

マルチ コンテキスト モード

この章では、ASA でマルチ 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。

- セキュリティ コンテキストについて （1 ページ）
- マルチ コンテキスト モードのライセンス （13 ページ）
- マルチ コンテキスト モードの前提条件 （15 ページ）
- マルチ コンテキスト モードのガイドライン （15 ページ）
- マルチ コンテキスト モードのデフォルト （16 ページ）
- マルチ コンテキストの設定 （17 ページ）
- コンテキストとシステム実行スペースの切り替え （28 ページ）
- セキュリティ コンテキストの管理 （29 ページ）
- セキュリティ コンテキストのモニタリング （33 ページ）
- マルチ コンテキスト モードの履歴 （36 ページ）

セキュリティ コンテキストについて

単一の ASA は、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パーティション化できます。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として機能します。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、マルチ コンテキスト モードのガイドライン （15 ページ）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。

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 コンテキストを有効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する場合。

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、ASA 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。

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）サーバー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（サーバー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、ユーザー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ー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。このコンテキストの名前は "admin" です。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 がパケットを分類する方法

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。

（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。

（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。MAC アドレスの自動生成を有効にできます。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。

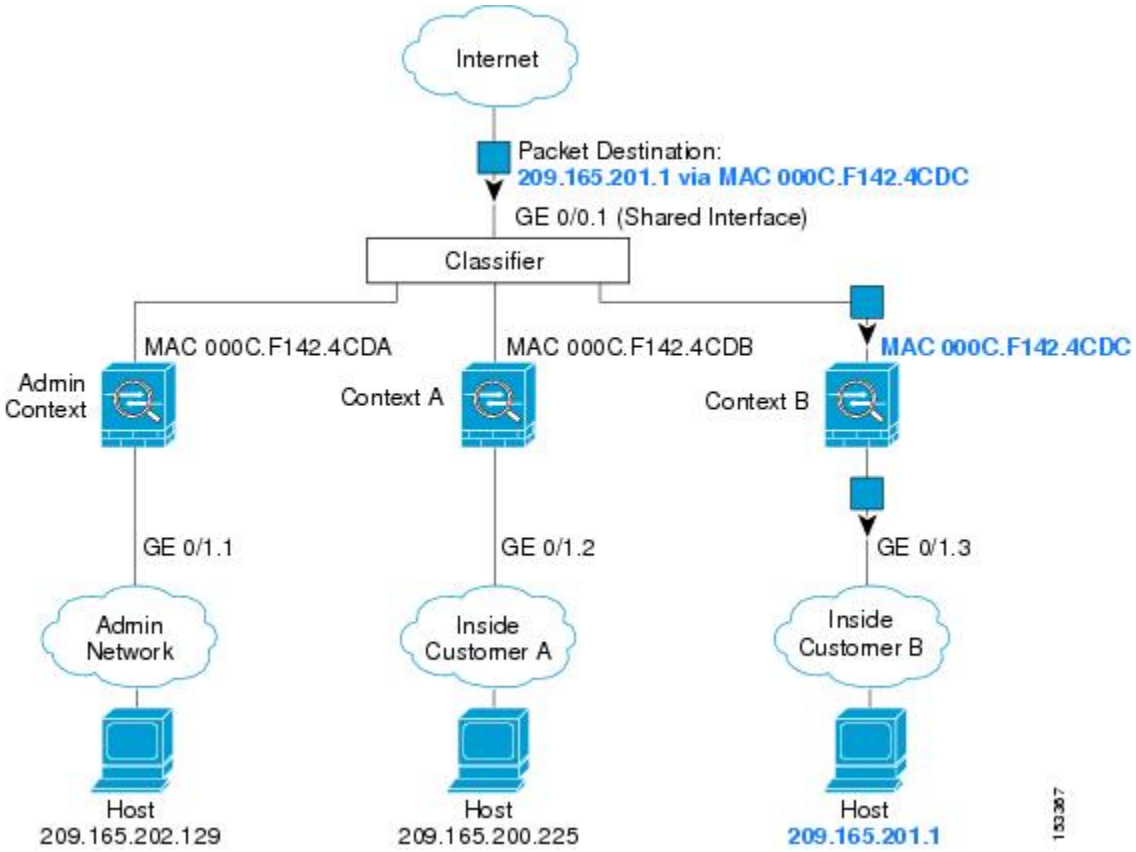
NAT の設定

固有の MAC アドレスの使用を有効にしなければ、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。

分類例

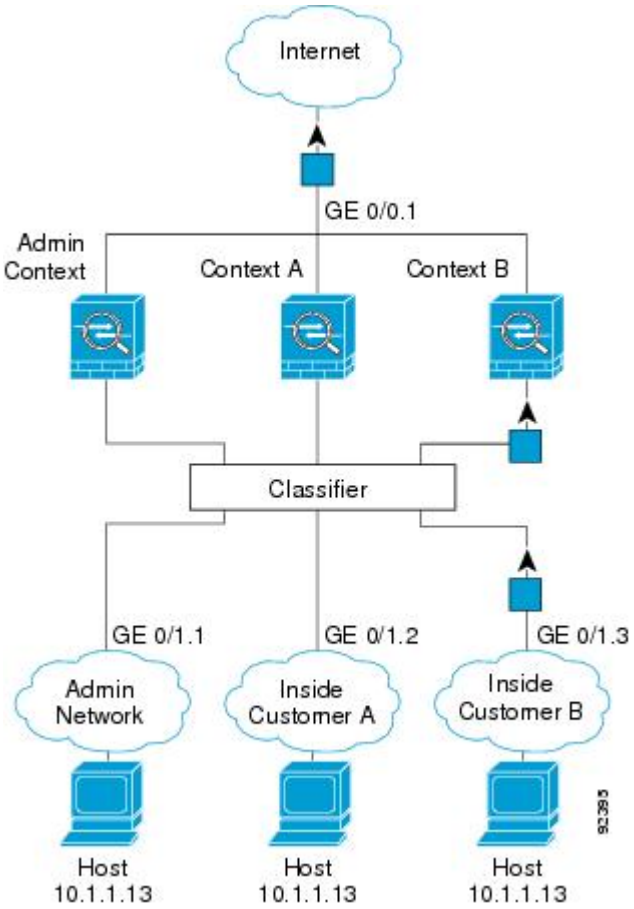
次の図に、外部インターフェイスを共有するマルチ コンテキストを示します。コンテキスト B にはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをコンテキスト B に割り当てます。

