CHAPTER 3

マルチ コンテキスト モードのイネーブル化

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。

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。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

コンテキスト コンフィギュレーション ファイル

この項では、セキュリティ アプライアンスがマルチ コンテキスト モードのコンフィギュレーションを実装する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 コンフィギュレーション」（P.3-2）
- 「システム設定」（P.3-2）
- 「管理コンテキストの設定」（P.3-2）

コンテキスト コンフィギュレーション

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。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。

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、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。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。

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.3-3）
- 「無効な分類子の基準」（P.3-4）
- 「分類の例」（P.3-5）

（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.3-3）
- 「固有の MAC アドレス」（P.3-3）
- 「NAT コンフィギュレーション」（P.3-4）

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。各インターフェイスを設定するときに、手動で MAC アドレスを設定できます（「インターフェイスの設定」（P.7-2）を参照）。または、MAC アドレスを自動的に生成することもできます（「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.6-11）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 3-1 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 3-1　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

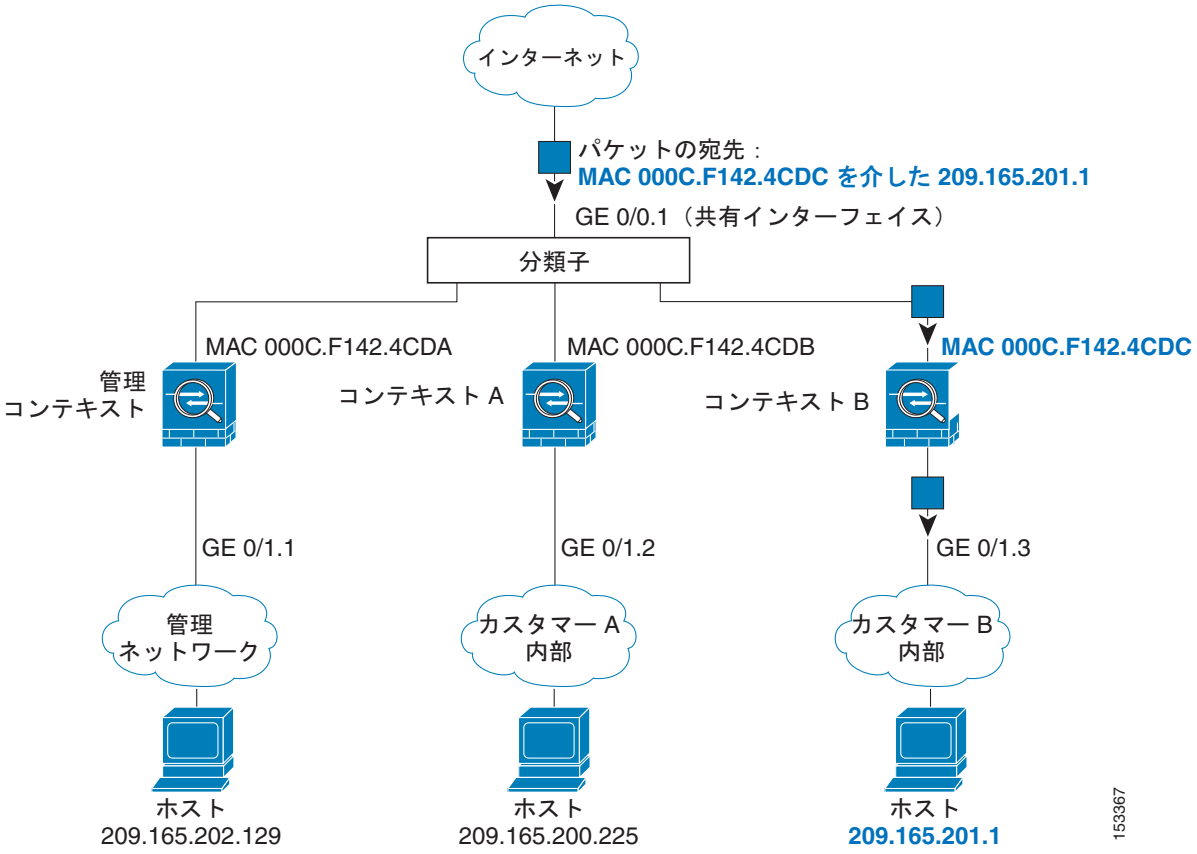
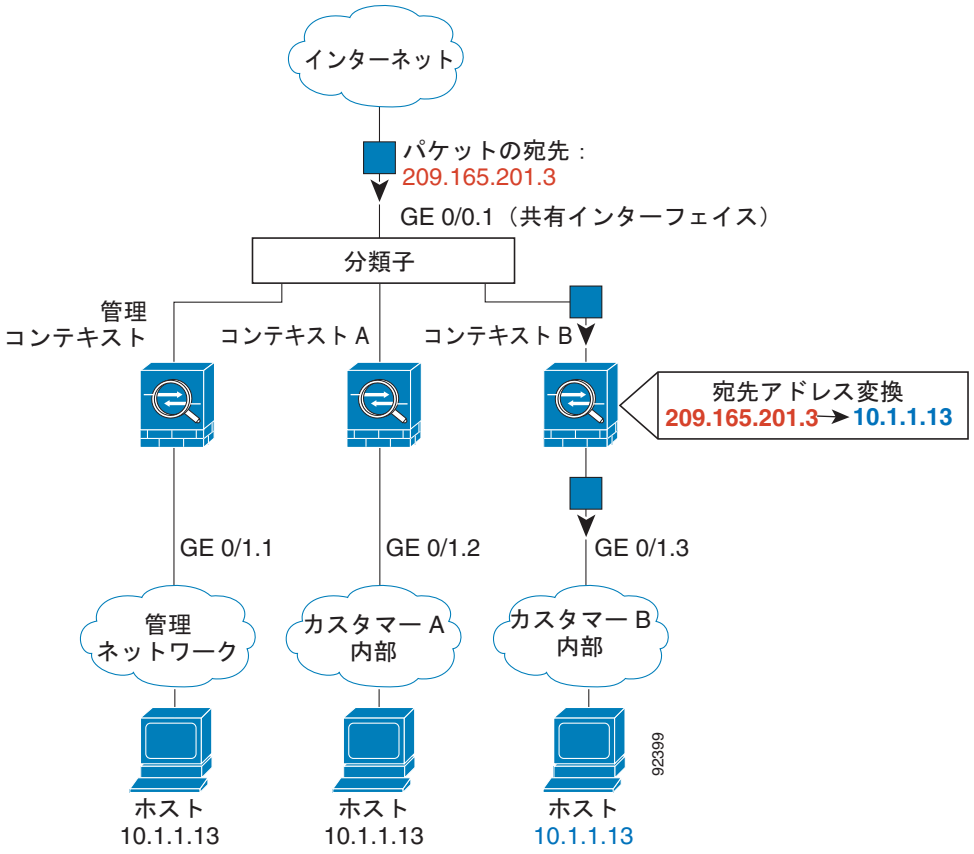


