CHAPTER 9

セキュリティ コンテキストの設定

この章では、セキュリティ コンテキストの使用方法とマルチ コンテキスト モードをイネーブルにする方法について説明します。この章は、次の項で構成されています。

セキュリティ コンテキストの概要

1 台のセキュリティ アプライアンスを、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することができます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスです。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 モードでは、ルーティング テーブル、ファイア ウォール機能、IPS、管理など、多くの機能がサポートされます。VPN、ダイナミック ルーティング プロトコルなど、いくつかの機能はサポートされません。

マルチ コンテキスト モードの場合、セキュリティ アプライアンス には、セキュリティ ポリシー、インターフェイス、およびスタンドアロン デバイスで設定できるほとんどのオプションを識別するコンテキストごとのコンフィギュレーションが含まれます。システム管理者は、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、セキュリティ アプライアンス 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。

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。

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 コンテキストへの管理アクセス」（P.9-9）

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。セキュリティ アプライアンス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。
- 複数のセキュリティ アプライアンスが必要なネットワークを使用している。

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。

- ダイナミック ルーティング プロトコル

  セキュリティ コンテキストは、スタティック ルートのみサポートします。マルチコンテキスト モードで OSPF または Routing Information Protocol（RIP）をイネーブルにすることはできません。
- VPN
- マルチキャスト ルーティング。マルチキャスト ブリッジはサポートされています。
- 脅威の検出

コンテキスト コンフィギュレーション ファイル

それぞれのコンテキストにコンフィギュレーション ファイルがあり、セキュリティ ポリシーおよびインターフェイスが指定されます。サポートされる機能のオプションはすべて、スタンドアロン装置で設定できます。コンテキスト コンフィギュレーションは、内部フラッシュ メモリまたは外部フラッシュ メモリ カードに保存することも、TFTP サーバ、FTP サーバ、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。

セキュリティ アプライアンスには、個別のセキュリティ コンテキストだけでなく、コンテキストのリストなどセキュリティ アプライアンスの基本設定を識別するシステム コンフィギュレーションが含まれています。シングル モード コンフィギュレーションと同様、このコンフィギュレーションもスタートアップ コンフィギュレーションに常駐しています。

システム コンフィギュレーションには、自分自身のネットワーク インターフェイスまたはネットワーク設定は含まれません。システムがネットワーク リソースにアクセスする必要が生じたとき（サーバからコンテキストをダウンロードするときなど）は、管理コンテキストとして指定された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。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。

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

セキュリティ アプライアンス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、セキュリティ アプライアンスは、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.9-3）
- 「無効な分類子の基準」（P.9-4）
- 「分類の例」（P.9-5）

（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.9-3）
- 「固有の MAC アドレス」（P.9-3）
- 「NAT コンフィギュレーション」（P.9-3）

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、セキュリティ アプライアンス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

マルチ コンテキストがインターフェイスを共有している場合、分類子はインターフェイス MAC アドレスを使用します。セキュリティ アプライアンスでは、各コンテキストで異なる MAC アドレスを同一の共有インターフェイス（共有物理インターフェイスまたは共有サブインターフェイス）に割り当てることができます。デフォルトでは、共有インターフェイスには固有の MAC アドレスがありません。インターフェイスは、すべてのコンテキストの物理インターフェイスの焼き付け済み MAC アドレスを使用します。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。それぞれのインターフェイスを設定するときに、手動で MAC アドレスを設定できます（[Add/Edit Interface] > [Advanced] を参照）。または、自動的に MAC アドレスを生成することもできます（セキュリティ コンテキストを参照）。

NAT コンフィギュレーション

固有の MAC アドレスがない場合、分類子はパケットを代行受信し、宛先 IP アドレス ルックアップを実行します。その他のすべてのフィールドは無視され、宛先 IP アドレスだけが使用されます。分類に宛先アドレスを使用するには、分類子が、各セキュリティ コンテキストの背後にあるサブネットを認識できる必要があります。分類子は、Network Address Translation（NAT; ネットワーク アドレス変換）コンフィギュレーションに基づいて各コンテキストのサブネットを判別します。分類子は、宛先 IP アドレスを **static** コマンドまたは **global** コマンドのいずれかと照合します。**global** コマンドの場

合、分類子は、**nat** コマンドまたはアクティブな NAT セッションを照合してパケットを分類する必要がありません。分類後にパケットが宛先 IP アドレスと通信ができるかどうかは、NAT および NAT 制御の設定方法によります。

たとえば、コンテキスト管理者が各コンテキストの **static** コマンドを次のように設定した場合、分類子はサブネット 10.10.10.0、10.20.10.0、および 10.30.10.0 を認識します。

- コンテキスト A：

```
static (inside,shared) 10.10.10.0 10.10.10.0 netmask 255.255.255.0
```

- コンテキスト B：

```
static (inside,shared) 10.20.10.0 10.20.10.0 netmask 255.255.255.0
```

- コンテキスト C：

```
static (inside,shared) 10.30.10.0 10.30.10.0 netmask 255.255.255.0
```

（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。

無効な分類子の基準

次のコンフィギュレーションは、パケットの分類に使用されません。

- NAT 免除：分類子は、分類の目的では NAT 免除コンフィギュレーションは使用しません。これは、NAT 免除がマッピング インターフェイスを識別しないためです。
- ルーティング テーブル：コンテキストに、あるサブネットへのネクストホップとして外部ルータをポイントするスタティック ルートが含まれており、別のコンテキストに、同じサブネットに対する **static** コマンドが含まれている場合、分類子は **static** コマンドを使用してそのサブネットを宛先とするパケットを分類し、スタティック ルートを無視します。

分類の例

図 9-1 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 9-1　MAC アドレスを使用した共有インターフェイスを持つパケット分類