図 *1: MAC* アドレスを使用した共有インターフェイスのパケット分類



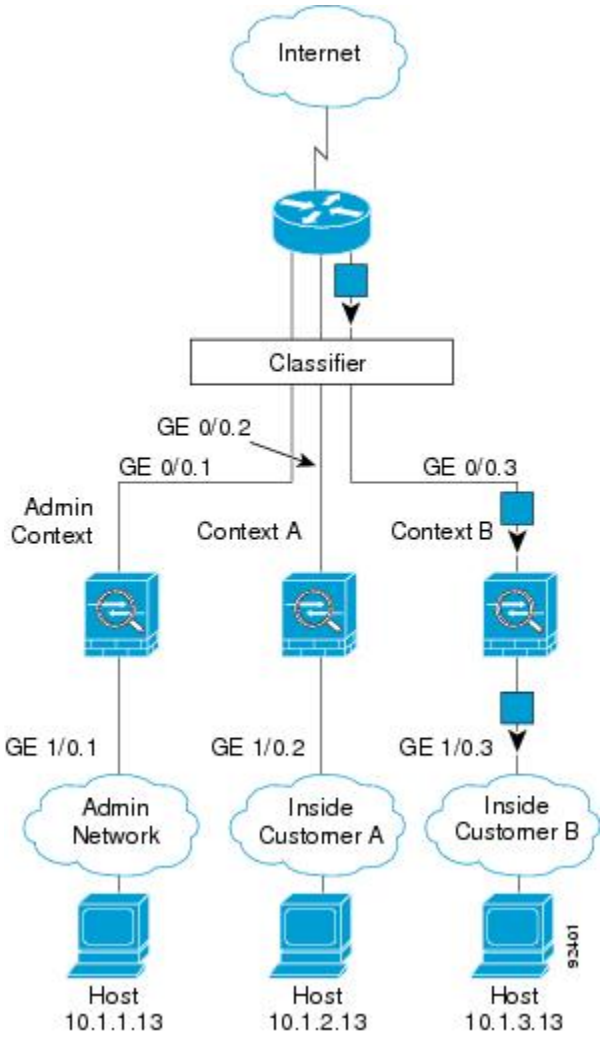
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のコンテキストBのホストを示します。分類子は、パケットをコンテキストBに割り当てます。これは、入力インターフェイスがギガビット イーサネット 0/1.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 *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。次の図に、ネットワーク内のコンテキストBのホストに向けられたインターネットからのパケットを示します。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:* トランスペアレント ファイアウォール コンテキスト



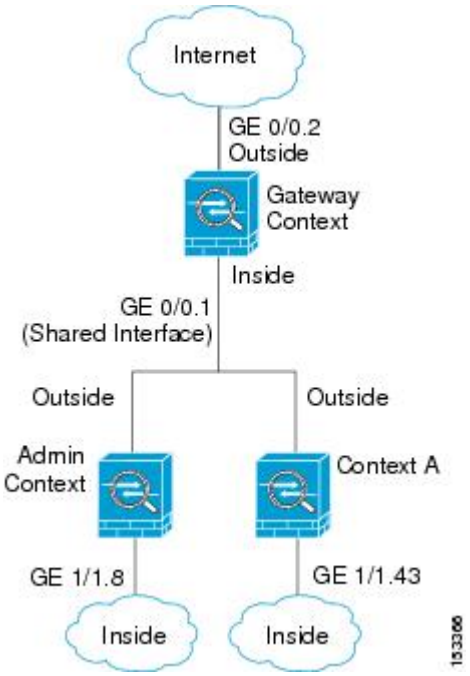
セキュリティ コンテキストのカスケード接続

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。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。

次の図に、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 *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。

システム管理者のアクセス

2 つの方法で、システム管理者として ASA をアクセスできます。

- 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

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。

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ー名をローカル 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。

インターフェイス使用率の管理

管理インターフェイスは、使用しているモデルに応じて、管理トラフィック専用の個別インターフェイスとなります。

ルーテッド ファイアウォール モードでは、管理インターフェイスをすべてのコンテキストで共有できます。

トランスペアレント ファイアウォール モードの管理インターフェイスは特殊です。許可される最大通過トラフィック インターフェイスに加えて、この管理インターフェイスを個別の管理専用インターフェイスとして使用できます。ただし、マルチコンテキストモードでは、どのインターフェイスもトランスペアレントコンテキスト間で共有させることはできません。代わりに、管理インターフェイスのサブインターフェイスを使用して、各コンテキストにインターフェイスを 1 つ割り当てることができます。ただし、サブインターフェイスを使用できるのは、Firepower デバイスモデル の管理インターフェイスに限られます。の ASA モデルの場合は、データインターフェイスまたはデータインターフェイスのサブインターフェイスを使用して、コンテキスト内のブリッジグループに追加する必要があります。

Firepower 4100/9300 シャーシトランスペアレントコンテキストでは、管理インターフェイスとサブインターフェイスのいずれも、特別なステータスを保持しません。この場合は、コンテキストをデータインターフェイスとして扱い、ブリッジグループに追加する必要があります(シングルコンテキストモードでは、管理インターフェイスで特別なステータスが保持されるので注意してください)。

トランスペアレントモードに関するもう 1 つの考慮事項：マルチコンテキストモードを有効にすると、設定されているすべてのインターフェイスが自動的に管理コンテキストに割り当てられます。たとえば、デフォルト設定に管理インターフェイスが含まれている場合、そのインターフェイスは管理コンテキストに割り当てられます。メインインターフェイスを管理コンテキストに割り当てたままで、ネイティブ VLAN を使用してメインインターフェイスを管理し、サブインターフェイスを使用して各コンテキストを管理するという選択肢もあります。管理コンテキストを透過的にすると、その IP アドレスは削除されることに注意してください。管理コンテキストをブリッジグループに割り当て、BVI に IP アドレスを割り当てる必要があります。

