Cisco ASA シリーズ ASDM コンフィギュレーション ガイド（一般的な操作）

ソフトウェア バージョン 7.3

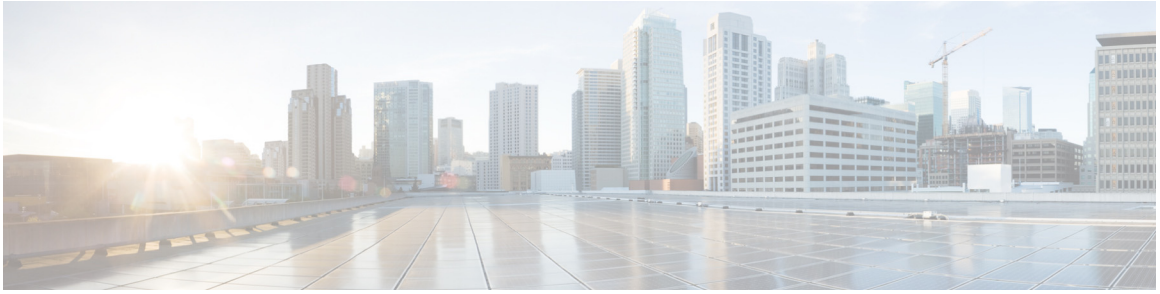
リリース：2014 年 7 月 24 日
更新：2014 年 9 月 16 日

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
住所、電話番号、FAX 番号は
以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices。

Text Part Number: なし、オンライン専用

Cisco ASA シリーズ ASDM コンフィギュレーション ガイド（一般的な操作）



このマニュアルについて

マニュアルの目的

このマニュアルの目的は、Adaptive Security Device Manager（ASDM）を使用して、Cisco ASA シリーズ用の一般的な動作の設定を支援することです。このマニュアルは、すべての機能を網羅しているわけではなく、ごく一般的なコンフィギュレーションの事例を紹介しています。

このマニュアルを通じて、「ASA」という語は、特に指定がない限り、サポートされているモデルに一般的に適用されます。

（注） ASDM では、多数の ASA バージョンをサポートしています。ASDM のマニュアルおよびオンライン ヘルプには、ASA でサポートされている最新機能がすべて含まれています。古いバージョンの ASA ソフトウェアを実行している場合、ご使用のバージョンでサポートされていない機能がこのマニュアルに含まれている場合があります。同様に、古いメジャー バージョンまたはマイナー バージョンのメンテナンス リリースに機能が追加された場合、この新機能は、以降のすべての ASA リリースで使用できない場合でも、ASDM のマニュアルに含まれています。各章の機能履歴テーブルを参照して、機能がいつ追加されたかを確認してください。各 ASA のバージョンでサポートされている ASDM の最小バージョンについては、『*Cisco ASA Series Compatibility*』を参照してください。

関連資料

詳細については、「*Navigating the Cisco ASA Series Documentation*」（http://www.cisco.com/go/asadocs）を参照してください。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
太字の `courier` フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字の `courier` フォント**で示しています。
イタリック体の `courier` フォント	ユーザが値を指定する引数は、*イタリック体の `courier` フォント*で示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『***What's New in Cisco Product Documentation***』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『***What's New in Cisco Product Documentation***』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

PART 1

ASA の開始

Cisco ASA の概要

リリース：2014 年 7 月 24 日
更新：2014 年 9 月 16 日

Cisco ASA は、高度なステートフル ファイアウォールと VPN コンセントレータの機能を 1 台のデバイスに集約した製品です。モデルによっては、IPS などのサービス モジュールが統合されています。ASA は多数の高度な機能を備えています。たとえば、マルチ セキュリティ コンテキスト（仮想ファイアウォールに類似）、クラスタリング（複数のファイアウォールを結合して 1 つのファイアウォールにする）、トランスペアレント（レイヤ 2）ファイアウォールまたはルーテッド（レイヤ 3）ファイアウォール動作、高度なインスペクション エンジン、IPsec VPN、SSL VPN、クライアントレス SSL VPN のサポートなどがあります。

（注） ASDM では、多数の ASA バージョンをサポートしています。ASDM のマニュアルおよびオンライン ヘルプには、ASA でサポートされている最新機能がすべて含まれています。古いバージョンの ASA ソフトウェアを実行している場合、ご使用のバージョンでサポートされていない機能がこのマニュアルに含まれている場合があります。同様に、古いメジャー バージョンまたはマイナー バージョンのメンテナンス リリースに機能が追加された場合、この新機能は、以降のすべての ASA リリースで使用できない場合でも、ASDM のマニュアルに含まれています。各章の機能履歴テーブルを参照して、機能がいつ追加されたかを確認してください。ASA の各バージョンでサポートされている ASDM の最小バージョンについては、「*Cisco ASA Compatibility*」を参照してください。「非推奨の特殊なレガシー サービス」（P.1-19）も参照してください。

ASDM の要件

ASDM クライアントのオペレーティング システムとブラウザの要件

表 1-1 には、ASDM に対応して推奨されるクライアント オペレーティング システムと Java のリストが表示されています。

表 1-1　オペレーティング システムとブラウザの要件

オペレーティング システム	ブラウザ				Java SE プラグイン
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows（英語および日本語）： • 8 • 7 • Vista • 2008 サーバ • XP	6.0 以降	1.5 以降	サポートなし	18.0 以降	6.0 以降
Apple OS X 10.4 以降	サポートなし	1.5 以降	2.0 以降	18.0 以降	6.0 以降
Red Hat Enterprise Linux 5（GNOME または KDE）： • Desktop • Desktop with Workstation	該当なし	1.5 以降	該当なし	18.0 以降	6.0 以降

Java およびブラウザの互換性

表 1-2 に、Java、ASDM、およびブラウザの互換性に関する警告を示します。

表 1-2　ASDM の互換性に関する警告

Java Version	条件	注意
7 Update 51	ASDM ランチャでは信頼できる証明書が必要	ランチャの使用を継続するには、次のいずれかを実行します。 • ASA に既知の CA から信頼できる証明書をインストールする。 • 自己署名証明書をインストールし、Java に登録する（http://www.cisco.com/go/asdm-certificate を参照）。 • Java を 7 Update 45 以下にダウングレードする。 • または、Java Web Start を使用する。 **（注）** ASDM 7.1(5) 以前は、Java 7 Update 51 ではサポートされていません。すでに Java をアップグレードしてあり、ASDM を起動してバージョン 7.2 にアップグレードすることができない場合でも、CLI を使用して ASDM をアップグレードするか、ASDM で管理する ASA ごとに Java コントロール パネルでセキュリティ例外を追加することができます。次の Web ページの「Workaround」の項を参照してください。 http://java.com/en/download/help/java_blocked.xml セキュリティ例外を追加したら、旧バージョンの ASDM を起動して、7.2 にアップグレードします。
	Java Web Start を使用している場合、まれにオンライン ヘルプがロードされないことがある	まれに、オンライン ヘルプを起動したときに、ブラウザ ウィンドウがロードを行ってもコンテンツが表示されず、ブラウザにエラー「接続不可能」が表示されることがあります。 回避策： • ASDM ランチャを使用します。 または： • Java ランタイム パラメータの **-Djava.net.preferIPv6Addresses=true** パラメータをクリアします。 a. Java コントロール パネルを起動します。 b. [Java] タブをクリックします。 c. [View] をクリックします。 d. **-Djava.net.preferIPv6Addresses=true** パラメータをクリアします。 e. [OK]、[Apply] の順にクリックし、[OK] を再度クリックします。

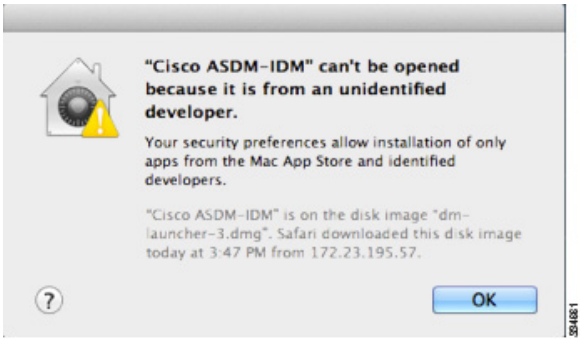
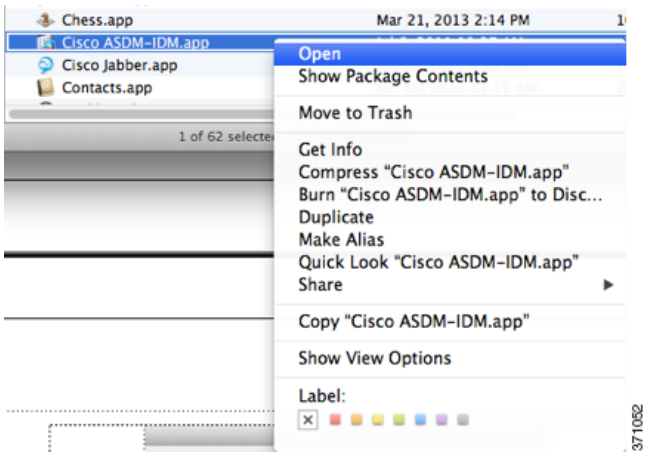
表 1-2　ASDM の互換性に関する警告 （続き）

Java Version	条件	注意
7 Update 45	信頼できない証明書が使用されている場合、ASDM で、不足している権限属性に関する警告が黄色で表示される	Java のバグにより、ASA に信頼できる証明書がインストールされていない場合、JAR マニフェストに不足している権限属性に関する警告が黄色で表示されます。**この警告を無視しても問題ありません**。ASDM 7.2 には権限属性が含まれています。警告が表示されないようにするには、既知の CA から信頼できる証明書をインストールするか、ASA で自己署名証明書を生成します（[Configuration] > [Device Management] > [Certificates] > [Identity Certificates] を選択）。ASDM を起動して、証明書に関する警告が表示されたら、[Always trust connections to websites] チェック ボックスをオンにします。
7	ASA では強力な暗号化ライセンス（3DES/AES）が必要	ASDM では、ASA に SSL 接続する必要があります。ASA に基本的な暗号化ライセンス（DES）しか付与されておらず、その結果、SSL 接続に対する暗号化サイファが脆弱な場合、ASDM を起動できません。また、Java 7 をアンインストールして、Java 6 をインストールする必要があります（http://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase6-419409.html）。暗号化が脆弱な場合、および Java 6 が使用されている場合には、回避策が必要になります（この表の以下を参照）。
6	50 文字を超えるユーザ名を使用できない	Java 6 を使用している場合、Java のバグにより、ASDM で 50 文字を超えるユーザ名を使用することができません。Java 7 では、50 文字を超えるユーザ名を使用できます。
	ASA では強力な暗号化ライセンス（3DES/AES）が必要（*または*、回避策が必要）	最初にブラウザを ASA に接続して ASDM のスプラッシュ画面をロードするとき、ブラウザは ASA に対して SSL 接続を試みます。ASA に基本的な暗号化ライセンス（DES）しか付与されておらず、その結果、SSL 接続に対する暗号化サイファが脆弱な場合、ASDM のスプラッシュ画面を表示できない可能性があります。ほとんどの最新のブラウザは、脆弱な暗号化サイファをサポートしていません。そのため、強力な暗号化ライセンス（3DES/AES）が付与されていない場合は、次のいずれかの回避策を使用します。 • 可能な場合は、ダウンロードしてある ASDM ランチャまたは Java Web Start のショートカットを使用します。ブラウザで Java 6 や脆弱な暗号化がサポートされていなくても、ASDM ランチャおよび Java Web Start のショートカットはこれらとともに使用することができます。 • Windows Internet Explorer の場合は、回避策として DES をイネーブルにすることができます。詳細については、http://support.microsoft.com/kb/929708 を参照してください。 • すべてのオペレーティング システムでの Firefox の場合は、回避策として security.ssl3.dhe_dss_des_sha 設定をイネーブルにすることができます。非表示のコンフィギュレーション プリファレンスを変更する方法については、http://kb.mozillazine.org/About:config を参照してください。

表 1-2　ASDM の互換性に関する警告 （続き）

Java Version	条件	注意
すべて	• 自己署名証明書または信頼できない証明書 • IPv6 • Firefox および Safari	ASA が自己署名証明書または信頼できない証明書を使用する場合、Firefox 4 以降と Safari では、IPv6 を介した HTTPS を使用して参照する場合にはセキュリティ例外を追加することができません。https://bugzilla.mozilla.org/show_bug.cgi?id=633001 を参照してください。この警告は、Firefox または Safari から ASA に発信されるすべての SSL 接続に影響します（ASDM 接続を含む）。この警告を回避するには、信頼できる認証局が ASA に対して発行した適切な証明書を設定します。
	• ASA で SSL 暗号化を行うには、RC4-MD5 と RC4-SHA1 を両方とも含めるか、Chrome で SSL false start をディセーブルにする必要があります。 • Chrome	RC4-MD5 および RC4-SHA1 アルゴリズム（これらのアルゴリズムはデフォルトでイネーブル）の両方を除外するために ASA の SSL 暗号化を変更した場合、Chrome の「SSL false start」機能のために Chrome は ASDM を起動できません。これらのアルゴリズムの 1 つを再度イネーブルにすることを推奨します（[Configuration] > [Device Management] > [Advanced] > [SSL Settings] ペインを参照）。または、http://www.chromium.org/developers/how-tos/run-chromium-with-flags に従って、**--disable-sslfalse-start** フラグを使用して Chrome の SSL false start をディセーブルにすることもできます。
	サーバの IE9	サーバの Internet Explorer 9.0 に対しては、[Do not save encrypted pages to disk] オプションがデフォルトでイネーブルになっています（[Tools] > [Internet Options] > [Advanced] を参照）。このオプションでは、最初の ASDM のダウンロードは失敗します。ASDM でダウンロードを行うには、このオプションを確実にディセーブルにしてください。
	OS X	OS X では、ASDM の初回実行時に、Java のインストールを要求される場合があります。必要に応じて、プロンプトに従います。インストールの完了後に ASDM が起動します。

表 1-2　ASDM の互換性に関する警告 （続き）

Java Version	条件	注意
すべて	OS X 10.8 以降	ASDM は Apple Developer ID で署名されていないため、実行できるようにする必要があります。セキュリティの設定を変更しないと、エラー画面が表示されます。  1. ASDM を実行できるようにするには、[Cisco ASDM-IDM Launcher] アイコンを右クリック（または Ctrl キーを押しながらクリック）して、[Open] を選択します。  2. 同様のエラー画面が表示されますが、この画面から ASDM を起動できます。[Open] をクリックします。ASDM-IDM ランチャが起動します。 

ハードウェアとソフトウェアの互換性

サポートされているハードウェアとソフトウェアの詳細なリストについては、次の Web ページの「*Cisco ASA Compatibility*」を参照してください。

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

VPN の互換性

次の Web ページの「*Supported VPN Platforms, Cisco ASA Series*」を参照してください。

http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html

新機能

- 「ASA 9.3(1)/ASDM 7.3(1) の新機能」（P.1-7）

（注）　追加、変更、および非推奨化された syslog メッセージは、syslog メッセージ ガイドに記載されています。

ASA 9.3(1)/ASDM 7.3(1) の新機能

リリース：2014 年 7 月 24 日

表 1-3 に、ASA バージョン 9.3(1)/ASDM バージョン 7.3(1) の新機能を示します。

表 1-3　ASA バージョン 9.3(1)/ASDM バージョン 7.3(1) の新機能

機能	説明
ファイアウォール機能	
IPv6 に対する SIP、SCCP、および TLS プロキシのサポート	SIP、SCCP、および TLS プロキシ（SIP または SCCP を使用）を使用している場合、IPv6 トラフィックを検査できるようになりました。 変更された ASDM 画面はありません。
Cisco Unified Communications Manager 8.6 のサポート	ASA と Cisco Unified Communications Manager バージョン 8.6 が相互運用されるようになりました（SCCPv21 のサポートを含む）。 変更された ASDM 画面はありません。
アクセス グループおよび NAT に関するルール エンジンのトランザクション コミット モデル	イネーブルの場合、ルールの編集の完了後、ルールの更新が適用されます。ルールの照合パフォーマンスへの影響はありません。 次の画面が導入されました。[Configuration] > [Device Management] > [Advanced] > [Rule Engine]。

表 1-3　ASA バージョン 9.3(1)/ASDM バージョン 7.3(1) の新機能 （続き）

機能	説明
リモート アクセス機能	
クライアントレス SSL VPN に対する XenDesktop 7 のサポート	クライアントレス SSL VPN に対する XenDesktop 7 のサポートが追加されました。自動サインオンを含むブックマークを作成する場合に、ランディング ページの URL またはコントロール ID を指定できるようになりました。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Bookmarks]。
モバイル導入プロキシ	モバイル導入プロキシ（ISE モバイル導入ソリューションのコンポーネント）を使用すると、オフプレミスのモバイル デバイスをオンプレミスのモバイル デバイスとまったく同じ方法で管理できるようになります。 **（注）** モバイル導入プロキシを使用するには、2015 年初めの次回の ISE リリースに含まれる ISE のサポートが必要になります。 次の画面が導入されました。[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [MDM Proxy]。
AnyConnect カスタム属性の強化	カスタム属性では、ASA に組み込まれていない AnyConnect の機能（遅延アップグレードなど）が定義および設定されます。カスタム属性の設定が強化され、複数の値やより大きな値を設定できるようになりました。現在は、カスタム属性のタイプ、名前、および値の指定が必要になっています。また、カスタム属性をダイナミック アクセス ポリシーおよびグループ ポリシーに追加できるようになりました。9.3.x にアップグレードすると、以前に定義したカスタム属性がこの強化された設定フォーマットに更新されます。 次の画面が導入または変更されました。 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Custom Attributes] [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Custom Attribute Names] [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [Advanced] > [AnyConnect Client] > [Custom Attributes] [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] > [Add/Edit] > [AnyConnect Custom Attributes]
デスクトップ プラットフォームの AnyConnect Identity Extension（ACIDex）	ACIDex（AnyConnect エンドポイント属性または Mobile Posture とも呼ばれる）は、AnyConnect VPN クライアントがポスチャ情報を ASA に伝える際に使用する方法です。ダイナミック アクセス ポリシーでは、ユーザの認証にこれらのエンドポイント属性が使用されます。 現在、AnyConnect VPN クライアントには、デスクトップ オペレーティング システム（Windows、Mac OS X、および Linux）のプラットフォーム識別機能が搭載されているほか、DAP で使用可能な MAC アドレス プールが用意されています。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Dynamic Access Policies] > [Add/Edit] > [Add/Edit (endpoint attribute)]。[Endpoint Attribute Type] では [AnyConnect] を選択します。[Platform] ドロップダウン リストにはオペレーティング システムが追加されています。また、[MAC Address] が [Mac Address Pool] に変更されました。

表 1-3　ASA バージョン 9.3(1)/ASDM バージョン 7.3(1) の新機能 （続き）

機能	説明
VPN に対する TrustSec SGT の割り当て	リモート ユーザが接続するときに、TrustSec セキュリティ グループ タグ（SGT）を ASA の SGT-IP テーブルに追加できるようになりました。 次の画面が導入または変更されました。 [Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] > [Edit User] > [VPN Policy] [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add a Policy]
ハイ アベイラビリティ機能	
クラスタリング内のモジュールのヘルス モニタリングに対するサポートの強化	クラスタリング内のモジュールのヘルス モニタリングに対するサポートサポートが強化されました。 変更された ASDM 画面はありません。
ハードウェア モジュールのヘルス モニタリングのディセーブル化	ASA はデフォルトで、設置されているハードウェア モジュール（ASA FirePOWER モジュールなど）のヘルス モニタリングを行います。特定のハードウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、モジュールのモニタリングをディセーブルにできます。 次の画面が変更になりました。[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Interfaces]
プラットフォーム機能	
ASP ロード バランシング	**asp load-balance per-packet** コマンドの新しい **auto** オプションを使用すると、ASA の各インターフェイス受信リングで、ASP ロード バランシングのオン/オフをパケットごとに柔軟に切り替えることができます。この自動メカニズムにより、非対称トラフィックが導入されているかどうかを検出し、次の問題を回避することができます。 • フロー上での突発的なトラフィックの増加によって発生するオーバーラン • 特定のインターフェイス受信リングをオーバーサブスクライブする大量のフローによって発生するオーバーラン • 1 つのコアでは耐えられないような、かなり大きな負荷がかかっているインターフェイス受信リングで発生するオーバーラン 変更された ASDM 画面はありません。
SNMP MIB	CISCO-REMOTE-ACCESS-MONITOR-MIB が ASASM をサポートするようになりました。

表 1-3　ASA バージョン 9.3(1)/ASDM バージョン 7.3(1) の新機能 （続き）

機能	説明
インターフェイス機能	
トランスペアレント モードのブリッジ グループの最大数が 250 に増加	ブリッジ グループの最大数が 8 個から 250 個に増えました。シングル モードでは最大 250 個、マルチ モードではコンテキストあたり最大 250 個のブリッジ グループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを設定できます。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Interfaces] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Bridge Group Interface] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface]
ルーティング機能	
ASA クラスタリングに対する BGP のサポート	ASA クラスタリングに対する BGP のサポートが追加されました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [General]。
ノンストップ フォワーディングに対する BGP のサポート	ノンストップ フォワーディングに対する BGP のサポートが追加されました。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Routing] > [BGP] > [General] [Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [Neighbor] [Monitoring] > [Routing] > [BGP Neighbors]
アドバタイズされたマップに対する BGP のサポート	アドバタイズされたマップに対する BGPv4 のサポートが追加されました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [Neighbor] > [Add BGP Neighbor] > [Routes]。
ノンストップ フォワーディング （NSF） に対する OSPF のサポート	NSF に対する OSPFv2 および OSPFv3 のサポートが追加されました。 次の画面が追加されました。 [Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [NSF Properties] [Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] > [NSF Properties]

表 1-3　ASA バージョン 9.3(1)/ASDM バージョン 7.3(1) の新機能 （続き）

機能	説明
AAA 機能	
レイヤ 2 セキュリティ グループのタグ インポジション	セキュリティ グループ タギングをイーサネット タギングと組み合わせて使用して、ポリシーを適用できるようになりました。SGT とイーサネット タギング（レイヤ 2 SGT インポジションとも呼ばれる）を利用すると、ASA でシスコ独自のイーサネット フレーミング（EtherType 0x8909）を使用して、ギガビット イーサネット インターフェイスでセキュリティ グループ タグを送受信できます。これにより、送信元のセキュリティ グループ タグをプレーン テキストのイーサネット フレームに挿入できます。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Interfaces] > [Add Interface] > [Advanced] [Configuration] > [Device Setup] > [Interfaces] > [Add Redundant Interface] > [Advanced] [Configuration] > [Device Setup] > [Add Ethernet Interface] > [Advanced] [Wizards] > [Packet Capture Wizard] [Tools] > [Packet Tracer]
AAA の Windows NT ドメイン認証の削除	リモート アクセス VPN ユーザに対する NTLM のサポートが削除されました。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups] > [Add AAA Server Group]。
ASDM Identity Certificate Wizard	最新バージョンの Java を使用している場合、ASDM ランチャにおいて信頼できる証明書が必要になります。証明書の要件は、自己署名付きの ID 証明書をインストールすることによって簡単に満たすことができます。[ASDM Identity Certificate Wizard] を使用すると、自己署名付きの ID 証明書を簡単に作成できます。最初に ASDM を起動したときに信頼できる証明書がない場合、Java Web Start を使用して ASDM を起動するよう要求されます。この新しいウィザードは自動的に開始されます。ID 証明書を作成したら、Java コントロール パネルに登録する必要があります。手順については、https://www.cisco.com/go/asdm-certificate を参照してください。 次の画面が追加されました。[Wizards] > [ASDM Identity Certificate Wizard]。
モニタリング機能	
物理インターフェイスの集約トラフィックのモニタリング	**show traffic** コマンドの出力が更新され、物理インターフェイス情報の集約トラフィックが含まれるようになりました。この機能をイネーブルにするには、最初に **sysopt traffic detailed-statistics** コマンドを入力する必要があります。

スイッチにおける ASA サービス モジュールの動作

Cisco IOS ソフトウェアを搭載した Catalyst 6500 シリーズおよび Cisco 7600 シリーズ スイッチで、スイッチのスーパーバイザおよび統合型 MSFC の両方に ASASM をインストールできます。

（注）　Catalyst オペレーティング システム（OS）はサポートされていません。

ASA は独自のオペレーティング システムで動作します。

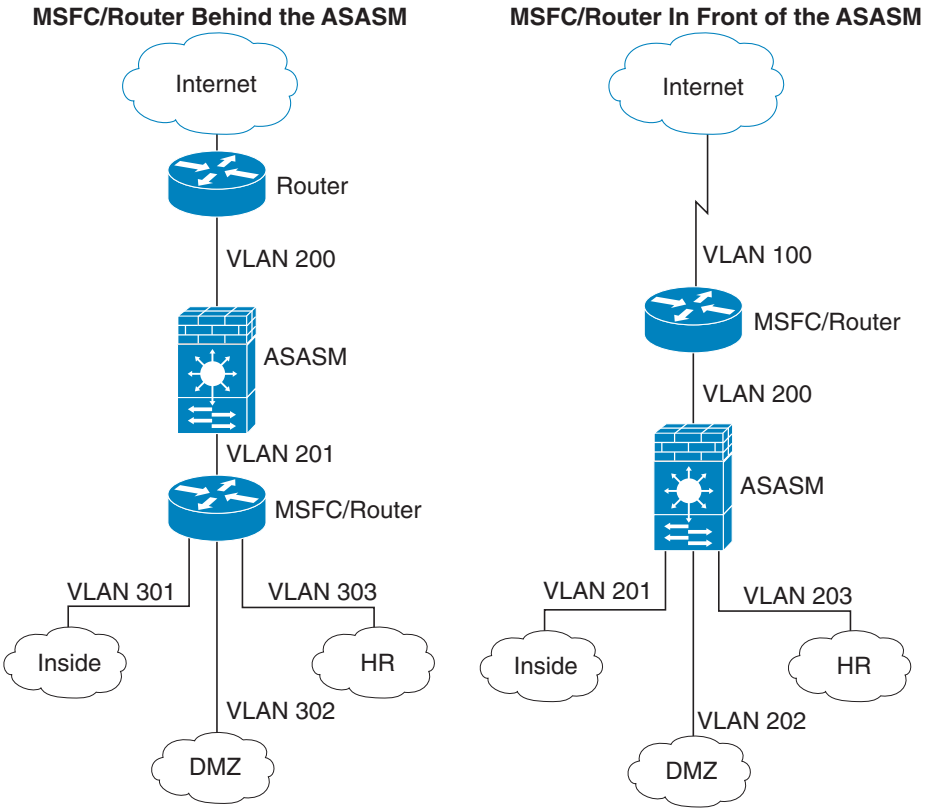
スイッチにはスイッチング プロセッサ（スーパーバイザ）とルータ（MSFC）が組み込まれています。MSFC はシステムの一部として必要ですが、使用しなくてもかまいません。使用することを選択する場合、MSFC に 1 つまたは複数の VLAN インターフェイスを割り当てることができます。MSFC の代わりに外部ルータを使用できます。

シングル コンテキスト モードでは、ファイアウォールの向こう側にルータを配置することも、ファイアウォールより手前に配置することもできます（図 1-1 を参照）。

ルータの位置は、割り当てる VLAN によって決まります。たとえば、図 1-1 の左側の例では、ASASM の内部インターフェイスに VLAN 201 を割り当てているので、ルータはファイアウォールより手前になります。図 1-1 の右側の例では、ASASM の外部インターフェイスに VLAN 200 を割り当てているので、ルータはファイアウォールの向こう側になります。

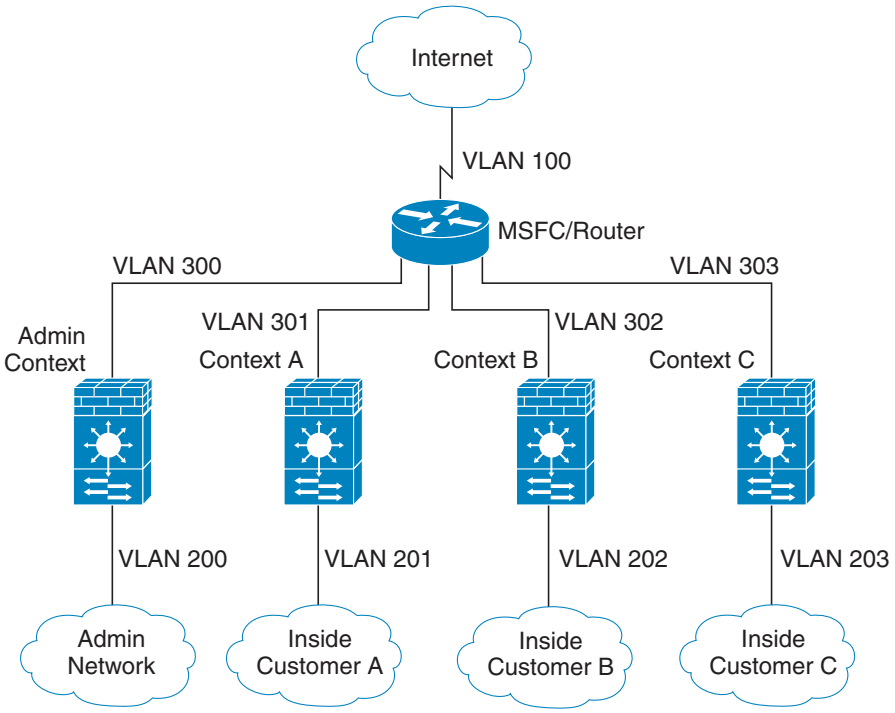
左側の例では、MSFC またはルータは VLAN 201、301、302、および 303 の間をルーティングします。宛先がインターネットの場合以外、内部トラフィックは ASASM を通過しません。右側の例では、ASASM は内部 VLAN 201、202、および 203 間のすべてのトラフィックを処理して保護します。

図 1-1　MSFC/Router の配置



マルチコンテキスト モードでは、ASASM より手前にルータを配置した場合、1 つのコンテキストに限定して接続する必要があります。ルータを複数のコンテキストに接続すると、ルータはコンテキスト間をルーティングすることになり、意図に反する可能性があります。複数のコンテキストの一般的なシナリオでは、インターネットとスイッチド ネットワーク間でルーティングするためにすべてのコンテキストの前にルータを使用します（図 1-2を参照）。

図 1-2　　マルチコンテキストの場合の MSFC/Router の配置



ファイアウォール機能の概要

ファイアウォールは、外部ネットワーク上のユーザによる不正アクセスから内部ネットワークを保護します。また、ファイアウォールは、人事部門ネットワークをユーザ ネットワークから分離するなど、内部ネットワーク同士の保護も行います。Web サーバまたは FTP サーバなど、外部のユーザが使用できるようにする必要のあるネットワーク リソースがあれば、ファイアウォールで保護された別のネットワーク（*非武装地帯*（DMZ）と呼ばれる）上に配置します。ファイアウォールによって DMZ へのアクセスを制限できますが、DMZ には公開サーバしかないため、この地帯が攻撃されても影響を受けるのは公開サーバに限定され、他の内部ネットワークに影響が及ぶことはありません。また、特定アドレスだけに許可する、認証または認可を義務づける、または外部の URL フィルタリング サーバと協調するといった手段によって、内部ユーザが外部ネットワーク（インターネットなど）にアクセスする機会を制御することもできます。

ファイアウォールに接続されているネットワークに言及する場合、*外部*ネットワークはファイアウォールの手前にあるネットワーク、*内部*ネットワークはファイアウォールの背後にある保護されているネットワーク、そして *DMZ* はファイアウォールの背後にあるが、外部ユーザに制限付きのアクセスが許されているネットワークです。ASA を使用すると、数多くのインターフェイスに対してさまざまなセキュリティ ポリシーが設定できます。このインターフェイスに

は、多数の内部インターフェイス、多数の DMZ、および必要に応じて多数の外部インターフェイスが含まれるため、ここでは、このインターフェイスの区分は一般的な意味で使用するだけです。

- 「セキュリティ ポリシーの概要」（P.1-14）
- 「ファイアウォール モードの概要」（P.1-17）
- 「ステートフル インスペクションの概要」（P.1-17）

セキュリティ ポリシーの概要

他のネットワークにアクセスするために、ファイアウォールを通過することが許可されるトラフィックがセキュリティ ポリシーによって決められます。デフォルトでは、内部ネットワーク（高セキュリティ レベル）から外部ネットワーク（低セキュリティ レベル）へのトラフィックは、自由に流れることが ASA によって許可されます。トラフィックにアクションを適用してセキュリティ ポリシーをカスタマイズすることができます。

- 「トラフィックの許可または拒否（アクセス ルールを使用）」（P.1-14）
- 「NAT の適用」（P.1-14）
- 「IP フラグメントからの保護」（P.1-15）
- 「通過トラフィックに対する AAA の使用」（P.1-15）
- 「HTTP、HTTPS、または FTP フィルタリングの適用」（P.1-15）
- 「アプリケーション インスペクションの適用」（P.1-15）
- 「サポート対象のハードウェア モジュールまたはソフトウェア モジュールへのトラフィックの送信」（P.1-15）
- 「QoS ポリシーの適用」（P.1-15）
- 「接続の制限と TCP 正規化の適用」（P.1-16）
- 「脅威検出のイネーブル化」（P.1-16）
- 「ボットネット トラフィック フィルタのイネーブル化」（P.1-16）
- 「Cisco Unified Communications の設定」（P.1-16）

トラフィックの許可または拒否（アクセス ルールを使用）

アクセス ルールは、内部から外部へのトラフィックを制限するため、または外部から内部へのトラフィックを許可するために使用できます。トランスペアレント ファイアウォール モードでは、非 IP トラフィックを許可するための EtherType アクセス リストも適用できます。

NAT の適用

NAT の利点のいくつかを次に示します。

- 内部ネットワークでプライベート アドレスを使用できます。プライベート アドレスは、インターネットにルーティングできません。
- NAT はローカル アドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。
- NAT は、重複 IP アドレスをサポートすることで、IP ルーティングの問題を解決できます。

IP フラグメントからの保護

ASA は IP フラグメント保護を提供します。この機能は、すべての ICMP エラー メッセージの完全リアセンブリ、および ASA を介してルーティングされる残りの IP フラグメントの仮想リアセンブリを実行します。セキュリティ チェックに失敗したフラグメントは、ドロップされログに記録されます。仮想リアセンブリはディセーブルにできません。

通過トラフィックに対する AAA の使用

HTTP など特定のタイプのトラフィックに対して、認証と認可のいずれかまたは両方を要求することができます。ASA は、RADIUS サーバまたは TACACS+ サーバにアカウンティング情報を送信することもあります。

HTTP、HTTPS、または FTP フィルタリングの適用

アクセス リストを使用して、特定の Web サイトまたは FTP サーバへの発信アクセスを禁止できますが、このような方法で Web サイトの使用方法を設定し管理することは、インターネットの規模とダイナミックな特性から、実用的とはいえません。

ASA ではクラウド Web セキュリティを設定できます。または、URL およびその他のフィルタリング サービス（ASA CX や ASA FirePOWER など）を提供する ASA モジュールをインストールすることができます。ASA は、Cisco Web セキュリティ アプライアンス（WSA）などの外部製品とともに使用することも可能です。

アプリケーション インスペクションの適用

インスペクション エンジンは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルは、ASA が詳細なパケット インスペクションを行うことを要求します。

サポート対象のハードウェア モジュールまたはソフトウェア モジュールへのトラフィックの送信

一部の ASA モデルでは、ソフトウェア モジュールの設定、またはハードウェア モジュールのシャーシへの挿入を行うことで、高度なサービスを提供することができます。これらのモジュールを通じてトラフィック インスペクションを追加することにより、設定済みのポリシーに基づいてトラフィックをブロックできます。また、これらのモジュールにトラフィックを送信することで、高度なサービスを利用することができます。

QoS ポリシーの適用

音声やストリーミング ビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。QoS は、この種のトラフィックにプライオリティを設定するネットワーク機能です。QoS とは、選択したネットワーク トラフィックによりよいサービスを提供するネットワークの機能です。

接続の制限と TCP 正規化の適用

TCP 接続、UDP 接続、および初期接続を制限することができます。接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA では、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

TCP 正規化は、正常に見えないパケットをドロップするように設計された高度な TCP 接続設定で構成される機能です。

脅威検出のイネーブル化

スキャン脅威検出と基本脅威検出、さらに統計情報を使用して脅威を分析する方法を設定できます。

基本脅威検出は、DoS 攻撃などの攻撃に関係している可能性のあるアクティビティを検出し、自動的にシステム ログ メッセージを送信します。

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、ASA のスキャンによる脅威の検出機能では、広範なデータベースが保持され、これに含まれるホスト統計情報をスキャン アクティビティに関する分析に使用できます。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定したり、自動的にホストを排除したりできます。

ボットネット トラフィック フィルタのイネーブル化

マルウェアとは、知らないうちにホストにインストールされている悪意のあるソフトウェアです。個人情報（パスワード、クレジット カード番号、キー ストローク、または独自データ）の送信などのネットワーク アクティビティを試みるマルウェアは、マルウェアが既知の不正な IP アドレスへの接続を開始したときにボットネット トラフィック フィルタによって検出できます。ボットネット トラフィック フィルタは、着信と発信の接続を既知の不正なドメイン名と IP アドレス（ブラックリスト）のダイナミック データベースと照合して確認し、不審なアクティビティのログを記録します。マルウェア アクティビティに関する syslog メッセージを確認すると、ホストを切り離して感染を解決するための手順を実行できます。

Cisco Unified Communications の設定

Cisco ASA シリーズは、統合された通信構成にプロキシの機能を提供する戦略的なプラットフォームです。プロキシの目的は、クライアントとサーバ間の接続を終端し、再発信することです。プロキシは、トラフィック インスペクション、プロトコルとの適合性、ポリシー制御など幅広いセキュリティ機能を提供し、内部ネットワークのセキュリティを保証します。プロキシの機能として広く普及しているのが、暗号化された接続を終端して、接続の機密性を維持しながらセキュリティ ポリシーを適用する機能です。

ファイアウォール モードの概要

ASA は、次の 2 つのファイアウォール モードで動作します。

- ルーテッド
- トランスペアレント

ルーテッド モードでは、ASA は、ネットワークのルータ ホップと見なされます。

トランスペアレント モードでは、ASA は「Bump In The Wire」または「ステルス ファイアウォール」のように動作し、ルータ ホップとは見なされません。ASA では、内部インターフェイスと外部インターフェイスに同じネットワークが接続されます。

トランスペアレント ファイアウォールは、ネットワーク コンフィギュレーションを簡単にするために使用できます。トランスペアレント モードは、攻撃者からファイアウォールが見えないようにする場合にも有効です。トランスペアレント ファイアウォールは、他の場合にはルーテッド モードでブロックされるトラフィックにも使用できます。たとえば、トランスペアレント ファイアウォールでは、EtherType アクセス リストを使用するマルチキャスト ストリームが許可されます。

ステートフル インスペクションの概要

ASAを通過するトラフィックはすべて、アダプティブ セキュリティ アルゴリズムを使用して検査され、通過が許可されるか、またはドロップされます。単純なパケット フィルタは、送信元アドレス、宛先アドレス、およびポートが正しいかどうかはチェックできますが、パケット シーケンスまたはフラグが正しいかどうかはチェックしません。また、フィルタは*すべて*のパケットをフィルタと照合してチェックするため、処理が低速になる場合があります。

（注） TCP ステート バイパス機能を使用すると、パケット フローをカスタマイズできます。

ただし、ASA のようなステートフル ファイアウォールは、パケットの次のようなステートについて検討します。

- 新規の接続かどうか。

  新規の接続の場合、ASA は、パケットをアクセス リストと照合してチェックする必要があり、これ以外の各種のタスクを実行してパケットの許可または拒否を決定する必要があります。このチェックを行うために、セッションの最初のパケットは「セッション管理パス」を通過しますが、トラフィックのタイプに応じて、「コントロール プレーン パス」も通過する場合があります。

  セッション管理パスで行われるタスクは次のとおりです。

  - アクセス リストとの照合チェック
  - ルート ルックアップ
  - NAT 変換（xlates）の割り当て
  - 「ファスト パス」でのセッションの確立

  ASA は、TCP トラフィックのファスト パスに転送フローとリバース フローを作成します。ASA は、高速パスも使用できるように、UDP、ICMP（ICMP インスペクションがイネーブルの場合）などのコネクションレス型プロトコルの接続状態の情報も作成するので、これらのプロトコルもファスト パスを使用できます。

（注）　SCTP などの他の IP プロトコルの場合、ASA はリバース パス フローを作成しません。そのため、これらの接続を参照する ICMP エラー パケットはドロップされます。

レイヤ 7 インスペクションが必要なパケット（パケットのペイロードの検査または変更が必要）は、コントロール プレーン パスに渡されます。レイヤ 7 インスペクション エンジンは、2 つ以上のチャネルを持つプロトコルで必要です。2 つ以上のチャネルの 1 つは周知のポート番号を使用するデータ チャネルで、その他はセッションごとに異なるポート番号を使用するコントロール チャネルです。このようなプロトコルには、FTP、H.323、および SNMP があります。

- 確立済みの接続かどうか。

  接続がすでに確立されている場合は、ASA でパケットの再チェックを行う必要はありません。一致するパケットの大部分は、両方向でファスト パスを通過できます。高速パスで行われるタスクは次のとおりです。

  – IP チェックサム検証
  – セッション ルックアップ
  – TCP シーケンス番号のチェック
  – 既存セッションに基づく NAT 変換
  – レイヤ 3 ヘッダー調整およびレイヤ 4 ヘッダー調整

  レイヤ 7 インスペクションを必要とするプロトコルに合致するデータ パケットも高速パスを通過できます。

  確立済みセッション パケットの中には、セッション管理パスまたはコントロール プレーン パスを引き続き通過しなければならないものがあります。セッション管理パスを通過するパケットには、インスペクションまたはコンテンツ フィルタリングを必要とする HTTP パケットが含まれます。コントロール プレーン パスを通過するパケットには、レイヤ 7 インスペクションを必要とするプロトコルのコントロール パケットが含まれます。

VPN 機能の概要

VPN は、TCP/IP ネットワーク（インターネットなど）上のセキュアな接続で、プライベートな接続として表示されます。このセキュアな接続はトンネルと呼ばれます。ASA は、トンネリング プロトコルを使用して、セキュリティ パラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを通したパケットの送信または受信、パケットのカプセル化の解除を行います。ASA は、双方向のトンネル エンドポイントとして機能します。たとえば、プレーン パケットを受信してカプセル化し、それをトンネルのもう一方の側に送信することができます。そのエンドポイントで、パケットはカプセル化が解除され、最終的な宛先に送信されます。また、セキュリティ アプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

ASA が実行する機能は次のとおりです。

- トンネルの確立
- トンネル パラメータのネゴシエーション
- ユーザの認証
- ユーザ アドレスの割り当て
- データの暗号化と復号化

- セキュリティ キーの管理
- トンネルを通したデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信データと発信データの転送の管理

ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

セキュリティ コンテキストの概要

1 台の ASA を、セキュリティ コンテキストと呼ばれる複数の仮想デバイスに分割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、さまざまな機能がサポートされています。ただし、サポートされていない機能もあります。詳細については、機能に関する各章を参照してください。

マルチ コンテキスト モードの場合、ASA 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。システム管理者がコンテキストを追加および管理するには、コンテキストをシステム コンフィギュレーションに設定します。これが、シングルモード設定と同じく、スタートアップ コンフィギュレーションとなります。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

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。ただし、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。

ASA クラスタリングの概要

ASA クラスタリングを利用すると、複数の ASA をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、マスター ユニット上でのみ実行します。コンフィギュレーションは、メンバ ユニットに複製されます。

非推奨の特殊なレガシー サービス

一部のサービスのマニュアルは、主要な設定ガイドおよびオンライン ヘルプとは別の場所にあります。ガイドの詳細なリストについては、次の Web ページを参照してください。

http://www.cisco.com/go/asadocs

- 「特殊なサービスに関するガイド」（P.1-20）
- 「非推奨のサービス」（P.1-20）
- 「レガシー サービス ガイド」（P.1-20）

特殊なサービスに関するガイド

特殊なサービスを利用して、たとえば、電話サービス（Unified Communications）用のセキュリティ プロキシを提供したり、ボットネット トラフィック フィルタリングを Cisco アップデート サーバのダイナミック データベースと組み合わせて提供したり、Cisco Web セキュリティ アプライアンス用の WCCP サービスを提供したりすることにより、ASA と他のシスコ製品の相互運用が可能になります。これらの特殊なサービスの一部について、別のガイドで説明します。

非推奨のサービス

非推奨の機能については、ASA バージョンの設定ガイドを参照してください。同様に、設計の見直しが行われた機能（NAT（バージョン 8.2 と 8.3 の間に見直しを実施）、トランスペアレント モードのインターフェイス（バージョン 8.3 と 8.4 の間に見直しを実施）など）については、各バージョンの設定ガイドを参照してください。ASDM は以前の ASA リリースとの後方互換性を備えていますが、設定ガイドおよびオンライン ヘルプでは最新のリリースの内容しか説明されていません。

レガシー サービス ガイド

レガシー サービスは現在も ASA でサポートされていますが、より高度なサービスを代わりに使用できる場合があります。レガシー サービスについては別のガイドで説明されています。

使用する前に

この章では、Cisco ASA の使用を開始する方法について説明します。

コマンドライン インターフェイスのコンソールへのアクセス

ASDM アクセスの基本的な設定を、CLI を使用して行う必要がある場合があります。

初期設定を行うには、コンソール ポートから直接 CLI にアクセスします。その後は、第 36 章「管理アクセス」の方法によって Telnet または SSH を使用してリモート アクセスを設定できます。システムがすでにマルチ コンテキスト モードで動作している場合は、コンソール ポートにアクセスするとシステムの実行スペースに入ります。

（注） ASAv のコンソール アクセスについては、ASAv のクイック スタート ガイドを参照してください。

アプライアンス コンソールへのアクセス

アプライアンス コンソールにアクセスするには、次の手順に従います。

手順

ステップ 1　付属のコンソール ケーブルを使用して PC をコンソール ポートに接続します。ターミナル エミュレータを回線速度 9600 ボー、データ ビット 8、パリティなし、ストップ ビット 1、フロー制御なしに設定して、コンソールに接続します。

コンソール ケーブルの詳細については、ご使用の ASA のハードウェア ガイドを参照してください。

ステップ 2　**Enter** キーを押して、次のプロンプトが表示されることを確認します。

ciscoasa>

このプロンプトは、ユーザ EXEC モードで作業していることを示します。ユーザ EXEC モードでは、基本コマンドのみを使用できます。

ステップ 3　特権 EXEC モードにアクセスするには、次のコマンドを入力します。

```
ciscoasa> enable
```

次のプロンプトが表示されます。

```
Password:
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

ステップ 4　プロンプトに対して、イネーブル パスワードを入力します。

デフォルトではパスワードは空白に設定されているため、**Enter** キーを押して先に進みます。イネーブル パスワードを変更するには、「ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定」（P.14-1）を参照してください。

プロンプトが次のように変化します。

```
ciscoasa#
```

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 5　グローバル コンフィギュレーション モードにアクセスするには、次のコマンドを入力します。

```
ciscoasa# configure terminal
```

プロンプトが次のように変化します。

```
ciscoasa(config)#
```

グローバル コンフィギュレーション モードから ASA の設定を開始できます。グローバル コンフィギュレーション モードを終了するには、**exit** コマンド、**quit** コマンド、または **end** コマンドを入力します。

ASA サービス モジュール コンソールへのアクセス

初期設定の場合、スイッチに（コンソール ポートに、あるいは Telnet または SSH を使用してリモートで）接続してコマンドライン インターフェイスにアクセスし、ASASM に接続します。ASASM には工場出荷時のデフォルト コンフィギュレーションが含まれていないため、ASDM を使用してアクセスする前に CLI での設定の実行が必要です。ここでは、ASASM CLI にアクセスする方法について説明します。

接続方法について

スイッチ CLI から、ASASM に接続するには、次の 2 つの方法が使用できます。

- 仮想コンソール接続：**service-module session** コマンドを使用して、ASASM への仮想コンソール接続を作成します。仮想コンソール接続は、実際のコンソール接続の利点と制限をすべて備えています。

  利点を次に示します。

  - 接続はリロード中も持続し、タイムアウトしません。
  - ASASM リロード中も接続を維持でき、スタートアップ メッセージが表示されます。
  - ASASM がイメージをロードできない場合、ROMMON にアクセスできます。
  - 初期パスワードの設定は必要ではありません。

  制限を次に示します。

  - 接続が低速です（9600 ボー）。
  - 一度にアクティブにできるコンソール接続は 1 つだけです。
  - このコマンドは、**Ctrl+Shift+6**、x がターミナル サーバ プロンプトに戻るためのエスケープ シーケンスであるターミナル サーバとともに使用することはできません。**Ctrl+Shift+6**、x は、ASASM コンソールをエスケープして、スイッチ プロンプトに戻るためのシーケンスでもあります。したがって、この状況で、ASASM コンソールを終了しようとすると、ターミナル サーバ プロンプトまで終了することになります。スイッチにターミナル サーバを再接続した場合、ASASM コンソール セッションがアクティブのままです。スイッチ プロンプトを終了することはできません。コンソールをスイッチ プロンプトに戻すには、直接シリアル接続を使用する必要があります。この場合、Cisco IOS でターミナル サーバまたはスイッチ エスケープ文字を変更するか、または Telnet **session** コマンドを使用します。

  （注） コンソール接続の永続性のため、ASASM を正しくログ アウトしないと、意図よりも長く接続が存在する可能性があります。他の人がログインする場合は、既存の接続を終了する必要があります。

- Telnet 接続：**session** コマンドを使用して、ASASM への Telnet 接続を作成します。

（注）　新しい ASASM に対してはこの方式を使用して接続できません。この方式では、ASASM 上での Telnet ログイン パスワードの設定が必要です（デフォルトのパスワードはありません）。**passwd** コマンドを使用してパスワードを設定した後に、この方式を使用できます。

利点を次に示します。

- ASASM への複数のセッションを同時に使用できます。
- Telnet セッションは、高速接続です。

制限を次に示します。

- Telnet セッションは、ASASM リロード時に終了し、タイムアウトします。
- 完全にロードするまで ASASM にアクセスできません。したがって、ROMMON にアクセスできません。
- 最初に Telnet ログイン パスワードを設定する必要があります。デフォルトのパスワードはありません。

ASA サービス モジュールへのログイン

初期設定の場合、スイッチに（スイッチのコンソール ポートに、あるいは Telnet または SSH を使用してリモートで）接続してコマンドライン インターフェイスにアクセスし、ASASM に接続します。

システムがすでにマルチ コンテキスト モードで動作している場合は、スイッチ環境から ASASM にアクセスするとシステムの実行スペースに入ります。

その後は、Telnet または SSH を使用してリモート アクセスを ASASM に直接設定できます。

手順

ステップ 1　スイッチから、次のいずれかを実行します。

- 最初のアクセスで使用可能：スイッチ CLI からこのコマンドを入力し、ASASM にコンソール アクセスします。

  service-module session [**switch** {**1** | **2**}] **slot** *number*

  例：

  ```
  Router# service-module session slot 3
  ciscoasa>
  ```

  VSS 内のスイッチの場合、**switch** 引数を入力します。

  モジュールのスロット番号を表示するには、スイッチ プロンプトで **show module** コマンドを入力します。

  ユーザ EXEC モードにアクセスします。

- ログイン パスワードの設定後に使用可能：スイッチ CLI からこのコマンドを入力し、バックプレーンを介して ASASM に Telnet 接続します。

  session [**switch** {**1** |**2**}] **slot** *number* **processor 1**

  ログイン パスワードの入力が求められます。

  ```
  ciscoasa passwd:
  ```

例：

```
Router# session slot 3 processor 1
ciscoasa passwd: cisco
ciscoasa>
```

VSS 内のスイッチの場合、**switch** 引数を入力します。

session *slot* **processor 0** コマンドは、他のサービス モジュールではサポートされていますが、ASASM ではサポートされていません。ASASM にはプロセッサ 0 がありません。

モジュールのスロット番号を表示するには、スイッチ プロンプトで **show module** コマンドを入力します。

ASASM へのログイン パスワードを入力します。**passwd** コマンドを使用してパスワードを設定します。デフォルトのパスワードはありません。

ユーザ EXEC モードにアクセスします。

ステップ 2　最高の特権レベルである特権 EXEC モードにアクセスします。

enable

例：

```
ciscoasa> enable
Password:
ciscoasa#
```

プロンプトに対して、イネーブル パスワードを入力します。デフォルトでは、パスワードは空白です。

特権 EXEC モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 3　グローバル コンフィギュレーション モードにアクセスします。

configure terminal

グローバル コンフィギュレーション モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

関連項目

- 「ASDM、Telnet、または SSH の ASA アクセスの設定」（P.36-1）
- 「ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定」（P.14-1）

コンソール セッションのログアウト

ASASM からログアウトしない場合、コンソール接続は維持され、タイムアウトはありません。ASASM コンソール セッションを終了してスイッチの CLI にアクセスするには、次の手順を実行します。

意図せずに開いたままになっている可能性のある、別のユーザのアクティブな接続を終了するには、「アクティブなコンソール接続の終了」（P.2-6）を参照してください。

手順

ステップ 1　スイッチ CLI に戻るには、次を入力します。

Ctrl+Shift+6、x

スイッチ プロンプトに戻ります。

```
asasm# [Ctrl-Shift-6, x]
Router#
```

（注）　米国および英国キーボードの Shift+6 はキャレット記号（^）を出力します。別のキーボードを使用しており、単独の文字としてキャレット記号（^）を出力できない場合、一時的または永続的に、エスケープ文字を別の文字に変更できます。**terminal escape-character** *ascii_number* コマンド（このセッションで変更する）、または **default escape-character** *ascii_number* コマンド（永続的に変更する）を使用します。たとえば、現在のセッションのシーケンスを **Ctrl+w**、**x** に変更するには、**terminal escape-character 23** を入力します。

アクティブなコンソール接続の終了

コンソール接続の永続性のため、ASASM を正しくログ アウトしないと、意図よりも長く接続が存在する可能性があります。他の人がログインする場合は、既存の接続を終了する必要があります。

手順

ステップ 1　スイッチ CLI から、**show users** コマンドを使用して、接続されたユーザを表示します。コンソール ユーザは「con」と呼ばれます。ホスト アドレスは、127.0.0.*slot*0 と表示されます（*slot* はモジュールのスロット番号です）。

```
Router# show users
```

たとえば、次のコマンド出力は、スロット 2 にあるモジュールのライン 0 のユーザ「con」を示しています。

```
Router# show users
Line       User       Host(s)              Idle       Location
*  0       con 0     127.0.0.20            00:00:02
```

ステップ 2　コンソール接続のあるラインをクリアするには、次のコマンドを入力します。

```
Router# clear line number
```

次に例を示します。

```
Router# clear line 0
```

Telnet セッションのログアウト

Telnet セッションを終了してスイッチ CLI にアクセスするには、次の手順を実行します。

手順

ステップ 1　スイッチ CLI に戻るには、ASASM 特権モードまたはユーザ EXEC モードから **exit** を入力します。コンフィギュレーション モードに入っている場合は、Telnet セッションが終了するまで繰り返し **exit** を入力します。

スイッチ プロンプトに戻ります。

```
asasm# exit
Router#
```

（注）　代わりに、エスケープ シーケンス **Ctrl+Shift+6**、x を使用して、Telnet セッションをエスケープすることができます。このエスケープ シーケンスを使用すると、スイッチ プロンプトで **Enter** キーを押すことで、Telnet セッションを再開できます。スイッチから Telnet セッションを切断するには、スイッチ CLI で **disconnect** を入力します。セッションを切断しない場合、ASASM 設定に従って、最終的にタイムアウトします。

ASDM アクセスの設定

ここでは、デフォルト コンフィギュレーションで ASDM にアクセスする方法、およびデフォルト設定がない場合にアクセスを設定する方法について説明します。

- 「ASDM アクセス（アプライアンス、ASAv）に対する工場出荷時のデフォルト コンフィギュレーションの使用」（P.2-7）
- 「アプライアンスおよび ASAv の ASDM アクセスのカスタマイズ」（P.2-8）
- 「ASA サービス モジュールの ASDM アクセスの設定」（P.2-10）

ASDM アクセス（アプライアンス、ASAv）に対する工場出荷時のデフォルト コンフィギュレーションの使用

工場出荷時のデフォルト コンフィギュレーションを使用する場合、ASDM 接続はデフォルトのネットワーク設定で事前設定されています。

手順

ステップ 1　次のインターフェイスおよびネットワーク設定を使用して ASDM に接続します。

- 管理インターフェイスは、ご使用のモデルによって異なります。
  - ASA 5512-X 以降：ASDM に接続するインターフェイスは Management 0/0 です。
  - ASAv：ASDM に接続するインターフェイスは Management 0/0 です。
- デフォルトの管理アドレスは次のとおりです。
  - ASA アプライアンス：192.168.1.1。
  - ASAv：導入時に管理インターフェイスの IP アドレスを設定します。

- ASDM にアクセスできるクライアントは次のとおりです。
  - ASA アプライアンス：クライアントは 192.168.1.0/24 ネットワーク上にある必要があります。デフォルト コンフィギュレーションにより DHCP がイネーブルにされるため、管理ステーションにはこの範囲内の IP アドレスを割り当てることができます。
  - ASAv：導入時に管理クライアントの IP アドレスを設定します。ASAv は、接続されたクライアントに対して DHCP サーバとして機能しません。

（注）　マルチ コンテキスト モードに変更すると、上記のネットワーク設定を使用して管理コンテキストから ASDM にアクセスできるようになります。

関連項目

- 「工場出荷時のデフォルト設定」（P.2-15）
- 「マルチ コンテキスト モードのイネーブル化とディセーブル化」（P.7-16）
- 「ASDM の起動」（P.2-12）

アプライアンスおよび ASAv の ASDM アクセスのカスタマイズ

次の条件に *1 つ以上*当てはまる場合は、この手順を使用します。

- 工場出荷時のデフォルト コンフィギュレーションがない。
- トランスペアレント ファイアウォール モードに変更したい。
- マルチ コンテキスト モードに変更したい。

シングル ルーテッド モードの場合、ASDM に迅速かつ容易にアクセスするために、独自の管理 IP アドレスを設定できるオプションを備えた工場出荷時のデフォルト コンフィギュレーションを適用することを推奨します。この項に記載されている手順は、特別なニーズ（トランスペアレント モードやマルチ コンテキスト モードの設定など）がある場合や、他の設定を維持する必要がある場合にのみ使用してください。

手順

ステップ 1　コンソール ポートで CLI にアクセスします。

ステップ 2　（オプション）トランスペアレント ファイアウォール モードをイネーブルにします。

このコマンドは、設定をクリアします。

```
firewall transparent
```

ステップ 3　管理インターフェイスを設定します。

```
interface management id
   nameif name
   security-level level
   no shutdown
   ip address ip_address mask
```

例：

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
```

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

security-level は、1 ～ 100 の数字です。100 が最も安全です。

ステップ 4　（直接接続された管理ホスト用）管理ネットワークの DHCP プールを設定します。

dhcpd address *ip_address-ip_address interface_name*
dhcpd enable *interface_name*

例：

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

この範囲内には管理アドレスを含めないでください。

ステップ 5　（リモート管理ホスト用）管理ホストへのルートを設定します。

route *management_ifc management_host_ip mask gateway_ip* **1**

例：

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

ステップ 6　ASDM の HTTP サーバをイネーブルにします。

http server enable

ステップ 7　管理ホストの ASDM へのアクセスを許可します。

http *ip_address mask interface_name*

例：

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

ステップ 8　設定を保存します。

write memory

ステップ 9　（オプション）モードをマルチ モードに設定します。

mode multiple

プロンプトが表示されたら、既存の設定を管理コンテキストに変換することを承認します。ASA をリロードするよう求められます。

例

次の設定では、ファイアウォール モードがトランスペアレント モードに変換され、Management 0/0 インターフェイスが設定され、管理ホストに対して ASDM がイネーブルにされます。

```
firewall transparent
interface management 0/0
    ip address 192.168.1.1 255.255.255.0
    nameif management
    security-level 100
    no shutdown
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

関連項目

- 「工場出荷時のデフォルト コンフィギュレーションの復元」（P.2-16）
- 「ファイアウォール モード（シングル モード）の設定」（P.5-10）
- 「アプライアンス コンソールへのアクセス」（P.2-2）
- 「ASDM の起動」（P.2-12）
- 第 7 章「マルチ コンテキスト モード」

ASA サービス モジュールの ASDM アクセスの設定

ASASM には物理インターフェイスがないため、ASDM アクセス用に事前設定されていません。ASASM の CLI を使用して ASDM アクセスを設定する必要があります。ASDM アクセス用に ASASM を設定するには、次の手順を実行します。

はじめる前に

ASASM のクイック スタート ガイドに従って、ASASM に VLAN インターフェイスを割り当てます。

手順

ステップ 1　ASASM に接続し、グローバル コンフィギュレーション モードにアクセスします。

ステップ 2　（オプション）トランスペアレント ファイアウォール モードをイネーブルにします。

```
firewall transparent
```

このコマンドは、設定をクリアします。

ステップ 3　ご使用のモードに応じて、次のいずれかの操作を行って管理インターフェイスを設定します。

- ルーテッド モード：インターフェイスをルーテッド モードで設定します。

```
interface vlan number
   ip address ip_address [mask]
   nameif name
   security-level level
```

例：

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

security-level は、1 ～ 100 の数字です。100 が最も安全です。

- トランスペアレント モード：ブリッジ仮想インターフェイスを設定し、ブリッジ グループに管理 VLAN を割り当てます。

```
interface bvi number
   ip address ip_address [mask]

interface vlan number
   bridge-group bvi_number
   nameif name
   security-level level
```

例：

```
ciscoasa(config)# interface bvi 1
```

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0

ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# bridge-group 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

security-level は、1 ～ 100 の数字です。100 が最も安全です。

ステップ 4　（直接接続された管理ホスト用）管理インターフェイス ネットワーク上の管理ホストの DHCP をイネーブルにします。

dhcpd address *ip_address*-*ip_address interface_name*
dhcpd enable *interface_name*

例：

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 inside
ciscoasa(config)# dhcpd enable inside
```

この範囲内には管理アドレスを含めないでください。

ステップ 5　（リモート管理ホスト用）管理ホストへのルートを設定します。

route *management_ifc management_host_ip mask gateway_ip* **1**

例：

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50
```

ステップ 6　ASDM の HTTP サーバをイネーブルにします。

http server enable

ステップ 7　管理ホストの ASDM へのアクセスを許可します。

http *ip_address mask interface_name*

例：

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

ステップ 8　設定を保存します。

write memory

ステップ 9　（オプション）モードをマルチ モードに設定します。

mode multiple

プロンプトが表示されたら、既存の設定を管理コンテキストに変換することを承認します。ASASM をリロードするよう求められます。

例

次のルーテッド モードの設定では、VLAN 1 のインターフェイスを設定し、管理ホストの ASDM のイネーブルにします。

```
interface vlan 1
    nameif inside
    ip address 192.168.1.1 255.255.255.0
```

```
    security-level 100
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

次の設定では、ファイアウォール モードをトランスペアレント モードに変換し、VLAN 1 インターフェイスを設定してから、BVI 1 に割り当て、管理ホストの ASDM をイネーブルにします。

```
firewall transparent
interface bvi 1
    ip address 192.168.1.1 255.255.255.0
interface vlan 1
    bridge-group 1
    nameif inside
    security-level 100
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

関連項目

- 「ASA サービス モジュール コンソールへのアクセス」（P.2-3）
- 第 7 章「マルチ コンテキスト モード」
- 「ファイアウォール モード（シングル モード）の設定」（P.5-10）

ASDM の起動

ASDM は、次の 2 つの方法で起動できます。

- ASDM-IDM ランチャ：ランチャは、ASA から Web ブラウザを使用してダウンロードされるアプリケーションです。これを使用すると、任意の ASA IP アドレスに接続できます。他の ASA に接続する場合に、ランチャを再度ダウンロードする必要はありません。またランチャでは、ローカルでダウンロードされたファイルを使用して、仮想 ASDM をデモ モードで実行することもできます。
- Java Web Start：管理する ASA ごとに、Web ブラウザに接続して、Java Web Start アプリケーションを保存または起動する必要があります。任意で PC にショートカットを保存できます。ただし、ASA IP アドレスごとにショートカットを分ける必要があります。

ASDM では、管理のために別の ASA IP アドレスを選択できます。ランチャと Java Web Start の機能の違いは、主に、ユーザが最初にどのように ASA に接続し、ASDM を起動するかにあります。

ASDM では複数の PC やワークステーションでそれぞれブラウザ セッションを開き、同じ ASA ソフトウェアを使用できます。1 つの ASA で、シングル ルーテッド モードの ASDM 並行セッションを 5 つまでサポートできます。PC またはワークステーションはそれぞれ、指定した ASA のセッションを 1 つだけブラウザで実行できます。マルチ コンテキスト モードの場合、コンテキストあたり 5 つの ASDM 並行セッションを実行でき、ASA あたり合計 32 セッションまで接続できます。

ここでは、まず ASDM に接続する方法について説明します。次にランチャまたは Java Web Start を使用して ASDM を起動する方法について説明します。

手順

ステップ 1　ASDM クライアントとして指定した PC で次の URL を入力します。

https://*asa_ip_address***/admin**

次のボタンを持つ ASDM 起動ページが表示されます。

- [Install ASDM Launcher and Run ASDM]
- [Run ASDM]
- [Run Startup Wizard]

ステップ 2　ランチャをダウンロードするには、次の手順を実行します。

a. [Install ASDM Launcher and Run ASDM] をクリックします。

b. ユーザ名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。HTTPS 認証が設定されていない場合は、ユーザ名および**イネーブル** パスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。注：HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。

c. インストーラを PC に保存して、インストーラを起動します。インストールが完了すると、ASDM-IDM ランチャが自動的に開きます。

d. 管理 IP アドレスを入力し、ユーザ名とパスワードを空白のままにし（新規インストールの場合）、[OK] をクリックします。注：HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。

ステップ 3　Java Web Start を使用するには：

a. [Run ASDM] または [Run Startup Wizard] をクリックします。

b. プロンプトが表示されたら、ショートカットを PC に保存します。オプションで、アプリケーションを保存せずに開くこともできます。

c. ショートカットから Java Web Start を起動します。

d. 表示されたダイアログボックスに従って、任意の証明書を受け入れます。Cisco ASDM-IDM Launcher が表示されます。

e. ユーザ名とパスワードを空白のままにし（新規インストールの場合）、[OK] をクリックします。注：HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。

ASDM の ID 証明書のインストール

Java 7 Update 51 以降を使用する場合、ASDM ランチャには信頼できる証明書が必要です。証明書の要件は、自己署名付きの ID 証明書をインストールすることによって簡単に満たすことができます。証明書をインストールするまで、Java Web Start を使用して ASDM を起動することができます。

ASDM で使用するために ASA に自己署名された ID 証明書をインストールし、Java を使用して証明書を登録するには、次のマニュアルを参照してください。

http://www.cisco.com/go/asdm-certificate

デモ モードでの ASDM の使用

アプリケーション ASDM Demo Mode を別途インストールして使用すると、実デバイスを使用せずに ASDM を実行できます。このモードでは、次の操作を実行できます。

- 実デバイス接続時と同じように、ASDM から設定と選択した監視タスクを実行する。
- ASDM インターフェイスによる ASDM または ASA 機能のデモを実行する。
- CSC SSM を使用して設定および監視タスクを実行する。
- リアルタイムの syslog メッセージを含む、シミュレーションしたモニタリング データやロギング データを取得する。表示データはランダムに生成されますが、実デバイスに接続しているような体験ができます。

このモードは、次の機能をサポートするようにアップデートされています。

- グローバル ポリシーに対し、シングル ルーテッド モードの ASA および侵入防御。
- オブジェクト NAT に対し、シングル ルーテッド モードの ASA およびファイアウォール DMZ。
- ボットネット トラフィック フィルタに対し、シングル ルーテッド モードの ASA およびセキュリティ コンテキスト。
- IPv6 を使用するサイトツーサイト VPN（クライアントレス SSL VPN および IPsec VPN）
- 無差別 IDS（侵入防御）
- Unified Communication Wizard

このモードでは、次の機能はサポートされません。

- GUI に表示されたコンフィギュレーションに加えた変更内容の保存
- ファイルまたはディスクの操作
- 履歴モニタリングデータ
- 非管理ユーザ
- 次の機能
  - [File] メニュー

    [Save Running Configuration to Flash]

    [Save Running Configuration to TFTP Server]

    [Save Running Configuration to Standby Unit]

    [Save Internal Log Buffer to Flash]

    [Clear Internal Log Buffer]
  - [Tools] メニュー

    [Command Line Interface]

    [Ping]

    [File Management]

    [Update Software]

    [File Transfer]

    [Upload Image from Local PC]

    [System Reload]

  - ツールバー /ステータスバー > [Save]
  - [Configuration] > [Interface] > [Edit Interface] > [Renew DHCP Lease]
  - フェールオーバー後のスタンバイ デバイスの設定
- コンフィギュレーションの再読み込みが発生する操作。再読み込みが行われると GUI が元のコンフィギュレーションに戻ります。
  - コンテキストの切り換え
  - [Interface] ペインの変更
  - [NAT] ペインの変更
  - [Clock] ペインの変更

ASDM をデモ モードで実行するには、次の手順を実行します。

手順

ステップ 1　ASDM Demo Mode インストーラの asdm-demo-*version*.msi を、次の場所からダウンロードします。http://www.cisco.com/cisco/web/download/index.html

ステップ 2　インストーラをダブルクリックして、ソフトウェアをインストールします。

ステップ 3　デスクトップ上の **Cisco ASDM Launcher** のショートカットをダブルクリックするか、または、[スタート] メニューから開きます。

ステップ 4　[Run in Demo Mode] チェックボックスをオンにします。

[Demo Mode] ウィンドウが表示されます。

工場出荷時のデフォルト設定

出荷時のデフォルトのコンフィギュレーションは、シスコが新しい ASA に適用しているコンフィギュレーションです。

- ASA アプライアンス：工場出荷時のデフォルト コンフィギュレーションによって管理用のインターフェイスが設定されるため、ASDM を使用してこのインターフェイスに接続し、設定を完了できます。
- ASAv：導入の一環として、導入設定（初期の仮想導入設定）によって管理用のインターフェイスが設定されるため、ASDM を使用してこのインターフェイスに接続し、設定を完了できます。フェールオーバー IP アドレスも設定できます。また、必要に応じて、「工場出荷時のデフォルト」コンフィギュレーションを適用することもできます。
- ASASM：デフォルト コンフィギュレーションはありません。コンフィギュレーションを開始するには、「ASA サービス モジュール コンソールへのアクセス」（P.2-3）を参照してください。

工場出荷時のデフォルト コンフィギュレーションは、ルーテッド ファイアウォール モードとシングル コンテキスト モードだけで使用できます。

（注）　イメージ ファイルと（隠された）デフォルト コンフィギュレーションに加え、log/、crypto_archive/、および coredumpinfo/coredump.cfg がフラッシュ メモリ内の標準のフォルダとファイルです。フラッシュ メモリ内で、これらのファイルの日付は、イメージ ファイルの日付と一致しない場合があります。これらのファイルは、トラブルシューティングに役立ちますが、障害が発生したことを示すわけではありません。

工場出荷時のデフォルト コンフィギュレーションの復元

この項では、工場出荷時のデフォルト コンフィギュレーションを復元する方法について説明します。CLI および ASDM の両方の手順が提供されています。ASAv では、この手順を実行することで導入設定が消去され、ASA アプライアンスの場合と同じ工場出荷時のデフォルト コンフィギュレーションが適用されます。

（注）ASASM で出荷時のデフォルト コンフィギュレーションを復元すると、設定は消去されます。工場出荷時のデフォルト コンフィギュレーションはありません。

はじめる前に

この機能は、ルーテッド ファイアウォール モードでのみ使用できます。トランスペアレント モードの場合、インターフェイスの IP アドレスがサポートされません。さらに、この機能はシングル コンテキスト モードでのみ使用できます。コンフィギュレーションがクリアされた ASA には、この機能を使用して自動的に設定する定義済みのコンテキストがありません。

手順

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[File] > [Reset Device to the Factory Default Configuration] の順に選択します。

[Reset Device to the Default Configuration] ダイアログボックスが表示されます。

ステップ 2　（オプション）デフォルト アドレス 192.168.1.1 を使用する代わりに、管理インターフェイスの [Management IP address] を入力します。

ステップ 3　（オプション）ドロップダウン リストから [Management Subnet Mask] を選択します。

ステップ 4　[OK] をクリックします。

確認用のダイアログボックスが表示されます。

（注）この操作により、ブート イメージが存在する場合はその場所も、他の設定とともにクリアされます。[Configuration] > [Device Management] > [System Image/Configuration] > [Boot Image/Configuration] ペインでは、外部メモリ上のイメージを含む、特定のイメージからブートできます。出荷時の設定に戻した後、次回 ASA をリロードすると、内部フラッシュ メモリの最初のイメージからブートします。*内部*フラッシュ メモリにイメージがない場合、ASA はブートしません。

ステップ 5　[Yes] をクリックします。

ステップ 6　デフォルト設定を復元したら、この設定を内部フラッシュ メモリに保存します。[File] > [Save Running Configuration to Flash] を選択します。

このオプションを選択すると、以前に別の場所を設定している場合でも、実行コンフィギュレーションがスタートアップ コンフィギュレーションのデフォルトの場所に保存されます。コンフィギュレーションをクリアした場合は、このパスもクリアされています。

ASAv 導入設定の復元

この項では、ASAv の導入設定を復元する方法について説明します。

手順

ステップ 1　フェールオーバーを行うために、スタンバイ装置の電源を切ります。

スタンバイ装置がアクティブになることを防止するために、電源を切る必要があります。電源を入れたままにした場合、アクティブ装置の設定を消去すると、スタンバイ装置がアクティブになります。以前アクティブであった装置がリロードされ、フェールオーバー リンクを介して再接続されると、古い設定は新しいアクティブ装置から同期され、必要な導入設定が消去されます。

ステップ 2　リロード後に導入設定を復元します。フェールオーバーを行うために、アクティブ装置で次のコマンドを入力します。

```
write erase
```

（注）　ASAv が現在の実行イメージをブートするため、元のブート イメージには戻りません。元のブート イメージを使用するには、**boot image** コマンドを参照してください。

コンフィギュレーションは保存しないでください。

ステップ 3　ASAv をリロードし、導入設定をロードします。

```
reload
```

ステップ 4　フェールオーバーを行うために、スタンバイ装置の電源を投入します。

アクティブ装置のリロード後、スタンバイ装置の電源を投入します。導入設定がスタンバイ装置と同期されます。

ASA アプライアンスのデフォルト コンフィギュレーション

ASA アプライアンスの工場出荷時のデフォルト コンフィギュレーションは、次のように設定されています。

  - 管理インターフェイス：Management 0/0（管理）。
- IP アドレス：管理アドレスは 192.168.1.1/24 です。
- DHCP サーバ：管理ホストでは DHCP サーバがイネーブルにされているため、管理インターフェイスに接続する PC には、192.168.1.2 ～ 192.168.1.254 の間のアドレスが割り当てられます。
- ASDM アクセス：管理ホストに許可されます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface management 0/0
```

```
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

ASAv の導入設定

ASAv を導入すると、ASDM を使用して、Management 0/0 インターフェイスへの接続を可能にする多数のパラメータをプリセットできます。一般的な構成には次の設定があります。

- Management 0/0 インターフェイス：
  - 名前は「management」
  - IP アドレスまたは DHCP
  - セキュリティ レベル 0
  - 管理専用
- デフォルト ゲートウェイを介した管理インターフェイスから管理ホスト IP アドレスへのスタティック ルート
- ASDM サーバの有効化
- 管理ホスト IP アドレス用の ASDM アクセス
- （オプション）GigabitEthernet 0/8 用のフェールオーバー リンク IP アドレス、Management0/0 のスタンバイ IP アドレス。

スタンドアロン ユニットについては、次の設定を参照してください。

```
interface Management0/0
 nameif management
 security-level 0
 ip address ip_address
 management-only
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
```

フェールオーバー ペアのプライマリ ユニットについては、次の設定を参照してください。

```
interface Management0/0
 nameif management
 security-level 0
 ip address ip_address standby standby_ip
 management-only
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
フェールオーバー
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip
```

設定の開始

ASA を設定およびモニタするには、次の手順を実行します。

ステップ 1　Startup Wizard を使用して初期設定を行うには、[Wizards] > [Startup Wizard] を選択します。

ステップ 2　IPsec VPN Wizard を使用して IPsec VPN 接続を設定するには、[Wizards] > [IPsec VPN Wizard] を選択して、表示される各画面で設定を行います。

ステップ 3　SSL VPN Wizard を使用して SSL VPN 接続を設定するには、[Wizards] > [SSL VPN Wizard] を選択して、表示される各画面で設定を行います。

ステップ 4　高可用性とスケーラビリティに関する設定値を設定するには、[Wizards] > [High Availability and Scalability Wizard] を選択します。

ステップ 5　Packet Capture Wizard を使用してパケット キャプチャを設定するには、[Wizards] > [Packet Capture Wizard] を選択します。

ステップ 6　ASDM GUI で使用できるさまざまな色とスタイルを表示するには、[View] > [Office Look and Feel] を選択します。

ステップ 7　機能を設定するには、ツールバーの [Configuration] ボタンをクリックし、いずれかの機能ボタンをクリックして、関連する設定ペインを表示します。

（注）　[Configuration] 画面が空白の場合は、ツールバーで [Refresh] をクリックして、画面のコンテンツを表示します。

ステップ 8　ASA をモニタするには、ツールバーの [Monitoring] ボタンをクリックし、機能ボタンをクリックして、関連するモニタリング ペインを表示します。

（注）　ASDM では、最大 512 KB の設定をサポートしています。このサイズを超えると、パフォーマンスの問題が生じることがあります。

ASDM でのコマンドライン インターフェイス ツールの使用

この項では、ASDM を使用してコマンドを入力する方法および CLI の使用方法について説明します。

- 「コマンドライン インターフェイス ツールの使用」（P.2-20）
- 「ASDM によって無視されるコマンドのデバイス上での表示」（P.2-21）

コマンドライン インターフェイス ツールの使用

この機能には、コマンドを ASA に送信して結果を表示する、テキストベースのツールが用意されています。

CLI ツールによって入力可能なコマンドは、ユーザ権限によって異なります。メイン ASDM アプリケーション ウィンドウの下部にあるステータスバーの権限レベルを見て、CLI 特権コマンドを実行するために必要な特権があるかどうかを確認してください。

はじめる前に

- ASDM の CLI ツールから入力したコマンドは、ASA の接続ターミナルから入力したコマンドと異なる動作をする場合があります。
- コマンド エラー：誤った入力コマンドによってエラーが発生した場合、その誤ったコマンドはスキップされ、その他のコマンドは処理されます。[Response] 領域には、他の関連情報とともに、エラーが発生したかどうかについての情報を示すメッセージが表示されます。
- インタラクティブ コマンド：インタラクティブ コマンドは、CLI ツールではサポートされていません。これらのコマンドを ASDM で使用するには、次のコマンドに示すように、**noconfirm** キーワード（使用できる場合）を使用します。

  ```
  crypto key generate rsa modulus 1024 noconfirm
  ```

- 他の管理者との競合を回避：複数の管理ユーザが ASA の実行コンフィギュレーションをアップデートできます。ASDM の CLI ツールでコンフィギュレーションを変更する場合は、アクティブな管理セッションが他にないことを事前に確認してください。複数のユーザが同時に ASA を設定する場合は、最新の変更が有効になります。

  同じ ASA で現在アクティブな他の管理セッションを表示するには、[Monitoring] > [Properties] > [Device Access] の順に選択します。

手順

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Command Line Interface] の順に選択します。

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

ステップ 2　必要なコマンドのタイプ（1 行または複数行）を選択し、ドロップダウン リストからコマンドを選択するか、または表示されたフィールドにコマンドを入力します。

ステップ 3　[Send] をクリックしてコマンドを実行します。

ステップ 4　新しいコマンドを入力するには、[Clear Response] をクリックしてから、実行する別のコマンドを選択（または入力）します。

ステップ 5　この機能の状況依存ヘルプを表示するには、[Enable context-sensitive help (?)] チェックボックスをオンにします。文脈依存ヘルプをディセーブルにするには、このチェックボックスをオフにします。

ステップ 6　設定を変更した場合は、[Command Line Interface] ダイアログボックスを閉じた後に、[Refresh] をクリックして ASDM での変更内容を表示します。

ASDM によって無視されるコマンドのデバイス上での表示

この機能により、ASDM がサポートしていないコマンドの一覧を表示できます。通常 ASDM は、これらのコマンドを無視します。ASDM は、ユーザの実行コンフィギュレーションのコマンドを変更、削除することはありません。詳細については、「サポートされていないコマンド」（P.3-35）を参照してください。

手順

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Show Commands Ignored by ASDM on Device] の順に選択します。

ステップ 2　完了したら、[OK] をクリックします。

ASDM コンフィギュレーション メモリの増大

ASDM でサポートされる最大設定サイズは 512 KB です。このサイズを超えると、パフォーマンスの問題が生じることがあります。たとえば、コンフィギュレーションのロード時には、完了したコンフィギュレーションの割合がステータス ダイアログボックスに表示されます。このとき、サイズの大きいコンフィギュレーションでは、ASDM によってまだコンフィギュレーションの処理が行われていても、完了した割合の増分が停止し、操作が中断されているように見えます。このような状況が発生した場合は、ASDM システム ヒープ メモリの増大を検討することを推奨します。

ASDM ヒープ メモリ サイズを増大するには、次の手順を実行してランチャのショートカットを変更します。

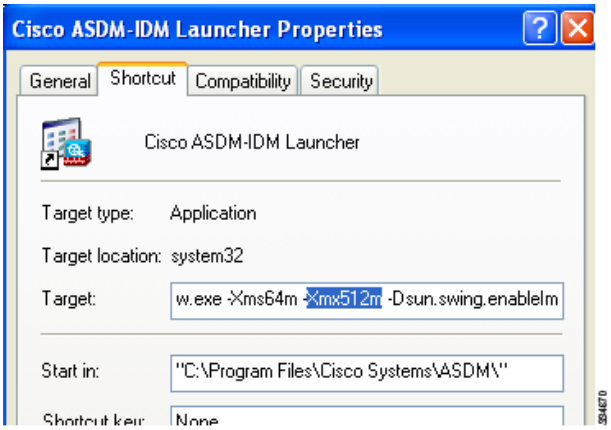
手順

ステップ 1　Windows の場合：

a. ASDM-IDM ランチャのショートカットを右クリックし、[Properties] を選択します。

b. [Shortcut] タブをクリックします。

c. [Target] フィールドで、「-Xmx」のプレフィックスが付いた引数を変更し、必要なヒープ サイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。



ステップ 2　Macintosh の場合：

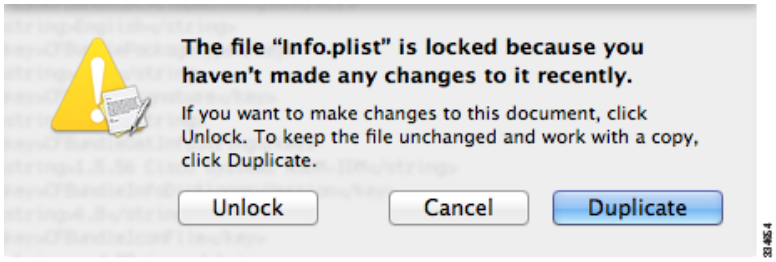
a. [Cisco ASDM-IDM] アイコンを右クリックし、[Show Package Contents] を選択します。

b. [Contents] フォルダで、**Info.plist** ファイルをダブルクリックします。開発者ツールをインストールしている場合は、**プロパティ リスト エディタ**で開きます。そうでない場合は、**TextEdit** で開きます。

c. [Java] > [VMOptions] で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープ サイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```
<key>Java</key>
<dict>
        <key>WorkingDirectory</key>
        <string>$APP_PACKAGE/Contents/Resources/Java</string>
        <key>VMOptions</key>
        <string>-Xms64mm -Xmx512mm</string>
        <key>MainClass</key>
        <string>com.cisco.launcher.Launcher</string>
        <key>JVMVersion</key>
        <string>1.5+</string>
```

d. このファイルがロックされると、次のようなエラーが表示されます。



e. [Unlock] をクリックし、ファイルを保存します。

[Unlock] ダイアログボックスが表示されない場合は、エディタを終了します。[Cisco ASDM-IDM] アイコンを右クリックし、[Copy Cisco ASDM-IDM] を選択して、書き込み権限がある場所（デスクトップなど）に貼り付けます。その後、このコピーからヒープ サイズを変更します。

接続に対するコンフィギュレーションの変更の適用

コンフィギュレーションに対してセキュリティ ポリシーの変更を加えた場合は、すべての*新しい*接続で新しいセキュリティ ポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。古い接続に対する **show** コマンドの出力は古いコンフィギュレーションを反映しており、場合によっては古い接続に関するデータが含まれないことがあります。

たとえば、インターフェイスから QoS **service-policy** を削除し、修正バージョンを再度追加する場合、**show service-policy** コマンドには、新しいサービス ポリシーと一致する新規接続と関連付けられている QoS カウンタのみ表示されます。古いポリシーの既存の接続はコマンド出力には表示されません。

すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。

接続を解除するには、次のいずれかのコマンドを入力します。

- **clear local-host** [*ip_address*] [**all**]

  このコマンドは、接続制限値や初期接続の制限など、クライアントごとのランタイム ステートを再初期化します。これにより、このコマンドは、これらの制限を使用しているすべての接続を削除します。現在のすべての接続をホスト別に表示するには、**show local-host all** コマンドを参照してください。

  引数を指定しないと、このコマンドは、影響を受けるすべての through-the-box 接続をクリアします。to-the-box 接続もクリアするには（現在の管理セッションを含む）、**all** キーワードを使用します。特定の IP アドレスへの、または特定の IP アドレスからの接続をクリアするには、*ip_address* 引数を使用します。

- **clear conn** [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]] [**port** *src_port*[**-***src_port*]] [**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[**-***dest_port*]]

  このコマンドは、すべての状態の接続を終了します。現在のすべての接続を表示するには、**show conn** コマンドを参照してください。

  引数を指定しないと、このコマンドはすべての through-the-box 接続をクリアします。to-the-box 接続もクリアするには（現在の管理セッションを含む）、**all** キーワードを使用します。送信元 IP アドレス、宛先 IP アドレス、ポート、プロトコルに基づいて特定の接続をクリアするには、必要なオプションを指定できます。

ASDM グラフィカル ユーザ インターフェイス

この章では、ASDM ユーザ インターフェイスの使用方法について説明します。

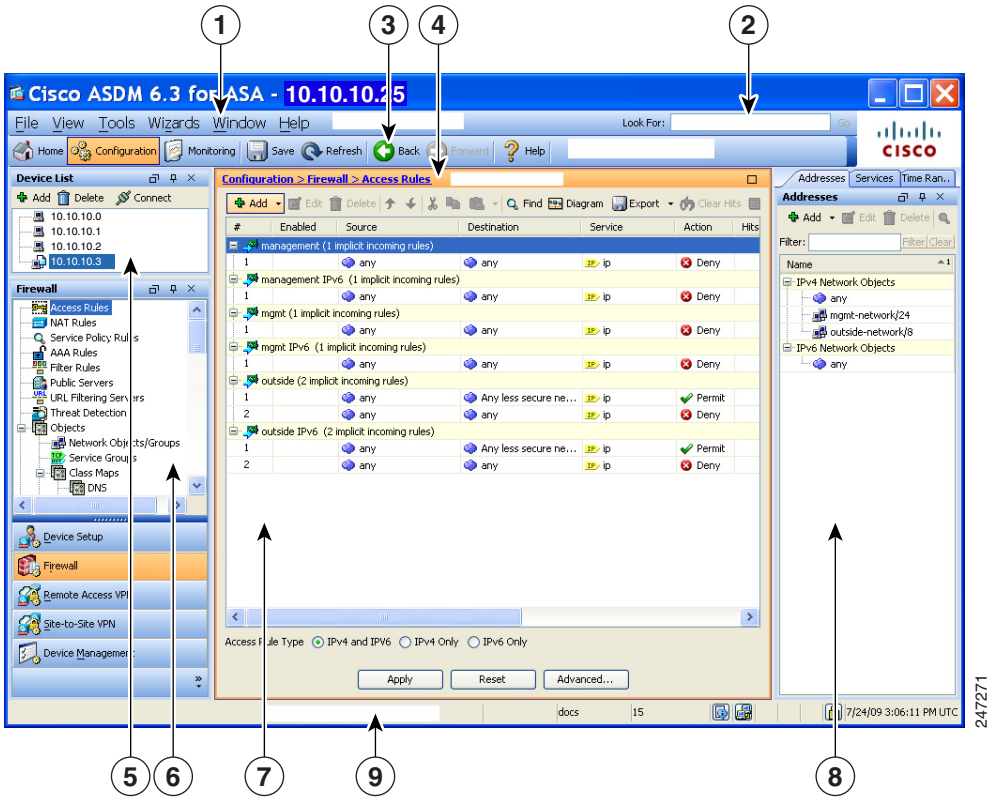
ASDM ユーザ インターフェイスについて

ASDM ユーザ インターフェイスは、ASA がサポートしているさまざまな機能に簡単にアクセスできるように設計されています。ASDM ユーザ インターフェイスには次の要素があります。

- ファイル、ツール、ウィザード、およびヘルプにすぐにアクセスできるメニューバー。メニュー項目の多くにはキーボード ショートカットもあります。
- ASDM のナビゲートをイネーブルにするツールバー。ツールバーから [Home] ペイン、[Configuration] ペイン、および [Monitoring] ペインにアクセスできます。また、ヘルプの参照やペイン間のナビゲーションもできます。
- ドッキング可能な左側の [Navigation] ペイン。[Configuration] ペインや [Monitoring] ペイン内の移動に使用します。ヘッダーにある 3 つのボタンをそれぞれクリックすると、ペインの最大化または復元、移動可能なフローティング ペインへの変更、ペインの非表示化、またはペインを閉じることができます。[Configuration] ペインおよび [Monitoring] ペインにアクセスするには、次のいずれかを実行します。
  - アプリケーション ウィンドウの左端にある左側の [Navigation] ペインのリンクをクリックします。選択した [Content] ペインのタイトルバーにパスが表示されます（[Configuration] > [Device Setup] > [Startup Wizard] など）。
  - 正確なパスがわかっている場合、左側の [Navigation] ペインでリンクをクリックしなくても、アプリケーション ウィンドウの右側にある [Content] ペインのタイトルバーに直接入力できます。
- [Content] ペインの右隅にある最大化および元のサイズに戻すボタン。左側の [Navigation] ペインの非表示や表示を行います。
- ドッキング可能な [Device List] ペイン。ASDM からアクセスできるデバイスのリストを表示します。ヘッダーにある 3 つのボタンをそれぞれクリックすると、ペインの最大化または復元、移動可能なフローティング ペインへの変更、ペインの非表示化、またはペインを閉じることができます。
- ステータス バー。時間、接続ステータス、ユーザ、メモリ ステータス、実行コンフィギュレーション ステータス、権限レベル、および SSL ステータスをアプリケーション ウィンドウの下部に表示します。
- 左側の [Navigation] ペイン。アクセス ルール、NAT ルール、AAA ルール、フィルタ ルール、およびサービス ルールの作成時にルール テーブルで使用できるさまざまなオブジェクトを表示します。ペイン内のタブ タイトルは、表示している機能に応じて変わります。また、このペインには **ASDM Assistant** が表示されます。

図 3-1（P.3-3）に、ASDM ユーザ インターフェイスの要素を示します。

図 3-1　　ASDM ユーザ インターフェイス



凡例

GUI 要素	説明
1	メニュー バー
2	検索フィールド
3	ツールバー
4	ナビゲーション パス
5	[Device List] ペイン
6	左側の [Navigation] ペイン
7	[Content] ペイン
8	右側の [Navigation] ペイン
9	ステータス バー

（注） ツール ヒントが、[Wizards] 、[Configuration] ペイン、[Monitoring] ペイン、**ステータス バー**を含む、GUI のさまざまな部分に追加されています。ツール ヒントを表示するには、マウスをステータスバーにあるアイコンなど、特定のユーザ インターフェイス要素の上に置きます。

ASDM ユーザ インターフェイスのナビゲーション

ASDM ユーザ インターフェイスを効率的に移動するために、前の項で説明したメニュー、ツールバー、ドッキング可能ペイン、および左側と右側の [Navigation] ペインを組み合わせて使用できます。使用できる機能は、[Device List] ペインの下のボタン リストに表示されます。たとえば、リストには次の機能ボタンが含まれます。

- [Device Setup]
- [Firewall]
- [Trend Micro Content Security]
- [Botnet Traffic Filter]
- [Remote Access VPN]
- [Site to Site VPN]
- [Device Management]

表示される機能ボタンのリストは、購入したライセンス機能に基づいて表示されます。コンフィギュレーション ビューまたはモニタリング ビューの選択した機能の最初のペインにアクセスするには、それぞれのボタンをクリックします。ホーム ビューでは、機能ボタンは使用できません。

機能ボタンの表示を変える場合は、次の手順を実行します。

ステップ 1　最後の機能ボタンの下にあるドロップダウン リスト ボタンを選択して、コンテキスト メニューを表示します。

ステップ 2　次のいずれかのオプションを選択します。

- 表示するボタンを増やすには、[Show More Buttons] をクリックします。
- 表示するボタンを減らすには、[Show Fewer Buttons] をクリックします。
- ボタンを追加または削除するには、[Add or Remove Buttons] をクリックし、表示されたリストから追加または削除するボタンをクリックします。
- [Option] を選択すると [Option] ダイアログボックスが表示され、ボタンのリストが現在の順序で表示されます。次のいずれかを選択します。
  - リスト内のボタンを上に移動するには、[Move Up] をクリックします。
  - リスト内のボタンを下に移動するには、[Move Down] をクリックします。
  - リスト内の項目の順序をデフォルト設定に戻すには、[Reset] をクリックします。

ステップ 3　[OK] をクリックして設定を保存し、ダイアログボックスを閉じます。

メニュー

ASDM の各メニューには、マウスまたはキーボードを使用してアクセスできます。キーボードを使用したメニュー バーへのアクセスの詳細については、「キーボード ショートカット」（P.3-13）を参照してください。

ASDM には次のメニューがあります。

- 「[File] メニュー」（P.3-5）
- 「[View] メニュー」（P.3-6）

- 「[Tools] メニュー」（P.3-7）
- 「[Wizards] メニュー」（P.3-8）
- 「[Window] メニュー」（P.3-9）
- 「[Help] メニュー」（P.3-9）

[File] メニュー

[File] メニューでは、ASA のコンフィギュレーションを管理できます。次の表に、[File] メニューを使用して実行できるタスクを示します。

[File] メニュー項目	説明
[Refresh ASDM with the Running Configuration on the Device]	実行コンフィギュレーションのコピーを ASDM にロードします。
[Refresh]	ASDM に実行コンフィギュレーションの最新のコピーが含まれるようにします。
[Reset Device to the Factory Default Configuration]	コンフィギュレーションを工場出荷時のデフォルトに復元します。
[Show Running Configuration in New Window]	現在の実行コンフィギュレーションを新しいウィンドウに表示します。
[Save Running Configuration to Flash]	実行コンフィギュレーションのコピーをフラッシュ メモリに書き込みます。
[Save Running Configuration to TFTP Server]	現在の実行コンフィギュレーション ファイルのコピーを TFTP サーバに保存します。
[Save Running Configuration to Standby Unit]	プライマリ装置の実行コンフィギュレーション ファイルのコピーを、フェールオーバー スタンバイ装置の実行コンフィギュレーションに送信します。
[Save Internal Log Buffer to Flash]	内部ログ バッファをフラッシュ メモリに保存します。
[Print]	現在のページを印刷します。ルールを印刷する場合、ページを横方向にすることをお勧めします。Internet Explorer の場合は、署名付きアプレットを最初に承認した時点で印刷権限が与えられています。
[Clear ASDM Cache]	ローカル ASDM イメージを削除します。ASDM に接続すると、ASDM によりイメージがローカルにダウンロードされます。
[Clear ASDM Password Cache]	新しいパスワードを定義した後に、それとは異なる既存のパスワードがまだ残っている場合は、パスワード キャッシュを削除します。
[Clear Internal Log Buffer]	syslog メッセージ バッファを空にします。
[Exit]	ASDM を閉じます。

[View] メニュー

[View] メニューでは、ASDM ユーザ インターフェイスのさまざまな部分を表示できます。現在のビューに応じた特定の項目が表示されます。現在のビューに表示できない項目は選択できません。次の表に、[View] メニューを使用して実行できるタスクを示します。

[View] メニュー項目	説明
[Home]	ホーム ビューを表示します。
[Configuration]	コンフィギュレーション ビューを表示します。
[Monitoring]	モニタリング ビューを表示します。
[Device List]	ドッキング可能なペインにデバイスのリストを表示します。詳細については、「[Device List]」（P.3-12）を参照してください。
[Navigation]	コンフィギュレーション ビューおよびモニタリング ビューで [Navigation] ペインを表示または非表示にします。
[ASDM Assistant]	タスクに応じた ASDM の使用方法のヘルプを検索し、見つけます。詳細については、「ASDM Assistant」（P.3-11）を参照してください。
[SIP Details]	音声ネットワーク情報を表示または非表示にします。
[Latest ASDM Syslog Messages]	ホーム ビューで [Latest ASDM Syslog Messages] ペインを表示または非表示にします。このペインは、ホーム ビューでのみ使用できます。最新のリリースにアップグレードするためのメモリが不足している場合は、syslog メッセージ %ASA-1-211004 が生成され、インストールされているメモリ、および必要なメモリが示されます。このメッセージは、メモリがアップグレードされるまで、24 時間ごとに再表示されます。
[Addresses]	[Addresses] ペインを表示または非表示にします。[Addresses] ペインは、コンフィギュレーション ビューの [Access Rules]、[NAT Rules]、[Service Policy Rules]、[AAA Rules]、および [Filter Rules] ペインでのみ使用できます。
[Services]	[Services] ペインを表示または非表示にします。[Services] ペインは、コンフィギュレーション ビューの [Access Rules]、[NAT Rules]、[Service Policy Rules]、[AAA Rules]、および [Filter Rules] ペインでのみ使用できます。
[Time Ranges]	[Time Ranges] ペインを表示または非表示にします。[Time Ranges] ペインは、コンフィギュレーション ビューの [Access Rules]、[Service Policy Rules]、[AAA Rules]、および [Filter Rules] ペインでのみ使用できます。
[Global Pools]	[Global Pools] ペインを表示または非表示にします。[Global Pools] ペインは、コンフィギュレーション ビューの [NAT Rules] ペインでのみ使用できます。
[Find in ASDM]	機能や **ASDM Assistant** などの項目を検索します。
[Back]	前のペインに戻ります。詳細については、「共通ボタン」（P.3-13）を参照してください。

[View] メニュー項目	説明
[Forward]	以前に表示した次のペインに移動します。詳細については、「共通ボタン」（P.3-13）を参照してください。
[Reset Layout]	レイアウトをデフォルトのコンフィギュレーションに戻します。
[Office Look and Feel]	画面のフォントと色を Microsoft Office 設定に変更します。

[Tools] メニュー

[Tools] メニューには ASDM で使用する次の一連のツールがあります。

[Tools] メニュー項目	説明
[Command Line Interface]	コマンドを ASA に送信して結果を表示します。
[Show Commands Ignored by ASDM on Device]	ASDM で無視された、サポート対象外のコマンドを表示します。
[Packet Tracer]	指定した送信元アドレスとインターフェイスから宛先まで、パケットをトレースします。プロトコルおよびポートをデータ タイプに関わりなく指定でき、そこで実行された処理の詳細データを含むパケットの一部始終を表示できます。詳細については、ファイアウォール コンフィギュレーション ガイドを参照してください。
[Ping]	ASA および関係する通信リンクのコンフィギュレーションや動作を検証し、他のネットワーク デバイスの基本的なテストを実行します。詳細については、ファイアウォール コンフィギュレーション ガイドを参照してください。
[Traceroute]	パケットが宛先に到着するまでのルートを判断します。詳細については、ファイアウォール コンフィギュレーション ガイドを参照してください。
[File Management]	フラッシュ メモリに保存されたファイルを表示、移動、コピー、および削除します。また、フラッシュ メモリにディレクトリを作成することもできます。また、TFTP、フラッシュ メモリ、ローカル PC などさまざまなファイル システム間でファイル転送ができます。
[Upgrade Software from Local Computer]	ASA イメージ、ASDM イメージ、またはユーザ PC の他のイメージをフラッシュ メモリにアップロードします。
[Check for ASA/ASDM Updates]	ウィザードを使用して ASA ソフトウェアおよび ASDM ソフトウェアをアップグレードします。
[Backup Configurations]	ASA のコンフィギュレーション、Cisco Secure Desktop イメージ、および SSL VPN Client イメージおよびプロファイルをバックアップします。
[Restore Configurations]	ASA のコンフィギュレーション、Cisco Secure Desktop イメージ、および SSL VPN Client イメージおよびプロファイルを復元します。
[System Reload]	ASDM を再起動し、保存したコンフィギュレーションをメモリにリロードします。

[Tools] メニュー項目	説明
[Administrator's Alerts to Clientless SSL VPN Users]	管理者が、クライアントレス SSL VPN ユーザにアラートメッセージを送信できるようにします。詳細については、VPN コンフィギュレーション ガイドを参照してください。
[Migrate Network Object Group Members]	8.3 以降に移行する場合、ASA は名前付きネットワーク オブジェクトを作成して、一部の機能のインライン IP アドレスを置き換えます。名前付きオブジェクトに加えて、ASDM はコンフィギュレーションで使用されているすべての IP アドレスに対して名前なしオブジェクトを自動的に作成します。これらの自動作成されるオブジェクトは *IP アドレス*によってのみ識別され、名前がなく、プラットフォーム設定に名前付きオブジェクトとしては存在しません。 移行の一部として名前付きオブジェクトを ASA が作成する場合、合致する非名前付き ASDM 専用オブジェクトは、名前付きオブジェクトに置換されます。唯一の例外は、ネットワーク オブジェクト グループの非名前付きオブジェクトです。ネットワーク オブジェクト グループ内にある IP アドレスの名前付きオブジェクトを ASA が作成する場合、ASDM は非名前付きオブジェクトを維持したまま、重複したオブジェクトを ASDM で作成します。これらのオブジェクトをマージするには、[Tools] > [Migrate Network Object Group Members] を選択します。 詳細については、「*Cisco ASA 5500 Migration to Version 8.3 and Later*」を参照してください。
[Preferences]	セッション間での特定の ASDM 機能の動作を変更します。詳細については、「ASDM 設定の定義」（P.3-32）を参照してください。
[ASDM Java Console]	Java コンソールを表示します。

[Wizards] メニュー

[Wizards] メニューにより、さまざまな機能を設定するウィザードを実行できます。次の表に、使用可能なウィザードおよびその機能を示します。

[Wizards] メニュー項目	説明
[Startup Wizard]	ASA の初期コンフィギュレーションの段階的な手順を示します。
[IPsec VPN Wizard]	ASA に IPSec VPN ポリシーを設定できます。詳細については、VPN コンフィギュレーション ガイドを参照してください。
[SSL VPN Wizard]	ASA に SSL VPN ポリシーを設定できます。詳細については、VPN コンフィギュレーション ガイドを参照してください。
[High Availability and Scalability Wizard]	VPN クラスタ ロード バランシングまたは ASA での ASA クラスタリングなどのフェールオーバーの設定ができます。

[Wizards] メニュー項目	説明
[Unified Communication Wizard]	ASA に IP フォンなどのユニファイド コミュニケーション機能を設定できます。詳細については、ファイアウォール コンフィギュレーション ガイドを参照してください。
[ASDM Identity Certificate Wizard]	Java 7 Update 51 以降を使用する場合、ASDM ランチャには信頼できる証明書が必要です。証明書の要件は、自己署名付きの ID 証明書をインストールすることによって簡単に満たすことができます。このウィザードを使用して証明書をインストールするまでは、Java Web Start を使用して ASDM を起動することができます。詳細については、http://www.cisco.com/go/asdm-certificate を参照してください。
[Packet Capture Wizard]	ASA にパケット キャプチャを設定できます。このウィザードは、入出力インターフェイスのそれぞれでパケット キャプチャを 1 回実行します。キャプチャの実行後、キャプチャをコンピュータに保存し、パケット アナライザを使用してキャプチャを調査および分析できます。

[Window] メニュー

[Window] メニューを使用して、ASDM のウィンドウ間を移動できます。アクティブなウィンドウが選択されたウィンドウとして表示されます。

[Help] メニュー

[Help] メニューでは、オンライン ヘルプへのリンクの他に、ASDM と ASA の情報も提供されます。次の表に、[Help] メニューを使用して実行できるタスクを示します。

[Help] メニュー項目	説明
[Help Topics]	新しいブラウザ ウィンドウを開いて、左側のフレームに目次、ウィンドウ名、および索引で構成されたヘルプを表示します。これらの方法を使用して任意のトピックのヘルプを探すか、[Search] タブを使用して検索します。
[Help for Current Screen]	その画面に関する状況依存ヘルプを開きます。ウィザードは、その時点で開いている画面、ペイン、またはダイアログボックスのヘルプを表示します。また、**疑問符**（**?**）の**ヘルプ** アイコンをクリックして表示することもできます。
[Release Notes]	Cisco.com にある最新バージョンの ***ASDM リリース ノート***を開きます。リリース ノートには、ASDM のソフトウェアとハードウェア要件の最新情報、およびソフトウェア変更に関する最新情報が記載されています。
[ASDM Assistant]	Cisco.com からダウンロード可能なコンテンツを検索でき、特定のタスクの実行に関する詳細がわかる **ASDM Assistant** を開きます。

[Help] メニュー項目	説明
[About Cisco Adaptive Security Appliance (ASA)]	ソフトウェア バージョン、ハードウェア構成、スタートアップ時にロードされるコンフィギュレーション ファイルやソフトウェア イメージなど、ASA に関する情報を表示します。これらはトラブルシューティングの際に役立つ情報です。
[About Cisco ASDM]	ソフトウェア バージョン、ホスト名、権限レベル、オペレーティング システム、デバイス タイプ、Java のバージョンなど、ASDM に関する情報を表示します。

ツールバー

メニューの下にある**ツールバー**から、ホーム ビュー、コンフィギュレーション ビュー、およびモニタリング ビューにアクセスできます。また、マルチ コンテキスト モードでシステムとセキュリティ コンテキストを選択したり、ナビゲーションおよびその他よく使用する機能を実行できます。次の表に、**ツールバー**を使用して実行できるタスクを示します。

ツールバー ボタン	説明
[System/Contexts]	どのコンテキストにいるかを表示します。左ペインのコンテキスト リストを開くには**下**矢印をクリックします。コンテキストのドロップダウン リストを元に戻すには**上**矢印をクリックします。このリストが展開されているときに**左**矢印をクリックするとペインは折りたたまれ、**右**矢印をクリックするとペインが元に戻ります。システムを管理するには、ドロップダウン リストから [System] を選択します。コンテキストを管理するには、ドロップダウン リストからコンテキストを選択します。
[Home]	インターフェイスのステータス、実行中のバージョン、ライセンス情報、パフォーマンスなどの、ASA に関する重要な情報を表示できる [Home] ペインを表示します。詳細については、「[Home] ペイン（シングル モードとコンテキスト）」（P.3-18）を参照してください。マルチ モードの場合、[Home] ペインはありません。
[Configuration]	ASA を設定します。左側の [Navigation] ペインの機能ボタンをクリックして機能を設定します。
[Monitoring]	ASA をモニタします。左側の [Navigation] ペインの機能ボタンをクリックして機能を設定します。
[Back]	直前に表示した ASDM のペインに戻ります。
[Forward]	直前に表示した ASDM のペインに進みます。
[Search]	ASDM の機能を検索します。検索機能は、各ペインのタイトルをすべて検索して一致項目を表示します。ハイパーリンクをクリックすると、該当ペインがただちに表示されます。[Back] または [Forward] をクリックすると、検出した 2 つのペインをすばやく切り替えることができます。詳細については、「ASDM Assistant」（P.3-11）を参照してください。
[Refresh]	現在の実行コンフィギュレーションで ASDM をリフレッシュします。ただし、モニタリング ペインのグラフはリフレッシュしません。

ツールバー ボタン	説明
[Save]	書き込みアクセスが可能なコンテキストに限り、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として保存します。
[Help]	その時点で表示されている画面の状況依存ヘルプを表示します。

ASDM Assistant

ASDM Assistant では、特定のタスクについての ASDM の使用方法のヘルプを検索して表示できます。この機能は、シングル コンテキストとシステム コンテキストのルーテッド モードおよびトランスペアレント モードで使用できます。

情報にアクセスするには、[View] > [ASDM Assistant] > [How Do I?] を選択するか、メニューバーの [Look For] フィールドに検索要求を入力します。[Find] ドロップダウン リストから[How Do I?] を選択して検索を開始します。

ASDM Assistant を使用するには、次の手順を実行します。

ステップ 1　[View] > [ASDM Assistant] を選択します。

[ASDM Assistant] ペインが表示されます。

ステップ 2　[Search] フィールドに検索する情報を入力して [Go] をクリックします。

要求された情報が [Search Results] ペインに表示されます。

ステップ 3　[Search Results] 領域および [Features] 領域に表示される任意のリンクをクリックし、詳細情報を入手します。

ステータス バー

ステータス バーは ASDM ウィンドウの下部に表示されます。次の表に、左から右に表示される領域を示します。

領域	説明
[Status]	コンフィギュレーションのステータス（「Device configuration loaded successfully.」など）。
[Failover]	フェールオーバー装置のステータスで、アクティブまたはスタンバイのいずれか。
[User Name]	ASDM ユーザのユーザ名。ユーザ名なしでログインした場合、ユーザ名は「admin」です。
[User Privilege]	ASDM ユーザの特権。
[Commands Ignored by ASDM]	アイコンをクリックすると、ASDM で処理されなかったコンフィギュレーションのコマンドのリストが表示されます。これらのコマンドはコンフィギュレーションから削除されません。
[Connection to Device]	ASDM と ASA の接続ステータス。詳細については、「[Connection to Device]」（P.3-12）を参照してください。

領域	説明
[Syslog Connection]	syslog 接続が動作しており、ASA がモニタされています。
[SSL Secure]	ASDM への接続に SSL を使用し、安全であることを示します。
[Time]	ASA に設定された時刻。

[Connection to Device]

ASDM は ASA との接続を常に維持し、[Monitoring] ペインおよび [Home] ペインのデータを最新に保ちます。このダイアログボックスに接続ステータスが表示されます。コンフィギュレーションを変更する場合、変更している間 ASDM は接続をもう一つ開き、変更が終わるとその接続を閉じますが、このダイアログボックスには 2 つ目の接続は表示されません。

[Device List]

[Device List] はドッキング可能なペインです。ヘッダーにある 3 つのボタンをそれぞれクリックすると、ペインの最大化または復元、移動可能なフローティング ペインへの変更、ペインの非表示化、またはペインを閉じることができます。このペインはホーム、コンフィギュレーション、モニタリング、およびシステムの各ビューで使用できます。このペインを使用して、別のデバイスに切り替えることができますが、そのデバイスでも現在実行しているものと同じバージョンの ASDM が実行されている必要があります。ペインを完全に表示するには、少なくとも 2 つのデバイスがリストに表示されている必要があります。このペインは、シングル コンテキスト、マルチ コンテキストおよびシステム コンテキストのルーテッド モードおよびトランスペアレント モードで使用できます。

このペインを使用して別のデバイスに接続するには、次の手順を実行します。

ステップ 1　[Add] をクリックしてリストに別のデバイスを追加します。

[Add Device] ダイアログボックスが表示されます。

ステップ 2　デバイス名またはデバイスの IP アドレスを入力し、[OK] をクリックします。

ステップ 3　リストから選択したデバイスを削除するには、[Delete] をクリックします。

ステップ 4　[Connect] をクリックして別のデバイスに接続します。

[Enter Network Password] ダイアログボックスが表示されます。

ステップ 5　ユーザ名とパスワードを該当するフィールドに入力し、[Login] をクリックします。

共通ボタン

多くの ASDM ペインには、次の表に示すボタンが含まれています。目的の作業を完了するには、該当するボタンをクリックします。

ボタン	説明
[Apply]	ASDM での変更内容を ASA に送信し、実行コンフィギュレーションに適用します。
[Save]	実行コンフィギュレーションのコピーをフラッシュ メモリに書き込みます。
[Reset]	変更内容を破棄して、変更前、または [Refresh] や [Apply] を最後にクリックした時点の表示情報に戻します。[Reset] をクリックした後、[Refresh] をクリックして、現在の実行コンフィギュレーションの情報が表示されていることを確認します。
[Restore Default]	選択した設定をクリアしてデフォルト設定に戻します。
[Cancel]	変更内容を破棄して、前のペインに戻ります。
[Enable]	機能について読み取り専用の統計情報を表示します。
[Close]	開いているダイアログボックスを閉じます。
[Clear]	フィールドから情報を削除します。または、チェックボックスをオフにします。
[Back]	前のペインに戻ります。
[Forward]	次のペインに移動します。
[Help]	選択したペインまたはダイアログボックスを表示します。

キーボード ショートカット

キーボードを使用して ASDM ユーザ インターフェイスをナビゲートできます。

表 3-1 は、ASDM ユーザ インターフェイスの 3 つの主要な領域間を移動するために使用できるキーボード ショートカットの一覧です。

表 3-1　メイン ウィンドウ内のキーボード ショートカット

表示対象	Windows/Linux	MacOS
[Home] ペイン	Ctrl+H	Shift+Command+H
[Configuration] ペイン	Ctrl+G	Shift+Command+G
[Monitoring] ペイン	Ctrl+M	Shift+Command+M
ヘルプ	F1	Command+?
前のペイン	Alt+左矢印	Command+[
次のペイン	Alt+右矢印	Command+]
表示のリフレッシュ	F5	Command+R
切り取り	Ctrl+X	Command+X
コピー	Ctrl+C	Command+C

表 3-1　メイン ウィンドウ内のキーボード ショートカット （続き）

表示対象	Windows/Linux	MacOS
貼り付け	Ctrl+V	Command+V
コンフィギュレーションの保存	Ctrl+S	Command+S
ポップアップ メニュー	Shift+F10	—
セカンダリ ウィンドウを閉じる	Alt+F4	Command+W
検索	Ctrl+F	Command+F
終了	Alt+F4	Command+Q
テーブルまたはテキスト領域の終了	Ctrl_Shift または Ctrl+Shift+Tab	Ctrl+Shift または Ctrl+Shift+Tab

表 3-2 は、ペイン内部のナビゲーションに使用できるキーボード ショートカットの一覧です。

表 3-2　ペイン内部のキーボード ショートカット

フォーカスの移動先	キー
次のフィールド	タブ
前のフィールド	Shift+Tab
次のフィールド（テーブル内にフォーカスがある場合）	Ctrl+Tab
前のフィールド（テーブル内にフォーカスがある場合）	Shift+Ctrl+Tab
次のタブ（タブにフォーカスがある場合）	右矢印
前のタブ（タブにフォーカスがある場合）	左矢印
テーブル内の次のセル	タブ
テーブル内の前のセル	Shift+Tab
次のペイン（複数のペインが表示されている場合）	F6
前のペイン（複数のペインが表示されている場合）	Shift+F6

表 3-3 は、Log Viewer で使用できるキーボード ショートカットの一覧です。

表 3-3　Log Viewer のキーボード ショートカット

目的	Windows/Linux	MacOS
Real-Time Log Viewer の一時停止および再開	Ctrl+U	Command+
ログ バッファ ペインのリフレッシュ	F5	Command+R
内部ログ バッファの消去	Ctrl+Delete	Command+Delete
選択したログ エントリのコピー	Ctrl+C	Command+C
ログの保存	Ctrl+S	Command+S
印刷	Ctrl+P	Command+P
セカンダリ ウィンドウを閉じる	Alt+F4	Command+W

表 3-4 は、メニュー項目へのアクセスに使用できるキーボード ショートカットの一覧です。

表 3-4　メニュー項目にアクセスするためのキーボード ショートカット

アクセス対象	Windows/Linux
メニュー バー	Alt
次のメニュー	右矢印
前のメニュー	左矢印
次のメニュー オプション	下矢印
前のメニュー オプション	上矢印
選択したメニュー オプション	Enter

多くの ASDM ペインでの検索機能

一部の ASDM ペインには、多くの要素を持つテーブルが含まれています。特定のエントリを簡単に検索および強調表示して編集するために、複数の ASDM ペインには、これらのペイン内のオブジェクトを検索できる検索機能が含まれています。

検索を実行する場合は、[Find] フィールドにフレーズを入力し、特定のペイン内のすべてのカラムを検索できます。フレーズにはワイルドカード文字の「*」および「?」を含めることができます。* は 1 つ以上の文字と一致し、? は 任意の 1 文字と一致します。[Find] フィールドの右にある上矢印と下矢印を使用して、次（上）または前（下）のフレーズの出現に移動します。[Match Case] チェックボックスをオンにすると、入力した大文字および小文字に正確に一致するエントリを検索します。

たとえば、B*ton-L* と入力すると、次の一致が返されます。

```
Boston-LA、Boston-Lisbon、Boston-London
```

Bo?ton と入力すると、次の一致が返されます。

```
Boston、Bolton
```

次のリストに、検索機能を使用できる ASDM ペインを示します。

- [AAA Server Groups] ペイン
- [ACL Manager] ペイン：[ACL Manager] ペインの検索機能は、他のペインの検索機能とは異なります。詳細については、「[ACL Manager] ペインの検索機能」（P.3-16）を参照してください。
- [Certificate-to-Conn Profile Maps-Rules] ペイン
- [DAP] ペイン
- [Identity Certificates] ペイン
- [IKE Policies] ペイン
- [IPSec Proposals (Transform Sets)] ペイン
- [Local User] ペイン
- [Portal-Bookmark] ペイン
- [Portal-Customization] ペイン
- [Portal-Port Forwarding] ペイン

- [CA Certificates] ペイン
- [Portal-Smart Tunnels] ペイン
- [Portal-Web Contents] ペイン
- [VPN Connection Profiles] ペイン
- [VPN Group Policies] ペイン

[ACL Manager] ペインの検索機能

ACL および ACE にはさまざまなタイプの多数の要素が含まれているため、[ACL Manager] ペインの検索機能では、他のペインの検索機能よりも対象を絞った検索を実行できます。

[ACL Manager] ペイン内で要素を検索するには、次の手順を実行します。

ステップ 1　[ACL Manager] ペインで [Find] をクリックします。

ステップ 2　[Filter] フィールドで、ドロップダウン リストから次のオプションのいずれかを選択します。

- [Source]：検索には、トラフィックを許可または拒否する送信元のネットワーク オブジェクト グループの IP アドレス、インターフェイスの IP アドレス、またはその他のアドレスが含まれます。このアドレスはステップ 4 で指定します。
- [Destination]：検索には、[Source] セクションにリストされている IP アドレスへのトラフィックの送信を許可または拒否されている宛先 IP アドレス（ホストまたはネットワーク）が含まれます。このアドレスはステップ 4 で指定します。
- [Source or Destination]：検索には、送信元または宛先のいずれかのアドレスが含まれます。このアドレスはステップ 4 で指定します。
- [Service]：検索には、サービス グループまたは事前定義済みのサービス ポリシーが含まれます。これらのサービスはステップ 4 で指定します。
- [Query]：ドロップダウン リストから [Query] を選択する場合は、[Query] をクリックして、前の 4 つのすべてのオプション（[Source]、[Destination]、[Source or Destination]、および [Service]）による詳細検索を指定します。

ステップ 3　2 番目のフィールドで、ドロップダウン リストから次のいずれかのオプションを選択します。

- [is]：ステップ 4 で入力する詳細に対する完全一致を指定します。
- [contains]：ステップ 4 で入力する詳細を含むが、それに限定されない ACL または ACE の検索を指定します。

ステップ 4　3 番目のフィールドで、検索する ACL または ACE に関する具体的な条件を入力するか、[Browse] をクリックして ACL または ACE のコンフィギュレーションにおける主要な要素を検索します。

ステップ 5　検索を実行するには、[Filter] をクリックします。

ASDM の検索機能により、指定した条件を含む ACL および ACE のリストが返されます。

ステップ 6　検出された ACL および ACE のリストをクリアするには、[Clear] をクリックします。

ステップ 7　赤い [**x**] をクリックして、検索機能ダイアログボックスを閉じます。

拡張スクリーン リーダ サポートのイネーブル化

デフォルトでは、**Tab** キーを押してペイン内を移動するときに、ラベルと説明はタブの移動先から除外されます。JAWS のような一部のスクリーン リーダは、フォーカスのある画面オブジェクトのみを読み上げます。拡張スクリーン リーダ サポートをイネーブルにすると、ラベルと説明にもタブを移動させることができます。

拡張スクリーン リーダ サポート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　[Tools] > [Preferences] を選択します。

[Preferences] ダイアログボックスが表示されます。

ステップ 2　[General] タブの [Enable screen reader support] チェックボックスをオンにします。

ステップ 3　[OK] をクリックします。

ステップ 4　スクリーン リーダ サポートをアクティブにするには、ASDM を再起動します。

整理用フォルダー

コンフィギュレーション ビューおよびモニタリング ビューのナビゲーション ペインに含まれる一部のフォルダには、関連付けられたコンフィギュレーション ペインやモニタリング ペインがありません。これらのフォルダは、関連するコンフィギュレーション タスクやモニタリング タスクを整理するために使用します。これらのフォルダをクリックすると、右側の [**Navigation**] ペインにサブ項目のリストが表示されます。サブ項目の名前をクリックするとその項目に移動できます。

ヘルプ ウィンドウについて

必要な情報を取得するには、次の表にリストされている、該当するボタンをクリックします。

ボタン	説明
[About ASDM]	ASDM に関する情報を表示します。ホスト名、バージョン番号、デバイス タイプ、ASA のソフトウェア バージョン番号、権限レベル、ユーザ名、使用するオペレーティング システムなどが含まれます。
[Search]	オンライン ヘルプ項目から情報を検索します。
[Using Help]	オンライン ヘルプの最も効率的な使用方法について説明します。
[Glossary]	ASDM および ASA で使用されている用語のリストを表示します。
[Contents]	目次を表示します。
[Screens]	ヘルプ ファイルのリストを画面の名前ごとに表示します。
[Index]	ASDM のオンライン ヘルプにあるヘルプ項目の索引を表示します。

[Home] ペイン（シングル モードとコンテキスト）

ASDM の [Home] ペインでは、ASA に関する重要な情報を表示します。[Home] ペインのステータス情報は 10 秒間隔で更新されます。このペインには通常、[Device Dashboard] と [Firewall Dashboard] の 2 つのタブがあります。

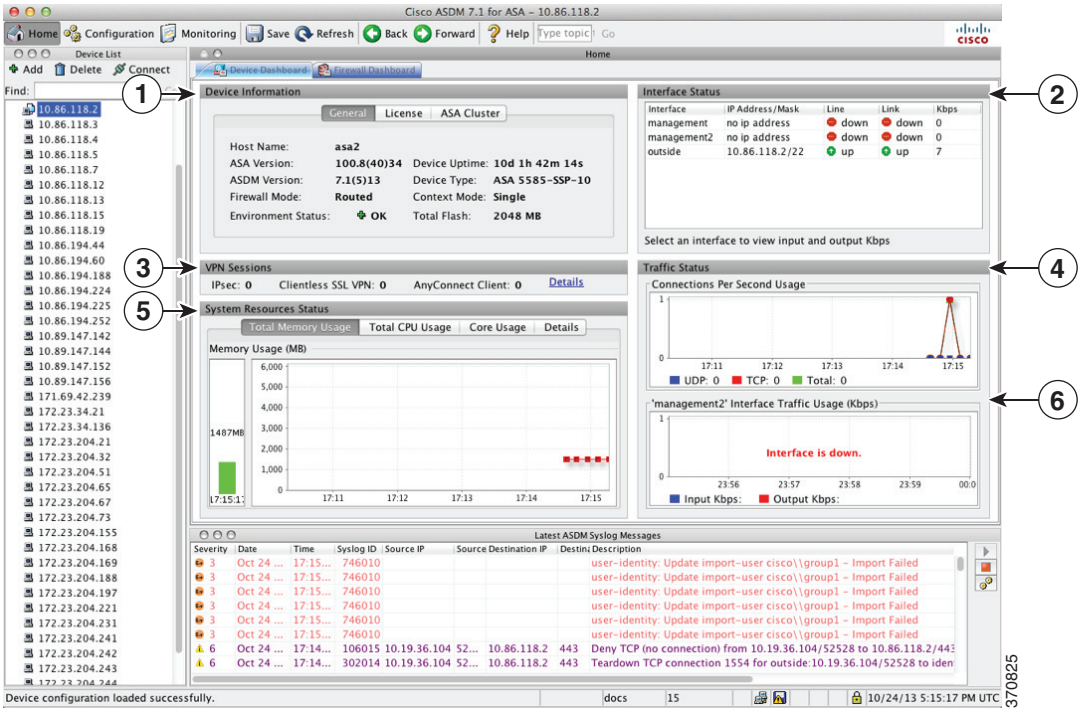
IPS モジュールや CX モジュールのようなハードウェアまたはソフトウェアのモジュールがデバイスにインストールされている場合、それらのモジュール用に別のタブが表示されます。

[Device Dashboard] タブ

[Device Dashboard] タブでは、インターフェイスのステータス、実行中のバージョン、ライセンス情報、パフォーマンスなど、ASA の重要な情報を一目で確認できます。

図 3-2 に、[Device Dashboard] タブの要素を示します。

図 3-2　[Device Dashboard] タブ



凡例

GUI 要素	説明
1	「[Device Information] ペイン」（P.3-19）
2	「[Interface Status] ペイン」（P.3-20）
3	「[VPN Sessions] ペイン」（P.3-20）
4	「[Traffic Status] ペイン」（P.3-21）

GUI 要素	説明
5	「[System Resources Status] ペイン」（P.3-21）
6	「[Traffic Status] ペイン」（P.3-21）
—	「[Device List]」（P.3-12）
—	「[Latest ASDM Syslog Messages] ペイン」（P.3-21）

[Device Information] ペイン

[Device Information] ペインには、[General] タブと [License] タブというデバイス情報を表示する 2 つのタブがあります。[General] タブでは、システム ヘルスが一目でわかる [Environment Status] ボタンにアクセスできます。

[General] タブ

このタブには、ASA に関する基本情報が表示されます。

- [Host name]：デバイスのホスト名を表示します。
- [ASA version]：デバイス上で実行されている ASA ソフトウェアのバージョンを表示します。
- [ASDM version]：デバイス上で実行されている ASDM ソフトウェアのバージョンを表示します。
- [Firewall mode]：デバイスが実行されているファイアウォール モードを表示します。
- [Total flash]：現在使用されている RAM の合計を表示します。
- [ASA Cluster Role]：クラスタリングがイネーブルの場合に、この装置のロール（マスターまたはスレーブ）を表示します。
- [Device uptime]：最後にソフトウェアをアップロードしてから、デバイスが動作している時間を表示します。
- [Context mode]：デバイスが実行されているコンテキスト モードを表示します。
- [Total Memory]：ASA にインストールされている DRAM を表示します。
- [Environment status]：システム ヘルスを表示します。ASA 5585-X は、[General] タブの [Environment Status] ラベルの右側にあるプラス記号（+）をクリックすると、提供可能なハードウェアの一連の統計情報を表示します。設置されている電源装置数の確認、ファンと電源モジュールの動作ステータスの追跡、および CPU の温度とシステムの周囲温度の追跡を実行できます。

  一般に、[Environment Status] ボタンでシステム ヘルスが一目でわかります。システム内のモニタ対象のすべてのハードウェア コンポーネントが正常な範囲内で動作している場合、プラス記号（+）ボタンは正常を示す緑色で表示されます。一方、ハードウェア システム内のコンポーネントが 1 つでも正常な範囲外で動作している場合は、プラス記号（+）ボタンが赤色の丸になってクリティカル ステータスを示し、ハードウェア コンポーネントに関してすぐに対処が必要であることを示します。

  特定のハードウェアの統計情報に関する詳細については、そのデバイスのハードウェア ガイドを参照してください。

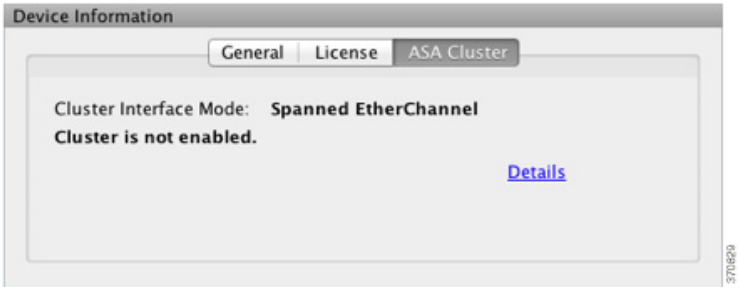
（注）　最新リリースの ASA にアップグレードするためのメモリが不足している場合には、[Memory Insufficient Warning] ダイアログボックスが表示されます。このダイアログボックスに表示される指示に従って、サポートされている方法で ASA および ASDM を継続して使用します。[OK] をクリックして、このダイアログボックスを閉じます。

[License] タブ

このタブには、ライセンス機能のサブセットが表示されます。詳細なライセンス情報の表示または新しいアクティベーション キーの入力を行うには、[More Licenses] をクリックします。[Configuration] > [Device Management] > [Licensing] > [Activation Key] ペインが表示されます。

[Cluster] タブ

このタブには、クラスタのインターフェイス モードおよびクラスタのステータスが表示されます。



[Virtual Resources] タブ（ASAv）

このタブには、ASAv によって使用されている仮想リソースが表示されます。vCPU の数、RAM、ASAv のプロビジョニングの過不足が含まれます。

[Interface Status] ペイン

このペインには、各インターフェイスのステータスが表示されます。インターフェイスの行を選択すると、入力および出力スループットが Kbps 単位でテーブルの下に表示されます。

[VPN Sessions] ペイン

このペインには、VPN トンネル ステータスが表示されます。[Details] をクリックすると、[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] ペインに移動します。

[Failover Status] ペイン

このペインには、フェールオーバー ステータスが表示されます。

[Configure] をクリックして、High Availability and Scalability Wizard を起動します。このウィザードを完了すると、フェールオーバー コンフィギュレーション ステータス（[Active/Active] または [Active/Standby]）が表示されます。

フェールオーバーが設定されている場合は、[Details] をクリックすると、[Monitoring] > [Properties] > [Failover] > [Status] ペインが開きます。

[System Resources Status] ペイン

このペインには、CPU およびメモリの使用状況に関する統計情報が表示されます。

[Traffic Status] ペイン

このペインには、インターフェイス全体の秒単位の接続数と、セキュリティが最も低いインターフェイスのトラフィック スループットのグラフが表示されます。

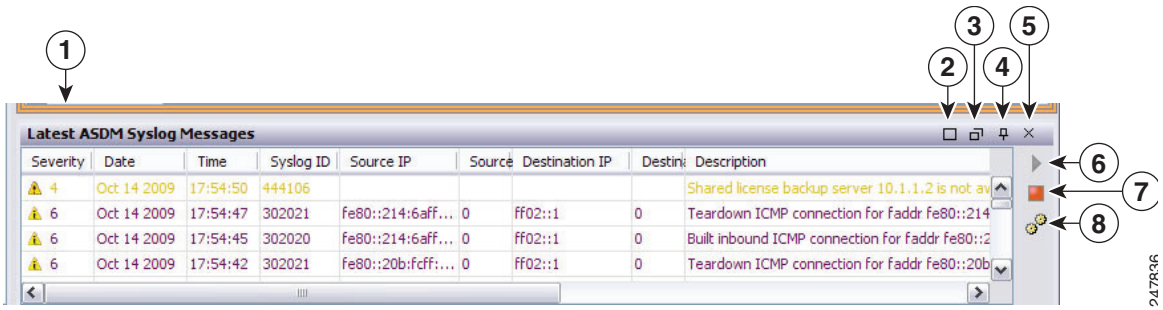
コンフィギュレーションにセキュリティ レベルが最も低いインターフェイスが複数含まれており、そのいずれかの名前が「outside」である場合、そのインターフェイスがトラフィック スループットのグラフに使用されます。それ以外の場合、ASDM はセキュリティ レベルが最も低いインターフェイスのアルファベット順のリストから最初のインターフェイスを選択します。

[Latest ASDM Syslog Messages] ペイン

このペインには、ASA が生成した最新のシステム メッセージが 100 個まで表示されます。ロギングがディセーブルになっている場合は、[Enable Logging] をクリックしてイネーブルにします。

図 3-3 に、[Latest ASDM Syslog Messages] ペインの要素を示します。

図 3-3　[Latest ASDM Syslog Messages] ペイン



凡例

GUI 要素	説明
1	ペインのサイズを変更するには、**ディバイダ**を上または下にドラッグします。
2	ペインを拡大します。ペインをデフォルトの サイズに戻すには、**二重の正方形**のアイコンをクリックします。
3	フローティング ペインを作成します。ペインをドッキングするには、**ドッキングしたペイン** アイコンをクリックします。
4	自動非表示をイネーブルまたはディセーブルにします。自動非表示がイネーブルな場合は、左下隅にある [Latest ASDM Syslog Messages] ボタンの上にカーソルを移動すると、ペインが表示されます。カーソルをペインから離すと、ペインは非表示になります。
5	ペインを閉じます。ペインを表示するには、[View Latest ASDM Syslog Messages] を選択します。

GUI 要素	説明
6	右側にある**緑**のアイコンをクリックすると、syslog メッセージの表示の更新を続行します。
7	右側にある**赤い**アイコンをクリックすると、syslog メッセージの表示の更新を停止します。
8	右側にある**フィルタ** アイコンをクリックすると、[Logging Filters] ペインが開きます。

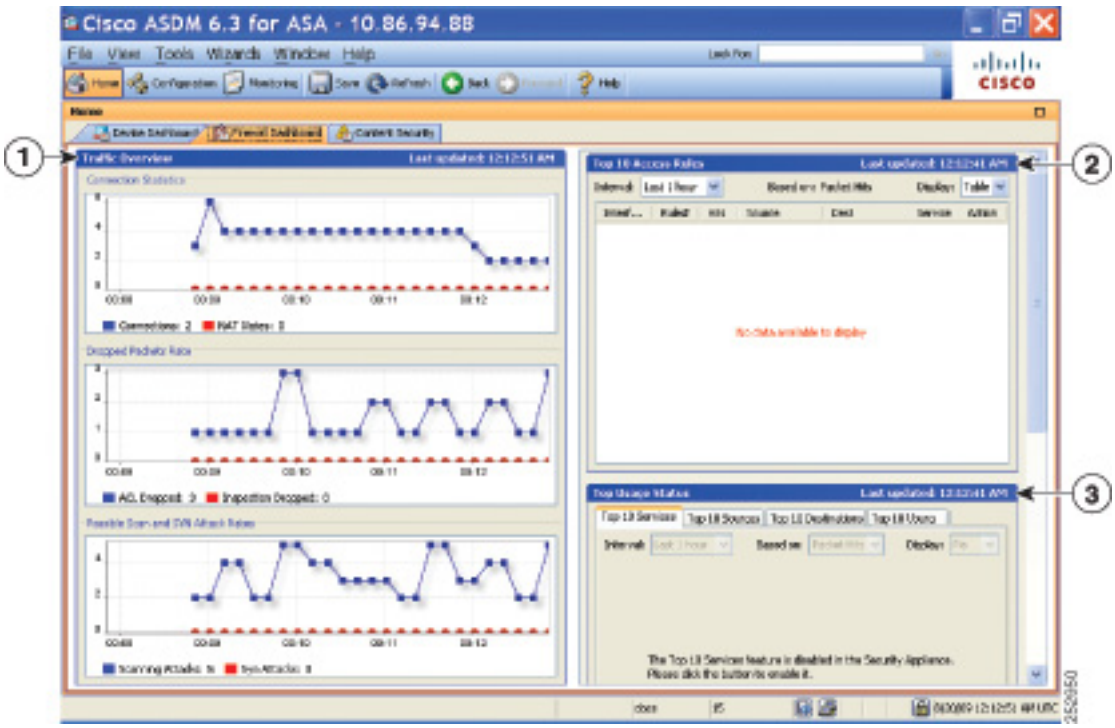
- イベントを右クリックして [Clear Content] を選択すると、現在のメッセージを消去します。
- イベントを右クリックして [Save Content] をクリックすると、現在のメッセージを PC 上のファイルに保存します。
- イベントを右クリックして [Copy] を選択すると、現在の内容をコピーします。
- イベントを右クリックして [Color Settings] を選択すると、重大度に基づいて syslog メッセージの背景色と前景色を変更します。

[Firewall Dashboard] タブ

[Firewall Dashboard] タブでは、ASA を通過するトラフィックに関する重要な情報を確認できます。このダッシュボードは、シングル コンテキスト モードまたはマルチ コンテキスト モードのどちらであるかにより異なります。マルチ コンテキスト モードでは、[Firewall Dashboard] は各コンテキスト内に表示できます。

図 3-4 に、[Firewall Dashboard] タブの要素の一部を示します。

図 3-4　　[Firewall Dashboard] タブ



凡例

GUI 要素	説明
1	「[Traffic Overview] ペイン」（P.3-23）
2	「[Top 10 Access Rules] ペイン」（P.3-23）
3	「[Top Usage Status] ペイン」（P.3-23）
（表示なし）	「[Top Ten Protected Servers Under SYN Attack] ペイン」（P.3-24）
（表示なし）	「[Top 200 Hosts] ペイン」（P.3-24）
（表示なし）	「[Top Botnet Traffic Filter Hits] ペイン」（P.3-25）

[Traffic Overview] ペイン

デフォルトでは、イネーブルです。基本脅威検出をディセーブルにすると（ファイアウォール コンフィギュレーション ガイドを参照）、この領域には [Enable] ボタンが表示されます。[Enable] ボタンを使用して基本脅威検出をイネーブルにできます。実行時の統計情報には、*表示専用*の次の情報が含まれます。

- 接続数と NAT 変換数。
- アクセス リストによる拒否およびアプリケーション インスペクションによってドロップされたパケット数/秒。
- ドロップ パケット数/秒。これは、スキャン攻撃の一部として特定される場合と、不完全なセッションとして検出される場合（TCP SYN 攻撃やデータなし UDP セッション攻撃を検出した場合など）があります。

[Top 10 Access Rules] ペイン

デフォルトでは、イネーブルです。アクセス ルールの脅威検出統計情報をディセーブルにすると（ファイアウォール コンフィギュレーション ガイドを参照）、この領域には [Enable] ボタンが表示されます。[Enable] ボタンを使用してアクセス ルールの統計情報をイネーブルにできます。

テーブル ビューでは、リストからルールを選択して右クリックし、ポップアップ メニュー項目の [Show Rule] を表示できます。この項目を選択して [Access Rules] テーブルに移動し、テーブル内にあるそのルールを選択します。

[Top Usage Status] ペイン

デフォルトでは、ディセーブルです。このペインには、次の 4 つのタブがあります。

- [Top 10 Services]：脅威検出サービス
- [Top 10 Sources]：脅威検出サービス
- [Top 10 Destinations]：脅威検出サービス
- [Top 10 Users]：アイデンティティ ファイアウォール サービス

最初の 3 つのタブ（[Top 10 Services]、[Top 10 Sources]、および [Top 10 Destinations]）では、脅威検出サービスに関する統計情報を提供します。各タブには、それぞれの脅威検出サービスをイネーブルにする [Enable] ボタンがあります。ファイアウォール コンフィギュレーション ガイドに従って、これらをイネーブルにすることができます。

[Top 10 Services Enable] ボタンを使用すると、ポートとプロトコルの両方の統計情報がイネーブルになります（どちらも表示用にイネーブルにする必要があります）。[Top 10 Sources] ボタンおよび [Top 10 Destinations Enable] ボタンを使用すると、ホストの統計情報がイネーブルになります。ホスト（送信元および宛先）の上位使用ステータス統計情報、およびポートとプロトコルが表示されます。

4 番目のタブ [Top 10 Users] では、アイデンティティ ファイアウォール サービスに関する統計情報を提供します。アイデンティティ ファイアウォール サービスでは、ユーザのアイデンティティに基づくアクセス コントロールを提供します。送信元 IP アドレスではなくユーザ名とユーザ グループ名に基づいてアクセス ルールとセキュリティ ポリシーを設定できます。ASA は、IP とユーザのマッピング データベースにアクセスして、このサービスを提供します。

ASA でアイデンティティ ファイアウォール サービスを設定している場合（Microsoft Active Directory や Cisco Active Directory（AD）エージェントなどの追加コンポーネントの設定を含む）にのみ、[Top 10 Users] タブにデータが表示されます。

選択したオプションに応じて、[Top 10 Users] タブに、上位 10 ユーザの受信した EPS パケット、送信した EPS パケット、および送信された攻撃に関する統計情報が表示されます。（*domain\user_name* として表示される）各ユーザに関して、このタブには、そのユーザの平均 EPS パケット、現在の EPS パケット、トリガー、および合計イベント数が表示されます。

注意　統計情報をイネーブルにすると、イネーブルにした統計情報のタイプに応じて、ASA のパフォーマンスに影響することがあります。ホストの統計情報をイネーブルにすると、パフォーマンスに大きな影響があります。トラフィックの負荷が高い場合は、このタイプの統計情報は一時的にイネーブルにすることを検討してください。ただし、ポートの統計情報をイネーブルにしても、それほど影響はありません。

[Top Ten Protected Servers Under SYN Attack] ペイン

デフォルトでは、ディセーブルです。この領域に表示されている [Enable] ボタンを使用して、この機能をイネーブルにできます。または、ファイアウォール コンフィギュレーション ガイドに従ってイネーブルにすることもできます。攻撃を受けて保護された上位 10 サーバの統計情報が表示されます。

平均攻撃レートの場合、ASA はレート間隔（デフォルトは 30 分）に対して 30 秒ごとにデータをサンプリングします。

複数の攻撃者がいる場合は、「<various>」の後に最後の攻撃者の IP アドレスが表示されます。

[Detail] をクリックして、10 台のサーバだけでなく、すべてのサーバ（最大 1000 台）の統計情報を表示します。履歴サンプリング データを確認することもできます。ASA はレート間隔中に攻撃回数を 60 回サンプリングするため、デフォルトの 30 分間では 60 秒ごとに統計情報が収集されます。

[Top 200 Hosts] ペイン

デフォルトでは、ディセーブルです。ASA 経由で接続された上位 200 のホストを表示します。ホストの各エントリには、ホストの IP アドレスと、ホストによって開始された接続の数が含まれ、このエントリは 120 秒ごとにアップデートされます。この表示をイネーブルにするには **hpm topnenable** コマンドを入力します。

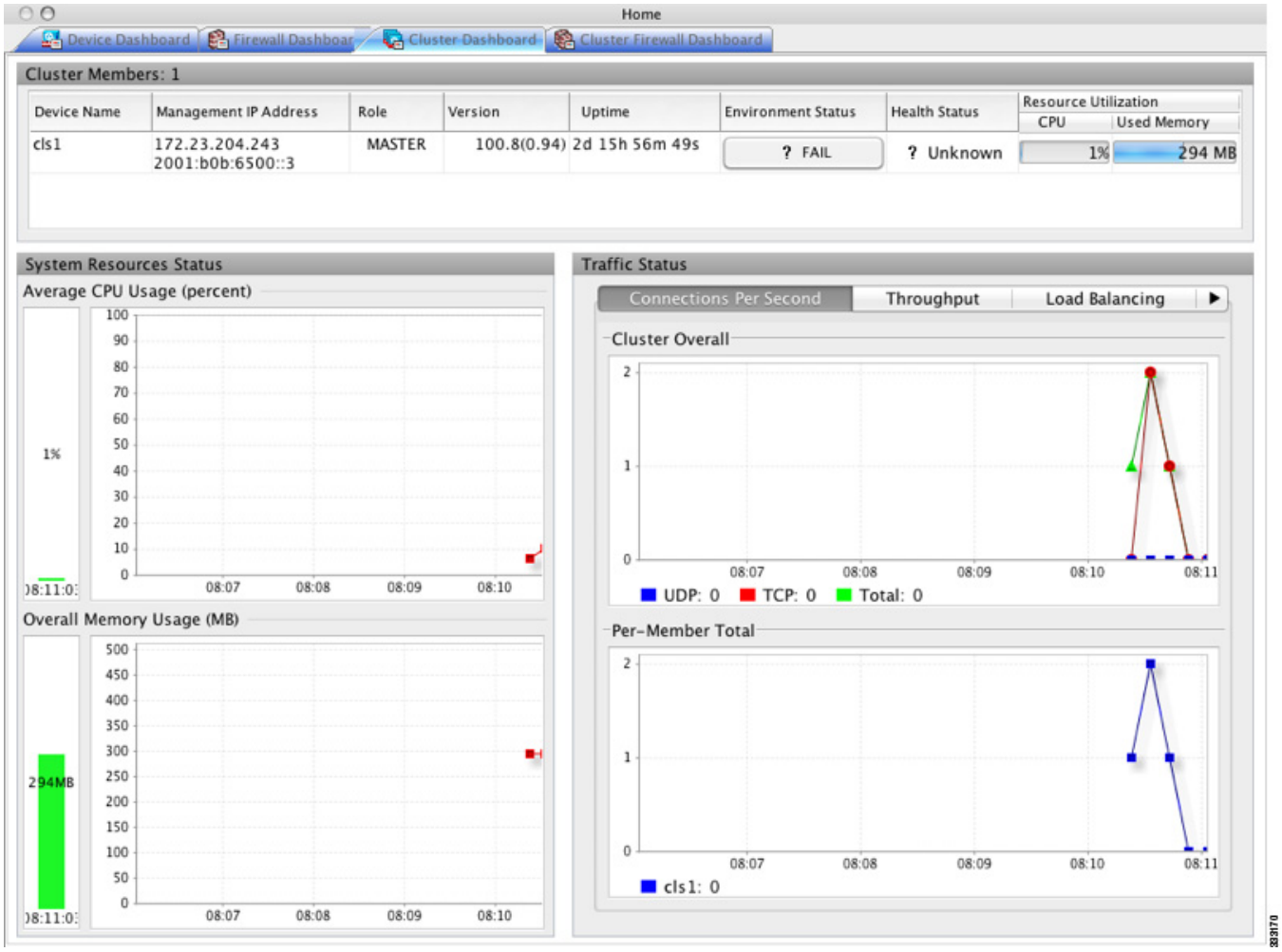
[Top Botnet Traffic Filter Hits] ペイン

デフォルトでは、ディセーブルです。この領域には、ボットネット トラフィック フィルタを設定するためのリンクが含まれています。上位 10 個のボットネット サイト、ポート、および感染ホストのレポートは、データのスナップショットを提供し、統計情報の収集開始以降の上位 10 項目に一致しない場合があります。IP アドレスを右クリックすると、whois ツールが起動してボットネット サイトの詳細が表示されます。

詳細については、ファイアウォール コンフィギュレーション ガイドを参照してください。

[Cluster Dashboard] タブ

[Cluster Dashboard] タブには、クラスタのメンバーシップとリソース使用率のサマリーが表示されます。



- [Cluster Members]：クラスタを構成するメンバーの名前と基本情報（管理 IP アドレス、バージョン、クラスタ内のロールなど）およびメンバーのヘルス ステータス（環境ステータス、ヘルス ステータス、およびリソース使用率）を表示します。

（注）　マルチ コンテキスト モードでは、管理コンテキストに ASDM を接続し、次に別のコンテキストに変更しても、リスト表示されている管理 IP アドレスは現在のコンテキストの管理 IP アドレスに変更されません。ASDM が現在接続されているメインクラスタの IP アドレスを含む管理コンテキストの管理 IP アドレスを、引き続き表示し続けます。

- [System Resource Status]：クラスタ全体のリソース使用率（CPU およびメモリ）とトラフィックのグラフ（クラスタ全体およびデバイスごと）を表示します。
- [Traffic Status]：各タブには次のグラフがあります。
  - [Connections Per Second] タブ

    [Cluster Overal]：クラスタ全体の秒単位の接続数が表示されます。

    [Per-Member Total]：各メンバーの秒単位の平均接続数が表示されます。
  - [Throughput] タブ

    [Cluster Overall]：クラスタ全体の総出力スループットが表示されます。

    [Per-Member Throughput]：メンバーのスループットが、メンバーごとに 1 行ずつ表示されます。
  - [Load Balancing] タブ

    [Per-Member Percentage of Total Traffic]：メンバーが受信した総クラスタ トラフィックの割合が、メンバーごとに表示されます。

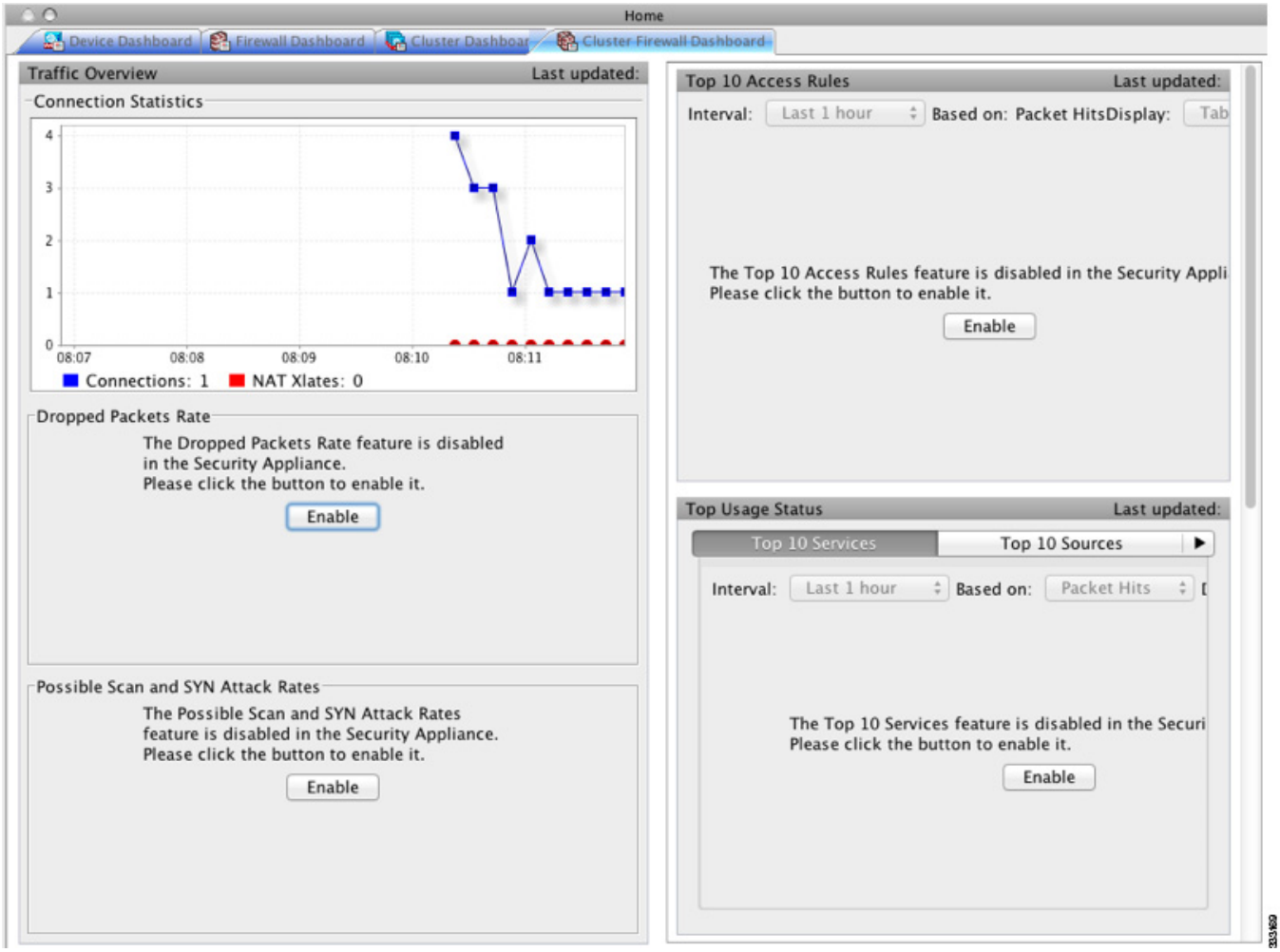
    [Per-Member Locally Processed Traffic]：ローカルに処理されたトラフィックの割合が、メンバーごとに表示されます。
  - [Control Link Usage] タブ

    [Per-Member Receival Capacity Utilization]：送信容量の使用率が、メンバーごとに表示されます。

    [Per-Member Transmittal Capacity Utilization]：受信容量の使用率が、メンバーごとに表示されます。

[Cluster Firewall Dashboard] タブ

[Cluster Firewall Dashboard] タブには、[Firewall Dashboard] に表示される情報と同様のトラフィックの概要および「top N」統計情報が表示されますが、クラスタ全体にわたる総計は表示されません。



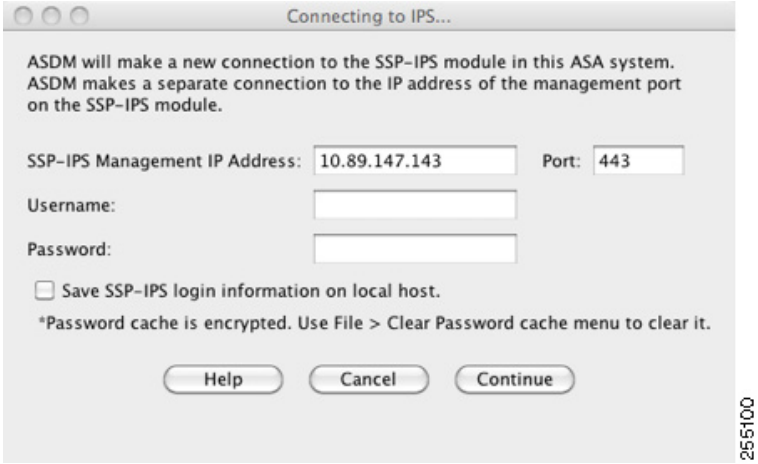
[Intrusion Prevention] タブ

[Intrusion Prevention] タブでは、IPS に関する重要な情報を確認できます。このタブは、ASA にインストールされている IPS モジュールがある場合にのみ表示されます。

IPS モジュールに接続するには、次の手順を実行します。

ステップ 1　[Intrusion Prevention] タブをクリックします。

[Connecting to IPS] ダイアログボックスが表示されます。



ステップ 2　IP アドレス、ポート、ユーザ名、パスワードを入力します。デフォルトの IP アドレスおよびポートは、192.168.1.2:443 です。デフォルトのユーザ名およびパスワードは、**cisco** と **cisco** です。

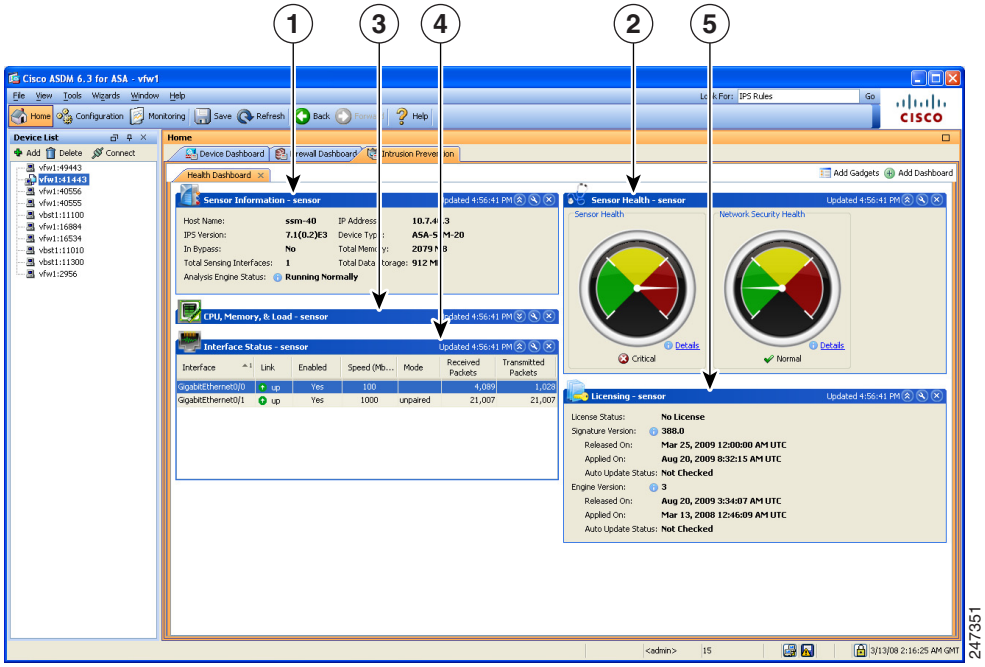
ステップ 3　ログイン情報をローカル PC に保存するには、[Save IPS login information on local host] チェックボックスをオンにします。

ステップ 4　[Continue] をクリックします。

侵入防御に関する詳細については、ファイアウォール コンフィギュレーション ガイドを参照してください。

図 3-5 に、[Intrusion Prevention] タブにある [Health Dashboard] タブの要素を示します。

図 3-5　[Intrusion Prevention] タブ（Health Dashboard）

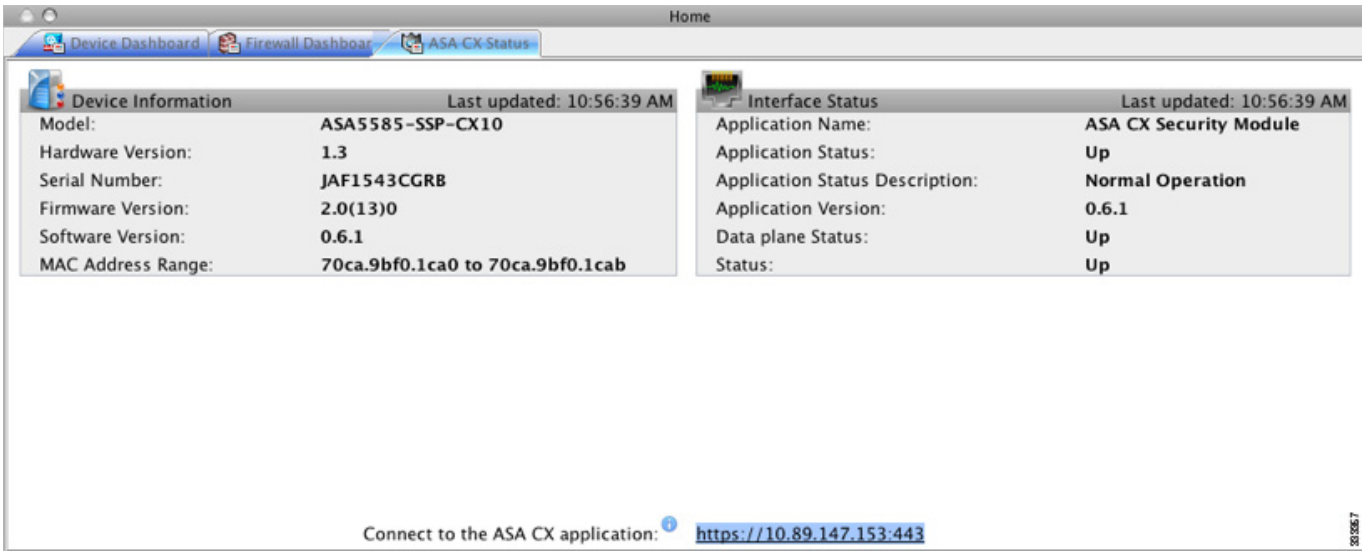


凡例

GUI 要素	説明
1	[Sensor Information] ペイン。
2	[Sensor Health] ペイン。
3	[CPU, Memory, and Load] ペイン。
4	[Interface Status] ペイン。
5	[Licensing] ペイン。

[ASA CX Status] タブ

[ASA CX Status] タブには、ASA CX モジュールに関する重要な情報が表示されます。このタブは、ASA に ASA CX モジュールがインストールされている場合にのみ表示されます。



[ASA FirePOWER Status] タブ

[ASA FirePOWER Status] タブには、このモジュールに関する情報が表示されます。この情報には、モデル、シリアル番号、ソフトウェア バージョンなどのモジュール情報と、アプリケーション名、アプリケーション ステータス、データ プレーン ステータス、全体のステータスなどのモジュール ステータスが含まれます。このモジュールが FireSIGHT 管理センター に登録されている場合は、リンクをクリックしてアプリケーションを開き、追加の分析やモジュールの設定を行うことができます。

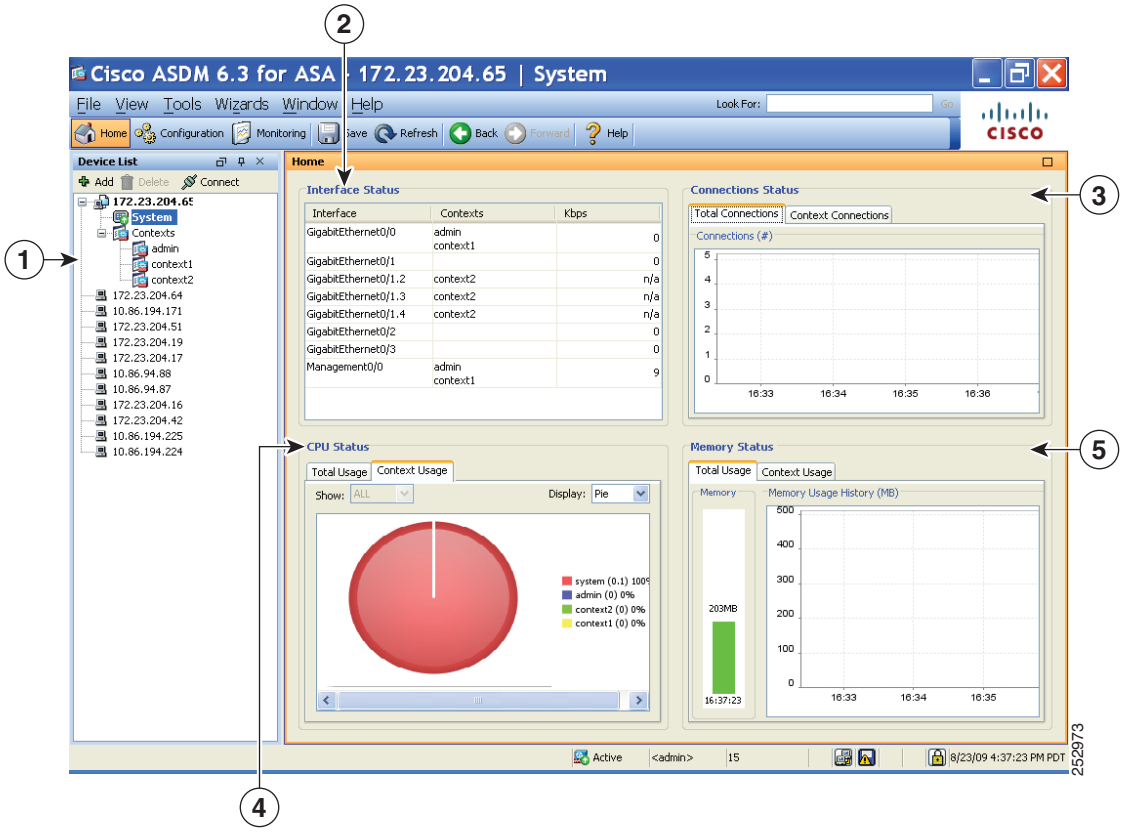
このタブは、ASA FirePOWER モジュールがデバイスにインストールされている場合にのみ表示されます。

[Home] ペイン（System）

ASDM システムの [Home] ペインでは、ASA に関する重要なステータス情報を確認できます。ASDM システムの [Home] ペインに表示される詳細の多くは ASDM の他の場所でも参照できますが、このペインでは ASA の動作状態を一目で確認できます。システムの [Home] ペインのステータス情報は 10 秒間隔で更新されます。

図 3-6（P.3-31）に、システムの [Home] ペインの要素を示します。

図 3-6　　システムの [Home] ペイン



凡例

GUI 要素	説明
1	システムと コンテキストの選択。
2	[Interface Status] ペイン。インターフェイスを通過するトラフィックの総数を表示するには、インターフェイスを選択します。
3	[Connection Status] ペイン。
4	[CPU Status] ペイン。
5	[Memory Status] ペイン。

ASDM 設定の定義

この機能により、特定の ASDM 設定の動作を定義できます。

ASDM のさまざまな設定を変更するには、次の手順を実行します。

ステップ 1　[Tools] > [Preferences] を選択します。

[General]、[Rules Table]、および [Syslog] の 3 つのタブのある [Preferences] ダイアログボックスが表示されます。

ステップ 2　設定を定義するには、これらのタブの 1 つをクリックします。[General] タブでは汎用プリファレンスを指定し、[Rules Table] タブでは [Rules] テーブルのプリファレンスを指定します。また、[Syslog] タブでは、[Home] ペインに表示される syslog メッセージの外観を指定したり、NetFlow 関連の syslog メッセージの警告メッセージの表示をイネーブルにしたりできます。

ステップ 3　[General] タブでは、次の項目を指定します。

a. [Warn that configuration in ASDM is out of sync with the configuration in ASA] チェックボックスをオンにし、スタートアップ コンフィギュレーションと実行コンフィギュレーションが同期していないときは通知するように設定します。

b. 起動時に read-only ユーザに対して次のメッセージを表示するには、[Show configuration restriction message to read-only user] チェックボックスをオンにします。このオプションは、デフォルトでオンです。

```
"You are not allowed to modify the ASA configuration, because you do not have
sufficient privileges."
```

c. ASDM を閉じるときに終了を確認するプロンプトが表示されるようにするには、[Confirm before exiting ASDM] チェックボックスをオンにします。このオプションは、デフォルトでオンです。

d. スクリーン リーダーをイネーブルにするには、[Enable screen reader support (requires ASDM restart)] チェックボックスをオンにします。このオプションをイネーブルにするには、ASDM を再起動する必要があります。

e. ASA メモリの最小空き容量が、ASDM アプリケーションの完全な機能を実行するには不十分である場合に通知を受信するには、[Warn of insufficient ASA memory when ASDM loads] チェックボックスをオンにします。ASDM は、起動時にテキスト バナー メッセージにメモリ警告を表示し、ASDM のタイトル バー テキストにメッセージを表示し、24 時間ごとに syslog アラートを送信します。

f. ASDM によって生成される CLI コマンドを表示するには、[Preview commands before sending them to the device] チェックボックスをオンにします。

g. ASA に複数のコマンドを 1 つのグループとして送信するには、[Enable cumulative (batch) CLI delivery] チェックボックスをオンにします。

h. タイムアウト メッセージ送信設定の最短時間を秒単位で入力します。デフォルトは 60 秒です。

i. **Packet Capture Wizard** で、キャプチャされたパケットが表示されるようにするには、ネットワーク スニファ アプリケーションの名前を入力するか、または [Browse] をクリックしてファイル システム内で指定します。

ステップ 4　[Rules Table] タブで、次の項目を指定します。

a. [Display settings] では、[Rules] テーブルでのルールの表示方法を変更できます。

- Auto-Expand Prefix 設定に基づいて自動展開されたネットワークおよびサービス オブジェクト グループを表示するには、[Auto-expand network and service object groups with specified prefix] チェックボックスをオンにします。
- [Auto-Expand Prefix] フィールドに、表示するときに自動的に展開するネットワークおよびサービス オブジェクト グループのプレフィックスを入力します。
- ネットワークおよびサービス オブジェクト グループのメンバーとそのグループ名を [Rules] テーブルに表示するには、[Show members of network and service object groups] チェックボックスをオンにします。チェックボックスがオフの場合は、グループ名だけが表示されます。
- [Limit Members To] フィールドに、表示するネットワークおよびサービス オブジェクト グループの数を入力します。オブジェクト グループ メンバが表示されるときには、最初の ***n*** 個のメンバだけが表示されます。
- [Rules] テーブルにすべてのアクションを表示するには、[Show all actions for service policy rules] チェックボックスをオンにします。オフの場合は、サマリーが表示されます。

b. [Deployment Settings] では、[Rules] テーブルに変更内容を適用するときの ASA の動作を設定できます。

- 新しいアクセス リストを適用するときに NAT テーブルをクリアするには、[Issue “clear xlate” command when deploying access lists] チェックボックスをオンにします。この設定により、ASA で設定されるアクセス リストが、すべての変換アドレスに対して確実に適用されるようにします。

c. [Access Rule Hit Count Settings] では、[Access Rules] テーブルのヒット数をアップデートする頻度を設定できます。ヒット数は、明示的なルールにだけ適用されます。暗黙的なルールのヒット数は、[Access Rules] テーブルには表示されません。

- [Access Rules] テーブルでヒット数が自動的にアップデートされるようにするには、[Update access rule hit counts automatically] チェックボックスをオンにします。
- [Access Rules] テーブルに、ヒット数カラムを更新する頻度を秒単位で指定します。有効値の範囲は 10 ～ 86400 秒です。

ステップ 5　[Syslogl] タブでは、次の項目を指定します。

- [Syslog Colors] 領域では、重大度レベルごとに背景色と前景色を設定し、メッセージ表示をカスタマイズできます。[Severity] カラムには、各重大度レベルが名前および番号ごとに表示されます。各重大度レベルでメッセージの背景色または前景色を変更するには、対応するカラムをクリックします。[Pick a Color] ダイアログボックスが表示されます。次のいずれかのタブをクリックします。
  - [Swatches] タブでパレットから色を選択し、[OK] をクリックします。
  - [HSB] タブで H、S、B の設定を指定し、[OK] をクリックします。
  - [RGB] タブで赤、緑、青の設定を指定し、[OK] をクリックします。
- 冗長な syslog メッセージをディセーブルにするよう警告するメッセージの表示をイネーブルにするには、[NetFlow] 領域で [Warn to disable redundant syslog messages when NetFlow action is first applied to the global service policy rule] チェックボックスをオンにします。

ステップ 6　これら 3 つのタブの設定を指定した後で、[OK] をクリックして設定を保存し、[Preferences] ダイアログボックスを閉じます。

（注）　プリファレンス設定をオンまたはオフにするたびに、変更内容は .conf ファイルに保存され、その時点でワークステーション上で実行中のその他の ASDM セッションから利用できるようになります。すべての変更を有効にするには、ASDM を再起動する必要があります。

ASDM Assistant での検索

ASDM Assistant ツールでは、タスクに応じた ASDM の使用方法のヘルプを検索し、表示できます。

情報にアクセスするには、[View] > [ASDM Assistant] > [How Do I?] を選択するか、メニューバーの [Look For] フィールドに検索要求を入力します。[Find] ドロップダウン リストから [How Do I?] を選択して検索を開始します。

（注）　この機能は、PIX セキュリティ アプライアンスでは使用できません。

ASDM Assistant を表示するには、次の手順を実行します。

ステップ 1　[View] > [ASDM Assistant] を選択します。

[ASDM Assistant] ペインが表示されます。

ステップ 2　[Search] フィールドに検索する情報を入力して [**Go**] をクリックします。

要求された情報が [Search Results] ペインに表示されます。

ステップ 3　[Search Results] セクションおよび [Features] セクションに表示される任意のリンクをクリックし、詳細情報を入手します。

履歴メトリックのイネーブル化

[Configuration] > [Device Management] > [Advanced] > [History Metrics] ペインでは、さまざまな統計情報の履歴を保存するように ASA を設定し、ASDM を使用してグラフやテーブルで表示できます。履歴メトリックをイネーブルにしない場合、監視できるのはリアルタイムの統計情報だけです。履歴メトリックをイネーブルにすると、直前の 10 分間、60 分間、12 時間、5 日間の統計グラフを表示できます。

履歴メトリックを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Advanced] > [History Metrics] を選択します。

[History Metrics] ペインが表示されます。

ステップ 2　[ASDM History Metrics] チェックボックスをオンにして履歴メトリックをイネーブルにし、[Apply] をクリックします。

サポートされていないコマンド

ASA で使用可能なコマンドはほとんどすべて ASDM でサポートされますが、既存のコンフィギュレーションのコマンドの一部は ASDM で無視される場合があります。これらのコマンドのほとんどはコンフィギュレーションに残すことができます。詳細については、[Tools] > [Show Commands Ignored by ASDM on Device] を参照してください。

無視される表示専用コマンド

表 3-5 には、CLI で追加した場合に ASDM のコンフィギュレーションでサポートしているものの、ASDM で追加または編集ができないコマンドのリストが表示されています。ASDM で無視されるコマンドは ASDM の GUI に一切表示されません。表示専用コマンドは GUI に表示されますが、編集はできません。

表 3-5　サポート対象外のコマンド リスト

サポートされていないコマンド	ASDM の動作
capture	無視されます。
coredump	無視されます。これは、CLI を使用してのみ設定できます。
crypto engine large-mod-accel	無視されます。
dhcp-server（トンネル グループ名一般属性）	ASDM では、すべての DHCP サーバに対して 1 つの設定のみが許可されます。
eject	サポート対象外
established	無視されます。
failover timeout	無視されます。
fips	無視されます。
nat-assigned-to-public-ip	無視されます。
pager	無視されます。
pim accept-register route-map	無視されます。ASDM では **list** オプションだけ設定可。

service-policy global	**match access-list** クラスで使用されている場合は無視。次に例を示します。
	`access-list myacl extended permit ip any any`
	`class-map mycm`
	`  match access-list myacl`
	`policy-map mypm`
	`  class mycm`
	`  inspect ftp`
	`service-policy mypm global`

set metric	無視されます。
sysopt nodnsalias	無視されます。

表 3-5　サポート対象外のコマンド リスト （続き）

サポートされていないコマンド	ASDM の動作
sysopt uauth allow-http-cache	無視されます。
terminal	無視されます。
threat-detection rate	無視されます。

サポート対象外のコマンドによる影響

既存の実行コンフィギュレーションを ASDM にロードした場合、そこにサポート対象外のコマンドがあっても、ASDM の操作には影響しません。サポート対象外のコマンドを表示するには、[Tools] > [Show Commands Ignored by ASDM on Device] を選択します。

サポート対象外の連続していないサブネット マスク

ASDM では、255.255.0.255 のように連続していないサブネット マスクはサポートされていません。たとえば、次は使用できません。

```
ip address inside 192.168.2.1 255.255.0.255
```

ASDM CLI ツールでサポートされていないインタラクティブ ユーザ コマンド

ASDM CLI ツールは、インタラクティブ ユーザ コマンドをサポートしていません。インタラクティブな確認を必要とする CLI コマンドを入力すると、「[yes/no]」の入力を要求するプロンプトが表示されますが、入力内容は認識されません。続いて ASDM は、応答の待機をタイムアウトします。

次に例を示します。

1. [Tools] > [Command Line Interface] を選択します。
2. **crypto key generate rsa** コマンドを入力します。

   デフォルトの 1024 ビット RSA キーが生成されます。
3. **crypto key generate rsa** コマンドを再度入力します。

   以前の RSA キーを上書きして再生成するのではなく、次のエラーが表示されます。

```
Do you really want to replace them?[yes/no]:WARNING: You already have RSA
ke0000000000000$A key
Input line must be less than 16 characters in length.

%Please answer 'yes' or 'no'.
Do you really want to replace them [yes/no]:

%ERROR: Timed out waiting for a response.
ERROR: Failed to create new RSA keys names <Default-RSA-key>
```

回避策：

- [ASDM] ペインから、ユーザ介入が必要なほとんどのコマンドを設定できます。
- **noconfirm** オプションがある CLI コマンドについては、CLI コマンド入力時にこのオプションを使用します。次に例を示します。

  ```
  crypto key generate rsa noconfirm
  ```

機能ライセンス

ライセンスでは、特定の Cisco ASA 上でイネーブルにするオプションを指定します。このマニュアルでは、ライセンス アクティベーション キーの取得方法とアクティベーションの方法について説明します。また、各モデルに使用できるライセンスについても説明します。

（注） この章では、バージョン 9.3 のライセンシングについて説明します。その他のバージョンについては、次の URL でお使いのバージョンに該当するライセンシング マニュアルを参照してください。

http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-licensing-information-listing.html

モデルごとにサポートされている機能のライセンス

この項では、各モデルに使用できるライセンスと、ライセンスに関する特記事項について説明します。

モデルごとのライセンス

この項では、各モデルに使用できる機能のライセンスを示します。

- 「ASA 5525-X」（P.4-5）
- 「ASA 5545-X」（P.4-6）
- 「ASA 5555-X」（P.4-7）
- 「ASA 5585-X（SSP-10）」（P.4-8）
- 「ASA 5585-X（SSP-20）」（P.4-9）
- 「ASA 5585-X（SSP-40 および -60）」（P.4-10）
- 「ASA サービス モジュール」（P.4-11）
- 「ASAv（仮想 CPU × 1 を搭載）」（P.4-12）
- 「ASAv（仮想 CPU × 4 を搭載）」（P.4-13）

*イタリック体*で示された項目は、基本ライセンス（または Security Plus など）ライセンス バージョンを置換できる個別のオプション ライセンスです。ライセンスは組み合わせることができます。たとえば、24 ユニファイド コミュニケーション ライセンスと Strong Encryption ライセンス、500 AnyConnect Premium ライセンスと GTP/GPRS ライセンス、または 4 つのライセンスをすべて同時に使用することができます。

（注）一部の機能は互換性がありません。互換性情報については、個々の機能の章を参照してください。

ペイロード暗号化機能のないモデルの場合は、次に示す機能の一部がサポートされません。サポートされない機能のリストについては、「ペイロード暗号化機能のないモデル」（P.4-30）を参照してください。

ライセンスの詳細については、「ライセンスの注釈」（P.4-14）を参照してください。

ASA 5512-X

表 4-1　ASA 5512-X ライセンスの機能

ライセンス	基本ライセンス						Security Plus ライセンス					
ファイアウォール ライセンス												
Botnet Traffic Filter	ディセーブル	*オプションの時間ベース ライセンス：使用可能*					ディセーブル	*オプションの時間ベース ライセンス：使用可能*				
ファイアウォールの接続、同時	100,000						250,000					
GTP/GPRS	サポートなし						ディセーブル	*オプション ライセンス：使用可能*				
Intercompany Media Engine	ディセーブル	*オプション ライセンス：使用可能*					ディセーブル	*オプション ライセンス：使用可能*				
UC Phone 代理権限セッション、総 UC 代理権限セッション	2	*オプション ライセンス：*					2	*オプション ライセンス：*				
		24	*50*	*100*	*250*	*500*		*24*	*50*	*100*	*250*	*500*
VPN ライセンス												
Adv.Endpoint Assessment	ディセーブル	*オプション ライセンス：使用可能*					ディセーブル	*オプション ライセンス：使用可能*				

表 4-1　ASA 5512-X ライセンスの機能 （続き）

ライセンス	基本ライセンス					Security Plus ライセンス				
Cisco VPN Phone 用の AnyConnect	ディセーブル	*オプション ライセンス：使用可能*				ディセーブル	*オプション ライセンス：使用可能*			
AnyConnect Essentials	ディセーブル	*オプション ライセンス：使用可能（250 セッション）*				ディセーブル	*オプション ライセンス：使用可能（250 セッション）*			
AnyConnect for Mobile	ディセーブル	*オプション ライセンス：使用可能*				ディセーブル	*オプション ライセンス：使用可能*			
AnyConnect Premium（セッション）	2	*オプション永続ライセンス*				2	*オプション永続ライセンス*			
		10	*25*	*50*	*100*		*10*	*25*	*50*	*100*
		オプションの時間ベース（VPN Flex ライセンス）：			*250*		*オプションの時間ベース（VPN Flex ライセンス）：*			*250*
	オプションの共有ライセンス：Participant または Server。サーバの場合:					*オプションの共有ライセンス：Participant または Server。サーバの場合:*				
	500 ～ 50,000（500 単位で増加）		*50,000 ～ 545,000（1000 単位で増加）*			*500 ～ 50,000（500 単位で増加）*		*50,000 ～ 545,000（1000 単位で増加）*		
合計 VPN（セッション）。全タイプの合計	250					250				
他の VPN（セッション）	250					250				
VPN ロード バランシング	サポートなし					サポートあり				
一般ライセンス										
暗号化	基本（DES）	*オプション ライセンス：強化（3DES/AES）*				基本（DES）	*オプション ライセンス：強化（3DES/AES）*			
フェールオーバー	サポートなし					アクティブ/スタンバイまたはアクティブ/アクティブ				
全タイプのインターフェイス、最大。	716					916				
セキュリティ コンテキスト	サポートなし					2	*オプション ライセンス：*			*5*
クラスタリング	サポートなし					2				
IPS モジュール	ディセーブル	*オプション ライセンス：使用可能*				ディセーブル	*オプション ライセンス：使用可能*			
VLAN、最大	50					100				

ASA 5515-X

表 4-2　ASA 5515-X ライセンスの機能

ライセンス	基本ライセンス						
ファイアウォール ライセンス							
Botnet Traffic Filter	ディセーブル	*オプションの時間ベース ライセンス：使用可能*					
ファイアウォールの接続、同時	250,000						
GTP/GPRS	ディセーブル	*オプション ライセンス：使用可能*					
Intercompany Media Engine	ディセーブル	*オプション ライセンス：使用可能*					
UC Phone 代理権限セッション、総 UC 代理権限セッション	2	*オプション ライセンス：*	*24*	*50*	*100*	*250*	*500*
VPN ライセンス							
Adv.Endpoint Assessment	ディセーブル	*オプション ライセンス：使用可能*					
Cisco VPN Phone 用の AnyConnect	ディセーブル	*オプション ライセンス：使用可能*					
AnyConnect Essentials	ディセーブル	*オプション ライセンス：使用可能（250 セッション）*					
AnyConnect for Mobile	ディセーブル	*オプション ライセンス：使用可能*					
AnyConnect Premium（セッション）	2	*オプションの永続ライセンス：*					
		10	*25*	*50*	*100*	*250*	
		オプションの時間ベース（VPN Flex ライセンス）：	*250*				
	オプションの共有ライセンス：Participant または Server。サーバの場合:						
	500 ～ 50,000（500 単位で増加）				*50,000 ～ 545,000（1000 単位で増加）*		
合計 VPN（セッション）。全タイプの合計	250						
他の VPN（セッション）	250						
VPN ロード バランシング	サポートあり						
一般ライセンス							
暗号化	基本（DES）	*オプション ライセンス：強化（3DES/AES）*					
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ						
全タイプのインターフェイス、最大。	916						
セキュリティ コンテキスト	2	*オプション ライセンス：*	*5*				
クラスタリング	2						
IPS モジュール	ディセーブル	*オプション ライセンス：使用可能*					
VLAN、最大	100						

ASA 5525-X

表 4-3　ASA 5525-X ライセンスの機能

ライセンス	基本ライセンス								
ファイアウォール ライセンス									
Botnet Traffic Filter	ディセーブル	*オプションの時間ベース ライセンス：使用可能*							
ファイアウォールの接続、同時	500,000								
GTP/GPRS	ディセーブル	*オプション ライセンス：使用可能*							
Intercompany Media Engine	ディセーブル	*オプション ライセンス：使用可能*							
UC Phone 代理権限セッション、総 UC 代理権限セッション	2	*オプション ライセンス：*	*24*	*50*	*100*	*250*	*500*	*750*	*1000*
VPN ライセンス									
Adv.Endpoint Assessment	ディセーブル	*オプション ライセンス：使用可能*							
Cisco VPN Phone 用の AnyConnect	ディセーブル	*オプション ライセンス：使用可能*							
AnyConnect Essentials	ディセーブル	*オプション ライセンス：使用可能（750 セッション）*							
AnyConnect for Mobile	ディセーブル	*オプション ライセンス：使用可能*							
AnyConnect Premium（セッション）	2	*オプションの永続ライセンス：*							
		10	*25*	*50*	*100*	*250*	*500*	*750*	
		オプションの時間ベース（VPN Flex ライセンス）：						*750*	
	オプションの共有ライセンス：Participant または Server。サーバの場合:								
	500 ～ 50,000（500 単位で増加）					*50,000 ～ 545,000（1000 単位で増加）*			
合計 VPN（セッション）。全タイプの合計	750								
他の VPN（セッション）	750								
VPN ロード バランシング	サポートあり								
一般ライセンス									
暗号化	基本（DES）	*オプション ライセンス：強化（3DES/AES）*							
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ								
全タイプのインターフェイス、最大。	1316								
セキュリティ コンテキスト	2	*オプション ライセンス：*	*5*	*10*	*20*				
クラスタリング	2								
IPS モジュール	ディセーブル	*オプション ライセンス：使用可能*							
VLAN、最大	200								

ASA 5545-X

表 4-4　ASA 5545-X ライセンスの機能

ライセンス	基本ライセンス									
ファイアウォール ライセンス										
Botnet Traffic Filter	ディセーブル	*オプションの時間ベース ライセンス：使用可能*								
ファイアウォールの接続、同時	750,000									
GTP/GPRS	ディセーブル	*オプション ライセンス：使用可能*								
Intercompany Media Engine	ディセーブル	*オプション ライセンス：使用可能*								
UC Phone 代理権限セッション、総 UC 代理権限セッション	2	*オプション ライセンス：*	*24*	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*
VPN ライセンス										
Adv.Endpoint Assessment	ディセーブル	*オプション ライセンス：使用可能*								
Cisco VPN Phone 用の AnyConnect	ディセーブル	*オプション ライセンス：使用可能*								
AnyConnect Essentials	ディセーブル	*オプション ライセンス：使用可能（2500 セッション）*								
AnyConnect for Mobile	ディセーブル	*オプション ライセンス：使用可能*								
AnyConnect Premium（セッション）	2	*オプションの永続ライセンス：*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*
		オプションの時間ベース（VPN Flex ライセンス）：								*2500*
	オプションの共有ライセンス：Participant または Server。サーバの場合:									
	500 ～ 50,000（500 単位で増加）					*50,000 ～ 545,000（1000 単位で増加）*				
合計 VPN（セッション）。全タイプの合計	2500									
他の VPN（セッション）	2500									
VPN ロード バランシング	サポートあり									
一般ライセンス										
暗号化	基本（DES）	*オプション ライセンス：強化（3DES/AES）*								
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ									
全タイプのインターフェイス、最大。	1716									
セキュリティ コンテキスト	2	*オプション ライセンス：*	*5*	*10*	*20*	*50*				
クラスタリング	2									
IPS モジュール	ディセーブル	*オプション ライセンス：使用可能*								
VLAN、最大	300									

ASA 5555-X

表 4-5　ASA 5555-X ライセンスの機能

ライセンス	基本ライセンス									
ファイアウォール ライセンス										
Botnet Traffic Filter	ディセーブル	*オプションの時間ベース ライセンス：使用可能*								
ファイアウォールの接続、同時	1,000,000									
GTP/GPRS	ディセーブル	*オプション ライセンス：使用可能*								
Intercompany Media Engine	ディセーブル	*オプション ライセンス：使用可能*								
UC Phone 代理権限セッション、総 UC 代理権限セッション	2	*オプション ライセンス：*								
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN ライセンス										
Adv.Endpoint Assessment	ディセーブル	*オプション ライセンス：使用可能*								
Cisco VPN Phone 用の AnyConnect	ディセーブル	*オプション ライセンス：使用可能*								
AnyConnect Essentials	ディセーブル	*オプション ライセンス：使用可能（5000 セッション）*								
AnyConnect for Mobile	ディセーブル	*オプション ライセンス：使用可能*								
AnyConnect Premium（セッション）	2	*オプションの永続ライセンス：*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*
		オプションの時間ベース（VPN Flex ライセンス）：								*5000*
	オプションの共有ライセンス：Participant または Server。サーバの場合:									
	500 ～ 50,000（500 単位で増加）					*50,000 ～ 545,000（1000 単位で増加）*				
合計 VPN（セッション）。全タイプの合計	5000									
他の VPN（セッション）	5000									
VPN ロード バランシング	サポートあり									
一般ライセンス										
暗号化	基本（DES）	*オプション ライセンス：強化（3DES/AES）*								
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ									
全タイプのインターフェイス、最大。	2516									
セキュリティ コンテキスト	2	*オプション ライセンス：*			*5*	*10*	*20*	*50*	*100*	
クラスタリング	2									
IPS モジュール	ディセーブル	*オプション ライセンス：使用可能*								
VLAN、最大	500									

ASA 5585-X（SSP-10）

同一のシャーシで同じレベルの 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-10 と SSP-20 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。

表 4-6　ASA 5585-X（SSP-10）ライセンスの機能

ライセンス	基本ライセンスと Security Plus ライセンス									
ファイアウォール ライセンス										
Botnet Traffic Filter	ディセーブル	*オプションの時間ベース ライセンス：使用可能*								
ファイアウォールの接続、同時	1,000,000									
GTP/GPRS	ディセーブル	*オプション ライセンス：使用可能*								
Intercompany Media Engine	ディセーブル	*オプション ライセンス：使用可能*								
UC Phone 代理権限セッション、総 UC 代理権限セッション	2	*オプション ライセンス：*								
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN ライセンス										
Adv.Endpoint Assessment	ディセーブル	*オプション ライセンス：使用可能*								
Cisco VPN Phone 用の AnyConnect	ディセーブル	*オプション ライセンス：使用可能*								
AnyConnect Essentials	ディセーブル	*オプション ライセンス：使用可能（5000 セッション）*								
AnyConnect for Mobile	ディセーブル	*オプション ライセンス：使用可能*								
AnyConnect Premium（セッション）	2	*オプションの永続ライセンス：*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*
		オプションの時間ベース（VPN Flex ライセンス）：								*5000*
	オプションの共有ライセンス：Participant または Server。サーバの場合:									
	500 ～ 50,000（500 単位で増加）					*50,000 ～ 545,000（1000 単位で増加）*				
合計 VPN（セッション）。全タイプの合計	5000									
他の VPN（セッション）	5000									
VPN ロード バランシング	サポートあり									
一般ライセンス										
10 GE I/O	**基本ライセンス**：ディセーブル。ファイバ ifcs は 1 GE で動作します					**Security Plus ライセンス**：イネーブル。ファイバ ifcs は 10 GE で動作します				
暗号化	基本（DES）	*オプション ライセンス：強化（3DES/AES）*								
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ									
全タイプのインターフェイス、最大。	4612									
セキュリティ コンテキスト	2	*オプション ライセンス：*		*5*	*10*	*20*	*50*	*100*		
クラスタリング	ディセーブル	*オプション ライセンス: 16 単位で利用可能*								
VLAN、最大	1024									

ASA 5585-X（SSP-20）

同一のシャーシで同じレベルの 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-20 と SSP-40 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。

表 4-7　ASA 5585-X（SSP-20）ライセンスの機能

ライセンス	基本ライセンスと Security Plus ライセンス										
ファイアウォール ライセンス											
Botnet Traffic Filter	ディセーブル	*オプションの時間ベース ライセンス：使用可能*									
ファイアウォールの接続、同時	2,000,000										
GTP/GPRS	ディセーブル	*オプション ライセンス：使用可能*									
Intercompany Media Engine	ディセーブル	*オプション ライセンス：使用可能*									
UC Phone 代理権限セッション、総 UC 代理権限セッション	2	*オプション ライセンス：*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN ライセンス											
Adv.Endpoint Assessment	ディセーブル	*オプション ライセンス：使用可能*									
Cisco VPN Phone 用の AnyConnect	ディセーブル	*オプション ライセンス：使用可能*									
AnyConnect Essentials	ディセーブル	*オプション ライセンス：使用可能（10,000 セッション）*									
AnyConnect for Mobile	ディセーブル	*オプション ライセンス：使用可能*									
AnyConnect Premium（セッション）	2	*オプションの永続ライセンス：*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*	*10,000*
		オプションの時間ベース（VPN Flex ライセンス）：										*10,000*
	オプションの共有ライセンス：Participant または Server。サーバの場合:										
	500 ～ 50,000（500 単位で増加）					*50,000 ～ 545,000（1000 単位で増加）*					
合計 VPN（セッション）。全タイプの合計	10,000										
他の VPN（セッション）	10,000										
VPN ロード バランシング	サポートあり										
一般ライセンス											
10 GE I/O	**基本ライセンス**：ディセーブル。ファイバ ifcs は 1 GE で動作します					**Security Plus ライセンス**：イネーブル。ファイバ ifcs は 10 GE で動作します					
暗号化	基本（DES）	*オプション ライセンス：強化（3DES/AES）*									
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ										
全タイプのインターフェイス、最大。	4612										
セキュリティ コンテキスト	2	*オプション ライセンス：*		*5*	*10*	*20*	*50*	*100*	*250*		
クラスタリング	ディセーブル	*オプション ライセンス: 16 単位で利用可能*									
VLAN、最大	1024										

1. 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシ セッションの最大数は 5000 です。

ASA 5585-X（SSP-40 および -60）

同一のシャーシで同じレベルの 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-40 と SSP-60 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。

表 4-8　ASA 5585-X（SSP-40 および -60）ライセンスの機能

ライセンス	基本ライセンス											
ファイアウォール ライセンス												
Botnet Traffic Filter	ディセーブル	*オプションの時間ベース ライセンス：使用可能*										
ファイアウォールの接続、同時	**5585-X（SSP-40）**：4,000,000					**5585-X（SSP-60）**：10,000,000						
GTP/GPRS	ディセーブル	*オプション ライセンス：使用可能*										
Intercompany Media Engine	ディセーブル	*オプション ライセンス：使用可能*										
UC Phone 代理権限セッション、総 UC 代理権限セッション	2	*オプション ライセンス：*										
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN ライセンス												
Adv.Endpoint Assessment	ディセーブル	*オプション ライセンス：使用可能*										
Cisco VPN Phone 用の AnyConnect	ディセーブル	*オプション ライセンス：使用可能*										
AnyConnect Essentials	ディセーブル	*オプション ライセンス：使用可能（10,000 セッション）*										
AnyConnect for Mobile	ディセーブル	*オプション ライセンス：使用可能*										
AnyConnect Premium（セッション）	2	*オプションの永続ライセンス：*										
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*	*10,000*
		オプションの時間ベース（VPN Flex ライセンス）：										*10,000*
	オプションの共有ライセンス：Participant または Server。サーバの場合:											
	500 ～ 50,000（500 単位で増加）					*50,000 ～ 545,000（1000 単位で増加）*						
合計 VPN（セッション）。全タイプの合計	10,000											
他の VPN（セッション）	10,000											
VPN ロード バランシング	サポートあり											
一般ライセンス												
10 GE I/O	イネーブル。ファイバ インターフェイスは 10 GE で動作											
暗号化	基本（DES）	*オプション ライセンス：強化（3DES/AES）*										
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ											
全タイプのインターフェイス、最大。	4612											
セキュリティ コンテキスト	2	*オプション ライセンス：*		*5*	*10*	*20*	*50*	*100*	*250*			
クラスタリング	ディセーブル	*オプション ライセンス: 16 単位で利用可能*										
VLAN、最大	1024											

1. 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシ セッションの最大数は 5000 です。

ASA サービス モジュール

表 4-9　ASASM ライセンス機能

ライセンス	基本ライセンス										
ファイアウォール ライセンス											
Botnet Traffic Filter	ディセーブル	*オプションの時間ベース ライセンス：使用可能*									
ファイアウォールの接続、同時	10,000,000										
GTP/GPRS	ディセーブル	*オプション ライセンス：使用可能*									
Intercompany Media Engine	ディセーブル	*オプション ライセンス：使用可能*									
UC Phone 代理権限セッション、総 UC 代理権限セッション	2	*オプション ライセンス：*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN ライセンス											
Adv.Endpoint Assessment	ディセーブル	*オプション ライセンス：使用可能*									
Cisco VPN Phone 用の AnyConnect	ディセーブル	*オプション ライセンス：使用可能*									
AnyConnect Essentials	ディセーブル	*オプション ライセンス：使用可能（10,000 セッション）*									
AnyConnect for Mobile	ディセーブル	*オプション ライセンス：使用可能*									
AnyConnect Premium（セッション）	2	*オプションの永続ライセンス：*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*	*10,000*
		オプションの時間ベース（VPN Flex ライセンス）：										*10,000*
	オプションの共有ライセンス：Participant または Server。サーバの場合:										
	500 ～ 50,000（500 単位で増加）					*50,000 ～ 545,000（1000 単位で増加）*					
合計 VPN（セッション）。全タイプの合計	10,000										
他の VPN（セッション）	10,000										
VPN ロード バランシング	サポートあり										
一般ライセンス											
暗号化	基本（DES）	*オプション ライセンス：強化（3DES/AES）*									
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ										
セキュリティ コンテキスト	2	*オプション ライセンス：*									
		5	*10*	*20*	*50*	*100*	*250*				
クラスタリング	サポートなし										
VLAN、最大	1000										