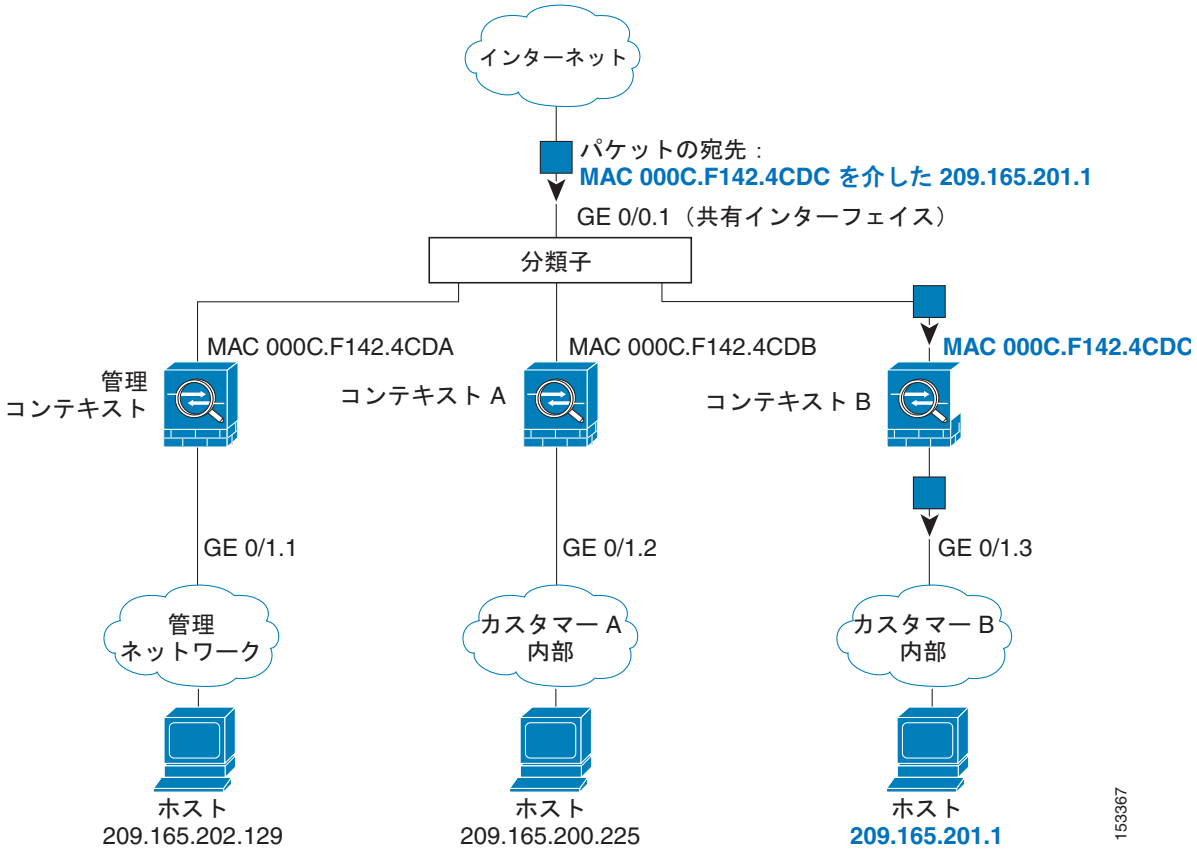
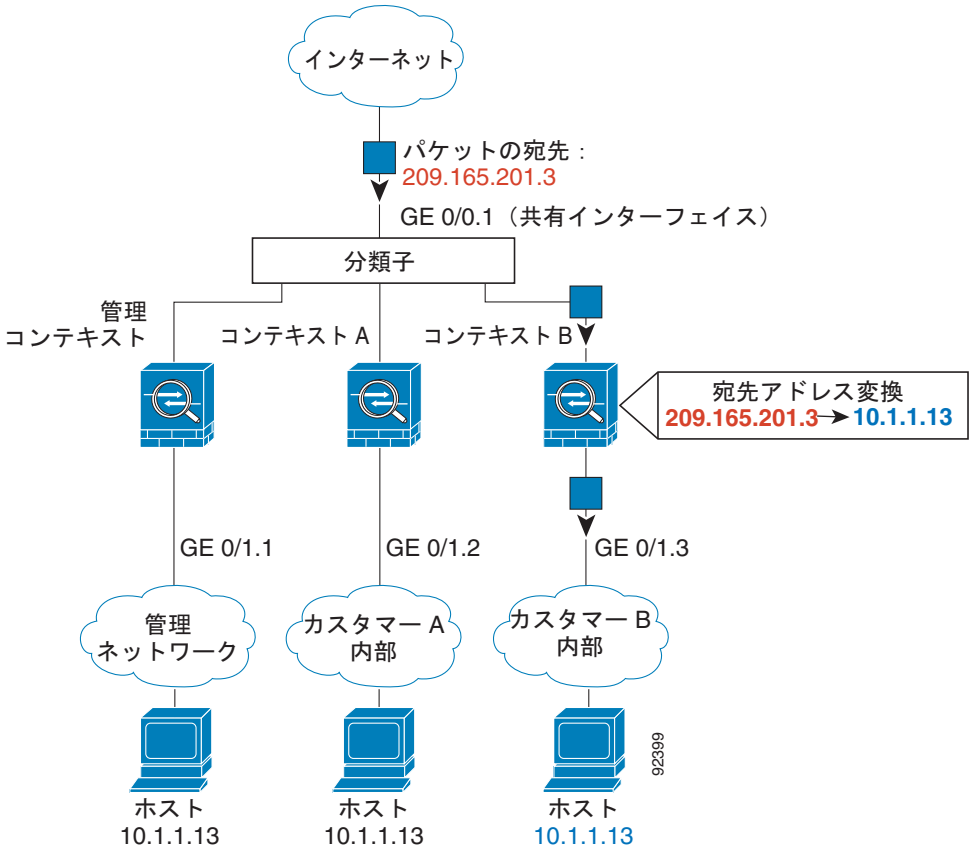


図 9-2 に、MAC アドレスが割り当てられていない外部インターフェイスを共有するマルチコンテキストを示します。コンテキスト B には宛先アドレスに一致するアドレス変換が含まれるため、分類子はパケットをコンテキスト B に割り当てます。