リソース管理の概要

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。

リソース クラス

ASA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、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。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。

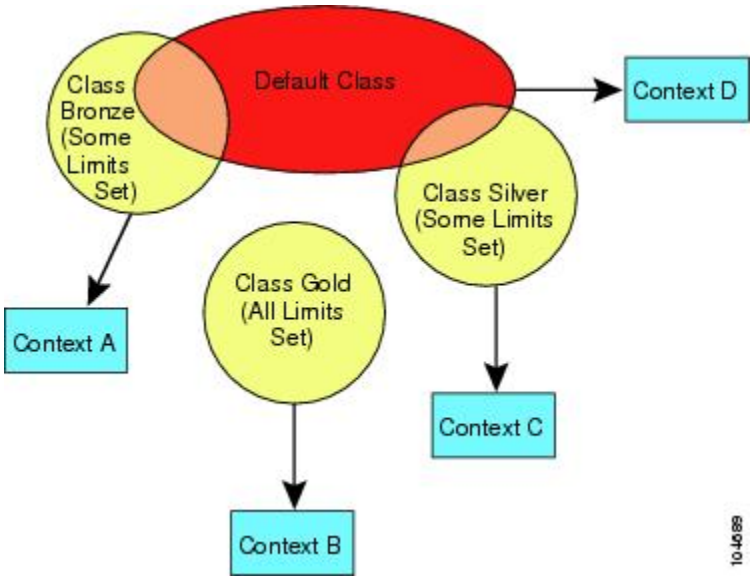
ほとんどのリソースについては、デフォルトクラスではすべてのコンテキストがリソースに無制限でアクセスできます。ただし、次の制限を除きます。

- 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）。

- ASDM 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：（モデルによって異なる）。（システムの最大値）。
- セキュアクライアント ピア — 0 セッション。（セキュアクライアント ピア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）。
- 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）。

次の図に、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。

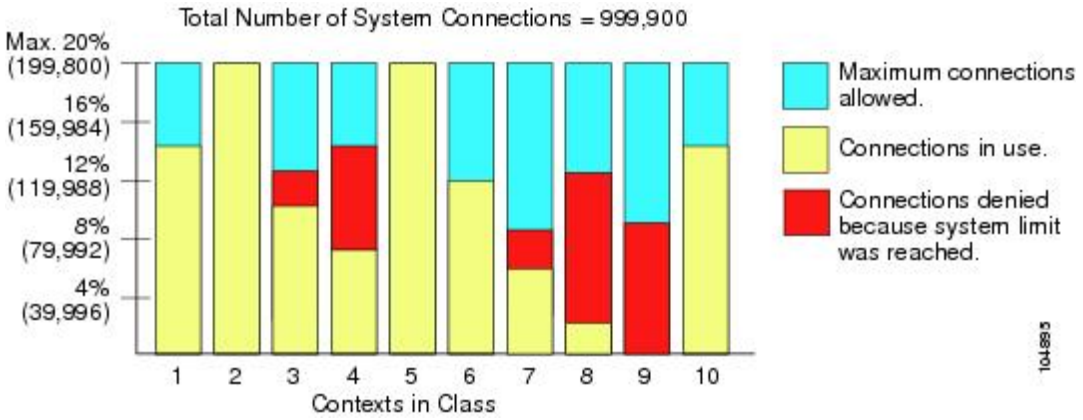
図 *5:* リソース クラス



オーバーサブスクライブ リソースの使用

ASA をオーバーサブスクライブするには、割り当て率の合計が 100% を超えるようにあるリソースをすべてのコンテキストに割り当てます（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。

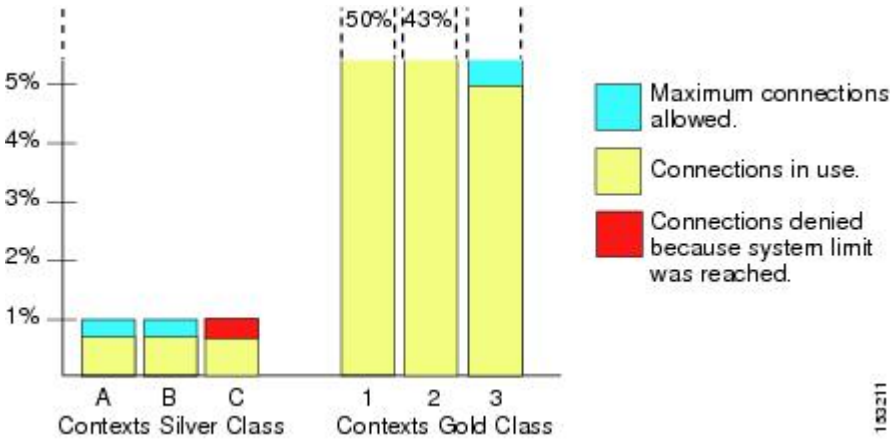
図 *6:* リソース オーバーサブスクリプション



無限リソースの使用

ASA は、パーセンテージや絶対値ではなく、クラス内の 1 つ以上のリソースに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、これらの制限の合計である 3% に達することは不可能になります無制限アクセスの設定は、ASA のオーバーサブスクライブと同様ですが、システムをどの程度オーバーサブスクライブできるかを詳細には制御できません。

図 *7:* 無限リソース



MAC アドレスについて

手動で MAC アドレスを割り当ててデフォルトをオーバーライドできます。マルチコンテキストモードでは、（コンテキストに割り当てられているすべてのインターフェイスの）一意の MAC アドレスと（サブインターフェイスの）シングルコンテキストモードを自動的に生成できます。。



（注） 親インターフェイスと同じ組み込みの MAC アドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA デバイスで特定のインスタンスでのトラフィックの中断を回避できます。

マルチコンテキスト モードでの MAC アドレス

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。

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で仮想 MAC アドレスの自動生成を有効にしてください。

