CHAPTER 7

セキュリティ コンテキストの設定

ここでは、次の項目について説明します。

セキュリティ コンテキストの概要

1 台の FWSM を、セキュリティ コンテキストと呼ばれる複数の仮想装置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ちます。マルチコンテキストは、複数のスタンドアロン装置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、管理など、多くの機能がサポートされます。ほとんどのダイナミック 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、多数の顧客にセキュリティ サービスを販売する。FWSM 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、顧客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。
- 複数のファイアウォール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。

- ほとんどのダイナミック ルーティング プロトコル。BGP スタブ モードがサポートされています。

  セキュリティ コンテキストは、スタティック ルートまたは BGP スタブ モードのみをサポートします。マルチコンテキスト モードでは、OSPF または RIP をイネーブルにできません。
- マルチキャスト ルーティング。マルチキャスト ブリッジングがサポートされています。

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、FWSM 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

FWSM 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装置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 コンフィギュレーション

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、およびシステム コンフィギュレーションのその他のコンテキスト実行パラメータを設定することでコンテキストを追加および管理します。システム コンフィギュレーションは、シングルモード コンフィギュレーションと同様に、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、FWSM 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、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。

管理コンテキスト コンフィギュレーション

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一切制限されないため、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に対する管理者特権が与えられるため、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。

FWSM によるパケットの分類方法

FWSM 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、FWSM 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。FWSM では、すべてのインターフェイスに対してグローバル MAC アドレスを 1 つだけ使用します。通常、マルチコンテキストでインターフェイスの共有が必要でない限り、MAC アドレス 1 つで問題ありません。すべての IP アドレスが同じ MAC アドレスに解決されると、ルータは、パケットを同じネットワークの IP アドレスに転送できません。また、スイッチのブリッジング テーブルは、MAC アドレスが 1 つのインターフェイスから別のインターフェイスに移動するときに絶えず変化します。セキュリティ コンテキストの分類子は、この状況を解決するためのものです。

ここでは、次の項目について説明します。

- 有効な分類子の基準（P.7-4）
- 無効な分類子の基準（P.7-4）
- 分類の例（P.7-5）

有効な分類子の基準

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、FWSM はパケットをそのコンテキストに分類します。透過ファイアウォール 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。

マルチコンテキストでインターフェイスを共有している場合、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、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分類子が認識できなければなりません。分類子は、アクティブな NAT セッ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。アクティブな NAT セッションは、永続的なセッションを作成する **static** コマンドか、またはアクティブなダイナミック NAT セッションのいずれかで作成されます。