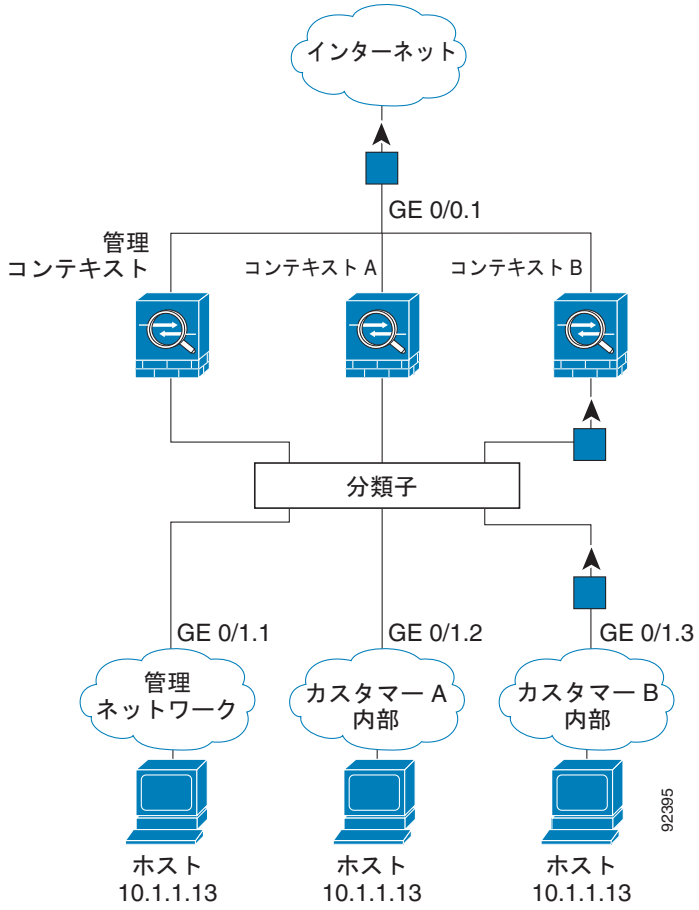
図 9-2　NAT を使用した共有インターフェイスを持つパケット分類



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 9-3 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。

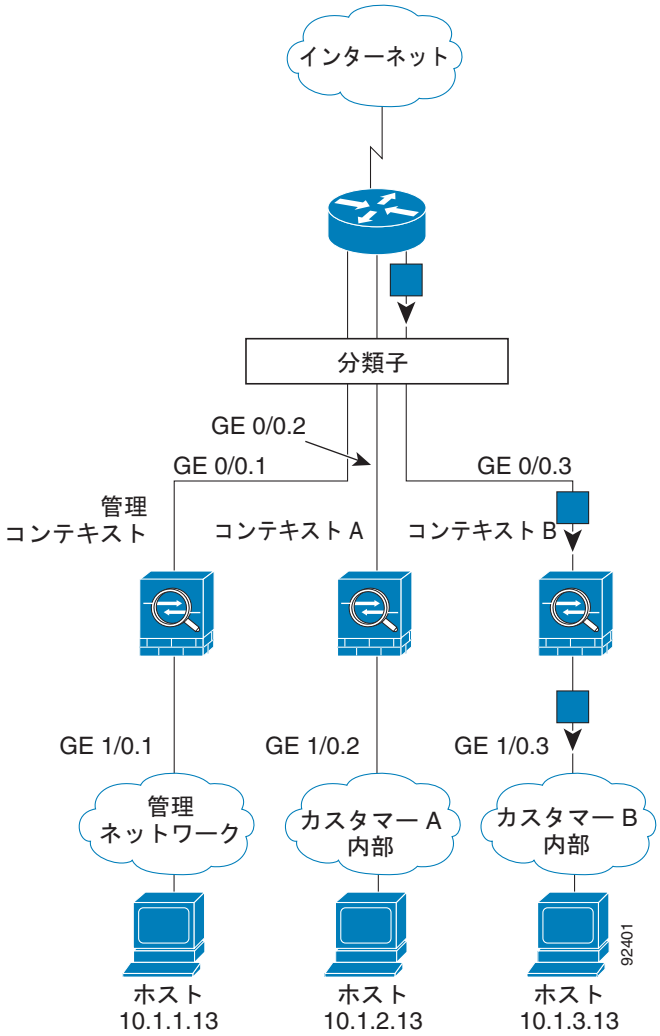
（注） *内部*インターフェイスを共有し、固有の MAC アドレスを使用していない場合、分類子には重要な制限事項がいくつかあります。分類子は、アドレス変換コンフィギュレーションに基づいてコンテキスト内のパケットを分類します。そのトラフィックの*宛先*アドレスを変換する必要があります。通常は外部アドレスに対して NAT を実行しないため、パケットを共有インターフェイスの内部から外部へ送信できない場合もあります。これは、Web のように巨大な外部ネットワークで、外部 NAT コンフィギュレーションのアドレスを予測できないためです。内部インターフェイスを共有する場合、固有の MAC アドレスを使用することをお勧めします。

図 9-3　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 9-4 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 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 9-4　トランスペアレント ファイアウォールのコンテキスト



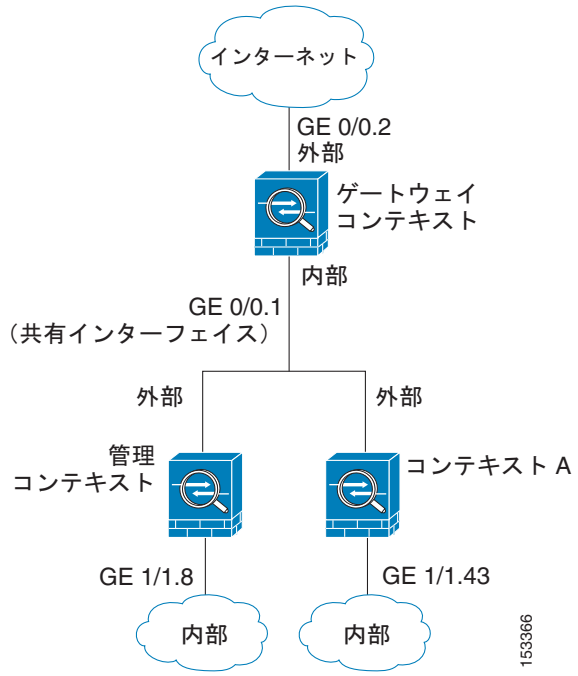
セキュリティ コンテキストのカスケード接続

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。あるコンテキストの外部インターフェイスは、別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 アドレスを設定する必要があります。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 9-5 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 9-5　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