自動 MAC アドレス

マルチ コンテキスト モードでは、自動生成によって一意の MAC アドレスがコンテキストに割り当てられているすべてのインターフェイスに割り当てられます。

MAC アドレスを手動で割り当てた場合、自動生成が有効になっていても、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（有効な場合）。

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、インターフェイスの MAC アドレスを手動で設定できます。

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。

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 MAC アドレスの最後の 2 バイトに基づいて自動生成されるプレフィックスです。*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*）。

A24**D.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*

（注） プレフィックスのない MAC アドレス形式は従来のバージョンです。従来の形式に関する詳細については、コマンド リファレンスの **mac-address auto** コマンドを参照してください。

VPN サポート

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。

マルチ コンテキスト モードでサイト間 VPN を使用できます。

リモート アクセス VPN の場合は、SSL VPN および IKEv2 プロトコルに AnyConnect 3.x 以降を使用する必要があります。 セキュアクライアント のイメージとカスタマイズ、およびすべてのコンテキストで共有フラッシュメモリを使用するために、コンテキストごとにフラッシュストレージをカスタマイズできます。サポートされていない機能については、マルチ コンテキスト モードのガイドライン （15 ページ） を参照してください。ASA リリースごとにサポートされる VPN 機能の詳細なリストについては、マルチ コンテキスト モードの履歴 （36 ページ） を参照してください。

（注） マルチコンテキストモードでは Secure Client Premier ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。

マルチ コンテキスト モードのライセンス

モデル	ライセンス要件
Firepower 1010	サポートしない

モデル	ライセンス要件
Firepower 1100	Essentialsライセンス：2 コンテキスト オプションライセンス、最大： *Firepower 1120*：*5* *Firepower 1140*：*10* *Firepower 1150*：*25*
Firepower 2100	Essentialsライセンス：2 コンテキスト オプションライセンス、最大： *Firepower 2110*：*25* *Firepower 2120*：*25* *Firepower 2130*：*30* *Firepower 2140*：*40*
Cisco Secure Firewall 3100	Essentialsライセンス：2 コンテキスト オプションライセンス、最大： Secure Firewall 3105：100 *Cisco Secure Firewall 3110*：*100* *Cisco Secure Firewall 3120*：*100* *Cisco Secure Firewall 3130*：*100* *Cisco Secure Firewall 3140*：*100*
Firepower 4100	Essentialsライセンス：10 コンテキスト オプションライセンス：最大 *250* コンテキスト
Firepower 9300	Essentialsライセンス：10 コンテキスト オプションライセンス：最大 *250* コンテキスト
ISA 3000	サポートしない
ASA 仮想	サポートしない

（注） 管理コンテキストに管理専用インターフェイスのみが含まれていて、通過トラフィックのデータインターフェイスが含まれていない場合は、制限に対してカウントされません。

（注） マルチコンテキストモードでは Secure Client Premier ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。

マルチ コンテキスト モードの前提条件

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。

マルチ コンテキスト モードのガイドライン

フェールオーバー

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

クロス コンテキスト IPv6 ルーティングはサポートされません。

サポートされない機能

マルチコンテキスト モードでは、次の機能をサポートしません。

- 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
- 仮想トンネルインターフェイス（VTI）
- スタティック ルート トラッキング

マルチ コンテキスト モードでは、次のリモート アクセス VPN の機能を現在サポートしません。

- AnyConnect 2.x 以前

- IKEv1
- SAML
- WebLaunch
- VLAN Mapping
- HostScan
- VPN ロード バランシング
- カスタマイゼーション
- L2TP

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。
- フラッシュ メモリのルート ディレクトリにコンテキスト コンフィギュレーションを保存する場合、一部のモデルでは、メモリに空き容量があっても、そのディレクトリに保存する余地がなくなることがあります。この場合は、コンフィギュレーションファイルのサブディレクトリを作成します。背景：の一部のモデルでは、内蔵フラッシュメモリに FAT16 ファイルシステムが使用されています。8.3 形式に準拠した短い名前を使用しない場合、または大文字の文字を使用した場合、ファイルシステムが長いファイル名の保存にスロットを使用するため、保存できるファイルとフォルダの数は 512 未満となります（https://support.microsoft.com を参照）。
- ACI では、すべてのリーフで同じ MAC アドレスを使用してポリシーベースリダイレクト（PBR）ヘルスチェックが実行されます（L2 ping）。これにより、MAC フラップが発生します。MAC フラップを解決するには、インラインセットでタップモードオプションを設定します。ただし、Firewall Threat Defense ハイアベイラビリティが設定されている場合は、フェールオーバー中の接続処理のために MAC 学習を有効にする必要があります。したがって、インラインセットインターフェイスを使用する HA ペアの Firewall Threat Defense を含む ACI 環境では、パケット損失を回避するために、スタンドアロンかクラスタで Firewall Threat Defense を展開します。

マルチ コンテキスト モードのデフォルト

- 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 （9 ページ） を参照してください。

マルチ コンテキストの設定

手順

ステップ 1 マルチ コンテキスト モードの有効化または無効化 （17 ページ）。

ステップ 2 （オプション）リソース管理用のクラスの設定 （20 ページ）。

（注） VPN のサポートのために、リソース クラスの VPN リソースを設定する必要があります。デフォルト クラスは VPN を許可しません。

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。

- Firepower 1100、アプライアンスモードの Firepower 2100、Secure Firewall 3100：基本的なインターフェイス設定。
- プラットフォームモードの Firepower 2100：スタートアップ ガイドを参照してください。
- Firepower 4100/9300：論理デバイス Firepower 4100/9300

ステップ 4 セキュリティ コンテキストの設定 （24 ページ）。

ステップ 5 （オプション）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 （28 ページ）。

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。ルーテッド モードおよびトランスペアレント モードのインターフェイス を参照してください。