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
```

ダイナミック NAT を使用する場合、実際のホストが共有インターフェイスを通じて接続を作成するときに、アクティブ NAT セッションが作成されます。ホストに戻るトラフィックでは、パケットの分類にアクティブ NAT セッションが使用されます。

異なるコンテキスト間に重複があると接続問題の原因になります。この重複を迅速に識別するには、システム実行スペースで **show np 3 static** コマンドを入力します。

（注） インターフェイス用管理トラフィックでは、インターフェイス IP アドレスが分類用として使用されます。

無効な分類子の基準

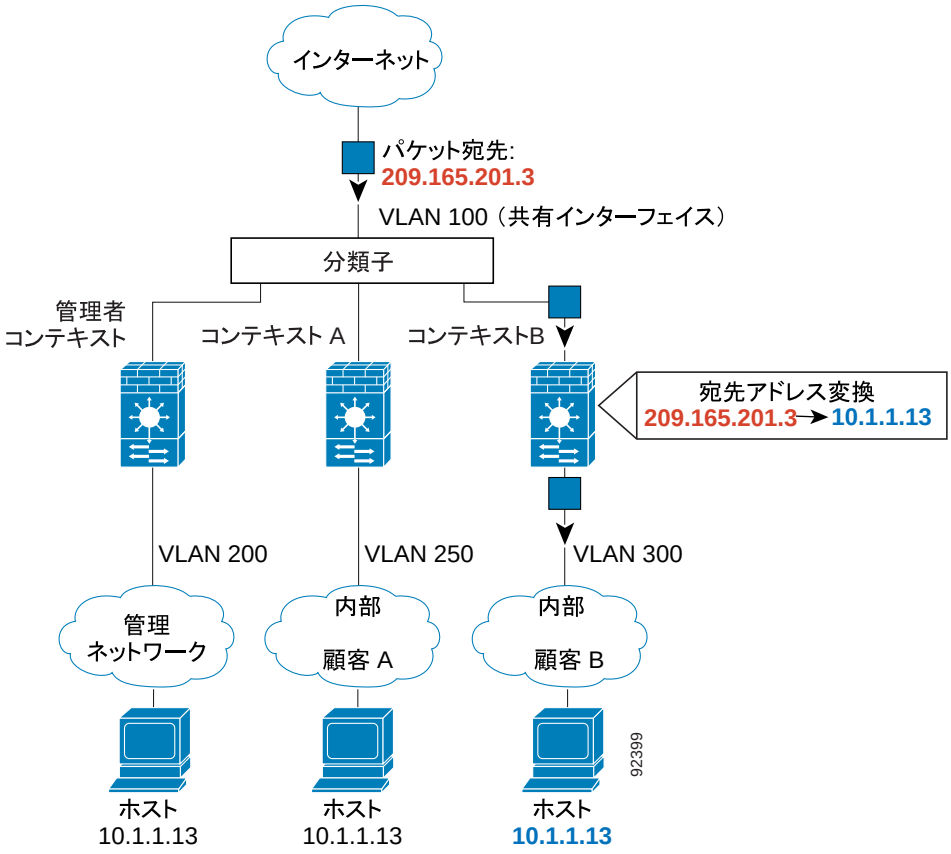
次のコンフィギュレーションは、パケットの分類に使用されません。

- 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を使用しません。これは、NAT 免除がマッピング（共有）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：分類子は、分類にルーティング テーブルを使用しません。たとえば、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 ルートがコンテキストに含まれていて、同じサブネットに対する **static** コマンドが別のコンテキストに含まれている場合、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 7-1 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。内部インターフェイスは固有であり、IP アドレスは重複が可能です。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 7-1　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 7-2 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 VLAN 300 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 7-2　内部ネットワークからの着信トラフィック

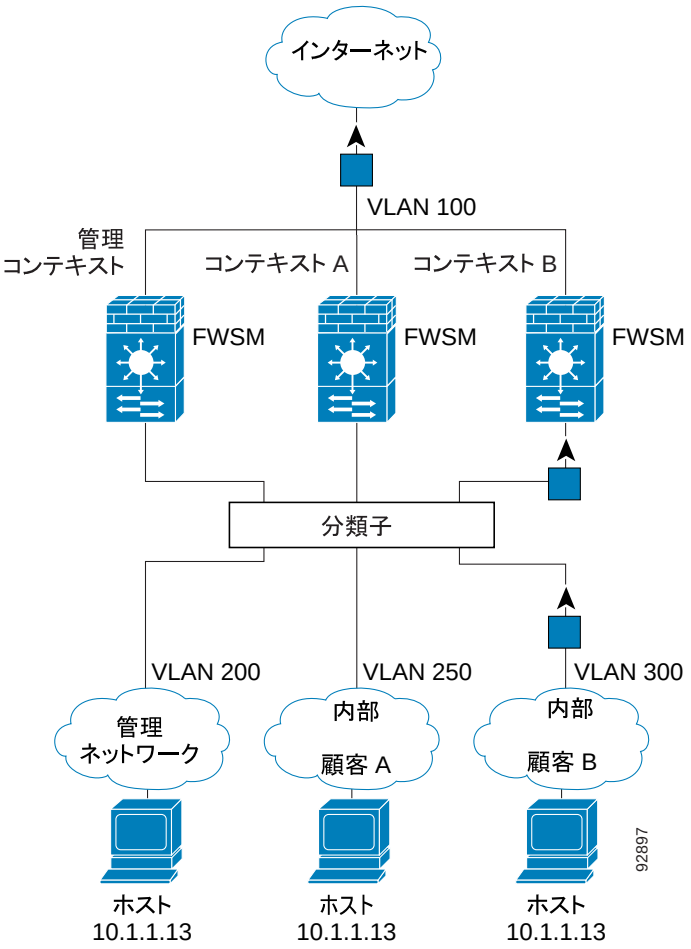
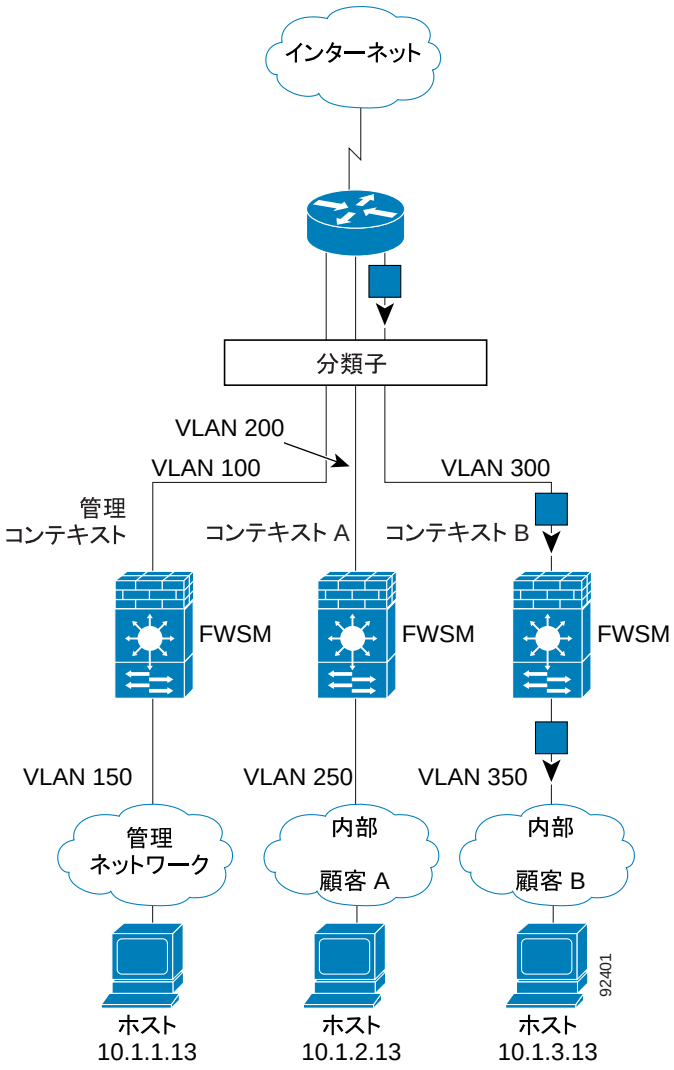