セキュリティ アプライアンスでは、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.9-10）
- 「コンテキスト管理者のアクセス」（P.9-10）

システム管理者のアクセス

セキュリティ アプライアンス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。

- セキュリティ アプライアンス 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。

- 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 13 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。

管理またはシステム コンテキストから特定のコンテキストに変更すると、ユーザ名がデフォルトの「enable_15」ユーザ名に変更されます。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か、またはコンテキストのコマンド許可コンフィギュレーションで十分な特権を与えられる別の名前でログインできます。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 に変更したら、ユーザ名が変わるため、**login** コマンドを入力して再度「admin」で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 SDM アクセスをイネーブルにして管理認証を設定するには、第 13 章「管理アクセスの設定」を参照してください。

CLI でのマルチ コンテキスト モードのイネーブル化またはディセーブル化

シスコへの発注方法によっては、セキュリティ アプライアンス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。ただし、アップグレードする場合は、この項で説明する手順に従ってシングル モードからマルチ モードに変換することが必要になる場合があります。

ASDM では、High Availability and Scalability Wizard を使用し、Active/Active フェールオーバーをイネーブルにした場合、シングル モードからマルチ モードへの変更をサポートします。詳細については、「High Availability and Scalability Wizard へのアクセスと使用」（P.14-5）を参照してください。

Active/Active フェールオーバーを使用しない場合、またはシングル モードに戻す場合は、CLI でモードを変更する必要があります。この項では、CLI でのモード変更について説明します。説明する内容は次のとおりです。

この項では、次のトピックについて取り上げます。

- 「シングルコンテキスト モードの復元」（P.9-11）

シングル モード コンフィギュレーションのバックアップ

シングル モードからマルチ モードに変換すると、セキュリティ アプライアンス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ないため、実行コンフィギュレーションと異なる場合は、手順を進める前にバックアップを取る必要があります。

マルチ コンテキスト モードのイネーブル化

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、**mode** コマンドを使用して、新規デバイスのモードを match に設定します。

シングル モードからマルチ モードに変換すると、セキュリティ アプライアンス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（内部フラッシュ メモリのルート ディレクトリ内）として保存されます。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。セキュリティ アプライアンスは、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。

マルチモードをイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# mode multiple
```

セキュリティ アプライアンス 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

マルチ モードからシングル モードに変換する場合は、先にスタートアップ コンフィギュレーション全体（使用可能な場合）をセキュリティ アプライアンスにコピーすることを推奨します。マルチ モードから継承されるシステム コンフィギュレーションは、シングル モード デバイスで完全に機能するコンフィギュレーションではありません。システム コンフィギュレーションは、自身のコンフィギュレーションの一部としてネットワーク インターフェイスを持たないため、コンソールからセキュリティ アプライアンスにアクセスしてコピーをとる必要があります。

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、システム実行スペースで次の手順を実行します。

ステップ 1　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するには、システムの実行スペースで次のコマンドを入力します。

```
hostname(config)# copy flash:old_running.cfg startup-config
```

（注）　現在実行中のコンフィギュレーションを保存しないように注意してください。保存するとコピーしたコンフィギュレーションが上書きされます。

ステップ 2　モードをシングルモードに設定するには、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)# mode single
```

セキュリティ アプライアンス がリブートします。

リソース クラスの設定

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。

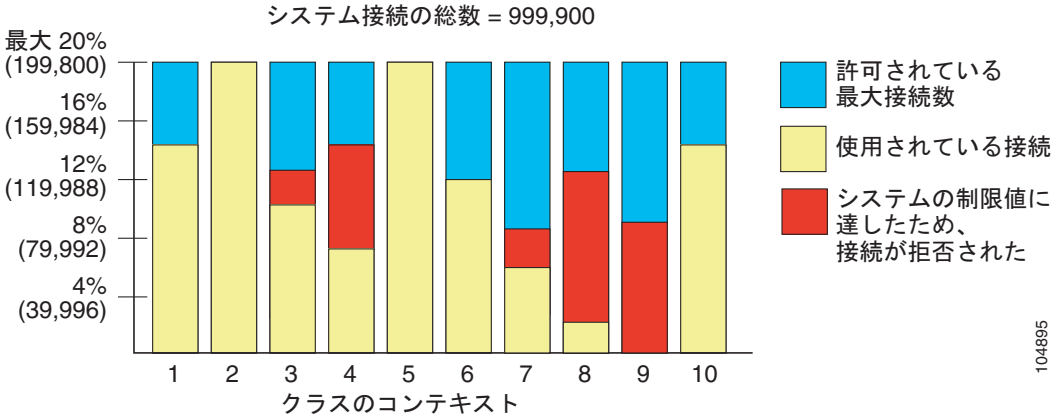
リソース制限

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 9-6 を参照）。

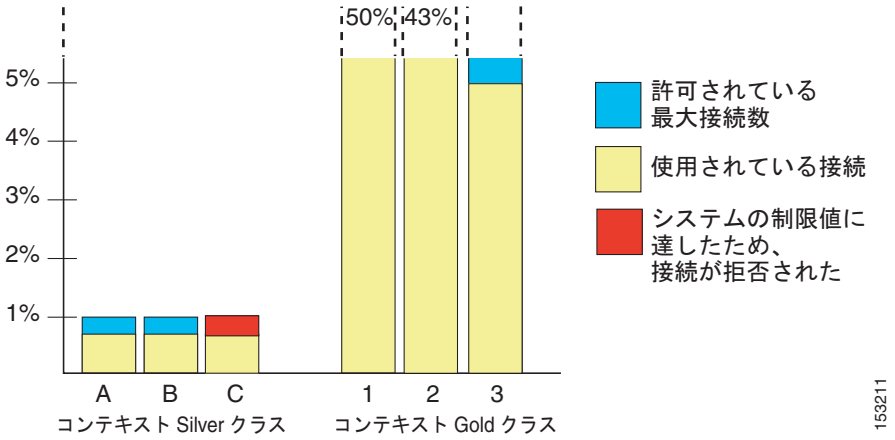
図 9-6　リソースのオーバーサブスクライブ



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 9-7 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、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 9-7　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。