1. 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシ セッションの最大数は 5000 です。

ASAv（仮想 CPU × 1 を搭載）

表 4-10　1 つの vCPU ライセンスを持つ ASAv の機能

ライセンス	標準および Premium ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートあり	
ファイアウォールの接続、同時	100,000	
GTP/GPRS	サポートあり	
Intercompany Media Engine	サポートあり	
UC Phone 代理権限セッション、総 UC 代理権限セッション	250	
VPN ライセンス		
Adv.Endpoint Assessment	**標準ライセンス**：サポートなし	**Premium ライセンス**：サポートあり
AnyConnect Essentials	**標準ライセンス**：サポートなし	**Premium** ライセンス：サポートなし
Cisco VPN Phone 用の AnyConnect	**標準ライセンス**：サポートなし	**Premium ライセンス**：サポートあり
AnyConnect for Mobile	**標準ライセンス**：サポートなし	**Premium ライセンス**：サポートあり
AnyConnect Premium（セッション）	**標準ライセンス**：2	**Premium ライセンス**：250
	共有ライセンス：サポートなし	
合計 VPN（セッション）。全タイプの合計	250	
他の VPN（セッション）	250	
VPN ロード バランシング	サポートあり	
一般ライセンス		
暗号化	強化（3DES/AES）	
フェールオーバー	アクティブ/スタンバイ	
全タイプのインターフェイス、最大。	716	
セキュリティ コンテキスト	サポートなし	
クラスタリング	サポートなし	
VLAN、最大	50	
RAM、vCPU 周波数限界	2 GB、5000 MHz	

ASAv（仮想 CPU × 4 を搭載）

表 4-11　4 つの vCPU ライセンスを持つ ASAv の機能

ライセンス	標準および Premium ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートあり	
ファイアウォールの接続、同時	500,000	
GTP/GPRS	サポートあり	
Intercompany Media Engine	サポートあり	
UC Phone 代理権限セッション、総 UC 代理権限セッション	1000	
VPN ライセンス		
Adv.Endpoint Assessment	**標準ライセンス**：サポートなし	**Premium ライセンス**：サポートあり
AnyConnect Essentials	**標準ライセンス**：サポートなし	**Premium** ライセンス：サポートなし
Cisco VPN Phone 用の AnyConnect	**標準ライセンス**：サポートなし	**Premium ライセンス**：サポートあり
AnyConnect for Mobile	**標準ライセンス**：サポートなし	**Premium ライセンス**：サポートあり
AnyConnect Premium（セッション）	**標準ライセンス**：2	**Premium ライセンス**：750
	共有ライセンス：サポートなし	
合計 VPN（セッション）。全タイプの合計	750	
他の VPN（セッション）	750	
VPN ロード バランシング	サポートあり	
一般ライセンス		
暗号化	強化（3DES/AES）	
フェールオーバー	アクティブ/スタンバイ	
全タイプのインターフェイス、最大。	1316	
セキュリティ コンテキスト	サポートなし	
クラスタ	サポートなし	
VLAN、最大	200	
RAM、vCPU 周波数限界	8 GB、20000 MHz **（注）** 4 つの vCPU ライセンスを適用するが 2 つまたは 3 つの vCPU を導入する場合は、次の値を参照してください。 2 つの仮想 CPU：4 GB の RAM、10000 MHz の vCPU 周波数限界、250,000 の同時ファイアウォール接続。 3 つの仮想 CPU：4 GB の RAM、15000 MHz の vCPU 周波数限界、350,000 の同時ファイアウォール接続。	

ライセンスの注釈

表 4-12 に、「モデルごとのライセンス」（P.4-1）の複数の表で共有される一般的な補足説明を示します。

表 4-12　ライセンスの注釈

ライセンス	注意
AnyConnect Essentials	AnyConnect Essentials セッションには、次の VPN タイプが含まれています。 • SSL VPN • IKEv2 を使用した IPsec リモート アクセス このライセンスは、ブラウザベース（クライアントレス）の SSL VPN アクセスまたは Cisco Secure Desktop はサポートしていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。 **（注）** AnyConnect Essentials ライセンスを所有する VPN ユーザは、Web ブラウザを使用してログインし、AnyConnect クライアントをダウンロードおよび起動（WebLaunch）することができます。 このライセンスと AnyConnect Premium ライセンスのいずれでイネーブル化されたかには関係なく、AnyConnect クライアント ソフトウェアには同じクライアント機能のセットが装備されています。 特定の ASA では、AnyConnect Premium ライセンス（全タイプ）または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。 デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、**webvpn** を使用し、次に **no anyconnect-essentials** コマンドまたは ASDM で [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Essentials] ペインを使用することで、AnyConnect Essentials ライセンスをディセーブルにして他のライセンスを使用できます。 「VPN ライセンスと機能の互換性」（P.4-19）も参照してください。
Cisco VPN Phone 用の AnyConnect	このライセンスを AnyConnect Premium ライセンスとともに使用すると、AnyConnect の互換性に組み込まれているハードウェア IP 電話からアクセスできます。

表 4-12　ライセンスの注釈（続き）

ライセンス	注意
AnyConnect for Mobile	このライセンスは、Windows Mobile 5.0、6.0、および 6.1 を実行しているタッチスクリーン モバイル デバイスでの AnyConnect クライアントへのアクセスを提供します。AnyConnect 2.3 以降のバージョンへのモバイル アクセスをサポートする場合は、このライセンスを使用することをお勧めします。このライセンスを使用する場合は、AnyConnect Essentials または AnyConnect Premium のいずれかのライセンスをアクティブにする必要があります。これは、許可される SSL VPN セッションの合計数を指定するためです。 **Mobile Posture サポート** リモート アクセス コントロールを適用し、モバイル デバイスからポスチャ データを収集するには、AnyConnect Mobile ライセンスと、AnyConnect Essentials または AnyConnect Premium ライセンスのいずれかが ASA にインストールされている必要があります。インストールしたライセンスに基づいて、次の機能を使用できます。 • AnyConnect Premium ライセンス機能 – DAP 属性およびその他の既存のエンドポイント属性に基づいて、サポート対象モバイル デバイスに DAP ポリシーを適用します。これには、モバイル デバイスからのリモート アクセスの許可または拒否が含まれます。 • AnyConnect Essentials ライセンス機能 – モバイル デバイス アクセスをグループ単位でイネーブルまたはディセーブルにします。この機能を、ASDM を使用して設定します。 – CLI または ASDM を使用して接続モバイル デバイスに関する情報を表示します（ただし、DAP ポリシーを適用したり、これらのモバイル デバイスへのリモート アクセスを拒否/許可したりする機能はありません）。
AnyConnect Premium	AnyConnect Premium セッションには、次の VPN タイプが含まれています。 • SSL VPN • クライアントレス SSL VPN • IKEv2 を使用した IPsec リモート アクセス
AnyConnect Premium Shared	共有ライセンスによって、ASA は複数のクライアントの ASA の共有ライセンス サーバとして機能します。共有ライセンス プールは大規模ですが、個々の ASA によって使用されるセッションの最大数は、永続的なライセンスで指定される最大数を超えることはできません。
Botnet Traffic Filter	ダイナミック データベースをダウンロードするには、強力な暗号化（3DES/AES）ライセンスが必要です。
暗号化	DES ライセンスはディセーブルにできません。3DES ライセンスをインストールしている場合、DES は引き続き使用できます。強力な暗号化だけを使用したい場合に DES の使用を防止するには、強力な暗号化だけを使用するようにすべての関連コマンドを設定する必要があります。

表 4-12　ライセンスの注釈（続き）

ライセンス	注意
Intercompany Media Engine	Intercompany Media Engine（IME）ライセンスをイネーブルにすると、TLS プロキシセッションを設定された TLS プロキシの制限まで使用できます。また、Unified Communications（UC; ユニファイド コミュニケーション）ライセンスがインストールされており、その制限数がデフォルトの TLS プロキシの制限数より多い場合、お使いのモデルに応じて、ASA が UC ライセンスの制限数にまでセッション数を加えた制限を設定します。TLS プロキシの制限は、**tls-proxy maximum-sessions** コマンドまたは ASDM で [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して手動で設定できます。モデルの制限を表示するには、**tls-proxy maximum-sessions ?** コマンドを入力します。UC ライセンスもインストールすると、UC で使用できる TLS プロキシセッションは IME セッションでも使用可能になります。たとえば、設定された制限が 1000 TLS プロキシ セッションの場合、750 セッションの UC ライセンスを購入すると、最初の 250 IME セッションまでは、UC に使用可能なセッション数に影響を与えません。IME に 250 を超えるセッションが必要になると、プラットフォームの制限の残りの 750 セッションが UC と IME によって先着順に使用されます。 • 「K8」で終わるライセンス製品番号の場合、TLS プロキシ セッションは 1000 までに制限されます。 • 「K9」で終わるライセンス製品番号の場合、TLS プロキシ制限は、使用する設定とプラットフォーム モデルに依存します。 （注）　K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。 接続には、SRTP 暗号化セッションを使用する場合もあります。 • K8 ライセンスの場合、SRTP セッションは 250 までに制限されます。 • K9 ライセンスの場合、制限はありません。 （注）　メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。
全タイプのインターフェイス、最大。	VLAN、物理、冗長、ブリッジ グループ、および EtherChannel インターフェイスなど、すべてを合わせたインターフェイスの最大数。コンフィギュレーションで定義されているすべての **interface** が、この制限に対してカウントされます。

表 4-12　ライセンスの注釈（続き）

ライセンス	注意
IPS モジュール	IPS モジュール ライセンスがあると、ASA で IPS ソフトウェア モジュールを実行することができます。また、IPS 側の IPS シグニチャ サブスクリプションが必要です。 次のガイドラインを参照してください。 • IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です（製品番号に、たとえば ASA5515-IPS-K9 のように「IPS」が含まれている必要があります）。IPS ではない製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。 • フェールオーバーについては、両方のユニットで IPS シグネチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスでないため、フェールオーバー時に共有されません。 • フェールオーバーについては、IPS シグネチャ サブスクリプションにはユニットごとに一意の IPS モジュール ライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュール ライセンスも技術的にはフェールオーバー クラスタ ライセンスで共有されます。ただし、IPS シグネチャ サブスクリプションの要件に対応するために、フェールオーバーの各単位について別の IPS モジュールのライセンスを購入する必要があります。
その他の VPN	その他の VPN セッションには、次の VPN タイプが含まれています。 • IKEv1 を使用した IPsec リモート アクセス VPN • IKEv1 を使用した IPsec サイトツーサイト VPN • IKEv2 を使用した IPsec サイトツーサイト VPN このライセンスは基本ライセンスに含まれています。
合計 VPN（セッション）。全タイプの合計	• VPN セッションの最大数の合計が、VPN AnyConnect とその他の VPN セッションの最大数よりも多くなっても、組み合わせたセッション数が VPN セッションの制限を超えることはできません。VPN の最大セッション数を超えた場合、ASA をオーバーロードして、ネットワークのサイズを適切にすることができます。 • クライアントレス SSL VPN セッションを開始した後、ポータルから AnyConnect クライアント セッションを開始した場合は、合計 1 つのセッションが使用されています。これに対して、最初に AnyConnect クライアントを（スタンドアロン クライアントなどから）開始した後、クライアントレス SSL VPN ポータルにログインした場合は、2 つのセッションが使用されています。

表 4-12　ライセンスの注釈（続き）

ライセンス	注意
UC Phone 代理権限セッション、総 UC 代理権限セッション	次のアプリケーションでは、接続時に TLS プロキシ セッションを使用します。これらのアプリケーションで使用される各 TLS プロキシ セッション（およびこれらのアプリケーションのみ）は UC ライセンスの制限に対してカウントされます。 • 電話プロキシ • プレゼンス フェデレーション プロキシ • 暗号化音声インスペクション TLS プロキシ セッションを使用するその他のアプリケーション（ライセンスが不要な Mobility Advantage Proxy、個別の IME ライセンスが必要な IME など）では、UC 制限に対してカウントしません。 UC アプリケーションによっては、1 つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続が 2 つあるため、UC Proxy セッションも 2 つ使用されます。 TLS プロキシの制限は、**tls-proxy maximum-sessions** コマンドまたは ASDM で [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して個別に設定できます。モデルの制限を表示するには、**tls-proxy maximum-sessions ?** コマンドを入力します。デフォルトの TLS プロキシ制限よりも高い UC ライセンスを適用する場合、ASA では、その UC 制限に一致するように TLS プロキシの制限が自動的に設定されます。UC ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限を UC ライセンスよりも少なく設定すると、UC ライセンスですべてのセッションを使用できません。 **（注）** 「K8」で終わるライセンス製品番号（たとえばユーザ数が 250 未満のライセンス）では、TLS プロキシ セッション数は 1000 までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザ数が 250 以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。 （たとえば **clear configure all** コマンドを使用して）コンフィギュレーションをクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトが UC ライセンスの制限よりも小さいと、**tls-proxy maximum-sessions** コマンドを使用したときに、再び制限を高めるようにエラー メッセージが表示されます（ASDM の [TLS Proxy] ペインを使用）。フェールオーバーを使用して、**write standby** コマンドを入力するか、または ASDM でプライマリ装置に対して [File] > [Save Running Configuration to Standby Unit] を使用して強制的にコンフィギュレーションの同期を行うと、セカンダリ装置で **clear configure all** コマンドが自動的に生成され、セカンダリ装置に警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。 接続には、SRTP 暗号化セッションを使用する場合もあります。 • K8 ライセンスでは、SRTP セッション数は 250 までに制限されます。 • K9 ライセンスに制限はありません。 **（注）** メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。

表 4-12　ライセンスの注釈（続き）

ライセンス	注意
仮想 CPU	ASAv で仮想 CPU ライセンスをインストールする必要があります。ライセンスをインストールするまで、スループットは 100 Kbps に制限されるため、予備接続テストを実行できます。通常の操作には、仮想 CPU ライセンスが必要です。
VLAN、最大	VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。
VPN ロード バランシング	VPN ロード バランシングには、強力な暗号化（3DES/AES）ライセンスが必要です。

VPN ライセンスと機能の互換性

表 4-13 に、VPN ライセンスと機能を組み合わせる方法を示します。

AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスでサポートされている機能の詳細なリストについては、『*AnyConnect Secure Mobility Client Features, Licenses, and OSs*』を参照してください。

- バージョン 3.1：
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect31/feature/guide/anyconnect31features.html
- バージョン 3.0：
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/feature/guide/anyconnect30features.html
- バージョン 2.5：
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/feature/guide/anyconnect25features.html

表 4-13　VPN ライセンスと機能の互換性

	次のいずれかのライセンスをイネーブルにします。[1]	
サポートする機能	AnyConnect Essentials	AnyConnect Premium
Cisco VPN Phone 用の AnyConnect	No	Yes
AnyConnect for Mobile[2]	Yes	Yes
Advanced Endpoint Assessment	No	Yes
AnyConnect Premium Shared	No	Yes
クライアントベースの SSL VPN	Yes	Yes
ブラウザベース（クライアントレス）の SSL VPN	No	Yes
IPsec VPN	Yes	Yes
VPN ロード バランシング	Yes	Yes
Cisco Secure Desktop	No	Yes

1. AnyConnect Essentials ライセンスまたは AnyConnect Premium ライセンスのいずれか一方のライセンス タイプだけをアクティブにできます。デフォルトでは、ASA には 2 セッション用の AnyConnect Premium ライセンスが組み込まれています。AnyConnect Essentials ライセンスをインストールすると、それがデフォルトで使用されます。代わりに Premium ライセンスをイネーブルにするには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Essentials] ペインを選択します。
2. Mobile Posture サポートは、AnyConnect Essentials の場合と AnyConnect Premium ライセンスの場合とでは異なります。詳細については、表 4-12（P.4-14）を参照してください。

機能のライセンスに関する情報

ライセンスでは、特定の ASA 上でイネーブルにするオプションを指定します。ライセンスは、160 ビット（32 ビットのワードが 5 個、または 20 バイト）値であるアクティベーション キーで表されます。この値は、シリアル番号（11 文字の文字列）とイネーブルになる機能とを符号化します。

事前インストールされているライセンス

デフォルトでは、ASA は、ライセンスがインストールされた状態で出荷されます。このライセンスは、注文した内容およびベンダーがインストールした内容に応じて、ライセンスを追加できる基本ライセンスの場合と、すべてのライセンスがすでにインストールされている場合があります。インストールされているライセンスを特定するには、「ライセンスのモニタリング」（P.4-37）を参照してください。

永続ライセンス

永続アクティベーション キーを 1 つインストールできます。永続アクティベーション キーは、1 つのキーにすべてのライセンス機能を格納しています。時間ベース ライセンスもインストールすると、ASA は永続ライセンスと時間ベース ライセンスを 1 つの実行ライセンスに結合します。ASA がライセンスを結合する方法については、「永続ライセンスと時間ベース ライセンスの結合」（P.4-21）を参照してください。

時間ベース ライセンス

永続ライセンスに加えて、時間ライセンスを購入したり、時間制限のある評価ライセンスを入手したりできます。たとえば、SSL VPN の同時ユーザの短期増加に対処するために時間ベースの AnyConnect Premium ライセンスを購入したり、1 年間有効なボットネット トラフィック フィルタ時間ベース ライセンスを注文したりできます。

時間ベース ライセンス アクティベーションのガイドライン

- 複数の時間ベース ライセンスをインストールし、同じ機能に複数のライセンスを組み込むことができます。ただし、一度にアクティブ化できる時間ベース ライセンスは、1 機能につき 1 つだけです。非アクティブのライセンスはインストールされたままで、使用可能な状態です。たとえば、1000 セッション AnyConnect Premium ライセンスと 2500 セッション AnyConnect Premium ライセンスをインストールした場合、これらのライセンスのうちいずれか 1 つだけをアクティブにできます。
- キーの中に複数の機能を持つ評価ライセンスをアクティブにした場合、そこに含まれている機能のいずれかに対応する時間ベース ライセンスを同時にアクティブ化することはできません。たとえば、評価ライセンスにボットネット トラフィック フィルタと 1000 セッション AnyConnect Premium ライセンスが含まれる場合、スタンドアロンの時間ベース 2500 セッション AnyConnect Premium ライセンスをこの評価ライセンスと同時にアクティブ化することはできません。

時間ベース ライセンス タイマーの動作

- 時間ベース ライセンスのタイマーは、ASA 上でライセンスをアクティブにした時点でカウント ダウンを開始します。
- タイムアウト前に時間ベース ライセンスの使用を中止すると、タイマーが停止します。時間ベース ライセンスを再度アクティブ化すると、タイマーが再開します。
- 時間ベース ライセンスがアクティブになっているときにASAをシャットダウンしても、タイマーはカウント ダウンを続行します。ASA を長期にわたってシャットダウンしたままにする場合は、シャットダウンする前に時間ベース ライセンスを非アクティブにする必要があります。

（注） 時間ベース ライセンスをインストールした後は、システム クロックを変更しないことをお勧めします。システム クロックを先の日付に進めてからリロードした場合、ASA ではクロックが元のインストール日時と比較され、実際よりも長い使用時間が経過したものと見なされます。システム クロックを遅らせて、元のインストール日時との時間差よりも実際の実行時間が長くなった場合は、リロード直後にライセンスが無効になります。

永続ライセンスと時間ベース ライセンスの結合

時間ベース ライセンスをアクティブにすると、永続ライセンスと時間ベース ライセンスに含まれる機能を組み合わせた実行ライセンスが作成されます。永続ライセンスと時間ベース ライセンスの組み合わせ方は、ライセンスのタイプに依存します。表 4-14 に、各機能ライセンスの組み合わせルールを示します。

（注） 永続ライセンスが使用されていても、時間ベース ライセンスがアクティブな場合はカウント ダウンが続行されます。

表 4-14　時間ベース ライセンスの組み合わせルール

時間ベース機能	結合されたライセンスのルール
AnyConnect Premium（セッション）	時間ベース ライセンスまたは永続ライセンスのうち、値の高い方が使用されます。たとえば、永続ライセンスが 1000 セッション、時間ベース ライセンスが 2500 セッションの場合、2500 セッションがイネーブルになります。通常は、永続ライセンスよりも機能の低い時間ベース ライセンスをインストールすることはありませんが、そのようなインストールが行われた場合は永続ライセンスが使用されます。
Unified Communications Proxy セッション	時間ベース ライセンスのセッションは、プラットフォームの制限数まで永続セッションに追加されます。たとえば、永続ライセンスが 2500 セッション、時間ベース ライセンスが 1000 セッションの場合、時間ベース ライセンスがアクティブである限り、3500 セッションがイネーブルになります。
セキュリティ コンテキスト	時間ベース ライセンスのコンテキストは、プラットフォームの制限数まで永続コンテキストに追加されます。たとえば、永続ライセンスが 10 コンテキスト、時間ベース ライセンスが 20 コンテキストの場合、時間ベース ライセンスがアクティブである限り、30 コンテキストがイネーブルになります。
Botnet Traffic Filter	使用可能な永続ボットネット トラフィック フィルタ ライセンスはありません。時間ベース ライセンスが使用されます。
その他	時間ベース ライセンスまたは永続ライセンスのうち、値の高い方が使用されます。ライセンスのステータスがイネーブルまたはディセーブルの場合、イネーブル ステータスのライセンスが使用されます。数値ティアを持つライセンスの場合、高い方の値が使用されます。通常は、永続ライセンスよりも機能の低い時間ベース ライセンスをインストールすることはありませんが、そのようなインストールが行われた場合は永続ライセンスが使用されます。

結合されたライセンスを表示するには、「ライセンスのモニタリング」（P.4-37）を参照してください。

時間ベース ライセンスのスタッキング

多くの場合、時間ベース ライセンスは更新の必要があり、旧ライセンスから新しいライセンスへシームレスに移行する必要があります。時間ベース ライセンスだけで使用される機能では、新しいライセンスが適用される前に、ライセンスの有効期限が切れてしまわないことが特に重要です。ASA では時間ベース ライセンスを*スタック*できるので、ライセンスの有効期限が切れたり、新しいライセンスを早めにインストールしたために時間が無駄になったりする心配はありません。

すでにインストールされているのと同じ時間ベース ライセンスをインストールすると、それらのライセンスは結合され、有効期間は両者を合わせた期間になります。

次に例を示します。

1. 52 週のボットネット トラフィック フィルタ ライセンスをインストールし、このライセンスを 25 週間使用します（残り 27 週）。
2. 次に、別の 52 週ボットネット トラフィック フィルタ ライセンスを購入します。2 つめのライセンスをインストールすると、ライセンスが結合され、有効期間は 79 週（52 + 27 週）になります。

同様の例を示します。

1. 8 週 1000 セッションの AnyConnect Premium ライセンスをインストールし、これを 2 週間使用します（残り 6 週）。
2. 次に、別の 8 週 1000 セッションのライセンスをインストールすると、これらのライセンスは結合され、14 週（8 + 6 週）1000 セッションのライセンスになります。

これらのライセンスが同一でない場合（たとえば、1000 セッション AnyConnect Premium ライセンスと ライセンスが同じでない場合（たとえば 1000 セッション SSL VPN ライセンスと 2500 セッション ライセンス）、それらのライセンスは結合*されません*。1 つの機能につき時間ベース ライセンスを 1 つだけアクティブにできるので、ライセンスのうちいずれか 1 つだけをアクティブにすることができます。ライセンスのアクティブ化の詳細については、「キーのアクティブ化および非アクティブ化」（P.4-34）を参照してください。

同一でないライセンスは結合されませんが、現在のライセンスの有効期限が切れた場合、同じ機能のインストール済みライセンスが使用可能であれば、ASA はそのライセンスを自動的にアクティブにします。詳細については、「時間ベース ライセンスの有効期限」（P.4-23）を参照してください。

時間ベース ライセンスの有効期限

機能に対応する現在のライセンスが期限切れになると、同じ機能のインストール済みライセンスが使用可能であれば、ASA はそのライセンスを自動的にアクティブにします。その機能に使用できる時間ベース ライセンスが他にない場合は、永続ライセンスが使用されます。

その機能に対して複数の時間ベース ライセンスを追加でインストールした場合、ASA は最初に検出されたライセンスを使用します。どのライセンスを使用するかは、ユーザが設定することはできず、内部動作に依存します。ASA がアクティブ化したライセンスとは別の時間ベース ライセンスを使用するには、目的のライセンスを手動でアクティブにする必要があります。「キーのアクティブ化および非アクティブ化」（P.4-34）を参照してください。

たとえば、2500 セッションの時間ベース AnyConnect Premium ライセンス（アクティブ）、1000 セッションの時間ベース AnyConnect Premium ライセンス（非アクティブ）、500 セッションの永続 AnyConnect Premium ライセンスを所有しているとします。2500 セッション ライセンスの有効期限が切れると、ASA は 1000 セッション ライセンスをアクティブにします。1000 セッション ライセンスの有効期限が切れると、ASA は 500 セッションの永続ライセンスを使用します。

AnyConnect Premium（共有）ライセンス

AnyConnect Premium（共有）を使用すると、多数の AnyConnect Premium セッションを購入し、それらのセッションを ASA のグループ間で必要に応じて共有できます。そのためには、いずれかの ASA を共有ライセンス サーバとして、残りを共有ライセンス参加システムとして設定します。この項では、共有ライセンスの動作方法について説明します。

- 「共有ライセンスのサーバと参加システムに関する情報」（P.4-24）
- 「参加システムとサーバの間の通信に関する問題」（P.4-24）
- 「共有ライセンス バックアップ サーバに関する情報」（P.4-25）
- 「フェールオーバーと共有ライセンス」（P.4-25）
- 「参加システムの最大数」（P.4-27）

共有ライセンスのサーバと参加システムに関する情報

次に、共有ライセンスの動作手順を示します。

1. いずれのASAを共有ライセンス サーバとするかを決定し、デバイス シリアル番号を使用する共有ライセンス サーバのライセンスを購入します。
2. いずれの ASA を共有ライセンス バックアップ サーバを含む共有ライセンス参加者とするかを決定し、各デバイス シリアル番号を使用して各デバイスに対して共有ライセンス参加ライセンスを取得します。
3. （オプション）別の ASA を共有ライセンス バックアップ サーバとして指定します。バックアップ サーバには 1 台のみ指定できます。

   （注）　共有ライセンス バックアップ サーバに必要なのは参加ライセンスのみです。

4. 共有ライセンス サーバ上に共有秘密を設定します。共有秘密を保持する参加者であればいずれも共有ライセンスを使用できます。
5. ASA を参加者として設定する場合、ローカル ライセンスおよびモデル情報を含む自身の情報を送信することで共有ライセンス サーバに登録します。

   （注）　参加者は IP ネットワークを経由してサーバと通信できる必要がありますが、同じサブネット上にある必要はありません。

6. 共有ライセンス サーバは、参加者がサーバにポーリングするべき頻度の情報で応答します。
7. 参加者がローカル ライセンスのセッションを使い果たした場合、参加者は共有ライセンス サーバに 50 セッション単位で追加セッションの要求を送信します。
8. 共有ライセンス サーバは、共有ライセンスで応答します。1 台の参加者が使用する合計セッション数は、プラットフォーム モデルの最大セッション数を超えられません。

   （注）　共有ライセンス サーバは、共有ライセンス プールに参加することもできます。参加には参加ライセンスもサーバ ライセンスも必要ありません。

   a. 参加者に対して共有ライセンス プールに十分なセッションがない場合、サーバは使用可能な限りのセッション数で応答します。
   b. 参加者はさらなるセッションを要求するリフレッシュ メッセージの送信をサーバが要求に適切に対応できるまで続けます。
9. 参加者の負荷が減少した場合、参加者はサーバに共有セッションを解放するようにメッセージを送信します。

（注）　ASA は、サーバと参加者間のすべての通信の暗号化に SSL を使用します。

参加システムとサーバの間の通信に関する問題

参加者とサーバ間の通信問題については、次のガイドラインを参照してください。

- 参加者が更新の送信に失敗して更新間隔 3 倍の時間が経過した後で、サーバはセッションを解放して共有ライセンス プールに戻します。

- 参加者が更新を送信するためにライセンス サーバに到達できない場合、参加者はサーバから受信した共有ライセンスを最大 24 時間使用し続けられます。
- 24 時間を経過しても参加者がまだライセンス サーバと通信できない場合、参加者はセッションがまだ必要であっても共有ライセンスを解放します。参加者は既存の確立している接続を維持しますが、ライセンス制限を超えて新しい接続を受け入れられません。
- 参加者が 24 時間経過前にサーバに再接続したが、サーバが参加セッションを期限切れにした後である場合、参加者はセッションに対する新しい要求を送信する必要があります。サーバは、参加者に再割り当てできる限りのセッション数で応答します。

共有ライセンス バックアップ サーバに関する情報

共有ライセンス バックアップ サーバは、バックアップの役割を実行する前にメインの共有ライセンス サーバへの登録に成功している必要があります。登録時には、メインの共有ライセンス サーバは共有ライセンス情報に加えてサーバ設定もバックアップと同期します。情報には、登録済み参加者の一覧および現在のライセンス使用状況が含まれます。メイン サーバとバックアップ サーバは、10 秒間隔でデータを同期します。初回同期の後で、バックアップ サーバはリロード後でもバックアップの役割を実行できます。

メイン サーバがダウンすると、バックアップ サーバがサーバ動作を引き継ぎます。バックアップ サーバは継続して最大 30 日間動作できます。30 日を超えると、バックアップ サーバは参加者へのセッション発行を中止し、既存のセッションはタイムアウトします。メイン サーバをこの 30 日間中に確実に復旧するようにします。クリティカル レベルの syslog メッセージが 15 日めに送信され、30 日めに再送信されます。

メイン サーバが復旧した場合、メイン サーバはバックアップ サーバと同期してから、サーバ動作を引き継ぎます。

バックアップ サーバがアクティブでないときは、メインの共有ライセンス サーバの通常の参加者として動作します。

（注）　メインの共有ライセンス サーバの初回起動時には、バックアップ サーバは独立して 5 日間のみ動作できます。動作制限は 30 日に到達するまで日ごとに増加します。また、メイン サーバがその後短時間でもダウンした場合、バックアップ サーバの動作制限は日ごとに減少します。メイン サーバが復旧した場合、バックアップ サーバは再び日ごとに増加を開始します。たとえば、メイン サーバが 20 日間ダウンしていて、その期間中バックアップ サーバがアクティブであった場合、バックアップ サーバには、10 日間の制限のみが残っています。バックアップ サーバは、非アクティブなバックアップとしてさらに 20 日間が経過した後で、最大の 30 日間まで「充電」されます。この充電機能は共有ライセンスの誤使用を防ぐために実装されています。

フェールオーバーと共有ライセンス

この項では、共有ライセンスとフェールオーバーの相互作用について説明します。

- 「フェールオーバーと共有ライセンス サーバ」（P.4-25）
- 「フェールオーバーと共有ライセンス参加システム」（P.4-27）

フェールオーバーと共有ライセンス サーバ

この項では、メイン サーバおよびバックアップ サーバと、フェールオーバーとの相互作用について説明します。共有ライセンス サーバでは、VPN ゲートウェイやファイアウォールなど、ASA としての通常機能も実行されます。このため、メインとバックアップの共有ライセンス サーバにフェールオーバーを設定して、信頼性を高めることをお勧めします。

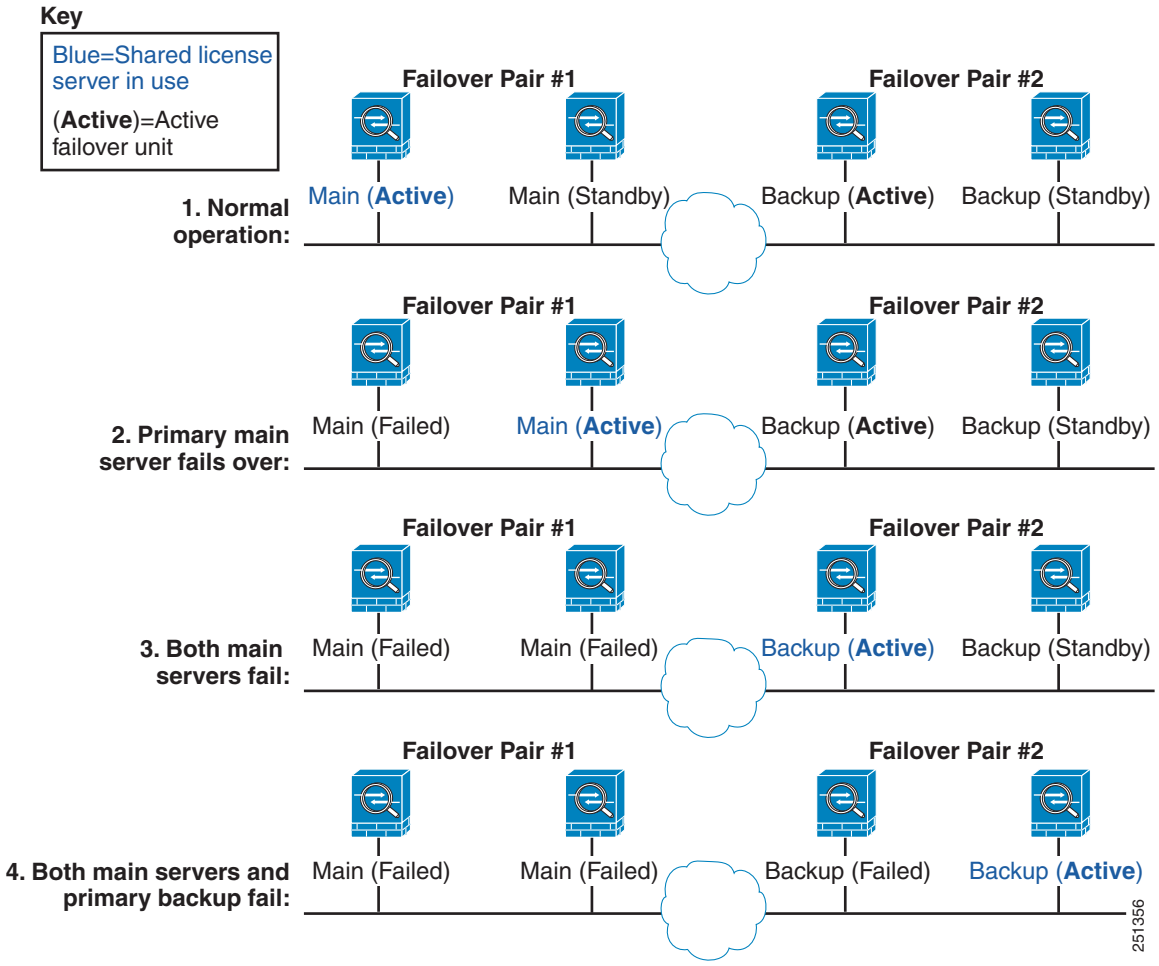
（注）　バックアップ サーバ メカニズムとフェールオーバーは異なりますが、両者には互換性があります。

共有ライセンスはシングル コンテキスト モードでだけサポートされるため、アクティブ/アクティブ フェールオーバーはサポートされません。

アクティブ/スタンバイ フェールオーバーでは、プライマリ装置が主要な共有ライセンス サーバとして機能し、スタンバイ装置はフェールオーバー後に主要な共有ライセンス サーバとして機能します。スタンバイ装置は、バックアップの共有ライセンス サーバとしては機能*しません*。必要に応じて、バックアップ サーバとして機能する装置のペアを追加します。

たとえば、2 組のフェールオーバー ペアがあるネットワークを使用するとします。ペア #1 にはメインのライセンス サーバが含まれます。ペア #2 にはバックアップ サーバが含まれます。ペア #1 のプライマリ装置がダウンすると、ただちに、スタンバイ装置が新しくメイン ライセンス サーバになります。ペア #2 のバックアップ サーバが使用されることはありません。ペア #1 の装置が両方ともダウンした場合だけ、ペア #2 のバックアップ サーバが共有ライセンス サーバとして使用されるようになります。ペア #1 がダウンしたままで、ペア #2 のプライマリ装置もダウンした場合は、ペア #2 のスタンバイ装置が共有ライセンス サーバとして使用されるようになります（図 4-1を参照）。

図 4-1　　フェールオーバーと共有ライセンス サーバ



スタンバイ バックアップ サーバは、プライマリ バックアップ サーバと同じ動作制限を共有します。スタンバイ装置がアクティブになると、その時点からプライマリ装置のカウントダウンを引き継ぎます。詳細については、「共有ライセンス バックアップ サーバに関する情報」（P.4-25）を参照してください。

フェールオーバーと共有ライセンス参加システム

参加システムのペアについては、両方の装置を共有ライセンス サーバに登録します。登録時には、個別の参加システム ID を使用します。アクティブ装置の参加システム ID は、スタンバイ装置と同期されます。スタンバイ装置は、アクティブに切り替わるときに、この ID を使用して転送要求を生成します。この転送要求によって、以前にアクティブだった装置から新しくアクティブになる装置に共有セッションが移動します。

参加システムの最大数

ASA では、共有ライセンスの参加システム数に制限がありません。ただし、共有ネットワークの規模が非常に大きいと、ライセンス サーバのパフォーマンスに影響する場合があります。この場合は、参加システムのリフレッシュ間隔を長くするか、共有ネットワークを 2 つ作成することをお勧めします。

フェールオーバーまたは ASA クラスタ ライセンス

いくつかの例外を除き、フェールオーバーおよびクラスタ ユニットは、各ユニット上で同一のライセンスを必要としません。以前のバージョンについては、お使いのバージョンに該当するライセンシング マニュアルを参照してください。

フェールオーバー ライセンスの要件および例外

フェールオーバー ユニットは、各ユニット上で同一のライセンスを必要としません。

旧バージョンの ASA ソフトウェアは、各ユニット上のライセンスが一致する必要がありました。バージョン 8.3(1) から、同一のライセンスをインストールする必要がなくなりました。通常、ライセンスをプライマリ ユニット専用に購入します。アクティブ/スタンバイ フェールオーバーでは、セカンダリ ユニットがアクティブになるとプライマリ ライセンスを継承します。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバー クラスタ ライセンスに結合されます。

このルールの例外は次のとおりです。

- ASA 5512-X の Security Plus ライセンスの場合：基本ライセンスはフェールオーバーをサポートしないため、基本ライセンスのみを保持するスタンバイ ユニットではフェールオーバーをイネーブルにできません。
- 暗号化ライセンス：両方のユニットに同じ暗号化ライセンスが必要です。

- ASA 5512-X から ASA 5555-X までの IPS モジュール ライセンス：両方の装置で IPS モジュール ライセンスが必要です。両方の装置の IPS 側で IPS シグニチャ サブスクリプションも必要です。次のガイドラインを参照してください。
  - IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です（製品番号に、たとえば ASA5515-IPS-K9 のように「IPS」が含まれている必要があります）。IPS ではない製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。
  - 両方の装置に IPS シグニチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスではないため、フェールオーバー間で共有されません。
  - IPS シグニチャ サブスクリプションには、装置ごとに個別の IPS モジュール ライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュール ライセンスも技術的にはフェールオーバー クラスタ ライセンスで共有されます。しかし、IPS シグニチャ サブスクリプションの要件によって、装置ごとに個別の IPS モジュール ライセンスを購入する必要があります。
- ASAv 仮想 CPU：フェールオーバー配置では、スタンバイ装置に割り当てられる vCPU の数をプライマリ装置に割り当てられる数と同じにしてください（対応する数の vCPU ライセンスも必要です）。

（注）　有効な永続キーが必要です。まれに、認証キーを削除できることもあります。キーがすべて 0 の場合は、フェールオーバーをイネーブルにするには有効な認証キーを再インストールする必要があります。

ASA クラスタ ライセンスの要件および例外

クラスタ ユニットは、各ユニット上で同一のライセンスを必要としません。一般的には、マスター ユニット用のライセンスのみを購入します。スレーブ ユニットはマスターのライセンスを継承します。複数のユニットにライセンスがある場合は、これらが結合されて単一の実行 ASA クラスタ ライセンスとなります。

このルールの例外は次のとおりです。

- クラスタリング ライセンス：各ユニットにクラスタリング ライセンスが必要です。
- 暗号化ライセンス：各ユニットに同じ暗号化ライセンスが必要です。

フェールオーバーまたは ASA クラスタ ライセンスの結合方法

フェールオーバー ペアまたは ASA クラスタでは、各ユニットのライセンスが結合されて 1 つの実行クラスタ ライセンスとなります。ユニットごとに別のライセンスを購入した場合は、結合されたライセンスには次のルールが使用されます。

- 数値ティアを持つライセンスの場合は（セッション数など）、各ユニットのライセンスの値が合計されます。ただし、プラットフォームの制限を上限とします。使用されているライセンスがすべて時間ベースの場合は、ライセンスのカウント ダウンは同時に行われます。

  たとえば、フェールオーバーの場合は次のようになります。
  - 10 AnyConnect Premium セッションの ASA を 2 つ所有しています。ライセンスは結合され、合計で 20 AnyConnect Premium セッションになります。
  - それぞれに 500 の AnyConnect Premium セッションがある 2 つの ASA 5525-X を所有しています。プラットフォーム制限は 750 であるため、結合されたライセンスでは 750 の AnyConnect Premium セッションが可能です。

（注）　上記の例で、AnyConnect Premium ライセンスが時間ベースの場合、いずれか 1 つのライセンスをディセーブルにすると、プラットフォーム制限のために 500 セッションのライセンスで 250 セッションしか使用できないという「無駄」が生じることはありません。

– 2 つの ASA 5545-X ASA があり、一方は 20 コンテキスト、もう一方は 10 コンテキストである場合、結合されたライセンスでは 30 コンテキストを使用できます。アクティブ/アクティブ フェールオーバーの場合は、コンテキストが 2 つのユニットに分配されます。たとえば、一方のユニットが 18 コンテキストを使用し、他方が 12 コンテキストを使用します（合計 30 の場合）。

たとえば、ASA クラスタリングの場合は次のようになります。

– SSP-10、それぞれ 50 コンテキストの 3 つのユニット、およびデフォルトの 2 コンテキストの 1 ユニットを持つ ASA 5585-X ASA を 4 つ所有しています。プラットフォームの制限が 100 であるため、結合されたライセンスでは最大 100 のコンテキストが許容されます。したがって、マスター ユニット上で最大 100 コンテキストを設定できます。各スレーブ ユニットも、コンフィギュレーションの複製を介して 100 コンテキストを持つことになります。

– SSP-60、それぞれ 50 コンテキストの 3 つのユニット、およびデフォルトの 2 コンテキストの 1 ユニットを持つ ASA 5585-X ASA を 4 つ所有しています。プラットフォームの制限が 250 であるため、ライセンスは合計で 152 コンテキストに結合されます。したがって、マスター ユニット上で最大 152 コンテキストを設定できます。各スレーブ ユニットも、コンフィギュレーションの複製を介して 152 コンテキストを持つことになります。

- ライセンスのステータスがイネーブルまたはディセーブルの場合、イネーブル ステータスのライセンスが使用されます。
- イネーブルまたはディセーブル状態（かつ数値ティアを持たない）の時間ベース ライセンスの場合、有効期間はすべてのライセンスの期間の合計となります。最初にプライマリ/マスター ユニットのライセンスがカウント ダウンされ、期限切れになると、セカンダリ/スレーブ ユニットのライセンスのカウント ダウンが開始し、以下も同様です。このルールは、アクティブ/アクティブ フェールオーバーと ASA クラスタリングにも適用されます（すべてのユニットがアクティブに動作していても適用されます）。

  たとえば、2 つのユニットのボットネット トラフィック フィルタ ライセンスの有効期間が 48 週残っている場合は、結合された有効期間は 96 週です。

結合されたライセンスを表示するには、「ライセンスのモニタリング」（P.4-37）を参照してください。

フェールオーバーまたは ASA クラスタ ユニット間の通信の途絶

ユニットの通信が途絶えてからの期間が 30 日を超えた場合は、各ユニットにはローカルにインストールされたライセンスが適用されます。30 日の猶予期間中は、結合された実行ライセンスが引き続きすべてのユニットで使用されます。

30 日間の猶予期間中に通信が復旧した場合は、時間ベース ライセンスについては、経過した時間がプライマリ/マスター ライセンスから差し引かれます。プライマリ/マスター ライセンスが期限切れになるまでは、セカンダリ/スレーブ ライセンスのカウント ダウンが開始することはありません。

30 日間の期間が終了しても通信が復旧しなかった場合は、時間ベース ライセンスについては、その時間がすべてのユニットのライセンスから差し引かれます（インストールされている場合）。これらはそれぞれ別のライセンスとして扱われ、ライセンスの結合によるメリットはありません。経過時間には 30 日の猶予期間も含まれます。

次に例を示します。

1. 52 週のボットネット トラフィック フィルタ ライセンスが 2 つのユニットにインストールされています。結合された実行ライセンスでは、合計期間は 104 週になります。
2. これらのユニットが、1 つのフェールオーバー ユニット/ASA クラスタとして 10 週間動作すると、結合ライセンスの期間の残りは 94 週となります（プライマリ/マスターに 42 週、セカンダリ/スレーブに 52 週）。
3. ユニットの通信が途絶えた場合（たとえば、プライマリ/マスター ユニットが停止した場合）は、セカンダリ/スレーブ ユニットは結合されたライセンスを引き続き使用し、94 週からカウント ダウンを続行します。
4. 時間ベース ライセンスの動作は、通信がいつ復元されるかによって次のように異なります。

- 30 日以内：経過した時間がプライマリ/マスター ユニットのライセンスから差し引かれます。この場合、通信は 4 週間後に復元されます。したがって、4 週がプライマリ/マスター ライセンスから差し引かれて、残りは合計 90 週となります（プライマリに 38 週、セカンダリに 52 週）。
- 30 日経過以降：経過時間が両方の装置から差し引かれます。この場合、通信は 6 週間後に復元されます。したがって、6 週がプライマリ/マスターとセカンダリ/スレーブの両方のライセンスから差し引かれて、残りは合計 84 週となります（プライマリ/マスターに 36 週、セカンダリ/スレーブに 46 週）。

フェールオーバー ペアのアップグレード

フェールオーバー ペアでは、両方の装置に同一のライセンスがインストールされている必要はないので、ダウンタイムなしに各装置に新しいライセンスを適用できます。リロードが必要な永続ライセンス（表 4-15（P.4-34）を参照）を適用する場合、リロード中に他の装置へのフェールオーバーを実行できます。両方の装置でリロードが必要な場合は、各装置を個別にリロードするとダウンタイムは発生しません。

ペイロード暗号化機能のないモデル

ペイロード暗号化機能のないモデルを購入することができます。輸出先の国によっては、Cisco ASA シリーズでペイロード暗号化をイネーブルにできません。ASA ソフトウェアは、ペイロード暗号化なしモデルを検出し、次の機能をディセーブルにします。

- ユニファイド コミュニケーション
- [VPN]

このモデルでも管理接続用に高度暗号化（3DES/AES）ライセンスをインストールできます。たとえば、ASDM HTTPS/SSL、SSHv2、Telnet、および SNMPv3 を使用できます。ボットネット トラフィック フィルタ（SSL を使用）用のダイナミック データベースをダウンロードすることもできます。

ライセンスを表示すると（「ライセンスのモニタリング」（P.4-37）を参照）、VPN およびユニファイド コミュニケーションのライセンスはリストに示されません。

ライセンスの FAQ

Q. AnyConnect Premium とボットネット トラフィック フィルタなど、複数の時間ベース ライセンスをアクティブにできますか。

A. はい。一度に使用できる時間ベース ライセンスは、1 機能につき 1 つです。

Q. 複数の時間ベース ライセンスを「スタック」し、時間制限が切れると自動的に次のライセンスが使用されるようにできますか。

A. はい。ライセンスが同一の場合は、複数の時間ベース ライセンスをインストールすると、時間制限が結合されます。ライセンスが同一でない場合（1000 セッション AnyConnect Premium ライセンスと 2500 セッション ライセンスなど）、ASA はその機能に対して検出された次の時間ベース ライセンスを自動的にアクティブにします。

Q. アクティブな時間ベース ライセンスを維持しながら、新しい永続ライセンスをインストールできますか。

A. はい。永続ライセンスをアクティブ化しても、時間ベース ライセンスには影響しません。

Q. フェールオーバーのプライマリ装置として共有ライセンス サーバを、セカンダリ装置として共有ライセンス バックアップ サーバを使用できますか。

A. いいえ。セカンダリ装置は、プライマリ装置と同じ実行ライセンスを使用します。共有ライセンス サーバには、サーバ ライセンスが必要です。バックアップ サーバには、参加ライセンスが必要です。バックアップ サーバは、2 つのバックアップ サーバの別々のフェールオーバー ペアに配置できます。

Q. フェールオーバー ペアのセカンダリ装置用に、同じライセンスを購入する必要がありますか。

A. いいえ。バージョン 8.3(1) から、両方の装置に同一のライセンスをインストールする必要はなくなりました。一般的に、ライセンスはプライマリ装置で使用するために購入されます。セカンダリ装置は、アクティブになるとプライマリ ライセンスを継承します。セカンダリ装置に別のライセンスを持っている場合は（たとえば、8.3 よりも前のソフトウェアに一致するライセンスを購入した場合）、ライセンスは実行フェールオーバー クラスタ ライセンスに結合されます。ただし、モデルの制限が最大数になります。

Q. AnyConnect Premium（共有）ライセンスに加えて、時間ベースまたは永続の AnyConnect Premium ライセンスを使用できますか。

A. はい。ローカルにインストールされたライセンス（時間ベース ライセンスまたは永続ライセンス）のセッション数を使い果たした後、共有ライセンスが使用されます。**注**：共有ライセンス サーバでは、永続 AnyConnect Premium ライセンスは使用されません。ただし、共有ライセンス サーバ ライセンスと同時に時間ベース ライセンスを使用することはできます。この場合、時間ベース ライセンスのセッションは、ローカルの AnyConnect Premium セッションにだけ使用できます。共有ライセンス プールに追加して参加システムで使用することはできません。

ガイドラインと制限事項

アクティベーション キーについては、次のガイドラインを参照してください。

コンテキスト モードのガイドライン

- マルチ コンテキスト モードでシステム実行スペース内にアクティベーション キーを適用します。
- 共有ライセンスは、マルチ コンテキスト モードではサポートされていません。

ファイアウォール モードのガイドライン

ルーテッド モードとトランスペアレント モードの両方で、すべてのライセンス タイプを使用できます。

フェールオーバーのガイドライン

- 共有ライセンスは、アクティブ/アクティブ モードではサポートされていません。詳細については、「フェールオーバーと共有ライセンス」（P.4-25）を参照してください。
- 「フェールオーバーまたは ASA クラスタ ライセンス」（P.4-27）を参照してください。

アップグレードとダウングレードのガイドライン

任意の旧バージョンから最新バージョンにアップグレードした場合、アクティベーション キーの互換性は存続します。ただし、ダウングレード機能の維持には問題が生じる場合があります。

- バージョン 8.1 以前にダウングレードする場合：アップグレード後に、*8.2 よりも前*に導入された機能のライセンスを追加でアクティブ化すると、ダウングレードした場合でも旧バージョンに対するアクティベーション キーの互換性は存続します。ただし、*8.2 以降*で導入された機能ライセンスをアクティブ化した場合は、アクティベーション キーの下位互換性がなくなります。互換性のないライセンス キーがある場合は、次のガイドラインを参照してください。
  - 旧バージョンでアクティベーション キーを入力した場合は、そのキーが ASA で使用されます（バージョン 8.2 以降でアクティブ化した新しいライセンスがない場合）。
  - 新しいシステムで、以前のアクティベーション キーがない場合は、旧バージョンと互換性のある新しいアクティベーション キーを要求する必要があります。
- バージョン 8.2 以前にダウングレードする場合：バージョン 8.3 では、よりロバストな時間ベース キーの使用およびフェールオーバー ライセンスの変更が次のとおり導入されました。
  - 複数の時間ベースのアクティベーション キーがアクティブな場合、ダウングレード時には一番最近アクティブ化された時間ベース キーのみがアクティブになれます。他のキーはすべて非アクティブ化されます。最後の時間ベース ライセンスが 8.3 で導入された機能に対応している場合、そのライセンスは旧バージョンでの使用はできなくても、アクティブ ライセンスのままです。永続キーまたは有効な時間ベース キーを再入力してください。
  - フェールオーバー ペアに不一致のライセンスがある場合、ダウングレードによりフェールオーバーはディセーブルになります。キーが一致した場合でも、使用するライセンスは、結合されたライセンスではなくなります。
  - 1 つの時間ベース ライセンスをインストールしているが、それが 8.3 で導入された機能に対応している場合、ダウングレードの実行後、その時間ベース ライセンスはアクティブなままです。この時間ベース ライセンスをディセーブルにするには、永続キーを再入力する必要があります。

その他のガイドラインと制限事項

- アクティベーション キーは、コンフィギュレーション ファイルには保存されません。隠しファイルとしてフラッシュ メモリに保存されます。
- アクティベーション キーは、デバイスのシリアル番号に関連付けられます。機能ライセンスは、デバイス間で転送できません（ハードウェア障害の発生時を除く）。ハードウェア障害が発生したためにデバイスを交換する必要があり、このことが Cisco TAC によってカバーされている場合は、シスコのライセンス チームに連絡して、既存のライセンスを新しいシリアル番号に転送するよう依頼してください。シスコのライセンス チームから、製品認証キーの参照番号と既存のシリアル番号を求められます。
- 購入後に、返金またはアップグレードしたライセンスのためにライセンスを返却できません。
- 1 つのユニット上で、同じ機能の 2 つの別個のライセンスを加算することはできません。たとえば、25 セッション SSL VPN ライセンスを購入した後で 50 セッション ライセンスを購入しても、75 個のセッションを使用できるわけではなく、使用できるのは最大 50 個のセッションです。（アップグレード時に、数を増やしたライセンスを購入できることがあります。たとえば 25 セッションから 75 セッションへの増加です。このタイプのアップグレードは、2 つのライセンスの加算とは別のものです）。
- すべてのライセンス タイプをアクティブ化できますが、機能によっては、機能どうしの組み合わせができないものがあります。AnyConnect Essentials ライセンスの場合、次のライセンスとは互換性がありません。AnyConnect Premium ライセンス、AnyConnect Premium（共有）ライセンス、および Advanced Endpoint Assessment ライセンス。デフォルトでは、AnyConnect Essentials ライセンスをインストールした場合（使用中のモデルで利用できる場合）、このライセンスが前述のライセンスの代わりに使用されます。を使用する [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Essentials] ペインを使用することで、AnyConnect Essentials ライセンスをコンフィギュレーションでディセーブルにし、他のライセンスを使用できます。

ライセンスの設定

アクティベーション キーの取得

アクティベーション キーを取得するには、シスコの代理店から購入できる製品認証キーが必要です。機能ライセンスごとに個別の製品認証キーを購入する必要があります。たとえば、基本ライセンスがある場合は、Advanced Endpoint Assessment 用と追加の AnyConnect Premium セッション用に別々のキーを購入する必要があります。

製品認証キーを取得したら、次の手順を実行して Cisco.com にそれらのキーを登録します。

手順の詳細

ステップ 1　ASA のシリアル番号を、[Configuration] > [Device Management] > [Licensing] > [Activation Key] を選択して、（マルチ コンテキスト モードでは、システム実行領域でシリアル番号を表示）取得します。

ステップ 2　Cisco.com に登録する準備が整っていない場合は、アカウントを作成します。

ステップ 3　次のライセンス Web サイトに移動します。

http://www.cisco.com/go/license

ステップ 4　プロンプトが表示されたら、次の情報を入力します。

- 製品認証キー（キーが複数ある場合は、まず 1 つを入力します。キーごとに個別のプロセスとして入力する必要があります）
- ASA のシリアル番号
- 電子メール アドレス

アクティベーション キーが自動的に生成され、指定した電子メール アドレスに送信されます。このキーには、永続ライセンス用にそれまでに登録した機能がすべて含まれています。時間ベース ライセンスの場合は、ライセンスごとに個別のアクティベーション キーがあります。

ステップ 5　製品認証キーがさらにある場合は、製品認証キーごとにステップ 4 を繰り返します。すべての製品認証キーを入力した後、最後に送信されるアクティベーション キーには、登録した永続機能がすべて含まれています。

キーのアクティブ化および非アクティブ化

この項では、新しいアクティベーション キーの入力と、時間ベース キーのアクティブ化および非アクティブ化の方法について説明します。

前提条件

- すでにマルチ コンテキスト モードに入っている場合は、システム実行スペースにこのアクティベーション キーを入力します。
- 一部の永続ライセンスでは、アクティブ化後にASAをリロードする必要があります。表 4-15 に、リロードが必要なライセンスを示します。

表 4-15　永続ライセンスのリロード要件

モデル	リロードが必要なライセンス アクション
すべてのモデル	暗号化ライセンスのダウングレード
ASAv	vCPU ライセンスのダウングレード

制限事項

任意の旧バージョンから最新バージョンにアップグレードした場合、アクティベーション キーの互換性は存続します。ただし、ダウングレード機能の維持には問題が生じる場合があります。

- バージョン 8.1 以前にダウングレードする場合：アップグレード後に、*8.2 よりも前*に導入された機能のライセンスを追加でアクティブ化すると、ダウングレードした場合でも旧バージョンに対するアクティベーション キーの互換性は存続します。ただし、*8.2 以降*で導入された機能ライセンスをアクティブ化した場合は、アクティベーション キーの下位互換性がなくなります。互換性のないライセンス キーがある場合は、次のガイドラインを参照してください。
  - 旧バージョンでアクティベーション キーを入力した場合は、そのキーが ASA で使用されます（バージョン 8.2 以降でアクティブ化した新しいライセンスがない場合）。
  - 新しいシステムで、以前のアクティベーション キーがない場合は、旧バージョンと互換性のある新しいアクティベーション キーを要求する必要があります。

- バージョン 8.2 以前にダウングレードする場合：バージョン 8.3 では、よりロバストな時間ベース キーの使用およびフェールオーバー ライセンスの変更が次のとおり導入されました。
  - 複数の時間ベースのアクティベーション キーがアクティブな場合、ダウングレード時には一番最近アクティブ化された時間ベース キーのみがアクティブになれます。他のキーはすべて非アクティブ化されます。
  - フェールオーバー ペアに不一致のライセンスがある場合、ダウングレードによりフェールオーバーはディセーブルになります。キーが一致した場合でも、使用するライセンスは、結合されたライセンスではなくなります。

手順の詳細

ステップ 1　[Configuration]> [Device Management] を選択し、モデルに応じて、[Licensing]> [Activation Key] または [Licensing Activation Key] ペインを選択します。

ステップ 2　永続または時間ベースの新しいアクティベーション キーを入力するには、[New Activation Key] フィールドで新しいアクティベーション キーを入力します。

キーは、5 つの要素で構成される 16 進ストリングで、各要素は 1 つのスペースで区切られています。先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。次に例を示します。

```
ASA0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

1 つの永続キーおよび複数の時間ベース キーをインストールできます。新しい永続キーを入力した場合、すでにインストール済みのキーが上書きされます。新しい時間ベース キーを入力した場合、デフォルトでアクティブになり、[Time-based License Keys Installed] テーブルに表示されます。特定の機能に対して最後にアクティブ化した時間ベース キーがアクティブになります。

ステップ 3　インストール済みの時間ベース キーをアクティブ化または非アクティブ化するには、そのキーを [Time-based License Keys Installed] テーブルで選択し、[Activate] または [Deactivate] をクリックします。

各機能でアクティブにできる時間ベース キーは 1 つのみです。詳細については、「時間ベース ライセンス」（P.4-20）を参照してください。

ステップ 4　[Update Activation Key] をクリックします。

永続ライセンスによっては、新しいアクティベーション キーの入力後に ASA をリロードする必要があります。リロードが必要なライセンスの一覧については、表 4-15（P.4-34）を参照してください。必要な場合は、リロードするよう求められます。

共有ライセンスの設定

この項では、共有ライセンス サーバと参加システムを設定する方法について説明します。共有ライセンスの詳細については、「AnyConnect Premium（共有）ライセンス」（P.4-23）を参照してください。

共有ライセンス サーバの設定

この項では、ASA を共有ライセンス サーバとして設定する方法について説明します。

前提条件

サーバが共有ライセンス サーバ キーを持っている必要があります。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Licenses] > [Shared SSL VPN Licenses] ペインの順に選択します。

ステップ 2　[Shared Secret] フィールドに、共有秘密を 4 ～ 128 ASCII 文字のストリングで入力します。

この秘密を持つすべての参加ユニットがライセンス サーバを使用できます。

ステップ 3　（オプション）[TCP IP Port] フィールドに、サーバが参加ユニットからの SSL 接続を受信するポート（1 ～ 65535）を入力します。

デフォルトは、TCP ポート 50554 です。

ステップ 4　（オプション）[Refresh interval] フィールドで、10 ～ 300 秒の更新間隔を入力します。

この値は、サーバと通信する頻度を設定するために参加ユニットに提供されます。デフォルトは 30 秒です。

ステップ 5　共有ライセンス領域が表示されるインターフェイスで、[Shares Licenses] チェックボックスをオンにします。パーティシパントからサーバへの通信には、このチェックボックスに対応するインターフェイスが使用されます。

ステップ 6　（オプション）バックアップ サーバを指定するには、オプションのバックアップ共有 SSL VPN ライセンス サーバ領域で次の手順を実行します。

a.　[Backup server IP address] フィールドにバックアップ サーバの IP アドレスを入力します。

b.　[Primary backup server serial number] フィールドにバックアップ サーバのシリアル番号を入力します。

c.　バックアップ サーバがフェールオーバー ペアの一部の場合は、[Secondary backup server serial number] フィールドでスタンバイ ユニットのシリアル番号を指定します。

1 つのバックアップ サーバとそのオプションのスタンバイ ユニットのみを指定できます。

ステップ 7　[Apply] をクリックします。

次の作業

「共有ライセンス参加ユニット、およびオプションのバックアップ サーバの設定」（P.4-36）を参照してください。

共有ライセンス参加ユニット、およびオプションのバックアップ サーバの設定

この項では、共有ライセンス サーバと通信するように共有ライセンス参加ユニットを設定する方法について説明します。オプションで参加ユニットをバックアップ サーバとして設定する方法についても説明します。

前提条件

参加システムが共有ライセンス参加キーを持っている必要があります。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Licenses] > [Shared SSL VPN Licenses] ペインの順に選択します。

ステップ 2　[Shared Secret] フィールドに、共有秘密を 4 ～ 128 ASCII 文字のストリングで入力します。

ステップ 3　（オプション）[TCP IP Port] フィールドに、SSL を使用してサーバと通信するポート（1 ～ 65535）を入力します。

デフォルトは、TCP ポート 50554 です。

ステップ 4　（オプション）参加ユニットをバックアップ サーバとして指定するには、[Select backup role of participant] エリアで、次の手順を実行します。

a.　[Backup Server] オプション ボタンをクリックします。

b.　[Shares Licenses] チェックボックスをオンにします。パーティシパントからバックアップ サーバへの通信には、このチェックボックスに対応するインターフェイスが使用されます。

ステップ 5　[Apply] をクリックします。

ライセンスのモニタリング

現在のライセンスの表示

この項では、現在のライセンスと、時間ベース アクティベーション キーの残り時間を表示する方法について説明します。

ガイドライン

ペイロード暗号化機能のないモデルでライセンスを表示すると、VPN および Unified Communications ライセンスは一覧に示されません。詳細については、「ペイロード暗号化機能のないモデル」（P.4-30）を参照してください。

手順の詳細

ステップ 1　永続ライセンスとアクティブな時間ベース ライセンスの組み合わせである実行ライセンスを表示するには、[Configuration] > [Device Management] > [Licensing] > [Activation Key] ペインを選択し、[Running Licenses] 領域を表示します。

マルチ コンテキスト モードでは、[Configuration] > [Device Management] > [Activation Key] ペインを選択し、システム実行スペースでアクティベーション キーを表示します。

フェールオーバー ペアの場合、表示される実行ライセンスは、プライマリ装置とセカンダリ装置からの結合されたライセンスです。詳細については、「フェールオーバーまたは ASA クラスタ ライセンスの結合方法」（P.4-28）を参照してください。数値が割り当てられた時間ベース ライセンス（期間は結合されません）の場合、[License Duration] カラムには、プライマリ装置またはセカンダリ装置からの最短の時間ベース ライセンスが表示されます。このライセンスの有効期限が切れると他の装置のライセンスの期間が表示されます。

ステップ 2　（オプション）時間ベース ライセンスの詳細（ライセンスに含まれる機能やライセンス期間など）を [Time-Based License Keys Installed] 領域に表示するには、ライセンス キーを選択し、[Show License Details] をクリックします。

ステップ 3　（オプション）フェールオーバー ユニットでは、そのユニットにインストールされている（プライマリ装置とセカンダリ装置からの結合ライセンスではない）ライセンスを [Running Licenses] 領域に表示するには、[Show information of license specifically purchased for this device alone] をクリックします。

共有ライセンスのモニタリング

共有ライセンスを監視するには、[Monitoring] > [VPN] > [Clientless SSL VPN] > [Shared Licenses] を選択するか、。

ライセンスの機能履歴

表 4-16 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 4-16　ライセンスの機能履歴

機能名	プラットフォーム リリース	機能情報
接続数と VLAN 数の増加	7.0(5)	次の制限値が増加されました。 • ASA5510 Base ライセンス接続は 32000 から 5000 に、VLAN は 0 から 10 に増加。 • ASA5510 Security Plus ライセンス接続は 64000 から 130000 に、VLAN は 10 から 25 に増加。 • ASA5520 接続は 130000 から 280000 に、VLAN は 25 から 100 に増加。 • ASA5540 接続は 280000 から 400000 に、VLAN は 100 から 200 に増加。
SSL VPN ライセンス	7.1(1)	SSL VPN ライセンスが導入されました。
SSL VPN ライセンスの追加	7.2(1)	5000 ユーザの SSL VPN ライセンスが ASA 5550 以降に対して導入されました。

表 4-16　　ライセンスの機能履歴 （続き）

機能名	プラットフォームリリース	機能情報
ASA 5510 上の基本ライセンスに対する増加したインターフェイス	7.2(2)	ASA 5510 上の基本ライセンスについて、最大インターフェイス数が 3 プラス管理インターフェイスから無制限のインターフェイスに増加しました。
VLAN 数の増加	7.2(2)	ASA 5505 上の Security Plus ライセンスに対する VLAN 最大数が、5（3 つのフル機能インターフェイス、1 つのフェールオーバー インターフェイス、1 つのバックアップ インターフェイスに制限されるインターフェイス）から 20 のフル機能インターフェイスに増加されました。また、トランク ポート数も 1 から 8 に増加されました。フル機能のインターフェイスの数が 20 になり、バックアップ ISP インターフェイスを停止するために backup interface コマンドを使用する必要がなくなりました。つまり、バックアップ ISP インターフェイス用にフル機能のインターフェイスを使用できるようになりました。backup interface コマンドは、これまでどおり Easy VPN 設定用に使用できます。 VLAN の制限値も変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。
ASA 5510 Security Plus ライセンスに対するギガビット イーサネット サポート	7.2(3)	ASA 5510 は、Security Plus ライセンスを使用する Ethernet 0/0 および 0/1 ポート用にギガビット イーサネット（1000 Mbps）をサポートしています。基本ライセンスでは、これらのポートは引き続きファスト イーサネット（100 Mbps）ポートとして使用されます。いずれのライセンスに対しても、Ethernet 0/2、0/3、および 0/4 はファスト イーサネット ポートのままです。 **（注）**　インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。

表 4-16　ライセンスの機能履歴 （続き）

機能名	プラットフォームリリース	機能情報
Advanced Endpoint Assessment ライセンス	8.0(2)	Advanced Endpoint Assessment ライセンスが導入されました。Cisco AnyConnect またはクライアントレス SSL VPN 接続の条件としてリモート コンピュータでスキャン対象となる、アンチウイルス アプリケーションやアンチスパイウェア アプリケーション、ファイアウォール、オペレーティング システム、および関連アップデートの種類が、大幅に拡張されました。また、任意のレジストリ エントリ、ファイル名、およびプロセス名を指定してスキャン対象にすることもできます。スキャン結果を ASA に送信します。ASA は、ユーザ ログイン クレデンシャルとコンピュータ スキャン結果の両方を使用して、ダイナミック アクセス ポリシー（DAP）を割り当てます。 Advanced Endpoint Assessment ライセンスを使用すると、バージョン要件を満たすように非準拠コンピュータのアップデートを試行する機能を設定して、Host Scan を拡張できます。 シスコは、Host Scan でサポートされるアプリケーションとバージョンの一覧に、Cisco Secure Desktop とは異なるパッケージで、タイムリーなアップデートを提供できます。
ASA 5510 の VPN ロード バランシング	8.0(2)	VPN ロード バランシングが ASA 5510 Security Plus ライセンスでサポートされるようになりました。
AnyConnect for Mobile ライセンス	8.0(3)	AnyConnect for Mobile ライセンスが導入されました。これにより Windows モバイル デバイスは AnyConnect クライアントを使用して ASA に接続できます。
時間ベース ライセンス	8.0(4)/8.1(2)	時間ベース ライセンスがサポートされるようになりました。
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。
Unified Communications Proxy セッション ライセンス	8.0(4)	UC Proxy セッション ライセンスが導入されました。電話プロキシ、Presence Federation Proxy、および Encrypted Voice Inspection アプリケーションでは、それらの接続に TLS プロキシ セッションが使用されます。各 TLS プロキシ セッションは、UC ライセンスの制限に対してカウントされます。これらのアプリケーションは、すべて UC Proxy として包括的にライセンスされるので、混在させたり、組み合わせたりできます。 この機能は、バージョン 8.1 では使用できません。
ボットネット トラフィック フィルタ ライセンス	8.2(1)	ボットネット トラフィック フィルタ ライセンスが導入されました。ボットネット トラフィック フィルタでは、既知の不正なドメインや IP アドレスに対する接続を追跡して、マルウェア ネットワーク アクティビティから保護します。

表 4-16　ライセンスの機能履歴 （続き）

機能名	プラットフォームリリース	機能情報
AnyConnect Essentials ライセンス	8.2(1)	AnyConnect Essentials ライセンスが導入されました。このライセンスにより、AnyConnect VPN クライアントは ASA へのアクセスが可能になります。このライセンスでは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop はサポートされていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。 **（注）** AnyConnect Essentials ライセンスを所有する VPN ユーザは、Web ブラウザを使用してログインし、AnyConnect クライアントをダウンロードおよび起動（WebLaunch）することができます。 このライセンスと AnyConnect Premium ライセンスのいずれでイネーブル化されたかには関係なく、AnyConnect クライアント ソフトウェアには同じクライアント機能のセットが装備されています。 特定の ASA では、AnyConnect Premium ライセンス（全タイプ）または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。 デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Essentials pane] ペインを使用すると、AnyConnect Essentials ライセンスをディセーブルにして他のライセンスを使用できます。
SSL VPN ライセンスの AnyConnect Premium SSL VPN Edition ライセンスへの変更	8.2(1)	SSL VPN ライセンスの名前が AnyConnect Premium SSL VPN Edition ライセンスに変更されました。
SSL VPN の共有ライセンス	8.2(1)	SSL VPN の共有ライセンスが導入されました。複数の ASA で、SSL VPN セッションのプールを必要に応じて共有できます。
モビリティ プロキシ アプリケーションでの Unified Communications Proxy ライセンス不要化	8.2(2)	モビリティ プロキシに UC Proxy ライセンスが必要なくなりました。

表 4-16　ライセンスの機能履歴 （続き）

機能名	プラットフォームリリース	機能情報
ASA 5585-X（SSP-20）用 10 GE I/O ライセンス	8.2(3)	ASA 5585-X（SSP-20）の 10 GE I/O ライセンスを導入し、ファイバ ポートでの 10 ギガビット イーサネットの速度をイネーブルにしました。SSP-60 は、デフォルトで 10 ギガビット イーサネットの速度をサポートします。 **（注）** ASA 5585-X は 8.3(x) ではサポートされていません。
ASA 5585-X（SSP-10）用 10 GE I/O ライセンス	8.2(4)	ASA 5585-X（SSP-10）の 10 GE I/O ライセンスを導入し、ファイバ ポートでの 10 ギガビット イーサネットの速度をイネーブルにしました。SSP-40 は、デフォルトで 10 ギガビット イーサネットの速度をサポートします。 **（注）** ASA 5585-X は 8.3(x) ではサポートされていません。
同一でないフェールオーバー ライセンス	8.3(1)	フェールオーバー ライセンスが各ユニット上で同一である必要がなくなりました。両方のユニットで使用するライセンスは、プライマリ ユニットおよびセカンダリ ユニットからの結合されたライセンスです。 ASDM 画面、[Configuration] > [Device Management] > [Licensing] > [Activation Key] が変更されました。
スタック可能な時間ベース ライセンス	8.3(1)	時間ベース ライセンスがスタッカブルになりました。多くの場合、時間ベース ライセンスは更新の必要があり、旧ライセンスから新しいライセンスへシームレスに移行する必要があります。時間ベース ライセンスだけで使用される機能では、新しいライセンスが適用される前に、ライセンスの有効期限が切れてしまわないことが特に重要です。ASA では時間ベース ライセンスを*スタック*できるので、ライセンスの有効期限が切れたり、新しいライセンスを早めにインストールしたために時間が無駄になったりする心配はありません。
Intercompany Media Engine ライセンス	8.3(1)	IME ライセンスが導入されました。
複数の時間ベース ライセンスの同時アクティブ化	8.3(1)	時間ベース ライセンスを複数インストールできるようになり、同時に機能ごとに 1 つのアクティブなライセンスを保持できるようになりました。 画面、[Configuration] > [Device Management] > [Licensing] > [Activation Key] が変更されました。
時間ベース ライセンスのアクティブ化と非アクティブ化の個別化	8.3(1)	コマンドを使用して、時間ベース ライセンスをアクティブ化または非アクティブ化できるようになりました。 画面、[Configuration] > [Device Management] > [Licensing] > [Activation Key] が変更されました。
AnyConnect Premium SSL VPN Edition ライセンスの AnyConnect Premium SSL VPN ライセンスへの変更	8.3(1)	AnyConnect Premium SSL VPN Edition ライセンスの名前が AnyConnect Premium SSL VPN ライセンスに変更されました。

表 4-16　ライセンスの機能履歴 （続き）

機能名	プラットフォームリリース	機能情報
輸出用のペイロード暗号化なしイメージ	8.3(2)	ASA 5505 ～ 5550 にペイロード暗号化機能のないソフトウェアをインストールした場合、Unified Communications、強力な暗号化 VPN、強力な暗号化管理プロトコルをディセーブルにします。 （注）　この特殊なイメージは 8.3(x) でのみサポートされます。8.4(1) 以降で暗号化機能のないソフトウェアをサポートするには、ASA の特別なハードウェア バージョンを購入する必要があります。
ASA 5550、5580、および 5585-X でのコンテキストの増加	8.4(1)	ASA 5550 および ASA 5585-X（SSP-10）では、コンテキストの最大数が 50 から 100 に引き上げられました。ASA 5580 および 5585-X（SSP-20）以降では、コンテキストの最大数が 50 から 250 に引き上げられました。
ASA 5580 および 5585-X での VLAN 数の増加	8.4(1)	ASA 5580 および ASA 5585-X では、VLAN の最大数が 250 から 1024 に引き上げられました。
ASA 5580 および 5585-X での接続数の増加	8.4(1)	ファイアウォール接続の最大数が次のように引き上げられました。 • ASA 5580-20：1,000,000 から 2,000,000 へ。 • ASA 5580-40：2,000,000 から 4,000,000 へ。 • ASA 5585-X with SSP-10：750,000 から 1,000,000 へ。 • ASA 5585-X with SSP-20：1,000,000 から 2,000,000 へ。 • ASA 5585-X with SSP-40：2,000,000 から 4,000,000 へ。 • ASA 5585-X with SSP-60：2,000,000 から 10,000,000 へ。
AnyConnect Premium SSL VPN ライセンスの AnyConnect Premium ライセンスへの変更	8.4(1)	AnyConnect Premium SSL VPN ライセンスの名前が AnyConnect Premium ライセンスに変更されました。ライセンス情報の表示が「SSL VPN ピア」から「AnyConnect Premium ピア」に変更されました。
ASA 5580 での AnyConnect VPN セッション数の増加	8.4(1)	AnyConnect VPN セッションの最大数が 5,000 から 10,000 に引き上げられました。
ASA 5580 での AnyConnect 以外の VPN セッション数の増加	8.4(1)	AnyConnect 以外の VPN セッションの最大数が 5,000 から 10,000 に引き上げられました。

表 4-16　ライセンスの機能履歴 （続き）

機能名	プラットフォームリリース	機能情報
IKEv2 を使用した IPsec リモート アクセス	8.4(1)	AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスに IKEv2 を使用した IPsec リモート アクセス VPN が追加されました。 （注） ASA での IKEv2 のサポートには次の制限があります。 現時点では、重複したセキュリティ アソシエーションはサポートしていません。 Other VPN ライセンス（以前の IPsec VPN）には IKEv2 サイトツーサイト セッションが追加されました。Other VPN ライセンスは基本ライセンスに含まれています。
輸出用のペイロード暗号化なしハードウェア	8.4(1)	ペイロード暗号化機能のないモデルでは（ASA 5585-X など）、ASA ソフトウェアは ASA で特定の国にエクスポートできるようにして、Unified Communications と VPN 機能をディセーブルにします。
デュアル SSP（SSP-20 および SSP-40）	8.4(2)	SSP-40 および SSP-60 の場合、同じシャーシでレベルが同じ 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-40 と SSP-60 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。2 個の SSP をシャーシで使用する場合、VPN はサポートされません。しかし、VPN がディセーブルになっていないことに注意してください。
ASA 5512-X ～ ASA 5555-X での IPS モジュール ライセンス	8.6(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X での IPS SSP ソフトウェア モジュールには IPS モジュール ライセンスが必要です。
ASA 5580 および ASA 5585-X のクラスタリング ライセンス。	9.0(1)	クラスタリング ライセンスが ASA 5580 および ASA 5585-X に対して追加されました。
ASASM での VPN のサポート	9.0(1)	ASASM は、すべての VPN 機能をサポートするようになりました。
ASASM でのユニファイド コミュニケーションのサポート	9.0(1)	ASASM は、すべてのユニファイド コミュニケーション機能をサポートするようになりました。
SSP-10 および SSP-20 に対する ASA 5585-X デュアル SSP サポート（SSP-40 および SSP-60 に加えて）、デュアル SSP に対する VPN サポート	9.0(1)	ASA 5585-X は、すべての SSP モデルでデュアル SSP をサポートするようになりました（同一シャーシ内で同じレベルの SSP を 2 つ使用できます）。デュアル SSP を使用するときに VPN がサポートされるようになりました。

表 4-16　　ライセンスの機能履歴 （続き）

機能名	プラットフォームリリース	機能情報
ASA 5500-X でのクラスタリングのサポート	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X および ASA 5555-X が 2 ユニット クラスタをサポートするようになりました。2 ユニットのクラスタリングは、基本ライセンスではデフォルトでイネーブルになります。ASA 5512-X では Security Plus ライセンスが必要です。
ASA 5585-X の 16 のクラスタ メンバのサポート	9.2(1)	ASA 5585-X が 16 ユニット クラスタをサポートするようになりました。
ASAv の 1 vCPU および 4 vCPU 標準および Premium ライセンスの導入	9.2(1)	シンプルなライセンス方式で ASAv が導入されました（標準または Premium レベルで 1 vCPU または 4 vCPU 永続ライセンス）。アドオン ライセンスは使用できません。

トランスペアレントまたはルーテッド ファイアウォール モード

この章では、ファイアウォール モードをルーテッドまたはトランスペアレントに設定する方法と、ファイアウォールが各ファイアウォール モードでどのように機能するかについて説明します。この章には、トランスペアレント ファイアウォール動作のカスタマイズに関する情報も含まれます。

マルチコンテキスト モードでは、コンテキストごとに別個にファイアウォール モードを設定できます。

ファイアウォール モードに関する情報

ルーテッド ファイアウォール モードに関する情報

ルーテッド モードでは、Cisco ASA がネットワークのルータ ホップと見なされます。ルーテッド モードは多数のインターフェイスをサポートしています。インターフェイスはそれぞれ異なるサブネット上に置かれます。コンテキスト間でインターフェイスを共有することもできます。

ASA は、接続されたネットワーク間のルータとして機能します。インターフェイスごとに、異なるサブネット上の IP アドレスが必要です。ASA は、複数のダイナミック ルーティング プロトコルをサポートします。ただし、ルーティングのニーズが広範に及ぶ場合は、ASA に依存するのではなく、アップストリームとダウンストリームのルータの高度なルーティング機能を使用することを推奨します。

トランスペアレント ファイアウォール モードに関する情報

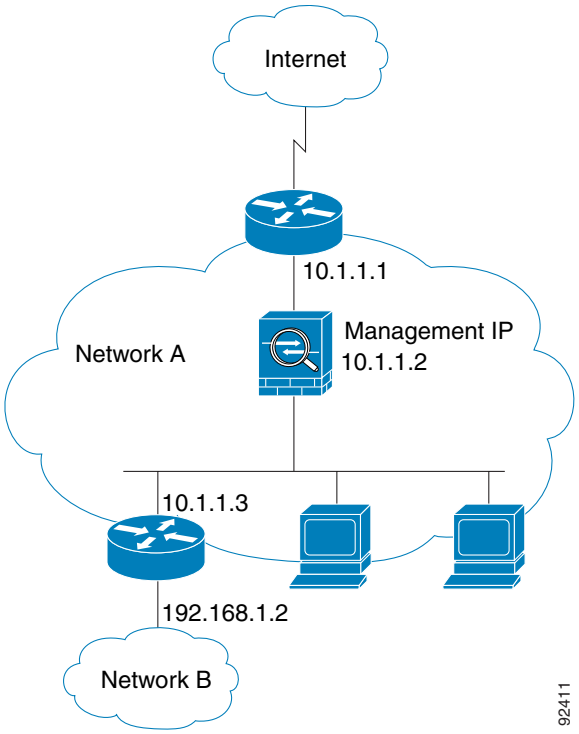
従来、ファイアウォールはルーテッド ホップであり、保護されたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。これに対し、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ネットワークでのトランスペアレント ファイアウォールの使用

ASA は、自身のインターフェイス間を同じネットワークで接続します。トランスペアレント ファイアウォールはルーティングされたホップではないので、既存のネットワークに簡単に導入できます。

図 5-1 に、外部デバイスが内部デバイスと同じサブネット上にある一般的なトランスペアレント ファイアウォール ネットワークを示します。内部ルータとホストは、外部ルータに直接接続されているように見えます。

図 5-1　　トランスペアレント ファイアウォール ネットワーク

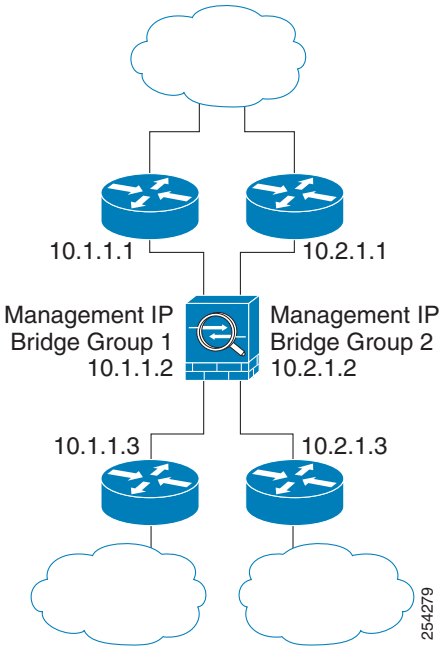


ブリッジ グループ

セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジ グループにグループ化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックは ASA 内の他のブリッジ グループにはルーティングされません。また、トラフィックは外部ルータから ASA 内の他のブリッジ グループにルーティングされる前に、ASA から出る必要があります。ブリッジング機能はブリッジ グループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、すべてのブリッジ グループで共有されます。セキュリティ ポリシーを完全に分離するには、各コンテキスト内に 1 つのブリッジ グループにして、セキュリティ コンテキストを使用します。

図 5-2 に、2 つのブリッジ グループを持つ、ASA に接続されている 2 つのネットワークを示します。

図 5-2　　2 つのブリッジ グループを持つトランスペアレント ファイアウォール ネットワーク



（注）　ブリッジ グループにはそれぞれ管理 IP アドレスが必要です。ASA はブリッジ グループが発信元になるパケットの送信元アドレスとして、この IP アドレスを使用します。管理 IP アドレスは、接続されているネットワークと同じサブネット内にある必要があります。別の管理方法については、「管理インターフェイス（ASA 5512-X 以降）」（P.5-4）を参照してください。

ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。管理 IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

管理インターフェイス（ASA 5512-X 以降）

各ブリッジ グループの管理 IP アドレスのほかに、別の Management *slot*/*port* インターフェイスを追加できます。このインターフェイスはどのブリッジ グループにも属さず、ASA への管理トラフィックのみを許可します。詳細については、「管理インターフェイス」（P.10-2）を参照してください。

レイヤ 3 トラフィックの許可

- ユニキャストの IPv4 および IPv6 トラフィックは、セキュリティの高いインターフェイスから低いインターフェイスに移動する場合、ACL なしで自動的にトランスペアレント ファイアウォールを通過できます。

（注）　ブロードキャストおよびマルチキャスト トラフィックは、アクセス ルールを使用して通過させることができます。詳細については、ファイアウォール コンフィギュレーション ガイドを参照してください。

- ARP は、ACL なしで、両方向ともトランスペアレント ファイアウォールを通過できます。ARP トラフィックは、ARP インスペクションによって制御できます。
- セキュリティの低いインターフェイスからセキュリティの高いインターフェイスに移動するレイヤ 3 トラフィックの場合、セキュリティの低いインターフェイスで拡張 ACL が必要です。詳細については、ファイアウォール コンフィギュレーション ガイドを参照してください。

許可される MAC アドレス

次の宛先 MAC アドレスは、トランスペアレント ファイアウォールを通過できます。このリストにない MAC アドレスはドロップされます。

- FFFF.FFFF.FFFF の TRUE ブロードキャスト宛先 MAC アドレス
- 0100.5E00.0000 ～ 0100.5EFE.FFFF までの IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ～ 3333.FFFF.FFFF までの IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD の BPDU マルチキャスト アドレス
- 0900.0700.0000 ～ 0900.07FF.FFFF までの AppleTalk マルチキャスト MAC アドレス

ルーテッド モードで許可されないトラフィックの通過

ルーテッド モードでは、ACL で許可しても、いくつかのタイプのトラフィックは ASA を通過できません。ただし、トランスペアレント ファイアウォールは、拡張 ACL（IP トラフィックの場合）または EtherType ACL（非 IP トラフィックの場合）を使用してほとんどすべてのトラフィックを許可できます。

IP 以外のトラフィック（AppleTalk、IPX、BPDU、および MPLS など）は、EtherType ACL を使用して通過するように構成できます。

（注）　トランスペアレント モードの ASA は、CDP パケットおよび 0x600 以上の有効な EtherType を持たないパケットの通過を拒否します。サポートされる例外は、BPDU および IS-IS です。

ルーテッド モード機能のためのトラフィックの通過

トランスペアレント ファイアウォールで直接サポートされていない機能の場合は、アップストリーム ルータとダウンストリーム ルータが機能をサポートできるようにトラフィックの通過を許可することができます。たとえば、拡張 ACL を使用して、DHCP トラフィック（サポートされない DHCP リレー機能の代わりに）または IP/TV によって作成されたマルチキャスト トラフィックを許可できます。トランスペアレント ファイアウォールでルーティング プロトコルの隣接関係を確立することもできます。つまり、拡張 ACL に基づいて、OSPF、RIP、EIGRP、または BGP トラフィックを許可できます。同様に、protocols like HSRP や VRRP などのプロトコルは ASA を通過できます。

BPDU の処理

スパニングツリー プロトコルを使用するときのループを防止するために、デフォルトで BPDU が渡されます。BPDU をブロックするには、BPDU を拒否するように EtherType ACL を設定する必要があります。フェールオーバーを使用している場合、BPDU をブロックして、トポロジが変更されたときにスイッチ ポートがブロッキング ステートに移行することを回避できます。詳細については、「トランスペアレント ファイアウォール モードの要件」（P.8-15）を参照してください。

MAC アドレス ルックアップと ルート ルックアップ

ASA がトランスペアレント モードで動作している場合、パケットの発信インターフェイスは、ルート ルックアップではなく MAC アドレス ルックアップを実行することによって決定されます。

ただし、次のトラフィック タイプにはルート ルックアップが必要です。

- ASA で発信されたトラフィック：たとえば、syslog サーバがリモート ネットワークにある場合は、ASA がそのサブネットに到達できるようにスタティック ルートを使用する必要があります。
- NAT がイネーブルである ASA から 1 ホップ以上離れているトラフィック：ASA でネクスト ホップ ゲートウェイを検索するためのルート ルックアップを実行する必要があります。実際のホスト アドレスを把握するには、ASA にスタティック ルートを追加する必要があります。
- インスペクションがイネーブルであり、エンドポイントが ASA から少なくとも 1 ホップ離れている Voice over IP（VoIP）および DNS トラフィック：たとえば、CCM と H.323 ゲートウェイの間にトランスペアレント ファイアウォールを使用し、トランスペアレント ファイアウォールと H.323 ゲートウェイの間にルータがある場合、正常にコールを完了させるには ASA に H.323 ゲートウェイ用のスタティック ルートを追加する必要があります。検査されるトラフィックに対して NAT をイネーブルにすると、スタティック ルートは、パケットに埋め込まれている本当のホスト アドレスの出力インターフェイスを決定する必要があります。影響を受けるアプリケーションは次のとおりです。
  - CTIQBE
  - DNS
  - GTP
  - H.323
  - MGCP
  - RTSP
  - SIP
  - Skinny（SCCP）

ARP Inspection

デフォルトでは、すべての ARP パケットが ASA を通過できます。ARP パケットのフローを制御するには、ARP インスペクションをイネーブルにします。

ARP インスペクションをイネーブルにすると、ASA は、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。

- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、ASA はパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするように ASA を設定できます。

（注） 専用の管理インターフェイス（存在する場合）は、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

ARP インスペクションによって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホスト トラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

MAC Address Table

ASA は、通常のブリッジやスイッチと同様の方法で、MAC アドレス テーブルをラーニングし、構築します。デバイスが ASA 経由でパケットを送信すると、ASA はこの MAC アドレスをテーブルに追加します。テーブルで MAC アドレスと発信元インターフェイスが関連付けられているため、ASA は、パケットが正しいインターフェイスからデバイスにアドレス指定されていることがわかります。

ASA はファイアウォールなので、パケットの宛先 MAC アドレスがテーブルにない場合、ASA は通常のブリッジとは異なり、元のパケットをすべてのインターフェイスにフラッドすることはありません。代わりに、直接接続されたデバイスまたはリモート デバイスに対して次のパケットを生成します。

- 直接接続されたデバイスへのパケット：ASA は宛先 IP アドレスに対して ARP 要求を生成し、ASA は ARP 応答を受信したインターフェイスをラーニングします。
- リモート デバイスへのパケット：ASA は宛先 IP アドレスへの ping を生成し、ASA は ping 応答を受信したインターフェイスをラーニングします。

元のパケットはドロップされます。

ファイアウォール モードのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

デフォルト設定

デフォルト モードはルーテッド モードです。

トランスペアレント モードのデフォルト

- デフォルトでは、すべての ARP パケットが ASA を通過できます。
- ARP インスペクションをイネーブルにした場合、デフォルト設定では、一致しないパケットはフラッドします。
- ダイナミック MAC アドレス テーブルのデフォルトのタイムアウト値は 5 分です。
- デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、ASA は対応するエントリを MAC アドレス テーブルに追加します。

注意事項と制約事項

コンテキスト モードのガイドライン

コンテキストごとにファイアウォール モードを設定します。

トランスペアレント ファイアウォール ガイドライン

- トランスペアレント ファイアウォール モードでは、管理インターフェイスによってデータ インターフェイスと同じ方法で MAC アドレス テーブルがアップデートされます。したがって、いずれかのスイッチ ポートをルーテッド ポートとして設定しない限り、管理インターフェイスおよびデータ インターフェイスを同じスイッチに接続しないでください（デフォルトでは、Catalyst スイッチがすべての VLAN スイッチ ポートの MAC アドレスを共有します）。そうしないと、物理的に接続されたスイッチから管理インターフェイスにトラフィックが到着すると、ASA によって、データ インターフェイスではなく、*管理*インターフェイスを使用してスイッチにアクセスするように MAC アドレス テーブルがアップデートされます。この処理が原因で、一時的にトラフィックが中断します。セキュリティ上の理由から、少なくとも 30 秒間は、スイッチからデータ インターフェイスへのパケットのために MAC アドレス テーブルが ASA によって再アップデートされることはありません。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- ブリッジ グループ管理 IP アドレスを、接続されたデバイスのデフォルト ゲートウェイとして指定しないでください。ASA の他方の側にあるルータをデバイスのデフォルト ゲートウェイとして指定する必要があります。
- 管理トラフィックの戻りパスを指定するために必要な、トランスペアレント ファイアウォールのデフォルト ルートは、1 つのブリッジ グループ ネットワークからの管理トラフィックにだけ適用されます。これは、デフォルト ルートはブリッジ グループのインターフェイスとブリッジ グループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジ グループ ネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別するスタティック ルートを指定する必要があります。

詳細なガイドラインについては、「トランスペアレント モードのインターフェイスのデフォルト設定」（P.13-5）を参照してください。

IPv6 のガイドライン

IPv6 をサポートします。

その他のガイドラインと制限事項

- ファイアウォール モードを変更すると、ASA は実行コンフィギュレーションをクリアします。これは、多くのコマンドが両方のモードでサポートされていないためです。スタートアップ コンフィギュレーションは変更されません。保存しないでリロードすると、スタートアップ コンフィギュレーションがロードされて、モードは元の設定に戻ります。コンフィギュレーション ファイルのバックアップについては、「ファイアウォール モード（シングル モード）の設定」（P.5-10）を参照してください。
- **firewall transparent** コマンドを使用してモードを変更するテキスト コンフィギュレーションを ASA にダウンロードする場合は、このコマンドをコンフィギュレーションの先頭に配置します。先頭に配置することによって、ASA でこのコマンドが読み込まれるとすぐにモードが変更され、その後引き続きダウンロードされたコンフィギュレーションが読み込まれます。このコマンドがコンフィギュレーションの後ろの方にあると、ASA はそれ以前に記述されているコンフィギュレーションの行をすべてクリアします。

トランスペアレント モードでサポートされていない機能

表 5-1 にトランスペアレント モードでサポートされていない機能を示します。

表 5-1　　トランスペアレント モードでサポートされていない機能

機能	説明
ダイナミック DNS	—
DHCP リレー	トランスペアレント ファイアウォールは DHCP サーバとして機能することができますが、DHCP リレー コマンドはサポートしません。2 つの拡張 ACL を使用して DHCP トラフィックを通過させることができるので、DHCP リレーは必要ありません。1 つは内部インターフェイスから外部インターフェイスへの DHCP 要求を許可し、もう 1 つはサーバからの応答を逆方向に許可します。
ダイナミック ルーティング プロトコル	ただし、ASA で発信されたトラフィックのスタティック ルートを追加できます。拡張 ACL を使用して、ダイナミック ルーティング プロトコルが ASA を通過できるようにすることもできます。
マルチキャスト IP ルーティング	拡張 ACL で許可することによって、マルチキャスト トラフィックが ASA を通過できるようにすることができます。
QoS	—
通過トラフィック用の VPN ターミネーション	トランスペアレント ファイアウォールは、管理接続に対してのみサイトツーサイト VPN トンネルをサポートします。これは、ASA を通過するトラフィックに対して VPN 接続を終端しません。拡張 ACL を使用して VPN トラフィックに ASA を通過させることはできますが、非管理接続は終端されません。クライアントレス SSL VPN もサポートされていません。
ユニファイド コミュニケーション	—

ファイアウォール モード（シングル モード）の設定

この項では、CLI を使用してファイアウォール モードを変更する方法を説明します。シングル モードの場合およびマルチ モードで現在接続されているコンテキスト（通常は管理コンテキスト）の場合は、ASDM でモードを変更できません。他のマルチ モードのコンテキストでは、コンテキストごとに ASDM でモードを設定できます。「セキュリティ コンテキストの設定」（P.7-20）を参照してください。

（注）　ファイアウォール モードを変更すると実行コンフィギュレーションがクリアされるので、他のコンフィギュレーションを行う前にファイアウォール モードを設定することをお勧めします。

前提条件

モードを変更すると、ASA は実行コンフィギュレーションをクリアします（詳細については、「注意事項と制約事項」（P.5-8）を参照してください）。

- 設定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コンフィギュレーションをバックアップしてください。新しいコンフィギュレーション作成時の参照としてこのバックアップを使用できます。
- モードを変更するには、コンソール ポートで CLI を使用します。ASDM コマンドライン インターフェイス ツールや SSH などの他のタイプのセッションを使用すると、コンフィギュレーションがクリアされるときに切断されるので、いずれにしてもコンソール ポートを使用して ASA に再接続する必要があります。
- コンテキスト内でモードを設定します。

手順の詳細

（注）　設定が削除された後にファイアウォール モードをトランスペアレントに設定し、ASDM への管理アクセスを設定するには、「ASA サービス モジュールの ASDM アクセスの設定」（P.2-10）または「ASA サービス モジュールの ASDM アクセスの設定」（P.2-10）を参照してください。

コマンド	目的
firewall transparent **例：** `ciscoasa(config)# firewall transparent`	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。モードをルーテッドに変更するには、**no firewall transparent** コマンドを入力します。 （注）　ファイアウォール モードの変更では確認は求められず、ただちに変更が行われます。

トランスペアレント ファイアウォール用の ARP インスペクションの設定

この項では、ARP インスペクションを設定する方法について説明します。

ARP インスペクションの設定のタスク フロー

ARP インスペクションを設定するには、次の手順を実行します。

ステップ 1　「スタティック ARP エントリの追加」（P.5-11）に従って、スタティック ARP エントリを追加します。ARP インスペクションは ARP パケットを ARP テーブルのスタティック ARP エントリと比較するので、この機能にはスタティック ARP エントリが必要です。

ステップ 2　「ARP インスペクションのイネーブル化」（P.5-12）に従って、ARP インスペクションをイネーブルにします。

スタティック ARP エントリの追加

ARP インスペクションは、ARP パケットを ARP テーブルのスタティック ARP エントリと比較します。ホストは IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARP テーブルは、ARP 応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合など）、エントリは更新される前にタイムアウトします。

（注）　トランスペアレント ファイアウォールは、ASA との間のトラフィック（管理トラフィックなど）に、ARP テーブルのダイナミック ARP エントリを使用します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Advanced] > [ARP] > [ARP Static Table] ペインを選択します。

ステップ 2　（オプション）ダイナミック ARP エントリに ARP タイムアウトを設定するには、[ARP Timeout] フィールドに値を入力します。

このフィールドでは、ASA が ARP テーブルを再構築するまでの時間を、60 ～ 4294967 秒の範囲で設定します。デフォルトは 14400 秒です。ARP テーブルを再構築すると、自動的に新しいホスト情報が更新され、古いホスト情報が削除されます。ホスト情報は頻繁に変更されるため、タイムアウトを短くすることが必要になる場合があります。

ステップ 3　（任意、8.4（5）のみ）非接続サブネットを使用するには、[Allow non-connected subnets] チェックボックスをオンにします。ASA ARP キャッシュには、直接接続されたサブネットからのエントリだけがデフォルトで含まれています。ARP キャッシュをイネーブルにして、間接接続されたサブネットを含めることもできます。セキュリティ リスクを認識していない場合は、この機能をイネーブルにすることは推奨しません。この機能は、ASA に対するサービス拒否（DoS）攻撃の手助けをしてきました。任意のインターフェイスのユーザが大量の ARP 応答を送信して、偽エントリで ASA ARP テーブルにがあふれる可能性があります。

次の機能を使用する場合は、この機能を使用する必要がある可能性があります。

- セカンダリ サブネット。
- トラフィック転送の隣接ルートのプロキシ ARP。

ステップ 4　[Add] をクリックします。

[Add ARP Static Configuration] ダイアログボックスが表示されます。

ステップ 5　[Interface] ドロップダウン リストから、ホスト ネットワークに接続されるインターフェイスを選択します。

ステップ 6　[IP Address] フィールドに、ホストの IP アドレスを入力します。

ステップ 7　[MAC Address] フィールドに、ホストの MAC アドレスを入力します。たとえば、「00e0.1e4e.3d8b」のように入力します。

ステップ 8　このアドレスでプロキシ ARP を実行するには、[Proxy ARP] チェックボックスをオンにします。

ASA は、指定された IP アドレスの ARP 要求を受信すると、指定された MAC アドレスで応答します。

ステップ 9　[OK]、続いて [Apply] をクリックします。

次の作業

「ARP インスペクションのイネーブル化」（P.5-12）に従って、ARP インスペクションをイネーブルにします。

ARP インスペクションのイネーブル化

この項では、ARP インスペクションをイネーブルにする方法について説明します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Advanced] > [ARP] > [ARP Inspection] ペインを選択します。

ステップ 2　ARP インスペクションをイネーブルにするインターフェイス行を選択し、[Edit] をクリックします。

[Edit ARP Inspection] ダイアログボックスが表示されます。

ステップ 3　ARP インスペクションをイネーブルにするには、[Enable ARP Inspection] チェックボックスをオンにします。

ステップ 4　（オプション）一致しない ARP パケットをフラッドするには、[Flood ARP Packets] チェックボックスをオンにします。

デフォルトでは、スタティック ARP エントリのどの要素にも一致しないパケットが、送信元のインターフェイスを除くすべてのインターフェイスからフラッドされます。MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、ASA はパケットをドロップします。

このチェックボックスをオフにすると、一致しないパケットはすべてドロップされます。これにより、スタティック エントリにある ARP だけが ASA を通過するように制限されます。

（注）　Management 0/0 または 0/1 インターフェイスあるいはサブインターフェイスがある場合、これらのインターフェイスは、このパラメータがフラッドに設定されていてもパケットをフラッドしません。

ステップ 5　[OK]、続いて [Apply] をクリックします。

トランスペアレント ファイアウォール用の MAC アドレス テーブルのカスタマイズ

ここでは、MAC アドレス テーブルをカスタマイズする方法について説明します。

- 「スタティック MAC アドレスの追加」（P.5-13）
- 「MAC アドレス ラーニングのディセーブル化」（P.5-14）

スタティック MAC アドレスの追加

通常、MAC アドレスは、特定の MAC アドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。スタティック MAC アドレスは、必要に応じて MAC アドレス テーブルに追加できます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エントリと同じ MAC アドレスを持つクライアントが、そのスタティック エントリに一致しないインターフェイスにトラフィックを送信しようとした場合、ASA はトラフィックをドロップし、システム メッセージを生成します。スタティック ARP エントリを追加するときに（「スタティック ARP エントリの追加」（P.5-11）を参照）、スタティック MAC アドレス エントリは MAC アドレス テーブルに自動的に追加されます。

MAC アドレス テーブルにスタティック MAC アドレスを追加するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Setup] > [Bridging] > [MAC Address Table] ペインを選択します。

ステップ 2　（オプション）MAC アドレス エントリがタイムアウトするまでに MAC アドレス テーブルに残る時間を設定するには、[Dynamic Entry Timeout] フィールドに値を入力します。

この値は、5 ～ 720 分（12 時間）の範囲で指定します。5 分がデフォルトです。

ステップ 3　[Add] をクリックします。

[Add MAC Address Entry] ダイアログボックスが表示されます。

ステップ 4　[Interface Name] ドロップダウン リストから、MAC アドレスに関連付けられている送信元インターフェイスを選択します。

ステップ 5　[MAC Address] フィールドに、MAC アドレスを入力します。

ステップ 6　[OK]、続いて [Apply] をクリックします。

MAC アドレス ラーニングのディセーブル化

デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、ASA は対応するエントリを MAC アドレス テーブルに追加します。必要に応じて MAC アドレス ラーニングをディセーブルにできますが、この場合、MAC アドレスをテーブルにスタティックに追加しないと、トラフィックが ASA を通過できなくなります。

MAC アドレス ラーニングをディセーブルにするには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Setup] > [Bridging] > [MAC Learning] ペインを選択します。

ステップ 2　MAC ラーニングをディセーブルにするには、インターフェイス行を選択して、[Disable] をクリックします。

ステップ 3　MAC ラーニングを再度イネーブルにするには、[Enable] をクリックします。

ステップ 4　[Apply] をクリックします。

ファイアウォール モードの例

ここでは、トラフィックが ASA を通過する様子の例を示します。

- 「ルーテッド ファイアウォール モードで ASA を通過するデータ」（P.5-14）
- 「トランスペアレント ファイアウォールを通過するデータの動き」（P.5-20）

ルーテッド ファイアウォール モードで ASA を通過するデータ

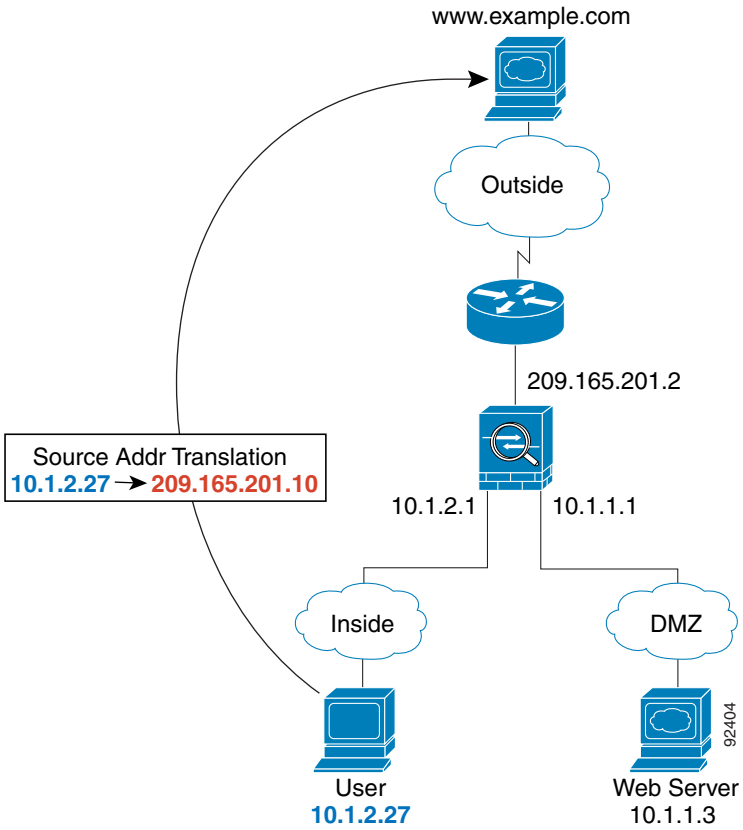
ここでは、ルーテッド ファイアウォール モードでデータが ASA をどのように通過するのかを説明します。

- 「内部ユーザが Web サーバにアクセスする」（P.5-15）
- 「外部ユーザが DMZ 上の Web サーバにアクセスする」（P.5-16）
- 「内部ユーザが DMZ 上の Web サーバにアクセスする」（P.5-17）
- 「外部ユーザが内部ホストにアクセスしようとする」（P.5-18）
- 「DMZ ユーザが内部ホストにアクセスしようとする」（P.5-19）

内部ユーザが Web サーバにアクセスする

図 5-3 は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 5-3　　内部から外部へ



次の手順では、データが ASA をどのように通過するかを示します（図 5-3 を参照）。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

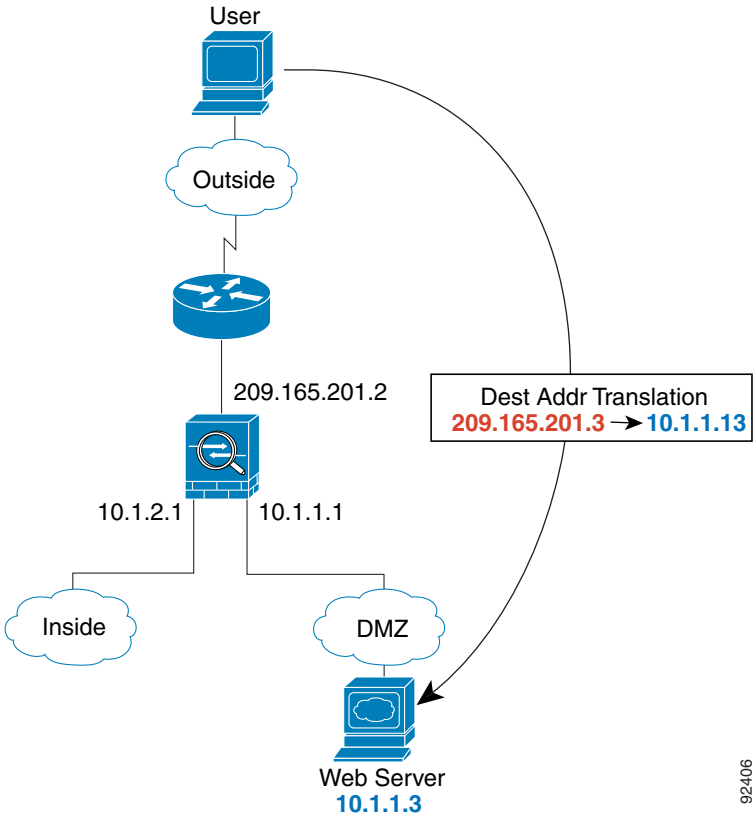
   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. ASA は、ローカル送信元アドレス（10.1.2.27）を、外部インターフェイス サブネット上のグローバル アドレス 209.165.201.10 に変換します。

   グローバル アドレスは任意のサブネット上に置くことができますが、外部インターフェイス サブネットに置くとルーティングが簡素化されます。
4. 次に、ASA はセッションが確立されたことを記録し、外部インターフェイスからパケットを転送します。
5. www.example.com が要求に応答すると、パケットは ASA を通過します。これはすでに確立されているセッションであるため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。ASA は、グローバル宛先アドレスをローカル ユーザ アドレス 10.1.2.27 に変換せずに、NAT を実行します。
6. ASA は、パケットを内部ユーザに転送します。

外部ユーザが DMZ 上の Web サーバにアクセスする

図 5-4 は、外部ユーザが DMZ Web サーバにアクセスしていることを示しています。

図 5-4　外部から DMZ へ



次の手順では、データが ASA をどのように通過するかを示します（図 5-4 を参照）。

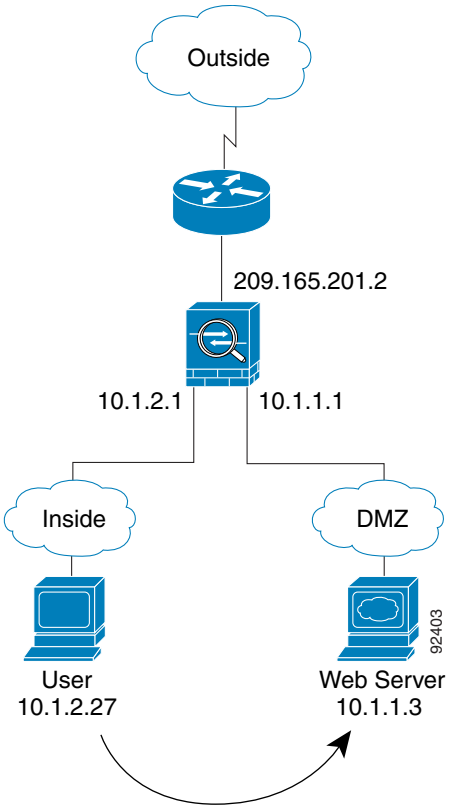
1. 外部ネットワーク上のユーザは、外部インターフェイス サブネット上にあるグローバル宛先アドレス 209.165.201.3 を使用して DMZ Web サーバから Web ページを要求します。
2. ASA は、パケットを受信し、ローカル アドレス 10.1.1.3 に対する宛先アドレスは変換しません。
3. 新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、ASA はパケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
4. 次に、ASA はセッション エントリを高速パスに追加し、DMZ インターフェイスからパケットを転送します。
5. DMZ Web サーバが要求に応答すると、パケットは ASA を通過します。また、セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。ASA は、ローカル送信元アドレスを 209.165.201.3 に変換することによって、NAT を実行します。
6. ASA は、パケットを外部ユーザに転送します。

内部ユーザが DMZ 上の Web サーバにアクセスする

図 5-5 は、内部ユーザが DMZ Web サーバにアクセスしていることを示しています。

図 5-5　　内部から DMZ へ



次の手順では、データが ASA をどのように通過するかを示します（図 5-5 を参照）。

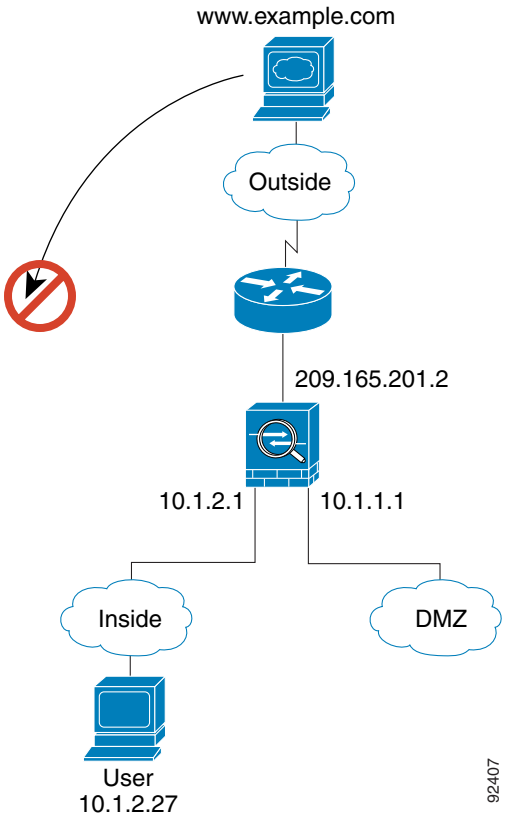
1. 内部ネットワーク上のユーザは、宛先アドレス 10.1.1.3 を使用して DMZ Web サーバから Web ページを要求します。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. 次に、ASA はセッションが確立されたことを記録し、DMZ インターフェイスからパケットを転送します。
4. DMZ Web サーバが要求に応答すると、パケットは高速パスを通過します。これのため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
5. ASA は、パケットを内部ユーザに転送します。

外部ユーザが内部ホストにアクセスしようとする

図 5-6 は、外部ユーザが内部ネットワークにアクセスしようとしていることを示しています。

図 5-6　外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します（図 5-6 を参照）。

1. 外部ネットワーク上のユーザが、内部ホストに到達しようとします（ホストにルーティング可能な IP アドレスがあると想定します）。

   内部ネットワークがプライベート アドレスを使用している場合、外部ユーザが NAT なしで内部ネットワークに到達することはできません。外部ユーザは既存の NAT セッションを使用して内部ユーザに到達しようとすることが考えられます。

2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）に従って、パケットが許可されているかどうかを確認します。

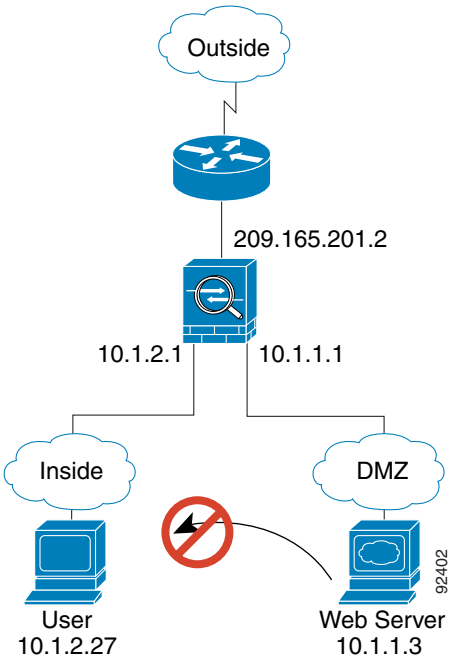
3. パケットが拒否され、ASA はパケットをドロップし、接続試行をログに記録します。

   外部ユーザが内部ネットワークを攻撃しようとした場合、ASA は多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。

DMZ ユーザが内部ホストにアクセスしようとする

図 5-7 は、DMZ 内のユーザが内部ネットワークにアクセスしようとしていることを示しています。

図 5-7　　DMZ から内部へ



次の手順では、データが ASA をどのように通過するかを示します（図 5-7 を参照）。

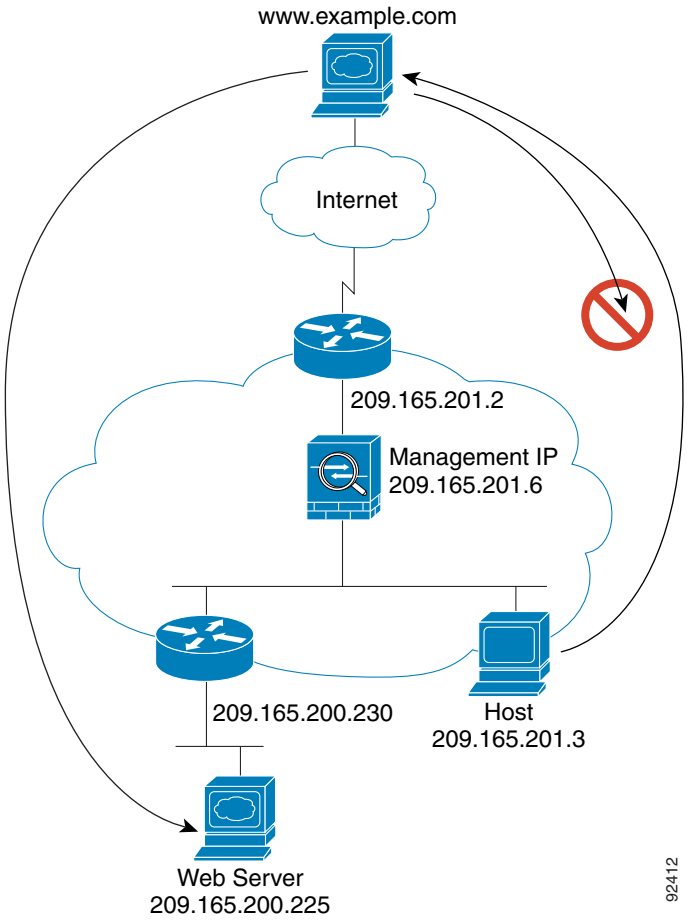
1. DMZ ネットワーク上のユーザが、内部ホストに到達しようとします。DMZ はインターネット上のトラフィックをルーティングする必要がないので、プライベート アドレッシング方式はルーティングを回避しません。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）に従って、パケットが許可されているかどうかを確認します。

   パケットが拒否され、ASA はパケットをドロップし、接続試行をログに記録します。

トランスペアレント ファイアウォールを通過するデータの動き

図 5-8 に、パブリック Web サーバを含む内部ネットワークを持つ一般的なトランスペアレント ファイアウォールの実装を示します。内部ユーザがインターネット リソースにアクセスできるよう、ASA にはアクセス リストがあります。別のアクセス リストによって、外部ユーザは内部ネットワーク上の Web サーバだけにアクセスできます。

図 5-8　　一般的なトランスペアレント ファイアウォールのデータ パス



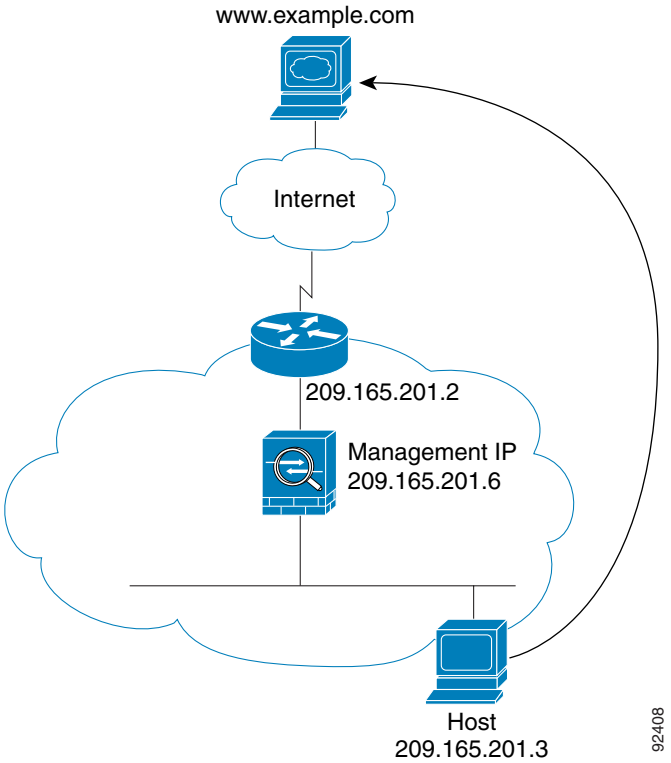
ここでは、データが ASA をどのように通過するかを示します。

- 「内部ユーザが Web サーバにアクセスする」（P.5-21）
- 「NAT を使用して内部ユーザが Web サーバにアクセスする」（P.5-22）
- 「外部ユーザが内部ネットワーク上の Web サーバにアクセスする」（P.5-23）
- 「外部ユーザが内部ホストにアクセスしようとする」（P.5-24）

内部ユーザが Web サーバにアクセスする

図 5-9 は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 5-9　　内部から外部へ



次の手順では、データが ASA をどのように通過するかを示します（図 5-9 を参照）。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。
2. ASA はパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

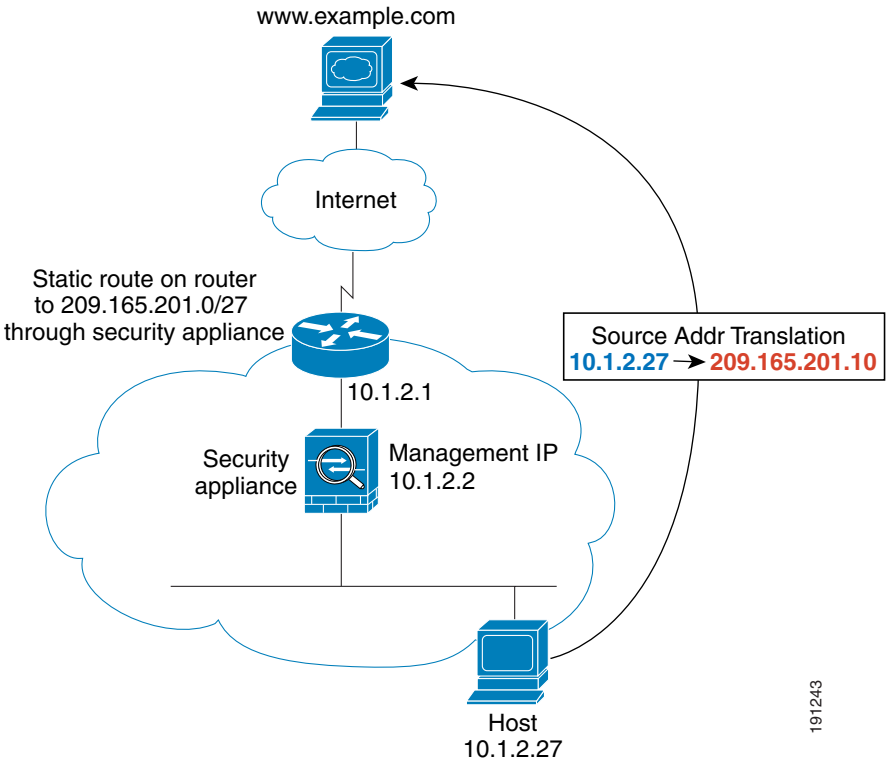
   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. ASA は、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、ASA は外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータのアドレス 209.165.201.2 です。

   宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求または ping を送信します。最初のパケットはドロップされます。
5. Web サーバが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
6. ASA は、パケットを内部ユーザに転送します。

NAT を使用して内部ユーザが Web サーバにアクセスする

図 5-10 は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 5-10　NAT を使用して内部から外部へ



次の手順では、データが ASA をどのように通過するかを示します（図 5-10 を参照）。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。
2. ASA はパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、ASA は、固有なインターフェイスに従ってパケットを分類します。
3. ASA は実際のアドレス（10.1.2.27）をマッピング アドレス 209.165.201.10 に変換します。

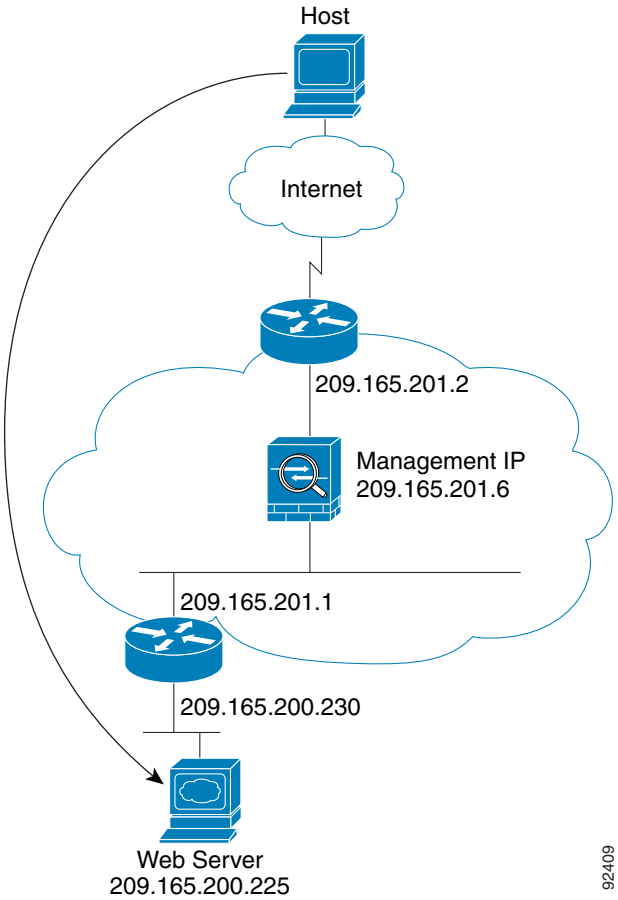
   マッピング アドレスは外部インターフェイスと同じネットワーク上にないため、アップストリーム ルータに ASA をポイントするマッピング ネットワークへのスタティック ルートがあることを確認します。
4. 次に、ASA はセッションが確立されたことを記録し、外部インターフェイスからパケットを転送します。
5. 宛先 MAC アドレスがテーブル内にある場合、ASA は外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータのアドレス 10.1.2.1 です。

   宛先 MAC アドレスが ASA のテーブルにない場合、ASA は、ARP 要求と ping を送信して、MAC アドレスを検出しようとします。最初のパケットはドロップされます。
6. Web サーバが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
7. ASA は、マッピング アドレスを実際のアドレス 10.1.2.27 にせずに、NAT を実行します。

外部ユーザが内部ネットワーク上の Web サーバにアクセスする

図 5-11 は、外部ユーザが内部 Web サーバにアクセスしていることを示しています。

図 5-11　　外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します（図 5-11 を参照）。

1. 外部ネットワーク上のユーザは、内部 Web サーバから Web ページを要求します。
2. ASA はパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

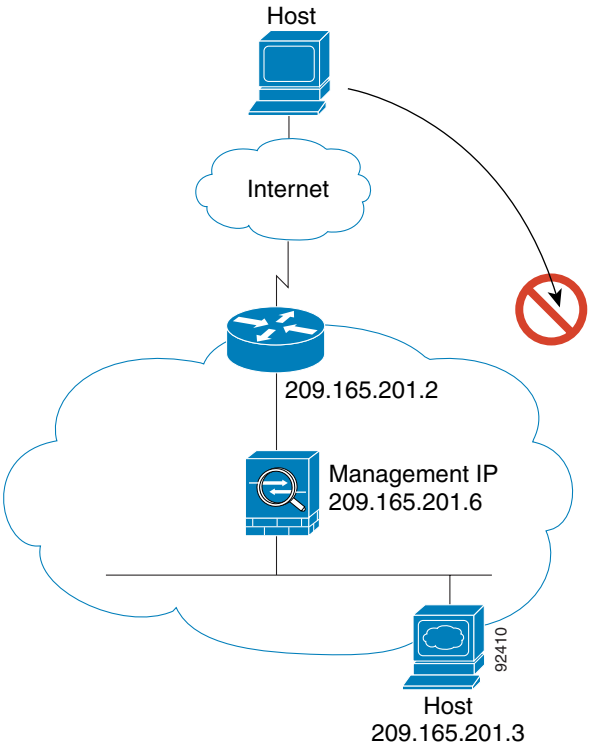
   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. ASA は、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、ASA は内部インターフェイスからパケットを転送します。宛先 MAC アドレスは、ダウンストリーム ルータ 209.165.201.1 のアドレスです。

   宛先 MAC アドレスが ASA のテーブルにない場合、ASA は、ARP 要求と ping を送信して、MAC アドレスを検出しようとします。最初のパケットはドロップされます。
5. Web サーバが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
6. ASA は、パケットを外部ユーザに転送します。

外部ユーザが内部ホストにアクセスしようとする

図 5-12 は、外部ユーザが内部ネットワーク上のホストにアクセスしようとしていることを示しています。

図 5-12　外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します（図 5-12 を参照）。

1. 外部ネットワーク上のユーザが、内部ホストに到達しようとします。
2. ASA はパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されているかどうかを確認します。

   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. 外部ホストを許可するアクセス リストは存在しないため、パケットは拒否され、ASA によってドロップされます。
4. 外部ユーザが内部ネットワークを攻撃しようとした場合、ASA は多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。

ファイアウォール モードの機能履歴

表 5-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 5-2　ファイアウォール モードの機能履歴

機能名	プラットフォーム リリース	機能情報
トランスペアレント ファイアウォール モード	7.0(1)	トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。 **firewall transparent**、および **show firewall** コマンドが導入されました。 ASDM ではファイアウォール モードを設定できません。コマンドライン インターフェイスを使用する必要があります。
ARP インスペクション	7.0(1)	ARP インスペクションは、すべての ARP パケットの MAC アドレス、IP アドレス、および送信元インターフェイスを、ARP テーブルのスタティック エントリと比較します。 **arp**、**arp-inspection**、および **show arp-inspection** コマンドが導入されました。
MAC アドレス テーブル	7.0(1)	トランスペアレント ファイアウォール モードは MAC アドレス テーブルを使用します。 **mac-address-table static**、**mac-address-table aging-time**、**mac-learn disable**、および **show mac-address-table** コマンドが導入されました。
トランスペアレント ファイアウォール ブリッジ グループ	8.4(1)	セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジ グループにグループ化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。ブリッジ グループのトラフィックは他のブリッジ グループから隔離されます。シングル モードでは最大 8 個、マルチ モードではコンテキストあたり最大 8 個のブリッジ グループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを追加できます。 **（注）** ASA 5505 に複数のブリッジ グループを設定できますが、ASA 5505 のトランスペアレント モードのデータ インターフェイスは 2 つという制限は、実質的にブリッジ グループを 1 つだけ使用できることを意味します。 次の画面が変更または導入されました。 [Configuration] > [Device Setup] > [Interfaces] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Bridge Group Interface] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface]

表 5-2　ファイアウォール モードの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
間接接続されたサブネットの ARP キャッシュの追加	8.4(5)/9.1(2)	ASA ARP キャッシュには、直接接続されたサブネットからのエントリだけがデフォルトで含まれています。また、ARP キャッシュに間接接続されたサブネットを含めることができるようになりました。セキュリティ リスクを認識していない場合は、この機能をイネーブルにすることは推奨しません。この機能は、ASA に対するサービス拒否（DoS）攻撃の手助けをしてきました。任意のインターフェイスのユーザが大量の ARP 応答を送信して、偽エントリで ASA ARP テーブルにがあふれる可能性があります。 次の機能を使用する場合は、この機能を使用する必要がある可能性があります。 • セカンダリ サブネット。 • トラフィック転送の隣接ルートのプロキシ ARP。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced]> [ARP] > [ARP Static Table]。
マルチ コンテキスト モードのファイアウォール モードの混合がサポートされます。	8.5(1)/9.0(1)	セキュリティ コンテキスごとに個別のファイアウォール モードを設定できます。したがってその一部をトランスペアレント モードで実行し、その他をルーテッド モードで実行することができます。 **firewall transparent** コマンドが変更されました。 シングル モードでは、ASDM でファイアウォール モードを設定することはできません。コマンドライン インターフェイスを使用する必要があります。 マルチ モードでは、次の画面が変更になりました。[Configuration] > [Context Management] > [Security Contexts]。
トランスペアレント モードのブリッジ グループの最大数が 250 に増加	9.3(1)	ブリッジ グループの最大数が 8 個から 250 個に増えました。シングル モードでは最大 250 個、マルチ モードではコンテキストあたり最大 250 個のブリッジ グループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを設定できます。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Interfaces] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Bridge Group Interface] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface]

スタートアップ ウィザード

この章では、ASDM Startup Wizard について説明します。このウィザードでは、Cisco ASA の初期設定を手順に従って行い、基本設定を定義できます。

Startup Wizard へのアクセス

Startup Wizard にアクセスするには、以下のいずれかのオプションを選択します。

- [Wizards] > [Startup Wizard] を選択する。
- [Configuration] > [Device Setup] > [Startup Wizard] を選択して、[Launch Startup Wizard] をクリックする。

Startup Wizard のガイドライン

コンテキスト モードのガイドライン

Startup Wizard はシステム コンテキストではサポートされません。

Startup Wizard の画面

画面の実際の順序は、設定時の選択によって決まります。特に明記していない限り、各画面はすべてのモードまたはモデルで使用できます。

Starting Point または Welcome

- 既存の設定を変更するには、[Modify existing configuration] オプション ボタンをクリックします。

- 設定を工場出荷時のデフォルト値に設定するには、[Reset configuration to factory defaults] オプション ボタンをクリックします。
  - Management 0/0 インターフェイスの IP アドレスとサブネット マスクをデフォルト値（192.168.1.1）と異なる値に設定するには、[Configure the IP address of the management interface] チェックボックスをオンにします。

（注）　設定を工場出荷時のデフォルト値にリセットすると、[Cancel] をクリックしたり、この画面を閉じたりしても、変更を元に戻せません。

マルチ コンテキスト モードでは、この画面にパラメータは含まれていません。

基本設定

この画面では、ホスト名、ドメイン名、およびイネーブル パスワードを設定します。

関連項目

「ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定」（P.14-1）

インターフェイスの画面

インターフェイスの画面は、選択したモードとモデルによって異なります。

外部インターフェイスの設定（ルーテッド モード）

- 外部インターフェイス（セキュリティ レベルが最も低いインターフェイス）の IP アドレスを設定します。
- IPv6 アドレスを設定します。

関連項目

- 「一般的なインターフェイス パラメータの設定」（P.12-6）
- 「IPv6 アドレッシングの設定」（P.12-15）

外部インターフェイスの設定 - PPPoE（ルーテッド モード、シングル モード）

外部インターフェイスの PPPoE 設定を行います。

関連項目

「PPPoE IP Address and Route Settings」（P.12-11）

Management IP Address Configuration（トランスペアレント モード）

IPv4 の場合は、管理トラフィックと、ASA を通過するトラフィックの両方の各ブリッジ グループに対し、管理 IP アドレスが必要です。この画面では、BVI 1 の IP アドレスを設定します。

関連項目

「ブリッジ グループの設定」（P.13-7）

その他のインターフェイスの設定

その他のインターフェイスのパラメータを設定します。

関連項目

- 「一般的なインターフェイス パラメータの設定」（P.12-6）
- 「同じセキュリティ レベルの通信の許可」（P.12-20）

スタティック ルート

スタティック ルートを設定します。

関連項目

「スタティック ルートの設定」（P.20-2）

DHCP サーバ

DHCP サーバを設定します。

関連項目

「DHCP サーバの設定」（P.15-4）

アドレス変換（NAT/PAT）

外部（セキュリティ レベルが最も低いインターフェイス）にアクセスするときの内部アドレス（セキュリティ レベルが最も高いインターフェイス）の NAT または PAT を設定します。詳細については、ファイアウォール コンフィギュレーション ガイドを参照してください。

管理アクセス

- ASDM、Telnet、または SSH アクセスを設定します。
- ASDM にアクセスするための HTTP サーバへのセキュアな接続をイネーブルにするには、[Enable HTTP server for HTTPS/ASDM access] チェックボックスをオンにします。
- [Enable ASDM history metrics] チェックボックスをオンにします 。

関連項目

- 「管理アクセスの設定」（P.36-3）
- 「履歴メトリックのイネーブル化」（P.3-34）

IPS の基本設定

シングル コンテキスト モードでは、ASDM で Startup Wizard を使用して、基本的な IPS ネットワーク設定を行います。これらの設定は、ASA コンフィギュレーションではなく、IPS コンフィギュレーションに保存されます。詳細については、ファイアウォール コンフィギュレーション ガイドを参照してください。

ASA CX の基本設定（ASA 5585-X）

ASDM の Startup Wizard を使用して、ASA CX の管理アドレスおよび Auth Proxy Port を設定できます。これらの設定は、ASA コンフィギュレーションではなく ASA CX コンフィギュレーションに保存されます。ASA CX CLI での追加のネットワーク設定も必要です。この画面については、ファイアウォール コンフィギュレーション ガイドを参照してください。

ASA FirePOWER の基本設定

ASDM の Startup Wizard を使用して、ASA FirePOWER の管理アドレス情報を設定し、エンドユーザ ライセンス契約（EULA）を承認することができます。これらの設定は、ASA コンフィギュレーションではなく、ASA FirePOWER コンフィギュレーションに保存されます。ASA FirePOWER CLI サーバ上でも、いくつかの値を設定する必要があります。詳細については、ファイアウォール コンフィギュレーション ガイドの ASA FirePOWER モジュールの章を参照してください。

タイム ゾーンおよびクロック コンフィギュレーション

時計のパラメータを設定します。

関連項目

「日時の設定」（P.14-7）

Auto Update Server（シングル モード）

- [Enable Auto Update Server for ASA] チェックボックスをオンにして、Auto Update サーバを設定します。
- IPS モジュールがある場合は、[Enable Signature and Engine Updates from Cisco.com] チェックボックスをオンにします。次の追加パラメータを設定します。
  - Cisco.com のユーザ名とパスワードを入力し、確認のためにパスワードを再入力します。
  - 24 時間制を使用して、hh:mm:ss 形式で開始時間を入力します。

関連項目

「Auto Update の設定」（P.37-30）

Startup Wizard Summary

この画面には、ASAに対して行ったすべての設定の概要が表示されます。

- [Back] をクリックして、前の画面の設定を変更します。
- 次のいずれかを選択します。
  - Startup Wizard をブラウザから直接起動した場合は、[Finish] をクリックすると、ウィザードで作成されたコンフィギュレーション設定が ASA に自動的に送信され、フラッシュ メモリに保存されます。
  - ASDM 内で Startup Wizard を実行した場合は、[File] > [Save] [Running Configuration to Flash] を選択し、その設定を明示的にフラッシュ メモリに保存する必要があります。

Startup Wizard の履歴

表 6-1　Startup Wizard の履歴

機能名	プラットフォーム リリース	説明
スタートアップ ウィザード	7.0(1)	このウィザードが導入されました。 [Wizards] > [Startup Wizard] 画面が導入されました。
IPS の設定	8.4(1)	IPS モジュールでは、[IPS Basic Configuration] 画面が Startup Wizard に追加されました。IPS モジュールに対するシグニチャ アップデートが、[Auto Update] 画面に追加されました。ASA でクロックが設定されるように、[Time Zone and Clock Configuration] 画面が追加されました。IPS モジュールはそのクロックを ASA から取得します。 次の画面が導入または変更されました。 [Wizards] > [Startup Wizard] > [IPS Basic Configuration] [Wizards] > [Startup Wizard] > [Auto Update] [Wizards] > [Startup Wizard] > [Time Zone and Clock Configuration]

PART 2

ハイ アベイラビリティとスケーラビリティ

マルチ コンテキスト モード

この章では、Cisco ASA にマルチ セキュリティ コンテキストを設定する方法について説明します。

セキュリティ コンテキストに関する情報

1 台の ASA を、セキュリティ コンテキストと呼ばれる複数の仮想デバイスに分割することができます。各コンテキストは独立したデバイスとして動作し、独自のセキュリティ ポリシー、インターフェイス、および管理者を持ちます。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでサポートされない機能については、「注意事項と制約事項」（P.7-14）を参照してください。

この項では、セキュリティ コンテキストの概要について説明します。

セキュリティ コンテキストの一般的な使用方法

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

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

コンテキスト コンフィギュレーション ファイル

この項では、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」（P.7-2）
- 「システム設定」（P.7-2）
- 「管理コンテキストの設定」（P.7-2）

コンテキスト コンフィギュレーション

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

システム設定

システム管理者は、各コンテキスト コンフィギュレーションの場所、割り当てられたインターフェイス、およびその他のコンテキスト操作パラメータをシステム コンフィギュレーションに設定することで、コンテキストを追加および管理します。このコンフィギュレーションは、シングル モードのコンフィギュレーション同様、スタートアップ コンフィギュレーションです。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバからコンテキストをダウンロードするなど）、システムは*管理コンテキスト*として指定されているコンテキストのいずれかを使用します。システム コンフィギュレーションに含まれているものに、フェールオーバー トラフィック専用の特殊なフェールオーバー インターフェイスがあります。

管理コンテキストの設定

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインする

と、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザに制限する必要があります。管理コンテキストは、リモートではなくフラッシュ メモリに置く必要があります。

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

ASA によるパケットの分類方法

ASA に入ってくるパケットはいずれも分類する必要があります。その結果、ASA は、どのコンテキストにパケットを送信するかを決定できます。

- 「有効な分類子の基準」（P.7-3）
- 「分類の例」（P.7-4）

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

有効な分類子の基準

この項では、分類子で使用される基準について説明します。

- 「固有のインターフェイス」（P.7-3）
- 「固有の MAC アドレス」（P.7-3）
- 「NAT コンフィギュレーション」（P.7-4）

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

ルーティング テーブルはパケット分類には使用されません。

固有のインターフェイス

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

固有の MAC アドレス

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

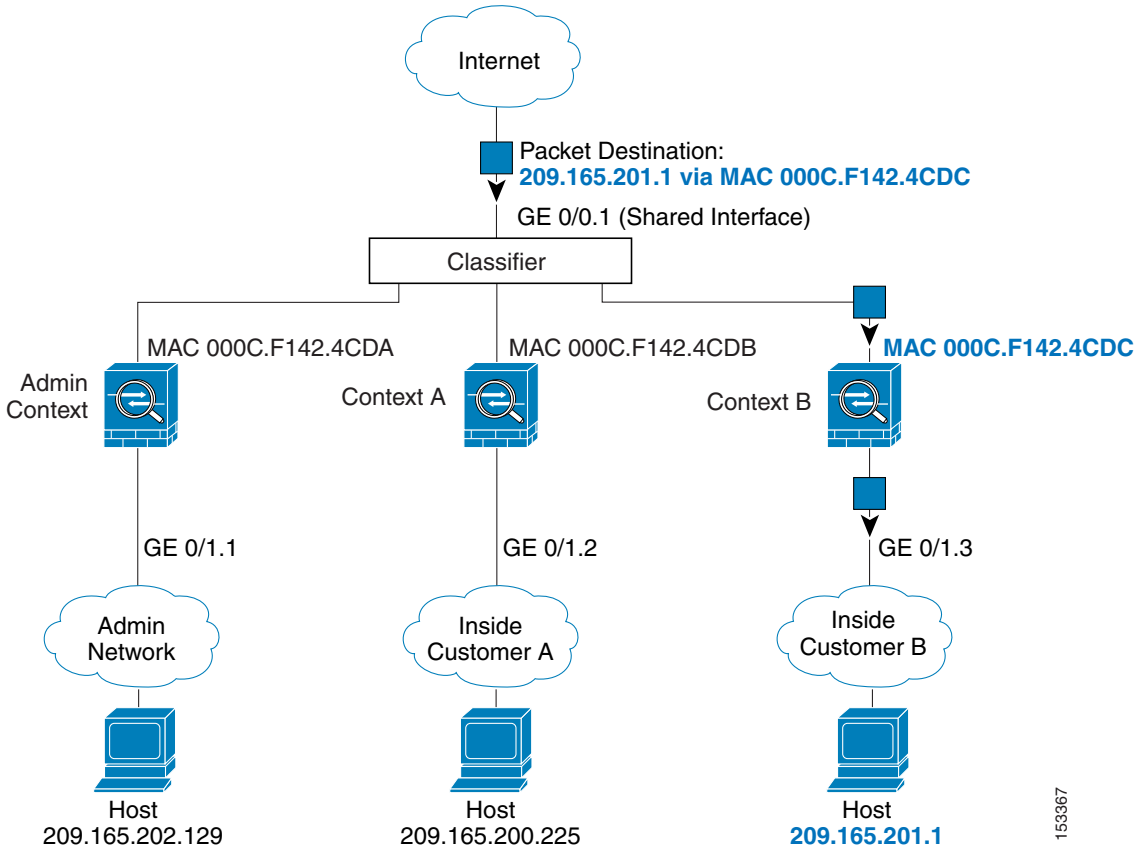
NAT コンフィギュレーション

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

分類の例

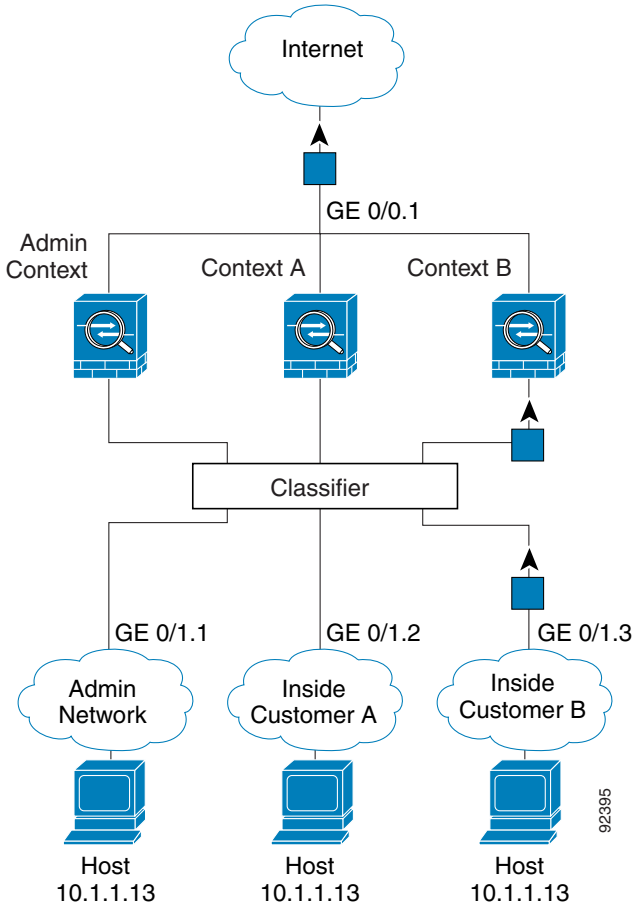
図 7-1 に、外部インターフェイスを共有するマルチ コンテキストを示します。コンテキスト B にはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをコンテキスト B に割り当てます。

図 7-1　　インターフェイスを共有しているときの MAC アドレスを使用したパケット分類



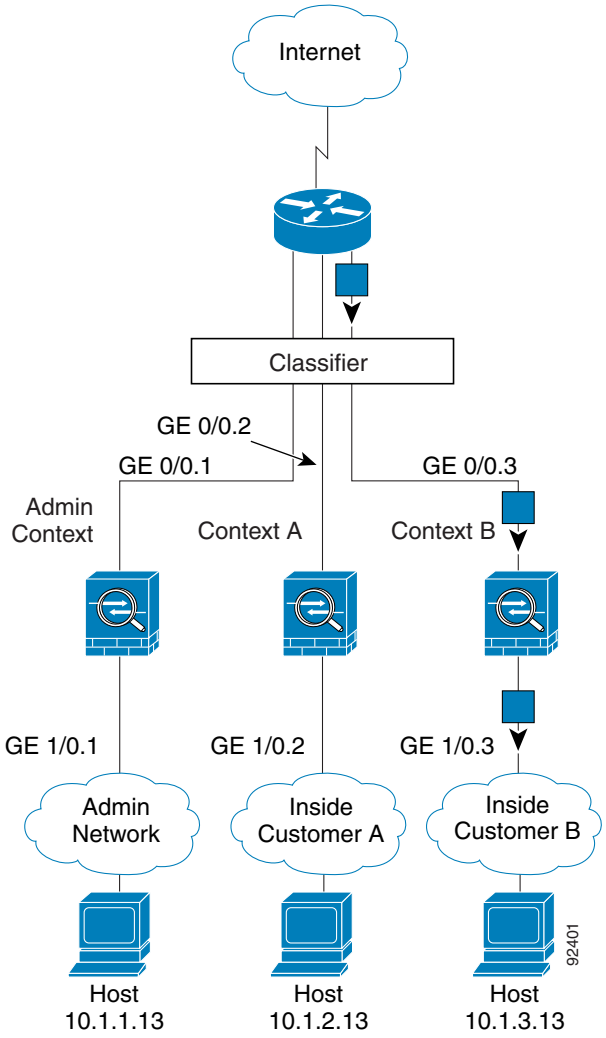
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。図 7-2 に、内部ネットワークのコンテキスト B 上のホストがインターネットにアクセスしている場合を示します。分類子は、パケットをコンテキスト B に割り当てます。これは、入力インターフェイスがギガビット イーサネット 0/1.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 7-2　　内部ネットワークからの着信トラフィック



トランスペアレント ファイアウォールでは、固有のインターフェイスを使用する必要があります。図 7-3 に示すパケットは、インターネットから、内部ネットワークのコンテキスト B 上のホスト宛てです。分類子は、パケットをコンテキスト B に割り当てます。これは、入力インターフェイスがギガビット イーサネット 1/0.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 7-3　　トランスペアレント ファイアウォールのコンテキスト



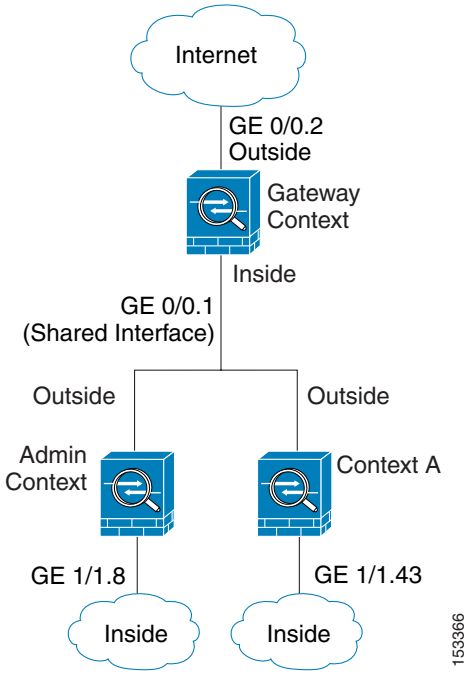
セキュリティ コンテキストのカスケード接続

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

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

図 7-4 に、ゲートウェイの背後に 2 つのコンテキストがあるゲートウェイ コンテキストを示します。

図 7-4　　コンテキストのカスケード接続



セキュリティ コンテキストへの管理アクセス

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

- 「システム管理者のアクセス」（P.7-8）
- 「コンテキスト管理者のアクセス」（P.7-8）

システム管理者のアクセス

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

- ASA コンソールにアクセスします。

  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します。

  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 36 章「管理アクセス」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ユーザ名「enable_15」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必要があります。または、十分な特権が与えられた別の名前でログインします。新しいユーザ名でログインするには、**login** コマンドを入力します。たとえば、「admin」というユーザ名で管理コンテキストにログインします。管理コンテキストにコマンド許可コンフィギュレーションはありませんが、それ以外のすべてのコンテキストにはコマンド許可があります。便宜を図るために、各コンテキスト コンフィギュレーションには、最大特権を持つ「admin」ユーザが含まれています。管理コンテキストからコンテキスト A に変更したときは、ユーザ名が enable_15 に変更されるので、**login** コマンドを入力して再度「admin」としてログインする必要があります。コンテキスト B に変更したら、再度 **login** コマンドを入力して、「admin」でログインする必要があります。

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

コンテキスト管理者のアクセス

Telnet、SSH、または ASDM を使用して、コンテキストにアクセスできます。管理外コンテキストにログインすると、アクセスできるのはそのコンテキストのコンフィギュレーションだけになります。そのコンテキストに個別のログインを付与できます。Telnet、SSH、および ASDM アクセスをイネーブルにする方法、また管理認証を設定する方法については、第 36 章「管理アクセス」を参照してください。

リソース管理に関する情報

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

リソース クラス

ASA では、リソース クラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。クラスの設定を使用するには、コンテキストを定義するときに、そのコンテキストをクラスに割り当てます。すべてのコンテキストは、別のクラスに割り当てられていなければ、デフォルト クラスに属します。したがって、コンテキストをデフォルト クラスに割り当てる必要は特にありません。コンテキストは 1 つのリソース クラスにだけ割り当てることができます。このルールの例外は、メンバー クラスで未定義の制限はデフォルト クラスから継承されることです。そのため実際には、コンテキストがデフォルト クラスおよび別のクラスのメンバになります。

リソース制限値

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

ほとんどのリソースについては、ASA は、クラスに割り当てられたコンテキストごとにリソースの一部を確保することはしません。代わりに、ASA はコンテキストごとに上限を設定します。リソースをオーバーサブスクライブする場合や、または一部のリソースを無制限にする場合は、少数のコンテキストがそのリソースを「使い果たす」ことがあり、他のコンテキストへのサービスに影響する可能性があります。例外は、VPN リソース タイプです。このリソースはオーバーサブスクライブできないため、各コンテキストに割り当てられたリソースは保証されます 割り当てられた量を超える、VPN セッションの一時的なバーストに対応できるように、ASA は「burst」という VPN リソース タイプをサポートしています。このリソースは、残りの未割り当て VPN セッションに等しくなります。バースト セッションはオーバーサブスクライブでき、コンテキストが先着順で使用できます。

デフォルト クラス

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルト クラスに属します。コンテキストをデフォルト クラスに積極的に割り当てる必要はありません。

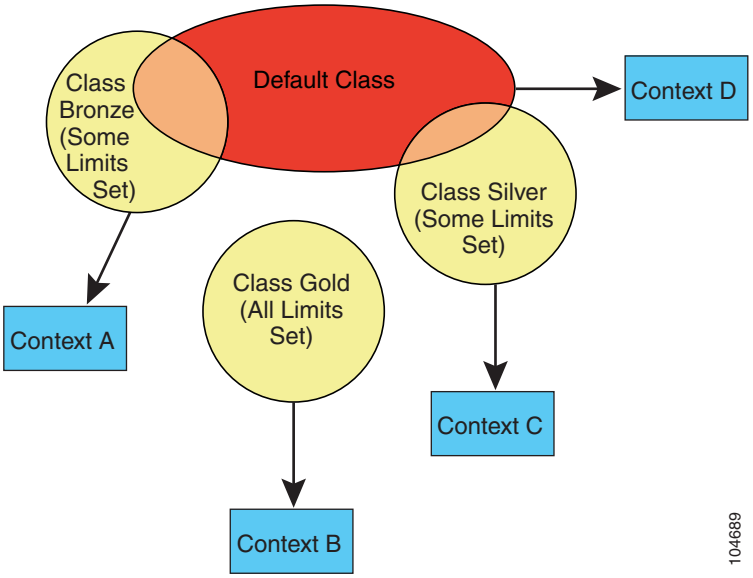
コンテキストがデフォルト クラス以外のクラスに属する場合、それらのクラス設定は常にデフォルト クラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバ コンテキストはそれらの制限にデフォルト クラスを使用します。たとえば、すべての同時接続に 2% の制限を設定したがその他の制限を設定せずにクラスを作成した場合、他のすべての制限はデフォルト クラスから継承されます。これとは逆に、すべてのリソースに対する制限値を設定してクラスを作成すると、そのクラスではデフォルト クラスの設定を何も使用しません。

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

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

図 7-5 に、デフォルト クラスと他のクラスの関係を示します。コンテキスト A および C は、いくつかの制限が設定されたクラスに属しており、それ以外の制限はデフォルト クラスから継承します。コンテキスト B は、属している Gold クラスですべての制限が設定されているため、デフォルト クラスから制限値を継承しません。コンテキスト D はクラスに割り当てられなかったため、デフォルトでデフォルト クラスのメンバになります。

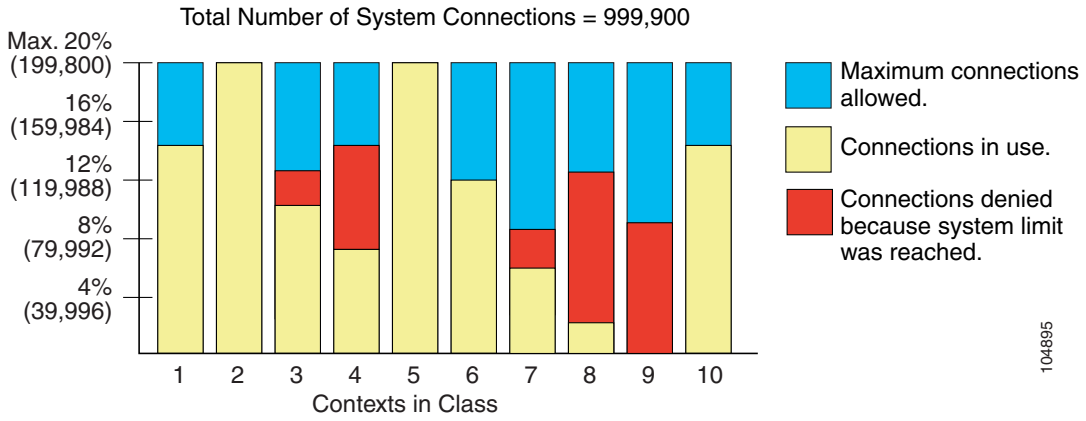
図 7-5　　リソース クラス



オーバーサブスクライブ型リソースの使用

ASA をオーバーサブスクライブするには、あるリソースをコンテキストに割り当てた率の合計が 100% を超えるように割り当てます（非バーストの VPN リソースを除く）。たとえば、接続がコンテキストあたり 20% までに制限されるように Bronze クラスを設定し、それから 10 個のコンテキストをそのクラスに割り当てれば、リソースの合計を 200% にできます。コンテキストがシステム制限を超えて同時に使用する場合、各コンテキストは意図した 20% を下回ります（図 7-6 を参照）。

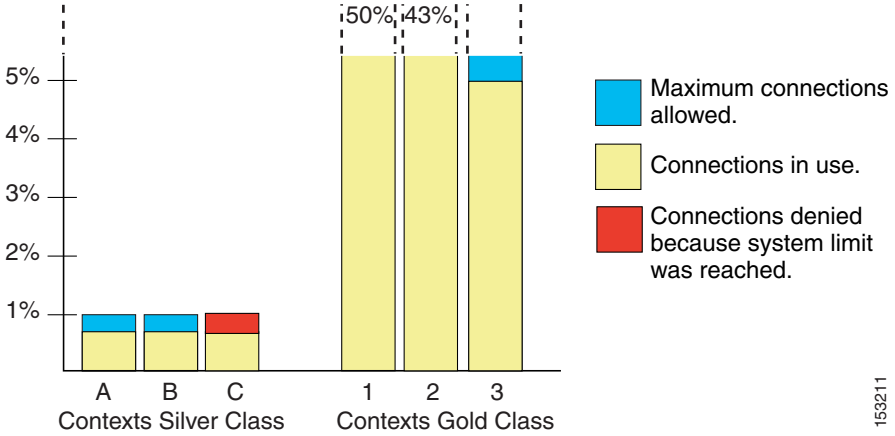
図 7-6　　リソースのオーバーサブスクライブ



無制限リソースの使用

ASA では、割合や絶対値ではなく、クラス内の 1 つ以上のリソースへの無制限アクセスを割り当てることができます。リソースが無制限の場合、コンテキストはシステムで使用可能な量までリソースを使用できます。たとえば、コンテキスト A、B、C が Silver クラスに属しており、クラスの各メンバの使用量が接続の 1% に制限されていて、合計 3% が割り当てられているが、3 つのコンテキストが現在使用しているのは合計 2% だけだとします。Gold クラスは、接続に無制限にアクセスできます。Gold クラスのコンテキストは、「未割り当て」接続のうち 97% を超える分も使用できます。つまり、現在コンテキスト A、B、C で使用されていない、接続の 1% も使用できます。その場合は、コンテキスト A、B、C の使用量が、こ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（図 7-7 を参照）。無制限アクセスの設定は、システムのオーバーサブスクライブ量を制御する機能が劣る点を除いて、ASA のオーバーサブスクライブに類似しています。

図 7-7　　無制限リソース



MAC アドレスに関する情報

コンテキストがインターフェイスを共有できるようにするために、ASA はデフォルトで各共有コンテキスト インターフェイスに仮想 MAC アドレスを割り当てます。自動生成をカスタマイズまたはディセーブルにするには、「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」（P.7-25）を参照してください。

MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。あるインターフェイスを共有させる場合に、コンテキストごとにそのインターフェイスの固有 MAC アドレスを設定していなかった場合は、他の分類方法が試行されますが、その方法では十分にカバーされないことがあります。パケットの分類の詳細については、「ASA によるパケットの分類方法」（P.7-3）を参照してください。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、コンテキスト内のインターフェイスの MAC アドレスを手動で設定できます。MAC アドレスの手動設定の詳細については、「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）を参照してください。

デフォルトの MAC アドレス

（8.5(1.7) 以降）MAC アドレスの自動生成はデフォルトでイネーブルです。ASA は、インターフェイス（ASA 5500-X）またはバックプレーン（ASASM）MAC アドレスの最後の 2 バイトに基づいてプレフィックスを自動生成します。必要に応じて、プレフィックスをカスタマイズできます。

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

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

「MAC アドレス形式」（P.7-12）も参照してください。

（注）（8.5(1.6) 以前）中断のないフェールオーバー ペアのアップグレードを維持するために、フェイルオーバーがイネーブルの場合には、ASA はリロードに対する既存のレガシーの自動生成の設定を変換しません。ただし、フェールオーバーを使用するときは、プレフィックスによる生成方式に手動で変更することを強く推奨します（特に ASASM の場合）。プレフィックス方式を使用しない場合、異なるスロット番号にインストールされた ASASM では、フェールオーバーが発生した場合に MAC アドレスの変更が行われ、トラフィックの中断が発生することがあります。アップグレード後に、プレフィックス方式での MAC アドレス生成を使用するには、MAC アドレス自動生成を再度イネーブルにすると、プレフィックスが使用されるようになります。従来の方法についての詳細については、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。

手動 MAC アドレスとの通信

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

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

フェールオーバー用の MAC アドレス

フェールオーバーで使用できるように、ASA はインターフェイスごとにアクティブとスタンバイの両方の MAC アドレスを生成します。アクティブ ユニットがフェールオーバーしてスタンバイ ユニットがアクティブになると、その新規アクティブ ユニットがアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。詳細については、「MAC アドレス形式」（P.7-12）を参照してください。

MAC アドレス形式

ASA は、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

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

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

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

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

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

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

マルチ コンテキスト モードのライセンス要件

モデル	ライセンス要件
ASA 5512-X	• 基本ライセンス：サポートされない。 • Security Plus ライセンス：2 コンテキスト *オプション ライセンス：5 コンテキスト*
ASA 5515-X	基本ライセンス：2 コンテキスト *オプション ライセンス：5 コンテキスト*
ASA 5525-X	基本ライセンス：2 コンテキスト *オプション ライセンス：5、10、または 20 コンテキスト*
ASA 5545-X	基本ライセンス：2 コンテキスト *オプション ライセンス：5、10、20、または 50 コンテキスト*
ASA 5555-X	基本ライセンス：2 コンテキスト *オプション ライセンス：5、10、20、50、または 100 コンテキスト。*
ASA 5585-X（SSP-10）	基本ライセンス：2 コンテキスト *オプション ライセンス：5、10、20、50、または 100 コンテキスト。*
ASA 5585-X（SSP-20、-40、および -60）	基本ライセンス：2 コンテキスト *オプション ライセンス:5、10、20、50、100、または 250 コンテキスト。*
ASASM	基本ライセンス：2 コンテキスト *オプション ライセンス:5、10、20、50、100、または 250 コンテキスト。*
ASAv	サポートしない

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。ASA に接続する方法の詳細については、第 2 章「使用する前に」を参照してください。

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

ファイアウォール モードのガイドライン

ルーテッドおよびトランスペアレント ファイアウォール モードでサポートされます。コンテキストごとにファイアウォール モードを設定します。

フェールオーバーのガイドライン

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

IPv6 のガイドライン

IPv6 をサポートします。

（注）　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。

サポートされていない機能

マルチ コンテキスト モードでサポートされていない機能は、次のとおりです。

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

その他のガイドライン

- コンテキスト モード（シングルまたはマルチ）は、リブートされても持続されますが、コンフィギュレーション ファイルには保存されません。コンフィギュレーションを別のデバイスにコピーする必要がある場合は、新規デバイスのモードを match に設定します。
- 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：一部のモデル（ASA 5585-X など）では内部フラッシュ メモリに FAT 16 ファイル システムが使用されており、8.3 形式に準拠した短い名前を使用しないか、大文字を使用すると、長いファイル名を保存するためにファイル システムのスロットが使い尽くされるため、512 以上のファイルおよびフォルダを保存できません（http://support.microsoft.com/kb/120138/en-us を参照）。

デフォルト設定

- デフォルトで、ASA はシングル コンテキスト モードになります。
- 「デフォルト クラス」（P.7-9）を参照してください。
- 「デフォルトの MAC アドレス」（P.7-12）を参照してください。

マルチ コンテキストの設定

この項では、マルチ コンテキスト モードを設定する方法について説明します。

マルチ コンテキスト モードの設定のタスク フロー

マルチ コンテキスト モードを設定するには、次の手順を実行します。

ステップ 1　マルチ コンテキスト モードをイネーブルにします。「マルチ コンテキスト モードのイネーブル化とディセーブル化」（P.7-16）を参照してください。

ステップ 2　（オプション）リソース管理のクラスを設定します。「リソース管理のクラスの設定」（P.7-17）を参照してください。**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。

- ASA 5500-X：第 10 章「基本的なインターフェイス コンフィギュレーション（ASA 5512-X 以降）」
- ASASM：第 2 章「使用する前に」

ステップ 4　セキュリティ コンテキストを設定します。「セキュリティ コンテキストの設定」（P.7-20）を参照してください。

ステップ 5　（オプション）MAC アドレス割り当てをカスタマイズします。「コンテキスト インターフェイスへの MAC アドレスの自動割り当て」（P.7-25）を参照してください。

ステップ 6　コンテキストのインターフェイス コンフィギュレーションを完成させます。第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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 モードのイネーブル化とディセーブル化

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

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、第 8 章「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 モードのイネーブル化

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

前提条件

スタートアップ コンフィギュレーションをバックアップします。シングル モードからマルチ モードに変換すると、ASA は実行コンフィギュレーションを 2 つのファイルに変換します。元のスタートアップ コンフィギュレーションは保存されません。「ファイルの管理」（P.37-14）を参照してください。

手順の詳細

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

シングル コンテキスト モードの復元

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

前提条件

この手順はシステム実行スペースで実行します。

手順の詳細

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

リソース管理のクラスの設定

システム コンフィギュレーションでクラスを設定するには、次の手順を実行します。新しい値を指定してコマンドを再入力すると、特定のリソース制限値を変更できます。

前提条件

この手順はシステム実行スペースで実行します。

ガイドライン

表 7-1 に、リソース タイプと制限を示します。

表 7-1　リソース名と制限

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限[1]	説明
ASDM Sessions	同時接続数	最小 1 最大 5	32	ASDM 管理セッション。 **（注）** ASDM セッションでは、2 つの HTTPS 接続を使用します。1 つは常に存在するモニタリング用の接続、もう 1 つは変更時にのみ存在するコンフィギュレーション変更用の接続です。たとえば、ASDM セッションのシステム制限が 32 の場合、HTTPS セッション数は 64 に制限されます。
接続手段 Conns/sec[2]	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、「モデルごとにサポートされている機能のライセンス」（P.4-1）を参照してください。 レート：該当なし	任意の 2 つのホスト間の TCP または UDP 接続（1 つのホストと他の複数のホストとの間の接続を含む）。
Hosts	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	レート	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	65,535	トランスペアレント ファイアウォール モードでは、MAC アドレス テーブルで許可される MAC アドレス数。
Routes	同時接続数	該当なし	該当なし	ダイナミック ルート。
Site-to-Site VPN Burst	同時接続数	該当なし	モデルに応じた Other VPNvpn セッション数から、Site-to-Site 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。	Site-to-Site 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、Site-to-Site 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 Site-to-Site VPN Burst に使用できます。コンテキストに対するセッションを保証する Site-to-Site VPN とは異なり、Site-to-Site VPN Burst 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は、先着順にバースト プールを使用できます。

表 7-1　　リソース名と制限 （続き）

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限[1]	説明
Site-to-Site 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」（P.4-1）を参照してください。	サイトツーサイト VPN セッション。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたセッションは、そのコンテキストに対して保証されます。
SSH	同時接続数	最小 1 最大 5	100	SSH セッション
Syslogs/sec	レート	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[2]	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。

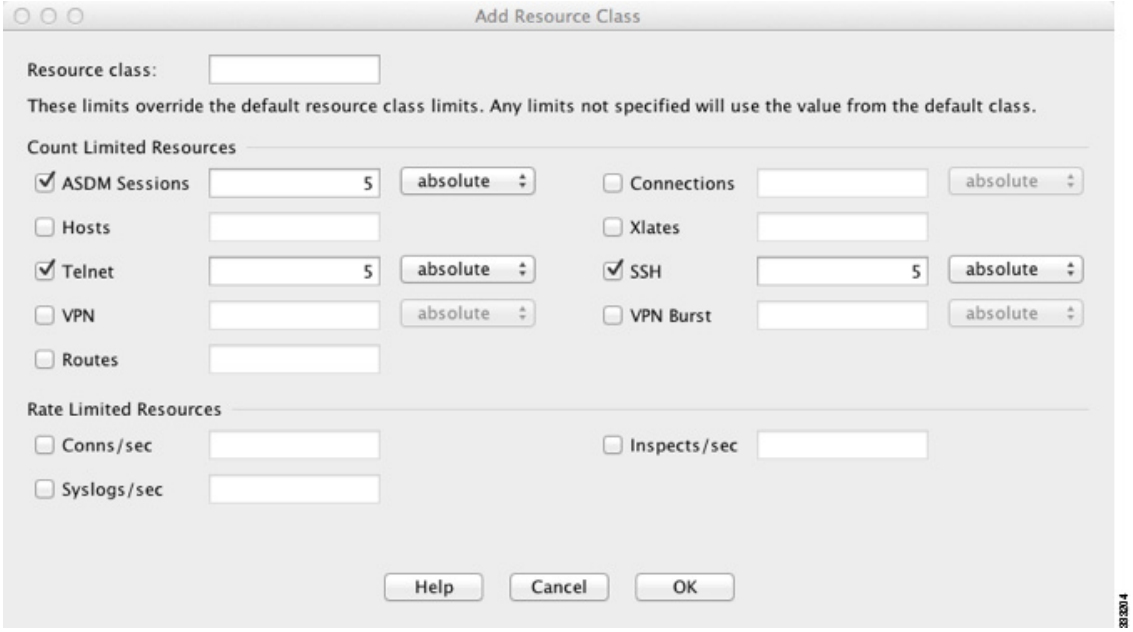
1. このカラムに「該当なし」と記述されている場合、そのリソースにはハード システム制限がないため、リソースのパーセンテージを設定できません。
2. syslog メッセージは、xlates または conns のいずれか制限が低い方に対して生成されます。たとえば、xlates の制限を 7、conns の制限を 9 に設定した場合、ASA は syslog メッセージ 321001（「Resource 'xlates' limit of 7 reached for context 'ctx1'」）のみ生成し、321002（「Resource 'conn rate' limit of 5 reached for context 'ctx1'」）は生成しません。

手順の詳細

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] > [Resource Class] の順に選択し、[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。

各リソース タイプの説明については、表 7-1（P.7-18）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。

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、表 7-1（P.7-18）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 は制限を無制限と設定

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。

前提条件

- この手順はシステム実行スペースで実行します。
- ASASM では、第 2 章「使用する前に」に従ってスイッチ上の ASASM に VLAN を割り当てます。

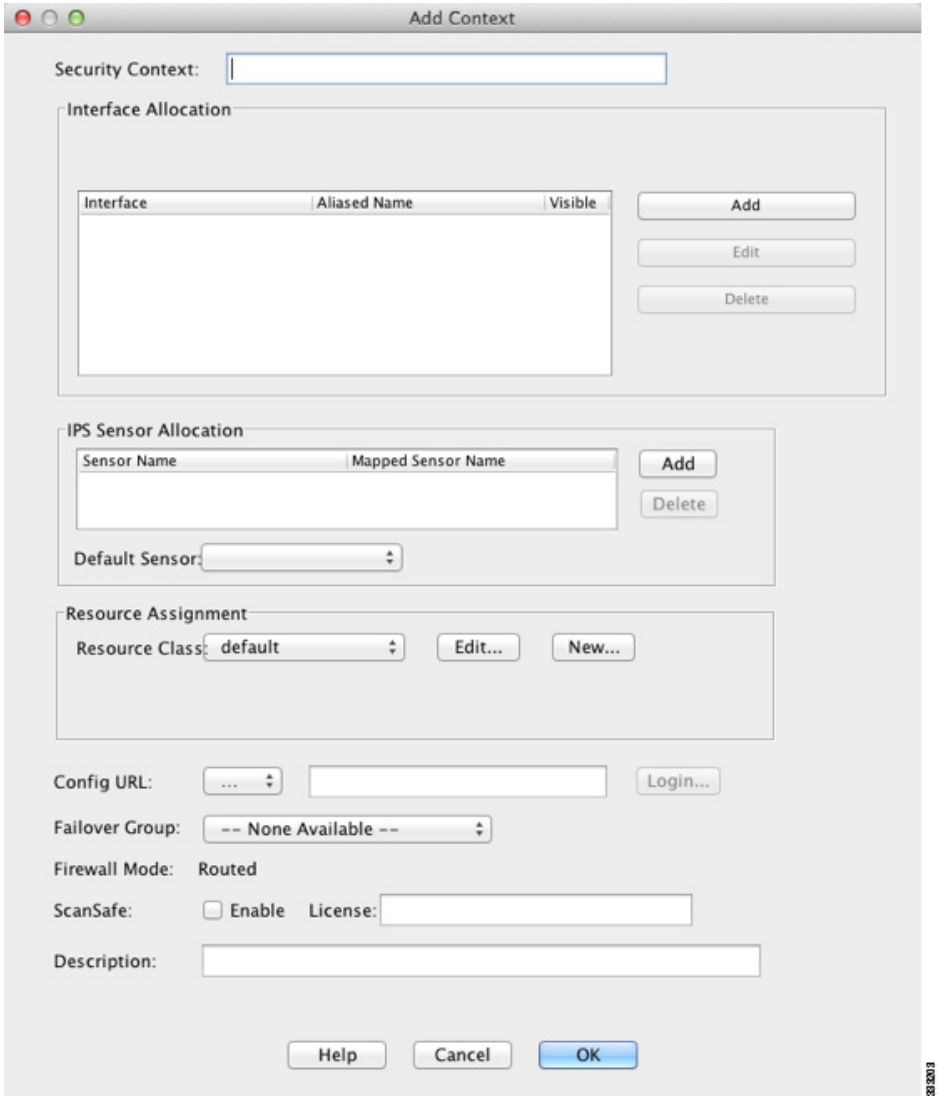
- ASA 5500-X では、物理インターフェイス パラメータ、VLAN サブインターフェイス、EtherChannel、および冗長インターフェイスを第 10 章「基本的なインターフェイス コンフィギュレーション（ASA 5512-X 以降）」に従って設定します。

手順の詳細

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、[Add] をクリックします。

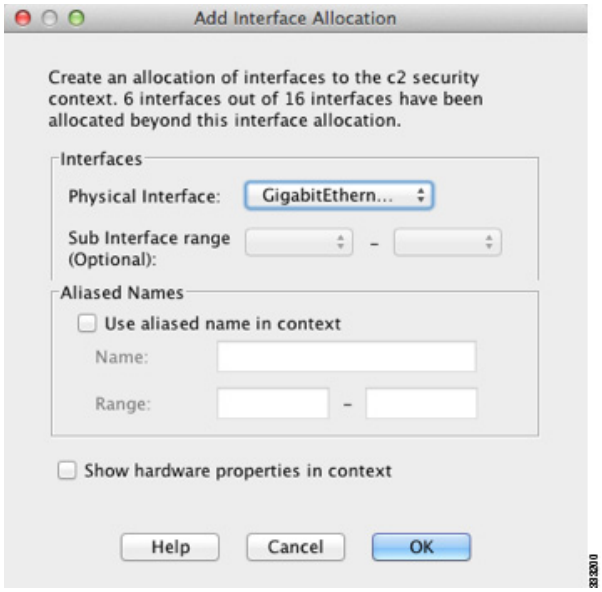
[Add Context] ダイアログボックスが表示されます。



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。

この名前では大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という 2 つのコンテキストを保持できます。「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。



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）[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。

a. （オプション）[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。

– [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。

– （オプション）[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。

b. （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 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。

c. [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 5　（オプション）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、ファイアウォール コンフィギュレーション ガイドを参照してください。

ステップ 6　（オプション）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、「リソース管理のクラスの設定」（P.7-17）を参照してください。

ステップ 7　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

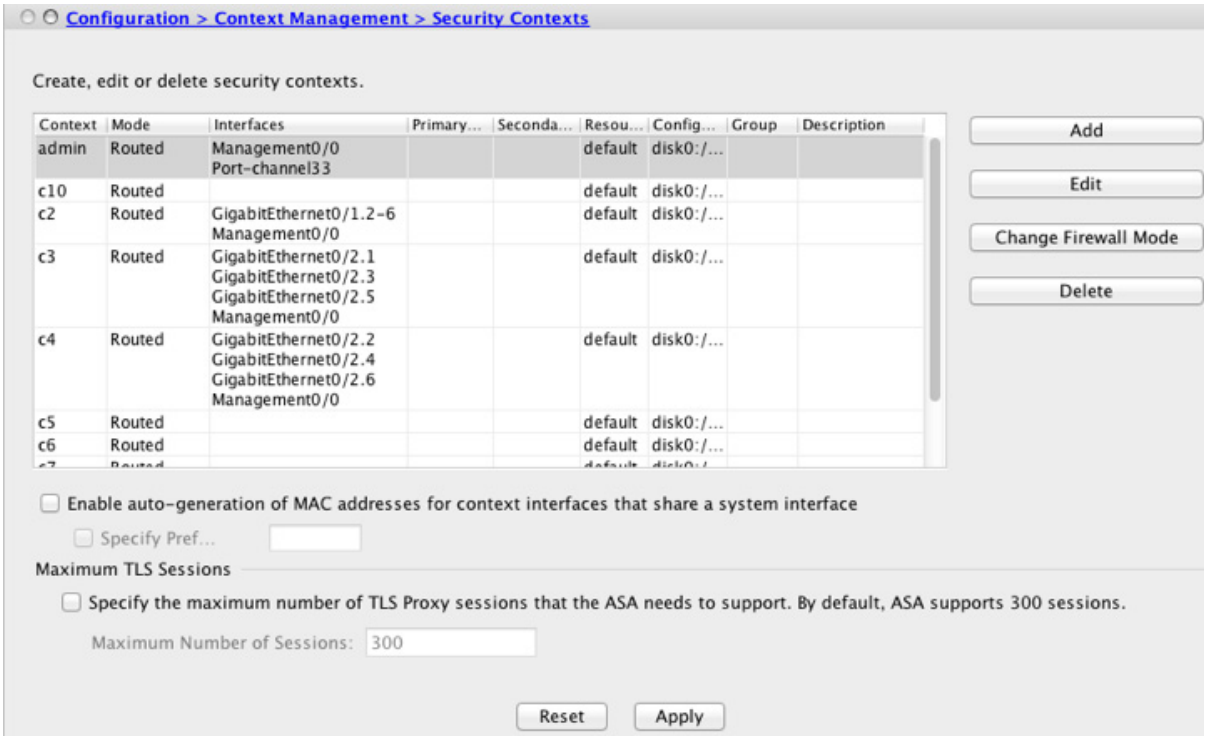
a.　（オプション）外部ファイルシステムの場合、[Login] をクリックしてユーザ名とパスワードを設定します。

ステップ 8　（オプション）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 9　（オプション）このコンテキストの ScanSafe インスペクションをイネーブルにするには、[Enable] をクリックします。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、[License] フィールドにライセンスを入力します。

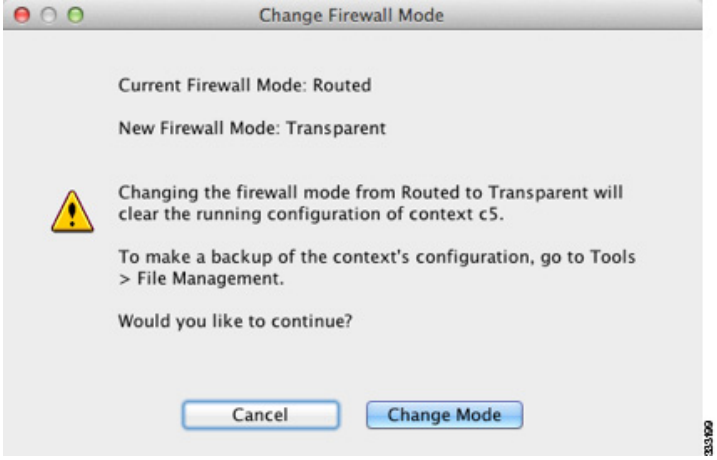
ステップ 10　（オプション）[Description] フィールドに説明を追加します。

ステップ 11　[OK] をクリックして、[Security Contexts] ペインに戻ります。



ステップ 12　（オプション）ファイアウォール モードをトランスペアレントに設定するには、コンテキストを選択し、[Change Firewall Mode] をクリックします。

次の確認ダイアログボックスが表示されます。



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。[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」（P.5-10）を参照してください。

ステップ 13　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」（P.7-25）を参照してください。

ステップ 14　デバイスに対して最大 TLS プロキシ セッション数を指定するには、[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てください。TLS プロキシに関する詳細については、ファイアウォール コンフィギュレーション 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。詳細については、「MAC アドレスに関する情報」（P.7-11）を参照してください（特に、以前の ASA バージョンからアップグレードする場合）。「割り当てられた MAC アドレスの表示」（P.7-33）も参照してください。

ガイドライン

- 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。MAC アドレスの手動設定の詳細については、「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）を参照してください。

手順の詳細

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、[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（ASA 5500-X）またはバックプレーン（ASASM）MAC アドレスの最後の 2 バイトに基づいてプレフィックスが自動生成されます。

ステップ 3　（オプション）[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。

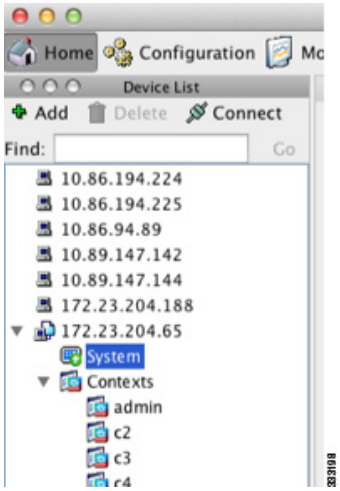
このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。プレフィックスの使用方法の詳細については、「MAC アドレス形式」（P.7-12）を参照してください。

コンテキストとシステム実行スペースの切り替え

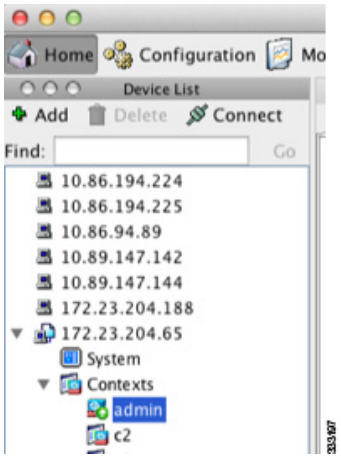
システム実行スペース（または管理コンテキスト）にログインした場合は、コンテキストを切り替えながら、各コンテキスト内でコンフィギュレーションやタスクのモニタリングを実行することができます。コンフィギュレーション モードで編集される実行コンフィギュレーションは、ユーザのログイン先によって決まります。システム実行スペースにログインした場合、実行コンフィギュレーションはシステム コンフィギュレーションのみで構成され、コンテキストにログインした場合は、実行コンフィギュレーションはそのコンテキストのみで構成されます。

手順の詳細

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　コンテキストを変更するには、[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」（P.7-27）
- 「管理コンテキストの変更」（P.7-27）
- 「セキュリティ コンテキスト URL の変更」（P.7-29）
- 「セキュリティ コンテキストのリロード」（P.7-30）

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。

前提条件

この手順はシステム実行スペースで実行します。

手順の詳細

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（サーバからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザに制限する必要があります。

（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。

ガイドライン

コンフィギュレーション ファイルが内部フラッシュ メモリに保存されている限り、任意のコンテキストを管理コンテキストとして設定できます。

前提条件

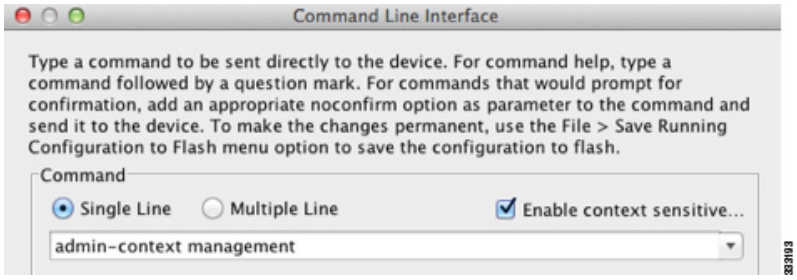
この手順はシステム実行スペースで実行します。

手順の詳細

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。

ガイドライン

- セキュリティ コンテキスト URL は、新しい URL からコンフィギュレーションをリロードしないと変更できません。ASA は、新しいコンフィギュレーションを現在の実行コンフィギュレーションにマージします。
- 同じ URL を再入力した場合でも、保存されたコンフィギュレーションが実行コンフィギュレーションにマージされます。
- マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。
  - コンフィギュレーションが同じ場合、変更は発生しません。
  - コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。実行コンフィギュレーションが空白の場合（たとえば、サーバが使用不可でコンフィギュレーションがダウンロードされなかった場合）は、新しいコンフィギュレーションが使用されます。
- コンフィギュレーションをマージしない場合は、コンテキストを経由する通信を妨げる実行コンフィギュレーションをクリアしてから、新しい URL からコンフィギュレーションをリロードすることができます。

前提条件

この手順はシステム実行スペースで実行します。

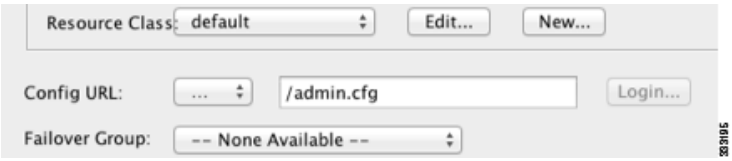
手順の詳細

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」（P.7-30）
- 「コンテキストの削除および再追加によるリロード」（P.7-31）

コンフィギュレーションのクリアによるリロード

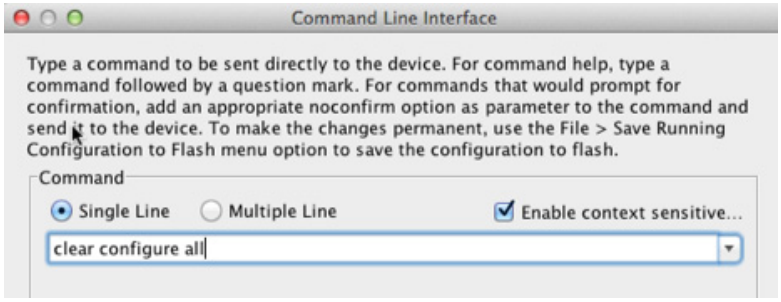
コンテキストをリロードするために、コンテキスト コンフィギュレーションをクリアしてコンフィギュレーションを URL からリロードするには、次の手順を実行します。

手順の詳細

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。

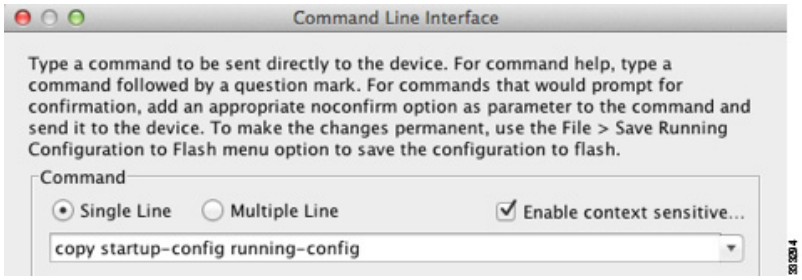
```
clear configure all
```

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、次の各項で説明してある手順を実行してください。

1. 「セキュリティ コンテキストの削除」（P.7-27）[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。
2. 「セキュリティ コンテキストの設定」（P.7-20）

セキュリティ コンテキストのモニタリング

この項では、コンテキスト情報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　」（P.7-31）
- 「割り当てられた MAC アドレスの表示」（P.7-33）

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/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 コンフィギュレーションでの MAC アドレスの表示」（P.7-33）
- 「コンテキスト内の MAC アドレスの表示」（P.7-34）

システム コンフィギュレーションでの MAC アドレスの表示

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

ガイドライン

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

手順の詳細

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。

手順の詳細

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 モードの機能履歴

表 7-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 7-2　マルチ コンテキスト モードの機能履歴

機能名	プラットフォーム リリース	機能情報
マルチセキュリティ コンテキスト	7.0(1)	マルチ コンテキスト モードが導入されました。 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]。
IPS 仮想センサー	8.0(2)	IPS ソフトウェアのバージョン 6.0 以降を実行している AIP SSM では、複数の仮想センサーを実行できます。つまり、AIP SSM に複数のセキュリティ ポリシーを設定することができます。各コンテキストまたはシングル モードASAを 1 つまたは複数の仮想センサーに割り当てる、または複数のセキュリティ コンテキストを同じ仮想センサーに割り当てることができます。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts]。

表 7-2　マルチ コンテキスト モードの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
MAC アドレス自動割り当ての機能強化	8.0(5)/8.2(2)	MAC アドレス形式が変更されました。プレフィックスが使用され、固定開始値（A2）が使用されます。また、フェールオーバー ペアのプライマリ装置とセカンダリ装置の MAC アドレスそれぞれに異なるスキームが使用されます。MAC アドレスはリロード後も維持されるようになりました。コマンド パーサーは現在、自動生成がイネーブルになっているかどうかをチェックします。MAC アドレスを手動でも割り当てることができるようにする場合は、A2 を含む手動 MAC アドレスは開始できません。 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イネーブル化	8.5(1)	MAC アドレスの自動割り当てが、デフォルトでイネーブルになりました。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts]。
MAC アドレス プレフィックスの自動生成	8.6(1)	マルチ コンテキスト モードでは、現在、ASA は、MAC アドレスの自動生成設定をデフォルトのプレフィックスを使用するように変換します。ASA は、インターフェイス（ASA 5500-X）またはバックプレーン（ASASM）MAC アドレスの最後の 2 バイトに基づいてプレフィックスを自動生成します。この変換は、リロード時または MAC アドレス生成を再度イネーブルにすると、自動的に行われます。生成のプレフィックス方式は、セグメント上で一意の MAC アドレスがより適切に保証されるなど、多くの利点をもたらします。プレフィックスを変更する場合、カスタム プレフィックスによって機能を再設定できます。MAC アドレス生成の従来の方法は使用できなくなります。 **（注）** フェールオーバー ペアのヒットレス アップグレードを維持するため、ASA は、フェールオーバーがイネーブルである場合、リロード時に既存のコンフィギュレーションの MAC アドレス方式を変換*しません*。ただし、フェールオーバーを使用するときは、プレフィックスによる生成方式に手動で変更することを強く推奨します（特に ASASM の場合）。プレフィックス方式を使用しない場合、異なるスロット番号にインストールされた ASASM では、フェールオーバーが発生した場合に MAC アドレスの変更が行われ、トラフィックの中断が発生することがあります。アップグレード後に、MAC アドレス生成のプレフィックス方式を使用するには、デフォルトのプレフィックスを使用する MAC アドレス生成を再びイネーブルにします。 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。

表 7-2　マルチ コンテキスト モードの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
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]

ハイ アベイラビリティのためのフェールオーバー

この章では、Cisco ASA のハイ アベイラビリティを実現するために、アクティブ/スタンバイ フェールオーバーまたはアクティブ/アクティブ フェールオーバーを設定する方法について説明します。

フェールオーバーについて

フェールオーバーの概要

フェールオーバーの設定では、専用フェールオーバー リンク（および任意でステート リンク）を介して相互に接続された 2 つの同じ ASA が必要です。アクティブ装置およびインターフェイスのヘルスがモニタされて、所定のフェールオーバー条件に一致しているかどうかが判断されます。所定の条件に一致すると、フェールオーバーが行われます。

ASA は、アクティブ/アクティブ フェールオーバーとアクティブ/スタンバイ フェールオーバーの 2 つのフェールオーバー モードをサポートします。各フェールオーバー モードには、フェールオーバーを判定および実行する独自の方式があります。

- アクティブ/スタンバイ フェールオーバーでは、1 台の装置がアクティブ装置です。この装置がトラフィックを渡します。スタンバイ装置は、アクティブにトラフィックを渡しません。フェールオーバーが発生すると、アクティブ装置がスタンバイ装置にフェールオーバーし、そのスタンバイ装置がアクティブになります。シングルまたはマルチ コンテキスト モードでは、ASA のアクティブ/スタンバイ フェールオーバーを使用できます。
- アクティブ/アクティブ フェールオーバー構成では、両方の ASA がネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードの ASA でのみ使用できます。アクティブ/アクティブ フェールオーバーでは、ASA のセキュリティ コンテキストを 2 つの *フェールオーバー グループ*に分割します。フェールオーバー グループは、1 つまたは複数のセキュリティ コンテキストの論理グループにすぎません。一方のグループは、プライマリ ASA でアクティブになるよう割り当てられます。他方のグループは、セカンダリ ASA でアクティブになるよう割り当てられます。フェールオーバーが行われる場合は、フェールオーバー グループ レベルで行われます。

両方のフェールオーバー モードとも、ステートフルまたはステートレス フェールオーバーをサポートします。

フェールオーバーのシステム要件

この項では、フェールオーバー構成における ASA のハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。

- 「ハードウェア要件」（P.8-2）
- 「ソフトウェア要件」（P.8-3）
- 「ライセンス要件」（P.8-3）

ハードウェア要件

フェールオーバー構成の 2 つの装置は、次の条件を満たしている必要があります。

- 同じモデルであること。
- インターフェイスの数とタイプが同じであること。
- 同じモジュール（存在する場合）がインストールされていること。
- 同じ RAM がインストールされていること。

フェールオーバー構成で装置に異なるサイズのフラッシュ メモリを使用している場合、小さい方のフラッシュ メモリを取り付けた装置に、ソフトウェア イメージ ファイルおよびコンフィギュレーション ファイルを格納できる十分な容量があることを確認してください。十分な容量がない場合、フラッシュ メモリの大きい装置からフラッシュ メモリの小さい装置にコンフィギュレーションの同期が行われると、失敗します。

ソフトウェア要件

フェールオーバー構成の 2 つの装置は、次の条件を満たしている必要があります。

- ファイアウォール モードが同じであること（ルーテッドまたは透過）。
- コンテキスト モードが同じであること（シングルまたはマルチ）。
- ソフトウェア バージョンが、メジャー（最初の番号）およびマイナー（2 番目の番号）ともに同じであること。ただし、アップグレード プロセス中は、異なるバージョンのソフトウェアを一時的に使用できます。たとえば、ある装置をバージョン 8.3(1) からバージョン 8.3(2) にアップグレードし、フェールオーバーをアクティブ状態のままにできます。長期的に互換性を維持するために、両方の装置を同じバージョンにアップグレードすることをお勧めします。

  フェールオーバー ペアでのソフトウェアのアップグレードについては、「フェールオーバー ペアまたは ASA クラスタのアップグレード」（P.37-7）を参照してください。
- 同じ AnyConnect イメージを持っていること。中断のないアップグレードを実行するときにフェールオーバー ペアのイメージが一致しないと、アップグレード プロセスの最後のリブート手順でクライアントレス SSL VPN 接続が切断され、データベースには孤立したセッションが残り、IP プールではクライアントに割り当てられた IP アドレスが「使用中」として示されます。

ライセンス要件

フェールオーバー構成の 2 台の装置は、ライセンスが同じである必要はありません。これらのライセンスは結合され、1 つのフェールオーバー クラスタ ライセンスが構成されます。詳細については、「フェールオーバーまたは ASA クラスタ ライセンス」（P.4-27）を参照してください。

フェールオーバー リンクとステートフル フェールオーバー リンク

フェールオーバー リンクとオプションのステートフル フェールオーバー リンクは、2 つの装置間の専用接続です。

- 「フェールオーバー リンク」（P.8-4）
- 「ステートフル フェールオーバー リンク」（P.8-5）
- 「フェールオーバーの中断の回避とデータ リンク」（P.8-6）

注意　フェールオーバー リンクおよびステート リンク経由で送信される情報は、IPsec トンネルまたはフェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端に ASA を使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。ASA を使用して VPN トンネルを終端する場合は、フェールオーバー通信を IPsec トンネルまたはフェールオーバー キーによってセキュリティ保護することをお勧めします。

フェールオーバー リンク

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。

- 「フェールオーバー リンク データ」（P.8-4）
- 「フェールオーバー リンクのインターフェイス」（P.8-4）
- 「フェールオーバー リンクの接続」（P.8-4）

フェールオーバー リンク データ

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態（アクティブまたはスタンバイ）
- hello メッセージ（キープアライブ）
- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期

フェールオーバー リンクのインターフェイス

使用されていないインターフェイス（物理、冗長、または EtherChannel）はどれでも、フェールオーバー リンクとして使用できます。ただし、現在名前が設定されているインターフェイスは指定できません。フェールオーバー リンク インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバー リンク用にのみ使用できます（オプションでステートリンク用としても使用できます）。

フェールオーバー リンクの接続

フェールオーバー リンクを次の 2 つの方法のいずれかで接続します。

- スイッチを使用します。同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）上で他のデバイスを ASA のフェールオーバー インターフェイスとしては使用しません。
- イーサネット ケーブルを使用して装置を直接接続します。外部スイッチは必要ありません。

装置間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらの装置のものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

ASA は銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているので、クロス ケーブルまたはストレート ケーブルのどちらでも使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

ステートフル フェールオーバー リンク

ステートフル フェールオーバーを使用するには、接続ステート情報を渡すためのステートフル フェールオーバー リンク（別名ステート リンク）を設定する必要があります。

ステート リンク用のインターフェイス オプションは 3 つあります。

- 「専用インターフェイス（推奨）」（P.8-5）
- 「フェールオーバー リンクと共有」（P.8-5）
- 「通常のデータ インターフェイスと共有（非推奨）」（P.8-5）

（注）　ステート リンクに管理インターフェイスを使用しないでください。

専用インターフェイス（推奨）

ステート リンクに専用のインターフェイス（物理、冗長、または EtherChannel）を使用できます。次の 2 つの方法のいずれかで、専用のステート リンクを接続します。

- スイッチを使用します。同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）上で他のデバイスを ASA のフェールオーバー インターフェイスとしては使用しません。
- イーサネット ケーブルを使用してアプライアンスを直接接続します。外部スイッチは必要ありません。

  装置間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらの装置のものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

  ASA は銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているので、クロス ケーブルまたはストレート ケーブルのどちらでも使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

長距離のフェールオーバーを使用する場合のフェールオーバー リンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要があります。遅延が 10 ミリ秒を超えると、フェールオーバー メッセージの再送信により、どうしてもパフォーマンスが低下します。

フェールオーバー リンクと共有

十分なインターフェイスがない場合は、フェールオーバー リンクとの共有が必要となる場合があります。フェールオーバー リンクをステート リンクとして使用する場合は、使用可能な最も速いイーサネット インターフェイスを使用します。このインターフェイスでパフォーマンス上の問題が発生した場合は、別のインターフェイスをステート リンク専用にすることを検討してください。

通常のデータ インターフェイスと共有（非推奨）

データ インターフェイスとステート リンクを共有すると、リプレイ アタックを受けやすくなる場合があります。さらに、大量のステートフル フェールオーバー トラフィックがインターフェイスで送信され、そのネットワーク セグメントでパフォーマンス上の問題が発生することがあります。

データ インターフェイスをステート リンクとして使用する場合、シングル コンテキストのルーテッド モードのみがサポートされます。

フェールオーバーの中断の回避とデータ リンク

すべてのインターフェイスで同時に障害が発生する可能性を減らすために、フェールオーバー リンクとデータ インターフェイスは異なるパスを通すことを推奨します。フェールオーバー リンクがダウンした場合、フェールオーバーが必要かどうかの決定に、ASA はデータ インターフェイスを使用できます。その後、フェールオーバー動作は、フェールオーバー リンクのヘルスが復元されるまで停止されます。

耐障害性のあるフェールオーバー ネットワークの設計については、次の接続シナリオを参照してください。

シナリオ 1：非推奨

単一のスイッチまたはスイッチ セットが 2 つの ASA 間のフェールオーバー インターフェイスとデータ インターフェイスの両方の接続に使用される場合、スイッチまたはスイッチ間リンクがダウンすると、両方の ASA がアクティブになります。したがって、図 8-1 および図 8-2 で示されている次の 2 つの接続方式は推奨しません。

図 8-1　　単一のスイッチを使用した接続：非推奨

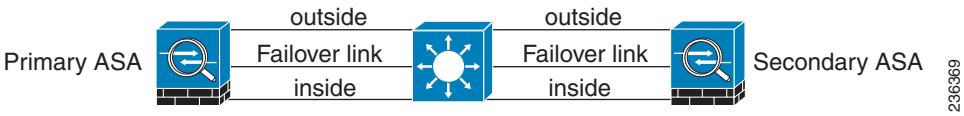
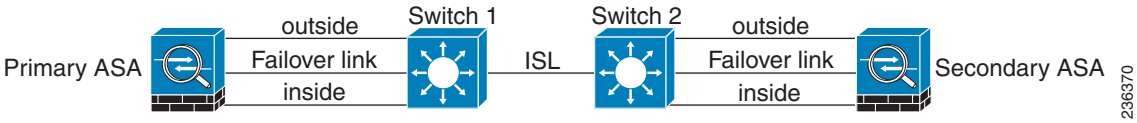


図 8-2　　2 つのスイッチを使用した接続：非推奨



シナリオ 2：推奨

フェールオーバー リンクには、データ インターフェイスと同じスイッチを使用しないことを推奨します。代わりに、図 8-3 および図 8-4 に示すように、別のスイッチを使用するか直接ケーブルを使用して、フェールオーバー リンクを接続します。

図 8-3　　異なるスイッチを使用した接続

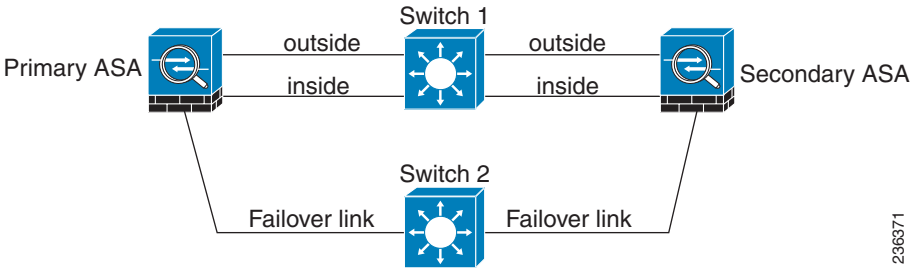
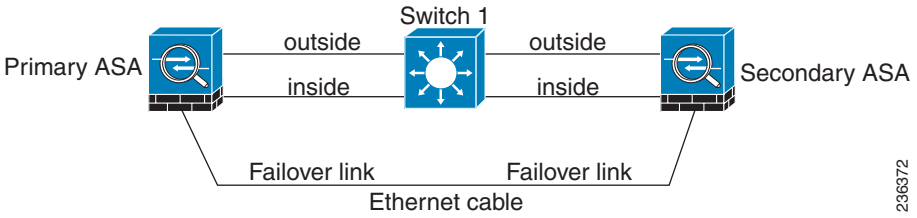


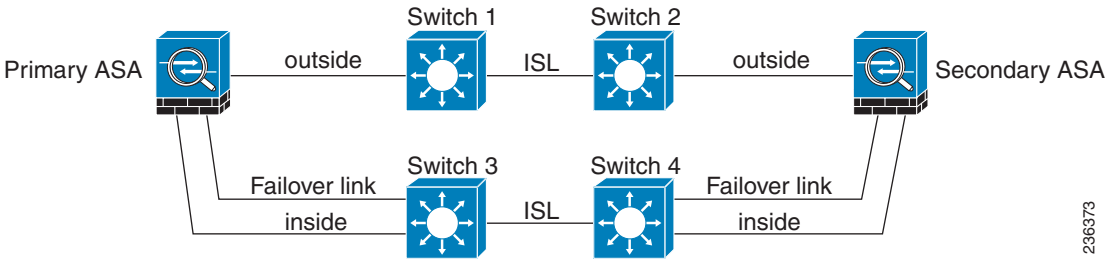
図 8-4　　ケーブルを使用した接続



シナリオ 3：推奨

ASA データ インターフェイスが複数セットのスイッチに接続されている場合、フェールオーバー リンクはいずれかのスイッチに接続できます。できれば、図 8-5 に示すように、ネットワークのセキュアな側（内側）のスイッチに接続します。

図 8-5　　セキュアなスイッチを使用した接続



シナリオ 4：推奨

最も信頼性の高いフェールオーバー構成では、図 8-6 および図 8-7 に示すように、フェールオーバー リンクに冗長インターフェイスを使用します。

図 8-6　　冗長インターフェイスを使用した接続

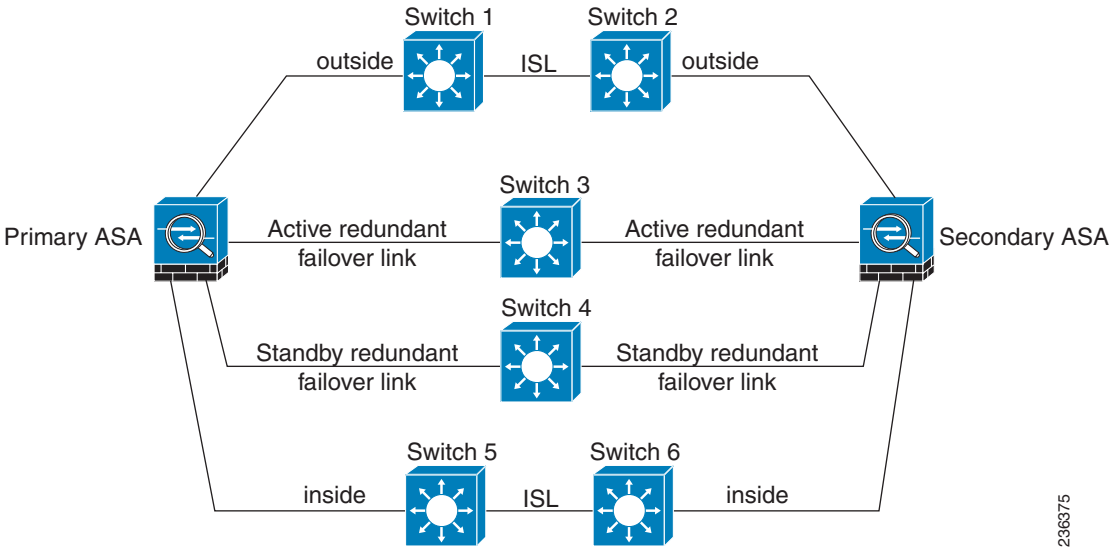
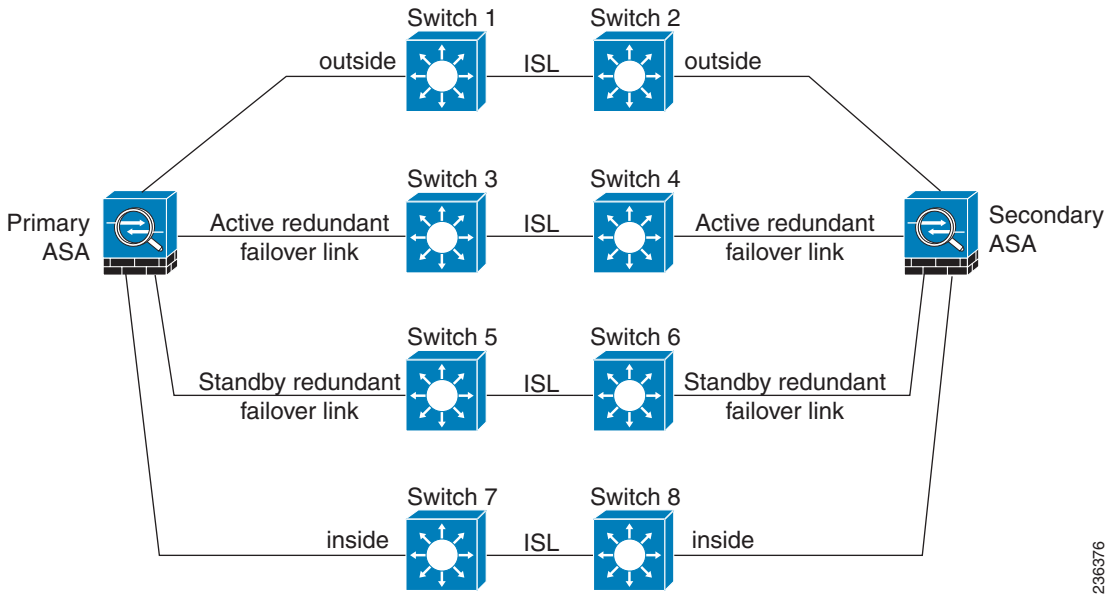


図 8-7　　スイッチ間リンクを使用した接続



MAC アドレスと IP アドレス

インターフェイスを設定する場合、同じネットワーク上のアクティブ IP アドレスとスタンバイ IP アドレスを指定する必要があります。

1. プライマリ装置またはフェールオーバー グループが故障すると、セカンダリ装置はプライマリ装置の IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。
2. 現在スタンバイになっている装置が、スタンバイの IP アドレスと MAC アドレスを引き継ぎます。

ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

（注）　セカンダリ装置がプライマリ装置を検出せずにブートした場合、セカンダリ装置がアクティブ装置になります。プライマリ装置の MAC アドレスを認識していないため、自分の MAC アドレスを使用します。ただし、プライマリ装置が使用可能になると、（アクティブな）セカンダリ装置は MAC アドレスをプライマリ装置の MAC アドレスに変更するため、ネットワーク トラフィックが中断することがあります。同様にプライマリ装置を新しいハードウェアに交換する場合も、新しい MAC アドレスが使用されます。

仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。マルチ コンテキスト モードでは、ASA はアクティブおよびスタンバイの仮想 MAC アドレスをデフォルトで生成します。詳細については、「MAC アドレスに関する情報」（P.7-11）を参照してください。シングル コンテキスト モードでは、手動で仮想 MAC アドレスを設定できます。詳細については、「アクティブ/アクティブ フェールオーバーの設定」（P.8-29）を参照してください。

仮想 MAC アドレスを設定しなかった場合、トラフィック フローを復元するために、接続されたルータの ARP テーブルのクリアが必要になる場合があります。ASA は MAC アドレスを変更するときに、スタティック NAT アドレスに対して Gratuitous ARP を送信しません。そのため、接続されたルータはこれらのアドレスの MAC アドレスの変更を認識できません。

（注）　ステート リンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。唯一の例外は、ステート リンクが通常のデータ インターフェイスに設定されている場合です。

ASA サービス モジュール のシャーシ内およびシャーシ間のモジュール配置

プライマリとセカンダリの ASASM は、同じスイッチ内または 2 台の異なるスイッチに搭載できます。ここでは、各オプションについて説明します。

- 「シャーシ内フェールオーバー」（P.8-9）
- 「シャーシ間フェールオーバー」（P.8-10）

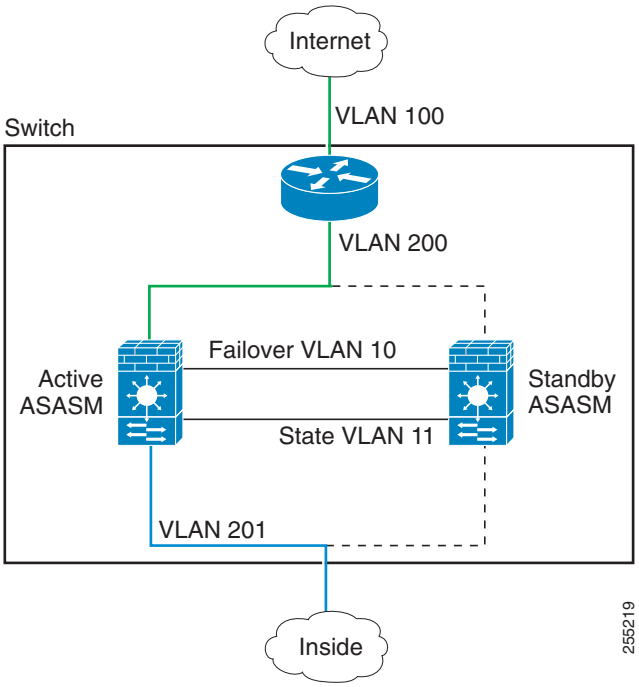
シャーシ内フェールオーバー

セカンダリ ASASM をプライマリ ASASM と同じスイッチに搭載した場合は、モジュール レベルの障害から保護されます。モジュール レベルの障害に加えてスイッチ レベルの障害から保護するには、「シャーシ間フェールオーバー」（P.8-10）を参照してください。

両方の ASASM に同じ VLAN が割り当てられますが、ネットワーキングに参加するのはアクティブ モジュールだけです。スタンバイ モジュールは、トラフィックを転送しません。

図 8-8 に、一般的なスイッチ内の構成を示します。

図 8-8　　スイッチ内フェールオーバー



シャーシ間フェールオーバー

スイッチレベルの障害から保護するため、セカンダリ ASASM を別のスイッチに搭載することができます。ASASM はスイッチでフェールオーバーを直接取り扱うわけではなく、スイッチのフェールオーバー動作に対して協調的に動作します。スイッチのフェールオーバー設定については、スイッチのマニュアルを参照してください。

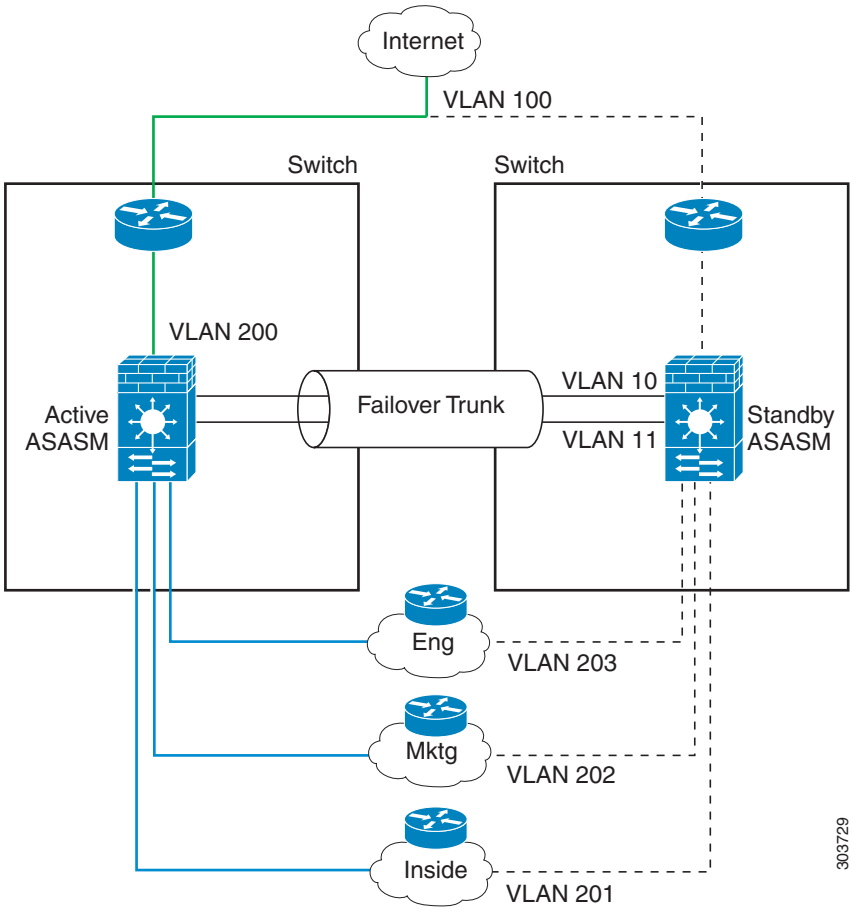
ASASM 間のフェールオーバー通信の信頼性を高めるために、2 台のスイッチ間に EtherChannel トランク ポートを設定して、フェールオーバーおよびステート VLAN を伝送することをお勧めします。

他の VLAN については、両方のスイッチがすべてのファイアウォール VLAN にアクセスでき、モニタ対象 VLAN が両方のスイッチ間で正常に hello パケットを渡すことができるようにします。

図 8-9 に、スイッチと ASASM の一般的な冗長構成を示します。2 台のスイッチ間のトランクは、フェールオーバー ASASM VLAN（VLAN 10 と 11）を転送します。

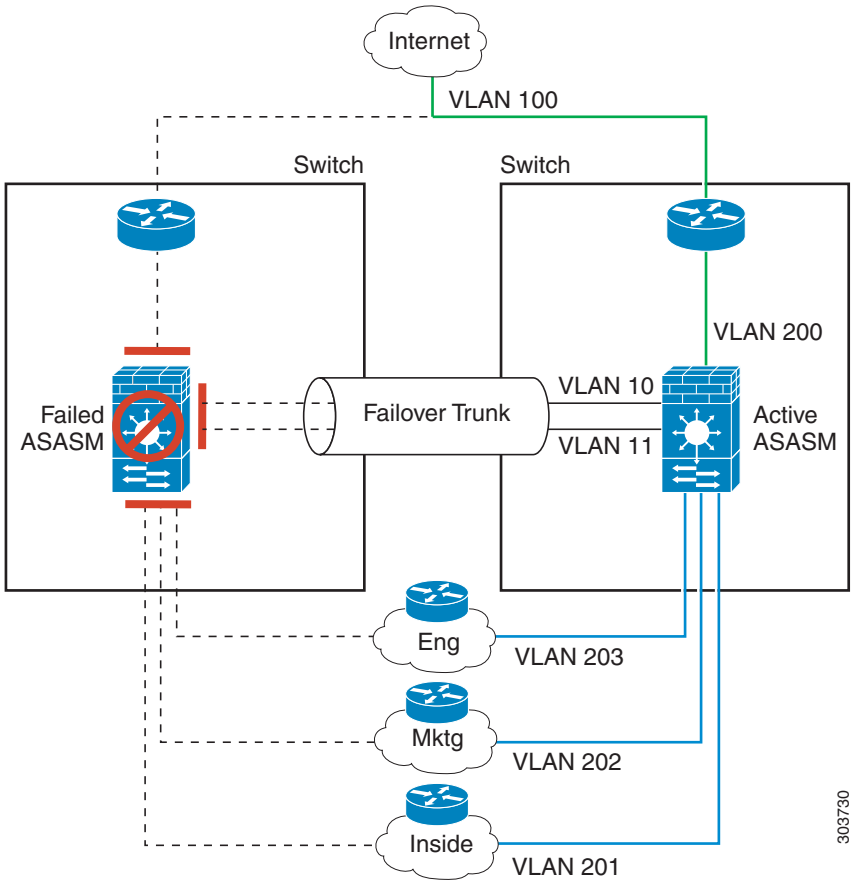
（注）　ASASM のフェールオーバーはスイッチのフェールオーバーに依存しない独立した機能ですが、スイッチのフェールオーバーが発生した場合には、ASASM もそれに対応します。

図 8-9　　通常の動作



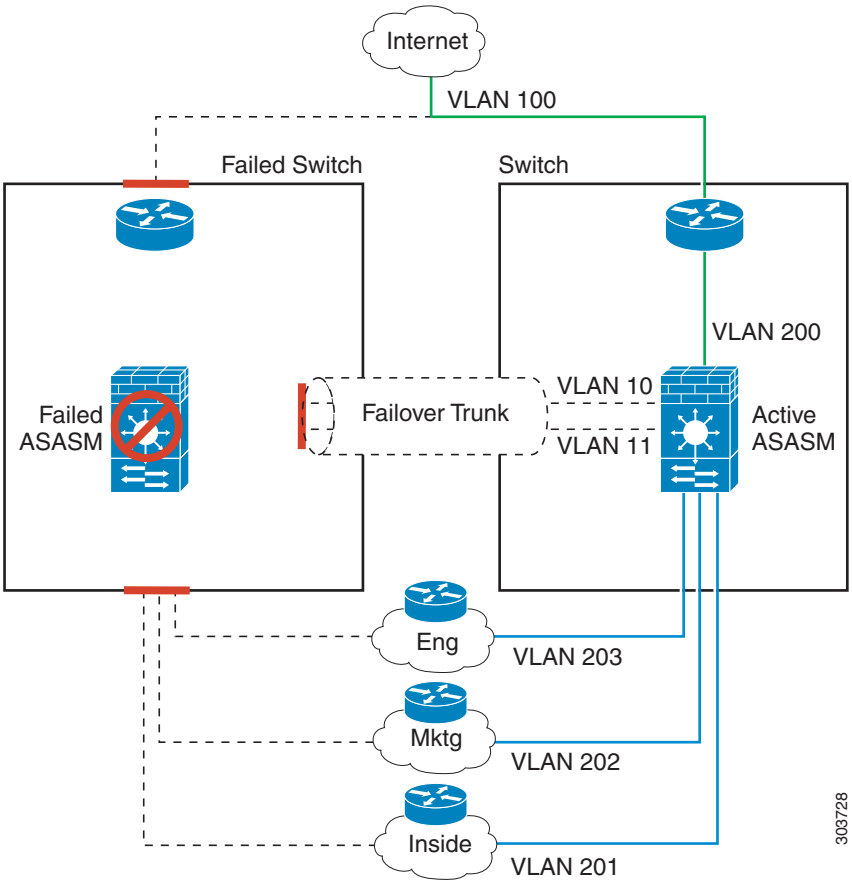
プライマリ ASASM に障害が発生すると、セカンダリ ASASM がアクティブになってファイアウォール VLAN を通過します（図 8-10）。

図 8-10　ASASM の障害



スイッチ全体に障害が発生し、ASASM にも障害が発生した場合（電源切断など）には、スイッチと ASASM の両方でセカンダリ ユニットへのフェールオーバーが実行されます（図 8-11）。

図 8-11　　スイッチの障害



ステートレス フェールオーバーとステートフル フェールオーバー

ASA は、アクティブ/スタンバイ モードとアクティブ/アクティブ モードの両方に対して、ステートレスとステートフルの 2 種類のフェールオーバーをサポートします。

- 「ステートレス フェールオーバー」（P.8-13）
- 「ステートフル フェールオーバー」（P.8-13）

（注）　クライアントレス SSL VPN の一部のコンフィギュレーション要素（ブックマークやカスタマイゼーションなど）は VPN フェールオーバー サブシステムを使用していますが、これはステートフル フェールオーバーの一部です。フェールオーバー ペアのメンバ間でこれらの要素を同期するには、ステートフル フェールオーバーを使用する必要があります。ステートレス フェールオーバーは、クライアントレス SSL VPN には推奨されません。

ステートレス フェールオーバー

フェールオーバーが行われると、アクティブ接続はすべてドロップされます。新しいアクティブ装置が引き継ぐ場合、クライアントは接続を再確立する必要があります。

（注）　クライアントレス SSL VPN の一部のコンフィギュレーション要素（ブックマークやカスタマイゼーションなど）は VPN フェールオーバー サブシステムを使用していますが、これはステートフル フェールオーバーの一部です。フェールオーバー ペアのメンバ間でこれらの要素を同期するには、ステートフル フェールオーバーを使用する必要があります。ステートレス（標準）フェールオーバーは、クライアントレス SSL VPN には推奨できません。

ステートフル フェールオーバー

ステートフル フェールオーバーがイネーブルの場合、アクティブ装置は接続ごとのステート情報をスタンバイ装置に継続的に渡します。アクティブ/アクティブ フェールオーバーの場合は、アクティブとスタンバイのフェールオーバー グループ間でこれが行われます。フェールオーバーの発生後も、新しいアクティブ装置で同じ接続情報が利用できます。サポートされているエンドユーザのアプリケーションでは、同じ通信セッションを保持するために再接続する必要はありません。

- 「サポートされる機能」（P.8-13）
- 「サポートされていない機能」（P.8-14）

サポートされる機能

ステートフル フェールオーバーがイネーブルのときは、次のステート情報がスタンバイ ASA に渡されます。

- NAT 変換テーブル
- TCP 接続状態
- UDP 接続状態
- ARP テーブル
- レイヤ 2 ブリッジ テーブル（トランスペアレント ファイアウォール モードで動作中の場合）
- HTTP 接続状態（HTTP 複製がイネーブルの場合）：デフォルトでは、ステートフル フェールオーバーがイネーブルのときには、ASA は HTTP セッション情報を複製しません。HTTP セッションは通常は存続期間が短く、また HTTP クライアントは接続試行が失敗すると通常は再試行するため、HTTP セッションの複製をしないことでシステムのパフォーマンスが向上します。複製をしなくても重要なデータや接続は失われません。
- ISAKMP および IPSec SA テーブル
- GTP PDP 接続データベース
- SIP シグナリング セッション
- ICMP 接続状態：ICMP 接続の複製は、個々のインターフェイスが非対称ルーティング グループに割り当てられている場合にだけイネーブルになります。
- ダイナミック ルーティング プロトコル：ステートフル フェールオーバーはダイナミック ルーティング プロトコル（OSPF や EIGRP など）に参加するため、アクティブ装置上のダイナミック ルーティング プロトコルによる学習ルートが、スタンバイ装置の Routing Information Base（RIB）テーブルに維持されます。フェールオーバー イベントが発生した場合、最初にアクティブなセカンダリ ASA がプライマリ ASA をミラーリングするルール

があるため、トラフィックの最小限の中断でパケットは正常に送信されます。フェールオーバーの直後に、新しくアクティブになった装置で再コンバージェンス タイマーが開始されます。次に、RIB テーブルのエポック番号が増加します。再コンバージェンス中に、OSPF および EIGRP ルートは新しいエポック番号で更新されます。タイマーが期限切れになると、失効したルート エントリ（エポック番号によって決定される）はテーブルから削除されます。これで、RIB には新しくアクティブになった装置での最新のルーティング プロトコル転送情報が含まれています。

（注）　ルートは、アクティブ装置上のリンクアップまたはリンクダウン イベントの場合のみ同期されます。スタンバイ装置上でリンクがアップまたはダウンすると、アクティブ装置から送信されたダイナミック ルートが失われることがあります。これは正常な予期された動作です。

- Cisco IP SoftPhone セッション：コール セッション ステート情報がスタンバイ装置に複製されるため、Cisco IP SoftPhone セッションの実行中にフェールオーバーが起こっても、コールは実行されたままです。コールが終了すると、IP SoftPhone クライアントは Cisco Call Manager との接続を失います。これは、CTIQBE ハングアップ メッセージのセッション情報がスタンバイ装置に存在しないために発生します。IP SoftPhone クライアントでは、一定の時間内に CallManager からの応答が受信されない場合、CallManager に到達できないものと判断されて登録が解除されます。
- VPN：VPN エンド ユーザはフェールオーバー後に VPN セッションを再認証または再接続する必要はありません。ただし、VPN 接続上で動作するアプリケーションは、フェールオーバー プロセス中にパケットを失って、パケット損失から回復できない可能性があります。

サポートされていない機能

ステートフル フェールオーバーがイネーブルのときに、次のステート情報はスタンバイ ASA に渡され*ません*。

- HTTP 接続テーブル（HTTP 複製がイネーブルでない場合）
- ユーザ認証（uauth）テーブル
- 高度な TCP ステート トラッキングの対象となるアプリケーション インスペクション：これらの接続の TCP 状態は自動的には複製されません。これらの接続はスタンバイ装置に複製されますが、TCP ステートを再確立するためにベスト エフォート型の試行が行われます。
- DHCP サーバ アドレスのリース
- ASA IPS SSP や ASA CX SSP などのモジュールのステート情報。
- 電話のプロキシ接続：アクティブ装置がダウンした場合は、コールが失敗し、メディアのフローが停止するので、障害が発生した装置から電話の登録を解除し、アクティブ装置に再登録する必要があります。コールは再確立する必要があります。
- 一部のクライアントレス SSL VPN 機能
  - スマート トンネル
  - ポート転送
  - プラグイン
  - Java アプレット
  - IPv6 クライアントレスまたは Anyconnect セッション
  - Citrix 認証（Citrix ユーザはフェールオーバー後に再認証が必要です）

トランスペアレント ファイアウォール モードの要件

アプライアンスのトランスペアレント モードの要件

アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニングツリー プロトコル（STP）を実行している接続済みスイッチ ポートは、トポロジ変更を検出すると 30 ～ 50 秒間ブロッキング ステートに移行する場合があります。ポートがブロッキング ステートである間のトラフィックの損失を回避するために、スイッチ ポート モードに応じて次の回避策のいずれかを設定できます。

- アクセス モード：スイッチで STP PortFast 機能をイネーブルにします。