図 7-3 に、インターネットにアクセスするコンテキスト B 内部ネットワークにホストがある透過ファイアウォールを示します。分類子は、パケットをコンテキスト B に割り当てます。これは、入力インターフェイスが VLAN 300 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 7-3　透過ファイアウォールのコンテキスト



コンテキスト間のインターフェイス共有

ルーテッド モードのみ

FWSM では、複数のコンテキストで 1 つのインターフェイスを共有できます。ただし、パケット分類要件により、インターフェイスを共有できないことがあります。分類子は、アクティブ NAT セッションに基づいて宛先アドレスをコンテキストに分類するので、NAT の設定内容によって制限を受けます。NAT を実行しない場合は、固有のインターフェイスを使用する必要があります。

（注） FWSM では、コンテキストの外部インターフェイスを別のコンテキストの内部インターフェイスとして共有すること（カスケード コンテキスト）はサポートされていません。あるコンテキストからの発信トラフィック（高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイスへ）は、着信トラフィック（低位から高位へ）としてのみ別のコンテキストに入ることができます。両方のコンテキストの発信にすることも、両方のコンテキストの着信にすることもできません。

ここでは、次の項目について説明します。

NAT およびトラフィックの発信元

設定する NAT のタイプによって、共有インターフェイスでトラフィックを発信できるか、または既存の接続への応答のみが可能かが決まります。ダイナミック NAT を使用する場合、実際のアドレスへの接続を開始することはできません。このため、共有インターフェイスからのトラフィックは、既存の接続への応答でなければなりません。ただし、スタティック NAT では接続を開始できるため、共有インターフェイスで接続を開始できます。

外部インターフェイスの共有

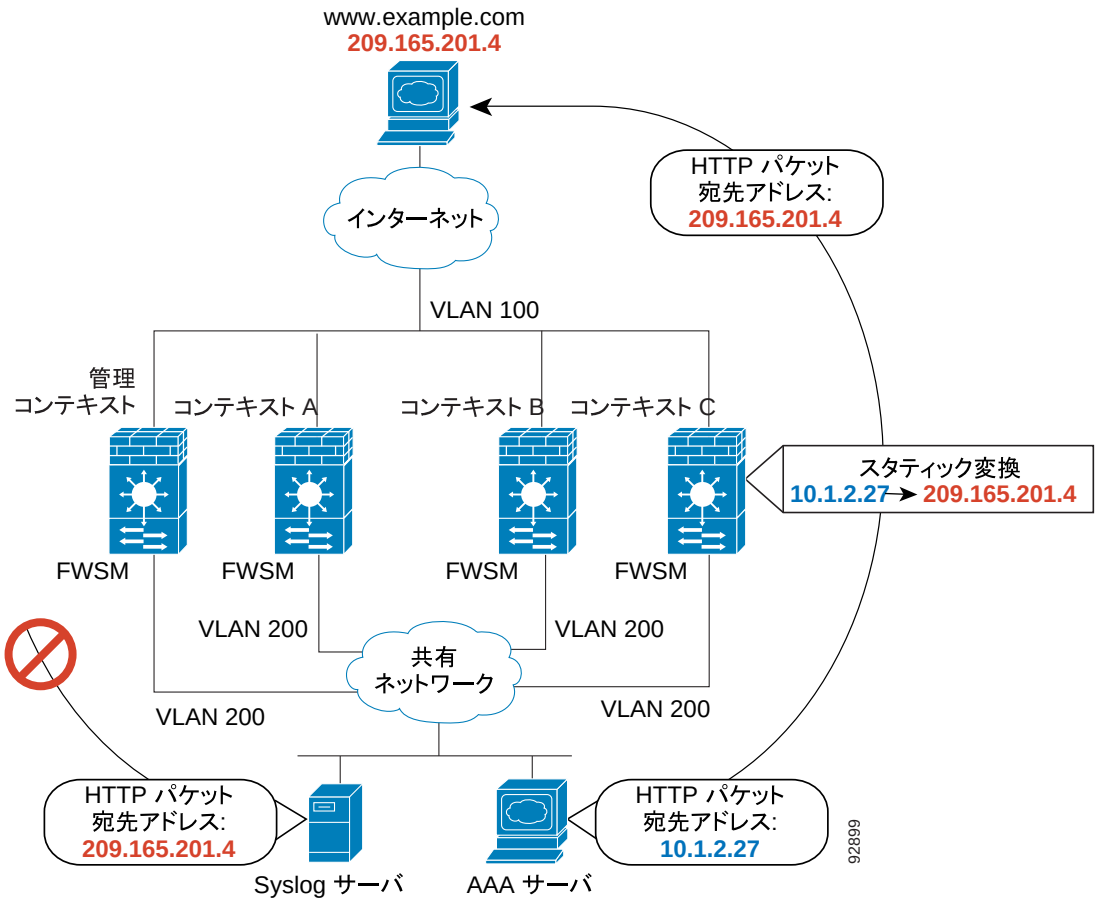
外部共有インターフェイス（インターネットへの接続など）を使用している場合、内部の宛先アドレスは数に限りがあり、システム管理者は内部の宛先アドレスについて把握しています。このため、スタティック NAT の場合でも、内部の宛先のアドレスに対する NAT の設定は簡単です。

内部インターフェイスの共有

一方、限りない宛先アドレスが存在する環境であるインターネットと共有インターフェイス間の通信を許可する場合、内部インターフェイスを共有に設定すると問題が生じます。たとえば、共有インターフェイス上の内部ホストからインターネットへのトラフィックの開始を許可する場合、各インターネット アドレスに対してスタティック NAT 文を設定する必要があります。この要件により、必然的に内部共有インターフェイス上のユーザに提供できるインターネット アクセスの種類が制限されます（インターネット サーバのアドレスをスタティックに変換する場合は、DNS エントリのアドレスと NAT によってそれがどのような影響を受けるかという点も考慮する必要があります。たとえば、サーバが www.example.com にパケットを送信すると、DNS サーバは変換対象アドレスを返す必要があります。NAT コンフィギュレーションによって DNS エントリの管理が決まります）。