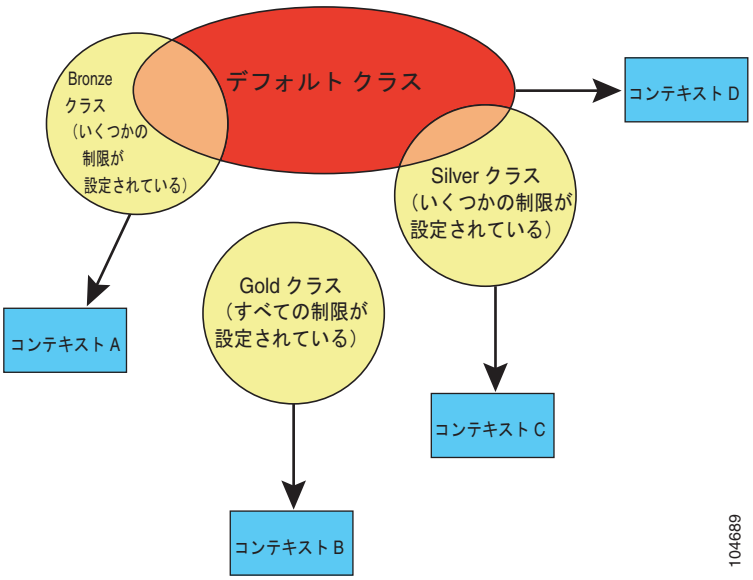
コンテキストがデフォルト クラス以外のクラスに属する場合、それらのクラス設定は常にデフォルト クラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバ コンテキストはそれらの制限にデフォルト クラスを使用します。たとえば、すべての同時接続に 2% の制限を設定したがその他の制限を設定せずにクラスを作成した場合、他のすべての制限はデフォルト クラスから継承されます。これとは逆に、すべてのリソースに対する制限値を設定してクラスを作成すると、そのクラスではデフォルト クラスの設定を何も使用しません。

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 9-8 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 9-8　　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。

リソース クラスの追加

リソース クラスを追加するには、次の手順を実行します。

ステップ 1　まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2　[Context Management] > [Resource Class] ペインで、[Add] をクリックします。

[Add Resource Class] ダイアログボックスが表示されます。

ステップ 3　[Resource Class] フィールドに、クラスの名前を 20 文字以内で入力します。

ステップ 4　[Count Limited Resources] 領域で、リソースの同時接続制限を設定します。

システム制限のないリソースは、パーセント（%）で設定できません。設定できるのは絶対値だけです。制限を設定しない場合、デフォルト クラスの制限値が継承されます。制限値がデフォルト クラスにない場合は、リソースは無制限またはシステム制限値（使用できる場合）に設定されます。

次の制限から 1 つまたは複数を設定できます。

- [Hosts] : セキュリティ アプライアンスを通して同時に接続できるホスト数の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
- [Telnet] : Telnet 同時セッションの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合は、1 ～ 5 の範囲で整数を入力し、リストの [Absolute] をクリックします。システムの最大セッション数は、コンテキスト全体で 100 です。
- [ASDM Sessions] : ASDM の同時セッションの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合は、1 ～ 5 の範囲で整数を入力し、リストの [Absolute] をクリックします。システムの最大セッション数は、コンテキスト全体で 80 です。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 セッション数のシステム制限値が 32 の場合は、すべてのコンテキストで HTTPS セッション数が 64 で制限されます。
- [Connections] : TCP または UDP で同時接続する、任意の 2 つのホスト間の接続数の制限値を設定します。これには、1 台のホストと他の複数台のホストとの接続も含まれます。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合、0（システム制限値）と使用するモデルのシステム制限値の範囲で整数を入力し、リストの [Absolute] をクリックします。使用するモデルの接続制限については、『*Cisco ASDM Release Notes*』を参照してください。
- [Xlates] : アドレス変換の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
- [SSH] : SSH セッションの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り

当てることができます。また、制限値を絶対値で設定する場合は、1 ～ 5 の範囲で整数を入力し、リストの [Absolute] をクリックします。システムの最大セッション数は、コンテキスト全体で 100 です。

- [MAC Entries]：（トランスペアレント モードの場合だけ）MAC アドレス テーブルに登録できる MAC アドレス エントリの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合は、0（システム制限値）～ 65535 の範囲で整数を入力し、リストの [Absolute] をクリックします。

ステップ 5　[Rate Limited Resources] 領域で、リソースのレート制限を設定します。

制限を設定しない場合、デフォルト クラスの制限値が継承されます。制限値がデフォルト クラスにない場合は、デフォルトでは無制限になります。

次の制限から 1 つまたは複数を設定できます。

- [Conns/sec]：接続数 / 秒の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
- [Syslogs/sec]：システム ログ メッセージ数 / 秒の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
- [Inspects/sec]：アプリケーション インスペクション数 / 秒の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。

ステップ 6　[OK] をクリックします。

コンテキスト リソースの使用状況のモニタ

システム実行スペースからすべてのコンテキストのリソース使用状況を監視するには、次の手順を実行します。

ステップ 1　まだシステム モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2　ツールバーの [Monitoring] ボタンをクリックします。

ステップ 3　[Context Resource Usage] をクリックします。

すべてのコンテキストのリソース使用状況を表示するには、次の各リソース タイプをクリックします。

- [ASDM]：ASDM 接続の使用状況を表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [Existing Connections (#)]：既存の接続の数を表示します。
  - [Existing Connections (%)]：このコンテキストで使用されている接続数を、すべてのコンテキストで使用されている接続の総数のパーセントとして表示します。
  - [Peak Connections (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク接続数を表示します。
- [Telnet]：Telnet 接続の使用状況を表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [Existing Connections (#)]：既存の接続の数を表示します。

