールオーバー装置の設定」（P.10-10）を参照してください。
ステップ 8	（任意） **scansafe** [**license** *key*] **例：** hostname(config-ctx)# scansafe	このコンテキストに対してクラウド Web セキュリティをイネーブルにします。 **license** を指定しない場合は、システム コンフィギュレーションで設定されているライセンスがこのコンテキストで使用されます。ASA は、要求がどの組織からのものかを示すために、認証キーを クラウド Web セキュリティ プロキシ サーバに送信します。認証キーは 16 バイトの 16 進数です。 ScanSafe の詳細については、「Cisco クラウド Web セキュリティ用の ASA の設定」（P.60-1）を参照してください。

例

次の例では、管理コンテキストを「administrator」と設定し、「administrator」というコンテキストを内部フラッシュ メモリに作成してから、2 つのコンテキストを FTP サーバから追加します。

```
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 disk0:/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

この項では、MAC アドレスの自動生成の設定方法について説明します。

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。詳細については、「MAC アドレスに関する情報」（P.6-11）を参照してください（特に、以前の ASA バージョンからアップグレードする場合）。「割り当てられた MAC アドレスの表示」（P.6-38）も参照してください。

ガイドライン

- コンテキストのインターフェイスに **nameif** コマンドを設定すると、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設定した後でこの機能をイネーブルにした場合は、イネーブルにした直後に、すべてのインターフェイスの MAC アドレスが生成されます。この機能をディセーブルにすると、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。
- 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、「MAC アドレスおよび MTU の設定」（P.13-10）を参照してください。

手順の詳細

コマンド	目的
mac-address auto [**prefix** *prefix*]	プライベート MAC アドレスを各コンテキスト インターフェイスに自動的に割り当てます。
例： `hostname(config)# mac-address auto prefix 19`	プレフィックスを入力しない場合は、ASA によって、インターフェイス（ASA 5500）またはバックプレーン（ASASM）MAC アドレスの最後の 2 バイトに基づいてプレフィックスが自動生成されます。 手動でプレフィックスを入力する場合は、*prefix* に 0 ～ 65535 の 10 進数値を指定します。このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。プレフィックスの使用方法の詳細については、「MAC アドレス形式」（P.6-12）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（または管理コンテキスト）にログインした場合は、コンテキストを切り替えながら、各コンテキスト内でコンフィギュレーションやタスクのモニタリングを実行することができます。コンフィギュレーション モードで編集される、つまり **copy** コマンドや **write** コマンドで使用される実行コンフィギュレーションは、ユーザのログイン先によって決まります。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。

手順の詳細

コマンド	目的
changeto context *name*	コンテキストに変更します。プロンプトが次のように変化します。 hostname/*name*#
changeto system	システム実行スペースに切り替えます。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

現在の管理コンテキストは削除できません。ただし、**clear context** コマンドを使用してすべてのコンテキストを削除すれば、管理コンテキストも削除できます。

（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。

前提条件

この手順はシステム実行スペースで実行します。

手順の詳細

コマンド	目的
no context *name*	シングル コンテキストを削除します。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。コンテキスト コンフィギュレーション ファイルがコンフィギュレーション URL の場所から削除されることはありません。
clear context	すべてのコンテキスト（管理コンテキストを含みます）を削除します。コンテキスト コンフィギュレーション ファイルがコンフィギュレーション URL の場所から削除されることはありません。

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。

ガイドライン

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。

前提条件

この手順はシステム実行スペースで実行します。

手順の詳細

コマンド	目的
admin-context *context_name* **例：** `hostname(config)# admin-context administrator`	管理コンテキストを設定します。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）** いくつかのシステム コンフィギュレーション コマンド、たとえば **ntp server** では、管理コンテキストに所属するインターフェイス名が指定されます。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

この項では、コンテキスト URL を変更する方法について説明します。

ガイドライン

- 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。ASA 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。

前提条件

この手順はシステム実行スペースで実行します。

手順の詳細

	コマンド	目的

ステップ 1	（マージを実行しない場合は、任意）
	changeto context *name*
	clear configure all
	
	例：
	`hostname(config)# changeto context ctx1`
	`hostname/ctx1(config)# clear configure all`
		コンテキストに切り替えて、設定を削除します。マージを実行する場合は、ステップ 2 にスキップします。

ステップ 2	**changeto system**
	
	例：
	`hostname/ctx1(config)# changeto system`
	`hostname(config)#`
		システム実行スペースに切り替えます。

	コマンド	目的
ステップ 3	**context** *name* **例：** hostname(config)# context ctx1	変更するコンテキストのコンテキスト コンフィギュレーション モードを開始します。
ステップ 4	**config-url** *new_url* **例：** hostname(config)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/ctx1.cfg	新しい URL を入力します。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.6-28）
- 「コンテキストの削除および再追加によるリロード」（P.6-29）

コンフィギュレーションのクリアによるリロード

コンテキストをリロードするために、コンテキスト コンフィギュレーションをクリアしてコンフィギュレーションを URL からリロードするには、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	**changeto context** *name* **例：** hostname(config)# changeto context ctx1 hostname/ctx1(comfig)#	リロードするコンテキストに変更します。

	コマンド	目的
ステップ 2	**clear configure all** **例：** `hostname/ctx1(config)# clear configure all`	実行コンフィギュレーションをクリアします。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 3	**copy startup-config running-config** **例：** `hostname/ctx1(config)# copy startup-config running-config`	設定をリロードします。ASA 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. 「セキュリティ コンテキストの削除」（P.6-25）。
2. 「セキュリティ コンテキストの設定」（P.6-20）

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.6-29）
- 「リソース割り当ての表示」（P.6-31）
- 「リソースの使用状況の表示」（P.6-34）
- 「コンテキストでの SYN 攻撃のモニタリング」（P.6-36）
- 「割り当てられた MAC アドレスの表示」（P.6-38）

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。

コマンド	目的
show context [*name* | **detail**| **count**]	すべてのコンテキストを表示します。 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。 **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。 **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。この出力例は、3 個のコンテキストを示しています。