マルチ コンテキスト モードの有効化または無効化

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。

ASDM では、[ハイ アベイラビリティおよび拡張性（High Availability and Scalability）] ウィザードを使用し、アクティブ/アクティブ フェールオーバーを有効にした場合、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、ハイ アベイラビリティのためのフェールオーバーを参照してください。アクティブ/アクティブ フェールオーバーを使用するか、またはシングル モードに戻す場合は、CLI を使用してモードを変更する必要があります。モードの変更には確認を必要とするため、コマンドライン インターフェイス ツールは使用できません。この項では、CLI でのモード変更について説明します。

マルチ コンテキスト モードの有効化

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。これらはシステム 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。

始める前に

スタートアップ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と異なっている場合は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。ファイルの管理を参照してください。

手順

マルチコンテキストモードに変更します。

mode multiple

例：

モードを変更して設定を変換し、システムをリロードするように求められます。

（注） SSH接続を再確立する前に、管理コンテキストでRSAキーペアを再生成する必要があります。コンソールから、**crypto key generate rsa modulus** コマンドを入力します。詳細については、SSH アクセスの設定を参照してください。

例：

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!
The old running configuration file will be written to flash

Converting the configuration - this may take several minutes for a large configuration

The admin context configuration will be written to flash

The new running configuration file was written to flash
Security context mode: multiple
ciscoasa(config)#
```

```
***
*** --- START GRACEFUL SHUTDOWN ---
***
*** Message to all terminals:
***
***   change mode
Shutting down isakmp
Shutting down webvpn
Shutting down License Controller
Shutting down File system


***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
```

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。

始める前に

この手順はシステム実行スペースで実行します。

手順

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します。

copy disk0:old_running.cfg startup-config

例：

```
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

ステップ 2 モードをシングル モードに設定します。

mode single

例：

```
ciscoasa(config)# mode single
```

ASA をリブートするよう求められます。

リソース管理用のクラスの設定

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。

始める前に

- この手順はシステム実行スペースで実行します。
- 以下の表に、リソース タイプおよび制限を記載します。



（注） 「システム制限」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。

表 *1*: リソース名および制限

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	説明
ASDM Sessions	同時接続数	最小 1 最大 5	200	ASDM 管理セッション。 ASDM セッションでは、2 つの HTTPS 接続が使用されます。一方は常に存在するモニター用で、もう一方は変更を行ったときにだけ存在する設定変更用です。たとえば、ASDM セッションのシステム制限が 200 の場合、HTTPS セッション数は 400 に制限されます。

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	説明
Connections Conns/Sec	同時またはレート	該当なし	同時接続数：モデルごとの接続制限については、モデルごとのライセンス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）。 （注） syslog メッセージは、xlates または conns のいずれか制限が低い方に対して生成されます。たとえば、xlates の制限を 7、conns の制限を 9 に設定した場合、ASA は syslog メッセージ 321001（「Resource 'xlates' limit of 7 reached for context 'ctx1'」）のみ生成し、321002（「Resource 'conn rate' limit of 5 reached for context 'ctx1'」）は生成しません。
ホスト	同時接続数	該当なし	該当なし	ASA 経由で接続可能なホスト。
Inspects/sec	利率	該当なし	該当なし	アプリケーション インスペクション数/秒。
MAC Entries	同時接続数	該当なし	（モデルによって異なる）	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。
ルート	同時接続数	該当なし	該当なし	ダイナミック ルート。

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	説明
セキュアクライアント Burst	同時接続数	該当なし	モデルに応じた セキュアクライアント ピア数から、セキュアクライアント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。	セキュアクライアント 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 セキュアクライアント セッションの数。たとえば、使用するモデルで 5000 のピアがサポートされており、セキュアクライアントで割り当てたピア数の合計が全コンテキストで 4000 の場合は、残りの 1000 セッションがセキュアクライアント Burst に使用可能です。セキュアクライアント 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 セキュアクライアント Burst 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。
セキュアクライアント	同時接続数	該当なし	ご使用のモデルに使用できる セキュアクライアント Premium ピアについては、モデルごとのライセンスを参照してください。	セキュアクライアントピア。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ピアは、そのコンテキストに対して保証されます。
Other VPN Burst	同時接続数	該当なし	モデルに応じた Other VPN セッション数から、Other VPN 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。	Other VPN 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。たとえばモデルが 5000 セッションをサポートしており、Other VPN のすべてのコンテキスト全体で 4000 セッションを割り当てると、残りの 1000 セッションは Other VPN Burst に使用できます。Other VPN 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 Other VPN Burst ではオーバーサブスクライブが可能です。すべてのコンテキストでバースト プールを先着順に使用できます。

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	説明
その他の VPN	同時接続数	該当なし	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。
IKEv1 SAs In Negotiation	同時（パーセンテージのみ）	該当なし	このコンテキストに割り当てられている Other VPN セッションのパーセンテージ。セッションをコンテキストに割り当てるには、Other VPN リソースを参照してください。	コンテキストでの Other VPN パーセンテージ制限として表される、着信 IKEv1 SA ネゴシエーション。
SSH	同時接続数	最小 1 最大 5	100	SSH セッション。
ストレージ	MB	最大値は、指定するフラッシュ メモリのドライブによって異なります。	最大値は、指定するフラッシュ メモリのドライブによって異なります。	コンテキストでのディレクトリのストレージ制限（MB 単位）。
Syslogs/sec	利率	該当なし	該当なし	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	該当なし	該当なし	ネットワーク アドレス変換。

手順

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の 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 **[設定（Configuration）] > [コンテキスト管理（Context Management）] > [リソース クラス（Resource Class）]** の順に選択し、[追加（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、最大 20 文字のクラス名を入力します。

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。

各リソース タイプの説明については、上記の表を参照してください。

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。ほとんどのリソースについて、0 を指定すると無制限と設定されます。VPN タイプについて、0 を指定すると制限なしと設定されます。

（注） また、コンテキスト内で **[Configuration]** > **[Device Management]** > **[Management Access]** > **[Management Session Quota]** も設定して、最大管理セッション（SSH など）を設定した場合は、小さい方の値が使用されます。