  - [Existing Connections (%)]：このコンテキストで使用されている接続数を、すべてのコンテキストで使用されている接続の総数のパーセントとして表示します。
  - [Peak Connections (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク接続数を表示します。
- [SSH]：SSH 接続の使用状況を表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [Existing Connections (#)]：既存の接続の数を表示します。
  - [Existing Connections (%)]：このコンテキストで使用されている接続数を、すべてのコンテキストで使用されている接続の総数のパーセントとして表示します。
  - [Peak Connections (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク接続数を表示します。
- [Xlates]：ネットワーク アドレス変換の使用状況を表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [Xlates (#)]：現在の xlate の数を表示します。
  - [Xlates (%)]：このコンテキストで使用されている xlate 数を、すべてのコンテキストで使用されている xlate の総数のパーセントとして表示します。
  - [Peak (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク xlate 数を表示します。
- [NATs]：NAT ルールの数を表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [NATs (#)]：現在の NAT ルールの数を表示します。
  - [NATs (%)]：このコンテキストで使用されている NAT ルール数を、すべてのコンテキストで使用されている NAT ルールの総数のパーセントとして表示します。
  - [Peak NATs (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク NAT ルール数を表示します。
- [Syslogs]：システム ログ メッセージのレートを表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [Syslog Rate (#/sec)]：システム ログ メッセージの現在のレートを表示します。
  - [Syslog Rate (%)]：このコンテキストで生成されたシステム ログ メッセージ数を、すべてのコンテキストで生成されたシステム ログ メッセージの総数のパーセントとして表示します。
  - [Peak Syslog Rate (#/sec)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のシステム ログ メッセージのピーク レートを表示します。

ステップ 4　表示をリフレッシュするには、[Refresh] をクリックします。

[Resource Class] フィールドの説明

この項では、[Resource Class] 画面のフィールドについて説明します。次の項目を取り上げます。

- 「Resource Class」（P.9-18）
- 「Add/Edit Resource Class」（P.9-18）

Resource Class

[Resource Class] ペインには、設定されているクラスと各クラスの情報を示します。クラスを追加、編集、または削除することもできます。

フィールド

- [Class]：クラス名を示します。
- [All Resources]：個別設定されていないすべてのリソース制限を示します。0 のみを使用でき、無制限を意味します。
- [Connections]：TCP または UDP で接続する、任意の 2 つのホスト間の接続数の制限値を示します。これには、1 台のホストと他の複数台のホストとの接続も含まれます。
- [Hosts]：セキュリティ アプライアンスを通して接続できるホスト数の制限値を示します。
- [Xlates]：アドレス変換の制限値を示します。
- [Telnet]：Telnet セッション数の制限値を示します。デフォルトは 5 です。
- [SSH]：SSH セッション数の制限値を示します。デフォルトは 5 です。
- [ASDM Sessions]：ASDM 管理セッション数の制限値を示します。デフォルトは 5 です。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 セッション数のシステム制限値が 32 の場合は、すべてのコンテキストで HTTPS セッション数が 64 で制限されます。
- [MAC]：トランスペアレント ファイアウォール モードで MAC アドレス テーブルに登録できる MAC アドレス数の制限値を示します。デフォルトは 65535 です。
- [Conns/sec]：接続数/秒の制限値を示します。
- [Fixups/sec]：アプリケーション インスペクション数/秒の制限値を示します。
- [Syslogs/sec]：システム ログ メッセージ数/秒の制限値を示します。
- [Contexts]：このクラスに割り当てられたコンテキストを示します。
- [Add]：クラスを追加します。
- [Edit]：クラスを編集します。
- [Delete]：クラスを削除します。デフォルト クラスは削除できません。コンテキストが割り当てられているクラスを削除すると、コンテキストはデフォルト クラスに戻ります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

Add/Edit Resource Class

[Add/Edit Resource Class] ダイアログボックスでは、リソース クラスを追加または編集できます。

フィールド

- [Resource Class]：クラス名を 20 文字以内で設定します。
- [Count Limited Resources]：リソースの同時接続制限を設定します。システム制限のないリソースは、パーセント（%）で設定できません。設定できるのは絶対値だけです。制限を設定しない場合、デフォルト クラスの制限値が継承されます。制限値がデフォルト クラスにない場合は、リソースは無制限またはシステム制限値（使用できる場合）に設定されます。
  - [Hosts]：セキュリティ アプライアンスを通して同時に接続できるホスト数の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
  - [Telnet]：Telnet 同時セッションの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合は、1 ～ 5 の範囲で整数を入力し、リストの [Absolute] をクリックします。システムの最大セッション数は、コンテキスト全体で 100 です。
  - [ASDM Sessions]：ASDM の同時セッションの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合は、1 ～ 5 の範囲で整数を入力し、リストの [Absolute] をクリックします。システムの最大セッション数は、コンテキスト全体で 80 です。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 セッション数のシステム制限値が 32 の場合は、すべてのコンテキストで HTTPS セッション数が 64 で制限されます。
  - [Connections]：TCP または UDP で同時接続する、任意の 2 つのホスト間の接続数の制限値を設定します。これには、1 台のホストと他の複数台のホストとの接続も含まれます。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合、0（システム制限値）と使用するモデルのシステム制限値の範囲で整数を入力し、リストの [Absolute] をクリックします。使用するモデルの接続制限については、『*Cisco ASDM Release Notes*』を参照してください。
  - [Xlates]：アドレス変換の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
  - [SSH]：SSH セッションの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合は、1 ～ 5 の範囲で整数を入力し、リストの [Absolute] をクリックします。システムの最大セッション数は、コンテキスト全体で 100 です。
  - [MAC Entries]：（トランスペアレント モードの場合だけ）MAC アドレス テーブルに登録できる MAC アドレス エントリの制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値をパーセントで設定する場合は、1 より大きい整数を入力し、リストの [Percent] をクリックします。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。また、制限値を絶対値で設定する場合は、0（システム制限値）～ 65535 の範囲で整数を入力し、リストの [Absolute] をクリックします。
- [Rate Limited Resources]：リソースのレート制限を設定します。制限を設定しない場合、デフォルト クラスの制限値が継承されます。制限値がデフォルト クラスにない場合は、デフォルトでは無制限になります。