図 3-2 に、MAC アドレスが割り当てられていない外部インターフェイスを共有するマルチコンテキストを示します。コンテキスト B には宛先アドレスに一致するアドレス変換が含まれるため、分類子はパケットをコンテキスト B に割り当てます。

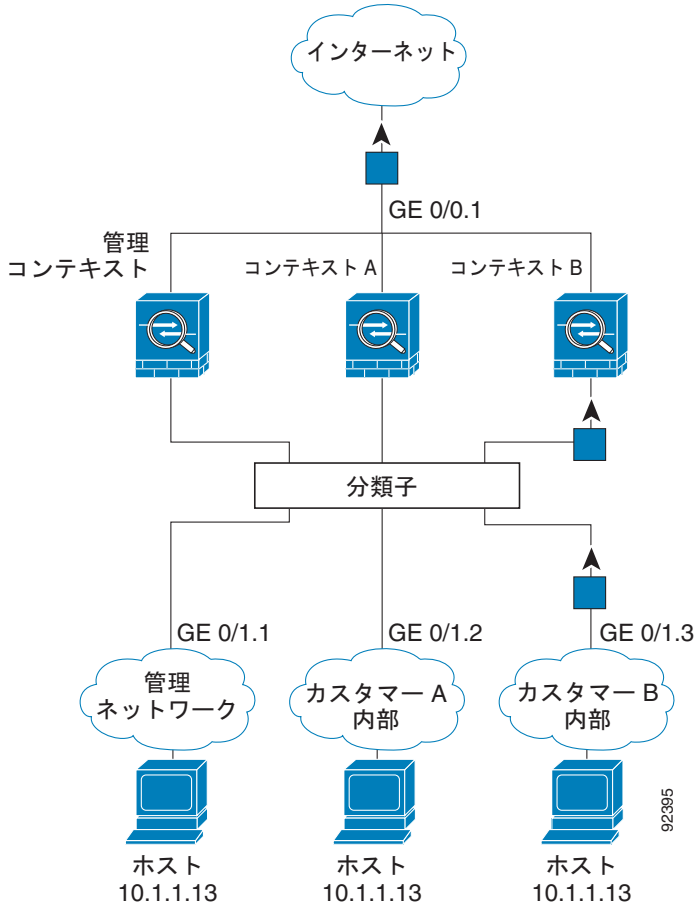
図 3-2　NAT を使用した共有インターフェイスを持つパケット分類



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 3-3 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。