図 7-4 に、内部共有インターフェイス上の 2 つのサーバを示します。一方のサーバは Web サーバの変換対象アドレスにパケットを送信します。FWSM はパケットを分類し、そのアドレスのスタティック変換がコンテキスト C にあるので、パケットをコンテキスト C に転送します。他方のサーバは、変換されない実際のアドレスにパケットを送信しますが、FWSM はパケットを分類できないので、そのパケットはドロップされます。

図 7-4　共有インターフェイス上を発信元とするトラフィック



CLI での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

シスコへの発注内容によっては、FWSM 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 はモードの変更をサポートしていないため、CLI を使用してモードを変更する必要があります。

ここでは、次の項目について説明します。

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、FWSM 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、リブートしても保持されますが、コンフィギュレーション ファイルには保存されません。別の装置にコンフィギュレーションをコピーする必要がある場合、**mode** コマンドを実行して新しい装置のモードを一致するように設定します。

シングルモードからマルチモードに変換すると、FWSM 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。その 2 つは、システム コンフィギュレーションを構成する新しいスタートアップ コンフィギュレーションと、管理コンテキストを構成する admin.cfg です（内部フラッシュ メモリのルート　ディレクトリに作成されます）。元の実行コンフィギュレーションは、old_running.cfg として保存されます（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。管理コンテキストのエントリは、「admin」という名前でシステム コンフィギュレーションに FWSM によって自動的に追加されます。

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
```