- [Conns/sec]：接続数/秒の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
- [Syslogs/sec]：システム ログ メッセージ数/秒の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。
- [Inspects/sec]：アプリケーション インスペクション数/秒の制限値を設定します。チェックボックスをオンにして、この制限値をイネーブルにします。制限値を 0 に設定すると、無制限になります。

- [Show Actual Class Limits]：（デフォルト クラス以外の場合のみ）クラスを編集した場合、このボタンをクリックすると、設定した制限値と、設定しなかったがデフォルト クラスから継承された制限値が表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

セキュリティ コンテキストの設定

この項では、セキュリティ コンテキストを追加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 コンテキストの追加」（P.9-20）
- 「MAC アドレスの自動割り当て」（P.9-22）
- 「[Security Context] フィールドの説明」（P.9-23）

セキュリティ コンテキストの追加

セキュリティ コンテキストを追加するには、次の手順を実行します。

ステップ 1　まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2　[Context Management] > [Security Contexts] ペインで、[Add] をクリックします。

[Add Context] ダイアログボックスが表示されます。

ステップ 3　[Security Context] フィールドに、コンテキストの名前を 32 文字以内の文字列で入力します。

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 2 つのコンテキストを保持できます。「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 4　[Interface Allocation] 領域で、[Add] ボタンをクリックし、コンテキストにインターフェイスを割り当てます。

ステップ 5　[Interfaces] > [Physical Interface] ドロップダウン リストからインターフェイスを選択します。

メイン インターフェイスを割り当てる場合、サブインターフェイス ID を空白にします。サブインターフェイスまたはその範囲を指定すると、このインターフェイスに設定されます。トランスペアレント ファイアウォール モードでは、他のコンテキストに割り当てられていないインターフェイスだけが表示されます。メイン インターフェイスが他のコンテキストに割り当てられている場合、サブインターフェイスを選択する必要があります。

ステップ 6　（任意）[Interfaces] > [Subinterface Range] (optional) ドロップダウン リストで、サブインターフェイス ID を選択します。

サブインターフェイス ID の範囲を指定する場合、2 つ目のドロップダウン リストが有効であれば、そこから最後の ID を選択します。

トランスペアレント ファイアウォール モードでは、他のコンテキストに割り当てられていないサブインターフェイスだけが表示されます。

ステップ 7　（任意）[Aliased Names] 領域で、[Use Aliased Name in Context] をオンにして、このインターフェイスに対して、コンテキスト コンフィギュレーションでインターフェイス ID の代わりに使用するエイリアス名を設定します。

a.　[Name] フィールドに、エイリアス名を設定します。

エイリアス名の先頭および最後は英字にします。間の文字として使用できるのは、英字、数字、下線だけです。このフィールドで名前の最後を英字または下線にした場合、その名前の後に追加する数字を [Range] フィールドで設定できます。

b.　（任意）[Range] フィールドで、エイリアス名のサフィックスを数字で設定します。

サブインターフェイスに範囲がある場合、範囲の数字を入力して名前の後に追加できます。

ステップ 8　（任意）エイリアス名を設定した場合でもコンテキスト ユーザが物理インターフェイスのプロパティを表示できるようにするには、[Show Hardware Properties in Context] をオンにします。

ステップ 9　[OK] をクリックして、[Add Context] ダイアログボックスに戻ります。

ステップ 10　（任意）IPS 仮想センサーを使用する場合、センサーを [IPS Sensor Allocation] 領域のコンテキストに割り当てます。

IPS および仮想センサーの詳細については、第 39 章「IPS の設定」を参照してください。

ステップ 11　（任意）このコンテキストをリソース クラスに割り当てるには、[Resource Assignment] > [Resource Class] ドロップダウン リストからクラス名を選択します。

この領域から直接リソース クラスを追加または編集できます。詳細については、「リソース クラスの設定」（P.9-12）を参照してください。

ステップ 12　コンテキスト コンフィギュレーションの場所を設定するには、[Config URL] ドロップダウン リストからファイル システム タイプを選択し、フィールドにパスを入力して URL を指定します。

FTP の場合、URL は次の形式になります。

ftp://server.example.com/configs/admin.cfg

ステップ 13　（任意）外部ファイルシステムの場合、[Login] をクリックしてユーザ名とパスワードを設定します。

ステップ 14　（任意）Active/Active フェールオーバーのフェールオーバー グループを設定するには、[Failover Group] ドロップダウン リストでグループ名を選択します。

ステップ 15　（任意）[Description] フィールドに説明を追加します。

MAC アドレスの自動割り当て

この項では、コンテキスト インターフェイスに一意の MAC アドレスを割り当てる方法について説明します。次の項目を取り上げます。

MAC アドレスの概要

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.9-3）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。

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 インターフェイスの作成後にこのオプションをイネーブルにすると、その直後に、MAC アドレスがすべてのインターフェイス用に生成されます。このオプション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。

MAC アドレスは次の形式を使用して生成します。

- 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.5-5）を参照してください。

MAC アドレス自動割り当てのイネーブル化

MAC アドレスの自動割り当てをイネーブルにするには、次の手順を実行します。

ステップ 1　まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2　[Context Management] > [Security Contexts] ペインで、[Mac-Address auto] をオンにします。

[Security Context] フィールドの説明

この項では、[Resource Class] 画面のフィールド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」（P.9-23）
- 「Add/Edit Context」（P.9-24）
- 「Add/Edit Interface Allocation」（P.9-26）

セキュリティ コンテキスト

フィールド

- [Context]：コンテキスト名を示します。
- [Interfaces]：コンテキストに割り当てられたインターフェイスおよびサブインターフェイスを示します。コンテキストで表示するインターフェイス名にエイリアスを割り当てると、エイリアス名がカッコ内に表示されます。サブインターフェイスの範囲を指定すると、先頭のインターフェイス番号と最後のインターフェイス番号の範囲がダッシュで示されます。
- [Resource]：各コンテキストのリソース クラスを示します。
- [Config URL]：コンテキスト コンフィギュレーションの場所を示します。
- [Group]：このコンテキストが属するフェールオーバー グループを示します。
- [Description]：コンテキストの説明を示します。
- [Add]：コンテキストを追加します。
- [Edit]：コンテキストを編集します。
- [Delete]：コンテキストを削除します。
- [Mac-Address auto]：プライベート 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ます。