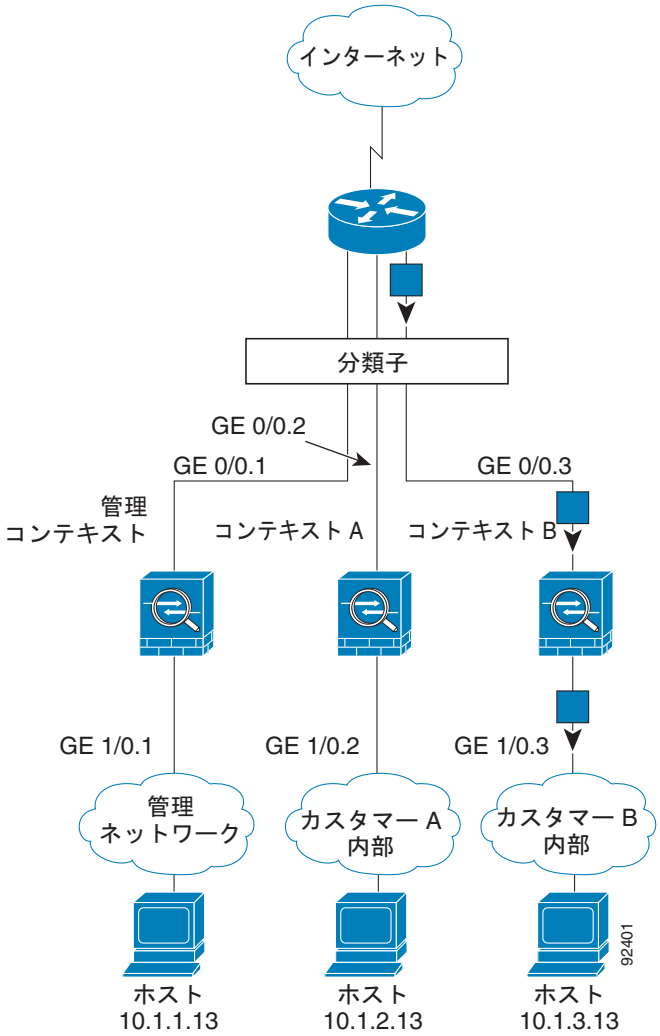
（注） *内部*インターフェイスを共有し、固有の MAC アドレスを使用していない場合、分類子には重要な制限事項がいくつかあります。分類子は、アドレス変換コンフィギュレーションに基づいてコンテキスト内のパケットを分類します。そのトラフィックの*宛先*アドレスを変換する必要があります。通常は外部アドレスに対して NAT を実行しないため、パケットを共有インターフェイスの内部から外部へ送信できない場合もあります。これは、Web のように巨大な外部ネットワークで、外部 NAT コンフィギュレーションのアドレスを予測できないためです。内部インターフェイスを共有する場合、固有の MAC アドレスを使用す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

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



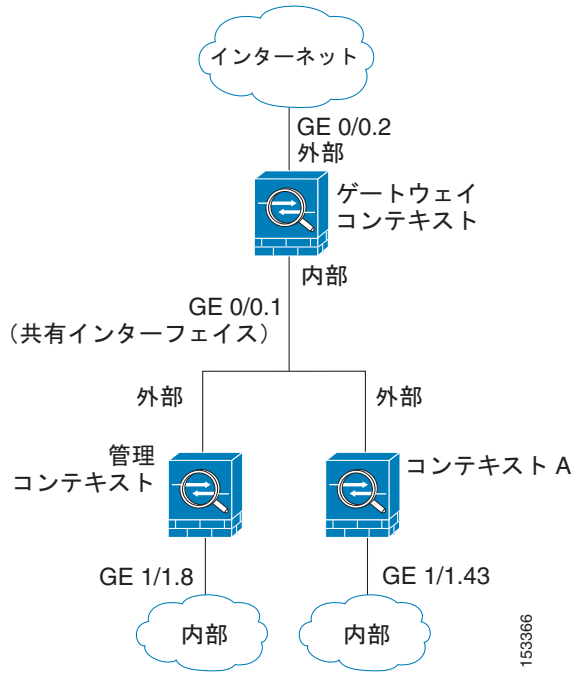
セキュリティ コンテキストのカスケード接続

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 3-5 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 3-5　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.3-10）
- 「コンテキスト管理者のアクセス」（P.3-10）

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 SDM アクセスをイネーブルにするには、第 40 章「システム アクセスの管理」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 に変更したときも、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 による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 40 章「システム アクセスの管理」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、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 ではモードの変更はサポートされていないため、CLI を使用してモードを変更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。

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 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。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
```

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。