FWSM 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、最初にスタートアップ コンフィギュレーション全体を FWSM にコピーします（可能な場合）。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、シングルモードの装置にとっては完全に機能するコンフィギュレーションではないからです。たとえば、以前のシングルモード実行コンフィギュレーションがある場合は、スタートアップ コンフィギュレーションとして復元できます。システム コンフィギュレーションには、コンフィギュレーションの一部としてネットワーク インターフェイスが含まれていないので、スイッチ コンソールから FWSM にアクセスしてコピーを実行する必要があります。

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 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
```

FWSM 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、コンテキストごとの最大限度が設定されている場合を除いて、すべてのセキュリティ コンテキストは FWSM のリソースに無制限にアクセスできます。ただし、1 つまたは複数のコンテキストがリソースを使用し過ぎて、他のコンテキストが接続できなくなる場合には、リソース管理の設定を行い、コンテキストごとのリソースの使用を制限することができます。FWSM では、コンテキストをリソース クラスに割り当てることによりリソースを管理します。各コンテキストには、クラスごとに設定されたリソース制限が適用されます。

（注）　FWSM　は、コンテキストごとに帯域幅を制限しませんが、FWSM　が搭載されているスイッチは VLAN ごとに帯域幅を制限できます。詳細については、スイッチのマニュアルを参照してください。

ここでは、次の項目について説明します。

- クラスおよびクラス メンバーの概要（P.7-12）
- リソース クラスの追加（P.7-15）

クラスおよびクラス メンバーの概要

FWSM では、コンテキストをリソース クラスに割り当てることによりリソースを管理します。各コンテキストには、クラスごとに設定されたリソース制限が適用されます。ここでは、次の項目について説明します。

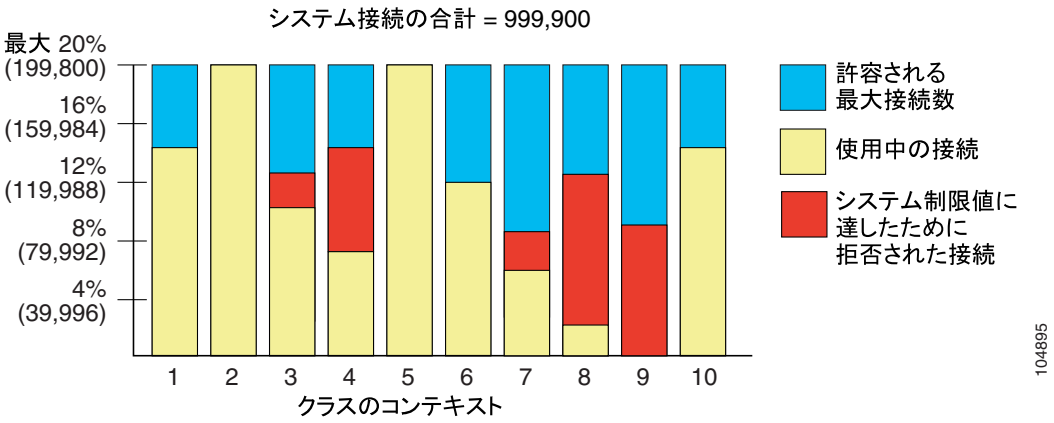
- リソース制限の概要（P.7-12）
- デフォルト クラスの概要（P.7-14）
- クラス　メンバーの概要（P.7-14）

リソース制限の概要

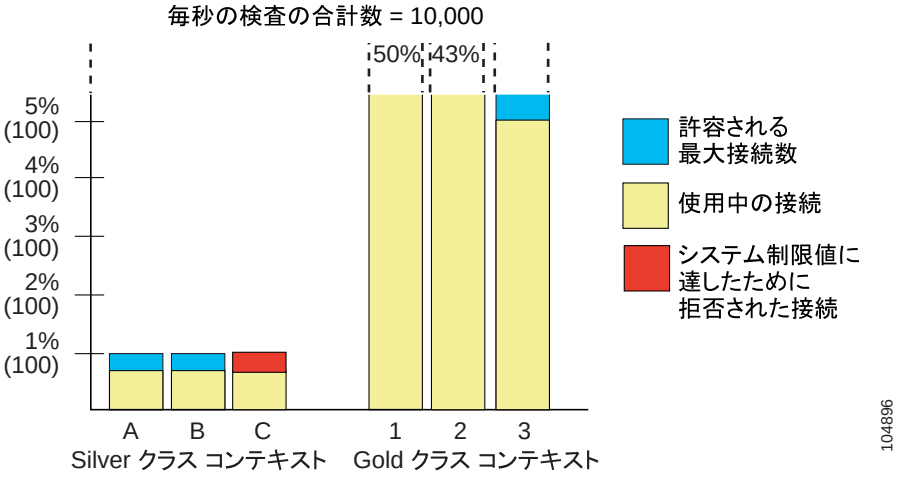
クラスを作成すると、FWSM は、そのクラスに割り当てられたコンテキストごとに一定のリソースを確保するのではなく、コンテキストが使用できるリソースの最大限度を設定します。リソースをオーバーサブスクライブしたり、特定のリソースを無制限にしたりすると、いくつかのコンテキストがリソースを使い果たして、他のコンテキストに対するサービスに影響が出ることがあります。

すべてのリソースを一括して制限を設定できます。デバイスで使用できる合計値をパーセントで指定します。また、個々のリソースに、制限をパーセントまたは絶対値で設定できます。

すべてのコンテキスト合計で 100% を超えるリソースを割り当てると、FWSM 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、Bronze クラスにはコンテキストごとに 20% の接続制限を設定してから、そのクラスに 10 のコンテキストを割り当てると、合計は 200% になります。いくつかのコンテキストがシステムの制限を超えて同時に使用すれば、各コンテキストは、当初想定した 20% に満たなくなります（次の図を参照）。



FWSM では、あるクラスの 1 つまたは複数のリソースに、パーセントや絶対値ではなく、無制限アクセスを割り当てることができます。あるリソースが無制限の場合、コンテキストは、システムで利用できるリソースをすべて使用できます。たとえば、Silver クラスの中にコンテキスト A、B、C があるとします。各クラス メンバーに毎秒 1% のシステム検査制限を課すと合計が 3% になりますが、3 つのコンテキストが、現在合計 2% しか使用していないとします。一方、Gold クラスには検査への無制限アクセスが設定されているとします。この場合、Gold クラスのコンテキストは、97% より多い「未割り当て」検査を使用できます。コンテキスト A、B、C が現在使用していない 1% の検査も使用できるからです（その結果、コンテキスト A、B、C が合計 3% の制限より少ないリソースしか使用できなくなることがあります）。次の図を参照してください。無制限アクセスの設定は、FWSM のオーバーサブスクライブに似ています。相違点は、システムのオーバーサブスクライブの程度をあまり制御できないという点です。



デフォルト クラスの概要

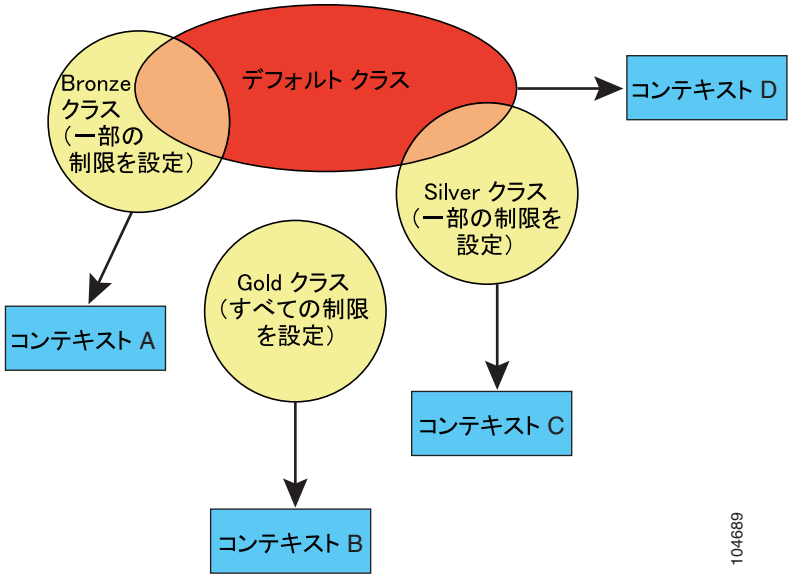
すべてのコンテキストは、別のクラスに割り当てられていなければ、デフォルト クラスに属します。したがって、コンテキストをデフォルト クラスに特に割り当てる必要はありません。

コンテキストがデフォルト クラス以外のクラスに属している場合、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、他のクラス設定が定義されていない場合、メンバー コンテキストはデフォルト クラスを制限用に使用します。たとえば、同時接続に 2% を設定されたクラスを作成し、その他の制限がない場合、その他すべての制限はデフォルト クラスから継承されます。反対に、すべてのリソースに 2% の制限のあるクラスを作成する場合、そのクラスはデフォルト クラス設定を使用しません。

デフォルトでは、デフォルト クラスのすべてのコンテキストには、リソースへの無制限アクセスが付与されます。ただし、次の制限については、デフォルトでコンテキストごとの最大値に設定されます。

- 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

次の図に、デフォルト クラスと他のクラスとの関係を示します。コンテキスト A と C は、いくつか制限のあるクラスに属しています。他の制限は、デフォルト クラスから継承されます。コンテキスト B は、すべての制限がそのクラス（Gold クラス）に設定されているので、デフォルト クラスから制限を継承することはありません。コンテキスト D はクラスに割り当てられていないため、デフォルトでデフォルト クラスのメンバーになります。



クラス メンバーの概要

クラスの設定を使用するには、コンテキストの定義時に、コンテキストをその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 クラスに特に割り当てる必要はありません。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、メンバー クラスで未定義の制限がデフォルト クラスから継承される点です。したがって、実際には、コンテキストはデフォルト クラスと別のクラスのメンバーということになります。

リソース クラスの追加

この項では、リソース クラスの設定で使用できるペインについて説明します。次の項目を取り上げます。

Resource Class

Resource Class ペインで、設定されているクラスと各クラスの情報を示します。クラスの追加、編集、削除もできます。