  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.9-3）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。

  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 インターフェイスの作成後にこのオプションをイネーブルにすると、その直後に、MAC アドレスがすべてのインターフェイス用に生成されます。このオプション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。

MAC アドレスは次の形式を使用して生成します。

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.5-5）を参照してください。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

Add/Edit Context

フィールド

- [Security Context]：コンテキスト名を 32 文字以内で設定します。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 2 つのコンテキストを保持できます。「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。
- [Interface Allocation]：コンテキストに割り当てられたインターフェイスおよびサブインターフェイスを示します。
  - [Interface]：インターフェイス ID を表示します。サブインターフェイスの範囲を指定すると、先頭のインターフェイス番号と最後のインターフェイス番号の範囲がダッシュで示されます。
  - [Aliased Name]：インターフェイス ID の代わりにコンテキスト コンフィギュレーションで使用できるインターフェイスのエイリアス名を示します。
  - [Visible]：エイリアス名が設定されている場合でも、コンテキスト ユーザが物理インターフェイスのプロパティを表示できるかどうかを示します。

  - [Add]：コンテキストにインターフェイスを追加します。
  - [Edit]：インターフェイス プロパティを編集します。
  - [Delete]：インターフェイスを削除します。
- [IPS Sensor Allocation]：各コンテキストに 1 つ以上の IPS 仮想センサーを割り当てることができます。次に、トラフィックを AIP SSM に送信するようコンテキストを設定する場合、コンテキストに割り当てられるセンサーを指定できます。コンテキストに割り当てなかったセンサーは指定できません。コンテキストにセンサーが割り当てられていない場合は、AIP SSM に設定されているデフォルト センサーが使用されます。同じセンサーを複数のコンテキストに割り当てることができます。詳細については、「仮想センサーの使用」（P.39-3）を参照してください。
  - [Sensor Name]：割り当てられているセンサーを示します。AIP SSM で使用できるセンサーのみを割り当てることができます。
  - [Mapped Sensor Name]：センサーのマッピング名を示します。このセンサー名は、コンテキスト内で実際のセンサー名の代わりに使用できます。マッピング名を指定しない場合、センサー名がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているセンサーをコンテキスト管理者に知らせない場合があります。または、コンテキスト コンフィギュレーションを一般化する場合もあります。たとえば、すべてのコンテキストで「sensor1」および「sensor2」というセンサーを使用する場合、コンテキスト A の sensor1 と sensor2 に「highsec」センサーと「lowsec」センサーをマッピングし、コンテキスト B の sensor1 と sensor2 に「medsec」センサーと「lowsec」センサーをマッピングできます。
  - [Add]：センサーを追加します。
  - [Delete]：センサーを削除します。
  - [Default Sensor]：セキュリティ コンテキストにデフォルト センサーを割り当てます。コンテキスト コンフィギュレーション内に IPS を設定するときにセンサー名を指定しない場合、コンテキストはデフォルト センサーを使用します。コンテキストごとに設定できるデフォルト センサーは 1 つのみです。センサーをデフォルトとして指定せず、コンテキスト コンフィギュレーションにセンサー名が含まれていない場合、トラフィックは AIP SSM のデフォルト センサーを使用します。
- [Resource Assignment]：コンテキストをリソース クラスに割り当てます。
  - [Resource Class]：リストからクラスを選択します。
  - [Edit]：選択されたリソース クラスを編集します。
  - [New]：リソース クラスを追加します。
- [Config URL]：URL としてコンテキスト コンフィギュレーションの場所を指定します。リストのファイル システム タイプを選択し、フィールドにサーバ（リモート ファイル システムの場合）、パス、およびファイル名を入力します。FTP の場合、URL は次の形式になります。

  ftp://server.example.com/configs/admin.cfg
- [Login]：リモート ファイル システムのユーザ名とパスワードを設定します。
- [Failover Group]：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 グループを設定します。
- [Description]：コンテキストのオプションの説明を設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

Add/Edit Interface Allocation

フィールド

- [Interfaces]：物理インターフェイスおよびサブインターフェイス ID を指定します。
  - [Physical Interface]：コンテキストに割り当てるように物理インターフェイスを設定します。メイン インターフェイスを割り当てる場合、サブインターフェイス ID を空白にします。サブインターフェイスまたはその範囲を指定すると、このインターフェイスに設定されます。トランスペアレント ファイアウォール モードでは、他のコンテキストに割り当てられていないインターフェイスだけが表示されます。メイン インターフェイスが他のコンテキストに割り当てられている場合、サブインターフェイスを選択する必要があります。
  - [Sub Interface Range (Optional)]：サブインターフェイス ID またはサブインターフェイス ID の範囲を設定します。1 つのサブインターフェイスを指定するには、最初のリスト内の ID を選択します。範囲を指定するには、（使用可能な場合）2 つめのリスト内の最後の ID を選択します。トランスペアレント ファイアウォール モードでは、他のコンテキストに割り当てられていないサブインターフェイスだけが表示されます。
- [Aliased Name]：インターフェイス ID の代わりにコンテキスト コンフィギュレーションで使用できるインターフェイスのエイリアス名を設定します。
  - [Use Aliased Name in Context]：コンテキストのエイリアス名をイネーブルにします。
  - [Name]：エイリアス名を設定します。エイリアス名の先頭および最後は英字にします。間の文字として使用できるのは、英字、数字、下線だけです。このフィールドで名前の最後を英字または下線にした場合、その名前の後に追加する数字を [Range] フィールドで設定できます。
  - [Range]：エイリアス名の数値のサフィックスを設定します。サブインターフェイスに範囲がある場合、範囲の数字を入力して名前の後に追加できます。
- [Show Hardware Properties in Context]：エイリアス名を設定した場合でも、コンテキスト ユーザが物理インターフェイスのプロパティを表示できるようにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•