  ```
  interface interface_id
    spanning-tree portfast
  ```

  PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- トランク モード：EtherType アクセス ルールを使用して ASA の内部および外部インターフェイスの両方で BPDU をブロックします。

  BPDU をブロックすると、スイッチの STP はディセーブルになります。ネットワーク レイアウトで ASA を含むループを設定しないでください。

上記のオプションのどちらも使用できない場合は、フェールオーバー機能または STP の安定性に影響する、推奨度の低い次の回避策のいずれかを使用できます。

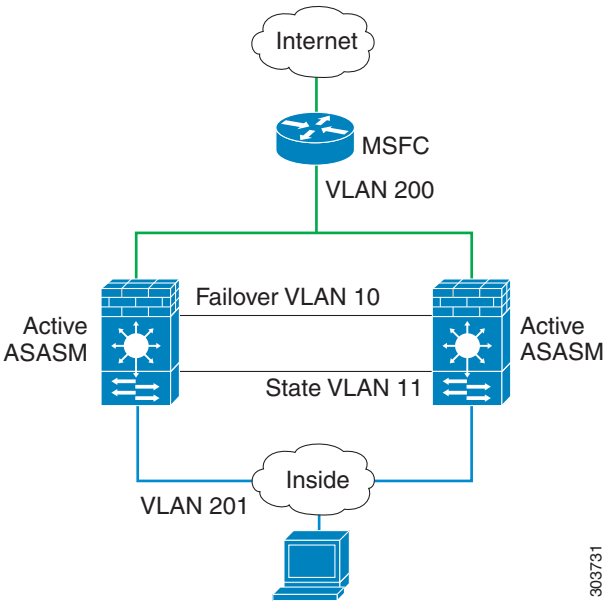
- インターフェイス モニタリングをディセーブルにします。
- ASA がフェールオーバーする前に、インターフェイスのホールド時間を STP が収束可能になる大きい値に増やします。
- STP がインターフェイスのホールド時間よりも速く収束するように、STP タイマーを減らします。

モジュールのトランスペアレント モードの要件

トランスペアレント モードでのフェールオーバーの使用時にループを回避するには、BPDU の通過を許可し（デフォルト）、BPDU 転送をサポートするスイッチ ソフトウェアを使用する必要があります。

両方のモジュールが互いの存在を検出中のときや、不正なフェールオーバー リンクなどによって、両方のモジュールが同時にアクティブの場合に、ループが発生することがあります。両方の ASASM が同じ 2 つの VLAN の間でパケットをブリッジするので、外部宛ての内部パケットが両方の ASASM によって無限に複製され、ループが発生します（図 8-12 を参照）。BPDU がタイミングよく交換された場合は、スパニングツリー プロトコルによって、これらのループが遮断されます。ループを遮断するには、VLAN 200 と VLAN 201 間で送信される BPDU をブリッジングする必要があります。

図 8-12　　トランスペアレント モードのループ



フェールオーバー ヘルスのモニタリング

ASA は、各装置について全体的なヘルスおよびインターフェイス ヘルスをモニタします。この項では、各装置の状態を判断するために、ASA がテストを実行する方法について説明します。

- 「装置ヘルスのモニタリング」（P.8-16）
- 「インターフェイスのモニタリング」（P.8-17）

装置ヘルスのモニタリング

ASA は、フェールオーバー リンクをモニタして相手装置のヘルスを判断します。フェールオーバー リンクで 3 回連続して hello メッセージを受信しなかったときは、フェールオーバー リンクを含む各データ インターフェイスでインターフェイス hello メッセージを送信し、ピアが応答するかどうかを確認します。ASA が行うアクションは、相手装置からの応答によって決まります。次の可能なアクションを参照してください。

- ASA がフェールオーバー リンクで応答を受信した場合、フェールオーバーは行われません。
- ASA がフェールオーバー リンクで応答を受信せず、データ インターフェイスで応答を受信した場合、装置のフェールオーバーは行われません。フェールオーバー リンクが故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
- ASA がどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブ モードに切り替わり、相手装置を故障に分類します。

インターフェイスのモニタリング

最大 250 のインターフェイスをモニタできます（マルチ モードでは、すべてのコンテキスト間で分割）。重要なインターフェイスをモニタする必要があります。たとえばマルチ モードでは、共有インターフェイスをモニタするためのコンテキストを 1 つ設定できます （インターフェイスが共有されているため、すべてのコンテキストがそのモニタリングでモニタされます）。

設定した保持時間が半分経過しても装置がモニタ対象のインターフェイスで hello メッセージを受信しない場合は、次のテストを実行します。

1. リンク アップ/ダウン テスト：インターフェイスのステータスのテスト。リンク アップ/ダウン テストでインターフェイスが動作していることが示された場合、ASA はネットワーク テストを実行します。一連のテストでは、障害が発生している装置を判別するためのネットワーク トラフィックが生成されます。各テストの開始時に、各装置はインターフェイスの受信パケット カウントをリセットします。各テストの終了時には、各装置はトラフィックを受信したかどうかをチェックします。トラフィックを受信していれば、インターフェイスは正常に動作していると見なされます。いずれか一方の装置だけがテスト用のトラフィックを受信している場合は、トラフィックを受信しなかった装置が故障していると見なされます。どちらの装置もトラフィックを受信しなかった場合は、次のテストが使用されます。
2. ネットワーク アクティビティ テスト：受信ネットワーク アクティビティ テスト。装置は、最大 5 秒間、すべての受信パケット数をカウントします。この時間間隔の間にパケットが受信されると、インターフェイスが正常に動作しているものと見なされ、テストは停止します。トラフィックが受信されなかった場合、ARP テストが開始します。
3. ARP テスト：取得したエントリの最後の 2 つの装置 ARP キャッシュの読み取り。装置は、ネットワーク トラフィックを発生させるために、1 回に 1 つずつ、これらのマシンに ARP 要求を送信します。各要求後、装置は最大 5 秒間受信したトラフィックをすべてカウントします。トラフィックが受信されれば、インターフェイスは正常に動作していると見なされます。トラフィックが受信されなければ、ARP 要求が次のマシンに送信されます。リストの最後まで、まったくトラフィックが受信されなかった場合、ping テストが開始します。
4. ブロードキャスト ping テスト：ブロードキャスト ping 要求の送信で構成される ping テスト。装置は、最大 5 秒間、すべての受信パケット数をカウントします。この時間間隔の間にパケットが受信されると、インターフェイスが正常に動作しているものと見なされ、テストは停止します。

モニタ対象のインターフェイスには、次のステータスがあります。

- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down：インターフェイスまたは VLAN は管理のためにダウンしています。
- No Link：インターフェイスの物理リンクがダウンしています。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

インターフェイスに IPv4 および IPv6 アドレスが設定されている場合、ASA は IPv4 を使用してヘルス モニタリングを実行します。

インターフェイスに IPv6 アドレスだけが設定されている場合、ASA は ARP ではなく IPv6 ネイバー探索を使用してヘルス モニタリング テストを実行します。ブロードキャスト ping テストの場合、ASA は IPv6 全ノード アドレス（FE02::1）を使用します。

1 つのインターフェイスに対するネットワーク テストがすべて失敗したが、相手装置のこのインターフェイスが正常にトラフィックを渡し続けている場合、そのインターフェイスは故障していると見なされます。故障したインターフェイスがしきい値を超えている場合は、フェールオーバーが行われます。相手装置のインターフェイスでもすべてのネットワーク テストに失敗した場合、両方のインターフェイスは “Unknown” 状態になり、フェールオーバーの限界値に向けてのカウントは行われません。

インターフェイスは、何らかのトラフィックを受信すると、再度動作状態になります。故障した ASA は、インターフェイス障害しきい値が満たされなくなった場合、スタンバイ モードに戻ります。

（注）　障害が発生した装置が回復せず、実際には障害は発生していないと考えられる場合は、**failover reset** コマンドを使用して状態をリセットできます。ただし、フェールオーバー条件が継続している場合、装置は再び障害状態になります。

フェールオーバー時間

表 8-1 に、最小、デフォルト、最大フェールオーバー時間を示します。

表 8-1　ASA のフェールオーバー時間

フェールオーバー条件	最小	デフォルト	最大
アクティブ装置で電源断が生じる、または通常の動作が停止する。	800 ミリ秒	15 秒	45 秒
アクティブ装置のメインボード インターフェイス リンクがダウンする。	500 ミリ秒	5 秒	15 秒
アクティブ装置の 4GE モジュール インターフェイス リンクがダウンする。	2 秒	5 秒	15 秒
アクティブ装置の IPS または CSC モジュールに障害がある。	2 秒	2 秒	2 秒
アクティブ装置のインターフェイスは実行されているが、接続の問題によりインターフェイス テストを行っている。	5 秒	25 秒	75 秒

コンフィギュレーション同期

フェールオーバーには、2 種類のコンフィギュレーション同期があります。

- 「コンフィギュレーションの複製の実行」（P.8-18）
- 「コマンドの複製」（P.8-19）

コンフィギュレーションの複製の実行

コンフィギュレーションの複製は、フェールオーバー ペアの一方または両方のデバイスのブート時に実行されます。コンフィギュレーションは常に、アクティブ装置からスタンバイ装置に同期化されます。スタンバイ装置は、その初期スタートアップを完了すると、自分の実行コンフィギュレーションを削除し（アクティブ装置との通信に必要なフェールオーバー コマンドを除く）、アクティブ装置は自分のコンフィギュレーション全体をスタンバイ装置に送信します。

複製が開始されると、アクティブ装置の ASA コンソールに「Beginning configuration replication: Sending to mate,」というメッセージが表示され、完了すると ASA に「End Configuration Replication to mate.」というメッセージが表示されます。コンフィギュレーションのサイズによって、複製には数秒から数分かかります。

スタンバイ装置の場合、コンフィギュレーションは実行メモリにだけ存在します。コンフィギュレーションをフラッシュ メモリに保存する必要があります。

（注） 複製中に、アクティブ装置で入力したコマンドはスタンバイ装置に正しく複製されない可能性があり、スタンバイ装置で入力したコマンドはアクティブ装置から複製されるコンフィギュレーションによって上書きされる可能性があります。コンフィギュレーションの複製処理中に、いずれかの装置にコマンドを入力することは避けてください。

（注） **crypto ca server** コマンドおよび関連するサブコマンドは、フェールオーバー ピアに同期化されません。

（注） コンフィギュレーションの同期は次のファイルと構成コンポーネントを複製しません。したがって、これらのファイルが一致するように手動でコピーする必要があります。

- AnyConnect イメージ
- CSD イメージ
- AnyConnect プロファイル
- ローカル認証局（CA）
- ASA イメージ
- ASDM イメージ

コマンドの複製

起動した後、アクティブ装置で入力したコマンドはただちにスタンバイ装置に複製されます。コマンドを複製する場合、アクティブ コンフィギュレーションをフラッシュ メモリに保存する必要はありません。

アクティブ/アクティブ フェールオーバーでは、システム実行スペースに入力した変更は、フェールオーバー グループ 1 がアクティブ状態である装置から複製されます。

コマンドの複製を行うのに適切な装置上で変更を入力しなかった場合は、コンフィギュレーションは同期されません。この変更内容は、次回に初期コンフィギュレーション同期が行われると失われることがあります。

スタンバイ ASA に複製されるコマンドは、次のとおりです。

- **mode**、**firewall**、および **failover lan unit** を除く、すべてのコンフィギュレーション コマンド
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**

- **rmdir**
- **write memory**

スタンバイ ASA に複製*されない*コマンドは、次のとおりです。

- **copy running-config startup-config** を除く、すべての形式の **copy** コマンド
- **write memory** を除く、すべての形式の **write** コマンド
- **debug**
- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** および **pager**

アクティブ/スタンバイ フェールオーバーについて

アクティブ/スタンバイ フェールオーバーでは、障害が発生した装置の機能を、スタンバイ ASA に引き継ぐことができます。アクティブ装置が故障すると、スタンバイ状態に変わり、そしてスタンバイ装置がアクティブ状態に変わります。

（注）　マルチ コンテキスト モードの場合、ASA は装置全体（すべてのコンテキストを含む）をフェールオーバーできますが、個々のコンテキストを別々にフェールオーバーすることはできません。

- 「プライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス」（P.8-20）
- 「起動時のアクティブ装置の判別」（P.8-21）
- 「フェールオーバー イベント」（P.8-21）

プライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス

フェールオーバー ペアの 2 台の装置の主な相違点は、どちらの装置がアクティブでどちらの装置がスタンバイであるか、つまりどちらの IP アドレスを使用するかおよびどちらの装置がアクティブにトラフィックを渡すかということに関連します。

しかし、プライマリである装置（コンフィギュレーションで指定）とセカンダリである装置との間で、いくつかの相違点があります。

- 両方の装置が同時にスタート アップした場合（さらに動作ヘルスが等しい場合）、プライマリ装置が常にアクティブ装置になります。
- プライマリ装置の MAC アドレスは常に、アクティブ IP アドレスと結び付けられています。このルールの例外は、セカンダリ装置がアクティブであり、フェールオーバー リンク経由でプライマリ装置の MAC アドレスを取得できない場合に発生します。この場合、セカンダリ装置の MAC アドレスが使用されます。

起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時にブートされた場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。

フェールオーバー イベント

アクティブ/スタンバイ フェールオーバーでは、フェールオーバーは装置ごとに行われます。マルチ コンテキスト モードで動作中のシステムでも、個々のコンテキストまたはコンテキストのグループをフェールオーバーすることはできません。

表 8-2 に、各障害イベントに対するフェールオーバー アクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ装置が行うアクション、スタンバイ装置が行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 8-2　　フェールオーバー動作

障害の状況	ポリシー	アクティブ アクション	スタンバイ アクション	注意
アクティブ装置が故障（電源またはハードウェア）	フェールオーバー	該当なし	アクティブになる アクティブに故障とマークする	モニタ対象インターフェイスまたはフェールオーバー リンクで hello メッセージは受信されません。
以前にアクティブであった装置の復旧	フェールオーバーなし	スタンバイになる	動作なし	なし。
スタンバイ装置が故障（電源またはハードウェア）	フェールオーバーなし	スタンバイに故障とマークする	該当なし	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。
動作中にフェールオーバー リンクに障害が発生した	フェールオーバーなし	フェールオーバー リンクに故障とマークする	フェールオーバー リンクに故障とマークする	フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
スタートアップ時にフェールオーバー リンクに障害が発生した	フェールオーバーなし	フェールオーバー リンクに故障とマークする	アクティブになる	スタートアップ時にフェールオーバー リンクがダウンしていると、両方の装置がアクティブになります。
ステート リンクの障害	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。

表 8-2　　フェールオーバー動作 （続き）

障害の状況	ポリシー	アクティブ アクション	スタンバイ アクション	注意
アクティブ装置におけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブに故障とマークする	アクティブになる	なし。
スタンバイ装置におけるしきい値を超えたインターフェイス障害	フェールオーバーなし	動作なし	スタンバイに故障とマークする	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。

アクティブ/アクティブ フェールオーバーについて

この項では、アクティブ/アクティブ フェールオーバーについて説明します。

- 「アクティブ/アクティブ フェールオーバーの概要」（P.8-22）
- 「フェールオーバー グループのプライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス」（P.8-23）
- 「フェールオーバー イベント」（P.8-23）

アクティブ/アクティブ フェールオーバーの概要

アクティブ/アクティブ フェールオーバー構成では、両方の ASA がネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードの ASA でのみ使用できます。アクティブ/アクティブ フェールオーバーでは、ASA のセキュリティ コンテキストを 2 つまでのフェールオーバー グループに分割します。

フェールオーバー グループは、1 つまたは複数のセキュリティ コンテキストの論理グループにすぎません。フェールオーバー グループをプライマリ ASA でアクティブに割り当て、フェールオーバー グループ 2 をセカンダリ ASA でアクティブに割り当てることができます。フェールオーバーが行われる場合は、フェールオーバー グループ レベルで行われます。たとえば、インターフェイス障害パターンに応じて、フェールオーバー グループ 1 をセカンダリ ASA にフェールオーバーし、続いてフェールオーバー グループ 2 をプライマリ ASA にフェールオーバーすることができます。このイベントは、プライマリ ASA でフェールオーバー グループ 1 のインターフェイスがダウンしたがセカンダリ ASA ではアップしており、セカンダリ ASA でフェールオーバー グループ 2 のインターフェイスがダウンしたがプライマリ ASA ではアップしている場合に発生する可能性があります。

管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。未割り当てセキュリティ コンテキストもまた、デフォルトでフェールオーバー グループ 1 のメンバです。アクティブ/アクティブ フェールオーバーが必要であるが複数コンテキストは必要ない場合、最もシンプルな設定は他のコンテキストを 1 つ追加し、それをフェールオーバー グループ 2 に割り当てることです。

（注） アクティブ/アクティブ フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにしてください。

（注）　必要に応じて両方のフェールオーバー グループを 1 つの ASA に割り当てることもできますが、この場合、アクティブな ASA を 2 つ持つというメリットはありません。

フェールオーバー グループのプライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス

アクティブ/スタンバイ フェールオーバーの場合のように、アクティブ/アクティブ フェールオーバー ペアの一方の装置がプライマリ装置に指定され、もう一方の装置がセカンダリ装置に指定されます。アクティブ/スタンバイ フェールオーバーの場合とは異なり、両方の装置が同時に起動された場合、この指定ではどちらの装置がアクティブになるか指示しません。代わりに、プライマリまたはセカンダリの指定時に、次の 2 つの点を判定します。

- ペアが同時に起動したときに、プライマリ装置が実行コンフィギュレーションを提供します。
- コンフィギュレーションの各フェールオーバー グループは、プライマリまたはセカンダリ装置プリファレンスが設定されます。

起動時のフェールオーバー グループのアクティブ装置の決定

フェールオーバー グループがアクティブになる装置は、次のように決定されます。

- ピア装置が使用できないときに装置がブートされると、両方のフェールオーバー グループがピア装置でアクティブになります。
- ピア装置がアクティブ（両方のフェールオーバー グループがアクティブ状態）の場合に装置がブートされると、フェールオーバー グループは、アクティブ装置でアクティブ状態のままになります。これは、次のいずれかの状態になるまで、フェールオーバー グループのプライマリ プリファレンスまたはセカンダリ プリファレンスには関係ありません。
  - フェールオーバーが発生した。
  - 手動でフェールオーバーを強制実行した。
  - フェールオーバー グループにプリエンプションを設定した。この設定により、優先する装置が使用可能になると、フェールオーバー グループはその装置上で自動的にアクティブになります。
- 同時に両方の装置がブートされると、コンフィギュレーションが同期化された後、各フェールオーバー グループは優先する装置上でアクティブになります。

フェールオーバー イベント

アクティブ/アクティブ フェールオーバー構成では、フェールオーバーは、システムごとに行うのではなく、フェールオーバー グループごとに行われます。たとえば、プライマリ装置で両方のフェールオーバー グループをアクティブと指定し、フェールオーバー グループ 1 が故障すると、フェールオーバー グループ 2 はプライマリ装置でアクティブのままですが、フェールオーバー グループ 1 はセカンダリ装置でアクティブになります。

フェールオーバー グループには複数のコンテキストを含めることができ、また各コンテキストには複数のインターフェイスを含めることができるので、1 つのコンテキストのインターフェイスがすべて故障しても、そのコンテキストに関連するフェールオーバー グループが故障と判断されない可能性があります。

表 8-3 に、各障害イベントに対するフェールオーバー アクションを示します。各障害イベントに対して、ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ フェールオーバー グループのアクション、およびスタンバイ フェールオーバー グループのアクションを示します。

表 8-3　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動作

障害の状況	ポリシー	アクティブ グループのアクション	スタンバイ グループのアクション	注意
装置で電源断またはソフトウェア障害が発生した	フェールオーバー	スタンバイになり、故障とマークする	アクティブになる アクティブに故障とマークする	フェールオーバー ペアの装置が故障すると、その装置のアクティブ フェールオーバー グループはすべて故障とマークされ、ピア装置のフェールオーバー グループがアクティブになります。
アクティブ フェールオーバー グループにおけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブ グループに故障とマークする	アクティブになる	なし。
スタンバイ フェールオーバー グループにおけるしきい値を超えたインターフェイス障害	フェールオーバーなし	動作なし	スタンバイ グループに故障とマークする	スタンバイ フェールオーバー グループが故障とマークされている場合、インターフェイス フェールオーバー障害しきい値を超えても、アクティブ フェールオーバー グループはフェールオーバーを行いません。
以前にアクティブであったフェールオーバー グループの復旧	フェールオーバーなし	動作なし	動作なし	フェールオーバー グループのプリエンプションが設定されている場合を除き、フェールオーバー グループは現在の装置でアクティブのままです。
スタートアップ時にフェールオーバー リンクに障害が発生した	フェールオーバーなし	アクティブになる	アクティブになる	スタートアップ時にフェールオーバー リンクがダウンしていると、両方の装置の両方のフェールオーバー グループがアクティブになります。
ステート リンクの障害	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。
動作中にフェールオーバー リンクに障害が発生した	フェールオーバーなし	該当なし	該当なし	各装置で、フェールオーバー リンクが故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。

フェールオーバーのライセンス

アクティブ/スタンバイ フェールオーバー

モデル	ライセンス要件
ASA 5512-X	Security Plus ライセンス
ASAv	標準および Premium ライセンス
他のすべてのモデル	基本ライセンス

フェールオーバー ユニットは、各ユニット上で同一のライセンスを必要としません。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバー クラスタ ライセンスに結合されます。このルールの例外は次のとおりです。

- 5512-X の Security Plus ライセンス：基本ライセンスはフェールオーバーをサポートしないため、基本ライセンスのみを保持するスタンバイ装置ではフェールオーバーをイネーブルにできません。
- 暗号化ライセンス：両方のユニットに同じ暗号化ライセンスが必要です。
- ASA 5512-X から ASA 5555-X までの IPS モジュール ライセンス：両方の装置で IPS モジュール ライセンスが必要です。両方の装置の IPS 側で IPS シグニチャ サブスクリプションも必要です。次のガイドラインを参照してください。
  - IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です（製品番号に、たとえば ASA5515-IPS-K9 のように「IPS」が含まれている必要があります）。IPS ではない製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。
  - 両方の装置に IPS シグニチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスではないため、フェールオーバー間で共有されません。
  - IPS シグニチャ サブスクリプションには、装置ごとに個別の IPS モジュール ライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュール ライセンスも技術的にはフェールオーバー クラスタ ライセンスで共有されます。しかし、IPS シグニチャ サブスクリプションの要件によって、装置ごとに個別の IPS モジュール ライセンスを購入する必要があります。
- ASAv 仮想 CPU：フェールオーバー配置では、スタンバイ装置に割り当てられる vCPU の数をプライマリ装置に割り当てられる数と同じにしてください（対応する数の vCPU ライセンスも必要です）。

アクティブ/アクティブ フェールオーバー

モデル	ライセンス要件
ASA 5512-X	Security Plus ライセンス
ASAv	サポートしない
他のすべてのモデル	基本ライセンス

フェールオーバー ユニットは、各ユニット上で同一のライセンスを必要としません。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバー クラスタ ライセンスに結合されます。このルールの例外は次のとおりです。

- 5512-X の Security Plus ライセンス：基本ライセンスはフェールオーバーをサポートしないため、基本ライセンスのみを保持するスタンバイ装置ではフェールオーバーをイネーブルにできません。
- 暗号化ライセンス：両方のユニットに同じ暗号化ライセンスが必要です。
- ASA 5512-X から ASA 5555-X までの IPS モジュール ライセンス：両方の装置で IPS モジュール ライセンスが必要です。両方の装置の IPS 側で IPS シグニチャ サブスクリプションも必要です。次のガイドラインを参照してください。
  - IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です（製品番号に、たとえば ASA5515-IPS-K9 のように「IPS」が含まれている必要があります）。IPS ではない製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。
  - 両方の装置に IPS シグニチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスではないため、フェールオーバー間で共有されません。
  - IPS シグニチャ サブスクリプションには、装置ごとに個別の IPS モジュール ライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュール ライセンスも技術的にはフェールオーバー クラスタ ライセンスで共有されます。しかし、IPS シグニチャ サブスクリプションの要件によって、装置ごとに個別の IPS モジュール ライセンスを購入する必要があります。
- ASAv 仮想 CPU：フェールオーバー配置では、スタンバイ装置に割り当てられる vCPU の数をプライマリ装置に割り当てられる数と同じにしてください（対応する数の vCPU ライセンスも必要です）。

フェールオーバーの前提条件

「フェールオーバーのシステム要件」（P.8-2）を参照してください。

フェールオーバーのガイドライン

コンテキスト モードのガイドライン

- アクティブ/スタンバイ モードは、シングル コンテキスト モードとマルチ コンテキスト モードでサポートされます。
- アクティブ/アクティブ モードは、マルチ コンテキスト モードでのみサポートされます。
- マルチ コンテキスト モードでは、特に注記がない限り、手順はすべてシステム実行スペースで実行します。
- ASA フェールオーバー複製は、複数のコンテキストで設定を同時に変更しようとすると、失敗します。回避策は、各コンテキストで順番に設定変更を行うことです。

その他のガイドラインと制限事項

- ASA フェールオーバー ペアに接続されたスイッチ上でポート セキュリティを設定すると、フェールオーバー イベントが発生したときに通信の問題が起きることがあります。この問題は、あるセキュア ポートで設定または学習されたセキュア MAC アドレスが別のセキュア ポートに移動し、スイッチのポート セキュリティ機能によって違反フラグが付けられた場合に発生します。
- すべてのコンテキストにわたり、1 台の装置の最大 250 のインターフェイスをモニタできます。
- アクティブ/アクティブ フェールオーバーでは、同じコンテキスト内の 2 つのインターフェイスを同じ ASR グループ内で設定することはできません。
- アクティブ/アクティブ フェールオーバーでは、最大 2 つのフェールオーバー グループを定義できます。
- アクティブ/アクティブ フェールオーバーでフェールオーバー グループを削除する場合は、フェールオーバー グループ 1 を最後に削除する必要があります。フェールオーバー グループ 1 には常に管理コンテキストが含まれます。フェールオーバー グループに割り当てられていないコンテキストはすべて、デフォルトでフェールオーバー グループ 1 になります。コンテキストが明示的に割り当てられているフェールオーバー グループは削除できません。

関連項目

- 「フェールオーバー コンフィギュレーションでの Auto Update サーバ サポート」（P.37-31）

フェールオーバーのデフォルト

デフォルトでは、フェールオーバー ポリシーは次のように構成されています。

- ステートフル フェールオーバーでの HTTP 複製は行われません。
- 単一のインターフェイス障害でフェールオーバーが行われます。
- インターフェイスのポーリング時間は 5 秒です。
- インターフェイスのホールド時間は 25 秒です。
- 装置のポーリング時間は 1 秒です。
- 装置のホールド時間は 15 秒です。
- 仮想 MAC アドレスは、マルチ コンテキスト モードではイネーブルです。シングル コンテキスト モードではディセーブルです。
- すべての物理インターフェイスをモニタリングします。ASASM では、すべての VLAN インターフェイスをモニタリングします。

アクティブ/スタンバイ フェールオーバーの設定

High Availability and Scalability Wizard を使用して、手順を踏んでアクティブ/スタンバイ フェールオーバー コンフィギュレーションを作成することができます。

手順

ステップ 1　[Wizards] > [High Availability and Scalability] を選択します。次の手順でこのウィザードのガイドラインを確認してください。

ステップ 2　[Failover Peer Connectivity and Compatibility] 画面で、ピア装置の IP アドレスを入力します。このアドレスは、ASDM アクセスがイネーブルになっているインターフェイスである必要があります。

デフォルトでは、ピア アドレスは ASDM 管理インターフェイスのスタンバイ アドレスに割り当てられます。

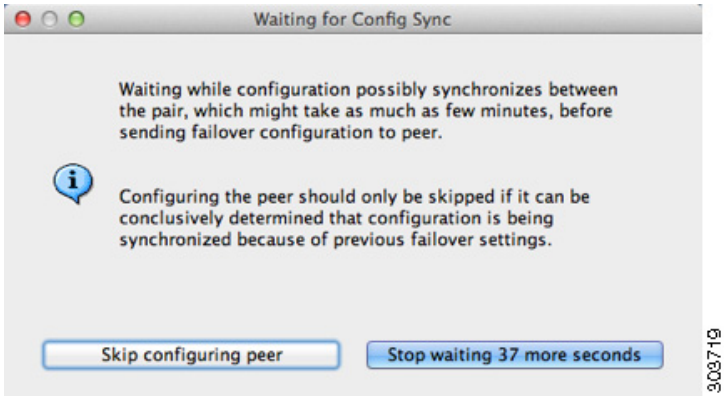
ステップ 3　[LAN Link Configuration] 画面で次のように設定します。

- [Active IP Address]：この IP アドレスは、未使用のサブネット上になければなりません。
- [Standby IP Address]：この IP アドレスは、アクティブ IP アドレスと同じネットワーク上になければなりません。
- （オプション）[Communications Encryption]：フェールオーバー リンクの通信を暗号化します。**注**：秘密キーの代わりに、IPsec 事前共有キーを使用することをお勧めします。これはウィザードを終了した後に設定できます（「フェールオーバーの設定変更」（P.8-37）を参照）。

ステップ 4　ステートフル フェールオーバー用に別のインターフェイスを選択する場合は、[State Link Configuration] 画面で次の設定を行います。

- [Active IP Address]：この IP アドレスは、フェールオーバー リンクとは異なる未使用のサブネット上になければなりません。
- [Standby IP Address]：この IP アドレスは、アクティブ IP アドレスと同じネットワーク上になければなりません。

ステップ 5　[Finish] をクリックすると、ウィザードは [Waiting for Config Sync] 画面を表示します。



指定された時間が経過した後に、ウィザードはセカンダリ装置にフェールオーバー設定を送信し、フェールオーバー設定が完了したことを示す情報画面が表示されます。

- フェールオーバーがセカンダリ装置でイネーブルになっているかどうかわからない場合は、指定した時間だけ待ちます。

- フェールオーバーがすでにイネーブルなことがわかっている場合は、[Skip configuring peer] をクリックします。
- セカンダリ装置でフェールオーバーがイネーブルでないことがわかっている場合は、[Stop waiting *xx* more seconds] をクリックすると、フェールオーバーのブートストラップ設定はすぐにセカンダリ装置に送信されます。

アクティブ/アクティブ フェールオーバーの設定

High Availability and Scalability Wizard を使用して、手順を踏んでアクティブ/アクティブ フェールオーバー コンフィギュレーションを作成することができます。

手順

ステップ 1　[Wizards] > [High Availability and Scalability] を選択します。次の手順でこのウィザードのガイドラインを確認してください。

ステップ 2　[Failover Peer Connectivity and Compatibility Check] 画面で、ピアの IP アドレスは、ASDM アクセスがイネーブルになっているインターフェイスでなければなりません。

デフォルトでは、ピア アドレスは、ASDM の接続先インターフェイスのスタンバイ アドレスに割り当てられます。

ステップ 3　[Security Context Configuration] 画面では、ウィザード内でマルチ コンテキスト モードに変換した場合、管理コンテキストのみが表示されます。ウィザードを終了した後に他のコンテキストを追加できます。

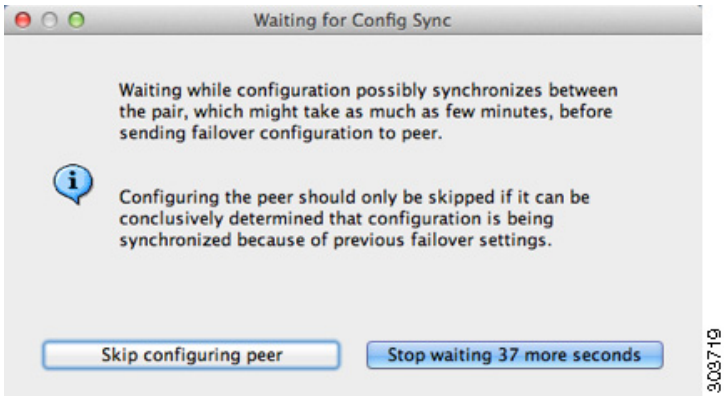
ステップ 4　[LAN Link Configuration] 画面で次のように設定します。

- [Active IP Address]：この IP アドレスは、未使用のサブネット上になければなりません。
- [Standby IP Address]：この IP アドレスは、アクティブ IP アドレスと同じネットワーク上になければなりません。
- （オプション）[Communications Encryption]：フェールオーバー リンクの通信を暗号化します。**注**：秘密キーの代わりに、IPsec 事前共有キーを使用することをお勧めします。これはウィザードを終了した後に設定できます（「フェールオーバーの設定変更」（P.8-37）を参照）。

ステップ 5　ステートフル フェールオーバー用に別のインターフェイスを選択する場合は、[State Link Configuration] 画面で次の設定を行います。

- [Active IP Address]：この IP アドレスは、フェールオーバー リンクとは異なる未使用のサブネット上になければなりません。
- [Standby IP Address]：この IP アドレスは、アクティブ IP アドレスと同じネットワーク上になければなりません。

ステップ 6　[Finish] をクリックすると、ウィザードは [Waiting for Config Sync] 画面を表示します。



指定された時間が経過した後に、ウィザードはセカンダリ装置にフェールオーバー設定を送信し、フェールオーバー設定が完了したことを示す情報画面が表示されます。

- フェールオーバーがセカンダリ装置でイネーブルになっているかどうかわからない場合は、指定した時間だけ待ちます。
- フェールオーバーがすでにイネーブルなことがわかっている場合は、[Skip configuring peer] をクリックします。
- セカンダリ装置でフェールオーバーがイネーブルでないことがわかっている場合は、[Stop waiting *xx* more seconds] をクリックすると、フェールオーバーのブートストラップ設定はすぐにセカンダリ装置に送信されます。

オプションのフェールオーバー パラメータの設定

必要に応じてフェールオーバー設定をカスタマイズできます。

- 「フェールオーバー基準、HTTP 複製、グループ プリエンプション、および MAC アドレスの設定」（P.8-30）
- 「インターフェイス モニタリングの設定およびスタンバイ アドレスの設定」（P.8-33）
- 「非対称にルーティングされたパケットのサポートの設定（アクティブ/アクティブ モード）」（P.8-34）

フェールオーバー基準、HTTP 複製、グループ プリエンプション、および MAC アドレスの設定

この項で変更可能な多くのパラメータのデフォルト設定については、「フェールオーバーのデフォルト」（P.8-27）を参照してください。アクティブ/アクティブ モードでは、ほとんどの条件をフェールオーバー グループごとに設定します。ここでは、アクティブ/アクティブ モードでのフェールオーバー グループごとの HTTP 複製のイネーブル化について説明します。アクティブ/スタンバイ モードで HTTP 複製を設定する場合は、「フェールオーバーの設定変更」（P.8-37）を参照してください。

はじめる前に

マルチ コンテキスト モードのシステム実行スペースで次の設定を行います。

手順

ステップ 7　[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Critical] タブを選択します。

ステップ 8　[Failover Poll Times] 領域で、装置のポーリング時間を設定します。

- [Unit Failover]：装置間の Hello メッセージの間の時間。範囲は 1 ～ 15 秒または 200 ～ 999 ミリ秒です。
- [Unit Hold Time]：装置がフェールオーバー リンク上で Hello メッセージを受信する必要がある時間（この時間に受信しなかった場合は、装置がピアの障害のテスト プロセスを開始する）を設定します。範囲は 1 ～ 45 秒または 800 ～ 999 ミリ秒です。ポーリング時間の 3 倍より少ない値は入力できません。

（注）　このペインの他の設定はアクティブ/スタンバイ モードにのみ適用されます。アクティブ/アクティブ モードでは、フェールオーバー グループごとに残りのパラメータを設定する必要があります。

ステップ 9　（アクティブ/アクティブ モードのみ）[Active/Active] タブをクリックし、フェールオーバー グループを選択して [Edit] をクリックします。

ステップ 10　（アクティブ/アクティブ モードのみ）フェールオーバー グループの優先するロールを変更するには、[Primary] または [Secondary] をクリックします。ウィザードを使用した場合、フェールオーバー グループ 1 はプライマリ装置に割り当てられ、フェールオーバー グループ 2 はセカンダリ装置に割り当てられます。標準以外の設定が必要な場合は、別の装置を優先するように指定できます。

ステップ 11　（アクティブ/アクティブ モードのみ）フェールオーバー グループ プリエンプションを設定するには、[Preempt after booting with optional delay of] チェックボックスをオンにします。

ある装置が他の装置よりも前に起動した場合、プライマリ設定であるかセカンダリ設定であるかにかかわらず、その装置で両方のフェールオーバー グループがアクティブになります。このオプションは、装置が使用可能になったときに、フェールオーバー グループが指定された装置で自動的にアクティブになるようにします。

オプションの delay 値に秒数を入力して、その時間フェールオーバー グループが現在の装置でアクティブ状態に維持され、その後に指定された装置で自動的にアクティブになるようにできます。有効な値は 1 ～ 1200 です。

（注）　ステートフル フェールオーバーがイネーブルの場合、プリエンプションは、フェールオーバー グループが現在アクティブになっている装置から接続が複製されるまで遅延されます。

ステップ 12　[Interface Policy] を設定するには、次のいずれかを選択します。

- [Number of failed interfaces that triggers failover]：フェールオーバーをトリガーするために必要な障害が発生したインターフェイスの具体的な数を 1 ～ 250 で定義します。障害が発生したモニタ対象インターフェイスの数が指定した値を超えると、ASA はフェールオーバーします。
- [Percentage of failed interfaces that triggers failover]：フェールオーバーをトリガーするために必要な障害が発生した設定済みインターフェイスの割合を定義します。障害が発生したモニタ対象インターフェイスの数が設定した割合を超えると、ASA はフェールオーバーします。

（注）　[Use system failover interface policy] オプションは使用しないでください。現時点ではグループごとのポリシーのみが設定できます。

ステップ 13　アクティブ/スタンバイ モードの場合、[Failover Poll Time] 領域でインターフェイス ポーリング時間を設定します。

アクティブ/アクティブ モードの場合、[Add/Edit Failover Group] ダイアログボックスでインターフェイス ポーリング時間を設定します。

- [Monitored Interfaces] : インターフェイス間でのポーリングの間の時間。範囲は 1 ～ 15 秒または 500 ～ 999 ミリ秒です。
- [Interface Hold Time] : データ インターフェイスが Hello メッセージを受信する必要がある時間を設定します。この時間が経過するとピアの障害発生が宣言されます。有効な値は 5 ～ 75 秒です。

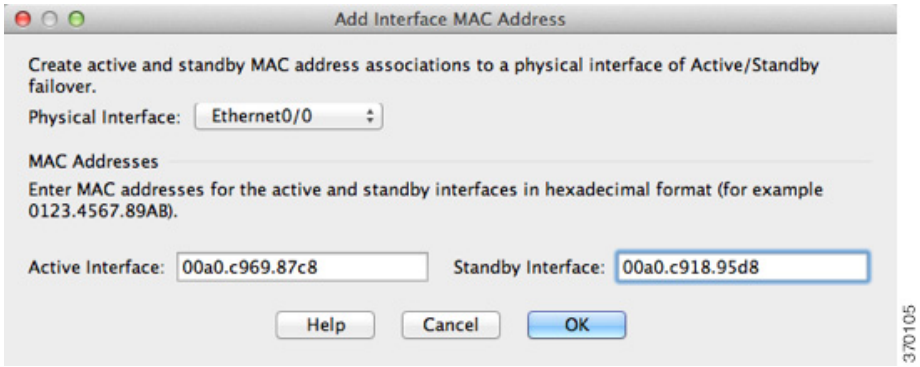
ステップ 14　（アクティブ/アクティブ モードのみ）HTTP 複製をイネーブルにするには、[Enable HTTP Replication] チェックボックスをオンにします。アクティブ/スタンバイ モードについては、「フェールオーバーの設定変更」（P.8-37）を参照してください。両方のモードに関して、HTTP 複製レートについては、「フェールオーバーの設定変更」（P.8-37）の項を参照してください。

ステップ 15　アクティブ/スタンバイ モードの場合、仮想 MAC アドレスを設定するには、[MAC Addresses] タブをクリックします。

アクティブ/アクティブ モードの場合は、[Active/Active] [タブの下部に移動します。

他の方法を使用して MAC アドレスを設定することもできますが、1 つの方法だけを使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

ステップ 16　新しい仮想 MAC アドレス エントリを追加するには、[Add] をクリックします。



[Add/Edit Interface MAC Address] ダイアログボックスが表示されます。

ステップ 17　[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。

ステップ 18　[Active MAC Address] フィールドに、アクティブ インターフェイスの新しい MAC アドレスを入力します。

ステップ 19　[Standby MAC Address] フィールドに、スタンバイ インターフェイスの新しい MAC アドレスを入力します。

ステップ 20　[OK] をクリックします。

インターフェイスがテーブルに追加されます。

ステップ 21　（アクティブ/アクティブ モードのみ）[OK] をクリックします。

ステップ 22　[Apply] をクリックします。

ステップ 23　（アクティブ/アクティブ モードのみ）必要に応じて他のフェールオーバー グループについてこの手順を繰り返します。

インターフェイス モニタリングの設定およびスタンバイ アドレスの設定

デフォルトでは、すべての物理インターフェイス（ASASM の場合はすべての VLAN インターフェイス）と、ASA にインストールされているすべてのハードウェア モジュールに対して、モニタリングはイネーブルになります。重要度の低いネットワークに接続されているインターフェイスがフェールオーバー ポリシーに影響を与えないように除外できます。

ウィザードでスタンバイ IP アドレスを設定しなかった場合は、手動で設定できます。

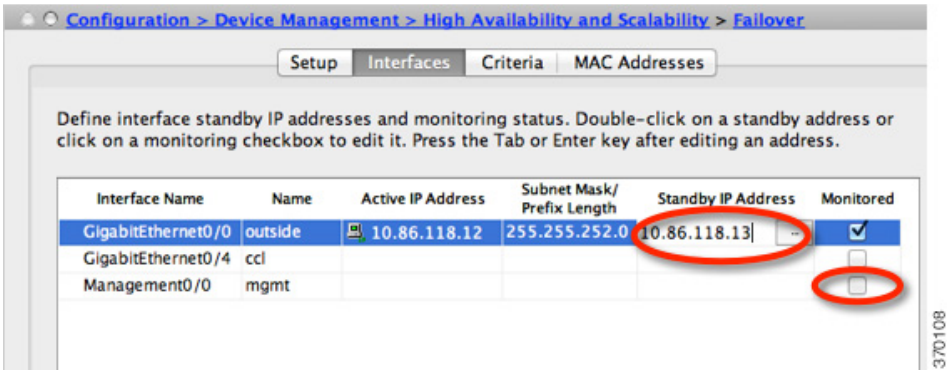
はじめる前に

- 装置ごとに最大 250 のインターフェイスをモニタできます（マルチ コンテキスト モードのすべてのコンテキストにわたって）。
- マルチ コンテキスト モードで、各コンテキスト内のインターフェイスを設定します。

手順

ステップ 1　シングル モードでは、[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces] を選択します。

マルチ コンテキスト モードでは、コンテキスト内で [Configuration] > [Device Management] > [Failover] > [Interfaces] を選択します。



設定されているインターフェイスのリストが、ASA FirePOWER モジュールなどのすべてのインストール済みのハードウェア モジュールと共に表示されます。[Monitored] カラムに、フェールオーバー基準の一部としてインターフェイスがモニタされているかどうかが表示されます。モニタされている場合は、[Monitored] チェックボックスがオンになっています。

特定のハードウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、モジュールのモニタリングをディセーブルにできます。

各インターフェイスの IP アドレスが [Active IP Address] カラムに表示されます。インターフェイスのスタンバイ IP アドレスが設定されている場合は、[Standby IP address] カラムに表示されます。フェールオーバー リンクおよびステート リンクについては IP アドレスは表示されません。これらのアドレスはこのタブから変更できません。

ステップ 2　表示されているインターフェイスのモニタリングをディセーブルにするには、インターフェイスの [Monitored] チェックボックスをオフにします。

ステップ 3　表示されているインターフェイスのモニタリングをイネーブルにするには、インターフェイスの [Monitored] チェックボックスをオンにします。

ステップ 4　スタンバイ IP アドレスを持っていない各インターフェイスに対して、[Standby IP Address] フィールドをダブルクリックしてフィールドに IP アドレスを入力します。

ステップ 5　[Apply] をクリックします。

非対称にルーティングされたパケットのサポートの設定（アクティブ/アクティブ モード）

アクティブ/アクティブ フェールオーバーでの実行中に、ピア装置を経由して開始された接続に対する返送パケットを、装置が受信する場合があります。そのパケットを受信する ASA にはそのパケットの接続情報がないために、パケットはドロップされます。このドロップが多く発生するのは、アクティブ/アクティブ フェールオーバー ペアの 2 台の ASA が異なるサービス プロバイダーに接続されており、アウトバウンド接続に NAT アドレスが使用されていない場合です。

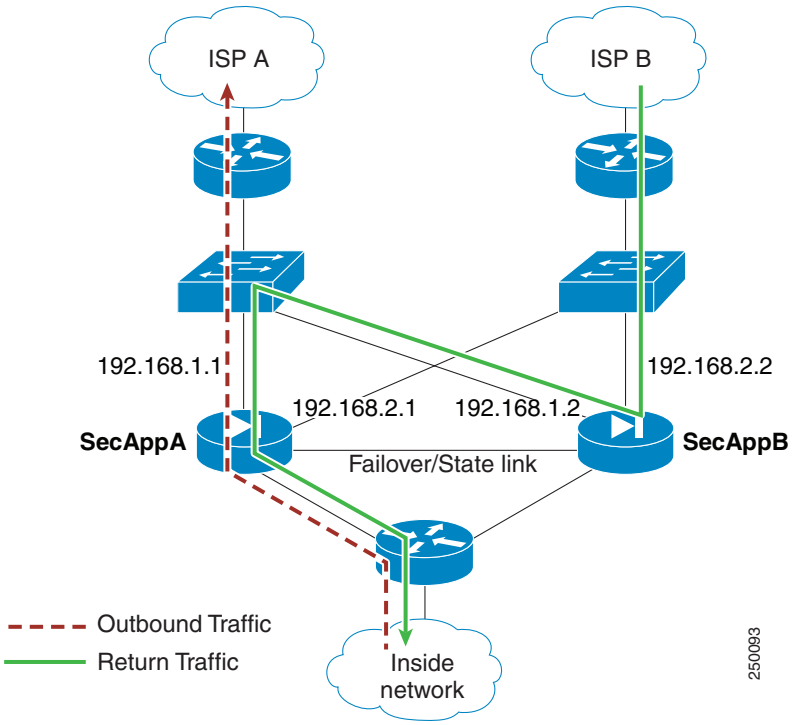
返送パケットのドロップは、非対称にルーティングされたパケットを許可することによって防ぐことができます。そのためには、それぞれの ASA の同様のインターフェイスを同じ ASR グループに割り当てます。たとえば、両方の ASA が、内部インターフェイスで内部ネットワークに接続しているが、外部インターフェイスでは別の ISP に接続しているとします。プライマリ装置で、アクティブ コンテキストの外部インターフェイスを ASR グループ 1 に割り当て、セカンダリ装置でも、アクティブ コンテキストの外部インターフェイスを同じ ASR グループ 1 に割り当てます。プライマリ装置の外部インターフェイスがセッション情報を持たないパケットを受信すると、同じグループ（この場合 ASR グループ 1）内のスタンバイ コンテキストの他のインターフェイスのセッション情報をチェックします。一致する情報が見つからない場合、パケットはドロップされます。一致する情報が見つかると、次の動作のうちいずれかが開始します。

- 着信トラフィックがピア装置に発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットは他の装置にリダイレクトされます。このリダイレクトは、セッションがアクティブである限り続行されます。
- 着信トラフィックが同じ装置の別のインターフェイスに発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットはストリームに再注入されます。

（注）　この機能は、非対称ルーティングを提供しません。非対称にルーティングされたパケットを正しいインターフェイスに戻します。

図 8-13 に、非対称にルーティングされたパケットの例を示します。

図 8-13　ASR の例



1. アウトバンド セッションが、アクティブな SecAppA コンテキストを持つ ASA を通過します。このパケットは、インターフェイス outsideISP-A（192.168.1.1）から送信されます。
2. 非対称ルーティングがアップストリームのどこかで設定されているため、リターン トラフィックは、アクティブな SecAppB コンテキストを持つ ASA のインターフェイス outsideISP-B（192.168.2.2）経由で戻ります。
3. 通常、リターン トラフィックは、そのインターフェイス 192.168.2.2 上にリターン トラフィックに関するセッション情報がないので、ドロップされます。しかし、このインターフェイスは、ASR グループ 1 の一部として設定されています。装置は、同じ ASR グループ ID で設定された他のインターフェイス上のセッションを探します。
4. このセッション情報は、SecAppB を持つ装置上のスタンバイ状態のインターフェイス outsideISP-A（192.168.1.2）にあります。ステートフル フェールオーバーは、SecAppA から SecAppB にセッション情報を複製します。
5. ドロップされる代わりに、レイヤ 2 ヘッダーはインターフェイス 192.168.1.1 の情報で書き直され、トラフィックはインターフェイス 192.168.1.2 からリダイレクトされます。そこから、発信元の装置のインターフェイスを経由して戻ります（SecAppA の 192.168.1.1）。この転送は、必要に応じて、セッションが終了するまで続行されます。

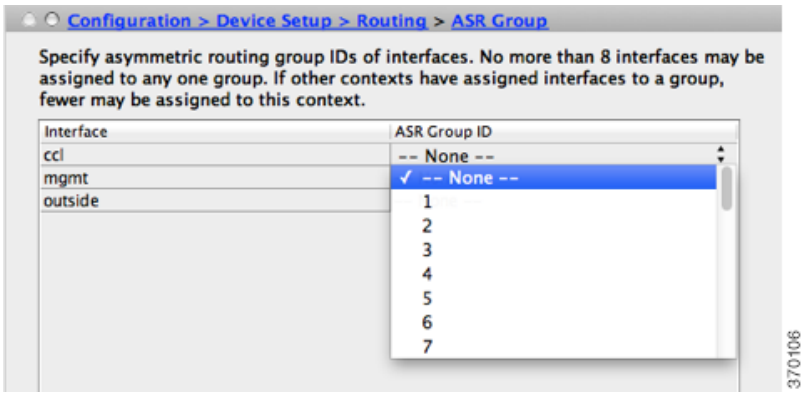
前提条件

- ステートフル フェールオーバー：アクティブ フェールオーバー グループにあるインターフェイスのセッションのステート情報を、スタンバイ フェールオーバー グループに渡します。

- HTTP 複製：HTTP セッションのステート情報は、スタンバイ フェールオーバー グループに渡されないため、スタンバイ インターフェイスに存在しません。ASA が非対称にルーティングされた HTTP パケットを再ルーティングできるように、HTTP ステート情報を複製する必要があります。
- プライマリ装置およびセカンダリ装置の各アクティブ コンテキスト内でこの手順を実行します。

手順の詳細

ステップ 1　プライマリ装置のアクティブ コンテキストで、[Configuration] > [Device Setup] > [Routing] > [ASR Groups] を選択します。



ステップ 2　非対称にルーティングされたパケットを受信するインターフェイスについて、ドロップダウン リストから ASR グループ番号を選択します。

ステップ 3　[Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

ステップ 4　ASDM をセカンダリ装置に接続し、プライマリ装置のコンテキストと同様のアクティブ コンテキストを選択します。

ステップ 5　[Configuration] > [Device Setup] > [Routing] > [ASR Groups] を選択します。

ステップ 6　この装置の同様のインターフェイスについて、同じ ASR グループ番号を選択します。

ステップ 7　[Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

フェールオーバーの管理

フェールオーバーの設定変更

ウィザードを使用しない場合や、設定を変更する場合に、手動でフェールオーバーを設定できます。ここでは、ウィザードに含まれていないため手動で設定する必要がある次のオプションについても説明します。

- フェールオーバー トラフィックを暗号化するための IPsec 事前共有キー
- HTTP 複製レート
- HTTP 複製（アクティブ/スタンバイ モード）

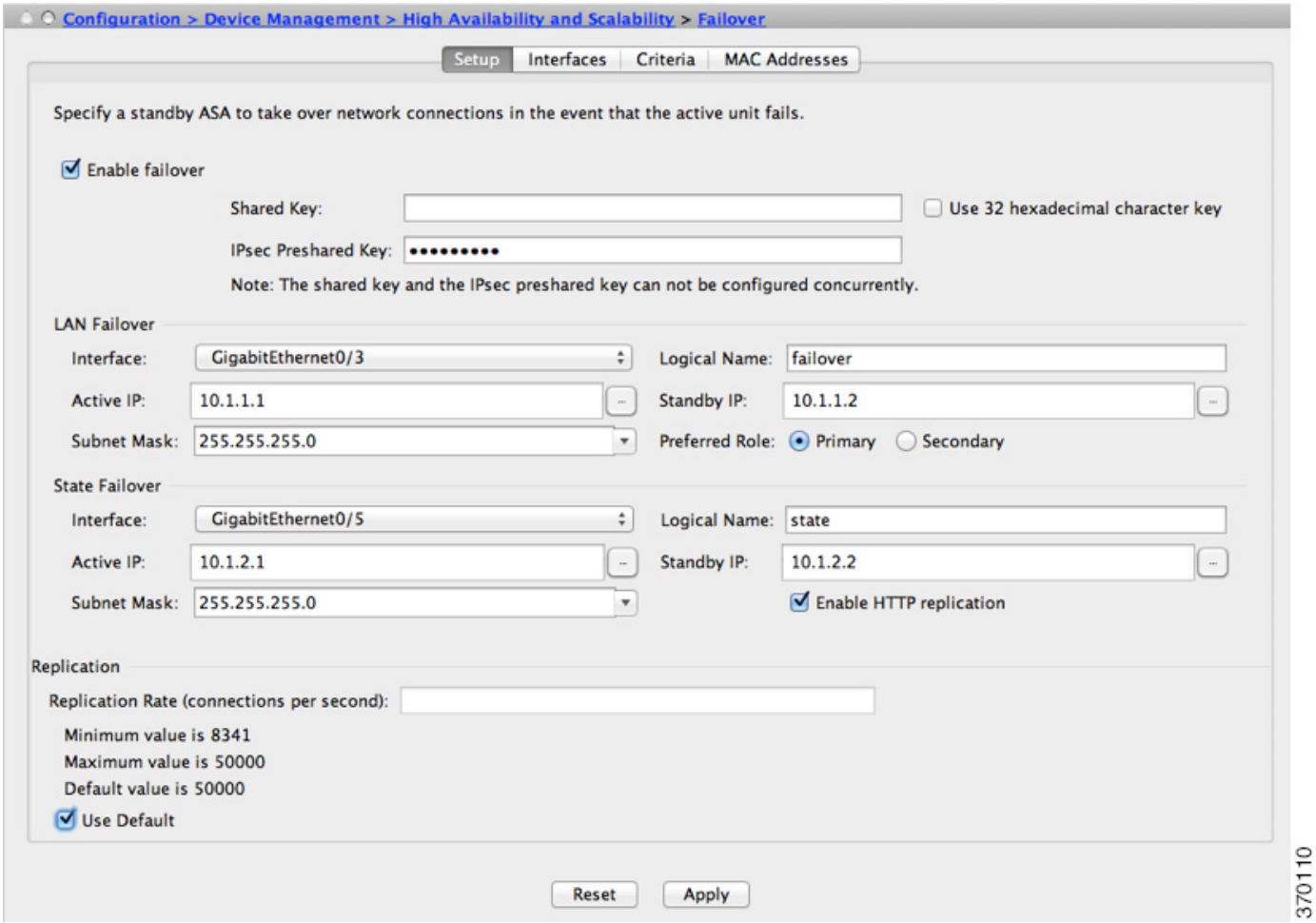
前提条件

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順の詳細

ステップ 1　シングル モードでは、[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Setup] を選択します。

マルチ コンテキスト モードでは、システム実行スペースで [Configuration] > [Device Management] > [Failover] > [Setup] を選択します。



ステップ 2　[Enable Failover] チェックボックスをオンにします。

（注）　デバイスに変更を適用するまで、フェールオーバーは実際にはイネーブルになりません。

ステップ 3　フェールオーバー リンクおよびステート リンクの通信を暗号化するには、次のオプションのいずれかを使用します。

- [IPsec Preshared Key]（優先）：フェールオーバー装置間のフェールオーバー リンクで IPsec LAN-to-LAN トンネルを確立するために、IKEv2 によって使用される事前共有キーです。注：フェールオーバー LAN-to-LAN トンネルは、IPsec（他の VPN）ライセンスには適用されません。
- [Secret Key]：フェールオーバー通信の暗号化に使用される秘密キーを入力します。このフィールドを空白のままにした場合は、コマンド複製中に送信されるコンフィギュレーション内のパスワードまたはキーを含め、フェールオーバー通信がクリア テキストになります。

  [Use 32 hexadecimal character key]：秘密キーに 32 文字の 16 進キーを使用するには、このチェックボックスをオンにします。

ステップ 4　[LAN Failover] 領域で、フェールオーバー リンクの次のパラメータを設定します。

- [Interface]：フェールオーバー リンクに使用するインターフェイスを選択します。フェールオーバーには専用インターフェイスが必要ですが、ステートフル フェールオーバーとインターフェイスを共有できます。

  このリストには、未設定のインターフェイスまたはサブインターフェイスのみが表示され、フェールオーバー リンクとして選択できます。インターフェイスをフェールオーバー リンクに指定すると、そのインターフェイスは [Configuration] > [Interfaces] ペインでは編集できません。
- [Logical Name]：「failover」などのフェールオーバー通信に使用するインターフェイスの論理名を指定します。この名前は情報を提供するためのものです。
- [Active IP]：インターフェイスのアクティブ IP アドレスを指定します。IP アドレスは、IPv4 または IPv6 アドレスのどちらにすることもできます。この IP アドレスは未使用のサブネット上になければなりません。
- [Standby IP]：インターフェイスのスタンバイ IP アドレスを指定します。アクティブ IP アドレスと同じサブネット上のアドレスを指定します。
- [Subnet Mask]：サブネット マスクを指定します。
- [Preferred Role]：この ASA の優先されるロールがプライマリ装置であるかセカンダリ装置であるかを指定するために、[Primary] または [Secondary] を選択します。

ステップ 5　（オプション）次の手順でステート リンクを設定します。

- [Interface]：ステート リンクに使用するインターフェイスを選択します。選択できるのは、未設定のインターフェイスまたはサブインターフェイス、フェールオーバー リンク、または [--Use Named--] オプションです。

  （注）　フェールオーバー リンク専用インターフェイスとステート リンク専用インターフェイスの 2 つのインターフェイスを別々に使用することを推奨します。

  未設定のインターフェイスまたはサブインターフェイスを選択した場合、そのインターフェイスのアクティブ IP、サブネット マスク、スタンバイ IP、および論理名を入力する必要があります。

フェールオーバー リンクを選択した場合は、アクティブ IP、サブネット マスク、論理名、およびスタンバイ IP の値を指定する必要はありません。フェールオーバー リンクに指定されている値が使用されます。

[--Use Named--] オプションを選択した場合、[Logical Name] フィールドは、名前のついたインターフェイスのドロップダウン リストになります。このリストからインターフェイスを選択します。アクティブ IP、サブネット マスク/プレフィックスの長さ、スタンバイ IP の値を指定する必要はありません。そのインターフェイスに指定された値が使用されます。

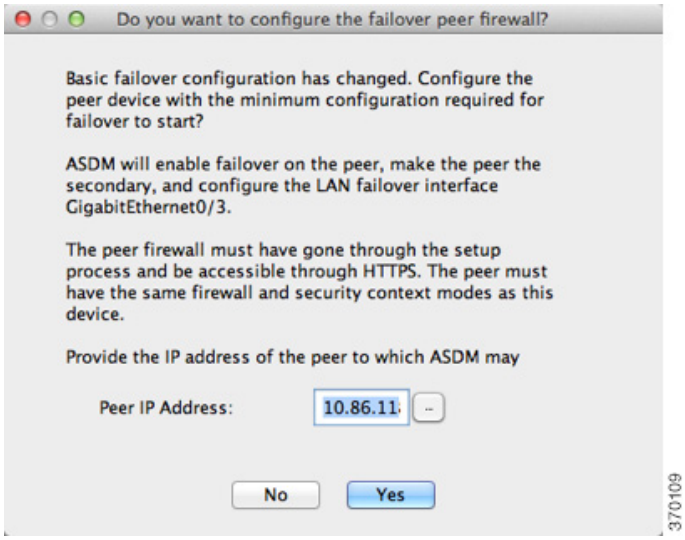
- [Logical Name]：「state」などのステートの通信に使用するインターフェイスの論理名を指定します。この名前は情報を提供するためのものです。
- [Active IP]：インターフェイスのアクティブ IP アドレスを指定します。IP アドレスは、IPv4 または IPv6 アドレスのどちらにすることもできます。この IP アドレスは、フェールオーバー リンクとは異なる未使用のサブネット上になければなりません。
- [Standby IP]：インターフェイスのスタンバイ IP アドレスを指定します。アクティブ IP アドレスと同じサブネット上のアドレスを指定します。
- [Subnet Mask]：サブネット マスクを指定します。
- （任意、アクティブ/スタンバイのみ）[Enable HTTP Replication]：[Enable HTTP Replication] チェックボックスをオンにすると、HTTP の複製をイネーブルにします。このオプションにより、アクティブ HTTP セッションをスタンバイ ファイアウォールにコピーするステートフル フェールオーバーがイネーブルになります。HTTP 複製を許可しない場合、HTTP 接続はフェールオーバーの発生時に切断されます。アクティブ/アクティブ モードでは、フェールオーバー グループごとに HTTP 複製を設定します。「フェールオーバー基準、HTTP 複製、グループ プリエンプション、および MAC アドレスの設定」（P.8-30）を参照してください。

ステップ 6　[Replication] 領域で、HTTP 複製レートを 1 秒あたり 8341 ～ 50000 接続の範囲で設定します。デフォルトは 50000 です。デフォルトを使用するには、[Use Default] チェックボックスをオンにします。

ステップ 7　[Apply] をクリックします。

コンフィギュレーションがデバイスに保存されます。

ステップ 8　フェールオーバーをイネーブルにすると、フェールオーバー ピアを設定するためのダイアログ ボックスが表示されます。



- 後でフェールオーバー ピアに接続して手動で同様の設定を行う場合は、[No] をクリックします。
- ASDM によって自動的にフェールオーバー ピア上の関連するフェールオーバー設定が行われるようにするには、[Yes] をクリックします。[Peer IP Address] フィールドにピアの IP アドレスを指定します。

フェールオーバーの強制実行

スタンバイ装置を強制的にアクティブにするには、次の手順を実行します。

前提条件

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順の詳細

ステップ 1　フェールオーバーを装置レベルで強制するには次を行います。

a. コンテキスト モードに応じて画面を選択します。

- シングル コンテキスト モードでは、[Monitoring] > [Properties] > [Failover] > [Status] を選択します。
- マルチ コンテキスト モードでは、システムで [Monitoring] > [Failover] > [System] を選択します。

b. 次のいずれかのボタンをクリックします。

- [Make Active] をクリックすると、この装置がアクティブ装置になります。
- [Make Standby] をクリックすると、相手装置がアクティブ装置になります。

ステップ 2　（アクティブ/アクティブ モードのみ）フェールオーバーをフェールオーバー グループ レベルで強制するには次を行います。

a. システムで、[Monitoring] > [Failover] > [Failover Group #] を開きます。# は、制御するフェールオーバー グループの番号です。

b. 次のいずれかのボタンをクリックします。

- [Make Active] をクリックすると、この装置でフェールオーバー グループがアクティブになります。
- [Make Standby] をクリックすると、相手装置でフェールオーバー グループがアクティブになります。

フェールオーバーのディセーブル化

フェールオーバーをディセーブルにするには、次の手順を実行します。

前提条件

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順の詳細

ステップ 1　シングル モードでは、[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Setup] を選択します。

マルチ コンテキスト モードでは、システム実行スペースで [Configuration] > [Device Management] > [Failover] > [Setup] を選択します。

ステップ 2　[Enable Failover] チェックボックスをオフにします。

ステップ 3　[Apply] をクリックします。

障害が発生した装置の復元

障害が発生した装置を障害のない状態に復元するには、次の手順を実行します。

前提条件

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順の詳細

ステップ 1　フェールオーバーを装置レベルで復元するには次を行います。

a.　コンテキスト モードに応じて画面を選択します。

- シングル コンテキスト モードでは、[Monitoring] > [Properties] > [Failover] > [Status] を選択します。
- マルチ コンテキスト モードでは、システムで [Monitoring] > [Failover] > [System] を選択します。

b.　[Reset Failover] をクリックします。

ステップ 2　（アクティブ/アクティブ モードのみ）フェールオーバーをフェールオーバー グループ レベルで復元するには次を行います。

a.　システムで、[Monitoring] > [Failover] > [Failover Group #] を開きます。# は、制御するフェールオーバー グループの番号です。

b.　[Reset Failover] をクリックします。

コンフィギュレーションの再同期

複製されたコマンドは、実行コンフィギュレーションに保存されます。複製されたコマンドをスタンバイ装置のフラッシュ メモリに保存するには、[File] > [Save Running Configuration to Flash] の順に選択します。

フェールオーバー動作のモニタ

フェールオーバー メッセージ

フェールオーバーが発生すると、両方の ASA がシステム メッセージを送信します。

フェールオーバーの syslog メッセージ

ASA は、フェールオーバーに関連する多くの syslog メッセージを、深刻な状況を表すプライオリティ レベル 2 で送信します。これらのメッセージについては、syslog メッセージ ガイドを参照してください。ロギングをイネーブルにするには、第 40 章「ロギング」を参照してください。

（注）　フェールオーバーの最中に、インターフェイスは論理的にシャットダウンされてから起動し、syslog メッセージ 411001 および 411002 が生成されます。これは通常のアクティビティです。

フェールオーバー デバッグ メッセージ

デバッグ メッセージを表示するには、**debug fover** コマンドを入力します。詳細については、コマンド リファレンスを参照してください。

（注）　CPU プロセスではデバッグ出力に高プライオリティが割り当てられているため、デバッグ出力を行うとシステム パフォーマンスに大きく影響することがあります。このため、**debug fover** コマンドは、特定の問題に対するトラブルシューティングや、Cisco TAC とのトラブルシューティング セッションに限定して使用してください。

SNMP のフェールオーバー トラップ

フェールオーバーに対する SNMP syslog トラップを受信するには、SNMP トラップを SNMP 管理ステーションに送信するように SNMP エージェントを設定し、syslog ホストを定義し、お使いの SNMP 管理ステーションに Cisco syslog MIB をコンパイルします。詳細については、第 41 章「SNMP」を参照してください。

フェールオーバー動作のモニタ

（注）フェールオーバー イベントが発生した後、デバイスのモニタリングを継続するには、ASDM を再起動するか、または [Devices] ペインに表示される別のデバイスに切り替えて、元の ASA に戻る手順を実行する必要があります。この操作が必要なのは、ASDM がデバイスから切断されて再接続された場合、接続のモニタリングが再確立されないためです。

[Monitoring] > [Properties] > [Failover] を選択して、アクティブ/スタンバイ フェールオーバーをモニタします。

[Monitoring] > [Properties] > [Failover] 領域で次の画面を使用して、アクティブ/アクティブ フェールオーバーをモニタします。

- 「システム」（P.8-43）
- 「[Failover Group 1] と [Failover Group 2]」（P.8-44）

システム

[System] ペインには、システムのフェールオーバー状態が表示されます。また、システムのフェールオーバー状態を次の方法で制御できます。

- デバイスのアクティブ/スタンバイ状態を切り替える。
- 障害が発生したデバイスをリセットする。
- スタンバイ装置をリロードする。

フィールド

[Failover state of the system]：*表示専用*。ASA のフェールオーバー状態を表示します。表示される情報は、**show failover** コマンドで受け取る出力と同じです。表示出力に関する詳細については、コマンド リファレンスを参照してください。

[System] ペインでは、次のアクションを使用できます。

- [Make Active]：アクティブ/スタンバイ コンフィギュレーションで、このボタンをクリックすると、ASA がアクティブ装置になります。アクティブ/アクティブ コンフィギュレーションで、このボタンをクリックすると、ASA で両方のフェールオーバー グループがアクティブになります。
- [Make Standby]：アクティブ/スタンバイ ペアで、このボタンをクリックすると、ASA がスタンバイ装置になります。アクティブ/アクティブ コンフィギュレーションで、このボタンをクリックすると、ASA で両方のフェールオーバー グループがスタンバイ状態になります。
- [Reset Failover]：このボタンをクリックして、システムを障害状態からスタンバイ状態にリセットします。システムをアクティブ状態にはリセットできません。アクティブ装置でこのボタンをクリックすると、スタンバイ装置がリセットされます。
- [Reload Standby]：このボタンをクリックして、スタンバイ装置を強制的にリロードします。
- [Refresh]：このボタンをクリックして、[system] フィールドのフェールオーバー状態にあるステータス情報をリフレッシュします。

[Failover Group 1] と [Failover Group 2]

[Failover Group 1] ペインおよび [Failover Group 2] ペインには、選択したグループのフェールオーバー状態が表示されます。また、グループのアクティブ/スタンバイ状態を切り替えるか、または障害が発生したグループをリセットして、グループのフェールオーバー状態を制御することもできます。

フィールド

[Failover state of Group[*x*]]：*表示専用*。選択したフェールオーバー グループのフェールオーバー状態を表示します。表示される情報は、**show failover group** コマンドで受け取る出力と同じです。

このペインで次のアクションを実行できます。

- [Make Active]：このボタンをクリックして、ASA でフェールオーバー グループをアクティブ装置にします。
- [Make Standby]：このボタンをクリックして、ASA でフェールオーバー グループを強制的にスタンバイ状態にします。
- [Reset Failover]：このボタンをクリックして、システムを障害状態からスタンバイ状態にリセットします。システムをアクティブ状態にはリセットできません。アクティブ装置でこのボタンをクリックすると、スタンバイ装置がリセットされます。
- [Refresh]：このボタンをクリックして、[system] フィールドのフェールオーバー状態にあるステータス情報をリフレッシュします。

フェールオーバーの機能履歴

表 8-4 に、この機能のリリース履歴を示します。

表 8-4　オプションのアクティブ/スタンバイ フェールオーバー設定の機能履歴

機能名	リリース	機能情報
アクティブ/スタンバイ フェールオーバー	7.0(1)	この機能が導入されました。
アクティブ/アクティブ フェールオーバー	7.0(1)	この機能が導入されました。
フェールオーバー キーの 16 進数値サポート	7.0(4)	フェールオーバー リンクの暗号化用に 16 進数値が指定できるようになりました。 次の画面が変更になりました。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup]。

表 8-4　　オプションのアクティブ/スタンバイ フェールオーバー設定の機能履歴

機能名	リリース	機能情報
フェールオーバー キーのマスター パスフレーズのサポート	8.3(1)	フェールオーバー キーが、実行コンフィギュレーションとスタートアップ コンフィギュレーションの共有キーを暗号化するマスター パスフレーズをサポートするようになりました。一方の ASA から他方に共有秘密をコピーする場合、たとえば、**more system:running-config** コマンドを使用して、正常に暗号化共有キーをコピーして貼り付けることができます。 （注）　**show running-config** の出力では、**failover key** の共有秘密は ***** のように表示されます。このマスクされたキーはコピーできません。 ASDM の変更はありませんでした。
フェールオーバーに IPv6 のサポートが追加されました。	8.2(2)	次の画面が変更されました。 [Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup]。 [Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces]。
フェールオーバー リンクおよびステート リンクの通信を暗号化する IPsec LAN-to-LAN トンネルのサポート	9.1(2)	フェールオーバー キーに独自の暗号化を使用する代わりに、フェールオーバー リンクおよびステート リンクの暗号化に IPsec LAN-to-LAN トンネルが使用できるようになりました。 （注）　フェールオーバー LAN-to-LAN トンネルは、IPsec（他の VPN）ライセンスには適用されません。 次の画面が変更になりました。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup]。
ハードウェア モジュールのヘルス モニタリングのディセーブル化	9.3(1)	ASA はデフォルトで、設置されているハードウェア モジュール（ASA FirePOWER モジュールなど）のヘルス モニタリングを行います。特定のハードウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、モジュールのモニタリングをディセーブルにできます。 次の画面が変更になりました。[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Interfaces]

ASA クラスタ

クラスタリングを利用すると、複数の ASA をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

（注） 一部の機能は、クラスタリングを使用する場合、サポートされません。「クラスタリングでサポートされない機能」（P.9-25）を参照してください。

ASA クラスタリングについて

ここでは、クラスタリング アーキテクチャとその動作について説明します。

- 「ロード バランシングの方式」（P.9-13）
- 「Inter-Site クラスタリング」（P.9-19）
- 「ASA クラスタが接続を管理する方法」（P.9-23）
- 「ASA の機能とクラスタリング」（P.9-25）

ASA クラスタをネットワークに適合させる方法

クラスタは、複数の ASA で構成され、これらは 1 つのユニットとして機能します。ASA をクラスタとして機能させるには、次のインフラストラクチャが必要です。

- クラスタ内通信用の、隔離された高速バックプレーン ネットワーク。*クラスタ制御リンク*と呼ばれます。
- 各 ASA への管理アクセス（コンフィギュレーションおよびモニタリングのため）。

クラスタをネットワーク内に配置するときは、クラスタが送受信するデータのロード バランシングを、アップストリームおよびダウンストリームのルータが次のいずれかの方法でできることが必要です。

- スパンド EtherChannel（推奨）：クラスタ内の複数のメンバのインターフェイスをグループ化して 1 つの EtherChannel とします。この EtherChannel がユニット間のロード バランシングを実行します。
- ポリシーベース ルーティング（ルーテッド ファイアウォール モードのみ）：アップストリームとダウンストリームのルータが、ルート マップと ACL を使用してユニット間のロード バランシングを実行します。
- 等コスト マルチパス ルーティング（ルーテッド ファイアウォール モードのみ）：アップストリームとダウンストリームのルータが、等コストのスタティックまたはダイナミックルートを使用してユニット間のロード バランシングを実行します。

関連項目

- 「ASA クラスタリングのライセンス」（P.9-32）
- 「クラスタ制御リンク」（P.9-6）
- 「ASA クラスタ管理」（P.9-12）
- 「スパンド EtherChannel（推奨）」（P.9-14）
- 「ポリシーベース ルーティング（ルーテッド ファイアウォール モードのみ）」（P.9-18）
- 「等コスト マルチパス ルーティング（ルーテッド ファイアウォール モードのみ）」（P.9-19）

パフォーマンス スケーリング係数

複数のユニットを結合して 1 つのクラスタとしたときに、期待できるパフォーマンスの概算値は次のようになります。

- 合計スループットの 70 %
- 最大接続数の 60 %
- 接続数/秒の 50 %

たとえば、スループットについては、ASA 5585-X と SSP-40 が処理できる実際のファイアウォール トラフィックは、単独動作時は約 10 Gbps となります。8 ユニットのクラスタでは、合計スループットの最大値は約 80 Gbps（8 ユニット x 10 Gbps）の 70 %、つまり 56 Gbps となります。

クラスタ メンバ

クラスタ メンバは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を実現します。ここでは、各メンバのロールの特長について説明します。

- 「ブートストラップ コンフィギュレーション」（P.9-3）
- 「マスターおよびスレーブ ユニットの役割」（P.9-3）
- 「マスター ユニット選定」（P.9-3）

ブートストラップ コンフィギュレーション

各デバイスで、最小限のブートストラップ コンフィギュレーション（クラスタ名、クラスタ制御リンク インターフェイスなどのクラスタ設定）を設定します。クラスタリングを最初にイネーブルにしたユニットが一般的にはマスターユニットとなります。以降のユニットに対してクラスタリングをイネーブルにすると、そのユニットは*スレーブ*としてクラスタに参加します。

マスターおよびスレーブ ユニットの役割

クラスタ内のメンバの 1 つがマスター ユニットです。マスター ユニットは、ブートストラップ コンフィギュレーション内のプライオリティ設定によって決まります。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。他のすべてのメンバはスレーブ ユニットです。一般的には、クラスタを作成した後で最初に追加したユニットがマスター ユニットとなります。これは単に、その時点でクラスタに存在する唯一のユニットであるからです。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、マスター ユニット上のみで実行する必要があります。コンフィギュレーションは、スレーブ ユニットに複製されます。物理的資産（たとえばインターフェイス）の場合は、マスター ユニットのコンフィギュレーションがすべてのスレーブ ユニット上でミラーリングされます。たとえば、GigabitEthernet 0/1 を内部インターフェイスとして、GigabitEthernet 0/0 を外部インターフェイスとして設定した場合は、これらのインターフェイスはスレーブ ユニット上でも、内部および外部のインターフェイスとして使用されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能についてはマスター ユニットがすべてのトラフィックを処理します。

関連項目

- 「クラスタリングの中央集中型機能」（P.9-26）

マスター ユニット選定

クラスタのメンバは、クラスタ制御リンクを介して通信してマスター ユニットを選定します。方法は次のとおりです。

1. ユニットに対してクラスタリングをイネーブルにしたとき（または、クラスタリングがイネーブル済みの状態でそのユニットを初めて起動したとき）に、そのユニットは選定要求を 3 秒間隔でブロードキャストします。
2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。
3. 45 秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットがマスターになります。

（注）　最高のプライオリティを持つユニットが複数ある場合は、クラスタ ユニット名、次にシリアル番号を使用してマスターが決定されます。

4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的にマスター ユニットになることはありません。既存のマスター ユニットは常にマスターのままです。ただし、マスター ユニットが応答を停止すると、その時点で新しいマスター ユニットが選定されます。

（注）　特定のユニットを手動で強制的にマスターにすることができます。中央集中型機能については、マスター ユニット変更を強制するとすべての接続がドロップされるので、新しいマスター ユニット上で接続を再確立する必要があります。

関連項目

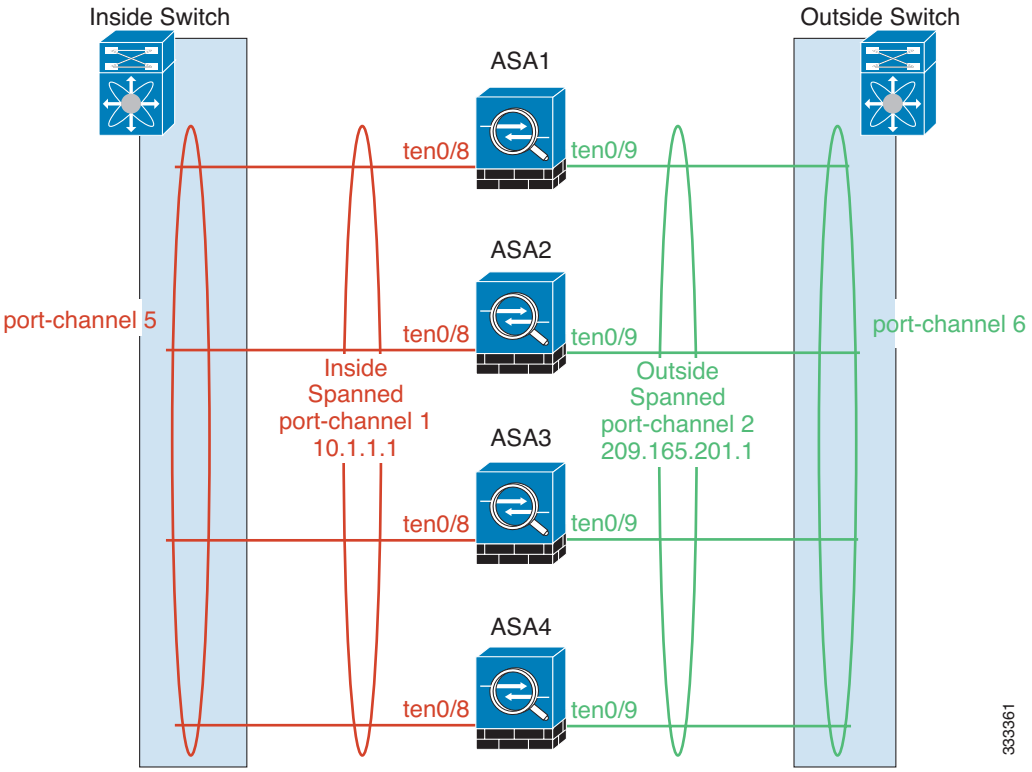
- 「クラスタリングの中央集中型機能」（P.9-26）

クラスタ インターフェイス

データ インターフェイスは、スパンド EtherChannel として設定することも、個別インターフェイスとして設定することもできます。1 つのクラスタ内のすべてのデータ インターフェイスのタイプが同一であることが必要です。

スパンド EtherChannel（推奨）

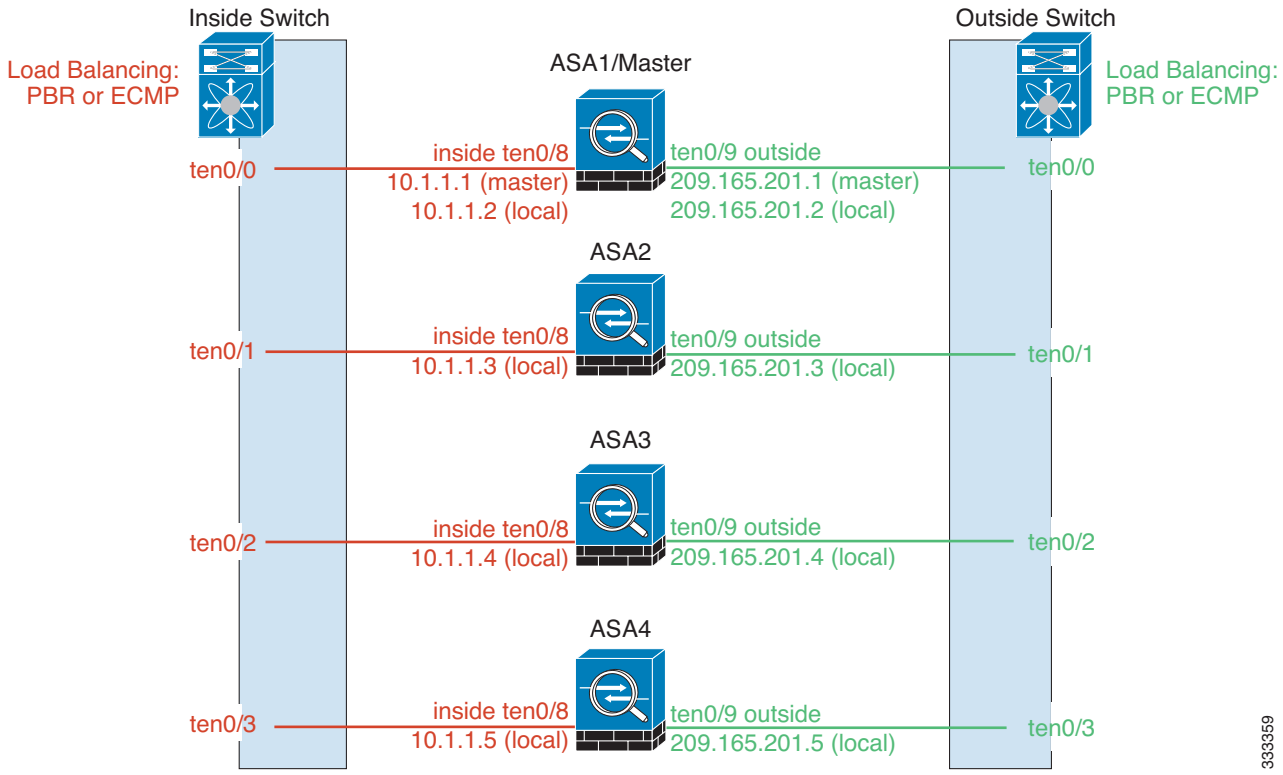
ユニットあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのユニットに広がる EtherChannel とすることができます。EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォール モードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはインターフェイスではなくブリッジ グループに割り当てられます。EtherChannel は初めから、ロード バランシング機能を基本的動作の一部として備えています。



個別インターフェイス（ルーテッド ファイアウォール モードのみ）

個別インターフェイスは通常のルーテッド インターフェイスであり、それぞれが専用の *ローカル IP アドレス*を持ちます。インターフェイス コンフィギュレーションはマスター ユニット上だけで行う必要があるため、このインターフェイス コンフィギュレーションの中で IP アドレス プールを設定して、このプールのアドレスをクラスタ メンバ（マスター用を含む）のインターフェイスに使用させることができます。*メイン クラスタ IP アドレス*は、そのクラスタのための固定アドレスであり、常に現在のマスター ユニットに属します。メイン クラスタ IP アドレスは、マスター ユニットのセカンダリ IP アドレスです。ローカル IP アドレスが常にルーティングのプライマリ アドレスになります。このメイン クラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。マスター ユニットが変更されると、メイン クラスタ IP アドレスは新しいマスター ユニットに移動するので、クラスタの管理をシームレスに続行できます。ただし、ロード バランシングを別途する必要があります（この場合はアップストリーム スイッチ上で）。

（注） 個別インターフェイスはルーティング プロトコルに基づきトラフィックをロード バランシングしますが、ルーティング プロトコルはリンク障害時にコンバージェンスが遅くなることがよくあるので、個別インターフェイスの代わりにスパンド EtherChannel を推奨します。



関連項目

- 「ロード バランシングの方式」（P.9-13）

クラスタ制御リンク

各ユニットの、少なくとも 1 つのハードウェア インターフェイスをクラスタ制御リンク専用とする必要があります。

- 「クラスタ制御リンク トラフィックの概要」（P.9-6）
- 「クラスタ制御リンク インターフェイスとネットワーク」（P.9-7）
- 「クラスタ制御リンクのサイジング」（P.9-7）
- 「クラスタ制御リンクの冗長性」（P.9-8）
- 「クラスタ制御リンクの信頼性」（P.9-9）
- 「クラスタ制御リンクの障害」（P.9-9）

クラスタ制御リンク トラフィックの概要

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- マスター選定。
- コンフィギュレーションの複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- ステート複製。
- 接続所有権クエリーおよびデータ パケット転送。

関連項目

- 「クラスタ メンバ」（P.9-3）
- 「コンフィギュレーションの複製」（P.9-11）
- 「ユニットのヘルス モニタリング」（P.9-9）
- 「データ パス接続状態の複製」（P.9-11）
- 「新しい TCP 接続のクラスタ全体での再分散」（P.9-24）

クラスタ制御リンク インターフェイスとネットワーク

次の例外を除き、クラスタ制御リンクには任意のデータ インターフェイスを使用できます。

- VLAN サブインターフェイスをクラスタ制御リンクとして使用することはできません。
- 管理 *x*/*x* インターフェイスをクラスタ制御リンクとして使用することはできません（単独か EtherChannel かにかかわらず）。
- ASA IPS モジュール搭載 ASA 5585-X では、モジュール インターフェイスをクラスタ制御リンクに使用することはできません。ただし、ASA 5585-X ネットワーク モジュールではインターフェイスを使用できます。

EtherChannel インターフェイスまたは冗長インターフェイスを使用できます。

ASA 5585-X と SSP-10 および SSP-20（2 個の 10 ギガビット イーサネット インターフェイスを持つ）については、一方のインターフェイスをクラスタ制御リンクに使用し、他方をデータに使用することを推奨します（データについてはサブインターフェイスを使用できます）。この設定は、クラスタ制御リンクの冗長性には対応しませんが、クラスタ制御リンクのサイズをデータ インターフェイスのサイズと一致させるという要件は満たされます。

各クラスタ制御リンクは、同じサブネット上の IP アドレスを持ちます。このサブネットは、他のすべてのトラフィックからは隔離し、ASA クラスタ制御リンク インターフェイスだけが含まれるようにしてください。

2 メンバー クラスタの場合、ASA と ASA の間をクラスタ制御リンクで直接接続しないでください。インターフェイスを直接接続した場合、一方のユニットで障害が発生すると、クラスタ制御リンクが機能せず、他の正常なユニットも動作しなくなります。スイッチを介してクラスタ制御リンクを接続した場合は、正常なユニットについてはクラスタ制御リンクは動作を維持します。

関連項目

- 「クラスタ制御リンクの冗長性」（P.9-8）
- 「クラスタ制御リンクのサイジング」（P.9-7）

クラスタ制御リンクのサイジング

各メンバの予想されるスループットと一致するように、クラスタ制御リンクのサイズを決定する必要があります。たとえば、ASA 5585-X と SSP-60 を使用する場合は、クラスタのユニットあたり最大 14 Gbps を通過させることができるので、クラスタ制御リンクに割り当てるインターフェイスも、最低 14 Gbps の通過が可能となるようにしてください。この場合は、たとえば 10 ギガビット イーサネット インターフェイス 2 つを EtherChannel としてクラスタ制御リンクに使用し、残りのインターフェイスを必要に応じてデータ リンクに使用します。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。たとえば、状態アップデートは通過トラフィック量の最大 10 % に及ぶことがあります（通過トラフィックの内容が、存続期間の短い TCP 接続のみの場合）。転送されるトラフィックの量は、ロード バランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。
- ネットワーク アクセスに対する AAA は一元的な機能であるため、すべてのトラフィックがマスター ユニットに転送されます。
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

（注）　クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

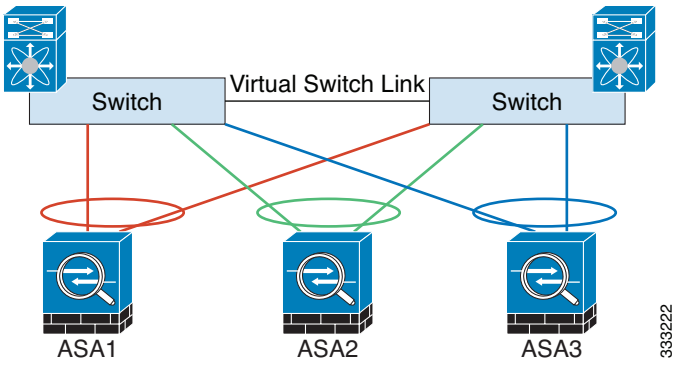
関連項目

- 「Inter-Site クラスタリング」（P.9-19）

クラスタ制御リンクの冗長性

クラスタ制御リンクには EtherChannel を使用することを推奨します。冗長性を実現しながら、EtherChannel 内の複数のリンクにトラフィックを渡すことができます。

次の図は、仮想スイッチング システム（VSS）または仮想ポート チャネル（vPC）環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリンクがアクティブです。スイッチが VSS または vPC の一部である場合は、同じ EtherChannel 内の ASA インターフェイスをそれぞれ、VSS または vPC 内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。この EtherChannel は、スパンド EtherChannel ではなく、デバイス ローカルであることに注意してください。



クラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間（RTT）が 20 ms 未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタ メンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクで ping を実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

クラスタ制御リンクの障害

ユニットのクラスタ制御リンク回線プロトコルがダウンした場合、クラスタリングはディセーブルになります。データ インターフェイスはシャット ダウンされます。クラスタ制御リンクの修復後、クラスタリングを再度イネーブルにして手動でクラスタに再参加する必要があります。

（注）ASA が非アクティブになると、すべてのデータ インターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはアクセスできません（マスター ユニットと同じメイン IP アドレスを使用するため）。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

関連項目

「クラスタへの再参加」（P.9-10）

ASA クラスタ内のハイ アベイラビリティ

ASA クラスタリングは、ユニットとインターフェイスの正常性を監視し、ユニット間で接続状態を複製することにより、ハイ アベイラビリティを提供します。

ユニットのヘルス モニタリング

マスター ユニットは、各スレーブ ユニットをモニタするために、クラスタ制御リンクを介してキープアライブ メッセージを定期的に送信します（間隔は設定可能です）。各スレーブ ユニットは、同じメカニズムを使用してマスター ユニットをモニタします。

インターフェイスのモニタ

各ユニットは、使用中のすべてのハードウェア インターフェイスのリンク ステータスをモニタし、ステータス変更をマスター ユニットに報告します。

- スパンド EtherChannel：クラスタ Link Aggregation Control Protocol（cLACP）を使用します。各ユニットは、リンク ステータスおよび cLACP プロトコル メッセージをモニタして、ポートがまだ EtherChannel でアクティブであるかどうかを判断します。ステータスがマスター ユニットに報告されます。
- 個別インターフェイス（ルーテッド モードのみ）：各ユニットが自身のインターフェイスを自己モニタし、インターフェイスのステータスをマスター ユニットに報告します。

ユニットまたはインターフェイスの障害

ヘルス モニタリングがイネーブルのときは、ユニットまたはそのインターフェイスで障害が発生するとそのユニットが削除されます。あるインターフェイスが、特定のユニット上では障害が発生したが、別のユニットではアクティブの場合は、そのユニットはクラスタから削除されます。ASA がメンバをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバであるか、またはクラスタに参加しようとしているかによって異なります。EtherChannel の場合（スパニングかどうかを問わない）は、確立済みメンバのインターフェイスがダウン状態のときに、ASA はそのメンバを 9 秒後に削除します。ASA は、ユニットがクラスタに参加する最初の 90 秒間はインターフェイスを監視ししません。この間にインターフェイスのステータスが変化しても、ASA はクラスタから削除されません。非 EtherChannel の場合は、メンバ状態に関係なく、ユニットは 500 ミリ秒後に削除されます。

クラスタ内のユニットで障害が発生したときに、そのユニットでホスティングされている接続は他のユニットにシームレスに移管されます。トラフィック フローのステート情報は、クラスタ制御リンクを介して共有されます。

マスター ユニットで障害が発生した場合は、そのクラスタの他のメンバのうち、プライオリティが最高（番号が最小）のものがマスターになります。

ASA は自動的にクラスタへの再参加を試みます。

（注）　ASA が非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータ インターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはアクセスできません（マスター ユニットと同じメイン IP アドレスを使用するため）。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

関連項目

「クラスタへの再参加」（P.9-10）

クラスタへの再参加

クラスタ メンバがクラスタから削除された後、クラスタに再参加できる方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害：クラスタ制御リンクの問題を解決した後、クラスタリングを再びイネーブルにすることによって、手動でクラスタに再参加する必要があります。

- データ インターフェイスの障害：ASA は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、ASA はクラスタリングをディセーブルにします。データ インターフェイスの問題を解決した後、手動でクラスタリングをイネーブルにする必要があります。
- ユニットの障害：ユニットがヘルス チェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働していて、クラスタリングがまだイネーブルになっているなら、ユニットは再起動するとクラスタに再参加することを意味します。

関連項目

- 「ASA クラスタ パラメータの設定」（P.9-54）

データ パス接続状態の複製

どの接続にも、1 つのオーナーおよび少なくとも 1 つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。

オーナーが使用不可能になった場合は、その接続からパケットを受け取る最初のユニット（ロード バランシングに基づく）がバックアップ オーナーに問い合わせて、関連するステート情報を取得し、これでそのユニットが新しいオーナーになることができます。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 9-1　クラスタ全体で複製される ASA の機能

トラフィック	状態のサポート	注意
Up time	Yes	システム アップ タイムをトラッキングします。
ARP Table	Yes	トランスペアレント モードのみ。
MAC アドレス テーブル	Yes	トランスペアレント モードのみ。
ユーザ アイデンティティ	Yes	AAA ルール（uauth）とアイデンティティ ファイアウォールが含まれます。
IPv6 ネイバー データベース	Yes	—
ダイナミック ルーティング	Yes	—
SNMP エンジン ID	**No**	—
VPN（サイト間）	**No**	VPN セッションは、マスター ユニットで障害が発生すると切断されます。

コンフィギュレーションの複製

クラスタ内のすべてのユニットは、単一のコンフィギュレーションを共有します。最初のブートストラップ コンフィギュレーションを除き、コンフィギュレーション変更を加えることができるのはマスター ユニット上だけであり、変更は自動的にクラスタ内の他のすべてのユニットに複製されます。

ASA クラスタ管理

ASA クラスタリングを使用することの利点の 1 つは、管理のしやすさです。ここでは、クラスタを管理する方法について説明します。

- 「管理ネットワーク」（P.9-12）
- 「管理インターフェイス」（P.9-12）
- 「マスター ユニット管理と スレーブ ユニット管理の違い」（P.9-13）
- 「RSA キー複製」（P.9-13）
- 「ASDM 接続証明書 IP アドレス不一致」（P.9-13）

管理ネットワーク

すべてのユニットを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

管理インターフェイス

管理インターフェイスについては、専用管理インターフェイスの 1 つを使用することを推奨します。管理インターフェイスは、個別インターフェイスとして設定することも（ルーテッド モードとトランスペアレント モードの両方）、スパンド EtherChannel インターフェイスとして設定することもできます。

管理用には、個別インターフェイスを使用することを推奨します（スパンド EtherChannel をデータ インターフェイスに使用している場合でも）。個別インターフェイスならば、必要に応じて各ユニットに直接接続できますが、スパンド EtherChannel インターフェイスでは、現在のマスター ユニットへのリモート接続しかできません。

（注）　スパンド EtherChannel インターフェイス モードを使用しているときに、管理インターフェイスを個別インターフェイスとして設定する場合は、管理インターフェイスに対してダイナミック ルーティングをイネーブルにすることはできません。スタティック ルートを使用する必要があります。

個別インターフェイスの場合は、メイン クラスタ IP アドレスはそのクラスタの固定アドレスであり、常に現在のマスター ユニットに属します。インターフェイスごとに、管理者はアドレス範囲も設定します。これで、各ユニット（現在のマスターも含まれます）がその範囲内のローカル アドレスを使用できるようになります。このメイン クラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。マスター ユニットが変更されると、メイン クラスタ IP アドレスは新しいマスター ユニットに移動するので、クラスタの管理をシームレスに続行できます。ローカル IP アドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。

たとえば、クラスタを管理するにはメイン クラスタ IP アドレスに接続します。このアドレスは常に、現在のマスター ユニットに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。

TFTP や syslog などの発信管理トラフィックの場合、マスター ユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバに接続します。

スパンド EtherChannel インターフェイスの場合は、IP アドレスは 1 つだけ設定でき、その IP アドレスは常にマスター ユニットに関連付けられます。EtherChannel インターフェイスを使用してスレーブ ユニットに直接接続することはできません。管理インターフェイスは個別インターフェイスとして設定することを推奨します。各ユニットに接続できるようにするためです。デバイス ローカル EtherChannel を管理に使用できます。

マスター ユニット管理と スレーブ ユニット管理の違い

ブートストラップ コンフィギュレーションを除き、すべての管理とモニタリングはマスター ユニットで実行できます。マスター ユニットから、すべてのユニットの実行時統計情報やリソース使用状況などのモニタリング情報を調べることができます。また、クラスタ内のすべてのユニットに対してコマンドを発行することや、コンソール メッセージをスレーブ ユニットからマスター ユニットに複製することもできます。

必要に応じて、スレーブ ユニットを直接モニタできます。マスター ユニットからでもできますが、ファイル管理をスレーブ ユニット上で実行できます（コンフィギュレーションのバックアップや、イメージの更新など）。次の機能は、マスター ユニットからは使用できません。

- ユニットごとのクラスタ固有統計情報のモニタリング。
- ユニットごとの Syslog モニタリング。
- SNMP
- NetFlow

RSA キー複製

マスター ユニット上で RSA キーを作成すると、そのキーはすべてのスレーブ ユニットに複製されます。メイン クラスタ IP アドレスへの SSH セッションがある場合に、マスター ユニットで障害が発生すると接続が切断されます。新しいマスター ユニットは、SSH 接続に対して同じキーを使用するので、新しいマスター ユニットに再接続するときに、キャッシュ済みの SSH ホスト キーを更新する必要はありません。

ASDM 接続証明書 IP アドレス不一致

デフォルトでは、自己署名証明書は、ローカル IP アドレスに基づいて ASDM 接続に使用されます。ASDM を使用してメイン クラスタ IP アドレスに接続する場合は、IP アドレス不一致に関する警告メッセージが表示されます。これは、証明書で使用されているのがローカル IP アドレスであり、メイン クラスタ IP アドレスではないからです。このメッセージは無視して、ASDM 接続を確立できます。ただし、この種の警告を回避するには、新しい証明書を登録し、この中でメイン クラスタ IP アドレスと、IP アドレス プールからのすべてのローカル IP アドレスを指定します。この証明書を各クラスタ メンバに使用します。

関連項目

- 第 35 章「デジタル証明書」

ロード バランシングの方式

使用可能なロード バランシング方式は、ファイアウォール モードとインターフェイスのタイプによって異なります。

- 「スパンド EtherChannel（推奨）」（P.9-14）
- 「ポリシーベース ルーティング（ルーテッド ファイアウォール モードのみ）」（P.9-18）
- 「等コスト マルチパス ルーティング（ルーテッド ファイアウォール モードのみ）」（P.9-19）

スパンド EtherChannel（推奨）

ユニットあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのユニットに広がる EtherChannel とすることができます。EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。

- 「スパンド EtherChannel の利点」（P.9-14）
- 「最大スループットのガイドライン」（P.9-14）
- 「ロード バランシング」（P.9-14）
- 「EtherChannel の冗長性」（P.9-15）
- 「VSS または vPC への接続」（P.9-15）

スパンド EtherChannel の利点

EtherChannel 方式のロードバランシングは、次のような利点から、他の方式よりも推奨されます。

- 障害検出までの時間が短い。
- コンバージェンス時間が短い。個別インターフェイスはルーティング プロトコルに基づきトラフィックをロード バランシングしますが、ルーティング プロトコルはリンク障害時にコンバージェンスが遅くなることがよくあります。
- コンフィギュレーションが容易である。

関連項目

「EtherChannel」（P.10-5）

最大スループットのガイドライン

最大スループットを実現するには、次のことを推奨します。

- 使用するロード バランシング ハッシュ アルゴリズムは「対称」であるようにします。つまり、どちらの方向からのパケットも同じハッシュを持たせて、スパンド EtherChannel 内の同じ ASA に送信します。送信元と宛先の IP アドレス（デフォルト）または送信元と宛先のポートをハッシュ アルゴリズムとして使用することを推奨します。
- ASA をスイッチに接続するときは、同じタイプのラインカードを使用します。すべてのパケットに同じハッシュ アルゴリズムが適用されるようにするためです。

ロード バランシング

EtherChannel リンクは、送信元または宛先 IP アドレス、TCP ポートおよび UDP ポート番号に基づいて、専用のハッシュ アルゴリズムを使用して選択されます。

（注）ASA では、デフォルトのロードバランシング アルゴリズムを変更しないでください。スイッチでは、アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS または Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタ内の ASA へのトラフィックが均等に分散されなくなることがあるため、ロードバランシング アルゴリズムでは、**vlan** キーワードを使用しないでください。

EtherChannel 内のリンク数はロード バランシングに影響を及ぼします。

対称ロード バランシングは常に可能とは限りません。NAT を設定する場合は、フォワード パケットとリターン パケットとで IP アドレスやポートが異なります。リターン トラフィックはハッシュに基づいて別のユニットに送信されるため、クラスタはほとんどのリターン トラフィックを正しいユニットにリダイレクトする必要があります。

関連項目

- 「EtherChannel のカスタマイズ」（P.10-24）
- 「ロード バランシング」（P.10-7）
- 「NAT とクラスタリング」（P.9-30）

EtherChannel の冗長性

EtherChannel には、冗長性機能が組み込まれています。これは、すべてのリンクの回線プロトコル ステータスをモニタします。リンクの 1 つで障害が発生すると、トラフィックは残りのリンク間で再分散されます。EtherChannel のすべてのリンクが特定のユニット上で停止したが、他方のユニットがまだアクティブである場合は、そのユニットはクラスタから削除されます。

VSS または vPC への接続

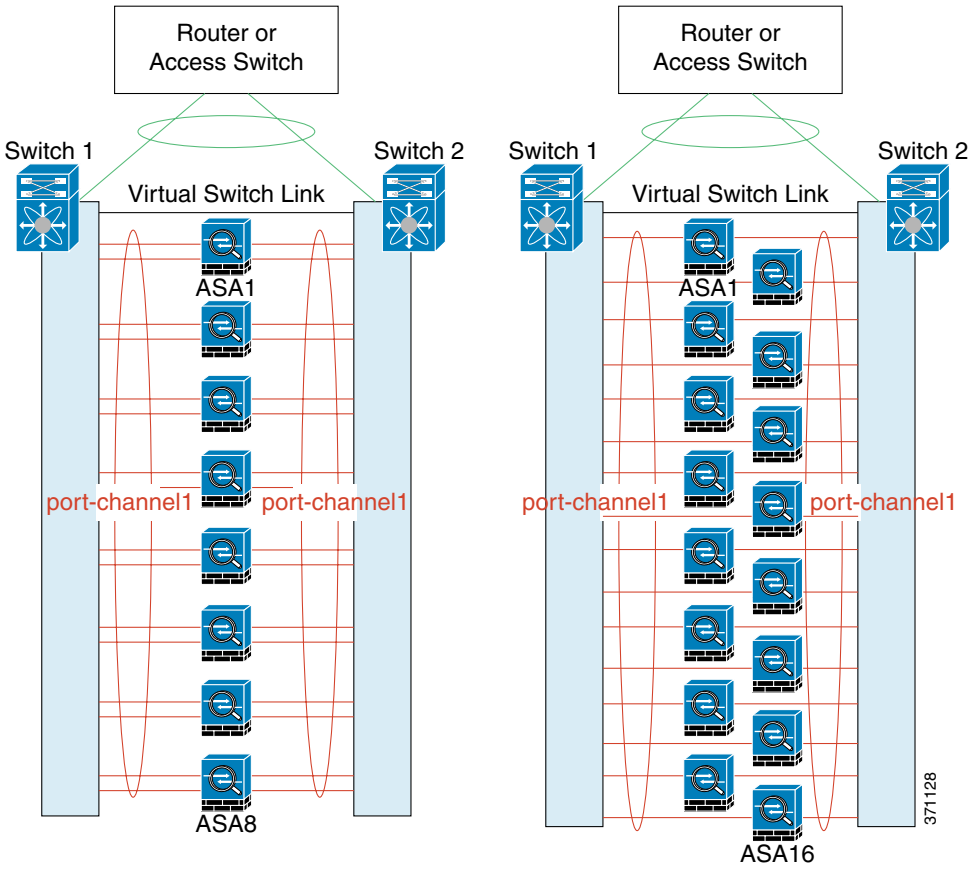
1 つの ASA につき複数のインターフェイスを、スパンド EtherChannel に入れることができます。1 つの ASA につき複数のインターフェイスが特に役立つのは、VSS または vPC の両方のスイッチに接続するときです。

スイッチによっては、スパンド EtherChannel に最大 32 個のアクティブ リンクを設定できます。この機能では、vPC 内の両方のスイッチが、それぞれ 16 個のアクティブ リンクの EtherChannel をサポートする必要があります（例 : Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。

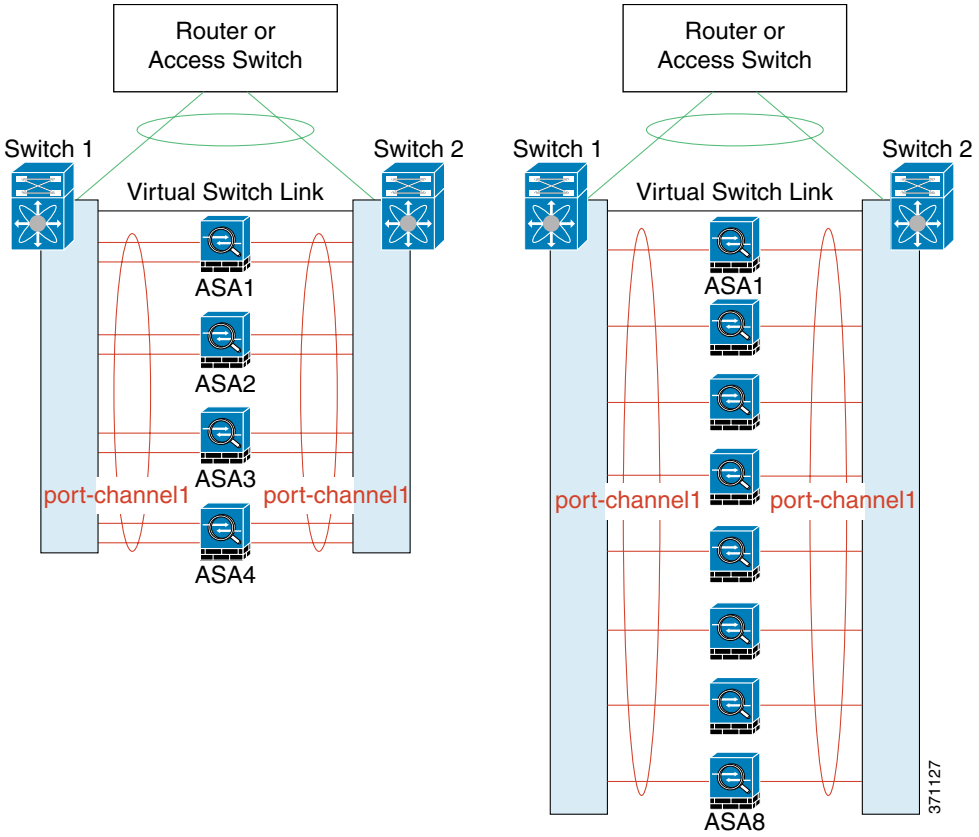
EtherChannel で 8 個のアクティブ リンクをサポートするスイッチの場合、VSS/vPC で 2 台のスイッチに接続すると、スパンド EtherChannel に最大 16 個のアクティブ リンクを設定できます。

スパンド EtherChannel で 8 個より多くのアクティブ リンクを使用する場合は、スタンバイ リンクも使用できません。9 ～ 32 個のアクティブ リンクをサポートするには、スタンバイ リンクの使用を可能にする cLACP ダイナミック ポート プライオリティをディセーブルにする必要があります。それでも、必要であれば、たとえば 1 台のスイッチに接続するときに、8 個のアクティブ リンクと 8 個のスタンバイ リンクを使用できます。

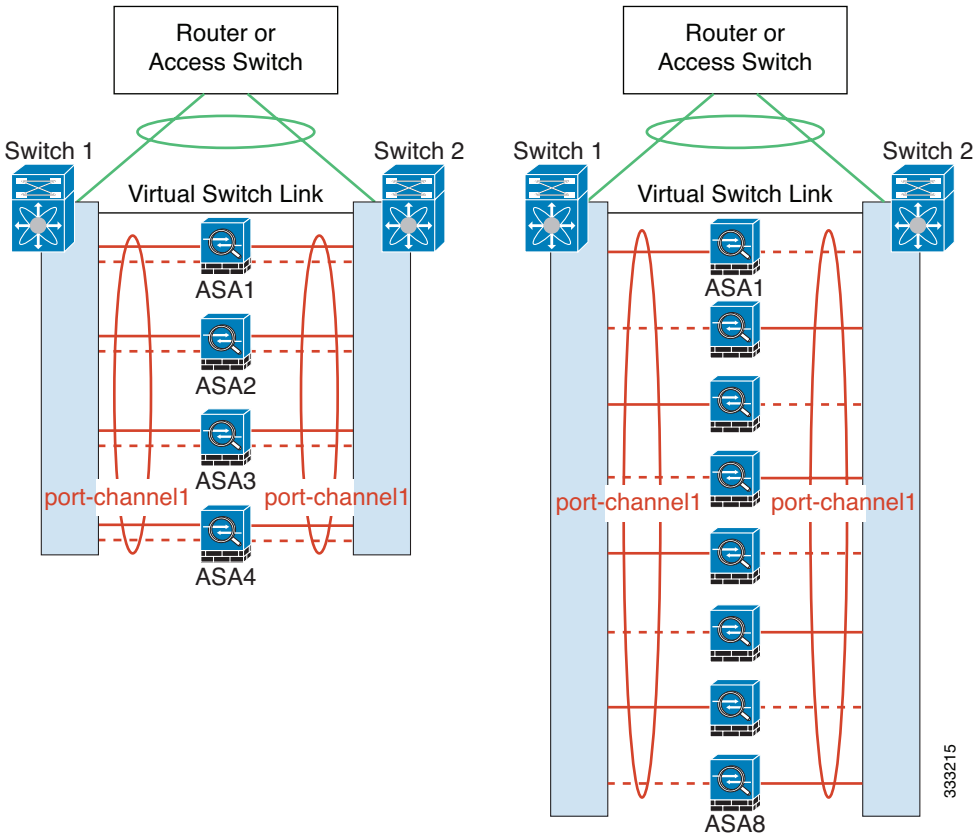
次の図では、8 ASA クラスタおよび 16 ASA クラスタでの 32 アクティブ リンクのスパンド EtherChannel を示します。


Router or
Access Switch
Switch 1
Switch 2
Virtual Switch Link
ASA1
port-channel1
port-channel1
ASA8
Router or
Access Switch
Switch 1
Switch 2
Virtual Switch Link
ASA1
port-channel1
port-channel1
ASA16
371128

次の図では、4 ASA クラスタおよび 8 ASA クラスタでの 16 アクティブ リンクのスパンド EtherChannel を示します。



次の図では、4 ASA クラスタおよび 8 ASA クラスタでの従来の 8 アクティブ リンク/8 スタンバイ リンクのスパンド EtherChannel を示します。アクティブ リンクは実線で、非アクティブ リンクは点線で示しています。cLACP ロードバランシングは、EtherChannel のリンクのうち最良の 8 本を自動的に選択してアクティブにすることができます。つまり、cLACP は、リンク レベルでのロード バランシング実現に役立ちます。



ポリシーベース ルーティング（ルーテッド ファイアウォール モードのみ）

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。ロード バランシング方法の 1 つが、ポリシーベース ルーティング（PBR）です。

この方法が推奨されるのは、すでに PBR を使用しており、既存のインフラストラクチャを活用したい場合です。この方法は、スパンド EtherChannel に対しても、追加調整オプションを提供する場合があります。

PBR は、ルート マップおよび ACL に基づいて、ルーティングの決定を行います。管理者は、手動でトラフィックをクラスタ内のすべての ASA に分ける必要があります。PBR は静的であるため、常に最適なロード バランシング結果を実現できないこともあります。最高のパフォーマンスを達成するには、PBR ポリシーを設定するときに、同じ接続のフォワードとリターンのパケットが同じ物理的 ASA に送信されるように指定することを推奨します。たとえば、Cisco ルータがある場合は、冗長性を実現するには Cisco IOS PBR をオブジェクト トラッキングとともに使用します。Cisco IOS オブジェクト トラッキングは、ICMP ping を使用して各 ASA をモニタします。これで、PBR は、特定の ASA の到達可能性に基づいてルート マップをイネーブルまたはディセーブルにできます。詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

（注）　このロードバランシング方法を使用する場合は、デバイス ローカル EtherChannel を個別インターフェイスとして使用できます。

等コスト マルチパス ルーティング（ルーテッド ファイアウォール モードのみ）

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。ロード バランシング方法の 1 つが、等コスト マルチパス（ECMP）ルーティングです。

この方法が推奨されるのは、すでに ECMP を使用しており、既存のインフラストラクチャを活用したい場合です。この方法は、スパンド EtherChannel に対しても、追加調整オプションを提供する場合があります。

ECMP ルーティングでは、ルーティング メトリックが同値で最高である複数の「最適パス」を介してパケットを転送できます。EtherChannel のように、送信元および宛先の IP アドレスや送信元および宛先のポートのハッシュを使用してネクスト ホップの 1 つにパケットを送信できます。ECMP ルーティングにスタティック ルートを使用する場合は、ASA の障害発生時に問題が起きることがあります。ルートは引き続き使用されるため、障害が発生した ASA へのトラフィックが失われるからです。スタティック ルートを使用する場合は必ず、オブジェクト トラッキングなどのスタティック ルート モニタリング機能を使用してください。ダイナミック ルーティング プロトコルを使用してルートの追加と削除を行うことを推奨します。この場合は、ダイナミック ルーティングに参加するように各 ASA を設定する必要があります。

（注）　このロードバランシング方法を使用する場合は、デバイス ローカル EtherChannel を個別インターフェイスとして使用できます。

Inter-Site クラスタリング

サイト間インストールの場合、次のガイドラインに従う限り ASA クラスタリングを利用できます。

- 「Inter-Site クラスタリングのガイドライン」（P.9-19）
- 「Data Center Interconnect のサイジング」（P.9-20）
- 「Inter-Site での例」（P.9-21）

Inter-Site クラスタリングのガイドライン

Inter-Site クラスタリングについては、次のガイドラインを参照してください。

- 次のインターフェイスおよびファイアウォール モードで Inter-Site クラスタリングをサポートします。

	ファイアウォール モード	
インターフェイス モード	ルーテッド	トランスペアレント
個別インターフェイス	**Yes**	該当なし
スパンド EtherChannel	No	**Yes**

- クラスタ制御リンクの遅延が、ラウンドトリップ時間（RTT）20 ms 未満である必要があります。
- クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、専用リンクを使用する必要があります。
- 接続の再分散を設定しないでください。異なるサイトのクラスタ メンバには接続を再分散できません。
- クラスタの実装では複数のサイトのメンバが区別されません。したがって、特定の接続に対する接続のロールが複数のサイトにまたがる場合があります。これは想定されている動作です。
- トランスペアレント モードの場合、両方の内部ルータが同じ MAC アドレスを共有し、両方の外部ルータが同じ MAC アドレスを共有する必要があります。サイト 1 のクラスタ メンバがサイト 2 のメンバに接続を転送する時、宛先 MAC アドレスは維持されます。MAC アドレスがサイト 1 のルータと同じである場合にのみ、パケットはサイト 2 のルータに到達します。
- スパンド EtherChannel モードの場合、サイト間の ASA クラスタに直接接続されているデータ VLAN を拡張しないでください。ループが発生します。拡張データ VLAN はすべて、ルータによってクラスタから分離する必要があります。

関連項目

- 「新しい TCP 接続のクラスタ全体での再分散」（P.9-24）
- 「接続のロール」（P.9-23）

Data Center Interconnect のサイジング

次の計算と同等の帯域幅をクラスタ制御リンク トラフィック用に Data Center Interconnect（DCI）に確保する必要があります。

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

メンバの数が各サイトで異なる場合、計算には大きい方の値を使用します。DCI の最小帯域幅は、1 つのメンバに対するクラスタ制御リンクのサイズ未満にすることはできません。

次に例を示します。

- 2 サイトの 4 メンバの場合。
  - 合計 4 クラスタ メンバ
  - 各サイト 2 メンバ
  - メンバあたり 5 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 5 Gbps（2/2 x 5 Gbps）。
- 2 サイトの 8 メンバの場合、サイズは増加します。
  - 合計 8 クラスタ メンバ
  - 各サイト 4 メンバ
  - メンバあたり 5 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 10 Gbps（4/2 x 5 Gbps）。
- 3 サイトの 6 メンバの場合。
  - 合計 6 クラスタ メンバ
  - サイト 1 は 3 メンバ、サイト 2 は 2 メンバ、サイト 3 は 1 メンバ

  - メンバあたり 10 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 15 Gbps（3/2 x 10 Gbps）。

- 2 サイトの 2 メンバの場合。
  - 合計 2 クラスタ メンバ
  - 各サイト 1 メンバ
  - メンバあたり 10 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 10 Gbps（1/2 x 10 Gbps = 5 Gbps、ただし最小帯域幅がクラスタ制御リンク（10 Gbps）のサイズ未満になってはなりません）。

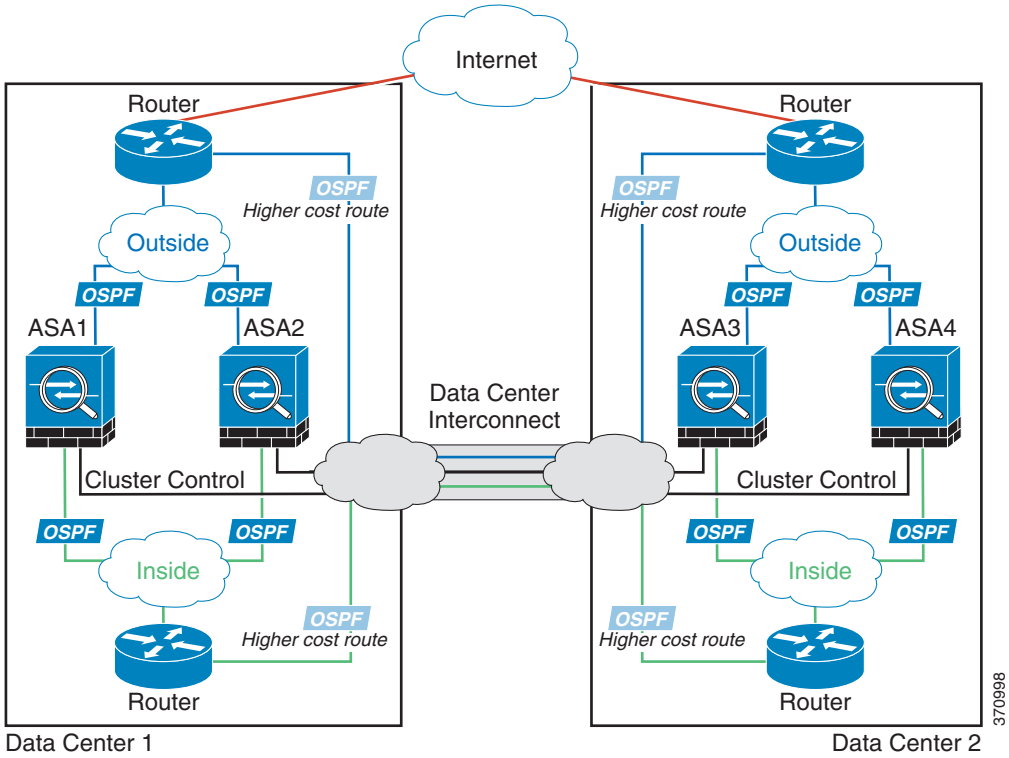
Inter-Site での例

次の例ではサポートされるクラスタの導入を示します。

- 「個別インターフェイス Inter-Site の例」（P.9-21）
- 「スパンド EtherChannel トランスペアレント モード Inter-Site の例」（P.9-22）

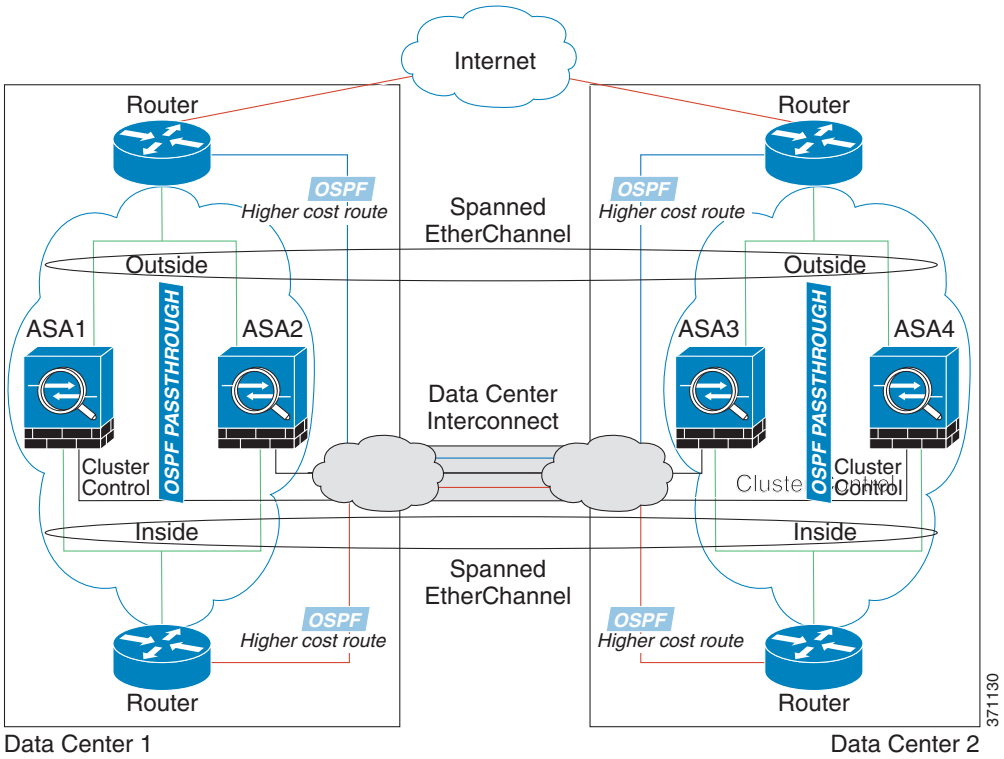
個別インターフェイス Inter-Site の例

次の例では、2 つのデータセンターのそれぞれに 2 つの ASA クラスタ メンバがある場合を示します。クラスタ メンバは、DCI 経由のクラスタ制御リンクによって接続されています。各データセンターの内部ルータと外部ルータは、OSPF と PBR または ECMP を使用してクラスタ メンバ間でトラフィックをロード バランスします。DCI に高コスト ルートを割り当てることにより、特定のサイトのすべての ASA クラスタ メンバがダウンしない限り、トラフィックは各データセンター内に維持されます。1 つのサイトのすべてのクラスタ メンバに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトの ASA クラスタ メンバに送られます。



スパンド EtherChannel トランスペアレント モード Inter-Site の例

次の例では、2 つのデータセンターのそれぞれに 2 つの ASA クラスタ メンバがある場合を示します。クラスタ メンバは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバは、内部および外部のスパンド EtherChannels を使用してローカル スイッチに接続します。ASA EtherChannel は、クラスタ内のすべての ASA にスパンされます。各データセンターの内部ルータと外部ルータは OSPF を使用し、トランスペアレント ASA を通過します。MAC とは異なり、ルータの IP はすべてのルータで一意です。DCI に高コスト ルートを割り当てることにより、特定のサイトのすべての ASA クラスタ メンバがダウンしない限り、トラフィックは各データセンター内に維持されます。クラスタが非対称型の接続を維持するため、ASA を通過する低コストのルートは、各サイトで同じブリッジ グループを横断する必要があります。1 つのサイトのすべてのクラスタ メンバに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトの ASA クラスタ メンバに送られます。



各サイトのスイッチの実装には、次のものを含めることができます。

- Inter-Site VSS/vPC：このシナリオでは、データセンター 1 に 1 台のスイッチをインストールし、データセンター 2 に別のスイッチをインストールします。1 つのオプションとして、各データセンターの ASA クラスタ ユニットはローカル スイッチだけに接続し、VSS/vPC トラフィックは DCI を経由します。この場合、接続のほとんどの部分は各データセンターに対してローカルに維持されます。オプションとして、DCI が余分なトラフィック量を処理できる場合、各 ASA ユニットを DCI 経由で両方のスイッチに接続できます。この場合、トラフィックは複数のデータセンターに分散されるため、DCI を非常に堅牢にするためには不可欠です。
- 各サイトのローカル VSS/vPC：スイッチの冗長性を高めるには、各サイトに 2 つの異なる VSS/vPC ペアをインストールできます。この場合、ASA は、両方のローカル スイッチだけに接続されたデータセンター 1 ASA およびこれらのローカル スイッチに接続されたデータセンター 2 ASA とはスパンド EtherChannel を使用しますが、スパンド EtherChannel は基本的に「分離」しています。各ローカル VSS/vPC は、スパンド EtherChannel をサイト ローカルの EtherChannel として認識します。

ASA クラスタが接続を管理する方法

接続をクラスタの複数のメンバにロードバランスできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

- 「接続のロール」（P.9-23）
- 「新しい接続の所有権」（P.9-23）
- 「サンプル データ フロー」（P.9-24）
- 「新しい TCP 接続のクラスタ全体での再分散」（P.9-24）

接続のロール

ASA には次の 3 種類のロールがあり、各接続に対して定義されます。

- オーナー：最初に接続を受信するユニット。オーナーは、TCP 状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。
- ディレクタ：フォワーダからのオーナー ルックアップ要求を処理するユニット。また、オーナーが停止した場合はバックアップとなり、接続の状態を保持します。オーナーが新しい接続を受信すると、オーナーは、送信元/宛先 IP アドレスおよび TCP ポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにメッセージをそのディレクタに送信します。パケットがオーナー以外のユニットに到着した場合は、そのユニットはどのユニットがオーナーかをディレクタに問い合わせます。これで、パケットを転送できるようになります。1 つの接続に対してディレクタは 1 つだけです。
- フォワーダ：パケットをオーナーに転送するユニット。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください （TCP シーケンスのランダム化をディセーブルにした場合、SYN クッキーは使用されません。ディレクタへの問い合わせが必要です）。DNS や ICMP などの存続期間が短いフローの場合は、問い合わせを行う代わりに、フォワーダはすぐにディレクタにパケットを送信し、ディレクタはそれをオーナーに送信します。1 つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが 1 つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

新しい接続の所有権

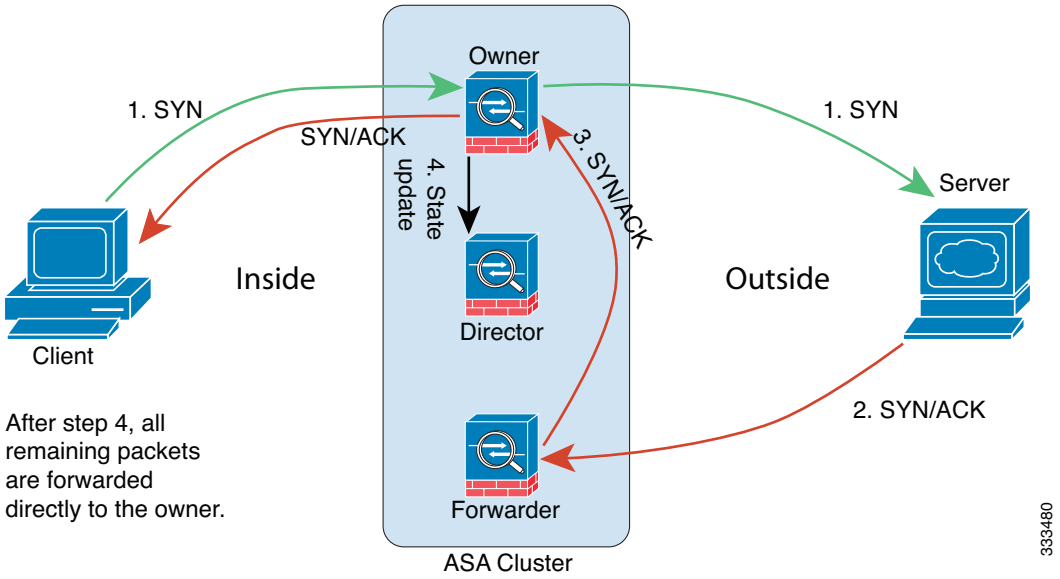
新しい接続がロード バランシング経由でクラスタのメンバに送信される場合は、そのユニットがその接続の両方向のオーナーとなります。接続のパケットが別のユニットに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナー ユニットに転送されます。最適なパフォーマンスを得るには、適切な外部ロード バランシングが必要です。1 つのフローの両方向が同じユニットに到着するとともに、フローがユニット間に均等に分散されるようにするためです。逆方向のフローが別のユニットに到着した場合は、元のユニットにリダイレクトされます。

関連項目

- 「ロード バランシングの方式」（P.9-13）

サンプル データ フロー

次の例は、新しい接続の確立を示します。



1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロード バランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP ステート情報を記録します。ディレクタは、この接続のバックアップ オーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のユニットに配信された場合は、そのユニットはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

新しい TCP 接続のクラスタ全体での再分散

アップストリームまたはダウンストリーム ルータによるロード バランシングの結果として、フロー分散に偏りが生じた場合は、新しい TCP フローを過負荷のユニットから他のユニットにリダイレクトするように設定できます。既存のフローは他のユニットには移動されません。

ASA の機能とクラスタリング

ASA の一部の機能は ASA クラスタリングではサポートされず、一部はマスター ユニットだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

これらの機能は、クラスタリングがイネーブルのときは設定できず、コマンドは拒否されます。

- ユニファイド コミュニケーション
- リモート アクセス VPN（SSL VPN および IPSec VPN）
- 次のアプリケーション インスペクション：
  - CTIQBE
  - GTP
  - H323、H225、および RAS
  - IPsec パススルー
  - MGCP
  - MMP
  - RTSP
  - SIP
  - SCCP（Skinny）
  - WAAS
  - WCCP
- Botnet Traffic Filter
- Auto Update Server
- DHCP クライアント、サーバ、リレー、およびプロキシ
- VPN ロード バランシング
- フェールオーバー
- ASA CX モジュール

クラスタリングの中央集中型機能

次の機能は、マスター ユニット上だけでサポートされます。クラスタの場合もスケーリングされません。たとえば、8 ユニット（5585-X と SSP-60）から成るクラスタがあるとします。Other VPN ライセンスでは、1 台の ASA 5585-X と SSP-60 に対して許可されるサイト間 IPSec トンネルの最大数は 10,000 です。8 ユニット クラスタ全体で使用できるトンネル数は 10,000 までです。この機能はスケーリングしません。

（注）中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバ ユニットからマスター ユニットに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、マスター以外のユニットに転送されることがあります。この場合は、トラフィックがマスター ユニットに送り返されます。

中央集中型機能については、マスター ユニットで障害が発生するとすべての接続がドロップされるので、新しいマスター ユニット上で接続を再確立する必要があります。

- サイト間 VPN
- 次のアプリケーション インスペクション：
  - DCERPC
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- ダイナミック ルーティング（スパンド EtherChannel モードのみ）
- マルチキャスト ルーティング（個別インターフェイス モードのみ）
- スタティック ルート モニタリング
- IGMP マルチキャスト コントロール プレーン プロトコル処理（データ プレーン フォワーディングはクラスタ全体に分散されます）
- PIM マルチキャスト コントロール プレーン プロトコル処理（データ プレーン フォワーディングはクラスタ全体に分散されます）
- ネットワーク アクセスの認証および許可。アカウンティングは非集中型です。
- フィルタリング サービス

関連項目

- 「クラスタ制御リンクのサイジング」（P.9-7）
- 「新しい TCP 接続のクラスタ全体での再分散」（P.9-24）

個々のユニットに適用される機能

これらの機能は、クラスタ全体またはマスター ユニットではなく、各 ASA ユニットに適用されます。

- QoS：QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは、各ユニットに対して個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て行くトラフィックに適用されます。8 ユニットから成るクラスタがあり、トラフィックが均等に分散している場合は、適合レートは実際にクラスタのレートの 8 倍になります。
- 脅威検出：脅威検出は、各ユニットに対して個別に機能します。たとえば、上位統計情報は、ユニット別です。たとえば、ポート スキャン検出が機能しないのは、スキャン トラフィックが全ユニット間で分散されるので、1 つのユニットがすべてのトラフィックを読み取ることはないからです。
- リソース管理：マルチ コンテキスト モードでのリソース管理は、ローカル使用状況に基づいて各ユニットに個別に適用されます。
- ASA FirePOWER モジュール：ASA FirePOWER モジュール間でのコンフィギュレーションの同期や状態の共有は行われません。ユーザーが FireSIGHT 管理センター を使用してクラスタの ASA FirePOWER モジュールでの一貫性のあるポリシーを維持する必要があります。クラスタ内のデバイスに異なる ASA インターフェイスベースのゾーン定義を使用しないでください。
- ASA IPS モジュール : IPS モジュール間でのコンフィギュレーションの同期や状態の共有は行われません。IPS シグニチャによっては、IPS が複数の接続にわたって状態を保持することが必要になります。たとえば、ポート スキャン シグニチャが使用されるのは、同じ人物が同じサーバへの多数の接続を、それぞれ異なるポートを使用して開いていることを IPS モジュールが検出した場合です。クラスタリングでは、これらの接続は複数の ASA デバイス間で分散されます。これらのデバイスそれぞれに専用の IPS モジュールがあります。これらの IPS モジュールはステート情報を共有しないので、結果としてのポート スキャンをクラスタが検出できない場合があります。

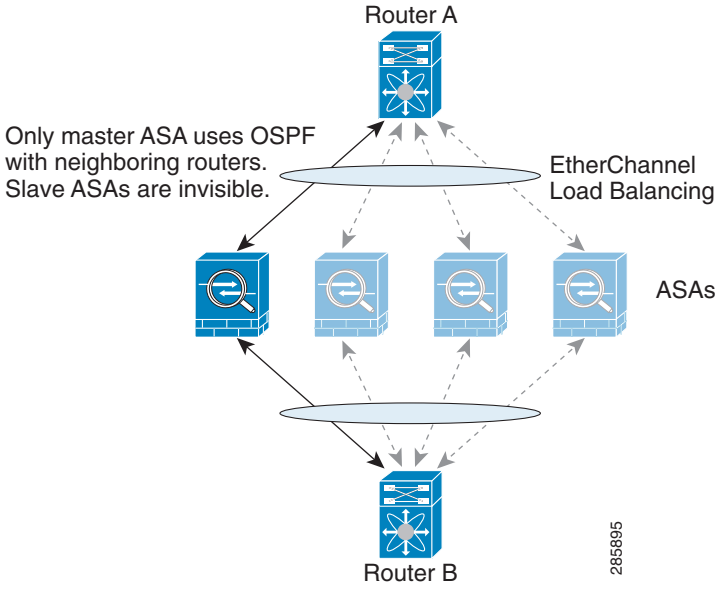
ダイナミック ルーティングおよびクラスタリング

- 「スパンド EtherChannel モードでのダイナミック ルーティング」（P.9-27）
- 「個別インターフェイス モードでのダイナミック ルーティング」（P.9-29）

スパンド EtherChannel モードでのダイナミック ルーティング

スパンド EtherChannel モードでは、ルーティング プロセスはマスター ユニット上だけで実行されます。ルートはマスター ユニットを介して学習され、スレーブに複製されます。ルーティング パケットがスレーブに到着した場合は、マスター ユニットにリダイレクトされます。

図 9-1　スパンド EtherChannel モードでのダイナミック ルーティング



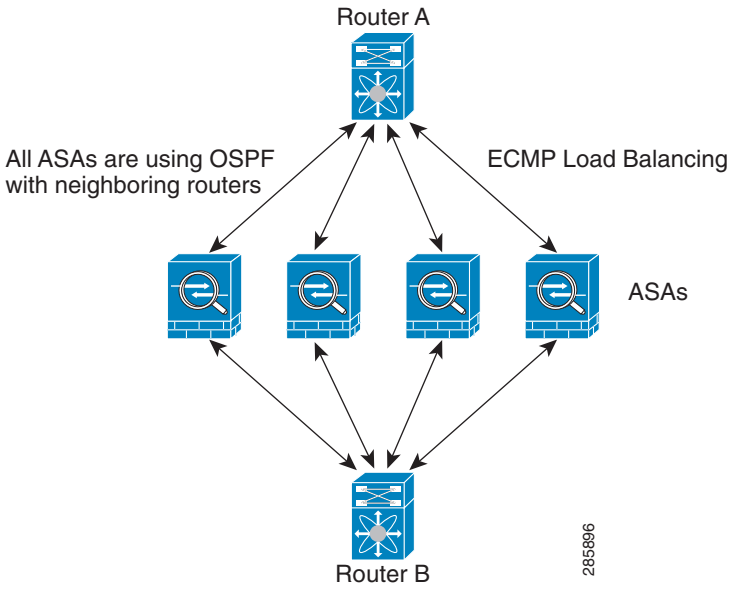
スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスター ユニットからスレーブ ユニットに同期されません。マスター ユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します 必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。

個別インターフェイス モードでのダイナミック ルーティング

個別インターフェイス モードでは、各ユニットがスタンドアロン ルータとしてルーティング プロトコルを実行します。ルートの学習は、各ユニットが個別に行います。

図 9-2　　個別インターフェイス モードでのダイナミック ルーティング



上の図では、ルータ A はルータ B への等コスト パスが 4 本あることを学習します。パスはそれぞれ 1 つの ASA を通過します。ECMP を使用して、4 パス間でトラフィックのロード バランシングを行います。各 ASA は、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ユニットが別のルータ ID を使用できるように、ルータ ID のクラスタ プールを設定する必要があります。

マルチキャスト ルーティングとクラスタリング

マルチキャスト ルーティングは、インターフェイス モードによって動作が異なります。

- 「スパンド EtherChannel モードでのマルチキャスト ルーティング」（P.9-29）
- 「個別インターフェイス モードでのマルチキャスト ルーティング」（P.9-29）

スパンド EtherChannel モードでのマルチキャスト ルーティング

スパンド EtherChannel モードでは、ファースト パス転送が確立されるまでの間、マスター ユニットがすべてのマルチキャスト ルーティング パケットとデータ パケットを処理します。接続が確立された後は、各スレーブがマルチキャスト データ パケットを転送できます。

個別インターフェイス モードでのマルチキャスト ルーティング

個別インターフェイス モードでは、マルチキャストに関してユニットが個別に動作することはありません。データおよびルーティングのパケットはすべてマスター ユニットで処理されて転送されるので、パケット レプリケーションが回避されます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。着信および発信の NAT パケットが、クラスタ内のそれぞれ別の ASA に送信されることがあります。ロード バランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用されるときは、着信と発信とで、パケットの IP アドレスやポートが異なるからです。接続のオーナーではない ASA に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるので、大量のトラフィックがクラスタ制御リンク上で発生します。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- プロキシ ARP なし：個別インターフェイスの場合は、マッピング アドレスについてプロキシ ARP 応答が送信されることはありません。これは、クラスタに存在しなくなった可能性のある ASA と隣接ルータとがピア関係を維持することを防ぐためです。アップストリーム ルータは、メイン クラスタ IP アドレスを指すマッピング アドレスについてはスタティック ルートまたは PBR とオブジェクト トラッキングを使用する必要があります。これは、スパンド EtherChannel の問題ではありません。クラスタ インターフェイスには関連付けられた IP アドレスが 1 つしかないためです。
- 個別インターフェイスのインターフェイス PAT なし：インターフェイス PAT は、個別インターフェイスではサポートされていません。
- ダイナミック PAT 用 NAT プール アドレス分散：マスター ユニットは、アドレスをクラスタ全体に均等に分配します。メンバが接続を受信したときに、そのメンバのアドレスが 1 つも残っていない場合は、接続はドロップされます（他のメンバにはまだ使用可能なアドレスがある場合でも）。最低でも、クラスタ内のユニットと同数の NAT アドレスが含まれていることを確認してください。各ユニットが確実に 1 つのアドレスを受け取るようにするためです。アドレス割り当てを表示するには、**show nat pool cluster** コマンドを使用します。
- ラウンド ロビンなし：PAT プールのラウンド ロビンは、クラスタリングではサポートされません。
- マスター ユニットによって管理されるダイナミック NAT xlate：マスター ユニットが xlate テーブルを維持し、スレーブ ユニットに複製します。ダイナミック NAT を必要とする接続をスレーブ ユニットが受信したときに、その xlate がテーブル内にない場合は、スレーブはマスター ユニットに xlate を要求します。スレーブ ユニットが接続を所有します。
- Per-session PAT 機能：クラスタリングに限りませんが、Per-session PAT 機能によって PAT のスケーラビリティが向上します。クラスタリングの場合は、各スレーブ ユニットが独自の PAT 接続を持てるようになります。対照的に、Multi-Session PAT 接続はマスター ユニットに転送する必要があり、マスター ユニットがオーナーとなります。デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-session PAT xlate を使用します。Multi-Session PAT を必要とするトラフィックについては（たとえば H.323、SIP、Skinny）、Per-Session PAT をディセーブルにできます。Per-session PAT の詳細については、ファイアウォール コンフィギュレーション ガイドを参照してください。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - すべての VoIP アプリケーション

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウンティングの 3 つのコンポーネントで構成されます。認証とアカウンティングは、クラスタリング マスター上で中央集中型機能として実装されており、データ構造がクラスタ スレーブに複製されます。マスターが選定されたときは、確立済みの認証済みユーザおよびユーザに関連付けられた許可を引き続き中断なく運用するのに必要なすべての情報を、新しいマスターが保有します。ユーザ認証のアイドルおよび絶対タイムアウトは、マスター ユニット変更が発生したときも維持されます。

アカウンティングは、クラスタ内の分散型機能として実装されています。アカウンティングはフロー単位で実行されるので、フローを所有するクラスタ ユニットがアカウンティング開始と停止のメッセージを AAA サーバに送信します（フローに対するアカウンティングが設定されているとき）。

syslog および NetFlow とクラスタリング

- syslog：クラスタの各ユニットは自身の syslog メッセージを生成します。各ユニットの syslog メッセージ ヘッダー フィールドで使用されるデバイス ID を同一にするか、別にするかを設定できます。たとえば、ホスト名コンフィギュレーションはクラスタ内のすべてのユニットに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合は、どのユニットで生成された syslog メッセージも 1 つのユニットからのように見えます。クラスタ ブートストラップ コンフィギュレーションで割り当てられたローカル ユニット名をデバイス ID として使用するようにロギングを設定した場合は、syslog メッセージはそれぞれ別のユニットからのように見えます。
- NetFlow：クラスタの各ユニットは自身の NetFlow ストリームを生成します。NetFlow コレクタは、各 ASA を独立した NetFlow エクスポータとしてのみ扱うことができます。

関連項目

- 「非 EMBLEM 形式の syslog メッセージへのデバイス ID の出力」（P.40-22）

SNMP とクラスタリング

SNMP エージェントは、個々の ASA を、そのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメイン クラスタ IP アドレスをポーリングする場合は、新しいマスターが選定されたときに、新しいマスター ユニットのポーリングに失敗します。

VPN とクラスタリング

サイトツーサイト VPN は、中央集中型機能です。マスター ユニットだけが VPN 接続をサポートします。

（注） リモート アクセス VPN は、クラスタリングではサポートされません。

VPN 機能を使用できるのはマスター ユニットだけであり、クラスタのハイ アベイラビリティ能力は活用されません。マスター ユニットで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN ユーザにとってはサービスの中断となります。新しいマスターが選定されたときに、VPN 接続を再確立する必要があります。

VPN トンネルをスパンド EtherChannel アドレスに接続すると、接続が自動的にマスター ユニットに転送されます。PBR または ECMP を使用するときの個別インターフェイスへの接続については、ローカル アドレスではなく、常にメイン クラスタ IP アドレスに接続する必要があります。

VPN 関連のキーと証明書は、すべてのユニットに複製されます。

FTP とクラスタリング

- FTP データ チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバによって所有されている場合は、データ チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。
- FTP アクセスに AAA を使用している場合、制御チャネルのフローはマスター ユニットに集中化されます。

Cisco TrustSec とクラスタリング

マスター ユニットだけがセキュリティ グループ タグ（SGT）情報を学習します。マスター ユニットからこの SGT がスレーブに渡されるので、スレーブは、セキュリティ ポリシーに基づいて SGT の一致の決定を行うことができます。

ASA クラスタリングのライセンス

モデル	ライセンス要件
ASA 5585-X	クラスタ ライセンス、最大 16 ユニットをサポートします。 各ユニット上にクラスタ ライセンスが必要です。その他の機能ライセンスについては、各クラスタ ユニットのライセンスが同一でなくてもかまいません。複数のユニットに機能ライセンスがある場合は、これらが結合されて単一の実行 ASA クラスタ ライセンスとなります。 **（注）**　各ユニットに、同じ暗号化ライセンスおよび同じ 10 GE I/O ライセンスが必要です。
ASA 5512-X	Security Plus ライセンス、2 ユニットをサポートします。 **（注）**　各ユニットに同じ暗号化ライセンスが必要です。
ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X	基本ライセンス、2 ユニットをサポートします。 **（注）**　各ユニットに同じ暗号化ライセンスが必要です。
他のすべてのモデル	サポートしない

ASA クラスタリングの前提条件

ASA のハードウェアおよびソフトウェア要件

クラスタ内のすべてのユニット：

- 同じ DRAM を使用する同じモデルである必要があります。フラッシュ メモリの容量は同一である必要はありません。
- イメージ アップグレード時を除き、同じソフトウェアを実行する必要があります。ヒットレス アップグレードがサポートされます。
- 個別インターフェイス モードを使用すると、クラスタ メンバを異なる地理的な場所（サイト間）に配置できます。
- セキュリティ コンテキスト モードが一致している必要があります（シングルまたはマルチ）。
- （シングル コンテキスト モード）ファイアウォール モードが一致している必要があります（ルーテッドまたはトランスペアレント）。
- コンフィギュレーション複製前の初期クラスタ制御リンク通信のために、新しいクラスタ メンバは、マスター ユニットと同じ SSL 暗号化設定（**ssl encryption** コマンド）を使用する必要があります。
- 同じクラスタ ライセンス、暗号化ライセンス、そして ASA 5585-X の場合は 10 GE I/O ライセンスが必要です。

スイッチの前提条件

- ASA でクラスタリングを設定する前に、スイッチのコンフィギュレーションを完了する必要があります。
- 次の表は、ASA クラスタリングとの相互運用がサポートされる外部ハードウェアおよびソフトウェアの一覧です。

表 9-2　ASA クラスタリングに関する外部ハードウェアおよびソフトウェアのサポート

外部ハードウェア	外部ソフトウェア	ASA のバージョン
Cisco Nexus 9300	Cisco NX-OS 6.1(2)I2(1) 以降	9.2(1) 以降
Cisco Nexus 7000	Cisco NX-OS 5.2(5) 以降	9.0(1) 以降
Cisco Nexus 5000	Cisco NX-OS 7.0(1) 以降	9.1(4) 以降
Catalyst 6500 と Supervisor 32、720、および 720-10GE	Cisco IOS 12.2(33)SXI7、SXI8、SXI9 以降	9.0(1) 以降
Catalyst 3750-X	Cisco IOS 15.0(2) 以降	9.1(4) 以降

ASA の必須条件

- ユニットを管理ネットワークに追加する前に、一意の IP アドレスを各ユニットに提供します。
  - ASA への接続および管理 IP アドレスの設定に関する詳細については、「使用する前に」の章を参照してください。
  - マスター装置（通常は最初にクラスタに追加された装置）で使用される IP アドレスを除き、これらの管理 IP アドレスは一時的に使用されるだけです。
  - スレーブがクラスタに参加すると、管理インターフェイス設定はマスター装置からの複製に置き換えられます。

- クラスタ制御リンクでジャンボ フレームを使用する場合は（推奨）、クラスタリングをイネーブルにする前に、ジャンボ フレームの予約をイネーブルにする必要があります。

その他の前提条件

ターミナル サーバを使用して、すべてのクラスタ メンバ ユニットのコンソール ポートにアクセスすることをお勧めします。初期設定および継続的な管理（ユニットがダウンしたときなど）では、ターミナル サーバがリモート管理に役立ちます。

関連項目

- 「ASA クラスタリングのガイドライン」（P.9-34）
- 「ジャンボ フレーム サポートのイネーブル化」（P.10-31）
- 「ブートストラップ コンフィギュレーション」（P.9-3）

ASA クラスタリングのガイドライン

コンテキスト モード

各メンバ ユニットのモードが一致する必要があります。

ファイアウォール モード

シングル モードの場合、ファイアウォール モードがすべてのユニットで一致している必要があります。

フェールオーバー

フェールオーバーは、クラスタリングを行うときはサポートされません。

IPv6

クラスタ制御リンクは、IPv4 のみを使用してサポートされます。

モデル

以下でサポートされます。

- ASA 5585-X

  ASA 5585-X と SSP-10 および SSP-20（2 個の 10 ギガビット イーサネット インターフェイスを持つ）については、一方のインターフェイスをクラスタ制御リンクに使用し、他方をデータに使用することを推奨します（データについてはサブインターフェイスを使用できます）。この設定は、クラスタ制御リンクの冗長性には対応しませんが、クラスタ制御リンクのサイズをデータ インターフェイスのサイズと一致させるという要件は満たされます。

- ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X

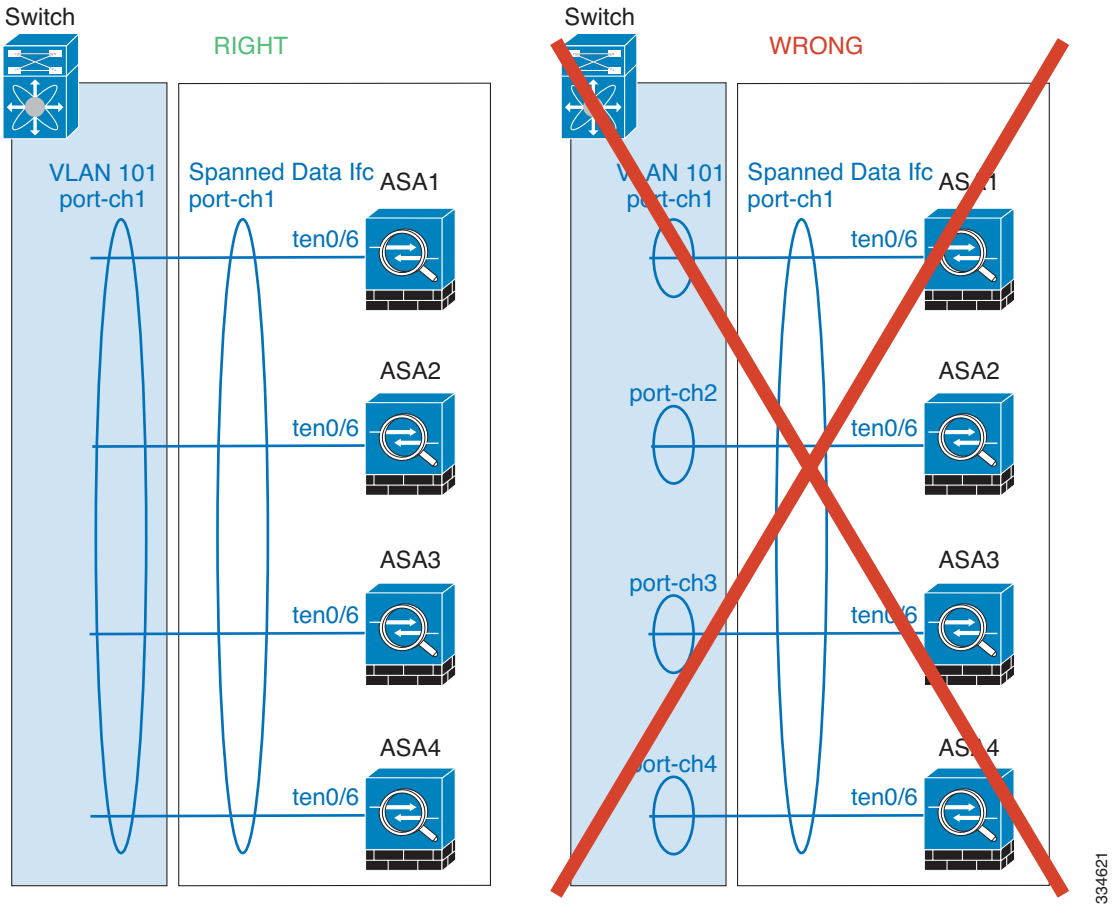
スイッチ

- クラスタ制御リンク インターフェイスのスイッチでは、ASA に接続されるスイッチ ポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。

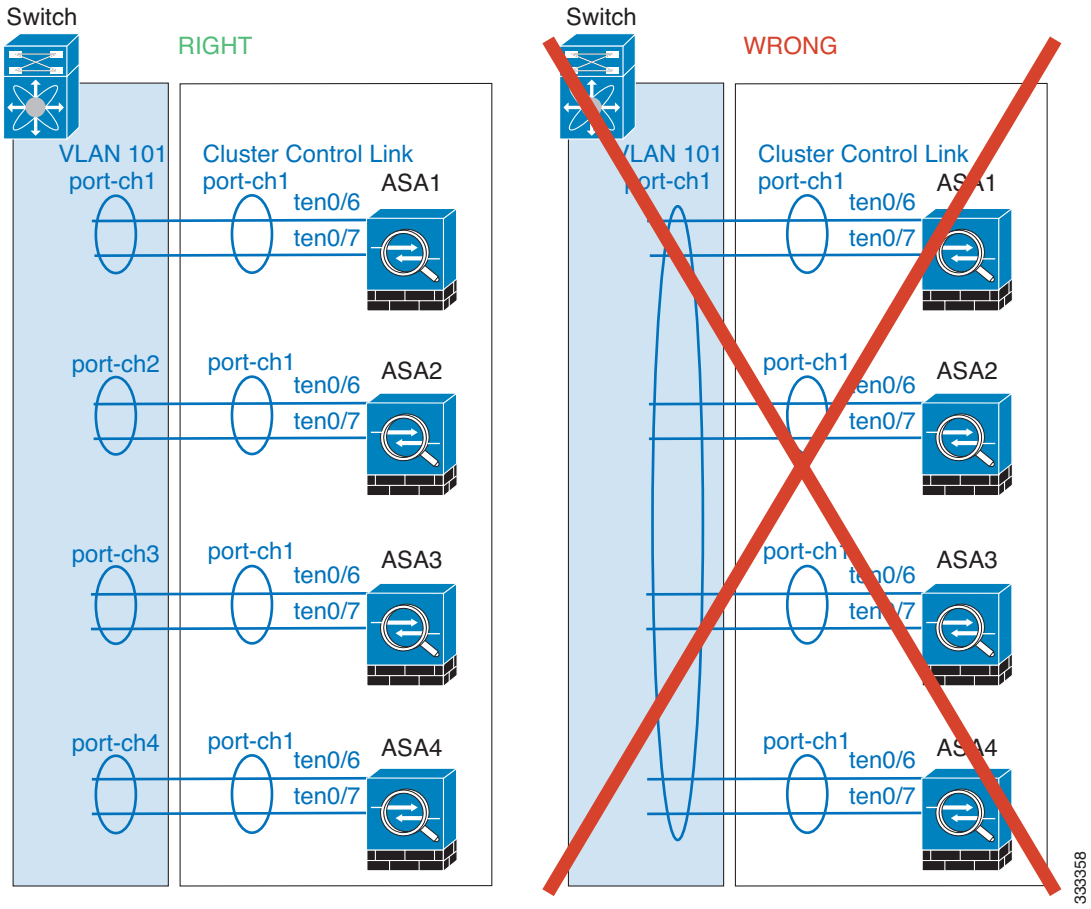
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタ内の ASA へのトラフィックが均等に分散されなくなることがあるため、ロードバランシング アルゴリズムでは、**vlan** キーワードを使用しないでください。ASA のデフォルトのロードバランシング アルゴリズムを変更しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリー プロトコルが再起動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- Cisco Nexus スイッチのクラスタに接続されたすべての EtherChannel インターフェイスで、LACP グレースフル コンバージェンス機能をディセーブルにする必要があります。
- 一部のスイッチは、LACP でのダイナミック ポート プライオリティをサポートしていません（アクティブおよびスタンバイ リンク）。ダイナミック ポート プライオリティをディセーブルにすることで、スパンド EtherChannel との互換性を高めることができます。
- クラスタ制御リンク パスのネットワーク エレメントでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。

EtherChannel

- ASA は、スイッチ スタックへの EtherChannel の接続をサポートしていません。ASA EtherChannel がクロス スタックに接続されている場合、マスター スイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。
- スパンド EtherChannel と デバイス ローカル EtherChannel のコンフィギュレーション：スイッチをスパンド EtherChannel または デバイス ローカル EtherChannel に合わせて適切に設定します。
  - スパンド EtherChannel：ASA *スパンド* EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャネル グループ内にあることを確認してください。



– デバイス ローカル EtherChannel：ASA *デバイス ローカル* EtherChannel（クラスタ制御リンク用に設定された EtherChannel もこれに含まれます）は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数の ASA EtherChannel を結合して 1 つの EtherChannel としないでください。



その他のガイドライン

- 重要なトポロジ変更を行うとき（たとえば、EtherChannel インターフェイスの追加または削除、ASA またはスイッチ上のインターフェイスのイネーブル化またはディセーブル化、VSS または vPC を形成するスイッチの追加）は、ヘルス チェック機能をディセーブルにしてください。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。
- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel に接続された Windows 2003 Server を使用している場合、syslog サーバ ポートがダウンし、サーバが ICMP エラー メッセージを調整しないと、多数の ICMP メッセージが ASA クラスタに送信されます。このようなメッセージにより、ASA クラスタの一部のユニットで高い CPU 使用率が発生してパフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。

関連項目

- 「クラスタ制御リンクのサイジング」（P.9-7）
- 「ブートストラップ コンフィギュレーション」（P.9-3）

- 「クラスタリングでサポートされない機能」（P.9-25）
- 「EtherChannel の設定」（P.10-22）
- 「EtherChannel のガイドライン」（P.10-12）

ASA クラスタリングのデフォルト

- スパンド EtherChannel を使用するときは、cLACP システム ID は自動生成され、システム プライオリティはデフォルトで 1 です。
- クラスタのヘルス チェック機能は、デフォルトでイネーブルになり、ホールド時間は 3 秒です。
- 接続再分散は、デフォルトではディセーブルです。接続再分散をイネーブルにした場合の、デフォルトの負荷情報交換間隔は 5 秒です。

ASA クラスタリングの設定

（注）　クラスタリングをイネーブルまたはディセーブルにするには、コンソール接続（CLI の場合）または ASDM 接続を使用します。

クラスタリングを設定するには、次のタスクを実行します。

ステップ 1　「ASA クラスタリングの前提条件」（P.9-33）および「ASA クラスタリングのガイドライン」（P.9-34）に従って、スイッチと ASA に対するすべての事前設定を完了します。

ステップ 2　「クラスタ ユニットのケーブル接続とアップストリームおよびダウンストリーム機器の設定」（P.9-39）

ステップ 3　「コンフィギュレーションのバックアップ（推奨）」（P.9-40）

ステップ 4　「マスター ユニットでのクラスタ インターフェイス モードの設定」（P.9-41）クラスタリングに対して設定できるインターフェイスのタイプは、スパンド EtherChannel と個別インターフェイスのうち 1 つのみです。

ステップ 5　「（推奨、マルチ コンテキスト モードでは必須）マスター ユニットでのインターフェイスの設定」（P.9-44）インターフェイスがクラスタ対応でない場合は、クラスタリングをイネーブルにできません。シングル コンテキスト モードでは、High Availability and Scalability ウィザードで代わりに多くのインターフェイス設定を構成できますが、すべてのインターフェイス オプションをウィザードで使用できるわけではなく、ウィザードのマルチ コンテキスト モードではインターフェイスを設定できません。

ステップ 6　「ASA クラスタの作成または ASA クラスタへの参加」（P.9-50）

ステップ 7　セキュリティ ポリシーをマスター ユニット上で設定します。サポートされる機能をマスター ユニット上で設定するには、このマニュアルの該当する章を参照してください。コンフィギュレーションはスレーブ ユニットに複製されます。

クラスタ ユニットのケーブル接続とアップストリームおよびダウンストリーム機器の設定

クラスタリングを設定する前に、クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。

（注）　クラスタに参加するようにユニットを設定する前に、少なくとも、アクティブなクラスタ制御リンク ネットワークが必要です。

アップストリームとダウンストリームの機器も設定する必要があります。たとえば、EtherChannel を使用する場合は、EtherChannel のアップストリーム/ダウンストリーム機器を設定する必要があります。

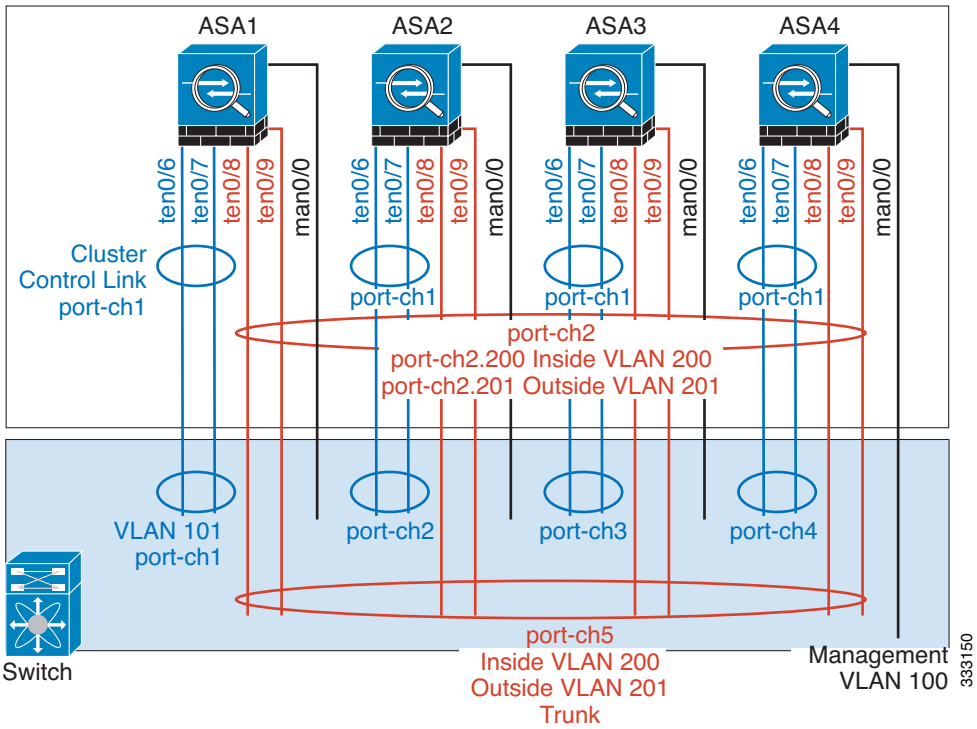
例

（注）　この例では、ロードバランシングに EtherChannel を使用します。PBR または ECMP を使用する場合は、スイッチ コンフィギュレーションが異なります。

たとえば、4 台の ASA 5585-X のそれぞれにおいて、次のものを使用します。

- デバイス ローカル EtherChannel の 10 ギガビット イーサネット インターフェイス 2 個（クラスタ制御リンク用）。
- スパンド EtherChannel の 10 ギガビット イーサネット インターフェイス 2 個（内部および外部ネットワーク用）。各インターフェイスは、EtherChannel の VLAN サブインターフェイスです。サブインターフェイスを使用すると、内部と外部の両方のインターフェイスが EtherChannel の利点を活用できます。
- 管理インターフェイス 1 個。

内部と外部の両方のネットワーク用に 1 台のスイッチがあります。



目的	4 台の各 ASA の接続インターフェイス	スイッチ ポートへ
クラスタ制御リンク	TenGigabitEthernet 0/6 および TenGigabitEthernet 0/7	合計 8 ポート TenGigabitEthernet 0/6 と TenGigabitEthernet 0/7 のペアごとに、4 個の EtherChannel（ASA ごとに 1 個の EC）を設定します。 これらの EtherChannel すべてが、同一の独立クラスタ制御 VLAN 上（たとえば VLAN 101）に存在する必要があります。
内部および外部インターフェイス	TenGigabitEthernet 0/8 および TenGigabitEthernet 0/9	合計 8 ポート 単一の EtherChannel を設定します（すべての ASA にまたがる）。 スイッチでは、この VLAN およびネットワークをここで設定できます。たとえば、VLAN 200（内部用）および VLAN 201（外部用）が含まれるトランクを設定します。
管理インターフェイス	Management 0/0	合計 4 ポート すべてのインターフェイスを、同一の独立管理 VLAN（たとえば VLAN 100）上に置きます。

コンフィギュレーションのバックアップ（推奨）

スレーブ ユニットでクラスタリングをイネーブルにすると、現在のコンフィギュレーションは同期したマスター ユニットの設定に置き換えられます。クラスタ全体を解除する場合、使用可能な管理インターフェイス コンフィギュレーションのバックアップ コンフィギュレーションを取っておくと役立つ場合があります。

はじめる前に

各ユニットのバックアップを実行します。

手順

ステップ 1　[Tools] > [Backup Configurations] を選択します。

ステップ 2　最低でも実行コンフィギュレーションをバックアップします。詳細な手順については、「ローカル CA サーバのバックアップ」（P.37-26）を参照してください。

関連項目

- 「クラスタからの脱退」（P.9-60）

マスター ユニットでのクラスタ インターフェイス モードの設定

クラスタリング用に設定できるインターフェイスのタイプは、スパンド EtherChannel と個別インターフェイスのいずれか一方のみです。1 つのクラスタ内でインターフェイス タイプを混在させることはできません。

（注）マスター ユニットからスレーブ ユニットを追加しない場合は、マスター ユニットだけでなく全ユニットのインターフェイス モードをこの項の説明に従って手動で設定する必要があります。マスター ユニットからスレーブ ユニットを追加する場合は、ASDM がスレーブ ユニットのインターフェイス モードを自動的に設定します。

はじめる前に

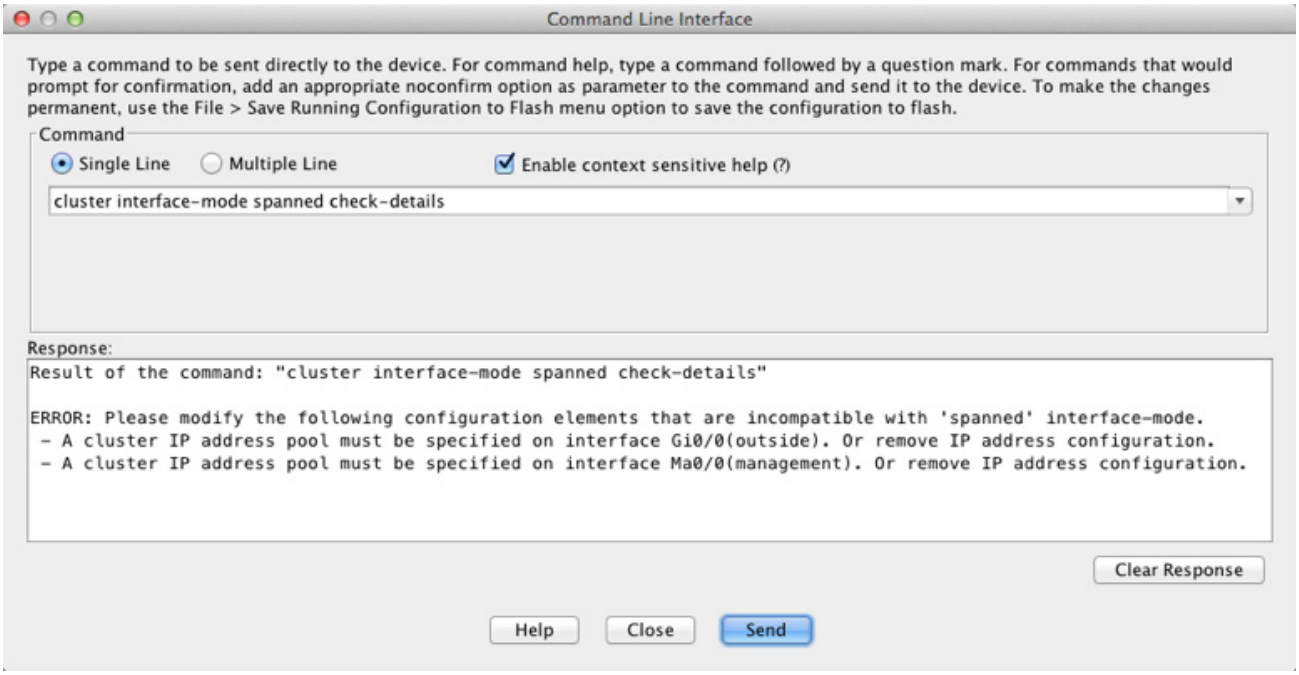
- 管理専用インターフェイスはいつでも、個別インターフェイス（推奨）として設定できます（スパンド EtherChannel モードのときでも）。管理インターフェイスは、個別インターフェイスとすることができます（トランスペアレント ファイアウォール モードのときでも）。
- スパンド EtherChannel モードでは、管理インターフェイスを個別インターフェイスとして設定すると、管理インターフェイスに対してダイナミック ルーティングをイネーブルにできません。スタティック ルートを使用する必要があります。
- マルチ コンテキスト モードでは、すべてのコンテキストに対して 1 つのインターフェイス タイプを選択する必要があります。たとえば、トランスペアレント モードとルーテッド モードのコンテキストが混在している場合は、すべてのコンテキストにスパンド EtherChannel モードを使用する必要があります。これが、トランスペアレント モードで許可される唯一のインターフェイス タイプであるからです。

手順

ステップ 1　マスター ユニットの ASDM で、[Tools] > [Command Line Interface] の順に選択します。互換性のないコンフィギュレーションを表示し、強制的にインターフェイス モードにして後でコンフィギュレーションを修正できるようにします。このコマンドではモードは変更されません。