フィールド

- Class：クラスの名前を示します。
- 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。デフォルトは 0 で、無制限を意味します。
- Connections：任意の 2 つのホスト間の TCP 接続または UDP 接続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：FWSM 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 セッションは、2 つの HTTPS 接続を使用します。1 つは常駐の監視用、もう 1 つは変更時にのみ使用されるコンフィギュレーション変更用です。たとえば、ASDM セッション数のシステム制限値が 80 の場合は、すべてのコンテキスト合計で HTTPS セッション数が 160 に制限されます。
- IPSec：IPSec 管理セッションの制限値を示します。デフォルトは 5 です。
- MAC Addresses：透過ファイアウォール 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：アプリケーション検査数 / 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、コンテキストのクラスはデフォルトに戻ります。

モード

次の表に、この機能を使用できるモードを示します。

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、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：クラスの名前を 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。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。デフォルト クラスが制限値を設定しない場合、デフォルトで制限値はシステム制限値になります。
  - All Resources：すべてのリソースに制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。また、特定のリソースに制限値を設定すると、設定した制限値は、すべてのリソースに設定した制限値より優先されます。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。また、無制限に設定するには、値を **0** に設定し、リストの **Absolute** をクリックします。その他の絶対値は設定できません。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。
  - Hosts : FWSM 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。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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）～ 262144 の範囲で整数を入力し、リストの **Absolute** をクリックします。
  - Telnet : Telnet　同時セッションの制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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、すべてのコンテキスト合計で 100 です。
  - IPSec : IPSec 同時セッションの制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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、すべてのコンテキスト合計で 10 です。
  - ASDM Sessions：ASDM の同時セッションの制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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、すべてのコンテキスト合計で 80 です。ASDM セッションは 2 つの HTTPS 接続を使用します。1 つは常駐の監視用、もう 1 つは変更時のみ使用されるコンフィギュレーション変更用です。たとえば、ASDM セッション数のシステム制限値が 80 の場合は、すべてのコンテキスト合計で HTTPS セッション数が 160 に制限されます。
  - Connections：任意の 2 つのホスト間の TCP または UDP の同時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。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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）～ 999900 の範囲で整数を入力し、リストの **Absolute** をクリックします。

（注）　同時接続の場合、FWSM は、接続を受け入れる 2 つの NP のそれぞれに制限値の半分を割り当てます。通常、接続数は NP 間で均等に分割されます。ただし、状況によっては、接続数が均等に分割されず、一方の NP で最大接続制限に達する前に、もう一方の NP で最大接続制限に達してしまうことがあります。このような場合、許可される最大接続数は設定した制限よりも少なくなります。NP への分配は、アルゴリズムに基づいてスイッチが制御します。スイッチでこのアルゴリズムを調整するか、不均衡の原因となる接続制限を引き上げて調整することができます。

  - Xlates : アドレス変換の制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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）～ 266144 の範囲で整数を入力し、リストの **Absolute** をクリックします。
  - SSH : SSH セッションの制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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 :（透過モードのみ）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。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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。デフォルト クラスが制限値を設定しない場合、デフォルトで制限値はシステム制限値になります。
  - Conns/sec : 接続数 / 秒の制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。また、制限値を絶対値で設定する場合は、0 ～ 102400 の範囲で整数を入力し、リストの **Absolute** をクリックします。