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。

各リソース タイプの説明については、上記の表を参照してください。

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。0 は制限を無制限に設定します。

ステップ 6 [OK] をクリックします。

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。

始める前に

- この手順はシステム実行スペースで実行します。
- インターフェイスを設定します。トランスペアレントモードのコンテキストでは、コンテキスト間でインターフェイスを共有できないため、サブインターフェイスの使用が必要になる場合があります。管理インターフェイスの使用計画については、「インターフェイス使用率の管理 （8 ページ）」を参照してください。
  - Firepower 1100、アプライアンスモードの Firepower 2100、Secure Firewall 3100：基本的なインターフェイス設定。
  - プラットフォームモードの Firepower 2100：スタートアップ ガイドを参照してください。

• Firepower 4100/9300：論理デバイス Firepower 4100/9300

手順

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、[デバイス リスト（Device List）] ペインで、アクティブなデバイスの IP アドレスの下にある [システム（System）] をダブルクリックします。

ステップ 2 **[構成（Configuration）] > [コンテキスト管理（Context Management）] > [セキュリティ コンテキスト（Security Contexts）]** の順に選択し、[追加（Add）] をクリックします。

[コンテキストの追加（Add Context）] ダイアログボックスが表示されます。

ステップ 3 [セキュリティ コンテキスト（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。

この名前は大文字と小文字が区別されるため、たとえば「customerA」と「CustomerA」という 2 つのコンテキストを設定できます。「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 [インターフェイス割り当て（Interface Allocation）] 領域で、[追加（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。

a) **[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。

b) （オプション）**[インターフェイス（Interfaces）]>[サブインターフェイス範囲（Subinterface Range）]** ドロップダウン リストから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。

c) （オプション）[エイリアス名（Aliased Names）] 領域で、[コンテキストでエイリアス名を使用する（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。

- [名前（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 [範囲（Range）] フィールドで設定できます。

- （オプション）[範囲（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。

d) （オプション）エイリアス名を設定した場合でも、コンテキストのユーザー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、[コンテキストでハードウェアプロパティを表示する（Show Hardware Properties in Context）] をオンにします。

e) [OK] をクリックして、[コンテキストの追加（Add Context）] ダイアログボックスに戻ります。

ステップ 5 （任意）[リソース割り当て（Resource Assignment）] 領域で、[リソース クラス（Resource Class）] ドロップダウン リストから、このコンテキストをリソース クラスに割り当てる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。

ステップ 6 [構成 URL（Config URL）] ドロップダウン リストから、ファイル システム タイプを選択します。フィールドに、コンテキスト コンフィギュレーションの場所の 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 7 （任意）[ログイン（Login）] をクリックし、外部ファイル システムのユーザー名とパスワードを設定します。

ステップ 8 （任意）[フェールオーバーグループ（Failover Group）] ドロップダウン リストからグループ名を選択し、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。

ステップ 9 （任意）[クラウド Web セキュリティ（Cloud Web Security）] の [有効化（Enable）] をクリックして、このコンテキストで Web セキュリティ インスペクションを有効にします。システム コンフィギュレーションに設定されたライセンスを上書きする場合は、[ライセンス（License）] フィールドにライセンスを入力します。

ステップ 10 （任意）[説明（Description）] フィールドに、説明を追加します。

ステップ 11 （任意）[ストレージURL割り当て（Storage URL Assignment）] 領域では、各コンテキストでフラッシュメモリを使用して セキュアクライアント などの VPN パッケージを保存できるだけでなく、セキュアクライアント およびクライアントレス SSL VPN ポータルのカスタマイズ用のストレージも提供できます。たとえば、マルチコンテキストモードを使用してダイナミック アクセス ポリシーに セキュアクライアント プロファイルを設定する場合、コンテキスト固有のプライベートおよび共有ストレージを計画する必要があります。読み取り専用の共有記憶域だけでなく、コンテキストごとに専用の記憶域も使用できます。**注：[ツール（Tools）]>[ファイル管理（File Management）]** を使用して、指定するディスク上にターゲットディレクトリが存在することを確認してください。

a) [プライベート ストレージ割り当ての構成（Configure private storage assignment）] チェックボックスをオンにして、[選択（Select）] ドロップダウン リストから専用ストレージ ディレクトリを選択します。private で指定できる専用記憶域は、コンテキストごとに 1 つに限られます。コンテキスト内から（およびシステム実行スペースから）、このディレクトリの読み取り/書き込み/削除操作を実行できます。ASA は指定されたパスにサブディレクトリを作成し、コンテキストに基づく名前を付けます。たとえば、contextA の場合、**disk1:/private-storage** をパスとして指定すると、ASA はこのコンテキストのサブディレクトリを **disk1:/private-storage/contextA/** に作成します。オプションで、ファイル システムがコンテキスト管理者に公開されないよう、このパスにコンテキスト内での名前を指定することもできます。それには、[マッピング先（is mapped to）] フィールドに名前を入力します。たとえば、**context** をマップされる名前として指定すると、コンテキスト内からは、このディレクトリは **context:** と呼ばれます。コンテキストごとに許容するディスク容量を制御する方法については、リソース管理用のクラスの設定 （20 ページ）を参照してください。

b) [共有ストレージ割り当ての構成（Configure shared storage assignment）] チェックボックスをオンにして、[選択（Select）] ドロップダウン リストから共有ストレージ ディレクトリを選択します。指定できる読み取り専用の **shared** 記憶域はコンテキストごとに 1 つですが、共有ディレクトリは複数作成できます。セキュアクライアント パッケージなど、すべてのコンテキストで共有できる共通の大きなファイルの重複を減らすために、共有のストレージスペースを使用できます。この記憶域は複数のコンテキストで共有されるため、ASA は記憶域にはコンテキストのサブディレクトリを作成しません。共有ディレクトリの書き込みおよび削除操作は、システム実行スペースでのみ実行できます。

ステップ 12 [OK] をクリックして、[セキュリティ コンテキスト（Security Contexts）] ペインに戻ります。

ステップ 13 （任意） コンテキストを選択してから [ファイアウォール モードの変更（Change Firewall Mode）] をクリックし、ファイアウォール モードをトランスペアレントに設定します。