```
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	ASA 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、コマンド リファレンス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。

コマンド	目的
show resource allocation [**detail**]	リソース割り当てを表示します。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.6-34）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%
 Routes                       5000           N/A
 Telnet                         35           35.00%
 Xlates                      91749           N/A
 Other VPN Sessions             20           2.66%
 Other VPN Burst                20           2.66%
 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。
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、ASA 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%

Routes           default          all       C  unlimited                N/A
                 gold               1       D  unlimited          5     N/A
                 silver             1      CA         10         10     N/A
                 bronze             0      CA          5                N/A
                 All Contexts:      3                            20     N/A

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。 ASA 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、ASA 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。

コマンド	目的
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
Other VPN Sessions        0            10       10           740 Summary
Other VPN Burst           0            10       10           730 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
Routes                      0            0        N/A             0    System
IPSec                       0            0          5             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
Other VPN Sessions          0           10        750           740    System
Other VPN Burst             0           10        750           730    System
```

コンテキストでの SYN 攻撃のモニタリング

ASA 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、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。

次のコマンドを使用して SYN 攻撃をモニタします。

コマンド	目的
show perfmon	各コンテキストについて、攻撃の割合をモニタリングします。
show resource usage detail	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の量をモニタします。
show resource usage summary detail	システム全体の TCP 代行受信で使用されるリソースをモニタします。

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 （**太字**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（**太字**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
```

割り当てられた MAC アドレスの表示

システム コンフィギュレーション内またはコンテキスト内の自動生成された MAC アドレスを表示できます。この項では、次のトピックについて取り上げます。

- 「システム コンフィギュレーションでの MAC アドレスの表示」（P.6-38）
- 「コンテキスト内の MAC アドレスの表示」（P.6-39）

システム コンフィギュレーションでの MAC アドレスの表示

この項では、システム コンフィギュレーション内の MAC アドレスを表示する方法について説明します。

ガイドライン

MAC アドレスをインターフェイスに手動で割り当てるものの、その際に自動生成がイネーブルになっていると、手動 MAC アドレスが使用中のアドレスとなりますが、コンフィギュレーションには自動生成されたアドレスが引き続き表示されます。後で手動 MAC アドレスを削除すると、表示されている自動生成アドレスが使用されます。