```
cluster interface-mode {individual | spanned} check-details
```

例：

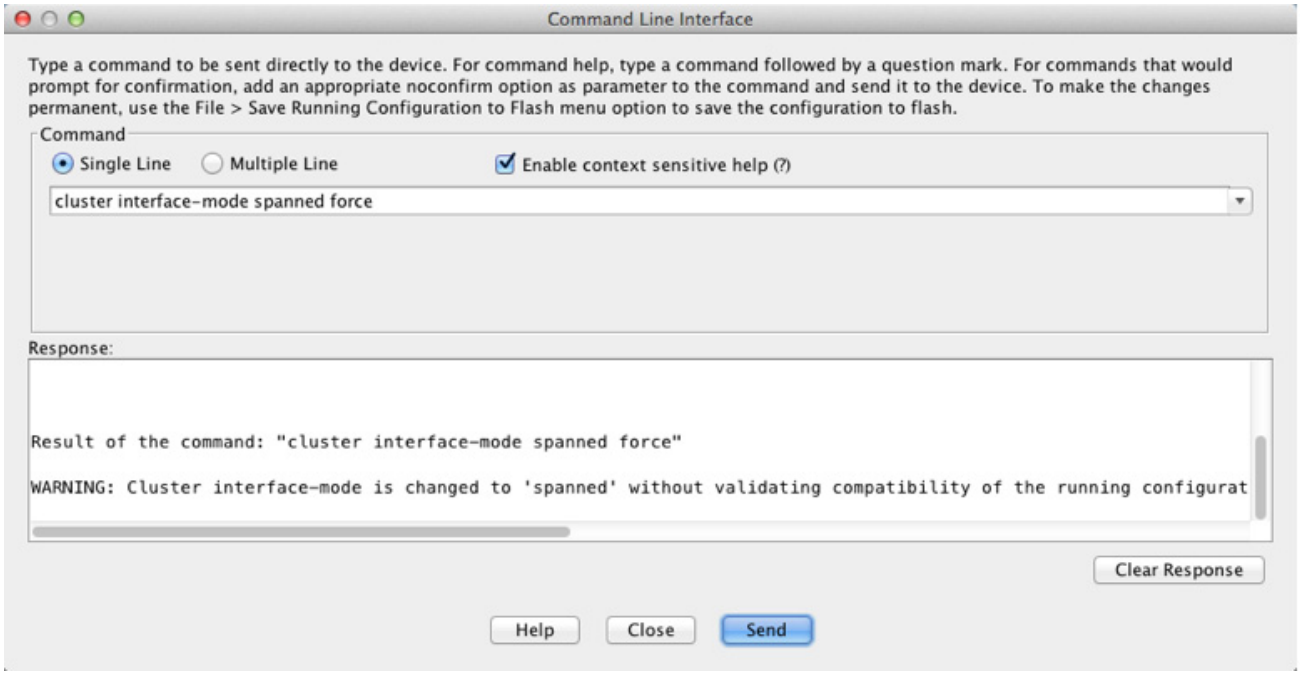


注意　インターフェイス モードを設定した後は、続けてインターフェイスに接続できます。ただし、クラスタリング要件に適合するように管理インターフェイスを設定する前に、ASA をリロードする場合は（たとえば、クラスタ IP プールの追加）、クラスタと互換性のないインターフェイス コンフィギュレーションが削除されるため、再接続できなくなります。その場合は、コンソール ポートに接続してインターフェイス コンフィギュレーションを修正する必要があります。

ステップ 2　クラスタリング用にインターフェイス モードを設定します。

```
cluster interface-mode {individual | spanned} force
```

例：



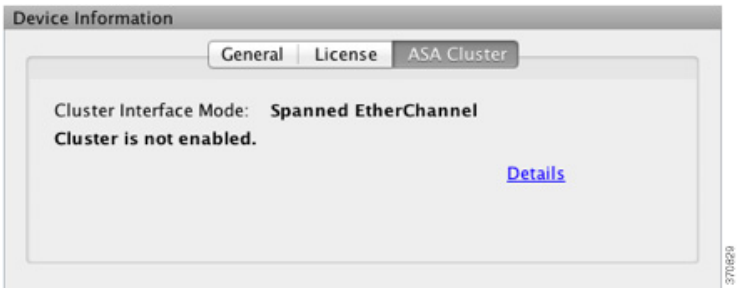
デフォルト設定はありません。明示的にモードを選択する必要があります。モードを設定していない場合は、クラスタリングをイネーブルにできません。

force オプションを指定すると、互換性のないコンフィギュレーションの検査は行わずにモードが変更されます。コンフィギュレーションの問題がある場合は、モードを変更した後に手動で解決する必要があります。インターフェイス コンフィギュレーションの修正ができるのはモードの設定後に限られるので、**force** オプションを使用することを推奨します。このようにすれば、最低でも、既存のコンフィギュレーションの状態から開始できます。さらにガイダンスが必要な場合は、モードを設定した後で **check-details** オプションを再実行します。

force オプションを指定しないと、互換性のないコンフィギュレーションがある場合は、コンフィギュレーションをクリアしてリロードするように求められるので、コンソール ポートに接続して管理アクセスを再設定する必要があります。コンフィギュレーションに互換性の問題がない場合は（まれなケース）、モードが変更され、コンフィギュレーションは維持されます。コンフィギュレーションをクリアしたくない場合は、**n** を入力してコマンドを終了します。

インターフェイス モードを解除するには、**no cluster interface-mode** コマンドを入力します。

ステップ 3　ASDM を終了し、リロードします。クラスタ インターフェイス モードに正しく対応するように ASDM を再起動する必要があります。リロードの後、ホーム ページに [ASA Cluster] タブが表示されます。



関連項目

- 「（推奨、マルチ コンテキスト モードでは必須）マスター ユニットでのインターフェイスの設定」（P.9-44）

（推奨、マルチ コンテキスト モードでは必須）マスター ユニットでのインターフェイスの設定

クラスタリングをイネーブルにする*前*に、現在 IP アドレスが設定されているインターフェイスをクラスタ対応に変更する必要があります。少なくとも、ASDM が現在接続されている管理インターフェイスを変更する必要があります。他のインターフェイスについては、クラスタリングをイネーブルにする前またはした後で設定できます。完全なコンフィギュレーションが新しいクラスタ メンバと同期するように、すべてのインターフェイスを事前に設定することを推奨します。マルチ コンテキスト モードでは、この項の手順を使用して、既存のインターフェイスを修正するか、新しいインターフェイスを設定する必要があります。一方、シングル モードでは、この項を省略し、High Availability and Scalability ウィザードで共通インターフェイス パラメータを設定できます（「ASA クラスタの作成または ASA クラスタへの参加」（P.9-50）を参照）。個別インターフェイス用の EtherChannel の作成などの高度なインターフェイス設定はウィザードでは実行できないことに注意してください。

ここでは、クラスタリング互換となるようにインターフェイスを設定する方法について説明します。データ インターフェイスは、スパンド EtherChannel として設定することも、個別インターフェイスとして設定することもできます。各方式は別のロードバランシング メカニズムを使用します。同じコンフィギュレーションで両方のタイプを設定することはできません。ただし、管理インターフェイスは例外で、スパンド EtherChannel モードであっても個別インターフェイスにできます。

- 「個別インターフェイスの設定（管理インターフェイスの場合に推奨）」（P.9-44）
- 「スパンド EtherChannel の設定」（P.9-47）

関連項目

- 「クラスタ インターフェイス」（P.9-4）

個別インターフェイスの設定（管理インターフェイスの場合に推奨）

個別インターフェイスは通常のルーテッド インターフェイスであり、それぞれが専用の IP アドレスを IP アドレス プールから取得します。メイン クラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在のマスター ユニットに属します。

スパンド EtherChannel モードでは、管理インターフェイスを個別インターフェイスとして設定することを推奨します。個別管理インターフェイスならば、必要に応じて各ユニットに直接接続できますが、スパンド EtherChannel インターフェイスでは、現在のマスター ユニットへの接続しかできません。

はじめる前に

- 管理専用インターフェイスの場合を除き、個別インターフェイス モードであることが必要です。
- マルチ コンテキスト モードの場合は、この手順を各コンテキストで実行します。まだコンテキスト コンフィギュレーション モードに入っていない場合は、[Configuration] > [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。

- 個別インターフェイスの場合は、ネイバー デバイスでのロード バランシングを設定する必要があります。管理インターフェイスには、外部のロード バランシングは必要ありません。
- （オプション）インターフェイスをデバイス ローカル EtherChannel インターフェイスとして設定する、冗長インターフェイスを設定する、およびサブインターフェイスを設定する作業を必要に応じて行います。
  - EtherChannel の場合、この EtherChannel はユニットに対してローカルであり、スパンド EtherChannel ではありません。
  - 管理専用インターフェイスを冗長インターフェイスにすることはできません。
- ASDM を使用して管理インターフェイスにリモートに接続している場合は、将来のスレーブ ユニットの現在の IP アドレスは一時的なものです。
  - 各メンバには、マスター ユニットで定義されたクラスタ IP プールから IP アドレスが割り当てられます。
  - クラスタ IP プールには、将来のスレーブの IP アドレスを含む、ネットワークですでに使用中のアドレスを含めることはできません。

    次に例を示します。

    a. マスター ユニットに 10.1.1.1 を設定します。

    b. 他のユニットには、10.1.1.2、10.1.1.3、10.1.1.4 を使用します。

    c. マスター ユニットのクラスタの IP プールを設定する場合、使用中であるために .2、.3、.4 のアドレスをプールに含めることはできません。

    d. 代わりに、.5、.6、.7、.8 のような、ネットワークの他の IP アドレスを使用する必要があります。

    （注） プールには、マスター ユニットを含むクラスタのメンバ数分のアドレスが必要です。元の .1 アドレスはメイン クラスタ IP アドレスであり、現在のマスター ユニットのものです。

    e. クラスタに参加すると古い一時的なアドレスは放棄され、他の場所で使用できます。

手順

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　インターフェイス行を選択して、[Edit] をクリックします。インターフェイスのパラメータを設定します。次のガイドラインを参照してください。

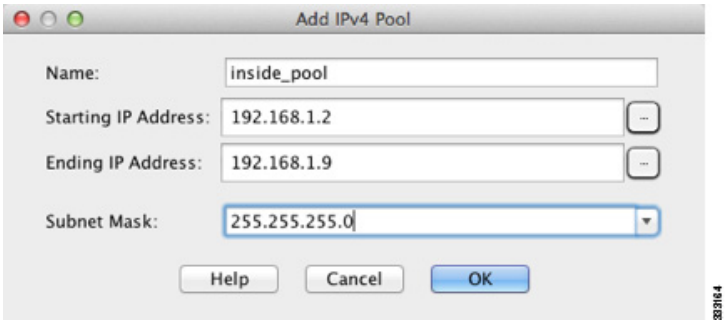
- （スパンド EtherChannel モードの管理インターフェイスでは必須）[Dedicate this interface to management only]：インターフェイスを管理専用モードに設定してトラフィックが通過しないようにします。デフォルトでは、管理タイプのインターフェイスは管理専用として設定されます。トランスペアレント モードでは、このコマンドは管理タイプのインターフェイスに対して常にイネーブルになります。
- [Use Static IP]：DHCP と PPPoE はサポートされません。

ステップ 3　IPv4 クラスタ IP プールの追加、および任意での MAC アドレス プールの追加には、[Advanced] タブをクリックします。

a. [ASA Cluster] 領域で、[IP Address Pool] フィールドの横にある [...] ボタンをクリックしてクラスタ IP プールを作成します。表示される有効範囲は、[General] タブで設定するメイン IP アドレスにより決定します。

b. [Add] をクリックします。

c. メイン クラスタの IP アドレスを含まないアドレス範囲を設定します。ネットワーク内で現在使用されているアドレスも含みません。範囲は、たとえば 8 アドレスというように、クラスタのサイズに合わせて十分に大きくする必要があります。



d. [OK] をクリックして、新しいプールを作成します。

e. 作成した新しいプールを選択して、[Assign] をクリックし、次に [OK] をクリックします。

プール名が [IP Address Pool] フィールドに表示されます。

ステップ 4　IPv6 アドレスを設定するには、[IPv6] タブをクリックします。

a. [Enable IPv6] チェックボックスをオンにします。

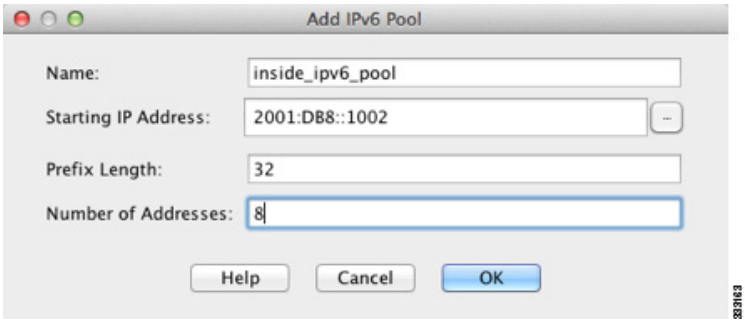
b. [Interface IPv6 Addresses] エリアで、[Add] をクリックします。

[Enable address autoconfiguration] オプションはサポートされません。

[Add IPv6 Address for Interface] ダイアログボックスが表示されます。

c. [Address/Prefix Length] フィールドに、グローバル IPv6 アドレスと IPv6 プレフィックスの長さを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。[**...**] ボタンをクリックして、クラスタ IP プールを設定します。

d. [Add] をクリックします。



e. プールの開始 IP アドレス（ネットワーク プレフィックス）、プレフィックス長、アドレス数を設定します。

f. [OK] をクリックして、新しいプールを作成します。

g. 作成した新しいプールを選択して、[Assign] をクリックし、次に [OK] をクリックします。

[ASA Cluster IP Pool] フィールドにプールが表示されます。

h. [OK] をクリックします。

ステップ 5　[OK] をクリックして、[Interfaces] ペインに戻ります。

ステップ 6　[Apply] をクリックします。

関連項目

- 「管理インターフェイス」（P.9-12）
- 「マスター ユニットでのクラスタ インターフェイス モードの設定」（P.9-41）
- 「ロード バランシングの方式」（P.9-13）
- 「EtherChannel の設定」（P.10-22）
- 「冗長インターフェイスの設定」（P.10-18）
- 「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.10-28）

スパンド EtherChannel の設定

スパンド EtherChannel は、クラスタ内のすべての ASA に広がるものであり、EtherChannel の動作の一部としてロード バランシングを行うことができます。

はじめる前に

- スパンド EtherChannel インターフェイス モードにする必要があります。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで開始します。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は、[Configuration] > [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。
- トランスペアレント モードの場合は、ブリッジ グループを設定します。
- EtherChannel の最大および最小のリンク数を指定*しないでください*。EtherChannel の最大および最小のリンク数の指定は、ASA とスイッチのどちらにおいても行わないことを推奨します。これらを使用する必要がある場合は、次の点に注意してください。
  - ASA 上で設定されるリンクの最大数は、クラスタ全体のアクティブ ポートの合計数です。スイッチ上で設定された最大リンク数の値が、ASA での値を超えていないことを確認してください。
  - ASA 上で設定される最小リンク数は、ポートチャネル インターフェイスを起動するための最小アクティブ ポート数（*ユニットあたり*）です。スイッチ上では、最小リンク数はクラスタ全体の最小リンク数であるため、この値は ASA での値とは一致しません。
- デフォルトのロードバランシング アルゴリズムを変更*しないでください*。スイッチでは、アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタ内の ASA へのトラフィックが均等に分散されなくなることがあるため、ロードバランシング アルゴリズムでは、**vlan** キーワードを使用しないでください。
- スパンド EtherChannel を使用している場合、クラスタリングが完全にイネーブルになるまで、ポートチャネル インターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

手順

ステップ 1　コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

ステップ 2　[Add] > [EtherChannel Interface] を選択します。

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

ステップ 3　次をイネーブルにします。

- **Port Channel ID**
- **Span EtherChannel across the ASA cluster**
- **Enable Interface**（デフォルトでオンになります）
- [Members in Group]：[Members in Group] リストに、インターフェイスを少なくとも 1 つ追加する必要があります。ユニットごとに複数のインターフェイスが EtherChannel に含まれていると、VSS または vPC のスイッチに接続する場合に役立ちます。デフォルトでは、クラスタの全メンバで最大 16 個のアクティブ インターフェイスのうち、スパンド EtherChannel が使用できるのは 8 個だけであることに注意してください。残りの 8 インターフェイスはリンク障害時のためのスタンバイです。8 個より多くのアクティブ インターフェイスを使用するには（ただしスタンバイ インターフェイスではなく）、ダイナミック ポート プライオリティをディセーブルにします。ダイナミック ポート プライオリティをディセーブルにすると、クラスタ全体で最大 32 個のアクティブ リンクを使用できます。たとえば、16 台の ASA から成るクラスタの場合は、各 ASA で最大 2 個のインターフェイスを使用でき、スパンド EtherChannel の合計は 32 インターフェイスとなります。

  すべてのインターフェイスが同じタイプと速度であるようにします。最初に追加するインターフェイスによって、EtherChannel のタイプと速度が決まります。一致しないインターフェイスを追加すると、そのインターフェイスは停止状態になります。ASDM では、一致しないインターフェイスの追加は防止されません。

この画面の残りのフィールドは、この手順の後半で説明します。

ステップ 4　（オプション）すべてのメンバー インターフェイスについて、メディア タイプ、二重通信、速度、フロー制御のポーズ フレームを上書きするには、[Configure Hardware Properties] をクリックします。これらのパラメータはチャネル グループのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。

[OK] をクリックして [Hardware Properties] の変更を受け入れます。

ステップ 5　MAC アドレスおよびオプション パラメータを設定するには、[Advanced] タブをクリックします。

- [MAC Address Cloning] 領域で、EtherChannel の手動 MAC アドレスを設定します。スタンバイ MAC アドレスを設定しないでください。無視されます。スパンド EtherChannel の MAC アドレスを設定する必要があります。現在のマスター ユニットがクラスタから脱退しても MAC アドレスが変更されないようにするためです。MAC アドレスが手動設定されている場合は、その MAC アドレスは現在のマスター ユニットに留まります。

  マルチ コンテキスト モードでは、インターフェイスをコンテキスト間で共有する場合に、MAC アドレスの自動生成がデフォルトでイネーブルになっています。したがって、共有インターフェイスの MAC アドレスを手動で設定する必要があるのは、自動生成をディセーブルにした場合だけです。非共有インターフェイスについては MAC アドレスを手動で設定する必要があることに注意してください。自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

- （オプション）VSS または vPC の 2 台のスイッチに ASA を接続する場合は、[Enable load balancing between switch pairs in VSS or vPC mode] チェックボックスをオンにして、VSS ロード バランシングをイネーブルにする必要があります。この機能を使用すると、ASA と VSS（または vPC）ペアとの間の物理リンク接続の負荷が確実に分散されます。

  [Member Interface Configuration] 領域で、**1** または **2** のどちらのスイッチに特定のインターフェイスを接続するかを特定する必要があります。

（注）　[Minimum Active Members] と [Maximum Active Members] は設定*しない*ことを推奨します。

ステップ 6　（オプション）この EtherChannel に VLAN サブインターフェイスを設定します。この手順の残りの部分は、サブインターフェイスに適用されます。

ステップ 7　（マルチ コンテキスト モード）この手順を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。

a. [OK] をクリックして変更内容を確定します。

b. インターフェイスを割り当てます。

c. ユーザが設定するコンテキストを変更します。[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。

d. [Configuration] > [Device Setup] > [Interfaces] ペインを選択し、カスタマイズするポートチャネル インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。

ステップ 8　[General] タブをクリックします。

ステップ 9　（トランスペアレント モード）[Bridge Group] ドロップダウン リストから、このインターフェイスを割り当てるブリッジ グループを選択します。

ステップ 10　[Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 11　[Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

ステップ 12　（ルーテッド モード）IPv4 アドレスに対して [Use Static IP] オプション ボタンをクリックし、IP およびマスクを入力します。DHCP と PPPoE はサポートされません。トランスペアレント モードの場合は、EtherChannel インターフェイスではなく、ブリッジ グループ インターフェイスの IP アドレスを設定します。

ステップ 13　（ルーテッド モード）IPv6 アドレスを設定するには、[IPv6] タブをクリックします。

トランスペアレント モードの場合は、EtherChannel インターフェイスではなく、ブリッジ グループ インターフェイスの IP アドレスを設定します。

a. [Enable IPv6] チェックボックスをオンにします。

b. [Interface IPv6 Addresses] エリアで、[Add] をクリックします。

[Add IPv6 Address for Interface] ダイアログボックスが表示されます。

注：[Enable address autoconfiguration] オプションはサポートされません。

c. [Address/Prefix Length] フィールドに、グローバル IPv6 アドレスと IPv6 プレフィックスの長さを入力します。たとえば、2001:DB8::BA98:0:3210/64。

d. （オプション）ホスト アドレスとして Modified EUI-64 インターフェイス ID を使用するには、[EUI-64] チェックボックスをオンにします。この場合は、単に [Address/Prefix Length] フィールドにプレフィックスを入力します。

e. [OK] をクリックします。

ステップ 14　[OK] をクリックして、[Interfaces] 画面に戻ります。

ステップ 15　[Apply] をクリックします。

関連項目

- 「マスター ユニットでのクラスタ インターフェイス モードの設定」（P.9-41）
- 「ブリッジ グループの設定」（P.13-7）
- 「ASA クラスタの作成または ASA クラスタへの参加」（P.9-50）
- 「EtherChannel の設定」（P.10-22）
- 「EtherChannel のガイドライン」（P.10-12）
- 「VSS または vPC への接続」（P.9-15）
- 「物理インターフェイスのイネーブル化およびイーサネット パラメータの設定」（P.10-15）
- 「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.10-28）
- 「セキュリティ コンテキストの設定」（P.7-20）
- 「セキュリティ レベル」（P.12-1）
- 「ASA クラスタ パラメータの設定」（P.9-54）
- 「ASA クラスタリングのガイドライン」（P.9-34）

ASA クラスタの作成または ASA クラスタへの参加

クラスタ内の各ユニットがクラスタに参加するには、ブートストラップ コンフィギュレーションが必要です。1 台のユニット（マスター ユニットになる）上で High Availability and Scalability ウィザードを実行してクラスタを作成し、続いてスレーブ ユニットを追加します。

（注）　マスター ユニットに対して、cLACP システム ID およびプライオリティのデフォルトを変更する場合は、ウィザードを使用できません。クラスタを手動で設定する必要があります。

はじめる前に

- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。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、[Configuration] > [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。
- クラスタ制御リンクの MTU を 1600 バイト以上に設定することを推奨します。このようにするには、この手順を続ける前に各ユニットでジャンボ フレームの予約をイネーブルにする必要があります。ジャンボ フレームの予約には、ASA のリロードが必要です。
- クラスタ制御リンク インターフェイスに使用するインターフェイスは、接続されたスイッチでアップ状態になっている必要があります。
- 稼働中のクラスタにユニットを追加すると、一時的に、限定的なパケット/接続ドロップが発生することがあります。これは予定どおりの動作です。

手順

ステップ 1　[Wizard] > [High Availability and Scalability Wizard] を選択します。次の手順でこのウィザードのガイドラインを確認してください。

ステップ 2　[Interfaces] 画面からは新しい EtherChannel を作成できません（クラスタ制御リンクを除く）。

ステップ 3　[ASA Cluster Configuration] 画面で、ブートストラップの設定を構成します。

- [Member Priority] : マスター ユニット選定用に、このユニットのプライオリティを 1 ～ 100 の範囲内で設定します。1 が最高のプライオリティです。
- （オプション）[Shared Key] : クラスタ制御リンクの制御トラフィックの暗号キーを設定します。共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、暗号キーを生成するために使用されます。このパラメータは、データパス トラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリアテキストとして送信されます。パスワードの暗号化サービスをイネーブルにする場合にも、このパラメータを設定する必要があります。
- （オプション）[Enable connection rebalancing for TCP traffic across all the ASAs in the cluster] : 接続の再分散をイネーブルにします。このパラメータはデフォルトではディセーブルになっています。イネーブルの場合は、クラスタの ASA は定期的に負荷情報を交換し、負荷のかかっているデバイスから負荷の少ないデバイスに新しい接続をオフロードします。負荷情報を交換する間隔を、1 ～ 360 秒の範囲内で指定します。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。

  （注）　サイト間トポロジに対しては接続の再分散を設定しないでください。異なるサイトのクラスタ メンバには接続を再分散できません。

- （オプション）[Enable health monitoring of this device within the cluster] : クラスタのヘルス チェック機能をイネーブルにします。これには、ユニットのヘルス モニタリングおよびインターフェイスのヘルス モニタリングが含まれます。ユニットのヘルスを確認するため、ASA のクラスタ ユニットはクラスタ制御リンクで他のユニットにキープアライブ メッセージを送信します。ユニットがホールド時間内にピア ユニットからキープアライブ メッセージを受信しない場合は、そのピア ユニットは応答不能またはデッド状態と見なされます。インターフェイスのヘルス チェックはリンク障害をモニタします。あるインターフェイスが、特定のユニット上では障害が発生したが、別のユニットではアクティブの場合は、そのユニットはクラスタから削除されます。ユニットがホールド時間内にインターフェイス ステータス メッセージを受信しない場合に、ASA がメンバをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバであるか、またはクラスタに参加しようとしているかによって異なります。

  （注）　何らかのトポロジ変更を行うとき（たとえば、データ インターフェイスの追加または削除、ASA またはスイッチ上のインターフェイスのイネーブル化またはディセーブル化、VSS または vPC を形成するスイッチの追加）は、ヘルス チェックをディセーブルにする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェックを再度イネーブルにします。

- [Time to Wait Before Device Considered Failed]：この値は、ユニットのキープアライブ ステータス メッセージの間隔を指定します。0.8 ～ 45 秒です。デフォルトは 3 秒です。ホールド時間の値はユニットのヘルス チェックのみに適用されることに注意してください。インターフェイス ヘルスの場合は、ASA はインターフェイスのステータス（アップまたはダウン）を使用します。
- （オプション）[Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support]：クラスタ制御リンクが EtherChannel として設定されていて（推奨）、VSS または vPC ペアに接続されている場合は、このオプションをイネーブルにすることが必要になる場合があります。一部のスイッチでは、VSS/vPC の 1 つのユニットがシャットダウンまたは起動すると、そのスイッチに接続されている EtherChannel メンバー インターフェイスが ASA に対してアップと認識される場合がありますが、スイッチ側にはトラフィックが渡されていません。ASA のホールド時間のタイムアウトが低い値（0.8 秒など）に設定されていて、ASA がこれらの EtherChannel インターフェイスの 1 つでキープアライブ メッセージを送信する場合、ASA が誤ってクラスタから除去される可能性があります。このオプションをイネーブルにすると、ASA はクラスタ制御リンクのすべての EtherChannel インターフェイスでキープアライブ メッセージをフラッディングして、少なくとも 1 台のスイッチがそれを受信できることを確認します。

- （オプション）[Replicate console output to the master’s console]：スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。この機能はデフォルトで無効に設定されています。ASA は、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力します。コンソール複製をイネーブルにすると、スレーブ ユニットからマスター ユニットにコンソール メッセージが送信されるので、モニタが必要になるのはクラスタのコンソール ポート 1 つだけとなります。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。
- [Cluster Control Link]：クラスタ制御リンク インターフェイスを指定します。
  - （オプション）[MTU]：クラスタ制御リンク インターフェイスの最大伝送単位を 64 ～ 65,535 バイトの範囲内で指定します。MTU 値よりも大きいデータは、送信前にフラグメント化されます。デフォルトの MTU は 1500 バイトです。すでにジャンボ フレームの予約をイネーブルにしてある場合は、MTU を 1600 バイト以上に設定することを推奨します。ジャンボ フレームを使用する必要があり、まだジャンボ フレームの予約をイネーブルにしていない場合は、ウィザードを終了し、ジャンボ フレームをイネーブルにしてから、この手順を再開する必要があります。

ステップ 4　[Finish] をクリックします。

ステップ 5　ASA は実行コンフィギュレーションをスキャンして、クラスタリングに対応していない機能の非互換コマンドの有無を調べます。デフォルト コンフィギュレーションにあるコマンドも、これに該当することがあります。互換性のないコマンドを削除するには [OK] をクリックします。[Cancel] をクリックすると、クラスタリングはイネーブルになりません。

ステップ 6　しばらくすると、ASDM がクラスタをイネーブルにして ASA に再接続し、ASA がクラスタに追加されたことを確認する [Information] 画面が表示されます。

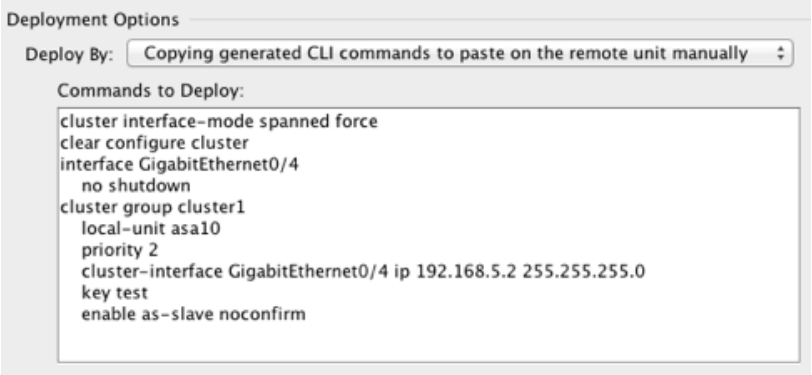
（注）　場合によっては、ウィザードの完了後にクラスタに参加した際にエラーが発生する可能性があります。ASDM が切断されていると、ASDM はそれに続くエラーを ASA から受信しません。ASDM に再接続した後もクラスタリングがディセーブルの場合は、ASA コンソール ポートに接続して、クラスタリングがディセーブルになっている詳細なエラー状況を判断する必要があります。たとえば、クラスタ制御リンクがダウンしている可能性があります。

ステップ 7　スレーブ ユニットを追加するには、[Yes] をクリックします。

マスターからウィザードを再実行する場合、ウィザードを最初に開始するときに [Add another member to the cluster] オプションを選択してスレーブ ユニットを追加できます。

ステップ 8　[Deployment Options] 領域で、次の [Deploy By] オプションのいずれかを選択します。

- [Sending CLI commands to the remote unit now] : ブートストラップ コンフィギュレーションをスレーブ（一時）管理 IP アドレスに送信します。スレーブ管理 IP アドレス、ユーザ名、パスワードを入力します。
- [Copying generated CLI commands to paste on the remote unit manually] : スレーブ ユニットの CLI でコマンドをカット アンド ペースト、または ASDM の CLI ツールを使用するようにコマンドを生成します。[Commands to Deploy] ボックスで、後で使用するためのコマンドを選択してコピーします。



関連項目

- 「ASA クラスタ パラメータの設定」（P.9-54）
- 「ジャンボ フレーム サポートのイネーブル化」（P.10-31）
- 「スパンド EtherChannel の設定」（P.9-47）
- 「個別インターフェイスの設定（管理インターフェイスの場合に推奨）」（P.9-44）
- 「インターフェイスのモニタ」（P.9-10）

ASA クラスタ メンバの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタ メンバを管理できます。

- 「ASA クラスタ パラメータの設定」（P.9-54）
- 「マスター ユニットからの新しいスレーブの追加」（P.9-57）
- 「非アクティブなメンバーになる」（P.9-58）
- 「マスター ユニットからのスレーブ メンバの非アクティブ化」（P.9-59）
- 「クラスタからの脱退」（P.9-60）
- 「マスター ユニットの変更」（P.9-61）
- 「クラスタ全体でのコマンドの実行」（P.9-62）

ASA クラスタ パラメータの設定

クラスタへのユニットの追加にウィザードを使用しない場合は、クラスタ パラメータを手動で設定できます。すでにクラスタリングがイネーブルであれば、いくつかのクラスタ パラメータを編集できます。クラスタリングがイネーブルになっている間は編集できないものは、グレイ表示されます。この手順には、ウィザードに含まれていない高度なパラメータも含まれます。

はじめる前に

- クラスタに参加する前に、各ユニットでクラスタ制御リンク インターフェイスを事前に設定します。シングル インターフェイスの場合、イネーブルにする必要があります。他の設定を構成しないでください。EtherChannel インターフェイスの場合は、イネーブルにして、EtherChannel モードを On に設定します。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。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、[Configuration] > [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。

手順

ステップ 1　[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] の順に選択します。

すでにクラスタにデバイスが追加されており、それがマスター ユニットの場合は、このペインは [Cluster Configuration] タブにあります。

ステップ 2　[Configure ASA cluster settings] チェックボックスをオンにします。

チェックボックスをオフにすると、設定が消去されます。パラメータの設定がすべて完了するまで、[Participate in ASA cluster] をオンにしないでください。

（注）　クラスタリングをイネーブルにした後、[Configure ASA cluster settings] チェックボックスをオフにする場合は、結果をよく理解したうえで行ってください。オフにすると、すべてのクラスタ コンフィギュレーションがクリアされ、ASDM が接続されている管理インターフェイスを含むすべてのインターフェイスもシャットダウンします。この場合、接続を復元するには、コンソール ポートで CLI にアクセスする必要があります。

ステップ 3　次のブートストラップ パラメータを設定します。

- [Cluster Name]：クラスタに名前を付けます。名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。クラスタはユニットあたり 1 つしか設定できません。クラスタのすべてのメンバが同じ名前を使用する必要があります。
- [Member Name] : このクラスタ メンバの固有の名前を 1 ～ 38 文字の ASCII 文字列で指定します。
- [Member Priority] : マスター ユニット選定用に、このユニットのプライオリティを 1 ～ 100 の範囲内で設定します。1 が最高のプライオリティです。
- （オプション）[Shared Key]：クラスタ制御リンクの制御トラフィックの暗号キーを設定します。共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、暗号キーを生成するために使用されます。このパラメータは、データパス トラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリアテキストとして送信されます。パスワードの暗号化サービスをイネーブルにする場合にも、このパラメータを設定する必要があります。

- （オプション）[Enable connection rebalancing for TCP traffic across all the ASAs in the cluster]：接続の再分散をイネーブルにします。このパラメータはデフォルトではディセーブルになっています。イネーブルの場合は、クラスタの ASA は定期的に負荷情報を交換し、負荷のかかっているデバイスから負荷の少ないデバイスに新しい接続をオフロードします。負荷情報を交換する間隔を、1 ～ 360 秒の範囲内で指定します。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。
- （オプション）[Enable health monitoring of this device within the cluster]：クラスタのヘルスチェック機能をイネーブルにします。これには、ユニットのヘルス モニタリングおよびインターフェイスのヘルス モニタリングが含まれます。**注**：クラスタに新しいユニットを追加して、ASA またはスイッチ上でトポロジに変更を加えるときは、クラスタが完成するまで、この機能を一時的にディセーブルにする必要があります。クラスタとトポロジの変更が完了したら、この機能を再度イネーブルにすることができます。ユニットのヘルスを確認するため、ASA のクラスタ ユニットはクラスタ制御リンクで他のユニットにキープアライブ メッセージを送信します。ユニットがホールド時間内にピア ユニットからキープアライブ メッセージを受信しない場合は、そのピア ユニットは応答不能またはデッド状態と見なされます。インターフェイス ステータス メッセージによって、リンク障害が検出されます。あるインターフェイスが、特定のユニット上では障害が発生したが、別のユニットではアクティブの場合は、そのユニットはクラスタから削除されます。ユニットがホールド時間内にインターフェイス ステータス メッセージを受信しない場合に、ASA がメンバをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバであるか、またはクラスタに参加しようとしているかによって異なります。

  （注） 何らかのトポロジ変更を行うとき（たとえば、データ インターフェイスの追加または削除、ASA またはスイッチ上のインターフェイスのイネーブル化またはディセーブル化、VSS または vPC を形成するスイッチの追加）は、ヘルス チェックをディセーブルにする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェックを再度イネーブルにします。

  – （オプション）[Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support]：クラスタ制御リンクが EtherChannel として設定されていて（推奨）、VSS または vPC ペアに接続されている場合は、このオプションをイネーブルにすることが必要になる場合があります。一部のスイッチでは、VSS/vPC の 1 つのユニットがシャットダウンまたは起動すると、そのスイッチに接続されている EtherChannel メンバー インターフェイスが ASA に対してアップと認識される場合がありますが、スイッチ側にはトラフィックが渡されていません。ASA のホールド時間のタイムアウトが低い値（0.8 秒など）に設定されていて、ASA がこれらの EtherChannel インターフェイスの 1 つでキープアライブ メッセージを送信する場合、ASA が誤ってクラスタから除去される可能性があります。このオプションをイネーブルにすると、ASA はクラスタ制御リンクのすべての EtherChannel インターフェイスでキープアライブ メッセージをフラッディングして、少なくとも 1 台のスイッチがそれを受信できることを確認します。
- （オプション）[Replicate console output to the master’s console]：スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。この機能はデフォルトで無効に設定されています。ASA は、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力します。コンソール複製をイネーブルにすると、スレーブ ユニットからマスター ユニットにコンソール メッセージが送信されるので、モニタが必要になるのはクラスタのコンソール ポート 1 つだけとなります。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。

- [Cluster Control Link]：クラスタ制御リンク インターフェイスを指定します。このインターフェイスは、設定されている名前を使用できません。使用可能なインターフェイスがドロップダウン リストに表示されます。
  - [Interface]：インターフェイス ID、できれば EtherChannel を指定します。サブインターフェイスと管理タイプ インターフェイスは許可されません。
  - [IP Address]：IP アドレスには IPv4 アドレスを指定します。IPv6 は、このインターフェイスではサポートされません。
  - [Subnet Mask]：サブネット マスクを指定します。
  - （オプション）[MTU]：クラスタ制御リンク インターフェイスの最大伝送単位を 64 ～ 65,535 バイトの範囲内で指定します。MTU 値よりも大きいデータは、送信前にフラグメント化されます。デフォルトの MTU は 1500 バイトです。MTU を 1600 バイト以上に設定することを推奨します。このようにするには、ジャンボ フレームの予約をイネーブルにする必要があります。
- （オプション）[Cluster LACP]：スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。cLACP ネゴシエーションのときに、同じクラスタ内の ASA は互いに連携し、スイッチに対して全体で 1 つの（仮想）デバイスであるかのように見せます。
  - [Enable static port priority]：LACP のダイナミック ポート プライオリティをディセーブルにします。一部のスイッチはダイナミック ポート プライオリティをサポートしていないので、このパラメータによりスイッチの互換性が向上します。さらに、8 個より多くのアクティブなスパンド EtherChannel メンバのサポートがイネーブルになります（最大 32 メンバ）。このパラメータを使用しないと、サポートされるのは 8 個のアクティブ メンバと 8 個のスタンバイ メンバのみです。このパラメータをイネーブルにした場合、スタンバイ メンバは使用できません。すべてのメンバがアクティブです。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。
  - [Virtual System MAC Address]：MAC アドレス形式である cLACP システム ID を設定します。すべての ASA が同じシステム ID を使用します。これはマスター ユニットによって自動生成され（デフォルト）、すべてのスレーブに複製されます。または手動で、*H.H.H* の形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。ただし、クラスタリングをイネーブルにした後は、この値は変更できません。
  - [System Priority]：1 ～ 65535 の範囲でシステム プライオリティを設定します。プライオリティは意思決定を担当するユニットの決定に使用されます。デフォルトでは、ASA はプライオリティ 1（最高のプライオリティ）を使用します。このプライオリティは、スイッチのプライオリティよりも高いことが必要です。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。ただし、クラスタリングをイネーブルにした後は、この値は変更できません。

ステップ 4　[Participate in ASA cluster] チェックボックスをオンにして、クラスタに参加します。

ステップ 5　[Apply] をクリックします。

関連項目

- 「インターフェイスのモニタ」（P.9-10）
- 「ジャンボ フレーム サポートのイネーブル化」（P.10-31）

マスター ユニットからの新しいスレーブの追加

マスター ユニットからクラスタに追加スレーブを追加することができます。High Availability and Scalability ウィザードを使用してスレーブを追加することもできます。マスター ユニットからスレーブを追加すると、クラスタ制御リンクを設定でき、追加する各スレーブ ユニットにクラスタ インターフェイス モードを設定できるというメリットがあります。

または、スレーブ ユニットにログインし、ユニット上で直接クラスタリングを設定することもできます。ただし、クラスタリングをイネーブルにした後は、ASDM セッションが切断されるので、再接続する必要があります。

はじめる前に

- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。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、[Configuration] > [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。
- 管理ネットワーク上でブートストラップ コンフィギュレーションを送信する場合は、スレーブ ユニットにアクセス可能な IP アドレスがあることを確認してください。

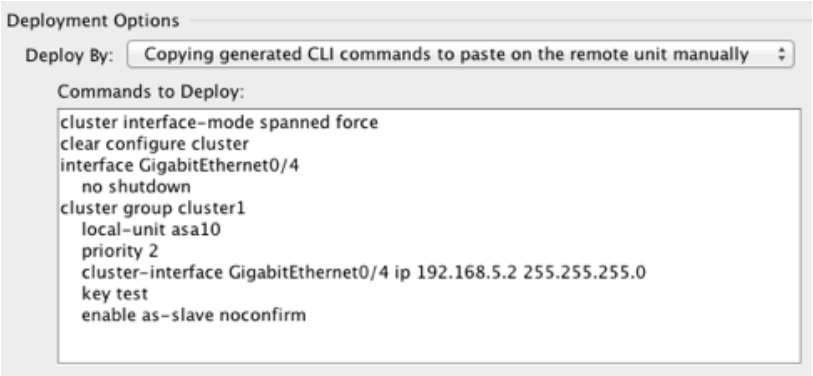
手順

ステップ 1　[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Members] の順に選択します。

ステップ 2　[Add] をクリックします。

ステップ 3　次のパラメータを設定します。

- [Member Name] : このクラスタ メンバの固有の名前を 1 ～ 38 文字の ASCII 文字列で指定します。
- [Member Priority] : マスター ユニット選定用に、このユニットのプライオリティを 1 ～ 100 の範囲内で設定します。1 が最高のプライオリティです。
- [Cluster Control Link] > [IP Address] : マスター クラスタ制御リンクと同じネットワーク上で、クラスタ制御リンクのこのメンバに一意の IP アドレスを指定します。
- [Deployment Options] 領域で、次の [Deploy By] オプションのいずれかを選択します。
  - [Sending CLI commands to the remote unit now] : ブートストラップ コンフィギュレーションをスレーブ（一時）管理 IP アドレスに送信します。スレーブ管理 IP アドレス、ユーザ名、パスワードを入力します。
  - [Copying generated CLI commands to paste on the remote unit manually] : スレーブ ユニットの CLI でコマンドをカット アンド ペースト、または ASDM の CLI ツールを使用するようにコマンドを生成します。[Commands to Deploy] ボックスで、後で使用するためのコマンドを選択してコピーします。



ステップ 4　[OK] をクリックし、さらに [Apply] をクリックします。

関連項目

- 「ASA クラスタ パラメータの設定」（P.9-54）

非アクティブなメンバーになる

クラスタの非アクティブ メンバになるには、クラスタリング コンフィギュレーションは変更せずに、そのユニット上でクラスタリングをディセーブルにします。

（注）　ASA が（手動で、またはヘルス チェック エラーにより）非アクティブになると、すべてのデータ インターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開させるには、クラスタリングを再びイネーブルにします。または、そのユニットをクラスタから完全に削除します。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはアクセスできません（マスター ユニットと同じメイン IP アドレスを使用するため）。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

はじめる前に

- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。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は、[Configuration] > [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。

手順

ステップ 1　[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] の順に選択します。

すでにクラスタにデバイスが追加されており、それがマスター ユニットの場合は、このペインは [Cluster Configuration] タブにあります。

ステップ 2　[Participate in ASA cluster] チェックボックスをオフにします。

（注）　[Configure ASA cluster settings] チェックボックスをオフにしないでください。オフにすると、すべてのクラスタ コンフィギュレーションがクリアされ、ASDM が接続されている管理インターフェイスを含むすべてのインターフェイスもシャットダウンします。この場合、接続を復元するには、コンソール ポートで CLI にアクセスする必要があります。

ステップ 3　[Apply] をクリックします。

このユニットがマスター ユニットであった場合は、新しいマスターの選定が実行され、別のメンバがマスター ユニットになります。

クラスタ コンフィギュレーションは維持されるので、後でクラスタリングを再度イネーブルにできます。

関連項目

- 「クラスタからの脱退」（P.9-60）

マスター ユニットからのスレーブ メンバの非アクティブ化

スレーブ メンバを非アクティブにするには、次の手順を実行します。

（注）　ASA が非アクティブになると、すべてのデータ インターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開させるには、クラスタリングを再びイネーブルにします。または、そのユニットをクラスタから完全に削除します。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはアクセスできません（マスター ユニットと同じメイン IP アドレスを使用するため）。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

はじめる前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。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は、[Configuration] > [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。

手順

ステップ 1　ユニットをクラスタから削除します。

cluster remove unit *unit_name*

例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2.To bring it back
to the cluster please logon to that unit and re-enable clustering
```

ブートストラップ コンフィギュレーションは変更されず、マスター ユニットから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスター ユニットを削除するためにスレーブ ユニットでこのコマンドを入力した場合は、新しいマスター ユニットが選定されます。

メンバ名を一覧表示するには、**cluster remove unit ?** と入力するか、**show cluster info** コマンドを入力します。

ステップ 1　[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] の順に選択します。

ステップ 2　削除するスレーブを選択して [Delete] をクリックします。

スレーブ ブートストラップ コンフィギュレーションは同じであり、その設定を失うことなく以後スレーブを再追加できます。

ステップ 3　[Apply] をクリックします。

関連項目

- 「クラスタからの脱退」（P.9-60）

クラスタからの脱退

クラスタから完全に脱退するには、クラスタ ブートストラップ コンフィギュレーション全体を削除する必要があります。各メンバの現在のコンフィギュレーションは同一（マスター ユニットから同期された）であるため、クラスタから脱退すると、クラスタリング前のコンフィギュレーションをバックアップから復元するか、IP アドレスの競合を避けるためコンフィギュレーションを消去して初めからやり直すことも必要になります。

はじめる前に

コンソール ポートを使用する必要があります。クラスタのコンフィギュレーションを削除すると、管理インターフェイスとクラスタ制御リンクを含むすべてのインターフェイスがシャットダウンされます。

手順

ステップ 1　スレーブ ユニットの場合、クラスタリングをディセーブルにします。

```
cluster group cluster_name
no enable
```

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

クラスタリングがスレーブ ユニット上でイネーブルになっている間は、コンフィギュレーション変更を行うことはできません。

ステップ 2　クラスタ コンフィギュレーションをクリアします。

```
clear configure cluster
```

ASA は、管理インターフェイスとクラスタ制御リンクを含むすべてのインターフェイスをシャットダウンします。

ステップ 3　クラスタ インターフェイス モードをディセーブルにします。

no cluster interface-mode

モードはコンフィギュレーションには保存されないため、手動でリセットする必要があります。

ステップ 4　バックアップ コンフィギュレーションがある場合、実行コンフィギュレーションにバックアップ コンフィギュレーションをコピーします。

copy *backup_cfg* **running-config**

例：

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

ステップ 5　コンフィギュレーションをスタートアップに保存します。

write memory

ステップ 6　バックアップ コンフィギュレーションがない場合は、管理アクセスを再設定します。たとえば、インターフェイス IP アドレスを変更し、正しいホスト名を復元します。

関連項目

- 第 2 章「使用する前に」

マスター ユニットの変更

注意　マスター ユニットを変更する最善の方法は、マスター ユニットでクラスタリングをディセーブルにし、新しいマスターの選択を待った後、クラスタリングを再度イネーブルにします。マスターにするユニットを厳密に指定する必要がある場合は、この項の手順を使用します。ただし、中央集中型機能の場合は、この手順を使用してマスター ユニット変更を強制するとすべての接続がドロップされるので、新しいマスター ユニット上で接続を再確立する必要があります。

マスター ユニットを変更するには、次の手順を実行します。

はじめる前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。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は、[Configuration] > [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。

手順

ステップ 1　[Monitoring] > [ASA Cluster] > [Cluster Summary] を選択します。

ステップ 2　[Change Master To] ドロップダウン リストから、マスターにするスレーブ ユニットを選択し、[Make Master] をクリックします。

ステップ 3　マスター ユニット変更の確認を求められます。[Yes] をクリックします。

ステップ 4　ASDM を終了し、メイン クラスタ IP アドレスを使用して再接続します。

関連項目

- 「非アクティブなメンバーになる」（P.9-58）
- 「クラスタリングの中央集中型機能」（P.9-26）

クラスタ全体でのコマンドの実行

コマンドをクラスタ内のすべてのメンバに、または特定のメンバに送信するには、次の手順を実行します。**show** コマンドをすべてのメンバに送信すると、すべての出力が収集されて現在のユニットのコンソールに表示されます。その他のコマンド、たとえば **capture** や **copy** も、クラスタ全体での実行を活用できます。

はじめる前に

コマンドライン インターフェイス ツールでこの手順を実行します。[Tools] > [Command Line Interface] を選択します。

手順

ステップ 1　コマンドをすべてのメンバに送信します。ユニット名を指定した場合は、特定のメンバに送信されます。

cluster exec [**unit** *unit_name*] *command*

例：

```
cluster exec show xlate
```

メンバ名を一覧表示するには、**cluster exec unit ?**（現在のユニットを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

例

同じキャプチャ ファイルをクラスタ内のすべてのユニットから同時に TFTP サーバにコピーするには、マスター ユニットで次のコマンドを入力します。

```
cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ユニットから 1 つずつ）が TFTP サーバにコピーされます。宛先のキャプチャ ファイル名には自動的にユニット名が付加され、capture1_asa1.pcap、capture1_asa2.pcap などとなります。この例では、asa1 および asa2 がクラスタ ユニット名です。

次の例では、**cluster exec show port-channel summary** コマンドの出力に、クラスタの各メンバの EtherChannel 情報が表示されています。

```
cluster exec show port-channel summary
primary(LOCAL):*********************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1              LACP      Yes  Gi0/0(P)
2         Po2              LACP      Yes  Gi0/1(P)
 secondary:*****************************************************************
```

```
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1              LACP      Yes   Gi0/0(P)
2         Po2              LACP      Yes   Gi0/1(P)
```

ASA クラスタのモニタ

クラスタの状態と接続をモニタおよびトラブルシューティングできます。

- 「クラスタの状態のモニタリング」（P.9-63）
- 「クラスタ全体のパケットのキャプチャ」（P.9-63）
- 「クラスタ リソースのモニタリング」（P.9-64）
- 「クラスタ トラフィックのモニタリング」（P.9-64）
- 「クラスタ制御リンクのモニタリング」（P.9-64）
- 「クラスタリングのロギングの設定」（P.9-64）

クラスタの状態のモニタリング

クラスタの状態のモニタリングについては、次の画面を参照してください。

- [Monitoring] > [ASA Cluster] > [Cluster Summary]

  このペインには、接続相手のユニットとクラスタのその他のユニットの情報が表示されます。また、このペインでマスター ユニットを変更することができます。

- **Cluster Dashboard**

  マスター ユニットのホーム ページの [Cluster Dashboard] と [Cluster Firewall Dashboard] を使用してクラスタをモニタできます。

関連項目

- 「[Cluster Firewall Dashboard] タブ」（P.3-27）
- 「[Cluster Dashboard] タブ」（P.3-25）

クラスタ全体のパケットのキャプチャ

クラスタでのパケットのキャプチャについては、次の画面を参照してください。

[Wizards] > [Packet Capture Wizard]

クラスタ全体のトラブルシューティングをサポートするには、マスター ユニット上でのクラスタ固有トラフィックのキャプチャをイネーブルにします。これで、クラスタ内のすべてのスレーブ ユニットでも自動的にイネーブルになります。

関連項目

- 「Packet Capture Wizard を使用したキャプチャの設定と実行」（P.39-1）

クラスタ リソースのモニタリング

クラスタ リソースのモニタリングについては、次の画面を参照してください。

- [Monitoring] > [ASA Cluster] > [System Resources Graphs] > [CPU]

  このペインでは、クラスタ メンバ全体の CPU 使用率を示すグラフまたはテーブルを作成することができます。

- [Monitoring] > [ASA Cluster] > [System Resources Graphs] > [Memory]。このペインでは、クラスタ メンバ全体の [Free Memory] と [Used Memory] を表示するグラフまたはテーブルを作成することができます。

クラスタ トラフィックのモニタリング

クラスタ トラフィックのモニタリングについては、次の画面を参照してください。

- [Monitoring] > [ASA Cluster] > [Traffic] > [Graphs] > [Connections]。

  このペインでは、クラスタ メンバ全体の接続を示すグラフまたはテーブルを作成することができます。

- [Monitoring] > [ASA Cluster] > [Traffic] > [Graphs] > [Throughput]。

  このペインでは、クラスタ メンバ全体のトラフィックのスループットを示すグラフまたはテーブルを作成することができます。

クラスタ制御リンクのモニタリング

クラスタの状態のモニタリングについては、次の画面を参照してください。

[Monitoring] > [Properties] > [System Resources Graphs] > [Cluster Control Link]。

このペインでは、クラスタ制御リンクの [Receival] および [Transmittal] 容量使用率を表示するグラフまたはテーブルを作成することができます。

クラスタリングのロギングの設定

クラスタリングのロギングの設定については、次の画面を参照してください。

[Configuration] > [Device Management] > [Logging] > [Syslog Setup]

クラスタ内の各ユニットは、syslog メッセージを個別に生成します。同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。

関連項目

- 「指定した出力先へのクラス内のすべての syslog メッセージの送信」（P.40-21）

ASA クラスタリングの例

以下の例には、一般的な導入での ASA のクラスタ関連のすべてのコンフィギュレーションが含まれます。

- 「ASA およびスイッチのコンフィギュレーションの例」（P.9-65）
- 「Firewall on a Stick」（P.9-68）
- 「トラフィックの分離」（P.9-70）
- 「スパンド EtherChannel とバックアップ リンク（従来の 8 アクティブ/8 スタンバイ）」（P.9-72）

ASA およびスイッチのコンフィギュレーションの例

次のコンフィギュレーション例は、ASA とスイッチ間の次のインターフェイスを接続します。

ASA インターフェイス	スイッチ インターフェイス
GigabitEthernet 0/2	GigabitEthernet 1/0/15
GigabitEthernet 0/3	GigabitEthernet 1/0/16
GigabitEthernet 0/4	GigabitEthernet 1/0/17
GigabitEthernet 0/5	GigabitEthernet 1/0/18

- 「ASA のコンフィギュレーション」（P.9-65）
- 「Cisco IOS スイッチのコンフィギュレーション」（P.9-67）

ASA のコンフィギュレーション

各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ASA1 マスター ブートストラップ コンフィギュレーション

```
interface GigabitEthernet0/0
 channel-group 1 mode on
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit A
 cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
 priority 10
 key emphyri0
 enable noconfirm
```

ASA2 スレーブ ブートストラップ コンフィギュレーション

```
interface GigabitEthernet0/0
 channel-group 1 mode on
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit B
 cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
 priority 11
 key emphyri0
 enable as-slave
```

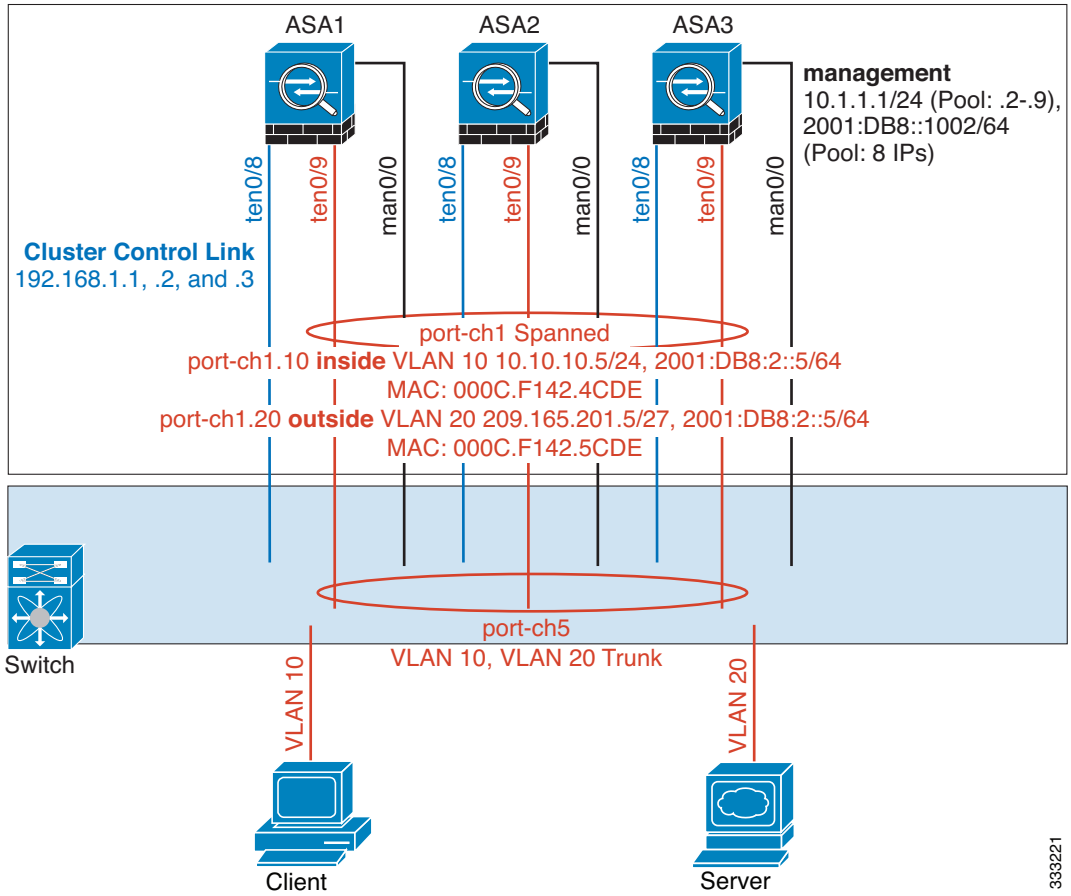
マスター インターフェイス コンフィギュレーション

```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

interface GigabitEthernet0/2
 channel-group 10 mode active
 no shutdown
!
interface GigabitEthernet0/3
 channel-group 10 mode active
 no shutdown
!
interface GigabitEthernet0/4
 channel-group 11 mode active
 no shutdown
!
interface GigabitEthernet0/5
 channel-group 11 mode active
 no shutdown
!
interface Management0/0
 management-only
 nameif management
 ip address 10.53.195.230 cluster-pool mgmt-pool
 security-level 100
 no shutdown
!
interface Port-channel10
 port-channel span-cluster
 mac-address aaaa.bbbb.cccc
 nameif inside
 security-level 100
 ip address 209.165.200.225 255.255.255.224
!
interface Port-channel11
 port-channel span-cluster
 mac-address aaaa.dddd.cccc
 nameif outside
 security-level 0
 ip address 209.165.201.1 255.255.255.224
```

Cisco IOS スイッチのコンフィギュレーション

```
interface GigabitEthernet1/0/15
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/16
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/17
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active
!
interface GigabitEthernet1/0/18
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active

interface Port-channel10
 switchport access vlan 201
 switchport mode access

interface Port-channel11
 switchport access vlan 401
 switchport mode access
```

Firewall on a Stick



異なるセキュリティ ドメインからのデータ トラフィックには、異なる VLAN が関連付けられます。たとえば内部ネットワーク用には VLAN 10、外部ネットワークには VLAN 20 とします。各 ASA は単一の物理ポートがあり、外部スイッチまたはルータに接続されます。トランキングがイネーブルになっているので、物理リンク上のすべてのパケットが 802.1q カプセル化されます。ASA は、VLAN 10 と VLAN 20 の間のファイアウォールです。

スパンド EtherChannel を使用するときは、スイッチ側ですべてのデータ リンクがグループ化されて 1 つの EtherChannel となります。ASA の 1 つが使用不可能になった場合は、スイッチは残りのユニット間でトラフィックを再分散します。

各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ASA1 マスター ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/8
    no shutdown
    description CCL

cluster group cluster1
    local-unit asa1
    cluster-interface tengigabitethernet0/8 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

ASA2 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/8
    no shutdown
    description CCL

cluster group cluster1
    local-unit asa2
    cluster-interface tengigabitethernet0/8 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    enable as-slave
```

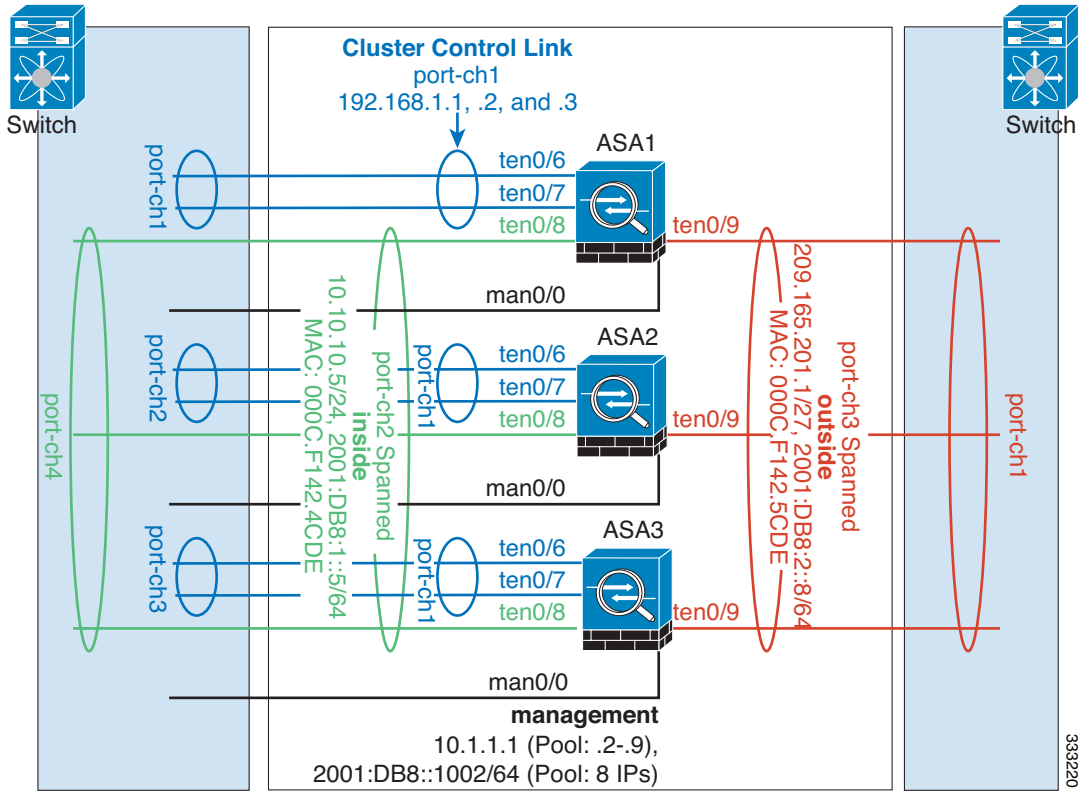
ASA3 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/8
    no shutdown
    description CCL

cluster group cluster1
    local-unit asa3
    cluster-interface tengigabitethernet0/8 ip 192.168.1.3 255.255.255.0
    priority 3
    key chuntheunavoidable
    enable as-slave
```

マスター インターフェイス コンフィギュレーション

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
    security-level 100
    management-only
    no shutdown

interface tengigabitethernet 0/9
    channel-group 2 mode active
    no shutdown
interface port-channel 2
    port-channel span-cluster
interface port-channel 2.10
    vlan 10
    nameif inside
    ip address 10.10.10.5 255.255.255.0
    ipv6 address 2001:DB8:1::5/64
    mac-address 000C.F142.4CDE
interface port-channel 2.20
    vlan 20
    nameif outside
    ip address 209.165.201.1 255.255.255.224
    ipv6 address 2001:DB8:2::8/64
    mac-address 000C.F142.5CDE
```

トラフィックの分離



内部ネットワークと外部ネットワークの間で、トラフィックを物理的に分離することができます。

上の図に示すように、左側に一方のスパンド EtherChannel があり、内部スイッチに接続されています。他方は右側にあり、外部スイッチに接続されています。必要であれば、各 EtherChannel 上に VLAN サブインターフェイスを作成することもできます。

各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ASA1 マスター ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

ASA2 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa2
    cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    enable as-slave
```

ASA3 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa3
    cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
    priority 3
    key chuntheunavoidable
    enable as-slave
```

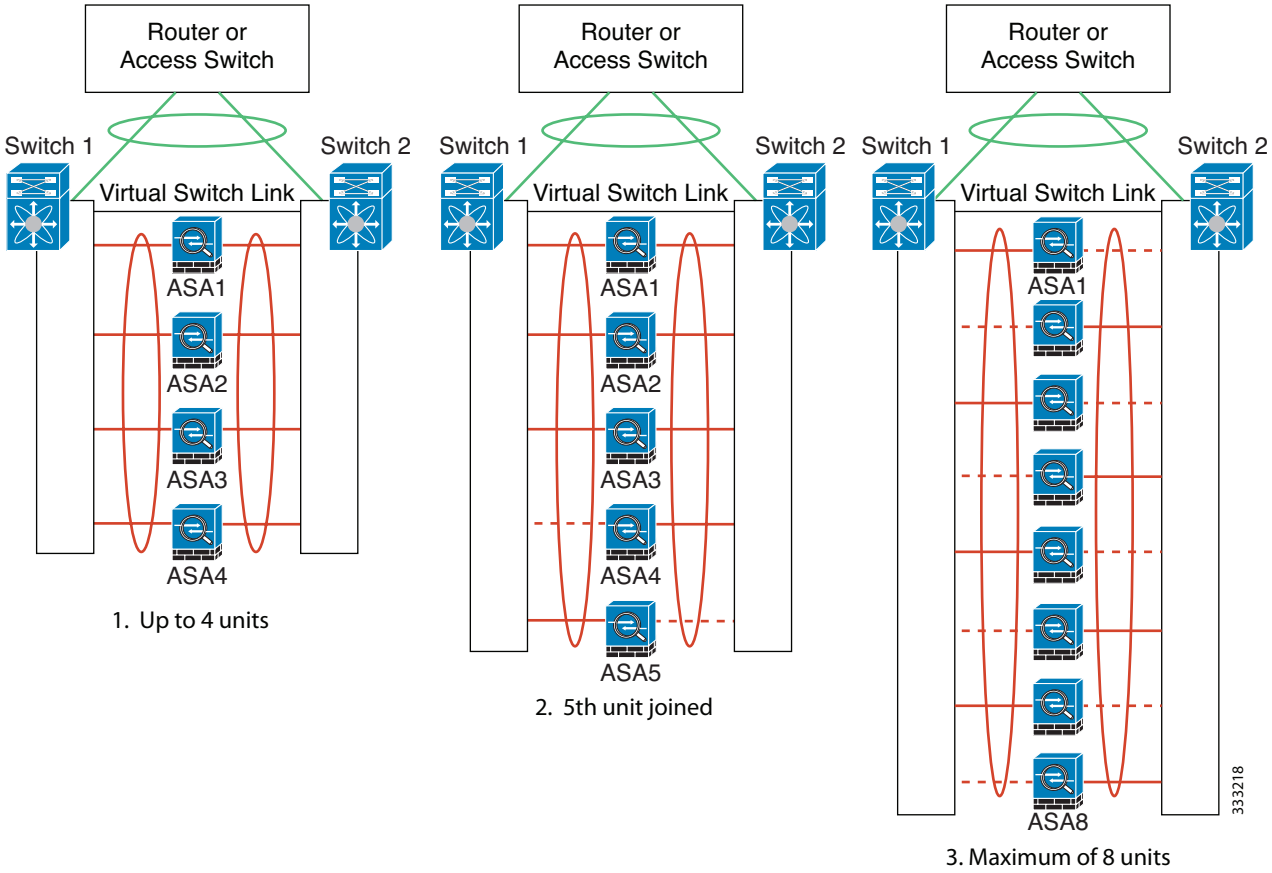
マスター インターフェイス コンフィギュレーション

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
    security-level 100
    management-only
    no shutdown

interface tengigabitethernet 0/8
    channel-group 2 mode active
    no shutdown
interface port-channel 2
    port-channel span-cluster
    nameif inside
    ip address 10.10.10.5 255.255.255.0
    ipv6 address 2001:DB8:1::5/64
    mac-address 000C.F142.4CDE

interface tengigabitethernet 0/9
    channel-group 3 mode active
    no shutdown
interface port-channel 3
```

```
port-channel span-cluster
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

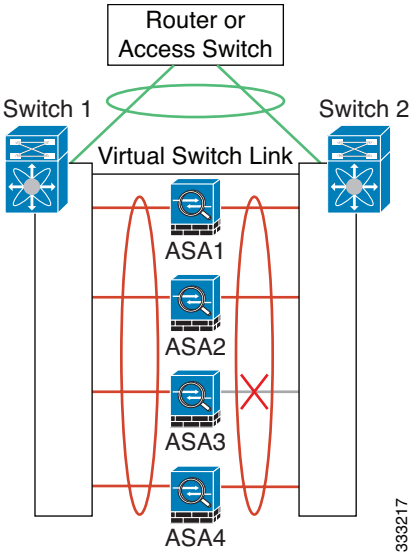
スパンド EtherChannel とバックアップ リンク（従来の 8 アクティブ/8 スタンバイ）

従来の EtherChannel のアクティブ ポートの最大数は、スイッチ側からの 8 に制限されます。8 台の ASA から成るクラスタがあり、EtherChannel にユニットあたり 2 ポートを割り当てた場合は、合計 16 ポートのうち 8 ポートをスタンバイ モードにする必要があります。ASA は、どのリンクをアクティブまたはスタンバイにするかを、LACP を使用してネゴシエートします。VSS または vPC を使用してマルチスイッチ EtherChannel をイネーブルにした場合は、スイッチ間の冗長性を実現できます。ASA では、すべての物理ポートが最初にスロット番号順、次にポート番号順に並べられます。次の図では、番号の小さいポートが「プライマリ」ポートとなり（たとえば GigabitEthernet 0/0）、他方が「セカンダリ」ポートとなります（たとえば GigabitEthernet 0/1）。ハードウェア接続の対称性を保証する必要があります。つまり、すべてのプライマリ リンクは 1 台のスイッチが終端となり、すべてのセカンダリ リンクは別のスイッチが終端となっている必要があります（VSS/vPC が使用されている場合）。次の図は、クラスタに参加するユニットが増えてリンクの総数が増加したときに、どのようになるかを示しています。

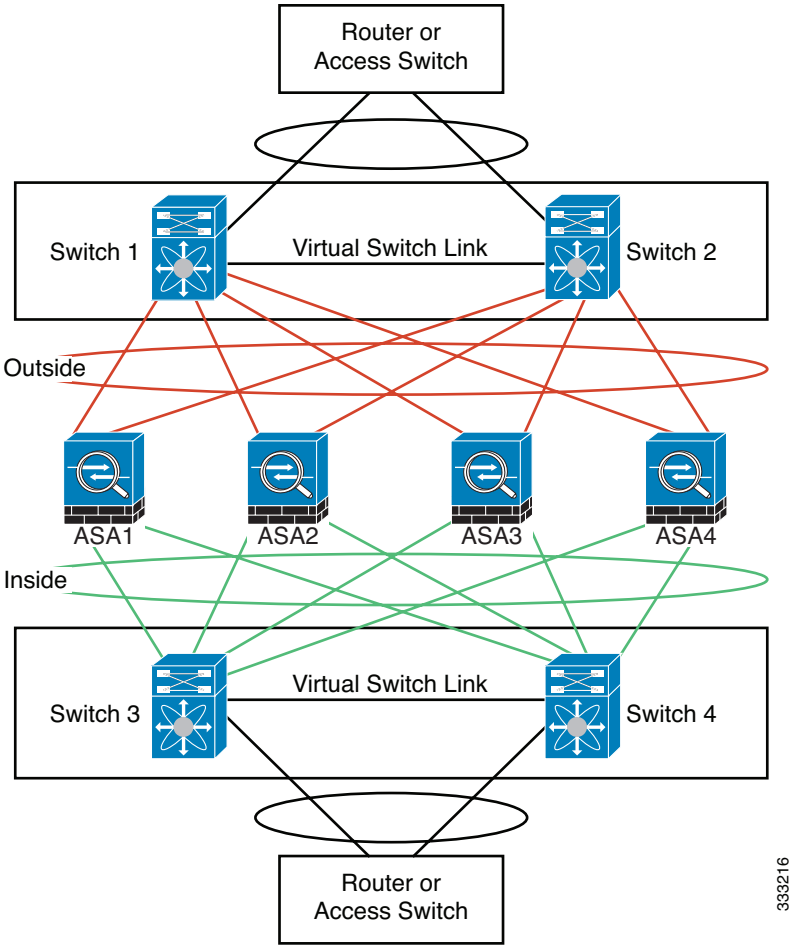


原則として、初めにチャネル内のアクティブ ポート数を最大化し、そのうえで、アクティブなプライマリ ポートとアクティブなセカンダリ ポートの数のバランスを保ちます。5 番目のユニットがクラスタに参加したときは、トラフィックがすべてのユニットに均等には分散されないことに注意してください。

リンクまたはデバイスの障害が発生したときも、同じ原則で処理されます。その結果、ロードバランシングが理想的な状態にはならないこともあります。次の図は、4 ユニットのクラスタを示しています。このユニットの 1 つで、単一リンク障害が発生しています。



ネットワーク内に複数の EtherChannel を設定することも考えられます。次の図では、EtherChannel が内部に 1 つ、外部に 1 つあります。ASA は、一方の EtherChannel でプライマリとセカンダリの両方のリンクが障害状態になった場合にクラスタから削除されます。これは、その ASA がすでに内部ネットワークへの接続を失っているにもかかわらず、外部ネットワークからトラフィックを受信するのを防ぐためです。



各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ASA1 マスター ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL
```

```
cluster group cluster1
    local-unit asa1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

ASA2 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa2
    cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    enable as-slave
```

ASA3 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa3
    cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
    priority 3
    key chuntheunavoidable
    enable as-slave
```

ASA4 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
```

```
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa4
    cluster-interface port-channel1 ip 192.168.1.4 255.255.255.0
    priority 4
    key chuntheunavoidable
    enable as-slave
```

マスター インターフェイス コンフィギュレーション

```
ip local pool mgmt 10.1.1.2-10.1.1.9

interface management 0/0
    channel-group 2 mode active
    no shutdown
interface management 0/1
    channel-group 2 mode active
    no shutdown
interface port-channel 2
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    security-level 100
    management-only

interface tengigabitethernet 1/6
    channel-group 3 mode active vss-id 1
    no shutdown
interface tengigabitethernet 1/7
    channel-group 3 mode active vss-id 2
    no shutdown
interface port-channel 3
    port-channel span-cluster vss-load-balance
    nameif inside
    ip address 10.10.10.5 255.255.255.0
    mac-address 000C.F142.4CDE

interface tengigabitethernet 1/8
    channel-group 4 mode active vss-id 1
    no shutdown
interface tengigabitethernet 1/9
    channel-group 4 mode active vss-id 2
    no shutdown
interface port-channel 4
    port-channel span-cluster vss-load-balance
    nameif outside
    ip address 209.165.201.1 255.255.255.224
    mac-address 000C.F142.5CDE
```

ASA クラスタリングの履歴

機能名	プラットフォームリリース	機能情報
ASA 5580 および 5585-X の ASA クラスタリング	9.0(1)	ASA クラスタリングを利用すると、複数の ASA をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。ASA クラスタリングは、ASA 5580 および ASA 5585-X でサポートされます。1 つのクラスタ内のすべてのユニットが同一モデル、同一ハードウェア仕様であることが必要です。クラスタリングがイネーブルのときにサポートされない機能のリストについては、コンフィギュレーション ガイドを参照してください。 次の画面が導入または変更されました。 [Home] > [Device Dashboard] [Home] > [Cluster Dashboard] [Home] > [Cluster Firewall Dashboard] [Configuration] > [Device Management] > [Advanced] > [Address Pools] > [MAC Address Pools] [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] [Configuration] > [Device Management] > [Logging] > [Syslog Setup] > [Advanced] [Configuration] > [Device Setup] > [Interfaces]> [Add/Edit Interface] > [Advanced] [Configuration] > [Device Setup] > [Interfaces]> [Add/Edit Interface] > [IPv6] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit EtherChannel Interface] > [Advanced] [Configuration] > [Firewall] > [Advanced] > [Per-Session NAT Rules] [Monitoring] > [ASA Cluster] [Monitoring] > [Properties] > [System Resources Graphs] > [Cluster Control Link] [Tools] > [Preferences] > [General] [Tools] > [System Reload] [Tools] > [Upgrade Software from Local Computer] [Wizards] > [High Availability and Scalability Wizard] [Wizards] > [Packet Capture Wizard] [Wizards] > [Startup Wizard]
ASA 5500-X でのクラスタリングのサポート	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X および ASA 5555-X が 2 ユニット クラスタをサポートするようになりました。2 ユニットのクラスタリングは、基本ライセンスではデフォルトでイネーブルになります。ASA 5512-X では Security Plus ライセンスが必要です。 変更された ASDM 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
ヘルス チェック モニタリングの VSS および vPC によるサポートの強化	9.1(4)	クラスタ制御リンクが EtherChannel として設定されていて（推奨）、VSS または vPC ペアに接続されている場合、ヘルス チェック モニタリングによって安定性を高めることができます。一部のスイッチ（Cisco Nexus 5000 など）では、VSS/vPC の 1 つのユニットがシャットダウンまたは起動すると、そのスイッチに接続されている EtherChannel メンバー インターフェイスが ASA に対してアップと認識される場合がありますが、スイッチ側にはトラフィックが渡されていません。ASA のホールド時間のタイムアウトが低い値（0.8 秒など）に設定されていて、ASA がこれらの EtherChannel インターフェイスの 1 つでキープアライブ メッセージを送信する場合、ASA が誤ってクラスタから除去される可能性があります。VSS/vPC ヘルス チェック機能をイネーブルにすると、ASA はクラスタ制御リンクのすべての EtherChannel インターフェイスでキープアライブ メッセージをフラッディングして、少なくとも 1 台のスイッチがそれを受信できることを確認します。 画面 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] が変更されました。
異なる地理的位置にあるクラスタ メンバのサポート（サイト間）。個別インターフェイス モードのみ	9.1(4)	個別インターフェイス モードを使用すると、クラスタ メンバを異なる地理的な場所に配置できるようになりました。 変更された ASDM 画面はありません。
トランスペアレント モードでの異なる地理的位置にあるクラスタ メンバのサポート（サイト間）	9.2(1)	トランスペアレント ファイアウォール モードでスパンド EtherChannel モードを使用すると、クラスタ メンバを異なる地理的な場所に配置できるようになりました。ルーテッド ファイアウォール モードのスパンド EtherChannel での Inter-Site クラスタリングはサポートされません。 変更された ASDM 画面はありません。
クラスタリングに対するスタティック LACP ポート プライオリティのサポート	9.2(1)	一部のスイッチは、LACP でのダイナミック ポート プライオリティをサポートしていません（アクティブおよびスタンバイ リンク）。ダイナミック ポート プライオリティをディセーブルにすることで、スパンド EtherChannel との互換性を高めることができるようになりました。次の注意事項にも従う必要があります。 • クラスタ制御リンク パスのネットワーク エレメントでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。 • ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。 画面 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] が変更されました。

機能名	プラットフォームリリース	機能情報
スパンド EtherChannel での 32 個のアクティブ リンクのサポート	9.2(1)	ASA EtherChannels は最大 16 個のアクティブ リンクをサポートするようになりました。*スパンド* EtherChannel ではその機能が拡張されて、vPC の 2 台のスイッチで使用し、ダイナミック ポート プライオリティをディセーブルにした場合、クラスタ全体で最大 32 個のアクティブ リンクをサポートします。スイッチは、16 個のアクティブ リンクの EtherChannel をサポートする必要があります（例：Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。 8 個のアクティブ リンクをサポートする VSS または vPC のスイッチの場合は、スパンド EtherChannel に 16 個のアクティブ リンクを設定できます（各スイッチに接続された 8 個）。従来は、VSS/vPC で使用する場合であっても、スパンド EtherChannel は 8 個のアクティブ リンクと 8 個のスタンバイ リンクしかサポートしませんでした。 **（注）** スパンド EtherChannel で 8 個より多くのアクティブ リンクを使用する場合は、スタンバイ リンクも使用することはできません。9 ～ 32 個のアクティブ リンクをサポートするには、スタンバイ リンクの使用を可能にする cLACP ダイナミック ポート プライオリティをディセーブルにする必要があります。 画面 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] が変更されました。
ASA 5585-X の 16 のクラスタ メンバのサポート	9.2(1)	ASA 5585-X が 16 ユニット クラスタをサポートするようになりました。 変更された ASDM 画面はありません。
ASA クラスタリングに対する BGP のサポート	9.3(1)	ASA クラスタリングに対する BGP のサポートが追加されました。 次の ASDM 画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [General]

PART 3

インターフェイス

基本的なインターフェイス コンフィギュレーション（ASA 5512-X 以降）

この章では、Cisco ASA 5512-X 以降のインターフェイス コンフィギュレーションを開始するためのタスクについて説明します。イーサネット設定、冗長インターフェイス、および EtherChannel の設定が含まれています。

（注） マルチ コンテキスト モードでは、この項のすべてのタスクをシステム実行スペースで実行してください。まだシステム実行スペースに入っていない場合は、[Configuration] > [Device List] ペイン内で、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。

ASA クラスタ インターフェイスについては、特別な要件があるため、第 9 章「ASA クラスタ」を参照してください。

ASA 5512-X 以降のインターフェイス コンフィギュレーションの開始に関する情報

Auto-MDI/MDIX 機能

RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレートケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。ギガビット イーサネットの速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常にイネーブルになり、ディセーブルにできません。

トランスペアレント モードのインターフェイス

トランスペアレント モードのインターフェイスは、「ブリッジ グループ」に属しており、ブリッジ グループはネットワークにつき 1 個です。コンテキストまたはシングル モードごとに、それぞれ 4 つのインターフェイスからなる最大 8 個のブリッジ グループを設定できます。ブリッジ グループの詳細については、「トランスペアレント モードのブリッジ グループ」（P.13-1）を参照してください。

管理インターフェイス

管理インターフェイスの概要

次のインターフェイスに接続して ASA を管理できます。

- 任意の通過トラフィック インターフェイス
- 専用の Management *Slot*/*Port* インターフェイス（使用しているモデルが対応している場合）

第 36 章「管理アクセス」の説明に従って、管理アクセスへのインターフェイスを設定する必要がある場合があります。

Management *Slot/Port* インターフェイス

表 10-1 に、モデルごとの管理インターフェイスを示します。

表 10-1　モデルごとの管理インターフェイス

モデル	Management 0/0[1]	Management 0/1	Management 1/0	Management 1/1	通過トラフィックに対して設定可能[2]	サブインターフェイスを使用可能
ASA 5512-X	**Yes**	No	No	No	No	No
ASA 5515-X	**Yes**	No	No	No	No	No
ASA 5525-X	**Yes**	No	No	No	No	No
ASA 5545-X	**Yes**	No	No	No	No	No
ASA 5555-X	**Yes**	No	No	No	No	No
ASA 5585-X	**Yes**	**Yes**	**Yes**[3]	**Yes**[3]	**Yes**	**Yes**
ASASM	No	No	No	No	該当なし	該当なし
ASAv	**Yes**	No	No	No	No	No

1. Management 0/0 インターフェイスは、デフォルトの出荷時のコンフィギュレーションの一部として、ASDM アクセス用に設定されています。詳細については、「工場出荷時のデフォルト設定」（P.2-15）を参照してください。
2. デフォルトでは、Management 0/0 インターフェイスは管理専用トラフィック用に設定されています。ルーテッド モードでサポートされるモデルの場合、制限を削除してトラフィックを通過させることができます。使用しているモデルに他の管理インターフェイスが含まれている場合、それを通過トラフィックにも使用できます。ただし、管理インターフェイスは通過トラフィックには最適化されていない場合があります。
3. SSP をスロット 1 に設置した場合は、Management 1/0 および 1/1 ではスロット 1 の SSP への管理アクセスのみが提供されます。

（注） モジュールをインストールした場合は、モジュール管理インターフェイスでは、モジュールの管理アクセスのみが提供されます。ASA 5512-X ～ ASA 5555-X では、ソフトウェア モジュールによって ASA と同じ物理的な Management 0/0 インターフェイスが使用されます。

管理専用トラフィックに対する任意のインターフェイスの使用

任意のインターフェイスを、管理トラフィック用として設定することによって管理専用インターフェイスとして使用できます。これには、EtherChannel インターフェイスも含まれます。

トランスペアレント モードの管理インターフェイス

トランスペアレント ファイアウォール モードでは、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、管理インターフェイス（物理インターフェイス、サブインターフェイス（使用しているモデルでサポートされている場合）、管理インターフェイスからなる EtherChannel インターフェイス（複数の管理インターフェイスがある場合）のいずれか）を個別の管理インターフェイスとして使用できます。他のインターフェイス タイプは管理インターフェイスとして使用できません。

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（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。コンテキスト単位で管理を行うには、管理インターフェイスのサブインターフェイスを作成し、管理サブインターフェイ

スを各コンテキストに割り当てます。ASA 5512-X ～ ASA 5555-X では、管理インターフェイスのサブインターフェイスは許可されないので、コンテキスト単位で管理を行うには、データ インターフェイスに接続する必要があります。

管理インターフェイスは、通常のブリッジ グループの一部ではありません。動作上の目的から、設定できないブリッジ グループの一部です。

（注）トランスペアレント ファイアウォール モードでは、管理インターフェイスによってデータ インターフェイスと同じ方法で MAC アドレス テーブルがアップデートされます。したがって、いずれかのスイッチ ポートをルーテッド ポートとして設定しない限り、管理インターフェイスおよびデータ インターフェイスを同じスイッチに接続しないでください（デフォルトでは、Catalyst スイッチがすべての VLAN スイッチ ポートの MAC アドレスを共有します）。そうしないと、物理的に接続されたスイッチから管理インターフェイスにトラフィックが到着すると、ASA によって、データ インターフェイスではなく、*管理*インターフェイスを使用してスイッチにアクセスするように MAC アドレス テーブルがアップデートされます。この処理が原因で、一時的にトラフィックが中断します。セキュリティ上の理由から、少なくとも 30 秒間は、スイッチからデータ インターフェイスへのパケットのために MAC アドレス テーブルが ASA によって再アップデートされることはありません。

冗長管理インターフェイスでのサポートなし

冗長インターフェイスは、Management *slot*/*port* インターフェイスをメンバとしてサポートしません。また、管理以外のインターフェイスで構成される冗長インターフェイスを、管理専用として設定することはできません。

ASA 5512-X ～ ASA 5555-X の Management 0/0 インターフェイス

ASA 5512-X ～ ASA 5555-X の Management 0/0 インターフェイスには、次の特性があります。

- 通過トラフィックはサポートされません。
- サブインターフェイスはサポートされません
- プライオリティ キューはサポートされません
- マルチキャスト MAC はサポートされません
- ソフトウェア モジュールは、Management 0/0 インターフェイスを共有します。ASA とモジュールのそれぞれに別の MAC アドレスと IP アドレスがサポートされます。モジュールのオペレーティング システムでモジュールの IP アドレスのコンフィギュレーションを実行する必要があります。ただし、物理特性（インターフェイスのイネーブル化など）は、ASA 上で設定されます。

冗長インターフェイス

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブ インターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定して ASA の信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものですが、必要な場合はデバイスレベルのフェールオーバーとともに冗長インターフェイスも設定できます。

冗長インターフェイスの MAC アドレス

冗長インターフェイスは、最初に追加された物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバー インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに MAC アドレスを割り当てることができます。これはメンバー インターフェイスの MAC アドレスに関係なく使用されます（「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）または「マルチ コンテキストの設定」（P.7-15）を参照）。アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーすると、トラフィックが中断しないように同じ MAC アドレスが維持されます。

EtherChannel

802.3ad EtherChannel は、単一のネットワークの帯域幅を増やすことができるように、個別のイーサネット リンク（チャネル グループ）のバンドルで構成される論理インターフェイスです（ポートチャネル インターフェイスと呼びます）。ポートチャネル インターフェイスは、インターフェイス関連の機能を設定するときに、物理インターフェイスと同じように使用します。

最大 48 個の EtherChannel を設定できます。

- 「チャネル グループのインターフェイス」（P.10-5）
- 「別のデバイスの EtherChannel への接続」（P.10-5）
- 「Link Aggregation Control Protocol」（P.10-6）
- 「ロード バランシング」（P.10-7）
- 「EtherChannel MAC アドレス」（P.10-7）

チャネル グループのインターフェイス

各チャネル グループは、最大 16 個のアクティブ インターフェイスを設定できます。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。16 個のアクティブ インターフェイスの場合、スイッチがこの機能をサポートしている必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。

チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

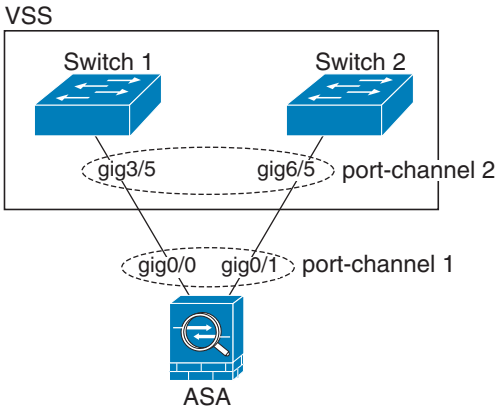
EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。インターフェイスは、送信元または宛先 MAC アドレス、IP アドレス、TCP および UDP ポート番号、および VLAN 番号に基づいて、専用のハッシュ アルゴリズムを使用して選択されます。

別のデバイスの EtherChannel への接続

ASA EtherChannel の接続先のデバイスも 802.3ad EtherChannel をサポートしている必要があります。たとえば、Catalyst 6500 スイッチまたは Cisco Nexus 7000 に接続できます。

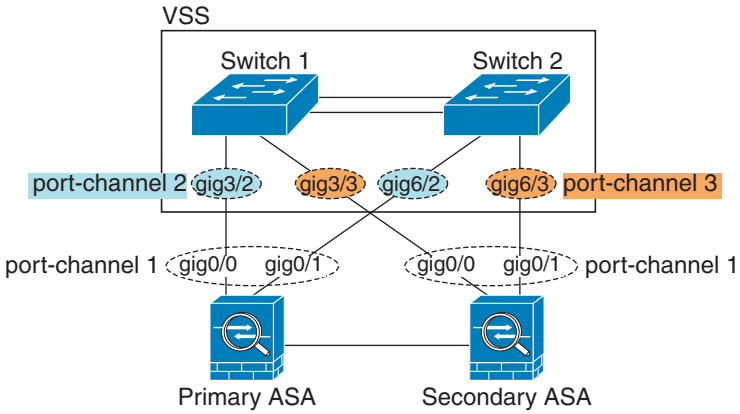
スイッチが仮想スイッチング システム（VSS）または 仮想ポート チャネル（vPC）の一部である場合、同じ EtherChannel 内の ASA インターフェイスを VSS/vPC 内の個別のスイッチに接続できます。個別のスイッチは単一のスイッチのように動作するため、スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです（図 10-1 を参照）。

図 10-1　　VSS/vPC への接続



ASA をアクティブ/スタンバイ フェールオーバー配置で使用する場合、ASA ごとに 1 つ、VSS/vPC 内のスイッチで個別の EtherChannel を作成する必要があります（図 10-1 を参照）。各 ASA で、1 つの EtherChannel が両方のスイッチに接続します。すべてのスイッチ インターフェイスを両方の ASA に接続する単一の EtherChannel にグループ化できる場合でも（この場合、個別の ASA システム ID のため、EtherChannel は確立されません）、単一の EtherChannel は望ましくありません。これは、トラフィックをスタンバイ ASA に送信しないようにするためです。

図 10-2　　アクティブ/スタンバイ フェールオーバーと VSS/vPC



Link Aggregation Control Protocol

Link Aggregation Control Protocol（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理インターフェイスを次のように設定できます。

- アクティブ：LACP 更新を送受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- パッシブ：LACP 更新を受信します。パッシブ EtherChannel は、アクティブ EtherChannel のみと接続を確立できます。
- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバー インターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

ロード バランシング

ASA は、パケットの送信元および宛先 IP アドレスをハッシュすることによって、パケットを EtherChannel 内のインターフェイスに分散します（この基準は設定可能です。「EtherChannel のカスタマイズ」（P.10-24）を参照してください）。生成されたハッシュをアクティブ リンクの数で割ったときの剰余（モジュロ演算）によってフローを行うインターフェイスが決まります。*hash_value* **mod** *active_links* の結果が 0 となるすべてのパケットは、EtherChannel 内の最初のインターフェイスへ送信され、以降は結果が 1 となるものは 2 番目のインターフェイスへ、結果が 2 となるものは 3 番目のインターフェイスへ、というように送信されます。たとえば、15 個のアクティブ リンクがある場合、モジュロ演算では 0 ～ 14 の値が得られます。6 個のアクティブ リンクの場合、値は 0 ～ 5 となり、以降も同様になります。

クラスタリングのスパンド EtherChannel では、ロード バランシングは ASA ごとに行われます。たとえば、8 台の ASA にわたるスパンド EtherChannel 内に 32 個のアクティブ インターフェイスがあり、EtherChannel 内の 1 台の ASA あたり 4 個のインターフェイスがある場合、ロード バランシングは 1 台の ASA の 4 個のインターフェイス間でのみ行われます。

アクティブ インターフェイスがダウンし、スタンバイ インターフェイスに置き換えられない場合、トラフィックは残りのリンク間で再バランスされます。失敗はレイヤ 2 のスパニングツリーとレイヤ 3 のルーティング テーブルの両方からマスクされるため、他のネットワーク デバイスへのスイッチオーバーはトランスペアレントです。

EtherChannel MAC アドレス

1 つのチャネル グループに含まれるすべてのインターフェイスは、同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。

ポート チャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アドレスとして使用します。または、ポートチャネル インターフェイスの MAC アドレスを手動で設定することもできます。マルチ コンテキスト モードでは、EtherChannel ポート インターフェイスを含め、固有の MAC アドレスをインターフェイスに自動的に割り当てることができます。グループ チャネル インターフェイスのメンバーシップを変更する場合は、固有の MAC アドレスを手動で設定するか、またはマルチ コンテキスト モードで自動的に設定することを推奨します。ポートチャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。

最大伝送単位および TCP 最大セグメント サイズのフラグメンテーションの制御

MTU の概要

最大伝送単位（MTU）は、ASA が特定のイーサネット インターフェイスで送信する最大フレーム ペイロード サイズを指定します。MTU の値は、イーサネット ヘッダー、FCS、VLAN タギングなどを*含まない*フレーム サイズです。イーサネット ヘッダーは 14 バイトで、FCS は 4 バイトです。MTU を 1500 に設定すると、予想されるフレーム サイズは、ヘッダーを含めて 1518 バイトです。VLAN タギングを使用する場合（追加の 4 バイトが付加されます）、MTU を 1500 に設定すると、予想されるフレーム サイズは 1522 です。これらのヘッダーに対応するために MTU 値を高く設定しないでください。カプセル化の TCP ヘッダーへの対応については、MTU 設定を変更するのではなく、TCP 最大セグメント サイズを変更してください（「TCP 最大セグメント サイズの概要」（P.10-9））。

出力 IP パケットが指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは送信先（場合によっては中継先）で組立て直されますが、フラグメント化はパフォーマンス低下の原因となります。したがってフラグメント化を避けるために、IP パケットを MTU サイズ以内に収める必要があります。

（注）　ASA はメモリに空きがある限り、設定された MTU よりも大きいフレームを受信します。大きなフレームに対応するためのメモリの増設については、「ジャンボ フレーム サポートのイネーブル化」（P.10-31）を参照してください。

デフォルト MTU

ASA のデフォルト MTU は、1500 バイトです。この値には、イーサネット ヘッダー、CRC、VLAN タギングなどのための 18 バイト以上は含まれません。

パス MTU ディスカバリ

ASA は、Path MTU Discovery（RFC 1191 に規定）をサポートします。つまり、2 台のホスト間のネットワーク パス内のすべてのデバイスで MTU を調整できます。したがってパスの最小 MTU の標準化が可能です。

MTU とジャンボ フレームの設定

「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）を参照してください。マルチ コンテキスト モードでは、各コンテキスト内で MTU を設定します。

「ジャンボ フレーム サポートのイネーブル化」（P.10-31）を参照してください。マルチ コンテキスト モードの場合、システム実行スペースでジャンボ フレーム サポートを設定します。

次のガイドラインを参照してください。

- トラフィック パスの MTU の一致 : すべての ASA インターフェイスとトラフィック パス内のその他のデバイスのインターフェイスでは、MTU が同じになるように設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボ フレームへの対応 : ジャンボ フレームをイネーブルにすると、MTU は 9198 バイトまで設定できます。

TCP 最大セグメント サイズの概要

TCP 最大セグメント サイズ（TCP MSS）とは、あらゆる TCP ヘッダーが追加される*前の* TCP ペイロードのサイズです。UDP パケットは影響を受けません。接続を確立するときのスリーウェイ ハンドシェイク中に、クライアントとサーバは TCP MSS 値を交換します。

ASA の TCP MSS を設定することもできます。いずれかのエンドポイント接続が ASA で設定されている値よりも大きな TCP MSS を要求した場合、ASA は要求パケットの TCP MSS を ASA の最大値で上書きします。ホストまたはサーバが TCP MSS を要求しない場合、ASA は RFC 793 のデフォルト値 536 バイトを想定しますが、パケットは変更しません。TCP の最小 MSS も設定できます。ホストまたはサーバが非常に小さい TCP MSS を要求した場合、ASA は値を調整します。デフォルトでは、最小 TCP MSS はイネーブルではありません。

たとえば、MTU を デフォルトの 1500 バイトに設定します。ホストが 1700 の MSS を要求します。ASA の最大 TCP MSS が 1380 の場合は、ASA は TCP 要求パケットの MSS 値を 1380 に変更します。サーバは、1380 バイトのパケットを送信します。

デフォルト TCP MSS

デフォルトでは、ASA の最大 TCP MSS は 1380 バイトです。このデフォルトは、最大 120 バイトのヘッダーを追加できる VPN 接続に対応しています。この値は、MTU の デフォルトの 1500 バイト内にも収まっています。

VPN および非 VPN トラフィックの TCP MSS の設定

「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）を参照してください。マルチ コンテキスト モードでは、各コンテキスト内で TCP MSS を設定します。

次のガイドラインを参照してください。

- 非 VPN トラフィック : VPN を使用せず、ヘッダーのための余分な領域を必要としない場合、TCP MSS 制限をディセーブルにし、接続エンドポイント間に確立された値を受け入れる必要があります。通常接続エンドポイントは MTU から TCP MSS を取得するため、非 VPN パケットは通常この TCP MSS を満たしています。
- VPN トラフィック : 最大 TCP MSS を MTU - 120 に設定します。たとえば、ジャンボ フレームを使用しており、MTU の値を高めに設定すると、TCP MSS も MTU に合わせて設定する必要があります。

ASA 5512-X 以降のインターフェイスのライセンス要件

モデル	ライセンス要件
ASA 5512-X	VLAN： 基本ライセンス：50 Security Plus ライセンス：100 すべての種類のインターフェイス： 基本ライセンス：716 Security Plus ライセンス：916
ASA 5515-X	VLAN： 基本ライセンス：100 すべての種類のインターフェイス： 基本ライセンス：916
ASA 5525-X	VLAN： 基本ライセンス：200 すべての種類のインターフェイス： 基本ライセンス：1316
ASA 5545-X	VLAN： 基本ライセンス：300 すべての種類のインターフェイス： 基本ライセンス：1716
ASA 5555-X	VLAN： 基本ライセンス：500 すべての種類のインターフェイス： 基本ライセンス：2516
ASA 5585-X	VLAN： 基本ライセンスと Security Plus ライセンス：1024 SSP-10 および SSP-20 のインターフェイス速度： 基本ライセンス：ファイバ インターフェイスの場合 1 ギガビット イーサネット 10 GE I/O ライセンス（Security Plus）：ファイバ インターフェイスの場合 10 ギガビット イーサネット （SSP-40 および SSP-60 は 10 ギガビット イーサネットをデフォルトでサポートします）。 すべての種類のインターフェイス： 基本ライセンスと Security Plus ライセンス：4612

（注）　VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。

すべてのタイプのインターフェイスには、VLAN、物理、冗長、ブリッジ グループ、EtherChannel インターフェイスなど、すべてを合わせたインターフェイスの最大数が含まれます。コンフィギュレーションで定義されているすべての **interface** が、この制限に対してカウントされます。

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

マルチ コンテキスト モードでは、「インターフェイス コンフィギュレーションの開始（ASA 5512-X 以降）」（P.10-14）に従って、システム実行スペースで物理インターフェイスを設定します。次に、第 12 章「ルーテッド モードのインターフェイス」または第 13 章「トランスペアレント モードのインターフェイス」に従って、コンテキスト実行スペースで論理インターフェイス パラメータを設定します。

ファイアウォール モードのガイドライン

- トランスペアレント モードでは、コンテキストごとに、またはシングル モードのデバイスに対して、最大 8 個のブリッジ グループを設定できます。
- 各ブリッジ グループには、最大 4 つのインターフェイスを含めることができます。
- マルチ コンテキストのトランスペアレント モードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。

フェールオーバーのガイドライン

- 冗長インターフェイスまたは EtherChannel インターフェイスをフェールオーバー リンクとして使用する場合、フェールオーバー ペアの両方の装置でその事前設定を行う必要があります。プライマリ装置で設定し、セカンダリ装置に複製されることは想定できません。これは、*複製にはフェールオーバー リンク自体が必要である*ためです。
- 冗長インターフェイスまたは EtherChannel インターフェイスをステート リンクに対して使用する場合、特別なコンフィギュレーションは必要ありません。コンフィギュレーションは通常どおりプライマリ装置から複製されます。
- 冗長インターフェイスまたは EtherChannel インターフェイスをモニタすると、フェールオーバーが発生したかどうかがわかります。アクティブなメンバー インターフェイスがスタンバイ インターフェイスにフェールオーバーした場合、デバイスレベルのフェールオーバーをモニタしているときには、冗長インターフェイスまたは EtherChannel インターフェイスで障害が発生しているように見えません。すべての物理インターフェイスで障害が発生した場合にのみ、冗長インターフェイスまたは EtherChannel インターフェイスで障害が発生しているように見えます（EtherChannel インターフェイスでは、障害の発生が許容されるメンバー インターフェイスの数を設定できます）。
- EtherChannel インターフェイスをフェールオーバー リンクまたはステート リンクに対して使用する場合、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバー リンクとして使用中の

EtherChannel の設定は変更できません。設定を変更するには、変更時に EtherChannel をシャットダウンするか、フェールオーバーを一時的にディセーブルにする必要があります。どちらの操作でも、その間はフェールオーバーは行われません。

- データ インターフェイスと、フェールオーバーまたはステートのインターフェイスを共有することはできません。

クラスタリングのガイドライン

- スパンド EtherChannel を設定するには、「スパンド EtherChannel の設定」（P.9-47）を参照してください。
- 個別クラスタ インターフェイスを設定するには、「個別インターフェイスの設定（管理インターフェイスの場合に推奨）」（P.9-44）を参照してください。

冗長インターフェイスのガイドライン

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- すべての ASA コンフィギュレーションは、メンバ物理インターフェイスではなく論理冗長インターフェイスを参照します。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを ASA 上で設定することができます。
- アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。
- 冗長インターフェイスは、Management *slot*/*port* インターフェイスをメンバとしてサポートしません。また、管理以外のインターフェイスで構成される冗長インターフェイスを、管理専用として設定することはできません。
- フェールオーバーのガイドラインについては、「フェールオーバーのガイドライン」（P.10-11）を参照してください。
- クラスタリングのガイドラインについては、「クラスタリングのガイドライン」（P.10-12）を参照してください。

EtherChannel のガイドライン

- 最大 48 個の EtherChannel を設定できます。
- 各チャネル グループは、最大 16 個のアクティブ インターフェイスを設定できます。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。
- チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。
- ASA EtherChannel の接続先のデバイスも 802.3ad EtherChannel をサポートしている必要があります。たとえば、Catalyst 6500 スイッチまたは Cisco Nexus 7000 スイッチに接続できます。

- ASA は、VLAN タグ付きの LACPDU をサポートしていません。Cisco IOS **vlan dot1Q tag native** コマンドを使用して、隣接スイッチのネイティブ VLAN タギングをイネーブルにすると ASA はタグ付きの LACPDU をドロップします。隣接スイッチのネイティブ VLAN タギングは、必ずディセーブルにしてください。マルチ コンテキスト モードでは、これらのメッセージはパケット キャプチャに含まれていないため、問題を効率的に診断できません。
- ASA は、スイッチ スタックへの EtherChannel の接続をサポートしていません。ASA EtherChannel がクロス スタックに接続されている場合、マスター スイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。
- すべての ASA コンフィギュレーションは、メンバ物理インターフェイスではなく論理 EtherChannel インターフェイスを参照します。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを ASA 上で設定することができます。
- フェールオーバーのガイドラインについては、「フェールオーバーのガイドライン」（P.10-11）を参照してください。
- クラスタリングのガイドラインについては、「クラスタリングのガイドライン」（P.10-12）を参照してください。

デフォルト設定

この項では、工場出荷時のデフォルト コンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。工場出荷時のデフォルト コンフィギュレーションに関する情報については、「工場出荷時のデフォルト設定」（P.2-15）を参照してください。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキスト モードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングル モードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。
- EtherChannel ポートチャネル インターフェイス：イネーブル。ただし、トラフィックが EtherChannel を通過するためには、チャネル グループ物理インターフェイスもイネーブルになっている必要があります。

デフォルトの速度および二重通信

- デフォルトでは、銅線（RJ-45）インターフェイスの速度と二重通信は、オート ネゴシエーションに設定されます。
- 5585-X のファイバ インターフェイスでは、自動リンク ネゴシエーションの速度が設定されます。

デフォルトのコネクタ タイプ

一部のモデルは、銅線 RJ-45 とファイバ SFP の 2 種類のコネクタを備えています。RJ-45 がデフォルトです。ASA を設定すると、ファイバ SFP コネクタを使用できます。

デフォルトの MAC アドレス

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。

インターフェイス コンフィギュレーションの開始（ASA 5512-X 以降）

インターフェイス コンフィギュレーションを開始するためのタスク フロー

（注）　既存のコンフィギュレーションがあり、使用中のインターフェイスを冗長インターフェイスまたは EtherChannel インターフェイスに変換する場合は、CLI を使用してコンフィギュレーションをオフラインで実行し、切断を最小限にします。「使用中のインターフェイスの冗長インターフェイスまたは EtherChannel インターフェイスへの変換」（P.10-32）を参照してください。

インターフェイス コンフィギュレーションを開始するには、次の手順を実行します。

ステップ 1　（マルチ コンテキスト モード）この項のタスクはすべてシステム実行スペースで実行します。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は、[Configuration] > [Device List] ペイン内で、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　物理インターフェイスをイネーブルにし、必要に応じてイーサネット パラメータを変更します。「物理インターフェイスのイネーブル化およびイーサネット パラメータの設定」（P.10-15）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ディセーブルになっています。

ステップ 3　（オプション）冗長インターフェイス ペアを設定します。「冗長インターフェイスの設定」（P.10-18）を参照してください。

論理冗長インターフェイスは、アクティブとスタンバイの物理インターフェイスからなるペアです。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。

ステップ 4　（オプション）EtherChannel を設定します。「EtherChannel の設定」（P.10-22）を参照してください。

EtherChannel によって、複数のイーサネット インターフェイスが 1 つの論理インターフェイスにグループ化されます。

ステップ 5　（オプション）VLAN サブインターフェイスを設定します。「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.10-28）を参照してください。

ステップ 6　（オプション）「ジャンボ フレーム サポートのイネーブル化」（P.10-31）に従って、ジャンボ フレームのサポートをイネーブルにします。

ステップ 7　（マルチ コンテキスト モードのみ）システム実行スペースでインターフェイス コンフィギュレーションを実行するには、第 7 章「マルチ コンテキスト モード」に記載されている次のタスクを実行します。

- インターフェイスをコンテキストに割り当てるには、「セキュリティ コンテキストの設定」（P.7-20）を参照してください。
- （オプション）固有の MAC アドレスをコンテキスト インターフェイスに自動的に割り当てるには、「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」（P.7-25）を参照してください。

MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。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。また、「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）に従って、コンテキスト内の MAC アドレスを手動で割り当てることもできます。

ステップ 8　第 12 章「ルーテッド モードのインターフェイス」または第 13 章「トランスペアレント モードのインターフェイス」に従って、インターフェイス コンフィギュレーションを実行します。

物理インターフェイスのイネーブル化およびイーサネット パラメータの設定

ここでは、次の方法について説明します。

- 物理インターフェイスをイネーブルにする。
- 特定の速度と二重通信（使用できる場合）を設定する。
- フロー制御のポーズ フレームのイネーブル化

前提条件

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。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は、[Configuration] > [Device List] ペイン内で、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。

手順の詳細

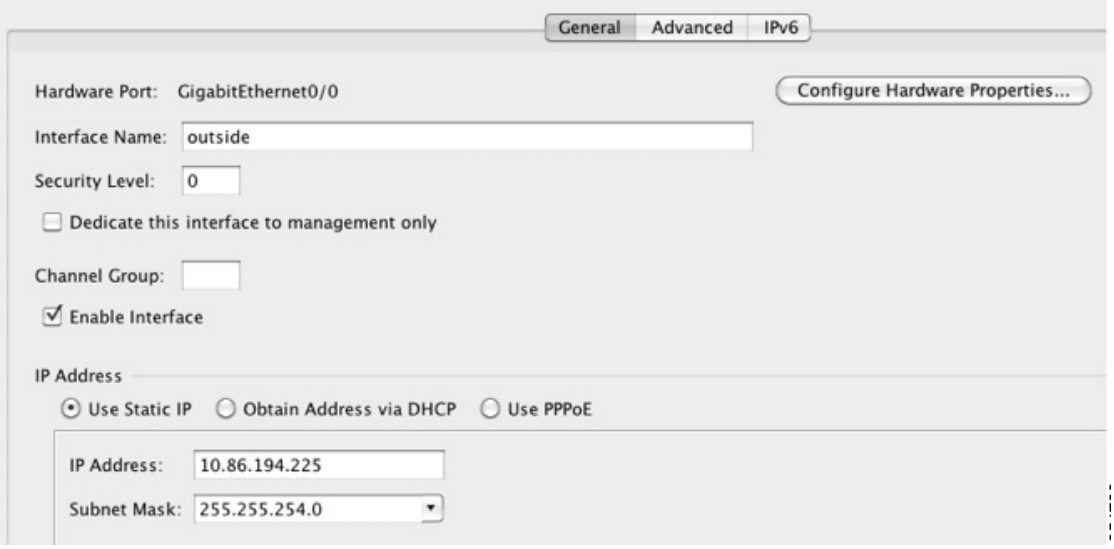
ステップ 1　コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

デフォルトでは、すべての物理インターフェイスが一覧表示されます。

ステップ 2　設定する物理インターフェイスをクリックし、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。



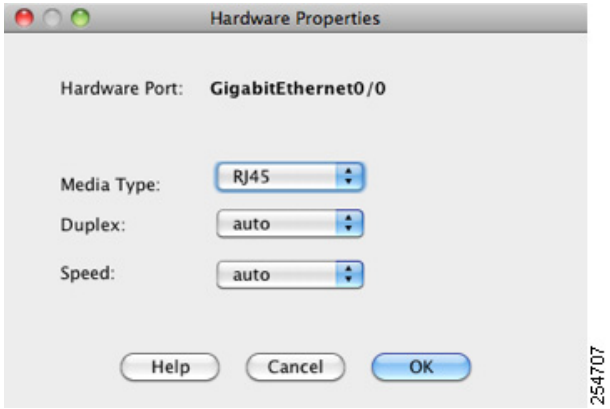
（注）　シングル モードの場合、この手順では [Edit Interface] ダイアログボックスでのパラメータのサブセットのみを対象としています。他のパラメータを設定する場合は、第 12 章「ルーテッド モードのインターフェイス」または第 13 章「トランスペアレント モードのインターフェイス」を参照してください。マルチ コンテキスト モードの場合、インターフェイス コンフィギュレーションを行う前に、インターフェイスをコンテキストに割り当てる必要があることに注意してください。「マルチ コンテキストの設定」（P.7-15）を参照してください。

ステップ 3　インターフェイスをイネーブルにするには、[Enable Interface] チェックボックスをオンにします。

ステップ 4　説明を追加するには、[Description] フィールドにテキストを入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 5　（オプション）メディア タイプ、二重通信、速度を設定し、フロー制御のポーズ フレームをイネーブルにするには、[Configure Hardware Properties] をクリックします。



a. インターフェイス タイプに応じて、[Media Type] ドロップダウン リストから [RJ-45] または [SFP] のいずれかを選択できます。

RJ-45 がデフォルトです。

b. RJ-45 インターフェイスに二重通信を設定するには、[Duplex] ドロップダウン リストからインターフェイス タイプに応じて [Full]、[Half]、または [Auto] を選択します。

（注） EtherChannel インターフェイスの二重通信の設定は [Full] または [Auto] である必要があります。

c. 速度を設定するには、[Speed] ドロップダウン リストから値を選択します。

使用できる速度は、インターフェイス タイプによって異なります。SFP インターフェイスでは、速度を [Negotiate] または [Nonegotiate] に設定できます。[Negotiate]（デフォルト）ではリンク ネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。[Nonegotiate] では、リンク パラメータのネゴシエーションを行いません。RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。「Auto-MDI/MDIX 機能」（P.10-2）を参照してください。

d. 1 ギガビット イーサネット インターフェイスおよび 10 ギガビット イーサネット インターフェイスでフロー制御のポーズ（XOFF）フレームをイネーブルにするには、[Enable Pause Frame] チェックボックスをオンにします。

トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズ フレームをイネーブルにすると、このような問題の発生を抑制できます。ポーズ（XOFF）および XON フレームは、FIFO バッファ使用量に基づいて、NIC ハードウェアによって自動的に生成されます。バッファ使用量が高ウォーターマークを超えると、ポーズ フレームが送信されます。デフォルトの *high_water* 値は 128 KB（10 ギガビット イーサネット）および 24 KB（1 ギガビット イーサネット）です。0 ～ 511（10 ギガビット イーサネット）または 0 ～ 47 KB（1 ギガビット イーサネット）に設定でき

ます。ポーズの送信後、バッファ使用量が低ウォーター マークよりも下回ると、XON フレームを送信できます。デフォルトでは、*low_water* 値は 64 KB（10 ギガビット イーサネット）および 16 KB（1 ギガビット イーサネット）です。0 ～ 511（10 ギガビット イーサネット）または 0 ～ 47 KB（1 ギガビット イーサネット）に設定できます。リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のタイマー値によって制御されます。デフォルトの *pause_time* 値は 26624 です。この値は 0 ～ 65535 に設定できます。バッファの使用量が継続的に高基準値を超えている場合は、ポーズ リフレッシュのしきい値に指定された間隔でポーズ フレームが繰り返し送信されます。

[Low Watermark]、[High Watermark]、[Pause Time] のデフォルト値を変更するには、[Use Default Values] チェックボックスをオフにします。

（注） 802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティベースのフロー制御はサポートされていません。

e. [OK] をクリックして [Hardware Properties] の変更を受け入れます。

ステップ 6　[OK] をクリックして [Interface] の変更を受け入れます。

次の作業

オプション タスク：

- 冗長インターフェイス ペアを設定します。「冗長インターフェイスの設定」（P.10-18）を参照してください。
- EtherChannel を設定します。「EtherChannel の設定」（P.10-22）を参照してください。
- VLAN サブインターフェイスを設定します。「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.10-28）を参照してください。
- ジャンボ フレーム サポートを設定します。「ジャンボ フレーム サポートのイネーブル化」（P.10-31）を参照してください。

必須タスク：

- マルチ コンテキスト モードの場合は、インターフェイスをコンテキストに割り当てます（固有の MAC アドレスがコンテキスト インターフェイスに自動的に割り当てられます）。「マルチ コンテキストの設定」（P.7-15）を参照してください。
- シングル コンテキスト モードの場合は、インターフェイス コンフィギュレーションを実行します。第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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。

冗長インターフェイスの設定

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブ インターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定して ASA の信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものですが、必要な場合はフェールオーバーとともに冗長インターフェイスも設定できます。

この項では、冗長インターフェイスを設定する方法について説明します。

- 「冗長インターフェイスの設定」（P.10-19）
- 「アクティブ インターフェイスの変更」（P.10-21）

冗長インターフェイスの設定

この項では、冗長インターフェイスを作成する方法について説明します。デフォルトでは、冗長インターフェイスはイネーブルになっています。

注意事項と制約事項

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- 冗長インターフェイス遅延値は設定可能ですが、デフォルトでは、ASA はそのメンバー インターフェイスの物理タイプに基づくデフォルトの遅延値を継承します。
- 「冗長インターフェイスのガイドライン」（P.10-12）も参照してください。

前提条件

- 両方のメンバー インターフェイスが同じ物理タイプである必要があります。たとえば、両方ともギガビット イーサネットにする必要があります。
- 名前が設定されている場合は、物理インターフェイスを冗長インターフェイスに追加できません。最初に、[Configuration] > [Device Setup] > [Interfaces] ペインで名前を削除する必要があります。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。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は、[Configuration] > [Device List] ペイン内で、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。

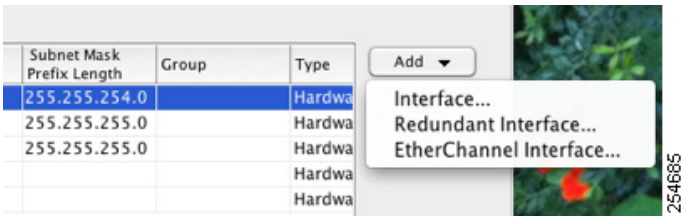
注意　コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

手順の詳細

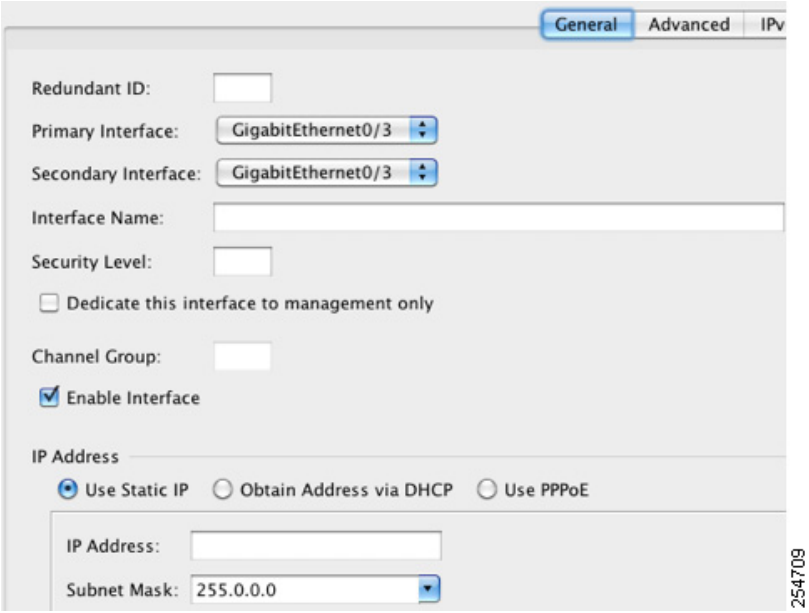
ステップ 1　コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

ステップ 2　[Add] > [Redundant Interface] を選択します。



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



（注） シングル モードの場合、この手順では [Edit Redundant Interface] ダイアログボックスでのパラメータのサブセットのみを対象としています。他のパラメータを設定する場合は、第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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 モードの場合、インターフェイス コンフィギュレーションを行う前に、インターフェイスをコンテキストに割り当てる必要があることに注意してください。「マルチ コンテキストの設定」（P.7-15）を参照してください。

ステップ 3　[Redundant ID] フィールドで、1 ～ 8 の整数を入力します。

ステップ 4　[Primary Interface] ドロップダウン リストから、プライマリにする物理インターフェイスを選択します。

サブインターフェイスを持たず、まだ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を必ず選択してください。冗長インターフェイスは、Management *slot/port* インターフェイスをメンバとしてサポートしません。

ステップ 5　[Secondary Interface] ドロップダウン リストから、セカンダリにする物理インターフェイスを選択します。

ステップ 6　インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

インターフェイスはデフォルトでイネーブルになっています。ディセーブルにするには、このチェックボックスをオフにします。

ステップ 7　説明を追加するには、[Description] フィールドにテキストを入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。フェールオーバーまたはステート リンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 8　[OK] をクリックします。

[Interfaces] ペインに戻ります。メンバー インターフェイスで、基本パラメータのみが設定できることを示すロックが、インターフェイス ID の左側に表示されます。冗長インターフェイスがテーブルに追加されます。

GigabitEthernet0/2	Enabled	No	Redundant8	Hardware	native
GigabitEthernet0/3	Enabled	No		Hardware	native
GigabitEthernet0/3.10	Enabled	No		Logical	vlan100
GigabitEthernet0/3.11	Enabled	No		Logical	vlan11
Management0/0	Enabled	No		Hardware	native
Redundant8	Enabled	Yes		Logical	native

254710

次の作業

オプション タスク：

- VLAN サブインターフェイスを設定します。「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.10-28）を参照してください。
- ジャンボ フレーム サポートを設定します。「ジャンボ フレーム サポートのイネーブル化」（P.10-31）を参照してください。

必須タスク：

- マルチ コンテキスト モードの場合は、インターフェイスをコンテキストに割り当てます（固有の MAC アドレスがコンテキスト インターフェイスに自動的に割り当てられます）。「マルチ コンテキストの設定」（P.7-15）を参照してください。
- シングル コンテキスト モードの場合は、インターフェイス コンフィギュレーションを実行します。第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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。

アクティブ インターフェイスの変更

デフォルトでは、コンフィギュレーションで最初にリストされているインターフェイスが（使用可能であれば）、アクティブ インターフェイスになります。どのインターフェイスがアクティブかを表示するには、[Tools] > [Command Line Interface tool] で次のコマンドを入力します。

```
show interface redundantnumber detail | grep Member
```

次に例を示します。

```
show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

アクティブ インターフェイスを変更するには、次のコマンドを入力します。

```
redundant-interface redundantnumber active-member physical_interface
```

redundant *number* 引数には、冗長インターフェイス ID（**redundant1** など）を指定します。

physical_interface には、アクティブにするメンバー インターフェイスの ID を指定します。

EtherChannel の設定

ここでは、EtherChannel ポートチャネル インターフェイスの作成、インターフェイスの EtherChannel への割り当て、EtherChannel のカスタマイズ方法について説明します。

- 「EtherChannel へのインターフェイスの追加」（P.10-22）
- 「EtherChannel のカスタマイズ」（P.10-24）

EtherChannel へのインターフェイスの追加

ここでは、EtherChannel ポートチャネル インターフェイスを作成し、インターフェイスを EtherChannel に割り当てる方法について説明します。デフォルトでは、ポートチャネル インターフェイスはイネーブルになっています。

注意事項と制約事項

- 最大 48 個の EtherChannel を設定できます。
- 各チャネル グループは、最大 16 個のアクティブ インターフェイスを設定できます。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。
- クラスタリング用にスパンド EtherChannel を設定するには、この手順の代わりに「スパンド EtherChannel の設定」（P.9-47）を参照してください。
- 「EtherChannel のガイドライン」（P.10-12）も参照してください。

前提条件

- チャネル グループのすべてのインターフェイスは、同じタイプ、速度、および二重通信である必要があります。半二重はサポートされません。
- 名前が設定されている場合は、物理インターフェイスをチャネル グループに追加できません。最初に、[Configuration] > [Device Setup] > [Interfaces] ペインで名前を削除する必要があります。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。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は、[Configuration] > [Device List] ペイン内で、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。

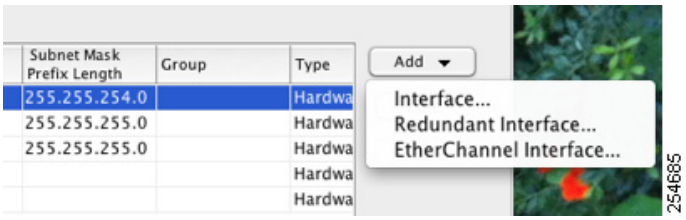
注意　コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

手順の詳細

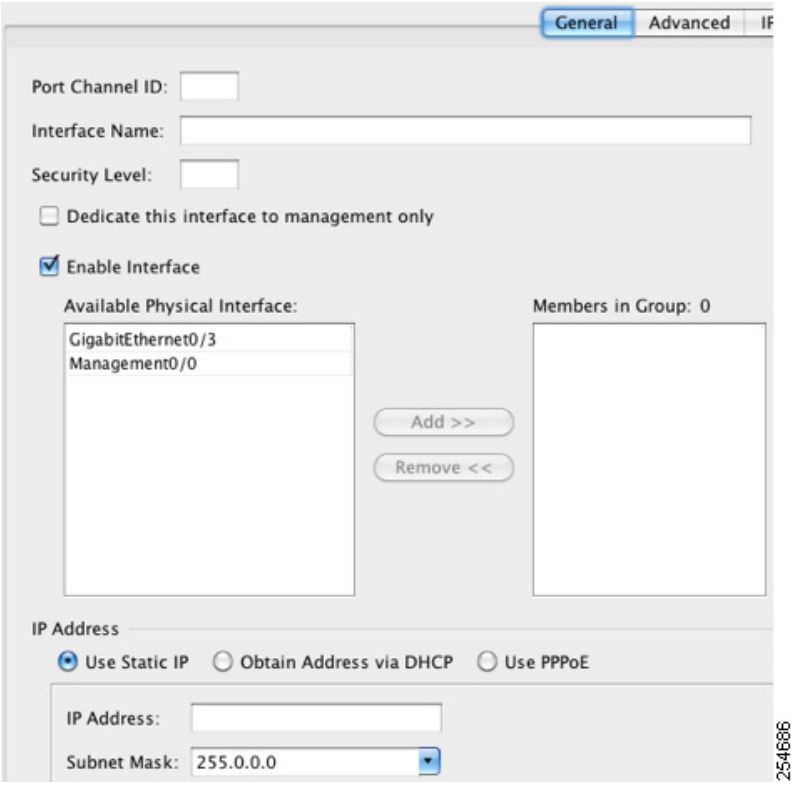
ステップ 1　コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

ステップ 2　[Add] > [EtherChannel Interface] を選択します。



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



（注） シングル モードの場合、この手順では [Edit EtherChannel Interface] ダイアログボックスでのパラメータのサブセットのみを対象としています。他のパラメータを設定する場合は、第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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 モードの場合、インターフェイス コンフィギュレーションを行う前に、インターフェイスをコンテキストに割り当てる必要があることに注意してください。「マルチ コンテキストの設定」（P.7-15）を参照してください。

ステップ 3　[Port Channel ID] フィールドに 1 ～ 48 の範囲の数値を入力します。

ステップ 4　[Available Physical Interface] 領域で、インターフェイスをクリックし、[Add >>] をクリックしてそれを [Members in Group] 領域に移動します。

トランスペアレント モードで、複数の管理インターフェイスがあるチャネル グループを作成する場合は、この EtherChannel を管理専用インターフェイスとして使用できます。

（注）　EtherChannel モードをオンに設定する場合、最初はインターフェイスを 1 個のみ含める必要があります。この手順を完了後、メンバー インターフェイスを編集し、このモードをオンに設定します。変更を適用し、EtherChannel を編集してメンバー インターフェイスをさらに追加します。

ステップ 5　チャネル グループに追加するインターフェイスごとに繰り返します。

すべてのインターフェイスが同じタイプと速度であるようにします。最初に追加するインターフェイスによって、EtherChannel のタイプと速度が決まります。一致しないインターフェイスを追加すると、そのインターフェイスは停止状態になります。ASDM では、一致しないインターフェイスの追加は防止されません。

ステップ 6　[OK] をクリックします。

[Interfaces] ペインに戻ります。メンバー インターフェイスで、基本パラメータのみが設定できることを示すロックが、インターフェイス ID の左側に表示されます。EtherChannel インターフェイスがテーブルに追加されます。

ステップ 7　[Apply] をクリックします。すべてのメンバー インターフェイスは自動的にイネーブルになります。

次の作業

オプション タスク：

- EtherChannel インターフェイスをカスタマイズします。「EtherChannel のカスタマイズ」（P.10-24）を参照してください。
- VLAN サブインターフェイスを設定します。「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.10-28）を参照してください。

必須タスク：

- マルチ コンテキスト モードの場合は、インターフェイスをコンテキストに割り当てます（固有の MAC アドレスがコンテキスト インターフェイスに自動的に割り当てられます）。「マルチ コンテキストの設定」（P.7-15）を参照してください。
- シングル コンテキスト モードの場合は、インターフェイス コンフィギュレーションを実行します。第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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。

EtherChannel のカスタマイズ

この項では、EtherChannel のインターフェイスの最大数、EtherChannel をアクティブにするための動作インターフェイスの最小数、ロード バランシング アルゴリズム、およびその他のオプション パラメータを設定する方法について説明します。

手順の詳細

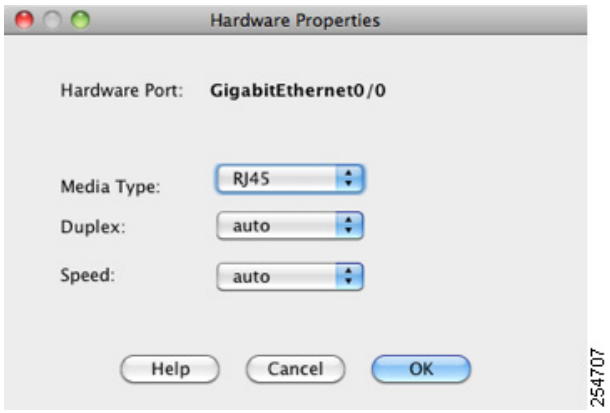
ステップ 1　コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

ステップ 2　カスタマイズするポートチャネル インターフェイスをクリックし、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。

ステップ 3　すべてのメンバー インターフェイスについて、メディア タイプ、二重通信、速度、およびフロー制御のポーズ フレームを上書きするには、[Configure Hardware Properties] をクリックします。これらのパラメータはチャネル グループのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。



a.　インターフェイス タイプに応じて、[Media Type] ドロップダウン リストから [RJ-45] または [SFP] のいずれかを選択できます。

RJ-45 がデフォルトです。

b.　RJ-45 インターフェイスに二重通信を設定するには、[Duplex] ドロップダウン リストからインターフェイス タイプに応じて [Full] または [Auto] を選択します。EtherChannel では [Half] はサポートされません。

c.　速度を設定するには、[Speed] ドロップダウン リストから値を選択します。

使用できる速度は、インターフェイス タイプによって異なります。SFP インターフェイスでは、速度を [Negotiate] または [Nonegotiate] に設定できます。[Negotiate]（デフォルト）ではリンク ネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。[Nonegotiate] では、リンク パラメータのネゴシエーションを行いません。RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。「Auto-MDI/MDIX 機能」（P.10-2）を参照してください。

d.　1 ギガビット イーサネット インターフェイスおよび 10 ギガビット イーサネット インターフェイスでフロー制御のポーズ（XOFF）フレームをイネーブルにするには、[Enable Pause Frame] チェックボックスをオンにします。

トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズ フレームをイネーブルにすると、このような問題の発生を抑制できます。ポーズ（XOFF）および XON フレームは、FIFO バッファ使用量に基づい

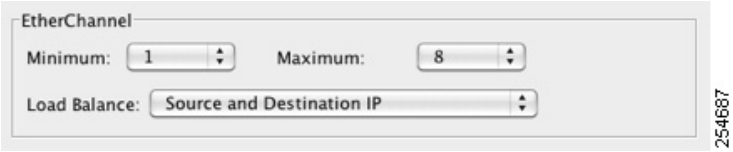
て、NIC ハードウェアによって自動的に生成されます。バッファ使用量が最高水準点を超えると、ポーズ フレームが送信されます。デフォルト値は 128 KB です。この値は 0 ～ 511 に設定できます。ポーズの送信後、バッファ使用量が最低水準点よりも下回ると、XON フレームを送信できます。デフォルトでは、この値は 64 KB です。この値は 0 ～ 511 に設定できます。リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のポーズ時間の値によって制御されます。デフォルト値は 26624 です。この値は 0 ～ 65535 に設定できます。バッファの使用量が継続的に最高水準点を超えている場合は、ポーズ リフレッシュのしきい値に指定された間隔でポーズ フレームが繰り返し送信されます。

[Low Watermark]、[High Watermark]、[Pause Time] のデフォルト値を変更するには、[Use Default Values] チェックボックスをオフにします。

（注）　802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティベースのフロー制御はサポートされていません。

e. [OK] をクリックして [Hardware Properties] の変更を受け入れます。

ステップ 4　EtherChannel をカスタマイズするには、[Advanced] タブをクリックします。



a. [EtherChannel] 領域で、[Minimum] ドロップダウン リストから、EtherChannel をアクティブにするために必要なアクティブ インターフェイスの最小数を 1 ～ 16 の範囲で選択します。デフォルトは 1 です。

b. [Maximum] ドロップダウン リストから、EtherChannel で許可されるアクティブ インターフェイスの最大数を 1 ～ 16 の範囲で選択します。デフォルト値は 16 です。スイッチが 16 個のアクティブ インターフェイスをサポートしていない場合、このコマンドは必ず 8 以下に設定する必要があります。

c. [Load Balance] ドロップダウン リストから、パケットをグループ チャネル インターフェイス間でロード バランスするために使用する基準を選択します。デフォルトでは、ASA はパケットの送信元および宛先 IP アドレスに従って、インターフェイスでのパケットのロードをバランスします。パケットが分類される基準になるプロパティを変更する場合は、別の基準のセットを選択します。たとえば、トラフィックが同じ送信元および宛先 IP アドレスに大きく偏っている場合、EtherChannel 内のインターフェイスに対するトラフィックの割り当てがアンバランスになります。別のアルゴリズムに変更すると、トラフィックはより均等に分散される場合があります。ロード バランシングの詳細については、「ロード バランシング」（P.10-7）を参照してください。

ステップ 5　[OK] をクリックします。

[Interfaces] ペインに戻ります。

ステップ 6　チャネル グループ内の物理インターフェイスのモードおよびプライオリティを設定するには、次の手順を実行します。

a. [Interfaces] テーブルで物理インターフェイスを選択し、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。

b. [Advanced] タブをクリックします。

c. [EtherChannel] 領域で、[Mode] ドロップダウン リストから、[Active]、[Passive]、または [On] を選択します。[Active] モード（デフォルト）を使用することを推奨します。アクティブ、パッシブ、およびオンの各モードの詳細については、「Link Aggregation Control Protocol」（P.10-6）を参照してください。

d. [LACP Port Priority] フィールドで、ポート プライオリティを 1 ～ 65535 の範囲で設定します。デフォルト値は 32768 です。数字が大きいほど、プライオリティは低くなります。使用可能な数よりも多くのインターフェイスを割り当てた場合、ASA ではこの設定を使用して、アクティブ インターフェイスとスタンバイ インターフェイスを決定します。ポート プライオリティ設定がすべてのインターフェイスで同じ場合、プライオリティはインターフェイス ID（スロット/ポート）で決まります。最も小さいインターフェイス ID が、最も高いプライオリティになります。たとえば、GigabitEthernet 0/0 のプライオリティは GigabitEthernet 0/1 よりも高くなります。

あるインターフェイスについて、インターフェイス ID は大きいが、そのインターフェイスがアクティブになるように優先順位を付ける場合は、より小さい値を持つようにこのコマンドを設定します。たとえば、GigabitEthernet 1/3 を GigabitEthernet 0/7 よりも前にアクティブにするには、1/3 インターフェイスでプライオリティ値を 12345 にして、0/7 インターフェイスでデフォルトの 32768 にします。

EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。システム プライオリティを設定するには、ステップ 9 を参照してください。

ステップ 7　[OK] をクリックします。

[Interfaces] ペインに戻ります。

ステップ 8　[Apply] をクリックします。

ステップ 9　LACP システム プライオリティを設定するには、次の手順を実行します。EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。詳細については、ステップ 6dを参照してください。

a. コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [EtherChannel] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [EtherChannel] ペインを選択します。

b. [LACP System Priority] フィールドに、プライオリティを 1 ～ 65535 の範囲で入力します。

デフォルト値は 32768 です。

次の作業

オプション タスク：

- VLAN サブインターフェイスを設定します。「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.10-28）を参照してください。
- ジャンボ フレーム サポートを設定します。「ジャンボ フレーム サポートのイネーブル化」（P.10-31）を参照してください。

必須タスク：

- マルチ コンテキスト モードの場合は、インターフェイスをコンテキストに割り当てます（固有の MAC アドレスがコンテキスト インターフェイスに自動的に割り当てられます）。「マルチ コンテキストの設定」（P.7-15）を参照してください。
- シングル コンテキスト モードの場合は、インターフェイス コンフィギュレーションを実行します。第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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。

VLAN サブインターフェイスと 802.1Q トランキングの設定

サブインターフェイスを使用すると、1 つの物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたは ASA を追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。この機能は、各コンテキストに固有のインターフェイスを割り当てることができるので、マルチ コンテキスト モードで特に便利です。

注意事項と制約事項

- 最大サブインターフェイス数：使用するモデルで許容される VLAN サブインターフェイス数を決定するには、「ASA 5512-X 以降のインターフェイスのライセンス要件」（P.10-10）を参照してください。
- 物理インターフェイス上のタグなしパケットの禁止：サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。この特性は、冗長インターフェイス ペアのアクティブな物理インターフェイスと EtherChannel リンクにも当てはまります。トラフィックがサブ インターフェイスを通過するには、物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスがイネーブルになっている必要があるため、トラフィックが物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスを通過しないように、インターフェイスには名前を設定しないでください。物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスでタグのないパケットを通過させる場合は、通常通り name コマンドをに設定できます。インターフェイス コンフィギュレーションの詳細については、第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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。
- （ASA 5512-X ～ ASA 5555-X）サブインターフェイスは Management 0/0 インターフェイスでは設定できません。
- ASA はダイナミック トランキング プロトコル（DTP）をサポートしないため、接続されているスイッチ ポートを無条件にトランキングするように設定する必要があります。

前提条件

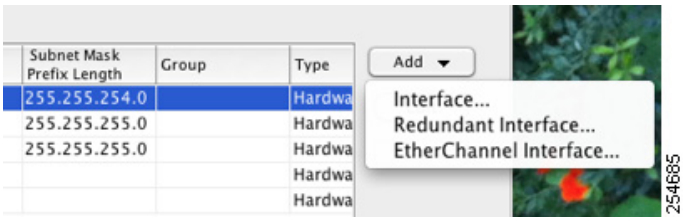
マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペイン内で、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順の詳細

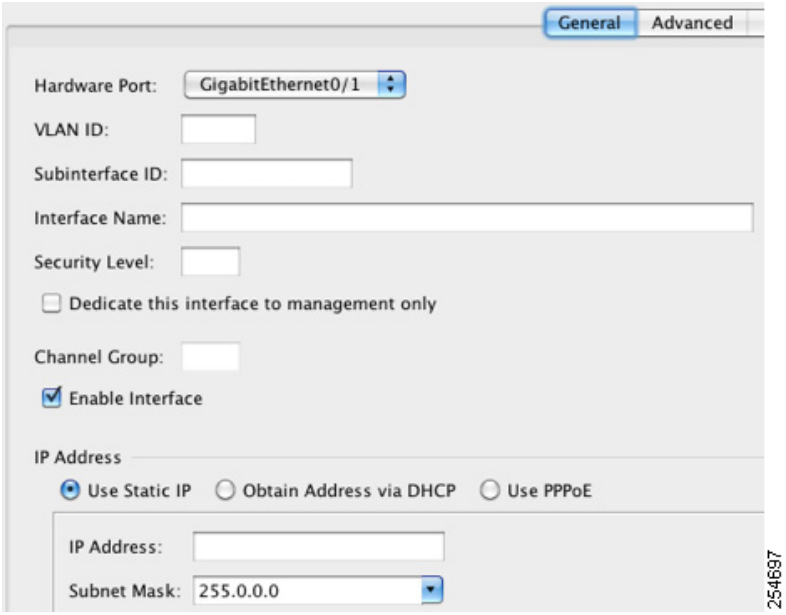
ステップ 1　コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

ステップ 2　[Add] > [Interface] を選択します。



[Add Interface] ダイアログボックスが表示されます。



（注）　シングル モードの場合、この手順では [Edit Interface] ダイアログボックスでのパラメータのサブセットのみを対象としています。他のパラメータを設定する場合は、第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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 モードの場合、インターフェイス コンフィギュレーションを行う前に、インターフェイスをコンテキストに割り当てる必要があることに注意してください。「マルチ コンテキストの設定」（P.7-15）を参照してください。

ステップ 3　[Hardware Port] ドロップダウン リストから、サブインターフェイスを追加する物理インターフェイス、冗長インターフェイス、またはポートチャネル インターフェイスを選択します。

ステップ 4　インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

インターフェイスはデフォルトでイネーブルになっています。ディセーブルにするには、このチェックボックスをオフにします。

ステップ 5　[VLAN ID] フィールドに、1 ～ 4095 の VLAN ID を入力します。

一部の VLAN ID は接続スイッチ用に予約されている場合があります。詳細 については、スイッチのマニュアルを確認してください。マルチ コンテキスト モードの場合、VLAN はシステム設定でしか設定できません。

ステップ 6　[Subinterface ID] フィールドに、サブインターフェイス ID を 1 ～ 4294967293 の整数で入力します。

許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。

ステップ 7　（オプション）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。フェールオーバーまたはステート リンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 8　[OK] をクリックします。

[Interfaces] ペインに戻ります。

次の作業

オプション タスク：

- ジャンボ フレーム サポートを設定します。「ジャンボ フレーム サポートのイネーブル化」（P.10-31）を参照してください。

必須タスク：

- マルチ コンテキスト モードの場合は、インターフェイスをコンテキストに割り当てます（固有の MAC アドレスがコンテキスト インターフェイスに自動的に割り当てられます）。「マルチ コンテキストの設定」（P.7-15）を参照してください。
- シングル コンテキスト モードの場合は、インターフェイス コンフィギュレーションを実行します。第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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。

ジャンボ フレーム サポートのイネーブル化

ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび FCS を含む）より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネット フレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能（ACL など）の最大使用量が制限される場合があります。詳細については、「最大伝送単位および TCP 最大セグメント サイズのフラグメンテーションの制御」（P.10-8）を参照してください。

前提条件

- マルチ コンテキスト モードでは、システム実行スペースでこのオプションを設定します。
- この設定を変更した場合は、ASA のリロードが必要です。
- ジャンボ フレームを送信する必要があるインターフェイスごとに MTU を必ず設定してください。MTU は、デフォルト値の 1500 よりも大きい値（たとえば 9198）に設定します。「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）を参照してください。マルチ コンテキスト モードでは、各コンテキスト内で MTU を設定します。
- TCP MSS は、非 VPN トラフィックについてディセーブルにするか、または「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）に従って MTU に応じて増加するように調整する必要があります。

手順の詳細

- マルチ モード：ジャンボ フレーム サポートをイネーブルにするには、[Configuration] > [Context Management] > [Interfaces] を選択し、[Enable jumbo frame support] チェックボックスをオンにします。
- シングル モード：1500 バイトを超える MTU を設定すると、ジャンボ フレームが自動的にイネーブルになります。この設定を手動でイネーブルまたはディセーブルにするには、[Configuration] > [Device Setup] > [Interfaces] を選択し、[Enable jumbo frame support] チェックボックスをオンにします。

次の作業

- マルチ コンテキスト モードの場合は、インターフェイスをコンテキストに割り当てます（固有の MAC アドレスがコンテキスト インターフェイスに自動的に割り当てられます）。「マルチ コンテキストの設定」（P.7-15）を参照してください。
- シングル コンテキスト モードの場合は、インターフェイス コンフィギュレーションを実行します。第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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。

使用中のインターフェイスの冗長インターフェイスまたは EtherChannel インターフェイスへの変換

既存のコンフィギュレーションがあり、現在使用中のインターフェイスに対して冗長インターフェイスまたは EtherChannel インターフェイス機能を利用する場合は、論理インターフェイスに変換するときにある程度のダウンタイムが発生します。

ここでは、既存のインターフェイスを冗長インターフェイスまたは EtherChannel インターフェイスに最小限のダウンタイムで変換する方法の概要について説明します。詳細については、「冗長インターフェイスの設定」（P.10-18）と「EtherChannel の設定」（P.10-22）を参照してください。

- 「手順の詳細（シングル モード）」（P.10-32）
- 「手順の詳細（マルチ モード）」（P.10-37）

手順の詳細（シングル モード）

次の理由から、コンフィギュレーションをオフラインでテキスト ファイルとして更新し、コンフィギュレーション全体を再インポートすることを推奨します。

- 冗長インターフェイスまたは EtherChannel インターフェイスのメンバとして名前付きインターフェイスは追加できないため、インターフェイスから名前を削除する必要があります。インターフェイスから名前を削除すると、その名前を参照していたコマンドは削除されます。インターフェイス名を参照するコマンドはコンフィギュレーション全体にわたっており、複数の機能に影響するため、CLI または ASDM で使用中のインターフェイス名を削除すると、新しいインターフェイス名に関係するすべての機能を再設定する間の重大なダウンタイムは言うまでもなく、コンフィギュレーションが大きく破壊されます。
- コンフィギュレーションをオフラインで変更すると、同じインターフェイス名を新しい論理インターフェイスに使用できるので、インターフェイス名を参照している機能コンフィギュレーションの変更が不要になります。変更が必要になるのは、インターフェイス コンフィギュレーションだけです。
- 実行コンフィギュレーションをクリアして新しいコンフィギュレーションをすぐに適用すると、インターフェイスのダウンタイムは最小になります。インターフェイスをリアルタイムで設定するのを待つことがありません。

ステップ 1　ASA に接続します。フェールオーバーを使用している場合は、アクティブな ASA に接続します。

ステップ 2　フェールオーバーを使用している場合は、[Configuration] > [Device Management] > [High Availability] > [Failover] の順に選択し、[Enable failover] チェックボックスをオフにします。[Apply] をクリックして、警告に進んで、フェールオーバーをディセーブルにします。

ステップ 3　[Tools] > [Backup Configurations] を選択して、実行コンフィギュレーションをローカル コンピュータにバックアップすることによって、実行コンフィギュレーションをコピーします。次に、zip ファイルを展開して、running-config.cfg ファイルをテキスト エディタで編集できます。

必ず、古いコンフィギュレーションの予備のコピーを保存しておいてください。編集時のエラーに備えるためです。

ステップ 4　冗長インターフェイスまたは EtherChannel インターフェイスに追加する使用中のインターフェイスごとに、新しい論理インターフェイスの作成で使用するために、**interface** コマンドの下のすべてのコマンドをインターフェイス コンフィギュレーション セクションの最後にカット アンド ペーストします。例外は次のコマンドのみであり、これらは物理インターフェイス コンフィギュレーションで使用されます。

- **media-type**
- **speed**

- **duplex**
- **flowcontrol**

（注）　EtherChannel インターフェイスまたは冗長インターフェイスに追加できるのは*物理*インターフェイスのみです。物理インターフェイスには VLAN を設定できません。

特定の EtherChannel インターフェイスまたは冗長インターフェイス内のすべてのインターフェイスについて、上記の値を必ず一致させてください。EtherChannel インターフェイスの二重通信の設定は [Full] または [Auto] である必要があります。

たとえば、次のインターフェイス コンフィギュレーションがあるとします。太字のコマンドは 3 つの新しい EtherChannel インターフェイスで使用するコマンドであり、インターフェイス セクションの最後にカット アンド ペーストする必要があります。

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 no shutdown
!
interface Management0/1
 shutdown
 no nameif
 no security-level
```

```
 no ip address
```

ステップ 5　ペーストした各コマンド セクションの上に、次のコマンドのいずれかを入力して、新しい論理インターフェイスを作成します。

- **interface redundant** *number* [1-8]
- **interface port-channel** *channel_id* [1-48]

次に例を示します。

```
...

interface port-channel 1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
 no shutdown
!
interface port-channel 2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface port-channel 3
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 no shutdown
```

ステップ 6　新しい論理インターフェイスに物理インターフェイスを割り当てます。

- 冗長インターフェイス：新しい **interface redundant** コマンドの下に次のコマンドを入力します。

  member-interface *physical_interface1*
  member-interface *physical_interface2*

  物理インターフェイスは、同じタイプの任意の 2 つのインターフェイス（以前使用していたか、または未使用）です。管理インターフェイスを冗長インターフェイスに割り当てることはできません。

  たとえば、既存の配線を利用するには、以前使用していたインターフェイスを引き続き、以前の役割のままで、内部および外部の冗長インターフェイスの一部として使用します。

```
interface redundant 1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
 member-interface GigabitEthernet0/0
 member-interface GigabitEthernet0/2

interface redundant 2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 member-interface GigabitEthernet0/1
 member-interface GigabitEthernet0/3
```

- EtherChannel インターフェイス：EtherChannel に追加する各インターフェイス（以前使用していたか、または未使用）の下に次のコマンドを入力します。EtherChannel ごとに最大 16 個のインターフェイスを割り当てることができます。ただし、アクティブにすることができるのは 8 個のみであり、他は障害に備えてスタンバイ状態です。

channel-group *channel_id* **mode active**

たとえば、既存の配線を利用するには、以前使用していたインターフェイスを、以前の役割で、内部および外部の EtherChannel インターフェイスの一部として引き続き使用します。

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
interface Management0/1
 channel-group 3 mode active
 shutdown
 no nameif
 no security-level
 no ip address

...
```

ステップ 7　以前は使用されていなかったが論理インターフェイスの一部になった各インターフェイスをイネーブルにします。**shutdown** コマンドの前に **no** を追加します。

たとえば、最終的な EtherChannel の設定は次のとおりです。

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/1
```

```
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
interface Management0/1
 channel-group 3 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface port-channel 1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
!
interface port-channel 2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
!
interface port-channel 3
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
```

（注） 他のオプションの EtherChannel パラメータは、新しいコンフィギュレーションをインポートした後で設定できます。「EtherChannel の設定」（P.10-22）を参照してください。

ステップ 8　変更したインターフェイス セクションを含め、新しいコンフィギュレーション全体を保存します。

ステップ 9　変更したコンフィギュレーションを含むバックアップ フォルダを再度圧縮します。

ステップ 10　[Tools] > [Restore Configurations] を選択し、変更したコンフィギュレーションの zip ファイルを選択します。マージするのではなく、既存の実行コンフィギュレーションを置き換えてください。詳細については、「バックアップの復元」（P.37-25）を参照してください。

ステップ 11　[Configuration] > [Device Management] > [High Availability] > [Failover] の順に選択し、[Enable failover] チェックボックスをオンにします。[Apply] をクリックし、基本的なフェールオーバー設定を行うかどうか確認するメッセージが表示されたら [No] をクリックして、フェールオーバーを再度イネーブルにします。

手順の詳細（マルチ モード）

次の理由から、システムおよびコンテキスト コンフィギュレーションをオフラインでテキスト ファイルとして更新し、それを再インポートすることを推奨します。

- 冗長インターフェイスまたは EtherChannel インターフェイスのメンバとして割り当て済みのインターフェイスは追加できないため、コンテキストからインターフェイスを割り当て解除する必要があります。インターフェイスを割り当て解除すると、そのインターフェイスを参照していたコンテキスト コマンドは削除されます。インターフェイスを参照するコマンドはコンフィギュレーション全体にわたっており、複数の機能に影響するため、CLI または ASDM で使用中のインターフェイスの割り当てを削除すると、新しいインターフェイスに関係するすべての機能を再設定する間の重大なダウンタイムは言うまでもなく、コンフィギュレーションが大きく破壊されます。
- コンフィギュレーションをオフラインで変更すると、同じインターフェイス名を新しい論理インターフェイスに使用できるので、インターフェイス名を参照している機能コンフィギュレーションの変更が不要になります。変更が必要になるのは、インターフェイス コンフィギュレーションだけです。
- 実行システム コンフィギュレーションをクリアして新しいコンフィギュレーションをすぐに適用すると、インターフェイスのダウンタイムは最小になります。インターフェイスをリアルタイムで設定するのを待つことがありません。

ステップ 1　ASA に接続し、システムに切り替えます。フェールオーバーを使用している場合は、アクティブな ASA に接続します。

ステップ 2　フェールオーバーを使用している場合は、[Configuration] > [Device Management] > [High Availability] > [Failover] の順に選択し、[Enable failover] チェックボックスをオフにします。[Apply] をクリックして、警告に進んで、フェールオーバーをディセーブルにします。

ステップ 3　システムでは、[File] > [Show Running Configuration in New Window] を選択し、表示出力をテキスト エディタにコピーすることによって実行コンフィギュレーションをコピーします。

必ず、古いコンフィギュレーションの予備のコピーを保存しておいてください。編集時のエラーに備えるためです。

たとえば、次のインターフェイス コンフィギュレーションおよび割り当てがシステム コンフィギュレーションにあり、2 つのコンテキスト間に共有インターフェイスがあるとします。

システム

```
interface GigabitEthernet0/0
    no shutdown
interface GigabitEthernet0/1
    no shutdown
interface GigabitEthernet0/2
    shutdown
```

```
interface GigabitEthernet0/3
    shutdown
interface GigabitEthernet0/4
    shutdown
interface GigabitEthernet0/5
    shutdown
interface Management0/0
    no shutdown
interface Management1/0
    shutdown
!
context customerA
    allocate-interface gigabitethernet0/0 int1
    allocate-interface gigabitethernet0/1 int2
    allocate-interface management0/0 mgmt
context customerB
    allocate-interface gigabitethernet0/0
    allocate-interface gigabitethernet0/1
    allocate-interface management0/0
```

ステップ 4　新しい EtherChannel インターフェイスまたは冗長インターフェイスを使用するすべてのコンテキスト コンフィギュレーションのコピーを取得します。「コンフィギュレーションまたはその他のファイルのバックアップおよび復元」（P.37-22）を参照してください。

たとえば、次のコンテキスト コンフィギュレーションをダウンロードします（インターフェイス コンフィギュレーションが表示されています）。

CustomerA コンテキスト

```
interface int1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
!
interface int2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface mgmt
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 management-only
```

CustomerB コンテキスト

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.20.15.5 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.6.78 255.255.255.0
!
interface Management0/0
 nameif mgmt
 security-level 100
 ip address 10.8.1.8 255.255.255.0
 management-only
```

ステップ 5　システム コンフィギュレーションで、「冗長インターフェイスの設定」（P.10-18）または「EtherChannel の設定」（P.10-22）に従って、新しい論理インターフェイスを作成します。論理インターフェイスの一部として使用する追加物理インターフェイスで **no shutdown** コマンドを入力してください。

（注）　EtherChannel インターフェイスまたは冗長インターフェイスに追加できるのは*物理*インターフェイスのみです。物理インターフェイスには VLAN を設定できません。

特定の EtherChannel インターフェイスまたは冗長インターフェイス内のすべてのインターフェイスについて、速度や二重通信などの物理インターフェイス パラメータを必ず一致させてください。EtherChannel インターフェイスの二重通信の設定は [Full] または [Auto] である必要があります。

たとえば、新しいコンフィギュレーションは次のとおりです。

システム

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 no shutdown
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
interface Management0/1
 channel-group 3 mode active
 no shutdown
!
interface port-channel 1
interface port-channel 2
interface port-channel 3
```

ステップ 6　コンテキストごとのインターフェイス割り当てを、新しい EtherChannel インターフェイスまたは冗長インターフェイスを使用するように変更します。「セキュリティ コンテキストの設定」（P.7-20）を参照してください。

たとえば、既存の配線を利用するには、以前使用していたインターフェイスを引き続き、以前の役割のままで、内部および外部の冗長インターフェイスの一部として使用します。

```
context customerA
```

```
    allocate-interface port-channel1 int1
    allocate-interface port-channel2 int2
    allocate-interface port-channel3 mgmt
context customerB
    allocate-interface port-channel1
    allocate-interface port-channel2
    allocate-interface port-channel3
```

（注） まだ行っていない場合は、この機会を利用して、マップされた名前をインターフェイスに割り当てることができます。たとえば、customerA のコンフィギュレーションは変更の必要がなく、ASA で再適用する必要だけがあります。ただし、customerB のコンフィギュレーションは、インターフェイス ID をすべて変更する必要があります。customerB についてマップされた名前を割り当てると、コンテキスト コンフィギュレーションでのインターフェイス ID の変更は必要ですが、マッピングされた名前が今後のインターフェイスの変更に役立つ場合があります。

ステップ 7　マップされた名前を使用しないコンテキストの場合、新しい EtherChannel インターフェイス ID または冗長インターフェイス ID を使用するようにコンテキスト コンフィギュレーションを変更します。（マップされたインターフェイス名を使用するコンテキストでは、変更は必要ありません）。

次に例を示します。

CustomerB コンテキスト

```
interface port-channel1
 nameif outside
 security-level 0
 ip address 10.20.15.5 255.255.255.0
!
interface port-channel2
 nameif inside
 security-level 100
 ip address 192.168.6.78 255.255.255.0
!
interface port-channel3
 nameif mgmt
 security-level 100
 ip address 10.8.1.8 255.255.255.0
 management-only
```

ステップ 8　新しいコンテキスト コンフィギュレーション ファイルを古いファイルの上にコピーします。たとえば、フラッシュ メモリのコンテキストの場合は、システムで [Tools] > [File Management] の順に選択し、次に [File Transfer] > [Between Local PC and Flash] の順に選択します。このツールを使用して、コンフィギュレーション ファイルを選択し、ローカル コンピュータにコピーすることができます。この変更は、スタートアップ コンフィギュレーションのみに影響します。実行コンフィギュレーションでは古いコンテキスト コンフィギュレーションがまだ使用されています。

ステップ 9　変更したインターフェイス セクションを含め、新しいシステム コンフィギュレーション全体をクリップボードにコピーします。

ステップ 10　ASDM で、[Tools] > [Command Line Interface] を選択し、[Multiple Line] オプション ボタンをクリックします。

ステップ 11　最初の行として **clear configure all** を入力し、その後に新しいコンフィギュレーションを貼り付け、[Send] をクリックします。**clear** コマンドによって、新しいコンフィギュレーションを適用する前に、実行コンフィギュレーション（システムとコンテキストの両方）がクリアされます。

ASA を通過するトラフィックは、このポイントで停止します。新しいコンテキスト コンフィギュレーションがすべてリロードされます。リロードが終了すると、ASA を通過するトラフィックは再開されます。

ステップ 12　[Command Line Interface] ダイアログボックスを閉じ、[File] > [Refresh ASDM with the Running Configuration] を選択します。

ステップ 13　[Configuration] > [Device Management] > [High Availability] > [Failover] の順に選択し、[Enable failover] チェックボックスをオンにします。[Apply] をクリックし、基本的なフェールオーバー設定を行うかどうか確認するメッセージが表示されたら [No] をクリックして、フェールオーバーを再度イネーブルにします。

インターフェイスのモニタリング

- 「ARP Table」（P.12-23）を参照してください。
- 「MAC Address Table」（P.12-26）を参照してください。
- 「Interface Graphs」（P.12-26）を参照してください。

次の作業

- マルチ コンテキスト モードの場合：
  - **a.** インターフェイスをコンテキストに割り当てます（固有の MAC アドレスがコンテキスト インターフェイスに自動的に割り当てられます）。第 7 章「マルチ コンテキスト モード」を参照してください。
  - **b.** 第 12 章「ルーテッド モードのインターフェイス」または第 13 章「トランスペアレント モードのインターフェイス」に従って、インターフェイス コンフィギュレーションを実行します。
- シングル コンテキスト モードの場合は、第 12 章「ルーテッド モードのインターフェイス」または第 13 章「トランスペアレント モードのインターフェイス」に従って、インターフェイス コンフィギュレーションを実行します。

ASA 5512-X 以降のインターフェイスの機能履歴

表 10-2 に、この機能のリリース履歴を示します。

表 10-2　インターフェイスの機能履歴

機能名	リリース	機能情報
VLAN 数の増加	7.0(5)	次の制限値が増加されました。 • ASA 5510 基本ライセンスの VLAN 数が 0 から 10 に増えました。 • ASA 5510 Security Plus ライセンスの VLAN 数が 10 から 25 に増えました。 • ASA 5520 の VLAN 数が 25 から 100 に増えました。 • ASA 5540 の VLAN 数が 100 から 200 に増えました。
ASA 5510 上の基本ライセンスに対する増加したインターフェイス	7.2(2)	ASA 5510 上の基本ライセンスについて、最大インターフェイス数が 3 プラス管理インターフェイスから無制限のインターフェイスに増加しました。
VLAN 数の増加	7.2(2)	VLAN の制限値が変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。
ASA 5510 Security Plus ライセンスに対するギガビット イーサネット サポート	7.2(3)	ASA 5510 ASA は、GE（ギガビット イーサネット）を Security Plus ライセンスのあるポート 0 および 1 でサポートするようになりました。ライセンスを Base から Security Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 ポートの容量は、元の FE（ファスト イーサネット）の 100 Mbps から GE の 1000 Mbps に増加します。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。
冗長インターフェイス	8.0(2)	論理冗長インターフェイスは、アクティブとスタンバイの物理インターフェイスからなるペアです。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定して ASA の信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものですが、必要な場合はフェールオーバーとともに冗長インターフェイスも設定できます。最大 8 個の冗長インターフェイス ペアを設定できます。

表 10-2　インターフェイスの機能履歴 （続き）

機能名	リリース	機能情報
ASA 5580 に対するジャンボ パケット サポート	8.1(1)	Cisco ASA 5580 はジャンボ フレームをサポートしています。ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび FCS を含む）より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネット フレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能（ACL など）の最大使用量が制限される場合があります。 この機能は、ASA 5585-X でもサポートされます。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface] > [Advanced]。
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。
ASA 5580 10 ギガビット イーサネット インターフェイスでのフロー制御のポーズ フレームのサポート	8.2(2)	フロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりました。 この機能は、ASA 5585-X でもサポートされます。 次の画面が変更されました。 （シングル モード）[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface] > [General] （マルチ モード、システム）[Configuration] > [Interfaces] > [Add/Edit Interface]
ギガビット イーサネット インターフェイスでのフロー制御のポーズ フレームのサポート	8.2(5)/8.4(2)	すべてのモデルでギガビット インターフェイスのフロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりました。 次の画面が変更されました。 （シングル モード）[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface] > [General] （マルチ モード、システム）[Configuration] > [Interfaces] > [Add/Edit Interface]

表 10-2　インターフェイスの機能履歴 （続き）

機能名	リリース	機能情報
EtherChannel サポート	8.4(1)	最大 48 個の 802.3ad EtherChannel（1 つあたりのアクティブ インターフェイス 8 個）を設定できます。 次の画面が変更または導入されました。 [Configuration] > [Device Setup] > [Interfaces] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit EtherChannel Interface] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface] [Configuration] > [Device Setup] > [EtherChannel] **（注）** EtherChannel は ASA 5505 ではサポートされません。
EtherChannel あたり 16 個のアクティブ リンクのサポート	9.2(1)	EtherChannel あたり最大で 16 個のアクティブ リンクを設定できるようになりました。これまでは、8 個のアクティブ リンクと 8 個のスタンバイ リンクが設定できました。スイッチは、16 個のアクティブ リンクをサポート可能である必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。 **（注）** 旧バージョンの ASA からアップグレードする場合、互換性を得るために、アクティブ インターフェイスの最大数は 8 に設定します。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit EtherChannel Interface] > [Advanced]。

基本インターフェイスの設定（ASAv）

この章では、Cisco ASAv のインターフェイス コンフィギュレーションを開始するためのタスクについて説明します。イーサネット設定、冗長インターフェイス、および VLAN サブインターフェイスの設定が含まれています。

ASAv インターフェイス コンフィギュレーションの開始に関する情報

ASAv インターフェイスおよび仮想 NIC

ASAv は、仮想プラットフォーム上のゲストとして、基盤となる物理プラットフォームのネットワーク インターフェイスを利用します。ASAv の各インターフェイスは仮想 NIC（vNIC）にマッピングされます。

ASAv インターフェイス

ASAv は、次のギガビット イーサネット インターフェイスがあります。

- Management 0/0
- GigabitEthernet 0/0 ～ 0/8。ASAv をフェールオーバー ペアの一部として展開する場合は GigabitEthernet 0/8 がフェールオーバー リンクに使用されることに注意してください。

サポートされる vNIC

ASAv は次の vNIC をサポートします。

vNIC のタイプ	ハイパーバイザのサポート		ASAv のバージョン	注意
	VMware	KVM		
VMXNET3	**Yes**	No	9.2(1) 以降	VMXNET3 を使用する場合、TCP パフォーマンスの低下を避けるために大量受信オフロード（LRO）をディセーブルにする必要があります。次の VMware のサポート記事を参照してください。 http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1027511 http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=2055140
e1000	**Yes**	**Yes**	9.2(1) 以降	デフォルトです。

VMware における ASAv インターフェイスと vNIC の対応

[vSphere Client Virtual Machine Properties] 画面（ASAv インスタンスを右クリックし、[Edit Settings] を選択）には、各ネットワーク アダプタと割り当てられたネットワークが表示されます。ただし、この画面には ASAv インターフェイス ID は表示されません（ネットワーク アダプタ ID のみ）。次のネットワーク アダプタ ID と ASAv ID の対応一覧を参照してください。

ネットワーク アダプタ ID	ASAv インターフェイス ID
ネットワーク アダプタ 1	Management0/0
ネットワーク アダプタ 2	GigabitEthernet0/0
ネットワーク アダプタ 3	GigabitEthernet0/1
ネットワーク アダプタ 4	GigabitEthernet0/2
ネットワーク アダプタ 5	GigabitEthernet0/3
ネットワーク アダプタ 6	GigabitEthernet0/4
ネットワーク アダプタ 7	GigabitEthernet0/5
ネットワーク アダプタ 8	GigabitEthernet0/6
ネットワーク アダプタ 9	GigabitEthernet0/7
ネットワーク アダプタ 10	GigabitEthernet0/8

トランスペアレント モードのインターフェイス

トランスペアレント モードのインターフェイスは、「ブリッジ グループ」に属しており、ブリッジ グループはネットワークにつき 1 個です。最大で、4 つのインターフェイスによるブリッジ グループを 8 個設定できます。ブリッジ グループの詳細については、「トランスペアレント モードのブリッジ グループ」（P.13-1）を参照してください。

管理インターフェイス

管理インターフェイスの概要

次のインターフェイスに接続して ASA を管理できます。

- 任意の通過トラフィック インターフェイス
- 専用 Management 0/0 インターフェイス

第 36 章「管理アクセス」の説明に従って、管理アクセスへのインターフェイスを設定する必要がある場合があります。

管理専用トラフィックに対する任意のインターフェイスの使用

任意のインターフェイスを、管理トラフィック用として設定することによって管理専用インターフェイスとして使用できます。

トランスペアレント モードの管理インターフェイス

トランスペアレント ファイアウォール モードでは、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、Management 0/0 インターフェイス（物理インターフェイスまたはサブインターフェイス）を個別の管理インターフェイスとして使用できます。他のインターフェイス タイプは管理インターフェイスとして使用できません。管理インターフェイスは、通常のブリッジ グループの一部ではありません。動作上の目的から、設定できないブリッジ グループの一部です。

（注）トランスペアレント ファイアウォール モードでは、管理インターフェイスによってデータ インターフェイスと同じ方法で MAC アドレス テーブルがアップデートされます。したがって、いずれかのスイッチ ポートをルーテッド ポートとして設定しない限り、管理インターフェイスおよびデータ インターフェイスを同じスイッチに接続しないでください（デフォルトでは、Catalyst スイッチがすべての VLAN スイッチ ポートの MAC アドレスを共有します）。そうしないと、物理的に接続されたスイッチから管理インターフェイスにトラフィックが到着すると、ASA によって、データ インターフェイスではなく、*管理*インターフェイスを使用してスイッチにアクセスするように MAC アドレス テーブルがアップデートされます。この処理が原因で、一時的にトラフィックが中断します。セキュリティ上の理由から、少なくとも 30 秒間は、スイッチからデータ インターフェイスへのパケットのために MAC アドレス テーブルが ASA によって再アップデートされることはありません。

通過トラフィックのサポートなし

Management 0/0 インターフェイスは常に管理専用に設定されます。このインターフェイスを通過トラフィックのサポートに使用することはできません。

冗長インターフェイス

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブ インターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定して ASA の信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものですが、必要な場合はデバイスレベルのフェールオーバーとともに冗長インターフェイスも設定できます。

冗長インターフェイスの MAC アドレス

冗長インターフェイスは、最初に追加された物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバー インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに MAC アドレスを割り当てることができます。これはメンバー インターフェイスの MAC アドレスに関係なく使用されます（「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）または「マルチ コンテキストの設定」（P.7-15）を参照）。アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーすると、トラフィックが中断しないように同じ MAC アドレスが維持されます。

最大伝送単位および TCP 最大セグメント サイズのフラグメンテーションの制御

MTU の概要

最大伝送単位（MTU）は、ASA が特定のイーサネット インターフェイスで送信する最大フレーム ペイロード サイズを指定します。MTU の値は、イーサネット ヘッダー、FCS、VLAN タギングなどを*含まない*フレーム サイズです。イーサネット ヘッダーは 14 バイトで、FCS は 4 バイトです。MTU を 1500 に設定すると、予想されるフレーム サイズは、ヘッダーを含めて 1518 バイトです。VLAN タギングを使用する場合（追加の 4 バイトが付加されます）、MTU を 1500 に設定すると、予想されるフレーム サイズは 1522 です。これらのヘッダーに対応するために MTU 値を高く設定しないでください。カプセル化のための TCP ヘッダーに対応する場合は、MTU 設定を変更するのではなく、TCP 最大セグメント サイズを変更してください（「TCP 最大セグメント サイズの概要」（P.11-5）を参照）。

（注）　ASA はメモリに空きがある限り、設定された MTU よりも大きいフレームを受信します。大きなフレームに対応するためのメモリの増設については、「ジャンボ フレーム サポートのイネーブル化」（P.11-16）を参照してください。

デフォルト MTU

ASA のデフォルト MTU は、1500 バイトです。この値には、イーサネット ヘッダー、CRC、VLAN タギングなどのための 18 バイト以上は含まれません。

パス MTU ディスカバリ

ASA は、Path MTU Discovery（RFC 1191 に規定）をサポートします。つまり、2 台のホスト間のネットワーク パス内のすべてのデバイスで MTU を調整できます。したがってパスの最小 MTU の標準化が可能です。

MTU とジャンボ フレームの設定

「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）を参照してください。

「ジャンボ フレーム サポートのイネーブル化」（P.11-16）を参照してください。

次のガイドラインを参照してください。

- トラフィック パスの MTU の一致 : すべての ASA インターフェイスとトラフィック パス内のその他のデバイスのインターフェイスでは、MTU が同じになるように設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボ フレームへの対応 : ジャンボ フレームをイネーブルにすると、MTU は 9000 バイトまで設定できます。

TCP 最大セグメント サイズの概要

TCP 最大セグメント サイズ（TCP MSS）とは、あらゆる TCP ヘッダーが追加される*前の* TCP ペイロードのサイズです。UDP パケットは影響を受けません。接続を確立するときのスリーウェイ ハンドシェイク中に、クライアントとサーバは TCP MSS 値を交換します。

ASA の TCP MSS を設定することもできます。いずれかのエンドポイント接続が ASA で設定されている値よりも大きな TCP MSS を要求した場合、ASA は要求パケットの TCP MSS を ASA の最大値で上書きします。ホストまたはサーバが TCP MSS を要求しない場合、ASA は RFC 793 のデフォルト値 536 バイトを想定しますが、パケットは変更しません。TCP の最小 MSS も設定できます。ホストまたはサーバが非常に小さい TCP MSS を要求した場合、ASA は値を調整します。デフォルトでは、最小 TCP MSS はイネーブルではありません。

たとえば、MTU を デフォルトの 1500 バイトに設定します。ホストが 1700 の MSS を要求します。ASA の最大 TCP MSS が 1380 の場合は、ASA は TCP 要求パケットの MSS 値を 1380 に変更します。サーバは、1380 バイトのパケットを送信します。

デフォルト TCP MSS

デフォルトでは、ASA の最大 TCP MSS は 1380 バイトです。このデフォルトは、最大 120 バイトのヘッダーを追加できる VPN 接続に対応しています。この値は、MTU の デフォルトの 1500 バイト内にも収まっています。

VPN および非 VPN トラフィックの TCP MSS の設定

「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）を参照してください。

次のガイドラインを参照してください。

- 非 VPN トラフィック：VPN を使用せず、ヘッダーのための余分な領域を必要としない場合、TCP MSS 制限をディセーブルにし、接続エンドポイント間に確立された値を受け入れる必要があります。通常接続エンドポイントは MTU から TCP MSS を取得するため、非 VPN パケットは通常この TCP MSS を満たしています。
- VPN トラフィック：最大 TCP MSS を MTU - 120 に設定します。たとえば、ジャンボ フレームを使用しており、MTU の値を高めに設定すると、TCP MSS も MTU に合わせて設定する必要があります。

ASAv インターフェイスのライセンス要件

モデル	ライセンス要件
ASAv（仮想 CPU × 1 を搭載）	VLAN： 標準および Premium ライセンス：50 すべての種類のインターフェイス： 標準および Premium ライセンス：716
ASAv（仮想 CPU × 4 を搭載）	VLAN： 標準および Premium ライセンス：200 すべての種類のインターフェイス： 標準および Premium ライセンス：1316

（注）　VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。

すべてのタイプのインターフェイスには、VLAN、物理、冗長、ブリッジ グループ インターフェイスなど、すべてを合わせたインターフェイスの最大数が含まれます。コンフィギュレーションで定義されているすべての **interface** が、この制限に対してカウントされます。

注意事項および制約事項

この項では、この機能のガイドラインと制限事項について説明します。

ファイアウォール モードのガイドライン

- トランスペアレント モードでは、最大 8 個のブリッジ グループを設定できます。
- 各ブリッジ グループには、最大 4 つのインターフェイスを含めることができます。

フェールオーバーのガイドライン

- 冗長インターフェイスをフェールオーバー リンクとして使用する場合、フェールオーバーペアの両方の装置でその事前設定を行う必要があります。プライマリ装置で設定し、セカンダリ装置に複製されることは想定できません。これは、*複製にはフェールオーバー リンク自体が必要であるため*です。
- 冗長インターフェイスをステート リンクに対して使用する場合、特別なコンフィギュレーションは必要ありません。コンフィギュレーションは通常どおりプライマリ装置から複製されます。
- フェールオーバーが発生しているかどうか冗長インターフェイスをモニタできます。アクティブなメンバー インターフェイスがスタンバイ インターフェイスにフェールオーバーした場合、デバイスレベルのフェールオーバーをモニタしているときには、冗長インターフェイスで障害が発生しているように見えません。冗長インターフェイスで障害が発生しているように見えるのは、すべての物理インターフェイスで障害が発生したときだけです。
- データ インターフェイスと、フェールオーバーまたはステートのインターフェイスを共有することはできません。

冗長インターフェイスのガイドライン

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- すべての ASA コンフィギュレーションは、メンバ物理インターフェイスではなく論理冗長インターフェイスを参照します。
- アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。
- 冗長インターフェイスを管理専用として設定することはできません。
- フェールオーバーのガイドラインについては、「フェールオーバーのガイドライン」（P.11-7）を参照してください。

デフォルト設定

この項では、工場出荷時のデフォルト コンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。工場出荷時のデフォルト コンフィギュレーションに関する情報については、「工場出荷時のデフォルト設定」（P.2-15）を参照してください。

インターフェイスのデフォルトの状態

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

デフォルトの速度および二重通信

- デフォルトでは、インターフェイスの速度とデュプレックスはオート ネゴシエーションに設定されます。

デフォルトの MAC アドレス

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。

デフォルトの vNIC

すべてのインターフェイスは、E1000 エミュレーションを使用します。

インターフェイス コンフィギュレーションの開始（ASAv）

インターフェイス コンフィギュレーションを開始するためのタスク フロー

インターフェイス コンフィギュレーションを開始するには、次の手順を実行します。

ステップ 1　物理インターフェイスをイネーブルにし、必要に応じてイーサネット パラメータを変更します。「物理インターフェイスのイネーブル化およびイーサネット パラメータの設定」（P.11-8）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ディセーブルになっています。

ステップ 2　（オプション）冗長インターフェイス ペアを設定します。「冗長インターフェイスの設定」（P.11-11）を参照してください。

論理冗長インターフェイスは、アクティブとスタンバイの物理インターフェイスからなるペアです。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。

ステップ 3　（オプション）VLAN サブインターフェイスを設定します。「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.11-14）を参照してください。

ステップ 4　（オプション）「ジャンボ フレーム サポートのイネーブル化」（P.11-16）に従って、ジャンボ フレームのサポートをイネーブルにします。

物理インターフェイスのイネーブル化およびイーサネット パラメータの設定

ここでは、次の方法について説明します。

- 物理インターフェイスをイネーブルにする。
- 特定の速度と二重通信を設定する。
- フロー制御のポーズ フレームのイネーブル化

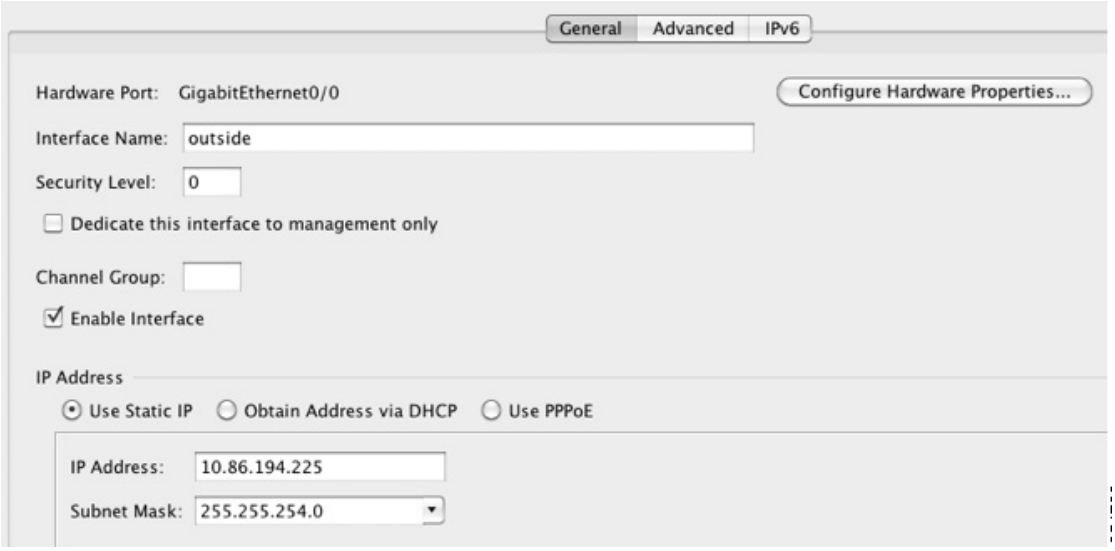
手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

デフォルトでは、すべての物理インターフェイスが一覧表示されます。

ステップ 2　設定する物理インターフェイスをクリックし、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。



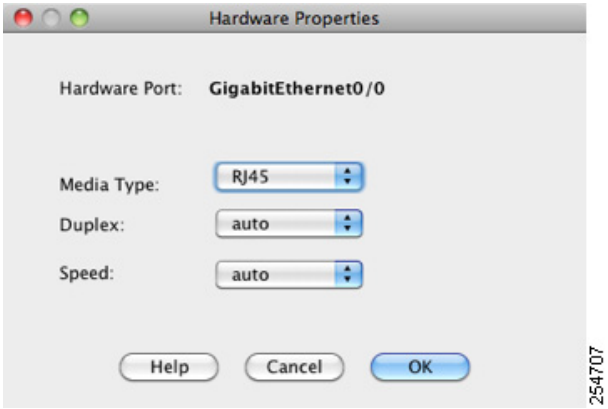
（注）　この手順では [Edit Interface] ダイアログボックスでのパラメータのサブセットのみを対象としています。他のパラメータを設定する場合は、第 12 章「ルーテッド モードのインターフェイス」または第 13 章「トランスペアレント モードのインターフェイス」を参照してください。

ステップ 3　インターフェイスをイネーブルにするには、[Enable Interface] チェックボックスをオンにします。

ステップ 4　説明を追加するには、[Description] フィールドにテキストを入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 5　（オプション）メディア タイプ、二重通信、速度を設定し、フロー制御のポーズ フレームをイネーブルにするには、[Configure Hardware Properties] をクリックします。



（注）　メディア タイプは常に RJ-45 です。

a. RJ-45 インターフェイスに二重通信を設定するには、[Duplex] ドロップダウン リストからインターフェイス タイプに応じて [Full]、[Half]、または [Auto] を選択します。

b. 速度を設定するには、[Speed] ドロップダウン リストから値を選択します。

c. [OK] をクリックして [Hardware Properties] の変更を受け入れます。

d. フロー制御のポーズ（XOFF）フレームをイネーブルにするには、[Enable Pause Frame] チェックボックスをオンにします。

   トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズ フレームをイネーブルにすると、このような問題の発生を抑制できます。ポーズ（XOFF）および XON フレームは、FIFO バッファ使用量に基づいて、NIC ハードウェアによって自動的に生成されます。バッファ使用量が高ウォーターマークを超えると、ポーズ フレームが送信されます。デフォルトの *high_water* 値は 24 KB です。この値は 0 ～ 47 KB に設定できます。ポーズの送信後、バッファ使用量が低ウォーター マークよりも下回ると、XON フレームを送信できます。デフォルトでは、*low_water* 値は 16 KB です。この値は 0 ～ 47 KB に設定できます。リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のタイマー値によって制御されます。デフォルトの *pause_time* 値は 26624 です。この値は 0 ～ 65535 に設定できます。バッファの使用量が継続的に高基準値を超えている場合は、ポーズ リフレッシュのしきい値に指定された間隔でポーズ フレームが繰り返し送信されます。

   [Low Watermark]、[High Watermark]、[Pause Time] のデフォルト値を変更するには、[Use Default Values] チェックボックスをオフにします。

   （注）　802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティベースのフロー制御はサポートされていません。

ステップ 6　[OK] をクリックして [Interface] の変更を受け入れます。

次の作業

オプション タスク：

- 冗長インターフェイス ペアを設定します。「冗長インターフェイスの設定」（P.11-11）を参照してください。
- VLAN サブインターフェイスを設定します。「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.11-14）を参照してください。
- ジャンボ フレーム サポートを設定します。「ジャンボ フレーム サポートのイネーブル化」（P.11-16）を参照してください。

必須タスク：

- インターフェイス コンフィギュレーションを実行します。第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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。

冗長インターフェイスの設定

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブ インターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定して ASA の信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものですが、必要な場合はフェールオーバーとともに冗長インターフェイスも設定できます。

この項では、冗長インターフェイスを設定する方法について説明します。

- 「冗長インターフェイスの設定」（P.11-11）
- 「アクティブ インターフェイスの変更」（P.11-13）

冗長インターフェイスの設定

この項では、冗長インターフェイスを作成する方法について説明します。デフォルトでは、冗長インターフェイスはイネーブルになっています。

注意事項と制約事項

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- 冗長インターフェイス遅延値は設定可能ですが、デフォルトでは、ASA はそのメンバー インターフェイスの物理タイプに基づくデフォルトの遅延値を継承します。
- 「冗長インターフェイスのガイドライン」（P.11-7）も参照してください。

前提条件

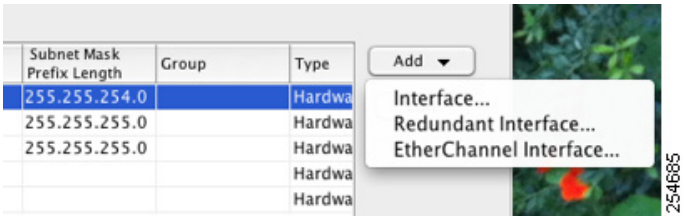
- 両方のメンバー インターフェイスが同じ物理タイプである必要があります。たとえば、両方ともギガビット イーサネットにする必要があります。
- 名前が設定されている場合は、物理インターフェイスを冗長インターフェイスに追加できません。最初に、[Configuration] > [Device Setup] > [Interfaces] ペインで名前を削除する必要があります。

注意　コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

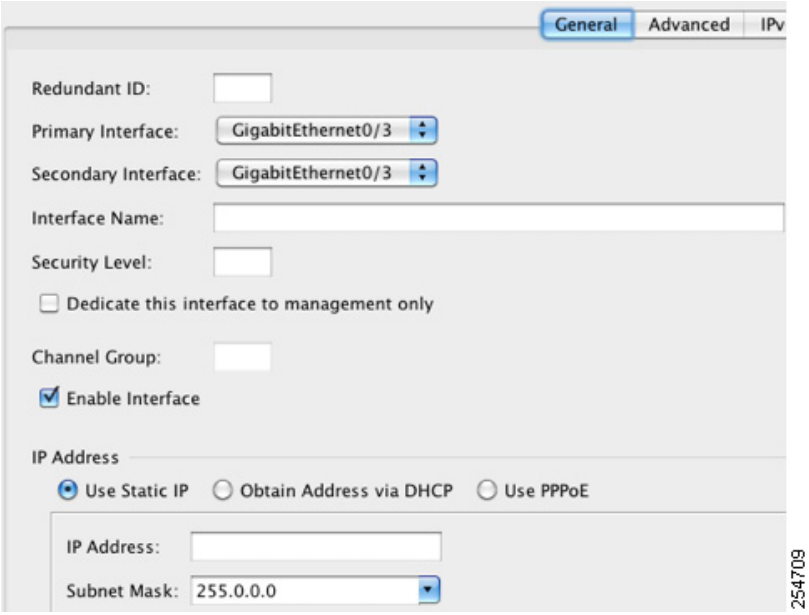
手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　[Add] > [Redundant Interface] を選択します。



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



（注）　この手順では [Edit Redundant Interface] ダイアログボックスでのパラメータのサブセットのみを対象としています。他のパラメータを設定する場合は、第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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。

ステップ 3　[Redundant ID] フィールドで、1 ～ 8 の整数を入力します。

ステップ 4　[Primary Interface] ドロップダウン リストから、プライマリにする物理インターフェイスを選択します。

サブインターフェイスを持たず、まだ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を必ず選択してください。

ステップ 5　[Secondary Interface] ドロップダウン リストから、セカンダリにする物理インターフェイスを選択します。

ステップ 6　インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

インターフェイスはデフォルトでイネーブルになっています。ディセーブルにするには、このチェックボックスをオフにします。

ステップ 7　説明を追加するには、[Description] フィールドにテキストを入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 8　[OK] をクリックします。

[Interfaces] ペインに戻ります。メンバー インターフェイスで、基本パラメータのみが設定できることを示すロックが、インターフェイス ID の左側に表示されます。冗長インターフェイスがテーブルに追加されます。

GigabitEthernet0/2	Enabled	No	Redundant8	Hardware	native
GigabitEthernet0/3	Enabled	No		Hardware	native
GigabitEthernet0/3.10	Enabled	No		Logical	vlan100
GigabitEthernet0/3.11	Enabled	No		Logical	vlan11
Management0/0	Enabled	No		Hardware	native
Redundant8	Enabled	Yes		Logical	native

254710

次の作業

オプション タスク：

- VLAN サブインターフェイスを設定します。「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.11-14）を参照してください。
- ジャンボ フレーム サポートを設定します。「ジャンボ フレーム サポートのイネーブル化」（P.11-16）を参照してください。

必須タスク：

- インターフェイス コンフィギュレーションを実行します。第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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。

アクティブ インターフェイスの変更

デフォルトでは、コンフィギュレーションで最初にリストされているインターフェイスが（使用可能であれば）、アクティブ インターフェイスになります。どのインターフェイスがアクティブかを表示するには、[Tools] > [Command Line Interface tool] で次のコマンドを入力します。

```
show interface redundantnumber detail | grep Member
```

次に例を示します。

```
show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

アクティブ インターフェイスを変更するには、次のコマンドを入力します。

redundant-interface redundant*number* **active-member** *physical_interface*

redundant *number* 引数には、冗長インターフェイス ID（**redundant1** など）を指定します。

physical_interface には、アクティブにするメンバー インターフェイスの ID を指定します。

VLAN サブインターフェイスと 802.1Q トランキングの設定

サブインターフェイスを使用すると、1 つの物理インターフェイスまたは冗長インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたは ASA を追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。

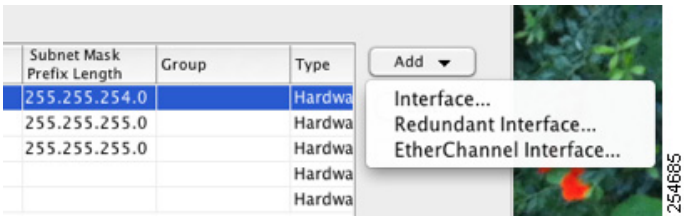
注意事項と制約事項

- 最大サブインターフェイス数：使用するモデルで許容される VLAN サブインターフェイス数を決定するには、「ASAv インターフェイスのライセンス要件」（P.11-6）を参照してください。
- 物理インターフェイス上のタグなしパケットの禁止：サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。この特性は、冗長インターフェイス ペアのアクティブな物理インターフェイスにも当てはまります。トラフィックがサブインターフェイスを通過するには、物理インターフェイスまたは冗長インターフェイスがイネーブルになっている必要があるため、トラフィックが物理インターフェイスまたは冗長インターフェイスを通過しないように、インターフェイスには名前を設定しないでください。物理インターフェイスまたは冗長インターフェイスでタグのないパケットを通過できるようにする場合は、通常どおりに名前を設定できます。インターフェイス コンフィギュレーションの詳細については、第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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。

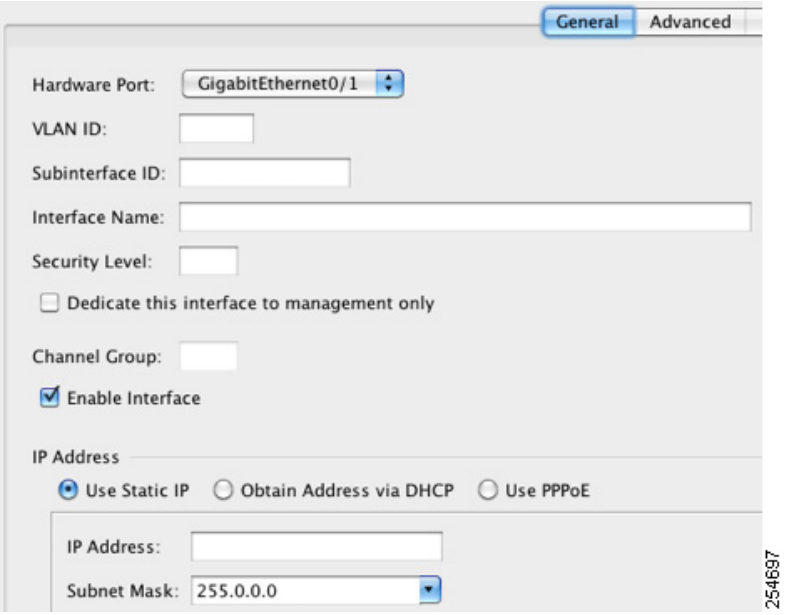
手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　[Add] > [Interface] を選択します。