  - 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。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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）～ 102400 の範囲で整数を入力し、リストの **Absolute** をクリックします。
  - Fixups/sec : アプリケーション検査数 / 秒の制限値を設定します。この制限値をイネーブルにするには、チェックボックスをオンにします。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。100 パーセントより大きな値を割り当てると、デバイスをオーバーサブスクライブできます。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）～ 10000 の範囲で整数を入力し、リストの **Absolute** をクリックします。
- 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

次の表に、この機能を使用できるモードを示します。

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
•	•	—	—	•

メモリ パーティションの設定

マルチコンテキスト モードで、FWSM は、ルール コンフィギュレーションに割り当てられたメモリをパーティションに分割し、各コンテキストをパーティションに割り当てます。デフォルトで、コンテキストは、ACE、AAA ルールなど最大数のルールを提供する 12 のパーティションのうちの 1 つに属します。ルールの制限のリストについては、P.A-7 の「ルール制限」を参照してください。FWSM は、起動時にロードされる順番でコンテキストをパーティションに割り当てます。たとえば、12 のコンテキストを設定し、ルールの最大数が 14,103 の場合、各コンテキストはそれぞれ個別のパーティションに割り当てられ、14,103 のルールを使用できます。さらに 1 つのコンテキストを追加すると、コンテキスト番号 1 および新しいコンテキスト番号 13 の両方がパーティション 1 に割り当てられ、2 つのコンテキスト合計で 14,103 のルールを使用できます。他の 11 のコンテキストは、引き続きそれぞれが 14,103 のルールを使用できます。コンテキストを削除しても、パーティションのメンバーシップは変わりません。したがって、リブートしてコンテキストが均等に分配されるまで、コンテキストの分配が不均一になることがあります。

（注） ルールは先着順で使用されるため、コンテキストによっては使用するルールが他のコンテキストよりも多くなることがあります。

ルールの制限の詳細については、P.A-7 の「ルール制限」を参照してください。

コンテキストをパーティションに手動で割り当てることもできます。コンテキストをパーティションに割り当てるには、P.7-20 の「セキュリティ コンテキストの設定」を参照してください。また、コンテキストの数と一致するように、パーティションの数を減らすこともできます。

（注） パーティションの数を変更した場合、FWSM をリロードする必要があります。

メモリ パーティションの数を変更するには、次の手順を実行します。

ステップ 1　システム実行スペースで、Configuration > Security Contexts にアクセスし、Number of ACL Partitions フィールドにパーティションの数を 1 ～ 12 で設定します。

（注）　コンテキストをパーティションに割り当てる場合、パーティション番号は 0 から始まります。したがって、パーティションが 12 個ある場合、パーティション番号は 0 ～ 11 になります。コンテキストをパーティションに割り当てる方法については、P.7-20 の「セキュリティ コンテキストの設定」を参照してください。

ステップ 2　**Apply** をクリックします。

ステップ 3　FWSM をリロードして変更を有効にするには、**Tools > System Reload** を選択します。

フェールオーバーを使用している場合、両方の装置でメモリ パーティションが一致しなければならないため、他のフェールオーバー装置もリロードする必要があります。両方の装置が同時にダウンするため、トラフィック ロスが生じる可能性があります。

ステップ 4　フェールオーバーを使用している場合、もう一方の装置をリロードします。

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。

前提条件

コンテキストを ASDM で設定する前に、FWSM がマルチコンテキスト モードになっていることを確認してください。Home > Device Information > General タブに、現在のコンテキスト モードがマルチかシングルかが表示されます。シングルモードからマルチモードに変更するには、「CLI での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」を参照してください。

Security Contexts

Security Contexts ペインで、設定されたコンテキストと各コンテキストの情報を示します。コンテキストの追加、編集、削除もできます。マルチコンテキスト モードの詳細については、「セキュリティ コンテキストの概要」を参照してください。

フィールド

- Context：コンテキストの名前を示します。
- Mode：コンテキストがルーテッド モードか透過モードかを示します。
- Interfaces：コンテキストに割り当てられたインターフェイスを示します。コンテキストで表示するインターフェイスにエイリアス名を割り当てると、エイリアス名がカッコ内に表示されます。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：コンテキストが割り当てられるリソース 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。
- ACL Partition：コンテキストが割り当てられるメモリ パーティションを示します。デフォルトで、コンテキストは起動時の順番でパーティションに割り当てられます。
- 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。
- Change Firewall Mode：ファイアウォール モードを変更します。透過モードの場合は、ルーテッド モードに変更します。ルーテッド モードの場合は、透過モードに変更します。ASDM で管理コンテキストのモードを変更することはできません。CLI でのモードの変更については、「CLI での透過またはルーテッド ファイアウォール モードの設定」を参照してください。モードを変更すると、FWSM は実行コンフィギュレーションをクリアします。これは、多くのコマンドがどちらかのモードでしかサポートされていないからです。すでに実装済みのコンフィギュレーションがある場合は、モードを変更する前に必ずコンフィギュレーションのバックアップを作成してください。新しくコンフィギュレーションを作成するときにこのバックアップを参照する場合があります。Tools > File Management ペイン、または Tools > File Transfer ペインを参照してください。デフォルトのルーテッド モードで新しいコンテキストを追加した場合、ファイアウォール モードを変更する前に、新しいコンテキストを適用してください。モードを変更するには、コンテキストが実行中である必要があるからです。

- Delete：コンテキストを削除します。