手順の詳細

コマンド	目的
show running-config all context [*name*]	システム実行スペースから割り当てられた MAC アドレスを表示します。 割り当てられた MAC アドレスを表示するには、**all** オプションが必要です。**mac-address auto** コマンドは、グローバル コンフィギュレーション モードに限りユーザ設定可能ですが、コンテキスト コンフィギュレーション モードでは、このコマンドは読み取り専用エントリとして、割り当てられた MAC アドレスとともに表示されます。コンテキスト内で **nameif** コマンドで設定される割り当て済みのインターフェイスだけに MAC アドレスが割り当てられます。

例

show running-config all context admin コマンドからの次の出力には、Management0/0 インターフェイスに割り当てられたプライマリおよびスタンバイ MAC アドレスが表示されます。

```
hostname# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

show running-config all context コマンドからの次の出力には、すべてのコンテキスト インターフェイスのすべての MAC アドレス（プライマリおよびスタンバイ）が表示されます。GigabitEthernet0/0 と GigabitEthernet0/1 の各メイン インターフェイスはコンテキスト内部に **nameif** コマンドで設定されないため、それらのインターフェイスの MAC アドレスは生成されていないことに注意してください。

```
hostname# show running-config all context

admin-context admin
```

```
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

コンテキスト内の MAC アドレスの表示

この項では、コンテキスト内で MAC アドレスを表示する方法について説明します。

手順の詳細

コマンド	目的
show interface | include (Interface)|(MAC)	コンテキスト内で各インターフェイスに使用されている MAC アドレスを表示します。

例

たとえば、次のように入力します。

```
hostname/context# show interface | include (Interface)|(MAC)

Interface GigabitEthernet1/1.1 "g1/1.1", is down, line protocol is down
        MAC address a201.0101.0600, MTU 1500
Interface GigabitEthernet1/1.2 "g1/1.2", is down, line protocol is down
        MAC address a201.0102.0600, MTU 1500
```

```
Interface GigabitEthernet1/1.3 "g1/1.3", is down, line protocol is down
        MAC address a201.0103.0600, MTU 1500
...
```

（注）　**show interface** コマンドは、使用中の MAC アドレスを表示します。MAC アドレスを手動で割り当てた場合に、自動生成がイネーブルになっていたときは、システム コンフィギュレーション内の未使用の自動生成アドレスのみを表示できます。

マルチ コンテキスト モードの設定例

次に例を示します。

- 各コンテキストの MAC アドレスを、カスタム プレフィックスを使用して自動的に設定します。
- conns のデフォルト クラス制限を、無制限ではなく 10% に設定し、VPN other セッション数を 10、バーストを 5 に設定します。
- gold リソース クラスを作成します。
- 管理コンテキストを「administrator」と設定します。
- 「administrator」というコンテキストを、デフォルトのリソース クラスの一部になるように、内部フラッシュ メモリ上に作成します。
- gold リソース クラスの一部として FTP サーバから 2 個のコンテキストを追加します。

```
hostname(config)# mac-address auto prefix 19

hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
hostname(config-class)# limit-resource vpn other 10
hostname(config-class)# limit-resource vpn burst other 5

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
hostname(config-class)# limit-resource routes 700
hostname(config-class)# limit-resource vpn other 100
hostname(config-class)# limit-resource vpn burst other 50

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 disk0:/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 gold
```

マルチ コンテキスト モードの機能履歴

表 6-5 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 6-5　マルチ コンテキスト モードの機能履歴

機能名	プラットフォーム リリース	機能情報
マルチセキュリティ コンテキスト	7.0(1)	マルチ コンテキスト モードが導入されました。 **context**、**mode**、**class** の各コマンドが導入されました。
MAC アドレス自動割り当て	7.2(1)	コンテキスト インターフェイスへの MAC アドレス自動割り当てが導入されました。 **mac-address auto** コマンドが導入されました。
リソース管理	7.2(1)	リソース管理が導入されました。 **class**、**limit-resource**、**member** の各コマンドが導入されました。
IPS 仮想センサー	8.0(2)	IPS ソフトウェアのバージョン 6.0 以降を実行している AIP SSM では、複数の仮想センサーを実行できます。つまり、AIP SSM に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。各コンテキストまたはシングル モード 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。 **allocate-ips** コマンドが導入されました。