[Add Interface] ダイアログボックスが表示されます。



（注）　この手順では [Edit Interface] ダイアログボックスでのパラメータのサブセットのみを対象としています。他のパラメータを設定する場合は、第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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。

ステップ 3　[Hardware Port] ドロップダウン リストから、サブインターフェイスを追加する物理インターフェイスまたは冗長インターフェイスを選択します。

ステップ 4　インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

インターフェイスはデフォルトでイネーブルになっています。ディセーブルにするには、このチェックボックスをオフにします。

ステップ 5　[VLAN ID] フィールドに、1 ～ 4095 の VLAN ID を入力します。

一部の VLAN ID は接続スイッチ用に予約されている場合があります。詳細については、スイッチのマニュアルを確認してください。

ステップ 6　[Subinterface ID] フィールドに、サブインターフェイス ID を 1 ～ 4294967293 の整数で入力します。

許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。

ステップ 7　（オプション）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 8　[OK] をクリックします。

[Interfaces] ペインに戻ります。

次の作業

オプション タスク：

- ジャンボ フレーム サポートを設定します。「ジャンボ フレーム サポートのイネーブル化」（P.11-16）を参照してください。

必須タスク：

- インターフェイス コンフィギュレーションを実行します。第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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。

ジャンボ フレーム サポートのイネーブル化

ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび FCS を含む）より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネット フレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能（ACL など）の最大使用量が制限される場合があります。詳細については、「最大伝送単位および TCP 最大セグメント サイズのフラグメンテーションの制御」（P.11-4）を参照してください。

前提条件

- この設定を変更した場合は、ASA のリロードが必要です。
- ジャンボ フレームを送信する必要があるインターフェイスごとに MTU を必ず設定してください。「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）を参照してください。
- 必ず、TCP MSS 調整して、非 VPN トラフィックの TCP MSS をディセーブルにするか、「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）に従い、MTU に従って TCP MSS を増やしてください。

手順の詳細

1500 バイトを超える MTU を設定すると、ジャンボ フレームが自動的にイネーブルになります。この設定を手動でイネーブルまたはディセーブルにするには、[Configuration] > [Device Setup] > [Interfaces] を選択し、[Enable jumbo frame support] チェックボックスをオンにします。

次の作業

インターフェイス コンフィギュレーションを実行します。第 12 章「ルーテッド モードのインターフェイス」または第 13 章「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。

インターフェイスのモニタリング

ARP テーブル

[Monitoring] > [Interfaces] > [ARP Table] ペインには、スタティックとダイナミック エントリを含む ARP テーブルが表示されます。ARP テーブルには、MAC アドレスを所定のインターフェイスの IP アドレスにマッピングするエントリが含まれます。

フィールド

- [Interface]：マッピングに関連付けられているインターフェイス名を一覧表示します。
- [IP Address]：IP アドレスを表示します。
- [MAC Address]：MAC アドレスを表示します。
- [Proxy ARP]：インターフェイスでプロキシ ARP がイネーブルになっている場合は [Yes] と表示します。インターフェイスでプロキシ ARP がイネーブルになっていない場合は [No] と表示します。
- [Clear]：ダイナミック ARP テーブルのエントリをクリアします。スタティック エントリはクリアされません。
- [Refresh]：ASA の現在の情報でテーブルをリフレッシュし、[Last Updated] の日付と時刻を更新します。
- [Last Updated]：*表示専用*。表示が更新された日付と時刻を示します。

MAC Address Table

[Monitoring] > [Interfaces] > [MAC Address Table] ペインには、スタティックおよびダイナミック MAC アドレス エントリが表示されます。MAC アドレス テーブルおよび追加のスタティック エントリに関する詳細情報については、「MAC Address Table」（P.11-17）を参照してください。

フィールド

- [Interface]：エントリに関連付けられているインターフェイス名を表示します。
- [MAC Address]：MAC アドレスを表示します。
- [Type]：エントリがスタティックかダイナミックかを表示します。
- [Age]：エントリの経過時間を分数で表示します。タイムアウトを設定するには、「MAC Address Table」（P.11-17）を参照してください。
- [Refresh]：ASA の現在の情報でテーブルをリフレッシュします。

Interface Graphs

[Monitoring] > [Interfaces] > [Interface Graphs] ペインには、インターフェイス統計情報をグラフ形式またはテーブル形式で表示できます。サブインターフェイスに表示される統計情報の数は、物理インターフェイスに表示される統計情報の数のサブセットです。

フィールド

- [Available Graphs for]：モニタリングに使用可能な統計情報のタイプを一覧表示します。1 つのグラフ ペインに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ペインを同時に開くことができます。
  - [Byte Counts]：インターフェイスのバイト入力およびバイト出力の数を表示します。
  - [Packet Counts]：インターフェイスのパケット入力およびパケット出力の数を表示します。

– [Packet Rates]：インターフェイスのパケット入力およびパケット出力のレートを表示します。

– [Bit Rates]：インターフェイスの入出力のビット レートを表示します。

– [Drop Packet Count]：インターフェイスでドロップされたパケットの数を表示します。

物理インターフェイスに追加して表示できる統計情報は次のとおりです。

– [Buffer Resources]：次の統計情報を表示します。

[Overruns]：入力速度が、ASA のデータ処理能力を超えたため、ASA がハードウェア バッファに受信したデータを処理できなかった回数。

[Underruns]：ASA で処理できる速度より速くトランスミッタが動作した回数。

[No Buffer]：メイン システムにバッファ スペースがなかったために廃棄された受信パケットの数。この数を、無視された数と比較してください。イーサネット ネットワーク上のブロードキャスト ストームは、多くの場合、入力バッファ イベントがないことに原因があります。

– [Packet Errors]：次の統計情報を表示します。

[CRC]：巡回冗長検査エラーの数。ステーションがフレームを送信すると、フレームの末尾に CRC を付加します。この CRC は、フレーム内のデータに基づくアルゴリズムから生成されます。送信元と宛先の間でフレームが変更された場合、ASA は CRC が一致しないことを通知します。CRC の数値が高いことは、通常、コリジョンの結果であるか、ステーションが不良データを送信することが原因です。

[Frame]：フレーム エラーの数。不良フレームには、長さが正しくないパケットや、フレーム チェックサムが正しくないパケットがあります。このエラーは通常、コリジョンまたはイーサネット デバイスの誤動作が原因です。

[Input Errors]：ここにリストされている他のタイプのものも含めた入力エラーの合計数。また、その他の入力関連のエラーによって入力エラー数が増えたり、一部のデータグラムに複数のエラーが存在していたりする可能性があります。したがって、この合計は、他のタイプにリストされているエラーの数を超えることがあります。

[Runts]：最小パケット サイズの 64 バイトよりも小さかったために廃棄されたパケットの数。ラントは通常、コリジョンによって発生します。不適切な配線や電気干渉によって発生することもあります。

[Giants]：最大パケット サイズを超えたために廃棄されたパケットの数。たとえば、1518 バイトよりも大きいイーサネット パケットはジャイアントと見なされます。

[Deferred]：FastEthernet インターフェイスだけ。リンク上のアクティビティが原因で送信前に保留されたフレームの数。

– [Miscellaneous]：受信したブロードキャストの統計情報を表示します。

– [Collision Counts]：FastEthernet インターフェイスだけ。次の統計情報を表示します。

[Output Errors]：設定されている衝突の最大数を超えたために伝送されなかったフレームの数。このカウンタは、ネットワーク トラフィックが多い場合にのみ増加します。

[Collisions]：イーサネット衝突（1 つまたは複数の衝突）が原因で、再度伝送されたメッセージ数。これは通常、過度に延長した LAN で発生します（イーサネット ケーブルまたはトランシーバ ケーブルが長すぎる、ステーション間のリピータが 2 つよりも多い、またはマルチポート トランシーバのカスケードが多すぎる場合）。衝突するパケットは、出力パケットによって 1 回だけカウントされます。

[Late Collisions]：通常の衝突ウィンドウの外で衝突が発生したために伝送されなかったフレームの数。レイト コリジョンは、パケットの送信中に遅れて検出されるコリジョンです。これは通常発生しません。2 つのイーサネット ホストが同時に通信しよ

うとした場合、早期にパケットが衝突して両者がバックオフするか、2 番目のホストが 1 番目のホストの通信状態を確認して待機します。レイト コリジョンが発生すると、デバイスは割り込みを行ってイーサネット上にパケットを送信しようとしますが、ASA はパケットの送信を部分的に完了しています。ASA は、パケットの最初の部分を保持するバッファを解放した可能性があるため、パケットを再送しません。このことはあまり問題になりません。その理由は、ネットワーキング プロトコルはパケットを再送することでコリジョンを処理する設計になっているためです。ただし、レイト コリジョンはネットワークに問題が存在することを示しています。一般的な問題は、リピータで接続された大規模ネットワーク、および仕様の範囲を超えて動作しているイーサネット ネットワークです。

– [Input Queue]：入力キューの現在のパケット数および最大パケット数を表示します。次の統計情報が含まれます。

  [Hardware Input Queue]：ハードウェア キューのパケット数。

  [Software Input Queue]：ソフトウェア キューのパケット数。

– [Output Queue]：出力キューの現在のパケット数および最大パケット数を表示します。次の統計情報が含まれます。

  [Hardware Output Queue]：ハードウェア キューのパケット数。

  [Software Output Queue]：ソフトウェア キューのパケット数。

- [Add]：選択した統計タイプを、選択したグラフ ペインに追加します。
- [Remove]：選択したグラフ ペインから、選択した統計タイプを削除します。削除しようとしている項目が他のペインから追加されたものであり、[Available Graphs] ペインに戻されない場合、このボタン名は [Delete] に変わります。
- [Show Graphs]：統計タイプを追加するグラフ ペイン名を表示します。すでにグラフ ペインを開いている場合は、デフォルトで新しいグラフ ペインがリストされます。すでに開いているグラフに統計タイプを追加する場合は、開いているグラフ ペインの名前を選択します。すでにグラフに含まれている統計情報が [Selected Graphs] ペインに表示され、タイプを追加できます。グラフ ペインには ASDM、インターフェイスの IP アドレス、および「Graph」という順番で名前が付けられます。後続のグラフは、「Graph (2)」のように名前が付けられます。
- [Selected Graphs]：選択したグラフ ペインに表示する統計タイプを表示します。表示できるタイプは 4 つまでです。
  – [Show Graphs]：グラフ ペインを表示するか、または、追加した場合は追加の統計タイプでグラフを更新します。

Graph/Table

[Monitoring] > [Interfaces] > [Interface Graphs] > [Graph/Table] ペインには、選択した統計情報のグラフが表示されます。[Graph] ペインには、最大 4 つのグラフおよびテーブルを同時に表示することができます。デフォルトで、グラフまたはテーブルにリアルタイムな統計情報が表示されます。履歴メトリック（「履歴メトリックのイネーブル化」（P.3-34）を参照）をイネーブルにすると、過去の期間の統計情報を表示できます。

フィールド

- [View]：グラフまたはテーブルを表示する期間を設定します。リアルタイム以外の期間を表示するには、履歴メトリック（「履歴メトリックのイネーブル化」（P.3-34）を参照）をイネーブルにします。次のオプションの指定に従ってデータが更新されます。
  – Real-time, data every 10 sec
  – Last 10 minutes, data every 10 sec

  - Last 60 minutes, data every 1 min
  - Last 12 hours, data every 12 min
  - Last 5 days, data every 2 hours

- [Export]：グラフをカンマ区切り形式でエクスポートします。[Graph] ペインに複数のグラフまたはテーブルがある場合、[Export Graph Data] ダイアログボックスが表示されます。名前の横のチェックボックスを選択して、リストされているグラフおよびテーブルを 1 つ以上選択します。
- [Print]：グラフまたはテーブルを印刷します。[Graph] ペインに複数のグラフまたはテーブルがある場合、[Print Graph] ダイアログボックスが表示されます。[Graph/Table Name] リストから印刷するグラフまたはテーブルを選択します。
- [Bookmark]：ブラウザ ペインに、[Graph] ペイン上のすべてのグラフおよびテーブルへのリンク 1 つと、各グラフまたはテーブルへの個別のリンクが表示されます。ブラウザでこれらの URL をブックマークとしてコピーできますグラフの URL を開くときに、ASDM を実行している必要はありません。ブラウザによって ASDM が起動され、グラフが表示されます。

次の作業

第 12 章「ルーテッド モードのインターフェイス」または第 13 章「トランスペアレント モードのインターフェイス」に従って、インターフェイス コンフィギュレーションを実行します。

ASAv インターフェイスの機能履歴

表 11-1　インターフェイスの機能履歴

機能名	プラットフォーム リリース	機能情報
ASAv のサポート	9.2(1)	ASAv が導入されました。

ルーテッド モードのインターフェイス

この章では、ルーテッド ファイアウォール モードですべてのモデルのインターフェイス コンフィギュレーションを実行するためのタスクについて説明します。

（注） マルチ コンテキスト モードでは、この項のタスクをコンテキスト実行スペースで実行してください。[Configuration] > [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。

ルーテッド モードでのインターフェイス コンフィギュレーションの実行の概要

セキュリティ レベル

各インターフェイスには、0（最下位）～ 100（最上位）のセキュリティ レベルを設定する必要があります。たとえば、内部ホスト ネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル 0 が割り当てられる場合があります。DMZ など、その他のネットワークはその中間に設定できます。複数のインターフェイスを同じセキュリティ レベルに割り当てることができます。詳細については、「同じセキュリティ レベルの通信の許可」（P.12-20）を参照してください。

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。ACL をインターフェイスに適用して、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイスの通信をイネーブルにすると（「同じセキュリティ レベルの通信の許可」（P.12-20）を参照）、同じセキュリティ レベルまたはそれより低いセキュリティ レベルの他のインターフェイスにアクセスするインターフェイスは、暗黙的に許可されます。

- インスペクション エンジン：一部のアプリケーション インスペクション エンジンはセキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。
  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - SQL*Net インスペクション エンジン：SQL*Net（旧称 OraServ）ポートとの制御接続が一対のホスト間に存在する場合、着信データ接続だけが ASA を通過することが許可されます。

- フィルタリング：HTTP(S) および FTP フィルタリングは、（高いレベルから低いレベルへの）発信接続にのみ適用されます。

  同じセキュリティ レベルのインターフェイス間の通信をイネーブルにすると、どちらの方向のトラフィックにもフィルタリングが適用できます。

- **established** コマンド：このコマンドを使用すると、高いレベルのホストから低いレベルのホストへの接続がすでに確立されている場合、低いセキュリティ レベルのホストから高いセキュリティ レベルのホストへの戻り接続が許可されます。

  セキュリティ レベルが同じインターフェイス間の通信をイネーブルにすると、両方向に対して **established** コマンドを設定できます。

デュアル IP スタック（IPv4 および IPv6）

Cisco ASA は、1 つのインターフェイス上で IPv6 と IPv4 の両方のコンフィギュレーションをサポートします。そのために特別なコマンドを入力する必要はありません。単純に、IPv4 コンフィギュレーション コマンドと IPv6 コンフィギュレーション コマンドを通常と同じように入力します。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

ルーテッド モードでインターフェイス コンフィギュレーションを実行するためのライセンス要件

モデル	ライセンス要件
ASA 5512-X	VLAN： 基本ライセンス：50 Security Plus ライセンス：100 すべての種類のインターフェイス： 基本ライセンス：716 Security Plus ライセンス：916
ASA 5515-X	VLAN： 基本ライセンス：100 すべての種類のインターフェイス： 基本ライセンス：916
ASA 5525-X	VLAN： 基本ライセンス：200 すべての種類のインターフェイス： 基本ライセンス：1316
ASA 5545-X	VLAN： 基本ライセンス：300 すべての種類のインターフェイス： 基本ライセンス：1716
ASA 5555-X	VLAN： 基本ライセンス：500 すべての種類のインターフェイス： 基本ライセンス：2516
ASA 5585-X	VLAN： 基本ライセンスと Security Plus ライセンス：1024 SSP-10 および SSP-20 のインターフェイス速度： 基本ライセンス：ファイバ インターフェイスの場合 1 ギガビット イーサネット 10 GE I/O ライセンス（Security Plus）：ファイバ インターフェイスの場合 10 ギガビット イーサネット （SSP-40 および SSP-60 は 10 ギガビット イーサネットをデフォルトでサポートします）。 すべての種類のインターフェイス： 基本ライセンスと Security Plus ライセンス：4612

（注）　VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。

すべてのタイプのインターフェイスは、結合されたインターフェイスに最大数を設定しています。たとえば、VLAN、物理、冗長、ブリッジ グループ、および EtherChannel などのインターフェイスです。コンフィギュレーションで定義されているすべての **interface** が、この制限に対してカウントされます。

モデル	ライセンス要件
ASASM	VLAN： 基本ライセンス：1000

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

- マルチ コンテキスト モードでの ASA 5512-X 以降の場合、第 10 章「基本的なインターフェイス コンフィギュレーション（ASA 5512-X 以降）」に従って、システム実行スペースで物理インターフェイスを設定します。次に、この章に従って、コンテキスト実行スペースで論理インターフェイス パラメータを設定します。マルチ コンテキスト モードの ASASM の場合は、スイッチのスイッチ ポートおよび VLAN を設定し、第 2 章「使用する前に」に従って VLAN を ASASM に割り当てます。

  ASAv はマルチ コンテキスト モードをサポートしません。
- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.7-15）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- PPPoE は、マルチ コンテキスト モードではサポートされていません。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでサポートされています。トランスペアレント モードについては、第 13 章「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。

フェールオーバーのガイドライン

フェールオーバー インターフェイスの設定は、この章の手順では完了しません。フェールオーバーおよびステート リンクの設定については、第 8 章「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。マルチ コンテキスト モードでは、フェールオーバー インターフェイスがシステム コンフィギュレーションに設定されます。

IPv6 のガイドライン

IPv6 をサポートします。

ASASM の VLAN ID に関するガイドライン

コンフィギュレーションにはあらゆる VLAN ID を追加できますが、トラフィックを転送できるのはスイッチによって ASA に割り当てられた VLAN だけです。**show vlan** コマンドを使用して、ASA に割り当てられたすべての VLAN を表示します。

スイッチによって ASA にまだ割り当てられていない VLAN にインターフェイスを追加した場合、そのインターフェイスはダウン ステートになります。ASA に VLAN を割り当てた時点で、インターフェイスはアップ ステートに変化します。インターフェイス ステートの詳細については、**show interface** コマンドを参照してください。

デフォルト設定

この項では、工場出荷時のデフォルト コンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。工場出荷時のデフォルト コンフィギュレーションに関する情報については、「工場出荷時のデフォルト設定」（P.2-15）を参照してください。

デフォルトのセキュリティ レベル

デフォルトのセキュリティ レベルは 0 です。インターフェイスに名前「inside」を付けて、明示的にセキュリティ レベルを設定しないと、ASA はセキュリティ レベルを 100 に設定します。

（注）　インターフェイスのセキュリティ レベルを変更したときに、既存の接続がタイムアウトするまで待機せずに新しいセキュリティ情報を使用する必要がある場合は、**clear local-host** コマンドを使用して接続をクリアできます。

ASASM のインターフェイスのデフォルトの状態

- シングル モードまたはシステム実行スペースでは、VLAN インターフェイスがデフォルトでイネーブルになります。
- マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

ジャンボ フレーム サポート

デフォルトでは、ASASM はジャンボ フレームをサポートしています。「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）に従って、目的のパケット サイズの MTU を設定します。

ルーテッド モードでのインターフェイス コンフィギュレーションの実行

- 「IPv6 アドレッシングの設定」（P.12-15）
- 「同じセキュリティ レベルの通信の許可」（P.12-20）

インターフェイス コンフィギュレーションを実行するためのタスク フロー

ステップ 1　モデルに応じてインターフェイスを設定します。

- ASA 5512-X 以降：第 10 章「基本的なインターフェイス コンフィギュレーション（ASA 5512-X 以降）」
- ASASM：第 2 章「使用する前に」
- ASAv：第 11 章「基本インターフェイスの設定（ASAv）」

ステップ 2　（マルチ コンテキスト モード）「マルチ コンテキストの設定」（P.7-15）に従って、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 3　（マルチ コンテキスト モード）[Configuration] > [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 4　インターフェイス名、セキュリティ レベル、IPv4 アドレスなどの一般的なインターフェイス パラメータを設定します。「一般的なインターフェイス パラメータの設定」（P.12-6）を参照してください。

ステップ 5　（オプション）MAC アドレスと MTU を設定します。「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）を参照してください。

ステップ 6　（オプション）IPv6 アドレッシングを設定します。「IPv6 アドレッシングの設定」（P.12-15）を参照してください。

ステップ 7　（オプション）2 つのインターフェイス間の通信を許可するか、またはトラフィックが同じインターフェイスに入って同じインターフェイスから出ることを許可することで、同じセキュリティ レベルの通信を許可します。「同じセキュリティ レベルの通信の許可」（P.12-20）を参照してください。

一般的なインターフェイス パラメータの設定

この手順では、名前、セキュリティ レベル、IPv4 アドレス、およびその他のオプションを設定する方法について説明します。

ASA 5512-X 以降および ASAv では、次のインターフェイス タイプのインターフェイス パラメータを設定する必要があります。

- 物理インターフェイス
- VLAN サブインターフェイス
- 冗長インターフェイス
- EtherChannel インターフェイス

ASASM では、次のインターフェイス タイプのインターフェイス パラメータを設定する必要があります。

- VLAN インターフェイス

注意事項と制約事項

フェールオーバーを使用している場合は、フェールオーバー通信およびステートフル フェールオーバー通信に予約されているインターフェイスには、この方法で名前を付けないでください。フェールオーバーおよびステート リンクの設定については、第 8 章「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。

制限事項

- PPPoE は、マルチ コンテキスト モードではサポートされていません。
- ASASM では、PPPoE および DHCP はサポートされません。

前提条件

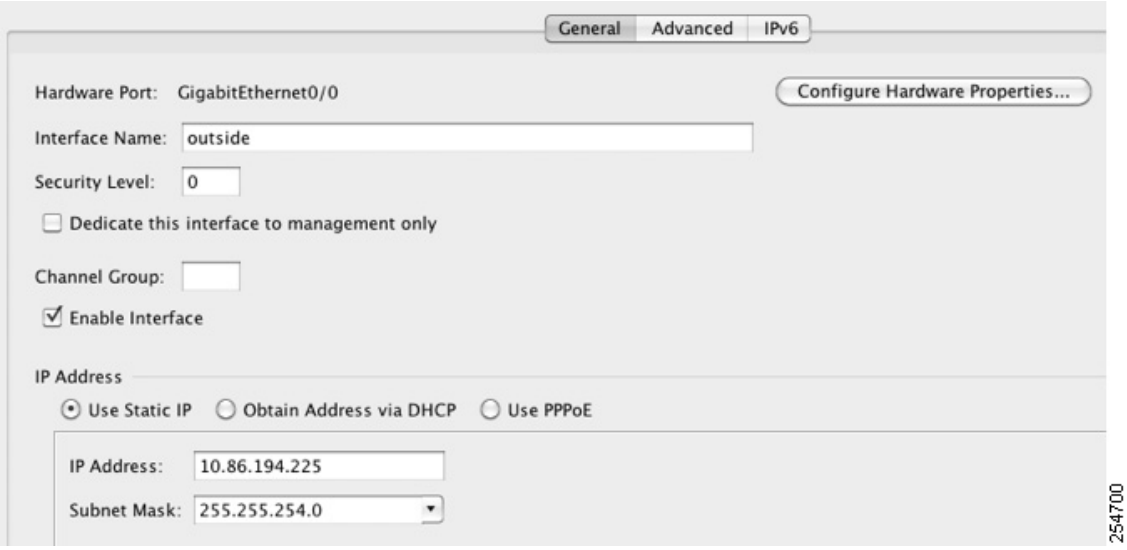
- モデルに応じてインターフェイスを設定します。
  - ASA 5512-X 以降：第 10 章「基本的なインターフェイス コンフィギュレーション（ASA 5512-X 以降）」
  - ASASM：第 2 章「使用する前に」
  - ASAv：第 11 章「基本インターフェイスの設定（ASAv）」
- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.7-15）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [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。

手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　インターフェイス行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。



ステップ 3　[Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 4　[Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

詳細については、「セキュリティ レベル」（P.12-1）を参照してください。

ステップ 5　（任意。冗長インターフェイスではサポートされていません）このインターフェイスを管理専用インターフェイスとして設定するには、[Dedicate this interface to management-only] チェックボックスをオンにします。

管理専用インターフェイスでは、通過トラフィックは受け入れられません。ASA 5585-X での詳細については、「前提条件」（P.12-7）を参照してください。

（ASA 5512-X ～ ASA 5555-X）Management 0/0 インターフェイスではこのオプションをディセーブルにできません。

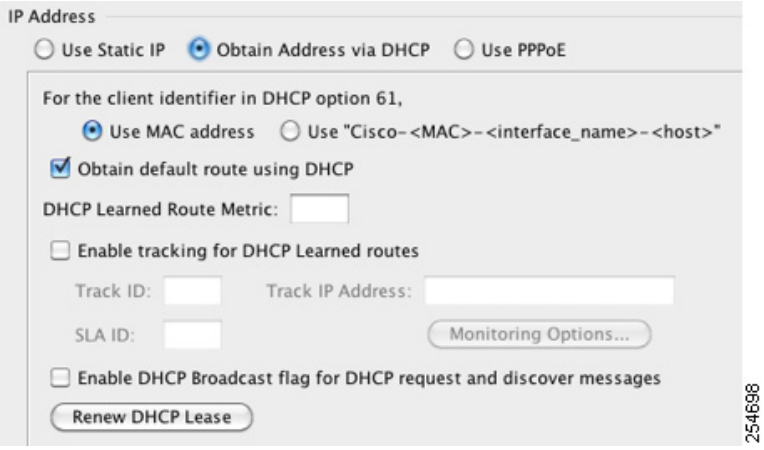
（注）　[Channel Group] フィールドは読み取り専用で、インターフェイスが EtherChannel の一部であるかどうかを示します。

ステップ 6　インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

ステップ 7　IP アドレスを設定するには、次のいずれかのオプションを使用します。

（注）　フェールオーバーで使用する場合、IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces] タブのスタンバイ IP アドレスを設定します。

- IP アドレスを手動で設定するには、[Use Static IP] オプション ボタンをクリックして IP アドレスとマスクを入力します。
- DHCP サーバから IP アドレスを取得するには、[Obtain Address via DHCP] オプション ボタンをクリックします。



a. MAC アドレスがオプション 61 の DHCP 要求パケット内に保存されるようにするには、[Use MAC Address] オプション ボタンをクリックします。

いくつかの ISP はインターフェイスの MAC アドレスにオプション 61 が必要です。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。

b. オプション 61 用に生成された文字列を使用するには、[Use “Cisco-<MAC>-<interface_name>-<host>”] をクリックします。

c. （オプション）DHCP サーバからデフォルト ルートを取得するには、[Obtain Default Route Using DHCP] をオンにします。

d. （オプション）アドミニストレーティブ ディスタンスを既知のルートに割り当てるには、[DHCP Learned Route Metric] フィールドに 1 ～ 255 の値を入力します。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。

e. （オプション）DHCP の既知のルートのトラッキングをイネーブルにするには、[Enable Tracking for DHCP Learned Routes] をオンにします。次の値を設定します。

[Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

[Track IP Address]：トラッキングの対象 IP アドレスを入力します。通常、ルートのネクスト ホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。

（注） ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

[SLA ID]：SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。

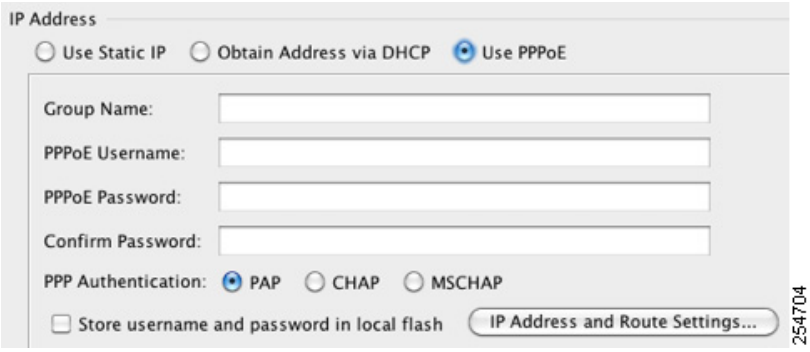
[Monitor Options]：このボタンをクリックすると [Route Monitoring Options] ダイアログボックスが開きます。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。

f. （オプション）DHCP クライアントが IP アドレス要求の探索を送信する場合に、DHCP パケット ヘッダーでブロードキャスト フラグを 1 に設定するには、[Enable DHCP Broadcast flag for DHCP request and discover messages] をオンにします。

DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。

g. （オプション）リースを更新するには、[Renew DHCP Lease] をクリックします。

- （シングル モードのみ）PPPoE を使用して IP アドレスを取得するには、[Use PPPoE] をオンにします。



a. [Group Name] フィールドで、グループ名を指定します。

b. [PPPoE Username] フィールドで、ISP から提供されたユーザ名を指定します。

c. [PPPoE Password] フィールドで、ISP から提供されたパスワードを指定します。

d. [Confirm Password] フィールドに、パスワードを再入力します。

e. PPP 認証の場合、[PAP]、[CHAP]、または [MSCHAP] のいずれかのオプション ボタンをクリックします。

PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。

f. （オプション）フラッシュ メモリにユーザ名とパスワードを保存するには、[Store Username and Password in Local Flash] チェックボックスをオンにします。

ASA は、NVRAM の特定の場所にユーザ名とパスワードを保存します。Auto Update Server が **clear config** コマンドを ASA に送信して、接続が中断されると、ASA は NVRAM からユーザ名とパスワードを読み取り、アクセス コンセントレータに対して再度認証できます。

g. （オプション）[PPPoE IP Address and Route Settings] ダイアログボックスを表示し、アドレッシングおよびトラッキングのオプションを選択するには、[IP Address and Route Settings] をクリックします。詳細については、「PPPoE IP Address and Route Settings」（P.12-11）を参照してください。

ステップ 8　（オプション）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

（注）（ASA 5512-X 以降）[Configure Hardware Properties] ボタンに関する情報については、「物理インターフェイスのイネーブル化およびイーサネット パラメータの設定」（P.10-15）を参照してください。

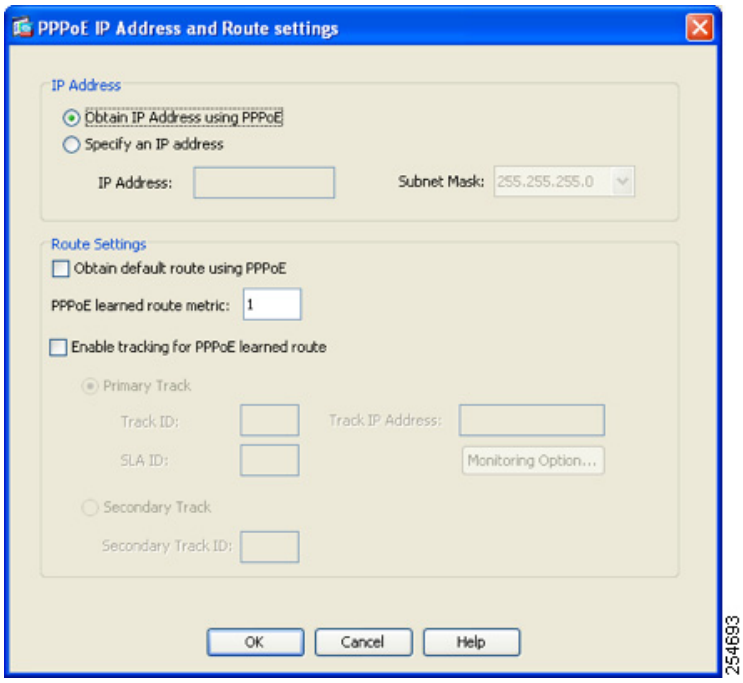
ステップ 9　[OK] をクリックします。

次の作業

- （オプション）MAC アドレスと MTU を設定します。「MAC アドレス、MTU、および TCP MSS の設定」（P.12-12）を参照してください。
- （オプション）IPv6 アドレッシングを設定します。「IPv6 アドレッシングの設定」（P.12-15）を参照してください。

PPPoE IP Address and Route Settings

[Configuration] > [Interfaces] > [Add/Edit Interface] > [General] > [PPPoE IP Address and Route Settings] > [PPPoE IP Address and Route Settings] ダイアログボックスで、PPPoE 接続のアドレッシング オプションとトラッキング オプションを選択できます。



フィールド

- [IP Address] エリア：IP アドレスを PPP から取得する方法または IP アドレスを指定する方法を選択します。次のフィールドがあります。
  - [Obtain IP Address using PPP]：ASA を選択してイネーブルにし、PPP を使用して IP アドレスを取得します。

– [Specify an IP Address]：ASA は、PPPoE サーバとネゴシエートするのではなく、IP アドレスとマスクを指定してアドレスを動的に割り当てます。

- [Route Settings] エリア：ルートおよびトラッキングの設定を行います。次のフィールドがあります。
  – [Obtain default route using PPPoE]：PPPoE クライアントがまだ接続を確立していない場合に、デフォルト ルートを設定します。このオプションを使用する場合は、スタティックに定義されたルートを設定に含めることができません。

    [PPPoE learned route metric]：アドミニストレーティブ ディスタンスを既知のルートに割り当てます。有効な値は、1 ～ 255 です。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。

  – [Enable tracking]：PPPoE の既知のルートのトラッキングをイネーブルにします。

    （注） ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

  – [Primary Track]：プライマリ PPPoE ルート トラッキングを設定するには、このオプションを選択します。
  – [Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。
  – [Track IP Address]：トラッキングの対象 IP アドレスを入力します。通常、ルートのネクスト ホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。
  – [SLA ID]：SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。
  – [Monitor Options]：このボタンをクリックすると [Route Monitoring Options] ダイアログボックスが開きます。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。
  – [Secondary Track]：セカンダリ PPPoE ルート トラッキングを設定するには、このオプションを選択します。
  – [Secondary Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

MAC アドレス、MTU、および TCP MSS の設定

ここでは、インターフェイスの MAC アドレスの設定方法、MTU の設定方法、および TCP MSS の設定方法を説明します。

MAC アドレスに関する情報

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。

ASASM では、すべての VLAN がバックプレーンから提供される同じ MAC アドレスを使用します。

冗長インターフェイスは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。このコマンドを使用して冗長インターフェイスに MAC アドレスを割り当てると、メンバー インターフェイスの MAC アドレスに関係なく、割り当てた MAC アドレスが使用されます。

EtherChannel の場合は、そのチャネル グループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。ポート チャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アドレスとして使用します。または、ポートチャネル インターフェイスの MAC アドレスを手動で設定することもできます。マルチ コンテキスト モードでは、EtherChannel ポート インターフェイスを含め、固有の MAC アドレスをインターフェイスに自動的に割り当てることができます。グループ チャネル インターフェイスのメンバーシップを変更する場合は、固有の MAC アドレスを手動で設定するか、またはマルチ コンテキスト モードで自動的に設定することを推奨します。ポートチャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。

マルチ コンテキスト モードでは、コンテキスト間でインターフェイスを共有している場合、固有の MAC アドレスをそれぞれのコンテキストのインターフェイスに割り当てることができます。この機能を使用すると、ASA はパケットを適切なコンテキストに容易に分類できます。固有の MAC アドレスがなくても共有インターフェイスを使用できますが、制限があります。詳細については、「ASA によるパケットの分類方法」（P.7-3）を参照してください。コンテキストの共有インターフェイスには、手動で各 MAC アドレスを割り当てることも、自動生成することもできます。MAC アドレスの自動生成については、「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」（P.7-25）を参照してください。MAC アドレスを自動生成する場合、この手順を使用して生成されたアドレスを上書きできます。

シングル コンテキスト モード、またはマルチ コンテキスト モードで共有されないインターフェイスの場合は、固有の MAC アドレスをサブインターフェイスに割り当てることを推奨します。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 コントロールを実行する場合があります。

MTU および TCP MSS に関する情報

「最大伝送単位および TCP 最大セグメント サイズのフラグメンテーションの制御」（P.10-8）を参照してください。

前提条件

- モデルに応じてインターフェイスを設定します。
  - ASA 5512-X 以降：第 10 章「基本的なインターフェイス コンフィギュレーション（ASA 5512-X 以降）」
  - ASASM：第 2 章「使用する前に」
  - ASAv：第 11 章「基本インターフェイスの設定（ASAv）」
- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.7-15）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [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。

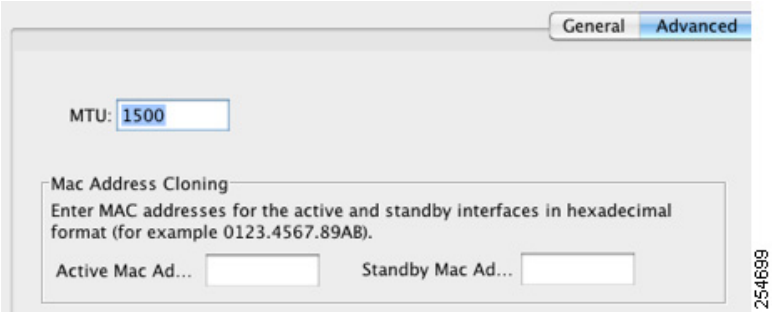
手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　インターフェイス行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[Advanced] タブをクリックします。



ステップ 4　MTU を設定する場合、またはジャンボ フレームのサポートをイネーブルにする（サポート対象モデルのみ）場合、[MTU] フィールドに 300 ～ 9198 バイト（ASAv の場合は 9000）の値を入力します。

デフォルトは 1500 バイトです。

（注）　冗長インターフェイスまたはポートチャネル インターフェイスに MTU を設定すると、ASA は、この設定をすべてのメンバー インターフェイスに適用します。

- ジャンボ フレームをサポートする、シングル モードのモデルの場合：いずれかのインターフェイスに 1500 を超える値を入力すると、ジャンボ フレーム サポートがすべてのインターフェイスに対して自動的にイネーブルになります。すべてのインターフェイスの MTU の設定を 1500 未満に戻すと、ジャンボ フレーム サポートがディセーブルになります。
- ジャンボ フレームをサポートするマルチ モードの場合：いずれかのインターフェイスに 1500 を超える値を入力する場合、必ずシステム コンフィギュレーションのジャンボ フレーム サポートをイネーブルにしてください。「ジャンボ フレーム サポートのイネーブル化」（P.10-31）を参照してください。

（注）　ジャンボ フレーム サポートをイネーブルまたはディセーブルにするには、ASA をリロードする必要があります。

ステップ 5　MAC アドレスをこのインターフェイスに手動で割り当てるには、[Active Mac Address] フィールドに MAC アドレスを H.H.H 形式（H は 16 ビットの 16 進数）で入力します。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

ステップ 6　フェールオーバーを使用する場合、[Standby Mac Address] フィールドにスタンバイ MAC アドレスを入力します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな 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。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 7　TCP MSS を設定するには、[Configuration] > [Firewall] > [Advanced] > [TCP Options] の順に選択します。次のオプションを設定します。

- [Force Maximum Segment Size for TCP]：最大 TCP セグメント サイズを 48 から最大数の範囲のバイト数で設定します。デフォルト値は 1380 バイトです。この機能は、0 バイトに設定することによってディセーブルにできます。
- [Force Minimum Segment Size for TCP]：48 から最大数の間で、ユーザが設定したバイト数未満にならないように最大セグメント サイズを上書きします。この機能は、デフォルトでディセーブルです（0 に設定）。

ステップ 8　セキュリティ グループ タグについては、「SGT とイーサネット タギングのイネーブル化」（P.33-24）を参照してください。

次の作業

（オプション）IPv6 アドレッシングを設定します。「IPv6 アドレッシングの設定」（P.12-15）を参照してください。

IPv6 アドレッシングの設定

この項では、IPv6 アドレッシングを設定する方法について説明します。

IPv6 に関する情報

ここでは、IPv6 の設定方法について説明します。

IPv6 アドレス指定

次の 2 種類の IPv6 のユニキャスト アドレスを設定できます。

- グローバル：グローバル アドレスは、パブリック ネットワークで使用可能なパブリック アドレスです。

- リンクローカル：リンクローカル アドレスは、直接接続されたネットワークだけで使用できるプライベート アドレスです。ルータは、リンクローカル アドレスを使用してパケットを転送するのではなく、特定の物理ネットワーク セグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決およびネイバー探索などの ND 機能に使用できます。

最低限、IPv6 が動作するようにリンクローカル アドレスを設定する必要があります。グローバル アドレスを設定すると、リンクローカル アドレスがインターフェイスに自動的に設定されるため、リンクローカル アドレスを個別に設定する必要はありません。グローバル アドレスを設定しない場合は、リンクローカル アドレスを自動的にするか、手動で設定する必要があります。

Modified EUI-64 インターフェイス ID

RFC 3513「Internet Protocol Version 6 (IPv6) Addressing Architecture」では、バイナリ値 000 で始まるものを除き、すべてのユニキャスト IPv6 アドレスのインターフェイス識別子部分は長さが 64 ビットで、Modified EUI-64 形式で組み立てることが要求されています。ASA では、ローカル リンクに接続されたホストにこの要件を適用できます。

この機能がインターフェイスでイネーブルになっていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
%ASA-3-325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカル リンク上のホストに対してのみ実行できます。ルータの背後にあるホストから受信したパケットは、アドレス形式の検証に失敗してドロップされます。これは、その送信元 MAC アドレスがルータの MAC アドレスであり、ホストの MAC アドレスではないためです。

グローバル IPv6 アドレスの設定

グローバル IPv6 アドレスを設定するには、次の手順を実行します。

（注）　グローバル アドレスを設定すると、リンクローカル アドレスは自動的に設定されるため、別々に設定する必要はありません。

制限事項

ASA は、IPv6 エニーキャスト アドレスはサポートしません。

前提条件

- モデルに応じてインターフェイスを設定します。
  - ASA 5512-X 以降：第 10 章「基本的なインターフェイス コンフィギュレーション（ASA 5512-X 以降）」
  - ASASM：第 2 章「使用する前に」
  - ASAv：第 11 章「基本インターフェイスの設定（ASAv）」
- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.7-15）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [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。

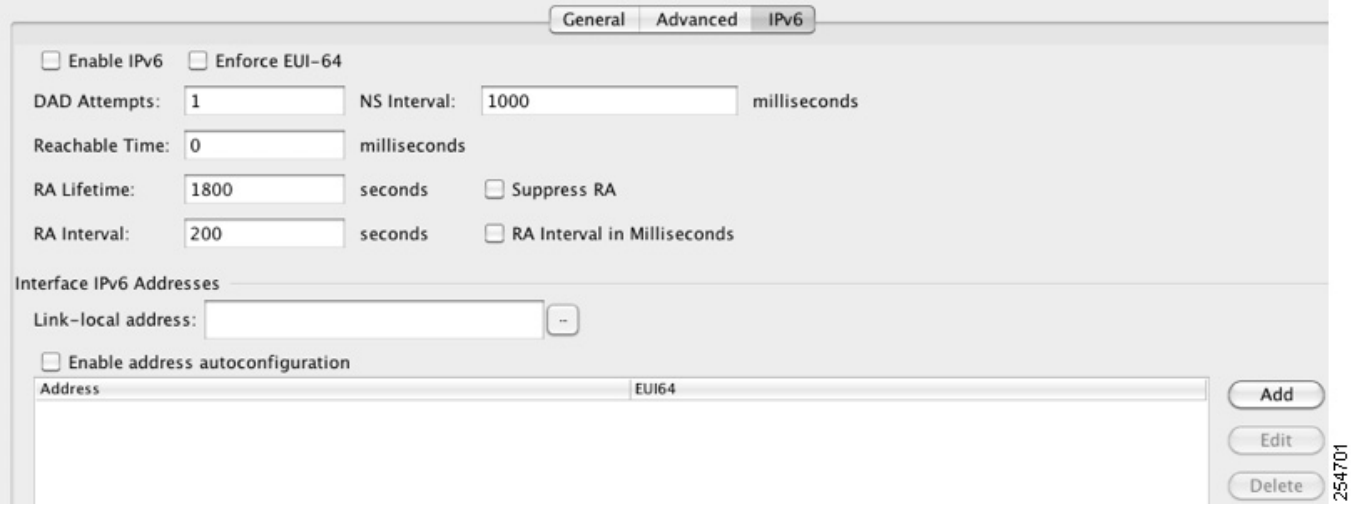
手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[IPv6] タブをクリックします。



ステップ 4　[Enable IPv6] チェックボックスをオンにします。

ステップ 5　（オプション）ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[Enforce EUI-64] チェックボックスをオンにします。

詳細については、「Modified EUI-64 インターフェイス ID」（P.12-16）を参照してください。

ステップ 6　（オプション）上部で、第 26 章「IPv6 ネイバー探索」を参照して IPv6 設定をカスタマイズします。

ステップ 7　グローバル IPv6 アドレスを次のいずれかの方法で設定します。

- ステートレス自動設定：[Interface IPv6 Addresses] エリアで、[Enable address autoconfiguration] チェックボックスをオンにします。

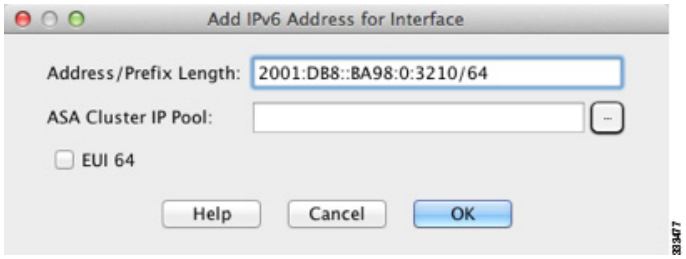
  インターフェイス上でステートレス自動設定をイネーブルにすると、受信したルータ アドバタイズメント メッセージのプレフィックスに基づいて IPv6 アドレスを設定します。ステートレスな自動設定がイネーブルになっている場合、インターフェイスのリンクローカル アドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

（注）　RFC 4862 では、ステートレスな自動設定に設定されたホストはルータ アドバタイズメント メッセージを送信しないと規定していますが、ASA はこの場合、ルータ アドバタイズメント メッセージを送信します。メッセージを非表示にする場合は、[Suppress RA] チェックボックスを参照してください。

- 手動設定：グローバル IPv6 アドレスを手動で設定するには、次の手順を実行します。

  a. [Interface IPv6 Addresses] エリアで、[Add] をクリックします。

  [Add IPv6 Address for Interface] ダイアログボックスが表示されます。



  b. [Address/Prefix Length] フィールドに、インターフェイス ID を含む完全なグローバル IPv6 アドレス、または IPv6 プレフィックス長と IPv6 プレフィックスのいずれかを入力します。プレフィックスだけを入力した場合は、必ず [EUI 64] チェックボックスをオンにして、Modified EUI-64 形式を使用してインターフェイス ID を生成するようにしてください。たとえば、2001:0DB8::BA98:0:3210/48（完全なアドレス）または 2001:0DB8::/48（プレフィックス、[EUI 64] はオン）。IPv6 アドレッシングの詳細については、「IPv6 形式のアドレス」（P.43-5）を参照してください。

  （注） ASA クラスタ IP プールについては、「個別インターフェイスの設定（管理インターフェイスの場合に推奨）」（P.9-44）を参照してください。

  c. [OK] をクリックします。

ステップ 8　（オプション）IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定するには、「ルータ アドバタイズメントの IPv6 プレフィックスの設定」（P.26-11）を参照してください。

ステップ 9　[OK] をクリックします。

[Configuration] > [Device Setup] > [Interfaces] ペインに戻ります。

IPv6 ネイバー探索の設定

IPv6 ネイバー探索を設定するには、第 26 章「IPv6 ネイバー探索」を参照してください。

（オプション）リンクローカル アドレスの自動設定

グローバル アドレスを設定する必要がなく、リンクローカル アドレスだけを設定する必要がある場合は、リンクローカル アドレスをインターフェイスの MAC アドレス（Modified EUI-64 形式。MAC アドレスで使用するビット数は 48 ビットであるため、インターフェイス ID に必要な 64 ビットを埋めるために追加ビットを挿入する必要があります。）

リンクローカル アドレスを手動で割り当てる場合（非推奨）については、「（オプション）リンクローカル アドレスの手動設定」（P.12-19）を参照してください。

Modified EUI-64 形式の適用および DAD 設定を含むその他の IPv6 オプションについては、「グローバル IPv6 アドレスの設定」（P.12-16）を参照してください。

リンクローカル アドレスをインターフェイスに自動的に設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[IPv6] タブをクリックします。

ステップ 4　[IPv6 configuration] 領域で、[Enable IPv6] チェックボックスをオンにします。

このオプションでは、IPv6 をイネーブルにし、インターフェイスの MAC アドレスに基づく Modified EUI-64 インターフェイス ID を使用してリンクローカル アドレスを自動的に生成します。

ステップ 5　[OK] をクリックします。

（オプション）リンクローカル アドレスの手動設定

グローバル アドレスを設定する必要がなく、リンクローカル アドレスだけを設定する必要がある場合は、リンクローカル アドレスを手動で定義できます。Modified EUI-64 形式に基づくリンクローカル アドレスを自動的に割り当てることを推奨します。たとえば、他のデバイスが Modified EUI-64 形式の使用を必要とする場合、手動で割り当てたリンクローカル アドレスのパケットはドロップされる可能性があります。

リンクローカル アドレスを自動的に割り当てる場合（推奨）については、「（オプション）リンクローカル アドレスの自動設定」（P.12-18）を参照してください。

Modified EUI-64 形式の適用および DAD 設定を含むその他の IPv6 オプションについては、「グローバル IPv6 アドレスの設定」（P.12-16）を参照してください。

インターフェイスにリンクローカル アドレスを割り当てるには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[IPv6] タブをクリックします。

ステップ 4　リンクローカル アドレスを設定するには、[Link-local address] フィールドにアドレスを入力します。

リンクローカル アドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。たとえば fe80::20d:88ff:feee:6a82 のようになります。IPv6 アドレッシングの詳細については、「IPv6 形式のアドレス」（P.43-5）を参照してください。

ステップ 5　[OK] をクリックします。

同じセキュリティ レベルの通信の許可

デフォルトでは、同じセキュリティ レベルのインターフェイスは相互に通信することができません。また、パケットは同じインターフェイスを出入りすることができません。この項では、複数のインターフェイスが同じセキュリティ レベルの場合にインターフェイス間通信をイネーブルにする方法と、インターフェイス内通信をイネーブルにする方法について説明します。

インターフェイス間通信に関する情報

同じセキュリティ レベルのインターフェイスで相互通信を許可する利点としては、次のものがあります。

- 101 より多い数の通信インターフェイスを設定できます。

  各インターフェイスで異なるセキュリティ レベルを使用したときに、同一のセキュリティ レベルにインターフェイスを割り当てないと、各レベル（0 ～ 100）に 1 つのインターフェイスしか設定できません。

- ACL がなくても同じセキュリティ レベルのインターフェイスすべての間で自由にトラフィックが流れるようにできます。

同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。

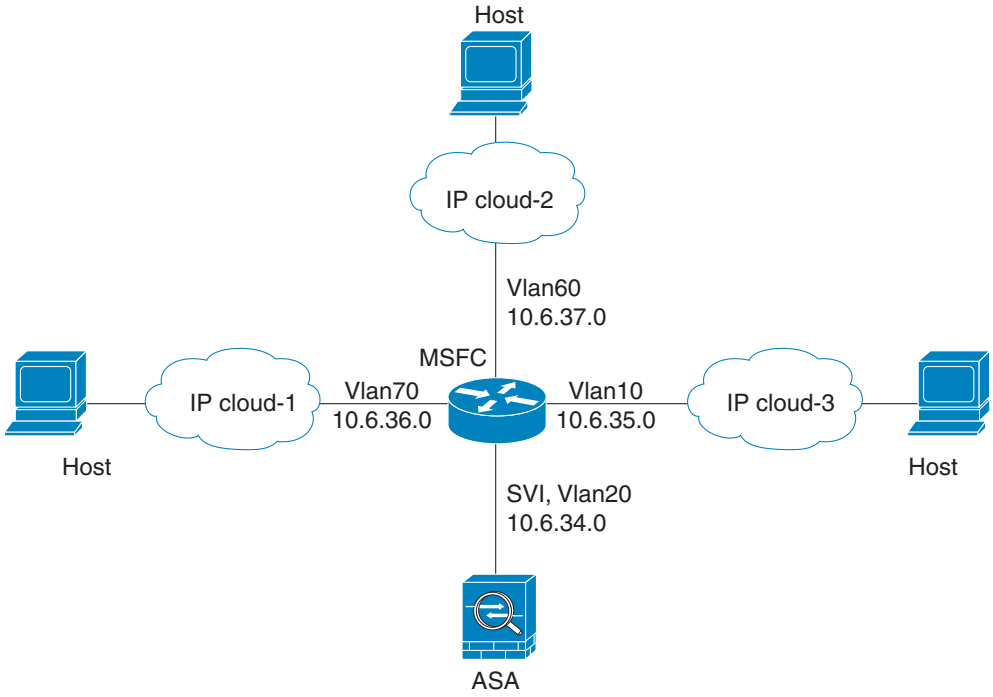
インターフェイス内通信に関する情報

インターフェイス内通信は、インターフェイスに入ってくる VPN トラフィックに対して使用できますが、その場合は同じインターフェイスのルートから外されます。この場合、VPN トラフィックは暗号化解除されたり、別の VPN 接続のために再度暗号化されたりする場合があります。たとえば、ハブ アンド スポーク VPN ネットワークがあり、ASA がハブ、リモート VPN ネットワークがスポークの場合、あるスポークが別のスポークと通信するためには、トラフィックは ASA に入ってから他のスポークに再度ルーティングされる必要があります。

（注）この機能で許可されたすべてのトラフィックは、引き続きファイアウォール規則に従います。リターン トラフィックが ASA を通過できない原因となるため、非対称なルーティング状態にしないよう注意してください。

ASASM の場合、この機能をイネーブルにするには、まず、パケットがスイッチ経由で宛先ホストに直接送信されるのではなく、ASA MAC アドレスに送信されるように、MSFC を正しく設定する必要があります。図 12-1 に、同一インターフェイス上のホストが通信する必要があるネットワークを示します。

図 12-1　　同一インターフェイス上のホスト間の通信



次の設定例では、図 12-1 に示すネットワークのポリシー ルーティングをイネーブルにするために使用される Cisco IOS **route-map** コマンドを示します。

```
route-map intra-inter3 permit 0
    match ip address 103
    set interface Vlan20
    set ip next-hop 10.6.34.7
!
route-map intra-inter2 permit 20
    match ip address 102
    set interface Vlan20
    set ip next-hop 10.6.34.7
!
route-map intra-inter1 permit 10
    match ip address 101
    set interface Vlan20
    set ip next-hop 10.6.34.7
```

手順の詳細

- 同じセキュリティ レベルのインターフェイス間の通信をイネーブルにするには、[Configuration] > [Interfaces] ペインで、[Enable traffic between two or more interfaces which are configured with same security level] をオンにします。
- 同じインターフェイスに接続されているホスト間の通信をイネーブルにするには、[Enable traffic between two or more hosts connected to the same interface] をオンにします。

インターフェイスのオン/オフ

ここでは、インターフェイスのオン/オフの方法について説明します。

デフォルトでは、すべてのインターフェイスがイネーブルです。マルチ コンテキスト モードでは、コンテキスト内でインターフェイスをディセーブルにした場合、または再度イネーブルにした場合は、そのコンテキスト インターフェイスだけが影響を受けます。ただし、システム実行スペースでインターフェイスをディセーブルにした場合、または再度イネーブルにした場合は、全コンテキストに対応するそのインターフェイスに影響します。

手順の詳細

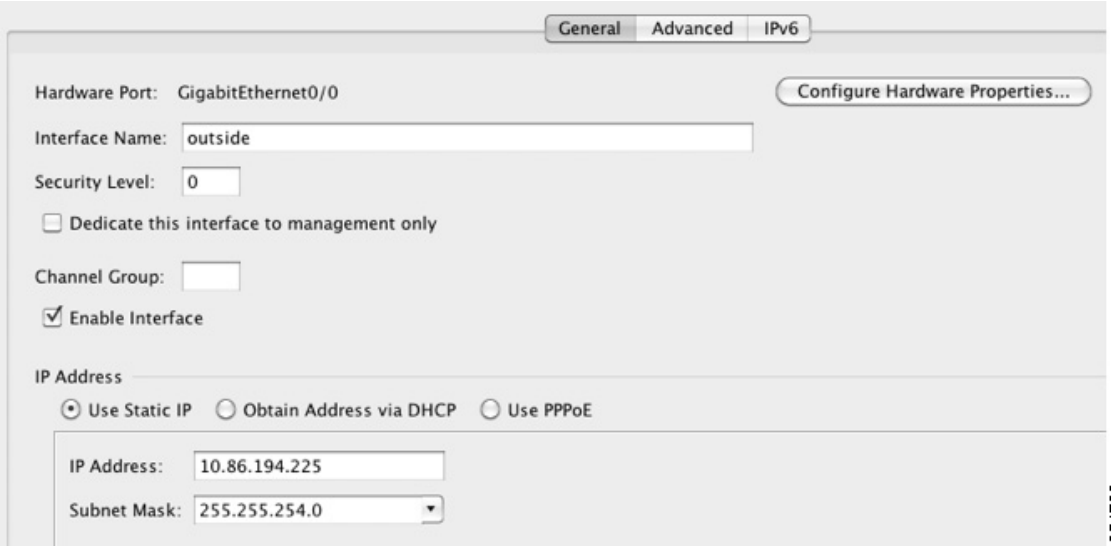
ステップ 1　コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

デフォルトでは、すべての物理インターフェイスが一覧表示されます。

ステップ 2　設定する VLAN インターフェイスをクリックし、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。



ステップ 3　インターフェイスをイネーブルまたはディセーブルにするには、[Enable Interface] チェックボックスをオンまたはオフにします。

インターフェイスのモニタリング

- 「ARP Table」（P.12-23）
- 「DHCP」（P.12-23）
- 「MAC Address Table」（P.12-26）

- 「Dynamic ACLs」（P.12-26）
- 「Interface Graphs」（P.12-26）
- 「PPPoE Client」（P.12-29）
- 「インターフェイス接続」（P.12-29）

ARP Table

[Monitoring] > [Interfaces] > [ARP Table] ペインには、スタティックとダイナミック エントリを含む ARP テーブルが表示されます。ARP テーブルには、MAC アドレスを所定のインターフェイスの IP アドレスにマッピングするエントリが含まれます。

フィールド

- [Interface]：マッピングに関連付けられているインターフェイス名を一覧表示します。
- [IP Address]：IP アドレスを表示します。
- [MAC Address]：MAC アドレスを表示します。
- [Proxy ARP]：インターフェイスでプロキシ ARP がイネーブルになっている場合は [Yes] と表示します。インターフェイスでプロキシ ARP がイネーブルになっていない場合は [No] と表示します。
- [Clear]：ダイナミック ARP テーブルのエントリをクリアします。スタティック エントリはクリアされません。
- [Refresh]：ASA の現在の情報でテーブルをリフレッシュし、[Last Updated] の日付と時刻を更新します。
- [Last Updated]：*表示専用*。表示が更新された日付と時刻を示します。

DHCP

ASA では、クライアントに割り当てられているアドレス、ASA インターフェイスのリース情報、および DHCP 統計情報を含む DHCP ステータスをモニタできます。

DHCP Server Table

[Monitoring] > [Interfaces] > [DHCP] > [DHCP Server Table] には、DHCP クライアントに割り当てられている IP アドレスが一覧表示されます。

フィールド

- [IP Address]：クライアントに割り当てられている IP アドレスを表示します。
- [Client-ID]：クライアントの MAC アドレスまたは ID を表示します。
- [Lease Expiration]：DHCP リースの期限が満了する日付を表示します。リースは、クライアントが割り当てられている IP アドレスを使用できる期間を示します。また、残り時間は、[Last Updated] 表示専用フィールドのタイムスタンプを基準に秒数で表示されます。
- [Number of Active Leases]：DHCP リースの合計数を表示します。
- [Refresh]：ASA の情報をリフレッシュします。
- [Last Updated]：テーブルのデータが最後に更新された日付を表示します。

DHCP Client Lease Information

DHCP サーバから ASA インターフェイスの IP アドレスを取得すると、[Monitoring] > [Interfaces] > [DHCP] > [DHCP Server Table] > [DHCP Client Lease Information] ペインには、DHCP リースに関する情報が表示されます。

フィールド

- [Select an interface]：ASA のインターフェイスを一覧表示します。DHCP リースを表示するインターフェイスを選択します。インターフェイスに DHCP リースが複数ある場合、表示するインターフェイスと IP アドレスのペアを選択します。
- [Attribute and Value]：インターフェイス DHCP リースの属性と値を一覧表示します。
  - [Temp IP addr]：*表示専用*。インターフェイスに割り当てられている IP アドレス。
  - [Temp sub net mask]：*表示専用*。インターフェイスに割り当てられているサブネット マスク。
  - [DHCP lease server]：*表示専用*。DHCP サーバ アドレス。
  - [state]：*表示専用*。DHCP リースの状態で、次のとおりです。

    [Initial]：初期化状態で、ASA がリースを取得するプロセスを開始します。この状態は、リースが終了したか、リースのネゴシエーションに失敗したときにも表示されます。

    [Selecting]：ASA は 1 つ以上の DHCP サーバから DHCPOFFER メッセージを受信することを待機しており、メッセージを選択できます。

    [Requesting]：ASA は、要求を送信した送信先サーバからの応答を待機しています。

    [Purging]：ASA は、エラーが発生したためリースを削除しています。

    [Bound]：ASA は有効なリースを保持し、正常に動作しています。

    [Renewing]：ASA はリースを更新しようとしています。DHCPREQUEST メッセージを現在の DHCP サーバに定期的に送信し、応答を待機します。

    [Rebinding]：ASA は元のサーバのリースを更新することに失敗したため、いずれかのサーバから応答を受け取るかリースが終了するまで DHCPREQUEST メッセージを送信します。

    [Holddown]：ASA はリースを削除するプロセスを開始しました。

    [Releasing]：ASA は IP アドレスが不要になったことを示すリリース メッセージをサーバに送信します。
  - [Lease]：*表示専用*。DHCP サーバによって指定される、インターフェイスがこの IP アドレスを使用できる時間の長さ。
  - [Renewal]：*表示専用*。インターフェイスがこのリースを自動的に更新しようとするまでの時間の長さ。
  - [Rebind]：*表示専用*。ASA が DHCP サーバに再バインドしようとするまでの時間の長さ。再バインドが発生するのは、ASA が元の DHCP サーバと通信できず、リース期間の 87.5% を経過した場合です。ASA は、DHCP 要求をブロードキャストすることによって、使用可能な任意の DHCP サーバに接続を試みます。
  - [Next timer fires after]：*表示専用*。内部タイマーがトリガーするまでの秒数。
  - [Retry count]：*表示専用*。ASA がリースを設定しようとしているとき、このフィールドは、ASA が DHCP メッセージの送信を試行した回数を示します。たとえば、ASA が Selecting 状態の場合、この値は ASA が探索メッセージを送信した回数を示します。ASA が Requesting 状態の場合、この値は ASA が要求メッセージを送信した回数を示します。

  - [Client-ID]：*表示専用*。サーバとのすべての通信に使用したクライアント ID。
  - [Proxy]：*表示専用*。このインターフェイスが VPN クライアント用のプロキシ DHCP クライアントかどうかを True または False で指定します。
  - [Hostname]：*表示専用*。クライアントのホスト名。

DHCP Statistics

[Monitoring] > [Interfaces] > [DHCP] > [DHCP Statistics] ペインには、DHCP サーバ機能の統計情報が表示されます。

フィールド

- [Message Type]：送受信された DHCP メッセージのタイプを一覧表示します。
  - BOOTREQUEST
  - DHCPDISCOVER
  - DHCPREQUEST
  - DHCPDECLINE
  - DHCPRELEASE
  - DHCPINFORM
  - BOOTREPLY
  - DHCPOFFER
  - DHCPACK
  - DHCPNAK
- [Count]：特定のメッセージが処理された回数を表示します。
- [Direction]：メッセージ タイプが Sent か Received かを示します。
- [Total Messages Received]：ASA で受信したメッセージの合計数を表示します。
- [Total Messages Sent]：ASA で送信したメッセージの合計数を表示します。
- [Counter]：次のような DHCP の全般的な統計データを表示します。
  - DHCP UDP Unreachable Errors
  - DHCP Other UDP Errors
  - Address Pools
  - Automatic Bindings
  - Expired Bindings
  - Malformed Messages
- [Value]：各カウンタ項目の数を表示します。
- [Refresh]：DHCP テーブルのリストを更新します。
- [Last Updated]：テーブルのデータが最後に更新された日付を表示します。

MAC Address Table

[Monitoring] > [Interfaces] > [MAC Address Table] ペインには、スタティックおよびダイナミック MAC アドレス エントリが表示されます。MAC アドレス テーブルおよび追加のスタティック エントリに関する詳細情報については、「MAC Address Table」（P.12-26）を参照してください。

フィールド

- [Interface]：エントリに関連付けられているインターフェイス名を表示します。
- [MAC Address]：MAC アドレスを表示します。
- [Type]：エントリがスタティックかダイナミックかを表示します。
- [Age]：エントリの経過時間を分数で表示します。タイムアウトを設定するには、「MAC Address Table」（P.12-26）を参照してください。
- [Refresh]：ASA の現在の情報でテーブルをリフレッシュします。

Dynamic ACLs

[Monitoring] > [Interfaces] > [Dynamic ACLs] ペインには、ダイナミック ACL のテーブルが表示されます。ダイナミック ACL は、ASA によって自動的に作成、アクティブ化、削除される点を除いて、ユーザ設定の ACL と機能上同じです。これらの ACL はコンフィギュレーションには表示されず、このテーブルだけに表示されます。ダイナミック ACL は、ACL ヘッダーの “(dynamic)” キーワードで区別されます。

このテーブルで ACL を選択すると、その ACL の内容が下部のテキスト フィールドに表示されます。

フィールド

- [ACL]：ダイナミック ACL の名前を表示します。
- [Element Count]：ACL の要素の数を表示します。
- [Hit Count]：ACL のすべての要素に対する合計ヒット数を表示します。

Interface Graphs

[Monitoring] > [Interfaces] > [Interface Graphs] ペインには、インターフェイス統計情報をグラフ形式またはテーブル形式で表示できます。インターフェイスをコンテキスト間で共有している場合、ASA には現在のコンテキストの統計情報だけが表示されます。サブインターフェイスに表示される統計情報の数は、物理インターフェイスに表示される統計情報の数のサブセットです。

フィールド

- [Available Graphs for]：モニタリングに使用可能な統計情報のタイプを一覧表示します。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。
  - [Byte Counts]：インターフェイスのバイト入力およびバイト出力の数を表示します。
  - [Packet Counts]：インターフェイスのパケット入力およびパケット出力の数を表示します。
  - [Packet Rates]：インターフェイスのパケット入力およびパケット出力のレートを表示します。

– [Bit Rates]：インターフェイスの入出力のビット レートを表示します。

– [Drop Packet Count]：インターフェイスでドロップされたパケットの数を表示します。

物理インターフェイスに追加して表示できる統計情報は次のとおりです。

– [Buffer Resources]：次の統計情報を表示します。

[Overruns]：入力速度が、ASA のデータ処理能力を超えたため、ASA がハードウェア バッファに受信したデータを処理できなかった回数。

[Underruns]：ASA で処理できる速度より速くトランスミッタが動作した回数。

[No Buffer]：メイン システムにバッファ スペースがなかったために廃棄された受信パケットの数。この数を、無視された数と比較してください。イーサネット ネットワーク上のブロードキャスト ストームは、多くの場合、入力バッファ イベントがないことに原因があります。

– [Packet Errors]：次の統計情報を表示します。

[CRC]：巡回冗長検査エラーの数。ステーションがフレームを送信すると、フレームの末尾に CRC を付加します。この CRC は、フレーム内のデータに基づくアルゴリズムから生成されます。送信元と宛先の間でフレームが変更された場合、ASA は CRC が一致しないことを通知します。CRC の数値が高いことは、通常、コリジョンの結果であるか、ステーションが不良データを送信することが原因です。

[Frame]：フレーム エラーの数。不良フレームには、長さが正しくないパケットや、フレーム チェックサムが正しくないパケットがあります。このエラーは通常、コリジョンまたはイーサネット デバイスの誤動作が原因です。

[Input Errors]：ここにリストされている他のタイプのものも含めた入力エラーの合計数。また、その他の入力関連のエラーによって入力エラー数が増えたり、一部のデータグラムに複数のエラーが存在していたりする可能性があります。したがって、この合計は、他のタイプにリストされているエラーの数を超えることがあります。

[Runts]：最小パケット サイズの 64 バイトよりも小さかったために廃棄されたパケットの数。ラントは通常、コリジョンによって発生します。不適切な配線や電気干渉によって発生することもあります。

[Giants]：最大パケット サイズを超えたために廃棄されたパケットの数。たとえば、1518 バイトよりも大きいイーサネット パケットはジャイアントと見なされます。

[Deferred]：FastEthernet インターフェイスだけ。リンク上のアクティビティが原因で送信前に保留されたフレームの数。

– [Miscellaneous]：受信したブロードキャストの統計情報を表示します。

– [Collision Counts]：FastEthernet インターフェイスだけ。次の統計情報を表示します。

[Output Errors]：設定されている衝突の最大数を超えたために伝送されなかったフレームの数。このカウンタは、ネットワーク トラフィックが多い場合にのみ増加します。

[Collisions]：イーサネット衝突（1 つまたは複数の衝突）が原因で、再度伝送されたメッセージ数。これは通常、過度に延長した LAN で発生します（イーサネット ケーブルまたはトランシーバ ケーブルが長すぎる、ステーション間のリピータが 2 つよりも多い、またはマルチポート トランシーバのカスケードが多すぎる場合）。衝突するパケットは、出力パケットによって 1 回だけカウントされます。

[Late Collisions]：通常の衝突ウィンドウの外で衝突が発生したために伝送されなかったフレームの数。レイト コリジョンは、パケットの送信中に遅れて検出されるコリジョンです。これは通常発生しません。2 つのイーサネット ホストが同時に通信しようとした場合、早期にパケットが衝突して両者がバックオフするか、2 番目のホストが 1 番目のホストの通信状態を確認して待機します。レイト コリジョンが発生すると、

デバイスは割り込みを行ってイーサネット上にパケットを送信しようとしますが、ASA はパケットの送信を部分的に完了しています。ASA は、パケットの最初の部分を保持するバッファを解放した可能性があるため、パケットを再送しません。このことはあまり問題になりません。その理由は、ネットワーキング プロトコルはパケットを再送することでコリジョンを処理する設計になっているためです。ただし、レイト コリジョンはネットワークに問題が存在することを示しています。一般的な問題は、リピータで接続された大規模ネットワーク、および仕様の範囲を超えて動作しているイーサネット ネットワークです。

– [Input Queue]：入力キューの現在のパケット数および最大パケット数を表示します。次の統計情報が含まれます。

  [Hardware Input Queue]：ハードウェア キューのパケット数。

  [Software Input Queue]：ソフトウェア キューのパケット数。

– [Output Queue]：出力キューの現在のパケット数および最大パケット数を表示します。次の統計情報が含まれます。

  [Hardware Output Queue]：ハードウェア キューのパケット数。

  [Software Output Queue]：ソフトウェア キューのパケット数。

- [Add]：選択した統計タイプを、選択したグラフ ウィンドウに追加します。
- [Remove]：選択したグラフ ウィンドウから、選択した統計タイプを削除します。削除している項目が他のパネルから追加され、[Available Graphs] ペインに戻されていない場合、このボタン名は [Delete] に変わります。
- [Show Graphs]：統計タイプを追加するグラフ ウィンドウ名を表示します。すでにグラフ ウィンドウを開いている場合は、デフォルトで新しいグラフ ウィンドウがリストされます。すでに開いているグラフに統計タイプを追加する場合は、開いているグラフ ウィンドウの名前を選択します。すでにグラフに含まれている統計情報が [Selected Graphs] ペインに表示され、タイプを追加できます。グラフ ウィンドウには ASDM、インターフェイスの IP アドレス、および "Graph" という順番で名前が付けられます。後続のグラフは、「Graph (2)」のように名前が付けられます。
- [Selected Graphs]：選択したグラフ ウィンドウに表示する統計タイプを表示します。タイプを 4 つまで含めることができます。
  – [Show Graphs]：グラフ ウィンドウを表示するか、または、追加した場合は追加の統計タイプでグラフを更新します。

Graph/Table

[Monitoring] > [Interfaces] > [Interface Graphs] > [Graph/Table] ウィンドウには、選択した統計情報のグラフが表示されます。 [Graph] ウィンドウには、最大 4 つのグラフおよびテーブルを同時に表示することができます。デフォルトで、グラフまたはテーブルにリアルタイムな統計情報が表示されます。履歴メトリック（「履歴メトリックのイネーブル化」（P.3-34）を参照）をイネーブルにすると、過去の期間の統計情報を表示できます。

フィールド

- [View]：グラフまたはテーブルを表示する期間を設定します。リアルタイム以外の期間を表示するには、履歴メトリック（「履歴メトリックのイネーブル化」（P.3-34）を参照）をイネーブルにします。次のオプションの指定に従ってデータが更新されます。
  – Real-time, data every 10 sec
  – Last 10 minutes, data every 10 sec

  - Last 60 minutes, data every 1 min
  - Last 12 hours, data every 12 min
  - Last 5 days, data every 2 hours
- [Export]：グラフをカンマ区切り形式でエクスポートします。[Graph] ウィンドウに複数のグラフまたはテーブルがある場合、[Export Graph Data] ダイアログボックスが表示されます。名前の横のチェックボックスを選択して、リストされているグラフおよびテーブルを 1 つ以上選択します。
- [Print]：グラフまたはテーブルを印刷します。[Graph] ウィンドウに複数のグラフまたはテーブルがある場合、[Print Graph] ダイアログボックスが表示されます。[Graph/Table Name] リストから印刷するグラフまたはテーブルを選択します。
- [Bookmark]：ブラウザ ウィンドウに、[Graph] ウィンドウ上のすべてのグラフおよびテーブルへのリンク 1 つと、各グラフまたはテーブルへの個別のリンクが表示されます。ブラウザでこれらの URL をブックマークとしてコピーできますグラフの URL を開くときに、ASDM を実行している必要はありません。ブラウザによって ASDM が起動され、グラフが表示されます。

PPPoE Client

[Monitoring] > [Interfaces] > [PPPoE Client] > [PPPoE Client Lease Information] ペインには、現在の PPPoE 接続に関する情報が表示されます。

フィールド

[Select a PPPoE interface]：PPPoE クライアントのリース情報を表示するインターフェイスを選択します。

[Refresh]：ASA から最新の PPPoE 接続情報をロードして表示します。

インターフェイス接続

[Monitoring] > [Interfaces] ツリーの [Monitoring] > [Interfaces] > *インターフェイス接続*ノードは、スタティック ルート トラッキングが設定されている場合にだけ表示されます。複数のルートを追跡している場合、追跡されるルートが含まれている各インターフェイスにノードがあります。

ルート トラッキングに関する詳細については、次の項を参照してください。

- 「[Track Status for]」（P.12-29）
- 「[Monitoring Statistics for]」（P.12-30）

[Track Status for]

[Monitoring] > [Interfaces] > インターフェイス接続 > [Track Status for] ペインには、トラッキング対象オブジェクトに関する情報が表示されます。

フィールド

- [Tracked Route]：*表示専用*。トラッキング プロセスに関連付けられているルートを表示します。
- [Route Statistics]：*表示専用*。オブジェクトの到達性情報を表示します。到達性情報で最後に変更があった場合は、オペレーションのリターンコード、およびトラッキングを実行するプロセスを表示します。

[Monitoring Statistics for]

[Monitoring] > [Interfaces] > インターフェイス接続 > [Monitoring Statistics for] ペインには、SLA モニタリング プロセスの統計情報が表示されます。

フィールド

- [SLA Monitor ID]：*表示専用*。SLA モニタリング プロセスの ID を表示します。
- [SLA statistics]：*表示専用*。プロセスが変更された最後の時刻、試行されたオペレーション回数、スキップされたオペレーション回数などの SLA モニタリング統計情報を表示します。

ルーテッド モードのインターフェイスの機能履歴

表 12-1 に、この機能のリリース履歴を示します。

表 12-1　　インターフェイスの機能履歴

機能名	リリース	機能情報
VLAN 数の増加	7.0(5)	次の制限値が増加されました。 • ASA 5510 基本ライセンスの VLAN 数が 0 から 10 に増えました。 • ASA 5510 Security Plus ライセンスの VLAN 数が 10 から 25 に増えました。 • ASA 5520 の VLAN 数が 25 から 100 に増えました。 • ASA 5540 の VLAN 数が 100 から 200 に増えました。
VLAN 数の増加	7.2(2)	ASA 5505 上の Security Plus ライセンスに対する VLAN 最大数が、5（3 つのフル機能インターフェイス、1 つのフェールオーバー インターフェイス、1 つのバックアップ インターフェイスに制限されるインターフェイス）から 20 のフル機能インターフェイスに増加されました。また、トランク ポート数も 1 から 8 に増加されました。フル機能のインターフェイスの数が 20 になり、バックアップ ISP インターフェイスを停止するために backup interface コマンドを使用する必要がなくなりました。つまり、バックアップ ISP インターフェイス用にフル機能のインターフェイスを使用できるようになりました。backup interface コマンドは、これまでどおり Easy VPN 設定用に使用できます。 VLAN の制限値も変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。

表 12-1　インターフェイスの機能履歴 （続き）

機能名	リリース	機能情報
ASA 5510 Security Plus ライセンスに対するギガビット イーサネット サポート	7.2(3)	ASA 5510 は、GE（ギガビット イーサネット）を Security Plus ライセンスのあるポート 0 および 1 でサポートするようになりました。ライセンスを Base から Security Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 ポートの容量は、元の FE（ファスト イーサネット）の 100 Mbps から GE の 1000 Mbps に増加します。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。
ASA 5505 に対するネイティブ VLAN サポート	7.2(4)/8.0(4)	ネイティブ VLAN を ASA 5505 トランク ポートに割り当てることができるようになりました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interfaces] > [Switch Ports] > [Edit Switch Port]。
ASA 5580 に対するジャンボ パケット サポート	8.1(1)	Cisco ASA 5580 はジャンボ フレームをサポートしています。ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび FCS を含む）より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネット フレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能（ACL など）の最大使用量が制限される場合があります。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface] > [Advanced]。
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。
トランスペアレント モードの IPv6 のサポート	8.2(1)	トランスペアレント ファイアウォール モードの IPv6 サポートが導入されました。
ASA 5580 10 ギガビット イーサネット インターフェイスでのフロー制御のポーズ フレームのサポート	8.2(2)	フロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりました。 次の画面が変更されました。 （シングル モード）[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface] > [Advanced] （マルチ モード、システム）[Configuration] > [Interfaces] > [Add/Edit Interface]

トランスペアレント モードのインターフェイス

この章では、トランスペアレント ファイアウォール モードですべてのモデルのインターフェイス コンフィギュレーションを実行するためのタスクについて説明します。

（注） マルチ コンテキスト モードでは、この項のタスクをコンテキスト実行スペースで実行してください。[Configuration] > [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。

トランスペアレント モードのインターフェイスに関する情報

トランスペアレント モードのブリッジ グループ

セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジ グループにグループ化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックは Cisco ASA 内の他のブリッジ

グループにはルーティングされません。また、トラフィックは外部ルータから ASA 内の他のブリッジ グループにルーティングされる前に、ASA から出る必要があります。ブリッジング機能はブリッジ グループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、すべてのブリッジ グループで共有されます。セキュリティ ポリシーを完全に分離するには、各コンテキスト内に 1 つのブリッジ グループにして、セキュリティ コンテキストを使用します。コンテキストまたはシングル モードごとに、少なくとも 1 つのブリッジ グループが必要です。

ブリッジ グループにはそれぞれ管理 IP アドレスが必要です。別の管理方法については、「管理インターフェイス」（P.10-2）を参照してください。

（注）　ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。管理 IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

セキュリティ レベル

各インターフェイスには、0（最下位）～ 100（最上位）のセキュリティ レベルを設定する必要があります。たとえば、内部ホスト ネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル 0 が割り当てられる場合があります。DMZ など、その他のネットワークはその中間に設定できます。複数のインターフェイスを同じセキュリティ レベルに割り当てることができます。詳細については、「同じセキュリティ レベルの通信の許可」（P.13-22）を参照してください。

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。ACL をインターフェイスに適用して、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイスの通信をイネーブルにすると（「同じセキュリティ レベルの通信の許可」（P.13-22）を参照）、同じセキュリティ レベルまたはそれより低いセキュリティ レベルの他のインターフェイスにアクセスするインターフェイスは、暗黙的に許可されます。

- インスペクション エンジン：一部のアプリケーション インスペクション エンジンはセキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。
  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - SQL*Net インスペクション エンジン：SQL*Net（旧称 OraServ）ポートとの制御接続が一対のホスト間に存在する場合、着信データ接続だけが ASA を通過することが許可されます。

- フィルタリング：HTTP(S) および FTP フィルタリングは、（高いレベルから低いレベルへの）発信接続にのみ適用されます。

  同じセキュリティ レベルのインターフェイス間の通信をイネーブルにすると、どちらの方向のトラフィックにもフィルタリングが適用できます。

- **established** コマンド：このコマンドを使用すると、高いレベルのホストから低いレベルのホストへの接続がすでに確立されている場合、低いセキュリティ レベルのホストから高いセキュリティ レベルのホストへの戻り接続が許可されます。

  セキュリティ レベルが同じインターフェイス間の通信をイネーブルにすると、両方向に対して **established** コマンドを設定できます。

トランスペアレント モードのインターフェイスのライセンス要件

モデル	ライセンス要件
ASA 5512-X	VLAN： 基本ライセンス：50 Security Plus ライセンス：100 すべての種類のインターフェイス： 基本ライセンス：716 Security Plus ライセンス：916
ASA 5515-X	VLAN： 基本ライセンス：100 すべての種類のインターフェイス： 基本ライセンス：916
ASA 5525-X	VLAN： 基本ライセンス：200 すべての種類のインターフェイス： 基本ライセンス：1316
ASA 5545-X	VLAN： 基本ライセンス：300 すべての種類のインターフェイス： 基本ライセンス：1716
ASA 5555-X	VLAN： 基本ライセンス：500 すべての種類のインターフェイス： 基本ライセンス：2516
ASA 5585-X	VLAN： 基本ライセンスと Security Plus ライセンス：1024 SSP-10 および SSP-20 のインターフェイス速度： 基本ライセンス：ファイバ インターフェイスの場合 1 ギガビット イーサネット 10 GE I/O ライセンス（Security Plus）：ファイバ インターフェイスの場合 10 ギガビット イーサネット （SSP-40 および SSP-60 は 10 ギガビット イーサネットをデフォルトでサポートします）。 すべての種類のインターフェイス： 基本ライセンスと Security Plus ライセンス：4612

（注）　VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。

すべてのタイプのインターフェイスには、VLAN、物理、冗長、ブリッジ グループ、EtherChannel インターフェイスなど、すべてを合わせたインターフェイスの最大数が含まれます。コンフィギュレーションで定義されているすべての **interface** が、この制限に対してカウントされます。

モデル	ライセンス要件
ASASM	VLAN： 基本ライセンス：1000

トランスペアレント モードのインターフェイスに関するガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

- マルチ コンテキスト モードでの ASA 5512-X 以降の場合、第 10 章「基本的なインターフェイス コンフィギュレーション（ASA 5512-X 以降）」に従って、システム実行スペースで物理インターフェイスを設定します。次に、この章に従って、コンテキスト実行スペースで論理インターフェイス パラメータを設定します。マルチ コンテキスト モードの ASASM の場合は、スイッチのスイッチ ポートおよび VLAN を設定し、第 2 章「使用する前に」に従って VLAN を ASASM に割り当てます。

  ASAv はマルチ コンテキスト モードをサポートしません。

- 設定できるのは、システム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。

ファイアウォール モードのガイドライン

- シングル モードまたはマルチ モードのコンテキストごとに、最大 250 個のブリッジ グループを設定できます。少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があることに注意してください。
- 各ブリッジ グループには、最大 4 つのインターフェイスを含めることができます。
- IPv4 の場合は、管理トラフィックと、ASA を通過するトラフィックの両方の各ブリッジ グループに対し、管理 IP アドレスが必要です。

  各インターフェイスに IP アドレスが必要なルーテッド モードとは異なり、トランスペアレント ファイアウォールではブリッジ グループ全体に 1 つの IP アドレスが割り当てられています。ASA は、この IP アドレスを、システム メッセージや AAA 通信など、ASA で発信されるパケットの送信元アドレスとして使用します。ブリッジ グループ管理アドレスに加えて、一部のモデルの管理インターフェイスをオプションで設定できます。詳細については、「管理インターフェイス」（P.10-2）を参照してください。

管理 IP アドレスは、接続されているネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。管理 IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。管理 IP サブネットの詳細については、「ブリッジ グループの設定」（P.13-7）を参照してください。

- IPv6 の場合は、少なくとも通過トラフィック用に各インターフェイスにリンクローカル アドレスを設定する必要があります。ASA の管理を含むフル機能のためには、各ブリッジ グループにグローバル IPv6 アドレスを設定する必要があります。
- マルチ コンテキスト モードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。
- マルチ コンテキスト モードでは、通常、各コンテキストが別個のサブネットを使用します。重複するサブネットを使用することもできますが、ルーティング スタンドポイントから可能にするため、ネットワーク トポロジにルータと NAT コンフィギュレーションが必要です。

フェールオーバーのガイドライン

フェールオーバー インターフェイスの設定は、この章の手順では完了しません。フェールオーバーおよびステート リンクの設定については、第 8 章「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。マルチ コンテキスト モードでは、フェールオーバー インターフェイスがシステム コンフィギュレーションに設定されます。

IPv6 のガイドライン

トランスペアレント モードでは IPv6 エニーキャスト アドレスをサポートしません。

ASASM の VLAN ID に関するガイドライン

コンフィギュレーションにはあらゆる VLAN ID を追加できますが、トラフィックを転送できるのはスイッチによって ASA に割り当てられた VLAN だけです。**show vlan** コマンドを使用して、ASA に割り当てられたすべての VLAN を表示します。

スイッチによって ASA にまだ割り当てられていない VLAN にインターフェイスを追加した場合、そのインターフェイスはダウン ステートになります。ASA に VLAN を割り当てた時点で、インターフェイスはアップ ステートに変化します。インターフェイス ステートの詳細については、**show interface** コマンドを参照してください。

トランスペアレント モードのインターフェイスのデフォルト設定

この項では、工場出荷時のデフォルト コンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。工場出荷時のデフォルト コンフィギュレーションに関する情報については、「工場出荷時のデフォルト設定」（P.2-15）を参照してください。

デフォルトのセキュリティ レベル

デフォルトのセキュリティ レベルは 0 です。インターフェイスに名前「inside」を付けて、明示的にセキュリティ レベルを設定しないと、ASA はセキュリティ レベルを 100 に設定します。

（注）インターフェイスのセキュリティ レベルを変更したときに、既存の接続がタイムアウトするまで待機せずに新しいセキュリティ情報を使用する必要がある場合は、**clear local-host** コマンドを使用して接続をクリアできます。

ASASM のインターフェイスのデフォルトの状態

- シングル モードまたはシステム実行スペースでは、VLAN インターフェイスがデフォルトでイネーブルになります。
- マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

ジャンボ フレーム サポート

デフォルトでは、ASASM はジャンボ フレームをサポートしています。「MAC アドレス、MTU、TCP MSS の設定」（P.13-15）に従って、目的のパケット サイズの MTU を設定します。

トランスペアレント モードのインターフェイス コンフィギュレーションの実行

インターフェイス コンフィギュレーションを実行するためのタスク フロー

ステップ 1　モデルに応じてインターフェイスを設定します。

- ASA 5512-X 以降：第 10 章「基本的なインターフェイス コンフィギュレーション（ASA 5512-X 以降）」
- ASASM：第 2 章「使用する前に」
- ASAv：第 11 章「基本インターフェイスの設定（ASAv）」

ステップ 2　（マルチ コンテキスト モード）「マルチ コンテキストの設定」（P.7-15）に従って、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 3　（マルチ コンテキスト モード）[Configuration] > [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 4　IPv4 アドレスを含む、1 つ以上のブリッジ グループを設定します。「ブリッジ グループの設定」（P.13-7）を参照してください。

ステップ 5　インターフェイスが属するブリッジ グループ、インターフェイス名、セキュリティ レベルなど、一般的なインターフェイス パラメータを設定します。「一般的なインターフェイス パラメータの設定」（P.13-8）を参照してください。

ステップ 6　（オプション）管理インターフェイスを設定します。「管理インターフェイスの設定（ASA 5512-X 以降および ASAv）」（P.13-11）を参照してください。

ステップ 7　（オプション）MAC アドレスと MTU を設定します。「MAC アドレス、MTU、TCP MSS の設定」（P.13-15）を参照してください。

ステップ 8　（オプション）IPv6 アドレッシングを設定します。「IPv6 アドレッシングの設定」（P.13-17）を参照してください。

ステップ 9　（オプション）2 つのインターフェイス間の通信を許可するか、またはトラフィックが同じインターフェイスに入って同じインターフェイスから出ることを許可することで、同じセキュリティ レベルの通信を許可します。「同じセキュリティ レベルの通信の許可」（P.13-22）を参照してください。

ブリッジ グループの設定

ブリッジ グループにはそれぞれ管理 IP アドレスが必要です。ASA はブリッジ グループが発信元になるパケットの送信元アドレスとして、この IP アドレスを使用します。管理 IP アドレスは、接続されているネットワークと同じサブネット内にある必要があります。IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、管理 IP アドレスが必要です。IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカル アドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。

注意事項と制約事項

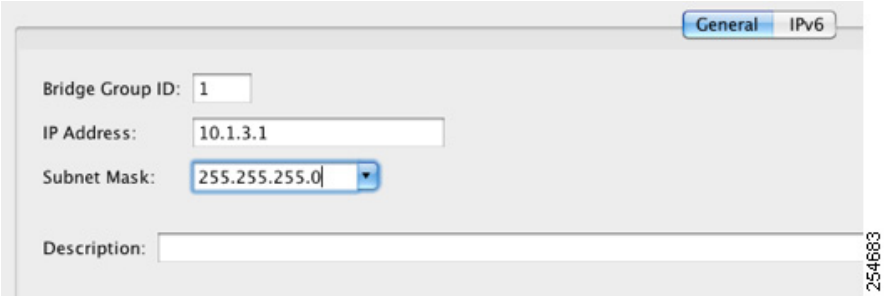
シングル モードまたはマルチ モードのコンテキストごとに、最大 250 個のブリッジ グループを設定できます。少なくとも 1 つのブリッジ グループを使用しなければならないことに注意してください。データ インターフェイスはブリッジ グループに属している必要があります。

（注）　個別の管理インターフェイスでは（サポートされているモデルの場合）、設定できないブリッジ グループ（ID 301）は、設定に自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。

手順の詳細

ステップ 1　[Configuration] > [Interfaces] ペインを選択し、[Add] > [Bridge Group Interface] を選択します。

[Add Bridge Group] ダイアログボックスが表示されます。



ステップ 2　[Bridge Group ID] フィールドで、1 ～ 250 の間のブリッジ グループ ID を入力します。

ステップ 3　[IP Address] フィールドに管理 IPv4 アドレスを入力します。

ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。管理 IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

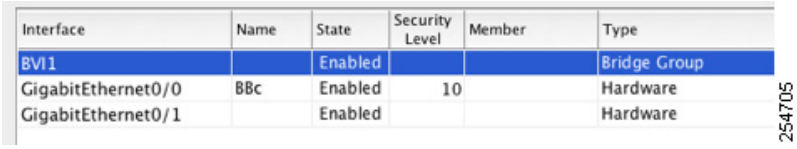
ステップ 4　[Subnet Mask] フィールドで、サブネット マスクを入力するか、またはメニューから選択します。

トランスペアレント ファイアウォールにホスト アドレス（/32 または 255.255.255.255）を割り当てないでください。また、/30 サブネットなど（255.255.255.252）、ホスト アドレスが 3 つ未満（アップストリーム ルータ、ダウンストリーム ルータ、トランスペアレント ファイアウォールにそれぞれ 1 つずつ）の他のサブネットを使用しないでください。ASA は、サブネットの先頭アドレスと最終アドレスとの間で送受信されるすべての ARP パケットをドロップします。たとえば、/30 サブネットを使用し、そのサブネットからアップストリーム ルータへの予約アドレスを割り当てた場合、ASA はダウンストリーム ルータからアップストリーム ルータへの ARP 要求をドロップします。

ステップ 5　（オプション）[Description] フィールドに、このブリッジ グループの説明を入力します。

ステップ 6　[OK] をクリックします。

ステップ 7　ブリッジ グループ仮想インターフェイス（BVI）が、物理およびサブインターフェイスとともに、インターフェイス テーブルに追加されます。



Interface	Name	State	Security Level	Member	Type
BVI1		Enabled			Bridge Group
GigabitEthernet0/0	BBc	Enabled	10		Hardware
GigabitEthernet0/1		Enabled			Hardware

254705

次の作業

一般的なインターフェイス パラメータを設定します。「一般的なインターフェイス パラメータの設定」（P.13-8）を参照してください。

一般的なインターフェイス パラメータの設定

この手順は、トランスペアレント インターフェイスの名前、セキュリティ レベル、およびブリッジ グループを設定する方法について説明します。

個別の管理インターフェイスを設定するには、「管理インターフェイスの設定（ASA 5512-X 以降および ASAv）」（P.13-11）を参照してください。

ASA 5512-X 以降および ASAv では、次のインターフェイス タイプのインターフェイス パラメータを設定する必要があります。

- 物理インターフェイス
- VLAN サブインターフェイス
- 冗長インターフェイス
- EtherChannel インターフェイス

ASASM では、次のインターフェイス タイプのインターフェイス パラメータを設定する必要があります。

- VLAN インターフェイス

注意事項と制約事項

- ブリッジ グループあたり最大 4 つのインターフェイスを設定できます。
- セキュリティ レベルについては、「セキュリティ レベル」（P.13-2）を参照してください。
- フェールオーバーを使用している場合は、フェールオーバー通信およびステートフル フェールオーバー通信に予約されているインターフェイスには、この方法で名前を付けないでください。フェールオーバーおよびステート リンクの設定については、第 8 章「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。

前提条件

- モデルに応じてインターフェイスを設定します。
  - ASA 5512-X 以降：第 10 章「基本的なインターフェイス コンフィギュレーション（ASA 5512-X 以降）」
  - ASASM：第 2 章「使用する前に」
  - ASAv：第 11 章「基本インターフェイスの設定（ASAv）」
- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.7-15）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [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。

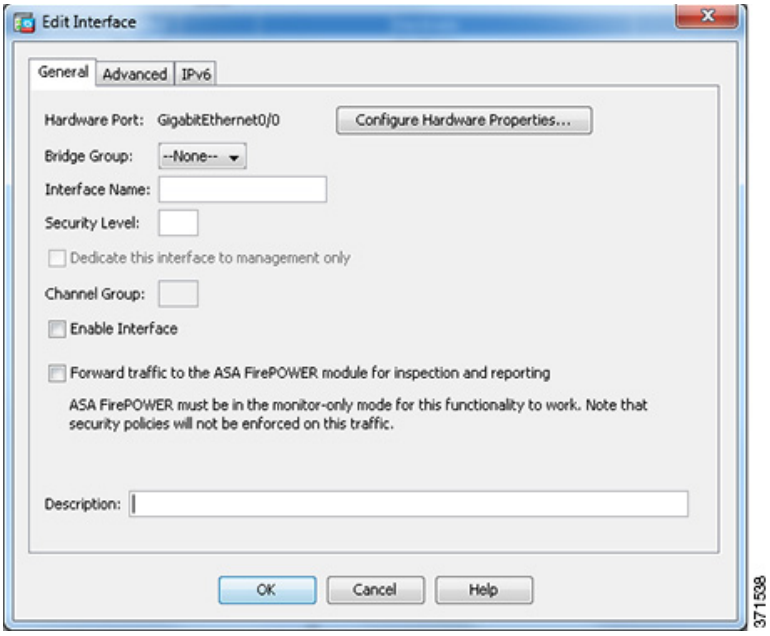
手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

BVI は、物理インターフェイス、サブインターフェイス、冗長インターフェイス、EtherChannel ポートチャネル インターフェイスとともにテーブルに表示されます。マルチ コンテキスト モードでは、システム実行スペースでコンテキストに割り当てられたインターフェイスだけがテーブルに表示されます。

ステップ 2　非 BVI インターフェイスの行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。



管理インターフェイスにはこの手順を使用しないでください。管理インターフェイスを設定する場合は、「管理インターフェイスの設定（ASA 5512-X 以降および ASAv）」（P.13-11）を参照してください。

ステップ 3　[Bridge Group] ドロップダウン メニューで、このインターフェイスを割り当てるブリッジ グループを選択します。

ステップ 4　[Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 5　[Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

詳細については、「セキュリティ レベル」（P.13-2）を参照してください。

（注）　[Dedicate this interface to management only] チェックボックスをオンにしないでください。このオプションについては、「管理インターフェイスの設定（ASA 5512-X 以降および ASAv）」（P.13-11）を参照してください。

ステップ 6　インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

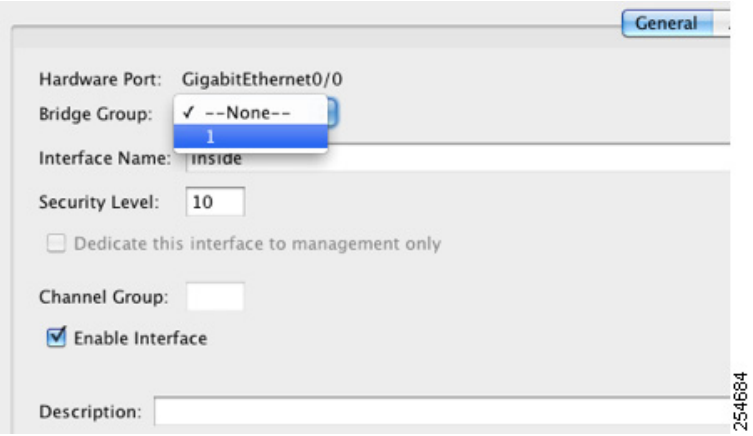
（注）　[Channel Group] フィールドは読み取り専用で、インターフェイスが EtherChannel の一部であるかどうかを示します。

ステップ 7　（オプション）ASA CX または ASA FirePOWER モジュールを取り付けて非本番 ASA 上でモジュール機能をデモンストレーションする場合、[Forward traffic to the ASA module for inspection and reporting] チェックボックスをオンにします。詳細については、ファイアウォール コンフィギュレーション ガイドのモジュールに関する章を参照してください。

ステップ 8　（オプション）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

（注）　（ASA 5512-X 以降、シングル モード）[Configure Hardware Properties] ボタンに関する情報については、「物理インターフェイスのイネーブル化およびイーサネット パラメータの設定」（P.10-15）を参照してください。



ステップ 9　[OK] をクリックします。

次の作業

- （オプション）管理インターフェイスを設定します。「管理インターフェイスの設定（ASA 5512-X 以降および ASAv）」（P.13-11）を参照してください。
- （オプション）MAC アドレスと MTU を設定します。「MAC アドレス、MTU、TCP MSS の設定」（P.13-15）を参照してください。
- （オプション）IPv6 アドレッシングを設定します。「IPv6 アドレッシングの設定」（P.13-17）を参照してください。

管理インターフェイスの設定（ASA 5512-X 以降および ASAv）

1 つの管理インターフェイスをシングル モードで、またはコンテキストごとに、ブリッジ グループとは独立して設定できます。詳細については、「管理インターフェイス」（P.10-2）を参照してください。

制限事項

- 「管理インターフェイス」（P.10-2）を参照してください。
- このインターフェイスをブリッジ グループに割り当てないでください。設定できないブリッジ グループ（ID 101）は、コンフィギュレーションに自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。
- モデルに管理インターフェイスが含まれていない場合、データ インターフェイスからトランスペアレント ファイアウォールを管理する必要があります。この手順はスキップします。（ASASM など）。
- 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（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。コンテキスト単位で管理を行うには、管理インターフェイスのサブインターフェイスを作成し、管理サブインターフェイスを各コンテキストに割り当てます。ASA 5512-X ～ ASA 5555-X では、管理インターフェイスのサブインターフェイスは許可されないので、コンテキスト単位で管理を行うには、データ インターフェイスに接続する必要があります。

前提条件

- 第 10 章「基本的なインターフェイス コンフィギュレーション（ASA 5512-X 以降）」の手順を実行します。
- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.7-15）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [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。

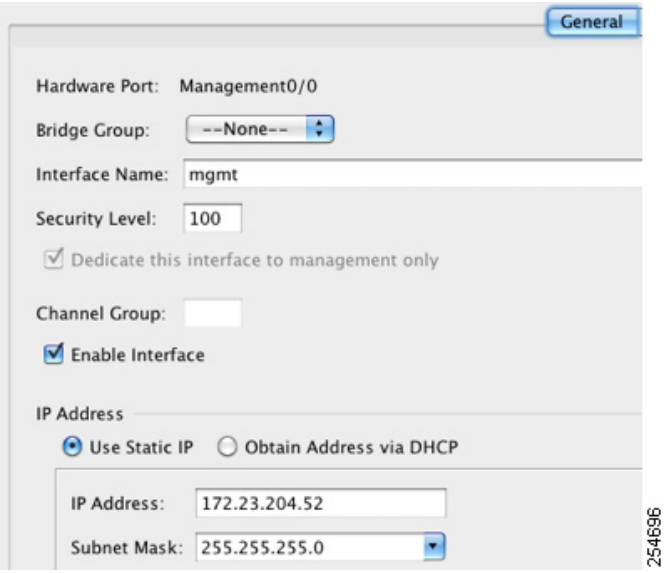
手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

BVI は、物理インターフェイス、サブインターフェイス、冗長インターフェイス、EtherChannel ポートチャネル インターフェイスとともにテーブルに表示されます。マルチ コンテキスト モードでは、システム実行スペースでコンテキストに割り当てられたインターフェイスだけがテーブルに表示されます。

ステップ 2　管理インターフェイス、サブインターフェイス、または管理インターフェイスからなる EtherChannel ポートチャネル インターフェイスの行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。



ステップ 3　[Bridge Group] ドロップダウン メニューで、デフォルトの [--None--] のままにします。管理インターフェイスをブリッジ グループに割り当てることはできません。

ステップ 4　[Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 5　[Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

詳細については、「セキュリティ レベル」（P.13-2）を参照してください。

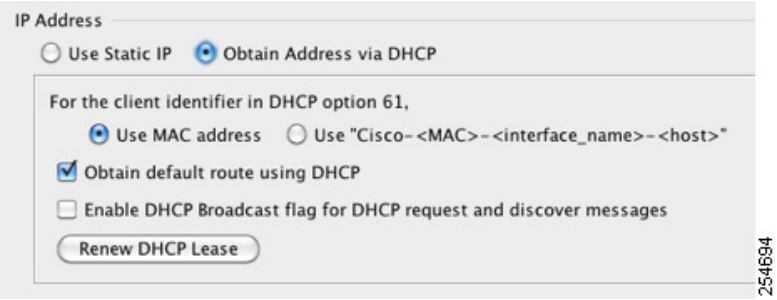
（注）　[Dedicate this interface to management only] チェックボックスは、デフォルトでイネーブルであり、設定することはできません。

ステップ 6　インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

ステップ 7　IP アドレスを設定するには、次のいずれかのオプションを使用します。

（注）　フェールオーバーとともに使用する場合は、IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP はサポートされません。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces] タブのスタンバイ IP アドレスを設定します。

- IP アドレスを手動で設定するには、[Use Static IP] オプション ボタンをクリックして IP アドレスとマスクを入力します。
- DHCP サーバから IP アドレスを取得するには、[Obtain Address via DHCP] オプション ボタンをクリックします。



a. MAC アドレスがオプション 61 の DHCP 要求パケット内に保存されるようにするには、[Use MAC Address] オプション ボタンをクリックします。

いくつかの ISP はインターフェイスの MAC アドレスにオプション 61 が必要です。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。

b. オプション 61 用に生成された文字列を使用するには、[Use “Cisco-<MAC>-<interface_name>-<host>”] をクリックします。

c. （オプション）DHCP サーバからデフォルト ルートを取得するには、[Obtain Default Route Using DHCP] をオンにします。

d. （オプション）DHCP クライアントが IP アドレス要求の探索を送信する場合に、DHCP パケット ヘッダーでブロードキャスト フラグを 1 に設定するには、[Enable DHCP Broadcast flag for DHCP request and discover messages] をオンにします。

DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。

e. （オプション）リースを更新するには、[Renew DHCP Lease] をクリックします。

ステップ 8　（オプション）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。

（注）　（ASA 5512-X 以降、シングル モード）[Configure Hardware Properties] ボタンに関する情報については、「物理インターフェイスのイネーブル化およびイーサネット パラメータの設定」（P.10-15）を参照してください。

ステップ 9　[OK] をクリックします。

次の作業

- （オプション）MAC アドレスと MTU を設定します。「MAC アドレス、MTU、TCP MSS の設定」（P.13-15）を参照してください。
- （オプション）IPv6 アドレッシングを設定します。「IPv6 アドレッシングの設定」（P.13-17）を参照してください。

MAC アドレス、MTU、TCP MSS の設定

ここでは、インターフェイスの MAC アドレスの設定方法、MTU の設定方法、および TCP MSS の設定方法を説明します。

MAC アドレスに関する情報

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。

ASASM では、すべての VLAN がバックプレーンから提供される同じ MAC アドレスを使用します。

冗長インターフェイスは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバー インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。このコマンドを使用して冗長インターフェイスに MAC アドレスを割り当てると、メンバー インターフェイスの MAC アドレスに関係なく、割り当てた MAC アドレスが使用されます。

EtherChannel の場合は、そのチャネル グループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。ポート チャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アドレスとして使用します。または、ポートチャネル インターフェイスの MAC アドレスを手動で設定することもできます。マルチ コンテキスト モードでは、EtherChannel ポート インターフェイスを含め、固有の MAC アドレスをインターフェイスに自動的に割り当てることができます。グループ チャネル インターフェイスのメンバーシップを変更する場合は、固有の MAC アドレスを手動で設定するか、またはマルチ コンテキスト モードで自動的に設定することを推奨します。ポートチャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。

マルチ コンテキスト モードでは、コンテキスト間でインターフェイスを共有している場合、固有の MAC アドレスをそれぞれのコンテキストのインターフェイスに割り当てることができます。この機能を使用すると、ASA はパケットを適切なコンテキストに容易に分類できます。固有の MAC アドレスがなくても共有インターフェイスを使用できますが、制限があります。詳細については、「ASA によるパケットの分類方法」（P.7-3）を参照してください。コンテキストの共有インターフェイスには、手動で各 MAC アドレスを割り当てることも、自動生成することもできます。MAC アドレスの自動生成については、「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」（P.7-25）を参照してください。MAC アドレスを自動生成する場合、この手順を使用して生成されたアドレスを上書きできます。

シングル コンテキスト モード、またはマルチ コンテキスト モードで共有されないインターフェイスの場合は、固有の MAC アドレスをサブインターフェイスに割り当てることを推奨します。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 コントロールを実行する場合があります。

MTU および TCP MSS に関する情報

「最大伝送単位および TCP 最大セグメント サイズのフラグメンテーションの制御」（P.10-8）を参照してください。

前提条件

- モデルに応じてインターフェイスを設定します。
  - ASA 5512-X 以降：第 10 章「基本的なインターフェイス コンフィギュレーション（ASA 5512-X 以降）」
  - ASASM：第 2 章「使用する前に」
  - ASAv：第 11 章「基本インターフェイスの設定（ASAv）」
- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.7-15）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [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。

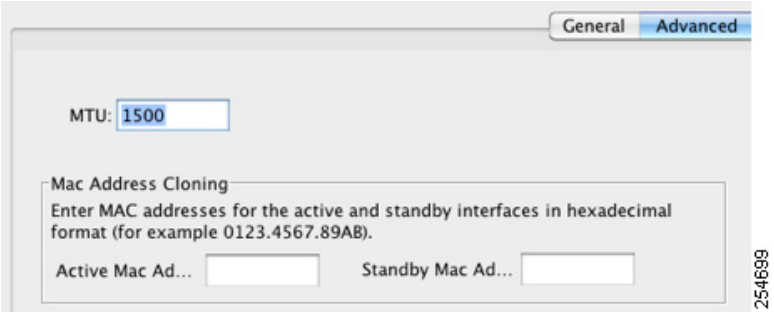
手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　インターフェイス行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[Advanced] タブをクリックします。



ステップ 4　MTU を設定する場合、またはジャンボ フレームのサポートをイネーブルにする（サポート対象モデルのみ）場合、[MTU] フィールドに 300 ～ 9198 バイト（ASAv の場合は 9000）の値を入力します。

デフォルトは 1500 バイトです。

（注）　冗長インターフェイスまたはポートチャネル インターフェイスに MTU を設定すると、ASA は、この設定をすべてのメンバー インターフェイスに適用します。

- ジャンボ フレームをサポートする、シングル モードのモデルの場合：いずれかのインターフェイスに 1500 を超える値を入力すると、ジャンボ フレーム サポートがすべてのインターフェイスに対して自動的にイネーブルになります。すべてのインターフェイスの MTU の設定を 1500 未満に戻すと、ジャンボ フレーム サポートがディセーブルになります。

- ジャンボ フレームをサポートするマルチ モードの場合：いずれかのインターフェイスに 1500 を超える値を入力する場合、必ずシステム コンフィギュレーションのジャンボ フレーム サポートをイネーブルにしてください。「ジャンボ フレーム サポートのイネーブル化」（P.10-31）を参照してください。

（注）　ジャンボ フレーム サポートをイネーブルまたはディセーブルにするには、ASA をリロードする必要があります。

ステップ 5　MAC アドレスをこのインターフェイスに手動で割り当てるには、[Active Mac Address] フィールドに MAC アドレスを H.H.H 形式（H は 16 ビットの 16 進数）で入力します。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

ステップ 6　フェールオーバーを使用する場合、[Standby Mac Address] フィールドにスタンバイ MAC アドレスを入力します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな 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。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 7　TCP MSS を設定するには、[Configuration] > [Firewall] > [Advanced] > [TCP Options] の順に選択します。次のオプションを設定します。

- [Force Maximum Segment Size for TCP]：最大 TCP セグメント サイズを 48 から最大数の範囲のバイト数で設定します。デフォルト値は 1380 バイトです。この機能は、0 バイトに設定することによってディセーブルにできます。
- [Force Minimum Segment Size for TCP]：48 から最大数の間で、ユーザが設定したバイト数未満にならないように最大セグメント サイズを上書きします。この機能は、デフォルトでディセーブルです（0 に設定）。

ステップ 8　**セキュリティ グループ タグ**については、「SGT とイーサネット タギングのイネーブル化」（P.33-24）を参照してください。

次の作業

（オプション）IPv6 アドレッシングを設定します。「IPv6 アドレッシングの設定」（P.13-17）を参照してください。

IPv6 アドレッシングの設定

この項では、IPv6 アドレッシングを設定する方法について説明します。

IPv6 に関する情報

ここでは、IPv6 の設定方法について説明します。

- 「IPv6 アドレス指定」（P.13-18）
- 「Modified EUI-64 インターフェイス ID」（P.13-18）
- 「サポートされていないコマンド」（P.13-19）

IPv6 アドレス指定

次の 2 種類の IPv6 のユニキャスト アドレスを設定できます。

- グローバル：グローバル アドレスは、パブリック ネットワークで使用可能なパブリック アドレスです。このアドレスは、インターフェイスごとに設定するのではなく、ブリッジ グループごとに設定する必要があります。また、管理インターフェイスのグローバルな IPv6 アドレスを設定することもできます。
- リンクローカル：リンクローカル アドレスは、直接接続されたネットワークだけで使用できるプライベート アドレスです。ルータは、リンクローカル アドレスを使用してパケットを転送するのではなく、特定の物理ネットワーク セグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決およびネイバー探索などの ND 機能に使用できます。リンクローカル アドレスは 1 つのセグメント上だけで使用可能であり、インターフェイスの MAC アドレスに関連付けられているため、インターフェイスごとにリンクローカル アドレスを設定する必要があります。

最低限、IPv6 が動作するようにリンクローカル アドレスを設定する必要があります。グローバル アドレスを設定する場合、各インターフェイスにリンクローカル アドレスが自動的に設定されるため、特にリンクローカル アドレスを設定する必要はありません。グローバル アドレスを設定しない場合は、リンクローカル アドレスを自動的にするか、手動で設定する必要があります。

Modified EUI-64 インターフェイス ID

RFC 3513「Internet Protocol Version 6 (IPv6) Addressing Architecture」では、バイナリ値 000 で始まるものを除き、すべてのユニキャスト IPv6 アドレスのインターフェイス識別子部分は長さが 64 ビットで、Modified EUI-64 形式で組み立てることが要求されています。ASA では、ローカル リンクに接続されたホストにこの要件を適用できます。

この機能がインターフェイスでイネーブルになっていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
%ASA-3-325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカル リンク上のホストに対してのみ実行できます。ルータの背後にあるホストから受信したパケットは、アドレス形式の検証に失敗してドロップされます。これは、その送信元 MAC アドレスがルータの MAC アドレスであり、ホストの MAC アドレスではないためです。

サポートされていないコマンド

次の IPv6 コマンドにはルータ機能が必要であるため、トランスペアレント ファイアウォール モードではサポートされません。

- **ipv6 address autoconfig**
- **ipv6 nd prefix**
- **ipv6 nd ra-interval**
- **ipv6 nd ra-lifetime**
- **ipv6 nd suppress-ra**

グローバル IPv6 アドレスの設定

ブリッジ グループまたは管理インターフェイスのグローバル IPv6 アドレスを設定するには、次の手順を実行します。

（注）　グローバル アドレスを設定すると、リンクローカル アドレスは自動的に設定されるため、別々に設定する必要はありません。

制限事項

ASA は、IPv6 エニーキャスト アドレスはサポートしません。

前提条件

- モデルに応じてインターフェイスを設定します。
  - ASA 5512-X 以降：第 10 章「基本的なインターフェイス コンフィギュレーション（ASA 5512-X 以降）」
  - ASASM：第 2 章「使用する前に」
  - ASAv：第 11 章「基本インターフェイスの設定（ASAv）」
- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.7-15）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [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。

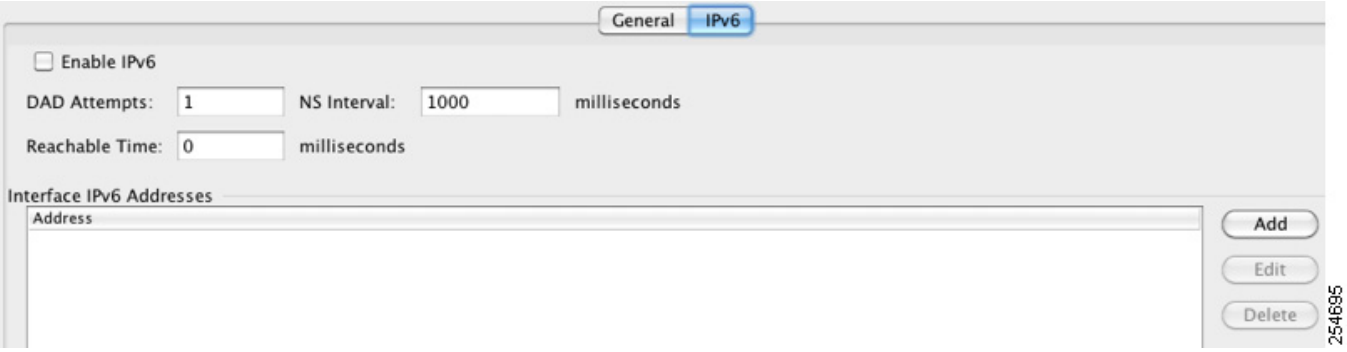
手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　BVI または管理インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[IPv6] タブをクリックします。



ステップ 4　[Enable IPv6] チェックボックスをオンにします。

ステップ 5　（オプション）ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[Enforce EUI-64] チェックボックスをオンにします。

詳細については、「Modified EUI-64 インターフェイス ID」（P.13-18）を参照してください。

ステップ 6　（オプション）上部で、第 26 章「IPv6 ネイバー探索」を参照して IPv6 設定をカスタマイズします。

ステップ 7　グローバル IPv6 アドレスを設定する場合：

a.　[Interface IPv6 Addresses] エリアで、[Add] をクリックします。

[Add IPv6 Address for Interface] ダイアログボックスが表示されます。

b.　[Address/Prefix Length] フィールドに、グローバル IPv6 アドレスと IPv6 プレフィックスの長さを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、「IPv6 形式のアドレス」（P.43-5）を参照してください。

c.　[OK] をクリックします。

ステップ 8　[OK] をクリックします。

[Configuration] > [Device Setup] > [Interfaces] ペインに戻ります。

IPv6 ネイバー探索の設定

IPv6 ネイバー探索を設定するには、第 26 章「IPv6 ネイバー探索」を参照してください。

（オプション）リンクローカル アドレスの自動設定

グローバル アドレスを設定する必要がなく、リンクローカル アドレスだけを設定する必要がある場合は、リンクローカル アドレスをインターフェイスの MAC アドレス（Modified EUI-64 形式。MAC アドレスで使用するビット数は 48 ビットであるため、インターフェイス ID に必要な 64 ビットを埋めるために追加ビットを挿入する必要があります。）

リンクローカル アドレスを手動で割り当てる場合（非推奨）については、「（オプション）リンクローカル アドレスの手動設定」（P.13-21）を参照してください。

Modified EUI-64 形式の適用および DAD 設定を含むその他の IPv6 オプションについては、「グローバル IPv6 アドレスの設定」（P.13-19）を参照してください。

リンクローカル アドレスを管理インターフェイスまたはブリッジ グループ メンバー インターフェイスに自動的に設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　BVI または管理インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[IPv6] タブをクリックします。

ステップ 4　[IPv6 configuration] 領域で、[Enable IPv6] をオンにします。

このオプションでは、IPv6 をイネーブルにし、インターフェイスの MAC アドレスに基づく Modified EUI-64 インターフェイス ID を使用してリンクローカル アドレスをメンバー インターフェイスに自動的に生成します。

ステップ 5　[OK] をクリックします。

（オプション）リンクローカル アドレスの手動設定

グローバル アドレスを設定する必要がなく、リンクローカル アドレスだけを物理インターフェイスまたはサブインターフェイスに設定する必要がある場合は、リンクローカル アドレスを手動で定義できます。Modified EUI-64 形式に基づくリンクローカル アドレスを自動的に割り当てることを推奨します。たとえば、他のデバイスが Modified EUI-64 形式の使用を必要とする場合、手動で割り当てたリンクローカル アドレスのパケットはドロップされる可能性があります。

リンクローカル アドレスを自動的に割り当てる場合（推奨）については、「（オプション）リンクローカル アドレスの自動設定」（P.13-20）を参照してください。

Modified EUI-64 形式の適用および DAD 設定を含むその他の IPv6 オプションについては、「グローバル IPv6 アドレスの設定」（P.13-19）を参照してください。

リンクローカル アドレスを、管理インターフェイスを含む物理インターフェイスまたはサブインターフェイスに割り当てるには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[IPv6] タブをクリックします。

ステップ 4　リンクローカル アドレスを設定するには、[Link-local address] フィールドにアドレスを入力します。

リンクローカル アドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。たとえば fe80::20d:88ff:feee:6a82 のようになります。IPv6 アドレッシングの詳細については、「IPv6 形式のアドレス」（P.43-5）を参照してください。

ステップ 5　[OK] をクリックします。

同じセキュリティ レベルの通信の許可

デフォルトでは、同じセキュリティ レベルのインターフェイスは相互に通信することができません。また、パケットは同じインターフェイスを出入りすることができません。ここでは、複数のインターフェイスが同じセキュリティ レベルの場合にインターフェイス間通信をイネーブルにする方法について説明します。

インターフェイス間通信に関する情報

同じセキュリティ レベルのインターフェイスが互いに通信できるようにすると、ACL リストがなくても同じセキュリティ レベルのインターフェイスすべての間で自由にトラフィックが流れるようにする場合に便利です。

同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。

手順の詳細

同じセキュリティ レベルのインターフェイス間の通信をイネーブルにするには、[Configuration] > [Interfaces] ペインで、[Enable traffic between two or more interfaces which are configured with same security level] をオンにします。

インターフェイスのオン/オフ

ここでは、インターフェイスのオン/オフの方法について説明します。

デフォルトでは、すべてのインターフェイスがイネーブルです。マルチ コンテキスト モードでは、コンテキスト内でインターフェイスをディセーブルにした場合、または再度イネーブルにした場合は、そのコンテキスト インターフェイスだけが影響を受けます。ただし、システム実行スペースでインターフェイスをディセーブルにした場合、または再度イネーブルにした場合は、全コンテキストに対応するそのインターフェイスに影響します。

手順の詳細

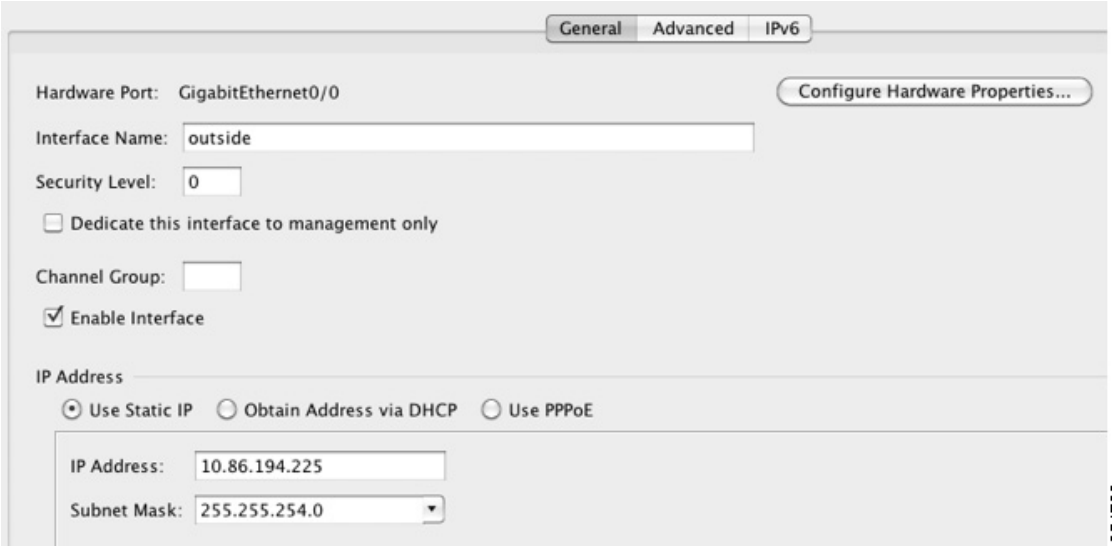
ステップ 1　コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

デフォルトでは、すべての物理インターフェイスが一覧表示されます。

ステップ 2　設定する VLAN インターフェイスをクリックし、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。



ステップ 3　インターフェイスをイネーブルまたはディセーブルにするには、[Enable Interface] チェックボックスをオンまたはオフにします。

インターフェイスのモニタリング

- 「ARP Table」（P.12-23）を参照してください。
- 「DHCP」（P.12-23）を参照してください。
- 「MAC Address Table」（P.12-26）を参照してください。
- 「Dynamic ACLs」（P.12-26）を参照してください。
- 「Interface Graphs」（P.12-26）を参照してください。
- 「PPPoE Client」（P.12-29）を参照してください。
- 「インターフェイス接続」（P.12-29）を参照してください。

トランスペアレント モードのインターフェイスの機能履歴

表 13-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 13-1　トランスペアレント モードのインターフェイスの機能履歴

機能名	プラットフォーム リリース	機能情報
VLAN 数の増加	7.0(5)	次の制限値が増加されました。 • ASA 5510 基本ライセンスの VLAN 数が 0 から 10 に増えました。 • ASA 5510 Security Plus ライセンスの VLAN 数が 10 から 25 に増えました。 • ASA 5520 の VLAN 数が 25 から 100 に増えました。 • ASA 5540 の VLAN 数が 100 から 200 に増えました。
VLAN 数の増加	7.2(2)	ASA 5505 上の Security Plus ライセンスに対する VLAN 最大数が、5（3 つのフル機能インターフェイス、1 つのフェールオーバー インターフェイス、1 つのバックアップ インターフェイスに制限されるインターフェイス）から 20 のフル機能インターフェイスに増加されました。また、トランク ポート数も 1 から 8 に増加されました。フル機能のインターフェイスの数が 20 になり、バックアップ ISP インターフェイスを停止するために backup interface コマンドを使用する必要がなくなりました。つまり、バックアップ ISP インターフェイス用にフル機能のインターフェイスを使用できるようになりました。backup interface コマンドは、これまでどおり Easy VPN 設定用に使用できます。 VLAN の制限値も変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。
ASA 5510 Security Plus ライセンスに対するギガビット イーサネット サポート	7.2(3)	ASA 5510 は、GE（ギガビット イーサネット）を Security Plus ライセンスのあるポート 0 および 1 でサポートするようになりました。ライセンスを Base から Security Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 ポートの容量は、元の FE（ファスト イーサネット）の 100 Mbps から GE の 1000 Mbps に増加します。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。
ASA 5505 に対するネイティブ VLAN サポート	7.2(4)/8.0(4)	ネイティブ VLAN を ASA 5505 トランク ポートに割り当てることができるようになりました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interfaces] > [Switch Ports] > [Edit Switch Port]。

表 13-1　トランスペアレント モードのインターフェイスの機能履歴（続き）

機能名	プラットフォーム リリース	機能情報
ASA 5580 に対するジャンボ パケット サポート	8.1(1)	Cisco ASA 5580 はジャンボ フレームをサポートしています。ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび FCS を含む）より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネット フレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能（ACL など）の最大使用量が制限される場合があります。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface] > [Advanced]。
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。
トランスペアレント モードの IPv6 のサポート	8.2(1)	トランスペアレント ファイアウォール モードの IPv6 サポートが導入されました。
ASA 5580 10 ギガビット イーサネット インターフェイスでのフロー制御のポーズ フレームのサポート	8.2(2)	フロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりました。 次の画面が変更されました。 （シングル モード）[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface] > [General] （マルチ モード、システム）[Configuration] > [Interfaces] > [Add/Edit Interface]
トランスペアレント モードのブリッジ グループ	8.4(1)	セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジ グループにグループ化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。ブリッジ グループのトラフィックは他のブリッジ グループから隔離されます。シングル モードまたはコンテキストごとに、それぞれ 4 つのインターフェイスからなる最大 8 個のブリッジ グループを設定できます。 次の画面が変更または導入されました。 [Configuration] > [Device Setup] > [Interfaces] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Bridge Group Interface] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface]

表 13-1　トランスペアレント モードのインターフェイスの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
トランスペアレント モードのブリッジ グループの最大数が 250 に増加	9.3(1)	ブリッジ グループの最大数が 8 個から 250 個に増えました。シングル モードでは最大 250 個、マルチ モードではコンテキストあたり最大 250 個のブリッジ グループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを設定できます。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Interfaces] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Bridge Group Interface] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface]

PART 4

基本設定

基本設定

この章では、ASA 上で機能を果たすコンフィギュレーションに通常必要とされる基本設定を行う方法について説明します。

ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定

ホスト名、ドメイン名、イネーブル パスワード、Telnet パスワードを設定するには、次の手順を実行します。

はじめる前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースとシステム実行スペースの両方のホスト名とドメイン名を設定できます。
- イネーブル パスワードと Telnet パスワードは、各コンテキストで設定します。システムでは使用できません。マルチ コンテキスト モードのスイッチから ASASM へのセッションを実行する場合、ASASM は管理コンテキストで設定したログイン パスワードを使用します。
- システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [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。

手順

ステップ 1 [Configuration] > [Device Setup] > [Device Name/Password] を選択します。

ステップ 2 ホスト名を入力します。デフォルトのホスト名は「ciscoasa」です。

ホスト名はコマンドラインのプロンプトに表示されます。このホスト名によって、複数のデバイスとのセッションを確立する場合に、コマンドを入力する場所が常に把握できます。ホスト名は syslog メッセージでも使用されます。

マルチコンテキスト モードでは、システム実行スペースで設定したホスト名がすべてのコンテキストのコマンド ラインのプロンプトに表示されます。コンテキストで設定したホスト名を、コマンドラインに表示せず、バナーに表示するオプションもあります。

ステップ 3　ドメイン名を入力します。デフォルト ドメイン名は default.domain.invalid です。

ASA は、修飾子を持たない名前のサフィクスとして、ドメイン名を付加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバとして非修飾名「jupiter」を指定した場合は、ASA によって名前が修飾されて「jupiter.example.com」となります。

ステップ 4　特権モード（イネーブル）パスワードを変更します。デフォルトのパスワードはブランクです。

enable 認証を設定しない場合、イネーブル パスワードによって特権 EXEC モードが開始されます。

HTTP 認証を設定しない場合、イネーブル パスワードによって空のユーザ名で ASDM にログインできます。

a. [Change the privileged mode password] チェックボックスをオンにします。

b. 古いパスワード（デフォルトのパスワードは空白）、新しいパスワードを入力し、新しいパスワードを確認します。

ステップ 5　Telnet アクセスのためのログイン パスワードを設定します。デフォルトのパスワードはありません。

Telnet 認証を設定しない場合、ログイン パスワードは Telnet アクセスに使用されます。**session** コマンドを使用してスイッチから ASASM にアクセスする場合にも、このパスワードを使用します。

a. [Change the password to access the console of the security appliance] チェックボックスをオンにします。

b. 古いパスワード（新しい ASA の場合、このフィールドは空白にしておきます）、新しいパスワードを入力し、新しいパスワードを確認します。

ステップ 6　[Apply] をクリックして変更内容を保存します。

イネーブル パスワードと Telnet パスワードの回復

イネーブル パスワードまたは Telnet パスワードを忘れた場合は、それらを回復できます。手順は、デバイス タイプによって異なります。CLI を使用してタスクを実行する必要があります。

- 「ASA のパスワードの回復」（P.14-3）
- 「ASA 5506、5506-W および ASA 5508 のパスワードの回復」（P.14-4）
- 「ASAv のパスワードまたはイメージの回復」（P.14-5）
- 「パスワード回復のディセーブル化」（P.14-6）

ASA のパスワードの回復

ASA のパスワードを回復するには、次の手順を実行します。

手順

ステップ 1　ASA コンソール ポートに接続します。

ステップ 2　ASA の電源を切ってから、投入します。

ステップ 3　スタートアップ後、ROMMON モードに入るようにプロンプトが表示されたら、**Escape** キーを押します。

ステップ 4　コンフィギュレーション レジスタ値をアップデートするには、次のコマンドを入力します。

```
rommon #1> confreg 0x41
Update Config Register (0x41) in NVRAM...
```

ステップ 5　スタートアップ コンフィギュレーションを無視するように ASA を設定するには、次のコマンドを入力します。

```
rommon #1> confreg
```

ASA によって現在のコンフィギュレーションのレジスタ値が表示され、それを変更するかどうかが尋ねられます。

```
Current Configuration Register: 0x00000041
Configuration Summary:
boot default image from Flash
  ignore system configuration

Do you wish to change this configuration?y/n [n]: y
```

ステップ 6　後で回復できるように、現在のコンフィギュレーションのレジスタ値を記録します。

ステップ 7　値を変更する場合は、プロンプトに対して **Y** を入力します。

ASA によって、新しい値の入力を求めるプロンプトが表示されます。

ステップ 8　「disable system configuration?」の値を除き、すべての設定についてデフォルト値を受け入れます。

ステップ 9　プロンプトに対して、**Y** を入力します。

ステップ 10　次のコマンドを入力して、ASA をリロードします。

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa800-226-k8.bin... Booting...Loading...
```

ASA は、スタートアップ コンフィギュレーションの代わりにデフォルト コンフィギュレーションをロードします。

ステップ 11　次のコマンドを入力して、特権 EXEC モードにアクセスします。

```
ciscoasa# enable
```

ステップ 12　パスワードの入力を求められたら、**Enter** キーを押します。

パスワードは空白です。

ステップ 13　次のコマンドを入力して、スタートアップ コンフィギュレーションをロードします。

```
ciscoasa# copy startup-config running-config
```

ステップ 14　次のコマンドを入力して、グローバル コンフィギュレーション モードにアクセスします。

```
ciscoasa# configure terminal
```

ステップ 15　次のコマンドを入力して、デフォルト コンフィギュレーションで必要に応じてパスワードを変更します。

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

ステップ 16　次のコマンドを入力して、デフォルト コンフィギュレーションをロードします。

```
ciscoasa(config)# no config-register
```

デフォルト コンフィギュレーションのレジスタ値は 0x1 です。コンフィギュレーション レジスタの詳細については、コマンド リファレンスを参照してください。

ステップ 17　次のコマンドを入力して、新しいパスワードをスタートアップ コンフィギュレーションに保存します。

```
ciscoasa(config)# copy running-config startup-config
```

ASA 5506、5506-W および ASA 5508 のパスワードの回復

ASA 5506、5506-W および 5508 のパスワードを回復するには、次の手順を実行します。

手順

ステップ 1　ASA コンソール ポートに接続します。

ステップ 2　ASA の電源を切ってから、投入します。

ステップ 3　スタートアップ後、ROMMON モードに入るようにプロンプトが表示されたら、**Escape** キーを押します。

ステップ 4　コンフィギュレーション レジスタ値をアップデートするには、次のコマンドを入力します。

```
rommon #1> confreg 0x41

You must reset or power cycle for new config to take effect
```

ASA には現在のコンフィギュレーション レジスタ値と構成オプションのリストが表示されます。後で回復できるように、現在のコンフィギュレーションのレジスタ値を記録します。

```
Configuration Register: 0x00000041

Configuration Summary
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ...... auto-boot index 1 image in disks
```

ステップ 5　次のコマンドを入力して、ASA をリロードします。

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.
```

```
Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

ASA は、スタートアップ コンフィギュレーションの代わりにデフォルト コンフィギュレーションをロードします。

ステップ 6　次のコマンドを入力して、特権 EXEC モードにアクセスします。

```
ciscoasa# enable
```

ステップ 7　パスワードの入力を求められたら、**Enter** キーを押します。

パスワードは空白です。

ステップ 8　次のコマンドを入力して、スタートアップ コンフィギュレーションをロードします。

```
ciscoasa# copy startup-config running-config
```

ステップ 9　次のコマンドを入力して、グローバル コンフィギュレーション モードにアクセスします。

```
ciscoasa# configure terminal
```

ステップ 10　次のコマンドを入力して、デフォルト コンフィギュレーションで必要に応じてパスワードを変更します。

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

ステップ 11　次のコマンドを入力して、デフォルト コンフィギュレーションをロードします。

```
ciscoasa(config)# no config-register
```

デフォルト コンフィギュレーションのレジスタ値は 0x1 です。コンフィギュレーション レジスタの詳細については、コマンド リファレンスを参照してください。

ステップ 12　次のコマンドを入力して、新しいパスワードをスタートアップ コンフィギュレーションに保存します。

```
ciscoasa(config)# copy running-config startup-config
```

ASAv のパスワードまたはイメージの回復

ASAv のパスワードまたはイメージを回復するには、次の手順を実行します。

手順

ステップ 1　実行コンフィギュレーションを ASAv のバックアップ ファイルにコピーします。

copy running-config *filename*

例：

```
ciscoasa# copy running-config backup.cfg
```

ステップ 2　ASAv を再起動します。

reload

ステップ 3　[GNU GRUB] メニューから、下矢印を押し、**コンフィギュレーションをロードしない**オプションで **<filename>** を選択し、Enter キーを押します。ファイル名は、ASAv のデフォルトのブート イメージのファイル名です。デフォルトのブート イメージは、**fallback** コマンドによって自動的にブートされることはありません。その後、選択したブート イメージをロードします。

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

例：

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

ステップ 4　実行コンフィギュレーションにバックアップ コンフィギュレーション ファイルをコピーします。

copy *filename* **running-config**

例：

```
ciscoasa(config)# copy backup.cfg running-config
```

ステップ 5　パスワードをリセットします。

イネーブル パスワード

例：

```
ciscoasa(config)# enable password cisco123
```

ステップ 6　新しい設定を保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

パスワード回復のディセーブル化

（注）　ASAv 上でパスワード回復をディセーブルにすることはできません。

権限のないユーザがパスワード回復メカニズムを使用して ASA を危険にさらすことがないように、パスワード回復をディセーブルにするには、次の手順を実行します。

はじめる前に

ASA で、**no service password-recovery** コマンドを使用すると、ROMMON モードに入って、コンフィギュレーションを変更するのを防ぐことができます。ROMMON モードに入ると、ASA では、すべてのフラッシュ ファイル システムの消去を求めるプロンプトが表示されます。最初に消去を実行しないと、ROMMON モードを開始できません。フラッシュ ファイル システムを消去しない場合、ASA はリロードされます。パスワード回復は ROMMON モードの使用と既存のコンフィギュレーションの保持に依存しているので、この消去によって、パスワードの回復ができなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合、システムを動作可能な状態に回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（入手できる場合）をロードします。

コンフィギュレーション ファイルに表示される **service password-recovery** コマンドは、情報のためだけのものです。CLI プロンプトに対してコマンドを入力すると、設定は NVRAM に保存されます。設定を変更する唯一の方法は、CLI プロンプトでコマンドを入力することです。このコマンドの異なるバージョンで新規コンフィギュレーションをロードしても、設定は変更されません。ASA が（パスワード回復の準備で）スタートアップ時にスタートアップ コンフィギュレーションを無視するように設定されている場合にパスワード回復をディセーブルにすると、ASA は通常どおりスタートアップ コンフィギュレーションをロードするように設定を変更します。フェールオーバーを使用し、スタートアップ コンフィギュレーションを無視するようにスタンバイ装置が設定されている場合は、**no service password recovery** コマンドでスタンバイ装置に複製したときにコンフィギュレーション レジスタに同じ変更が加えられます。

手順

ステップ 1　パスワード回復をディセーブルにします。

```
no service password-recovery
```

例：

```
ciscoasa (config)# no service password-recovery
```

日時の設定

（注）　ASASM の日時を設定しないでください。この設定は、ホスト スイッチから受信します。

- 「NTP サーバを使用した日付と時刻の設定」（P.14-7）
- 「手動での日付と時刻の設定」（P.14-8）

NTP サーバを使用した日付と時刻の設定

NTP を利用して階層的なサーバ システムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイム スタンプを含む場合など、時刻が重要な操作で必要になります。複数の NTP サーバを設定できます。ASA は一番下の階層からサーバを選択し、データ信頼度の尺度にします。

手動で設定した時刻はすべて、NTP サーバから取得された時刻によって上書きされます。

はじめる前に

マルチ コンテキスト モードでは、時刻はシステム コンフィギュレーションに対してだけ設定できます。

手順

ステップ 1　[Configuration] > [Device Setup] > [System Time] > [NTP] を選択します。

ステップ 2　[Add] をクリックして、[Add NTP Server Configuration] ダイアログボックスを表示します。

ステップ 3　NTP サーバの IP アドレスを入力します。

ステップ 4　[Preferred] チェックボックスをオンにして、このサーバを優先サーバに設定します。NTP では、どのサーバの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバに同期します。精度が同じ程度であれば、優先サーバを使用します。ただし、優先サーバよりも精度が大幅に高いサーバがある場合、ASA では、精度の高いそのサーバを使用します。

ステップ 5　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。この設定では、NTP パケットの発信インターフェイスが指定されます。インターフェイスが空白の場合、ASA が使用するデフォルトの管理コンテキスト インターフェイスは、ルーティング テーブルによって決まります。管理コンテキスト（および使用可能なインターフェイス）を変更する際の安定性のために [None]（デフォルトのインターフェイス）を選択します。

ステップ 6　ドロップダウン リストから、キー番号を選択します。この設定では、この認証キーのキー ID を指定します。これにより、MD5 認証を使用して NTP サーバと通信できます。NTP サーバのパケットも、常にこのキー ID を使用する必要があります。以前に別のサーバに対してキー ID を設定した場合は、そのキー ID をリストから選択できます。それ以外の場合は、1 ～ 4294967295 の数字を入力します。

ステップ 7　[Trusted] チェックボックスをオンにして、この認証キーを信頼できるキーとして指定します。これは、認証を成功させるために必要です。

ステップ 8　認証キーを設定するめのキー値を入力します。この値は、最大 32 文字の文字列です。

ステップ 9　このキー値を再入力して、正しく 2 回入力したことを確認します。

ステップ 10　[OK] をクリックします。

ステップ 11　[Enable NTP authentication] チェックボックスをオンにして、NTP 認証を有効にします。

ステップ 12　[Apply] をクリックして変更内容を保存します。

手動での日付と時刻の設定

日付と時刻を手動で設定するには、次の手順を実行します。

はじめる前に

マルチ コンテキスト モードでは、時刻はシステム コンフィギュレーションに対してだけ設定できます。

手順

ステップ 1　[Configuration] > [Device Setup] > [System Time] > [Clock] を選択します。

ステップ 2　ドロップダウン リストからタイム ゾーンを選択します。この設定では、適切な時差を GMT に加えた（または GMT から差し引いた）タイム ゾーンを指定します。[Eastern Time]、[Central Time]、[Mountain Time]、または [Pacific Time] ゾーンを選択すると、次の時間帯で、時間が自動的に夏時間に調整されます。3 月の第二日曜日の午前 2 時～ 11 月の第一日曜日の午前 2 時。

（注）　ASA の時間帯を変更すると、インテリジェント SSM との接続がドロップされる場合があります。

ステップ 3　[**Date**] ドロップダウン リストをクリックしてカレンダーを表示します。続いて、次の方法を使用して正しい日付を検索します。

- 月の名前をクリックし、月のリストを表示し、次に目的の月をクリックします。カレンダーがその月に変わります。
- 年をクリックして年を変更します。上矢印と下矢印を使用して複数年をスクロールすることも、入力フィールドに年を入力することもできます。
- 年月の左右にある矢印をクリックすると、カレンダーが一度に 1 か月ずつ前後にスクロールします。
- カレンダーの日にちをクリックして日を設定します。

ステップ 4　時刻（時間、分、および秒）を手動で入力します。

ステップ 5　[Update Display Time] をクリックして、ASDM ペインの右下に表示される時刻を更新します。現在時刻は 10 秒ごとに自動更新されます。

マスター パスフレーズの設定

マスター パスフレーズを利用すると、プレーン テキストのパスワードが安全に、暗号化形式で保存され、1 つのキーを使用してすべてのパスワードを一様に暗号化またはマスキングできるようになります。このようにしても、機能は一切変更されません。マスター パスフレーズを使用する機能としては、次のものがあります。

- OSPF
- EIGRP
- VPN ロード バランシング
- VPN (リモート アクセスおよびサイトツーサイト)
- フェールオーバー
- AAA サーバ
- ロギング
- 共有ライセンス

（注）　フェールオーバーがイネーブルであっても、フェールオーバー共有キーが設定されていない場合に、マスター パスフレーズを変更すると、エラー メッセージが表示されます。このメッセージには、マスター パスフレーズの変更がプレーン テキストとして送信されないよう、フェールオーバー共有キーを入力する必要があることが示されます。

[Configuration] > [Device Management] > [High Availability] > [Failover] の順に選択し、[Shared Key] フィールドに任意の文字を入力するか、またはフェールオーバー 16 進キーを選択している場合はバックスペースを除く 32 の 16 進数（0-9A-Fa-f）を入力します。次に、[Apply] をクリックします。

マスター パスフレーズの追加または変更

マスター パスフレーズを追加または変更するには、次の手順を実行します。

はじめる前に

この手順を実行できるのは、HTTPS を介したコンソール、SSH、ASDM などによるセキュアセッションにおいてのみです。

手順

ステップ 1　次のいずれかのオプションを選択します。

- シングル コンテキスト モードで、[Configuration] > [Device Management] > [Advanced] > [Master Passphrase] を選択します。
- マルチ コンテキスト モードで、[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase] の順に選択します。

ステップ 2　[Advanced Encryption Standard (AES) password encryption] チェックボックスをオンにします。

有効なマスター パスフレーズがない場合は、[Apply] をクリックすると警告メッセージが表示されます。[OK] または [Cancel] をクリックして続行できます。

後からパスワードの暗号化をディセーブルにすると、暗号化された既存のパスワードはいずれも変更されず、マスター パスフレーズが存在する限り、暗号化されたパスワードはアプリケーションによって必要に応じて復号化されます。

ステップ 3　[Change the encryption master passphrase] チェックボックスをオンにして、新しいマスター パスフレーズを入力および確認できるようにします。デフォルトでは、これらはディセーブルです。

新しいマスター パスフレーズの長さは 8 ～ 128 文字にする必要があります。

既存のパスフレーズを変更する場合は、新しいパスフレーズを入力する前に、古いパスフレーズを入力する必要があります。

マスター パスフレーズを削除するには [New] および [Confirm master passphrase] フィールドを空白のままにします。

ステップ 4　[Apply] をクリックします。

マスター パスフレーズのディセーブル化

マスター パスフレーズをディセーブルにすると、暗号化されたパスワードがプレーン テキスト パスワードに戻ります。暗号化されたパスワードをサポートしていない以前のソフトウェアバージョンにダウングレードする場合は、パスフレーズを削除しておくと便利です。

はじめる前に

- ディセーブルにする現在のマスター パスフレーズがわかっていなければなりません。パスフレーズが不明の場合は、「マスター パスフレーズの削除」（P.14-11）を参照してください。
- この手順が機能するのは、HTTPS を介した Telnet、SSH、または ASDM によるセキュアセッションだけです。

手順

ステップ 1　次のいずれかのオプションを選択します。

- シングル コンテキスト モードで、[Configuration] > [Device Management] > [Advanced] > [Master Passphrase] を選択します。
- マルチ コンテキスト モードで、[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase] の順に選択します。

ステップ 2　[Advanced Encryption Standard (AES) password encryption] チェックボックスをオンにします。

有効なマスター パスフレーズがない場合は、[Apply] をクリックすると警告文が表示されます。[OK] または [Cancel] をクリックして続行します。

ステップ 3　[Change the encryption master passphrase] チェックボックスをオンにします。

ステップ 4　[Old master passphrase] フィールドに、古いマスター パスフレーズを入力します。ディセーブルにする古いマスター パスフレーズを指定する必要があります。

ステップ 5　[New master passphrase] フィールドと [Confirm master passphrase] フィールドを空白のままにします。

ステップ 6　[Apply] をクリックします。

マスター パスフレーズの削除

マスター パスフレーズは回復できません。マスター パスフレーズがわからなくなった場合や不明な場合は、削除できます。

手順

ステップ 1　マスター キーと、暗号化されたパスワードが含まれているコンフィギュレーションを削除します。

write erase

例：

```
ciscoasa(config)# write erase
```

ステップ 2　ASA を、マスター キーや暗号化パスワードのないスタートアップ コンフィギュレーションを使用してリロードします。

reload

例：