- Number of ACL partitions (1-12)：メモリ パーティションの数を設定します。デフォルトは 12 です。マルチコンテキスト モードで、FWSM は、ルール コンフィギュレーションに割り当てられたメモリをパーティションに分割し、各コンテキストをパーティションに割り当てます。デフォルトで、コンテキストは、ACE、AAA ルールなど最大 12,130 のルールを提供する 12 のパーティションのうちの 1 つに属します。FWSM は、起動時にロードされる順番でコンテキストをパーティションに割り当てます。たとえば、12 のコンテキストがある場合、各コンテキストは個別のパーティションに割り当てられ、12,130 のルールを使用できます。さらに 1 つのコンテキストを追加すると、コンテキスト番号 1 および新しいコンテキスト番号 13 の両方がパーティション 1 に割り当てられ、2 つのコンテキスト合計で 12,130 のルールを使用できます。他の 11 のコンテキストは、引き続きそれぞれが 12,130 のルールを使用できます。コンテキストを削除しても、パーティションのメンバーシップは変わりません。したがって、リブートしてコンテキストが均等に分配されるまで、コンテキストの分配が不均一になることがあります。

  ルールは先着順で使用されるため、コンテキストによっては使用するルールが他のコンテキストよりも多くなることがあります。

  コンテキストをパーティションに手動で割り当てることもできます。また、コンテキストの数と一致するように、パーティションの数を減らすこともできます。

（注）　パーティションの数を変更した場合、FWSM をリロードする必要があります。

詳細情報

セキュリティ コンテキストの概要

CLI での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

ファイアウォール モードの概要

CLI での透過またはルーテッド ファイアウォール モードの設定

モード

次の表に、この機能を使用できるモードを示します。

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

Add/Edit Context ダイアログボックスで、セキュリティ コンテキストの追加または編集、およびコンテキスト パラメータの定義ができます。

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。大文字と小文字が区別されるため、たとえば「customerA」と「CustomerA」の 2 種類のコンテキストを使用できます。「System」および「Null」（大文字および小文字）は予約されている名前であるため、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を示します。
  - Interface：インターフェイス ID を示します。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：インターフェイスをコンテキストに追加します。
  - Edit：インターフェイスの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。
- Resource Assignment：コンテキストをリソース クラスとメモリ パーティションに割り当てます。
  - Resource Class：リストからクラスを選択します。
  - Edit：選択したリソース クラスを編集します。
  - New：リソース クラスを追加します。
  - ACL Partition：メモリ パーティションを選択します。FWSM が、起動時に次に使用可能なパーティションにコンテキストを割り当てるようにする場合は、**Default** を選択します。コンテキストをパーティションに手動で割り当てると、パーティションは*排他的*になります。排他的パーティションには、そのパーティションに特別に割り当てたコンテキストのみが含まれます。特別に割り当てたコンテキストがないパーティションは包括的であり、コンテキストはラウンドロビン式に割り当てられます。すべてのパーティションにコンテキストを割り当てた場合、すべて排他的になります。ただし、パーティションに割り当てられていないコンテキストを後から追加する場合は、デフォルトでパーティション 0 に割り当てられます。
- Config URL：コンテキスト コンフィギュレーションの場所を URL として指定します。リストでファイル システムのタイプをクリックして、サーバ（リモート ファイル システムの）、パス、ファイル名をボックスに入力します。FTP の場合、URL は次の形式になります。

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

  ファイルがまだ存在しない場合は、FWSM がそのファイルを作成します。
- 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コンテキストにフェールオーバー グループを設定します。
- Firewall Mode：ファイアウォール モードを示します。「ルーテッド」または「透過」です。管理コンテキストでないコンテキストのファイアウォール モードを変更するには、Security Contexts ペインの Change Firewall Mode ボタンを表示してください。デフォルトは、ルーテッド モードです。
- Description：（オプション）コンテキストの説明を入力します。

モード

次の表に、この機能を使用できるモードを示します。

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

Add/Edit Interface Allocation ダイアログボックスで、インターフェイスをコンテキストに割り当て、インターフェイス パラメータを設定できます。

フィールド

- Vlans：コンテキストに割り当てるインターフェイスを指定します。
  - Vlan Range：インターフェイス ID またはインターフェイス ID の範囲を設定します。インターフェイスを 1 つだけ指定する場合は、最初のリストで ID をクリックします。範囲を指定する場合は、次のリストで最後の ID（ある場合）をクリックします。透過ファイアウォール 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。
- Aliased Names：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は英字、最後は英字または数字にします。間の文字として使用できるのは、英字、数字、下線だけです。このボックス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 ボックスで設定できます。マルチコンテキストで同じ名前を使用できます。また、マルチコンテキストの VLAN ID は、指定した名前と同じにすることも、違う名前にすることもできます。同じコンテキストの異なる VLAN ID に同じ名前を使用することはできません。
  - Range：エイリアス名の拡張子を数字で設定します。複数のインターフェイスを範囲指定する場合、名前の後に追加する数字を範囲で入力できます。
- Show Hardware Properties in Context：エイリアス名が設定されている場合でも、コンテキスト ユーザはコンテキスト内の VLAN ID を表示できます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	—	—	•