表 6-5　マルチ コンテキスト モードの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
MAC アドレス自動割り当ての機能強化	8.0(5)/8.2(2)	MAC アドレス形式が変更されました。プレフィックスが使用され、固定開始値（A2）が使用されます。また、フェールオーバー ペアのプライマリ装置とセカンダリ装置の MAC アドレスそれぞれに異なるスキームが使用されます。MAC アドレスはリロード後も維持されるようになりました。コマンド パーサーは現在、自動生成がイネーブルになっているかどうかをチェックします。MAC アドレスを手動でも割り当てることができるようにする場合は、A2 を含む手動 MAC アドレスは開始できません。 **mac-address auto prefix** コマンドが変更されました。
ASA 5550 および 5580 の最大コンテキスト数の増加	8.4(1)	ASA 5550 の最大セキュリティ コンテキスト数が 50 から 100 に増加しました。ASA 5580 での最大数が 50 から 250 に増加しました。
MAC アドレスの自動割り当てのデフォルトでのイネーブル化	8.5(1)	MAC アドレスの自動割り当てが、デフォルトでイネーブルになりました。 **mac-address auto** コマンドが変更されました。

表 6-5　マルチ コンテキスト モードの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
MAC アドレス プレフィックスの自動生成	8.6(1)	マルチ コンテキスト モードでは、現在、ASA は、MAC アドレスの自動生成設定をデフォルトのプレフィックスを使用するように変換します。ASA は、インターフェイス（ASA 5500）またはバックプレーン（ASASM）MAC アドレスの最後の 2 バイトに基づいてプレフィックスを自動生成します。この変換は、リロード時または MAC アドレス生成を再度イネーブルにすると、自動的に行われます。生成のプレフィックス方式は、セグメント上で一意の MAC アドレスがより適切に保証されるなど、多くの利点をもたらします。**show running-config mac-address** コマンドを入力して、自動生成されたプレフィックスを表示できます。プレフィックスを変更する場合、カスタム プレフィックスによって機能を再設定できます。MAC アドレス生成の従来の方法は使用できなくなります。 **（注）** フェールオーバー ペアのヒットレス アップグレードを維持するため、ASA は、フェールオーバーがイネーブルである場合、リロード時に既存のコンフィギュレーションの MAC アドレス方式を変換*しません*。ただし、フェールオーバーを使用するときは、プレフィックスによる生成方式に手動で変更することを強く推奨します（特に ASASM の場合）。プレフィックス方式を使用しない場合、異なるスロット番号にインストールされた ASASM では、フェールオーバーが発生した場合に MAC アドレスの変更が行われ、トラフィックの中断が発生することがあります。アップグレード後に、MAC アドレス生成のプレフィックス方式を使用するには、デフォルトのプレフィックスを使用する MAC アドレス生成を再びイネーブルにします。 **mac-address auto** コマンドが変更されました。
セキュリティ コンテキストでのダイナミック ルーティング	9.0(1)	EIGRP と OSPFv2 ダイナミック ルーティング プロトコルが、マルチ コンテキスト モードでサポートされるようになりました。OSPFv3、RIP、およびマルチキャスト ルーティングはサポートされません。
ルーティング テーブル エントリのための新しいリソース タイプ	9.0(1)	新規リソース タイプ routes が作成されました。これは、各コンテキストでのルーティング テーブル エントリの最大数を設定するためです。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各コマンドが変更されました。

表 6-5　マルチ コンテキスト モードの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
マルチ コンテキスト モードのサイトツーサイト VPN	9.0(1)	サイトツーサイト VPN トンネルが、マルチ コンテキスト モードでサポートされるようになりました。
サイトツーサイト VPN トンネルのための新しいリソース タイプ	9.0(1)	新しいリソース タイプ vpn other と vpn burst other が作成されました。これは、各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するためです。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各コマンドが変更されました。