```
ciscoasa(config)# reload
```

DNS サーバの設定

ASA がホスト名を IP アドレスに解決できるようにするには、DNS を設定する必要があります。

- 「DNS サーバの設定」（P.14-12）
- 「DNS キャッシュのモニタリング」（P.14-13）

DNS サーバの設定

一部の ASA 機能では、ドメイン名で外部サーバにアクセスするために DNS サーバを使用する必要があります。たとえば、ボットネット トラフィック フィルタ機能では、ダイナミック データベース サーバにアクセスして、スタティック データベースのエントリを解決するために DNS サーバが必要です。他の機能（**ping** コマンドや **traceroute** コマンドなど）では、ping またはトレースルートする名前を入力できます。ASA では、DNS サーバと通信してこの名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。

また、アクセス ルールに完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを使用するために、DNS サーバを設定する必要があります。

（注）　ASA では、機能に応じて DNS サーバの使用が限定的にサポートされます。

はじめる前に

DNS ドメイン ルックアップをイネーブルにするすべてのインターフェイスに対して適切なルーティングおよびアクセス ルールを設定し、DNS サーバに到達できるようにしてください。

手順

ステップ 1　[Configuration] > [Device Management] > [DNS] > [DNS Client] の順に選択します。

ステップ 2　DNS ルックアップが少なくとも 1 つのインターフェイスでイネーブルになっていることを確認します。DNS サーバ グループの表の下にある [DNS lookup] インターフェイス リストで、[DNS Enabled] 列をクリックして [True] を選択し、インターフェイスでのルックアップをイネーブルにします。

ステップ 3　[DNS Setup] 領域で、次のいずれかのオプションを選択します。

- [Configure one DNS server group]
- [Configure multiple DNS server groups]

ステップ 4　次のどちらかを実行します。

- DNS グループを選択して [Edit] をクリックします。
- 複数の DNS グループを設定することにした場合、[Add] をクリックして新しいグループを追加します。グループ名を入力します。

ステップ 5　DNS サーバ グループを設定します。

a. 設定済みのサーバの IP アドレスを入力し、[Add] をクリックします。

最大 6 個の DNS サーバを追加できます。ASA では、応答を受信するまで各 DNS サーバを順に試します。[Move Up]/[Move Down] ボタンを使用して、サーバを優先度の順に並べます。

b. [Other Settings] 領域のリスト内にある次の DNS サーバを試行するまでに待機する秒数（1 ～ 30 の間）を入力します。デフォルトは 2 秒です。ASA がサーバのリストを再試行するたびに、このタイムアウト時間は倍増します。

c. 設定済みサーバのグループの DNS ドメイン名を入力します。

d. [OK] をクリックします。

ステップ 6　複数のグループがある場合は、は、使用するグループを選択して [Set Active] をクリックします。このサーバ グループが DNS 要求に使用されます。

ステップ 7　クエリーごとに 1 つの DNS 応答を強制するには、[Enable DNS Guard on all interfaces] チェックボックスをオンにします。

DNS インスペクションを設定するときに、DNS ガードも設定できます。特定のインターフェイスでは、DNS インスペクションで設定されている DNS ガードの設定がこのグローバル設定より優先されます。デフォルトでは、DNS インスペクションは DNS ガードがイネーブルになっているすべてのインターフェイスでイネーブルになっています。

ステップ 8　[Apply] をクリックして変更内容を保存します。

DNS キャッシュのモニタリング

ASA では、特定のクライアントレス SSL VPN および certificate コマンドに送信された外部 DNS クエリーの DNS 情報のローカル キャッシュを提供します。各 DNS 変換要求は、ローカル キャッシュで最初に検索されます。ローカル キャッシュに情報がある場合、結果の IP アドレスが戻されます。ローカル キャッシュで要求を解決できない場合、設定されているさまざまな DNS サーバに DNS クエリーが送信されます。外部 DNS サーバによって要求が解決された場合、結果の IP アドレスが、対応するホスト名とともにローカル キャッシュに格納されます。

DNS キャッシュのモニタリングについては、次のコマンドを参照してください。

- **show dns-hosts**

  DNS キャッシュを表示します。これには、DNS サーバからダイナミックに学習したエントリと **name** コマンドを使用して手動で入力された名前および IP アドレスが含まれます。

ASP（高速セキュリティ パス）のパフォーマンスと動作の調整

ASP はポリシーおよび設定を利用可能にする実装レイヤです。Cisco Technical Assistance Center とのトラブルシューティング時以外は直接影響することはありません。ただし、パフォーマンスと信頼性に関連するいくつかの動作を調節することができます。

- 「ルール エンジンのトランザクション コミット モデルの選択」（P.14-14）
- 「ASP ロード バランシングのイネーブル化」（P.14-14）

ルール エンジンのトランザクション コミット モデルの選択

デフォルトでは、ルールベースのポリシー（アクセス ルールなど）を変更した場合、変更はただちに有効になります。ただし、この即時性によりパフォーマンスにわずかな負担がかかります。パフォーマンスへの負担は、たとえば、ASA が 1 秒あたり 18,000 個の接続を処理しているときに 25,000 個のルールを含むポリシーを変更しようとするなど、1 秒あたりの接続数が多い環境における非常に大きなルール リストにとってはより顕著です。

ルール エンジンはさらに迅速なルール ルックアップを実現するためにルールをコンパイルするため、パフォーマンスに影響します。デフォルトでは、システムは接続試行の評価時にコンパイルされていないルールも検索して、新しいルールが適用されるようにします。ルールがコンパイルされていないため、検索に時間がかかります。

この動作を変更して、ルール エンジンがトランザクション モデルを使用してルールの変更を導入し、新しいルールがコンパイルされて使用可能な状態になるまで古いルールを引き続き使用するようにできます。トランザクション モデルを使用することで、ルールのコンパイル中にパフォーマンスが落ちることはありません。次の表は、その動作の違いを明確にします。

モデル	コンパイル前	コンパイル中	コンパイル後
デフォルト	古いルールに一致します。	新しいルールに一致します (接続数/秒のレートは減少します)。	新しいルールに一致します。
トランザクション	古いルールに一致します。	古いルールに一致します (接続数/秒のレートは影響を受けません)。	新しいルールに一致します。

トランザクション モデルのその他のメリットには、インターフェイス上の ACL を交換するときに、古い ACL を削除して新しいポリシーを適用するまでに時間差がないことがあります。この機能により受け入れ可能な接続が操作中にドロップされる可能性が削減されます。

ヒント　ルール タイプのトランザクション モデルをイネーブルにする場合、コンパイルの先頭と末尾をマークする Syslog が生成されます。これらの Syslog には 780001 ～ 780004 までの番号が付けられます。

ルール エンジンのトランザクション コミット モデルをイネーブルにするには、[Configuration] > [Device Management] > [Advanced] > [Rule Engine] を選択し、必要なオプションを選択します。

- **Access group**：グローバルにまたはインターフェイスに適用されるアクセス ルール。
- **NAT**：ネットワーク アドレス変換ルール。

ASP ロード バランシングのイネーブル化

ASP のロード バランシング機能によって、次の問題を回避しやすくなります。

- フロー上での突発的なトラフィックの増加によって発生するオーバーラン
- 特定のインターフェイス受信リングをオーバーサブスクライブする大量のフローによって発生するオーバーラン
- シングル コアが負荷を維持できない、比較的負荷の高いインターフェイスの受信リングによって発生するオーバーラン

asp load-balance per-packet コマンドは、複数のコアが 1 つのインターフェイスの受信リングから受信したパケットを同時に処理できます。システムがパケットをドロップして、**show cpu** コマンドの出力が 100% を大幅に下回ると、パケットが多数の無関係の接続に属している場合にこのコマンドがスループットの促進に役立つ場合があります。**auto** オプションによって、ASA はパケット単位のロード バランシングのオンとオフを自動的に切り替えることができます。

複数のコアを搭載する ASA モデルでは、多くのパケットがドロップされていても CPU 使用率が 100% を著しく下回っている場合、ロード バランシング オプションをイネーブルにする必要があります。

[Configuration] > [Device] > [Management] > [Advanced] > [ASP] を選択し、[Enable per-packet ASP load balance] チェックボックスをオンにします。

[Dynamically enable or disable ASP load balancing based on traffic monitoring] チェックボックスをオンにして、ASA 5585 での ASP ロード バランシングを自動的にイネーブルにします。

基本設定の履歴

機能名	プラットフォーム リリース	説明
マスター パスフレーズ	8.3(1)	この機能が導入されました。マスター パスフレーズを利用すると、プレーン テキストのパスワードが安全に、暗号化形式で保存され、1 つのキーを使用してすべてのパスワードを一様に暗号化またはマスキングできるようになります。このようにしても、機能は一切変更されません。 次の画面が導入されました。[Configuration] > [Device Management] > [Advanced] > [Master Passphrase]。[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase]。

機能名	プラットフォーム リリース	説明
デフォルトの Telnet パスワードの削除	9.0(2)、9.1(2)	ASA への管理アクセスのセキュリティ向上のために、Telnet のデフォルト ログイン パスワードが削除されました。Telnet を使用してログインする前に、パスワードを手動で設定する必要があります。 （注） Telnet ユーザ認証を設定しない場合、ログイン パスワードが使用されるのは Telnet に対してのみです。 以前はパスワードをクリアすると、ASA がデフォルト「cisco」を復元していました。今ではパスワードをクリアすると、パスワードは削除されるようになりました。 ログイン パスワードは、スイッチから ASASM への Telnet セッションでも使用されます（**session** コマンドを参照）。最初 ASASM のアクセスでは、ログイン パスワードを設定するまで、**service-module session** コマンドを使用します。 変更された ASDM 画面はありません。
ASP ロード バランシング	9.3(2)	この機能が導入されました。ASP ロード バランシング メカニズムを利用すると、複数の CPU コアでインターフェイス受信リングからパケットを受信して個別に処理できるため、パケット損失が減少し、スループットが改善します。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced] > [ASP Load Balancing]。

DHCP サービス

この章では、DHCP サーバまたは DHCP リレーを設定する方法について説明します。

DHCP サーバについて

DHCP は、IP アドレスなどのネットワーク コンフィギュレーション パラメータを DHCP クライアントに提供します。Cisco ASA は、ASA インターフェイスに接続されている DHCP クライアントに、DHCP サーバを提供できます。DHCP サーバは、ネットワーク コンフィギュレーション パラメータを DHCP クライアントに直接提供します。

クライアントは、DHCP サーバを見つけてコンフィギュレーション情報の割り当てを要求するときに、予約された、リンク スコープのマルチキャスト アドレスを使用します。つまり、クライアントとサーバが同じリンクに接続されている必要があります。ただし、管理のしやすさ、コスト、またはスケーラビリティが問題となる場合は、DHCP クライアントから、同じリンクに接続されていないサーバにメッセージを送信できるようにすることを推奨します。DHCP リレー エージェント（クライアント ネットワーク上に常駐できます）は、クライアントとサーバの間でメッセージを中継できます。リレー エージェントの動作は、クライアントに対して透過的です。

IPv4 DHCP クライアントは、サーバに到達するために、マルチキャスト アドレスではなくブロードキャストを使用します。DHCP クライアントは UDP ポート 68 でメッセージを待ちます。DHCP サーバは UDP ポート 67 でメッセージを待ちます。

RFC 3315 で規定されている DHCP for IPv6（DHCPv6）を利用すると、IPv6 DHCP サーバがコンフィギュレーション パラメータ（ネットワーク アドレスまたはプレフィックスおよび DNS サーバ アドレスなど）を IPv6 ノード（つまり、DHCP クライアント）に送信できるようになります。DHCPv6 は次のマルチキャスト アドレスを使用します。

- All_DHCP_Relay_Agents_and_Servers（FF02::1:2）は、リンク スコープのマルチキャスト アドレスです。クライアントと、ネイバーの（つまり、オンリンクの）リレー エージェントおよびサーバとの通信に使用されます。すべての DHCPv6 サーバとリレー エージェントは、このマルチキャスト グループのメンバです。

- DHCPv6 リレー サービスとサーバは、UDP ポート 547 のメッセージをリッスンします。ASA DHCPv6 リレー エージェントは、UDP ポート 547 と All_DHCP_Relay_Agents_and_Servers マルチキャスト アドレスの両方をリッスンします。

DHCP リレー エージェントについて

インターフェイスで受信した DHCP 要求を 1 つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。DHCP クライアントは、最初の DHCPDISCOVER メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワーク セグメントにクライアントがある場合、ASA はブロードキャスト トラフィックを転送しないため、UDP ブロードキャストは通常転送されません。

ブロードキャストを受信している ASA のインターフェイスが DHCP 要求を別のインターフェイスの DHCP サーバに転送するように設定すると、この状況を改善できます。

DHCP サービスのライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

すべての ASA モデルで、DHCP クライアント アドレスの最大数はライセンスによって異なります。

- ホストが 10 台に制限されている場合、使用可能な DHCP の最大プールは 32 アドレスです。
- ホストが 50 台に制限されている場合、使用可能な DHCP の最大プールは 128 アドレスです。
- ホスト数に制限がない場合、使用可能な DHCP の最大プールは 256 アドレスです。

DHCP サービスのガイドライン

ファイアウォール モードのガイドライン

トランスペアレント ファイアウォール モードではサポートされません。詳細については、「DHCP リレーのガイドライン」（P.15-3）を参照してください。

IPv6 のガイドライン

インターフェイス固有の DHCP リレー サーバについては、IPv6 をサポートしません。

DHCP サーバのガイドライン

- 使用可能な DHCP の最大プールは 256 アドレスです。
- ASA のインターフェイスごとに 1 つの DHCP サーバだけを設定できます。各インターフェイスは、専用のアドレス プールのアドレスを使用できます。しかし、DNS サーバ、ドメイン名、オプション、ping のタイムアウト、WINS サーバなど他の DHCP 設定はグローバルに設定され、すべてのインターフェイス上の DHCP サーバによって使用されます。

- DHCP クライアントや DHCP リレー サービスは、サーバがイネーブルになっているインターフェイス上では設定できません。また、DHCP クライアントは、サーバがイネーブルになっているインターフェイスに直接接続する必要があります。
- ASA は、QIP DHCP サーバを DHCP プロキシ サービスとともに使用することはサポートしません。
- DHCP サーバもイネーブルになっている場合、リレー エージェントをイネーブルにすることはできません。
- ASA DHCP サーバは、BOOTP 要求をサポートしていません。マルチコンテキスト モードでは、複数のコンテキストで使用されるインターフェイスで DHCP サーバまたは DHCP リレー サービスをイネーブルにすることはできません。
- ASA が DHCP 要求を受信すると、DHCP サーバに検出メッセージが送信されます。このメッセージには、グループ ポリシー内の **dhcp-network-scope** コマンドで設定された IP アドレス（サブネットワーク内の）が含まれます。そのサブネットワークに含まれるアドレス プールがサーバにある場合、サーバから、検出メッセージの送信元 IP アドレスではなく、その IP アドレスにプール情報を含む提供メッセージが送信されます。
- クライアントが接続すると、ASA は、サーバ リスト内のすべてのサーバに検出メッセージを送信します。このメッセージには、グループ ポリシー内の **dhcp-network-scope** コマンドで設定された IP アドレス（サブネットワーク内の）が含まれます。ASA は最初に受信した提供メッセージを選択し、他のものをドロップします。そのサブネットワークに含まれるアドレス プールがサーバにある場合、サーバから、検出メッセージの送信元 IP アドレスではなく、その IP アドレスにプール情報を含む提供メッセージが送信されます。アドレスの更新が必要なときは、リース サーバ（アドレスを取得したサーバ）での更新を試みます。指定された再試行回数（4 回）の後で DHCP 更新に失敗した場合は、事前定義された時間が過ぎた後で ASA は DHCP 再バインド フェーズに移行します。再バインド フェーズでは、ASA はグループ内のすべてのサーバに同時に要求を送信します。ハイ アベイラビリティ環境では、リース情報が共有されるため、他のサーバがリースを許可し、ASA はバインド済みの状態に戻る場合があります。再バインド フェーズ中に、（3 回の再試行の後で）サーバ リスト内のサーバのいずれからも応答がない場合、ASA はそのエントリを消去します。

  たとえば、サーバに範囲が 209.165.200.225 ～ 209.165.200.254 でマスクが 255.255.255.0 のプールがあり、**dhcp-network-scope** コマンドで指定されている IP アドレスが 209.165.200.1 である場合、サーバからASAにそのプールが提供メッセージで送信されます。

  dhcp-network-scope コマンドの設定は、VPN ユーザにのみ適用されます。

DHCP リレーのガイドライン

- シングル モードおよびコンテキストごとに、グローバルおよびインターフェイス固有のサーバを合わせて 10 台までの DHCPv4 リレー サーバを設定できます。インターフェイスごとには、4 台まで設定できます。
- シングル モードおよびコンテキストごとに、10 台までの DHCPv6 リレー サーバを設定できます。IPv6 のインターフェイス固有のサーバはサポートされません。
- DHCP サーバもイネーブルになっている場合、リレー エージェントをイネーブルにできません。
- DHCP リレー サービスがイネーブルになっていて、複数の DHCP リレー サーバが定義されているときは、ASA によって、定義された各 DHCP リレー サーバにクライアントの要求が転送されます。また、クライアントの DHCP リレー バインディングが削除されるまで、サーバからの応答もクライアントに転送されます。ASA で ACK、NACK、ICMP 到達不能、拒否のいずれかの DHCP メッセージを受け取ると、バインディングが削除されます。

- DHCP プロキシ サービスとして動作しているインターフェイス上で DHCP リレー サービスをイネーブルにすることはできません。最初に VPN DHCP コンフィギュレーションを削除する必要があります。このようにしない場合は、エラー メッセージが表示されます。このエラーは、DHCP リレーと DHCP プロキシの両方のサービスのがイネーブルになっている場合に発生します。DHCP リレーと DHCP プロキシの両方ではなく一方のサービスだけがイネーブルになっていることを確認してください。
- DHCP リレー サービスはトランスペアレント ファイアウォール モードでは使用できません。ただし、アクセス リストを使用して DHCP トラフィックを通過させることはできます。トランスペアレント モードで DHCP 要求と応答が ASA を通過できるようにするには、2 つのアクセス リストを設定する必要があります。1 つは内部インターフェイスから外部への DCHP 要求を許可するもので、もう 1 つは逆方向に向かうサーバからの応答を許可するためのものです。
- IPv4 の場合、クライアントは直接 ASA に接続する必要があり、他のリレー エージェントやルータを介して要求を送信できません。IPv6 の場合、ASA は別のリレー サーバからのパケットをサポートします。
- マルチ コンテキスト モードでは、複数のコンテキストによって使用されるインターフェイス上で DHCP リレーをイネーブルにできません。
- DHCP クライアントは、ASA が要求をリレーする DHCP サーバとは別のインターフェイスに存在する必要があります。

DHCP サーバの設定

ここでは、ASA の DHCP サーバを設定する方法について説明します。

ステップ 1　DHCP サーバを有効にします。「DHCP サーバのイネーブル化」（P.15-4）を参照してください。

ステップ 2　高度な DHCP オプションを設定します。「高度な DHCP オプションの設定」（P.15-6）を参照してください。

ステップ 3　DHCPv4 リレー エージェントまたは DHCPv6 リレー エージェントを設定します。「DHCPv4 リレー エージェントの設定」（P.15-7）または「DHCPv6 リレー エージェントの設定」（P.15-8）を参照してください。

DHCP サーバのイネーブル化

ASA のインターフェイスで DHCP サーバをイネーブルにするには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [DHCP] > [DHCP Server] の順に選択します。

ステップ 2　インターフェイスを選択し、[Edit] をクリックします。

a. 選択したインターフェイス上で DHCP サーバをイネーブルにするには、[Enable DHCP Server] チェックボックスをオンにします。

b. [DHCP Address Pool] フィールドに、DHCP サーバが使用する最下位から最上位の IP アドレスの範囲を入力します。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。

c. [Optional Parameters] 領域で、次の項目を設定します。
   - インターフェイスに設定された DNS サーバ（1 および 2）。
   - インターフェイスに設定された WINS サーバ（プライマリおよびセカンダリ）。
   - インターフェイスのドメイン名。
   - インターフェイス上で ASA が ICMP ping の応答を待つ時間（ミリ秒単位）。
   - インターフェイス上に設定された DHCP サーバが、割り当てた IP アドレスの使用を DHCP クライアントに許可する時間。
   - ASA が指定インターフェイス（通常は外側）上で DHCP クライアントとして動作している場合に、自動コンフィギュレーションのための DNS、WINS、ドメイン名情報を提供する DHCP クライアントのインターフェイス。
   - より多くの DHCP オプションを設定するには、[Advanced] をクリックしして [Advanced DHCP Options] ダイアログボックスを表示します。詳細については、「高度な DHCP オプションの設定」（P.15-6）を参照してください。

d. [Dynamic Settings for DHCP Server] 領域の [Update DNS Clients] チェックボックスをオンにして、クライアントの PTR リソース レコードを更新するデフォルトのアクションに加えて、選択した DHCP サーバでの次の更新アクションの実行を指定します。
   - [Update Both Records] チェックボックスをオンにして、DHCP サーバが A レコードと PTR RR の両方を更新するように指定します。
   - [Override Client Settings] チェックボックスをオンにして、DHCP サーバのアクションが、DHCP クライアントによって要求された更新アクションを上書きするように指定します。

e. [OK] をクリックして、[Edit DHCP Server] ダイアログボックスを閉じます。

ステップ 3　指定したインターフェイス（通常は外側）で、ASA が DHCP クライアントとして動作している場合に限り、DHCP 自動コンフィギュレーションをイネーブルにするには、DHCP サーバ テーブルの下にある [Global DHCP Options] 領域の [Enable Auto-configuration from interface] チェックボックスをオンにします。

DHCP 自動コンフィギュレーションでは、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバ、ドメイン名、および WINS サーバの情報が、DHCP サーバから DHCP クライアントに提供されます。自動コンフィギュレーションを介して取得された情報が、[Global DHCP Options] 領域でも手動で指定されている場合、検出された情報よりも手動で指定した情報の方が優先されます。

ステップ 4　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。

ステップ 5　インターフェイスの DHCP または PPPoE クライアントの WINS パラメータを VPN クライアントのパラメータで上書きするには、[Allow VPN override] チェックボックスをオンにします。

ステップ 6　[DNS Server 1] フィールドに、DHCP クライアント用のプライマリ DNS サーバの IP アドレスを入力します。

ステップ 7　[DNS Server 2] フィールドに、DHCP クライアント用の代替 DNS サーバの IP アドレスを入力します。

ステップ 8　[Domain Name] フィールドに、DHCP クライアント用の DNS ドメイン名（たとえば、example.com）を入力します。

ステップ 9　[Lease Length] フィールドに、リースが期限切れになるまでにクライアントが割り当てられた IP アドレスを使用可能な時間を秒数で入力します。有効値の範囲は 300 ～ 1048575 秒です。デフォルト値は 3600 秒（1 時間）です。

ステップ 10　[Primary WINS Server] フィールドに、DHCP クライアント用のプライマリ WINS サーバの IP アドレスを入力します。

ステップ 11　[Secondary WINS Server] フィールドに、DHCP クライアント用の代替 WINS サーバの IP アドレスを入力します。

ステップ 12　アドレスの衝突を避けるために、ASA は、1 つのアドレスに ICMP ping パケットを 2 回送信してから、そのアドレスを DHCP クライアントに割り当てます。[Ping Timeout] フィールドに、ASA が DHCP ping の試行のタイムアウトを待つ時間をミリ秒単位で入力します。有効値の範囲は 10 ～ 10000 ミリ秒です。デフォルト値は 50 ミリ秒です。

ステップ 13　追加の DHCP オプションとパラメータを指定するには、[Advanced] をクリックしして [Configuring Advanced DHCP Options] ダイアログボックスを表示します。詳細については、「高度な DHCP オプションの設定」（P.15-6）を参照してください。

ステップ 14　[Dynamic DNS Settings for DHCP Server] 領域で、DHCP サーバ用の DDNS 更新設定を設定します。[Update DNS Clients] チェックボックスをオンにして、クライアントの PTR リソース レコードを更新するデフォルトのアクションに加えて、選択した DHCP サーバが次の更新アクションも実行するように指定します。

- [Update Both Records] チェックボックスをオンにして、DHCP サーバが A レコードと PTR RR の両方を更新するように指定します。
- [Override Client Settings] チェックボックスをオンにして、DHCP サーバのアクションが、DHCP クライアントによって要求された更新アクションを上書きするように指定します。

ステップ 15　[Apply] をクリックして変更内容を保存します。

高度な DHCP オプションの設定

ASA は、RFC 2132、RFC 2562、および RFC 5510 に記載されている情報を送信する DHCP オプションをサポートしています。

高度な DHCP オプションを使用して、DHCP クライアントに DNS、WINS、およびドメイン名の各パラメータを提供できます。DHCP 自動コンフィギュレーションの設定を使用して、これらの値を取得したり、これらを手動で定義したりできます。この情報の定義に 2 つ以上の方法を使用すると、次の優先順位で情報が DHCP クライアントに渡されます。

1. 手動で行われた設定
2. 高度な DHCP オプションの設定
3. DHCP 自動コンフィギュレーションの設定

たとえば、DHCP クライアントが受け取るドメイン名を手動で定義し、次に DHCP 自動コンフィギュレーションをイネーブルにできます。DHCP 自動コンフィギュレーションによって、DNS サーバおよび WINS サーバとともにドメインが検出されても、手動で定義したドメイン名が、検出された DNS サーバ名および WINS サーバ名とともに DHCP クライアントに渡されます。これは、DHCP 自動コンフィギュレーション プロセスで検出されたドメイン名よりも、手動で定義されたドメイン名の方が優先されるためです。

手順

ステップ 1　[Configuration] > [Device Management] > [DHCP] > [DHCP Server] の順に選択し、[Advanced] をクリックします。

ステップ 2　ドロップダウン リストからオプション コードを選択します。オプション 1、12、50 ～ 54、58 ～ 59、61、67、82 を 除き、すべての DHCP オプション（1 ～ 255）がサポートされています。

ステップ 3　設定するオプションを選択します。一部のオプションは標準です。標準オプションの場合、オプション名がオプション番号の後のカッコ内に表示され、オプション番号およびオプション パラメータは、オプションでサポートされるものに制限されます。他のすべてのオプションにはオプション番号だけが表示され、オプションに指定する適切なパラメータを選択する必要があります。たとえば、DHCP オプション 2（タイム オフセット）を選択した場合、このオプションに入力できるのは 16 進数値だけです。他のすべての DHCP オプションでは、すべてのオプション値タイプを使用できますが、適切なものを選択する必要があります。

ステップ 4　[Option Data] 領域に、このオプションによって DHCP クライアントに返す情報のタイプを指定します。標準 DHCP オプションの場合、サポートされるオプションの値タイプだけが使用可能です。他のすべての DHCP オプションでは、すべてのオプション値タイプを使用できます。[Add] をクリックして、オプションを DHCP オプション リストに追加します。[Delete] をクリックして、オプションを DHCP オプション リストから削除します。

- [IP Address] をクリックして、IP アドレスが DHCP クライアントに返されることを示します。IP アドレスは最大 2 つまで指定できます。IP アドレス 1 および IP アドレス 2 は、ドット付き 10 進数表記の IP アドレスを示します。

  （注）　関連付けられた [IP Address] フィールドの名前は、選択した DHCP オプションに基づいて変わります。たとえば、DHCP オプション 3（ルーター）を選択した場合、フィールド名は [Router 1] および [Router 2] に変わります。

- [ASCII] をクリックして、ASCII 値が DHCP クライアントに返されることを指定します。[Data] フィールドに ASCII 文字列を入力します。文字列にスペースを含めることはできません。

  （注）　関連付けられた [Data] フィールドの名前は、選択した DHCP オプションに基づいて変わります。たとえば、DHCP オプション 14（ダンプ ファイル名）を選択した場合、関連付けられた [Data] フィールドの名前は [File Name] に変わります。

- [Hex] をクリックして、16 進数値が DHCP クライアントに返されることを指定します。[Data] フィールドに、偶数個の数字（スペースを含まない）から成る 16 進数文字列を入力します。0x プレフィックスを使用する必要はありません。

  （注）　関連付けられた [Data] フィールドの名前は、選択した DHCP オプションに基づいて変わります。たとえば、DHCP オプション 2（タイム オフセット）を選択した場合、関連付けられた [Data] フィールドは [Offset] フィールドになります。

ステップ 5　[OK] をクリックして、[Advanced DHCP Options] ダイアログボックスを閉じます。

ステップ 6　[Apply] をクリックして変更内容を保存します。

DHCPv4 リレー エージェントの設定

インターフェイスに DHCP 要求が届くと、設定に基づいて、ASA からその要求がリレーされる DHCP サーバが決定されます。設定できるサーバのタイプは次のとおりです。

- インターフェイス固有の DHCP サーバ：特定のインターフェイスに DHCP 要求が届くと、ASA はその要求をインターフェイス固有のサーバにだけリレーします。

- グローバル DHCP サーバ：インターフェイス固有のサーバが設定されていないインターフェイスに DHCP 要求が届くと、ASA はその要求をすべてのグローバル サーバにリレーします。インターフェイスにインターフェイス固有のサーバが設定されている場合、グローバル サーバは使用されません。

DHCPv6 リレー エージェントの設定

インターフェイスに DHCPv6 要求が届くと、ASA はその要求をすべての DHCPv6 グローバル サーバにリレーします。

手順

ステップ 1　[Configuration] > [Device Management] > [DHCP] > [DHCP Relay] の順に選択します。

ステップ 2　[DHCP Relay Agent] 領域で、各インターフェイスの必要なサービスのチェックボックスをオンにします。

- [IPv4] > [DHCP Relay Enabled]。
- [IPv4] > [Set Route]：サーバからの DHCP メッセージのデフォルト ゲートウェイ アドレスを、元の DHCP 要求をリレーした DHCP クライアントに最も近い ASA インターフェイスのアドレスに変更します。このアクションを行うと、クライアントは、自分のデフォルト ルートを設定して、DHCP サーバで異なるルータが指定されている場合でも、ASA をポイントすることができます。パケット内にデフォルトのルータ オプションがなければ、ASA は、そのインターフェイスのアドレスを含んでいるデフォルト ルータを追加します。
- [IPv6] > [DHCP Relay Enabled]。
- [Trusted Interface]：信頼する DHCP クライアント インターフェイスを指定します。DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できます。DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、ASA DHCP リレー エージェントが受信した DHCP パケットに、Option 82 がすでに設定されているが、giaddr フィールド（サーバにパケットを転送する前にリレー エージェントによって設定された DHCP リレー エージェント アドレスを指定するフィールド）は 0 に設定されている場合、ASA はそのパケットをデフォルトでドロップします。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。[Set dhcp relay information as trusted on all interfaces] チェックボックスをオンにして、すべてのインターフェイスを信頼することもできます（ステップ 7 を参照）。

ステップ 3　[Global DHCP Relay Servers] 領域に、DHCP 要求をリレーする 1 つまたは複数の DHCP サーバを追加します。

a.　[Add] をクリックします。[Add Global DHCP Relay Server] ダイアログボックスが表示されます。

b.　[DHCP Server] フィールドに、DHCP サーバの IPv4 アドレスまたは IPv6 アドレスを入力します。

c.　[Interface] ドロップダウン リストから、指定した DHCP サーバが接続されているインターフェイスを選択します。

d.　[OK] をクリックします。

新たに追加されたグローバル DHCP リレー サーバが、[Global DHCP Relay Servers] リストに表示されます。

ステップ 4　（オプション）[IPv4 Timeout] フィールドに、DHCP アドレス処理のために許容する時間を秒数で入力します。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 60 秒です。

ステップ 5　（オプション）[IPv6 Timeout] フィールドに、DHCP アドレス処理のために許容する時間を秒数で入力します。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 60 秒です。

ステップ 6　[DHCP Relay Interface Servers] 領域で、特定のインターフェイスの DHCP 要求がリレーされるインターフェイス固有の DHCP サーバを 1 台以上追加します。

a. [Add] をクリックします。[Add DHCP Relay Server] ダイアログボックスが表示されます。

b. [Interface] ドロップダウン リストから、DHCP クライアントが接続されているインターフェイスを選択します。グローバル DHCP サーバのように要求の出力インターフェイスを指定しないことに注意してください。代わりに、ASA はルーティング テーブルを使用して出力インターフェイスを決定します。

c. [Server to**...**] フィールドに DHCP サーバの IPv4 アドレスを入力し、[Add>>] をクリックします。サーバが右側のリストに追加されます。全体の最大数に余裕があれば、4 台までサーバを追加します。インターフェイス固有のサーバでは、IPv6 はサポートされていません。

d. [OK] をクリックします。

新しく追加したインターフェイスの DHCP リレー サーバが、[DHCP Relay Interface Server] リストに表示されます。

ステップ 7　すべてのインターフェイスを信頼できるインターフェイスとして設定するには、[Set dhcp relay information as trusted on all interfaces] チェックボックスをオンにします。個別にインターフェイスを信頼することもできます（ステップ 2 を参照）。

ステップ 8　[Apply] をクリックして設定値を保存します。

DHCP サービスのモニタリング

DHCP サービスをモニタするには、次の画面を参照してください。

- [Monitoring] > [Interfaces] > [DHCP] > [DHCP Client Lease Information]

  このペインには、設定されている DHCP クライアントの IP アドレスが表示されます。

- [Monitoring] > [Interfaces] > [DHCP] > [DHCP Server Table]

  このペインには、設定されている動的な DHCP クライアントの IP アドレスが表示されます。

- [Monitoring] > [Interfaces] > [DHCP] > [DHCP Statistics]

  このペインには、DHCP メッセージのタイプ、カウンタ、値、方向、受信メッセージ数、および送信メッセージ数が表示されます。

- [Tools] > [Command Line Interface]

  このペインでは、非対話式のコマンドを ASA に送信して結果を表示します。

DHCP サービスの履歴

表 15-1　DHCP サービスの履歴

機能名	プラットフォーム リリース	説明
DHCP	7.0(1)	ASA は、DHCP サーバまたは DHCP リレー サービスを ASA のインターフェイスに接続されている DHCP クライアントに提供することができます。 次の画面が導入されました。 [Configuration] > [Device Management] > [DHCP] > [DHCP Relay] [Configuration] > [Device Management] > [DHCP] > [DHCP Server]
DHCP for IPv6（DHCPv6）	9.0(1)	IPv6 のサポートが追加されました。 次の画面が変更されました。[Configuration] > [Device Management] > [DHCP] > [DHCP Relay]。
インターフェイスごとの DHCP リレー サーバ（IPv4 のみ）	9.1(2)	DHCP リレー サーバをインターフェイスごとに設定できるようになりました。特定のインターフェイスに届いた要求は、そのインターフェイス用に指定されたサーバに対してのみリレーされます。インターフェイス単位の DHCP リレーでは、IPv6 はサポートされません。 次の画面が変更されました。[Configuration] > [Device Management] > [DHCP] > [DHCP Relay]。
DHCP の信頼できるインターフェイス	9.1(2)	DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できるようになりました。DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、ASA DHCP リレー エージェントが受信した DHCP パケットに、Option 82 がすでに設定されているが、giaddr フィールド（サーバにパケットを転送する前にリレー エージェントによって設定された DHCP リレー エージェント アドレスを指定するフィールド）は 0 に設定されている場合、ASA はそのパケットをデフォルトでドロップします。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。 次の画面が変更されました。[Configuration] > [Device Management] > [DHCP] > [DHCP Relay]。
DHCP 再バインド機能	9.1(4)	DHCP 再バインド フェーズに、クライアントはトンネル グループ リスト内の他の DHCP サーバへの再バインドを試みるようになりました。このリリース以前には、DHCP リースの更新に失敗した場合、クライアントは代替サーバへ再バインドしませんでした。 変更された ASDM 画面はありません。

ダイナミック DNS

この章では、ダイナミック DNS（DDNS）のアップデート方式の設定方法について説明します。

DDNS について

DDNS アップデートでは、DNS を DHCP に組み込みます。これら 2 つのプロトコルは相互補完します。DHCP は、IP アドレス割り当てを集中化および自動化します。DDNS アップデートは、割り当てられたアドレスとホスト名の間のアソシエーションを事前定義された間隔で自動的に記録します。DDNS は、頻繁に変わるアドレスとホスト名のアソシエーションを頻繁にアップデートできるようにします。これにより、たとえばモバイル ホストは、ユーザまたは管理者が操作することなく、ネットワーク内を自由に移動できます。DDNS は、DNS サーバ上で、名前からアドレスへのマッピングと、アドレスから名前へのマッピングをダイナミックにアップデートして、同期化します。

DDNS の名前とアドレスのマッピングは、DHCP サーバ上で 2 つのリソース レコード（RR）で行われます。A RR では、名前から IP アドレスへのマッピングが保持され、PTR RR では、アドレスから名前へのマッピングが行われます。DDNS 更新を実行するための 2 つの方式（RFC 2136 で規定されている IETF 標準、および一般的な HTTP 方式）のうち、ASA では、IETF 方式をサポートしています。

関連項目

- 「DHCP サーバの設定」（P.15-4）

DDNS アップデート コンフィギュレーション

2 つの最も一般的な DDNS アップデート コンフィギュレーションは次のとおりです。

- DHCP クライアントは A RR をアップデートし、DHCP サーバは PTR RR をアップデートします。
- DHCP サーバは、A RR と PTR RR の両方をアップデートします。

通常、DHCP サーバはクライアントの代わりに DNS PTR RR を保持します。クライアントは、必要なすべての DNS アップデートを実行するように設定できます。サーバは、これらのアップデートを実行するかどうかを設定できます。DHCP サーバは、PTR RR をアップデートするクライアントの完全修飾ドメイン名（FQDN）を認識している必要があります。クライアントは Client FQDN と呼ばれる DHCP オプションを使用して、サーバに FQDN を提供します。

UDP Packet Size

DDNS は、DNS 要求者が UDP パケットのサイズをアドバタイズできるようにし、512 オクテットより大きいパケットの転送を容易にします。DNS サーバは UDP 上で要求を受信すると、OPT RR から UDP パケット サイズを識別し、要求者により指定された最大 UDP パケット サイズにできるだけ多くのリソース レコードを含めることができるよう、応答のサイズを調整します。DNS パケットのサイズは、BIND の場合は最大 4096 バイト、Windows 2003 DNS サーバの場合は 1280 バイトです。次に示す追加の **message-length maximum** コマンドを使用できます。

- 既存のグローバル制限：**message-length maximum 512**
- クライアントまたはサーバ固有の制限：**message-length maximum client 4096** および **message-length maximum server 4096**
- OPT RR フィールドで指定されたダイナミック値：**message-length maximum client auto**

3 つのコマンドが同時に存在する場合、ASA は、設定されたクライアントまたはサーバ制限まで長さの自動設定を可能にします。他のすべての DNS トラフィックについては、message-length maximum が使用されます。

DDNS のガイドライン

コンテキスト モードのガイドライン

[DNS Client] ペイン用にトランスペアレント モードでのみサポートされています。

DDNS の設定

ここでは、DDNS の設定方法について説明します。

ダイナミック DNS を設定し、DNS サーバをアップデートするには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [DNS] > [Dynamic DNS] を選択します。

ステップ 2　[Add] をクリックして、[Add Dynamic DNS Update Method] ダイアログボックスを表示します。

ステップ 3　DDNS のアップデート方式の名前を入力します。

ステップ 4　アップデート方式で設定された DNS 更新試行間の更新間隔を日、時間、分、および秒で指定します。

- 更新試行間の日数を 0 ～ 364 日の間で選択します。
- 更新試行間の時間数を 0 ～ 23（整数）から選択します。
- 更新試行間の分数を 0 ～ 59（整数）から選択します。
- 更新試行間の秒数を 0 ～ 59（整数）から選択します。

これらの単位は、追加式です。つまり、日数に 0、時間数に 0、分数に 5、秒数に 15 を入力した場合、このアップデート方式がアクティブである限り、5 分 15 秒ごとに更新が試行されます。

ステップ 5　DNS クライアントがアップデートするサーバ リソース レコード アップデートを保存するには、次のいずれかのオプションを選択します。

- A リソース レコードと PTR リソース レコードの両方。
- A リソース レコードのみ。

ステップ 6　[OK] をクリックして、[Add Dynamic DNS Update Method] ダイアログボックスを表示します。

新しいダイナミック DNS クライアント設定が表示されます。

（注）　既存の方式を編集する場合、[Name] フィールドは*表示専用*となっており、編集のために選択した方式の名前が表示されます。

ステップ 7　設定されている各インターフェイスの DDNS 設定を追加するには、[Add] をクリックしての [Dynamic DNS Interface Settings] ダイアログボックスを表示します。

ステップ 8　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。

ステップ 9　インターフェイスに割り当てられたアップデート方式をドロップダウン リストから選択します。

ステップ 10　DDNS クライアントのホスト名を入力します。

ステップ 11　リソース レコード アップデートを保存するには、次のいずれかのオプションを選択します。

- [Default]（PTR Records）では、サーバによりクライアントが PTR レコードの更新を要求するように指定されます。
- [Both]（PTR Records および A Records）では、サーバによりクライアントが A および PTR DNS リソース レコードの両方を要求するように指定されます。
- [None] では、サーバによりクライアントが更新を要求しないように指定されます。

（注）　このアクションを有効にするには、選択したインターフェイス上で DHCP がイネーブルになっている必要があります。

ステップ 12　[OK] をクリックして、[Add Dynamic DNS Interface Settings] ダイアログボックスを閉じます。

新しいダイナミック DNS インターフェイス設定が表示されます。

ステップ 13　変更を保存するには [Apply] をクリックし、変更を破棄して新しく入力するには [Reset] をクリックします。

DDNS のモニタリング

DDNS ステータスのモニタリングについては、次の画面を参照してください。

- [Tools] > [Command Line Interface]

  このペインでは、非対話式のコマンドを ASA に送信して結果を表示します。

DDNS の履歴

表 16-1　DDNS の履歴

機能名	リリース	機能情報
DDNS	7.0(1)	この機能が導入されました。 次の画面が導入されました。 [Configuration] > [Device Management] > [DNS] > [DNS Client] [Configuration] > [Device Management] > [DNS] > [Dynamic DNS]

PART 5

オブジェクトと ACL

アクセス コントロールのオブジェクト

オブジェクトとは、コンフィギュレーションで使用するための再利用可能なコンポーネントです。インライン IP アドレス、サービス、名前などの代わりに、Cisco ASA コンフィギュレーションでオブジェクトを定義し、使用できます。オブジェクトを使用すると、コンフィギュレーションのメンテナンスが容易になります。これは、一箇所でオブジェクトを変更し、このオブジェクトを参照している他のすべての場所に反映できるからです。オブジェクトを使用しなければ、1 回だけ変更するのではなく、必要に応じて各機能のパラメータを変更する必要があります。たとえば、ネットワーク オブジェクトによって IP アドレスおよびサブネット マスクが定義されており、このアドレスを変更する場合、この IP アドレスを参照する各機能ではなく、オブジェクト定義でアドレスを変更することだけが必要です。

オブジェクトのガイドライン

IPv6 のガイドライン

IPv6 のサポートには次の制約が伴います。

- ASA は、ネストされた IPv6 ネットワーク オブジェクト グループはサポートしません。したがって、IPv6 エントリが含まれるオブジェクトを別の IPv6 オブジェクト グループの下でグループ化することはできません。
- 1 つのネットワーク オブジェクト グループの中で IPv4 および IPv6 のエントリを混在させることができます。NAT に対しては、混合オブジェクト グループは使用できません。

その他のガイドラインと制限事項

- オブジェクトおよびオブジェクト グループは同じネーム スペースを共有するため、オブジェクトの名前は固有のものでなければなりません。「Engineering」という名前のネットワーク オブジェクト グループと「Engineering」という名前のサービス オブジェクト グループを作成する場合、少なくとも 1 つのオブジェクト グループ名の最後に識別子（または「タグ」）を追加して、その名前を固有のものにする必要があります。たとえば、「Engineering_admins」と「Engineering_hosts」という名前を使用すると、オブジェクト グループの名前を固有のものにして特定可能にすることができます。
- オブジェクト名は、文字、数字、および！@#$%^& （）- _{} を含めて、64 文字までに制限されています。オブジェクト名は、大文字と小文字が区別されます。

- （アクセス ルールの詳細設定で）前方参照をイネーブルにしない限り、コマンドで使用されているオブジェクトを削除したり、空にすることはできません。

オブジェクトの設定

次の各項では、主にアクセス コントロールで使用されるオブジェクトを設定する方法について説明します。

- 「ネットワーク オブジェクトとグループの設定」（P.17-2）
- 「サービス オブジェクトとサービス グループの設定」（P.17-3）
- 「ローカル ユーザ グループの設定」（P.17-5）
- 「セキュリティ グループ オブジェクト グループの設定」（P.17-6）
- 「時間範囲の設定」（P.17-7）

ネットワーク オブジェクトとグループの設定

ネットワーク オブジェクトおよびグループは、IP アドレスまたはホスト名を特定します。これらのオブジェクトをアクセス コントロール リストで使用して、ルールを簡素化できます。

- 「ネットワーク オブジェクトの設定」（P.17-2）
- 「ネットワーク オブジェクト グループの設定」（P.17-3）

ネットワーク オブジェクトの設定

1 つのネットワーク オブジェクトには、1 つのホスト、ネットワーク IP アドレス、IP アドレスの範囲、または完全修飾ドメイン名（FQDN）を入れることができます。

また、オブジェクトに対して NAT ルールをイネーブルにすることもできます（FQDN オブジェクトを除く）。オブジェクト NAT の設定に関する詳細については、ファイアウォール コンフィギュレーション ガイドを参照してください。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Network Objects/Group] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] > [Network Object] を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存のオブジェクトを選択し、[Edit] をクリックします。

ステップ 3　オブジェクトの [Type] フィールドと [IP version] フィールドに基づいて、オブジェクトのアドレスを設定します。

- [Host]：単一ホストの IPv4 または IPv6 アドレス。たとえば、10.1.1.1 または 2001:DB8::0DB8:800:200C:417A。
- [Network]：ネットワーク アドレス。IPv4 の場合は、マスクを含めます。たとえば、**IP address** = 10.0.0.0 **Netmask** = 255.0.0.0。IPv6 の場合は、**IP Address** = 2001:DB8:0:CD30:: **Prefix Length** = 60 のように、プレフィックスを含めます。

- [Range]：アドレスの範囲。IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。
- [FQDN]：完全修飾ドメイン名。つまり、www.example.com のようなホスト名。

ステップ 4　[OK] をクリックし、続いて [Apply] をクリックします。

これでルールの作成時にこのネットワーク オブジェクトを使用できます。オブジェクトを編集した場合、変更内容は自動的にそのオブジェクトを使用するすべてのルールに継承されます。

ネットワーク オブジェクト グループの設定

ネットワーク オブジェクト グループには、インライン ネットワークやホストと同様に複数のネットワーク オブジェクトを含めることができます。ネットワーク オブジェクト グループは、IPv4 と IPv6 の両方のアドレスの混在を含めることができます。

ただし、IPv4 と IPv6 が混在するオブジェクト グループや、FQDN オブジェクトが含まれているオブジェクト グループを、NAT に使用することはできません。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] > [Network Object Group] を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存のオブジェクトを選択し、[Edit] をクリックします。

ステップ 3　次の技法を組み合わせて使用して、グループにネットワーク オブジェクトを追加します。

- **既存のネットワーク オブジェクト/グループ**：すでに定義されているネットワーク オブジェクトまたはグループを選択し、[Add] をクリックしてグループに含めます。
- **新しいネットワーク オブジェクト メンバの作成**：新しいネットワーク オブジェクトの条件を入力し、[Add] をクリックします。オブジェクトに名前を付ける場合、変更を適用すると新しいオブジェクトが作成され、グループに追加されます。ホストまたはネットワークを追加する場合、名前は任意です。

ステップ 4　すべてのメンバ オブジェクトを追加したら、[OK] をクリックしてから、[Apply] をクリックします。

これでルールの作成時にこのネットワーク オブジェクト グループを使用できます。編集したオブジェクト グループの場合、変更内容は自動的にそのグループを使用するすべてのルールに継承されます。

サービス オブジェクトとサービス グループの設定

サービス オブジェクトとグループでは、プロトコルおよびポートを指定します。これらのオブジェクトをアクセス コントロール リストで使用して、ルールを簡素化できます。

- 「サービス オブジェクトの設定」（P.17-4）
- 「サービス グループの設定」（P.17-4）

サービス オブジェクトの設定

サービス オブジェクトには、単一のプロトコル、ICMP、ICMPv6、TCP または UDP ポートまたはポート範囲を含めることができます。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Service Object/Group] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] > [Service Object] を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存のオブジェクトを選択し、[Edit] をクリックします。

ステップ 3　サービス タイプを選択し、必要に応じて詳細を入力します。

- プロトコル：0 ～ 255 の番号。または、**ip**、**tcp**、**udp**、**gre** といった既知の名前。番号、名前、およびその意味の一覧については、「プロトコルとアプリケーション」（P.43-11）を参照してください。
- ICMP、ICMP6：メッセージ タイプとコードのフィールドを空白のままにすると、ICMP/ICMP バージョン 6 のあらゆるメッセージに一致させることができます。ICMP タイプを名前または番号（0 ～ 255）で指定することで、オブジェクトをそのメッセージ タイプに制限できます（オプション）。タイプを指定する場合、そのタイプ（1 ～ 255）に対する ICMP コードを任意で指定できます。コードを指定しない場合は、すべてのコードが使用されます。ICMP タイプの一覧については、「ICMP タイプ」（P.43-15）を参照してください。
- TCP、UDP：送信元、宛先、またはその両方に対して、任意でポートを指定できます。ポートは名前または番号で指定できます（一覧については、「TCP ポートと UDP ポート」（P.43-12）を参照してください）。次の演算子を含めることができます。
  - **<**：小なり。たとえば、<80。
  - **>**：大なり。たとえば、>80。
  - **!=**：等しくない。たとえば、!=80。
  - **-**（ハイフン）：値の包括的な範囲。たとえば、100-200。

ステップ 4　[OK]、続いて [Apply] をクリックします。

サービス グループの設定

1 つのサービス オブジェクト グループには、さまざまなプロトコルが混在しています。必要に応じて、TCP または UDP の送信元および宛先のポートも入れることができます。

はじめる前に

ここで説明する一般的なサービス オブジェクト グループを使用して、すべてのサービスをモデル化できます。ただし、ASA 8.3(1) よりも前に使用可能であったサービス グループ オブジェクトのタイプを設定することもできます。こうした従来のオブジェクトには、TCP/UDP/TCP-UDP ポート グループ、プロトコル グループ、および ICMP グループが含まれます。これらのグループのコンテンツは、ICMP6 または ICMP コードをサポートしない ICMP グループを除く、一般的なサービス オブジェクト グループの関連する設定に相当します。これらの従来のオブジェクトを使用したい場合は、**object-service** コマンドに関する説明を Cisco.com のコマンド リファレンスで確認してください。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Service Objects/Groups] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] > [Service Group] を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存のオブジェクトを選択し、[Edit] をクリックします。

ステップ 3　次の技法を組み合わせて使用して、グループにサービス オブジェクトを追加します。

- **既存のサービス オブジェクト/グループ**：すでに定義されているサービス オブジェクトまたはグループを選択し、[Add] をクリックしてグループに含めます。
- **新しいサービス オブジェクト メンバの作成**：新しいサービス オブジェクトの条件を入力し、[Add] をクリックします。オブジェクトに名前を付ける場合、変更を適用すると新しいオブジェクトが作成され、グループに追加されます。そうでない場合、名前のないオブジェクトはこのグループだけのメンバです。TCP-UDP オブジェクトに名前を付けることはできません。これらはそのグループだけのメンバです。

ステップ 4　すべてのメンバ オブジェクトを追加したら、[OK] をクリックしてから、[Apply] をクリックします。

これでルールの作成時にこのサービス オブジェクト グループを使用できます。編集したオブジェクト グループの場合、変更内容は自動的にそのグループを使用するすべてのルールに継承されます。

ローカル ユーザ グループの設定

作成したローカル ユーザ グループは、アイデンティティ ファイアウォールをサポートする機能で使用できます。そのグループを拡張 ACL に入れると、たとえばアクセス ルールでも使用できるようになります。

ASA は、Active Directory ドメイン コントローラでグローバルに定義されているユーザ グループについて、Active Directory サーバに LDAP クエリーを送信します。ASA は、そのグループをアイデンティティ ベースのルール用にインポートします。ただし、ローカライズされたセキュリティ ポリシーを持つローカル ユーザ グループを必要とする、グローバルに定義されていないネットワーク リソースが ASA によりローカライズされている場合があります。ローカル ユーザ グループには、Active Directory からインポートされる、ネストされたグループおよびユーザ グループを含めることができます。ASA は、ローカル グループおよび Active Directory グループを統合します。

ユーザは、ローカル ユーザ グループと Active Directory からインポートされたユーザ グループに属することができます。

ACL でユーザ名とユーザ グループ名を直接使用できるため、次の場合にだけローカル ユーザ グループを設定する必要があります。

- ローカル データベースで定義されているユーザのグループを作成する。
- AD サーバで定義されている単一のユーザ グループでキャプチャされなかったユーザまたはユーザ グループのグループを作成する。

アイデンティティ ファイアウォールをイネーブルにする方法については、第 32 章「アイデンティティ ファイアウォール」を参照してください。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Local User Groups] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存のオブジェクトを選択し、[Edit] をクリックします。

ステップ 3　次のいずれかの方法を使用して、オブジェクトにユーザまたはグループを追加します。

- **既存のユーザまたはグループを選択**：ユーザまたはグループを含むドメインを選択してから、ユーザ名またはグループ名をリストから選択し、[Add] をクリックします。リストが長い場合、ユーザの検索をサポートするために [Find] ボックスを使用します。名前は、選択されたドメインのサーバから取得されます。
- **ユーザ名を手動で入力**：ユーザ名またはグループ名を下部の編集ボックスに入力し、[**Add**] をクリックするだけです。この方法を使用すると、選択されたドメイン名は無視され、ドメイン名を指定していない場合はデフォルト ドメインが使用されます。ユーザの場合、フォーマットは *domain_name\username*; for groups, there is a double \\, *domain_name\\group_name* です。

ステップ 4　すべてのメンバ オブジェクトを追加したら、[OK] をクリックしてから、[Apply] をクリックします。

これでルールの作成時にこのユーザ オブジェクト グループを使用できます。編集したオブジェクト グループの場合、変更内容は自動的にそのグループを使用するすべてのルールに継承されます。

セキュリティ グループ オブジェクト グループの設定

作成したセキュリティ グループ オブジェクト グループは、Cisco TrustSec をサポートする機能で使用できます。そのグループを拡張 ACL に入れると、たとえばアクセス ルールで使用できるようになります。

Cisco TrustSec と統合されているときは、ASA は ISE からセキュリティ グループの情報をダウンロードします。ISE はアイデンティティ リポジトリとしても動作し、Cisco TrustSec タグからユーザ アイデンティティへのマッピングと、Cisco TrustSec タグからサーバ リソースへのマッピングを行います。セキュリティ グループ ACL のプロビジョニングおよび管理は、中央集中型で ISE 上で行います。

ただし、ASA には、グローバルには定義されていない、ローカライズされたネットワーク リソースが存在することがあり、そのようなリソースにはローカル セキュリティ グループとローカライズされたセキュリティ ポリシーが必要です。ローカル セキュリティ グループには、ISE からダウンロードされた、ネストされたセキュリティ グループを含めることができます。ASA は、ローカルと中央のセキュリティ グループを統合します。

ASA 上でローカル セキュリティ グループを作成するには、ローカル セキュリティ オブジェクト グループを作成します。1 つのローカル セキュリティ オブジェクト グループに、1 つ以上のネストされたセキュリティ オブジェクト グループまたはセキュリティ ID またはセキュリティ グループ名を入れることができます。ユーザは、ASA 上に存在しない新しいセキュリティ ID またはセキュリティ グループ名を作成することもできます。

ASA 上で作成したセキュリティ オブジェクト グループは、ネットワーク リソースへのアクセスの制御に使用できます。セキュリティ オブジェクト グループを、アクセス グループやサービス ポリシーの一部として使用できます。

ASA と Trustsec を統合する方法については、第 33 章「ASA と Cisco TrustSec」を参照してください。

ヒント　ASA にとって不明なタグや名前を使用してグループを作成する場合、そのタグや名前が ISE で解決されるまで、そのグループを使用するすべてのルールが非アクティブになります。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Security Group Object Groups] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] を選択し、新しいオブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存のオブジェクトを選択し、[Edit] をクリックします。

ステップ 3　次のいずれかの方法を使用して、オブジェクトにセキュリティ グループを追加します。

- **既存のローカル セキュリティ グループ オブジェクト グループを選択**：すでに定義されているオブジェクトのリストから選択し、[Add] をクリックします。リストが長い場合、オブジェクトの検索をサポートするために [Find] ボックスを使用します。
- **ISE から検出されたセキュリティ グループを選択**：既存のグループのリストからグループを選択し、[Add] をクリックします。
- **セキュリティ タグまたは名前を手動で追加**：タグ番号またはセキュリティ グループ名を下部の編集ボックスに入力し、[Add] をクリックするだけです。タグは、1 から 65533 までの数字であり、IEEE 802.1X 認証、Web 認証、または ISE による MAC 認証バイパス（MAB）を通じてデバイスに割り当てられます。セキュリティ グループの名前は ISE 上で作成され、セキュリティ グループをわかりやすい名前で識別できるようになります。セキュリティ グループ テーブルによって、SGT がセキュリティ グループ名にマッピングされます。有効なタグと名前については、ISE の設定を参照してください。

ステップ 4　すべてのメンバ オブジェクトを追加したら、[OK] をクリックしてから、[Apply] をクリックします。

これでルールの作成時にこのセキュリティ グループ オブジェクト グループを使用できます。編集したオブジェクト グループの場合、変更内容は自動的にそのグループを使用するすべてのルールに継承されます。

時間範囲の設定

時間範囲オブジェクトは、開始時刻、終了時刻、およびオプションの繰り返しエントリで構成される特定の時刻を定義します。これらのオブジェクトは、特定の機能または資産に時間ベースでアクセスするために ACL ルールで使用されます。たとえば、勤務時間中にのみ特定のサーバへのアクセスを許可するアクセス ルールを作成できます。

（注）　時間範囲オブジェクトには複数の定期的エントリを含めることができます。1 つの時間範囲に absolute 値と periodic 値の両方が指定されている場合は、periodic 値は absolute の開始時刻に到達した後にのみ評価され、absolute の終了時刻に到達した後は評価されません。

時間範囲を作成してもデバイスへのアクセスは制限されません。この手順では、時間範囲だけを定義します。その後、アクセス コントロール ルールでオブジェクトを使用する必要があります。

手順

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Time Ranges] を選択します。

ステップ 2　次のどちらかを実行します。

- [Add] を選択し、新しい時間範囲を追加します。名前を入力し、任意で説明を入力します。
- 既存の時間範囲を選択し、[Edit] をクリックします。

ステップ 3　全体的な開始時刻および終了時刻を選択します。

デフォルトでは今すぐ開始し、終了することはありませんが、特定の日時を設定することもできます。時間範囲には、入力した時刻も含まれます。

ステップ 4　（オプション）時間範囲がアクティブになる曜日や週単位の繰り返し間隔など、全体的にアクティブな時間内に繰り返し期間を設定します。

a. [Add] をクリックするか、既存の期間を選択して [Edit] をクリックします。

b. 次のどちらかを実行します。

- [Specify days of the week and times on which this recurring range will be active] をクリックし、リストから日付と時刻を選択します。
- [Specify a weekly interval when this recurring range will be active] をクリックし、リストから日付と時刻を選択します。

c. [OK] をクリックします。

ステップ 5　[OK] をクリックし、さらに [Apply] をクリックします。

オブジェクトのモニタリング

ネットワーク、サービス、およびセキュリティ グループ オブジェクトに関して、個々のオブジェクトの使用状況を分析できます。[Configuration] > [Firewall] > [Objects] フォルダにある各オブジェクトのページで、[Where Used] ボタンをクリックします。

ネットワーク オブジェクトの場合、[Not Used] ボタンをクリックすると、ルールまたは他のオブジェクトで使用されていないオブジェクトを見つけることもできます。この表示によって、未使用のオブジェクトを簡単に削除できるようになります。

オブジェクトの履歴

機能名	Platform リリース	説明
オブジェクト グループ	7.0(1)	オブジェクト グループによって、ACL の作成とメンテナンスが簡素化されます。
正規表現およびポリシー マップ	7.2(1)	インスペクション ポリシー マップで使用される正規表現およびポリシー マップが導入されました。 **class-map type regex** コマンド、**regex** コマンド、および**match regex** コマンドが導入されました。
オブジェクト	8.3(1)	オブジェクトのサポートが導入されました。
アイデンティティ ファイアウォールでのユーザ オブジェクト グループの使用	8.4(2)	アイデンティティ ファイアウォールのためのユーザ オブジェクト グループが導入されました。
Cisco TrustSec のためのセキュリティ グループ オブジェクト グループ	8.4(2)	Cisco TrustSec のためのセキュリティ グループ オブジェクト グループが導入されました。
IPv4 および IPv6 の混合ネットワーク オブジェクト グループ	9.0(1)	以前は、ネットワーク オブジェクト グループに含まれているのは、すべて IPv4 アドレスであるか、すべて IPv6 アドレスでなければなりませんでした。現在では、ネットワーク オブジェクト グループが、IPv4 と IPv6 の両方のアドレスの混合をサポートするようになりました。 **（注）**　混合オブジェクト グループを NAT に使用することはできません。
ICMP コードによって ICMP トラフィックをフィルタリングするための拡張 ACL とオブジェクト機能拡張	9.0(1)	ICMP コードに基づいて ICMP トラフィックの許可または拒否ができるようになりました。 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [Objects] > [Service Objects/Groups] [Configuration] > [Firewall] > [Access Rule]

アクセス コントロール リスト

アクセス コントロール リスト（ACL）は、さまざまな機能で使用されます。ACL をアクセス ルールとしてインターフェイスに適用するか、グローバルに適用すると、アプライアンスを通過するトラフィックが許可または拒否されます。ACL では、他の機能のために、機能を適用するトラフィックを選択し、制御サービスではなく照合サービスを実行します。

ここでは、ACL の基本と ACL を設定およびモニタする方法について説明します。アクセス ルールとは、グローバルに、またはインターフェイスに適用される ACL のことです。これについては、『ファイアウォール コンフィギュレーション ガイド』で詳しく説明します。

ACL について

アクセス コントロール リスト（ACL）では、ACL のタイプに応じてトラフィック フローを 1 つまたは複数の特性（送信元および宛先 IP アドレス、IP プロトコル、ポート、EtherType、その他のパラメータを含む）で識別します。ACL は、さまざまな機能で使用されます。ACL は 1 つまたは複数のアクセス コントロール エントリ（ACE）で構成されます。

ACL タイプ

ASA では、次のタイプの ACL が使用されます。

- 拡張 ACL：主に使用されるタイプです。この ACL は、サービス ポリシー、AAA ルール、WCCP、ボットネット トラフィック フィルタ、VPN グループおよび DAP ポリシーを含むさまざまな機能で、トラフィックがデバイスを通過するのを許可および拒否するアクセス ルールとトラフィックの照合に使用されます。ASDM では、これらの機能の多くに独自のルール ページがあります。これらのページでは、ACL Manager で定義した拡張 ACL は使用できません。ただし、ACL Manager には、これらのページで作成した ACL が表示されます。「拡張 ACL の設定」（P.18-7）を参照してください。

- EtherType ACL：トランスペアレント ファイアウォール モードで IP 以外の レイヤ 2 トラフィックに適用されます。これらのルールを使用すると、レイヤ 2 パケット内の EtherType 値に基づいてトラフィックを許可またはドロップできます。EtherType ACL では、デバイスでの非 IP トラフィック フローを制御できます。『ファイアウォール コンフィギュレーション ガイド』のアクセス ルールの章を参照してください。
- Webtype ACL：クライアントレス SSL VPN トラフィックのフィルタリングに使用されます。この ACL では、URL または宛先アドレスに基づいてアクセスを拒否できます。「Webtype ACL の設定」（P.18-11）を参照してください。
- 標準 ACL：宛先アドレスだけでトラフィックを識別します。このタイプの ACL は、少数の機能（ルート マップと VPN フィルタ）でしか使用されません。VPN フィルタでは拡張アクセス リストも使用できるので、標準 ACL の使用はルート マップだけにしてください。「標準 ACL の設定」（P.18-10）を参照してください。

次の表に、ACL の一般的な使用目的と使用するタイプを示します。

表 18-1　ACL のタイプと一般的な使用目的

ACL の使用目的	ACL Type	説明
IP トラフィックのネットワーク アクセスの制御（ルーテッド モードおよびトランスペアレント モード）	拡張	ASA では、拡張 ACL により明示的に許可されている場合を除き、低位のセキュリティ インターフェイスから高位のセキュリティ インターフェイスへのトラフィックは認められません。 **（注）** また、ASA インターフェイスに管理アクセスの目的でアクセスするには、ホスト IP アドレスを許可する ACL は必要ありません。必要なのは、第 36 章「管理アクセス」の説明に従って管理アクセスを設定することだけです。
AAA ルールでのトラフィック識別	拡張	AAA ルールでは、ACL を使用してトラフィックを識別します。
特定のユーザの IP トラフィックに対するネットワーク アクセス コントロールの強化	拡張、ユーザごとに AAA サーバからダウンロード	ユーザに適用するダイナミック ACL をダウンロードするように RADIUS サーバを設定できます。または、ASA 上に設定済みの ACL の名前を送信するようにサーバを設定できます。
VPN アクセスおよびフィルタリング	拡張 規格	リモート アクセスおよびサイト間 VPN のグループ ポリシーでは、標準または拡張 ACL がフィルタリングに使用されます。リモート アクセス VPN では、クライアント ファイアウォール設定とダイナミック アクセス ポリシーにも拡張 ACL が使用されます。
モジュラ ポリシー フレームワークのトラフィック クラス マップ内でのトラフィック識別	拡張	ACL を使用すると、クラス マップ内のトラフィックを識別できます。このマップは、モジュラ ポリシー フレームワークをサポートする機能に使用されます。モジュラ ポリシー フレームワークをサポートする機能には、TCP および一般的な接続設定やインスペクションなどがあります。
トランスペアレント ファイアウォール モードの場合、IP 以外のトラフィックのネットワーク アクセスの制御	EtherType	EtherType に基づいてトラフィックを制御する ACL を設定できます。

表 18-1　ACL のタイプと一般的な使用目的（続き）

ACL の使用目的	ACL Type	説明
ルート フィルタリングおよび再配布の特定	規格 拡張	各種のルーティング プロトコルでは、IP アドレスのルート フィルタリングと（ルート マップを介した）再配布に ACL が使用されます（IPv4 アドレスの場合は標準 ACL が、IPv6 アドレスの場合は拡張 ACL がそれぞれ使用されます）。
クライアントレス SSL VPN のフィルタリング	Webtype	Webtype ACL は、URL と宛先をフィルタリングするように設定できます。

ACL Manager

ACL Manager は、次の 2 つの方法で表示できます。

- メイン ウィンドウで、たとえば [Configuration] > [Firewall] > [Advanced] > [ACL Manager] の順に選択する。この場合、ACL Manager には拡張 ACL のみが表示されます。これらの ACL には、[Access Rules]、[Service Policy Rules]、および [AAA Rules] の各ページで作成したルールによって生成された ACL が含まれます。ACL Manager で編集を行う場合は、これらのルールに悪影響を与えないように注意してください。ここで加えた変更は、これらの他のページに反映されます。
- ACL が必要なポリシーから、フィールドの横にある [Manage] ボタンをクリックする。この場合、ポリシーで標準 ACL と拡張 ACL が許可されていれば、両方の ACL のタブが個別に表示されます。許可されていない場合は、標準、拡張、または Webtype の ACL のみを表示するようにビューがフィルタリングされます。EtherType ACL は表示されません。

メイン ウィンドウで標準 ACL と Webtype ACL を設定できるように、これらの ACL 用の個別のページが用意されています。これらのページは、名前のない ACL Manager と機能的に同じです。

- 標準 ACL：[Configuration] > [Firewall] > [Advanced] > [Standard ACL]。
- Webtype ACL：[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Web ACLs]。

ACL 名

各 ACL には、outside_in、OUTSIDE_IN、101 などの名前または数値 ID があります。名前は 241 文字以下にする必要があります。実行コンフィギュレーションを表示するときに名前を簡単に見つけられるように、すべて大文字にすることを検討してください。

ACL の目的を識別するのに役立つ命名規則を作成します。ASDM では、「*interface-name_purpose_direction*」などの命名規則が使用されます。たとえば、「外部」インターフェイスにインバウンド方向で適用される ACL の場合には、「outside_access_in」のようになります。

従来、ACL ID は数値でした。標準 ACL は、1 ～ 99 または 1300 ～ 1999 の範囲にありました。拡張 ACL は、100 ～ 199 または 2000 ～ 2699 の範囲にありました。ASA では、これらの範囲は強制されませんが、数値を使用する場合は、IOS ソフトウェアを実行するルータとの一貫性を保つために、これらの命名規則を引き続き使用することをお勧めします。

ACE の順序

1 つの ACL は、1 つまたは複数の ACE で構成されます。特定の行に明示的に ACE を挿入しない限り、ある ACL 名について入力した各 ACE はその ACL の末尾に追加されます。

ACE の順序は重要です。ASA でパケットを転送するか廃棄するかを決定する場合、ASA は各 ACE に対して、エントリの指定順にパケットをテストします。一致が見つかると、ACE はそれ以上チェックされません。

したがって、一般的なルールの後に具体的なルールを配置した場合、具体的なルールは決してヒットしない可能性があります。たとえば、ネットワーク 10.1.1.0/24 を許可し、そのサブネット上のホスト 10.1.1.15 からのトラフィックをドロップする場合、10.1.1.15 を拒否する ACE は 10.1.1.0/24 を許可する ACE の前に置く必要があります。10.1.1.0/24 を許可する ACE を先にすると、10.1.1.15 は許可され、拒否 ACE は決して一致しません。

必要に応じて、[Up] ボタンと [Down] ボタンを使用してルールを再配置します。

許可/拒否と 一致/不一致の比較

アクセス コントロール エントリでは、ルールに一致するトラフィックを「許可」または「拒否」します。グローバル アクセス ルールやインターフェイス アクセス ルールなど、トラフィックが ASA の通過を許可されるか、ドロップされるかを決定する機能に ACL を適用する場合、「許可」と「拒否」は文字どおりの意味を持ちます。

サービス ポリシー ルールなどのその他の機能の場合、「許可」と「拒否」は実際には「一致」または「不一致」を意味します。この場合、ACL では、アプリケーション インスペクションやサービス モジュールへのリダイレクトなど、その機能のサービスを受けるトラフィックを選択しています。「拒否される」トラフィックは、単に ACL に一致せず、したがってサービスを受けないトラフィックのことです（ASDM では、たとえば、サービス ポリシー ルールでは実際には一致/不一致が使用され、AAA ルールでは認証/未認証が使用されますが、CLI では常に許可/拒否が使用されます）。

アクセス コントロールによる暗黙的な拒否

すべての ACL の末尾には、暗黙の deny ステートメントがあります。したがって、インターフェイスに適用される ACL などのトラフィック制御 ACL では、あるタイプのトラフィックを明示的に許可しない場合、そのトラフィックはドロップされます。たとえば、1 つまたは複数の特定のアドレス以外のすべてのユーザが ASA 経由でネットワークにアクセスできるようにするには、特定のアドレスを拒否してから、その他のすべてのアドレスを許可する必要があります。

サービス対象のトラフィックの選択に使用される ACL の場合は、明示的にトラフィックを「許可」する必要があります。「許可」されていないトラフィックはサービスの対象になりません。「拒否された」トラフィックはサービスをバイパスします。

EtherType ACL の場合、ACL の末尾にある暗黙的な拒否は、IP トラフィックや ARP には影響しません。たとえば、EtherType 8037 を許可する場合、ACL の末尾にある暗黙的な拒否によって、拡張 ACL で以前許可（または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暗黙的に許可）した IP トラフィックがブロックされることはありません。ただし、EtherType ACE で*明示的に*すべてのトラフィックを拒否すると、IP および ARP トラフィックが拒否されます。許可されるのは、自動ネゴシエーションなどの物理プロトコル トラフィックだけです。

NAT 使用時に拡張 ACL で使用する IP アドレス

NAT または PAT を使用すると、アドレスまたはポートが変換され、通常は内部アドレスと外部アドレスがマッピングされます。変換されたポートまたはアドレスに適用される拡張 ACL を作成する必要がある場合は、実際の（変換されていない）アドレスまたはポートを使用するか、マッピングされたアドレスまたはポートを使用するかを決定する必要があります。要件は機能によって異なります。

実際のアドレスとポートが使用されるので、NAT コンフィギュレーションが変更されても ACL を変更する必要はなくなります。

実際の IP アドレスを使用する機能

次のコマンドおよび機能では、インターフェイスに表示されるアドレスがマッピング アドレスである場合でも、実際の IP アドレスを使用します。

- アクセス ルール（**access-group** コマンドで参照される拡張 ACL）
- サービス ポリシー ルール（モジュラ ポリシー フレームワークの **match access-list** コマンド）
- ボットネット トラフィック フィルタのトラフィック分類（**dynamic-filter enable classify-list** コマンド）
- AAA ルール（**aaa ... match** コマンド）
- WCCP（**wccp redirect-list group-list** コマンド）

たとえば、内部サーバ 10.1.1.5 用の NAT を設定して、パブリックにルーティング可能な外部の IP アドレス 209.165.201.5 をこのサーバに付与する場合は、この内部サーバへのアクセスを外部トラフィックに許可するアクセス ルールの中で、サーバのマッピング アドレス（209.165.201.5）ではなく実際のアドレス（10.1.1.5）を参照する必要があります。

マッピング IP アドレスを使用する機能

次の機能は、ACL を使用しますが、これらの ACL は、インターフェイス上で認識されるマッピングされた値を使用します。

- IPsec ACL
- **capture** コマンドの ACL
- ユーザ単位 ACL
- ルーティング プロトコルの ACL
- 他のすべての機能の ACL

Time-Based ACE

ルールが一定期間だけアクティブになるように、拡張 ACE と Webtype ACE に時間範囲オブジェクトを適用することができます。このタイプのルールを使用すると、特定の時間帯には許容できるものの、それ以外の時間帯には許容できないアクティビティを区別できます。たとえば、勤務時間中に追加の制限を設け、勤務時間後または昼食時にその制限を緩めることができます。逆に、勤務時間外は原則的にネットワークをシャットダウンすることもできます。時間範囲オブジェクトの作成の詳細については、「時間範囲の設定」（P.17-7）を参照してください。

（注）　ACL を非アクティブにするための指定の終了時刻の後、約 80 ～ 100 秒の遅延が発生する場合があります。たとえば、指定の終了時刻が 3:50 の場合、この 3:50 は終了時刻に含まれているため、コマンドは、3:51:00 ～ 3:51:59 の間に呼び出されます。コマンドが呼び出された後、ASA は現在実行されているすべてのタスクを終了し、コマンドに ACL を無効にさせます。

ACL のガイドライン

ファイアウォール モードのガイドライン

標準 ACL と拡張 ACL は、ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされます。

Webtype ACL は、ルーテッド モードのみでサポートされます。

EtherType ACL は、トランスペアレント モードのみでサポートされます。

IPv6 のガイドライン

拡張 ACL と Webtype ACL では、IPv4 アドレスと IPv6 アドレスを組み合わせて使用できます。

標準 ACL では、IPv6 アドレスは使用できません。

EtherType ACL では、IP アドレスは使用しません。

（拡張 ACL のみ）アイデンティティ ファイアウォール、FQDN、Cisco TrustSec ACL をサポートしない機能

次の機能では、ACL を使用しますが、アイデンティティ ファイアウォール（個人またはグループ名を指定）、FQDN（完全修飾ドメイン名）、または Cisco TrustSec 値を含む ACL は使用できません。

- **route-map** コマンド
- VPN の **crypto map** コマンド
- VPN の **group-policy** コマンド、ただし、**vpn-filter** を除く
- WCCP
- DAP

その他のガイドラインと制限事項

- ネットワーク マスクを指定するときは、指定方法が Cisco IOS ソフトウェアの **access-list** コマンドとは異なることに注意してください。ASA では、ネットワーク マスク（たとえば、Class C マスクの 255.255.255.0）が使用されます。Cisco IOS マスクでは、ワイルドカード ビット（たとえば、0.0.0.255）が使用されます。

ACL の設定

次の各セクションでは、さまざまなタイプの汎用 ACL の設定方法について説明します。ただし、アクセス ルール（EtherType を含む）、サービス ポリシー ルール、および AAA ルールとして使用される ACL と、ASDM がこれらのルールベースのポリシー用に特定目的のページを提供しているその他の用途に使用される ACL は除きます。これらのその他の用途のためのルールの設定については、『ファイアウォール コンフィギュレーション ガイド』を参照してください。

- 「拡張 ACL の設定」（P.18-7）
- 「標準 ACL の設定」（P.18-10）
- 「Webtype ACL の設定」（P.18-11）

拡張 ACL の設定

拡張 ACL は ACE の名前付きコンテナとして表されます。新しい ACL を作成するには、まずコンテナを作成する必要があります。その後、ACL Manager でテーブルを使用して ACE を追加したり、既存の ACE を編集したり、ACE を並べ替えたりできます。

拡張 ACL には、IPv4 アドレスと IPv6 アドレスの組み合わせを含めることができます。

手順

ステップ 1　[Configuration] > [Firewall] > [Advanced] > [ACL Manager] を選択します。

ステップ 2　新しい ACL を作成する場合は、[Add] > [Add ACL] を選択し、名前を入力して [OK] をクリックします。

ACL コンテナがテーブルに追加されます。後でこのコンテナを選択して [Edit] をクリックすることにより、コンテナの名前を変更できます。

ステップ 3　次のいずれかを実行します。

- ACL の末尾に ACE を追加するには、ACL 名または ACL 内の任意の ACE を選択し、[Add] > [Add ACE] を選択します。
- ACE を特定の場所に挿入するには、既存の ACE を選択し、[Add] > [Insert] を選択してそのルールの上に ACE を追加するか、[Add] > [Insert After] を選択します。
- ルールを編集するには、ルールを選択して [Edit] をクリックします。

ステップ 4　ACE のプロパティを入力します。選択する主なオプションは次のとおりです。

- [Action: Permit/Deny]：指定したトラフィックを許可（選択）するか、拒否（選択解除、不一致）するかを選択します。
- [Source/Destination criteria]：送信元（発信アドレス）と宛先（トラフィック フローのターゲット アドレス）を定義します。通常は、ホストまたはサブネットの IPv4 アドレスまたは IPv6 アドレスを設定します。これはネットワークまたはネットワーク オブジェクト グループで表すことができます。送信元のユーザ名またはユーザ グループ名も指定できます。また、ルールをすべての IP トラフィックではなく、特定のトラフィックに限定して適用する場合は、[Service] フィールドを使用して具体的なトラフィック タイプを指定できます。Cisco TrustSec を実装している場合は、セキュリティ グループを使用して送信元と宛先を定義できます。

使用可能なすべてのオプションについては、「拡張 ACE のプロパティ」（P.18-8）を参照してください。

ACE の定義が完了したら、[OK] をクリックしてテーブルにルールを追加します。

ステップ 5　[Apply] をクリックします。

拡張 ACE のプロパティ

拡張 ACL の ACE を追加または編集するときに、次のプロパティを設定できます。多くのフィールドでは、編集ボックスの右にある「...」ボタンをクリックして、フィールドで使用できるオブジェクトを選択、作成、または編集できます。

- [Action: Permit/Deny]：指定したトラフィックを許可（選択）するか、拒否（選択解除、不一致）するかを選択します。
- [Source Criteria]：照合しようとしているトラフィックの発信者の特性を指定します。[Source] は設定する必要がありますが、その他のプロパティはオプションです。
  - [Source]：送信元の IPv4 または IPv6 アドレスです。デフォルト値は **any** です。これはすべての IPv4 または IPv6 アドレスに一致します。IPv4 のみをターゲットにする場合は **any4** を、IPv6 のみをターゲットにする場合は **any6** をそれぞれ使用できます。単一のホスト アドレス（10.100.10.5 または 2001:DB8::0DB8:800:200C:417A など）、サブネット（10.100.10.0/24 または 10.100.10.0/255.255.255.0 形式、または IPv6 の場合は 2001:DB8:0:CD30::/60）、ネットワーク オブジェクトまたはネットワーク オブジェクト グループの名前、またはインターフェイスの名前を指定できます。
  - [User]：アイデンティティ ファイアウォールを有効にしている場合は、ユーザまたはユーザ グループをトラフィックの送信元として指定できます。ユーザが現在使用している IP アドレスはルールに一致します。ユーザ名（DOMAIN\user）、ユーザ グループ（DOMAIN\\group（2 つの \ はグループ名を示します））、またはユーザ オブジェクト グループを指定できます。このフィールドでは、[...] をクリックして AAA サーバ グループから名前を選択するほうが名前を入力するよりもはるかに簡単です。。
  - [Security Group]：Cisco TrustSec を有効にしている場合は、セキュリティ グループの名前やタグ（1 ～ 65533）、またはセキュリティ グループ オブジェクトを指定できます。
  - [More Options] > [Source Service] : TCP または UDP を宛先サービスとして指定した場合は、TCP、UDP、または TCP-UDP を表す定義済みのサービス オブジェクトか、独自のオブジェクトをオプションで指定できます。通常は、宛先サービスのみを定義し、送信元サービスは定義しません。送信元サービスを定義する場合、宛先サービスのプロトコルは送信元サービスに一致する必要があります（たとえば、両方ともポート定義のある/ない TCP など）。
- [Destination Criteria]：照合しようとしているトラフィックのターゲットの特性を指定します。[Destination] は設定する必要がありますが、その他のプロパティはオプションです。
  - [Destination]：宛先の IPv4 または IPv6 アドレスです。デフォルト値は **any** です。これはすべての IPv4 または IPv6 アドレスに一致します。IPv4 のみをターゲットにする場合は **any4** を、IPv6 のみをターゲットにする場合は **any6** をそれぞれ使用できます。単一のホスト アドレス（10.100.10.5 または 2001:DB8::0DB8:800:200C:417A など）、サブネット（10.100.10.0/24 または 10.100.10.0/255.255.255.0 形式、または IPv6 の場合は 2001:DB8:0:CD30::/60）、ネットワーク オブジェクトまたはネットワーク オブジェクト グループの名前、またはインターフェイスの名前を指定できます。
  - [Security Group]：Cisco TrustSec を有効にしている場合は、セキュリティ グループの名前やタグ（1 ～ 65533）、またはセキュリティ グループ オブジェクトを指定できます。
  - [Service]：IP、TCP、UDP などのトラフィックのプロトコル。オプションで TCP および UDP のポートを指定できます。デフォルトは IP ですが、より具体的なプロトコルを指定して、ターゲットにするトラフィックをより細かく設定することができます。通常は、何らかのタイプのサービス オブジェクトを選択します。TCP および UDP の場合

は、tcp/80、tcp/http、tcp/10-20（ポート範囲）、tcp-udp/80（ポート 80 の任意の TCP または UDP トラフィックに一致）のようにポートを指定できます。サービスの指定の詳細については、「拡張 ACE のサービスの仕様」（P.18-9）を参照してください。

- [Description] : ACE の目的に関する説明を 1 行あたり 100 文字以下で入力します。複数行を入力できます。各行は CLI の注釈として追加され、注釈は ACE の前に配置されます。

（注） 1 つのプラットフォーム（Windows など）上で英語以外の文字でコメントを追加し、それらの文字を別のプラットフォーム（Linux など）から削除しようとした場合、元の文字が正しく認識されないため編集や削除を実行できない可能性があります。この制限は、各種言語の文字をさまざまな方法でエンコードするプラットフォームの依存性によるものです。

- [Enable Logging]、[Logging Level]、[More Options] > [Logging Interval] : ロギング オプションでは、ルールについて syslog メッセージをどのように生成するかを定義します。次のロギング オプションを実装できます。
  - [Deselect Enable Logging] : ルールのロギングを無効にします。このルールに一致するトラフィックについては、どのタイプの syslog も発行されません。
  - [Select Enable Logging with Logging Level = Default] : ルールのデフォルト ロギングを提供します。拒否されたパケットごとに syslog メッセージ 106023 が発行されます。アプライアンスが攻撃を受けている場合、このメッセージの発行頻度はサービスに影響を及ぼす可能性があります。
  - [Select Enable Logging with Non-Default Logging Level] : 106023 の代わりに、集約された syslog メッセージ 106100 を提供します。メッセージ 106100 は、まず最初にヒットしたときに発行されます。その後、[More Options] > [Logging Interval] で設定した間隔ごとに再発行され、その間隔内のヒット数を示します。推奨されるロギング レベルは [Informational] です。

    拒否メッセージを集約すると、攻撃の影響を軽減できるとともに、場合によってはメッセージの分析が容易になります。DoS 攻撃を受けている場合、メッセージ 106101 が表示されることがあります。これは、メッセージ 106100 のヒット カウントの生成に使用されるキャッシュされた拒否フローの数が、1 つの間隔における最大数を超えたことを示します。この時点で、アプライアンスは攻撃を軽減するために、次の間隔まで統計情報の収集を停止します。
- [More Options] > [Enable Rule] : ルールがデバイスでアクティブになっているかどうかを示します。無効になっているルールは、ルール テーブルに取り消し線付きのテキストで表示されます。ルールを無効にすると、ルールを削除することなく、ルールのトラフィックへの適用を停止できます。このため、そのルールが必要だと判断した場合は、後で再度有効にすることができます。
- [More Options] > [Time Range] : ルールがアクティブになっている必要がある時間帯と曜日を定義する時間範囲オブジェクトの名前。時間範囲を指定しない場合、ルールは常にアクティブです。

拡張 ACE のサービスの仕様

拡張 ACE の宛先サービスには、次の条件を指定できます。送信元サービスの場合は、オプションは似ていますが、より限定されており、TCP、UDP、または TCP-UDP 条件しか指定できません。

- オブジェクト名：任意のタイプのサービス オブジェクトまたはサービス オブジェクト グループの名前。これらのオブジェクトには、以下で説明するさまざまな仕様を含めることができます。このため、ACL 間でサービス定義を再利用することが簡単にできます。定義済みオブジェクトが多数用意されているため、手動で仕様を入力したり、独自のオブジェクトを作成したりすることなく、必要なオブジェクトが見つかる場合があります。
- プロトコル：1 ～ 255 の範囲の数値または**ip**、**tcp**、**udp**、**gre** などの既知の名前。番号、名前、およびその意味の一覧については、「プロトコルとアプリケーション」（P.43-11）を参照してください。
- TCP、UDP、TCP-UDP ポート：**tcp**、**udp**、および **tcp-udp** キーワードにポートを指定することができます。tcp-udp キーワードを使用すると、tcp と udp を個別に指定せずに両方のプロトコルのポートを定義できます。ポートは次の方法で指定できます。
  - 単一ポート：tcp/80、udp/80、tcp-udp/80、または tcp/www や udp/snmp などの既知のサービス名。ポートおよびキーワードの一覧については、「TCP ポートと UDP ポート」（P.43-12）を参照してください。
  - ポート範囲：tcp/1-100、udp/1-100、tcp-udp/1-100 は、ポート 1 ～ 1000（1 と 1000 を含む）に一致します。
  - ポートに等しくない：仕様の先頭に != を追加します。たとえば、TCP ポート 80（HTTP）以外の任意の TCP トラフィックに一致させるには、!=tcp/80 と指定します。
  - ポート番号より小さい：< を追加します。たとえば、150 未満の任意のポートの TCP トラフィックに一致させるには、<tcp/150 と指定します。
  - ポート番号より大きい：> を追加します。たとえば、150 超の任意のポートの TCP トラフィックに一致させるには、>tcp/150 と指定します。

  （注） DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk は、それぞれに TCP の定義と UDP の定義の両方が必要です。TACACS+ では、ポート 49 に対して 1 つの TCP 定義が必要です。

- ICMP、ICMP6 メッセージ：特定のメッセージ（ping エコー要求や応答メッセージなど）やメッセージ コードをターゲットにできます。ICMP（IPv4 向け）および ICMP6（IPv6 向け）をカバーする定義済みオブジェクトが多数用意されているため、手動での条件定義が不要になる場合があります。形式は次のようになります。

  icmp/*icmp_message_type*[/*icmp_message_code*]

  icmp6/*icmp6_message_type*[/*icmp6_message_code*]

  メッセージ タイプは 1 ～ 255 の範囲の数値または既知の名前で、コードは 0 ～ 255 の範囲の数値です。選択した数値が実際のタイプ/コードに一致することを確認します。そうしないと、ACE が一致しません。ICMP タイプの一覧については、「ICMP タイプ」（P.43-15）を参照してください。

標準 ACL の設定

標準 ACL は ACE の名前付きコンテナとして表されます。新しい ACL を作成するには、まずコンテナを作成する必要があります。その後、標準 ACL テーブルを使用して ACE を追加したり、既存の ACE を編集したり、ACE を並べ替えたりできます。このテーブルは、ACL を設定するときと ACL を使用するポリシーを設定するときに ACL Manager でタブとして表示されます。どちらの場合も、ウィンドウへの行き方を除いて手順は同じです。

標準 ACL では、IPv4 アドレスのみを使用して、宛先アドレスのみを定義します。

手順

ステップ 1　[Configuration] > [Firewall] > [Advanced] > [Standard ACL] を選択します。

ステップ 2　新しい ACL を作成する場合は、[Add] > [Add ACL] を選択し、名前を入力して [**OK**] をクリックします。

ACL コンテナがテーブルに追加されます。標準 ACL の名前は変更できません。

ステップ 3　次のいずれかを実行します。

- ACL の末尾に ACE を追加するには、ACL 名または ACL 内の任意の ACE を選択し、[Add] > [Add ACE] を選択します。
- ACE を特定の場所に挿入するには、既存の ACE を選択し、[Add] > [Insert] を選択してそのルールの上に ACE を追加するか、[Add] > [Insert After] を選択します。
- ルールを編集するには、ルールを選択して [Edit] をクリックします。

ステップ 4　ACE のプロパティを入力します。次のオプションがあります。

- [Action: Permit/Deny]：指定したトラフィックを許可（選択）するか、拒否（選択解除、不一致）するかを選択します。
- [Address]：トラフィック フローの宛先またはターゲット アドレスを定義します。10.100.1.1 などのホスト アドレスか、ネットワーク（10.100.1.0/24 または 10.100.1.0/255.255.255.0 形式）を指定できます。または、ネットワーク オブジェクトを選択することもできます（単にオブジェクトの内容が [Address] フィールドにロードされます）。
- [Description]：ACE の目的に関する説明を 1 行あたり 100 文字以下で入力します。複数行を入力できます。各行は CLI の注釈として追加され、注釈は ACE の前に配置されます。

（注）　1 つのプラットフォーム（Windows など）上で英語以外の文字でコメントを追加し、それらの文字を別のプラットフォーム（Linux など）から削除しようとした場合、元の文字が正しく認識されないため編集や削除を実行できない可能性があります。この制限は、各種言語の文字をさまざまな方法でエンコードするプラットフォームの依存性によるものです。

ACE の定義が完了したら、[OK] をクリックしてテーブルにルールを追加します。

ステップ 5　[Apply] をクリックします。

Webtype ACL の設定

Webtype ACL は、クライアントレス SSL VPN トラフィックのフィルタリング、特定のネットワーク、サブネット、ホスト、および Web サーバへのユーザ アクセスの制限に使用されます。フィルタを定義しない場合は、すべての接続が許可されます。Webtype ACL は ACE の名前付きコンテナとして表されます。新しい ACL を作成するには、まずコンテナを作成する必要があります。その後、Web ACL テーブルを使用して ACE を追加したり、既存の ACE を編集したり、ACE を並べ替えたりできます。このテーブルは、ACL を設定するときと ACL を使用するポリシーを設定するときに ACL Manager でタブとして表示されます。どちらの場合も、ウィンドウへの行き方を除いて手順は同じです。

Webtype ACL には、URL 仕様に加えて IPv4 アドレスと IPv6 アドレスの組み合わせを含めることができます。

手順

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Web ACLs] の順に選択します。

ステップ 2　新しい ACL を作成する場合は、[Add] > [Add ACL] を選択し、名前を入力して [OK] をクリックします。

ACL コンテナがテーブルに追加されます。後でこのコンテナを選択して [Edit] をクリックすることにより、コンテナの名前を変更できます。

ステップ 3　次のいずれかを実行します。

- ACL の末尾に ACE を追加するには、ACL 名または ACL 内の任意の ACE を選択し、[Add] > [Add ACE] を選択します。
- ACE を特定の場所に挿入するには、既存の ACE を選択し、[Add] > [Insert] を選択してそのルールの上に ACE を追加するか、[Add] > [Insert After] を選択します。
- ルールを編集するには、ルールを選択して [Edit] をクリックします。

ステップ 4　ACE のプロパティを入力します。選択する主なオプションは次のとおりです。

- [Action: Permit/Deny]：指定したトラフィックを許可（選択）するか、拒否（選択解除、不一致）するかを選択します。
- [Filter]：宛先に基づくトラフィック一致条件。プロトコルを選択してサーバ名（オプションでパスとファイル名）を入力することによって URL を指定するか、IPv4 または IPv6 アドレスと TCP サービスを指定することができます。

使用可能なすべてのオプションについては、「Webtype ACE のプロパティ」（P.18-12）を参照してください。

ACE の定義が完了したら、[OK] をクリックしてテーブルにルールを追加します。

ステップ 5　[Apply] をクリックします。

Webtype ACE のプロパティ

Webtype ACL の ACE を追加または編集するときに、次のプロパティを設定できます。多くのフィールドでは、編集ボックスの右にある「...」ボタンをクリックして、フィールドで使用できるオブジェクトを選択、作成、または編集できます。

特定の ACE について、URL またはアドレスでフィルタリングすることができます。ただし、両方でフィルタすることはできません。

- [Action: Permit/Deny]：指定したトラフィックを許可（選択）するか、拒否（選択解除、不一致）するかを選択します。
- [Filter on URL]：宛先 URL に基づくトラフィック一致条件。プロトコルを選択してサーバ名（オプションでパスとファイル名）を入力します。たとえば、http://www.example.com と指定します。または、すべてのサーバを対象にするには、http://*.example.com と指定します。以下では、URL の指定に関するヒントと制限事項をいくつか示します。
  - すべての URL に一致させるには、**any** を選択します。
  - 「Permit url any」と指定すると、「プロトコル://サーバ IP/パス」の形式の URL はすべて許可され、このパターンに一致しないトラフィック（ポート転送など）はブロックされます。暗黙の拒否が発生しないように、必要なポート（Citrix の場合はポート 1494）への接続を許可する ACE が必要です。

- スマート トンネルと ica プラグインは、smart-tunnel:// および ica:// タイプにしか一致しないため、「permit url any」を含む ACL の影響を受けません。
- 使用可能なプロトコルは、cifs://、citrix://、citrixs://、ftp://、http://、https://、imap4://、nfs://、pop3://、smart-tunnel://、および smtp:// です。プロトコルでワイルドカードも使用できます。たとえば、「htt*」は http と https に一致し、アスタリスク「*」はすべてのプロトコル一致します。たとえば、「*://*.example.com」は example.com ネットワークへのあらゆるタイプの URL ベースのトラフィックに一致します。
- 「smart-tunnel:// URL」と指定する場合、「URL」にはサーバ名のみを含めることができます。パスを含めることはできません。たとえば、「smart-tunnel://www.example.com」は使用できますが、「smart-tunnel://www.example.com/index.html」は使用できません。
- アスタリスク（*）：空の文字列を含む任意の文字列に一致します。すべての http URL に一致させるには、「http://*/*」と入力します。
- 疑問符（?）は 任意の 1 文字と完全に一致します。
- 角カッコ（[]）：文字の範囲を指定する際に使用する演算子です。角カッコ内に指定された範囲に属する任意の 1 文字に一致します。たとえば、http://www.cisco.com:80/ と http://www.cisco.com:81/ の両方に一致させるには、「http://www.cisco.com:8[01]/」と入力します。

- [Filter on Address and Service]：宛先アドレスとサービスに基づいてトラフィックを照合します。
  - [Address]：宛先の IPv4 または IPv6 アドレスです。すべてのアドレスに一致させるには、すべての IPv4 または IPv6 アドレスに一致する **any** を使用します。IPv4 のみに一致させるには **any4** を、IPv6 のみに一致させるには **any6** を使用します。単一のホスト アドレス（10.100.10.5 または 2001:DB8::0DB8:800:200C:417A など）、サブネット（10.100.10.0/24 または 10.100.10.0/255.255.255.0 形式、または IPv6 の場合は 2001:DB8:0:CD30::/60）を指定できます。または、ネットワーク オブジェクトを選択して、オブジェクトの内容をフィールドにロードすることもできます。
  - [Service]：単一の TCP サービス仕様。デフォルトはポートなしの **tcp** ですが、単一のポート（tcp/80 や tcp/www など）またはポート範囲（tcp/1-100 など）を指定できます。演算子を含めることができます。たとえば、!=tcp/80 は 80 以外のポート、<tcp/80 は 80 未満のすべてのポート、>tcp/80 は 80 超のすべてのポートです。
- [Enable Logging]、[Logging Level]、[More Options] > [Logging Interval]：ロギング オプションでは、実際にトラフィックを拒否するルールについて syslog メッセージをどのように生成するかを定義します。次のロギング オプションを実装できます。
  - [Deselect Enable Logging]：ルールのロギングを無効にします。このルールで拒否されるトラフィックについては、どのタイプの syslog も発行されません。
  - [Select Enable Logging with Logging Level = Default]：ルールのデフォルト ロギングを提供します。拒否されたパケットごとに syslog メッセージ 106103 が発行されます。アプライアンスが攻撃を受けている場合、このメッセージの発行頻度はサービスに影響を及ぼす可能性があります。
  - [Select Enable Logging with Non-Default Logging Level] : 106103 の代わりに、集約された syslog メッセージ 106102 を提供します。メッセージ 106102 は、まず最初にヒットしたときに発行されます。その後、[More Options] > [Logging Interval] で設定した間隔ごとに再発行され、その間隔内のヒット数を示します。推奨されるロギング レベルは [Informational] です。
- [More Options] > [Time Range]：ルールがアクティブになっている必要がある時間帯と曜日を定義する時間範囲オブジェクトの名前。時間範囲を指定しない場合、ルールは常にアクティブです。

Webtype ACL の例

以下では、Webtype ACL の URL ベースのルールの例をいくつか示します。

アクション	フィルタ	影響
拒否	url http://*.yahoo.com/	Yahoo! すべてへのアクセスを拒否します。
拒否	url cifs://fileserver/share/directory	指定された場所にあるすべてのファイルへのアクセスを拒否します。
拒否	url https://www.example.com/ directory/file.html	指定されたファイルへのアクセスを拒否します。
Permit	url https://www.example.com/directory	指定された場所へのアクセスを許可します。
拒否	url http://*:8080/	ポート 8080 を介した任意の場所への HTTPS アクセスを拒否します。
拒否	url http://10.10.10.10	10.10.10.10 への HTTP アクセスを拒否します。
Permit	url any	任意の URL へのアクセスを許可します。通常は、url アクセスを拒否する ACL のあとに使用されます。

ACL のモニタリング

ACL Manager、標準 ACL、Web ACL、および EtherType ACL テーブルには、ACL がまとめて表示されます。ただし、デバイスに設定されている内容を正確に表示するには、次のコマンドを使用します。コマンドを入力するには、[Tools] > [Command Line Interface] を選択します。

コマンド	目的
show access-list [*name*]	各 ACE の行番号とヒット カウントを含むアクセス リストを表示します。ACL 名を指定してください。そうしないと、すべてのアクセス リストが表示されます。
show running-config access-list [*name*]	現在実行しているアクセス リスト コンフィギュレーションを表示します。ACL 名を指定してください。そうしないと、すべてのアクセス リストが表示されます。

ACL の履歴

機能名	リリース	説明
標準、拡張、Webtype ACL	7.0(1)	ACL は、ネットワーク アクセスを制御したり、さまざまな機能を適用するトラフィックを指定したりするために使用されます。拡張アクセス コントロール リストは、through-the-box アクセス コントロールとその他のいくつかの機能に使用されます。標準 ACL は、ルート マップと VPN フィルタで使用されます。Webtype ACL は、クライアントレス SSL VPN フィルタリングで使用されます。EtherType ACL は、IP 以外のレイヤ 2 トラフィックを制御します。 ACL を設定するための ACL Manager およびその他のページが追加されました。
拡張 ACL での実際の IP アドレス	8.3(1)	NAT または PAT を使用するときは、さまざまな機能で、ACL でのマッピング アドレスおよびポートの使用が不要になります。これらの機能については、変換されていない実際のアドレスとポートを使用する必要があります。実際のアドレスとポートが使用されるので、NAT コンフィギュレーションが変更されても ACL を変更する必要はなくなります。詳細については、「NAT 使用時に拡張 ACL で使用する IP アドレス」（P.18-5）を参照してください。
拡張 ACL でのアイデンティティ ファイアウォールのサポート	8.4(2)	アイデンティティ ファイアウォールのユーザおよびグループを発信元と宛先に使用できるようになりました。アイデンティティ ファイアウォール ACL はアクセス ルールや AAA ルールとともに、および VPN 認証に使用できます。
EtherType ACL が IS-IS トラフィックをサポート	8.4(5)、9.1(2)	トランスペアレント ファイアウォール モードで、ASA が EtherType ACL を使用して IS-IS トラフィックを制御できるようになりました。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [EtherType Rules]。
拡張 ACL での Cisco TrustSec のサポート	9.0(1)	Cisco TrustSec セキュリティ グループを送信元と宛先に使用できるようになりました。アイデンティティ ファイアウォール ACL をアクセス ルールとともに使用できます。

機能名	リリース	説明
拡張 ACL と Webtype ACL での IPv4 アドレスと IPv6 アドレスの統合	9.0(1)	拡張 ACL と Webtype ACL で IPv4 アドレスと IPv6 アドレスがサポートされるようになりました。送信元および宛先に対して IPv4 および IPv6 アドレスの組み合わせも指定できます。**any** キーワードは、IPv4 および IPv6 トラフィックを表すように変更されました。IPv4 のみのトラフィックを表す **any4** キーワードと、IPv6 のみのトラフィックを表す **any6** キーワードが追加されました。IPv6 固有の ACL は非推奨です。既存の IPv6 ACL は拡張 ACL に移行されます。移行の詳細については、リリース ノートを参照してください。 次の画面が変更されました。 [Configuration] > [Firewall] > [Access Rules] [Configuration] > [Remote Access VPN] > [Network（Client）Access] > [Group Policies] > [General] > [More Options]
ICMP コードによって ICMP トラフィックをフィルタリングするための拡張 ACL とオブジェクト機能拡張	9.0(1)	ICMP コードに基づいて ICMP トラフィックの許可または拒否ができるようになりました。 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [Objects] > [Service Objects/Groups] [Configuration] > [Firewall] > [Access Rule]

PART 6

IP ルーティング

ルーティングの概要

この章では、Cisco ASA 内でのルーティング動作の基本概念と、サポートされているルーティング プロトコルについて説明します。

ルーティングについて

ルーティングは、発信元から宛先にインターネットワーク経由で情報を移動する行為のことです。その間に、通常は少なくとも 1 つの中間ノードがあります。ルーティングには、最適なルーティング パスの決定と、インターネットワーク経由での情報グループ（通常はパケットと呼ばれる）の転送という 2 つの基本的なアクティビティが含まれます。ルーティング プロセスのコンテキストでは、後者のアクティビティがパケット スイッチングと呼ばれます。パケット スイッチングは比較的単純ですが、パスの決定は非常に複雑になることがあります。

スイッチング

スイッチング アルゴリズムは比較的単純で、ほとんどのルーティング プロトコルで同じです。ほとんどの場合は、別のホストにパケットを送信しなければならないことをホストが決定します。何らかの方法でルータのアドレスを取得すると、送信元ホストは、ルータの物理（メディア アクセス コントロール（MAC）層）アドレスだけに向けてパケットを送信します。このときは、宛先ホストのプロトコル（ネットワーク層）アドレスも送信されます。

パケットの宛先プロトコル アドレスを確認するときに、ルータは、自身がネクスト ホップへのパケットの転送方法を認識しているかどうかを判断します。ルータがパケットの転送方法を認識していない場合は、通常はパケットをドロップします。ルータがパケットの転送方法を認識している場合は、宛先の物理アドレスをネクスト ホップのアドレスに変更し、パケットを送信します。

ネクスト ホップが最終的な宛先ホストであることもあります。最終的な宛先ホストでない場合、ネクスト ホップは通常は別のルータであり、このルータが、同じスイッチング決定プロセスを実行します。パケットがインターネットワークを移動すると、その物理アドレスは変化しますが、プロトコル アドレスは一定のままです。

パス判別

ルーティング プロトコルでは、メトリックを使用して、パケットの移動に最適なパスを評価します。メトリックは、宛先への最適なパスを決定するためにルーティング アルゴリズムが使用する、パスの帯域幅などの測定基準です。パスの決定プロセスを支援するために、ルーティング アルゴリズムは、ルート情報が格納されるルーティング テーブルを初期化して保持します。ルート情報は、使用するルーティング アルゴリズムによって異なります。

ルーティング アルゴリズムにより、さまざまな情報がルーティング テーブルに入力されます。宛先またはネクスト ホップの関連付けにより、最終的な宛先に達するまで、「ネクスト ホップ」を表す特定のルータにパケットを送信することによって特定の宛先に最適に到達できることがルータに示されます。ルータは、着信パケットを受信すると宛先アドレスを確認し、このアドレスとネクスト ホップとを関連付けようとします。

ルーティング テーブルには、パスの妥当性に関するデータなど、他の情報を格納することもできます。ルータは、メトリックを比較して最適なルートを決定します。これらのメトリックは、使用しているルーティング アルゴリズムの設計によって異なります。

ルータは互いに通信し、さまざまなメッセージの送信によりそのルーティング テーブルを保持しています。ルーティング アップデート メッセージはそのようなメッセージの 1 つで、通常はルーティング テーブル全体か、その一部で構成されています。ルーティング アップデートを他のすべてのルータから分析することで、ルータはネットワーク トポロジの詳細な全体像を構築できます。ルータ間で送信されるメッセージのもう 1 つの例であるリンクステート アドバタイズメントは、他のルータに送信元のリンクのステートを通知します。リンク情報も、ネットワークの宛先に対する最適なルートをルータが決定できるように、ネットワーク トポロジの全体像の構築に使用できます。

（注）　非対称ルーティングがサポートされるのは、マルチ コンテキスト モードでのアクティブ/アクティブ フェールオーバーに対してのみです。

サポートされるルート タイプ

ルータが使用できるルート タイプには、さまざまなものがあります。ASA では、次のルート タイプが使用されます。

- 「スタティックとダイナミックの比較」（P.19-3）
- 「シングルパスとマルチパスの比較」（P.19-3）
- 「フラットと階層型の比較」（P.19-3）
- 「リンクステートと距離ベクトル型の比較」（P.19-4）

スタティックとダイナミックの比較

スタティック ルーティング アルゴリズムは実際にはアルゴリズムではなく、ルーティングの開始前にネットワーク管理者によって確立されるテーブル マッピングです。このようなマッピングは、ネットワーク管理者が変更するまでは変化しません。スタティック ルートを使用するアルゴリズムは設計が容易であり、ネットワーク トラフィックが比較的予想可能で、ネットワーク設計が比較的単純な環境で正しく動作します。

スタティック ルーティング システムはネットワークの変更に対応できないため、一般に、変化を続ける大規模なネットワークには不向きであると考えられています。主なルーティング アルゴリズムのほとんどはダイナミック ルーティング アルゴリズムであり、受信したルーティング アップデート メッセージを分析することで、変化するネットワーク環境に適合します。メッセージがネットワークが変化したことを示している場合は、ルーティング ソフトウェアはルートを再計算し、新しいルーティング アップデート メッセージを送信します。これらのメッセージはネットワーク全体に送信されるため、ルータはそのアルゴリズムを再度実行し、それに従ってルーティング テーブルを変更します。

ダイナミック ルーティング アルゴリズムは、必要に応じてスタティック ルートで補足できます。たとえば、ラスト リゾート ルータ（ルーティングできないすべてのパケットが送信されるルータ）を、ルーティングできないすべてのパケットのリポジトリとして機能するように指定し、すべてのメッセージを少なくとも何らかの方法で確実に処理することができます。

シングルパスとマルチパスの比較

一部の高度なルーティング プロトコルは、同じ宛先に対する複数のパスをサポートしています。シングルパス アルゴリズムとは異なり、これらのマルチパス アルゴリズムでは、複数の回線でトラフィックを多重化できます。マルチパス アルゴリズムの利点は、スループットと信頼性が大きく向上することであり、これは一般に「ロード シェアリング」と呼ばれています。

フラットと階層型の比較

ルーティング アルゴリズムには、フラットなスペースで動作するものと、ルーティング階層を使用するものがあります。フラット ルーティング システムでは、ルータは他のすべてのルータのピアになります。階層型ルーティング システムでは、一部のルータが実質的なルーティング バックボーンを形成します。バックボーン以外のルータからのパケットはバックボーン ルータに移動し、宛先の一般エリアに達するまでバックボーンを通じて送信されます。この時点で、パケットは、最後のバックボーン ルータから、1 つ以上のバックボーン以外のルータを通じて最終的な宛先に移動します。

多くの場合、ルーティング システムは、ドメイン、自律システム、またはエリアと呼ばれるノードの論理グループを指定します。階層型のシステムでは、ドメイン内の一部のルータは他のドメインのルータと通信できますが、他のルータはそのドメイン内のルータ以外とは通信できません。非常に大規模なネットワークでは、他の階層レベルが存在することがあり、最も高い階層レベルのルータがルーティング バックボーンを形成します。

階層型ルーティングの第一の利点は、ほとんどの企業の組織に類似しているため、そのトラフィック パターンもサポートするという点です。ほとんどのネットワーク通信は、小さい企業グループ（ドメイン）内で発生します。ドメイン内ルータは、そのドメイン内の他のルータだけを認識していれば済むため、そのルーティング アルゴリズムを簡素化できます。また、使用しているルーティング アルゴリズムに応じて、ルーティング アップデート トラフィックを減少させることができます。

リンクステートと距離ベクトル型の比較

リンクステート アルゴリズム（最短パス優先アルゴリズムとも呼ばれる）は、インターネットワークのすべてのノードにルーティング情報をフラッドします。ただし、各ルータは、それ自体のリンクのステートを記述するルーティング テーブルの一部だけを送信します。リンクステート アルゴリズムでは、各ルータはネットワークの全体像をそのルーティング テーブルに構築します。距離ベクトル型アルゴリズム（Bellman-Ford アルゴリズムとも呼ばれる）では、各ルータが、そのネイバーだけに対してそのルーティング テーブル全体または一部を送信するように要求されます。つまり、リンクステート アルゴリズムは小規模なアップデートを全体に送信しますが、距離ベクトル型アルゴリズムは、大規模なアップデートをネイバー ルータだけに送信します。距離ベクトル型アルゴリズムは、そのネイバーだけを認識します。通常、リンク ステート アルゴリズムは OSPF ルーティング プロトコルとともに使用されます。

ASA 内でのルーティングの仕組み

ASA は、ルーティング テーブルと XLATE テーブルの両方をルーティングの決定に使用します。宛先 IP 変換トラフィック、つまり、変換されていないトラフィックを処理するために、ASA は既存の XLATE またはスタティック変換を検索して出力インターフェイスを選択します。

- 「出力インターフェイスの選択プロセス」（P.19-4）
- 「ネクスト ホップの選択プロセス」（P.19-4）

出力インターフェイスの選択プロセス

選択プロセスは次のとおりです。

1. 宛先 IP を変換する XLATE がすでに存在する場合は、パケットの出力インターフェイスは、ルーティング テーブルではなく XLATE テーブルから決定されます。
2. 宛先 IP を変換する XLATE が存在せず、一致するスタティック変換が存在する場合は、出力インターフェイスはスタティック NAT ルールから決定されて XLATE が作成され、ルーティング テーブルは使用されません。
3. 宛先 IP を変換する XLATE が存在せず、一致するスタティック変換も存在しない場合は、パケットの宛先 IP 変換は実行されません。ASA は、ルートをルックアップして出力インターフェイスを選択することでこのパケットを処理し、次に発信元 IP 変換が（必要に応じて）実行されます。

   通常のダイナミック発信 NAT では、最初の発信パケットは、ルート テーブルを使用し、XLATE を作成することでルーティングされます。着信返送パケットは、既存の XLATE だけを使用して転送されます。スタティック NAT では、宛先変換された着信パケットは、常に既存の XLATE またはスタティック変換ルールを使用して転送されます。

ネクスト ホップの選択プロセス

前述のいずれかの方法を使用して出力インターフェイスを選択した後、さらにルート ルックアップが実行され、これまでに選択した出力インターフェイスに属する適切なネクスト ホップが検出されます。選択されたインターフェイスに明示的に属するルートがルーティング テーブルにない場合は、パケットがドロップされてレベル 6 の syslog メッセージ 110001（ホストへのルートなし）が生成されます（別の出力インターフェイスに属する、指定の宛先ネットワークへの別のルートがあるかどうかにかかわらず）。選択した出力インターフェイスに属するルートが見つかると、パケットは対応するネクスト ホップに転送されます。

ASA でのロード シェアリングは、1 つの出力インターフェイスを使用して複数のネクスト ホップが使用できる場合に限り可能です。ロード シェアリングでは、複数の出力インターフェイスの共有はできません。

ダイナミック ルーティングが ASA で使用されており、XLATE の作成後にルート テーブルが変更された場合も（ルート フラップなど）、宛先変換トラフィックは、XLATE がタイムアウトするまでは、ルート テーブルではなく古い XLATE を使用して転送されます。トラフィックが、正しくないインターフェイスに転送されたり、ドロップされてレベル 6 の syslog メッセージ 110001（ホストへのルートなし）が生成されたりすることもあります（ルーティング プロセスによって古いルートが古いインターフェイスから削除されて別のインターフェイスに接続された場合）。

ASA 自体でルート フラップが発生していないにもかかわらず、その周りで一部のルーティング プロセスがフラッピングし、発信元変換された、同じフローに属するパケットを、別のインターフェイスを使用して ASA 経由で送信する場合は、同様の問題が発生することがあります。宛先変換された返送パケットは、間違った出力インターフェイスを使用して戻されることがあります。

セキュリティ トラフィック構成によっては、この問題が高い確率で発生します。具体的には、ほぼすべてのトラフィックが、フローの最初のパケットの方向に応じて、発信元変換されるか宛先変換されるような構成です。ルート フラップの後にこの問題が発生した場合は、**clear xlate** コマンドを使用して手動で解決することも、XLATE のタイムアウトによって自動的に解決することもできます。XLATE のタイムアウトは、必要に応じて小さくできます。この問題がほとんど発生しないようにするには、ASA やその周りでルート フラップが発生しないようにします。つまり、同じフローに属する宛先変換されたパケットが必ず同じ方法で ASA を通して転送されることを確認します。

ルーティングに対してサポートされているインターネット プロトコル

ASA は、ルーティングに対してさまざまなインターネット プロトコルをサポートしています。この項では、各プロトコルについて簡単に説明します。

- Enhanced Interior Gateway Routing Protocol（EIGRP）

  EIGRP は、IGRP ルータとの互換性とシームレスな相互運用性を提供するシスコ独自のプロトコルです。自動再配布メカニズムにより、IGRP ルートを Enhanced IGRP に、または Enhanced IGRP からインポートできるため、Enhanced IGRP を既存の IGRP ネットワークに徐々に追加できます。

  EIGRP の設定の詳細については、「EIGRP の設定」（P.24-4）を参照してください。

- Open Shortest Path First（OSPF）

  OSPF は、インターネット プロトコル（IP）ネットワーク向けに、インターネット技術特別調査委員会（IETF）の Interior Gateway Protocol（IGP）作業部会によって開発されたルーティング プロトコルです。OSPF は、リンクステート アルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

  OSPF の設定の詳細については、「OSPFv2 の設定」（P.23-6）を参照してください。

- ルーティング情報プロトコル（RIP）

  RIP は、ホップ カウントをメトリックとして使用するディスタンスベクトル プロトコルです。RIP は、グローバルなインターネットでトラフィックのルーティングに広く使用されている Interior Gateway Protocol（IGP）です。つまり、1 つの自律システム内部でルーティングを実行します。

  RIP の設定方法の詳細については、従来の機能ガイドを参照してください。

- Border Gateway Protocol（BGP）

  BGP は自律システム間のルーティング プロトコルです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。カスタマーは ISP に接続し、ISP は BGP を使用してカスタマーおよび ISP ルートを交換します。自律システム（AS）間で BGP を使用する場合、このプロトコルは外部 BGP（EBGP）と呼ばれます。サービス プロバイダーが BGP を使用して AS 内のルートを交換する場合、このプロトコルは内部 BGP（IBGP）と呼ばれます。

  BGP の設定の詳細については、「BGP の設定」（P.22-4）を参照してください。

ルーティング テーブルについて

ルーティング テーブルの表示

手順

ステップ 1　ルーティング テーブル内のすべてのルートを ASDM で表示するには、[Monitoring] > [Routing] > [Routes] の順に選択します。

このペインでは、各行がそれぞれ 1 つのルートを表します。

ルーティング テーブルへの入力方法

ASA のルーティング テーブルには、スタティックに定義されたルート、直接接続されているルート、および RIP、EIGRP、OSPF、BGP の各ルーティング プロトコルで検出されたルートを入力できます。ASA は、ルーティング テーブルに含まれるスタティック ルートと接続されているルートに加えて、複数のルーティング プロトコルを実行できるため、同じルートが複数の方法で検出または入力される可能性があります。同じ宛先への 2 つのルートがルーティング テーブルに追加されると、ルーティング テーブルに残るルートは次のように決定されます。

- 2 つのルートのネットワーク プレフィックス長（ネットワーク マスク）が異なる場合は、どちらのルートも固有と見なされ、ルーティング テーブルに入力されます。入力された後は、パケット転送ロジックが 2 つのうちどちらを使用するかを決定します。

  たとえば、RIP プロセスと OSPF プロセスが次のルートを検出したとします。

  - RIP：192.168.32.0/24
  - OSPF：192.168.32.0/19

  OSPF ルートのアドミニストレーティブ ディスタンスの方が適切であるにもかかわらず、これらのルートのプレフィックス長（サブネット マスク）はそれぞれ異なるため、両方のルートがルーティング テーブルにインストールされます。これらは異なる宛先と見なされ、パケット転送ロジックが使用するルートを決定します。

- ASA が、1 つのルーティング プロトコル（RIP など）から同じ宛先に複数のパスがあることを検知すると、（ルーティング プロトコルが判定した）メトリックがよい方のルートがルーティング テーブルに入力されます。

  メトリックは特定のルートに関連付けられた値で、ルートを最も優先されるものから順にランク付けします。メトリックの判定に使用されるパラメータは、ルーティング プロトコルによって異なります。メトリックが最も小さいパスは最適パスとして選択され、ルーティング テーブルにインストールされます。同じ宛先への複数のパスのメトリックが等しい場合は、これらの等コスト パスに対してロード バランシングが行われます。

- ASA が、ある宛先へのルーティング プロトコルが複数あることを検知すると、ルートのアドミニストレーティブ ディスタンスが比較され、アドミニストレーティブ ディスタンスが最も小さいルートがルーティング テーブルに入力されます。

ルートのアドミニストレーティブ ディスタンス

ルーティング プロトコルによって検出されるルート、またはルーティング プロトコルに再配布されるルートのアドミニストレーティブ ディスタンスは変更できます。2 つの異なるルーティング プロトコルからの 2 つのルートのアドミニストレーティブ ディスタンスが同じ場合、*デフォルト*のアドミニストレーティブ ディスタンスが小さい方のルートがルーティング テーブルに入力されます。EIGRP ルートと OSPF ルートの場合、EIGRP ルートと OSPF ルートのアドミニストレーティブ ディスタンスが同じであれば、デフォルトで EIGRP ルートが選択されます。

アドミニストレーティブ ディスタンスは、2 つの異なるルーティング プロトコルから同じ宛先への異なるルートが複数ある場合に、ASA が最適なパスの選択に使用するルート パラメータです。ルーティング プロトコルには、他のプロトコルとは異なるアルゴリズムに基づくメトリックがあるため、異なるルーティング プロトコルによって生成された、同じ宛先への 2 つのルートについて常に最適パスを判定できるわけではありません。

各ルーティング プロトコルには、アドミニストレーティブ ディスタンス値を使用して優先順位が付けられています。表 19-1 に、ASA がサポートするルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンス値を示します。

表 19-1　サポートされるルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンス

ルートの送信元	デフォルトのアドミニストレーティブ ディスタンス
接続されているインターフェイス	0
スタティック ルート	1
EIGRP サマリー ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
RIP	120
EIGRP 外部ルート	170
内部 BGP	200
不明	255

アドミニストレーティブ ディスタンス値が小さいほど、プロトコルの優先順位が高くなります。たとえば、ASA が OSPF ルーティング プロセス（デフォルトのアドミニストレーティブ ディスタンスが 110）と RIP ルーティング プロセス（デフォルトのアドミニストレーティブ ディスタンスが 120）の両方から特定のネットワークへのルートを受信すると、OSPF ルーティング プロセスの方が優先度が高いため、ASA は OSPF ルートを選択します。この場合、ルータは OSPF バージョンのルートをルーティング テーブルに追加します。

この例では、OSPF 導出ルートの送信元が（電源遮断などで）失われると、ASA は、OSPF 導出ルートが再度現れるまで、RIP 導出ルートを使用します。

アドミニストレーティブ ディスタンスはローカルの設定値です。たとえば、OSPF を通して取得したルートのアドミニストレーティブ ディスタンスを変更するために **distance-ospf** コマンドを使用する場合、その変更は、コマンドが入力された ASA のルーティング テーブルにだけ影響します。アドミニストレーティブ ディスタンスがルーティング アップデートでアドバタイズされることはありません。

アドミニストレーティブ ディスタンスは、ルーティング プロセスに影響を与えません。EIGRP、OSPF、RIP および BGP ルーティング プロセスは、そのルーティング プロセスによって検出されたルートまたはそのルーティング プロセスに再配布されたルートのみをアドバタイズします。たとえば、RIP ルーティング プロセスは、ASA のルーティング テーブルで OSPF ルーティング プロセスによって検出されたルートが使用されていても、RIP ルートをアドバタイズします。

バックアップ ルート

ルートを最初にルーティング テーブルにインストールしようとしたとき、他のルートがインストールされてしまい、インストールできなかった場合に、そのルートはバックアップ ルートとして登録されます。ルーティング テーブルにインストールされたルートに障害が発生すると、ルーティング テーブル メンテナンス プロセスが、登録されたバックアップ ルートを持つ各ルーティング プロトコル プロセスを呼び出し、ルーティング テーブルにルートを再インス

トールするように要求します。障害が発生したルートに対して、登録されたバックアップ ルートを持つプロトコルが複数ある場合、アドミニストレーティブ ディスタンスに基づいて優先順位の高いルートが選択されます。

このプロセスのため、ダイナミック ルーティング プロトコルによって検出されたルートに障害が発生したときにルーティング テーブルにインストールされるフローティング スタティック ルートを作成できます。フローティング スタティック ルートとは、単に、ASA で動作しているダイナミック ルーティング プロトコルよりも大きなアドミニストレーティブ ディスタンスが設定されているスタティック ルートです。ダイナミック ルーティング プロセスで検出された対応するルートに障害が発生すると、このスタティック ルートがルーティング テーブルにインストールされます。

転送の決定方法

転送は次のように決定されます。

- 宛先が、ルーティング テーブル内のエントリと一致しない場合、パケットはデフォルト ルートに指定されているインターフェイスを通して転送されます。デフォルト ルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティング テーブル内の 1 つのエントリと一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。
- 宛先が、ルーティング テーブル内の複数のエントリと一致し、そのエントリのネットワーク プレフィックス長がすべて同じ場合、同一のネットワーク プレフィックスおよび異なるインターフェイスを持つ 2 つのエントリはルーティング テーブル上で共存できません。
- 宛先が、ルーティング テーブル内の複数のエントリと一致し、そのエントリのネットワーク プレフィックス長が異なる場合、パケットはネットワーク プレフィックス長がより長いルートに関連付けられているインターフェイスから転送されます。

たとえば、192.168.32.1 宛てのパケットが、ルーティング テーブルの次のルートを使用して ASA のインターフェイスに到着したとします。

```
ciscoasa# show route
          ....
          R   192.168.32.0/24 [120/4] via 10.1.1.2
          O   192.168.32.0/19 [110/229840] via 10.1.1.3
          ....
```

この場合、192.168.32.1 は 192.168.32.0/24 ネットワークに含まれるため、192.168.32.1 宛てのパケットは 10.1.1.2 宛てに送信されます。このアドレスはまた、ルーティング テーブルの他のルートにも含まれますが、ルーティング テーブル内では 192.168.32.0/24 の方が長いプレフィックスを持ちます（24 ビットと 19 ビット）。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先されます。

ダイナミック ルーティングとフェールオーバー

スタティック ルーティング システムはネットワークの変更に対応できないため、一般に、変化を続ける大規模なネットワークには不向きであると考えられています。主なルーティング アルゴリズムのほとんどはダイナミック ルーティング アルゴリズムであり、受信したルーティング アップデート メッセージを分析することで、変化するネットワーク環境に適合します。メッセージがネットワークが変化したことを示している場合は、ルーティング ソフトウェアは

ルートを再計算し、新しいルーティング アップデート メッセージを送信します。これらのメッセージはネットワーク全体に送信されるため、ルータはそのアルゴリズムを再度実行し、それに従ってルーティング テーブルを変更します。

ダイナミック ルーティング アルゴリズムは、必要に応じてスタティック ルートで補足できます。たとえば、ラスト リゾート ルータ（ルーティングできないすべてのパケットが送信されるルータ）を、ルーティングできないすべてのパケットのリポジトリとして機能するように指定し、すべてのメッセージを少なくとも何らかの方法で確実に処理することができます。

アクティブ装置上でルーティング テーブルの変更がある場合、ダイナミック ルートはスタンバイ装置上で同期化されます。これは、アクティブ装置上のすべての追加、削除、または変更がすぐにスタンバイ装置に伝播されることを意味します。プライマリ装置が一定期間アクティブであった後にスタンバイ装置がアクティブになると、ルートがフェールオーバー バルク同期プロセスの一部として同期化されます。そのためアクティブ/スタンバイ フェールオーバー ペア上では、ルーティング テーブルが同じように表示されます。

スタティック ルートの詳細とその設定方法については、「スタティック ルートの設定」（P.20-2）を参照してください。

ダイナミック ルーティングおよびクラスタリング

ダイナミック ルーティングは、クラスタに完全に統合され、ルートはユニットで共有されます（クラスタでは最大 8 ユニットを使用できます）。ルーティング テーブル エントリは、クラスタのユニットにも複製されます。

1 つのユニットがスレーブからマスターに遷移すると、RIB テーブルのエポック番号（32 ビット シーケンス番号）が増加します。遷移後、新しいマスター ユニットには、まず以前のマスター ユニットのミラー イメージである RIB テーブル エントリが含まれます。さらに、再コンバージェンス タイマーが新しいマスター ユニットで開始されます。RIB テーブルのエポック番号が増加された場合、既存のすべてのエントリは古いと見なされます。IP パケットの転送は通常どおりに継続されます。新しいマスター ユニットで、ダイナミック ルーティング プロトコルが既存のルート エントリの更新または新しいエポック番号を持つ新しいルート エントリの作成を開始します。変更されたエントリまたは現在のエポック番号を持つ新しいエントリは、更新され、すべてのスレーブ ユニットと同期化されていることを示します。再コンバージェンス タイマーの期限が切れると、RIB テーブルの古いエントリが削除されます。OSPF ルート、RIP ルート、EIGRP ルートの RIB テーブル エントリはスレーブ ユニットに同期化されます。

バルク同期は、ユニットがクラスタに参加し、マスター ユニットから参加ユニットへのユニットである場合にのみ行われます。

ダイナミック ルーティング アップデートの場合、マスター ユニットが OSPF、RIP、または EIGRP によって取得した新しいルートを学習すると、マスター ユニットは、信頼できるメッセージ送信を介してすべてのスレーブ ユニットにアップデートを送信します。スレーブ ユニットはクラスタのルート アップデート メッセージを受信した後に RIB テーブルを更新します。

サポートされるダイナミック ルーティング プロトコル（OSPF、RIP、EIGRP）の場合、スレーブ ユニットのレイヤ 2 ロード バランシングのインターフェイスからのルーティング パケットがマスター ユニットに転送されます。マスター ユニットだけがダイナミック ルーティング プロトコル パケットを確認し、処理します。スレーブ ユニットがバルク同期を要求すると、レイヤ 2 ロード バランシングのインターフェイスを介して学習されたすべてのルーティング エントリが複製されます。

新しいルーティング エントリがマスター ユニットのレイヤ 2 ロード バランシングのインターフェイスを介して学習される場合、新しいエントリはすべてのスレーブ ユニットにブロードキャストされます。既存のルーティング エントリがネットワーク トポロジの変更が原因で変更された場合、変更されたエントリもすべてのスレーブ ユニットに同期化されます。既存のルーティング エントリがネットワーク トポロジの変更が原因で削除された場合、削除されたエントリもすべてのスレーブ ユニットに同期化されます。

レイヤ 2 およびレイヤ 3 ロード バランシングのインターフェイスの組み合わせがダイナミック ルーティング用に展開され、設定されている場合は、レイヤ 2 ロード バランシングのインターフェイスのマスター ユニットから RIB テーブルのエントリのみが同期化されるため、スレーブ ユニットは部分的なトポロジおよびルーティング プロセスのネイバー情報（レイヤ 3 ロード バランシングのインターフェイスを介して取得された詳細を含む）のみを持ちます。レイヤ 2 およびレイヤ 3 が異なるルーティング プロセスに属し、各ルーティング プロセスからの負荷を再配布するようにネットワークを設定する必要があります。

表 19-2 に、サポートされている設定の概要を示します。「Yes」は、2 つのプロセスの組み合わせ（レイヤ 2 に対する 1 つのプロセスおよびレイヤ 3 に対する 1 つのプロセス）が機能していることを示し、「No」は、2 つのプロセスの組み合わせが機能していないことを示しています。

表 19-2　　サポートされている設定の概要

レイヤ 2 またはレイヤ 3	OSPF（レイヤ 3）	EIGRP（レイヤ 3）	RIP（レイヤ 3）
OSPF（レイヤ 2）	Yes	Yes	Yes
EIGRP（レイヤ 2）	Yes	No	Yes
RIP（レイヤ 2）	Yes	Yes	No

クラスタ内のすべてのユニットは、同じモード（シングル モードまたはマルチ コンテキスト モード）である必要があります。マルチ コンテキスト モードでは、マスタースレーブ同期は、同期メッセージにすべてのコンテキストおよびすべてのコンテキストの RIB テーブル エントリを含めます。

クラスタリングでは、レイヤ 3 インターフェイスを設定した場合は、router-id プール設定を実行設定する必要があります。

ダイナミック ルーティングおよびクラスタリングの詳細については、第 9 章「ASA クラスタ」を参照してください。

マルチ コンテキスト モードのダイナミック ルーティング

マルチ コンテキスト モードでは、各コンテキストで個別のルーティング テーブルおよびルーティング プロトコル データベースが維持されます。これにより、各コンテキストの OSPFv2 および EIGRP を個別に設定することができます。EIGRP をあるコンテキストで設定し、OSPFv2 を同じまたは異なるコンテキストで設定できます。混合コンテキスト モードでは、ルーテッド モードのコンテキストの任意のダイナミック ルーティング プロトコルをイネーブルにできます。RIP および OSPFv3 は、マルチ コンテキスト モードではサポートされていません。

次の表に、EIGRP、OSPFv2、OSPFv2 および EIGRP プロセスへのルートの配布に使用されるルート マップ、およびマルチ コンテキスト モードで使用されている場合にエリアを出入りするルーティング アップデートをフィルタリングするために OSPFv2 で使用されるプレフィックス リストの属性を示します。

EIGRP	OSPFv2	ルート マップ およびプレフィックス リスト
コンテキストごとに 1 つのインスタンスがサポートされます。	コンテキストごとに 2 つのインスタンスがサポートされます。	該当なし
システム コンテキストでディセーブルになっています。		該当なし

EIGRP （続き）	OSPFv2 （続き）	ルート マップ およびプレフィックス リスト
2 つのコンテキストが同じまたは異なる自律システム番号を使用できます。	2 つのコンテキストが同じまたは異なるエリア ID を使用できます。	該当なし
2 つのコンテキストの共有インターフェイスでは、複数の EIGRP のインスタンスを実行できます。	2 つのコンテキストの共有インターフェイスでは、複数の OSPF のインスタンスを実行できます。	該当なし
共有インターフェイス間の EIGRP インスタンスの相互作用がサポートされます。	共有インターフェイス間の OSPFv2 インスタンスの相互作用がサポートされます。	該当なし
シングル モードで使用可能なすべての CLI はマルチ コンテキスト モードでも使用できます。		
各 CLI は使用されているコンテキストでだけ機能します。		

ルートのリソース管理

routes というリソース クラスが導入されました。このリソース クラスは、コンテキストに存在できるルーティング テーブル エントリの最大数を指定します。これは、別のコンテキストの使用可能なルーティング テーブル エントリに影響を与える 1 つのコンテキストの問題を解決し、コンテキストあたりの最大ルート エントリのより詳細な制御を提供します。

明確なシステム制限がないため、このリソース制限には絶対値のみを指定できます。割合制限は使用できません。また、コンテキストあたりの上限および下限がないため、デフォルト クラスは変更されません。コンテキストのスタティックまたはダイナミック ルーティング プロトコル（接続、スタティック、OSPF、EIGRP、および RIP）のいずれかに新しいルートを追加し、そのコンテキストのリソース制限を超えた場合、ルートの追加は失敗し、syslog メッセージが生成されます。

プロキシ ARP 要求のディセーブル化

あるホストから同じイーサネット ネットワーク上の別のデバイスに IP トラフィックを送信する場合、そのホストは送信先のデバイスの MAC アドレスを知る必要があります。ARP は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは IP アドレスの所有者を尋ねる ARP 要求を送信します。その IP アドレスを所有するデバイスは、自分が所有者であることを自分の MAC アドレスで返答します。

プロキシ ARP は、デバイスが ARP 要求に対してその IP アドレスを所有しているかどうかに関係なく自分の MAC アドレスで応答するときに使用されます。NAT を設定し、ASA インターフェイスと同じネットワーク上のマッピング アドレスを指定する場合、ASA でプロキシ ARP が使用されます。トラフィックがホストに到達できるようにする唯一の方法は、MAC アドレスが宛先のマッピング アドレスに割り当てられていると ASA がプロキシ ARP を使用して主張できるように設定することです。

まれに、NAT アドレスに対してプロキシ ARP をディセーブルにすることが必要になります。

既存のネットワークと重なる VPN クライアント アドレス プールがある場合、ASA は、デフォルトにより、すべてのインターフェイス上でプロキシ ARP 要求を送信します。同じレイヤ 2 ドメイン上にもう 1 つインターフェイスがあると、そのインターフェイスは ARP 要求を検出し、自分の MAC アドレスで応答します。その結果、内部ホストへの VPN クライアントのリターン トラフィックは、その誤ったインターフェイスに送信され、ドロップされます。この場合、プロキシ ARP 要求をそれらが不要なインターフェイスでディセーブルにする必要があります。

手順

ステップ 1　[Configuration] > [Device Setup] > [Routing] > [Proxy ARP/Neighbor Discovery] を選択します。

[Interface] フィールドにインターフェイス名が一覧表示されます。[Enabled] フィールドには、NAT グローバル アドレスに対してプロキシ ARP/ネイバー探索がイネーブルか（[Yes]）ディセーブルか（[No]）が表示されます。

ステップ 2　選択したインターフェイスに対してプロキシ ARP/ネイバー探索をイネーブルにするには、[Enable] をクリックします。デフォルトでは、プロキシ ARP/ネイバー探索はすべてのインターフェイスに対してイネーブルです。

ステップ 3　選択したインターフェイスに対してプロキシ ARP/ネイバー探索をディセーブルにするには、[Disable] をクリックします。

ステップ 4　[Apply] をクリックして設定を実行コンフィギュレーションに保存します。

スタティック ルートとデフォルト ルート

この章では、Cisco ASA でスタティック ルートとデフォルト ルートを設定する方法について説明します。

スタティック ルートとデフォルト ルートについて

接続されていないホストまたはネットワークにトラフィックをルーティングするには、そのホストまたはネットワークへのスタティック ルートを定義するか、または少なくとも、ネットワークと ASA の間にルータがある場合など、ASA が直接接続されていない任意のネットワークのデフォルト ルートを定義する必要があります。

スタティック ルートまたはデフォルト ルートが定義されていない場合は、接続されていないホストやネットワークへのトラフィックによって次の syslog メッセージが生成されます。

```
%ASA-6-110001: No route to dest_address from source_address
```

次の場合は、シングル コンテキスト モードでスタティック ルートを使用します。

- ネットワークで EIGRP、RIP または OSPF とは異なるルータ検出プロトコルを使用している。
- ネットワークが小規模でスタティック ルートを容易に管理できる。
- ルーティング プロトコルが関係するトラフィックまたは CPU のオーバーヘッドをなくす必要がある。

最も単純なオプションは、すべてのトラフィックをアップストリーム ルータに送信するようにデフォルト ルートを設定して、トラフィックのルーティングをルータに任せることです。しかし、デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティック ルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部の場合、デフォルト ルートは、ASA に直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。

トランスペアレント ファイアウォール モードでは、ASA から直接接続されていないネットワークに宛てたトラフィック用にデフォルト ルートまたはスタティック ルートを設定して、ASA がトラフィックの送信先インターフェイスを認識できるようにする必要があります。ASA から発信されるトラフィックには、syslog サーバ、Websense サーバまたは N2H2 サーバ、あるいは AAA サーバとの通信もあります。1 つのデフォルト ルートで到達できないサーバがある場合、スタティック ルートを設定する必要があります。さらに、ASA では、ロード バランシングのために、1 つのインターフェイスあたり最大で 3 つの等コスト ルートをサポートします。

スタティック ルートおよびデフォルト ルートのガイドライン

フェールオーバーのガイドライン

ダイナミック ルーティング プロトコルのステートフル フェールオーバーをサポートします。

その他のガイドライン

- IPv6 スタティック ルートは、ASDM においてトランスペアレント モードでサポートされていません。
- クラスタリングでは、スタティック ルート モニタリングは、マスター ユニットでのみサポートされます。クラスタリングの詳細については、第 9 章「ASA クラスタ」を参照してください。

スタティック ルートの設定

スタティック ルーティング アルゴリズムは、基本的にはルーティングの開始前にネットワーク管理者によって確立されるテーブル マッピングのことです。このようなマッピングは、ネットワーク管理者が変更するまでは変化しません。スタティック ルートを使用するアルゴリズムは設計が容易であり、ネットワーク トラフィックが比較的予想可能で、ネットワーク設計が比較的単純な環境で正しく動作します。したがって、スタティック ルーティング システムはネットワークの変更に対応できません。

スタティック ルートは、指定されたゲートウェイが利用できなくなってもルーティング テーブルに保持されています。指定されたゲートウェイが利用できなくなった場合は、スタティック ルートをルーティング テーブルから手動で削除する必要があります。ただし、スタティック ルートは、指定されたインターフェイスが停止するとルーティング テーブルから削除され、インターフェイスが復旧すると最適用されます。

（注） ASA で動作中のルーティング プロトコルのアドミニストレーティブ ディスタンスよりも長いアドミニストレーティブ ディスタンスを指定してスタティック ルートを作成すると、ルーティング プロトコルで検出される指定の宛先へのルートがスタティック ルートより優先されます。スタティック ルートは、ダイナミックに検出されたルートがルーティング テーブルから削除された場合に限り使用されます。

インターフェイスごとに同じ宛先でコストの等しいルートを 3 つまで定義できます。複数のインターフェイス間を通る等コスト マルチパス（ECMP）はサポートされていません。ECMP では、トラフィックは必ずしもルート間で均等に分割されるわけではありません。トラフィックは、送信元 IP アドレスおよび宛先 IP アドレスをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

スタティック null0 ルートの設定

通常、トラフィックのフィルタリングには ACL が使用され、ヘッダーに含まれている情報に基づくパケットのフィルタが可能になります。パケット フィルタリングでは、ASA ファイアウォールがパケット ヘッダーを検査してフィルタリングを決定するため、パケット処理のオーバーヘッドが加わり、パフォーマンスに影響します。

スタティック null0 ルーティングは、フィルタリングを補完するソリューションです。スタティック null0 ルートは、不要なトラフィックや望ましくないトラフィックをブラック ホールに転送するために使用されます。ヌル インターフェイスである null0 が、ブラック ホールの作成に使用されます。望ましくない宛先に対するスタティック ルートを作成し、そのスタティック ルートのコンフィギュレーションでヌル インターフェイスを指定します。宛先アドレスに最も一致するルートがブラック ホールのスタティック ルートであるすべてのトラフィックが自動的にドロップされます。ACL の場合とは異なり、スタティック null0 ルートはまったくパフォーマンスを低下させません。

スタティック null0 ルート設定は、ルーティング ループの防止に使用されます。BGP では、Remotely Triggered Black Hole ルーティングのためにスタティック null0 設定を活用します。

次に例を示します。

```
route null0 192.168.2.0 255.255.255.0
```

スタティック ルートを設定するには、次のいずれかを選択します。

- 「スタティック ルートの追加または編集」（P.20-3）
- 「スタティック ルート トラッキングの設定」（P.20-6）
- 「スタティック ルートの削除」（P.20-6）

スタティック ルートの追加または編集

手順

ステップ 1　メイン ASDM ウィンドウで [Configuration] > [Device Setup] > [Routing] > [Static Routes] を選択します。

ステップ 2　次のいずれかのオプション ボタンをクリックして、フィルタするルートを選択します。

- [Both]（IPv4 と IPv6 の両方をフィルタ）
- **IPv4 のみ**
- **IPv6 のみ**

デフォルトでは、[Both] オプション ボタンが選択され、IPv4 と IPv6 のアドレスがペイン内に表示されます。表示される選択肢を IPv4 アドレスを使用して設定されたルートに制限するには、[IPv4] オプション ボタンをクリックします。表示される選択肢を IPv6 アドレスを使用して設定されたルートに制限するには、[IPv6] オプション ボタンをクリックします。

ステップ 3　[Add] または [Edit] をクリックします。

[Add Static Route] または [Edit Static Route] ダイアログボックスが表示されます。

ステップ 4　[Interface] ドロップダウン リストから、[Interface] フィールドでイネーブルになっている内部または外部のネットワーク インターフェイス名を選択します。

- **management**（内部インターフェイス）
- **outside**（外部インターフェイス）

ステップ 5　[IP Address] フィールドに、宛先ネットワークの内部または外部ネットワーク IP アドレスを入力します。

IPv4 アドレスには、**0.0.0.0** を入力してデフォルト ルートを指定します。0.0.0.0 の IP アドレスは、0 と省略できます。オプションで、省略符号をクリックしアドレスを参照します。

IPv6 アドレスには、2 つのコロン（**::**）を入力してデフォルト ルートを指定します。オプションで、省略符号をクリックしアドレスを参照します。

ステップ 6　[Gateway IP] フィールドに、このルートのネクスト ホップ アドレスであるゲートウェイ ルータの IP アドレスを入力します。

デフォルトのルートを入力するには、IP アドレスとマスクを **0.0.0.0** と設定するか、または短縮形式の **0** と設定します。

オプションで、省略符号をクリックしアドレスを参照します。

（注）　1 つの ASA インターフェイスの IP アドレスがゲートウェイの IP アドレスとして使用される場合、ASA は、ゲートウェイ IP アドレスに ARP を実行するのではなく、パケットの指定 IP アドレスに ARP を実行します。

スタティック ルートに指定するアドレスは、ASA に到達して NAT を実行する前のパケットにあるアドレスです。

ステップ 7　ドロップダウン リストから宛先ネットワークのネットマスクを選択します。フィルタするように選択したルート（IPv4、IPv6、またはその両方）に応じて、次のいずれかの操作を実行します。

- IPv4 スタティック ルート（または、IPv4 と IPv6 両方のスタティック ルート）には、IP アドレスに適用されるネットワーク マスクのアドレスを入力します。デフォルト ルートを指定するには、**0.0.0.0** を入力します。ネットマスク **0.0.0.0** は、**0** に短縮できます。
- IPv6 のスタティック ルートにだけ、プレフィックスの長さを入力します。

ステップ 8　[Metric] フィールドに、メトリックまたはアドミニストレーティブ ディスタンスを入力します。

[Metric/distance] は、ルートのアドミニストレーティブ ディスタンスです。値を指定しない場合、デフォルトは 1 です。アドミニストレーティブ ディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。スタティック ルートのデフォルトのアドミニストレーティブ ディスタンスは 1 で、ダイナミック ルーティング プロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。

OSPF で検出されるルートのデフォルトのアドミニストレーティブ ディスタンスは 110 です。スタティック ルートとダイナミック ルートのアドミニストレーティブ ディスタンスが同じ場合、スタティック ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

ステップ 9　（オプション）[Options] 領域で、1 つのスタティック ルートに対して、次のいずれかのオプションを選択します。

- [None]：スタティック ルートにはオプションが指定されていません。この設定は、デフォルトです。
- [Tunneled]：ルートを VPN トラフィックのデフォルト トンネル ゲートウェイとして指定します。この設定はデフォルト ルートに対してのみ使用されます。1 つのデバイスに設定できるのは 1 つのトンネル ルートだけです。[Tunneled] オプションは、トランスペアレント モードではサポートされません。

- [Tracked]：ルートを追跡することを指定します。トラッキング オブジェクトの ID およびトラッキング対象のアドレスも表示されます。[Tracked] オプションは、シングル ルーテッド モードでだけサポートされます。[Tracked] オプションに対しては次の設定を指定します。
  - [Track ID] フィールドに、ルート トラッキング プロセスの固有識別子を入力します。
  - [Track IP Address/DNS Name] フィールドに、追跡される対象の IP アドレスまたはホスト名を入力します。これは通常、このルートのネクスト ホップ ゲートウェイの IP アドレスになりますが、そのインターフェイスから利用できる任意のネットワーク オブジェクトとすることもできます。
  - [SLA ID] フィールドに、SLA モニタリング プロセスの固有識別子を入力します。

（注） [Tracked] オプションは IPv6 ではサポートされません。

ステップ 10　（オプション）[Monitoring Options] をクリックします。

[Route Monitoring Options] ダイアログボックスが表示されます。ここから、次のトラッキング オブジェクトのモニタリング プロパティを変更します。

- [Frequency]：トラッキング対象の存在を ASA がテストする頻度（秒）を変更できます。有効な値の範囲は 1 ～ 604800 秒です。デフォルト値は 60 秒です。
- [Threshold]：しきい値を超えたイベントを示す時間（ミリ秒）を入力できます。この値に、タイムアウト値より大きい値は指定できません。
- [Timeout]：ルート モニタリング操作が要求パケットからの応答を待つ時間（ミリ秒）を変更できます。有効な値の範囲は 0 ～ 604800000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
- [Data Size]：エコー要求パケットで使用するデータ ペイロードのサイズを変更できます。デフォルト値は 28 です。有効な値の範囲は 0 ～ 16384 です。

（注） この設定では、ペイロードのサイズだけが指定されます。パケット全体のサイズは指定されません。

- [ToS]：エコー要求の IP ヘッダーにあるタイプ オブ サービスのバイト値を入力します。有効な値は、0 ～ 255 です。デフォルト値は 0 です
- [Number of Packets]：各テストに送信されるエコー要求の数を選択できます。有効な値の範囲は 1 ～ 100 です。デフォルト値は 1 です。

ステップ 11　[OK] をクリックします。

ステップ 12　[Apply] をクリックして、設定を保存します。

[Static Routes] ペインに追加または編集したルート情報が表示されます。新しく設定されたルートを保存するとすぐに、モニタリング プロセスが開始されます。

スタティック ルート トラッキングの設定

手順

（注）　スタティック ルート トラッキングは IPv4 のルートでだけ使用できます。

ステップ 1　対象を選択します。対象がエコー要求に応答することを確認してください。

ステップ 2　[Configuration] > [Device Setup] > [Routing] > [Static Routes] を選択して、[Static Routes] ペインを開きます。

ステップ 3　[Add] をクリックし、選択した対象の使用可能状況に基づいて使用されるスタティック ルートを設定します。このルートのインターフェイス、IP アドレス、マスク、ゲートウェイ、およびメトリックの設定を入力する必要があります。

ステップ 4　このルートには、[Options] 領域で [Tracked] オプション ボタンを選択します。

ステップ 5　トラッキング プロパティを設定します。一意のトラック ID、一意の SLA ID、および対象の IP アドレスを入力する必要があります。

ステップ 6　（オプション）モニタリング プロパティを設定するには、[Add Static Route] ダイアログボックスの [Monitoring Options] をクリックします。

ステップ 7　[OK] をクリックして変更を保存します。

追跡するルートを保存するとすぐに、モニタリング プロセスが開始されます。

ステップ 8　手順 1 ～ 7 を繰り返して、セカンダリ ルートを作成します。

セカンダリ ルートは、追跡されたルートと同じ宛先へのスタティック ルートですが、異なるインターフェイスまたはゲートウェイを経由します。このルートは、追跡されたルートより長いアドミニストレーティブ ディスタンス（メトリック）に割り当てる必要があります。

ステップ 9　[OK] をクリックして変更を保存します。

スタティック ルートの削除

手順

ステップ 1　[Configuration] > [Device Setup] > [Routing] > [Static Routes] を選択します。

ステップ 2　[Static Routes] ペインで、削除するルートを選択します。

デフォルトでは、[Both] オプション ボタンが選択され、IPv4 と IPv6 のアドレスがペイン内に表示されます。

- 表示される選択肢を IPv4 アドレスを使用して設定されたルートに制限するには、[IPv4] オプション ボタンをクリックします。
- 表示される選択肢を IPv6 アドレスを使用して設定されたルートに制限するには、[IPv6] オプション ボタンをクリックします。

ステップ 3　[Delete] をクリックします。

メインの [Static Routes] ペインにあるルートのリストから、削除されたルートが除外されます。

ステップ 4　[Apply] をクリックし、変更内容をコンフィギュレーションに保存します。

デフォルト スタティック ルートの設定

デフォルト ルートは、既知のルートもスタティック ルートも指定されていない IP パケットすべてを、ASA が送信するゲートウェイの IP アドレスを特定するルートです。デフォルト スタティック ルートは、宛先の IP アドレスとして 0.0.0.0/0 が指定された単なるスタティック ルートです。特定の宛先が特定されたルートはデフォルト ルートより優先されます。

（注）　バージョン 7.0(1) 以降で、異なるメトリックを持つ個別のインターフェイス上で 2 つのデフォルト ルートが設定されている場合は、それよりも大きいメトリックを持つインターフェイスから ASA への接続は失敗しますが、小さいメトリックを持つインターフェイスからの ASA への接続は予期したとおりに成功します。

デバイスあたり最大 3 つの等コスト デフォルト ルート エントリを定義することができます。複数の等コスト デフォルト ルート エントリを定義すると、デフォルト ルートに送信されるトラフィックは、指定されたゲートウェイの間に分散されます。複数のデフォルト ルートを定義する場合は、各エントリに同じインターフェイスを指定する必要があります。

4 つ以上の等コスト デフォルト ルートを定義しようとすると、またはすでに定義されているデフォルト ルートとは別のインターフェイスでデフォルト ルートを定義しようとすると、次のメッセージが表示されます。