新しいコンテキストの場合は、消去するための設定はありません。[モードの変更（Change Mode）] をクリックして、トランスペアレント ファイアウォール モードに変更します。

既存のコンテキストの場合は、モードを変更する前に設定をバックアップするのを忘れないでください。

（注） ASDM の現在接続されているコンテキストのモード（通常は管理コンテキスト）は変更できません。コマンドラインでモードを設定するには、ファイアウォール モード（シングル モード）の設定を参照してください。

ステップ 14 （任意） MAC アドレスの自動生成をカスタマイズするには、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 （28 ページ）を参照してください。

ステップ 15 （任意） デバイスの最大 TLS プロキシ セッション数を指定するには、[ASA でサポートされる必要がある TLS プロキシ セッションの最大数の指定（Specify the maximum number of TLS Proxy sessions that the ASA needs to support）] チェックボックスをオンにします。TLS プロキシの詳細については、ファイアウォールの設定ガイドを参照してください。

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。

始める前に

- コンテキストでインターフェイスの名前を設定すると、ただちに新規 MAC アドレスが生成されます。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。

手順

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、[デバイスリスト（Device List）] ペインで、アクティブなデバイスの IP アドレスの下にある [システム（System）] をダブルクリックします。

ステップ 2 **[設定（Configuration）] > [コンテキスト管理（Context Management）] > [セキュリティコンテキスト（Security Contexts）]** の順に選択し、[自動 MAC アドレス（Mac-Address auto）] をオンにします。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。

ステップ 3 （オプション）[プレフィックス（Prefix）] チェックボックスをオンにしてから、フィールドに 0 ～ 65535 の範囲内の 10 進数値を入力します。

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。

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実行コンフィギュレーション実行コンフィギュレーションは、ユーザー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。

手順

ステップ 1 [Device List] ペインでシステムを設定するには、アクティブなデバイスの 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 コンテキストを設定するには、[Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

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。

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。

（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。

始める前に

この手順はシステム実行スペースで実行します。

手順

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 **[Configuration]** > **[Context Management]** > **[Security Contexts]** の順に選択します。

ステップ 3 削除するユーザーを選択し、[Delete] をクリックします。

[Delete Context] ダイアログボックスが表示されます。

ステップ 4 このコンテキストを再追加するかもしれず、再使用できるようにコンフィギュレーションファイルを保持する場合は、[Also delete config URL file from the disk] チェックボックスをオフにします。

コンフィギュレーション ファイルを削除するには、チェックボックスをオンにしたままにします。

ステップ 5 [Yes] をクリックします。

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（サーバー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、ユーザー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ーに制限する必要があります。

（注） ASDM の場合、ASDM セッションが切断されるため、ASDM 内の管理コンテキストを変更できません。新しい管理コンテキストに再割り当てなければならないことに注意するコマンドライン インターフェイス ツールを使用してこの手順を実行できます。

始める前に

- 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。
- この手順はシステム実行スペースで実行します。

手順

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 **[Tools]** > **[Command Line Interface]** を選択します。

[Command Line Interface] ダイアログボックスが表示されます。

ステップ 3 次のコマンドを入力します。

admin-context *context_name*

ステップ 4 [Send] をクリックします。

Telnet、SSH、HTTPS（ASDM）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。

始める前に

- 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、サーバー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。
- この手順はシステム実行スペースで実行します。

手順

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 **[Configuration]** > **[Context Management]** > **[Security Contexts]** の順に選択します。

ステップ 3 編集するコンテキストを選択して、[Edit] をクリックします。

[Edit Context] ダイアログボックスが表示されます。

ステップ 4 [Config URL] フィールドに新しい URL を入力して、[OK] をクリックします。

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。

コンフィギュレーションのクリアによるリロード

手順

ステップ 1 [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

ステップ 2 **[Tools]** > **[Command Line Interface]** を選択します。

[Command Line Interface] ダイアログボックスが表示されます。

ステップ 3 次のコマンドを入力します。

clear configure all

ステップ 4 [Send] をクリックします。

コンテキストの設定が削除されます。

ステップ 5 **[Tools]** > **[Command Line Interface]** を再度選択します。

[Command Line Interface] ダイアログボックスが表示されます。

ステップ 6 次のコマンドを入力します。

copy startup-config running-config

ステップ 7 [Send] をクリックします。

ASA が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、次の手順を実行してください。

手順

ステップ 1 セキュリティ コンテキストの削除 （29 ページ）。[Also delete config URL file from the disk] チェックボックスがオフになっていることを確認します。

ステップ 2 セキュリティ コンテキストの設定 （24 ページ）

セキュリティ コンテキストのモニタリング

この項では、コンテキスト情報を表示およびモニタリングする方法について説明します。

コンテキスト リソースの使用状況のモニタリング

手順

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/Telnet/SSH]：ASDM、Telnet、SSH 接続状況を表示します。
  - [Context]：各コンテキストの名前を表示します。

    各アクセス方式に対して、次の使用状況統計が表示されます。
  - [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。

- [Routes]：ダイナミック ルート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。

- [VPN]：VPN サイトツーサイト トンネル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。
  - [VPN Connections]：保証された VPN セッションの使用状況を表示します。
  - [VPN Burst Connections]：バースト VPN セッションの使用状況を表示します。
    - [Existing (#)]：既存トンネルの数を表示します。
    - [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 トンネル数を表示します。

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。

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。

システム設定での 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。

始める前に

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

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 **[Configuration]** > **[Context Management]** > **[Security Contexts]** を選択し、[Primary MAC] カラムと [Secondary MAC] カラムを表示します。

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

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 **[Configuration]** > **[Interfaces]** を選択し、[MAC Address] アドレス カラムを表示します。

このテーブルには、使用中の MAC アドレスが表示されます。MAC アドレスを手動で割り当てており、自動生成もイネーブルになっている場合は、システム コンフィギュレーションからは未使用の自動済み生成アドレスのみを表示できます。