```
"ERROR: Cannot add route entry, possible conflict with existing routes."
```

トンネル トラフィックには、標準のデフォルト ルートの他に別のデフォルト ルートを 1 つ定義することができます。tunneled オプションを使用してデフォルト ルートを作成すると、ASA に着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用してルーティングできない場合、このルートに送信されます。トンネルから出るトラフィックの場合、このルートは、その他の設定または学習されたデフォルト ルートをすべて上書きします。

デフォルト スタティック ルートの設定の制限事項

tunneled オプションが指定されたデフォルト ルートには、次の制限事項が適用されます。

- トンネル ルートの出力インターフェイスで、ユニキャスト RPF（**ip verify reverse-path** コマンド）をイネーブルにしないでください。この設定を行うと、セッションでエラーが発生します。
- トンネル ルートの出力インターフェイスで、TCP 代行受信をイネーブルにしないでください。この設定を行うと、セッションでエラーが発生します。
- VoIP インスペクション エンジン（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS インスペクション エンジン、または DCE RPC インスペクション エンジンは、トンネル ルートでは使用しないでください。この設定を行うと、セッションでエラーが発生します。
- tunneled オプションでは、複数のデフォルト ルートを定義できません。
- トンネル トラフィックの ECMP はサポートされません。

手順

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Static Routes] を選択します。

ステップ 2　[Add] または [Edit] をクリックします。

ステップ 3　[Options] 領域で、[Tunneled] を選択します。

ステップ 4　[OK] をクリックします。

IPv6 デフォルト ルートおよびスタティック ルートの設定

ホストが接続されているインターフェイスが IPv6 に対応し、IPv6 ACL でトラフィックが許可されていれば、ASA は、直接接続されているホスト間で IPv6 トラフィックを自動的にルーティングします。

手順

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Static Routes] を選択します。

ステップ 2　[IPv6 only] オプション ボタンをクリックします。

ステップ 3　[Add] または [Edit] をクリックします。

ステップ 4　[OK] をクリックします。

スタティック ルートまたはデフォルト ルートのモニタ

スタティック ルートの問題の 1 つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。スタティック ルートは、ネクスト ホップ ゲートウェイが使用できなくなった場合でも、ルーティング テーブルに保持されています。スタティック ルートは、ASA 上の関連付けられたインターフェイスがダウンした場合に限りルーティング テーブルから削除されます。

スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリ ルートがダウンした場合のバックアップ ルートをインストールするための方式が用意されています。たとえば、ISP ゲートウェイへのデフォルト ルートを定義し、かつ、プライマリ ISP が使用できなくなった場合に備えて、セカンダリ ISP へのバックアップ デフォルト ルートを定義できます。

ASA では、定義されたモニタリング対象にスタティック ルートを関連付けることでこの機能を実行し、ICMP エコー要求を使用して対象をモニタリングします。指定された時間内にエコー応答がない場合は、そのオブジェクトはダウンしていると見なされ、関連付けられたルートはルーティング テーブルから削除されます。削除されたルートに代わって、すでに定義されているバックアップ ルートが使用されます。

モニタリング対象の選択時には、その対象が ICMP エコー要求に応答できることを確認してください。対象には任意のネットワーク オブジェクトを選択できますが、次のものを使用することを検討する必要があります。

- ISP ゲートウェイ アドレス（デュアル ISP サポート用）
- ネクスト ホップ ゲートウェイ アドレス（ゲートウェイの使用可能状況に懸念がある場合）
- ASA が通信を行う必要のある対象ネットワーク上のサーバ（AAA サーバなど）
- 宛先ネットワーク上の永続的なネットワーク オブジェクト

（注） 夜間にシャットダウンするデスクトップ PC やノートブック PC は適しません。

スタティック ルート トラッキングは、スタティックに定義されたルートや、DHCP または PPPoE を通じて取得したデフォルト ルートに対して設定することができます。設定済みのルート トラッキングでは、複数のインターフェイス上の PPPoE クライアントだけをイネーブルにすることができます。

手順

ステップ 1　[Monitoring] > [Routing] **>** [Routes] を選択します。

[Routes] ペインでは、それぞれの行が 1 つのルートを表しています。IPv4 接続、IPv6 接続、またはその両方でフィルタリングできます。ルーティング情報には、プロトコル、ルート タイプ、宛先 IP アドレス、ネットマスクまたはプレフィックスの長さ、ゲートウェイ IP アドレス、ルートに接続するときに経由するインターフェイス、およびアドミニストレーティブ ディスタンスが含まれています。

ステップ 2　現在のリストを更新するには、[Refresh] をクリックします。

スタティック ルートまたはデフォルト ルートの例

次の例は、スタティック ルートの作成方法を示します。スタティック ルートは、宛先が 10.1.1.0/24 のトラフィックすべてを内部インターフェイスに接続されているルータ（10.1.2.45）に送信します。また、外部インターフェイスで 3 つの異なるゲートウェイにトラフィックを誘導する 3 つの等コスト スタティック ルートを定義し、トンネル トラフィックのデフォルト ルートを追加します。ASA は、指定された複数のゲートウェイ間にトラフィックを分散します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Static Routes] を選択します。

ステップ 2　[Interfaces] ドロップダウン リストから [Management] を選択します。

ステップ 3　[IP Address] フィールドに **10.1.1.0** を入力します。

ステップ 4　[Mask] ドロップダウン リストから [**255.255.255.0**] を選択します。

ステップ 5　[Gateway IP] フィールドに **10.1.2.45 1** を入力します。

宛先が 10.1.1.0/24 のトラフィックがすべて、内部インターフェイスに接続されているルータ 10.1.2.45 に送信されるようにスタティック ルートが作成されます。

ステップ 6　[OK] をクリックします。

ステップ 7　[Configuration] > [Device Setup] > [Routing] > [Static Routes] を選択します。

ステップ 8　[Add] をクリックします。

ステップ 9　宛先ネットワークの [IP Address] フィールドに IP アドレスを入力します。

この場合、ルートの IP アドレスは 192.168.2.1、192.168.2.2、192.168.2.3、および 192.168.2.4 です。192.168.2.4 を追加するときに、[Options] 領域で [Tunneled] オプション ボタンをクリックします。

ステップ 10　ネクスト ホップ ルータのアドレスの [Gateway IP Address] フィールドに、ゲートウェイ IP アドレスを入力します。

スタティック ルートに指定するアドレスは、ASA に到達して NAT を実行する前のパケットにあるアドレスです。

ステップ 11　[NetMask] ドロップダウン リストから、宛先ネットワークのネットマスクを選択します。

ステップ 12　[OK] をクリックします。

スタティック ルートおよびデフォルト ルートの履歴

ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 20-1　スタティック ルートおよびデフォルト ルートの機能履歴

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	7.0(1)	スタティック ルートおよびデフォルト ルートが導入されました。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing]。
クラスタリング	9.0(1)	スタティック ルート モニタリングは、マスター ユニットでのみサポートされます。
スタティック null0 ルートの設定	9.2(1)	トラフィックを Null0 インターフェイスへ送信すると、指定したネットワーク宛のパケットはドロップします。この機能は、BGP の Remotely Triggered Black Hole (RTBH) の設定に役立ちます。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add] > [Add Static Route]

ルート マップ

ルート マップについて

ルート マップは、ルートを OSPF、RIP、EIGRP、または BGP ルーティング プロセスに再配布するときに使用します。また、デフォルト ルートを OSPF ルーティング プロセスに生成するときにも使用します。ルート マップは、指定されたルーティング プロトコルのどのルートを対象ルーティング プロセスに再配布できるのかを定義します。

ルート マップは、広く知られた ACL と共通の機能を数多く持っています。両方に共通する主な特性は次のとおりです。

- いずれも、それぞれが許可または拒否の結果を持つ個々の文を一定の順序で並べたものです。ACL またはルート マップの評価は、事前に定義された順序でのリストのスキャンと、一致する各文の基準の評価で構成されています。リストのスキャンは、文の一致が初めて見つかり、その文に関連付けられたアクションが実行されると中断します。
- これらは汎用メカニズムです。基準の一致と一致の解釈は、その適用方法によって指定されます。異なるタスクに適用される同じルート マップの解釈が異なることがあります。

次のように、ルート マップと ACL には違いがいくつかあります。

- ルート マップでは、一致基準として ACL を頻繁に使用します。
- ACL の評価の主な結果は、yes または no の答えとなります。つまり、ACL は入力データを許可するか拒否するかのいずれかです。再配布に適用された ACL は、特定のルートを再配布できるか（ルートが ACL の permit 文に一致）、再配布できないか（deny 文に一致）を判断します。一般的なルート マップでは、（一部の）再配布ルートを許可するだけではなく、別のプロトコルに再配布される場合は、ルートに関連付けられた情報も変更します。
- ルート マップは ACL よりも柔軟性が高く、ACL が確認できない基準に基づいてルートを確認できます。たとえば、ルート マップはルートのタイプが内部であるかどうかを確認できます。

- 各 ACL は、設計の表記法により暗黙的な deny 文で終了しますが、ルート マップには同様の表記法はありません。一致試行の間にルート マップの終わりに達した場合は、そのルート マップの特定のアプリケーションによって結果が異なります。幸いなことに、再配布に適用されたルート マップの動作は ACL と同じです。ルートがルート マップのどの句とも一致しない場合は、ルート マップの最後に deny 文が含まれている場合と同様にルートの再配布は拒否されます。

ダイナミック プロトコルの **redistribute** コマンドを使用すると、ルート マップを適用できます。Cisco ASDM の場合、再配布用のこの機能は、新しいルート マップを追加または編集するときに使用できます（「ルート マップの定義」（P.21-4）を参照）。ルート マップは、再配布中にルート情報を変更する場合や、ACL よりも強力な照合機能が必要な場合に推奨します。プレフィックスまたはマスクに基づいて一部のルートを選択的に許可することだけが必要な場合は、ルート マップを使用して、**redistribute** コマンドで ACL（または等価のプレフィックス リスト）に直接マップすることをお勧めします。ルート マップを使用して、プレフィックスまたはマスクに基づいて一部のルートを選択的に許可する場合は、通常はこれよりも多くのコンフィギュレーション コマンドを使用して同じ目標を達成します。

（注）　標準 ACL をルート マップの一致基準として使用する必要があります。拡張 ACL を使用しても機能しないため、ルートが再配布されなくなります。将来的に句を挿入する必要性が生じたときの番号の間隔を確保するために、10 単位で句に番号を指定することをお勧めします。

- 「permit 句と deny 句」（P.21-2）
- 「match 句と set 句の値」（P.21-2）
- 「BGP match 句および BGP set 句」（P.21-3）

permit 句と deny 句

ルート マップでは permit 句と deny 句を使用できます。**route-map ospf-to-eigrp** コマンドには、1 つの deny 句（シーケンス番号は 10）と 2 つの permit 句があります。deny 句は、ルートの照合の再配布を拒否します。したがって、次のルールが適用されます。

- ルート マップの permit 句で ACL を使用する場合は、その ACL で許可されるルートが再配布されます。
- ルート マップの deny 句で ACL を使用すると、その ACL で許可されるルートは再配布されなくなります。
- ルートマップの permit 句または deny 句で ACL を使用する場合に、その ACL でルートが拒否されるときは、そのルート マップ句に一致するものは見つからないことになり、次のルート マップ句が評価されます。

match 句と set 句の値

各ルート マップ句には、次の 2 種類の値があります。

- match 値は、この句が適用されるルートを選択するために使用されます。
- set 値は、ターゲット プロトコルに再配布される情報を変更します。

再配布される各ルートについて、ルータは最初にルート マップの句の一致基準を評価します。一致基準が満たされると、そのルートは、permit 句または deny 句に従って再配布または拒否され、そのルートの一部の属性が、ASDM の [Set Value] タブ、または **set** コマンドによって設定された値に変更されます。一致基準が満たされないと、この句はルートに適用されず、ソフト

ウェアはルートマップの次の句でルートを評価します。ルート マップのスキャンは、ルートが **match** コマンド（または ASDM の [Match Clause] タブで設定された [Match Clause]）と一致する句が見つかるまで、またはルート マップの終わりに達するまで続行します。

次のいずれかの条件が満たされる場合は、各句の match 値または set 値を省略したり、何回か繰り返したりできます。

- 1 つの句に複数の **match** コマンドまたは ASDM の [Match Clause] 値が含まれている場合、与えられたルートがその句と一致するには、そのルートに対して条件がすべて一致する必要があります（つまり、複数の match コマンドに対して論理積のアルゴリズムが適用されます）。
- 1 つのコマンド内で複数のオブジェクトが **match** コマンドまたは ASDM の [Match Clause] 値によって参照されている場合、そのうちのいずれかが一致する必要があります（論理和のアルゴリズムが適用されます）。たとえば、**match ip address 101 121** コマンドでは、ルートは ACL 101 または ACL 121 で許可されている場合に、許可されます。
- **match** コマンドまたは ASDM の [Match Clause] 値が存在しない場合、すべてのルートがその句に一致します。前の例では、句 30 に達したすべてのルートが一致しているため、ルート マップの終わりには達しません。
- ルート マップの permit 句に **set** コマンド（または ASDM の [Set Value]）が存在しない場合、ルートは、その現在の属性を変更されずに再配布されます。

（注） ルート マップの deny 句では **set** コマンドを設定しないでください。deny 句を指定するとルートの再配布が禁止され、情報は何も変更されないためです。

match コマンドまたは **set** コマンド（または ASDM の [Match] タブまたは [Set Value] タブで設定される [Match] または [Set Value]）がないルート マップ句はアクションを実行します。空の permit 句を使用すると、変更を加えずに残りのルートの再配布が可能になります。空の deny 句では、他のルートの再配布はできません。これは、ルート マップがすべてスキャンされたときに、明示的な一致が見つからなかったときのデフォルト アクションです。

BGP match 句および BGP set 句

前述の match および set の値に加えて、BGP ではルート マップに対して追加の match および set 機能が提供されています。

次の新しいルートマップ match 句が BGP でサポートされるようになっています。

- match as-path
- match community
- match policy-list
- match tag

次の新しいルートマップ set 句が BGP でサポートされるようになっています。

- set as-path
- set automatic-tag
- set community
- set local-preference
- set origin
- set weight

再配布される各 BGP ルートについて、ASA は最初にルート マップの句の BGP match 基準を評価します。BGP match 基準が満たされると、そのルートは、permit 句または deny 句に従って再配布または拒否され、そのルートの一部の属性が、ASDM の [BGP Set Clause] タブ、または **set** コマンドによって設定された値に変更されます。一致基準が満たされないと、この句はルートに適用されず、ソフトウェアはルート マップの次の句でルートを評価します。ルート マップのスキャンは、ルートが ASDM の [BGP Match Clause] タブで設定された **match** コマンドと一致する句が見つかるまで、またはルート マップの終わりに達するまで続行します。

ルート マップのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

その他のガイドライン

ルート マップは、ユーザ、ユーザ グループ、または完全修飾ドメイン名のオブジェクトを含む ACL をサポートしていません。

ルート マップの定義

ルート マップを定義する必要があるのは、指定したルーティング プロトコルからのどのルートを対象ルーティング プロセスに再配布できるのかを指定するときです。ASDM でルート マップを定義するには、ルート マップ名、シーケンス番号、または再配布を追加、編集、または削除します。

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [Route Maps] の順に選択します。

ステップ 2　[Add] をクリックします。

[Add Route Map] または [Edit Route Map] ダイアログボックスが表示されます。

ステップ 3　ルート マップ名とシーケンス番号を入力します。ルート マップ名とは、特定のルートに割り当てる名前です。シーケンス番号とは、ルート マップ エントリを ASA に追加または削除するときの順序です。

（注）　既存のルート マップ名を編集する場合、ルート マップ名とシーケンス番号のフィールドにはすでに値が入力されています。

ステップ 4　一致するルートの再配布を拒否するには、[Deny] をクリックします。ルート マップの Deny 句で ACL を使用すると、その ACL で許可されるルートは再配布されなくなります。一致するルートの再配布を許可するには、[Permit] をクリックします。ルートマップの Permit 句で ACL を使用すると、その ACL で許可されるルートが再配布されます。

さらに、ルートマップの Permit または Deny 句で ACL を使用する場合に、その ACL でルートが拒否されたときは、そのルート マップ句に一致するものは見つからなかったことになり、次のルート マップ句が評価されます。

ステップ 5　[Match Clause] タブをクリックして、この句を適用する必要のあるルートを選択し、次のパラメータを設定します。

- [Match first hop interface of route] チェックボックスをオンにして、ルートのファースト ホップ インターフェイスの照合をイネーブルにするか、オフにしてディセーブルにし、指定されたネクスト ホップ インターフェイスを任意のルートと照合します。2 つ以上のインターフェイスを指定する場合、ルートはいずれかのインターフェイスと一致します。
  - [Interface] フィールドにインターフェイス名を入力するか、または省略記号をクリックして [Browse Interface] ダイアログボックスを表示します。
  - 1 つ以上のインターフェイスを選択し、[Interface] をクリックして [OK] をクリックします。
  - [Match Address] チェックボックスをオンにして、ルートの一致アドレスをイネーブルにするか、オフにしてディセーブルにし、パケットを照合します。
  - [Match Next Hop] チェックボックスをオンにするとルートのネクスト ホップ アドレスの照合がイネーブルになり、オフにするとディセーブルになります。
  - [Match Route Source] チェックボックスをオンにするとルートのアドバタイジング ソース アドレスの照合がイネーブルになり、オフにするとディセーブルになります。
  - ドロップダウン リストで [Access List] から [Prefix List] を選択して、IP アドレスを照合します。
  - 以前の選択内容に従って、省略記号をクリックして [Browse Access List] または [Browse Prefix List] ダイアログボックスを表示します。
  - 必要な ACL またはプレフィックス リストを選択します。
- [Match metric of route] チェックボックスをオンにするとルートのメトリックの照合がイネーブルになり、オフにするとディセーブルになります。
  - [Metric Value] フィールドに、メトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ～ 4294967295 の範囲で指定します。
- [Match Route Type] チェックボックスをオンにするとルート タイプの照合がイネーブルになり、オフにするとディセーブルになります。有効なルート タイプは、External1、External2、Internal、Local、NSSA-External1、NSSA-External2 です。イネーブルの場合、複数のルート タイプをリストから選択することができます。

ステップ 6　[Set Clause] タブをクリックして、ターゲット プロトコルに再配布される次の情報を変更します。

- [Set Metric Clause] チェックボックスを使用して、宛先ルーティング プロトコルに対するメトリック値をイネーブルにするかディセーブルにするかを指定し、値を [Value] フィールドに入力します。
- [Set Metric Type] チェックボックスをオンにすると宛先ルーティング プロトコルのメトリック タイプがイネーブルになり、オフにするとディセーブルになります。ドロップダウン リストからメトリック タイプを選択します。

ステップ 7　[BGP Match Clause] タブをクリックして、この句を適用する必要のあるルートを選択し、次のパラメータを設定します。

- [Match AS path access lists] チェックボックスをオンにすると、BGP 自律システム パス アクセス リストと指定されたパス アクセス リストの照合がイネーブルになります。複数のパス アクセス リストを指定した場合、ルートはいずれかのパス アクセス リストと一致します。

- [Match Community] チェックボックスをオンにすると、BGP コミュニティと指定されたコミュニティの照合がイネーブルになります。複数のコミュニティを指定した場合、ルートはいずれかのコミュニティと一致します。少なくとも 1 つの Match コミュニティと一致しないルートは、アウトバウンド ルート マップにアドバタイズされません。
  - [Match the specified community exactly] チェックボックスをオンにすると、BGP コミュニティと指定されたコミュニティの厳密な照合がイネーブルになります。
- BGP ポリシーを評価および処理するためのルート マップを設定するには、[Match Policy list] チェックボックスをオンにします。複数のポリシー リストを指定した場合、ルートはいずれかのポリシー リストを処理できます。

ステップ 8　[BGP Set Clause] タブをクリックして、BGP プロトコルに再配布される次の情報を変更します。

- BGP ルートの自律システム パスを変更するには、[Set AS Path] チェックボックスをオンにします。
  - BGP ルートの前に任意の自律システム パス文字列を付加するには、[Prepend AS path] チェックボックスをオンにします。通常、ローカルな AS 番号が複数回追加され、自律システム パス長が増します。複数の AS パス番号を指定した場合、ルートはいずれかの AS 番号を付加できます。
  - 最後の AS 番号の AS パスを先頭に追加するには、[Prepend Last AS to the AS Path] チェックボックスをオンにします。AS 番号の値を 1 ～ 10 の範囲で入力します。
  - ルートのタグを自律システム パスに変換するには、[Convert route tag into AS Path] チェックボックスをオンにします。
- BGP コミュニティ属性を設定するには、[Set Community] チェックボックスをオンにします。
  - コミュニティ番号を入力するには、[Specify Community] をクリックします（必要な場合）。有効な値は、1 ～ 4294967200、internet、no-advertise、no-export です。
  - 既存のコミュニティにコミュニティを追加するには、[Add to the existing communities] チェックボックスをオンにします。
  - ルート マップをパスするプレフィックスからコミュニティ属性を除去するには、[None] をクリックします。
- 自律システム パスのプリファレンス値を指定するには、[Set local preference] チェックボックスをオンにします。
- ルーティング テーブルに対して BGP ウェイトを指定するには、[Set weight] チェックボックスをオンにします。0 ～ 65535 の範囲で値を入力します。
- BGP 送信元コードを指定するには、[Set origin] チェックボックスをオンにします。有効な値は [Local IGP] および [Incomplete] です。
- ルート マップの match 句を満たすパケットの出力アドレスを指定するには、[Set next hop] チェックボックスをオンにします。
  - パケットが出力されるネクスト ホップの IP アドレスを入力するには、[Specify IP address] をクリックします。隣接ルータである必要はありません。複数の IP アドレスを指定した場合、いずれかの IP アドレスでパケットを出力できます。
  - BGP ピア アドレスにするネクスト ホップを設定するには、[Use peer address] をクリックします。

ステップ 9　[OK] をクリックします。

ルート マップのカスタマイズ

ここでは、ルート マップをカスタマイズする方法について説明します。

特定の宛先アドレスに一致するルートの定義

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [Route Maps] の順に選択します。

ステップ 2　[Add] をクリックします。

[Add Route Map] ダイアログボックスが表示されます。このダイアログボックスでは、ルート マップ名、シーケンス番号、その再配布アクセス（許可または拒否）の割り当てまたは選択を行うことができます。ルート マップのエントリは順番に読み取られます。この順序は、シーケンス番号で指定できます。シーケンス番号が指定されていない場合は、ASA にエントリを追加した順序が使用されます。

ステップ 3　[Match Clause] タブをクリックして、この句を適用する必要のあるルートを選択し、次のパラメータを設定します。

- [Match first hop interface of route] チェックボックスをオンにして、ルートのファースト ホップ インターフェイスの照合をイネーブルにするか、オフにしてディセーブルにし、指定されたネクスト ホップ インターフェイスを任意のルートと照合します。2 つ以上のインターフェイスを指定する場合、ルートはいずれかのインターフェイスと一致します。
  - [Interface] フィールドにインターフェイス名を入力するか、または省略記号をクリックして [Browse Interface] ダイアログボックスを表示します。
  - インターフェイス タイプ（[inside] または [outside]）を選択し、[Selected Interface] をクリックして、[OK] をクリックします。
  - [Match IP Address] チェックボックスをオンにして、ルートの一致アドレスをイネーブルにするか、オフにしてディセーブルにし、パケットを照合します。
  - [Match Next Hop] チェックボックスをオンにするとルートのネクスト ホップ アドレスの照合がイネーブルになり、オフにするとディセーブルになります。
  - [Match Route Source] チェックボックスをオンにするとルートのアドバタイジング ソース アドレスの照合がイネーブルになり、オフにするとディセーブルになります。
  - ドロップダウン リストで [Access List] から [Prefix List] を選択して、IP アドレスを照合します。
  - 以前の選択内容に従って、省略記号をクリックして [Browse Access List] または [Browse Prefix List] ダイアログボックスを表示します。
  - 必要な ACL またはプレフィックス リストを選択します。
- [Match metric of route] チェックボックスをオンにするとルートのメトリックの照合がイネーブルになり、オフにするとディセーブルになります。

– [Metric Value] フィールドに、メトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ～ 4294967295 の範囲で指定します。

- [Match Route Type] チェックボックスをオンにするとルート タイプの照合がイネーブルになり、オフにするとディセーブルになります。有効なルート タイプは、External1、External2、Internal、Local、NSSA-External1、NSSA-External2 です。イネーブルの場合、複数のルート タイプをリストから選択することができます。

プレフィックス ルールの設定

（注）　プレフィックス ルールを設定する前に、プレフィックス リストを設定する必要があります。

プレフィックス ルールを設定するには、次の手順を実行します。

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [Prefix Rules] の順に選択します。

ステップ 2　[Add] をクリックし、[Add Prefix Rule] を選択します。

[Add Prefix Rule] ダイアログボックスが表示されます。このダイアログ ボックスでは、シーケンス番号を追加し、IP のバージョンを選択し（IPv4 または IPv6）、ネットワークのプレフィックス、再配布アドレス（許可または禁止）、プレフィックスの最小長と最大長を指定できます。

ステップ 3　シーケンス番号のデフォルト値を確認し、必要に応じて入力します。

ステップ 4　プレフィックス番号を IP アドレス/マスク長の形式で指定します。

ステップ 5　[Permit] または [Deny] オプション ボタンをクリックして再配布アクセスを指定します。

ステップ 6　必要に応じて、最小/最大プレフィックス長を入力します。

ステップ 7　完了したら、[OK] をクリックします。

新規追加または修正したプレフィックス ルールがリストに表示されます。

ステップ 8　自動生成したシーケンス番号を使用する場合は、[Enable Prefix list sequence numbering] チェックボックスをオンにします。

ステップ 9　[Apply] をクリックして変更内容を保存します。

プレフィックス リストの設定

ABR のタイプ 3 LSA フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されているときは、指定されたプレフィックスのみが OSPF エリア間で送信されます。その他のすべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックス リストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。デフォルトでは、シーケンス番号は自動的に生成され、開始値は 5 で 5 ずつ増えていきます。

プレフィックス リストを追加するには、次の手順を実行します。

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [Prefix Rules] の順に選択します。

ステップ 2　[Add] をクリックし、[Add Prefix List] を選択します。

[Add Prefix List] ダイアログボックスが表示されます。

ステップ 3　プレフィックス名と説明を入力して [OK] をクリックします。

ルート アクションのメトリック値の設定

ルート アクションのメトリック値を設定するには、次の手順を実行します。

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [Route Maps] の順に選択します。

ステップ 2　[Add] をクリックします。

[Add Route Map] または [Edit Route Map] ダイアログボックスが表示されます。このダイアログボックスでは、ルート マップ名、シーケンス番号、およびその再配布アクセス（許可または拒否）の割り当てまたは選択を行うことができます。ルート マップのエントリは順番に読み取られます。この順序は、シーケンス番号で指定できます。シーケンス番号が指定されていない場合は、ASA にルート マップ エントリを追加した順序が使用されます。

ステップ 3　[Set Clause] タブをクリックして、ターゲット プロトコルに再配布される次の情報を変更します。

- [Set Metric Clause] チェックボックスを使用して、宛先ルーティング プロトコルに対するメトリック値をイネーブルにするかディセーブルにするかを指定し、値を [Value] フィールドに入力します。
- [Set Metric Type] チェックボックスをオンにすると宛先ルーティング プロトコルのメトリック タイプがイネーブルになり、オフにするとディセーブルになります。ドロップダウン リストからメトリック タイプを選択します。

ルート マップの設定例

次の例は、ホップ カウント 1 でルートを OSPF に再配布する方法を示しています。

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [Route Maps] の順に選択します。

ステップ 2　[Add] をクリックします。

ステップ 3　[Route Map Name] フィールドに **1-to-2** と入力します。

ステップ 4　ルーティング シーケンス番号を [Sequence Number] フィールドに入力します。

ステップ 5　[Permit] オプション ボタンをクリックします。

デフォルトでは、このタブは一番上にあります。

ステップ 6　[Match Clause] タブをクリックします。

ステップ 7　[Match Metric of Route] チェックボックスをオンにして、メトリック値 **1** を入力します。

ステップ 8　[Set Clause] タブをクリックします。

ステップ 9　[Set Metric Value] チェックボックスをオンにして、メトリック値 **5** を入力します。

ステップ 10　[Set Metric-Type] チェックボックスをオンにして、[Type-1] を選択します。

ルート マップの機能履歴

表 21-1　ルート マップの機能履歴

機能名	プラットフォーム リリース	機能情報
ルート マップ	7.0(1)	この機能が導入されました。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [Route Maps]。
スタティックおよびダイナミック ルート マップのサポートの強化	8.0(2)	ダイナミックおよびスタティック ルート マップのサポートが強化されました。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	ルート マップは、マルチ コンテキスト モードでサポートされます。
BGP のサポート	9.2(1)	この機能が導入されました。 [Configuration] > [Device Setup] > [Routing] > [Route Maps] 画面が更新され、2 つのタブ [BGP match clause] および [BGP set clause] が追加されました。

BGP

この章では、Border Gateway Protocol（BGP）を使用してデータのルーティング、認証の実行、ルーティング情報の再配布を行うように Cisco ASA を設定する方法について説明します。

BGP について

BGP は相互自律システム ルーティング プロトコルです。自律システムとは、共通の管理下にあり、共通のルーティング ポリシーを使用するネットワークまたはネットワークのグループです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。

BGP を使用する状況

通常、大学や企業などの顧客ネットワークではネットワーク内でルーティング情報を交換するために OSPF などの Interior Gateway Protocol（IGP）を採用しています。カスタマーは ISP に接続し、ISP は BGP を使用してカスタマーおよび ISP ルートを交換します。自律システム（AS）間で BGP を使用する場合、このプロトコルは外部 BGP（EBGP）と呼ばれます。サービス プロバイダーが BGP を使用して AS 内のルートを交換する場合、このプロトコルは内部 BGP（IBGP）と呼ばれます。

ルーティング テーブルの変更

BGP ネイバーは、ネイバー間で最初に TCP 接続を確立する際に、完全なルーティング情報を交換します。ルーティング テーブルで変更が検出された場合、BGP ルータはネイバーに対し、変更されたルートのみを送信します。BGP ルータは、定期的にルーティング アップデートを送信しません。また BGP ルーティング アップデートは、宛先ネットワークに対する最適パスのアドバタイズのみを行います。

BGP により学習されたルートには、特定の宛先に対して複数のパスが存在する場合、宛先に対する最適なルートを決定するために使用されるプロパティが設定されています。これらのプロパティは BGP 属性と呼ばれ、ルート選択プロセスで使用されます。

- Weight：これは、シスコ定義の属性で、ルータに対してローカルです。Weight 属性は、隣接ルータにアドバタイズされません。ルータが同じ宛先への複数のルートがあることを学習すると、Weight が最も大きいルートが優先されます。
- Local preference：Local preference 属性は、ローカル AS からの出力点を選択するために使用されます。Weight 属性とは異なり、Local preference 属性は、ローカル AS 全体に伝搬されます。AS からの出力点が複数ある場合は、Local preference 属性が最も高い出力点が特定のルートの出力点として使用されます。
- Multi-exit discriminator：メトリック属性である Multi-exit discriminator（MED）は、メトリックをアドバタイズしている AS への優先ルートに関して、外部 AS への提案として使用されます。これが提案と呼ばれるのは、MED を受信している外部 AS がルート選択の際に他の BGP 属性も使用している可能性があるためです。MED メトリックが小さい方のルートが優先されます。
- Origin：Origin 属性は、BGP が特定のルートについてどのように学習したかを示します。Origin 属性は、次の 3 つの値のいずれかに設定することができ、ルート選択に使用されます。
  - IGP：ルートは発信側 AS の内部にあります。この値は、ネットワーク ルータ コンフィギュレーション コマンドを使用して BGP にルートを挿入する場合に設定されます。
  - EGP：ルートは Exterior Border Gateway Protocol（EBGP）を使用して学習されます。
  - Incomplete：ルートの送信元が不明であるか、他の方法で学習されています。Incomplete の Origin は、ルートが BGP に再配布されるときに発生します。
- AS_path：ルート アドバタイズメントが自律システムを通過すると、ルート アドバタイズメントが通過した AS 番号が AS 番号の順序付きリストに追加されます。AS_path リストが最も短いルートのみ、IP ルーティング テーブルにインストールされます。
- Next hop：EBGP の Next-hop 属性は、アドバタイズしているルータに到達するために使用される IP アドレスです。EBGP ピアの場合、ネクスト ホップ アドレスは、ピア間の接続の IP アドレスです。IBGP の場合、EBGP のネクスト ホップ アドレスがローカル AS に伝送されます。
- Community：Community 属性は、ルーティングの決定（承認、優先度、再配布など）を適用できる宛先をグループ化する方法、つまりコミュニティを提供します。ルート マップは、Community 属性を設定するために使用されます。事前定義済みの Community 属性は次のとおりです。
  - no-export：EBGP ピアにこのルートをアドバタイズしません。
  - no-advertise：どのピアにもこのルートをアドバイタイズしません。
  - internet：インターネット コミュニティにこのルートをアドバタイズします。ネットワーク内のすべてのルートがこのコミュニティに属します。

BGP パスの選択

BGP は、異なる送信元から同じルートの複数のアドバタイズメントを受信する場合があります。BGP は最適なパスとして 1 つのパスだけを選択します。このパスを選択すると、BGP は IP ルーティング テーブルに選択したパスを格納し、そのネイバーにパスを伝搬します。BGP は次の基準を使用して（示されている順序で）、宛先へのパスを選択します。

- パスで指定されているネクスト ホップが到達不能な場合、このアップデートは削除されます。
- Weight が最大のパスが優先されます。
- Weight が同じである場合、Local preference が最大のパスが優先されます。
- Local preference が同じである場合、このルータで動作している BGP により発信されたパスが優先されます。
- ルートが発信されていない場合、AS_path が最短のルートが優先されます。
- すべてのパスの AS_path の長さが同じである場合、Origin タイプが最下位のパス（IGP は EGP よりも低く、EGP は Incomplete よりも低い）が優先されます。
- Origin コードが同じである場合、最も小さい MED 属性を持つパスが優先されます。
- パスの MED が同じである場合、内部パスより外部パスが優先されます。
- それでもパスが同じである場合、最も近い IGP ネイバーを経由するパスが優先されます。
- 両方のパスが外部の場合、最初に受信したパス（最も古いパス）が優先されます。
- BGP ルータ ID で指定された、IP アドレスが最も小さいパスが優先されます。
- 送信元またはルータ ID が複数のパスで同じである場合、クラスタ リストの長さが最小のパスが優先されます。
- 最も小さいネイバー アドレスから発信されたパスが優先されます。

BGP のガイドライン

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

トランスペアレント ファイアウォール モードはサポートされません。BGP は、ルータ モードでのみサポートされています。

フェールオーバーのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでステートフル フェールオーバーをサポートします。

（注）　クラスタリングがイネーブルの場合、フェールオーバーはサポートされません。

クラスタリングのガイドライン

BGP は L2（EtherChannel タイプ）および L3（個別インターフェイス タイプ）クラスタリング モードでのみサポートされています。

（注）　ユーザ コンテキストで BGP 設定を削除および再適用する場合は、60 秒の遅延でスレーブ/スタンバイ ASA 装置を同期できます。

IPv6 のガイドライン

IPv6 をサポートします。グレースフル リスタートは、IPv6 アドレス ファミリではサポートされません。

BGP の設定

ここでは、システムで BGP プロセスをイネーブルにして設定する方法について説明します。

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] の順に選択します。

ステップ 2　[General] タブの [Enable BGP routing] チェックボックスをオンにして、BGP ルーティング プロセスをイネーブルにします。「BGP のイネーブル化」（P.22-4）を参照してください。

ステップ 3　[BGP] > [Best Path] タブで、BGP ルーティングの最適なパスの選択プロセスに関連する設定を定義します。「BGP ルーティング プロセスの最適なパスの定義」（P.22-6）を参照してください。

ステップ 4　[BGP] > [Policy Lists] タブで、BGP ルーティングのポリシー リストを設定します。「ポリシー リストの設定」（P.22-6）を参照してください。

ステップ 5　[BGP] > [AS Path Filters] タブで、BGP ルーティングの AS パス フィルタを設定します。「AS パス フィルタの設定」（P.22-8）を参照してください。

ステップ 6　[BGP] > [Community Rules] タブで、BGP ルーティングのコミュニティ ルールを設定します。「コミュニティ ルールの設定」（P.22-8）を参照してください。

ステップ 7　[BGP] > [IPv4 Family] タブで、IPv4 アドレス ファミリを設定します。「IPv4 アドレス ファミリの設定」（P.22-9）を参照してください。

BGP のイネーブル化

ここでは、BGP のイネーブル化、BGP ルーティング プロセスの確立、一般的な BGP パラメータの設定に必要な手順について説明します。

手順

ステップ 1　シングル モードの場合、ASDM で [Configuration] > [Device Setup] > [Routing] > [BGP] > [General] の順に選択します。

（注）　マルチ モードの場合、ASDM で [Configuration] > [Context Management] > [BGP] の順に選択します。BGP をイネーブルにした後に、セキュリティ コンテキストに切り替え、[Configuration] > [Device Setup] > [Routing] > [BGP] > [General] の順に選択して BGP をイネーブルにします。

[General] ペインが表示されます。

ステップ 2　[Enable BGP Routing] チェックボックスをオンにします。

ステップ 3　[AS Number] フィールドに、BGP プロセスの自律システム（AS）番号を入力します。AS 番号内部には、複数の自律番号が含まれます。AS 番号には、1 ～ 4294967295 または 1.0 ～ XX.YY を指定できます。

ステップ 4　（オプション）[Limit the number of AS numbers in the AS_PATH attribute of received routes] チェックボックスをオンにして、AS_path 属性の AS 番号の数を特定の数に制限します。有効値は 1 ～ 254 です。

ステップ 5　（オプション）[Log neighbor changes] チェックボックスをオンにして、BGP ネイバーの変更（アップ状態またはダウン状態）およびリセットのロギングをイネーブルにします。これは、ネットワーク接続の問題をトラブルシューティングしたり、ネットワークの安定性を評価する際に役に立ちます。

ステップ 6　（オプション）[Use TCP path MTU discovery] チェックボックスをオンにし、パス MTU ディスカバリ手法を使用して 2 つの IP ホスト間のネットワーク パスにおける最大伝送単位（MTU）のサイズを決定します。これにより、IP フラグメンテーションが回避されます。

ステップ 7　（オプション）[Enable fast external failover] チェックボックスをオンにして、リンク障害の発生時に外部 BGP セッションをただちにリセットします。

ステップ 8　（オプション）[Enforce that first AS is peer’s AS for EBGP routes] チェックボックスをオンにして、その AS 番号を AS_path 属性の 1 つ目のセグメントとしてリストしていない外部 BGP ピアから受信した着信アップデートを破棄します。これにより、誤って設定されたピアや許可されていないピアが、別の自律システムから送信されたかのようにルートをアドバイタイズしてトラフィックを誤った宛先に送信することがなくなります。

ステップ 9　（オプション）[Use dot notation for AS numbers] チェックボックスをオンにして、完全なバイナリ 4 バイトの AS 番号を、ドットで区切られた 16 ビットの 2 文字ずつに分割します。0 ～ 65553 の AS 番号は 10 進数で表され、65535 を超える AS 番号はドット付き表記を使用して表されます。

ステップ 10　[Neighbor timers] 領域でタイマー情報を指定します。

- **a.** [Keepalive interval] フィールドに、BGP ネイバーがキープアライブ メッセージを送信しなくなった後アクティブな状態を継続する時間を入力します。このキープアライブ インターバルが終わると、メッセージが送信されない場合、BGP ピアはデッドとして宣言されます。デフォルト値は 60 秒です。
- **b.** [Hold Time] フィールドに、BGP 接続が開始されて設定されている間 BGP ネイバーがアクティブな状態を維持する時間を入力します。デフォルト値は 180 秒です。
- **c.** （オプション）[Min.Hold Time] フィールドに、BGP 接続が開始されて設定されている間に BGP ネイバーがアクティブな状態を維持する最小時間を入力します。0 ～ 65535 の値を指定します。

ステップ 11　（オプション）[Non Stop Forwarding] セクションで、次の手順を実行します。

- **a.** [Enable Graceful Restart] チェックボックスをオンにして、ASA ピアがスイッチオーバー後のルート フラップを回避できるようにします。
- **b.** [Restart Time] フィールドに、BGP オープン メッセージを受信するまで ASA が古いルートを削除するのを待機する時間を入力します。デフォルト値は 120 秒です。有効な値は 1 ～ 3600 秒です。
- **c.** [Stale Path Time] フィールドに、リスタートする ASA から End Of Record（EOR）メッセージを受信した後、古いルートを削除するまで ASA が待機する時間を入力します。デフォルト値は 360 秒です。有効な値は 1 ～ 3600 秒です。

ステップ 12　[OK] をクリックします。

ステップ 13　[Apply] をクリックします。

BGP ルーティング プロセスの最適なパスの定義

ここでは、BGP の最適なパスを設定するために必要な手順について説明します。最適なパスの詳細については、「BGP パスの選択」（P.22-3）を参照してください。

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [Best Path] の順に選択します。

[Best Path configuration] ペインが表示されます。

ステップ 2　[Default Local Preference] フィールドに、0 ～ 4294967295 の値を指定します。デフォルト値は 100 です。値が大きいほど、優先度が高いことを示します。この優先度は、ローカル自律システム内のすべてのルータおよびアクセス サーバに送信されます。

ステップ 3　[Allow comparing MED from different neighbors] チェックボックスをオンにして、さまざまな自律システムのネイバーからのパスにおいて Multi-exit discriminator（MED）の比較ができるようにします。

ステップ 4　[Compare router-id for identical EBGP paths] チェックボックスをオンにして、最適なパスの選択プロセス中に、外部 BGP ピアから受信した類似のパスを比較し、最適なパスをルータ ID が最も小さいルートに切り替えます。

ステップ 5　[Pick the best MED path among paths advertised from the neighboring AS] チェックボックスをオンにして、連合ピアから学習したパス間における MED 比較をイネーブルにし、新しいネットワーク エントリを追加します。MED 間の比較は、外部の自律システムがパスに存在しない場合にのみ行われます。

ステップ 6　[Treat missing MED as the least preferred one] チェックボックスをオンにして、欠落している MED 属性は無限大の値を持つものとみなし、このパスを最も推奨度の低いパスにします。したがって、MED が欠落しているパスが最も優先度が低くなります。

ステップ 7　[OK] をクリックします。

ステップ 8　[Apply] をクリックします。

ポリシー リストの設定

ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の match 文すべてが評価され、処理されます。1 つのルート マップに 2 つ以上のポリシー リストを設定できる。ポリシー リストは、同じルート マップ内にあるがポリシー リストの外で設定されている他の既存の match および set 文とも共存できます。ここでは、ポリシー リストを設定するために必要な手順について説明します。

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [Policy Lists] の順に選択します。

ステップ 2　[Add] をクリックします。

[Add Policy List] ダイアログボックスが表示されます。このダイアログボックスでは、ポリシー リスト名、その再配布アクセス（許可または拒否）、一致インターフェイス、一致 IP アドレス、一致 AS パス、一致コミュニティ名リスト、一致メトリック、一致タグ番号を追加することができます。

ステップ 3　[Policy List Name] フィールドに、ポリシー リストの名前を入力します。

ステップ 4　[Permit] または [Deny] オプション ボタンをクリックして再配布アクセスを指定します。

ステップ 5　[Match Interfaces] チェックボックスをオンにして、指定のインターフェイスの 1 つのネクスト ホップを持つルートを配布し、次のいずれかを実行します。

- [Interface] フィールドに、インターフェイス名を入力します。
- [Interface] フィールドで、省略記号をクリックすると、手動でインターフェイスを参照し、指定できます。1 つ以上のインターフェイスを選択し、[Interface] をクリックして [OK] をクリックします。

ステップ 6　[Specify IP] 領域で、次のように設定します。

a. [Match Address] チェックボックスをオンにして、標準アクセス リストまたはプレフィックス リストで許可された宛先ネットワーク番号アドレスを持つルートを再配布し、パケットにポリシー ルーティングを実行します。

アクセス リストまたはプレフィックス リストを指定するか、省略記号をクリックして手動でアクセス リストを参照し、指定します。1 つ以上のアクセス リストを選択し、[Access List] をクリックして [OK] をクリックします。

b. [Match Next Hop] チェックボックスをオンにして、指定したアクセス リストまたはプレフィックス リストの 1 つから渡されたネクスト ホップ ルータ アドレスを持つルートを再配布します。

アクセス リストまたはプレフィックス リストを指定するか、省略記号をクリックして手動でアクセス リストを参照し、指定します。1 つ以上のアクセス リストを選択し、[Access List] をクリックして [OK] をクリックします。

c. [Match Route Source] チェックボックスをオンにして、アクセス リストまたはプレフィックス リストで指定されたアドレスのルータおよびアクセス サーバによってアドバタイズされたルートを再配布します。

アクセス リストまたはプレフィックス リストを指定するか、省略記号をクリックして手動でアクセス リストを参照し、指定します。1 つ以上のアクセス リストを選択し、[Access List] をクリックして [OK] をクリックします。

ステップ 7　[Match AS Path] チェックボックスをオンにして、BGP 自律システム パスを一致させます。

AS パス フィルタを指定するか、省略記号をクリックして手動で AS パス フィルタを参照し、指定します。1 つ以上の AS パス フィルタを選択し、[AS Path Filter] をクリックして [OK] をクリックします。

ステップ 8　[Match Community Names List] チェックボックスをオンにして、BGP コミュニティを一致させます。

a. コミュニティ ルールを指定するか、省略記号をクリックしてコミュニティ ルールを手動で参照し、指定します。1 つ以上のコミュニティ ルールを選択し、[Community Rules] をクリックして [OK] をクリックします。

b. [Match the specified community exactly] チェックボックスをオンにして、特定の BGP コミュニティを一致させます。

ステップ 9　[Match Metrices] チェックボックスをオンにして、指定したメトリックを持つルートを再配布します。複数のメトリックを指定する場合、ルートはいずれかのメトリックと一致します。

ステップ 10　[Match Tag Numbers] チェックボックスをオンにして、指定したタグと一致するルーティング テーブル内のルートを再配布します。複数のタグ番号を指定した場合、ルートはいずれかのメトリックと一致します。

ステップ 11　[OK] をクリックします。

ステップ 12　[Apply] をクリックします。

AS パス フィルタの設定

AS パス フィルタで、アクセス リストを使用してルーティング アップデート メッセージをフィルタリングし、アップデート メッセージ内の個々のプレフィックスを確認できます。アップデート メッセージ内のプレフィックスがフィルタ基準に一致すると、フィルタ エントリで実行するように設定されているアクションに応じて、個々のプレフィックスは除外されるか受け入れられます。ここでは、AS パス フィルタを設定するために必要な手順について説明します。

（注）　**AS パス アクセス リスト**は、通常のファイアウォール ACL とは異なります。

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [AS Path Filters] の順に選択します。

ステップ 2　[Add] をクリックします。

[Add Filter] ダイアログボックスが表示されます。このダイアログボックスで、フィルタの名前、その再配布アクセス（許可または拒否）、および正規表現を追加できます。

ステップ 3　[Name] フィールドに、AS パス フィルタの名前を入力します。

ステップ 4　[Permit] または [Deny] オプション ボタンをクリックして再配布アクセスを指定します。

ステップ 5　正規表現を指定します。正規表現を作成するには、[Build] をクリックします。

ステップ 6　[Test] をクリックして、正規表現が選択した文字列と一致するかどうかテストします。

ステップ 7　[OK] をクリックします。

ステップ 8　[Apply] をクリックします。

コミュニティ ルールの設定

コミュニティは、共通するいくつかの属性を共有する宛先のグループです。コミュニティ リストを使用すると、ルート マップの match 句で使用されるコミュニティ グループを作成できます。アクセス リストと同様に、一連のコミュニティ リストを作成できます。ステートメントは一致が見つかるまでチェックされ、1 つのステートメントが満たされると、テストは終了します。ここでは、コミュニティ ルールを設定するために必要な手順について説明します。

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [Community Rules] の順に選択します。

ステップ 2　[Add] をクリックします。

[Add Community Rule] ダイアログボックスが表示されます。このダイアログボックスで、ルール名、ルール タイプ、その再配布アクセス（許可または拒否）、および特定のコミュニティを追加できます。

ステップ 3　[Rule Name] フィールドに、コミュニティ ルールの名前を入力します。

ステップ 4　[Standard] または [Expanded] オプション ボタンをクリックして、コミュニティ ルール タイプを指定します。

ステップ 5　[Permit] または [Deny] オプション ボタンをクリックして再配布アクセスを指定します。

ステップ 6　標準コミュニティ ルールを追加するには、次の手順を実行します。

a.　[Communities] フィールドで、コミュニティ番号を指定します。有効な値は 1 ～ 4294967200 です。

b.　（オプション）[Internet]（既知のコミュニティ）チェックボックスをオンにして、インターネット コミュニティを指定します。このコミュニティのルートは、すべてのピア（内部および外部）にアドバタイズされます。

c.　（オプション）[Do not advertise to any peers]（既知のコミュニティ）チェックボックスをオンにして、no-advertise コミュニティを指定します。このコミュニティのあるルートはピア（内部または外部）にはアドバタイズされません。

d.　（オプション）[Do not export to next AS]（既知のコミュニティ）チェック ボックスをオンにして、no-export コミュニティを指定します。このコミュニティのあるルートは、同じ自律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。

ステップ 7　拡張コミュニティ ルールを追加するには、次の手順を実行します。

a.　[Regular Expression] フィールドに、正規表現を入力します。または、[**Build**] をクリックして正規表現を作成します。

b.　[Test] をクリックして、作成した正規表現が選択した文字列と一致するかどうか調べます。

ステップ 8　[OK] をクリックします。

ステップ 9　[Apply] をクリックします。

IPv4 アドレス ファミリの設定

BGP の IPv4 設定は、BGP 設定セットアップ内の IPv4 ファミリ オプションから指定できます。IPv4 ファミリ セクションには、一般設定、集約アドレスの設定、フィルタリング設定、ネイバー 設定のサブセクションが含まれます。これらの各サブセクションを使用して、IPv4 ファミリに固有のパラメータをカスタマイズすることができます。

ここでは、BGP IPv4 ファミリの設定をカスタマイズする方法について説明します。

- 「IPv4 ファミリの一般設定」（P.22-10）
- 「IPv4 ファミリ集約アドレスの設定」（P.22-11）
- 「IPv4 ファミリのフィルタリング設定」（P.22-11）

- 「IPv4 ファミリの BGP ネイバーの設定」（P.22-12）
- 「IPv4 ネットワークの設定」（P.22-15）
- 「再配布の設定」（P.22-16）
- 「ルート注入の設定」（P.22-16）

IPv4 ファミリの一般設定

ここでは、一般的な IPv4 の設定に必要な手順を説明します。

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] の順に選択します。

ステップ 2　[General] をクリックします。

[General IPv4 family BGP parameters] 設定ペインが表示されます。

ステップ 3　[Administrative Distances] 領域で、[External]、[Internal] および [Local] のディスタンスを指定します。

ステップ 4　[Learned Routes Map] ドロップダウン リストからルート マップ名を選択します。[Manage] をクリックして、ルート マップを追加および設定します。

ステップ 5　（オプション）[Generate Default Route] チェックボックスをオンにして、デフォルト ルート（ネットワーク 0.0.0.0）を配布するように BGP ルーティング プロセスを設定します。

ステップ 6　（オプション）[Summarize subnet routes into network-level routes] チェックボックスをオンにして、ネットワーク レベルのルートへのサブネット ルートの自動集約を設定します。

ステップ 7　（オプション）[Advertise inactive routes] チェックボックスをオンにして、ルーティング情報ベース（RIB）にインストールされていないルートをアドバタイズします。

ステップ 8　（オプション）[Redistribute iBGP into an IGP] チェックボックスをオンにして、IS-IS や OSPF などの Interior Gateway Protocol（IGP）への iBGP の再配布を設定します。

ステップ 9　（オプション）[Scanning Interval] フィールドに、ネクスト ホップの検証用に BGP ルータのスキャン間隔（秒）を入力します。有効な値は 5 ～ 60 秒です。

ステップ 10　（オプション）[Enable address tracking] チェックボックスをオンにして、BGP ネクスト ホップ アドレス トラッキングをイネーブルにします。[Delay Interval] フィールドで、ルーティング テーブルにインストールされている更新済みのネクスト ホップ ルートのチェック間の遅延間隔を指定します。

ステップ 11　（オプション）ルーティング テーブルにインストールできる並列の内部ボーダー ゲートウェイ プロトコル（iBGP）ルートの最大数を [Number of paths] フィールドで指定し、[iBGP multipaths] チェックボックスをオンにします。

ステップ 12　[Apply] をクリックします。

IPv4 ファミリ集約アドレスの設定

ここでは、特定のルートの 1 つのルートへの集約を定義するために必要な手順について説明します。

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] の順に選択します。

ステップ 2　[Aggregate Address] をクリックします。

[Aggregate Address parameters] 設定ペインが表示されます。

ステップ 3　[Add] をクリックします。

[Add Aggregate Address] ペインが表示されます。

ステップ 4　[Network] フィールドでネットワーク オブジェクトを指定します。

ステップ 5　[Generate autonomous system set path information] チェックボックスをオンにして、自律システムの設定パス情報を生成します。

ステップ 6　[Filters all more- specific routes from the updates] チェックボックスをオンにして、アップデートから固有性の強いルートをすべてフィルタリングします。

ステップ 7　[Attribute Map] ドロップダウン リストからルート マップを選択します。[Manage] をクリックして、ルート マップを追加または設定します。

ステップ 8　[Advertise Map] ドロップダウン リストからルート マップを選択します。[Manage] をクリックして、ルートを追加または設定します。

ステップ 9　[Suppress Map] ドロップダウン リストからルート マップを選択します。[Manage] をクリックして、ルートを追加または設定します。

ステップ 10　[OK] をクリックします。

ステップ 11　[Aggregate Timer] フィールドで、集約タイマーの値（秒）を指定します。有効な値は、0 または 6 ～ 60 の値です。

ステップ 12　[Apply] をクリックします。

IPv4 ファミリのフィルタリング設定

ここでは、着信 BGP アップデートで受信したルートまたはネットワークをフィルタリングするために必要な手順について説明します。

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] の順に選択します。

ステップ 2　[Filtering] をクリックします。

[Define filters for BGP updates] ペインが表示されます。

ステップ 3　[Add] をクリックします。

[Add Filter] ペインが表示されます。

ステップ 4　[Direction] ドロップダウン リストから方向を選択します。方向は、フィルタを着信アップデートに適用するか、または発信アップデートに適用するかを指定します。

ステップ 5　[Access List] ドロップダウン リストからアクセス リストを選択します。[Manage] をクリックして、新しい ACL を追加します。

ステップ 6　[Protocol] ドロップダウン リストからプロトコルを選択します。これは、発信方向を選択した場合にのみ適用できます。

ステップ 7　[Process ID] ドロップダウン リストから、指定したプロトコルのプロセス ID を選択します。

ステップ 8　[OK] をクリックします。

ステップ 9　[Apply] をクリックします。

IPv4 ファミリの BGP ネイバーの設定

ここでは、BGP ネイバーおよびネイバー設定を定義するために必要な手順について説明します。

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] の順に選択します。

ステップ 2　[Neighbor] クリックします。

ステップ 3　[Add] をクリックします。

ステップ 4　左側のペインで、[General] をクリックします。

ステップ 5　[IP Address] フィールドに BGP ネイバーの IP アドレスを入力します。この IP アドレスは、BGP ネイバー テーブルに追加されます。

ステップ 6　[Remote AS] フィールドに、BGP ネイバーが属する自律システムを入力します。

ステップ 7　（オプション）[Description] フィールドに BGP ネイバーの説明を入力します。

ステップ 8　（オプション）[Shutdown neighbor administratively] チェックボックスをオンにして、ネイバーまたはピア グループをディセーブルにします。

ステップ 9　（オプション）[Enable address family] チェックボックスをオンにして、BGP ネイバーとの通信をイネーブルにします。

ステップ 10　（オプション）[Global Restart Functionality for this peer] チェックボックスをオンにして、ASA ネイバーまたはピア グループの Border Gateway Protocol（BGP）グレースフル リスタート機能をイネーブルまたはディセーブルにします。

ステップ 11　左側のペインで、[Filtering] をクリックします。

ステップ 12　（オプション）[Filter routes using an access list] 領域で、適切な着信または発信アクセス コントロール リストを選択して BGP ネイバー情報を配布します。必要に応じて、[Manage] をクリックして、ACL と ACE を追加します。

ステップ 13　（オプション）[Filter routes using a route map] 領域で、適切な着信または発信ルート マップを選択して、着信ルートまたは発信ルートにルート マップを適用します。[Manage] をクリックして、ルート マップを設定します。

ステップ 14　（オプション）[Filter routes using a prefix list] 領域で、適切な着信または発信プレフィックス リストを選択して BGP ネイバー情報を配布します。[Manage] をクリックして、プレフィックス リストを設定します。

ステップ 15　（オプション）[Filter routes using AS path filter] 領域で、適切な着信または発信 AS パス フィルタを選択して BGP ネイバー情報を配布します。[Manage] をクリックして、AS パス フィルタを設定します。

ステップ 16　（オプション）[Limit the number of prefixes allowed from the neighbor] チェックボックスをオンにして、ネイバーから受信できるプレフィックスの数を制御します。

- [Maximum prefixes] フィールドに、特定のネイバーからの許可される最大プレフィックス数を入力します。
- [Threshold level] フィールドに、ルータが警告メッセージの生成を開始するパーセンテージ（最大数に対する）を入力します。有効な値は 1 ～ 100 の整数です。デフォルト値は 75 です。
- （オプション）[Control prefixes received from a peer] チェックボックスをオンにし、ピアから受信したプレフィックスに対する追加の制御を指定します。次のどちらかを実行します。
  - プレフィックス数の制限値に到達したときに BGP ネイバーを停止するには、[Terminate peering when prefix limit is exceeded] をクリックします。[Restart interval] フィールドで、BGP ネイバーが再起動するまでの時間を指定します。
  - 最大プレフィックス数の制限値を超えたときにログ メッセージを生成するには、[Give only warning message when prefix limit is exceeded] をクリックします。この場合、BGP ネイバーは終了しません。

ステップ 17　左側のペインで、[Routes] をクリックします。

ステップ 18　[Advertisement Interval] フィールドに、BGP ルーティング アップデートが送信される最小間隔（秒）を入力します。

ステップ 19　（オプション）[Generate Default route] チェックボックスをオンにして、ローカル ルータにネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。

- [Route map] ドロップダウン リストから、ルート 0.0.0.0 が条件に応じて注入されるように許可するルート マップを選択します。[Manage] をクリックして、ルート マップを追加および設定します。

ステップ 20　（オプション）条件に応じてアドバタイズされるルートを追加するには、次の手順を実行します。

a.　[Conditionally Advertised Routes] セクションで [Add] をクリックします。

b.　exist-map または non-exist-map の条件に一致した場合にアドバタイズされるルート マップを [Advertise Map] ドロップダウン リストから選択します。

c.　次のどちらかを実行します。

- [Exist Map] をクリックしてルート マップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。
- [Non-exist Map] をクリックしてルート マップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。

d.　[Ok] をクリックします。

ステップ 21　（オプション）[Remove private autonomous system (AS) numbers from outbound routing updates] チェックボックスをオンにし、プライベート AS 番号を発信ルートにおけるアドバイタイズ対象から除外します。

ステップ 22　左側のペインで、[Timers] をクリックします。

ステップ 23　（オプション）[Set timers for the BGP peer] チェックボックスをオンにし、キープアライブ頻度、保持時間、最小保持時間を設定します。

- ASA がキープアライブ メッセージをネイバーに送信する頻度（秒）を [Keepalive frequency] フィールドに入力します。有効な値は、0 ～ 65535 です。デフォルト値は 60 秒です。

- [Hold time] フィールドに、キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの時間（秒）を入力します。デフォルト値は 180 秒です。
- （オプション）[Min Hold time] フィールドに、キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの最小時間（秒）を入力します。

ステップ 24　左側のペインで、[Advanced] をクリックします。

ステップ 25　（オプション）[Enable Authentication] チェックボックスをオンにして、2 つの BGP ピア間の TCP 接続で MD5 認証をイネーブルにします。

- [Encryption Type] ドロップダウン リストから暗号化タイプを選択します。
- パスワードを [Password] フィールドに入力します。[Confirm Password] フィールドに、パスワードを再入力します。

（注）　パスワードは大文字と小文字を区別し、**service password-encryption** コマンドがイネーブルな場合は最大 25 文字、**service password-encryption** コマンドがイネーブルではない場合は最大 81 文字指定できます。最初の文字を数値にはできません。この文字列には、スペースも含め、あらゆる英数字を使用できます。数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

ステップ 26　（オプション）[Send Community Attribute to this neighbor] チェックボックスをオンにします。

ステップ 27　（オプション）[Use ASA as next hop for neighbor] チェックボックスをオンにし、ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。

ステップ 28　次のどちらかを実行します。

- [Allow connections with neighbor that is not directly connected] をクリックして、直接接続されていないネットワーク上で外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。
  - （オプション）[TTL hops] フィールドに存続可能時間を入力します。有効な値は、1 ～ 255 です。
  - （オプション）[Disable connection verification] チェックボックスをオンにし、ループバック インターフェイスを使用するシングル ホップ ピアと eBGP ピアリング セッションを確立するための接続確認をディセーブルにします。
- [Limit number of TTL hops to neighbor] をクリックして、BGP ピアリング セッションを保護できるようにします。
  - [TTL hops] フィールドに、eBGP ピアを区切るホップの最大数を入力します。有効な値は、1 ～ 254 です。

ステップ 29　（オプション）[Weight] フィールドに BGP ネイバー接続の重みを入力します。

ステップ 30　[BGP version] ドロップダウン リストから、ASA が受け入れる BGP バージョンを選択します。

（注）　バージョンを 2 に設定すると、指定されたネイバーとの間でバージョン 2 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。

ステップ 31　（オプション）[TCP Path MTU Discovery] チェックボックスをオンにして、BGP セッションの TCP トランスポート セッションをイネーブルにします。

ステップ 32　[TCP transport mode] ドロップダウン リストから TCP 接続モードを選択します。

ステップ 33　左側のペインで、[Migration] をクリックします。

ステップ 34　（オプション）[Customize the AS number for routes received from the neighbor] チェックボックスをオンにして、eBGP ネイバーから受信したルートの AS_path 属性をカスタマイズします。

- [Local AS Number] フィールドにローカル自律システム番号を入力します。有効な値は、1 ～ 65535 です。
- （オプション）[Do not prepend local AS number for routes received from neighbor] チェックボックスをオンにします。ローカル AS 番号は、eBGP ピアから受信したルートの前に追加されません。
- （オプション）[Replace real AS number with local AS number in routes received from neighbor] チェックボックスをオンにします。ローカル ルーティング プロセスの AS 番号は前に追加されません。
- （オプション）[Accept either real AS number or local AS number in routes received from neighbor] チェックボックスをオンにします。

ステップ 35　[OK] をクリックします。

ステップ 36　[Apply] をクリックします。

IPv4 ネットワークの設定

ここでは、BGP ルーティング プロセスによってアドバタイズされるネットワークを定義するために必要な手順について説明します。

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] の順に選択します。

ステップ 2　[Networks] をクリックします。

[Define networks to be advertised by the BGP routing process] 設定ペインが表示されます。

ステップ 3　[Add] をクリックします。

[Add Network] ペインが表示されます。

ステップ 4　[Address] フィールドで BGP がアドバタイズするネットワークを指定します。

ステップ 5　（オプション）[Netmask] ドロップダウン リストからネットワーク マスクまたはサブネットワーク マスクを選択します。

ステップ 6　[Route Map] ドロップダウン リストから、アドバタイズされるネットワークをフィルタリングするために調べる必要のあるルート マップを選択します。[Manage] をクリックして、ルート マップを設定または追加します。

ステップ 7　[OK] をクリックします。

ステップ 8　[Apply] をクリックします。

再配布の設定

ここでは、別のルーティング ドメインから BGP にルートを再配布する条件を定義するために必要な手順について説明します。

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] の順に選択します。

ステップ 2　[Redistribution] をクリックします。

[Redistribution] ペインが表示されます。

ステップ 3　[Add] をクリックします。

[Add Redistribution] ペインが表示されます。

ステップ 4　[Source Protocol] ドロップダウンリストから、どのプロトコルからルートを BGP ドメインに再配布するかを選択します。

ステップ 5　[Process ID] ドロップダウン リストからソース プロトコルのプロセス ID を選択します。

ステップ 6　（オプション）[Metric] フィールドに、再配布されるルートのメトリックを入力します。

ステップ 7　[Route Map] ドロップダウン リストから、再配布されるネットワークをフィルタリングするために調べる必要のあるルート マップを選択します。[Manage] をクリックして、ルート マップを設定または追加します。

ステップ 8　[Internal]、[External]、および [NSSA External Match] チェックボックスのうち 1 つ以上をオンにして、OSPF ネットワークからルートを再配布します。

（注）　この手順は、OSPF ネットワークからの再配布にのみ適用できます。

ステップ 9　[OK] をクリックします。

ステップ 10　[Apply] をクリックします。

ルート注入の設定

ここでは、条件に応じて BGP ルーティング テーブルに注入されるルートを定義するために必要な手順について説明します。

手順

ステップ 1　ASDM で、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] の順に選択します。

ステップ 2　[Route Injection] をクリックします。

[Route Injection] ペインが表示されます。

ステップ 3　[Add] をクリックします。

[Add Conditionally injected route] ペインが表示されます。

ステップ 4　[Inject Map] ドロップダウン リストから、ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップを選択します。

ステップ 5　[Exist Map] ドロップダウン リストから、BGP スピーカーが追跡するプレフィックスを含むルート マップを選択します。

ステップ 6　[Injected routes will inherit the attributes of the aggregate route] チェックボックスをオンにし、集約ルートの属性を継承するよう注入されたルートを設定します。

ステップ 7　[OK] をクリックします。

ステップ 8　[Apply] をクリックします。

BGP のモニタリング

次のコマンドを使用して、BGP ルーティング プロセスをモニタできます。コマンド出力の例と説明については、コマンド リファレンスを参照してください。また、ネイバー変更メッセージとネイバー警告メッセージのロギングをディセーブルにできます。

さまざまな BGP ルーティング統計情報をモニタするには、次の手順を実行します。

（注）　BGP ログ メッセージをディセーブルにするには、ルータ コンフィギュレーション モードで **no bgp log-neighbor-changes** コマンドを入力します。これにより、ネイバー変更メッセージのロギングがディセーブルになります。BGP ルーティング プロセスのルータ コンフィギュレーション モードでこのコマンドを入力します。
デフォルトでは、ネイバーの変更はロギングされます。

- [Monitoring] > [Routing] > [BGP Neighbors]

  各行は 1 つの BGP ネイバーを表します。リストには、ネイバーごとに、IP アドレス、AS 番号、ルータ ID、状態（アクティブ、アイドルなど）、稼働時間、グレースフル リスタート機能、再起動時間、stalepath 時間が含まれます。

- [Monitoring] > [Routing] > [BGP Routes]

  各行は 1 つの BGP ルートを表します。リストには、ルートごとに、ステータス コード、IP アドレス、ネクスト ホップ アドレス、ルート メトリック、Local preference 値、重み、パスが含まれます。

BGP の履歴

表 22-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 22-1　BGP 機能の履歴

機能名	プラットフォーム リリース	機能情報
BGP のサポート	9.2(1)	Border Gateway Protocol を使用した、データのルーティング、認証の実行、およびルーティング情報の再配布とモニタについて、サポートが追加されました。 次の ASDM 画面が導入されました。 [Configuration] > [Device Setup] > [Routing] > [BGP] [Monitoring] > [Routing] > [BGP Neighbors]、[Monitoring] > [Routing] > [BGP Routes] 次の ASDM 画面が変更されました。 [Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add] > [Add Static Route] [Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Add] > [Add Route Map]
ASA クラスタリングに対する BGP のサポート	9.3(1)	L2 および L3 クラスタリングのサポートが追加されました。 次の ASDM 画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [General]
ノンストップ フォワーディングに対する BGP のサポート	9.3(1)	ノンストップ フォワーディングのサポートが追加されました。 次の ASDM 画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [General]、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [Neighbor]、[Monitoring] > [Routing] > [BGP Neighbors]
アドバタイズされたマップに対する BGP のサポート	9.3(1)	アドバタイズされたマップに対する BGPv4 のサポートが追加されました。 次の ASDM 画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [Neighbor] > [Add BGP Neighbor] > [Routes]

OSPF

この章では、Open Shortest Path First（OSPF）ルーティング プロトコルを使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Cisco ASA を設定する方法について説明します。

この章は、次の項目を取り上げます。

OSPF について

OSPF は、パスの選択に距離ベクトル型ではなくリンク ステートを使用する Interior Gateway Routing Protocol（IGRP）です。OSPF は、ルーティング テーブル アップデートではなく、リンクステート アドバタイズメントを伝搬します。ルーティング テーブル全体ではなく LSA だけが交換されるため、OSPF ネットワークは RIP ネットワークよりも迅速に収束します。

OSPF は、リンクステート アルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

RIP に比べると OSPF は次の点で有利です。

- OSPF のリンクステート データベースのアップデート送信は RIP ほど頻繁ではありません。また、古くなった情報がタイムアウトしたときに、リンクステート データベースは徐々にアップデートされるのではなく、瞬時にアップデートされます。

- ルーティング決定はコストに基づいて行われます。これは、特定のインターフェイスを介してパケットを送信するためにオーバーヘッドが必要であることを示しています。ASA は、インターフェイスのコストをリンク帯域幅に基づいて計算し、宛先までのホップ数は使用しません。コストは優先パスを指定するために設定できます。

最短パス優先アルゴリズムの欠点は、CPU サイクルとメモリが大量に必要になることです。

ASA は、OSPF プロトコルのプロセス 2 つを異なるインターフェイス セット上で同時に実行できます。同じ IP アドレスを使用する複数のインターフェイス（NAT ではこのようなインターフェイスは共存可能ですが、OSPF ではアドレスの重複は許しません）があるときに、2 つのプロセスを実行する場合があります。あるいは、一方のプロセスを内部で実行しながら別のプロセスを外部で実行し、ルートのサブセットをこの 2 つのプロセス間で再配布する場合もあります。同様に、プライベート アドレスをパブリック アドレスから分離する必要がある場合もあります。

OSPF ルーティング プロセスには、別の OSPF ルーティング プロセスや RIP ルーティング プロセスから、または OSPF 対応インターフェイスに設定されているスタティック ルートおよび接続されているルートから、ルートを再配布できます。

ASA では、次の OSPF の機能がサポートされています。

- エリア内ルート、エリア間ルート、および外部ルート（タイプ I とタイプ II）。
- 仮想リンク。
- LSA フラッディング。
- OSPF パケットの認証（パスワード認証と MD5 認証の両方）。
- ASA の指定ルータまたは指定バックアップ ルータとしての設定。ASA は、ABR として設定することもできます。
- スタブ エリアと not so stubby エリア。
- エリア境界ルータのタイプ 3 LSA フィルタリング。

OSPF は、MD5 とクリア テキスト ネイバー認証をサポートしています。OSPF と他のプロトコル（RIP など）の間のルート再配布は、攻撃者によるルーティング情報の悪用に使用される可能性があるため、できる限りすべてのルーティング プロトコルで認証を使用する必要があります。

NAT が使用されている場合、OSPF がパブリック エリアおよびプライベート エリアで動作している場合、またアドレス フィルタリングが必要な場合は、2 つの OSPF プロセス（1 つはパブリック エリア用、1 つはプライベート エリア用）を実行する必要があります。

複数のエリアにインターフェイスを持つルータは、エリア境界ルータ（ABR）と呼ばれます。ゲートウェイとして動作し、OSPF を使用しているルータと他のルーティング プロトコルを使用しているルータの間でトラフィックを再配布するルータは、自律システム境界ルータ（ASBR）と呼ばれます。

ABR は LSA を使用して、使用可能なルータに関する情報を他の OSPF ルータに送信します。ABR タイプ 3 LSA フィルタリングを使用すると、ABR として機能する ASA を使用して、プライベート エリアとパブリック エリアを分けることができます。エリア間で Type 3 LSA（エリア間ルート）をフィルタリングできるため、プライベート ネットワークをアドバタイズすることなく NAT と OSPF を併用できます。

（注） フィルタリングできるのはタイプ 3 LSA だけです。プライベート ネットワーク内の ASBR として設定されている ASA は、プライベート ネットワークを記述するタイプ 5 LSA を送信しますが、これは AS 全体（パブリック エリアも含む）にフラッディングされます。

NAT が採用されているが、OSPF がパブリック エリアだけで実行されている場合は、パブリック ネットワークに対するルートを、デフォルトまたはタイプ 5 AS 外部 LSA としてプライベート ネットワーク内で再配布できます。ただし、ASA により保護されているプライベート ネットワークにはスタティック ルートを設定する必要があります。また、同一の ASA インターフェイス上で、パブリック ネットワークとプライベート ネットワークを混在させることはできません。

ASA では、2 つの OSPF ルーティング プロセス（1 つの RIP ルーティング プロセスと 1 つの EIGRP ルーティング プロセス）を同時に実行できます。

fast hello パケットに対する OSPF のサポート

fast hello パケットに対する OSPF のサポートには、1 秒未満のインターバルで hello パケットの送信を設定する方法が用意されています。このような設定により、Open Shortest Path First（OSPF）ネットワークでの統合がより迅速になります。

fast hello パケットに対する OSPF のサポートの前提条件

OSPF がネットワークですでに設定されているか、fast hello パケットに対する OSPF のサポートと同時に設定される必要があります。

fast hello パケットに対する OSPF のサポートについて

ここでは、fast hello パケットに対する OSPF のサポートに関連する概念について説明します。

- OSPF hello インターバルおよびデッド インターバル
- OSPF fast hello パケット
- OSPF fast hello パケットの利点

OSPF hello インターバルおよびデッド インターバル

OSPF hello パケットとは、OSPF プロセスがネイバーとの接続を維持するために OSPF ネイバーに送信するパケットです。hello パケットは、設定可能なインターバル（秒単位）で送信されます。デフォルトのインターバルは、イーサネット リンクの場合 10 秒、ブロードキャスト以外のリンクの場合 30 秒です。hello パケットには、デッド インターバル中に受信したすべてのネイバーのリストが含まれます。デッド インターバルも設定可能なインターバル（秒単位）で送信されます。デフォルトは hello インターバルの値の 4 倍です。hello インターバルの値は、ネットワーク内ですべて同一にする必要があります。デッド インターバルの値も、ネットワーク内ですべて同一にする必要があります。

この 2 つのインターバルは、リンクが動作していることを示すことにより、接続を維持するために連携して機能します。ルータがデッド インターバル内にネイバーから hello パケットを受信しない場合、ルータはこのネイバーがダウンしていると判定します。

OSPF fast hello パケット

OSPF fast hello パケットとは、1 秒よりも短いインターバルで送信される hello パケットのことです。fast hello パケットを理解するには、OSPF hello パケット インターバルとデッド インターバルとの関係についてあらかじめ理解しておく必要があります。「OSPF hello インターバルおよびデッド インターバル」（P.23-3）を参照してください。

OSPF fast hello パケットは、**ospf dead-interval** コマンドで設定されます。デッド インターバルは 1 秒に設定され、hello-multiplier の値は、その 1 秒間に送信する hello パケット数に設定されるため、1 秒未満の「fast」hello パケットになります。

インターフェイスで fast hello パケットが設定されている場合、このインターフェイスから送出される hello パケットでアドバタイズされる hello 間隔は 0 に設定されます。このインターフェイス経由で受信した hello パケットの hello 間隔は無視されます。

デッド インターバルは、1 つのセグメント上で一貫している必要があり、1 秒に設定するか（fast hello パケットの場合）、他の任意の値を設定します。デッド インターバル内に少なくとも 1 つの hello パケットが送信される限り、hello multiplier がセグメント全体で同じである必要はありません。

OSPF fast hello パケットの利点

OSPF fast hello パケット機能を利用すると、ネットワークがこの機能を使用しない場合よりも、短い時間で統合されます。この機能によって、失われたネイバーを 1 秒以内に検出できるようになります。この機能は、ネイバーの損失が Open System Interconnection（OSI）物理層またはデータ リンク層で検出されないことがあっても、特に LAN セグメントで有効です。

OSPFv2 および OSPFv3 間の実装の差異

OSPFv3 には、OSPFv2 との下位互換性はありません。OSPF を使用して、IPv4 および IPv6 トラフィックの両方をルーティングするには、OSPFv2 および OSPFv3 の両方を同時に実行する必要があります。これらは互いに共存しますが、相互に連携していません。

OSPFv3 では、次の追加機能が提供されます。

- リンクごとのプロトコル処理。
- アドレッシング セマンティックの削除。
- フラッディング スコープの追加。
- リンクごとの複数インスタンスのサポート。
- ネイバー探索およびその他の機能に対する IPv6 リンクローカル アドレスの使用。
- プレフィックスおよびプレフィックス長として表される LSA。
- 2 つの LSA タイプの追加。
- 未知の LSA タイプの処理。
- RFC-4552 で指定されている OSPFv3 ルーティング プロトコル トラフィックの IPsec ESP 標準を使用する認証サポート。

OSPF のガイドライン

コンテキスト モードのガイドライン

OSPFv2 は、シングル コンテキスト モードとマルチ コンテキスト モードをサポートしています。

OSPFv3 は、シングル モードのみをサポートしています。

ファイアウォール モードのガイドライン

OSPF は、ルーテッド ファイアウォール モードのみをサポートしています。OSPF は、トランスペアレント ファイアウォール モードをサポートしません。

フェールオーバーのガイドライン

OSPFv2 および OSPFv3 は、ステートフル フェールオーバーをサポートしています。

IPv6 のガイドライン

- OSPFv2 は IPv6 をサポートしません。
- OSPFv3 は IPv6 をサポートしています。
- OSPFv3 は、IPv6 を使用して認証を行います。
- ASA は、OSPFv3 ルートが最適なルートの場合、IPv6 RIB にこのルートをインストールします。
- OSPFv3 パケットは、**capture** コマンドの IPv6 ACL を使用してフィルタリングで除外できます。

クラスタリングのガイドライン

- OSPFv2 および OSPFv3 は、クラスタリングをサポートします。
- OSPFv3 暗号化はサポートされていません。クラスタリング環境で OSPFv3 暗号化を設定しようとすると、エラー メッセージが表示されます。
- スパンド インターフェイス モードでは、ダイナミック ルーティングは管理専用インターフェイスでサポートされていません。
- 個別インターフェイス モードで、OSPFv2 または OSPFv3 ネイバーとしてマスター ユニットおよびスレーブ ユニットが確立されていることを確認します。
- OSPFv2 と EIGRP の両方を設定すると、スパンド インターフェイス モードまたは個別インターフェイス モードのいずれかを使用できますが、2 つのモードを同時に使用することはできません。
- 個別インターフェイス モードでは、OSPFv2 との隣接関係は、マスター ユニットの共有インターフェイスの 2 つのコンテキスト間でのみ確立できます。スタティック ネイバーの設定は、ポイントツーポイン リンクでのみサポートされます。したがって、インターフェイスで許可されるのは 1 つのネイバー ステートメントだけです。
- ルータ ID は、OSPFv2、OSPFv3、および EIGRP ルータ コンフィギュレーション モードでオプションです。ルータ ID を明示的に設定しない場合、ルータ ID は自動的に生成され、各クラスタ ユニットのデータ インターフェイスにおける最大の IPv4 アドレスに設定されます。
- クラスタ インターフェイス モードが設定されていない場合は、ルータ ID として単一のドット付き 10 進数の IPv4 アドレスだけが許可され、**cluster pool** オプションはディセーブルになります。
- クラスタ インターフェイス モードがスパンド コンフィギュレーションに設定されている場合は、ルータ ID として単一のドット付き 10 進数の IPv4 アドレスだけが許可され、**cluster pool** オプションはディセーブルになります。
- クラスタ インターフェイス モードが個々のコンフィギュレーションに設定されている場合、**cluster pool** オプションは必須となり、単一の、ドット付き 10 進数の IPv4 アドレスがルータ ID として許可されません
- **check-detail** または **nocheck** オプションを指定せずに、クラスタ インターフェイス モードをスパンド コンフィギュレーションから個々のコンフィギュレーション（またはその逆）に変更すると、ルータ ID を含むコンフィギュレーション全体が削除されます。

- 新しいインターフェイス モードと互換性のないダイナミック ルーティング プロトコルのルータ ID がある場合は、コンソールにエラー メッセージが表示され、インターフェイス モード CLI は失敗します。エラー メッセージには、ダイナミック ルーティング プロトコル（OSPFv2、OSPFv3 および EIGRP）ごとに 1 行があり、互換性のない設定が発生した各コンテキストの名前がリストされます。
- **nocheck** オプションが **cluster interface mode** コマンドに指定されている場合は、インターフェイス モードを変更できます。ただし、すべてのルータ ID の設定に新しいモードとの互換性があるとは限りません。
- クラスタがイネーブルの場合、ルータ ID の互換性チェックが繰り返されます。非互換性が検出された場合、**cluster enable** コマンドは失敗します。管理者は、クラスタをイネーブルにする前に互換性のないルータ ID コンフィギュレーションを修正する必要があります。
- ユニットがスレーブとしてクラスタに参加する場合は、ルータ ID の互換性チェックが失敗しないように、**cluster interface mode** コマンドの **nocheck** オプションを指定することを推奨します。スレーブ ユニットは、マスター ユニットのルータ コンフィギュレーションを継承します。
- クラスタでマスターシップ ロールの変更が発生した場合、次の動作が発生します。
  - スパンド インターフェイス モードでは、ルータ プロセスはマスター ユニットでのみアクティブになり、スレーブ ユニットでは停止状態になります。コンフィギュレーションがマスター ユニットと同期されているため、各クラスタ ユニットには同じルータ ID があります。その結果、隣接ルータはロール変更時のクラスタのルータ ID の変更を認識しません。
  - 個別インターフェイス モードでは、ルータ プロセスはすべての個別のクラスタ ユニットでアクティブになります。各クラスタ ユニットは設定されたクラスタ プールから独自の個別のルータ ID を選択します。クラスタでマスターシップ ロールが変更されても、ルーティング トポロジは変更されません。

その他のガイドライン

- OSPFv2 および OSPFv3 は 1 つのインターフェイス上での複数インスタンスをサポートしています。
- OSPFv3 は、非クラスタ環境での ESP ヘッダーを介した暗号化をサポートしています。
- OSPFv3 は非ペイロード暗号化をサポートします。
- OSPFv2 は RFC 4811、4812 および 3623 でそれぞれ定義されている、Cisco NSF グレースフル リスタートおよび IETF NSF グレースフル リスタート メカニズムをサポートします。
- OSPFv3 は RFC 5187 で定義されているグレースフル リスタート メカニズムをサポートします。

OSPFv2 の設定

ここでは、ASA で OSPFv2 プロセスをイネーブルにする方法について説明します。

OSPFv2 をイネーブルにした後、ルート マップを定義する必要があります。詳細については、「ルート マップの定義」（P.21-4）を参照してください。その後、デフォルト ルートを生成します。詳細については、「スタティック ルートの設定」（P.20-2）を参照してください。

OSPFv2 プロセスのルート マップを定義した後で、ニーズに合わせてカスタマイズできます。ASA 上で OSPFv2 プロセスをカスタマイズする方法については、「OSPFv2 のカスタマイズ」（P.23-8）を参照してください。

OSPFv2 をイネーブルにするには、OSPFv2 ルーティング プロセスを作成し、このルーティング プロセスに関連付ける IP アドレスの範囲を指定し、さらにその IP アドレスの範囲にエリア ID を割り当てる必要があります。

最大 2 つの OSPFv2 プロセス インスタンスをイネーブルにできます。各 OSPFv2 プロセスには、独自のエリアとネットワークが関連付けられます。

OSPFv2 をイネーブルにするには、次の手順を実行します。

手順

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択します。

[OSPF Setup] ペインでは、OSPF プロセスのイネーブル化、OSPF エリアおよびネットワークの設定、および OSPF ルート集約の定義を行うことができます。

ステップ 2　ASDM で OSPF をイネーブルにするには、次の 3 つのタブを使用します。

- [Process Instances] タブでは、各コンテキストに対して最大 2 つの OSPF プロセス インスタンスをイネーブルにできます。シングル コンテキスト モードおよびマルチ コンテキスト モードの両方がサポートされます。[Enable Each OSPF Process] チェックボックスをオンにすると、その OSPF プロセスの固有識別子である数値識別子を入力できるようになります。このプロセス ID は内部的に使用されるものであり、他の OSPF デバイスでの OSPF プロセス ID と一致している必要はありません。有効な値の範囲は 1 ～ 65535 です。各 OSPF プロセスには、独自のエリアとネットワークが関連付けられます。

  [Advanced] をクリックすると、[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。ここで、各 OSPF プロセスに対して、[Router ID]、スパンド EtherChannel または個別インターフェイス クラスタリングのクラスタ IP アドレス プール、[Adjacency Changes]、[Administrative Route Distances]、[Timers] および [Default Information Originate] を設定することができます。

- [Area/Networks] タブでは、ASA 上で各 OSPF プロセスに対して指定されているエリアとネットワークが表示されます。このタブからは、エリア ID、エリア タイプ、およびそのエリアに対して設定された認証のタイプを表示できます。OSPF のエリアまたはネットワークを追加または編集する方法については、「OSPFv2 エリア パラメータの設定」（P.23-16）を参照してください。

- [Route Summarization] タブでは、ABR を設定できます。OSPF では、ABR が 1 つのエリアのネットワークを別のエリアにアドバタイズします。1 つのエリア内のネットワーク番号が連続するように割り当てられている場合は、サマリー ルートをアドバタイズするように ABR を設定できます。このサマリー ルートには、そのエリア内の個々のネットワークのうち、指定の範囲に当てはまるものがすべて含まれます。詳細については、「OSPFv2 エリア間のルート集約の設定」（P.23-12）を参照してください。

OSPF fast hello パケットの設定

ここでは、OSPF fast hello パケットを設定する方法について説明します。

手順

OSPFv2 のカスタマイズ

ここでは、OSPFv2 プロセスをカスタマイズする方法について説明します。

OSPFv2 へのルートの再配布

ASA は、OSPFv2 ルーティング プロセス間のルート再配布を制御できます。

（注） 指定されたルーティング プロトコルから、ターゲット ルーティング プロセスに再配布できるルートを定義することでルートを再配布する場合は、デフォルト ルートを最初に生成する必要があります。「スタティック ルートの設定」（P.20-2）を参照し、その後に「ルート マップの定義」（P.21-4）に従ってルート マップを定義します。

スタティック ルート、接続されているルート、RIP ルート、または OSPFv2 ルートを OSPFv2 プロセスに再配布するには、次の手順を実行します。

手順

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Redistribution] の順に選択します。

[Redistribution] ペインには、1 つのルーティング プロセスから OSPF ルーティング プロセスへのルートを再配布する場合のルールが表示されます。RIP および OSPF で検出されたルートを、EIGRP ルーティング プロセスに再配布することができます。スタティック ルートおよび接続

されているルートも、EIGRP ルーティング プロセスに再配布できます。スタティックまたは接続されているルートが、[Setup] > [Networks] タブで設定されたネットワークの範囲内にある場合は、そのルートを再配布する必要はありません。

ステップ 2　[Add] または [Edit] をクリックします。

または、[Redistribution] ペインでテーブル エントリ（ある場合）をダブルクリックすると、そのエントリの [Add/Edit OSPF Redistribution Entry] ダイアログボックスが開きます。

（注）　以降のステップはすべて、省略可能です。

[Add/Edit OSPF Redistribution Entry] ダイアログボックスでは、[Redistribution] テーブルに新しい再配布ルールを追加することや、既存の再配布ルールを編集することができます。既存の再配布ルールを編集するとき、一部の再配布ルール情報は変更できません。

ステップ 3　ルート再配布エントリに関連付ける OSPF プロセスを選択します。既存の再配布ルールを編集している場合、この設定は変更できません。

ステップ 4　どのソース プロトコルからルートを再配布するかを選択します。次のいずれかのオプションを選択できます。

- [Static]：スタティック ルートを OSPF ルーティング プロセスに再配布します。
- [Connected]：接続されたルート（インターフェイス上で IP アドレスをイネーブルにすることによって自動的に確立されるルート）を OSPF ルーティング プロセスに再配布します。接続済みルートは、AS の外部として再配布されます。
- [OSPF]：別の OSPF ルーティング プロセスからのルートを再配布します。リストから OSPF プロセス ID を選択してください。このプロトコルを選択すると、このダイアログボックスの [Match] のオプションが表示されます。これらのオプションは、スタティック、接続済み、RIP、または EIGRP ルートを再配布するときに選択できます。ステップ 5 に進みます。
- [RIP]：RIP ルーティング プロセスからルートを再配布します。
- [BGP]：BGP ルーティング プロセスからルートを再配布します。
- [EIGRP]：EIGRP ルーティング プロセスからルートを再配布します。リストから EIGRP ルーティング プロセスの自律システム番号を選択してください。

ステップ 5　OSPF をソース プロトコルとして選択した場合は、選択した OSPF ルーティング プロセスに別の OSPF ルーティング プロセスからのルートを再配布するのに使用される条件を選択します。これらのオプションは、スタティック、接続済み、RIP、または EIGRP ルートを再配布するときに選択できます。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。

- [Internal]：ルートは特定の AS の内部です。
- [External 1]：自律システムの外部だが、OSPF にタイプ 1 外部ルートとしてインポートされるルート。
- [External 2]：自律システムの外部だが、OSPF にタイプ 2 外部ルートとしてインポートされるルート。
- [NSSA External 1]：自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。
- [NSSA External 2]：自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。

ステップ 6　[Metric Value] フィールドに、再配布されるルーティングのメトリック値を入力します。有効値の範囲は 1 ～ 16777214 です。

同じデバイス上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。

ステップ 7　[Metric Type] で、次のオプションのいずれかを選択します。

- メトリックがタイプ 1 外部ルートの場合は、[**1**] を選択します。
- メトリックがタイプ 2 外部ルートの場合は、[**2**] を選択します。

ステップ 8　タグ値を [Tag Value] フィールドに入力します。

タグ値は 32 ビット 10 進数値です。この値は、OSPF 自身では使用されないが ASBR 間の情報伝達に使用できる外部ルートのそれぞれに関連付けられます。有効値の範囲は、0 ～ 4294967295 です。

ステップ 9　[Use Subnets] チェックボックスをオンにすると、サブネット化ルートの再配布がイネーブルになります。サブネットされていないルートだけを再配布するには、このチェックボックスをオフにします。

ステップ 10　再配布エントリに適用するルート マップの名前を [Route Map] ドロップダウン リストで選択します。

ステップ 11　ルート マップを追加または設定するには、[Manage] をクリックします。

[Configure Route Map] ダイアログボックスが表示されます。

ステップ 12　[Add] または [Edit] をクリックしてから、指定したルーティング プロトコルからのルートのうち、どれをターゲットのルーティング プロセスに再配布するかを定義します。詳細については、「ルート マップの定義」（P.21-4）を参照してください。

ステップ 13　[OK] をクリックします。

OSPFv2 にルートを再配布する場合のルート集約の設定

他のプロトコルからのルートを OSPF に再配布する場合、各ルートは外部 LSA で個別にアドバタイズされます。ただし、再配布されるルートのうち、指定のネットワーク アドレスとマスクに含まれるすべてのものを 1 つのルートで表し、そのルートだけをアドバタイズするように ASA を設定することができます。この設定によって OSPF リンクステート データベースのサイズが小さくなります。

指定した IP アドレス マスク ペアと一致するルートは廃止できます。ルート マップで再配布を制御するために、タグ値を一致値として使用できます。

ルート集約を設定するには、次のことができます。

- 「ルート サマリー アドレスの追加」（P.23-10）
- 「OSPF サマリー アドレスの追加または編集」（P.23-11）

ルート サマリー アドレスの追加

[Summary Address] ペインには、各 OSPF ルーティング プロセスに設定されたサマリー アドレスに関する情報が表示されます。

他のルーティング プロトコルから学習したルートをサマライズできます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。サマリー ルートは、ルーティング テーブルのサイズを削減するのに役立ちます。

OSPF のサマリー ルートを使用すると、OSPF ASBR は、そのアドレスでカバーされるすべての再配布ルートの集約として、1 つの外部ルートをアドバタイズします。OSPF に再配布されている、他のルーティング プロトコルからのルートだけをサマライズできます。

（注） OSPF は summary-address 0.0.0.0 0.0.0.0 をサポートしません。

ネットワーク アドレスとマスクに含まれる再配布ルートすべてに対して 1 つのサマリー ルートをアドバタイズするようにソフトウェアを設定するには、次の手順を実行します。

手順

ステップ 1　メインの ASDM ホーム ページで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Summary Address] を選択します。

ステップ 2　[Add] をクリックします。

[Add OSPF Summary Address Entry] ダイアログボックスが表示されます。[Summary Address] テーブルの既存のエントリに新しいエントリを追加できます。既存のエントリを編集するとき、一部のサマリー アドレス情報は変更できません。

ステップ 3　[OSPF Process] ドロップダウン リストから、サマリー アドレスに関連付けられた指定 OSPF プロセス ID を選択します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 4　[IP Address] フィールドにサマリー アドレスの IP アドレスを入力します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 5　サマリー アドレスのネットワーク マスクを [Netmask] ドロップダウン リストから選択します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 6　[Advertise] チェックボックスをオンにして、サマリー ルートをアドバタイズします。サマリー アドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェックボックスはオンになっています。

[Tag value] に表示される値は、各外部ルートに付加される 32 ビットの 10 進数値です。この値は OSPF 自身には使用されませんが、ASBR 間の情報伝達に使用できます。

ステップ 7　[OK] をクリックします。

OSPF サマリー アドレスの追加または編集

手順

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択します。

ステップ 2　[Route Summarization] タブをクリックします。

[Add/Edit Route Summarization Entry] ダイアログボックスが表示されます。

[Add/Edit Route Summarization Entry] ダイアログボックスでは、[Summary Address] テーブルに新しいエントリを追加したり、[Summary Address] テーブルの既存のエントリを変更したりできます。既存のエントリを編集するとき、一部のサマリー アドレス情報は変更できません。

ステップ 3　[OSPF Process] ドロップダウン リストから、サマリー アドレスに関連付けられた指定 OSPF プロセス ID を選択します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 4　[IP Address] フィールドにサマリー アドレスの IP アドレスを入力します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 5　サマリー アドレスのネットワーク マスクを [Netmask] ドロップダウン リストから入力します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 6　[Advertise] チェックボックスをオンにして、サマリー ルートをアドバタイズします。サマリー アドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェックボックスはオンになっています。

OSPFv2 エリア間のルート集約の設定

ルート集約は、アドバタイズされるアドレスを統合することです。この機能を実行すると、1 つのサマリー ルートがエリア境界ルータを通して他のエリアにアドバタイズされます。OSPF のエリア境界ルータは、ネットワークをある 1 つのエリアから別のエリアへとアドバタイズしていきます。あるエリアにおいて連続する複数のネットワーク番号が割り当てられている場合、指定された範囲に含まれるエリア内の個別のネットワークをすべて含むサマリー ルートをアドバタイズするようにエリア境界ルータを設定することができます。

ルート集約のアドレス範囲を定義するには、次の手順を実行します。

手順

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択します。

ステップ 2　[Route Summarization] タブをクリックします。

[Add/Edit Route Summarization Entry] ダイアログボックスが表示されます。

[Add/Edit Route Summarization Entry] ダイアログボックスでは、[Summary Address] テーブルに新しいエントリを追加したり、[Summary Address] テーブルの既存のエントリを変更したりできます。既存のエントリを編集するとき、一部のサマリー アドレス情報は変更できません。

ステップ 3　OSPF エリア ID を [Area ID] フィールドに入力します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 4　[IP Address] フィールドにサマリー アドレスの IP アドレスを入力します。既存のエントリを編集する場合、この情報は変更できません。

OSPFv2 インターフェイス パラメータの設定

必要に応じて一部のインターフェイス固有の OSPFv2 パラメータを変更できます。これらのパラメータは必ずしも変更する必要はありませんが、hello インターバル、デッド インターバル、認証キーの各インターフェイス パラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

OSPFv2 インターフェイス パラメータを設定するには、次の手順を実行します。

手順

ASDM では、[Interface] ペインでインターフェイス固有の OSPF ルーティング プロパティ（たとえば OSPF メッセージ認証やプロパティ）を設定できます。OSPF のインターフェイスを設定するためのタブは次の 2 つです。

- [Authentication] タブには、ASA インターフェイスの OSPF 認証情報が表示されます。
- [Properties] タブには、各インターフェイスに定義された OSPF プロパティがテーブル形式で表示されます。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Interface] の順に選択します。

ステップ 2　[Authentication] タブをクリックすると、ASA のインターフェイスの認証情報が表示されます。このテーブルの行をダブルクリックすると、選択したインターフェイスの [Edit OSPF Authentication Interface] ダイアログボックスが開きます。

ステップ 3　[Edit] をクリックします。

[Edit OSPF Authentication Interface] ダイアログボックスが表示されます。[Edit OSPF Interface Authentication] ダイアログボックスでは、選択したインターフェイスの OSPF 認証タイプおよびパラメータを設定できます。

ステップ 4　認証タイプを [Authentication] ドロップダウン リストから選択します。次の選択肢があります。

- [None] を選択すると、OSPF 認証がディセーブルになります。
- [Authentication Password] を選択すると、クリアテキストによるパスワード認証が使用されます（セキュリティの懸念がある場合は推奨しません）。
- [MD5] を選択すると、MD5 認証が使用されます（推奨）。
- [Area] を選択すると、エリアに対して指定された認証タイプを使用します（デフォルト）。エリア認証の設定については、「OSPFv2 エリア パラメータの設定」（P.23-16）を参照してください。エリア認証はデフォルトでディセーブルになっています。したがって、それ以前にエリア認証タイプを指定していない限り、エリア認証を設定するインターフェイスでは、設定するまで認証がディセーブルになっています。

ステップ 5　[Authentication Password] 領域のオプション ボタンをクリックします。この領域には、パスワード認証がイネーブルのときのパスワード入力に関する設定があります。

a.　[Enter Password] フィールドに、最大 8 文字のテキスト文字列を入力します。

b.　[Re-enter Password] フィールドに、パスワードを再入力します。

ステップ 6　MD5 の ID とキーの設定を [ID] 領域で選択します。この領域には、MD5 認証がイネーブルのときの MD5 キーとパラメータの入力に関する設定があります。OSPF 認証を使用するインターフェイス上のすべてのデバイスで、同じ MD5 キーおよび ID を使用する必要があります。

a.　[Key ID] フィールドに、数値のキー ID を入力します。有効値の範囲は、1 ～ 255 です。選択したインターフェイスのキー ID が表示されます。

b.　[Key] フィールドに、最大 16 バイトの英数字文字列を入力します。選択したインターフェイスのキーが表示されます。

c.　[Add] または [Delete] をクリックして、指定された MD5 キーを [MD5 ID and Key] テーブルに追加またはテーブルから削除します。

ステップ 7　[OK] をクリックします。

ステップ 8　[Properties] タブをクリックします。

ステップ 9　編集するインターフェイスを選択します。テーブルの行をダブルクリックすると、選択したインターフェイスの [Properties] タブ ダイアログボックスが開きます。

ステップ 10　[Edit] をクリックします。

[Edit OSPF Interface Properties] ダイアログボックスが表示されます。[Interface] フィールドに、OSPF プロパティ設定の対象であるインターフェイスの名前が表示されます。このフィールドは編集できません。

ステップ 11　このインターフェイスがブロードキャスト インターフェイスかどうかに応じて、[Broadcast] チェックボックスをオンまたはオフにします。

デフォルトでは、イーサネット インターフェイスの場合はこのチェックボックスがオンになっています。このチェックボックスをオフにすると、インターフェイスをポイントツーポイントの非ブロードキャスト インターフェイスとして指定したことになります。インターフェイスをポイントツーポイントの非ブロードキャストとして指定すると、OSPF ルートを VPN トンネル経由で送信できます。

インターフェイスをポイントツーポイント、非ブロードキャストとして設定すると、次の制限が適用されます。

- インターフェイスにはネイバーを 1 つだけ定義できます。
- ネイバーは手動で設定する必要があります 詳細については、「スタティック OSPFv2 ネイバーの定義」（P.23-20）を参照してください。
- クリプト ポイントを指すスタティック ルートを定義する必要があります。詳細については、「スタティック ルートの設定」（P.20-2）を参照してください。
- トンネル経由の OSPF がインターフェイスで実行中である場合は、アップストリーム ルータを使用する通常の OSPF を同じインターフェイス上で実行することはできません。
- OSPF ネイバーを指定する前に、クリプト マップをインターフェイスにバインドする必要があります。これは、OSPF アップデートが VPN トンネルを通過できるようにするためです。OSPF ネイバーを指定した後でクリプト マップをインターフェイスにバインドした場合は、**clear local-host all** コマンドを使用して OSPF 接続をクリアします。これで、OSPF 隣接関係を VPN トンネル経由で確立できるようになります。

ステップ 12　次のオプションを設定します。

- [Cost] フィールドに、このインターフェイスを通してパケット 1 個を送信するコストを決定する値を入力します。デフォルト値は 10 です。
- [Priority] フィールドに、OSPF ルータ優先順位の値を入力します。

  2 つのルータがネットワークに接続している場合、両方が指定ルータになろうとします。ルータ優先順位の高いデバイスが指定ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。

  この設定の有効値の範囲は 0 ～ 255 です。デフォルト値は 1 です。この設定に 0 を入力すると、適切でないルータが指定ルータになったり、指定ルータのバックアップが行われたりします。この設定は、ポイントツーポイントの非ブロードキャスト インターフェイスとして設定されているインターフェイスには適用されません。
- [MTU Ignore] チェックボックスをオンまたはオフにします。

  OSPF は、ネイバーが共通インターフェイスで同じ MTU を使用しているかどうかをチェックします。このチェックは、ネイバーによる DBD パケットの交換時に行われます。DBD パケットに受信した MTU が着信インターフェイスに設定されている IP MTU より高い場合、OSPF の隣接性は確立されません。

- [Database filter] チェックボックスをオンまたはオフにします。

  この設定は、同期とフラッディングのときに発信 LSA インターフェイスをフィルタリングするのに使用します。デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。完全メッシュ化トポロジでは、このフラッディングによって帯域幅が浪費されて、リンクおよび CPU の過剰使用につながることがあります。このチェックボックスをオンにすると、選択されているインターフェイスでは OSPF の LSA フラッディングが行われなくなります。

ステップ 13　（オプション）[Advanced] をクリックして [Edit OSPF Advanced Interface Properties] ダイアログボックスを開きます。ここでは、OSPF hello 間隔、再送信間隔、送信遅延、およびデッド間隔の値を変更できます。

通常は、ネットワーク上で OSPF の問題が発生した場合にだけ、これらの値をデフォルトから変更する必要があります。

ステップ 14　[Intervals] セクションには、次の値を入力します。

- [Hello Interval] には、インターフェイス上で送信される hello パケットの間隔を秒単位で指定します。hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバで同じである必要があります。有効値の範囲は 1 ～ 8192 秒です。デフォルト値は 10 秒です。
- [Retransmit Interval] には、このインターフェイスに属する隣接関係の LSA 再送信の間隔を秒単位で指定します。ルータはそのネイバーに LSA を送信すると、確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータは LSA を再送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効値の範囲は 1 ～ 8192 秒です。デフォルト値は 5 秒です。
- [Transmit Delay] には、このインターフェイス上で LSA パケット 1 個を送信するのに必要な時間の推定値を秒単位で指定します。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効値の範囲は 1 ～ 8192 秒です。デフォルト値は 1 秒です。

ステップ 15　[Detecting Lost Neighbors] セクションで、次のいずれかを実行します。

- [Configure interval within which hello packets are not received before the router declares the neighbor to be down] をクリックします。[Dead Interval] フィールドで、ルータがダウンしていると見なす基準となる時間を秒数で指定します。この時間が経過しても hello パケットが 1 つも受信されない場合は、ネイバーがルータのダウンを宣言します。有効値の範囲は 1 ～ 8192 秒です。この設定のデフォルト値は、[Hello Interval] フィールドで設定された時間の長さの 4 倍です。
- [Send fast hello packets within 1 seconds dead interval] をクリックします。[Hello multiplier] フィールドで、1 秒ごとに送信される hello パケットの数を指定します。有効な値は、3 ～ 20 です。

OSPFv2 エリア パラメータの設定

複数の OSPF エリア パラメータを設定できます。これらのエリア パラメータ（後述のタスク リストに表示）には、認証の設定、スタブ エリアの定義、デフォルト サマリー ルートへの特定のコストの割り当てがあります。認証では、エリアへの不正アクセスに対してパスワード ベースで保護します。

スタブ エリアに外部ルートに関する情報は送信されません その代わりに、ABR で生成されるデフォルトの外部ルートがあり、このルートは自律システムの外部の宛先としてスタブ エリアに送信されます。OSPF スタブ エリアのサポートを活用するには、デフォルトのルーティングをスタブ エリアで使用する必要があります。

手順

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択します。

ステップ 2　[Area/Networks] タブをクリックします。

[Add OSPF Area] ダイアログボックスが表示されます。

ステップ 3　次に示す [Area Type] のオプションのいずれかを選択します。

- [Normal] を選択すると、このエリアは標準の OSPF エリアとなります。エリアを最初に作成するときは、このオプションがデフォルトで選択されています。
- [Stub] を選択すると、このエリアはスタブ エリアとなります。スタブ エリアには、その向こう側にルータまたはエリアはありません。スタブ エリアは、AS External LSA（タイプ 5 LSA）がスタブ エリアにフラッドされないようにします。スタブ エリアを作成するときに、サマリー LSA（タイプ 3 および 4）がそのエリアにフラッディングされないように設定するには、[Summary] チェックボックスをオフにします。
- [Summary] チェックボックスは、エリアをスタブ エリアとして定義するときに、LSA がこのエリアに送信されないよう設定する場合にオフにします。デフォルトでは、スタブ エリアの場合にこのチェックボックスはオンになります。
- [NSSA] を選択すると、このエリアは Not-So-Stubby Area となります。NSSA は、タイプ 7 LSA を受け入れます。NSSA を作成するときに、[Summary] チェックボックスをオフにすることでサマリー LSA がそのエリアにフラッディングされないようにするオプションがあります。また、[Redistribute] チェックボックスをオフにし、[Default Information Originate] チェックボックスをオンにすることで、ルートの再配布をディセーブルにすることもできます。

ステップ 4　[IP Address] フィールドに、エリアに追加するネットワークまたはホストの IP アドレスを入力します。デフォルト エリアを作成するには、**0.0.0.0** およびネットマスク **0.0.0.0** を使用します。**0.0.0.0** を入力できるエリアは 1 つだけです。

ステップ 5　[Network Mask] フィールドに、エリアに追加する IP アドレスまたはホストのネットワーク マスクを入力します。ホストを追加する場合、**255.255.255.255** マスクを選択します。

ステップ 6　[OSPF Authentication type] で、次のオプションから選択します。

- [None] を選択すると、OSPF エリア認証がディセーブルになります。これがデフォルト設定です。
- [Password] を選択すると、クリア テキスト パスワードがエリア認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。
- [MD5] を選択すると、MD5 認証ができるようになります。

ステップ 7　[Default Cost] フィールドに値を入力して、[OSPF] エリアのデフォルト コストを指定します。

有効値の範囲は、0 ～ 65535 です。デフォルト値は 1 です。

ステップ 8　[OK] をクリックします。

OSPFv2 NSSA の設定

NSSA の OSPFv2 への実装は、OSPFv2 のスタブ エリアに似ています。NSSA は、タイプ 5 の外部 LSA をコアからエリアにフラッディングすることはありませんが、自律システムの外部ルートをある限られた方法でエリア内にインポートできます。

NSSA は、再配布によって、タイプ 7 の自律システムの外部ルートを NSSA エリア内部にインポートします。これらのタイプ 7 の LSA は、NSSA の ABR によってタイプ 5 の LSA に変換され、ルーティング ドメイン全体にフラッディングされます。変換中は集約とフィルタリングがサポートされます。

OSPFv2 を使用する中央サイトから異なるルーティング プロトコルを使用するリモート サイトに接続しなければならない ISP またはネットワーク管理者は、NSSA を使用することによって管理を簡略化できます。

NSSA が実装される前は、企業サイトの境界ルータとリモート ルータ間の接続では、OSPFv2 スタブ エリアとしては実行されませんでした。これは、リモート サイト向けのルートは、スタブ エリアに再配布することができず、2 種類のルーティング プロトコルを維持する必要があったためです。RIP のようなシンプルなプロトコルを実行して再配布を処理する方法が一般的でした。NSSA が実装されたことで、企業ルータとリモート ルータ間のエリアを NSSA として定義することにより、NSSA で OSPFv2 を拡張してリモート接続をカバーできます。

この機能を使用する前に、次のガイドラインを参考にしてください。

- 外部の宛先に到達するために使用可能なタイプ 7 のデフォルト ルートを設定できます。設定すると、NSSA または NSSA エリア境界ルータまでのタイプ 7 のデフォルトがルータによって生成されます。
- 同じエリア内のすべてのルータは、エリアが NSSA であることを認識する必要があります。そうでない場合、ルータは互いに通信できません。

手順

ステップ 1　メインの ASDM ホーム ページで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択します。

ステップ 2　[Area/Networks] タブをクリックします。

ステップ 3　[Add] をクリックします。

[Add OSPF Area] ダイアログボックスが表示されます。

ステップ 4　[Area Type] 領域の [NSSA] オプション ボタンをクリックします。

エリアを Not-So-Stubby Area にするには、このオプションを選択します。NSSA は、タイプ 7 LSA を受け入れます。NSSA を作成するときに、[Summary] チェックボックスをオフにすることでサマリー LSA がそのエリアにフラッディングされないようにするオプションがあります。また、[Redistribute] チェックボックスをオフにし、[Default Information Originate] チェックボックスをオンにすることで、ルートの再配布をディセーブルにすることもできます。

ステップ 5　[IP Address] フィールドに、エリアに追加するネットワークまたはホストの IP アドレスを入力します。デフォルト エリアを作成するには、**0.0.0.0** およびネットマスク **0.0.0.0** を使用します。**0.0.0.0** を入力できるエリアは 1 つだけです。

ステップ 6　[Network Mask] フィールドに、エリアに追加する IP アドレスまたはホストのネットワーク マスクを入力します。ホストを追加する場合、**255.255.255.255** マスクを選択します。

ステップ 7　[Authentication] 領域の [None] オプション ボタンをクリックすると、OSPF エリア認証がディセーブルになります。

ステップ 8　[Default Cost] フィールドに値を入力して、[OSPF] エリアのデフォルト コストを指定します。

有効値の範囲は、0 ～ 65535 です。デフォルト値は 1 です。

ステップ 9　[OK] をクリックします。

クラスタリングの IP アドレス プールの設定（OSPFv2 および OSPFv3）

個別インターフェイス クラスタリングを使用する場合は、ルータ ID のクラスタ プールの IPv4 アドレスの範囲を割り当てることができます。

手順

OSPFv2 の個別インターフェイスのルータ ID のクラスタ プールの IPv4 アドレスの範囲を割り当てるには、次の手順を実行します。

ステップ 1　メインの ASDM ホーム ページで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択します。

ステップ 2　[Process Instances] タブをクリックします。

ステップ 3　編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4　[Cluster Pool] オプション ボタンをクリックします。クラスタリングを使用している場合は、ルータ ID の IP アドレス プールを指定する必要はありません（つまりフィールドは空）。IP アドレス プールを入力しない場合、ASA は自動的に生成されたルータ ID を使用します。

ステップ 5　IP アドレス プールの名前を入力するか、省略記号をクリックして [Select IP Address Pool] ダイアログボックスを表示します。

ステップ 6　既存の IP アドレス プール名をダブルクリックして、[Assign] フィールドに追加します。[Add] をクリックして、新しい IP アドレス プールを作成することもできます。

[Add IPv4 Pool] ダイアログボックスが表示されます。

ステップ 7　[Name] フィールドに新しい IP アドレス プール名を入力します。

ステップ 8　開始 IP アドレスを入力するか、または省略記号をクリックして、[Browse Starting IP Address] ダイアログボックスを表示します。

ステップ 9　エントリをダブルクリックして、[Starting IP Address] フィールドに追加し、続いて [OK] をクリックします。

ステップ 10　最後の IP アドレスを入力するか、または省略記号をクリックして、[Browse Ending IP Address] ダイアログボックスを表示します。

ステップ 11　エントリをダブルクリックして、[Ending IP Address] フィールドに追加し、続いて [OK] をクリックします。

ステップ 12　ドロップダウン リストからサブネット マスクを選択し、続いて [OK] をクリックします。

[Select IP Address Pool] リストに、新しい IP アドレス プールが表示されます。

ステップ 13　新しい IP アドレス プール名をダブルクリックして、[Assign] フィールドに追加し、続いて [OK] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスの [Cluster Pool] フィールドに、新しい IP アドレス プール名が表示されます。

ステップ 14　[OK] をクリックします。

ステップ 15　新しく追加された IP アドレス プール設定を変更する場合は、[Edit] をクリックします。

[Edit IPv4 Pool] ダイアログボックスが表示されます。

ステップ 16　ステップ 4 ～ 14 を繰り返します。

（注）　すでに割り当てられ、1 つ以上の接続プロファイルによってすでに使用されている既存の IP アドレス プールを編集または削除することはできません。

ステップ 17　[**OK**] をクリックします。

OSPFv3 の個別インターフェイス クラスタリングのルータ ID のクラスタ プールに IPv4 アドレス範囲を割り当てるには、次の手順を実行します。

ステップ 1　メインの ASDM ホーム ページで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。

ステップ 2　[Process Instances] タブをクリックします。

ステップ 3　編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4　[Router ID] ドロップダウン リストから [Cluster Pool] オプションを選択します。ルータ ID の IP アドレス プールを指定する必要がない場合は、[Automatic] オプションを選択します。IP アドレス プールを設定しない場合、ASA は自動的に生成されたルータ ID を使用します。

ステップ 5　IP アドレス プール名を入力します。省略記号をクリックして、[IP Address Pool] ダイアログボックスを表示することもできます。

ステップ 6　既存の IP アドレス プール名をダブルクリックして、[Assign] フィールドに追加します。[Add] をクリックして、新しい IP アドレス プールを作成することもできます。

[Add IPv4 Pool] ダイアログボックスが表示されます。

ステップ 7　[Name] フィールドに新しい IP アドレス プール名を入力します。

ステップ 8　開始 IP アドレスを入力するか、または省略記号をクリックして、[Browse Starting IP Address] ダイアログボックスを表示します。

ステップ 9　エントリをダブルクリックして、[Starting IP Address] フィールドに追加し、続いて [OK] をクリックします。

ステップ 10　最後の IP アドレスを入力するか、または省略記号をクリックして、[Browse Ending IP Address] ダイアログボックスを表示します。

ステップ 11　エントリをダブルクリックして、[Ending IP Address] フィールドに追加し、続いて [OK] をクリックします。

ステップ 12　ドロップダウン リストからサブネット マスクを選択し、続いて [OK] をクリックします。

[Select IP Address Pool] リストに、新しい IP アドレス プールが表示されます。

ステップ 13　新しい IP アドレス プール名をダブルクリックして、[Assign] フィールドに追加し、続いて [OK] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスの [Cluster Pool] フィールドに、新しい IP アドレス プール名が表示されます。

ステップ 14　[OK] をクリックします。

ステップ 15　新しく追加されたクラスタ プールの設定を変更する場合は、[Edit] をクリックします。

[Edit IPv4 Pool] ダイアログボックスが表示されます。

ステップ 16　ステップ 4 ～ 14 を繰り返します。

（注）　すでに割り当てられ、別の OSPFv3 プロセスによってすでに使用されている既存の IP アドレス プールを編集または削除することはできません。

ステップ 17　[OK] をクリックします。

スタティック OSPFv2 ネイバーの定義

ポイントツーポイントの非ブロードキャスト ネットワークを介して OSPFv2 ルートをアドバタイズするには、スタティック OSPFv2 ネイバーを定義する必要があります。この機能により、OSPFv2 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

開始する前に、OSPFv2 ネイバーに対するスタティック ルートを作成する必要があります。スタティック ルートの作成方法の詳細については、第 20 章「スタティック ルートとデフォルト ルート」を参照してください。

手順

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Static Neighbor] の順に選択します。

ステップ 2　[Add] または [Edit] をクリックします。

[Add/Edit OSPF Neighbor Entry] ダイアログボックスが表示されます。このダイアログボックスでは、新しいスタティック ネイバーを定義することや、既存のスタティック ネイバーの情報を変更することができます。ポイントツーポイントの非ブロードキャスト インターフェイスごとに、スタティック ネイバーを 1 つ定義する必要があります。次の制約事項に注意してください。

- 異なる 2 つの OSPF プロセスに対して同じスタティック ネイバーを定義できません。
- 各スタティック ネイバーにスタティック ルートを定義する必要があります

ステップ 3　[OSPF Process] ドロップダウン リストで、スタティック ネイバーに関連付ける OSPF プロセスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。

ステップ 4　[Neighbor] フィールドに、スタティック ネイバーの IP アドレスを入力します。

ステップ 5　[Interface] フィールドで、スタティック ネイバーに関連付けるインターフェイスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。

ステップ 6　[OK] をクリックします。

ルート計算タイマーの設定

OSPFv2 によるトポロジ変更受信と最短パス優先（SPF）計算開始との間の遅延時間が設定できます。最初に SPF を計算してから次に計算するまでの保持時間も設定できます。

ルート計算タイマーを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択します。

ステップ 2　[Process Instances] タブをクリックします。

ステップ 3　編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4　[Timers] 領域では、LSA ペーシングおよび SPF 計算のタイマーの設定に使用される値を変更できます。[Timers] 領域で、次の値を入力します。

- [Initial SPF Delay] は、OSPF がトポロジ変更を受信してから SPF 計算が開始されるまでの時間（ミリ秒）を指定します。有効な値の範囲は、0 ～ 600000 ミリ秒です。
- [Minimum SPF Hold Time] は、連続する SPF 計算間の保持時間をミリ秒で指定します。有効な値の範囲は、0 ～ 600000 ミリ秒です。
- [Maximum SPF Wait Time] は、2 回の連続する SPF 計算間の最大待機時間を指定します。有効な値の範囲は、0 ～ 600000 ミリ秒です。

ステップ 5　[OK] をクリックします。

ネイバーがアップ状態またはダウン状態になった時点でのロギング

デフォルトでは、OSPFv2 ネイバーがアップ状態またはダウン状態になったときに、syslog メッセージが生成されます。

アップ状態またはダウン状態になった OSPFv2 ネイバーをログに記録するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択します。

ステップ 2　[Process Instances] タブをクリックします。

ステップ 3　[Advanced] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4　[Adjacency Changes] 領域には、syslog メッセージ送信を引き起こす隣接関係変更を定義するための設定があります。[Adjacency Changes] 領域で、次の値を入力します。

- [Log Adjacency Changes] チェックボックスをオンにすると、OSPFv2 ネイバーがアップ状態またはダウン状態になるたびに ASA によって syslog メッセージが送信されるようになります。この設定は、デフォルトでオンになっています。
- [Log Adjacency Changes Detail] チェックボックスをオンにすると、ネイバーがアップ状態またはダウン状態になったときだけでなく、状態の変更が発生したときにも ASA によって syslog メッセージが送信されるようになります。デフォルトでは、この設定はオフになっています。

ステップ 5　[OK] をクリックします。

（注）　ネイバーのアップまたはダウンのメッセージが送信されるには、ロギングがイネーブルになっている必要があります。

OSPF でのフィルタリングの設定

[Filtering] ペインには、各 OSPF プロセスに対して設定済みの ABR タイプ 3 LSA フィルタが表示されます。

ABR タイプ 3 LSA フィルタを設定すると、指定したプレフィックスだけが 1 つのエリアから別のエリアに送信され、その他のプレフィックスはすべて制限されます。このタイプのエリアフィルタリングは、特定の OSPF エリアから、特定の OSPF エリアへ、または同じ OSPF エリアへ同時に適用できます。

OSPF ABR タイプ 3 LSA フィルタリングによって、OSPF エリア間のルート再配布の制御が向上します。

（注）　フィルタリングされるのは、ABR から送信されるタイプ 3 LSA だけです。

OSPF でのフィルタリングを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Filtering] の順に選択します。

ステップ 2　[Add] または [Edit] をクリックします。

[Add or OSPF Filtering Entry] ダイアログボックスでは、新しいフィルタを [Filter] テーブルに追加することや、既存のフィルタを修正することができます。既存のフィルタを編集するとき、一部のフィルタリング情報は変更できません。

ステップ 3　フィルタ エントリに関連付ける OSPF プロセスを [OSPF Process] ドロップダウン リストで選択します。

ステップ 4　フィルタ エントリに関連付けるエリア ID を [Area ID] ドロップダウン リストで選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。

ステップ 5　プレフィックス リストを [Prefix List] ドロップダウン リストで選択します。

ステップ 6　フィルタリングするトラフィックの方向を [Traffic Direction] ドロップダウン リストで選択します。

OSPF エリアへの LSA をフィルタリングするには [Inbound] を選択し、OSPF エリアからの LSA をフィルタリングするには [Outbound] を選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。

ステップ 7　[Manage] をクリックすると [Configure Prefix Lists] ダイアログボックスが表示され、ここでプレフィックス リストとプレフィックス ルールを追加、編集、または削除できます。詳細については、「プレフィックス リストの設定」（P.21-8）および「ルート アクションのメトリック値の設定」（P.21-9）を参照してください。

ステップ 8　[OK] をクリックします。

OSPF の仮想リンクの設定

OSPF ネットワークにエリアを追加し、そのエリアをバックボーン エリアに直接接続できない場合、仮想リンクを作成する必要があります。仮想リンクは、通過エリアと呼ばれる共通エリアを持つ 2 つの OSPF デバイスを接続します。OSPF デバイスのいずれかは、バックボーン エリアに接続されている必要があります。

新しい仮想リンクを定義する、または既存の仮想リンクのプロパティを変更するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Virtual Link] の順に選択します。

ステップ 2　[Add] または [Edit] をクリックします。

[Add OSPF Virtual Link] または [Edit OSPF Virtual Link] ダイアログボックスが表示され、ここで新しい仮想リンクを定義することや、既存の仮想リンクのプロパティを変更することができます。

ステップ 3　仮想リンクに関連付ける OSPF プロセス ID を [OSPF Process] ドロップダウン リストで選択します。既存の仮想リンク エントリを編集している場合、この設定は変更できません。

ステップ 4　仮想リンクに関連付けるエリア ID を [Area ID] ドロップダウン リストで選択します。

ネイバー OSPF デバイスによって共有されるエリアを選択します。[NSSA] エリアまたは [Stub] エリアは選択できません。既存の仮想リンク エントリを編集している場合、この設定は変更できません。

ステップ 5　[Peer Router ID] フィールドに、仮想リンク ネイバーのルータ ID を入力します。

既存の仮想リンク エントリを編集している場合、この設定は変更できません。

ステップ 6　仮想リンクの詳細プロパティを編集するには、[Advanced] をクリックします。

[Advanced OSPF Virtual Link Properties] ダイアログボックスが表示されます。このエリアにある仮想リンクに対して、OSPF プロパティを設定できます。プロパティには、認証およびパケット間隔設定が含まれます。

ステップ 7　[Authentication] 領域で、[Authentication type] を選択します。次のオプション ボタンのいずれかをクリックします。

- [None] を選択すると、OSPF 認証がディセーブルになります。
- クリア テキスト パスワード認証を使用する場合は [Authentication Password]。セキュリティ面が懸念される場合は推奨しません。
- [MD5] を選択すると、MD5 認証が使用されます（推奨）。
- [Area] を選択すると、エリアに対して指定された認証タイプを使用します（デフォルト）。エリア認証の設定については、「OSPFv2 エリア パラメータの設定」（P.23-16）を参照してください。エリア認証はデフォルトでディセーブルになっています。したがって、それ以前にエリア認証タイプを指定していない限り、エリア認証を設定するインターフェイスでは、設定するまで認証がディセーブルになっています。

ステップ 8　[Authentication Password] 領域で、パスワードを入力し、もう一度入力します（パスワード認証がイネーブルのとき）。パスワードは、最大 8 文字のテキスト文字列であることが必要です。

ステップ 9　[MD5 IDs and Key] 領域で、MD5 のキーとパラメータを入力します（MD5 認証がイネーブルのとき）。OSPF 認証を使用するインターフェイス上のすべてのデバイスで、同じ MD5 キーおよび ID を使用する必要があります。次の設定を指定します。

a. [Key ID] フィールドに、数値のキー ID を入力します。有効値の範囲は、1 ～ 255 です。選択したインターフェイスのキー ID が表示されます。

b. [Key] フィールドに、最大 16 バイトの英数字文字列を入力します。選択したインターフェイスのキー ID が表示されます。

c. [Add] または [Delete] をクリックして、指定された MD5 キーを [MD5 ID and Key] テーブルに追加またはテーブルから削除します。

ステップ 10　[Interval] 領域で、パケットの間隔を指定します。次のオプションから選択します。

- [Hello Interval] には、インターフェイス上で送信される hello パケットの間隔を秒単位で指定します。hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバで同じである必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 10 秒です。
- [Retransmit Interval] には、このインターフェイスに属する隣接関係の LSA 再送信の間隔を秒単位で指定します。ルータはそのネイバーに LSA を送信すると、確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータは LSA を再送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
- [Transmit Delay] には、このインターフェイス上で LSA パケット 1 個を送信するのに必要な時間の推定値を秒単位で指定します。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。
- [Dead Interval] には、ルータがダウンしていると見なす基準となる時間を秒数で指定します。この時間が経過しても hello パケットが 1 つも受信されない場合は、ネイバーがルータのダウンを宣言します。有効な値の範囲は 1 ～ 65535 です。このフィールドのデフォルト値は、[Hello Interval] フィールドに設定されている時間間隔の 4 倍です。

ステップ 11　[OK] をクリックします。

OSPFv3 の設定

ここでは、OSPFv3 ルーティング プロセスの設定方法について説明します。

- 「OSPFv3 のイネーブル化」（P.23-25）
- 「OSPFv3 インターフェイスのパラメータの設定」（P.23-25）
- 「OSPFv3 エリア パラメータの設定」（P.23-27）
- 「仮想リンク ネイバーの設定」（P.23-28）

OSPFv3 のイネーブル化

OSPFv3 をイネーブルにするには、OSPFv3 ルーティング プロセスを作成し、OSPFv3 用のエリアを作成して、OSPFv3 のインターフェイスをイネーブルにする必要があります。その後、ターゲットの OSPFv3 ルーティング プロセスにルートを再配布する必要があります。

OSPFv3 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　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。

ステップ 2　[Process Instances] タブで、[Enable OSPFv3 Process] チェックボックスをオンにします。最大 2 つの OSPF プロセス インスタンスをイネーブルにできます。シングル コンテキスト モードだけがサポートされます。

ステップ 3　[Process ID] フィールドにプロセス ID を入力します。ID は、任意の正の整数が可能です。

ステップ 4　[Apply] をクリックして変更内容を保存します。

ステップ 5　以降の手順については、「OSPFv3 エリア パラメータの設定」（P.23-27）を参照してください。

OSPFv3 インターフェイスのパラメータの設定

必要に応じて特定のインターフェイス固有の OSPFv3 パラメータを変更できます。これらのパラメータは必ずしも変更する必要はありませんが、hello インターバルおよびデッド インターバルの各インターフェイス パラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

IPv6 の OSPFv3 インターフェイス パラメータを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Interfaces] の順に選択します。

ステップ 2　[Authentication] タブをクリックします。

ステップ 3　インターフェイスの認証パラメータを指定するには、インターフェイスを選択し、[Edit] をクリックします。

[Edit OSPFv3 Interface Authentication] ダイアログボックスが表示されます。

ステップ 4　[Authentication Type] ドロップダウン リストから認証タイプを選択します。使用可能なオプションは、[Area]、[Interface]、[None] です。[None] オプションを選択すると、認証が行われません。

ステップ 5　[Authentication Algorithm] ドロップダウン リストから認証アルゴリズムを選択します。サポートされる値は、[SHA-1] および [MD5] です。

ステップ 6　[Authentication Key] フィールドに認証キーを入力します。MD5 認証を使用する場合、キーの長さは 32 桁の 16 進数（16 バイト）である必要があります。SHA-1 認証を使用する場合、キーの長さは 40 桁の 16 進数（20 バイト）である必要があります。

ステップ 7　[Encryption Algorithm] ドロップダウン リストから暗号化アルゴリズムを選択します。サポートされる値は、[AES-CDC]、[3DES]、[DES] です。ヌルのエントリは暗号化されません。

ステップ 8　[Encryption Key] フィールドに暗号キーを入力します。

ステップ 9　[OK] をクリックします。

ステップ 10　[Properties] タブをクリックします。

ステップ 11　プロパティを変更するインタフェースを選択し、[Edit] をクリックします。

[Edit OSPFv3 Interface Properties] ダイアログボックスが表示されます。

ステップ 12　[Enable OSPFv3 on this interface] チェックボックスをオンにします。

ステップ 13　ドロップダウン リストからプロセス ID を選択します。

ステップ 14　ドロップダウン リストから領域 ID を選択します。

ステップ 15　（オプション）インターフェイスに割り当てる領域インスタンス ID を指定します。インターフェイスは、OSPFv3 エリアを 1 つだけ保有できます。複数のインターフェイスで同じエリアを使用でき、各インターフェイスは異なるエリア インスタンス ID を使用できます。

ステップ 16　ドロップダウン リストからネットワーク タイプを選択します。サポートされるオプションは、[Default]、[Broadcast]、[Point-to-Point] です。

ステップ 17　[Cost] フィールドにインターフェイスでのパケット送信コストを入力します。

ステップ 18　ルータ プライオリティを入力します。これは、ネットワークにおける指定ルータの特定に役立ちます。[Priority] フィールド。有効値の範囲は 0 ～ 255 です。

ステップ 19　[Disable MTU mismatch detection] チェックボックスをオンにして、DBD パケットが受信された場合の OSPF MTU 不一致検出をディセーブルにします。OSPF MTU 不一致検出は、デフォルトでイネーブルになっています。

ステップ 20　[Filter outgoing link state advertisements] チェックボックスをオンにして、OSPFv3 インターフェイスに対する出力 LSA をフィルタします。デフォルトでは、すべての発信 LSA がインターフェイスにフラッディングされます。

ステップ 21　[Timers] 領域の [Dead Interval] フィールドに hello パケットが表示されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間を秒単位で入力します。この値はネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。

ステップ 22　[Hello Interval] フィールドに、hello パケットがインターフェイスに送信される間隔を秒単位で入力します。この値は特定のネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。デフォルトの間隔は、イーサネット インターフェイスで 10 秒、非ブロードキャスト インターフェイスで 30 秒です。

ステップ 23　[Retransmit Interval] フィールドに、インターフェイスに属する隣接ルータの LSA 再送信間隔を秒単位で入力します。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。

ステップ 24　[Transmit Delay] フィールドに、インターフェイスでリンク ステート アップデート パケットを送信する予想時間を秒単位で入力します。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。

ステップ 25　[OK] をクリックします。

ステップ 26　[Apply] をクリックして変更内容を保存します。

OSPFv3 エリア パラメータの設定

OSPFv3 エリア パラメータを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。

ステップ 2　[Areas] タブをクリックします。

ステップ 3　新しいエリアを追加するには、[Add] をクリックします。既存のエリアを変更するには、[Edit] をクリックします。選択したエリアを削除するには、[Delete] をクリックします。

[Add OSPFv3 Area] ダイアログボックスまたは [Edit OSPFv3 Area] ダイアログボックスが表示されます。

ステップ 4　[OSPFv3 Process ID] ドロップダウン リストから、プロセス ID を選択します。

ステップ 5　ルートが集約されるエリアを指定するエリア ID を [Area ID] フィールドに入力します。

ステップ 6　[Area Type] ドロップダウン リストからエリア タイプを選択します。使用可能なオプションは、[Normal]、[NSSA]、[Stub] です。

ステップ 7　エリアにサマリー LSA の送信を許可する場合は、[Allow sending of summary LSAs into the area] チェックボックスをオンにします。

ステップ 8　標準および not so stubby エリアへのインポート ルートの再配布を許可するには、[Redistribution imports routes to normal and NSSA areas] チェックボックスをオンにします。

ステップ 9　OSPFv3 ルーティング ドメインにデフォルト外部ルートを生成するには、[Default information originate] チェックボックスをチェックします。

ステップ 10　デフォルト ルートの生成に使用するメトリックを [Metric] フィールドに入力します。デフォルト値は 10 です。有効なメトリック値の範囲は、0 ～ 16777214 です。

ステップ 11　[Metric Type] ドロップダウン リストからメトリック タイプを選択します。メトリック タイプは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。

ステップ 12　[Default Cost] フィールドにコストを入力します。

ステップ 13　[OK] をクリックします。

ステップ 14　[Route Summarization] タブをクリックします。

ステップ 15　ルートを統合および集約するための新しい範囲を指定するには、[Add] をクリックします。ルートを統合および集約する既存の範囲を変更するには、[Edit] をクリックします。

[Add Route Summarization] ダイアログボックスまたは [Edit Route Summarization] ダイアログボックスが表示されます。

ステップ 16　[Process ID] ドロップダウン リストからプロセス ID を選択します。

ステップ 17　[Area ID] ドロップダウン リストからエリア ID を選択します。

ステップ 18　[IPv6 Prefix/Prefix Length] フィールドに IPv6 プレフィックスとプレフィックス長を入力します。

ステップ 19　（オプション）このサマリー ルートのメトリックまたはコストを入力します。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効な値の範囲は 0 ～ 16777215 です。

ステップ 20　[Advertised] チェックボックスをオンにして、アドレス範囲の状態をアドバタイズされた設定し、タイプ 3 サマリー LSA を生成します。

ステップ 21　[OK] をクリックします。

ステップ 22　以降の手順については、「仮想リンク ネイバーの設定」（P.23-28）を参照してください。

仮想リンク ネイバーの設定

仮想リンク ネイバーを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Virtual Link] の順に選択します。

ステップ 2　新しい仮想リンク ネイバーを追加するには、[Add] をクリックします。既存の仮想リンク ネイバーを変更するには、[Edit] をクリックします。指定された仮想リンク ネイバーを削除するには、[Delete] をクリックします。

[Add Virtual Link] ダイアログボックスまたは [Edit Virtual Link] ダイアログボックスが表示されます。

ステップ 3　[Process ID] ドロップダウン リストからプロセス ID を選択します。

ステップ 4　[Area ID] ドロップダウン リストからエリア ID を選択します。

ステップ 5　[Peer Router ID] フィールドにピア ルータ ID（IP アドレス）を入力します。

ステップ 6　（オプション）[TTL Security] フィールドに仮想リンクの存続可能時間 (TTL) のセキュリティのホップ数を入力します。ホップ数の値は 1 ～ 254 の範囲で指定します。

ステップ 7　[Timers] 領域の [Dead Interval] フィールドに、hello パケットが表示されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間を秒単位で入力します。デッド間隔は符号なし整数です。デフォルトは hello 間隔の 4 倍または 40 秒です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバで同じであることが必要です。有効な値の範囲は 1 ～ 8192 です。

ステップ 8　[Hello Interval] フィールドに、インターフェイスで送信される hello パケットの間隔を秒単位で入力します。hello 間隔は、hello パケットでアドバタイズされる符号なし整数です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバで同じであることが必要です。有効な値の範囲は 1 ～ 8192 です。デフォルトは 10 です。

ステップ 9　[Retransmit Interval] フィールドに、インターフェイスに属している隣接ルータの LSA 再送信間隔を秒単位で入力します。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延より大きくなり、1 ～ 8192 の範囲で指定できます。デフォルトは 5 です。

ステップ 10　[Transmit Delay] フィールドに、インターフェイスのリンク ステート アップデート パケットの送信に必要な予想時間を秒単位で入力します。ゼロよりも大きい整数値を指定します。アップデート パケット内の LSA 自体の経過時間は、転送前にこの値の分だけ増分されます。値の範囲は 1 ～ 8192 です。デフォルトは 1 です。

ステップ 11　[Authentication] 領域の [Enable Authentication] チェックボックスをオンにして、認証をイネーブルにします。

ステップ 12　[Security Policy Index] フィールドに、セキュリティ ポリシー インデックスを入力します。値の範囲は、256～4294967295 の数字です。

ステップ 13　[Authentication Algorithm] ドロップダウン リストから認証アルゴリズムを選択します。サポートされる値は、[SHA-1] および [MD5] です。MD5 認証を使用する場合、キーの長さは 32 桁の 16 進数（16 バイト）である必要があります。SHA-1 認証を使用する場合、キーの長さは 40 桁の 16 進数（20 バイト）である必要があります。

ステップ 14　[Authentication Key] フィールドに認証キーを入力します。キーは 32 文字の 16 進数文字で構成される必要があります。

ステップ 15　[Encryption Algorithm] ドロップダウン リストから暗号化アルゴリズムを選択します。サポートされる値は、[AES-CDC]、[3DES]、[DES] です。ヌルのエントリは暗号化されません。

ステップ 16　[Encryption Key] フィールドに暗号キーを入力します。

ステップ 17　[OK] をクリックします。

ステップ 18　[Apply] をクリックして変更内容を保存します。

OSPFv3 パッシブ インターフェイスの設定

OSPFv3 パッシブ インターフェイスを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。

ステップ 2　[Process Instances] タブをクリックします。

ステップ 3　編集する OSPFv3 プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4　[Passive Interfaces] 領域では、インターフェイスのパッシブ OSPFv3 ルーティングをイネーブルにすることができます。パッシブ ルーティングは、OSPFv3 ルーティング情報のアドバタイズメントの制御に有効であり、インターフェイスでの OSPFv3 ルーティング更新の送受信をディセーブルにします。[Passive Interfaces] 領域で、次の設定を選択します。

- [Global passive] チェックボックスをオンにして、テーブルに表示されているインターフェイスすべてをパッシブにします。個々のインターフェイスをオフにすると、そのインターフェイスは非パッシブになります。
- [Global passive] チェックボックスをオフにすると、すべてのインターフェイスが非パッシブになります。個々のインターフェイスをオンにすると、そのインターフェイスはパッシブになります。

ステップ 5　[OK] をクリックします。

ステップ 6　[Apply] をクリックして変更内容を保存します。

OSPFv3 アドミニストレーティブ ディスタンスの設定

IPv6 ルートの OSPFv3 アドミニストレーティブ ディスタンスを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。

ステップ 2　[Process Instances] タブをクリックします。

ステップ 3　編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

[Administrative Route Distances] 領域では、管理ルート間隔の設定に使用された設定を変更することができます。管理ルート間隔は 10～254 の整数です。[Administrative Route Distances] 領域で、次の値を入力します。

- [Inter Area] には、IPv6 ルートの OSPV のエリア間ルートを指定します。
- [Intra Area] には、IPv6 ルートの OSPF のエリア内ルートを指定します。
- [External] には、IPv6 ルートの OSPF の外部タイプ 5 および外部タイプ 7 のルートを指定します。

ステップ 4　[OK] をクリックします。

ステップ 5　[Apply] をクリックして変更内容を保存します。

OSPFv3 タイマーの設定

OSPFv3 の LSA 到着タイマー、LSA ペーシング タイマー、およびスロットリング タイマーを設定できます。

ASA が OSPFv3 ネイバーから同じ LSA を受け入れる最小間隔を設定するには、次の手順を実行します。

LSA フラッド パケット ペーシングを設定するには、次の手順を実行します。

OSPFv3 LSA を収集してグループ化し、リフレッシュ、チェックサム計算、またはエージングを行う間隔を変更するには、次の手順を実行します。

LSA 再送信パケット ペーシングを設定するには、次の手順を実行します。

LSA および SPF スロットリングは、ネットワークが不安定になっている間に OSPFv3 の LSA 更新速度を低下し、ミリ秒単位の LSA レート制限を提供することにより、より高速な OSPFv3 コンバージェンスを許可するダイナミック メカニズムを提供します。

LSA および SPF スロットリング タイマーを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。

ステップ 2　[Process Instances] タブをクリックします。

ステップ 3　編集する OSPFv3 プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4　[Timers] 領域では、LSA 到着、LSA ペーシング、LSA 再送信、LSA スロットル、SPF スロットル時間の設定に使用された設定を変更することができます。[Timers] 領域で、次の値を入力します。

- [LSA Arrival] には、ネイバーから到着する同一 LSA の最短受信間隔をミリ秒単位で指定します。指定できる範囲は 0 ～ 6000,000 ミリ秒です。デフォルトは 1000 ミリ秒です。
- [LSA Flood Pacing] には、フラッディング キュー内の LSA のアップデートのペースをミリ秒単位で指定します。設定できる範囲は 5 ～ 100 ミリ秒です。デフォルト値は 33 ミリ秒です。
- [LSA Group Pacing] には、LSA をグループにまとめてリフレッシュ、チェックサム計算、エージングする間隔を秒単位で指定します。有効値の範囲は 10 ～ 1800 です。デフォルト値は 240 です。
- [LSA Retransmission Pacing] には、再送信キュー内の LSA がペースされる時間をミリ秒単位で指定します。設定できる範囲は 5 ～ 200 ミリ秒です。デフォルト値は 66 ミリ秒です。
- [LSA Throttle Initial] には、LSA の最初のオカレンスを生成する遅延をミリ秒単位で指定します。デフォルト値は 0 ミリ秒です。
- [LSA Throttle Min Hold] には、同じ LSA を発信する最短遅延時間をミリ秒単位で指定します。デフォルト値は 5000 ミリ秒です。
- [LSA Throttle Max Wait] には、同じ LSA を発信する最長遅延時間をミリ秒単位で指定します。デフォルト値は 5000 ミリ秒です。

（注）　LSA スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

- [SPF Throttle Initial] には、SPF 計算の変更を受信する遅延をミリ秒単位で指定します。デフォルト値は 5000 ミリ秒です。
- [SPF Throttle Min Hold] には、1 番目と 2 番目の SPF 計算の間の遅延をミリ秒単位で指定します。デフォルト値は 10000 ミリ秒です。
- [SPF Throttle Max Wait] には、SPF 計算の最長待機時間をミリ秒単位で指定する。デフォルト値は 10000 ミリ秒です。

（注）　SPF スロットリングでは、最短時間または最長時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

ステップ 5　[OK] をクリックします。

ステップ 6　[Apply] をクリックして変更内容を保存します。

スタティック OSPFv3 ネイバーの定義

ポイントツーポイントの非ブロードキャスト ネットワークを介して OSPFv3 ルートをアドバタイズするには、スタティック OSPF ネイバーを定義する必要があります。この機能により、OSPFv3 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

開始する前に、OSPFv3 ネイバーに対するスタティック ルートを作成する必要があります。スタティック ルートの作成方法の詳細については、第 20 章「スタティック ルートとデフォルト ルート」を参照してください。

スタティック OSPFv3 ネイバーを定義するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Static Neighbor] の順に選択します。

ステップ 2　[Add] または [Edit] をクリックします。

[Add Static Neighbor] または [Edit Static Neighbor] ダイアログボックスが表示されます。このダイアログボックスでは、新しいスタティック ネイバーを定義することや、既存のスタティック ネイバーの情報を変更することができます。ポイントツーポイントの非ブロードキャスト インターフェイスごとに、スタティック ネイバーを 1 つ定義する必要があります。次の制約事項に注意してください。

- 異なる 2 つの OSPFv3 プロセスに対して同じスタティック ネイバーを定義できません。
- 各スタティック ネイバーにスタティック ルートを定義する必要があります

ステップ 3　[Interface] ドロップダウン リストから、スタティック ネイバーに関連付けられたインターフェイスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。

ステップ 4　[Link-local address] フィールドに、スタティック ネイバーの IPv6 アドレスを入力します。

ステップ 5　（オプション）[Priority] フィールドに、プライオリティ レベルを入力します。

ステップ 6　（オプション）[Poll Interval] フィールドに、ポーリング間隔を秒単位で入力します。

ステップ 7　[OK] をクリックします。

syslog メッセージの送信

OSPFv3 ネイバーが起動または停止したときに syslog メッセージを送信するようにルータを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。

ステップ 2　[Process Instances] タブをクリックします。

ステップ 3　編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

[Adjacency Changes] 領域では、OSPFv3 ネイバーが起動または停止したときに syslog メッセージを送信するための設定を変更することができます。[Adjacency Changes] 領域で、次の手順を実行します。

- OSPFv3 ネイバーが起動または停止したときに syslog メッセージを送信するには、[Log Adjacency Changes] チェックボックスをオンにします。

- OSPFv3 ネイバーが起動または停止したときだけではなく、各状態の syslog メッセージを送信するには、[Include Details] チェックボックスをオンにします。

ステップ 4　[OK] をクリックします。

ステップ 5　[Apply] をクリックして変更内容を保存します。

syslog メッセージの抑止

ルータがサポートされていない LSA タイプ 6 Multicast OSPF（MOSPF）パケットを受信した場合の syslog メッセージの送信を抑止するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。

ステップ 2　[Process Instances] タブをクリックします。

ステップ 3　編集する OSPFv3 プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4　[Ignore LSA MOSPF] チェックボックスをオンにして、[OK] をクリックします。

サマリー ルート コストの計算

RFC 1583 に従ってサマリー ルート コストを計算するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。

ステップ 2　[Process Instances] タブをクリックします。

ステップ 3　編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4　[RFC1583 Compatible] チェックボックスをオンにして、[OK] をクリックします。

OSPFv3 ルーティング ドメインへのデフォルトの外部ルートの生成

OSPFv3 ルーティング ドメインへのデフォルト ルートを生成するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。

ステップ 2　[Process Instances] タブをクリックします。

ステップ 3　編集する OSPFv3 プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4　[Default Information Originate Area] で、次の手順を実行します。

a. [Enable] チェックボックスをオンにして、OSPFv3 ルーティング プロセスをイネーブルにします。

b. [Always advertise] チェックボックスをオンにして、出口が 1 つであるかどうかにかかわらず、常時デフォルト ルートをアドバタイズします。

c. デフォルト ルートの生成に使用するメトリックを [Metric] フィールドに入力します。有効なメトリック値の範囲は、0 ～ 16777214 です。デフォルト値は 10 です。

d. [Metric Type] ドロップダウン リストは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。有効な値は次のとおりです。

- 1：タイプ 1 外部ルート
- 2：タイプ 2 外部ルート

デフォルトはタイプ 2 外部ルートです。

e. [Route Map] ドロップダウン リストから、ルート マップが満たされている場合に、デフォルト ルートを生成するルーティング プロセスを選択します。

ステップ 5　[OK] をクリックします。

ステップ 6　[Apply] をクリックして変更内容を保存します。

IPv6 サマリー プレフィックスの設定

IPv6 サマリー プレフィックスを設定するには、次の手順を実行します。

ステップ 1　ASDM のメイン ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Summary Prefix] の順に選択します。

ステップ 2　新しいサマリー プレフィックスを追加するには、[Add] をクリックします。既存のサマリー プレフィックスを適用するには、[Edit] をクリックします。サマリー プレフィックスを削除するには、[Delete] をクリックします。

[Add Summary Prefix] ダイアログボックスまたは [Edit Summary Prefix] ダイアログボックスが表示されます。

ステップ 3　[Process ID] ドロップダウン リストからプロセス ID を選択します。

ステップ 4　[IPv6 Prefix/Prefix Length] フィールドに IPv6 プレフィックスとプレフィックス長を入力します。

ステップ 5　[Advertise] チェックボックスをオンにして、指定したプレフィックスとマスクのペアに一致するルートをアドバタイズします。このチェックボックスをオフにすると、指定されたプレフィックスとマスク ペアと一致するルートが抑制されます。

ステップ 6　ルート マップを使用して再配布を制御するように照合値として使用できるタグ値を [Tag] フィールドに入力します。

ステップ 7　[OK] をクリックします。

ステップ 8　[Apply] をクリックして変更内容を保存します。

IPv6 ルートの再配布

OSPFv3 に接続済みルートを再配布するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Redistribution] の順に選択します。

ステップ 2　OSPFv3 プロセスに接続済みルートを再配布するための新しいパラメータを追加するには、[Add] をクリックします。OSPFv3 プロセスに接続済みルートを再配布するための既存のパラメータを変更するには、[Edit] をクリックします。パラメータの選択したセットを削除するには [Delete] をクリックします。

[Add Redistribution] ダイアログボックスまたは [Edit Redistribution] ダイアログボックスが表示されます。

ステップ 3　[Process ID] ドロップダウン リストからプロセス ID を選択します。

ステップ 4　[Source Protocol] ドロップダウン リストから、ルートが再配布されるソース プロトコルを選択します。サポートされるプロトコルは、接続済み、スタティック、OSPF です。

ステップ 5　[Metric] フィールドにメトリック値を入力します。同じルータ上の一方の OSPF プロセスから他方の OSPF プロセスにルートを再配布する場合、メトリック値を指定しないと、メトリックは一方のプロセスから他方のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。

ステップ 6　[Metric Type] ドロップダウン リストからメトリック タイプを選択します。使用可能なオプションは、[None]、[1]、[2] です。

ステップ 7　（オプション）[Tag] フィールドにタグ値を入力します。このパラメータは、ASBR 間で情報の転送に使用される可能性のある各外部ルートに付加される 32 ビットの 10 進数値を指定します。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用されます。その他のプロトコルについては、ゼロが使用されます。有効な値は、0 ～ 4294967295 です。

ステップ 8　[Route Map] ドロップダウン リストからルート マップを選択して、ソース ルーティング プロトコルから現在のルーティング プロトコルへのルートのインポートのフィルタリングをオンにします。このパラメータを指定しない場合、すべてのルートが再配布されます。このパラメータを指定し、ルート マップ タグが表示されていない場合、ルートはインポートされません。

ステップ 9　再配布に接続済みルートを含めるには、[Include Connected] チェックボックスをオンにします。

ステップ 10　[Match] チェックボックスをオンにして他のルーティング ドメインへのルートを再配布し、次のチェックボックスの 1 つをオンにします。

- [Internal] は、特定の自律システムの内部にあるルートです。
- [External 1] は、自律システムの外部ながら、OSPFv3 にタイプ 1 外部ルートとしてインポートされるルートです。
- [External 2] は、自律システムの外部ながら、OSPFv3 にタイプ 2 外部ルートとしてインポートされるルートです。
- [NSSA External 1] は、自律システムの外部ながら、IPv6 用の NSSA の OSPFv3 にタイプ 1 の外部ルートとしてインポートされるルートです。
- [NSSA External 2] は、自律システムの外部ながら、IPv6 用の NSSA の OSPFv3 にタイプ 2 の外部ルートとしてインポートされるルートです。

ステップ 11　[OK] をクリックします。

ステップ 12　[Apply] をクリックして変更内容を保存します。

グレースフル リスタートの設定

ASA では、既知の障害状況が発生することがあります。これにより、スイッチング プラットフォーム全体でパケット転送に影響を与えることがあってはなりません。Non-Stop Forwarding（NSF）機能では、ルーティング プロトコル情報を復元している間に、既知のルートへのデータ転送が続行されます。この機能は、コンポーネントに障害がある場合（フェールオーバー（HA）モードで処理を引き継ぐスタンバイ ユニットが存在するアクティブ ユニットがクラッシュした場合や、クラスタ モードで新しいマスターとして選択されたスレーブ ユニットが存在するマスター ユニットがクラッシュした場合など）、またはスケジュールされたヒットレス ソフトウェア アップグレードがある場合に役立ちます。

グレースフル リスタートは、OSPFv2 と OSPFv3 の両方でサポートされています。NSF Cisco（RFC 4811 および RFC 4812）または NSF IETF（RFC 3623）のいずれかを使用して、OSPFv2 上でグレースフル リスタートを設定できます。graceful-restart（RFC 5187）を使用して、OSPFv3 上でグレースフル リスタートを設定できます。

NSF グレースフル リスタート機能の設定には、機能の設定と NSF 対応または NSF 認識としてのデバイスの設定という 2 つのステップが伴います。NSF 対応デバイスは、ネイバーに対して独自のリスタート アクティビティを示すことができ、NSF 認識デバイスはネイバーのリスタートをサポートすることができます。

デバイスは、いくつかの条件に応じて、NSF 対応または NSF 認識として設定できます。

- デバイスは、現在のデバイスのモードに関係なく、NSF 認識デバイスとして設定できます。
- デバイスを NSF 対応として設定するには、デバイスはフェールオーバーまたはスパンド EtherChannel（L2）クラスタ モードのいずれかである必要があります。
- デバイスを NSF 認識または NSF 対応にするには、必要に応じて opaque リンク ステート アドバタイズメント（LSA）/リンク ローカル シグナリング（LLS）ブロックの機能を使って設定する必要があります。

（注）　OSPFv2 用に fast hello が設定されている場合、アクティブ ユニットのリロードが発生し、スタンバイ ユニットがアクティブになっても、グレースフル リスタートは発生しません。これは、ロール変更にかかる時間は、設定されているデッド インターバルよりも大きいためです。

OSPFv2 のグレースフル リスタートの設定

OSPFv2、Cisco NSF および IETF NSF には、2 つのグレースフル リスタート メカニズムがあります。OSPF インスタンスに対しては、これらのグレースフル リスタート メカニズムのうち一度に設定できるのは 1 つだけです。NSF 認識デバイスは、Cisco NSF ヘルパーと IETF NSF ヘルパーの両方として設定できますが、NSF 対応デバイスは OSPF インスタンスに対して、Cisco NSF または IETF NSF モードのいずれかとして設定できます。

OSPFv2 の Cisco NSF グレースフル リスタートの設定

NSF 対応または NSF 認識デバイスに対して、OSPFv2 の Cisco NSF グレースフル リスタートを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [Advanced] > [Add NSF Properties] の順に選択します。

ステップ 2　[Configuring Cisco NSF] の下で、[Enable Cisco nonstop forwarding (NSF)] チェックボックスをオンにします。

ステップ 3　（オプション）必要に応じて、[Cancels NSF restart when non-NSF-aware neighboring networking devices are detected] チェックボックスをオンにします。

ステップ 4　（オプション）[Configuring Cisco NSF helper] の下で、[Enable Cisco nonstop forwarding (NSF) for helper mode] チェックボックスをオフにします。

（注）　このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスで Cisco NSF ヘルパー モードをディセーブルにするには、このチェックボックスをオフにします。

ステップ 5　[OK] をクリックします。

ステップ 6　[Apply] をクリックして変更内容を保存します。

OSPFv2 の IETF NSF グレースフル リスタートの設定

NSF 対応または NSF 認識デバイスに対して、OSPFv2 の IETF NSF グレースフル リスタートを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [Advanced] > [Add NSF Properties] の順に選択します。

ステップ 2　[Configuring IETF NSF] で、[Enable IETF nonstop forwarding (NSF)] チェックボックスをオンにします。

ステップ 3　（オプション）[Length of graceful restart interval] フィールドに、リスタート間隔を秒単位で入力します。

（注）　デフォルト値は 120 秒です。30 秒以下のリスタート間隔の場合、グレースフル リスタートは終了します。

ステップ 4　（オプション）[Configuring IETF NSF helper] の下で、[Enable IETF nonstop forwarding (NSF) for helper mode] チェックボックスをオフにします。

（注）　このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスで IETF NSF ヘルパー モードをディセーブルにするには、このチェックボックスをオフにします。

ステップ 5　[OK] をクリックします。

ステップ 6　[Apply] をクリックして変更内容を保存します。

OSPFv3 のグレースフル リスタートの設定

OSPFv3 の NSF グレースフル リスタート機能を設定するには、2 つのステップを伴います。NSF 対応としてのデバイスの設定と、NSF 認識としてのデバイスの設定です。OSPFv3 のグレースフル リスタートを設定するには、次の手順を実行します次のコマンドを入力します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] > [Advanced] > [Add NSF Properties] の順に選択します。

ステップ 2　[Configuring Graceful Restart] の下で、[Enable Graceful Restart] チェックボックスをオンにします。

ステップ 3　（オプション）[Restart Interval] フィールドにリスタート間隔の値を入力します。

（注）　デフォルト値は 120 秒です。30 秒以下のリスタート間隔の場合、グレースフル リスタートは終了します。

ステップ 4　[Configuring Graceful Restart Helper] の下で、[Enable Graceful Restart Helper] チェックボックスをオンにします。

（注）　このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスでグレースフル リスタート ヘルパー モードをディセーブルにするには、このチェックボックスをオフにします。

ステップ 5　（オプション）[Enable LSA checking] チェックボックスをオンにして、厳密なリンク ステート アドバタイズメント チェックをイネーブルにします。

（注）　イネーブルにすると、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させることを示します。

ステップ 6　[OK] をクリックします。

ステップ 7　[Apply] をクリックして変更内容を保存します。

OSPF 設定の削除

すでにイネーブルにした OSPFv2 コンフィギュレーション全体を削除するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択します。

ステップ 2　[Enable this OSPF Process] チェックボックスをオフにします。

ステップ 3　[Apply] をクリックします。

すでにイネーブルにした OSPFv3 コンフィギュレーション全体を削除するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。

ステップ 2　[Enable OSPFv3 Process] チェックボックスをオフにします。

ステップ 3　[Apply] をクリックします。

OSPFv2 の設定例

次の例に、さまざまなオプションのプロセスを使用して OSPFv2 をイネーブルにし、設定する方法を示します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択します。

ステップ 2　[Process Instances] タブをクリックし、[OSPF Process 1] フィールドに **2** と入力します。

ステップ 3　[Area/Networks] タブをクリックし、[Add] をクリックします。

ステップ 4　[Area ID] フィールドに **0** と入力します。

ステップ 5　[Area Networks] 領域の [IP Address] フィールドに **10.0.0.0** と入力します。

ステップ 6　[Netmask] ドロップダウン リストで [255.0.0.0] を選択します。

ステップ 7　[OK] をクリックします。

ステップ 8　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Redistribution] の順に選択します。

ステップ 9　[Add] をクリックします。

[Add/Edit OSPF Redistribution Entry] ダイアログボックスが表示されます。

ステップ 10　[Protocol] 領域の [OSPF] オプション ボタンをクリックして、ルートが再配布されるソース プロトコルを指定します。[OSPF] を選択すると、別の OSPF ルーティング プロセスからのルートが再配布されるようになります。

ステップ 11　OSPF プロセス ID を [OSPF Process] ドロップダウン リストで選択します。

ステップ 12　[Match] 領域の [Internal] チェックボックスをオンにします。

ステップ 13　[Metric Value] フィールドに、再配布されるルーティングのメトリック値として **5** を入力します。

ステップ 14　[Metric Type] ドロップダウン リストで、メトリック タイプの値として 1 を選択します。

ステップ 15　[Route Map] ドロップダウン リストで、1 を選択します。

ステップ 16　[OK] をクリックします。

ステップ 17　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Interface] の順に選択します。

ステップ 18　[Properties] タブで、[inside] インターフェイスを選択して [Edit] をクリックします。

[Edit OSPF Properties] ダイアログボックスが表示されます。

ステップ 19　[Cost] フィールドに **20** と入力します。

ステップ 20　[Advanced] をクリックします。

ステップ 21　[Retransmit Interval] フィールドに **15** と入力します。

ステップ 22　[Transmit Delay] フィールドに **20** と入力します。

ステップ 23　[Hello Interval] フィールドに **10** と入力します。

ステップ 24　[Dead Interval] フィールドに **40** と入力します。

ステップ 25　[OK] をクリックします。

ステップ 26　[Edit OSPF Properties] ダイアログボックスで、[Priorities] フィールドに **20** と入力して [OK] をクリックします。

ステップ 27　[Authentication] タブをクリックします。

[Edit OSPF Authentication] ダイアログボックスが表示されます。

ステップ 28　[Authentication] 領域の [MD5] オプション ボタンをクリックします。

ステップ 29　[MD5 and Key ID] 領域の [MD5 Key] フィールドに **cisco** と入力し、[MD5 Key ID] フィールドに **1** と入力します。

ステップ 30　[OK] をクリックします。

ステップ 31　[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択し、[Area/Networks] タブをクリックします。

ステップ 32　[OSPF 2] プロセスを選択し、[Edit] を選択します。

[Edit OSPF Area] ダイアログボックスが表示されます。

ステップ 33　[Area Type] 領域で、[Stub] を選択します。

ステップ 34　[Authentication] 領域で、[None] を選択し、[Default Cost] フィールドに **20** と入力します。

ステップ 35　[OK] をクリックします。

ステップ 36　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] の順に選択します。

ステップ 37　[Process Instances] タブをクリックし、[OSPF process 2] チェックボックスをオンにします。

ステップ 38　[Advanced] をクリックします。

[Edit OSPF Area] ダイアログボックスが表示されます。

ステップ 39　[Timers] 領域で、[SPF Delay Time] フィールドに **10** と入力し、[SPF Hold Time] フィールドに **20** と入力します。

ステップ 40　[Adjacency Changes] 領域の [Log Adjacency Change Details] チェックボックスをオンにします。

ステップ 41　[OK] をクリックします。

ステップ 42　[Reset] をクリックします。

OSPFv3の設定例

次に、ASDM で OSPFv3 ルーティングを設定する例を示します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] の順に選択します。

ステップ 2　[Process Instances] タブで、次の手順を実行します。

a. [Enable OSPFv3 Process] チェックボックスをオンにします。

b. [Process ID] フィールドに **1** を入力します。

ステップ 3　[Areas] タブをクリックします。続いて [Add] をクリックして、[Add OSPFv3 Area] ダイアログボックスを表示します。

ステップ 4　[OSPFv3 Process ID] ドロップダウン リストから、**1** を選択します。

ステップ 5　[Area ID] フィールドに **22** を入力します。

ステップ 6　[Area Type] ドロップダウン リストから [Normal] を選択します。

ステップ 7　[Default Cost] フィールドに **10** を入力します。

ステップ 8　[Redistribution imports routes to normal and NSSA areas] をオンにします。

ステップ 9　[Metric] フィールドに **20** を入力します。

ステップ 10　[Metric Type] ドロップダウン リストから **1** を選択します。

ステップ 11　使用されているインターフェイスの指定に合わせて、**内部**チェックボックスをオンにします。

ステップ 12　[Enable Authentication] チェックボックスをオンにします。

ステップ 13　[Security Policy Index] フィールドに **300** を入力します。

ステップ 14　[Authentication Algorithm] ドロップダウン リストから [SHA-1] を選択します。

ステップ 15　[Authentication Key] フィールドに **12345ABCDE** を入力します。

ステップ 16　[Encryption Algorithm] ドロップダウン リストから [DES] を選択します。

ステップ 17　[Encryption Key] フィールドに **1122334455aabbccddee** を入力します。

ステップ 18　[OK] をクリックします。

ステップ 19　[Route Summarization] タブをクリックし、続いて [Add] をクリックして、[Add Route Summarization] ダイアログボックスを表示します。

ステップ 20　[Process ID] ドロップダウン リストから **1** を選択します。

ステップ 21　[Area ID] ドロップダウン リストから **22** を選択します。

ステップ 22　[IPv6 Prefix/Prefix Length] フィールドに **2000:122::/64** を入力します。

ステップ 23　（オプション）[Cost] フィールドに **100** を入力します。

ステップ 24　[Advertised] チェックボックスをオンにします。

ステップ 25　[OK] をクリックします。

ステップ 26　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Interface] の順に選択します。

ステップ 27　[Properties] タブをクリックします。

ステップ 28　内部チェックボックスをオンにし、[Edit] をクリックして、[Edit OSPF Properties] ダイアログボックスを表示します。

ステップ 29　[Cost] フィールドに **20** と入力します。

ステップ 30　[Priority] フィールドに **1** を入力します。

ステップ 31　[Point-to-Point] チェックボックスをオンにします。

ステップ 32　[Dead Interval] フィールドに **40** と入力します。

ステップ 33　[Hello Interval] フィールドに **10** と入力します。

ステップ 34　[Retransmit Interval] フィールドに **15** と入力します。

ステップ 35　[Transmit Delay] フィールドに **20** と入力します。

ステップ 36　[OK] をクリックします。

ステップ 37　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Redistribution] の順に選択します。

ステップ 38　[Process ID] ドロップダウン リストから **1** を選択します。

ステップ 39　[Source Protocol] ドロップダウン リストから [OSPF] を選択します。

ステップ 40　[Metric] フィールドに **50** を入力します。

ステップ 41　[Metric Type] ドロップダウン リストから **1** を選択します。

ステップ 42　[OK] をクリックします。

ステップ 43　[Apply] をクリックして変更内容を保存します。

OSPF のモニタリング

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。提供される情報は、リソースの使用状況を判定してネットワークの問題を解決するために使用することもできます。また、ノードの到達可能性情報を表示して、デバイス パケットがネットワークを通過するときにとるルーティング パスを見つけることもできます。

OSPFv2 ルーティングのさまざまな統計情報を ASDM でモニタまたは表示するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Monitoring] > [Routing] > [OSPF LSAs] の順に選択します。

ステップ 2　選択してモニタできる OSPF LSA は、タイプ 1 ～ 5 と 7 です。各ペインには、次のように 1 つの LSA タイプが表示されます。

- [Type 1 LSAs] は、特定のエリア内の特定プロセス下にあるすべてのルートを表します。
- [Type 2 LSAs] には、ルータをアドバタイズする指定ルータの IP アドレスが表示されます。
- [Type 3 LSAs] には、宛先ネットワークの IP アドレスが表示されます。
- [Type 4 LSAs] には、AS 境界ルータの IP アドレスが表示されます。
- [Type 5 LSAs] と [Type 7 LSAs] には、AS 外部ネットワークの IP アドレスが表示されます。

ステップ 3　[Refresh] をクリックすると、各 LSA タイプのペインが更新されます。

ステップ 4　メイン ASDM ウィンドウで、[Monitoring] > [Routing] > [OSPF Neighbors] の順に選択します。

[OSPF Neighbors] ペインの各行は 1 つの OSPF ネイバーを表します。さらに、[OSPF Neighbors] ペインにはそのネイバーが実行されているネットワーク、優先度、状態、デッド時間（秒単位）、ネイバーの IP アドレス、および実行されているインターフェイスも表示されます。OSPF ネイバーが取る可能性のある状態の一覧については、RFC 2328 を参照してください。

ステップ 5　[Refresh] をクリックすると、[OSPF Neighbors] ペインが更新されます。

OSPFv3 ルーティングのさまざまな統計情報を ASDM でモニタまたは表示するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Monitoring] > [Routing] > [OSPFv3 LSAs] の順に選択します。

ステップ 2　OSPFv3 LSA を選択し、モニタすることができます。[Link State type] ドロップダウン リストでリンク ステート タイプを選択し、指定されたパラメータに従って状態を表示します。サポートされるリンク ステート タイプは、ルータ、ネットワーク、エリア間プレフィックス、エリア間ルータ、AS エクスターナル、NSSA、リンク、エリア内プレフィックスです。

ステップ 3　[Refresh] をクリックして、各リンク ステート タイプを更新します。

ステップ 4　メイン ASDM ウィンドウで、[Monitoring] > [Routing] > [OSPFv3 Neighbors] の順に選択します。

[OSPFv3 Neighbors] ペインの各行は 1 つの OSPFv3 ネイバーを表します。さらに、[OSPFv3 Neighbors] ペインには、ネイバーの IP アドレス、優先度、状態、秒単位のデッド タイム量、動作中のインターフェイスが表示されます。OSPFv3 ネイバーが取る可能性のある状態の一覧については、RFC 5340 を参照してください。

ステップ 5　[Refresh] をクリックすると、[OSPFv3 Neighbors] ペインが更新されます。

その他の関連資料

RFC

RFC	タイトル
2328	OSPFv2
4552	『OSPFv3 Authentication』
5340	『OSPF for IPv6』

OSPF の機能履歴

表 23-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 23-1　OSPF の機能履歴

機能名	プラットフォーム リリース	機能情報
OSPF サポート	7.0(1)	Open Shortest Path First（OSPF）ルーティング プロトコルを使用した、データのルーティング、認証、およびルーティング情報の再配布とモニタについて、サポートが追加されました。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [OSPF]。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	OSPFv2 ルーティングは、マルチ コンテキスト モードでサポートされます。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing]> [OSPF] > [Setup]
クラスタリング		OSPFv2 および OSPFv3 の場合、バルク同期、ルートの同期およびスパンド EtherChannel ロード バランシングは、クラスタリング環境でサポートされます。
IPv6 の OSPFv3 サポート		OSPFv3 ルーティングが IPv6 に対してサポートされます。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Interface]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Redistribution]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Summary Prefix]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Virtual Link]、[Monitoring] > [Routing] > [OSPFv3 LSAs]、[Monitoring] > [Routing] > [OSPFv3 Neighbors]。

表 23-1　OSPF の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
Fast Hello に対する OSPF サポート	9.2(1)	OSPF は、Fast Hello パケット機能をサポートしているため、OSPF ネットワークでのコンバージェンスが高速なコンフィギュレーションになります。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Interface] > [Edit OSPF Interface Advanced Properties]
タイマー		新しい OSPF タイマーを追加し、古いタイマーを廃止しました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [Edit OSPF Process Advanced Properties]
アクセス リストを使用したルート フィルタリング		ACL を使用したルート フィルタリングがサポートされるようになりました。 次の画面が追加されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > Filtering Rules] > [Add Filter Rules]
OSPF モニタリングの強化		OSPF モニタリングの詳細情報が追加されました。
OSPF 再配布 BGP		OSPF 再配布機能が追加されました。 次の画面が追加されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Redistribution]
ノンストップ フォワーディング（NSF）に対する OSPF のサポート	9.3(1)	NSF に対する OSPFv2 および OSPFv3 のサポートが追加されました。 次の画面が追加されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [NSF Properties]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] > [NSF Properties]

EIGRP

この章では、Enhanced Interior Gateway Routing Protocol（EIGRP）を使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Cisco ASA を設定する方法について説明します。

EIGRP に関する情報

EIGRP は、シスコが開発した、IGRP の拡張バージョンです。IGRP や RIP と異なり、EIGRP が定期的にルート アップデートを送信することはありません。EIGRP アップデートは、ネットワーク トポロジが変更された場合にだけ送信されます。EIGRP を他のルーティング プロトコルと区別する主な機能には、迅速なコンバージェンス、可変長サブネット マスクのサポート、部分的アップデートのサポート、複数のネットワーク レイヤ プロトコルのサポートなどがあります。

EIGRP を実行するルータでは、すべてのネイバー ルーティング テーブルが格納されているため、代替ルートに迅速に適応できます。適切なルートが存在しない場合、EIGRP はそのネイバーにクエリーを送信して代替のルートを検出します。これらのクエリーは、代替ルートが検出されるまで伝搬します。EIGRP では可変長サブネット マスクがサポートされているため、ルートはネットワーク番号の境界で自動的に集約されます。さらに、任意のインターフェイスの任意のビット境界で集約を行うように EIGRP を設定することもできます。EIGRP は定期的なアップデートを行いません。その代わり、ルートのメトリックが変更されたときだけ、部分的なアップデートを送信します。部分的アップデートの伝搬では、境界が自動的に設定されるため、その情報を必要とするルータだけがアップデートされます。これらの 2 つの機能により、EIGRP の帯域幅消費量は IGRP に比べて大幅に減少します。

ネイバー探索は、ASA が、直接接続されているネットワーク上にある他のルータをダイナミックに把握するために使用するプロセスです。EIGRP ルータは、マルチキャスト hello パケットを送信して、ネットワーク上に自分が存在していることを通知します。ASA は、新しいネイ

バーから hello パケットを受信すると、トポロジ テーブルに初期化ビットを設定してそのネイバーに送信します。ネイバーは、初期化ビットが設定されたトポロジ アップデートを受信すると、自分のトポロジ テーブルを ASA に返送します。

hello パケットはマルチキャスト メッセージとして送信されます。hello メッセージへの応答は想定されていません。ただし、スタティックに定義されたネイバーの場合は例外です。**neighbor** コマンドを使用して（または ASDM で [Hello Interval] を設定して）ネイバーを設定すると、そのネイバーへ送信される hello メッセージはユニキャスト メッセージとして送信されます。ルーティング アップデートと確認応答が、ユニキャスト メッセージとして送信されます。

このネイバー関係が確立した後は、ネットワーク トポロジが変更された場合にだけ、ルーティング アップデートが交換されます。ネイバー関係は、hello パケットによって維持されます。ネイバーから受信した各 hello パケットには、保持時間が含まれています。ASA は、この時間内にそのネイバーから hello パケットを受信すると想定できます。ASA が保持時間内にそのネイバーからアドバタイズされた hello パケットを受信しない場合、ASA はそのネイバーを使用不能と見なします。

EIGRP プロトコルでは、4 つの主要なアルゴリズム テクノロジー、4 つの主要なテクノロジーを使用します。これに含まれるものには、ネイバー探索/リカバリ、Reliable Transport Protocol（RTP）、DUAL（ルート計算に重要）があります。DUAL は、最小コストのルートだけでなく、宛先へのすべてのルートをトポロジ テーブルに保存します。最小コストのルートはルーティング テーブルに挿入されます。その他のルートは、トポロジ テーブルに残ります。メイン ルートに障害が起きると、他のルートが代わりの適切なルートから選ばれます。サクセサとは、宛先への最小コスト パスを持ち、パケット転送に使用される隣接ルータです。フィジビリティ計算によって、パスがルーティング ループを形成しないことが保証されます。

フィジブル サクセサがトポロジ テーブル内にない場合、必ずルート計算が発生します。ルートの再計算中、DUAL は EIGRP ネイバーにルートを求めるクエリーを送信して、次に EIGRP ネイバーがそのネイバーにクエリーを送信します。ルートのフィジブル サクセサがないルータは、到達不能メッセージを返します。

ルートの再計算中、DUAL は、ルートをアクティブとマークします。デフォルトでは、ASA は、ネイバーから応答が返ってくるのを 3 分間待ちます。ASA がネイバーから応答を受信しないと、そのルートは stuck-in-active とマークされます。トポロジ テーブル内のルートのうち、応答しないネイバーをフィジブル サクセサとして指しているものはすべて削除されます。

（注） EIGRP ネイバー関係では、GRE トンネルを使用しない IPsec トンネルの通過はサポートされていません。

クラスタリングの使用

EIGRP でクラスタリングを使用する方法については、「ダイナミック ルーティングおよびクラスタリング」（P.19-10）を参照してください。

EIGRP のライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

フェールオーバーのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでステートフル フェールオーバーをサポートします。

IPv6 のガイドライン

IPv6 はサポートされません。

クラスタリングのガイドライン

- EIGRP と OSPFv2 の両方を使用するように設定した場合、スパンド EtherChannel および個別インターフェイス クラスタリングがサポートされます。
- 個別インターフェイス クラスタ設定では、EIGRP の隣接関係がマスター ユニットの共有インターフェイスの 2 つのコンテキスト間でのみ確立されます。各クラスタ ノードに対応する複数のネイバー ステートメントを個別に手動で設定すると、この問題を回避できます。

その他のガイドライン

- マルチキャスト トラフィックのコンテキスト間交換がサポートされていないため、EIGRP インスタンスは共有インターフェイス間で相互に隣接関係を形成できません。
- 最大 1 つの EIGRP プロセスがサポートされます。

EIGRP プロセスを設定するためのタスク リスト

ASA での EIGRP ルーティングを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] の順に選択します。

ステップ 2　EIGRP ルーティング プロセスをイネーブルにするには、[Process Instances] タブの [Enable this EIGRP process] チェックボックスをオンにします。「EIGRP のイネーブル化」（P.24-4）または「EIGRP スタブ ルーティングのイネーブル化」（P.24-5）を参照してください。

ステップ 3　[Setup] > [Networks] タブで、EIGRP ルーティングに参加するネットワークとインターフェイスを定義します。詳細については、「EIGRP ルーティング プロセスのネットワークの定義」（P.24-7）を参照してください。

ステップ 4　（オプション）[Filter Rules] ペインでルート フィルタを定義します。ルート フィルタにより、EIGRP 更新で送受信することを許可されているルートをより細かく制御できます。詳細については、「EIGRP でのネットワークのフィルタリング」（P.24-15）を参照してください。

ステップ 5　（オプション）[Redistribution] ペインでルート再配布を定義します。

RIP および OSPF で検出されたルートを、EIGRP ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、EIGRP ルーティング プロセスに再配布できます。詳細については、「EIGRP へのルートの再配布」（P.24-13）を参照してください。

ステップ 6　（オプション）[Static Neighbor] ペインでスタティック EIGRP ネイバーを定義します。

詳細については、「EIGRP ネイバーの定義」（P.24-12）を参照してください。

ステップ 7　（オプション）[Summary Address] ペインで、サマリー アドレスを定義します。

サマリー アドレスの定義の詳細については、「インターフェイスでのサマリー集約アドレスの設定」（P.24-9）を参照してください。

ステップ 8　（オプション）[Interfaces] ペインで、インターフェイス固有の EIGRP パラメータを定義します。これらのパラメータには、EIGRP メッセージ認証、保持時間、hello 間隔、遅延メトリック、スプリットホライズンの使用などがあります。詳細については、「EIGRP のインターフェイスの設定」（P.24-8）を参照してください。

ステップ 9　（オプション）[Default Information] ペインで、EIGRP 更新でのデフォルト ルート情報の送受信を制御します。デフォルトでは、デフォルト ルートが送信され、受け入れられます。詳細については、「EIGRP でのデフォルト情報の設定」（P.24-18）を参照してください。

EIGRP の設定

この項では、システムで EIGRP プロセスをイネーブルにする方法について説明します。EIGRP をイネーブルにした後に、システムで EIGRP プロセスをカスタマイズする方法については、次の項を参照してください。

- 「EIGRP のイネーブル化」（P.24-4）
- 「EIGRP スタブ ルーティングのイネーブル化」（P.24-5）

EIGRP のイネーブル化

ASA では、EIGRP ルーティング プロセスを 1 つだけイネーブルにできます。

EIGRP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　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

[EIGRP Setup] ペインが表示されます。

メインの [EIGRP Setup] ペインには、EIGRP をイネーブルにするための次の 3 つのタブがあります。

- [Process Instances] タブでは、各コンテキストの EIGRP ルーティング プロセスをイネーブルにすることができます。シングル コンテキスト モードおよびマルチ コンテキスト モードの両方がサポートされます。詳細については、「EIGRP のイネーブル化」（P.24-4）と「EIGRP スタブ ルーティングのイネーブル化」（P.24-5）を参照してください。

- [Networks] タブでは、EIGRP ルーティング プロセスで使用されるネットワークを指定できます。EIGRP ルーティングに参加するインターフェイスは、これらのネットワーク エントリで定義されるアドレスの範囲内に存在する必要があります。アドバタイズされる直接接続およびスタティックのネットワークも、これらのネットワーク エントリの範囲内である必要があります。詳細については、「EIGRP ルーティング プロセスのネットワークの定義」（P.24-7）を参照してください。
- [Passive Interfaces] タブでは、1 つ以上のインターフェイスをパッシブ インターフェイスとして設定できます。EIGRP では、パッシブ インターフェイスはルーティング アップデートの送受信を行いません。[Passive Interface] テーブルには、パッシブ インターフェイスとして定義されているインターフェイスが一覧表示されます。

ステップ 2　[Enable this EIGRP process] チェックボックスをオンにします。

デバイスでイネーブルにすることができる EIGRP ルーティング プロセスは 1 つだけです。変更を保存できるようにするには、ルーティング プロセスの自律システム（AS）番号を [EIGRP Process] フィールドに入力する必要があります。

ステップ 3　[EIGRP Process] フィールドに、EIGRP プロセスの自律システム（AS）番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 4　（オプション）EIGRP プロセスの設定を指定するには、[Advanced] をクリックします。指定できる設定には、ルータ ID、デフォルトのメトリック、スタブ ルーティング、ネイバー変更、EIGRP ルートのアドミニストレーティブ ディスタンスなどがあります。

ステップ 5　[Networks] タブをクリックします。

ステップ 6　新しいネットワーク エントリを追加するには、[Add] をクリックします。

[Add EIGRP Network] ダイアログボックスが表示されます。ネットワーク エントリを削除するには、テーブルでそのエントリを選択して [Delete] をクリックします。

ステップ 7　ドロップダウン リストから、EIGRP ルーティング プロセスの AS 番号を選択します。

ステップ 8　[IP Address] フィールドに、EIGRP ルーティング プロセスに参加するネットワークの IP アドレスを入力します。

（注）　ネットワーク エントリを変更するには、まずそのエントリを削除してから新しいエントリを追加する必要があります。既存のエントリは編集できません。

ステップ 9　[Network Mask] フィールドに、IP アドレスに適用するネットワーク マスクを入力します。

ステップ 10　[OK] をクリックします。

EIGRP スタブ ルーティングのイネーブル化

ASA は、EIGRP スタブ ルータとしてイネーブル化し、設定することができます。スタブ ルーティングを使用すると、ASA で必要となるメモリおよび処理要件を減らすことができます。ASA をスタブ ルータとして設定すると、ローカル以外のトラフィックがすべて配布ルータに転送されるようになり、完全な EIGRP ルーティング テーブルを維持する必要がなくなります。一般に、配布ルータからスタブ ルートに送信する必要があるのは、デフォルト ルートだけです。

スタブ ルータから配布ルータには、指定されたルートだけが伝搬されます。スタブ ルータである ASA は、サマリー、接続されているルート、再配布されたスタティック ルート、外部ルート、および内部ルートに対するクエリーすべてに、応答として「inaccessible」というメッセージを返します。ASA がスタブとして設定されているときは、自身のスタブ ルータとして

のステータスを報告するために、特殊なピア情報パケットがすべての隣接ルータに送信されます。スタブ ステータスの情報を伝えるパケットを受信したネイバーはすべて、スタブ ルータにルートのクエリーを送信しなくなり、スタブ ピアを持つルータはそのピアのクエリーを送信しなくなります。スタブ ルータが正しいアップデートをすべてのピアに送信するには、配布ルータが必要です。

ASA を EIGRP スタブ ルーティング プロセスとして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　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2　[Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3　[EIGRP Process] フィールドに、EIGRP プロセスの自律システム（AS）番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 4　EIGRP スタブ ルーティング プロセスを設定するには、[Advanced] をクリックします。

[Edit EIGRP Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 5　[Edit EIGRP Process Advanced Properties] ダイアログボックスの [Stub] 領域で、次の EIGRP スタブ ルーティング プロセスのうち 1 つ以上を選択します。

- [Stub Receive only]：隣接ルータからルート情報を受信しても、それらの隣接ルータにルート情報を送信しない EIGRP スタブ ルーティング プロセスを設定します。このオプションを選択する場合は、他のスタブ ルーティング オプションを選択できません。
- [Stub Connected]：接続済みルートをアドバタイズします。
- [Stub Static]：スタティック ルートをアドバタイズします。
- [Stub Redistributed]：再配布ルートをアドバタイズします。
- [Stub Summary]：サマリー ルートをアドバタイズします。

ステップ 6　[OK] をクリックします。

ステップ 7　[Networks] タブをクリックします。

ステップ 8　[Add] をクリックして、新しいネットワーク エントリを追加します。

[Add EIGRP Network] ダイアログボックスが表示されます。ネットワーク エントリを削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。

ステップ 9　ドロップダウン リストから、EIGRP ルーティング プロセスの AS 番号を選択します。

ステップ 10　[IP Address] フィールドに、EIGRP ルーティング プロセスに参加するネットワークの IP アドレスを入力します。

（注）　ネットワーク エントリを変更するには、まずそのエントリを削除してから新しいエントリを追加する必要があります。既存のエントリは編集できません。

ステップ 11　[Network Mask] フィールドに、IP アドレスに適用するネットワーク マスクを入力します。

ステップ 12　[OK] をクリックします。

EIGRP のカスタマイズ

ここでは、EIGRP ルーティングをカスタマイズする方法について説明します。

EIGRP ルーティング プロセスのネットワークの定義

[Network] テーブルでは、EIGRP ルーティング プロセスで使用されるネットワークを指定できます。EIGRP ルーティングに参加するインターフェイスは、これらのネットワーク エントリで定義されるアドレスの範囲内に存在する必要があります。アドバタイズされる直接接続およびスタティックのネットワークも、これらのネットワーク エントリの範囲内である必要があります。

[Network] テーブルには、EIGRP ルーティング プロセス用に設定されているネットワークが表示されます。このテーブルの各行には、指定した EIGRP ルーティング プロセス用に設定されているネットワーク アドレスおよび関連するマスクが表示されます。

ネットワークの追加または削除を行うには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2　[Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3　[EIGRP Process] フィールドに、EIGRP プロセスの自律システム（AS）番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 4　[Networks] タブをクリックします。

ステップ 5　[Add] をクリックして、新しいネットワーク エントリを追加します。

[Add EIGRP Network] ダイアログボックスが表示されます。ネットワーク エントリを削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。

ステップ 6　ドロップダウン リストから、EIGRP ルーティング プロセスの AS 番号を選択します。

ステップ 7　[IP Address] フィールドに、EIGRP ルーティング プロセスに参加するネットワークの IP アドレスを入力します。

（注）　ネットワーク エントリを変更するには、まずそのエントリを削除してから新しいエントリを追加する必要があります。既存のエントリは編集できません。

ステップ 8　[Network Mask] フィールドに、IP アドレスに適用するネットワーク マスクを入力します。

ステップ 9　[OK] をクリックします。

EIGRP のインターフェイスの設定

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、インターフェイスが接続されているネットワークが対象に含まれるように ASA を設定し、そのインターフェイスが EIGRP アップデートを送受信しないようにします。

EIGRP についてインターフェイスを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2　[Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3　[OK] をクリックします。

ステップ 4　[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Interfaces] の順に選択します。

[Interface] ペインが表示され、EIGRP インターフェイスの設定が表示されます。[Interface Parameters] テーブルには、ASA のインターフェイスすべてが表示され、インターフェイスごとに次の設定を修正できます。

- 認証キーとモード。
- EIGRP hello 間隔と保持時間。
- EIGRP メトリックの計算で使用されるインターフェイス遅延メトリック。
- インターフェイスでのスプリットホライズンの使用。

ステップ 5　インターフェイス エントリを選択するには、インターフェイス エントリをダブルクリックするか、そのエントリを選択して [Edit] をクリックします。

[Edit EIGRP Interface Entry] ダイアログボックスが表示されます。

ステップ 6　[EIGRP Process] フィールドに、EIGRP プロセスの AS 番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 7　[Hello Interval] フィールドに、インターフェイス上で送信される EIGRP hello パケット間の間隔を入力します。

有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。

ステップ 8　[Hold Time] フィールドに、保持時間を秒単位で入力します。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 15 秒です。

ステップ 9　[Split Horizon] の [Enable] チェックボックスをオンにします。

ステップ 10　[Delay] フィールドに、遅延の値を入力します。遅延時間は 10 マイクロ秒単位です。有効な値の範囲は 1 ～ 16777215 です。

ステップ 11　[Enable MD5 Authentication] チェックボックスをオンにして、EIGRP プロセス メッセージの MD5 認証をイネーブルにします。

ステップ 12　[Key] または [Key ID] の値を入力します。

- [Key] フィールドに、EIGRP 更新を認証するキーを入力します。このキーには、最大 16 文字を含めることができます。
- [Key ID] フィールドに、キー ID 値を入力します。有効値の範囲は、1 ～ 255 です。

ステップ 13　[OK] をクリックします。

受動インターフェイスの設定

1 つ以上のインターフェイスを受動インターフェイスとして設定できます。EIGRP の場合、受動インターフェイスではルーティング アップデートが送受信されません。

受動インターフェイスを設定するには、次の手順を実行します。

（注）　ASDM の [Passive Interface] テーブルには、パッシブ インターフェイスとして設定されているインターフェイスが一覧表示されます。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2　[Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3　[OK] をクリックします。

ステップ 4　[Passive Interfaces] タブをクリックします。

ステップ 5　設定するインターフェイスをドロップダウン リストから選択します。

ステップ 6　[Suppress routing updates on all interfaces] チェックボックスをオンにすると、すべてのインターフェイスがパッシブとして指定されます。[Passive Interface] テーブルに表示されていないインターフェイスも、このチェックボックスがオンのときはパッシブとして設定されます。

ステップ 7　パッシブ インターフェイス エントリを追加するには [Add] をクリックします。

[Add EIGRP Passive Interface] ダイアログボックスが表示されます。パッシブにするインターフェイスを選択して [Add] をクリックします。パッシブ インターフェイスを削除するには、テーブルでそのインターフェイスを選択して [Delete] をクリックします。

ステップ 8　[OK] をクリックします。

インターフェイスでのサマリー集約アドレスの設定

サマリー アドレスはインターフェイスごとに設定できます。ネットワーク番号の境界以外でサマリー アドレスを作成する場合、または自動ルート集約がディセーブルになった ASA でサマリー アドレスを使用する場合は、手動でサマリー アドレスを定義する必要があります。ルー

ティング テーブルに他にも個別のルートがある場合、EIGRP は、他の個別ルートすべての中で最小のメトリックと等しいメトリックで、サマリー アドレスをインターフェイスからアドバタイズします。

サマリー アドレスを作成するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Interfaces] の順に選択します。

[Interface] ペインには、EIGRP インターフェイスの設定が表示されます。[Interface Parameters] テーブルには、ASA のすべてのインターフェイスが表示され、設定をインターフェイスごとに修正できます。これらの設定の詳細については、「EIGRP のインターフェイスの設定」（P.24-8）を参照してください。

ステップ 2　インターフェイスの EIGRP パラメータを設定するには、インターフェイス エントリをダブルクリックするか、そのエントリを選択して [Edit] をクリックします。

ステップ 3　[OK] をクリックします。

ステップ 4　[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Summary Address] の順に選択します。

[Summary Address] ペインには、スタティックに定義された EIGRP サマリー アドレスのテーブルが表示されます。デフォルトでは、EIGRP はサブネット ルートをネットワーク レベルに集約します。[Summary Address] ペインでは、サブネット レベルに集約されるスタティックに定義された EIGRP サマリー アドレスを作成できます。

ステップ 5　新しい EIGRP サマリー アドレスを追加するには [Add] をクリックし、テーブル内の既存の EIGRP サマリー アドレスを編集するには [Edit] をクリックします。

[Add Summary Address] または [Edit Summary Address] ダイアログボックスが表示されます。テーブルのエントリをダブルクリックして編集することもできます。

ステップ 6　[EIGRP Process] フィールドに、EIGRP プロセスの自律システム（AS）番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 7　[Interface] ドロップダウン リストで、どのインターフェイスからこのサマリー アドレスをアドバタイズするかを選択します。

ステップ 8　[IP Address] フィールドに、サマリー ルートの IP アドレスを入力します。

ステップ 9　[Netmask] フィールドで、IP アドレスに適用されるネットワーク マスクを選択するか入力します。

ステップ 10　ルートのアドミニストレーティブ ディスタンスを [Administrative Distance] フィールドに入力します。空白のままにすると、ルートのアドミニストレーティブ ディスタンスはデフォルト値の 5 になります。

ステップ 11　[OK] をクリックします。

インターフェイス遅延値の変更

インターフェイス遅延値は、EIGRP ディスタンス計算で使用されます。この値は、インターフェイスごとに変更できます。

インターフェイス遅延値を変更するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Interfaces] の順に選択します。

[Interface] ペインには、EIGRP インターフェイスの設定が表示されます。[Interface Parameters] テーブルには、ASA のすべてのインターフェイスが表示され、設定をインターフェイスごとに修正できます。これらの設定の詳細については、「EIGRP のインターフェイスの設定」（P.24-8）を参照してください。

ステップ 2　インターフェイスの EIGRP パラメータの遅延値を設定するには、インターフェイス エントリをダブルクリックするか、インターフェイス エントリを選択して [Edit] をクリックします。

[Edit EIGRP Interface Entry] ダイアログボックスが表示されます。

ステップ 3　[Delay] フィールドに、遅延時間を 10 マイクロ秒単位で入力します。有効な値は、1 ～ 16777215 です。

ステップ 4　[OK] をクリックします。

インターフェイスでの EIGRP 認証のイネーブル化

EIGRP ルート認証では、EIGRP ルーティング プロトコルからのルーティング アップデートに対する MD5 認証を提供します。MD5 キーを使用したダイジェストが各 EIGRP パケットに含まれており、承認されていない送信元からの不正なルーティング メッセージや虚偽のルーティング メッセージが取り込まれないように阻止します。

EIGRP ルート認証は、インターフェイスごとに設定します。EIGRP メッセージ認証対象として設定されたインターフェイス上にあるすべての EIGRP ネイバーには、隣接関係を確立できるように同じ認証モードとキーを設定する必要があります。

（注）　EIGRP ルート認証をイネーブルにするには、事前に EIGRP をイネーブルにする必要があります。

インターフェイスでの EIGRP 認証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　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2　[Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3　[EIGRP Process] フィールドに、EIGRP プロセスの自律システム（AS）番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 4　[Networks] タブをクリックします。

ステップ 5　[Add] をクリックして、新しいネットワーク エントリを追加します。

[Add EIGRP Network] ダイアログボックスが表示されます。ネットワーク エントリを削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。

ステップ 6　ドロップダウン リストから、EIGRP ルーティング プロセスの AS 番号を選択します。

ステップ 7　[IP Address] フィールドに、EIGRP ルーティング プロセスに参加するネットワークの IP アドレスを入力します。

（注）　ネットワーク エントリを変更するには、まずそのエントリを削除してから新しいエントリを追加する必要があります。既存のエントリは編集できません。

ステップ 8　[Network Mask] フィールドで、IP アドレスに適用されるネットワーク マスクを選択するか入力します。

ステップ 9　[OK] をクリックします。

ステップ 10　[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Interfaces] の順に選択します。

[Interface] ペインには、EIGRP インターフェイスの設定が表示されます。[Interface Parameters] テーブルには、ASA のすべてのインターフェイスが表示され、設定をインターフェイスごとに修正できます。これらの設定の詳細については、「EIGRP のインターフェイスの設定」（P.24-8）を参照してください。

ステップ 11　[Enable MD5 Authentication] チェックボックスをオンにして、EIGRP プロセス メッセージの MD5 認証をイネーブルにします。このチェックボックスをオンにした後で、次のいずれかを指定します。

- [Key] フィールドに、EIGRP 更新を認証するキーを入力します。このキーの最大長は 16 文字です。
- [Key ID] フィールドに、キー ID 値を入力します。有効値の範囲は、1 ～ 255 です。

ステップ 12　[OK] をクリックします。

EIGRP ネイバーの定義

EIGRP hello パケットはマルチキャスト パケットとして送信されます。EIGRP ネイバーが、トンネルなど、非ブロードキャスト ネットワークを越えた場所にある場合、手動でネイバーを定義する必要があります。手動で EIGRP ネイバーを定義すると、hello パケットはユニキャスト メッセージとしてそのネイバーに送信されます。

手動で EIGRP ネイバーを定義するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2　[Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3　[EIGRP Process] フィールドに、EIGRP プロセスの AS 番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 4　[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Static Neighbor] の順に選択します。

スタティックに定義された EIGRP ネイバーが [Static Neighbor] ペインに表示されます。EIGRP ネイバーは、ASA との間で EIGRP ルーティング情報を送受信します。通常は、ネイバー探索プロセスによってネイバーがダイナミックに検出されます。ただし、ポイントツーポイントの非ブロードキャスト ネットワークでは、ネイバーをスタティックに定義する必要があります。

[Static Neighbor] テーブルの各行には、ネイバーの EIGRP 自律システム番号、ネイバー IP アドレス、およびネイバーに接続するためのインターフェイスが表示されます。

[Static Neighbor] ペインでは、スタティック ネイバーを追加または編集できます。

ステップ 5　EIGRP スタティック ネイバーを追加または編集するには、[Add] または [Edit] をクリックします。

[Add EIGRP Neighbor Entry] または [Edit EIGRP Neighbor Entry] ダイアログボックスが表示されます。

ステップ 6　ネイバーを設定する EIGRP プロセスのドロップダウン リストで EIGRP AS 番号を選択します。

ステップ 7　インターフェイス名を [Interface Name] ドロップダウン リストで選択します。このインターフェイスを通してネイバーが使用可能になります。

ステップ 8　ネイバーの IP アドレスを [Neighbor IP Address] フィールドに入力します。

ステップ 9　[OK] をクリックします。

EIGRP へのルートの再配布

RIP および OSPF で検出されたルートを、EIGRP ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、EIGRP ルーティング プロセスに再配布できます。接続されているルートが、EIGRP コンフィギュレーション内の **network** 文で指定された範囲に含まれている場合は、再配布の必要はありません。

（注）　RIP 限定：この手順を開始する前に、ルート マップを作成し、指定されたルーティング プロトコルのうち RIP ルーティング プロセスに再配布されるルートを詳細に定義する必要があります。ルート マップの作成の詳細については、第 21 章「ルート マップ」を参照してください。

ルートを EIGRP ルーティング プロセスに再配布するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2　[Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3　[EIGRP Process] フィールドに、EIGRP プロセスの AS 番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 4　[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Redistribution] の順に選択します。

[Redistribution] ペインには、他のルーティング プロトコルから EIGRP ルーティング プロセスにルートを再配布するためのルールが表示されます。スタティック ルートや接続済みルートを EIGRP ルーティング プロセスに再配布する場合は、メトリックの設定は必須ではありませんが、設定することを推奨します。[Redistribution] ペインの各行に、1 つのルート再配布エントリが表示されます。

ステップ 5　新しい再配布ルールを追加するには、[Add] をクリックします。既存の再配布ルールを編集する場合は、ステップ 6 に進んでください。

[Add EIGRP Redistribution Entry] ダイアログボックスが表示されます。

ステップ 6　既存の EIGRP スタティック ネイバーを編集するには、テーブル内のアドレスを選択して [Edit] をクリックします。テーブル内のエントリをダブルクリックするという方法でも、そのエントリを編集できます。

[Edit EIGRP Redistribution Entry] ダイアログボックスが表示されます。

ステップ 7　このエントリが適用される EIGRP ルーティング プロセスの AS 番号をドロップダウン リストで選択します。

ステップ 8　[Protocol] 領域で、ルーティング プロセスのプロトコルとして次のいずれかを選択してそのオプション ボタンをクリックします。

- [Static] を選択すると、スタティック ルートが EIGRP ルーティング プロセスに再配布されます。ネットワーク設定の範囲内にあるスタティック ルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。
- [Connected] を選択すると、接続されているルートが EIGRP ルーティング プロセスに再配布されます。ネットワーク設定の範囲内にある接続済みルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。
- [RIP] を選択すると、RIP ルーティング プロセスで検出されたルートが EIGRP に再配布されます。
- [OSPF] を選択すると、OSPF ルーティング プロセスで検出されたルートが EIGRP に再配布されます。

ステップ 9　[Optional Metrics] 領域で、再配布されるルートに使用するメトリックとして次のいずれかを選択します。

- [Bandwidth] は EIGRP 帯域幅メトリックで、単位はキロビット/秒です。有効な値の範囲は 1 ～ 4294967295 です。
- [Delay] は EIGRP 遅延メトリックで、単位は 10 マイクロ秒です。有効値の範囲は、0 ～ 4294967295 です。
- [Reliability] は EIGRP 信頼性メトリックです。有効値の範囲は 0 ～ 255 で、255 は信頼性が 100 % であることを示します。
- [Loading] は EIGRP 有効帯域幅（負荷）メトリックです。有効値の範囲は 1 ～ 255 で、255 は負荷が 100 % であることを示します。
- [MTU] はパスの MTU です。有効な値の範囲は 1 ～ 65535 です。

ステップ 10　ルート マップを [Route Map] ドロップダウン リストで選択し、EIGRP ルーティング プロセスに再配布するルートを定義します。ルート マップの設定方法の詳細については、第 21 章「ルート マップ」を参照してください。

ステップ 11　[Optional OSPF Redistribution] 領域で、どの OSPF ルートを EIGRP ルーティング プロセスに再配布するかをさらに詳しく指定するために、次の OSPF オプション ボタンのいずれかをクリックします。

- [Match Internal] を選択すると、指定されている OSPF プロセスの内部であるルートが対象となります。
- [Match External 1] を選択すると、指定されている OSPF プロセスの外部であるタイプ 1 ルートが対象となります。
- [Match External 2] を選択すると、指定されている OSPF プロセスの外部であるタイプ 2 ルートが対象となります。

- [Match NSSA-External 1] を選択すると、指定されている OSPF NSSA の外部であるタイプ 1 ルートが対象となります。
- [Match NSSA-External 2] を選択すると、指定されている OSPF NSSA の外部であるタイプ 2 ルートが対象となります。

ステップ 12　[OK] をクリックします。

EIGRP でのネットワークのフィルタリング

（注）　この手順を開始する前に、標準の ACL を作成し、その中にアドバタイズするルートを定義する必要があります。つまり、標準の ACL を作成し、その中に送信または受信したアップデートからフィルタリングするルートを定義します。

EIGRP でネットワークをフィルタリングするには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2　[Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3　[EIGRP Process] フィールドに、EIGRP プロセスの AS 番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 4　[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Filter Rules] の順に選択します。

EIGRP ルーティング プロセスに対して設定されているルート フィルタリング ルールが [Filter Rules] ペインに表示されます。フィルタ ルールによって、EIGRP ルーティング プロセスで受け入れまたはアドバタイズされるルートを制御できます。

[Filter Rule] テーブルの各行には、特定のインターフェイスまたはルーティング プロトコルに適用されるフィルタ ルールについての情報が記載されます。たとえば、フィルタ ルールで外部インターフェイスでの「in」方向が指定されている場合は、外部インターフェイスで受信された EIGRP アップデートすべてにフィルタリングが適用されます。フィルタ ルールで方向が「out」、ルーティング プロトコルとして OSPF 10 が指定されている場合は、発信 EIGRP アップデートで EIGRP ルーティング プロセスに再配布されるルートにフィルタ ルールが適用されます。

ステップ 5　フィルタ ルールを追加するには [Add] をクリックします。既存のフィルタ ルールを編集する場合は、ステップ 6 に進んでください。

[Add Filter Rules] ダイアログボックスが表示されます。

ステップ 6　フィルタ ルールを編集するには、テーブルでそのフィルタ ルールを選択して [Edit] をクリックします。

[Edit Filter Rules] ダイアログボックスが表示されます。フィルタ ルールをダブルクリックして編集することもできます。フィルタ ルールを削除するには、テーブルでそのフィルタ ルールを選択して [Delete] をクリックします。

ステップ 7　このエントリが適用される EIGRP ルーティング プロセスの AS 番号をドロップダウン リストで選択します。

ステップ 8　フィルタ ルートの方向をドロップダウン リストで選択します。

着信 EIGRP ルーティング アップデートからのルートをフィルタリングするルールの場合は、[in] を選択します。ASA から送信される EIGRP ルーティング アップデートからのルートをフィルタリングするには、[out] を選択します。

[out] を選択した場合は、[Routing process] フィールドがアクティブになります。フィルタリングするルートのタイプを選択します。スタティック、接続済み、RIP、および OSPF のルーティング プロセスから再配布されるルートをフィルタリングできます。ルーティング プロセスを指定するフィルタは、すべてのインターフェイスで送信される更新からのルートをフィルタリングします。

ステップ 9　OSPF プロセス ID を [ID] フィールドに入力します。

ステップ 10　[Interface] オプション ボタンをクリックしてから、フィルタを適用するインターフェイスを選択します。

ステップ 11　[Add] または [Edit] をクリックして、フィルタ ルールの ACL を定義します。[Edit] をクリックすると、選択されているネットワーク ルールの [Network Rule] ダイアログボックスが開きます。

[Network Rule] ダイアログボックスが表示されます。

ステップ 12　[Action] ドロップダウン リストで、[Permit] を選択すると指定のネットワークのアドバタイズが許可され、[Deny] を選択すると指定のネットワークのアドバタイズが禁止されます。

ステップ 13　[IP Address] フィールドに、許可または禁止するネットワークの IP アドレスを入力します。すべてのアドレスを許可または禁止するには、IP アドレス **0.0.0.0** とネットワーク マスク **0.0.0.0** を使用します。

ステップ 14　[Netmask] ドロップダウン リストで、ネットワークの IP アドレスに適用するネットワーク マスクを選択します。このフィールドにネットワーク マスクを入力するか、リストから共通マスクの 1 つを選択します。

ステップ 15　[OK] をクリックします。

EIGRP Hello 間隔と保持時間のカスタマイズ

ASA は、定期的に hello パケットを送信して、ネイバーを検出したり、ネイバーが到達不能または動作不能になったことを把握したりします。デフォルトでは、hello パケットは 5 秒間隔で送信されます。

hello パケットは、ASA の保持時間をアドバタイズします。保持時間によって、EIGRP ネイバーに、ASA を到達可能と見なす時間の長さを知らせます。アドバタイズされた保持時間内にネイバーが hello パケットを受信しなかった場合、ASA は到達不能と見なされます。デフォルトでは、アドバタイズされる保持時間は 15 秒です（hello 間隔の 3 倍）。

hello 間隔とアドバタイズされる保持時間のいずれも、インターフェイスごとに設定します。保持時間は hello 間隔の 3 倍以上に設定することをお勧めします。

hello 間隔とアドバタイズされる保持時間を設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2　[Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3　[OK] をクリックします。

ステップ 4　[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Interfaces] の順に選択します。

[Interface] ペインに、EIGRP インターフェイスのすべての設定が表示されます。

ステップ 5　インターフェイス エントリをダブル クリックするか、またはエントリを選択して [Edit] をクリックします。

[Edit EIGRP Interface Entry] ダイアログボックスが表示されます。

ステップ 6　EIGRP AS 番号をドロップダウン リストで選択します。このリストに表示されるのは、EIGRP ルーティング プロセスをイネーブルにしたときに設定されていたシステム番号です。

ステップ 7　[Hello Interval] フィールドに、インターフェイス上で送信される EIGRP hello パケット間の間隔を入力します。

有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。

ステップ 8　[Hold Time] フィールドで、保持時間を秒単位で指定します。

有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 15 秒です。

ステップ 9　[OK] をクリックします。

自動ルート集約のディセーブル化

自動ルート集約は、デフォルトでイネーブルになっています。EIGRP ルーティング プロセスは、ネットワーク番号の境界で集約を行います。このことは、不連続ネットワークがある場合にルーティングの問題の原因となることがあります。

たとえば、ネットワーク 192.168.1.0、192.168.2.0、192.168.3.0 が接続されているルータがあり、それらのネットワークがすべて EIGRP に参加しているとすると、EIGRP ルーティング プロセスはそれらのルートに対しサマリー アドレス 192.168.0.0 を作成します。さらにネットワーク 192.168.10.0 と 192.168.11.0 が接続されているルータがこのネットワークに追加され、それらのネットワークが EIGRP に参加すると、これらもまた 192.168.0.0 として集約されます。トラフィックが誤った場所にルーティングされる可能性をなくすために、競合するサマリー アドレスを作成するルータでの自動ルート集約をディセーブルにする必要があります。

自動ルート集約を ASDM でディセーブルにするには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2　[Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3　[Process Instance] タブをクリックします。

ステップ 4　[Advanced] をクリックします。

ステップ 5　[Summary] 領域の [Auto-Summary] チェックボックスをオフにします。

（注）　この設定はデフォルトでイネーブルになっています。

ステップ 6　[OK] をクリックします。

EIGRP でのデフォルト情報の設定

EIGRP アップデート内のデフォルト ルート情報の送受信を制御できます。デフォルトでは、デフォルト ルートが送信され、受け入れられます。デフォルト情報の受信を禁止するように ASA を設定すると、候補のデフォルト ルート ビットが受信ルート上でブロックされます。デフォルト情報の送信を禁止するように ASA を設定すると、アドバタイズされるルートのデフォルト ルート ビット設定がディセーブルになります。

ASDM では、[Default Information] ペインに、EIGRP アップデートでのデフォルト ルート情報の送受信を制御するルールのテーブルが表示されます。EIGRP ルーティング プロセスごとに、「in」ルールと「out」ルールを 1 つずつ設定できます（現在は 1 つのプロセスだけがサポートされています）。

デフォルトでは、デフォルト ルートが送信され、受け入れられます。デフォルトのルート情報の送受信を制限またはディセーブルにするには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

メインの [EIGRP Setup] ペインが表示されます。

ステップ 2　[Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3　[OK] をクリックします。

ステップ 4　次のどちらかを実行します。

- 新しいエントリを作成するには、[Add] をクリックします。
- エントリを編集するには、テーブル内のエントリをダブルクリックするか、テーブル内のエントリを選択して [Edit] をクリックします。

  そのエントリの [Add Default Information] または [Edit Default Information] ダイアログボックスが表示されます。EIGRP AS 番号が [EIGRP] フィールドで自動的に選択されています。

ステップ 5　[Direction] フィールドで、ルールの方向として次のオプションのいずれかを選択します。

- [in]：このルールは、着信 EIGRP アップデートからのデフォルト ルート情報をフィルタリングします。
- [out]：このルールは、発信 EIGRP アップデートからのデフォルト ルート情報をフィルタリングします。

  EIGRP プロセスごとに、「in」ルールと「out」ルールを 1 つずつ設定できます。

ステップ 6　ネットワーク ルール テーブルにネットワーク ルールを追加します。ネットワーク ルールでは、デフォルト ルート情報を送受信するときに許可されるネットワークと拒否されるネットワークを定義します。デフォルト情報フィルタ ルールに追加するネットワーク ルールごとに、次の手順を繰り返します。

a.　ネットワーク ルールを追加するには [Add] をクリックします。既存のネットワーク ルールをダブルクリックしてルールを編集します。

b.　[Action] フィールドで、そのネットワークを許可する場合は [Permit] をクリックし、ブロックする場合は [Deny] をクリックします。

c.　[IP Address] フィールドと [Network Mask] フィールドに、ルールによって許可または拒否されるネットワークの IP アドレスとネットワーク マスクを入力します。

すべてのデフォルト ルート情報の受け入れや送信を拒否するには、ネットワーク アドレスとして **0.0.0.0** を入力し、ネットワーク マスクとして **0.0.0.0** を選択します。

d. 指定したネットワーク ルールをデフォルト情報フィルタ ルールに追加するには、[OK] をクリックします。

ステップ 7　デフォルト情報フィルタ ルールを受け入れるには、[OK] をクリックします。

EIGRP スプリット ホライズンのディセーブル化

スプリット ホライズンは、EIGRP アップデート パケットとクエリー パケットの送信を制御します。スプリット ホライズンがインターフェイスでイネーブルになると、アップデート パケットとクエリー パケットは、このインターフェイスがネクスト ホップとなる宛先には送信されません。この方法でアップデート パケットとクエリー パケットを制御すると、ルーティング ループが発生する可能性が低くなります。

デフォルトでは、スプリット ホライズンはすべてのインターフェイスでイネーブルになっています。

スプリット ホライズンは、ルート情報が、その情報の発信元となるインターフェイスからルータによってアドバタイズされないようにします。通常、特にリンクが切断された場合には、この動作によって複数のルーティング デバイス間の通信が最適化されます。ただし、非ブロードキャスト ネットワークでは、この動作が望ましくない場合があります。このような場合は、EIGRP を設定したネットワークを含め、スプリット ホライズンをディセーブルにする必要が生じることもあります。

インターフェイスでのスプリット ホライズンをディセーブルにする場合、そのインターフェイス上のすべてのルータとアクセス サーバに対してディセーブルにする必要があります。

EIGRP スプリット ホライズンをディセーブルにするには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Interfaces] の順に選択します。

[Interface] ペインが表示され、EIGRP インターフェイスの設定が表示されます。

ステップ 2　インターフェイス エントリをダブル クリックするか、またはエントリを選択して [**Edit**] をクリックします。

[Edit EIGRP Interface Entry] ダイアログボックスが表示されます。

ステップ 3　EIGRP 自律システム（AS）番号をドロップダウン リストで選択します。このリストに表示されるのは、EIGRP ルーティング プロセスをイネーブルにしたときに設定されていたシステム番号です。

ステップ 4　[Split Horizon] チェックボックスをオフにします。

ステップ 5　[OK] をクリックします。

EIGRP プロセスの再始動

EIGRP プロセスを再始動したり、再配布またはカウンタをクリアしたりするには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2　[Reset] をクリックします。

EIGRP のモニタリング

次のコマンドを使用して、EIGRP ルーティング プロセスをモニタできます。コマンド出力の例と説明については、コマンド リファレンスを参照してください。また、ネイバー変更メッセージとネイバー警告メッセージのロギングをディセーブルにできます。

さまざまな EIGRP ルーティング統計情報をモニタまたはディセーブル化するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Monitoring] > [Routing] > [EIGRP Neighbor] の順に選択します。

各行は 1 つの EIGRP ネイバーを表します。ネイバーごとに、リストにはその IP アドレス、接続先のネットワーク、保持時間、アップタイム、キュー長、シーケンス番号、スムーズ ラウンドトリップ時間、再送信タイムアウトが表示されます。考えられる状態変更のリストは次のとおりです。

- [NEW ADJACENCY]：新しいネイバーが確立されました。
- [PEER RESTARTED]：他のネイバーがネイバー関係のリセットを開始しました。メッセージを受け取ったルータは、ネイバーをリセットしているルータではありません。
- [HOLD TIME EXPIRED]：保持時間が経過しても、ルータは EIGRP パケットをネイバーから受け取っていません。
- [RETRY LIMIT EXCEEDED]：EIGRP は EIGRP 高信頼性パケットに対する確認応答をネイバーから受け取らなかったため、高信頼性パケットの再送信をすでに 16 回試行しましたが、一度も成功しませんでした。
- [ROUTE FILTER CHANGED]：ルート フィルタに変更があったため、EIGRP ネイバーがリセットしています。
- [INTERFACE DELAY CHANGED]：インターフェイスでの遅延パラメータの手動設定変更があったため、EIGRP ネイバーがリセットしています。
- [INTERFACE BANDWIDTH CHANGED]：インターフェイスでのインターフェイス帯域幅の手動設定変更があったため、EIGRP ネイバーがリセットしています。
- [STUCK IN ACTIVE]：EIGRP がアクティブ状態のままスタックしているため、EIGRP ネイバーがリセットしています。ネイバーがリセットされるのは、stuck-in-active 状態となったためです。

ステップ 2　モニタする EIGRP ネイバーをクリックします。

ステップ 3　現在のネイバー リストを削除するには、[Clear Neighbors] をクリックします。

ステップ 4　現在のネイバー リストの表示を更新するには、[Refresh] をクリックします。

（注）　デフォルトでは、ネイバー変更メッセージとネイバー警告メッセージはロギングされます。

EIGRP の機能履歴

表 24-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 24-1　EIGRP の機能履歴

機能名	プラットフォーム リリース	機能情報
EIGRP サポート	7.0(1)	Enhanced Interior Gateway Routing Protocol（EIGRP）を使用するデータのルーティング、認証の実行、およびルーティング情報の再配布とモニタリングのサポートが追加されました。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [EIGRP]。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	EIGRP ルーティングは、マルチ コンテキスト モードでサポートされます。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup]。
クラスタリング	9.0(1)	EIGRP の場合、バルク同期、ルートの同期およびレイヤ 2 ロード バランシングは、クラスタリング環境でサポートされます。
EIGRP Auto-Summary	9.2(1)	EIGRP の [Auto-Summary] フィールドは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] > [Device Setup] > [Routing] > [EIGRP] > [Setup] > [Edit EIGRP Process Advanced Properties]

マルチキャスト ルーティング

この章では、マルチキャスト ルーティング プロトコルを使用するように Cisco ASA を設定する方法について説明します。

マルチキャスト ルーティングに関する情報

マルチキャスト ルーティングは、単一の情報ストリームを数千もの企業や家庭に同時に配信することでトラフィックを軽減する帯域幅節約型のテクノロジーです。マルチキャスト ルーティングを活用するアプリケーションには、ビデオ会議、企業通信、遠隔学習に加えて、ソフトウェア、株価、およびニュースの配信などがあります。

マルチキャスト ルーティング プロトコルでは、競合テクノロジーのネットワーク帯域幅の使用量を最小限に抑えながら、発信元や受信者の負荷を増加させずに発信元のトラフィックを複数の受信者に配信します。マルチキャスト パケットは、Protocol Independent Multicast（PIM）やサポートする他のマルチキャスト プロトコルを使用した Cisco ルータによりネットワークで複製されるため、複数の受信者にできる限り高い効率でデータを配信できます。

ASA は、スタブ マルチキャスト ルーティングと PIM マルチキャスト ルーティングの両方をサポートしています。ただし、1 つの ASA に両方を同時に設定できません。

（注） UDP と非 UDP の両方のトランスポートがマルチキャスト ルーティングに対してサポートされます。ただし、非 UDP トランスポートでは FastPath 最適化は行われません。

スタブ マルチキャスト ルーティング

スタブ マルチキャスト ルーティングは、ダイナミック ホスト登録の機能を提供して、マルチキャスト ルーティングを容易にします。スタブ マルチキャスト ルーティングを設定すると、ASA は IGMP のプロキシ エージェントとして動作します。ASA は、マルチキャスト ルーティングに全面的に参加するのではなく、IGMP メッセージをアップストリームのマルチキャスト ルータに転送し、そのルータがマルチキャスト データの送信をセットアップします。スタブ マルチキャスト ルーティングを設定する場合は、ASA を PIM として設定できません。

ASA は、PIM-SM および双方向 PIM の両方をサポートしています。PIM-SM は、基盤となるユニキャスト ルーティング情報ベースまたは別のマルチキャスト対応ルーティング情報ベースを使用するマルチキャスト ルーティング プロトコルです。このプロトコルは、マルチキャスト グループあたり 1 つのランデブー ポイントをルートにした単方向の共有ツリーを構築し、オプションでマルチキャストの発信元ごとに最短パス ツリーを作成します。

PIM マルチキャスト ルーティング

双方向 PIM は PIM-SM の変形で、マルチキャストの発信元と受信者を接続する双方向の共有ツリーを構築します。双方向ツリーは、マルチキャスト トポロジの各リンクで動作する DF 選定プロセスを使用して構築されます。DF に支援されたマルチキャスト データは発信元からランデブー ポイントに転送されます。この結果、マルチキャスト データは発信元固有の状態を必要とせず、共有ツリーをたどって受信者に送信されます。DF 選定はランデブー ポイントの検出中に行われ、これによってデフォルト ルートがランデブー ポイントに提供されます。

（注）　ASA が PIM ランデブー ポイントの場合、ASA の未変換の外部アドレスをランデブー ポイント アドレスとして使用します。

マルチキャスト グループの概念

マルチキャストはグループの概念に基づくものです。受信者の任意のグループは、特定のデータ ストリームを受信することに関心があります。このグループには物理的または地理的な境界がなく、インターネット上のどの場所にホストを置くこともできます。特定のグループに流れるデータの受信に関心があるホストは、IGMP を使用してグループに加入する必要があります。ホストがデータ ストリームを受信するには、グループのメンバでなければなりません。マルチキャスト グループの設定方法の詳細については、「マルチキャスト グループの設定」（P.25-15）を参照してください。

マルチキャスト アドレス

マルチキャスト アドレスは、グループに加入し、このグループに送信されるトラフィックの受信を希望する IP ホストの任意のグループを指定します。

クラスタリング

マルチキャスト ルーティングは、クラスタリングをサポートします。レイヤ 2 クラスタリングでは、マスター ユニットが、ファースト パス転送が確立されるまで、すべてのマルチキャスト ルーティング パケットとデータ パケットを送信します。ファースト パス転送が確立されると、スレーブ ユニットがマルチキャスト データ パケットを転送できます。すべてのデータ フ

ローは、フル フローです。スタブ転送フローもサポートされます。1 つのユニットだけレイヤ 2 クラスタリングのマルチキャスト パケットを受信するため、マスター ユニットへのリダイレクションは共通です。レイヤ 3 クラスタリングでは、ユニットは個別に機能しません。すべてのデータとルーティング パケットはマスター ユニットで処理され、転送されます。スレーブ ユニットは、送信されたすべてのパケットをドロップします。

クラスタリングの詳細については、第 9 章「ASA クラスタ」を参照してください。

マルチキャスト ルーティングのライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードでサポートされています。マルチ コンテキスト モードでは、非共有インターフェイスと共有インターフェイスはサポートされません。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドライン

クラスタリングでは、IGMP および PIM の場合、この機能は、マスター ユニットでのみサポートされます。

マルチキャスト ルーティングのイネーブル化

マルチキャスト ルーティングをイネーブルにすると、ASA 上でマルチキャスト ルーティングをイネーブルにできます。マルチキャスト ルーティングがイネーブルになれば、デフォルトですべてのインターフェイス上の IGMP と PIM がイネーブルになります。IGMP は、直接接続されているサブネット上にグループのメンバが存在するかどうか学習するために使用されます。ホストは、IGMP 報告メッセージを送信することにより、マルチキャスト グループに参加します。PIM は、マルチキャスト データグラムを転送するための転送テーブルを維持するために使用されます。

（注）　マルチキャスト ルーティングでは、UDP トランスポート レイヤだけがサポートされています。

マルチキャスト ルーティング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　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] の順に選択します。

ステップ 2　[Multicast] ペインで、[Enable Multicast routing] チェックボックスをオンにします。

このチェックボックスをオンにすると、ASA 上で IP マルチキャスト ルーティングがイネーブルになります。このチェックボックスをオフにすると、IP マルチキャスト ルーティングがディセーブルになります。デフォルトでは、マルチキャストはディセーブルになっています。マルチキャスト ルーティングをイネーブルにすると、すべてのインターフェイス上でマルチキャストがイネーブルになります。マルチキャストはインターフェイスごとにディセーブルにできます。

表 25-1 に、ASAの RAM の量に基づいた特定のマルチキャスト テーブルのエントリの最大数を示します。この上限に達すると、新しいエントリは廃棄されます。

表 25-1　マルチキャスト テーブルのエントリ数の上限

Table	16 MB	128 MB	128 + MB
MFIB	1000	3000	30000
IGMP グループ	1000	3000	30000
PIM ルート	3000	7000	72000

マルチキャスト ルーティングのカスタマイズ

ここでは、マルチキャスト ルーティングをカスタマイズする方法について説明します。

- 「スタブ マルチキャスト ルーティングと IGMP メッセージ転送の設定」（P.25-4）
- 「スタティック マルチキャスト ルートの設定」（P.25-5）
- 「IGMP 機能の設定」（P.25-6）
- 「PIM 機能の設定」（P.25-11）
- 「マルチキャスト グループの設定」（P.25-15）
- 「双方向ネイバー フィルタの設定」（P.25-16）
- 「マルチキャスト境界の設定」（P.25-17）

スタブ マルチキャスト ルーティングと IGMP メッセージ転送の設定

（注）　スタブ マルチキャスト ルーティングと PIM は、同時にはサポートされません。

スタブ エリアへのゲートウェイとして動作している ASA は、PIM に参加する必要はありません。その代わりに、そのセキュリティ アプライアンスを IGMP プロキシ エージェントとして設定すると、あるインターフェイスに接続されているホストから、別のインターフェイスのアップストリーム マルチキャスト ルータに IGMP メッセージを転送することができます。ASA を IGMP プロキシ エージェントとして設定するには、ホスト加入（join）メッセージおよびホスト脱退（leave）メッセージをスタブ エリアからアップストリーム インターフェイスに転送します。

ホスト加入メッセージおよびホスト脱退メッセージを転送するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] の順に選択します。

ステップ 2　[Multicast] ペインで、[Enable Multicast routing] チェックボックスをオンにします。

ステップ 3　[Apply] をクリックして変更内容を保存します。

ステップ 4　[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Protocol] の順に選択します。

ステップ 5　どのインターフェイスから IGMP メッセージを転送するかを変更するには、インターフェイスを選択して [Edit] をクリックします。

[Configure IGMP Parameters] ダイアログボックスが表示されます。

ステップ 6　[Forward Interface] ドロップダウン リストで、どのインターフェイスから IGMP メッセージを送信するかを選択します。

ステップ 7　[OK] をクリックしてこのダイアログボックスを閉じてから、[Apply] をクリックして変更内容を保存します。

スタティック マルチキャスト ルートの設定

スタティック マルチキャスト ルートを設定すると、マルチキャスト トラフィックをユニキャスト トラフィックから分離できます。たとえば、送信元と宛先の間のパスでマルチキャスト ルーティングがサポートされていない場合は、その解決策として、2 つのマルチキャスト デバイスの間に GRE トンネルを設定し、マルチキャスト パケットをそのトンネル経由で送信します。

PIM を使用する場合、ASA は、ユニキャスト パケットを発信元に返送するときと同じインターフェイスでパケットを受信することを想定しています。マルチキャスト ルーティングをサポートしていないルートをバイパスする場合などは、ユニキャスト パケットで 1 つのパスを使用し、マルチキャスト パケットで別の 1 つのパスを使用することもあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

スタティック マルチキャスト ルートまたはスタブ エリアのスタティック マルチキャスト ルートを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [MRoute] の順に選択します。

ステップ 2　[Add] または [Edit] を選択します。

[Add Multicast Route] または [Edit Multicast Route] ダイアログボックスが表示されます。

ASA に新しいスタティック マルチキャスト ルートを追加する場合は、[Add Multicast Route] ダイアログボックスを使用します。既存のスタティック マルチキャスト ルートを変更する場合は、[Edit Multicast Route] ダイアログボックスを使用します。

ステップ 3　[Source Address] フィールドに、マルチキャスト送信元の IP アドレスを入力します。既存のスタティック マルチキャスト ルートを編集しているときは、この値は変更できません。

ステップ 4　[Source Mask] ドロップダウン リストからマルチキャスト送信元の IP アドレスのネットワーク マスクを選択します。

ステップ 5　[Incoming Interface] 領域で、[RPF Interface] オプション ボタンをクリックしてルートを転送する RPF を選択するか、[Interface Name] オプション ボタンをクリックし、次に以下を入力します。

- [Source Interface] フィールドで、ドロップダウン リストからマルチキャスト ルートの着信インターフェイスを選択します。
- [Destination Interface] フィールドで、どの宛先インターフェイスを通してルートを転送するかをドロップダウン リストで選択します。

（注）　インターフェイスまたは RPF ネイバーを指定できますが、同時に両方は指定できません。

ステップ 6　[Administrative Distance] フィールドで、スタティック マルチキャスト ルートのアドミニストレーティブ ディスタンスを選択します。スタティック マルチキャスト ルートのアドミニストレーティブ ディスタンスがユニキャスト ルートのアドミニストレーティブ ディスタンスと同じである場合は、スタティック マルチキャスト ルートが優先されます。

ステップ 7　[OK] をクリックします。

IGMP 機能の設定

IP ホストは、インターネット グループ管理プロトコル（IGMP）を使用して、そのグループ メンバーシップを、直接接続されているマルチキャスト ルータに報告します。

IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。ホストは、そのローカル マルチキャスト ルータに IGMP メッセージを送信することで、グループ メンバーシップを識別します。IGMP では、ルータは IGMP メッセージを受信し、定期的にクエリーを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

IGMP は、グループ アドレス（Class D IP アドレス）をグループ識別子として使用します。ホスト グループ アドレスとして使用できるのは、224.0.0.0 ～ 239.255.255.255 の範囲内のアドレスです。アドレス 224.0.0.0 がグループに割り当てられることはありません。アドレス 224.0.0.1 は、サブネットのシステムすべてに割り当てられます。アドレス 224.0.0.2 は、サブネットのルータすべてに割り当てられます。

ASA でマルチキャスト ルーティングをイネーブルにすると、IGMP バージョン 2 がすべてのインターフェイスで自動的にイネーブルになります。

（注）　**show run** コマンドを使用すると、インターフェイス コンフィギュレーションには **no igmp** コマンドだけが表示されます。デバイス コンフィギュレーションに **multicast-routing** コマンドがあると、すべてのインターフェイスで IGMP が自動的にイネーブルになります。

ここでは、インターフェイス単位で任意の IGMP 設定を行う方法について説明します。

- 「インターフェイスにおける IGMP のディセーブル化」（P.25-7）
- 「IGMP グループ メンバーシップの設定」（P.25-7）

インターフェイスにおける IGMP のディセーブル化

IGMP は、特定のインターフェイスでディセーブルにできます。この情報が役に立つのは、あるインターフェイス上にマルチキャスト ホストがないことがわかっている場合に、そのインターフェイス上で ASA からホスト クエリー メッセージが送信されないように設定するときです。

インターフェイスで IGMP をディセーブルにするには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Protocol] の順に選択します。

[Protocol] ペインには、ASA 上の各インターフェイスの IGMP パラメータが表示されます。

ステップ 2　ディセーブルにするインターフェイスを選択して [Edit] をクリックします。

ステップ 3　指定したインターフェイスをディセーブルにするには、[Enable IGMP] チェックボックスをオフにします。

ステップ 4　[OK] をクリックします。

[Protocol] ペインに「Yes」と表示される場合は IGMP がそのインターフェイス上でイネーブルになっており、「No」の場合はそのインターフェイス上で IGMP がディセーブルになっています。

IGMP グループ メンバーシップの設定

ASA をマルチキャスト グループのメンバとして設定できます。マルチキャスト グループに加入するように ASA を設定すると、アップストリーム ルータはそのグループのマルチキャスト ルーティング テーブル情報を維持して、このグループをアクティブにするパスを保持します。

（注）　特定のグループのマルチキャスト パケットを特定のインターフェイスに転送する必要がある場合に、ASA がそのパケットをそのグループの一部として受け付けることがないようにする方法については、「スタティック加入した IGMP グループの設定」（P.25-8）を参照してください。

マルチキャスト グループに ASA を加入するように設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Join Group] の順に選択します。

[Join Group] ペインが表示されます。

ステップ 2　[Add] または [Edit] をクリックします。

[Add IGMP Join Group] ダイアログボックスでは、インターフェイスをマルチキャスト グループのメンバーに設定することができます。[Edit IGMP Join Group] ダイアログボックスでは、既存のメンバーシップ情報を変更することができます。

ステップ 3　[Interface Name] フィールドで、ドロップダウン リストからインターフェイス名を選択します。既存のエントリを編集しているときは、この値は変更できません。

ステップ 4　[Multicast Group Address] フィールドで、インターフェイスが属するマルチキャスト グループのアドレスを入力します。有効なグループ アドレスの範囲は、224.0.0.0 ～ 239.255.255.255 です。

ステップ 5　[OK] をクリックします。

スタティック加入した IGMP グループの設定

設定によってはグループ メンバがグループ内で自分のメンバーシップを報告できない場合があります。また、ネットワーク セグメント上にグループのメンバが存在しないこともあります。しかし、それでも、そのグループのマルチキャスト トラフィックをそのネットワーク セグメントに送信することが必要になる場合があります。そのようなグループのマルチキャスト トラフィックをそのセグメントに送信するには、スタティック加入した IGMP グループを設定します。

メイン ASDM ウィンドウで、[Configuration] > [Routing] > [Multicast] > [IGMP] > [Static Group] の順に選択すると、ASA を、スタティックに接続されたグループ メンバーとして設定できます。この方法を使用した場合、ASA では、パケットが転送されるだけで、パケット自体は取得されません。そのため、スイッチングが高速に実施されます。発信インターフェイスは IGMP キャッシュ内に存在しますが、このインターフェイスはマルチキャスト グループのメンバーではありません。

インターフェイス上のマルチキャスト グループにスタティック加入を設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Static Group] の順に選択します。

[Static Group] ペインが表示されます。

ステップ 2　[Add] または [Edit] をクリックします。

インターフェイスに対してマルチキャスト グループをスタティックに割り当てる場合は、[Add IGMP Static Group] ダイアログボックスを使用します。既存のスタティック グループの割り当てを変更する場合は、[Edit IGMP Static Group] ダイアログボックスを使用します。

ステップ 3　[Interface Name] フィールドで、ドロップダウン リストからインターフェイス名を選択します。既存のエントリを編集しているときは、この値は変更できません。

ステップ 4　[Multicast Group Address] フィールドで、インターフェイスが属するマルチキャスト グループのアドレスを入力します。有効なグループ アドレスの範囲は、224.0.0.0 ～ 239.255.255.255 です。

ステップ 5　[OK] をクリックします。

マルチキャスト グループへのアクセスの制御

ASA インターフェイス上のホストが加入可能なマルチキャスト グループを制御するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Access Group] の順に選択します。

[Access Group] ペインが表示されます。[Access Group] ペインのテーブル エントリは、上から下の順に処理されます。具体的なエントリはテーブルの上方に、一般的なエントリは下方に配置してください。たとえば、特定のマルチキャスト グループを許可するためのアクセス グループ エントリはテーブルの上方に配置し、許可ルールに指定されたグループなど、一定のまとまりを持った複数のマルチキャスト グループを拒否するようなアクセス グループ エントリは下方に配置します。ただし、拒否ルールよりも許可ルールの方が優先的に適用されるため、許可ルールに指定されているグループは、拒否ルールが適用されて場合でも許可されます。

テーブルのエントリをダブルクリックすると、選択したエントリの [Add or Edit Access Group] ダイアログボックスが開きます。

ステップ 2　[Add] または [Edit] をクリックします。

[Add Access Group] または [Edit Access Group] ダイアログボックスが表示されます。[Add Access Group] ダイアログボックスでは、新しいアクセス グループを [Access Group] テーブルに追加できます。[Edit Access Group] ダイアログボックスでは、既存のアクセス グループ エントリの情報を変更できます。既存のエントリを編集するときは、一部のフィールドがグレー表示されることがあります。

ステップ 3　アクセス グループを関連付けるインターフェイスの名前を [Interface] ドロップダウン リストで選択します。既存のアクセス グループを編集しているときは、関連インターフェイスは変更できません。

ステップ 4　[permit] を [Action] ドロップダウン リストで選択すると、選択されているインターフェイス上でそのマルチキャスト グループが許可されます。[deny] を [Action] ドロップダウン リストで選択すると、選択されているインターフェイスからそのマルチキャスト グループがフィルタリングされます。

ステップ 5　[Multicast Group Address] フィールドで、そのアクセス グループの適用先となるマルチキャスト グループのアドレスを入力します。

ステップ 6　マルチキャスト グループ アドレスのネットワーク マスクを入力するか、一般的なネットワーク マスクの 1 つを [Netmask] ドロップダウン リストから選択します。

ステップ 7　[OK] をクリックします。

インターフェイスにおける IGMP 状態の数の制限

IGMP メンバーシップ報告の結果の IGMP 状態の数は、インターフェイスごとに制限することができます。設定された上限を超過したメンバーシップ報告は IGMP キャッシュに入力されず、超過した分のメンバーシップ報告のトラフィックは転送されません。

インターフェイスでの IGMP 状態の数を制限するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Protocol] の順に選択します。

ステップ 2　[Protocol] ペインのテーブルから限定するインターフェイスを選択し、[Edit] をクリックします。

[Configure IGMP Parameters] ダイアログボックスが表示されます。

ステップ 3　[Group Limit] フィールドに、1 つのインターフェイス上で加入できるホストの最大数を入力します。有効な値の範囲は、0 ～ 500 です。デフォルト値は 500 です。この値を 0 に設定すると、学習したグループが追加されなくなりますが、手動で定義したメンバーシップは引き続き許可されます。

ステップ 4　[OK] をクリックします。

マルチキャスト グループに対するクエリー メッセージの変更

ASA は、クエリー メッセージを送信して、インターフェイスに接続されているネットワークにメンバを持つマルチキャスト グループを検出します。メンバは、IGMP 報告メッセージで応答して、特定のグループに対するマルチキャスト パケットの受信を希望していることを示します。クエリー メッセージは、アドレスが 224.0.0.1 で存続可能時間値が 1 の全システム マルチキャスト グループ宛に送信されます。

これらのメッセージが定期的に送信されることにより、ASA に保存されているメンバーシップ情報はリフレッシュされます。ローカル メンバーが 1 つもないマルチキャスト グループがまだインターフェイスに接続されていることが ASA によって検出された場合は、そのグループへのマルチキャスト パケットは接続されているネットワークに転送されなくなり、そのパケットの送信元にプルーニング メッセージが返されます。

デフォルトでは、サブネット上の PIM 指定ルータがクエリー メッセージの送信を担当します。このメッセージは、デフォルトでは 125 秒間に 1 回送信されます。

クエリー応答時間を変更する場合は、IGMP クエリーでアドバタイズする最大クエリー応答時間はデフォルトで 10 秒になります。ASA がこの時間内にホスト クエリーの応答を受信しなかった場合、グループを削除します。

クエリー間隔、クエリー応答時間、クエリー タイムアウト値を変更するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Protocol] の順に選択します。

ステップ 2　[Protocol] ペインのテーブルから限定するインターフェイスを選択し、[Edit] をクリックします。

[Configure IGMP Parameters] ダイアログボックスが表示されます。

ステップ 3　[Query Interval] フィールドに、指定ルータから IGMP ホストクエリー メッセージを送信する間隔を秒単位で指定します。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 125 秒です。

指定されたタイムアウト値の時間が経過しても、ASA がインターフェイス上でクエリー メッセージを検出できなかった場合は、その ASA が指定ルータになり、クエリー メッセージの送信を開始します。

ステップ 4　[Query Timeout] フィールドには、秒数を入力します、前のリクエスタがリクエスタとしての動作を停止してからこの時間が経過すると、この ASA がそのインターフェイスのリクエスタの役割を引き継ぎます。有効な値の範囲は 60 ～ 300 秒です。デフォルト値は 255 秒です。

ステップ 5　[OK] をクリックします。

IGMP バージョンの変更

デフォルトでは、ASA は IGMP バージョン 2 を実行します。このバージョンでは、いくつかの追加機能を使用できます。

サブネットのマルチキャスト ルータはすべて、同じ IGMP バージョンをサポートしている必要があります。ASA が自動的にバージョン 1 ルータを検出してバージョン 1 に切り替えることはありません。しかし、サブネットに IGMP のバージョン 1 のホストとバージョン 2 のホストが混在しても問題はありません。IGMP バージョン 2 を実行しているASA は、IGMP バージョン 1 のホストが存在しても正常に動作します。

インターフェイスで動作中の IGMP のバージョンを制御するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Protocol] の順に選択します。

ステップ 2　どのインターフェイスの IGMP バージョンを変更するかを [Protocol] ペインのテーブルで選択し、[Edit] をクリックします。

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

ステップ 3　バージョン番号を [Version] ドロップダウン リストから選択します。

ステップ 4　[OK] をクリックします。

PIM 機能の設定

ルータは、PIM を使用してマルチキャスト ダイアグラムを転送する転送テーブルを維持します。ASA でマルチキャスト ルーティングをイネーブルにすると、PIM および IGMP がすべてのインターフェイスで自動的にイネーブルになります。

（注）　PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

ここでは、任意の PIM 設定を行う方法について説明します。

- 「インターフェイスでの PIM のイネーブルおよびディセーブル化」（P.25-11）
- 「スタティック ランデブー ポイント アドレスの設定」（P.25-12）
- 「指定ルータのプライオリティの設定」（P.25-13）
- 「PIM 登録メッセージの設定とフィルタリング」（P.25-13）
- 「PIM メッセージ間隔の設定」（P.25-14）
- 「ルート ツリーの設定」（P.25-14）
- 「PIM ネイバーのフィルタリング」（P.25-15）

インターフェイスでの PIM のイネーブルおよびディセーブル化

PIM は、特定のインターフェイスでイネーブルまたはディセーブルにできます。インターフェイスで PIM をイネーブルまたはディセーブルにするには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Protocol] の順に選択します。

ステップ 2　どのインターフェイスで PIM をイネーブルにするかを [Protocol] ペインのテーブルで選択し、[Edit] をクリックします。

[Edit PIM Protocol] ダイアログボックスが表示されます。

ステップ 3　[Enable PIM] チェックボックスをオンにします。PIM をディセーブルにするには、このチェックボックスをオフにします。

ステップ 4　[OK] をクリックします。

スタティック ランデブー ポイント アドレスの設定

共通の PIM スパース モードまたは双方向ドメイン内のルータはすべて、PIM RP アドレスを認識している必要があります。このアドレスは、**pim rp-address** コマンドを使用してスタティックに設定されます。

（注）　ASA は、Auto-RP または PIM BSR をサポートしていません

ASA を複数のグループの RP として機能するように設定することができます。ACL に指定されているグループ範囲によって、PIM RP のグループ マッピングが決まります。ACL が指定されていない場合は、マルチキャスト グループ全体の範囲（224.0.0.0/4）にグループの RP が適用されます。

PIM PR のアドレスを設定するには、次の手順を実行します。

（注）　ASA は、実際の双方向構成にかかわらず、PIM の hello メッセージを使用して双方向の機能を常時アドバタイズします。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Rendezvous Points] の順に選択します。

ステップ 2　[Add] または [Edit] をクリックします。

[Add Rendezvous Point] または [Edit Rendezvous Point] ダイアログボックスが表示されます。[Add Rendezvous Point] ダイアログボックスでは、新しいエントリを [Rendezvous Point] テーブルに追加できます。[Edit Rendezvous Point] ダイアログボックスでは、既存の RP エントリを変更できます。さらに、[Delete] をクリックして、選択されているマルチキャスト グループ エントリをテーブルから削除できます。

RP を使用する場合の制限事項は、次のとおりです。

- 同じ RP アドレスは、2 度使用できません。
- 複数の RP に対しては、[All Groups] を指定できません。

ステップ 3　[Rendezvous Point Address] フィールドに、RP の IP アドレスを入力します。

既存の RP エントリを編集しているときは、この値は変更できません。

ステップ 4　[Use bi-directional forwarding] チェックボックスをオンにすると、指定されているマルチキャスト グループは双方向モードで動作します。[Rendezvous Point] ペインに「Yes」と表示されている場合は、指定されているマルチキャスト グループが双方向モードで動作し、「No」の場合はスパース モードで動作します。双方向モードでは、ASA がマルチキャスト パケットを受信したときに、直接接続されたメンバーも PIM ネイバーも存在しない場合は、送信元にプルーニング メッセージが返されます。

ステップ 5　[Use this RP for All Multicast Groups] オプション ボタンをクリックすると、指定した RP がそのインターフェイス上のすべてのマルチキャスト グループに使用され、[Use this RP for the Multicast Groups as specified below] オプション ボタンをクリックすると、指定した RP をどのマルチキャスト グループで使用するかを指定できます。

マルチキャスト グループの詳細については、「マルチキャスト グループの設定」（P.25-15）を参照してください。

ステップ 6　[OK] をクリックします。

指定ルータのプライオリティの設定

DR は、PIM 登録メッセージ、PIM 加入メッセージ、およびプルーニング メッセージの RP への送信を担当します。1 つのネットワーク セグメントに複数のマルチキャスト ルータがある場合は、DR プライオリティに基づいて DR が選択されます。複数のデバイスの DR プライオリティが等しい場合、最上位の IP アドレスを持つデバイスが DR になります。

デフォルトでは、ASA の DR プライオリティは 1 です。この値を変更するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Protocol] の順に選択します。

ステップ 2　[Protocol] ペインのテーブルから PIM にイネーブルにするインターフェイスを選択し、[Edit] をクリックします。

[Edit PIM Protocol] ダイアログボックスが表示されます。

ステップ 3　[DR Priority] フィールドに、選択されているインターフェイスの指定ルータ プライオリティの値を入力します。サブネット上のルータのうち、DR プライオリティが最いものが指定ルータになります。有効な値の範囲は 0 ～ 4294967294 です。デフォルトの DR プライオリティは 1 です。この値を 0 に設定した場合は、その ASA インターフェイスがデフォルトのルータになることはありません。

ステップ 4　[OK] をクリックします。

PIM 登録メッセージの設定とフィルタリング

ASA が RP として動作しているときは、特定のマルチキャスト送信元を登録できないように制限することができます。このようにすると、未認可の送信元が RP に登録されるのを回避できます。[Request Filter] ペインでは、ASA で PIM 登録メッセージが受け入れられるマルチキャスト ソースを定義できます。

PIM 登録メッセージをフィルタリングするには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Request Filter] の順に選択します。

ステップ 2　[Add] をクリックします。

[Request Filter Entry] ダイアログボックスでは、ASA が RP として動作する場合に、ASA に登録できるマルチキャスト送信元を定義できます。送信元 IP アドレスおよび宛先マルチキャスト アドレスに基づいて、フィルタ ルールを作成します。

ステップ 3　[Action] ドロップダウン リストで、[Permit] を選択すると、指定のマルチキャスト トラフィックの指定の送信元に ASA への登録を許可するルールが作成され、[Deny] を選択すると指定のマルチキャスト トラフィックの指定の送信元による ASA への登録を禁止するルールが作成されます。

ステップ 4　[Source IP Address] フィールドに、登録メッセージの送信元の IP アドレスを入力します。

ステップ 5　[Source Netmask] フィールドに、登録メッセージの送信元のネットワーク マスクを入力するか、ドロップダウン リストから選択します。

ステップ 6　[Destination IP Address] フィールドに、マルチキャスト宛先アドレスを入力します。

ステップ 7　[Destination Netmask] フィールドに、マルチキャスト宛先アドレスのネットワーク マスクを入力するか、ドロップダウン リストから選択します。

ステップ 8　[OK] をクリックします。

PIM メッセージ間隔の設定

ルータ クエリー メッセージは、PIM DR の選択に使用されます。PIM DR は、ルータ クエリー メッセージを送信します。デフォルトでは、ルータ クエリー メッセージは 30 秒間隔で送信されます。さらに、60 秒ごとに、ASA から PIM 加入またはプルーニングのメッセージが送信されます。

これらの間隔を変更するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Protocol] の順に選択します。

ステップ 2　[Protocol] ペインのテーブルから PIM にイネーブルにするインターフェイスを選択し、[Edit] をクリックします。

[Edit PIM Protocol] ダイアログボックスが表示されます。

ステップ 3　[Hello Interval] フィールドに、インターフェイスから PIM hello メッセージを送信する間隔を秒単位で入力します。

ステップ 4　[Prune Interval] フィールドに、インターフェイスから PIM 加入およびプルーニングのアドバタイズメントを送信する間隔を秒単位で入力します。

ステップ 5　[OK] をクリックします。

ルート ツリーの設定

デフォルトでは、PIM リーフ ルータは、新しい送信元から最初のパケットが到着した直後に、最短パス ツリーに加入します。この方法では、遅延が短縮されますが、共有ツリーに比べて多くのメモリが必要になります。すべてのマルチキャスト グループまたは特定のマルチキャスト アドレスに対して、ASA を最短パス ツリーに加入させるか、共有ツリーを使用するかを設定できます。

PIM リーフ ルータ ツリーを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Route Tree] の順に選択します。

ステップ 2　次のいずれかのオプション ボタンをクリックします。

- [Use Shortest Path Tree for All Groups] : すべてのマルチキャスト グループに最短パス ツリーを使用する場合は、このオプションを選択します。
- [Use Shared Tree for All Groups]：すべてのマルチキャスト グループに共有ツリーを使用する場合は、このオプションを選択します。
- [Use Shared Tree for the Groups specified below]：[Multicast Groups] テーブルで指定したグループに共有ツリーを使用する場合は、このオプションを選択します。[Multicast Groups] テーブルで指定されていないグループには最短パス ツリーが使用されます。

  [Multicast Groups] テーブルには、共有ツリーを使用するマルチキャスト グループが表示されます。

テーブル エントリは、上から下の順で処理されます。ある範囲のマルチキャスト グループが含まれるエントリを作成し、その範囲の中から特定のグループを除外するには、その除外するグループに対する拒否ルールをテーブルの先頭に配置し、その範囲内のマルチキャスト グループ全体に対する許可ルールを deny 文の下に配置します。

マルチキャスト グループを編集するには、「マルチキャスト グループの設定」（P.25-15）を参照してください。

マルチキャスト グループの設定

マルチキャスト グループとは、どのマルチキャスト アドレスがグループの一部であるかを定義するアクセス ルールのリストです。1 つのマルチキャスト グループに、マルチキャスト アドレスが 1 つだけ含まれることも、特定の範囲のマルチキャスト アドレスが含まれることもあります。新しいマルチキャスト グループ ルールを作成する場合は、[Add Multicast Group] ダイアログボックスを使用します。既存のマルチキャスト グループ ルールを修正する場合は、[Edit Multicast Group] ダイアログボックスを使用します。

マルチキャスト グループを設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Rendezvous Points] の順に選択します。

ステップ 2　[Rendezvous Point] ペインが表示されます。設定するグループをクリックします。

[Edit Rendezvous Point] ダイアログボックスが表示されます。

ステップ 3　[Use this RP for the Multicast Groups as specified below] オプション ボタンをクリックすると、指定の RP とともに使用するマルチキャスト グループを指定できます。

ステップ 4　[Add] または [Edit] をクリックします。

[Add Multicast Group] または [Edit Multicast Group] ダイアログボックスが表示されます。

ステップ 5　[Action] ドロップダウン リストで、[Permit] を選択すると指定のマルチキャスト アドレスを許可するグループ ルールが作成され、[Deny] を選択すると指定のマルチキャスト アドレスをフィルタリングするグループ ルールが作成されます。

ステップ 6　[Multicast Group Address] フィールドに、このグループに関連付けるマルチキャスト アドレスを入力します。

ステップ 7　[Netmask] ドロップダウン リストで、マルチキャスト グループ アドレスのネットワーク マスクを選択します。

ステップ 8　[OK] をクリックします。

PIM ネイバーのフィルタリング

PIM ネイバーにできるルータの定義が可能です。PIM ネイバーにできるルータをフィルタリングすると、次の制御を行うことができます。

- 許可されていないルータが PIM ネイバーにならないようにする。
- 添付されたスタブ ルータが PIM に参加できないようにする。

PIM ネイバーになることができるネイバーを定義するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Neighbor Filter] の順に選択します。

ステップ 2　[Add]/[Edit]/[Insert] をクリックして、テーブルから設定する PIM ネイバーを選択します。

[Add/Edit/Insert Neighbor Filter Entry] ダイアログボックスが表示されます。[Add/Edit/Insert Neighbor Filter Entry] ダイアログボックスでは、マルチキャスト境界 ACL の ACL エントリを作成できます。選択されている PIM ネイバー エントリを削除することもできます。

ステップ 3　[Interface Name] ドロップダウン リストからインターフェイス名を選択します。

ステップ 4　[Action] ドロップダウン リストから、ネイバー フィルタ ACL エントリに対して [Permit] または [Deny] を選択します。

[Permit] を選択すると、マルチキャスト グループ アドバタイズメントがこのインターフェイスを通過できるようになります。[Deny] を選択すると、指定したマルチキャスト グループ アドバタイズメントはこのインターフェイスを通過できなくなります。インターフェイスに対してマルチキャスト境界を設定すると、ネイバー フィルタ エントリで許可されていない限り、すべてのマルチキャスト トラフィックが、インターフェイスの通過を拒否されます。

ステップ 5　[IP Address] テキスト フィールドに、許可または拒否するマルチキャスト PIM グループの IP アドレスを入力します。有効なグループ アドレスの範囲は、224.0.0.0 ～ 239.255.255.255.255 です。

ステップ 6　[Netmask] ドロップダウン リストで、マルチキャスト グループ アドレスのネットマスクを選択します。

ステップ 7　[OK] をクリックします。

双方向ネイバー フィルタの設定

ASA に PIM 双方向ネイバー フィルタが設定されている場合、[Bidirectional Neighbor Filter] ペインにそれらのフィルタが表示されます。PIM 双方向ネイバー フィルタは、DF 選定に参加できるネイバー デバイスを定義する ACL です。PIM 双方向ネイバー フィルタがインターフェイスに設定されていなければ、制限はありません。PIM 双方向ネイバー フィルタが設定されている場合は、ACL で許可されるネイバーだけが DF 選択プロセスに参加できます。

PIM 双方向ネイバー フィルタ設定が ASA に適用されると、実行コンフィギュレーション内に *interface-name*_multicast という名前の ACL が追加されます。*interface-name* は、このマルチキャスト境界フィルタが適用されるインターフェイスの名前です。そのような名前の ACL がすでに存在していた場合は、名前に番号が追加されます（inside_multicast_1 など）。この ACL により、どのデバイスが ASA の PIM ネイバーになれるか定義されます。

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。双方向で DF を選定するために、セグメント内のすべてのマルチキャスト ルータが双方向でイネーブルになっている必要があります。

PIM 双方向ネイバー フィルタを利用すると、スパース モード専用ネットワークから双方向ネットワークへの移行が可能になります。このフィルタで、DF 選定に参加するルータを指定する一方で、引き続きすべてのルータにスパース モード ドメインへの参加を許可できるからです。双方向にイネーブルにされたルータは、セグメントに非双方向ルータがある場合でも、それらのルータの中から DF を選定できます。非双方向ルータ上のマルチキャスト境界により、双方向グループから PIM メッセージやデータが双方向サブセット クラウドに出入りできないようにします。

PIM 双方向ネイバー フィルタがイネーブルの場合、その ACL によって許可されるルータは、双方向に対応していると見なされます。したがって、次のことが当てはまります。

- 許可されたネイバーが双方向対応でない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向対応である場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向をサポートしない場合、DF 選定が実行される可能性があります。

PIM 双方向ネイバー フィルタになることができるネイバーを定義するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Bidirectional Neighbor Filter] の順に選択します。

ステップ 2　[PIM Bidirectional Neighbor Filter] テーブルのエントリの 1 つをダブルクリックすると、そのエントリの [Edit Bidirectional Neighbor Filter Entry] ダイアログボックスが表示されます。

ステップ 3　[Add]/[Edit]/[Insert] をクリックして、テーブルから設定する PIM ネイバーを選択します。

[Add/Edit/Insert Bidirectional Neighbor Filter Entry] ダイアログボックスが表示され、ここで PIM 双方向ネイバー フィルタ ACL の ACL エントリを作成できます。

ステップ 4　[Interface Name] ドロップダウン リストからインターフェイス名を選択します。どのインターフェイスに対して PIM 双方向ネイバー フィルタ ACL エントリを設定するかを選択します。

ステップ 5　[Action] ドロップダウン リストから、ネイバー フィルタ ACL エントリに対して [Permit] または [Deny] を選択します。

[Permit] を選択すると、指定したデバイスが DF 選定に参加できるようになります。指定したデバイスを DF 選定プロセスに参加させない場合は、[Deny] を選択します。

ステップ 6　[IP Address] テキスト フィールドに、許可または拒否するマルチキャスト PIM グループの IP アドレスを入力します。有効なグループ アドレスの範囲は、224.0.0.0 ～ 239.255.255.255.255 です。

ステップ 7　[Netmask] ドロップダウン リストで、マルチキャスト グループ アドレスのネットマスクを選択します。

ステップ 8　[OK] をクリックします。

マルチキャスト境界の設定

アドレス スコーピングは、同じ IP アドレスを持つ RP が含まれるドメインが相互にデータを漏出させることのないように、ドメイン境界を定義します。スコーピングは、大きなドメイン内のサブネット境界や、ドメインとインターネットの間の境界で実行されます。

インターフェイス上でマルチキャスト グループ アドレスの管理スコープ境界を設定するには、ASDM で [Configuration] > [Routing] > [Multicast] > [MBoundary] の順に選択します。IANA では、239.0.0.0 ～ 239.255.255.255 のマルチキャスト アドレス範囲が管理スコープ アドレスとして指定されています。この範囲のアドレスは、さまざまな組織で管理されるドメイン内で再使用されます。このアドレスはグローバルではなく、ローカルで一意であると見なされます。

影響を受けるアドレスの範囲は、標準 ACL で定義します。境界が設定されると、マルチキャスト データ パケットは境界を越えて出入りできなくなります。境界を定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

管理スコープ境界で Auto-RP 検出メッセージと通知メッセージの設定、検証、フィルタリングができます。境界の ACL で拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境

界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

マルチキャスト境界を設定するには、次の手順を実行します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Routing] > [Multicast] > [MBoundary] の順に選択します。

[MBoundary] ペインでは、管理スコープ マルチキャスト アドレスのマルチキャスト境界を設定できます。マルチキャスト境界により、マルチキャスト データ パケット フローが制限され、同じマルチキャスト グループ アドレスを複数の管理ドメインで再利用できるようになります。インターフェイスに対してマルチキャスト境界が定義されている場合、フィルタ ACL により許可されたマルチキャスト トラフィックだけが、そのインターフェイスを通過します。

ステップ 2　[Edit] をクリックします。

[Edit Boundary Filter] ダイアログボックスに、マルチキャスト境界フィルタ ACL が表示されます。このダイアログボックスを使用すれば、境界フィルタ ACL エントリを追加したり削除したりできます。

境界フィルタのコンフィギュレーションが ASA に適用されると、実行コンフィギュレーションに *interface-name*_multicast という名前の ACL が追加されます。*interface-name* は、マルチキャスト境界フィルタが適用されるインターフェイスの名前です。そのような名前の ACL がすでに存在していた場合は、名前に番号が追加されます（inside_multicast_1 など）。

ステップ 3　どのインターフェイスに対してマルチキャスト境界フィルタ ACL を設定するかを [Interface] ドロップダウン リストで選択します。

ステップ 4　[Remove any Auto-RP group range] チェックボックスをオンにすると、境界 ACL で拒否された送信元からの Auto-RP メッセージがフィルタリングされます。[Remove any Auto-RP group range] チェックボックスがオフの場合は、すべての Auto-RP メッセージが通過できます。

ステップ 5　[OK] をクリックします。

マルチキャスト ルーティングの設定例

次の例に、さまざまなオプションのプロセスを使用してマルチキャスト ルーティングをイネーブルにし、設定する方法を示します。

ステップ 1　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] の順に選択します。

ステップ 2　[Multicast] ペインで、[Enable Multicast routing] チェックボックスをオンにして [**Apply**] をクリックします。

ステップ 3　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [MRoute] の順に選択します。

ステップ 4　[Add] または [Edit] をクリックします。

[Add Multicast Route] または [Edit Multicast Route] ダイアログボックスが表示されます。

ASA に新しいスタティック マルチキャスト ルートを追加する場合は、[Add Multicast Route] ダイアログボックスを使用します。既存のスタティック マルチキャスト ルートを変更する場合は、[Edit Multicast Route] ダイアログボックスを使用します。

ステップ 5　[Source Address] フィールドに、マルチキャスト送信元の IP アドレスを入力します。既存のスタティック マルチキャスト ルートを編集しているときは、この値は変更できません。

ステップ 6　[Source Mask] ドロップダウン リストからマルチキャスト送信元の IP アドレスのネットワーク マスクを選択します。

ステップ 7　[Incoming Interface] 領域で、[RPF Interface] オプション ボタンをクリックしてルートを転送する RPF を選択するか、[Interface Name] オプション ボタンをクリックし、次に以下を入力します。

- [Source Interface] フィールドで、ドロップダウン リストからマルチキャスト ルートの着信インターフェイスを選択します。
- [Destination Interface] フィールドでは、選択されているインターフェイスからどの宛先インターフェイスにルートを転送するかをドロップダウン リストで選択します。

（注）　インターフェイスまたは RPF ネイバーを指定できますが、同時に両方は指定できません。

ステップ 8　[Administrative Distance] フィールドで、スタティック マルチキャスト ルートのアドミニストレーティブ ディスタンスを選択します。スタティック マルチキャスト ルートのアドミニストレーティブ ディスタンスがユニキャスト ルートのアドミニストレーティブ ディスタンスと同じである場合は、スタティック マルチキャスト ルートが優先されます。

ステップ 9　[OK] をクリックします。

ステップ 10　メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Join Group] の順に選択します。

[Join Group] ペインが表示されます。

ステップ 11　[Add] または [Edit] をクリックします。

[Add IGMP Join Group] ダイアログボックスでは、インターフェイスをマルチキャスト グループのメンバーに設定することができます。[Edit IGMP Join Group] ダイアログボックスでは、既存のメンバーシップ情報を変更することができます。

ステップ 12　[Interface Name] フィールドで、ドロップダウン リストからインターフェイス名を選択します。既存のエントリを編集しているときは、この値は変更できません。

ステップ 13　[Multicast Group Address] フィールドで、インターフェイスが属するマルチキャスト グループのアドレスを入力します。有効なグループ アドレスの範囲は、224.0.0.0 ～ 239.255.255.255 です。

ステップ 14　[OK] をクリックします。

その他の関連資料

ルーティングに関するその他の情報については、次の項を参照してください。

- 「関連資料」（P.25-20）
- 「RFC」（P.25-20）

関連資料

関連項目	マニュアル タイトル
SMR 機能の実装に使用される IGMP およびマルチキャスト ルーティングの規格の技術詳細	IETF draft-ietf-idmr-igmp-proxy-01.txt

RFC

RFC	タイトル
RFC 2113	「IP Router Alert Option」
RFC 2236	「Internet Group Management Protocol, Version 2」
RFC 2362	「Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification」
RFC 2588	「IP Multicast and Firewalls」

マルチキャスト ルーティングの機能履歴

表 25-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 25-2　マルチキャスト ルーティングの機能履歴

機能名	プラットフォーム リリース	機能情報
マルチキャスト ルーティング サポート	7.0(1)	マルチキャスト ルーティング プロトコルを使用した、データのマルチキャスト ルーティング データ、認証、およびルーティング情報の再配布とモニタリングのサポートが追加されました。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [Multicast]。
クラスタリングのサポート	9.0(1)	クラスタリングのサポートが追加されました。

IPv6 ネイバー探索

IPv6 ネイバー ディスカバリについて

IPv6 ネイバー探索プロセスでは、ICMPv6 メッセージと送信要求ノード マルチキャスト アドレスを使用して、同一ネットワーク（ローカル リンク）上にあるネイバーのリンクレイヤ アドレスを判別し、ネイバーの到達可能性を検証して、隣接ルータの状態を追跡し続けます。

ノード（ホスト）はネイバー探索を使用して、添付されたリンクに常駐し、無効になったキャッシュ値を素早くパージすることがわかっているネイバーのリンク層アドレスを判断します。また、ホストはネイバー探索を使用して、ホストに代わってパケットを転送しようとしている隣接ルータを検出します。さらに、ノードはこのプロトコルを使用して、どのネイバーが到達可能でどのネイバーがそうでないかをアクティブに追跡するとともに、変更されたリンク層アドレスを検出します。ルータまたはルータへのパスが失敗すると、ホストは機能している代替ルータまたは代替パスをアクティブに検索します。

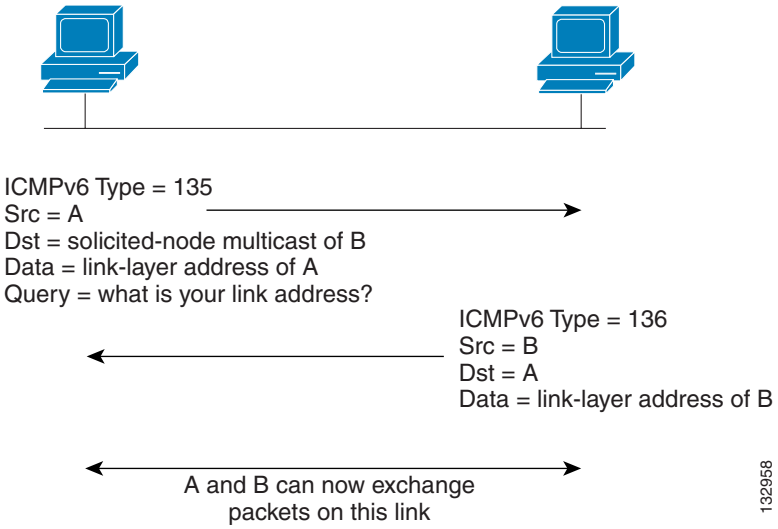
ネイバー送信要求メッセージ

ローカル リンク上にある他のノードのリンクレイヤ アドレスを検出するため、ノードからネイバー送信要求メッセージ（ICMPv6 Type 135）がローカル リンクに送信されます。ネイバー送信要求メッセージは送信要求ノード マルチキャストアドレスに送信されます。ネイバー送信要求メッセージ内の送信元アドレスは、ネイバー送信要求メッセージを送信したノードの IPv6 アドレスです。ネイバー送信要求メッセージには、送信元ノードのリンク層アドレスも含まれます。

ネイバー送信要求メッセージを受信すると、宛先ノードは、ネイバー アドバタイズメント メッセージ（ICPMv6 Type 136）をローカル リンク上に送信して応答します。ネイバー アドバタイズメント メッセージ内の送信元アドレスは、ネイバー アドバタイズメント メッセージを送信したノードの IPv6 アドレスです。宛先アドレスは、ネイバー送信要求メッセージを送信したノードの IPv6 アドレスです。ネイバー アドバタイズメント メッセージのデータ部分には、ネイバー アドバタイズメント メッセージを送信するノードのリンク層アドレスが含まれます。

送信元ノードがネイバー アドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。図 26-1 にネイバー送信要求と応答のプロセスを示します。

図 26-1　　IPv6 ネイバー探索 - ネイバー送信要求メッセージ



ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ノードがネイバーの到達可能性を確認するときに、ネイバー送信要求メッセージの宛先アドレスは、ネイバーのユニキャスト アドレスです。

ネイバー アドバタイズメント メッセージは、ローカル リンク上のノードのリンク層アドレスが変更されたときにも送信されます。そのような変更があった場合、ネイバー アドバタイズメントの宛先アドレスは全ノード マルチキャスト アドレスになります。

ネイバー到達可能時間

ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

重複アドレス検出

ステートレス自動設定プロセスにおいて、重複アドレス検出機能は、新規のユニキャスト IPv6 アドレスがインターフェイスに割り当てられる前に、その一意性を検証します（重複アドレス検出が実行されている間、新規アドレスは一時ステートのままです）。重複アドレス検出は、最初に新しいリンクローカル アドレスに対して行われます。リンクローカル アドレスが固有であることが検証されたら、次にインターフェイス上のその他すべての IPv6 ユニキャスト アドレスに対して重複アドレス検出が行われます。

重複アドレス検出は、管理上ダウンしているインターフェイスでは停止します。インターフェイスが管理上ダウンしている間、そのインターフェイスに割り当てられたユニキャスト IPv6 アドレスは保留状態に設定されます。管理上アップ状態に復帰したインターフェイスでは、重複アドレス検出がインターフェイス上のすべてのユニキャスト IPv6 アドレスに対して再開されます。

重複アドレスが検出されると、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用対象外となり、次のエラー メッセージが生成されます。

```
%ASA-4-325002: Duplicate address ipv6_address/MAC_address on interface
```

重複アドレスがインターフェイスのリンクローカル アドレスであれば、インターフェイス上で IPv6 パケットの処理はディセーブルになります。重複アドレスがグローバル アドレスであれば、そのアドレスは使用されません。ただし、その重複アドレスに関連付けられたすべてのコンフィギュレーション コマンドは、アドレスの状態が DUPLICATE に設定されている間、設定されたままになります。

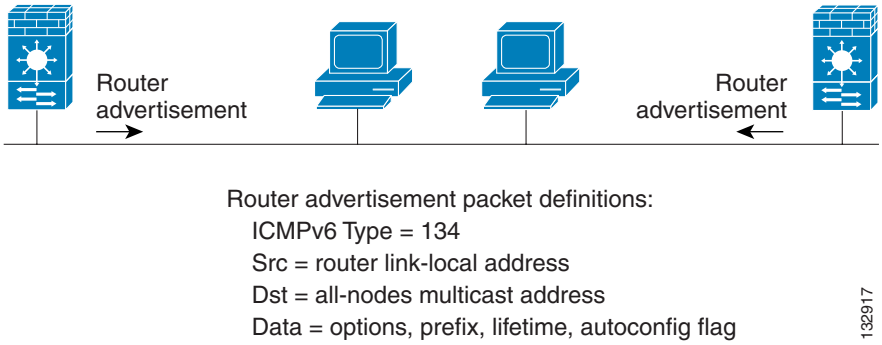
インターフェイスのリンクローカル アドレスが変更された場合、新しいリンクローカル アドレスで重複アドレス検出が実行され、インターフェイスに関連付けられた他のすべての IPv6 アドレスが再生成されます（重複アドレス検出は新規のリンクローカル アドレスでのみ実行されます）。

ASA は、ネイバー送信要求メッセージを使用して、重複アドレス検出を実行します。デフォルトでは、インターフェイスが重複アドレス検出を行う回数は 1 回です。

ルータ アドバタイズメント メッセージ

ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、Cisco ASA はルータ アドバタイズメントに参加できます。ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、ASA の IPv6 が設定された各インターフェイスから定期的に送信されます。ルータ アドバタイズメント メッセージは全ノード マルチキャスト アドレスに送信されます 図 26-2 は、IPv6 対応インターフェイスでルータ アドバタイズメント メッセージを送信する例を示しています。

図 26-2　IPv6 ネイバー探索 - ルータ アドバタイズメント メッセージ



ルータ アドバタイズメント メッセージには、通常、次の情報が含まれています。

- ローカル リンク上のノードが IPv6 アドレスを自動設定するために使用できる 1 つまたは複数の IPv6 プレフィックス。
- アドバタイズメントに含まれるプレフィックスごとのライフタイム情報。
- 実行できる自動設定のタイプを示すフラグのセット（ステートレスまたはステートフル）。
- デフォルト ルータ情報（アドバタイズメントを送信するルータをデフォルト ルータとして使用する必要があるかどうか、デフォルト ルータであれば、そのルータをデフォルト ルータとして使用する秒単位の時間）。
- ホストに関する追加情報。たとえば、ホストから発信するパケットで使用するホップ制限や MTU など。
- 特定のリンク上でのネイバー送信要求メッセージの再送信間隔。
- ノードがネイバーを到達可能と見なす時間。

ルータ アドバタイズメントもルータ送信要求メッセージに応答して送信されます（ICMPv6 Type 133）。ルータ送信要求メッセージは、ホストからシステムの起動時に送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。ルータ送信要求メッセージは、通常はホストからシステム起動時に送信されますが、ホストには設定済みのユニキャスト アドレスがないため、ルータ送信要求メッセージ内の送信元アドレスは通常は未指定 IPv6 アドレスとなります（0:0:0:0:0:0:0:0）。ホストに設定済みのユニキャスト アドレスがある場合、ルータ送信要求メッセージを送信するインターフェイスのユニキャスト アドレスが、メッセージ内の送信元アドレスとして使用されます。ルータ送信要求メッセージの宛先アドレスは、スコープがリンクである全ルータ マルチキャスト アドレスです。ルータ送信要求に応答してルータ アドバタイズメントが送信される場合、ルータ アドバタイズメント メッセージ内の宛先アドレスはルータ送信要求メッセージの送信元のユニキャスト アドレスです。

次の設定値をルータ アドバタイズメント メッセージに対して設定できます。

- ルータ アドバタイズメント メッセージの定期的な時間間隔。
- ルータ ライフタイム値。これは IPv6 ノードが ASA をデフォルト ルータと見なす時間を示します。
- リンクで使用されている IPv6 ネットワークのプレフィックス。
- ルータ アドバタイズメント メッセージをインターフェイスが送信するかどうか。

特に指定のない限り、ルータ アドバタイズメント メッセージ設定はインターフェイス固有のものであり、インターフェイス コンフィギュレーション モードで入力されます。

スタティック IPv6 ネイバー

ネイバーを手動で IPv6 ネイバー キャッシュに定義できます。IPv6 ネイバー探索プロセスによる学習を通して、指定された IPv6 アドレスのエントリがネイバー探索キャッシュにすでに存在する場合、エントリは自動的にスタティック エントリに変換されます。IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。

IPv6 ネイバー探索のライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

IPv6 ネイバー探索の前提条件

「IPv6 アドレッシングの設定」（P.12-15）に従って、IPv6 アドレッシングを設定します。

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド モードのみでサポートされます。トランスペアレント モードはサポートされていません。

その他のガイドラインと制限事項

- 送信間隔の値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。
- 時間を設定すると、使用不可能なネイバーの検出がイネーブルになります。設定時間を短くすると、使用不可能なネイバーをさらに迅速に検出できます。ただし、時間を短くすると、すべての IPv6 ネットワーク デバイスで IPv6 ネットワーク帯域幅および処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。
- **ipv6 nd ra-lifetime** コマンドを使用して ASA がデフォルト ルータとして設定されている場合、送信間隔は IPv6 ルータ アドバタイズメントのライフタイム以下にする必要があります。他の IPv6 ノードとの同期を防止するには、実際に使用される値を指定値の 20 % 以内でランダムに調整します。
- **ipv6 nd prefix** コマンドを使用すると、プレフィックスをアドバタイズするかどうかも含めて、プレフィックスごとに個々のパラメータを制御できます。

- デフォルトでは、**ipv6 address** コマンドを使用してインターフェイスにアドレスとして設定されるプレフィックスは、ルータ アドバタイズメントでアドバタイズされます。**ipv6 nd prefix** コマンドを使用してプレフィックスをアドバタイズメント用に設定すると、これらのプレフィックスだけがアドバタイズされます。
- **default** キーワードを使用すると、すべてのプレフィックスのデフォルト パラメータを設定できます。
- プレフィックスの有効期限を指定するための日付を設定できます。有効な推奨ライフタイムは、リアルタイムでカウントダウンされます。有効期限に達すると、プレフィックスはアドバタイズされなくなります。
- onlink がオン（デフォルト）のときは、指定されたプレフィックスがそのリンクに割り当てられます。指定されたプレフィックスを含むそのようなアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。
- autoconfig がオン（デフォルト）のときは、指定されたプレフィックスがローカル リンク上のホストの IPv6 自動設定に使用されます。
- ステートレス自動設定が正しく機能するには、ルータ アドバタイズメント メッセージでアドバタイズされるプレフィックス長が常に 64 ビットでなければなりません。
- ルータの有効期間の値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。値は、ASA がこのインターフェイス上でデフォルト ルータとして有効であることを示します。
- 値をゼロ以外の値に設定すると、ASA がこのインターフェイス上のデフォルト ルータであると見なされます。ルータ ライフタイム値としてゼロ以外の値を設定する場合は、その値がルータ アドバタイズメント間隔以上でなければなりません。

次のガイドラインと制限事項は、スタティック IPv6 ネイバーの設定に適用されます。

- **ipv6 neighbor** コマンドは **arp** コマンドに似ています。IPv6 ネイバー探索プロセスによる学習を通して、指定された IPv6 アドレスのエントリがネイバー探索キャッシュにすでに存在する場合、エントリは自動的にスタティック エントリに変換されます。これらのエントリは、copy コマンドを使用してコンフィギュレーションを格納すると、コンフィギュレーションに格納されます。
- IPv6 ネイバー探索キャッシュのスタティック エントリを表示するには、**show ipv6 neighbor** コマンドを使用します。
- **clear ipv6 neighbor** コマンドにより、スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。**no ipv6 neighbor** コマンドは、指定したスタティック エントリをネイバー探索キャッシュから削除します。このコマンドは、IPv6 ネイバー探索プロセスから認識されるエントリであるダイナミック エントリはキャッシュから削除しません。**no ipv6 enable** コマンドを使用してインターフェイスで IPv6 をディセーブルにすると、スタティック エントリを除いて、そのインターフェイス用に設定されたすべての IPv6 ネイバー探索キャッシュ エントリが削除されます（エントリの状態が INCMP [Incomplete] に変更されます）。
- IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。
- **clear ipv6 neighbor** コマンドを実行しても、スタティック エントリが IPv6 ネイバー探索キャッシュから削除されることはありません。ダイナミック エントリのクリアだけが行われます。
- 生成された ICMP syslog は、IPv6 ネイバー エントリの定期的な更新に起因します。IPv6 ネイバー エントリの ASA デフォルト タイマーは 30 秒であるため、ASA は 30 秒おきに ICMPv6 ネイバー探索および応答パケットを生成します。ASA にフェールオーバー LAN および IPv6 アドレスで設定された状態インターフェイスの両方がある場合は、30 秒ごとに、ICMPv6 ネ

イバー探索および応答パケットが、設定済みのリンクローカル IPv6 アドレスの 両方の ASA で生成されます。また、各パケットは複数の syslog（ICMP 接続およびローカル ホストの作成またはティアダウン）を生成するため、連続 ICMP syslog が生成されているように見えることがあります。IPV6 ネイバー エントリのリフレッシュ時間は、通常のデータ インターフェイスに設定可能ですが、フェールオーバー インターフェイスでは設定可能ではありません。ただし、この ICMP ネイバー探索トラフィックの CPU の影響はわずかです。

IPv6 ネイバー探索のデフォルト設定

表 26-1 に、IPv6 ネイバー探索のデフォルト設定を示します。

表 26-1　　IPv6 ネイバー探索のデフォルト パラメータ

パラメータ	デフォルト
value（ネイバー送信要求メッセージの送信間隔）	ネイバー送信要求の送信間隔は 1,000 秒です。
value（ネイバー到達可能時間）	デフォルトは 0 です。
value（ルータ アドバタイズメント送信間隔）	デフォルトは 200 秒です。
value（ルータ ライフタイム）	デフォルトは 1,800 秒です。
value（DAD 時に連続送信されるネイバー送信要求メッセージの数）	デフォルトは 1 メッセージです。
prefix lifetime	デフォルトのライフタイムは 2592000 秒（30 日間）、推奨ライフタイムは 604800 秒（7 日間）です。
on-link フラグ	このフラグはデフォルトでオンになります。これは、インターフェイスのアドバタイズでプレフィックスが使用されることを意味します。
autoconfig フラグ	このフラグはデフォルトでオンになります。これは、プレフィックスが自動設定に使用されることを意味します。
スタティック IPv6 ネイバー	スタティック エントリは、IPv6 ネイバー探索キャッシュに設定されません。

IPv6 ネイバー探索の設定

ネイバー送信要求メッセージの送信間隔の設定

インターフェイスに IPv6 ネイバー送信要求メッセージを再送信する間隔を設定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] を選択します。

ステップ 2　ネイバー送信要求メッセージの送信間隔を設定するインターフェイスを選択します。このインターフェイスは、IPv6 アドレスを使用して設定されている必要があります。詳細については、「IPv6 アドレッシングの設定」（P.12-15）を参照してください。

ステップ 3　[Edit] をクリックします。[General]、[Advanced]、および [IPv6] という 3 つのタブを持つ [Edit Interface] ダイアログボックスが表示されます。

ステップ 4　[IPv6] タブをクリックします。

ステップ 5　[NS Interval] フィールドで、時間間隔を入力します。

ステップ 6　[OK] をクリックします。

ステップ 7　[Apply] をクリックして、実行コンフィギュレーションを保存します。

ネイバー到達可能時間の設定

到達可能性確認イベントが発生した後でリモートの IPv6 ノードを到達可能と見なす時間を設定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] を選択します。

ステップ 2　時間を設定するインターフェイスを選択します。このインターフェイスは、IPv6 アドレスを使用して設定されている必要があります。詳細については、「IPv6 アドレッシングの設定」（P.12-15）を参照してください。

ステップ 3　[Edit] をクリックします。[General]、[Advanced]、および [IPv6] という 3 つのタブを持つ [Edit Interface] ダイアログボックスが表示されます。

ステップ 4　[IPv6] タブをクリックします。

ステップ 5　[Rachable Time] フィールドに有効な値を入力します。

ステップ 6　[OK] をクリックします。

ステップ 7　[Apply] をクリックして、実行コンフィギュレーションを保存します。

ルータ アドバタイズメントの送信間隔の設定

インターフェイスでの IPv6 ルータ アドバタイズメントの送信間隔を設定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] を選択します。

ステップ 2　時間を設定するインターフェイスを選択します。

このインターフェイスは、IPv6 アドレスを使用して設定されている必要があります。詳細については、「IPv6 アドレッシングの設定」（P.12-15）を参照してください。

ステップ 3　[Edit] をクリックします。[General]、[Advanced]、および [IPv6] という 3 つのタブを持つ [Edit Interface] ダイアログボックスが表示されます。

ステップ 4　[IPv6] タブをクリックします。

ステップ 5　[RA Interval] フィールドに、有効な送信間隔値を入力します。

（注）　（オプション）ルータ アドバタイズメント送信間隔の値を代わりにミリ秒単位で追加するには、[RA Interval in Milliseconds] チェックボックスをオンにしてから、500 ～ 1800000 の範囲内の値を入力します。

ステップ 6　[OK] をクリックします。

ステップ 7　[Apply] をクリックして、実行コンフィギュレーションを保存します。

ルータ ライフタイム値の設定

インターフェイス上の IPv6 ルータ アドバタイズメントのルータ ライフタイム値を設定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] を選択します。

ステップ 2　設定するインターフェイスを選択します。

このインターフェイスは、IPv6 アドレスを使用して設定されている必要があります。詳細については、「IPv6 アドレッシングの設定」（P.12-15）を参照してください。

ステップ 3　[Edit] をクリックします。

[General]、[Advanced]、および [IPv6] という 3 つのタブを持つ [Edit Interface] ダイアログボックスが表示されます。

ステップ 4　[IPv6] タブをクリックします。

ステップ 5　[RA Lifetime] フィールドに有効なライフタイム値を入力します。

ステップ 6　[OK] をクリックします。

ステップ 7　[Apply] をクリックして、実行コンフィギュレーションを保存します。

DAD 設定の指定

インターフェイスの DAD 設定を指定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] を選択します。

ステップ 2　設定するインターフェイスを選択します。

このインターフェイスは、IPv6 アドレスを使用して設定されている必要があります。詳細については、「IPv6 アドレッシングの設定」（P.12-15）を参照してください。

ステップ 3　[Edit] をクリックします。

[General]、[Advanced]、および [IPv6] という 3 つのタブを持つ [Edit Interface] ダイアログボックスが表示されます。

ステップ 4　[IPv6] タブをクリックします。

ステップ 5　許可される DAD の試行回数を入力します。この設定では、DAD が IPv6 アドレスで実行されている間に、インターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定します。有効な値の範囲は 0 ～ 600 です。この値がゼロの場合、指定されたインターフェイスでの DAD 処理がディセーブルになります。デフォルトは 1 メッセージです。

ルータ アドバタイズメント メッセージの抑止

ルータ アドバタイズメント メッセージは、ルータ送信要求メッセージへの応答として自動的に送信されます。ASA で IPv6 プレフィックスを提供する必要がないインターフェイス（外部インターフェイスなど）では、これらのメッセージをディセーブルにできます。

インターフェイス上の IPv6 ルータ アドバタイズメントのルータ ライフタイム値を抑制するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] を選択します。

ステップ 2　どのインターフェイスに対してルータ アドバタイズメント送信を抑制するかを選択します。このインターフェイスは、IPv6 アドレスを使用して設定されている必要があります。

ステップ 3　[Edit] をクリックします。

[General]、[Advanced]、および [IPv6] という 3 つのタブを持つ [Edit Interface] ダイアログボックスが表示されます。

ステップ 4　[IPv6] タブをクリックします。

ステップ 5　[Suppress RA] チェックボックスをオンにします。

IPv6 DHCP リレーのアドレス設定フラグの設定

IPv6 ルータ アドバタイズメントにフラグを追加して、IPv6 アドレスや DNS サーバ アドレスなどの追加情報を取得するために DHCPv6 を使用するよう IPv6 自動設定クライアントに通知できます。

手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] を選択します。

ステップ 2　設定するインターフェイスを選択します。

ステップ 3　[Edit] をクリックします。

[General]、[Advanced]、および [IPv6] という 3 つのタブを持つ [Edit Interface] ダイアログボックスが表示されます。

ステップ 4　[IPv6] タブをクリックします。

ステップ 5　[Hosts should use DHCP for address config] チェックボックスをオンにして、IPv6 ルータ アドバタイズメント パケットの Managed Address Config フラグを設定します。このフラグは、取得されるステートレス自動設定のアドレス以外のアドレスの取得に DHCPv6 を使用する必要があることを IPv6 自動設定クライアントに通知します。

[Hosts should use DHCP for non-address config] チェックボックスをオンにして、IPv6 ルータ アドバタイズメント パケットの Other Address Config フラグを設定します。このフラグは、DHCPv6 から DNS サーバ アドレスなどの追加情報の取得に DHCPv6 を使用する必要があることを IPv6 自動設定クライアントに通知します。

ルータ アドバタイズメントの IPv6 プレフィックスの設定

IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] を選択します。

ステップ 2　どのインターフェイスに対してルータ アドバタイズメント送信を抑制するかを選択します。このインターフェイスは、IPv6 アドレスを使用して設定されている必要があります。

ステップ 3　[Edit] をクリックします。

[General]、[Advanced]、および [IPv6] という 3 つのタブを持つ [Edit Interface] ダイアログボックスが表示されます。

ステップ 4　[IPv6] タブをクリックします。

ステップ 5　[Interface IPv6 Prefixes] エリアで、[Add] をクリックします。

[Add IPv6 Prefix for Interface] ダイアログボックスが表示されます。

ステップ 6　プレフィックスの長さとともに IPv6 アドレスを入力します。

ステップ 7　（オプション）IPv6 アドレスを手動で設定するには、[No Auto-Configuration] チェックボックスをオンにします。この設定は、指定したプレフィックスが IPv6 自動設定に使用できないことをローカル リンク上のホストに知らせます。

ステップ 8　（オプション）IPv6 プレフィックスをアドバタイズしないように指定するには、[No Advertisements] チェックボックスをオンにします。

ステップ 9　（オプション）[Off Link] チェックボックスでは、指定したプレフィックスをリンクに割り当てるかどうかを指定します。指定したプレフィックスを含むアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。このプレフィックスは、オンリンクの判別には使用しないでください。

ステップ 10　[Prefix Lifetime] 領域で、[Lifetime Duration] オプション ボタンをクリックし、次の内容を指定します。

a.　プレフィックスの秒単位の有効なライフタイムをドロップダウン リストから選択します。この設定は、指定の IPv6 プレフィックスが有効なものとしてアドバタイズする時間です。最大値は無限大です。有効な値は、0 ～ 4294967295 です。デフォルトは、2592000（30 日）です。

b.　プレフィックスに対して優先させるライフタイムをドロップダウン リストから選択します。この設定は、指定の IPv6 プレフィックスが優先であるとしてアドバタイズする時間です。最大値は無限大です。有効な値は、0 ～ 4294967295 です。デフォルト設定は、604800（7 日）です。

ステップ 11　プレフィックス ライフタイムの有効期限を定義するには、[Lifetime Expiration Date] オプション ボタンをクリックし、次の内容を指定します。

a.　有効な月と日をドロップダウン リストから選択し、時間を hh:mm 形式で入力します。

b.　優先する月と日をドロップダウン リストから選択し、時間を hh:mm 形式で入力します。

ステップ 12　[OK] をクリックして設定内容を保存します。

[Interface IPv6 Prefixes Address] フィールドに優先日と有効日が表示されます。

スタティック IPv6 ネイバーの設定

ネイバーを追加しようとする前に、少なくとも 1 つのインターフェイスで IPv6 がイネーブルになっていることを確認します。そうしないと、ASDM によって、設定が失敗したというエラーメッセージが返されます。

IPv6 アドレスの設定方法の詳細については、「IPv6 アドレッシングの設定」（P.12-15）を参照してください。

IPv6 スタティック ネイバーを追加するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Advanced] > [IPv6 Neighbor Discovery Cache] を選択します。

ステップ 2　[Add] をクリックします。

[Add IPv6 Static Neighbor] ダイアログボックスが表示されます。

ステップ 3　[Interface Name] ドロップダウン リストから、ネイバーを追加するインターフェイスを選択します。

ステップ 4　[IP Address] フィールドにローカル データリンク アドレスに対応する IPv6 アドレスを入力するか、省略符号（[...]）をクリックしてアドレスを参照します。

IPv6 ネイバー探索プロセスによる学習を通して、指定された IPv6 アドレスのエントリがネイバー探索キャッシュにすでに存在する場合、エントリは自動的にスタティック エントリに変換されます。

ステップ 5　[MAC address] フィールドに、ローカルのデータ回線（ハードウェア）MAC アドレスを入力します。

ステップ 6　[OK] をクリックします。

（注）　変更を適用してコンフィギュレーションを保存する前に [Reset] をクリックすると、変更をキャンセルして元の値に復元できます。

ステップ 7　[Apply] をクリックして、実行コンフィギュレーションを保存します。

ダイナミックに検出されたネイバーの表示とクリア

ホストまたはノードがネイバーと通信する場合、ネイバーはネイバー探索キャッシュに追加されます。ネイバーがキャッシュから削除されるのは、そのネイバーとの通信が行われなくなったときです。

ダイナミックに検出されたネイバーを表示し、そのネイバーを IPv6 ネイバー探索キャッシュから削除するには、次の手順を実行します。

ステップ 1　[Monitoring] > [Interfaces] > [IPv6 Neighbor Discovery Cache] を選択します。

[IPv6 Neighbor Discovery Cache] ペインでは、スタティックおよびダイナミックに検出されたネイバーをすべて表示できます。

ステップ 2　ダイナミックに検出されたネイバーをすべてキャッシュから削除するには、[Clear Dynamic Neighbor Entries] をクリックします。

ダイナミックに検出されたネイバーがキャッシュから削除されます。

（注）　この手順では、ダイナミックに検出されたネイバーだけがキャッシュから削除され、スタティックなネイバーは削除されません。

その他の関連資料

IPv6 プレフィックスの実装に関連する追加情報については、次の項を参照してください。

- 「IPv6 プレフィックスの関連資料」（P.26-14）
- 「IPv6 プレフィックスとドキュメンテーションに関する RFC」（P.26-14）

IPv6 プレフィックスの関連資料

関連項目	マニュアル タイトル
ipv6 コマンド	*コマンド リファレンス*

IPv6 プレフィックスとドキュメンテーションに関する RFC

RFC	タイトル
RFC 2373 には、ルータ アドバタイズメントに IPv6 ネットワーク アドレス番号を表示する方法に関するすべてのドキュメントが含まれます。コマンド引数 ***ipv6-prefix*** がこのネットワーク番号を示します。この中では、アドレスを 16 進数形式で指定し、16 ビット値をコロンで区切る必要があります。	『IP Version 6 Addressing Architecture』
RFC 3849 では、IPv6 アドレス プレフィックスをドキュメンテーションで使用するための要件が規定されています。IPv6 ユニキャスト アドレス プレフィックスのうち、ドキュメンテーションでの使用のために予約されているのは 2001:DB8::/32 です。	『IPv6 Address Prefix Reserved for Documentation』

IPv6 ネイバー探索の機能履歴

表 26-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 26-2　IPv6 ネイバー探索の機能履歴

機能名	リリース	機能情報
IPv6 ネイバー探索	7.0(1)	この機能が導入されました。 次の画面が導入されました。 [Monitoring] > [Interfaces] > [IPv6 Neighbor Discovery Cache]。 [Configuration] > [Device Management] > [Advanced] > [IPv6 Neighbor Discovery Cache]。 [Configuration] > [Device Setup] > [Interfaces] > [IPv6]。
IPv6 DHCP リレーのアドレス設定フラグ	9.0(1)	次の画面が変更されました。[Configuration] > [Device Setup] > [Interfaces] > [IPv6]。

PART 7

AAA サーバおよびローカル データベース

AAA について

この章では、認証、認可、アカウンティング（AAA は「トリプル A」と読む）について説明します。AAA は、コンピュータ リソースへのアクセスを制御するための一連のサービスで、サービスの課金に必要な情報を提供します。これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

認証

認証はユーザを特定する方法です。アクセスが許可されるには、ユーザは通常、有効なユーザ名と有効なパスワードが必要です。AAA サーバは、データベースに保存されている他のユーザ クレデンシャルとユーザの認証資格情報を比較します。クレデンシャルが一致する場合、ユーザはネットワークへのアクセスが許可されます。クレデンシャルが一致しない場合、認証は失敗し、ネットワーク アクセスは拒否されます。

次の項目を認証するように、Cisco ASA を設定できます。

- ASA へのすべての管理接続（この接続には、次のセッションが含まれます）
  - Telnet
  - SSH
  - シリアル コンソール
  - ASDM（HTTPS を使用）
  - VPN 管理アクセス
- **enable** コマンド
- ネットワーク アクセス層
- VPN アクセス

認可

認可はポリシーを使用するプロセスです。どのようなアクティビティ、リソース、サービスに対するアクセス許可をユーザが持っているのかを判断します。ユーザが認証されると、そのユーザはさまざまなタイプのアクセスやアクティビティを認可される可能性があります。

次の項目を認可するように、ASA を設定できます。

- 管理コマンド
- ネットワーク アクセス層
- VPN アクセス

アカウンティング

アカウンティングは、アクセス時にユーザが消費したリソースを測定します。そこには、システム時間またはセッション中にユーザが送受信したデータ量などが含まれます。アカウンティングは、許可制御、課金、トレンド分析、リソース使用率、キャパシティ プランニングのアクティビティに使用されるセッションの統計情報と使用状況情報のログを通じて行われます。

認証、認可、アカウンティング間の相互作用

認証だけで使用することも、認可およびアカウンティングとともに使用することもできます。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングだけで使用することも、認証および認可とともに使用することもできます。

AAA サーバ

AAA サーバは、アクセス コントロールに使用されるネットワーク サーバです。認証は、ユーザを識別します。認可は、認証されたユーザがアクセスする可能性があるリソースとサービスを決定するポリシーを実行します。アカウンティングは、課金と分析に使用される時間とデータのリソースを追跡します。

AAA サーバ グループ

認証、許可、またはアカウンティングに外部 AAA サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの AAA サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。AAA サーバ グループは名前で識別されます。各サーバ グループは、あるサーバまたはサービスに固有です。

ローカル データベースのサポート

ASA は、ユーザ プロファイルを取り込むことができるローカル データベースを管理します。AAA サーバの代わりにローカル データベースを使用して、ユーザ認証、認可、アカウンティングを提供することもできます。

AAA のローカル データベース

この章では、AAA のローカル サーバを設定する方法について説明します。

ローカル データベースについて

次の機能にローカル データベースを使用できます。

- ASDM ユーザごとのアクセス
- コンソール認証
- Telnet 認証および SSH 認証
- **enable** コマンド認証

  この設定は、CLI アクセスにだけ使用され、Cisco ASDM ログインには影響しません。
- コマンド許可

  ローカル データベースを使用するコマンド許可を有効にすると、Cisco ASA では、ユーザ特権レベルを参照して、どのコマンドが使用できるかが特定されます。コマンド許可がディセーブルの場合は通常、特権レベルは参照されません。デフォルトでは、コマンドの特権レベルはすべて、0 または 15 のどちらかです。ASDM には、コマンドへの割り当てをイネーブルにできる特権レベルが事前に定義されています。割り当てることができるレベルは、15（管理）、5（読み取り専用）、3（監視専用）の 3 種類です。事前定義済みのレベルを使用する場合は、ユーザを 3 種類の特権レベルのいずれかに割り当てます。
- ネットワーク アクセス認証
- VPN クライアント認証

マルチ コンテキスト モードの場合、システム実行スペースでユーザ名を設定し、**login** コマンドを使用して CLI で個々にログインできます。ただし、システム実行スペースではローカル データベースを参照する AAA ルールは設定できません。

（注）　ローカル データベースはネットワーク アクセス認可には使用できません。

フォールバック サポート

ローカル データベースは、複数の機能のフォールバック方式として動作できます。この動作は、ASA から誤ってロックアウトされないようにすることを意図しています。

ログインすると、コンフィギュレーション内で指定されている最初のサーバから、応答があるまでグループ内のサーバが順に 1 つずつアクセスされます。グループ内のすべてのサーバが使用できない場合、ローカル データベースがフォールバック方式（管理認証および許可限定）として設定されていると、ASA はローカル データベースに接続しようとします。フォールバック方式として設定されていない場合、ASA は引き続き AAA サーバにアクセスしようとします。

フォールバック サポートを必要とするユーザについては、ローカル データベース内のユーザ名およびパスワードと、AAA サーバ上のユーザ名およびパスワードとを一致させることを推奨します。これにより、透過フォールバックがサポートされます。ユーザは、AAA サーバとローカル データベースのどちらがサービスを提供しているかが判別できないので、ローカル データベースのユーザ名およびパスワードとは異なるユーザ名およびパスワードを AAA サーバで使用することは、指定するべきユーザ名とパスワードをユーザが確信できないことを意味します。

ローカル データベースでサポートされているフォールバック機能は次のとおりです。

- コンソールおよびイネーブル パスワード認証：グループ内のサーバがすべて使用できない場合、ASA ではローカル データベースを使用して管理アクセスを認証します。これには、イネーブル パスワード認証が含まれる場合があります。
- コマンド許可：グループ内の TACACS+ サーバがすべて使用できない場合、特権レベルに基づいてコマンドを認可するためにローカル データベースが使用されます。
- VPN 認証および認可：VPN 認証および認可は、通常この VPN サービスをサポートしている AAA サーバが使用できない場合、ASA へのリモート アクセスをイネーブルにするためにサポートされます。管理者である VPN クライアントが、ローカル データベースへのフォールバックを設定されたトンネル グループを指定する場合、AAA サーバ グループが使用できない場合でも、ローカル データベースが必要な属性で設定されていれば、VPN トンネルが確立できます。

グループ内の複数のサーバを使用したフォールバックの仕組み

サーバ グループ内に複数のサーバを設定し、サーバ グループのローカル データベースへのフォールバックをイネーブルにしている場合、ASA からの認証要求に対してグループ内のどのサーバからも応答がないと、フォールバックが発生します。次のシナリオで例証します。

サーバ 1、サーバ 2 の順で、LDAP サーバ グループに 2 台の Active Directory サーバを設定します。リモート ユーザがログインすると、ASA によってサーバ 1 に対する認証が試みられます。

サーバ 1 から認証エラー（「*user not found*」など）が返されると、ASA によるサーバ 2 に対する認証は試みられません。

タイムアウト期間内にサーバ 1 から応答がないと（または認証回数が、設定されている最大数を超えている場合）、ASA によってサーバ 2 に対する認証が試みられます。

グループ内のどちらのサーバからも応答がなく、ASA にローカル データベースへのフォールバックが設定されている場合、ASA によってローカル データベースに対する認証が試みられます。

ローカル データベースのガイドライン

ローカル データベースを認証または認可に使用する場合、ASA からのロックアウトを必ず防止してください。

関連項目

「ロックアウトからの回復」（P.36-29）

ユーザ アカウントのローカル データベースへの追加

ユーザをローカル データベースに追加するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] の順に選択し、[Add] をクリックします。

[Add User Account-Identity] ダイアログボックスが表示されます。

ステップ 2　4 ～ 64 文字の長さのユーザ名を入力します。

ステップ 3　3 ～ 32 文字のパスワードを入力します。パスワードでは大文字と小文字が区別されます。フィールドには、アスタリスクだけが表示されます。セキュリティを確保するために、パスワードの長さは 8 文字以上にすることを推奨します。

（注）　[User Accounts] ペインでイネーブル パスワードを設定する場合は、ユーザ名 enable_15 に対するパスワードを変更します。ユーザ名 enable_15 は常に [User Accounts] ペインに表示され、デフォルト ユーザ名を表します。この方法は、ASDM のシステム コンフィギュレーションでイネーブル パスワードを設定する唯一の方法です。CLI で他のイネーブル レベル パスワード（enable password 10 など）を設定すると、そのユーザ名は enable_10 という形式で表示されます。

ステップ 4　パスワードを再度入力します。

セキュリティ上の理由から、パスワードを入力するこの 2 つのフィールドには、アスタリスクだけが表示されます。

ステップ 5　[Member of] フィールドにグループ名を入力してユーザが所属している VPN グループを指定し、[Add] をクリックします。

ステップ 6　[Access Restriction] 領域で、ユーザの管理アクセス レベルを設定します。まず、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] タブの [Perform authorization for exec shell access] オプションをクリックして、管理認可をイネーブルにする必要があります。

次のいずれかのオプションを選択します。

- [Full Access (ASDM, Telnet, SSH and console)]：ローカル データベースを使用した管理アクセスの認証を設定する場合、このオプションを指定するとユーザは ASDM、SSH、Telnet、およびコンソール ポートを使用できます。さらに認証もイネーブルにすると、ユーザはグローバル コンフィギュレーション モードにアクセスできます。
  - [Privilege Level]：ローカル コマンド許可でユーザに適用する特権レベルを選択します。範囲は、0（最低）～ 15（最高）です。

- [CLI login prompt for SSH, Telnet and console (no ASDM access)]：ローカル データベースを使用した管理アクセスの認証を設定する場合、このオプションを指定するとユーザは SSH、Telnet、およびコンソール ポートを使用できます。ユーザは設定に ASDM を使用できません（HTTP 認証を設定している場合）。ASDM 監視は可能です。さらにイネーブル認証も設定すると、ユーザはグローバル コンフィギュレーション モードにアクセスできません。
- [No ASDM, SSH, Telnet, or console access]：ローカル データベースを使用した管理アクセスの認証を設定する場合、このオプションを指定すると、ユーザは認証用に設定した管理アクセス方式を利用できなくなります（ただし、[Serial] オプションは除きます。つまり、シリアル アクセスは許可されます）。

ステップ 7　（オプション）ASA への SSH 接続の公開キー認証をユーザ単位でイネーブルにするには、[Navigation] ペインで次のオプションのいずれかをクリックします。

- [Public Key Authentication]：Base64 でエンコードされた公開キーに貼り付けます。SSH-RSA raw キー（証明書なし）を生成可能な任意の SSH キー生成ソフトウェア（ssh keygen など）を使用して、キーを生成できます。既存のキーを表示する場合は、キーは SHA-256 ハッシュを使用して暗号化されます。ハッシュ キーをコピーして貼りつける場合は、[Key is hashed] チェックボックスをオンにします。

  認証キーを削除するには、[Delete Key] をクリックして、確認ダイアログボックスを表示します。認証キーを削除する場合は [Yes] をクリックし、認証キーを保持する場合は [No] をクリックします。

- [Public Key Using PKF]：[Specify a new PKF key] チェックボックスをクリックして、公開キー ファイル（PKF）でフォーマットされたキー（4096 ビットまで）を貼りつけるかインポートします。Base64 形式で貼り付けるには大きすぎるキーにはこのフォーマットを使用します。たとえば、ssh の keygen を使用して 4096 ビット キーを生成し、PKF に変換して、このペインでインポートします。既存のキーを表示する場合は、SHA-256 ハッシュを使用して暗号化されます。ハッシュ キーをコピーして貼り付ける必要がある場合は、[Public Key Athentication] ペインからコピーし、[Key is hashed] チェックボックスをオンにした新しい ASA のペインに貼り付けます。

  認証キーを削除するには、[Delete Key] をクリックして、確認ダイアログボックスを表示します。認証キーを削除する場合は [Yes] をクリックし、認証キーを保持する場合は [No] をクリックします。

ステップ 8　[VPN Policy] をクリックして、このユーザの VPN ポリシー属性を設定します。VPN コンフィギュレーション ガイドを参照してください。

ステップ 9　[Apply] をクリックします。

ユーザがローカル データベースに追加され、変更内容が実行コンフィギュレーションに保存されます。

ヒント　[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] ペインの各カラムで特定のテキストを検索できます。[Find] ボックスに検索する特定のテキストを入力し、[Up] または [Down] 矢印をクリックします。テキスト検索にアスタリスク（「*」）と疑問符（「?」）をワイルドカードとして使用することもできます。

次の例では、Linux または Macintosh システムの SSH の共有キーを生成して、ASA にインポートします。

ステップ 1　コンピュータで 4096 ビットの ssh-rsa 公開キーおよび秘密キーを生成します。

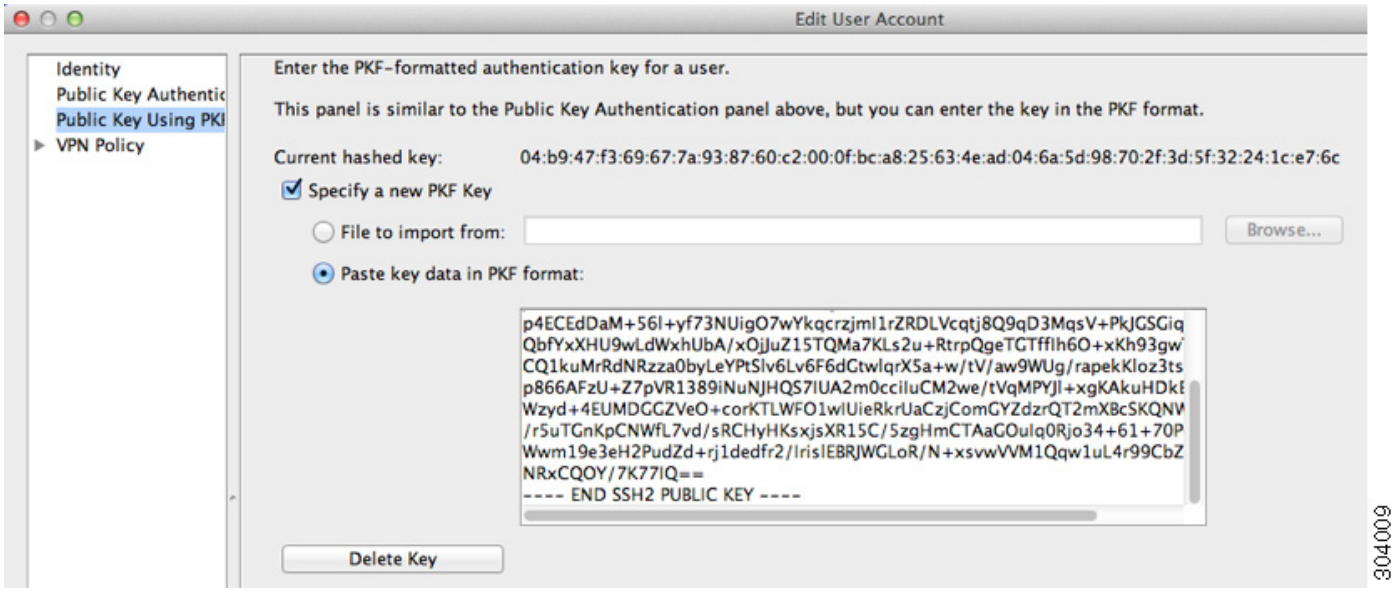
```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)?y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + .E         |
|  o o            |
| ooooo           |
+-----------------+
```

ステップ 2　PKF 形式にキーを変換します。

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by ramona@rboersma-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

ステップ 3　キーをクリップボードにコピーします。

ステップ 4　ASDM で、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] の順に選択し、ユーザ名を選択し、[Edit] をクリックします。[Public Key Using PKF] をクリックして、ウィンドウにキーを貼り付けます。



ステップ 5　ユーザが ASA に SSH できることを確認（テスト）します。

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)?yes
```