マルチ コンテキスト モードの履歴

表 *2:* マルチ コンテキスト モードの履歴

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。 次の画面が導入されました。[Configuration] > [Context Management]。
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。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts]。
リソース管理	7.2(1)	リソース管理が導入されました。 次の画面が導入されました。[Configuration] > [Context Management] > [Resource Management]。

機能名	プラットフォームリリース	機能情報
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たり、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。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts]。
MAC アドレス自動割り当ての機能強化	8.0(4) 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。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts]。
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有効化	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。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts]。

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、ASA が MAC アドレス自動生成のコンフィギュレーションを変換し、デフォルトのプレフィックスを使用できるようになりました。ASA は、インターフェイス（ASA 5500-X）またはバックプレーン（ASASM）の 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。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有効である場合、既存のコンフィギュレーションの MAC アドレス メソッドをリロード時に変換しません。ただし、フェールオーバーを使用するときは、生成メソッドをプレフィックス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 メソッドを使用しない場合、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。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts]
ASASM 以外のすべてのモデル上での MAC アドレスの自動割り当てはデフォルトでディセーブル	9.0(1)	自動 MAC アドレスの割り当ては ASASM を除いて、デフォルトでディセーブルになりました。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts]。
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。

機能名	プラットフォームリリース	機能情報
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。 次の画面が変更されました。[Configuration] > [Context Management] > [Resource Class] > [Add Resource Class]
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。 次の画面が変更されました。[Configuration] > [Context Management] > [Resource Class] > [Add Resource Class]
IKEv1 SA ネゴシエーションの新しいリソース タイプ	9.1(2)	CPU と暗号化エンジンの過負荷を防ぐため、コンテキストごとに IKEv1 SA ネゴシエーションの最大パーセンテージを設定するための新しいリソース タイプ ikev1 in-negotiation が作成されました。特定の条件（大容量の証明書、CRL、チェックなど）によっては、このリソースを制限する必要がある場合があります。 次の画面が変更されました。[Configuration] > [Context Management] > [Resource Class] > [Add Resource Class]
マルチ コンテキスト モードでのリモート アクセス VPN サポート	9.5(2)	次のリモートアクセス機能をマルチコンテキストモードで使用できるようになりました。 • AnyConnect 3.x 以降（SSL VPN のみ、IKEv2 はサポートしません） • 中央集中型 セキュアクライアント のイメージの設定 • セキュアクライアント のイメージのアップグレード • セキュアクライアント 接続のコンテキストリソース管理 （注） マルチコンテキストモードでは Secure Client Premier ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。 次の画面が変更されました。**[Configuration]** > **[Context Management]** > **[Resource Class]** > **[Add Resource Class]**

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 モードの場合の証明書の事前入力/ユーザー名	9.6(2)	セキュアクライアント SSL サポートが拡張され、これまでシングルモードでのみ使用可能だった証明書の事前入力とユーザー名取得機能の CLI がマルチコンテキストモードでも有効にできるようになりました。 変更された画面はありません。
リモート アクセス VPN のフラッシュ仮想化	9.6(2)	マルチ コンテキスト モードのリモート アクセス VPN はフラッシュ仮想化をサポートします。使用可能な合計フラッシュに基づき、コンテキストごとにプライベート記憶域と共有ストレージの場所が設定できます。 • プライベート記憶域：該当ユーザーのみに関連付けられ、該当ユーザー対象コンテンツ固有のファイルを保存します。 • 共有ストレージ：有効になると、この領域にファイルがアップロードされ、あらゆるユーザー コンテキストが読み取り/書き込みできるようこの領域へのアクセスが許可されます。 次の画面が変更されました。**[Configuration] > [Context Management] > [Resource Class] > [Add Resource Class]** **[Configuration] > [Context Management] > [Security Contexts]**
マルチコンテキストデバイスでのセキュアクライアントプロファイルのサポート	9.6(2)	セキュアクライアント プロファイルは、マルチコンテキストデバイスでサポートされます。ASDM を使用して新しいプロファイルを追加するには、セキュアクライアントリリース 4.2.00748 または 4.3.03013 以降が必要です。
マルチコンテキストモードの セキュアクライアント接続のステートフル フェールオーバー	9.6(2)	マルチコンテキストモードで セキュアクライアント 接続のステートフル フェールオーバーがサポートされるようになりました。 変更された画面はありません。
マルチ コンテキスト モードでリモート アクセス VPN ダイナミック アクセス ポリシー（DAP）がサポートされました。	9.6(2)	マルチ コンテキスト モードで、コンテキストごとに DAP を設定できるようになりました。 変更された画面はありません。
マルチ コンテキスト モードでリモート アクセス VPN CoA（認可変更）がサポートされました。	9.6(2)	マルチ コンテキスト モードで、コンテキストごとに CoA を設定できるようになりました。 変更された画面はありません。

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 モードで、リモート アクセス VPN のローカライズがサポートされました。	9.6(2)	ローカリゼーションがグローバルでサポートされました。複数のコンテキストで共有されるローカリゼーション ファイル セットは 1 つだけです。 変更された画面はありません。
IKEv2 のリモート アクセス VPN は、マルチ コンテキスト モードでサポートされています。	9.9(2)	リモート アクセス VPN は、IKEv2 のマルチ コンテキスト モードで構成できます。
管理セッションの設定可能な制限	9.12(1)	集約、ユーザー単位、およびプロトコル単位の管理セッションの最大数を設定できます。これまでは、セッションの集約数しか設定できませんでした。この機能がコンソール セッションに影響を与えることはありません。マルチ コンテキスト モードでは HTTPS セッションの数を設定することはできず、最大セッション数は 5 で固定されています。また、**quota management-session** コマンドはシステム コンフィギュレーションでは受け入れられず、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ようになっています。集約セッションの最大数が 15 になりました。0（無制限）または 16 以上に設定してアップグレードすると、値は 15 に変更されます。 新規/変更された画面：**[Configuration] > [Device Management] > [Management Access] > [Management Session Quota]**
Firepower 1140 の最大コンテキスト数が 5 から 10 に増加	9.16(1)	Firepower 1140 は、最大 10 のコンテキストをサポートするようになりました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。