次のダイアログボックスが、パスフレーズを入力するために表示されます。

一方、端末セッションでは、以下が表示されます。

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

ローカル データベースでの認証および認可のテスト

ASA がローカル データベースに接続して、ユーザを認証または許可できることを確認するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] > [AAA Server Groups] テーブルで、サーバが含まれるサーバ グループをクリックします。

ステップ 2　[Servers in the Selected Group] テーブルでテストするサーバをクリックします。

ステップ 3　[Test] をクリックします。

選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 4　実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

ステップ 5　ユーザ名を入力します。

ステップ 6　認証をテストする場合は、ユーザ名のパスワードを入力します。

ステップ 7　[OK] をクリックします。

認証または認可のテスト メッセージが ASA からサーバへ送信されます。テストが失敗した場合は、ASDM によりエラー メッセージが表示されます。

ローカル データベースのモニタリング

ローカル データベースのモニタリングについては、次の画面を参照してください。

- [Monitoring] > [Properties] > [AAA Servers]

  このペインには、AAA サーバの統計情報が表示されます。

ローカル データベースの履歴

表 28-1　ローカル データベースの履歴

機能名	プラットフォーム リリース	機能情報
AAA のローカル データベース設定	7.0(1)	AAA 用にローカル データベースを設定する方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Device Management] > [Users/AAA] > [User Accounts]。

表 28-1　ローカル データベースの履歴

機能名	プラットフォーム リリース	機能情報
SSH 公開キー認証のサポート	9.1(2)	ASA への SSH 接続の公開キー認証がユーザ単位でイネーブルにできるようになりました。公開キー ファイル（PKF）でフォーマットされたキーまたは Base64 キーを指定できます。PKF キーは、4096 ビットまで使用できます。Base64 形式（最大 2048 ビット）の ASA サポートには大きすぎるキーには、PKF 形式を使用します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Authentication] [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Using PKF] *8.4(4.1) でも使用可能。PKF キー形式は 9.1(2) でのみサポートされます。*

AAA の RADIUS サーバ

この章では、AAA 用に RADIUS サーバを設定する方法について説明します。

RADIUS サーバに関する情報

Cisco ASA は AAA について、次の RFC 準拠 RADIUS サーバをサポートしています。

- Cisco Secure ACS 3.2、4.0、4.1、4.2、および 5.x
- Cisco Identity Services Engine（ISE）
- RSA 認証マネージャ 5.2、6.1 および 7.x の RSA Radius
- Microsoft

サポートされている認証方式

ASA は、RADIUS サーバでの次の認証方式をサポートします。

- PAP：すべての接続タイプの場合。
- CHAP および MS-CHAPv1：L2TP-over-IPsec 接続の場合。
- MS-CHAPv2：L2TP-over-IPsec 接続の場合。また、パスワード管理機能がイネーブルで、通常の IPsec リモート アクセス接続の場合。MS-CHAPv2 は、クライアントレス接続でも使用できます。
- 認証プロキシ モード：RADIUS から Active Directory、RADIUS から RSA/SDI、Radius からトークン サーバ、RSA/SDI から RADIUS の各接続。

（注）MS-CHAPv2 を、ASA と RADIUS サーバの間の VPN 接続で使用されるプロトコルとしてイネーブルにするには、トンネル グループ一般属性でパスワード管理をイネーブルにする必要があります。パスワード管理をイネーブルにすると、ASA から RADIUS サーバへの MS-CHAPv2 認証要求が生成されます。詳細については、**password-management** コマンドの説明を参照してください。

二重認証を使用し、トンネル グループでパスワード管理をイネーブルにした場合は、プライマリ認証要求とセカンダリ認証要求に MS-CHAPv2 要求属性が含まれます。RADIUS サーバが MS-CHAPv2 をサポートしない場合は、**no mschapv2-capable** コマンドを使用して、そのサーバが MS-CHAPv2 以外の認証要求を送信するように設定できます。

VPN 接続のユーザ許可

ASA では RADIUS サーバを使用して、ダイナミック ACL またはユーザごとの ACL 名を使用する VPN リモート アクセスおよびファイアウォール カットスルー プロキシ セッションのユーザ許可を実行できます。ダイナミック ACL を実装するには、これをサポートするように RADIUS サーバを設定する必要があります。ユーザを認証する場合、RADIUS サーバによってダウンロード可能 ACL、または ACL 名が ASA に送信されます。所定のサービスへのアクセスが ACL によって許可または拒否されます。認証セッションの有効期限が切れると、ASA によって ACL が削除されます。

ACL に加え、ASA は、その他多数の許可属性、VPN リモート アクセスおよびファイアウォール カットスルー プロキシ セッションに対する許可の設定をサポートしています。

RADIUS 属性のサポートされるセット

ASA は、次の RADIUS 属性のセットをサポートします。

- RFC 2138 に定義されている認証属性
- RFC 2139 に定義されているアカウンティング属性
- RFC 2868 に定義されているトンネル プロトコル サポート用の RADIUS 属性
- Cisco IOS ベンダー固有属性（VSA）は、RADIUS ベンダー ID 9 で識別されます。
- RADIUS ベンダー ID 3076 によって識別される Cisco VPN 関連 VSA
- RFC 2548 に定義されている Microsoft VSA

- Cisco VSA（Cisco-Priv-Level）。特権の標準ランキングである 0 ～ 15 の数値を指定します。1 が最低レベルを示し、15 が最高レベルを示します。0 レベルは特権がないことを示します。第 1 レベル（login）では、このレベルで使用可能なコマンドに対する特権 EXEC アクセスが許可されます。第 2 レベル（enable）では CLI コンフィギュレーション特権が許可されます。

サポートされる RADIUS 認可属性

認可とは、権限または属性を適用するプロセスのことです。認証サーバとして定義されている RADIUS サーバは、権限または属性が設定されている場合はこれらを使用します。これらの属性のベンダー ID は 3076 です。

表 29-1 に、ユーザ認可に使用可能な、サポートされている RADIUS 属性の一覧を示します。

（注）RADIUS 属性名には、cVPN3000 プレフィックスは含まれていません。Cisco Secure ACS 4.x は、この新しい名前をサポートしますが、4.0 以前の ACS の属性名にはまだ cVPN3000 プレフィックスが含まれています。ASA によって RADIUS 属性が適用されるときは、属性名ではなく数値の属性 ID に基づいて適用されます。

表 29-1 に示した属性はすべてダウンストリーム属性であり、RADIUS サーバから ASA に送信されます。ただし、属性番号 146、150、151、および 152 を除きます。これらの属性番号はアップストリーム属性であり、ASA から RADIUS サーバに送信されます。RADIUS 属性 146 および 150 は、認証および許可の要求の場合に ASA から RADIUS サーバに送信されます。前述の 4 つの属性はすべて、アカウンティング開始、中間アップデート、および終了の要求の場合に ASA から RADIUS サーバに送信されます。アップストリーム RADIUS 属性 146、150、151、152 は、バージョン 8.4(3) で導入されました。

Cisco ACS 5x および Cisco ISE では、バージョン 9.0(1) の RADIUS 認証を使用する IP アドレスの割り当ての IPv6 Framed IP アドレスはサポートされません。

表 29-1　サポートされる RADIUS 認可属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Access-Hours	Y	1	文字列	シングル	時間範囲の名前（Business-hours など）
Access-List-Inbound	Y	86	文字列	シングル	ACL ID
Access-List-Outbound	Y	87	文字列	シングル	ACL ID
Address-Pools	Y	217	文字列	シングル	IP ローカル プールの名前
Allow-Network-Extension-Mode	Y	64	ブール	シングル	0 = ディセーブル 1 = イネーブル
Authenticated-User-Idle-Timeout	Y	50	整数	シングル	1 ～ 35791394 分
Authorization-DN-Field	Y	67	文字列	シングル	有効な値：UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER、use-entire-name
Authorization-Required		66	整数	シングル	0 = しない 1 = する

表 29-1　サポートされる RADIUS 認可属性（続き）

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Authorization-Type	Y	65	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP
Banner1	Y	15	文字列	シングル	Cisco VPN リモート アクセス セッション（IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2、およびクライアントレス SSL）に対して表示されるバナー文字列
Banner2	Y	36	文字列	シングル	Cisco VPN リモート アクセス セッション（IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2、およびクライアントレス SSL）に対して表示されるバナー文字列。Banner2 文字列は Banner1 文字列に連結されます（設定されている場合）。
Cisco-IP-Phone-Bypass	Y	51	整数	シングル	0 = ディセーブル 1 = イネーブル
Cisco-LEAP-Bypass	Y	75	整数	シングル	0 = ディセーブル 1 = イネーブル
Client Type	Y	150	整数	シングル	1 = Cisco VPN クライアント（IKEv1） 2 = AnyConnect クライアント SSL VPN 3 = クライアントレス SSL VPN 4 = カットスルー プロキシ 5 = L2TP/IPsec SSL VPN 6 = AnyConnect クライアント IPsec VPN（IKEv2）
Client-Type-Version-Limiting	Y	77	文字列	シングル	IPsec VPN のバージョン番号を示す文字列
DHCP-Network-Scope	Y	61	文字列	シングル	IP アドレス
Extended-Authentication-On-Rekey	Y	122	整数	シングル	0 = ディセーブル 1 = イネーブル
Group-Policy	Y	25	文字列	シングル	リモート アクセス VPN セッションのグループ ポリシーを設定します。バージョン 8.2.x 以降では、IETF-Radius-Class の代わりにこの属性を使用します。次の形式のいずれかを使用できます。 • *グループ ポリシー名* • OU=*グループ ポリシー名* • OU=*グループ ポリシー名*;
IE-Proxy-Bypass-Local		83	整数	シングル	0 = なし 1 = ローカル

表 29-1　サポートされる RADIUS 認可属性（続き）

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IE-Proxy-Exception-List		82	文字列	シングル	改行（\n）区切りの DNS ドメインのリスト
IE-Proxy-PAC-URL	Y	133	文字列	シングル	PAC アドレス文字列
IE-Proxy-Server		80	文字列	シングル	IP アドレス
IE-Proxy-Server-Policy		81	整数	シングル	1 = 変更なし 2 = プロキシなし 3 = 自動検出 4 = コンセントレータ設定を使用する
IKE-KeepAlive-Confidence-Interval	Y	68	整数	シングル	10 ～ 300 秒
IKE-Keepalive-Retry-Interval	Y	84	整数	シングル	2 ～ 10 秒
IKE-Keep-Alives	Y	41	ブール	シングル	0 = ディセーブル 1 = イネーブル
Intercept-DHCP-Configure-Msg	Y	62	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Allow-Passwd-Store	Y	16	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Authentication		13	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP（認可のみ） 3 = NT ドメイン 4 = SDI 5 = 内部 6 = RADIUS での Expiry 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	Y	42	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Backup-Server-List	Y	60	文字列	シングル	サーバ アドレス（スペース区切り）
IPsec-Backup-Servers	Y	59	文字列	シングル	1 = クライアントが設定したリストを使用する 2 = クライアント リストをディセーブルにして消去する 3 = バックアップ サーバ リストを使用する
IPsec-Client-Firewall-Filter-Name		57	文字列	シングル	クライアントにファイアウォール ポリシーとして配信するフィルタの名前を指定します。
IPsec-Client-Firewall-Filter-Optional	Y	58	整数	シングル	0 = 必須 1 = オプション
IPsec-Default-Domain	Y	28	文字列	シングル	クライアントに送信するデフォルト ドメイン名を 1 つだけ指定します（1 ～ 255 文字）。

表 29-1　サポートされる RADIUS 認可属性（続き）

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IPsec-IKE-Peer-ID-Check	Y	40	整数	シングル	1 = 必須 2 = ピア証明書でサポートされる場合 3 = チェックしない
IPsec-IP-Compression	Y	39	整数	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Mode-Config	Y	31	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Over-UDP	Y	34	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Over-UDP-Port	Y	35	整数	シングル	4001 ～ 49151。デフォルトは 10000 です。
IPsec-Required-Client-Firewall-Capability	Y	56	整数	シングル	0 = なし 1 = リモート FW Are-You-There（AYT）で定義されているポリシー 2 = Policy pushed CPP 4 = サーバからのポリシー
IPsec-Sec-Association		12	文字列	シングル	セキュリティ アソシエーションの名前
IPsec-Split-DNS-Names	Y	29	文字列	シングル	クライアントに送信するセカンダリドメイン名のリストを指定します（1 ～ 255 文字）。
IPsec-Split-Tunneling-Policy	Y	55	整数	シングル	0 = スプリット トンネリングなし 1 = スプリット トンネリング 2 = ローカル LAN を許可
IPsec-Split-Tunnel-List	Y	27	文字列	シングル	スプリット トンネルの包含リストを記述したネットワークまたは ACL の名前を指定します。
IPsec-Tunnel-Type	Y	30	整数	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPsec-User-Group-Lock		33	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPv6-Address-Pools	Y	218	文字列	シングル	IP ローカル プール IPv6 の名前
IPv6-VPN-Filter	Y	219	文字列	シングル	ACL 値
L2TP-Encryption		21	整数	シングル	ビットマップ： 1 = 暗号化が必要 2 =40 ビット 4 =128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化/ステートレスが必要
L2TP-MPPC-Compression		38	整数	シングル	0 = ディセーブル 1 = イネーブル

表 29-1　サポートされる RADIUS 認可属性（続き）

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Member-Of	Y	145	文字列	シングル	カンマ区切りの文字列。例： エンジニアリング、営業 ダイナミック アクセス ポリシーで使用できる管理属性。グループ ポリシーは設定されません。
MS-Client-Subnet-Mask	Y	63	ブール	シングル	IP アドレス
NAC-Default-ACL		92	文字列		ACL
NAC-Enable		89	整数	シングル	0 = しない 1 = する
NAC-Revalidation-Timer		91	整数	シングル	300 ～ 86400 秒
NAC-Settings	Y	141	文字列	シングル	NAC ポリシーの名前
NAC-Status-Query-Timer		90	整数	シングル	30 ～ 1800 秒
Perfect-Forward-Secrecy-Enable	Y	88	ブール	シングル	0 = しない 1 = する
PPTP-Encryption		20	整数	シングル	ビットマップ： 1 = 暗号化が必要 2 =40 ビット 4 =128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化/ステートレスが必要
PPTP-MPPC-Compression		37	整数	シングル	0 = ディセーブル 1 = イネーブル
Primary-DNS	Y	5	文字列	シングル	IP アドレス
Primary-WINS	Y	7	文字列	シングル	IP アドレス
Privilege-Level	Y	220	整数	シングル	0 ～ 15 の整数。
Required-Client- Firewall-Vendor-Code	Y	45	整数	シングル	1 = シスコ（Cisco Integrated Client を使用） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = シスコ（Cisco Intrusion Prevention Security Agent を使用）
Required-Client-Firewall-Description	Y	47	文字列	シングル	文字列

表 29-1　サポートされる RADIUS 認可属性（続き）

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Required-Client-Firewall-Product-Code	Y	46	整数	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Agent または Cisco Integrated Client（CIC） Zone Labs 製品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 製品： 1 = BlackIce Defender/Agent Sygate 製品： 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Required-Individual-User-Auth	Y	49	整数	シングル	0 = ディセーブル 1 = イネーブル
Require-HW-Client-Auth	Y	48	ブール	シングル	0 = ディセーブル 1 = イネーブル
Secondary-DNS	Y	6	文字列	シングル	IP アドレス
Secondary-WINS	Y	8	文字列	シングル	IP アドレス
SEP-Card-Assignment		9	整数	シングル	未使用
Session Subtype	Y	152	整数	シングル	0 = なし 1 = クライアントレス 2 = クライアント 3 = クライアントのみ Session Subtype が適用されるのは、Session Type（151）属性の値が 1、2、3、または 4 の場合のみです。
Session Type	Y	151	整数	シングル	0 = なし 1 = AnyConnect クライアント SSL VPN 2 = AnyConnect クライアント IPSec VPN（IKEv2） 3 = クライアントレス SSL VPN 4 = クライアントレス電子メール プロキシ 5 = Cisco VPN クライアント（IKEv1） 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN ロード バランシング
Simultaneous-Logins	Y	2	整数	シングル	0-2147483647
Smart-Tunnel	Y	136	文字列	シングル	スマート トンネルの名前

表 29-1　サポートされる RADIUS 認可属性（続き）

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Smart-Tunnel-Auto	Y	138	整数	シングル	0 = ディセーブル 1 = イネーブル 2 =自動スタート
Smart-Tunnel-Auto-Signon-Enable	Y	139	文字列	シングル	ドメイン名が付加された Smart Tunnel Auto Signon リストの名前
Strip-Realm	Y	135	ブール	シングル	0 = ディセーブル 1 = イネーブル
SVC-Ask	Y	131	文字列	シングル	0 = ディセーブル 1 = イネーブル 3 = デフォルト サービスをイネーブルにする 5 = デフォルト クライアントレスをイネーブルにする （2 と 4 は使用しない）
SVC-Ask-Timeout	Y	132	整数	シングル	5 ～ 120 秒
SVC-DPD-Interval-Client	Y	108	整数	シングル	0 = オフ 5 ～ 3600 秒
SVC-DPD-Interval-Gateway	Y	109	整数	シングル	0 = オフ 5 ～ 3600 秒
SVC-DTLS	Y	123	整数	シングル	0 = False 1 = True
SVC-Keepalive	Y	107	整数	シングル	0 = オフ 15 ～ 600 秒
SVC-Modules	Y	127	文字列	シングル	文字列（モジュールの名前）
SVC-MTU	Y	125	整数	シングル	MTU 値 256 ～ 1406 バイト
SVC-Profiles	Y	128	文字列	シングル	文字列（プロファイルの名前）
SVC-Rekey-Time	Y	110	整数	シングル	0 = ディセーブル 1 ～ 10080 分
Tunnel Group Name	Y	146	文字列	シングル	1 ～ 253 文字
Tunnel-Group-Lock	Y	85	文字列	シングル	トンネル グループの名前または「none」
Tunneling-Protocols	Y	11	整数	シングル	1 = PPTP 2 = L2TP 4 = IPSec（IKEv1） 8 = L2TP/IPSec 16 = WebVPN. 32 = SVC 64 = IPsec（IKEv2） 8 と 4 は相互排他。 0 ～ 11、16 ～ 27、32 ～ 43、48 ～ 59 は有効値。

表 29-1　サポートされる RADIUS 認可属性（続き）

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Use-Client-Address		17	ブール	シングル	0 = ディセーブル 1 = イネーブル
VLAN	Y	140	整数	シングル	0 ～ 4094
WebVPN-Access-List	Y	73	文字列	シングル	アクセス リスト名
WebVPN ACL	Y	73	文字列	シングル	デバイスの WebVPN ACL 名
WebVPN-ActiveX-Relay	Y	137	整数	シングル	0 = ディセーブル Otherwise = イネーブル
WebVPN-Apply-ACL	Y	102	整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Auto-HTTP-Signon	Y	124	文字列	シングル	予約済み
WebVPN-Citrix-Metaframe-Enable	Y	101	整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Content-Filter-Parameters	Y	69	整数	シングル	1 = Java ActiveX 2 = Java スクリプト 4 = イメージ 8 = イメージに含まれるクッキー
WebVPN-Customization	Y	113	文字列	シングル	カスタマイゼーションの名前
WebVPN-Default-Homepage	Y	76	文字列	シングル	URL（たとえば http://example-example.com）
WebVPN-Deny-Message	Y	116	文字列	シングル	有効な文字列（500 文字以内）
WebVPN-Download_Max-Size	Y	157	整数	シングル	0x7fffffff
WebVPN-File-Access-Enable	Y	94	整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Browsing-Enable	Y	96	整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Entry-Enable	Y	95	整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	Y	78	文字列	シングル	オプションのワイルドカード（*）を使用したカンマ区切りの DNS/IP（たとえば、*.cisco.com、192.168.1.*、wwwin.cisco.com）
WebVPN-Hidden-Shares	Y	126	整数	シングル	0 = なし 1 = 表示
WebVPN-Home-Page-Use-Smart-Tunnel	Y	228	ブール	シングル	クライアントレス ホーム ページをスマート トンネル経由で表示する場合にイネーブルにします。
WebVPN-HTML-Filter	Y	69	Bitmap	シングル	1 = Java ActiveX 2 = スクリプト 4 = イメージ 8 = クッキー

表 29-1　サポートされる RADIUS 認可属性（続き）

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-HTTP-Compression	Y	120	整数	シングル	0 = オフ 1 = デフレート圧縮
WebVPN-HTTP-Proxy-IP-Address	Y	74	文字列	シングル	http= または https= プレフィックス付きの、カンマ区切りの DNS/IP:ポート（例：http=10.10.10.10:80、https=11.11.11.11:443）
WebVPN-Idle-Timeout-Alert-Interval	Y	148	整数	シングル	0 ～ 30。0 = ディセーブル。
WebVPN-Keepalive-Ignore	Y	121	整数	シングル	0 ～ 900
WebVPN-Macro-Substitution	Y	223	文字列	シングル	無制限。例については、次の URL にある『*SSL VPN Deployment Guide*』を参照してください。 http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Macro-Substitution	Y	224	文字列	シングル	無制限。例については、次の URL にある『*SSL VPN Deployment Guide*』を参照してください。 http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Port-Forwarding-Enable	Y	97	整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	98	整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-List	Y	72	文字列	シングル	ポート転送リスト名
WebVPN-Port-Forwarding-Name	Y	79	文字列	シングル	名前の文字列（例、「Corporate-Apps」）。 このテキストでクライアントレス ポータル ホーム ページのデフォルト文字列「Application Access」が置き換えられます。
WebVPN-Post-Max-Size	Y	159	整数	シングル	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	Y	149	整数	シングル	0 ～ 30。0 = ディセーブル。
WebVPN Smart-Card-Removal-Disconnect	Y	225	ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Smart-Tunnel	Y	136	文字列	シングル	スマート トンネルの名前
WebVPN-Smart-Tunnel-Auto-Sign-On	Y	139	文字列	シングル	ドメイン名が付加されたスマート トンネル自動サインオン リストの名前

表 29-1　サポートされる RADIUS 認可属性（続き）

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Smart-Tunnel-Auto-Start	Y	138	整数	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動開始
WebVPN-Smart-Tunnel-Tunnel-Policy	Y	227	文字列	シングル	「e ネットワーク名」、「i ネットワーク名」、「a」のいずれか。ここで、ネットワーク名は、スマート トンネル ネットワークのリストの名前です。e はトンネルが除外されることを示し、i はトンネルが指定されることを示し、a はすべてのトンネルを示します。
WebVPN-SSL-VPN-Client-Enable	Y	103	整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SSL-VPN-Client-Keep-Installation	Y	105	整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SSL-VPN-Client-Required	Y	104	整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SSO-Server-Name	Y	114	文字列	シングル	有効な文字列
WebVPN-Storage-Key	Y	162	文字列	シングル	
WebVPN-Storage-Objects	Y	161	文字列	シングル	
WebVPN-SVC-Keepalive-Frequency	Y	107	整数	シングル	15 ～ 600 秒、0=オフ
WebVPN-SVC-Client-DPD-Frequency	Y	108	整数	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-DTLS-Enable	Y	123	整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-DTLS-MTU	Y	125	整数	シングル	MTU 値は 256 ～ 1406 バイトです。
WebVPN-SVC-Gateway-DPD-Frequency	Y	109	整数	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-Rekey-Time	Y	110	整数	シングル	4 ～ 10080 分、0=オフ
WebVPN-SVC-Rekey-Method	Y	111	整数	シングル	0（オフ）、1（SSL）、2（新しいトンネル）
WebVPN-SVC-Compression	Y	112	整数	シングル	0（オフ）、1（デフォルトの圧縮）
WebVPN-UNIX-Group-ID (GID)	Y	222	整数	シングル	UNIX での有効なグループ ID
WebVPN-UNIX-User-ID (UIDs)	Y	221	整数	シングル	UNIX での有効なユーザ ID
WebVPN-Upload-Max-Size	Y	158	整数	シングル	0x7fffffff
WebVPN-URL-Entry-Enable	Y	93	整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-URL-List	Y	71	文字列	シングル	URL リスト名
WebVPN-User-Storage	Y	160	文字列	シングル	
WebVPN-VDI	Y	163	文字列	シングル	設定のリスト

サポートされる IETF RADIUS 認可属性

表 29-2 に、サポートされている IETF RADIUS 属性を示します。

表 29-2　サポートされる IETF RADIUS 属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IETF-Radius-Class	Y	25		シングル	バージョン 8.2.x 以降の場合は、表 29-1 で説明している Group-Policy 属性（VSA 3076、#25）を使用することを推奨します。 • *グループ ポリシー名* • OU=*グループ ポリシー名* • OU=*グループ ポリシー名*
IETF-Radius-Filter-Id	Y	11	文字列	シングル	フル トンネルの IPsec クライアントと SSL VPN クライアントのみに適用される、ASA で定義された ACL 名。
IETF-Radius-Framed-IP-Address	Y	該当なし	文字列	シングル	IP アドレス
IETF-Radius-Framed-IP-Netmask	Y	該当なし	文字列	シングル	IP アドレス マスク
IETF-Radius-Idle-Timeout	Y	28	整数	シングル	秒
IETF-Radius-Service-Type	Y	6	整数	シングル	秒。使用可能なサービス タイプの値： • .Administrative：ユーザは configure プロンプトへのアクセスを許可されています。 • .NAS-Prompt：ユーザは exec プロンプトへのアクセスを許可されています。 • .remote-access：ユーザはネットワーク アクセスを許可されています。
IETF-Radius-Session-Timeout	Y	27	整数	シングル	秒

RADIUS アカウンティング切断の理由コード

これらのコードは、パケットを送信するときに ASA が切断された場合に返されます。

切断の理由コード
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6
ACCT_DISC_ADMIN_REBOOT = 7

切断の理由コード （続き）
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

RADIUS サーバのライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

その他のガイドライン

- シングル モードで最大 100 個のサーバ グループ、またはマルチ モードでコンテキストごとに 4 つのサーバ グループを持つことができます。

- 各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台のサーバを含めることができます。
- ローカル データベースを使用してフォールバック サポートを設定する必要がある場合は、「フォールバック サポート」（P.28-2）と「グループ内の複数のサーバを使用したフォールバックの仕組み」（P.28-2）を参照してください。
- RADIUS 認証を使用する場合に、ASA からのロックアウトを防止するには、「ロックアウトからの回復」（P.36-29）を参照してください。

RADIUS サーバの設定

RADIUS サーバを設定するためのタスク フロー

ステップ 1　ASA の属性を RADIUS サーバにロードします。属性をロードするために使用する方法は、使用している RADIUS サーバのタイプによって異なります。

- Cisco ACS を使用している場合：サーバには、これらの属性がすでに統合されています。したがって、この手順をスキップできます。
- 他のベンダーの RADIUS サーバ（たとえば Microsoft Internet Authentication Service）の場合：ASA の各属性を手動で定義する必要があります。属性を定義するには、属性名または番号、タイプ、値、ベンダー コード（3076）を使用します。

ステップ 2　RADIUS サーバ グループを追加します。「RADIUS サーバ グループの設定 」（P.29-15）を参照してください。

ステップ 3　サーバ グループの場合は、グループにサーバを追加します。「グループへの RADIUS サーバの追加」（P.29-17）を参照してください。

ステップ 4　（オプション）AAA 認証チャレンジ プロセスの実行中にユーザに表示するテキストを指定します。「認証プロンプトの追加」（P.29-19）を参照してください。

RADIUS サーバ グループの設定

認証、許可、またはアカウンティングに外部 RADIUS サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの RADIUS サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。AAA サーバ グループは名前で識別されます。

RADIUS サーバ グループを追加するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

ステップ 2　[AAA Server Groups] 領域で、[Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3　[Server Group] フィールドで、グループの名前を入力します。

ステップ 4　[Protocol] ドロップダウン リストから、RADIUS サーバ タイプを選択します。

ステップ 5　[Accounting Mode] フィールドで、[Simultaneous] または [Single] をクリックします。

[Single] モードの場合、ASA ではアカウンティング データが 1 つのサーバにだけ送信されます。

[Simultaneous] モードの場合、ASA ではアカウンティング データがグループ内のすべてのサーバに送信されます。

ステップ 6　[Reactivation Mode] フィールドで、[Depletion] または [Timed] をクリックします。

[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。

Timed モードでは、障害が発生したサーバは 30 秒の停止時間の後で再アクティブ化されます。

ステップ 7　[Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

[Dead Time] には、グループ内の最後のサーバがディセーブルになってから、すべてのサーバが再びイネーブルになるまでの時間間隔を分単位で指定します。

ステップ 8　[Max Failed Attempts] フィールドに、許容される試行の失敗回数を指定します。

このオプションで設定するのは、応答のないサーバを非アクティブと宣言するまでに許可される接続試行の失敗回数です。

ステップ 9　（オプション）RADIUS サーバのタイプを追加する場合には、次の手順を実行します。

a. クライアントレス SSL セッションおよび AnyConnect セッションに対して、マルチセッション アカウンティングをイネーブルにする場合は、[Enable interim accounting update] チェックボックスをオンにします。

b. [Enable Active Directory Agent Mode] チェックボックスをオンにして ASA と AD エージェント間の共有秘密を指定し、RADIUS サーバ グループにフル機能の RADIUS サーバではない AD エージェントを含めるよう指示します。ユーザ アイデンティティに関連付けることができるのは、このオプションを使用して設定された RADIUS サーバ グループのみです。

c. ISE が許可変更（CoA）RADIUS パケットを送信できるようにするには、[Enable dynamic authorization] チェックボックスをオンにします。これは、ISE で行われたポリシー変更を VPN 接続の存続期間中に強制できるようにします。

d. [Dynamic Authorization Port] に入力します。これは、RADIUS CoA 要求をリッスンするポートです。通常は 1700 です。有効な範囲は 1 ～ 65535 です。

e. RADIUS サーバ グループの認可専用モードをイネーブルにするには、[Use authorize only mode] チェックボックスをオンにします。このチェックボックスを選択する場合、個別の AAA サーバに対して設定する共通パスワードは不要なため、設定する必要はありません。

f. [VPN3K Compatibility Option] 下矢印をクリックしてリストを展開し、さらに次のいずれかのボタンをクリックして、RADIUS パケットから受け取ったダウンロード可能 ACL を、Cisco AV ペア ACL とマージするかどうかを指定します。

– **Do not merge**

– **Place the downloadable ACL after Cisco AV-pair ACL**

– **Place the downloadable ACL before Cisco AV-pair ACL**

ステップ 10　[OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバ グループが [AAA Server Groups] テーブルに追加されます。

ステップ 11　[AAA Server Groups] ダイアログボックスの [Apply] をクリックして、変更内容を実行コンフィギュレーションに保存します。

グループへの RADIUS サーバの追加

RADIUS サーバをグループに追加するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択し、[AAA Server Groups] 領域で、サーバを追加するサーバ グループをクリックします。

テーブル内の該当する行が選択されます。

ステップ 2　[Selected Group] 領域の [Servers]（下部ペイン）で、[Add] をクリックします。

サーバ グループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3　[Interface Name] ドロップダウン リストから、認証サーバが常駐するインターフェイスの名前を選択します。

ステップ 4　[Server Name] フィールドまたは [IP Address] フィールドに、グループに追加するサーバの名前または IP アドレスを入力します。

ステップ 5　[Timeout] フィールドで、タイムアウト値を入力します。デフォルト値をそのまま使用することもできます。[Timeout] フィールドには、ASA がバックアップ サーバへ要求を送信する前に、プライマリ サーバからの応答を待機する時間を秒単位で指定します。

ステップ 6　[ACL Netmask Convert] フィールドに、ダウンロード可能 ACL で受け取ったネットマスクを ASA が処理する方法を指定します。次のオプションから選択します。

- [Detect automatically] : 使用されているネットマスク表現のタイプの判別が ASA によって試みられます。ASA でワイルドカード ネットマスク表現が検出された場合は、ASA により標準ネットマスク表現に変換されます。

  （注）　一部のワイルドカード表現は明確な検出が困難なため、この設定を選択した場合には、ワイルドカード ネットマスク表現が誤って標準ネットマスク表現として検出されることもあります。

- [Standard]：ASA は、RADIUS サーバから受信したダウンロード可能 ACL に、標準ネットマスク表現のみが含まれていると見なします。ワイルドカード ネットマスク表現からの変換は実行されません。
- [Wildcard]：ASA は、RADIUS サーバから受信したダウンロード可能 ACL に、ワイルドカード ネットマスク表現のみが含まれていると見なし、ACL のダウンロード時にそれらのすべてを標準ネットマスク表現に変換します。

ステップ 7　[Common Password] フィールドに、この ASA を介して RADIUS 認可サーバにアクセスするユーザ間で共通の、大文字と小文字が区別されるパスワードを指定します。この情報は、RADIUS サーバ管理者に伝えてください。

（注）　RADIUS 認証サーバ（認可サーバではない）に対しては、共通のパスワードは設定しないでください。

このフィールドを空白のままにした場合は、RADIUS 認可サーバにアクセスする際のパスワードには、各ユーザ名が使用されます。

RADIUS 認可サーバを認証に使用することは避けてください。共通パスワードやユーザ名を転用したパスワードは、ユーザごとに一意のパスワードに比べ、安全性が低くなります。

このパスワードは、RADIUS プロトコルや RADIUS サーバによって要求されますが、ユーザが知っている必要はありません。

ステップ 8　二重認証を使用し、トンネル グループでパスワード管理をイネーブルにした場合は、プライマリ認証要求とセカンダリ認証要求に MS-CHAPv2 要求属性が含まれます。RADIUS サーバが MS-CHAPv2 をサポートしていない場合、このチェックボックスをオンにすれば、そのサーバから非 MS-CHAPv2 認証要求が送信されるようにできます。

ステップ 9　[Retry Interval] フィールドに、ASA がサーバへのアクセスを試行する間の待機時間を 1 ～10 秒で指定します。

（注）　その後の再試行の間隔は、入力した再試行間隔の設定にかかわらず、常に 50 ミリ秒または 100 ミリ秒です。これは意図された動作です。

ステップ 10　[Accounting Mode] フィールドで、[Simultaneous] または [Single] をクリックします。

[Single] モードの場合、ASA ではアカウンティング データが 1 つのサーバにだけ送信されます。

[Simultaneous] モードの場合、ASA ではアカウンティング データがグループ内のすべてのサーバに送信されます。

ステップ 11　[Server Accounting Port] フィールドに、ユーザのアカウンティングに使用するサーバ ポートを指定します。デフォルトのポートは 1646 です。

ステップ 12　[Server Authentication Port] フィールドに、ユーザの認証に使用するサーバ ポートを指定します。デフォルトのポートは 1645 です。

ステップ 13　[Server Secret Key] フィールドに、ASA に対する RADIUS サーバの認証に使用される共有秘密キーを指定します。設定したサーバ秘密キーは、RADIUS サーバで設定されたサーバ秘密キーと一致する必要があります。サーバ秘密キーが不明の場合は、RADIUS サーバの管理者に問い合わせてください。最大フィールド長は、64 文字です。

ステップ 14　[OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、AAA サーバが AAA サーバ グループに追加されます。

ステップ 15　[AAA Server Groups] ペインで [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

認証プロンプトの追加

RADIUS サーバからのユーザ認証が必要な場合に、ASA 経由の HTTP、FTP、Telnet アクセス用の AAA チャレンジ テキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワード プロンプトの上に表示されます。認証プロンプトを指定しない場合、RADIUS サーバでの認証時にユーザに対して表示される内容は次のようになります。

接続タイプ	デフォルトのプロンプト
FTP	FTP 認証
HTTP	HTTP 認証
Telnet	なし

認証プロンプトを追加するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt] ペインの [Prompt] フィールドに、ログイン時にユーザに対して表示されるユーザ名およびパスワードのプロンプトの上部にメッセージとして表示されるテキストを入力します。

次の表に、認証プロンプトの文字数制限を示します。

アプリケーション	文字制限
Microsoft Internet Explorer	37
Telnet	235
FTP	235

ステップ 2　[Messages] 領域の [User accepted message] フィールドおよび [User rejected message] フィールドにそれぞれメッセージを入力します。

Telnet からのユーザ認証を実行する場合、[User accepted message] オプションおよび [User rejected message] オプションを使用すれば、認証の試みが RADIUS サーバによって承認または拒否されたことを示す、異なる状態のプロンプトを表示できます。

これらのメッセージ テキストをそれぞれ指定した場合、ASA では、RADIUS サーバにより認証されたユーザに対してはユーザ承認メッセージ テキストが表示され、認証されなかったユーザに対しては ASA によりユーザ拒否メッセージ テキストが表示されます。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジ テキストのみが表示されます。ユーザ承認メッセージ テキストおよびユーザ拒否メッセージ テキストは表示されません。

ステップ 3　[Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

RADIUS サーバによる認証および許可のテスト

ASA において、RADIUS サーバへのアクセスやユーザの認証または認可が実行できるかどうかを判定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] > [AAA Server Groups] テーブルで、サーバが含まれるサーバ グループをクリックします。

テーブル内の該当する行が選択されます。

ステップ 2　[Selected Group] テーブルの [Servers] から、テストするサーバをクリックします。

テーブル内の該当する行が選択されます。

ステップ 3　[Test] をクリックします。

選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 4　実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

ステップ 5　[Username] フィールドにユーザ名を入力します。

ステップ 6　認証をテストする場合は、そのユーザ名に対応するパスワードを [Password] フィールドに入力します。

ステップ 7　[OK] をクリックします。

認証または認可のテスト メッセージが ASA からサーバへ送信されます。テストが失敗した場合は、ASDM によりエラー メッセージが表示されます。

RADIUS サーバのモニタリング

RADIUS サーバをモニタするには、次のペインを表示します。

パス	目的
[Monitoring] > [Properties] > [AAA Servers]	設定した RADIUS サーバの統計情報を表示します。
[Monitoring] > [Properties] > [AAA Servers]	RADIUS サーバの実行コンフィギュレーションを表示します。

その他の関連資料

RADIUS サーバを使用した AAA の実装に関する詳細については、「RFC」（P.29-21）を参照してください。

RFC

RFC	タイトル
2138	『*Remote Authentication Dial In User Service (RADIUS)*』
2139	『*RADIUS Accounting*』
2548	『*Microsoft Vendor-specific RADIUS Attributes*』
2868	『*RADIUS Attributes for Tunnel Protocol Support*』

RADIUS サーバの機能履歴

表 29-3 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 29-3　RADIUS サーバの機能履歴

機能名	プラットフォーム リリース	機能情報
AAA の RADIUS サーバ	7.0(1)	AAA 用の RADIUS サーバを設定する方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt]。
ASA からの RADIUS アクセス要求パケットおよび RADIUS アカウンティング要求パケットで送信された主なベンダー固有属性（VSA）	8.4(3)	4 つの新しい VSA：Tunnel Group Name（146）および Client Type（150）は、ASA からの RADIUS アクセス要求パケットで送信されます。Session Type（151）および Session Subtype（152）は、ASA からの RADIUS アカウンティング要求パケットで送信されます。4 つのすべての属性が、すべてのアカウンティング要求パケット タイプ（開始、中間アップデート、および終了）に送信されます。RADIUS サーバ（ACS や ISE など）は、認可属性やポリシー属性を強制適用したり、アカウンティングや課金のためにそれらの属性を使用したりできます。

AAA 用の TACACS+ サーバ

この章では、AAA で使われる TACACS+ サーバの設定方法について説明します。

TACACS+ サーバに関する情報

ASA は、ASCII、PAP、CHAP、MS-CHAPv1 の各プロトコルで TACACS+ サーバ認証をサポートします。

TACACS+ 属性の使用

Cisco ASA は、TACACS+ 属性をサポートします。TACACS+ 属性は、認証、許可、アカウンティングの機能を分離します。プロトコルでは、必須とオプションの 2 種類の属性をサポートします。サーバとクライアントの両方で必須属性を解釈できる必要があり、また、必須属性はユーザに適用する必要があります。オプションの属性は、解釈または使用できることも、できないこともあります。

（注） TACACS+ 属性を使用するには、NAS 上で AAA サービスがイネーブルになっていることを確認してください。

表 30-1 に、カットスルー プロキシ接続に対してサポートされている TACACS+ 認可応答属性の一覧を示します。表 30-2 に、サポートされている TACACS+ アカウンティング属性の一覧を示します。

表 30-1　サポートされる TACACS+ 認可応答属性

属性	説明
acl	接続に適用する、ローカルで設定済みの ACL を識別します。
idletime	認証済みユーザ セッションが終了する前に許可される非アクティブ時間（分）を示します。
timeout	認証済みユーザ セッションが終了する前に認証クレデンシャルがアクティブな状態でいる絶対時間（分）を指定します。

表 30-2　サポートされる TACACS+ アカウンティング属性

属性	説明
bytes_in	この接続中に転送される入力バイト数を指定します（ストップ レコードのみ）。
bytes_out	この接続中に転送される出力バイト数を指定します（ストップ レコードのみ）。
cmd	実行するコマンドを定義します（コマンド アカウンティングのみ）。
disc-cause	切断理由を特定する数字コードを示します（ストップ レコードのみ）。
elapsed_time	接続の経過時間（秒）を定義します（ストップ レコードのみ）。
foreign_ip	トンネル接続のクライアントの IP アドレスを指定します。最下位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。
local_ip	トンネル接続したクライアントの IP アドレスを指定します。最上位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。
NAS port	接続のセッション ID が含まれます。
packs_in	この接続中に転送される入力パケット数を指定します。
packs_out	この接続中に転送される出力パケット数を指定します。
priv-level	コマンド アカウンティング要求の場合はユーザの権限レベル、それ以外の場合は 1 に設定されます。
rem_iddr	クライアントの IP アドレスを示します。
service	使用するサービスを指定します。コマンド アカウンティングの場合にのみ、常に「shell」に設定されます。
task_id	アカウンティング トランザクションに固有のタスク ID を指定します。
username	ユーザの名前を示します。

TACACS+ サーバのライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

その他のガイドライン

- シングル モードで最大 100 個のサーバ グループ、またはマルチ モードでコンテキストごとに 4 つのサーバ グループを持つことができます。
- 各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台のサーバを含めることができます。
- ローカル データベースを使用してフォールバック サポートを設定する必要がある場合は、「フォールバック サポート」（P.28-2）と「グループ内の複数のサーバを使用したフォールバックの仕組み」（P.28-2）を参照してください。
- TACACS+ 認証または許可を使用する場合に ASA からのロック アウトを防止するには、「ロックアウトからの回復」（P.36-29）を参照してください。

TACACS+ サーバの設定

TACACS+ サーバを設定するためのタスク フロー

ステップ 1　TACACS+ サーバ グループを追加します。「TACACS+ サーバ グループの設定」（P.30-4）を参照してください。

ステップ 2　サーバ グループの場合は、グループにサーバを追加します。「グループへの TACACS+ サーバの追加」（P.30-5）を参照してください。

ステップ 3　（オプション）AAA 認証チャレンジ プロセスの実行中にユーザに表示するテキストを指定します。「認証プロンプトの追加」（P.30-5）を参照してください。

TACACS+ サーバ グループの設定

認証、許可、アカウンティングに TACACS+ サーバを使用する場合は、まず TACACS+ サーバ グループを少なくとも 1 つ作成し、各グループに 1 台以上のサーバを追加する必要があります。TACACS+ サーバ グループは名前で識別されます。

TACACS+ サーバ グループを追加するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

ステップ 2　[AAA Server Groups] 領域で、[Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3　[Server Group] フィールドで、グループの名前を入力します。

ステップ 4　[Protocol] ドロップダウン リストから、次のいずれかの TACACS+ サーバ タイプを選択します。

ステップ 5　[Accounting Mode] フィールドで、[Simultaneous] または [Single] をクリックします。

[Single] モードの場合、ASA ではアカウンティング データが 1 つのサーバにだけ送信されます。

[Simultaneous] モードの場合、ASA ではアカウンティング データがグループ内のすべてのサーバに送信されます。

ステップ 6　[Reactivation Mode] フィールドで、[Depletion] または [Timed] をクリックします。

[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。

Timed モードでは、障害が発生したサーバは 30 秒の停止時間の後で再アクティブ化されます。

ステップ 7　[Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

[Dead Time] には、グループ内の最後のサーバがディセーブルになってから、すべてのサーバが再びイネーブルになるまでの時間間隔を分単位で指定します。

ステップ 8　[Max Failed Attempts] フィールドに、許容される試行の失敗回数を指定します。

このオプションで設定するのは、応答のないサーバを非アクティブと宣言するまでに許可される接続試行の失敗回数です。

ステップ 9　[OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバ グループが [AAA Server Groups] テーブルに追加されます。

ステップ 10　[AAA Server Groups] ダイアログボックスの [Apply] をクリックして、変更内容を実行コンフィギュレーションに保存します。

グループへの TACACS+ サーバの追加

TACACS+ サーバをグループに追加するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択し、[AAA Server Groups] 領域で、サーバを追加するサーバ グループをクリックします。

テーブル内の該当する行が選択されます。

ステップ 2　[Selected Group] 領域の [Servers]（下部ペイン）で、[Add] をクリックします。

サーバ グループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3　[Interface Name] ドロップダウン リストから、認証サーバが常駐するインターフェイスの名前を選択します。

ステップ 4　[Server Name] フィールドまたは [IP Address] フィールドに、グループに追加するサーバの名前または IP アドレスを入力します。

ステップ 5　[Timeout] フィールドで、タイムアウト値を入力します。デフォルト値をそのまま使用することもできます。[Timeout] フィールドには、バックアップ サーバへ要求を送信した ASA が、プライマリ サーバからの応答を待機する時間を秒単位で指定します。

ステップ 6　サーバ ポートを指定します。サーバ ポートは、ポート番号 139、または ASA によって TACACS+ サーバとの通信に使用される TCP ポートの番号です。

ステップ 7　サーバ秘密キーを指定します。ASA で TACACS+ サーバを認証する際に使用される共有秘密キーを指定します。ここで設定したサーバ秘密キーは、TACACS+ サーバで設定されたサーバ秘密キーと一致する必要があります。サーバ秘密キーが不明の場合は、TACACS+ サーバの管理者に問い合わせてください。最大フィールド長は、64 文字です。

ステップ 8　[OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、AAA サーバが AAA サーバ グループに追加されます。

ステップ 9　[AAA Server Groups] ペインで [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

認証プロンプトの追加

AAA 認証チャレンジ プロセスの実行中にユーザに表示するテキストを指定できます。TACACS+ サーバからのユーザ認証が必要な場合に、ASA 経由の HTTP、FTP、Telnet アクセス用の AAA チャレンジ テキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワード プロンプトの上に表示されます。

認証プロンプトを指定しない場合、TACACS+ サーバでの認証時にユーザに対して表示される内容は次のようになります。

接続タイプ	デフォルトのプロンプト
FTP	FTP 認証
HTTP	HTTP 認証
Telnet	なし

認証プロンプトを追加するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt] の順に選択します。

ステップ 2　ログイン時にユーザ名とパスワード プロンプトの上に表示するメッセージとして追加するテキストを、[Prompt] フィールドに入力します。

次の表に、認証プロンプトの文字数制限を示します。

アプリケーション	認証プロンプトの文字数制限
Microsoft Internet Explorer	37
Telnet	235
FTP	235

ステップ 3　[Messages] 領域の [User accepted message] フィールドおよび [User rejected message] フィールドにそれぞれメッセージを入力します。

Telnet からのユーザ認証を実行する場合、[User accepted message] オプションおよび [User rejected message] オプションを使用すれば、認証試行が AAA サーバにより受け入れられた、または拒否されたことを示すさまざまな状態のプロンプトを表示できます。

これらのメッセージ テキストをそれぞれ指定した場合、ASA では、AAA サーバにより認証されたユーザに対してはユーザ承認メッセージ テキストが表示され、認証されなかったユーザに対しては ASA によりユーザ拒否メッセージ テキストが表示されます。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジ テキストのみが表示されます。ユーザ承認メッセージ テキストおよびユーザ拒否メッセージ テキストは表示されません。

ステップ 4　[Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

TACACS+ サーバによる認証および許可のテスト

ASA が TACACS+ サーバに接続して、ユーザを認証または承認できるかどうかを決定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] > [AAA Server Groups] テーブルで、サーバが含まれるサーバ グループをクリックします。

テーブル内の該当する行が選択されます。

ステップ 2　[Selected Group] テーブルの [Servers] から、テストするサーバをクリックします。

テーブル内の該当する行が選択されます。

ステップ 3　[Test] をクリックします。

選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 4　実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

ステップ 5　[Username] フィールドにユーザ名を入力します。

ステップ 6　認証をテストする場合は、そのユーザ名に対応するパスワードを [Password] フィールドに入力します。

ステップ 7　[OK] をクリックします。

認証または認可のテスト メッセージが ASA からサーバへ送信されます。テストが失敗した場合は、ASDM によりエラー メッセージが表示されます。

TACACS+ サーバのモニタリング

TACACS+ サーバ を監視するには、次のペインを確認します。

パス	目的
[Monitoring] > [Properties] > [AAA Servers]	設定した TACACS+ サーバの統計情報を表示します。
[Monitoring] > [Properties] > [AAA Servers]	TACACS+ サーバ実行コンフィギュレーションを表示します。

TACACS+ サーバの機能履歴

表 30-3 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 30-3　TACACS+ サーバの機能履歴

機能名	プラットフォーム リリース	機能情報
TACACS+ サーバ	7.0(1)	AAA に TACACS+ サーバを設定する方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt]。

AAA の LDAP サーバ

この章では、AAA で使用される LDAP サーバの設定方法について説明します。

LDAP および ASA に関する情報

Cisco ASA はほとんどの LDAPv3 ディレクトリ サーバと互換性があり、それには次のものが含まれます。

- Sun Microsystems JAVA System Directory Server（現在は Oracle Directory Server Enterprise Edition の一部、旧名 Sun ONE Directory Server）
- Microsoft Active Directory
- Novell
- OpenLDAP

デフォルトでは、ASA によって Microsoft Active Directory、Sun LDAP、Novell、OpenLDAP、または汎用 LDAPv3 ディレクトリ サーバに接続しているかどうかが自動検出されます。ただし、LDAP サーバ タイプの自動検出による決定が失敗した場合は、手動で設定できます。

LDAP サーバ ガイドライン

LDAP サーバを設定する場合、次の点に注意してください。

- Sun ディレクトリ サーバにアクセスするように ASA で設定されている DN は、そのサーバのデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACL を設定できます。

- Microsoft Active Directory および Sun サーバでのパスワード管理をイネーブルにするために LDAP over SSL を設定する必要があります。
- ASA では、Novell、OpenLDAP、およびその他の LDAPv3 ディレクトリ サーバを使用したパスワード管理はサポートされません。
- VPN 3000 コンセントレータと ASA/PIX 7.0 ソフトウェアでは、認証作業に Cisco LDAP スキーマが必要でした。バージョン 7.1.x 以降では、ASA は、ネイティブ LDAP スキーマを使用して認証および認可を行うため、Cisco スキーマは必要なくなりました。

LDAP での認証方法

認証中、ASA は、ユーザの LDAP サーバへのクライアント プロキシとして機能し、プレーンテキストまたは Simple Authentication and Security Layer（SASL）プロトコルのいずれかを使って LDAP サーバに対する認証を行います。デフォルトで、ASA は、通常はユーザ名とパスワードである認証パラメータを LDAP サーバにプレーン テキストで渡します。

ASA では、次の SASL メカニズムをサポートしています。次に、強度の低い順番に示します。

- Digest-MD5：ASA は、ユーザ名とパスワードから計算した MD5 値を使用して LDAP サーバに応答します。
- Kerberos：ASA は、GSSAPI Kerberos メカニズムを使用して、ユーザ名とレルムを送信することで LDAP サーバに応答します。

ASA と LDAP サーバは、これらの SASL メカニズムの任意の組み合わせをサポートします。複数のメカニズムを設定した場合、ASA ではサーバに設定されている SASL メカニズムのリストが取得され、認証メカニズムは ASA とサーバの両方に設定されているメカニズムのなかで最も強力なものに設定されます。たとえば、LDAP サーバと ASA の両方がこれら両方のメカニズムをサポートしている場合、ASA は、強力な方の Kerberos メカニズムを選択します。

ユーザ LDAP 認証が成功すると、LDAP サーバは認証されたユーザの属性を返します。VPN 認証の場合、通常これらの属性には、VPN セッションに適用される認可データが含まれます。この場合、LDAP の使用により、認証と許可を 1 ステップで実行できます。

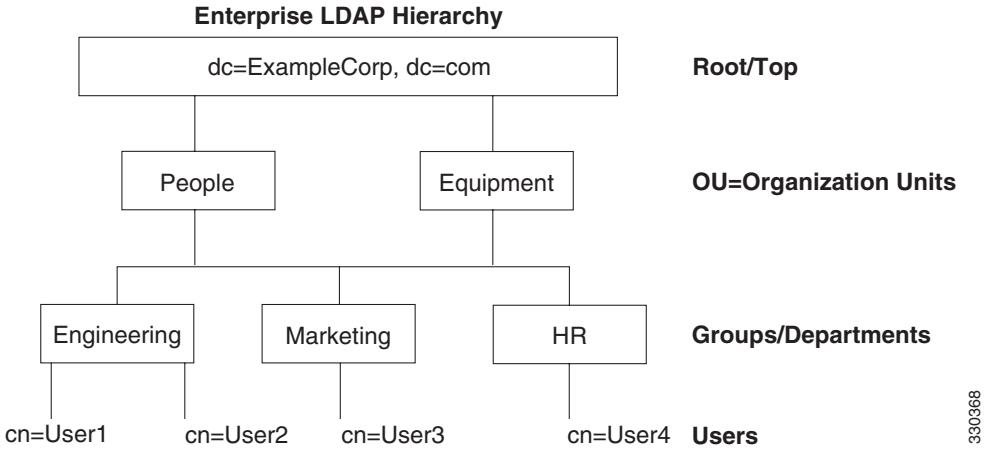
（注）　LDAP プロトコルの詳細については、RFC 1777、2251、および 2849 を参照してください。

LDAP の階層について

LDAP コンフィギュレーションは、組織の論理階層が反映されたものにする必要があります。たとえば、Example Corporation という企業の従業員 Employee1 を例に考えてみます。Employee1 は Engineering グループに従事しています。この企業の LDAP 階層は 1 つ以上のレベルを持つことができます。たとえば、シングルレベル階層をセットアップします。この中で、Employee1 は Example Corporation のメンバーであると見なされます。あるいは、マルチレベル階層をセットアップします。この中で、Employee1 は Engineering 部門のメンバーであると見なされ、この部門は People という名称の組織ユニットのメンバーであり、この組織ユニットは Example Corporation のメンバーです。マルチレベル階層の例については、図 31-1 を参照してください。

マルチレベル階層の方が詳細ですが、検索結果が速く返されるのはシングルレベル階層の方です。

図 31-1　マルチレベルの LDAP 階層



LDAP 階層の検索

ASA では、LDAP 階層内での検索を調整できます。ASA に次の 3 種類のフィールドを設定すると、LDAP 階層での検索開始場所とその範囲、および検索する情報のタイプを定義できます。これらのフィールドは、ユーザの権限が含まれている部分だけを検索するように階層の検索を限定します。

- LDAP Base DN では、サーバが ASA から認可要求を受信したときに LDAP 階層内のどの場所からユーザ情報の検索を開始するかを定義します。
- Search Scope では、LDAP 階層の検索範囲を定義します。この指定では、LDAP Base DN よりもかなり下位のレベルまで検索します。サーバによる検索を直下の 1 レベルだけにするか、サブツリー全体を検索するかを選択できます。シングルレベルの検索の方が高速ですが、サブツリー検索の方が広範囲に検索できます。
- Naming Attribute では、LDAP サーバのエントリを一意に識別する RDN を定義します。一般的な名前属性には、cn（一般名）、sAMAccountName、および userPrincipalName を含めることができます。

図 31-1 に、Example Corporation の LDAP 階層の例を示します。この階層が指定されると、複数の方法で検索を定義できます。表 31-1 に、2 つの検索コンフィギュレーションの例を示します。

最初のコンフィギュレーションの例では、Employee1 が IPSec トンネルを確立するときに LDAP 認可が必要であるため、ASA から LDAP サーバに検索要求が送信され、この中で Employee1 を Engineering グループの中で検索することが指定されます。この検索は短時間でできます。

2 番目のコンフィギュレーションの例では、ASA から送信される検索要求の中で、Employee1 を Example Corporation 全体の中で検索することが指定されています。この検索には時間がかかります。

表 31-1　検索コンフィギュレーションの例

番号	LDAP Base DN	検索範囲	名前属性	結果
1	group= Engineering,ou=People,dc=ExampleCorporation, dc=com	1 レベル	cn=Employee1	検索が高速
2	dc=ExampleCorporation,dc=com	サブツリー	cn=Employee1	検索に時間がかかる

LDAP サーバへのバインディングについて

ASA は、ログイン DN とログイン パスワードを使用して、LDAP サーバとの信頼（バインド）を築きます。Microsoft Active Directory の読み取り専用操作（認証、許可、グループ検索など）を行うとき、ASA では特権の低いログイン DN でバインドできます。たとえば、Login DN には、AD の「Member Of」の指定が Domain Users の一部であるユーザを指定することができます。VPN のパスワード管理操作では、Login DN にはより高い特権が必要となり、AD の Account Operators グループの一部を指定する必要があります。

次に、Login DN の例を示します。

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

ASA は次の認証方式をサポートしています。

- 暗号化されていないパスワードを使用したポート 389 での簡易 LDAP 認証
- ポート 636 でのセキュアな LDAP（LDAP-S）
- Simple Authentication and Security Layer（SASL）MD5
- SASL Kerberos

ASA は匿名認証をサポートしていません。

（注）　LDAP クライアントとしての ASA は、匿名のバインドや要求の送信をサポートしていません。

LDAP サーバのライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

LDAP サーバの設定

LDAP サーバを設定するためのタスク フロー

ステップ 1　LDAP サーバ グループを追加します。「LDAP サーバ グループの設定」（P.31-7）を参照してください。

ステップ 2　サーバをグループに追加し、サーバ パラメータを設定します。「LDAP サーバのグループへの追加　」（P.31-8）を参照してください。

ステップ 3　LDAP 属性マップを設定します。「LDAP 属性マップの設定」（P.31-5）を参照してください。LDAP サーバを LDAP サーバ グループに追加する前に、属性マップを追加する必要があります。

LDAP 属性マップの設定

ASA では、次の目的での認証のために LDAP ディレクトリを使用できます。

- VPN リモート アクセス ユーザ
- ファイアウォール ネットワークのアクセス/カットスルー プロキシ セッション
- ACL、ブックマーク リスト、DNS または WINS 設定、セッション タイマーなどのポリシーの権限（または許可属性と呼ばれる）の設定
- ローカル グループ ポリシーのキー属性の設定

ASA は、LDAP 属性マップを使用して、ネイティブ LDAP ユーザ属性を Cisco ASA 属性に変換します。それらの属性マップを LDAP サーバにバインドしたり、削除したりすることができます。また、属性マップを表示または消去することもできます。

ガイドライン

LDAP 属性マップは複数値属性をサポートしません。たとえば、あるユーザが複数の AD グループのメンバで、LDAP 属性マップが複数のグループと一致する場合、選択される値は一致するエントリのアルファベット順に基づくものです。

属性マッピング機能を適切に使用するには、LDAP 属性の名前と値およびユーザ定義の属性の名前と値を理解する必要があります。

頻繁にマッピングされる LDAP 属性の名前と、一般にマッピングされるユーザ定義の属性のタイプは次のとおりです。

- IETF-Radius-Class（ASA バージョン 8.2 以降における Group_Policy）：ディレクトリ部門またはユーザ グループ（たとえば、Microsoft Active Directory memberOf）属性値に基づいてグループ ポリシーを設定します。ASDM バージョン 6.2/ASA バージョン 8.2 以降では、IETF-Radius-Class 属性の代わりに group-policy 属性が使用されます。

- IETF-Radius-Filter-Id：VPN クライアント、IPSec、SSL に対するアクセス コントロール リスト（ACL）に適用されます。
- IETF-Radius-Framed-IP-Address：VPN リモート アクセス クライアント、IPSec、および SSL にスタティック IP アドレスを割り当てます。
- Banner1：VPN リモート アクセス ユーザのログイン時にテキスト バナーを表示します。
- Tunneling-Protocols：アクセス タイプに基づいて、VPN リモート アクセス セッションを許可または拒否します。

（注） 1 つの LDAP 属性マップに、1 つ以上の属性を含めることができます。特定の LADP サーバからは、1 つの LDAP 属性のみをマップすることができます。

LDAP 機能をマップするには、次の手順を実行します。

手順の詳細

ステップ 1 ローカル ユーザの場合は [Configuration] > [Remote Access VPN] > [AAA Local Users] > [LDAP Attribute Map] の順に、その他の全ユーザの場合は [Configuration] > [Device Management] > [Users/AAA] > [LDAP Attribute Map] の順に選択して、[Add] をクリックします。

[Map Name] タブが表示された状態で [Add LDAP Attribute Map] ダイアログボックスが開きます。

ステップ 2 [Name] フィールドに、この属性マップの名前を作成します。

ステップ 3 [LDAP Attribute Name] フィールドに、マッピングする LDAP 属性の名前を入力します。

ステップ 4 [Cisco Attribute Name] ドロップダウン リストから、Cisco 属性を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 属性がマップされます。さらに属性をマップする場合は、ステップ 1 ～ 5 を繰り返します。

ステップ 7 マップされている Cisco 属性の新しい値に LDAP 属性の値をマップする場合は、[Map Value] タブをクリックします。

ステップ 8 [Add] をクリックします。

[Add Mapping of Attribute Name] ダイアログボックスが表示されます。

ステップ 9 ドロップダウン リストから LDAP 属性を選択します。

ステップ 10 [LDAP Attribute Value] フィールドに、LDAP サーバから返されると予想されるこの LDAP 属性の値を入力します。

ステップ 11 [Cisco Attribute Value] フィールドに、この LDAP 属性が以前の LDAP 属性値を含める場合に、Cisco 属性で使用する値を入力します。

ステップ 12 [Add] をクリックします。

値がマップされます。

ステップ 13 さらに値をマップする場合は、ステップ 8 ～ 12 を繰り返します。

ステップ 14 [OK] をクリックして [Map Value] タブに戻り、再度 [OK] をクリックしてダイアログボックスを閉じます。

ステップ 15 [LDAP Attribute Map] ペインで [Apply] をクリックして、実行コンフィギュレーションにマップする値を保存します。

LDAP サーバ グループの設定

認証、許可、アカウンティングに外部 LDAP サーバを使用する場合は、まず少なくとも 1 つの LDAP サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。LDAP サーバ グループは名前で識別されます。各サーバ グループは、各サーバ タイプによって異なります。

ガイドライン

- シングルモードの場合は最大 100 台の LDAP サーバ グループを使用でき、マルチモードの場合は各コンテキストで最大 4 台の LDAP サーバ グループを使用できます。
- 各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台の LDAP サーバを含めることができます。
- ユーザがログインすると、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまで LDAP サーバが 1 つずつアクセスされます。グループ内のすべてのサーバが使用できない場合、ASA は、ローカル データベースがフォールバック方式として設定されていると、ローカル データベースに接続しようとします（管理認証および認可限定）。フォールバック方式として設定されていない場合、ASA は引き続き LDAP サーバにアクセスしようとします。

手順の詳細

次に、LDAP サーバ グループを作成し、このグループに LDAP サーバを追加する方法を示します。

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups]、または VPN ユーザの場合は [Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups] の順に選択します。

ステップ 2　[AAA Server Groups] 領域で、[Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3　[AAA Server Group] フィールドで、この AAA サーバ グループの名前を指定します。

ステップ 4　[Protocol] ドロップダウン リストから、LDAP サーバのタイプを選択します。

ステップ 5　[Reactivation Mode] フィールドで、目的のモードに対応するオプション ボタン（[Depletion] または [Timed]）をクリックします。

[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。

Timed モードでは、障害が発生したサーバは 30 秒の停止時間の後で再アクティブ化されます。

a.　[Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

[Dead Time] には、グループ内の最後のサーバがディセーブルになってから、すべてのサーバが再びイネーブルになるまでの時間間隔を分単位で指定します。

ステップ 6　[Max Failed Attempts] フィールドに、サーバに接続するための試行の許容失敗回数を指定します。

このオプションで設定するのは、応答のないサーバを非アクティブと宣言するまでに許可される接続試行の失敗回数です。

ステップ 7　[OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバ グループが [AAA Server Groups] テーブルに追加されます。

ステップ 8　変更内容を保存する場合は、[AAA Server Groups] ダイアログボックスで、[Apply] をクリックします。

変更内容が実行コンフィギュレーションに保存されます。

LDAP サーバのグループへの追加

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups]、または VPN ユーザの場合は [Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups] の順に選択し、[AAA Server Groups] 領域で、サーバを追加するサーバ グループを選択します。

ステップ 2　選択されたグループのサーバ リストの横にある [Add] をクリックします。

サーバ グループに対応する [Add AAA Server] ダイアログボックスが表示されます。

ステップ 3　[Interface Name] ドロップダウン リストから、LDAP サーバに接続するインターフェイスの名前を選択します。

ステップ 4　[Server Name or IP Address] フィールドに、LDAP サーバのサーバ名または IP アドレスを追加します。

ステップ 5　[Timeout] フィールドで、タイムアウト値を入力します。デフォルト値をそのまま使用することもできます。[Timeout] フィールドには、バックアップ サーバへ要求を送信した ASA が、プライマリ サーバからの応答を待機する時間を秒単位で指定します。

ステップ 6　認証および承認の領域の LDAP パラメータで、次のフィールドを設定します。

- [Enable LDAP over SSL]（セキュア LDAP または LDAP-S とも呼ばれる）：ASA と LDAP サーバの間のセキュアな通信に SSL を使用する場合にオンにします。

（注）　SASL プロトコルを設定しない場合は、SSL を使用して LDAP 通信のセキュリティを確保することを強く推奨します。

- [Server Port]：ASA から LDAP サーバへアクセスする際、単純認証（セキュアでない認証）に使用される TCP ポート番号 389 またはセキュアな認証（LDAP-S）に使用される TCP ポート番号 636 を指定します。LDAP サーバはすべて、認証および認可をサポートしています。Microsoft AD サーバおよび Sun LDAP サーバに限っては、さらに、LDAP-S を必要とする VPN リモート アクセス パスワード管理機能もサポートしています。
- [Server Type]：ドロップダウン リストから LDAP サーバ タイプを指定します。使用できるオプションは、次のとおりです。
  - Detect Automatically/Use Generic Type
  - Microsoft
  - Novell
  - OpenLDAP
  - Sun（現在では Oracle Directory Server Enterprise Edition の一部）

- [Base DN]：ベース識別名、または LDAP 要求を受け取ったサーバで検索が開始される LDAP 階層内の位置を指定します（例：OU=people, dc=cisco, dc=com）。
- [Scope]：ドロップダウン リストからの認証要求を受信する場合に、LDAP 階層内でサーバの実行が必要な検索範囲を指定します。次のオプションを使用できます。
  - [One Level]：ベース DN の 1 レベル下だけを検索します。このオプションを選択すると、検索の実行時間が短縮されます。
  - [All Levels]：ベース DN の下にあるすべてのレベル（つまりサブツリー階層全体）が検索対象となります。このオプションを選択すると、検索の実行に時間がかかります。
- [Naming Attribute（s）]：LDAP サーバのエントリを一意に識別する Relative Distinguished Name 属性を入力します。共通の名前付き属性は、Common Name（CN）、sAMAccountName、userPrincipalName、および User ID（uid）です。
- [Login DN and Login Password]：ASA は、LDAP サーバとの信頼（バインド）を確立するために、ログイン DN とログイン パスワードを使用します。ログイン DN のユーザ アカウントのパスワードをログイン パスワードとして指定します。入力した文字はアスタリスクに置き換えられます。
- [LDAP Attribute Map]：この LDAP サーバで使用するために作成された属性マップの 1 つを選択します。これらの属性マップは、LDAP 属性名をシスコの属性名と値にマップします。
- [SASL MD5 authentication]：ASA と LDAP サーバの間の通信を認証するための SASL の MD5 メカニズムをイネーブルにします。
- [SASL Kerberos authentication]：ASA と LDAP サーバの間のセキュアな認証通信のための SASL の Kerberos メカニズムをイネーブルにします。このオプションを有効にするためには、Kerberos サーバを定義しておく必要があります。
- [LDAP Parameters for Group Search]：この領域のフィールドは、ASA が AD グループを要求する方法を設定します。
  - [Group Base DN]：この DN により、LDAP 階層内で AD グループ（つまり、memberOf 列挙のリスト）の検索を開始する位置が指定されます。このフィールドの設定を行わない場合、ASA では、AD グループの取得にベース DN が使用されます。ASDM では、取得した AD グループのリストに基づいて、ダイナミック アクセス ポリシーの AAA 選択基準が定義されます。詳細については、「**show ad-groups** コマンド」を参照してください。
  - [Group Search Timeout] : 使用できるグループについてのクエリーに対して AD サーバから応答があるまでの最長待機時間を指定します。

ステップ 7　[OK] をクリックします。

[Add AAA Server] ダイアログボックスが閉じ、AAA サーバが AAA サーバ グループに追加されます。

ステップ 8　[AAA Server Groups] ペインで [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

LDAP サーバによる認証および許可のテスト

ASA において LDAP サーバへのアクセスやユーザの認証および許可が実行できるかどうかを判定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] ペインで、サーバが常駐するサーバ グループを選択します。

ステップ 2　[Selected Group] 領域の [Servers] から、テストするサーバをクリックします。

ステップ 3　[Test] をクリックします。

選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 4　実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

ステップ 5　ユーザ名を入力します。

ステップ 6　認証をテストする場合は、ユーザ名のパスワードを入力します。

ステップ 7　[OK] をクリックします。

認証または許可のテスト メッセージが ASA からサーバへ送信されます。テストが失敗した場合は、ASDM によりエラー メッセージが表示されます。

LDAP サーバのモニタリング

LDAP サーバを監視するには、次の手順を実行します。

ステップ 1　ASDM で、[Monitoring] > [Properties] > [AAA Servers] を選択します。

ステップ 2　LDAP サーバの状態を更新するには、[Update Server Statistics] でクリックして選択します。

ドロップダウン リストで選択された LDAP サーバを含む [Update AAA Server Status] ダイアログボックスが表示されます。

ステップ 3　[OK] をクリックします。

ステップ 4　現在表示されている統計情報を更新するには、[Clear Server Statistics] をクリックします。

LDAP サーバの機能履歴

表 31-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 31-2　AAA サーバの機能履歴

機能名	プラットフォーム リリース	機能情報
AAA の LDAP サーバ	7.0(1)	LDAP サーバの AAA のサポートと LDAP サーバの設定方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Remote Access VPN] > [AAA Local Users] > [LDAP Attribute Map]

アイデンティティ ファイアウォール

この章では、アイデンティティ ファイアウォール向けに ASA を設定する方法について説明します。

アイデンティティ ファイアウォールに関する情報

アイデンティティ ファイアウォールの概要

企業では、ユーザが 1 つ以上のサーバ リソースにアクセスする必要が生じることがよくあります。通常、ファイアウォールではユーザのアイデンティティは認識されないため、アイデンティティに基づいてセキュリティ ポリシーを適用することはできません。ユーザごとにアクセス ポリシーを設定するには、ユーザ認証プロキシを設定する必要があります。これには、ユーザとの対話（ユーザ名とパスワードのクエリー）が必要です。

ASA のアイデンティティ ファイアウォールでは、ユーザのアイデンティティに基づいたより細かなアクセス コントロールが実現されます。送信元 IP アドレスではなくユーザ名とユーザグループ名に基づいてアクセス ルールとセキュリティ ポリシーを設定できます。ASA は、IP アドレスと Windows Active Directory のログイン情報の関連付けに基づいてセキュリティ ポリシーを適用し、ネットワーク IP アドレスではなくマッピングされたユーザ名を使用してイベントを報告します。

アイデンティティ ファイアウォールは、実際のアイデンティティ マッピングを提供する外部 Active Directory（AD）エージェントと連携する Microsoft Active Directory と統合されます。ASA では、Windows Active Directory を送信元として使用して特定の IP アドレスについて現在のユーザのアイデンティティ情報を取得し、Active Directory ユーザにトランスペアレント認証を許可します。

アイデンティティに基づくファイアウォール サービスは、送信元 IP アドレスの代わりにユーザまたはグループを指定できるようにすることにより、既存のアクセス コントロールおよびセキュリティ ポリシー メカニズムを拡張します。アイデンティティに基づくセキュリティ ポリシーは、従来の IP アドレス ベースのルール間の制約を受けることなくインターリーブできます。

アイデンティティ ファイアウォールの主な利点には、次のようなものがあります。

- セキュリティ ポリシーからのネットワーク トポロジの分離
- セキュリティ ポリシー作成の簡略化
- ネットワーク リソースに対するユーザ アクティビティを容易に検出可能
- ユーザ アクティビティ モニタリングの効率化

アイデンティティ ファイアウォールの展開アーキテクチャ

アイデンティティ ファイアウォールは、実際のアイデンティティ マッピングを提供する外部 Active Directory（AD）エージェントとの連携により、Microsoft Active Directory と統合されます。

アイデンティティ ファイアウォールは、次の 3 つのコンポーネントにより構成されます。

- ASA
- Microsoft Active Directory

  Active Directory は ASA のアイデンティティ ファイアウォールの一部ですが、管理は Active Directory の管理者が行います。データの信頼性と正確さは、Active Directory のデータによって決まります。

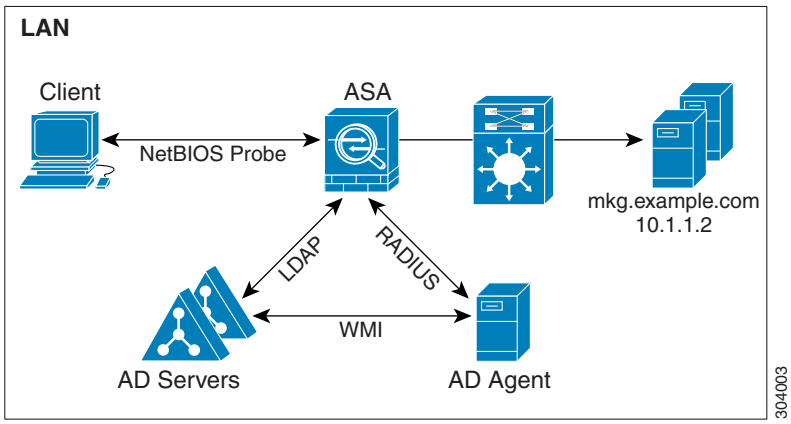
  サポートされているバージョンは、Windows 2003、Windows Server 2008、および Windows Server 2008 R2 サーバです。
- Active Directory（AD）エージェント

  AD エージェントは Windows サーバ上で実行されます。サポートされる Windows サーバは、Windows 2003、Windows 2008、および Windows 2008 R2 です。

（注） Windows 2003 R2 は、AD エージェント サーバとしてはサポートされていません。

図 32-1 は、アイデンティティ ファイアウォールのコンポーネントを示しています。次の表は、これらのコンポーネントのロールと相互に通信する方法を示しています。

図 32-1　　アイデンティティ ファイアウォールのコンポーネント



1	**ASA上**：管理者がローカル ユーザ グループとアイデンティティ ファイアウォール ポリシーを設定します。	4	**クライアント <-> ASA**：クライアントは Microsoft Active Directory を介してネットワークにログオンします。AD サーバは、ユーザを認証し、ユーザ ログイン セキュリティ ログを生成します。 または、クライアントはカットスルー プロキシまたは VPN 経由でネットワークにログオンすることもできます。
2	**ASA <-> AD サーバ**：ASA は、AD サーバに設定された Active Directory グループに対する LDAP クエリーを送信します。 ASA がローカル グループと Active Directory グループを統合し、ユーザ アイデンティティに基づくアクセス ルールおよびモジュラー ポリシー フレームワーク セキュリティ ポリシーを適用します。	5	**ASA <-> クライアント**：ASA は設定されているポリシーに基づいて、クライアントにアクセスを許可または拒否します。 設定されている場合、ASA ではクライアントの NetBIOS をプローブして、非アクティブなユーザおよび応答がないユーザを渡します。
3	**ASA <-> AD エージェント**：アイデンティティ ファイアウォールの設定に応じて、ASA は IP とユーザのデータベースをダウンロードするか、ユーザの IP アドレスをたずねる AD エージェントに RADIUS 要求を送信します。 ASA は、AD エージェントに対する Web 認証および VPN セッションから学習した新しいマッピング エントリを転送します。	6	**AD エージェント <-> AD サーバ**：AD エージェントは、ユーザ ID と IP アドレスのマッピング エントリのキャッシュを維持します。マッピングに変更があった場合は ASA に通知します。 AD エージェントは syslog サーバにログを送信します。

アイデンティティ ファイアウォールの機能

アイデンティティ ファイアウォールの主な機能は次のとおりです。

柔軟性

- ASA は、新しい IP アドレスごとに AD エージェントにクエリーを実行するか、ユーザ アイデンティティおよび IP アドレスのデータベース全体のローカル コピーを保持することにより、AD エージェントからユーザ アイデンティティと IP アドレスのマッピングを取得できます。

- ユーザ アイデンティティ ポリシーの送信先として、ホスト グループ、サブネット、または IP アドレスをサポートします。
- ユーザ アイデンティティ ポリシーの送信元および送信先として、Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）をサポートします。
- 5 タプル ポリシーと ID ベースのポリシーの組み合わせをサポートします。アイデンティティ ベースの機能は、既存の 5 タプル ソリューションと連携して動作します。
- IPS およびアプリケーション インスペクションの使用をサポートします。
- リモート アクセス VPN、AnyConnect VPN、L2TP VPN、およびカットスルー プロキシからユーザのアイデンティティ情報を取得します。取得されたすべてのユーザが、AD エージェントに接続しているすべての ASA に読み込まれます。

拡張性

- 各 AD エージェントは 100 台の ASA をサポートします。複数の ASA が 1 つの AD エージェントと通信できるため、より大規模なネットワーク展開での拡張性が提供されます。
- すべてのドメインが固有の IP アドレスを持つ場合に、30 台の Active Directory サーバをサポートします。
- ドメイン内の各ユーザ アイデンティティには、最大で 8 個の IP アドレスを含めることができます。
- ASA 5500 シリーズ モデルのアクティブなポリシーでサポートされるユーザ アイデンティティと IP アドレスのマッピング エントリは、最大 64,000 個です。この制限により、ポリシーが適用されるユーザの最大数が決まります。すべてのコンテキストに設定された全ユーザを集約したものが、ユーザ総数です。
- アクティブな ASA ポリシーでサポートされるユーザ グループは、最大 256 個です。
- 1 つのアクセス ルールに 1 つ以上のユーザ グループまたはユーザを含めることができます。
- 複数のドメインをサポートします。

アベイラビリティ

- ASA は、Active Directory からグループ情報を取得し、AD エージェントが送信元 IP アドレスをユーザ アイデンティティにマッピングできない場合に IP アドレスの Web 認証にフォールバックします。
- AD エージェントは、いずれかの Active Directory サーバまたは ASA が応答しない場合でも機能し続けます。
- ASA でのプライマリ AD エージェントとセカンダリ AD エージェントの設定をサポートします。プライマリ AD エージェントが応答を停止すると、ASA がセカンダリ AD エージェントに切り替えます。
- AD エージェントが使用できない場合、ASA はカットスルー プロキシや VPN 認証などの既存のアイデンティティ取得元にフォールバックできます。
- AD エージェントは、ダウンしたサービスを自動的に再開するウォッチドッグ プロセスを実行します。
- ASA 内で使用する分散 IP アドレス/ユーザ マッピング データベースを許可します。

展開シナリオ

環境要件に応じた次の方法で、アイデンティティ ファイアウォールのコンポーネントを展開できます。

図 32-2 は、冗長性のためのアイデンティティ ファイアウォールのコンポーネントの展開方法を示しています。シナリオ 1 は、コンポーネントの冗長性がない単純なインストールを示しています。シナリオ 2 も、冗長性がない単純なインストールを示しています。ただし、この展開シナリオでは、Active Directory サーバと AD エージェントが同一の Windows サーバに共存しています。

図 32-2　冗長性のない展開シナリオ

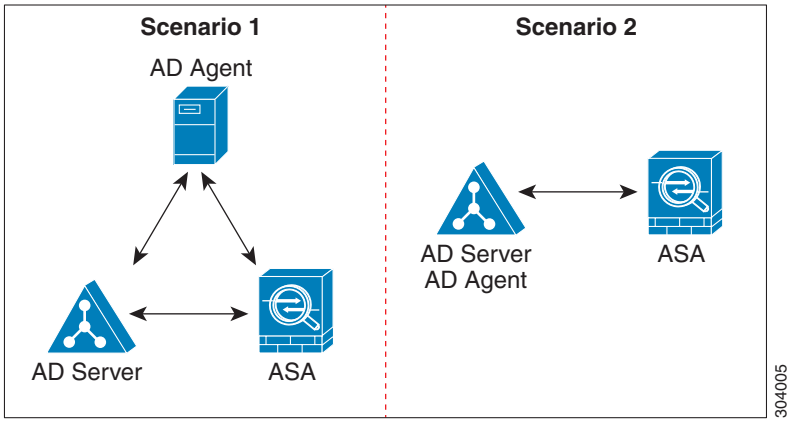


図 32-3 は、冗長性をサポートするためのアイデンティティ ファイアウォールのコンポーネントの展開方法を示しています。シナリオ 1 では、複数の Active Directory サーバと、AD エージェントをインストールした 1 台の Windows サーバを配置しています。シナリオ 2 では、複数の Active Directory サーバと、それぞれ AD エージェントがインストールされた複数の Windows サーバを配置しています。

図 32-3　冗長コンポーネントのある展開シナリオ

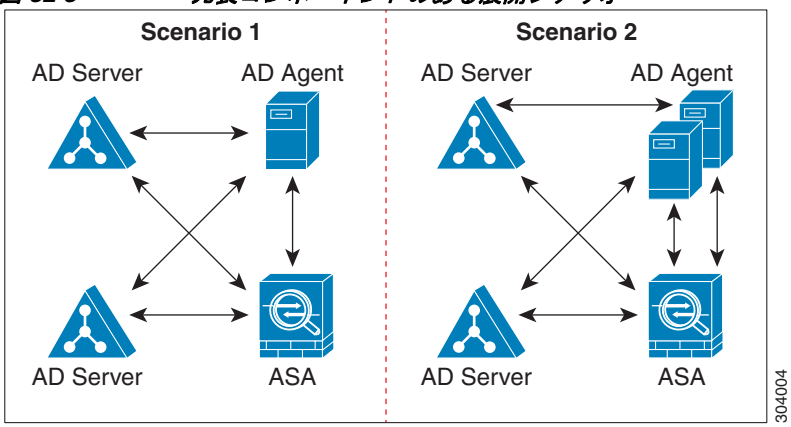


図 32-4 は、LAN 上にすべてのアイデンティティ ファイアウォール コンポーネント（Active Directory サーバ、AD エージェント、クライアント）がインストールされ通信する方法を示しています。

図 32-4　LAN ベースの展開

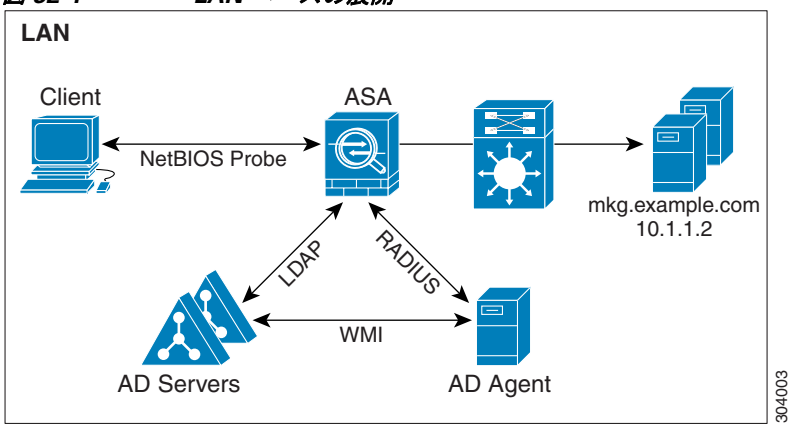


図 32-5 は、WAN を使用してリモート サイトと接続した展開方法を示しています。Active Directory サーバと AD エージェントはメイン サイトの LAN 上に配置されています。クライアントはリモート サイトに配置されており、WAN 経由でアイデンティティ ファイアウォール コンポーネントに接続しています。

図 32-5　WAN ベースの展開

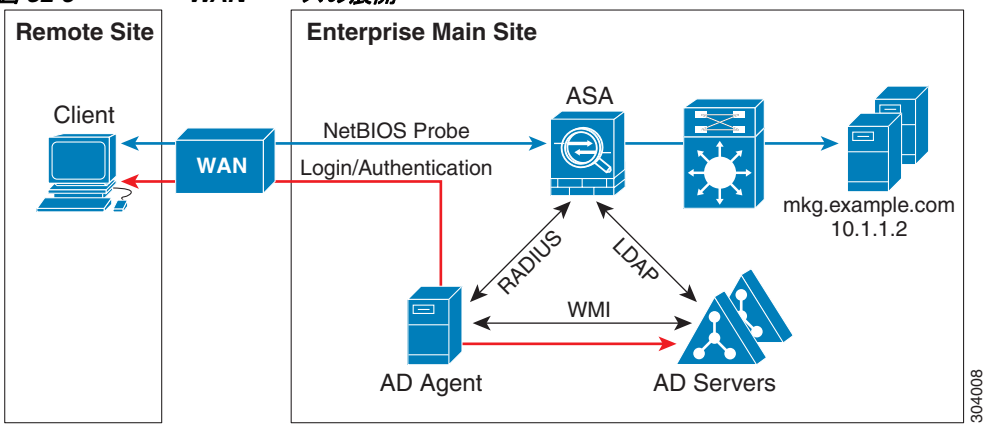


図 32-6 も WAN を使用したリモート サイトにまたがる展開方法を示しています。Active Directory サーバはメイン サイトの LAN にインストールされています。一方、AD エージェントはリモート サイトに配置され、同じサイト内のクライアントからアクセスされます。リモート クライアントは、WAN 経由でメイン サイトの Active Directory サーバに接続します。

図 32-6　リモート AD エージェントを使用した WAN ベースの展開

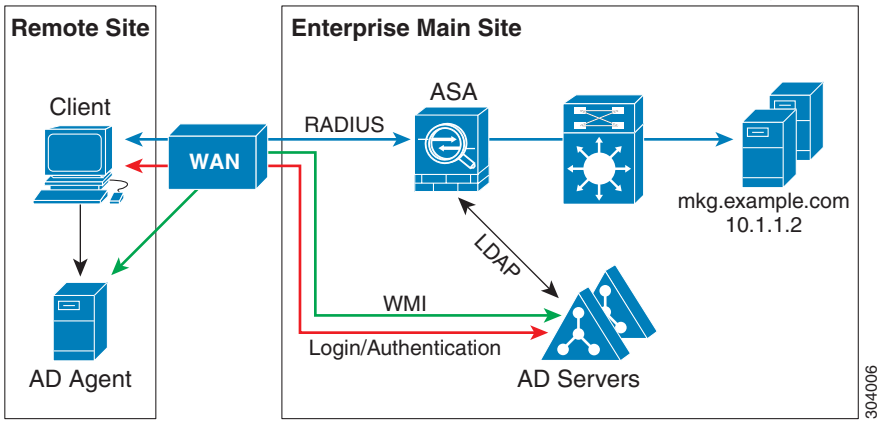
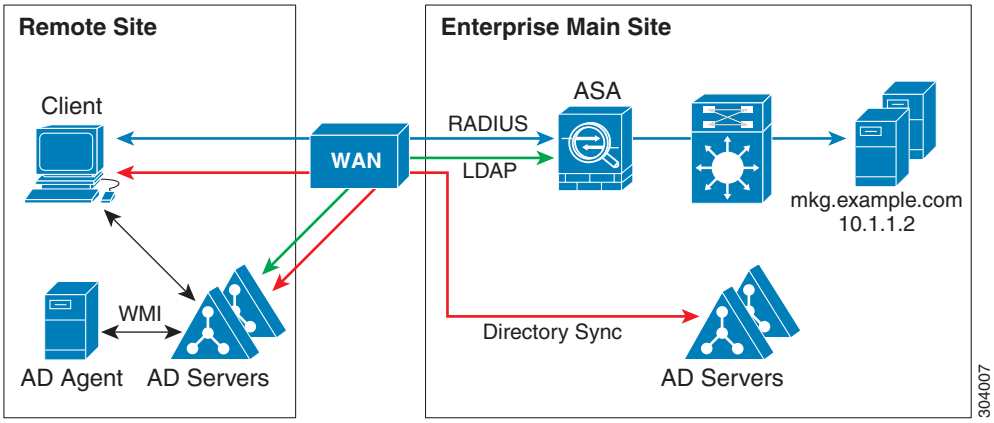


図 32-7 は、リモート サイトを拡張した WAN ベースの展開を示しています。AD エージェントと Active Directory サーバがリモート サイトに配置されています。クライアントは、メイン サイトに配置されているネットワーク リソースにログインする際に、これらのコンポーネントにローカルでアクセスします。リモート Active Directory サーバは、メイン サイトに配置された Active Directory サーバとの間でデータを同期する必要があります。

図 32-7　AD エージェントと AD サーバをリモート サイトに配置した WAN ベースの展開



アイデンティティ ファイアウォールのライセンス

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

フェールオーバーのガイドライン

- アイデンティティ ファイアウォールは、ステートフル フェールオーバーがイネーブルになっている場合、ユーザ アイデンティティと IP アドレスのマッピングおよび AD エージェント ステータスのアクティブからスタンバイへの複製をサポートします。ただし、複製されるのは、ユーザ アイデンティティと IP アドレスのマッピング、AD エージェント ステータス、およびドメイン ステータスだけです。ユーザおよびユーザ グループのレコードはスタンバイ ASA に複製されません。
- フェールオーバーを設定するときには、スタンバイ ASA についても、AD エージェントに直接接続してユーザ グループを取得するように設定する必要があります。スタンバイ ASA は、アイデンティティ ファイアウォールに NetBIOS プローブ オプションが設定されていても、クライアントに NetBIOS パケットを送信しません。
- クライアントが非アクティブであるとアクティブ ASA が判断した場合、情報はスタンバイ ASA に伝搬されます。ユーザ統計情報はスタンバイ ASA に伝搬されません。
- フェールオーバーを設定した場合は、AD エージェントをアクティブとスタンバイの両方の ASA と通信するように設定する必要があります。AD エージェント サーバで ASA を設定する手順については、『*Installation and Setup Guide for the Active Directory Agent*』を参照してください。

IPv6 のガイドライン

- IPv6 をサポートします。
- AD エージェントは IPv6 アドレスのエンドポイントをサポートします。AD エージェントは、ログ イベントで IPv6 アドレスを受け取り、それをキャッシュに保存し、RADIUS メッセージによって送信します。
- IPv6 上の NetBIOS はサポートされていません。

その他のガイドラインと制限事項

- 宛先アドレスとしての完全な URL の使用はサポートされていません。
- NetBIOS プローブが機能するためには、ASA、AD エージェント、およびクライアントを接続するネットワークが UDP でカプセル化された NetBIOS トラフィックをサポートしている必要があります。
- アイデンティティ ファイアウォールによる MAC アドレスのチェックは、仲介ルータがある場合は機能しません。同じルータの背後にあるクライアントにログオンしたユーザには、同じ MAC アドレスが割り当てられます。この実装では、ASA がルータの背後の実際の MAC アドレスを特定できないため、同じルータからのパケットはすべてチェックに合格します。

- 次の ASA 機能は、拡張 ACL でのアイデンティティに基づくオブジェクトおよび FQDN の使用をサポートしません。
  - ルート マップ
  - クリプト マップ
  - WCCP
  - NAT
  - グループ ポリシー（VPN フィルタを除く）
  - DAP
- **user-identity update active-user-database** コマンドを使用して、実行中に AD エージェントからのユーザ IP アドレスのダウンロードを開始できます。

  設計的に、前のダウンロード セッションが終了すると、ASA はこのコマンドを再度発行することを許しません。

  その結果、ユーザ IP データベースが非常に大きく、前のセッションが終了していない場合に、もう一度 **user-identity update active-user-database** を発行すると、次のエラー メッセージが表示されます。

  「エラー：1 つの update active-user-database がすでに実行中です。」

  前のセッションが完全に終了するまで待つ必要があります。その後、別の **user-identity update active-user-database** コマンドを発行できます。

  この動作のもう 1 つの例は、AD エージェントから ASA へのパケット損失で発生します。

  user-identity update active-user-database コマンドを発行すると、ASA はダウンロードされるユーザ IP マッピング エントリの総数を要求します。次に AD エージェントは ASA への UDP 接続を開始し、許可要求パケットの変更を送信します。

  何らかの理由でパケットが失われた場合、ASA にはこれを検出する機能はありません。その結果 ASA は 4～5 分間セッションを維持し、**user-identity update active-user-database** コマンドを発行すると、このエラー メッセージを表示し続けます。
- ASA または Cisco Ironport Web Security Appliance（WSA）とともに Cisco Context Directory Agent（CDA）を使用する場合は、次のポートを開くことを確認してください。
  - UDP の認証ポート：1645
  - UDP のアカウンティング ポート：1646
  - UDP のリスニング ポート：3799

    リスニング ポートは、CDA から ASA または WSA への許可要求の変更の送信に使用されます。
- ドメイン名では \/:*?"<>| の文字は無効です。命名規則については、http://support.microsoft.com/kb/909264 [英語] を参照してください。
- ユーザ名では \/[]:;=,+*?"<>|@ の文字は無効です。
- ユーザ グループ名では \/[]:;=,+*?"<>| の文字は無効です。

前提条件

ASA でアイデンティティ ファイアウォールを設定する前に、AD エージェントおよび Microsoft Active Directory の前提条件を満たす必要があります。

AD エージェント

- AD エージェントは、ASA がアクセスできる Windows サーバにインストールする必要があります。さらに、AD エージェントを Active Directory サーバから情報を取得し、ASA と通信するように設定します。
- サポートされる Windows サーバは、Windows 2003、Windows 2008、および Windows 2008 R2 です。

（注）　Windows 2003 R2 は、AD エージェント サーバとしてはサポートされていません。

- AD エージェントをインストールし設定する手順については、『*Installation and Setup Guide for the Active Directory Agent*』を参照してください。
- ASA に AD エージェントを設定する前に、AD エージェントと ASA が通信に使用する秘密キーの値を取得します。この値は AD エージェントと ASA で一致している必要があります。

Microsoft Active Directory

- Microsoft Active Directory は、Windows サーバにインストールされ、ASA からアクセス可能である必要があります。サポートされているバージョンは、Windows 2003、2008、および 2008 R2 サーバです。
- ASA に Active Directory サーバを設定する前に、Active Directory に ASA のユーザ アカウントを作成します。
- さらに、ASA は、LDAP 上でイネーブルになった SSL を使用して、暗号化されたログイン情報を Active Directory サーバに送信します。Active Directory で SSL をイネーブルにする必要があります。Active Directory で SSL をイネーブルにする方法については、Microsoft Active Directory のマニュアルを参照してください。

（注）　AD エージェントのインストーラを実行する前に、AD エージェントがモニタする各 Microsoft Active Directory サーバの「*Readme First for the Cisco Active Directory Agent*」に一覧表示されているパッチをインストールします。これらのパッチは、AD エージェントをドメイン コントローラ サーバに直接インストールする場合でも必要です。

アイデンティティ ファイアウォールの設定

ここでは、次の項目について説明します。

- 「アイデンティティ オプションの設定」（P.32-14）
- 「Identity-Based セキュリティ ポリシーの設定」（P.32-17）

アイデンティティ ファイアウォールの設定のタスク フロー

アイデンティティ ファイアウォールを設定するには、次の作業を実行します。

ステップ 1　ASA に Active Directory ドメインを設定します。

「Active Directory ドメインの設定」（P.32-11）および「Active Directory サーバ グループの設定」（P.32-12）を参照してください。

個々の環境の要件に合わせて Active Directory サーバを展開する方法については、「展開シナリオ」（P.32-5）を参照してください。

ステップ 2　ASA に AD エージェントを設定します。

「Active Directory サーバ グループの設定」（P.32-12）および「Active Directory エージェント グループの設定」（P.32-13）を参照してください。

個々の環境の要件に合わせて AD エージェントを展開する方法については、「展開シナリオ」（P.32-5）を参照してください。

ステップ 3　アイデンティティ オプションを設定します。

「アイデンティティ オプションの設定」（P.32-14）を参照してください。

ステップ 4　Identity-Based セキュリティ ポリシーの設定 AD ドメインと AD エージェントを設定した後、多くの機能で使用するために、アイデンティティに基づくオブジェクト グループおよび ACL を作成できます。

「Identity-Based セキュリティ ポリシーの設定」（P.32-17）を参照してください。

Active Directory ドメインの設定

ASA が AD エージェントから IP とユーザのマッピングを受信したときに特定のドメインから Active Directory グループをダウンロードし、ユーザ アイデンティティを受け取るためには、ASA 上の Active Directory ドメイン設定が必要となります。

前提条件

- Active Directory サーバの IP アドレス
- LDAP ベース DN の識別名
- アイデンティティ ファイアウォールが Active Directory ドメイン コントローラへの接続に使用する、Active Directory ユーザの識別名とパスワード

Active Directory ドメインを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Identity Options] の順に選択します。

ステップ 2　必要に応じて、[Enable User Identity] チェックボックスをオンにして、ユーザのアイデンティティをイネーブルにします。

ステップ 3　[Domains] セクションで、[Add] をクリックするか、リストからドメインを選択して [Edit] をクリックします。

[Domain] ダイアログボックスが表示されます。

ステップ 4　[Domain NETBIOS Name] フィールドに、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_=+[]{};,.] で構成される最大 32 文字の名前を入力します。ただし、先頭に "." と " " を使用することはできません。ドメイン名にスペースを含める場合は、スペースを引用符で囲む必要があります。ドメイン名では、大文字と小文字が区別されません。

既存のドメインの名前を編集する場合、既存のユーザおよびユーザ グループに関連付けられているドメイン名は変更されません。

ステップ 5　[AD Server Group] リストで、このドメインに関連付ける Active Directory サーバを選択するか、[Manage] をクリックして新しいサーバ グループをリストに追加します。「Active Directory サーバ グループの設定」（P.32-12）を参照してください。

ステップ 6　[OK] をクリックしてドメイン設定を保存し、ダイアログボックスを閉じます。

次の作業

「Active Directory サーバ グループの設定」（P.32-12）、および「Active Directory エージェント グループの設定」（P.32-13）を参照してください。

Active Directory サーバ グループの設定

Active Directory サーバ グループを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Identity Options] > [Add] > [Manage] の順に選択します。

[Configure Active Directory Server Groups] ダイアログボックスが表示されます。

ステップ 2　アイデンティティ ファイアウォールの Active Directory サーバ グループを追加するには、[Add] をクリックします。

[Add Active Directory Server Group] ダイアログボックスが表示されます。

ステップ 3　Active Directory サーバ グループにサーバを追加するには、[Active Directory Server Groups] リストから選択して、[Add] をクリックします。

[Add Active Directory Server] ダイアログボックスが表示されます。

ステップ 4　[OK] をクリックして設定を保存し、ダイアログボックスを閉じます。

次の作業

「Active Directory エージェントの設定」（P.32-13）、および「Active Directory エージェント グループの設定」（P.32-13）を参照してください。

Active Directory エージェントの設定

前提条件

AD エージェントを設定する前に、次の情報を用意してください。

- AD エージェントの IP アドレス
- ASA と AD エージェントとの共有秘密

AD エージェントを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Identity Options] の順に選択します。

ステップ 2　必要に応じて、[Enable User Identity] チェックボックスをオンにして、機能をイネーブルにします。

ステップ 3　[Active Directory Agent] セクションで、[Manage] をクリックします。

[Configure Active Directory Agents] ダイアログボックスが表示されます。

ステップ 4　AD エージェントを追加するには、[Add] ボタンをクリックします。またリストでエージェント グループを選択し、[Edit] をクリックします。

以降の手順については、「Active Directory エージェント グループの設定」（P.32-13）を参照してください。

ステップ 5　[OK] をクリックして変更を保存します。

次の作業

AD エージェント グループを設定します。「Active Directory エージェント グループの設定」（P.32-13）を参照してください。

アイデンティティ ファイアウォールのアクセス ルールを設定します。「Identity-Based セキュリティ ポリシーの設定」（P.32-17）を参照してください。

Active Directory エージェント グループの設定

AD エージェント サーバ グループのプライマリ AD エージェントとセカンダリ AD エージェントを設定します。プライマリ AD エージェントが応答していないことを ASA が検出し、セカンダリ AD エージェントが指定されている場合、ASA はセカンダリ AD エージェントに切り替えます。AD エージェントの Active Directory サーバは、通信プロトコルとして RADIUS を使用します。そのため、ASA と AD エージェントとの共有秘密のキー属性を指定する必要があります。

AD エージェント グループを設定するには、次の手順を実行します。

ステップ 1　[Configure Active Directory Agents] ダイアログボックスで、[Add] をクリックします。

[Add Active Directory Agent Group] ダイアログボックスが表示されます。

ステップ 2　AD エージェント グループの名前を入力します。

ステップ 3　[Primary Active Directory Agent] セクションで、ASA が AD エージェント サーバのトラフィックをリッスンするインターフェイスを指定し、サーバの FQDN または IP アドレスを入力します。

ステップ 4　[Primary Active Directory Agent] セクションに、AD エージェントが応答しない場合に ASA が続けて接続を試行する際のタイムアウト間隔と再試行間隔を入力します。

ステップ 5　プライマリ AD エージェントと ASA の間で使用される共有秘密キーを入力します。

ステップ 6　[Secondary Active Directory Agent] セクションで、ASA が AD エージェント サーバのトラフィックをリッスンするインターフェイスを指定し、サーバの FQDN または IP アドレスを入力します。

ステップ 7　[Secondary Active Directory Agent] セクションに、AD エージェントが応答しない場合に ASA が続けて接続を試行する際のタイムアウト間隔と再試行間隔を入力します。

ステップ 8　セカンダリ AD エージェントと ASA の間で使用される共有秘密キーを入力します。

ステップ 9　[OK] をクリックして変更を保存し、ダイアログボックスを閉じます。

次の作業

アイデンティティ ファイアウォールのアクセス ルールを設定します。「Identity-Based セキュリティ ポリシーの設定」（P.32-17）を参照してください。

アイデンティティ オプションの設定

このペインを使用して、アイデンティティ ファイアウォール機能を追加または編集するには、[Enable] チェックボックスをオンにします。デフォルトでは、アイデンティティ ファイアウォール機能はディセーブルになっています。

前提条件

アイデンティティ ファイアウォールのアイデンティティ オプションを設定する前に、AD エージェントおよび Microsoft Active Directory の前提条件を満たす必要があります。AD エージェントおよび Microsoft Active Directory のインストール要件については、「前提条件」（P.32-10）を参照してください。

アイデンティティ ファイアウォールのアイデンティティ オプションを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Identity Options] の順に選択します。

ステップ 2　必要に応じて、[Enable User Identity] チェックボックスをオンにして、機能をイネーブルにします。

ステップ 3　アイデンティティ ファイアウォールのドメインを追加するには、[Add] をクリックして [Add Domain] ダイアログボックスを表示します。

ステップ 4　以降の手順については、「Active Directory ドメインの設定」（P.32-11）を参照してください。

ステップ 5　[Domains] リストにすでに追加されているドメインについて、Active Directory ドメイン コントローラが応答していないため、そのドメインがダウンしている場合にルールをディセーブルにするかどうかを指定します。

ドメインがダウンしており、そのドメインに対してこのオプションが指定されている場合、ASA により、そのドメイン内のユーザに関連付けられているユーザ アイデンティティ ルールがディセーブルにされます。さらに、[Monitoring] > [Properties] > [Identity] > [Users] ペインでは、そのドメイン内のすべてのユーザ IP アドレスがディセーブルとマークされます。

ステップ 6　[Default Domain] ドロップダウン リストで、アイデンティティ ファイアウォールのデフォルト ドメインを選択します。

デフォルト ドメインは、ユーザまたはグループにドメインが明示的に設定されていない場合に、すべてのユーザおよびユーザ グループで使用されます。デフォルト ドメインを指定しない場合、ユーザおよびグループのデフォルト ドメインは LOCAL となります。

さらに、アイデンティティ ファイアウォールは、ローカルに定義されたすべのユーザ グループまたはユーザ（VPN または Web ポータルを使用してログインおよび認証を行うユーザ）に対して LOCAL ドメインを使用します。

（注） 選択するデフォルト ドメイン名は、Active Directory ドメイン コントローラに設定された NetBIOS ドメイン名と一致している必要があります。ドメイン名が一致しない場合、AD エージェントは、ユーザと IP のマッピングを ASA の設定時に入力されたドメイン名に誤って関連付けます。
NetBIOS ドメイン名を表示するには、任意のテキスト エディタで Active Directory ユーザ イベント セキュリティ ログを開きます。

マルチ コンテキスト モードでは、システム実行スペース内だけでなく、各コンテキストについてデフォルト ドメイン名を設定できます。

ステップ 7　[Active Directory Agent] セクションで、ドロップダウン リストから AD エージェント グループを選択します。AD エージェント グループを追加するには、[Manage] をクリックします。詳細については、「Active Directory エージェントの設定」（P.32-13）を参照してください。

ステップ 8　[Hello Timer] フィールドに、10 ～ 65535 秒の数値を入力します。

ASA と AD エージェントとの間の Hello タイマーは、ASA が hello パケットを交換する頻度を定義します。ASA は、hello パケットを使用して、ASA 複製ステータス（in-sync または out-of-sync）とドメイン ステータス（up または down）を取得します。ASA は、AD エージェントから応答を受信しなかった場合、指定された間隔が経過した後、hello パケットを再送信します。

ASA が AD エージェントに hello パケットを送信する回数を指定します。デフォルトでは、秒数は 30 に設定され、再試行回数は 5 に設定されます。

ステップ 9　各 ID について受領する最後のイベント タイム スタンプを追跡し、イベントのタイム スタンプが ASA のクロックより 5 分以上古い場合、またはタイム スタンプが最後のイベントのタイム スタンプよりも前の場合にすべてのメッセージを破棄するように ASA をイネーブルにするには、[Enable Event Timestamp] チェック ボックスをオンにします。

最後のイベントのタイム スタンプの情報がない新たに起動された ASA の場合は、ASA は自身のクロックとイベントのタイム スタンプを比較します。イベントから少なくとも 5 分以上経過している場合、ASA はメッセージを受け入れません。

NTP を使用して互いにクロックを同期させるように ASA、Active Directory、Active Directory エージェントを設定することを推奨します。

ステップ 10　[Poll Group Timer] フィールドで、完全修飾ドメイン名（FQDN）を解決するために ASA が DNS サーバにクエリーを実行する時間数を入力します。デフォルトでは、poll タイマーは 4 秒に設定されます。

ステップ 11　[Retrieve User Information] で、リストから次のいずれかのオプションを選択します。

- [On Demand]：ASA が新しい接続を必要とするパケットを受信し、その送信元 IP アドレスのユーザがユーザ アイデンティティ データベースに含まれていない場合に、ASA が AD エージェントから IP アドレスのユーザ マッピング情報を取得することを指定します。
- [Full Download]：ASA が、ASA の起動時に IP/ユーザ マッピング テーブル全体をダウンロードし、ユーザのログインおよびログアウト時に増分 IP/ユーザ マッピングを受信するように指示する要求を AD エージェントに送信することを指定します。

（注） on-demand には、受信パケットのユーザだけが取得および保存されるためにメモリの使用量が少なくなるというメリットがあります。

ステップ 12　[Error Conditions] セクションで、AD エージェントが応答していない場合にルールをディセーブルにするかどうかを選択します。

AD エージェントがダウンしており、このオプションが選択されている場合、ASA により、そのドメイン内のユーザに関連付けられているユーザ アイデンティティ ルールがディセーブルにされます。さらに、[Monitoring] > [Properties] > [Identity] > [Users] ペインでは、そのドメイン内のすべてのユーザ IP アドレスがディセーブルとマークされます。

ステップ 13　[Error Conditions] セクションで、NetBIOS プローブが失敗した場合にユーザの IP アドレスを削除するかどうかを選択します。

このオプションを選択すると、ユーザに対する NetBIOS プローブがブロックされた場合（たとえば、ユーザ クライアントが NetBIOS プローブに応答しない場合）のアクションが指定されます。また、そのクライアントへのネットワーク接続がブロックされている場合や、クライアントがアクティブでない場合もあります。このオプションが選択されている場合、そのユーザ IP アドレスに関連付けられているアイデンティティ ルールが ASA によってディセーブルにされます。

ステップ 14　[Error Conditions] セクションで、ASA が現在ユーザの MAC アドレスにマッピングしている IP アドレスと、その MAC アドレスが一致しない場合に、ユーザの MAC アドレスを削除するかどうかを選択します。このオプションが選択されている場合、特定のユーザに関連付けられているユーザ アイデンティティ ルールが ASA によってディセーブルにされます。

ステップ 15　[Error Conditions] セクションで、見つからないユーザを追跡するかどうかを選択します。

ステップ 16　[Users] セクションで [Idle Timeout] オプションを選択し、1 ～ 65535 分の分数を入力します。デフォルトでは、アイドル タイムアウトは 60 分に設定されます。

このオプションをイネーブルにすると、アクティブ ユーザがアイドル状態であると考えられる場合（指定された時間を超えても ASA がユーザの IP アドレスからトラフィックを受信しない場合）のタイマーが設定されます。タイマーの期限が切れると、ユーザの IP アドレスが非アクティブとマークされ、ローカル キャッシュ内の IP とユーザのデータベースから削除されます。これ以降、ASA は、この IP アドレスについて AD エージェントに通知しません。既存のトラフィックは通過を許可されます。[Idle Timeout] オプションをイネーブルにすると、ASA は NetBIOS ログアウト プローブが設定されている場合でも非アクティブ タイマーを実行します。

（注）　アイドル タイムアウト オプションは VPN ユーザまたはカットスルー プロキシ ユーザには適用されません。

ステップ 17　[NetBIOS Logout Probe] セクションで、NetBIOS プローブをイネーブルにし、ユーザの IP アドレスがプローブされるまでのプローブ タイマー（1 ～ 65535 分）とプローブの再試行間の再試行間隔（1 ～ 256 回の再試行）を設定します。

このオプションをイネーブルにすることにより、ASA がユーザ ホストのプローブによってユーザ クライアントがアクティブであるかどうかを確認する頻度を設定します。NetBIOS パケットを最小限に抑えるために、ASA は、[Idle Timeout minutes] フィールドで指定された分数を超えてユーザがアイドル状態である場合のみ NetBIOS プローブをクライアントに送信します。

ステップ 18　[NetBIOS Logout Probe] セクションで、[User Name] リストから次のいずれかのオプションを選択します。

- [Match Any]：ホストからの NetBIOS 応答に IP アドレスに割り当てられたユーザのユーザ名が含まれている場合、ユーザ アイデンティティは有効と見なされます。このオプションを指定する場合は、ホストで Messenger サービスがイネーブルになっており、WINS サーバが設定されている必要があります。

- [Exact Match]：NetBIOS 応答に IP アドレスに割り当てられたユーザのユーザ名だけが含まれている必要があります。そうでない場合、その IP アドレスのユーザ アイデンティティは無効と見なされます。このオプションを指定する場合は、ホストで Messenger サービスがイネーブルになっており、WINS サーバが設定されている必要があります。
- [User Not Needed]：ASA がホストから NetBIOS 応答を受信した場合、ユーザ アイデンティティは有効と見なされます。

ステップ 19　[Apply] をクリックし、アイデンティティ ファイアウォールの設定を保存します。

次の作業

Active Directory ドメインとサーバ グループを設定します。「Active Directory ドメインの設定」（P.32-11）および「Active Directory サーバ グループの設定」（P.32-12）を参照してください。

AD エージェントを設定します。「Active Directory サーバ グループの設定」（P.32-12）を参照してください。

Identity-Based セキュリティ ポリシーの設定

Identity-Based ポリシーは、多くの ASA 機能に組み込むことができます。拡張 ACL を使用する機能（「注意事項と制約事項」（P.32-8）でサポート対象外としてリストされている機能を除く）でアイデンティティ ファイアウォールを使用できます。拡張 ACL に、ネットワークベースのパラメータとともにユーザ アイデンティティ引数を追加できるようになりました。

次のような機能で、アイデンティティを使用できます。

- アクセス ルール：アクセス ルールは、ネットワーク情報を使用してインターフェイスのトラフィックを許可または拒否します。アイデンティティ ファイアウォールを使用して、ユーザ アイデンティティに基づいてアクセスを制御できるようになりました。ファイアウォール コンフィギュレーション ガイドを参照してください。
- AAA ルール：認証ルール（「カットスルー プロキシ」とも呼ばれます）は、ユーザに基づいてネットワーク アクセスを制御します。この機能がアクセス ルールとアイデンティティ ファイアウォールに非常に似ているため、AAA ルールは、ユーザの AD ログインの期限が切れた場合、認証のバックアップ方式として使用できます。たとえば、有効なログインのないユーザの場合、AAA ルールをトリガーできます。AAA ルールが有効なログインがないユーザに対してだけトリガーされるようにするには、拡張 ACL でアクセス ルールと AAA ルールに使用される特別なユーザ名 None（有効なログインのないユーザ）および Any（有効なログインを持つユーザ）を指定します。アクセス ルールでは、ユーザおよびグループのポリシーを通常どおりに設定しますが、すべての None ユーザを許可する AAA ルールを含めます。これらのユーザが後で AAA ルールをトリガーできるように、これらのユーザを許可する必要があります。次に、Any ユーザ（これらのユーザは、AAA ルールの対象ではなく、アクセス ルールによってすでに処理されています）を拒否し、すべての None ユーザを許可する AAA ルールを設定します。次に例を示します。

```
access-list 100 ex permit ip user CISCO\xyz any any
access-list 100 ex deny ip user CISCO\abc any any
access-list 100 ex permit ip user NONE any any
access-list 100 ex deny any any
access-group 100 in interface inside

access-list 200 ex deny ip user ANY any any
access-list 200 ex permit user NONE any any
aaa authenticate match 200 inside user-identity
```

詳細については、従来の機能ガイドを参照してください。

- クラウド Web セキュリティ：クラウド Web セキュリティ プロキシ サーバに送信されるユーザを制御できます。また、クラウド Web セキュリティに送信される ASA トラフィック ヘッダーに含まれているユーザ グループに基づくクラウド Web セキュリティ ScanCenter ポリシーを設定できます。ファイアウォール コンフィギュレーション ガイドを参照してください。
- VPN フィルタ：通常、VPN はアイデンティティ ファイアウォール ACL をサポートしませんが、VPN トラフィックにアイデンティティに基づくアクセス ルールを適用するように ASA を設定できます。デフォルトでは、VPN トラフィックはアクセス ルールの対象になりません。VPN クライアントをアイデンティティ ファイアウォール ACL（**no sysopt connection permit-vpn** コマンドによる）を使用するアクセス ルールに強制的に従わせることができます。また、アイデンティティ ファイアウォール ACL を VPN フィルタ機能とともに使用できます。VPN フィルタは、アクセス ルールを一般的に許可することと同様の効果を実現します。

アイデンティティ ファイアウォールのモニタリング

AD エージェントのモニタリング

アイデンティティ ファイアウォールの AD エージェント コンポーネントをモニタするには、次の手順を実行します。

ステップ 1　[Monitoring] > [Properties] > [Identity] > [AD Agent] の順に選択します。

ステップ 2　[Refresh] をクリックして、ペイン内のデータを更新します。

このペインには、プライマリ AD エージェントおよびセカンダリ AD エージェントに関する次の情報が表示されます。

- AD エージェントのステータス
- ドメインのステータス
- AD エージェントの統計情報

グループのモニタリング

アイデンティティ ファイアウォールに設定されたユーザ グループをモニタするには、次の手順を実行します。

ステップ 1　[Monitoring] > [Properties] > [Identity] > [Group] の順に選択します。

ステップ 2　選択したグループを使用するアクセス ルールのリストを表示するには、[Where used] をクリックします。

ステップ 3　[Refresh] をクリックして、ペイン内のデータを更新します。

このペインには、ユーザ グループのリストが *domain\group_name* の形式で表示されます。

アイデンティティ ファイアウォールのメモリ使用率のモニタリング

ASA 上でアイデンティティ ファイアウォールが消費するメモリ使用率をモニタするには、次の手順を実行します。

ステップ 1　[Monitoring] > [Properties] > [Identity] > [Memory Usage] の順に選択します。

ステップ 2　[Refresh] をクリックして、ペイン内のデータを更新します。

このペインには、アイデンティティ ファイアウォールの各種モジュールのメモリ使用率がバイト単位で表示されます。

- ユーザ
- グループ
- ユーザ統計
- LDAP

  ASA は、Active Directory サーバに設定された Active Directory グループに対する LDAP クエリーを送信します。Active Directory サーバは、ユーザを認証し、ユーザ ログイン セキュリティ ログを生成します。
- AD エージェント
- その他
- メモリ使用率合計

（注）　アイデンティティ ファイアウォールで設定した AD エージェントからユーザ情報を取得する方法によって、この機能が使用するメモリの量が変わります。ASA で on-demand 取得と full-download 取得のどちらを使用するかを指定します。on-demand を選択すると、受信パケットのユーザだけが取得および保存されるためにメモリの使用量が少なくなるというメリットがあります。詳細については、「アイデンティティ オプションの設定」（P.32-14）を参照してください。

アイデンティティ ファイアウォールのユーザのモニタリング

アイデンティティ ファイアウォールで使用される IP ユーザ マッピング データベースに含まれるすべてのユーザに関する情報を表示するには、次の手順を実行します。

ステップ 1　[Monitoring] > [Properties] > [Identity] > [User] の順に選択します。

（注）　アクティブ ユーザは緑色で強調表示されます。

ステップ 2　アクティブ ユーザに関する詳細情報を表示するには、リスト内のユーザを選択し、[Details] をクリックします。[Details] ボタンは、アクティブ ユーザでのみイネーブルになります。

ステップ 3　選択したユーザを使用するアクセス ルールのリストを表示するには、[Where used] をクリックします。

ステップ 4　[Refresh] をクリックして、ペイン内のデータを更新します。

このペインにはユーザに関する次の情報が表示されます。

domain\user_name	ステータス（アクティブまたは非アクティブ）	接続手段	アイドル時間（分数）

デフォルトのドメイン名は、実際のドメイン名、特別な予約語、LOCAL のいずれかです。アイデンティティ ファイアウォールは、ローカルに定義されたすべのユーザ グループまたはユーザ（VPN または Web ポータルを使用してログインおよび認証を行うユーザ）に対して LOCAL ドメイン名を使用します。デフォルト ドメインを指定しない場合、LOCAL がデフォルト ドメインとなります。

アイドル時間は、ユーザの IP アドレスごとではなくユーザごとに保存されます。

Active Directory サーバがダウンしている場合にルールをディセーブルにするオプションが指定されていて、ドメインがダウンしている場合、または AD エージェントがダウンしている場合にルールをディセーブルにするオプションが指定されていて、AD エージェントがダウンしている場合、ログインしているすべてのユーザのステータスがディセーブルになります。これらのオプションは、[Identity Options] ペインで設定します。

または、[Firewall Dashboard] ペインにアクセスして、ユーザの統計を表示することもできます。[Firewall Dashboard] タブでは、ASA を通過するトラフィックに関する重要な情報を確認できます。[Home] > [Firewall Dashboard] > [Top Usage Statistics] > [Top 10 Users] タブを選択します。

[Top 10 Users] タブには、ASA でアイデンティティ ファイアウォール機能を設定している場合（Microsoft Active Directory や Cisco Active Directory（AD）エージェントなどの追加コンポーネントの設定を含む）にのみデータが表示されます。詳細については、「アイデンティティ ファイアウォールの設定」（P.32-10）を参照してください。

選択したオプションに応じて、[Top 10 Users] タブに、上位 10 ユーザの受信した EPS パケット、送信した EPS パケット、および送信された攻撃に関する統計情報が表示されます。（***domain\user_name*** として表示される）各ユーザに関して、このタブには、そのユーザの平均 EPS パケット、現在の EPS パケット、トリガー、および合計イベント数が表示されます。

（注）　[Top Usage Status] 領域の最初の 3 つのタブには脅威検出のデータが表示されます。これは、アイデンティティ ファイアウォール機能とは関係ありません。

アイデンティティ ファイアウォールの機能履歴

表 32-1 に、この機能のリリース履歴を示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 32-1　アイデンティティ ファイアウォールの機能履歴

機能名	リリース	機能情報
アイデンティティ ファイアウォール	8.4(2)	アイデンティティ ファイアウォール機能が導入されました。 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [Identity Options] [Configuration] > [Firewall] > [Objects] > [Local User Groups] [Monitoring] > [Properties] > [Identity]

ASA と Cisco TrustSec

Cisco TrustSec と統合された ASA に関する情報

Cisco TrustSec の概要

従来、ファイアウォールなどのセキュリティ機能は、事前定義されている IP アドレス、サブネット、およびプロトコルに基づいてアクセス コントロールを実行していました。しかし、企業のボーダレス ネットワークへの移行に伴い、ユーザと組織の接続に使用されるテクノロジーおよびデータとネットワークを保護するためのセキュリティ要件が大幅に向上しています。エ

ンドポイントは、ますます遊動的となり、ユーザは通常さまざまなエンドポイント（ラップトップとデスクトップ、スマートフォン、タブレットなど）を使用します。つまり、ユーザ属性とエンドポイント属性の組み合わせにより、ファイアウォール機能または専用ファイアウォールを持つスイッチやルータなどの実行デバイスがアクセス コントロール判断のために信頼して使用できる既存の 6 タプル ベースのルール以外の主要な特性が提供されます。

その結果、お客様のネットワーク全体、ネットワークのアクセス レイヤ、分散レイヤ、コア レイヤ、およびデータセンターのセキュリティを有効にするためには、エンドポイント属性またはクライアント アイデンティティ属性のアベイラビリティと伝搬がますます重要な要件となります。

Cisco TrustSec は、既存の ID 認証インフラストラクチャを基盤とするアクセス コントロールです。ネットワーク デバイス間のデータ機密性保持を目的としており、セキュリティ アクセス サービスを 1 つのプラットフォーム上で統合します。Cisco TrustSec 機能では、実行デバイスはユーザ属性とエンドポイント属性の組み合わせを使用して、ロールベースおよびアイデンティティベースのアクセス コントロールを決定します。この情報のアベイラビリティおよび伝搬によって、ネットワークのアクセス レイヤ、分散レイヤ、およびコア レイヤでのネットワーク全体におけるセキュリティが有効になります。

ご使用の環境に Cisco TrustSec を実装する利点は、次のとおりです。

- デバイスからの適切でより安全なアクセスにより、拡大する複雑なモバイル ワークフォースを提供します。
- 有線または無線ネットワークへの接続元を包括的に確認できるため、セキュリティ リスクが低減されます。
- 物理またはクラウドベースの IT リソースにアクセスするネットワーク ユーザのアクティビティに対する非常に優れた制御が実現されます。
- 中央集中化、非常にセキュアなアクセス ポリシー管理、およびスケーラブルな実行メカニズムにより、総所有コストが削減されます。

Cisco TrustSec 機能を各種のシスコ製品で使用する方法については、「その他の関連資料」（P.33-27）を参照してください。

Cisco TrustSec の SGT および SXP サポートについて

Cisco TrustSec 機能では、セキュリティ グループ アクセスは、トポロジ認識ネットワークをロールベースのネットワークに変換するため、ロールベース アクセス コントロール（RBAC）に基づいて実施されるエンドツーエンド ポリシーがイネーブルになります。認証時に取得されたデバイスおよびユーザ クレデンシャルは、パケットをセキュリティ グループごとに分類するために使用されます。Cisco TrustSec クラウドに着信するすべてのパケットは、セキュリティ グループ タグ（SGT）でタグ付けされます。タギングは、信頼できる中継がパケットの送信元のアイデンティティを識別し、データ パスでセキュリティ ポリシーを適用するのに役立ちます。SGT は、SGT を使用してセキュリティ グループ ACL を定義する場合に、ドメイン全体の特権レベルを示すことができます。

SGT は、RADIUS ベンダー固有属性で発生する IEEE 802.1X 認証、Web 認証、または MAC 認証バイパス（MAB）を使用してデバイスに割り当てられます。SGT は、特定の IP アドレスまたはスイッチ インターフェイスにスタティックに割り当てることができます。SGT は、認証の成功後にスイッチまたはアクセス ポイントにダイナミックに渡されます。

セキュリティ グループ交換プロトコル（SXP）は、SGT およびセキュリティ グループ ACL をサポートしているハードウェアに対する SGT 対応ハードウェア サポートがないネットワーク デバイスに IP-to-SGT マッピング データベースを伝搬できるよう Cisco TrustSec 向けに開発されたプロトコルです。コントロール プレーン プロトコルの SXP は、IP-SGT マッピングを認証ポイント（レガシー アクセス レイヤ スイッチなど）からネットワークのアップストリーム デバイスに渡します。

SXP 接続はポイントツーポイントであり、基礎となる転送プロトコルとして TCP を使用します。SXP は接続を開始するために既知の TCP ポート番号 64999 を使用します。また、SXP 接続は、送信元および宛先 IP アドレスによって一意に識別されます。

Cisco TrustSec 機能のロール

アイデンティティおよびポリシーベースのアクセス実施を提供するために、Cisco TrustSec 機能には、次のロールがあります。

- アクセス要求側（AR）：アクセス要求側は、ネットワークの保護されたリソースへのアクセスを要求するエンドポイント デバイスです。これらのデバイスはアーキテクチャのプライマリ対象であり、そのアクセス権限はアイデンティティ クレデンシャルによって異なります。

  アクセス要求側には、PC、ラップトップ、携帯電話、プリンタ、カメラ、MACsec 対応 IP フォンなどのエンドポイント デバイスが含まれます。

- ポリシー デシジョン ポイント（PDP）：ポリシー デシジョン ポイントはアクセス コントロール判断を行います。PDP は 802.1x、MAB、Web 認証などの機能を提供します。PDP は VLAN、DACL および Security Group Access（SGACL/SXP/SGT）による許可および適用をサポートします。

  Cisco TrustSec 機能では、Cisco Identity Services Engine（ISE）が PDP として機能します。Cisco ISE はアイデンティティおよびアクセス コントロール ポリシーの機能を提供します。

- ポリシー情報ポイント（PiP）：ポリシー情報ポイントは、ポリシー デシジョン ポイントに外部情報（たとえば、評価、場所、および LDAP 属性）を提供する送信元です。

  ポリシー情報ポイントには、Session Directory、IPS センサー、Communication Manager などのデバイスが含まれます。

- ポリシー管理ポイント（PAP）：ポリシー管理ポイントはポリシーを定義し、許可システムに挿入します。PAP はアイデンティティ リポジトリとしても動作し、Cisco TrustSec タグからユーザ アイデンティティへのマッピングと、Cisco TrustSec タグからサーバ リソースへのマッピングを行います。

  Cisco TrustSec 機能では、Cisco Secure Access Control System（802.1x および SGT サポートと統合されたポリシー サーバ）が PAP として機能します。

- ポリシー エンフォースメント ポイント（PEP）：ポリシー エンフォースメント ポイントは、各 AR の PDP による決定（ポリシー ルールおよびアクション）を実行するエンティティです。PEP デバイスは、ネットワーク全体に存在するプライマリ通信パスを介してアイデンティティ情報を学習します。PEP デバイスは、エンドポイント エージェント、許可サーバ、ピア実行デバイス、ネットワーク フローなど、さまざまな送信元から各 AR のアイデンティティ属性を学習します。同様に、PEP デバイスは SXP を使用して、ネットワーク全体で相互信頼できるピア デバイスに IP-SGT マッピングを伝搬します。

  ポリシー エンフォースメント ポイントには、Catalyst Switches、ルータ、ファイアウォール（具体的には ASA）、サーバ、VPN デバイス、SAN デバイスなどのネットワーク デバイスが含まれます。

Cisco ASA は、アイデンティティ アーキテクチャの中で PEP の役割を果たします。SXP を使用して、ASA は、認証ポイントから直接アイデンティティ情報を学習し、その情報を使用してアイデンティティベースのポリシーを適用します。

セキュリティ グループ ポリシーの適用

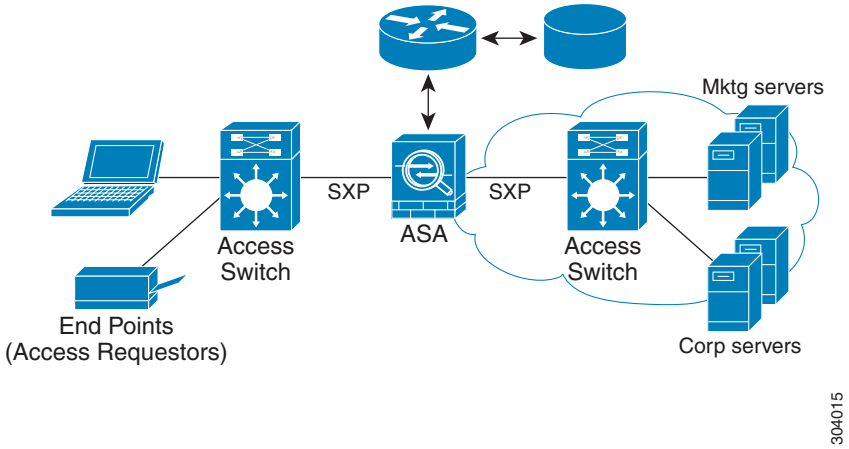
セキュリティ ポリシーの適用はセキュリティ グループの名前に基づきます。エンドポイントデバイスは、データセンターのリソースへのアクセスを試行します。ファイアウォールで設定された従来の IP ベースのポリシーと比較して、アイデンティティベースのポリシーは、ユーザおよびデバイス アイデンティティに基づいて設定されます。たとえば、mktg-contractor が mktg-server にアクセスできるとします。mktg-corp-user は、mktg-server および corp-server にアクセスできます。

このタイプの導入には次のような利点があります。

- ユーザ グループとリソースが 1 つのオブジェクト（SGT）を使用して定義されます（簡易ポリシー管理）。
- ユーザ アイデンティティとリソース アイデンティティは、Cisco TrustSec 対応スイッチ インフラストラクチャ全体で保持されます。

図 33-1 に、セキュリティ グループの名前ベースのポリシー適用のための展開を示します。

図 33-1　　セキュリティ グループ名に基づくポリシー適用の導入



Cisco TrustSec を実装すると、サーバのセグメンテーションをサポートするセキュリティ ポリシーを設定できます。また、Cisco TrustSec の実装には次のような特徴があります。

- 簡易ポリシー管理用に、サーバのプールに SGT を割り当てることができます。
- SGT 情報は、Cisco TrustSec 対応スイッチのインフラストラクチャ内に保持されます。
- ASA は、Cisco TrustSec ドメイン全体にポリシーを適用するために IP-SGT マッピングを利用できます。
- サーバの 802.1x 許可が必須であるため、導入を簡略化できます。

ASA によるセキュリティ グループベースのポリシーの適用

（注）　ユーザベースのセキュリティ ポリシーおよびセキュリティ グループベースのポリシーは、ASA で共存できます。セキュリティ ポリシーでは、ネットワーク属性、ユーザベースの属性、およびセキュリティ グループベースの属性の任意の組み合わせを設定できます。ユーザベースのセキュリティ ポリシーの設定については、第 32 章「アイデンティティ ファイアウォール」を参照してください。

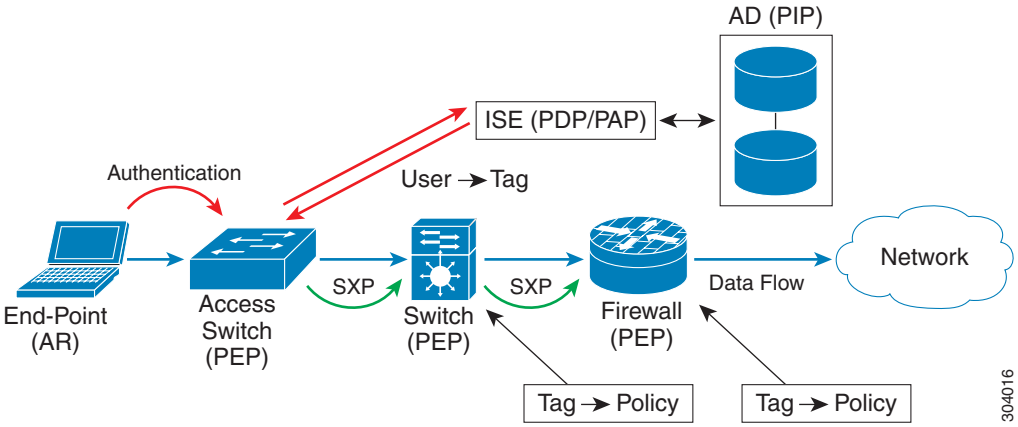
Cisco TrustSec と連携するように ASA を設定するには、ISE から Protected Access Credential（PAC）ファイルをインポートする必要があります。詳細については、「PAC ファイルのインポート」（P.33-16）を参照してください。

PAC ファイルを ASA にインポートすると、ISE との安全な通信チャネルが確立されます。チャネルが確立されると、ASA は、ISE を使用して PAC セキュア RADIUS トランザクションを開始し、Cisco TrustSec 環境データをダウンロードします（具体的には、セキュリティ グループ テーブル）。セキュリティ グループ テーブルによって、SGT がセキュリティ グループ名にマッピングされます。セキュリティ グループの名前は ISE 上で作成され、セキュリティ グループをわかりやすい名前で識別できるようになります。

ASA は、最初にセキュリティ グループ テーブルをダウンロードするときに、テーブル内のすべてのエントリを順を追って調べ、そこで設定されているセキュリティ ポリシーに含まれるすべてのセキュリティ グループの名前を解決します。次に、ASA は、それらのセキュリティ ポリシーをローカルでアクティブ化します。ASA がセキュリティ グループの名前を解決できない場合、不明なセキュリティ グループ名に対して syslog メッセージを生成します。

図 33-2 に、セキュリティ ポリシーが Cisco TrustSec で適用される仕組みを示します。

図 33-2　　セキュリティ ポリシーの適用



1. エンドポイント デバイスは、アクセス レイヤ デバイスに直接アクセスするか、またはリモート アクセスを介してアクセスし、Cisco TrustSec で認証します。
2. アクセス レイヤ デバイスは 802.1X や Web 認証などの認証方式を使用して ISE のエンドポイント デバイスを認証します。エンドポイント デバイスは、ロールおよびグループ メンバーシップ情報を渡して、デバイスを適切なセキュリティ グループに分類します。
3. アクセス レイヤ デバイスは SXP を使用して、アップストリーム デバイスに IP-SGT マッピングを伝搬します。
4. ASA はパケットを受信すると、SXP から渡された IP-SGT マッピングを使用して、送信元および宛先 IP アドレスの SGT を調べます。

   マッピングが新規の場合、ASA はそのマッピングをローカル IP-SGT マネージャ データベースに記録します。コントロール プレーンで実行される IP-SGT マネージャ データベースは、各 IPv4 または IPv6 アドレスの IP-SGT マッピングを追跡します。データベースでは、マッピングが学習された送信元が記録されます。SXP 接続のピア IP アドレスがマッピングの送信元として使用されます。各 IP-SGT にマップされたエントリには、送信元が複数存在する可能性があります。

   ASA が送信者として設定されている場合、ASA は SXP ピアに IP-SGT マッピング エントリをすべて送信します。詳細については、「ASA での送信者および受信者のロール」（P.33-7）を参照してください。

5. ASA で SGT またはセキュリティ グループの名前を使用してセキュリティ ポリシーが設定されている場合、ASA はそのポリシーを適用します（ASA では、SGT またはセキュリティ グループの名前を含むセキュリティ ポリシーを作成できます。セキュリティ グループの名前に基づいてポリシーを適用するには、ASA はセキュリティ グループ テーブルで SGT にセキュリティ グループの名前をマッピングする必要があります）。

   ASA がセキュリティ グループ テーブルでセキュリティ グループの名前を見つけることができず、その名前がセキュリティ ポリシーに含まれている場合、ASA は、セキュリティ グループの名前を不明と見なし、syslog メッセージを生成します。ISE からの ASA セキュリティ グループ テーブルの更新とセキュリティ グループの名前の学習後、ASA はセキュリティ グループの名前がわかっていることを示す syslog メッセージを生成します。

セキュリティ グループに対する変更が ISE に及ぼす影響

ASA は、ISE から最新のテーブルをダウンロードして、セキュリティ グループ テーブルを定期的に更新します。セキュリティ グループは、ダウンロードの合間に ISE で変更できます。これらの変更は、セキュリティ グループ テーブルが更新されるまで、ASA には反映されません。

ヒント　ISE のポリシー設定の変更は、メンテナンス時間中にスケジュールすることをお勧めします。さらに、セキュリティ グループの変更を確実に行うには、ASA でセキュリティ グループ テーブルを手動で更新します。

このようにポリシー設定の変更を行うことで、セキュリティ グループの名前を解決し、セキュリティ ポリシーを即座にアクティブ化できる可能性が最大限に高まります。

セキュリティ グループ テーブルは、環境データのタイマーが期限切れになると自動的に更新されます。セキュリティ グループ テーブルの更新は、オンデマンドでトリガーすることも可能です。

ISE でセキュリティ グループを変更する場合、ASA がセキュリティ グループ テーブルを更新するときに次のイベントが発生します。

- セキュリティ グループの名前を使用して設定されたセキュリティ グループ ポリシーだけは、セキュリティ グループ テーブルを通じて解決する必要があります。セキュリティ グループ タグを含むポリシーは、常にアクティブになります。
- セキュリティ グループ テーブルが初めて利用できるようになったときに、セキュリティ グループの名前を含むすべてのポリシーが確認され、セキュリティ グループの名前が解決され、ポリシーがアクティブ化されます。また、タグ付きのすべてのポリシーが確認されます。不明なタグの場合は syslog が生成されます。
- セキュリティ グループ テーブルの期限が切れていても、そのテーブルをクリアするか、新しいテーブルを使用できるようになるまで、最後にダウンロードしたセキュリティ グループ テーブルに従って引き続きポリシーが適用されます。
- ASA で解決済みのセキュリティ グループの名前が不明になると、セキュリティ ポリシーが非アクティブ化されます。ただし、ASA の実行コンフィギュレーションではセキュリティ ポリシーが保持されます。
- PAP で既存のセキュリティ グループが削除されると、既知のセキュリティ グループ タグが不明になる可能性がありますが、ASA のポリシー ステータスは変化しません。既知のセキュリティ グループの名前は未解決になる可能性があり、その場合、ポリシーは非アクティブになります。セキュリティ グループの名前が再利用される場合、新しいタグを使用してポリシーが再コンパイルされます。

- PAP で新しいセキュリティ グループが追加されると、不明なセキュリティ グループ タグが既知になる可能性があり、syslog メッセージが生成されます。ただし、ポリシー ステータスは変化しません。不明なセキュリティ グループの名前が解決される可能性があり、その場合、関連付けられているポリシーがアクティブ化されます。
- PAP でタグの名前が変更された場合、タグを使用して設定されたポリシーによって新しい名前が表示されます。ポリシー ステータスは変化しません。セキュリティ グループの名前を使用して設定されたポリシーは、新しいタグ値を使用して再コンパイルされます。

ASA での送信者および受信者のロール

ASA では、SXP の他のネットワーク デバイスとの間の IP-SGT マッピング エントリの送受信がサポートされます。SXP を使用すると、セキュリティ デバイスとファイアウォールが、ハードウェアをアップグレードまたは変更する必要なく、アクセス スイッチからのアイデンティティ情報を学習できます。また、SXP を使用して、アップストリーム デバイス（データセンター デバイスなど）からの IP-SGT マッピング エントリをダウンストリーム デバイスに渡すこともできます。ASA は、アップストリームおよびダウンストリームの両方向から情報を受信できます。

ASA での SXP ピアへの SXP 接続を設定する場合は、アイデンティティ情報を交換できるように、ASA を送信者または受信者として指定する必要があります。

- 送信者モード：ASA で収集されたアクティブな IP-SGT マッピング エントリをすべてポリシー適用のためアップストリーム デバイスに転送できるように ASA を設定します。
- 受信者モード：ダウンストリーム デバイス（SGT 対応スイッチ）からの IP-SGT マッピング エントリを受信し、ポリシー定義作成のためにこの情報を使用できるように ASA を設定します。

SXP 接続の一方の端が送信者として設定されている場合、もう一方の端は受信者として設定する必要があります。逆の場合も同様です。SXP 接続の両端の両方のデバイスに同じロール（両方とも送信者または両方とも受信者）が設定されている場合、SXP 接続が失敗し、ASA は syslog メッセージを生成します。

SXP 接続が複数ある場合でも、IP-SGT マッピング データベースからダウンロードされた IP-SGT マッピング エントリを学習できます。ASA で SXP ピアへの SXP 接続が確立されると、受信者が送信者から IP-SGT マッピング データベース全体をダウンロードします。この後に行われる変更はすべて、新しいデバイスがネットワークに接続されたときにのみ送信されます。このため、SXP の情報が流れる速さは、エンド ホストがネットワーク認証を行う速さに比例します。

SXP 接続を通じて学習された IP-SGT マッピング エントリは、SXP IP-SGT マッピング データベースで管理されます。同じマッピング エントリが異なる SXP 接続を介して学習される場合もあります。マッピング データベースは、学習した各マッピング エントリのコピーを 1 つ保持します。同じ IP-SGT マッピング値の複数のマッピング エントリは、マッピングを学習した接続のピア IP アドレスによって識別されます。SXP は IP-SGT マネージャに対して、新しいマッピングが初めて学習された場合にはマッピング エントリを追加するように、SXP データベース内の最後のコピーが削除された場合にはマッピング エントリを削除するように要求します。

SXP 接続が送信者として設定されている場合は必ず、SXP は IP-SGT マネージャに対して、デバイスで収集したすべてのマッピング エントリをピアに転送するよう要求します。新しいマッピングがローカルで学習されると、IP-SGT マネージャは SXP に対して、送信者として設定されている接続を介してそのマッピングを転送するよう要求します。

ASA を SXP 接続の送信者および受信者の両方として設定すると、SXP ループが発生する可能性があります。つまり、SXP データが最初にそのデータを送信した SXP ピアで受信される可能性があります。

SXP の対話

SXP の情報が流れる速さは、エンド ホストがネットワーク認証を行う速さに比例します。SXP ピアリングが確立されると、受信者デバイスは送信者デバイスから IP-SGT データベース全体をダウンロードします。その後、新しいデバイスがネットワークに接続された場合、またはデバイスのネットワーク接続が解除された場合にのみ、すべての変更が段階的に送信されます。また、新しいデバイスに接続されたアクセス デバイスのみがアップストリーム デバイスに対する差分更新を開始することにも注意してください。

つまり、SXP プロトコルは、認証サーバの性能によって制限される認証速度を超えることができません。したがって、SXP の対話は大きな問題になりません。

SXP タイマー

- 再試行開始タイマー：再試行開始タイマーは、デバイスで SXP 接続が確立されていない場合にトリガーされます。再試行開始タイマーの期限が切れると、デバイスは接続データベース全体を検索します。すべての接続が切断されているか、「保留中」状態の場合は、再試行開始タイマーが再開されます。タイマーのデフォルト値は 120 秒です。タイマー値がゼロの場合、再試行開始タイマーは開始されません。再試行開始タイマーは、すべての SXP 接続が確立されるか、再試行開始タイマーの値がゼロに設定されるまで動作を継続します。
- 削除ホールドダウン タイマー：接続固有の削除ホールドダウン タイマーは、受信者の接続が切断されるとトリガーされます。学習されたマッピング エントリはすぐには削除されず、削除ホールドダウン タイマーの期限が切れるまで保持されます。マッピング エントリは、このタイマーの期限が切れると削除されます。削除ホールドダウン タイマー値は 120 秒に設定されており、ユーザが設定することはできません。
- 調整タイマー：SXP 接続が削除ホールドダウン タイマーの動作中に確立された場合、その接続で一括更新が実行されます。つまり、最新のマッピング エントリが学習され、新しい接続インスタンス化 ID に関連付けられます。周期的な接続固有の調整タイマーは、バックグラウンドで開始されます。この調整タイマーの期限が切れると、SXP マッピング データベース全体がスキャンされ、現在の接続セッションで学習されなかったマッピング エントリ（接続インスタンス化 ID が一致しないマッピング エントリ）がすべて特定され、削除対象としてマークされます。これらのエントリは、続いて行われる調整レビューで削除されます。調整タイマーのデフォルト値は 120 秒です。ASA では、値をゼロに設定できません。これは、廃止エントリが不特定の期間にわたって保持され、ポリシーの適用において予期しない結果を招かないようにするためです。
- HA 調整タイマー：HA が有効になっている場合、アクティブ装置とスタンバイ装置の SXP マッピング データベースが同期されます。新しいアクティブ装置は、そのすべてのピアに対する新しい SXP 接続を確立し、最新のマッピング エントリを取得しようとします。HA 調整タイマーは、古いマッピング エントリを特定して削除するための方法を提供します。このタイマーは、フェールオーバーの発生後に開始されます。このため、ASA が最新のマッピング エントリを取得する時間が得られます。HA 調整タイマーの期限が切れると、ASA は SXP マッピング データベース全体をスキャンし、現在の接続セッションで学習されなかったマッピング エントリをすべて特定します。インスタンス化 ID が一致しないマッピング エントリは、削除対象としてマークされます。この調整メカニズムは、調整タイマーのメカニズムと同じです。タイマー値は調整タイマーと同じで、ユーザが設定できます。

SXP ピアが SXP 接続を終了すると、ASA は削除ホールドダウン タイマーを開始します。受信者として指定された SXP ピアのみが接続を終了できます。削除ホールドダウン タイマーの実行中に SXP ピアが接続されると、ASA は調整タイマーを開始します。次に、ASA は、IP-SGT マッピング データベースを更新して、最新のマッピングを学習します。

IP-SGT マネージャ データベース

IP-SGT マネージャ データベースは、アクティブ装置からスタンバイ装置へのエントリの同期を行いません。IP-SGT マネージャ データベースが IP-SGT マッピング エントリを受信する各送信元は、アクティブ装置からスタンバイ装置へのデータベースの同期を行ってから、スタンバイ装置上の IP-SGT マネージャに対して最終的な IP-SGT マッピングを提供します。

バージョン 9.0（1）の IP-SGT マネージャ データベースは、SXP の送信元からのみ IP-SGT マッピングの更新を受信します。

ASA-Cisco TrustSec 統合の機能

ASA には、アイデンティティベースのファイアウォール機能の一部として Cisco TrustSec が含まれています。Cisco TrustSec には次の機能があります。

柔軟性

- ASA を SXP 送信者または受信者、あるいはその両方として設定できます。
- ASA は、IPv6 と IPv6 対応ネットワーク デバイス用に SXP をサポートします。
- SXP は、IPv4 および IPv6 アドレスのマッピング エントリを変更できます。
- SXP エンドポイントは、IPv4 および IPv6 アドレスをサポートしています。
- ASA は、SXP バージョン 2 のみをサポートしています。
- ASA は、さまざまな SXP 対応ネットワーク デバイスの SXP バージョンをネゴシエートします。SXP バージョン ネゴシエーションによって、バージョンのスタティック コンフィギュレーションが不要になります。
- SXP 調整タイマーの期限が切れたときにセキュリティ グループ テーブルをリフレッシュするように ASA を設定できます。セキュリティ グループ テーブルはオンデマンドでダウンロードできます。ASA のセキュリティ グループ テーブルが ISE から更新された場合、この変更が適切なセキュリティ ポリシーに反映されます。
- ASA では、送信元フィールドまたは宛先フィールド、あるいはその両方のセキュリティ グループの名前に基づくセキュリティ ポリシーがサポートされます。セキュリティ グループ、IP アドレス、Active Directory グループ/ユーザ名、および FQDN の組み合わせに基づいて ASA のセキュリティ ポリシーを設定できます。

アベイラビリティ

- アクティブ/アクティブおよびアクティブ/スタンバイ コンフィギュレーションの両方で ASA のセキュリティ グループベースのポリシーを設定できます。
- ASA は、ハイ アベイラビリティ（HA）用に設定された ISE と通信できます。
- ASA では複数の ISE サーバを設定できます。最初のサーバが到達不能の場合、引き続き 2 番目以降のサーバに接続を試みます。ただし、サーバ リストが Cisco TrustSec 環境データの一部としてダウンロードされた場合、そのリストは無視されます。
- ISE からダウンロードされた PAC ファイルが ASA で期限切れとなり、ASA が更新されたセキュリティ グループ テーブルをダウンロードできない場合、ASA が更新されたテーブルをダウンロードするまで、最後にダウンロードされたセキュリティ グループ テーブルに基づいてセキュリティ ポリシーを適用し続けます。

クラスタリング

- レイヤ 2 ネットワークでは、すべての装置が同じ IP アドレスを共有します。インターフェイス アドレスを変更すると、変更された設定が他のすべての装置に送信されます。特定の装置のインターフェイスから IP アドレスが更新されると、その装置の IP-SGT ローカル データベースを更新するよう通知が送信されます。
- レイヤ 3 ネットワークでは、マスター装置のインターフェイスごとにアドレス プールが設定され、その設定がスレーブ装置に同期されます。マスター装置では、インターフェイスに割り当てられている IP アドレスの通知が送信され、IP-SGT ローカル データベースが更新されます。各スレーブ装置の IP-SGT ローカル データベースは、同期されたアドレス プールの設定を使用することにより、マスター装置の IP アドレス情報を通じて更新することができます。各インターフェイス用のプール内にある最初のアドレスは常に、マスター装置に属します。

  スレーブ装置は、起動時にマスター装置への通知を行います。通知を受け取ったマスター装置は、各インターフェイスのアドレス プールを検索し、通知を送信した新しいスレーブ装置の IP アドレスを計算して、マスター装置の IP-SGT ローカル データベースを更新します。マスター装置は他のスレーブ装置に対して、新しいスレーブ装置に関する通知を行います。各スレーブ装置は、この通知処理の一環として、新しいスレーブ装置の IP アドレスを計算し、各スレーブ装置の IP-SGT ローカル データベースにそのエントリを追加します。すべてのスレーブ装置で、IP アドレスの値を求めるためのアドレス プールが設定されます。各インターフェイスの値は、次のように求められます。

  マスター IP + （M - N）

  M：最大装置数（最大 8 台）

  N：通知を送信したスレーブ装置の番号

  任意のインターフェイスで IP アドレス プールが変更されたとき、すべてのスレーブ装置およびマスター装置の IP アドレスを再計算し、マスター装置だけでなく、他のすべてのスレーブ装置の IP-SGT ローカル データベースを更新する必要があります。古い IP アドレスは削除して、新しい IP アドレスを追加する必要があります。

  この変更されたアドレス プールの設定がスレーブ装置に同期されると、設定の変更処理の一環として、IP アドレスが変更されたマスター装置および他のすべてのスレーブ装置の IP アドレスが各スレーブ装置で再計算されます。その後、古い IP アドレスのエントリが削除され、新しい IP アドレスが追加されます。

拡張性

表 33-1 に、ASA がサポートする IP-SGT マッピング エントリの数を示します。

表 33-1　IP-SGT マッピング エントリの許容数

ASA モデル	IP-SGT マッピング エントリの数
5585-X（SSP-10）	18,750
5585-X（SSP-20）	25,000
5585-X（SSP-40）	50,000
5585-X（SSP-60）	100,000

表 33-2 に、ASA がサポートする SXP 接続の数を示します。

表 33-2　　SXP 接続

ASA モデル	SXP TCP 接続の数
5585-X（SSP-10）	150
5585-X（SSP-20）	250
5585-X（SSP-40）	500
5585-X（SSP-60）	1000

Cisco TrustSec のライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

Cisco TrustSec を使用するための前提条件

Cisco TrustSec を使用するように ASA を設定する前に、次のタスクを実行する必要があります。

- 「ASA の ISE への登録」（P.33-11）
- 「ISE でのセキュリティ グループの作成」（P.33-12）
- 「PAC ファイルの生成」（P.33-12）

ASA の ISE への登録

ASA が PAC ファイルを正常にインポートするには、ISE の認識された Cisco TrustSec ネットワーク デバイスとして ASA を設定する必要があります。ISE に ASA を登録するには、次の手順を実行します。

1. ISE にログインします。
2. [Administration] > [Network Devices] > [Network Devices] を選択します。
3. [Add] をクリックします。
4. ASA の IP アドレスを入力します。
5. ISE がユーザ認証用に使用されている場合、[Authentication Settings] 領域に共有秘密を入力します。

   ASA で AAA サーバを設定する場合は、ISE でここで作成した共有秘密を指定します。ASA の AAA サーバはこの共有秘密を使用して、ISE と通信します。
6. ASA のデバイス名、デバイス ID、パスワード、およびダウンロード間隔を指定します。これらのタスクの実行方法については、ISE のマニュアルを参照してください。

ISE でのセキュリティ グループの作成

ISE と通信するように ASA を設定する場合は、AAA サーバを指定します。AAA サーバを ASA で設定する場合は、サーバ グループを指定する必要があります。セキュリティ グループは、RADIUS プロトコルを使用するように設定する必要があります。ISE でセキュリティ グループを作成するには、次の手順を実行します。

1. ISE にログインします。
2. [Policy] > [Policy Elements] > [Results] > [Security Group Access] > [Security Group] を選択します。
3. ASA のセキュリティ グループを追加します （セキュリティ グループは、グローバルであり、ASA に固有ではありません）。

   ISE は、タグを使用して [Security Groups] でエントリを作成します。
4. [Security Group Access] 領域で、ASA のデバイス ID クレデンシャルおよびパスワードを設定します。

PAC ファイルの生成

PAC ファイルを生成する前に、ISE に ASA を登録する必要があります。PAC ファイルを生成するには、次の手順を実行します。

1. ISE にログインします。
2. [Administration] > [Network Resources] > [Network Devices] を選択します。
3. デバイスのリストから ASA を選択します。
4. [Security Group Access (SGA)] で、[Generate PAC] をクリックします。
5. PAC ファイルを暗号化するには、パスワードを入力します。

   PAC ファイルを暗号化するために入力するパスワード（または暗号キー）は、デバイス クレデンシャルの一部として ISE で設定したパスワードとは関係ありません。

ISE は PAC ファイルを生成します。ASA は、フラッシュから PAC ファイルをインポートすることができます。また、TFTP、FTP、HTTP、HTTPS、SMB を介してリモート サーバからインポートすることも可能です （PAC ファイルは、インポート前に ASA フラッシュに配置されている必要はありません）。

PAC ファイルについては、「PAC ファイルのインポート」（P.33-16）を参照してください。

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

SXP エンドポイント用に IPv6 をサポートします。

クラスタリングのガイドライン

クラスタリング環境内のマスター装置およびスレーブ装置でサポートされています。

フェールオーバーのガイドライン

設定によってサーバのリストをサポートします。最初のサーバが到達不能の場合、ASA はリストの 2 番目以降のサーバに順番に接続を試みます。ただし、Cisco TrustSec 環境データの一部としてダウンロードされたサーバ リストは無視されます。

アクティブ/スタンバイとアクティブ/アクティブの両方のシナリオをサポートします。アクティブ装置からスタンバイ装置に引き継がれると、すべての SXP データが複製されます。

その他のガイドライン

Cisco TrustSec は、シングル コンテキスト モードおよびマルチ コンテキスト モード（システム コンテキスト モードを除く）で Smart Call Home 機能をサポートしています。

制限事項

- ASA は、単一の Cisco TrustSec ドメインでのみ相互運用するように設定できます。
- ASA は、デバイスの SGT 名のマッピングのスタティック コンフィギュレーションをサポートしていません。
- NAT は SXP メッセージでサポートされません。
- SXP はネットワークのエンフォースメント ポイントに IP-SGT マッピングを伝搬します。アクセス レイヤ スイッチがエンフォースメント ポイントと異なる NAT ドメインに属している場合、アップロードする IP-SGT マップは無効であり、実行デバイスに対する IP-SGT マッピング データベース検索から有効な結果を得ることはできません。その結果、ASA は実行デバイスにセキュリティ グループ対応セキュリティ ポリシーを適用できません。
- SXP 接続に使用する ASA にデフォルト パスワードを設定するか、またはパスワードを使用しないようにします。ただし、接続固有パスワードは SXP ピアではサポートされません。設定されたデフォルト SXP パスワードは導入ネットワーク全体で一貫している必要があります。接続固有パスワードを設定すると、接続が失敗する可能性があり、警告メッセージが表示されます。デフォルト パスワードを使用して接続を設定しても設定されていない場合、結果はパスワードなしで接続を構成した場合と同じです。
- SXP 接続のループは、デバイスにピアへの双方向の接続がある場合、またはデバイスがデバイスの単方向に接続されたチェーンの一部である場合に発生します （ASA は、データセンターのアクセス レイヤからのリソースの IP-SGT マッピングを学習できます。ASA はこれらのタグをダウンストリーム デバイスに伝搬する必要がある場合があります）。SXP 接続ループによって、SXP メッセージ転送の予期しない動作が発生する可能性があります。ASA が送信者および受信者として設定されている場合、SXP 接続ループが発生し、SXP データが最初にそのデータを送信したピアで受信される可能性があります。
- ASA のローカル IP アドレスを変更する場合は、すべての SXP ピアでピア リストが更新されていることを確認する必要があります。さらに、SXP ピアがその IP アドレスを変更する場合は、変更が ASA に反映されていることを確認する必要があります。
- 自動 PAC ファイル プロビジョニングはサポートされません。ASA 管理者は、ISE 管理インターフェイスの PAC ファイルを要求し、それを ASA にインポートする必要があります。PAC ファイルについては、「PAC ファイルの生成」（P.33-12）と「PAC ファイルのインポート」（P.33-16）を参照してください。

- PAC ファイルには有効期限があります。現在の PAC ファイルが期限切れになる前に更新された PAC ファイルをインポートする必要があります。そうしないと、ASA は環境データの更新を取得できません。
- セキュリティ グループが ISE で変更された（名前変更、削除など）場合、ASA は、変更されたセキュリティ グループに関連付けられた SGT またはセキュリティ グループ名を含む ASA セキュリティ ポリシーのステータスを変更しません。ただし、ASA は、それらのセキュリティ ポリシーが変更されたことを示す syslog メッセージを生成します。

  ISE の変更を含めるために、ASA でセキュリティ グループ テーブルを手動で更新する方法については、「環境データのリフレッシュ」（P.33-20）を参照してください。
- マルチキャスト タイプは ISE 1.0 ではサポートされていません。
- SXP 接続は、次の例に示すように、ASA によって相互接続された 2 つの SXP ピア間で初期化状態のままとなります。

  （SXP ピア A）- - - - - -（ASA）-（SXP ピア B）

  したがって、Cisco TrustSec と統合するように ASA を設定する場合は、SXP 接続を設定するために、ASA で、no-NAT、no-SEQ-RAND、MD5-AUTHENTICATION TCP オプションをイネーブルにする必要があります。SXP ピア間の SXP ポート TCP 64999 宛てのトラフィックに対して TCP 状態バイパス ポリシーを作成します。そして、適切なインターフェイスにポリシーを適用します。

  たとえば、次のコマンド セットは、TCP 状態バイパス ポリシーの ASA の設定方法を示しています。

```
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
 tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
 match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
service-policy global_policy global
```

- ASA 5585-X のハードウェア アーキテクチャは、通常のパケットのロード バランシングを最適な方法で行えるように設計されていますが、レイヤ 2 セキュリティ グループのタギング インポジションでタグ付けされたインライン パケットに適したアーキテクチャではありません。ASA 5585-X では、タグ付けされた着信インライン パケットを処理する際に、パフォーマンスが大きく低下することがあります。この問題は、タグ付けされたインライン パケットを他の ASA プラットフォームで処理する際や、タグ付けされていないパケットを ASA 5585-X で処理する際には発生しません。回避策の 1 つは、タグ付けされたインライン パケットが ASA 5585-X に最小限しか送信されないようにアクセス ポリシーを調整することです。こうすることで、タグ付けされたポリシーの適用をスイッチで行えるようになります。ASA 5585-X において、タグ付けされたパケットを受信する必要なく、IP アドレスをセキュリティ グループ タグにマッピングできるように SXP を使用する方法も回避策になります。

- ASASM は、レイヤ 2 セキュリティ グループのタギング インポジションをサポートしていません。

Cisco TrustSec と統合するための ASA の設定

Cisco TrustSec と統合するための AAA サーバの設定

Cisco TrustSec と統合するための ASA の設定の一環として、ISE と通信できるように ASA を設定する必要があります。

前提条件

- 参照先のサーバ グループは、RADIUS プロトコルを使用するように設定する必要があります。ASA に非 RADIUS サーバ グループを追加すると、設定は失敗します。
- ISE もユーザ認証に使用する場合は、ISE に ASA を登録したときに ISE で入力した共有秘密を取得します。この情報については、ISE 管理者に問い合わせてください。

Cisco TrustSec との統合のために ISE と通信するように ASA を設定するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Firewall] > [Identity By TrustSec] の順に選択します。

ステップ 2　ASA にサーバ グループを追加するには、[Manage in the Server Group Setup] 領域で [Manage] をクリックします。[Configure AAA Server Group] ダイアログ ボックスが表示されます。

ステップ 3　[AAA Server Group] フィールドに、ASA 用 ISE で作成したセキュリティ グループの名前を入力します。

ここで指定するサーバ グループ名は、ASA 用 ISE で作成したセキュリティ グループの名前と一致している必要があります。2 つのグループ名が一致しない場合、ASA は ISE と通信できません。この情報については、ISE 管理者に問い合わせてください。

ステップ 4　[Protocol] ドロップダウン リストから [RADIUS] を選択します。

[AAA Server Group] ダイアログ ボックスの残りのフィールドの入力については、「RADIUS サーバ グループの設定 」（P.29-15）を参照してください。

ステップ 5　[OK] をクリックします。ASA が、AAA サーバ グループのリストにグループを追加します。

ステップ 6　グループにサーバを追加するには、作成した AAA サーバ グループを選択し、[Selected Group] 領域（ペイン下部）の [Servers] で [Add] をクリックします。[Add AAA Server] ダイアログ ボックスが表示されます。

ステップ 7　[Interface Name] フィールドで、ISE サーバが存在するネットワーク インターフェイスを選択します。

ステップ 8　[Server Name or IP Address] フィールドに、ISE サーバの IP アドレスを入力します。

[AAA Server] ダイアログ ボックスの残りのフィールドの入力については、「グループへの RADIUS サーバの追加」（P.29-17）を参照してください。

ステップ 9　[OK] をクリックします。ASA が、AAA サーバのリストに ISE サーバを追加します。

ステップ 10　[Apply] をクリックして、Cisco TrustSec と統合するために、ISE サーバとサーバ グループの追加を保存します。

変更内容が実行コンフィギュレーションに保存されます。

PAC ファイルのインポート

Protected Access Credential（PAC）ファイルを ASA にインポートすると、ISE との接続が確立されます。チャネルが確立されると、ASA は、ISE を使用してセキュア RADIUS トランザクションを開始し、Cisco TrustSec 環境データをダウンロードします（具体的には、セキュリティ グループ テーブル）。セキュリティ グループ テーブルによって、SGT がセキュリティ グループ名にマッピングされます。セキュリティ グループの名前は ISE 上で作成され、セキュリティ グループをわかりやすい名前で識別できるようになります。

具体的には、チャネルは RADIUS トランザクションの前には確立されません。ASA は、認証用の PAC ファイルを使用して ISE の RADIUS トランザクションを開始します。

ヒント　PAC ファイルには、ASA および ISE がその間で発生する RADIUS トランザクションを保護できる共有キーが含まれています。このキーは、その機密性により、ASA に安全に保存する必要があります。

PAC ファイルをインポートすると、ファイルが ASCII 16 進形式に変換され、非インタラクティブ モードの ASA に送信されます。ファイルのインポートが成功すると、ASA が Cisco TrustSec 環境データを ISE からダウンロードします。ISE で設定したデバイス パスワードは必要ありません。

前提条件

- ASA が PAC ファイルを生成するには、ISE の認識された Cisco TrustSec ネットワーク デバイスとして ASA を設定する必要があります。ASA は、任意の PAC ファイルをインポートできますが、PAC ファイルは、正しく設定された ISE によって生成された場合にのみ ASA で動作します。詳細については、「ASA の ISE への登録」（P.33-11）を参照してください。
- ISE での PAC ファイルの生成時に PAC ファイルを暗号化するために使用されたパスワードを取得します。

  ASA は、PAC ファイルをインポートし、復号化する場合にこのパスワードが必要となります。

- ISE で生成された PAC ファイルにアクセスします。ASA は、フラッシュから PAC ファイルをインポートすることができます。また、TFTP、FTP、HTTP、HTTPS、SMB を介してリモート サーバからインポートすることも可能です （PAC ファイルは、インポート前に ASA フラッシュに配置されている必要はありません）。
- ASA のサーバ グループを設定します。

制限事項

- ASA がフェールオーバー設定の一部である場合、プライマリ ASA デバイスに PAC ファイルをインポートする必要があります。
- ASA がクラスタリング設定の一部である場合、マスター デバイスに PAC ファイルをインポートする必要があります。

PAC ファイルをインポートするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Firewall] > [Identity By TrustSec] の順に選択します。

ステップ 2　[Enable Security Exchange Protocol] チェック ボックスをオンにして、SXP をイネーブルにします。

ステップ 3　[Server Group Setup] 領域で、[Import PAC] をクリックします。[Import PAC] ダイアログ ボックスが表示されます。

ステップ 4　[Filename] フィールドで、次の形式の 1 つを使用して PAC ファイルのパスとファイル名を入力します。

- disk0：disk0 のパスおよびファイル名
- disk1：disk1 のパスおよびファイル名
- flash：フラッシュのパスおよびファイル名

ステップ 5　[Password] フィールドに、PAC ファイルを暗号化するためのパスワードを入力します。このパスワードは、デバイス クレデンシャルの一部として ISE で設定したパスワードとは関係ありません。

ステップ 6　確認のために [Confirm Password] フィールドにもう一度パスワードを入力します。

ステップ 7　[Import] をクリックします。

ステップ 8　[Apply] をクリックして、変更内容を保存します。

変更内容が実行コンフィギュレーションに保存されます。

Security Exchange Protocol の設定

Security Exchange Protocol（SXP）の設定では、ASA のプロトコルをイネーブルにし、次の SXP のデフォルト値を設定します。

- SXP 接続の送信元 IP アドレス
- SXP ピア間の認証パスワード
- SXP 接続の再試行間隔
- Cisco TrustSec SXP 調整期間

（注）　SXP を ASA 上で動作させるには、少なくとも 1 つのインターフェイスを UP/UP ステートにする必要があります。

現在、すべてのインターフェイスがダウンした状態で SXP がイネーブルになっている場合、ASA では、SXP が動作していない、あるいは SXP をイネーブルにできなかったことを示すメッセージは表示されません。**show running-config** コマンドを入力して設定を確認すると、コマンドの出力に次のメッセージが表示されます。

「`WARNING: SXP configuration in process, please wait for a few moments and try again.`」

これは汎用のメッセージであり、SXP が動作していない理由を具体的に述べたものではありません。

Cisco TrustSec と ASA の統合のためのデフォルト設定を設定するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Firewall] > [Identity By TrustSec] の順に選択します。

ステップ 2　[Enable Security Exchange Protocol] チェック ボックスをオンにして、SXP をイネーブルにします。SXP は、デフォルトで、ディセーブルに設定されています。

マルチ コンテキスト モードで、ユーザ コンテキストの SXP をイネーブルにします。

ステップ 3　[Default Source] フィールドに、SXP 接続のデフォルト ローカル IP アドレスを入力します。IP アドレスは、IPv4 または IPv6 アドレスを使用できます。

（注）　ピア IP アドレスが到達可能な発信インターフェイスの IP アドレスとして、ASA が SXP 接続のローカル IP アドレスを指定します。設定されたローカル アドレスが発信インターフェイスの IP アドレスと異なる場合、ASA は SXP ピアに接続できず、syslog メッセージを生成します。

ステップ 4　[Default password] フィールドに、SXP ピアによる TCP MD5 認証用のデフォルト パスワードを入力します。デフォルトでは、SXP 接続にパスワードは設定されていません。

パスワードは、162 文字までの暗号化された文字列または 80 文字までの ASCII キー ストリングとして指定できます。パスワードの暗号化レベルの設定は任意です。暗号化レベルを設定する場合、設定できるレベルは 1 つのみです。

- レベル 0：暗号化されていないクリア テキスト
- レベル 8：暗号化テキスト

ステップ 5　[Retry Timer] フィールドで、ASA 試行間のデフォルトの時間間隔を入力し、SXP ピア間の新しい SXP 接続を設定します。

ASA は、接続に成功するまで、新しい SXP ピアへの接続を試みます。ASA で確立されていない SXP 接続が存在する限り、再試行タイマーがトリガーされます。

再試行タイマーの値は 0 ～ 64000 秒の範囲で入力します。0 秒を指定すると、タイマーの期限が切れず、ASA は SXP ピアへの接続を試行しません。デフォルトでは、タイマー値は 120 秒です。

再試行タイマーが期限切れになると、ASA は接続データベースを順に検索し、切断されているか、または「保留中」状態の接続がデータベースに含まれている場合、ASA は再試行タイマーを再開します。

ステップ 6　[Reconcile Timer] フィールドに、調整タイマーのデフォルト値を入力します。

SXP ピアが SXP 接続を終了すると、ASA はホールドダウン タイマーを開始します。ホールドダウン タイマーの実行中に SXP ピアが接続されると、ASA は調整タイマーを開始します。次に、ASA は、SXP マッピング データベースを更新して、最新のマッピングを学習します。

調整タイマーの期限が切れると、ASA は、SXP マッピング データベースをスキャンして、古いマッピング エントリ（前回の接続セッションで学習されたエントリ）を識別します。ASA は、これらの接続を廃止としてマークします。調整タイマーが期限切れになると、ASA は、SXP マッピング データベースから廃止エントリを削除します。

調整タイマーの値は 1 ～ 64000 秒の範囲で入力します。デフォルトでは、タイマー値は 120 秒です。

（注） 0 を指定すると調整タイマーが開始されないため、このタイマーには 0 秒を指定できません。調整タイマーを実行できないようにすると、未定義の時間の古いエントリが維持され、ポリシーの適用の結果が予期せぬものとなります。

ステップ 7　[**Apply**] をクリックして、デフォルト設定内容を保存します。

変更内容が実行コンフィギュレーションに保存されます。

SXP 接続のピアの追加

ピア間の SXP 接続はポイントツーポイントであり、基礎となる転送プロトコルとして TCP を使用します。

SXP 接続のピアを追加するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Firewall] > [Identity By TrustSec] の順に選択します。

ステップ 2　必要に応じて、[Enable Security Exchange Protocol] チェック ボックスをオンにして SXP をイネーブルにします。

ステップ 3　[Add] をクリックします。[Add Connection] ダイアログ ボックスが表示されます。

ステップ 4　[Peer IP Address] フィールドに、SXP ピアの IPv4 アドレスまたは IPv6 アドレスを入力します。ピア IP アドレスは、ASA 発信インターフェイスからアクセスできる必要があります。

ステップ 5　（オプション）[Source IP Address] フィールドに、SXP 接続のローカル IPv4 または IPv6 アドレスを入力します。送信元 IP アドレスの指定は任意ですが、選択することにより設定ミスを防ぐことができます。

ステップ 6　[Password] ドロップダウン リストから、次の値の 1 つを選択し、SXP 接続に認証キーを使用するかどうかを指定します。

- Default：SXP 接続用に設定されたデフォルト パスワードを使用します。

  「Security Exchange Protocol の設定」（P.33-17）を参照してください。

- None：SXP 接続にパスワードを使用しません。

ステップ 7　（オプション）[Mode] ドロップダウン リストから、次の値の 1 つを選択し、SXP 接続のモードを指定します。

- Local：ローカル SXP デバイスを使用します。
- Peer：ピア SXP デバイスを使用します。

ステップ 8　[Role] ドロップダウン リストから、ASA が SXP 接続で送信者または受信者のいずれとして機能するかを指定します。

- Speaker：ASA は IP-SGT マッピングをアップストリーム デバイスに転送できます。
- Listener：ASA はダウンストリーム デバイスから IP-SGT マッピングを受信できます。

「ASA での送信者および受信者のロール」（P.33-7）を参照してください。

ステップ 9　[OK] をクリックします。ピアが、[COnnection Peers] リストに表示されます。

ステップ 10　[Apply] をクリックして設定値を保存します。

変更内容が実行コンフィギュレーションに保存されます。

環境データのリフレッシュ

ASA は、ISE からセキュリティ グループ タグ（SGT）名テーブルなどの環境データをダウンロードします。ASA で次のタスクを完了すると、ASA は、ISE から取得した環境データを自動的にリフレッシュします。

- ISE と通信するように AAA サーバを設定します。
- ISE から PAC ファイルをインポートします。
- Cisco TrustSec 環境データを取得するために ASA で使用する AAA サーバ グループを識別します。

通常、ISE からの環境データを手動でリフレッシュする必要はありません。ただし、セキュリティ グループが ISE で変更されることがあります。ASA セキュリティ グループ テーブルのデータをリフレッシュするまで、これらの変更は ASA に反映されません。そのため、ASA のデータをリフレッシュして、ISE でのセキュリティ グループの変更が確実に ASA に反映されるようにします。

ヒント　メンテナンス時間中に ISE のポリシー設定および ASA での手動データ リフレッシュをスケジュールすることを推奨します。このようにポリシー設定の変更を処理すると、セキュリティ グループ名が解決される可能性が最大化され、セキュリティ ポリシーが ASA で即時にアクティブ化されます。

前提条件

Cisco TrustSec の変更が ASA に適用されるように、ASA は、ISE の認識された Cisco TrustSec ネットワークとして設定される必要があり、ASA は PAC ファイルを正常にインポートする必要があります。

制限事項

- ASA が HA 設定の一部である場合、プライマリ ASA デバイスで環境データをリフレッシュする必要があります。
- ASA がクラスタリング設定の一部である場合、マスター デバイスで環境データをリフレッシュする必要があります。

環境データをリフレッシュするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Firewall] > [Identity By TrustSec] の順に選択します。

ステップ 2　[Server Group Setup] 領域で、[Refresh Environment Data] をクリックします。

ASA は、ISE からの Cisco TrustSec 環境データをリフレッシュし、設定されたデフォルト値に調整タイマーをリセットします。

セキュリティ ポリシーの設定

Cisco TrustSec ポリシーは、多くの ASA 機能に組み込むことができます。拡張 ACL を使用する機能（この章でサポート対象外としてリストされている機能を除く）で Cisco TrustSec を使用できます。拡張 ACL に、従来のネットワークベースのパラメータとともにセキュリティ グループ引数を追加できるようになりました。

- アクセス ルールを設定する方法については、ファイアウォール コンフィギュレーション ガイドを参照してください。
- ACL で使用できるセキュリティ グループ オブジェクト グループを設定する方法については、「セキュリティ グループ オブジェクト グループの設定」（P.17-6）を参照してください。

たとえば、アクセス ルールは、ネットワーク情報を使用してインターフェイスのトラフィックを許可または拒否します。Cisco TrustSec では、セキュリティ グループに基づいてアクセスを制御できます。たとえば、sample_securitygroup1 10.0.0.0 255.0.0.0 のアクセス ルールを作成できます。これは、セキュリティ グループがサブネット 10.0.0.0/8 上のどの IP アドレスを持っていてもよいことを意味します。

セキュリティ グループの名前（サーバ、ユーザ、管理対象外デバイスなど）、ユーザベース属性、および従来の IP アドレスベースのオブジェクト（IP アドレス、Active Directory オブジェクト、および FQDN）の組み合わせに基づいてセキュリティ ポリシーを設定できます。セキュリティ グループ メンバーシップはロールを超えて拡張し、デバイスと場所属性を含めることができます。また、セキュリティ グループ メンバーシップは、ユーザ グループ メンバーシップに依存しません。

レイヤ 2 セキュリティ グループのタギング インポジションの設定

Cisco TrustSec は、各ネットワーク ユーザおよびリソースの特定と認証を行い、セキュリティ グループ タグ（SGT）と呼ばれる 16 ビットの番号を割り当てます。この ID は、ネットワーク ホップ間で順番に伝搬されます。これにより、ASA、スイッチ、ルータなどの任意の中間デバイスで、この ID タグに基づいてポリシーを適用できます。

SGT とイーサネット タギング（レイヤ 2 SGT インポジションとも呼ばれる）を利用すると、ASA でシスコ独自のイーサネット フレーミング（EtherType 0x8909）を使用して、イーサネット インターフェイスでセキュリティ グループ タグを送受信できます。これにより、送信元のセキュリティ グループ タグをプレーン テキストのイーサネット フレームに挿入できます。ASA は、インターフェイスごとの手動設定に基づいて、発信パケットにセキュリティ グループ タグを挿入し、着信パケットのセキュリティ グループ タグを処理します。この機能を使用することで、ネットワーク デバイス間におけるエンドポイント ID の伝搬をインラインかつホップバイホップで実行できます。また、各ホップ間でシームレスなレイヤ 2 SGT インポジションを実現できます。

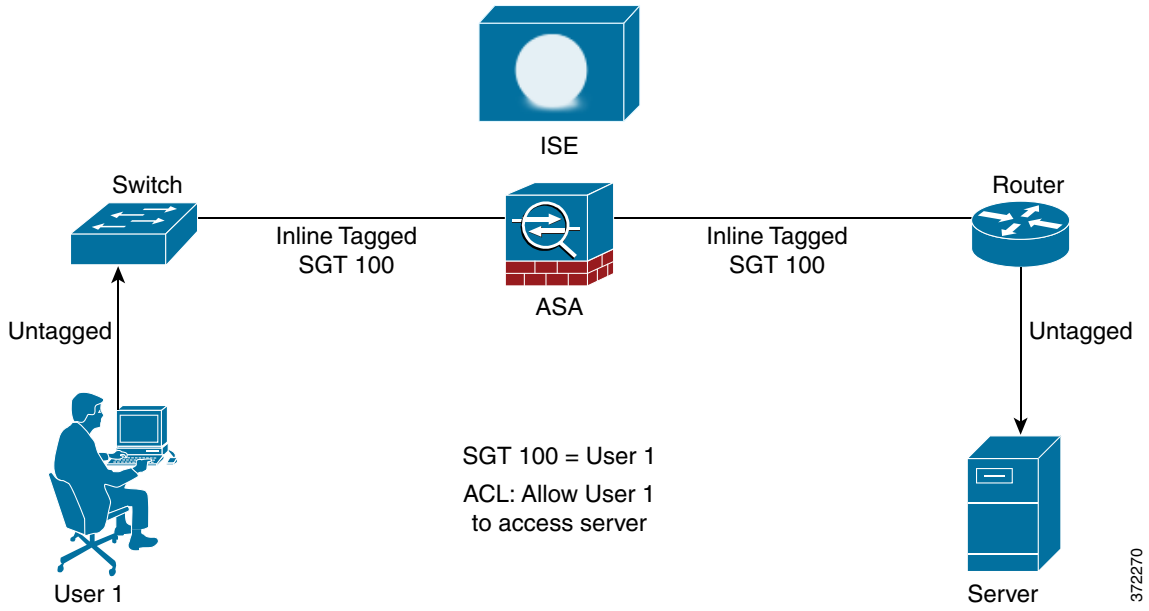
制限事項

- 物理インターフェイス、VLAN インターフェイス、ポート チャネル インターフェイス、および冗長インターフェイスでのみサポートされます。
- 論理インターフェイスまたは仮想インターフェイス（BVI など）ではサポートされません。

- SAP ネゴシエーションおよび MACsec を使用したリンク暗号化はサポートされていません。
- フェールオーバー リンクではサポートされません。
- クラスタ制御リンクではサポートされません。
- SGT が変更されても、ASA は既存のフローを再分類しません。以前の SGT に基づいて行われたポリシーに関する決定が、フローのライフサイクルにわたって適用され続けます。ただし、ASA は、パケットが以前の SGT に基づいて分類されたフローに属していても、SGT の変更内容を出力パケットに即座に反映できます。

図 33-3 に、レイヤ 2 SGT インポジションの一般的な例を示します。

図 33-3　　レイヤ 2 SGT インポジション



使用シナリオ

表 33-3 で、この機能を設定した場合の入力トラフィックの予期される動作について説明します。

表 33-3　　入力トラフィック

インターフェイス コンフィギュレーション	タグ付きの受信パケット	タグのない受信パケット
コマンドが発行されない。	パケットがドロップされる。	SGT 値が IP-SGT マネージャから取得される。
cts manual コマンドが発行される。	SGT 値が IP-SGT マネージャから取得される。	SGT 値が IP-SGT マネージャから取得される。

表 33-3　入力トラフィック

インターフェイス コンフィギュレーション	タグ付きの受信パケット	タグのない受信パケット
cts manual コマンドと **policy static sgt** *sgt_number* コマンドが両方とも発行される。	SGT 値が **policy static sgt** *sgt_number* コマンドで取得される。	SGT 値が **policy static sgt** *sgt_number* コマンドで取得される。
cts manual コマンドと **policy static sgt** *sgt_number* **trusted** コマンドが両方とも発行される。	SGT 値がパケットのインライン SGT から取得される。	SGT 値が **policy static sgt** *sgt_number* コマンドで取得される。

（注）　IP-SGT マネージャと一致する IP-SGT マッピングが存在しない場合、予約されている SGT 値（「不明」を表す「0x0」）が使用されます。

表 33-4 で、この機能を設定した場合の出力トラフィックの予期される動作について説明します。

表 33-4　出力トラフィック

インターフェイス コンフィギュレーション	送信パケットのタグの有無
コマンドが発行されない。	タグなし
cts manual コマンドが発行される。	タグ付き
cts manual コマンドと **propagate sgt** コマンドが両方とも発行される。	タグ付き
cts manual コマンドと **no propagate sgt** コマンドが両方とも発行される。	タグなし

表 33-5 で、この機能を設定した場合の to-the-box トラフィックと from-the-box トラフィックの予期される動作について説明します。

表 33-5　to-the-box トラフィックと from-the-box トラフィック

インターフェイス コンフィギュレーション	受信パケットのタグの有無
to-the-box トラフィック用の入力インターフェイスで、コマンドが発行されない。	パケットがドロップされる。
to-the-box トラフィック用の入力インターフェイスで、**cts manual** コマンドが発行される。	パケットは受け入れられるが、ポリシーの適用や SGT の伝搬は行われない。
cts manual コマンドが発行されない。または、from-the-box トラフィック用の出力インターフェイスで、**cts manual** コマンドと **no propagate sgt** コマンドが両方とも発行される。	タグなしパケットは送信されるが、ポリシーの適用は行われない。SGT 値が IP-SGT マネージャから取得される。
cts manual コマンドが発行される。または、from-the-box トラフィック用の出力インターフェイスで、**cts manual** コマンドと **propagate sgt** コマンドが両方とも発行される。	タグ付きパケットが送信される。SGT 値が IP-SGT マネージャから取得される。

（注）　IP-SGT マネージャと一致する IP-SGT マッピングが存在しない場合、予約されている SGT 値（「不明」を表す「0x0」）が使用されます。

SGT とイーサネット タギングのイネーブル化

SGT とイーサネット タギング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　ASDM で、次のオプションから 1 つを選択します。

- [Configuration] > [Device Setup] > [Interfaces] > [Add Interface] > [Advanced]
- [Configuration] > [Device Setup] > [Interfaces] > [Add Redundant Interface] > [Advanced]
- [Configuration] > [Device Setup] > [Interfaces] > [Add Ethernet Interface] > [Advanced]

ステップ 2　[Secure Group Tagging] 領域で、[Enable secure group tagging for Cisco TrustSec] チェック ボックスをオンにします。

インターフェイスでのセキュリティ グループ タグの伝搬

インターフェイスでのセキュリティ タグの伝搬をイネーブルまたはディセーブルにするには、次の手順を実行します。

ステップ 1　ASDM で、次のオプションから 1 つを選択します。

- [Configuration] > [Device Setup] > [Interfaces] > [Add Interface] > [Advanced]
- [Configuration] > [Device Setup] > [Interfaces] > [Add Redundant Interface] > [Advanced]
- [Configuration] > [Device Setup] > [Interfaces] > [Add Ethernet Interface] > [Advanced]

ステップ 2　[Secure Group Tagging] 領域で、[Enable secure group tagging for Cisco TrustSec] チェック ボックスをオンにします。

ステップ 3　[Tag egress packets with service group tags] チェック ボックスをオンにします。

手動で設定した Cisco TrustSec リンクへのポリシーの適用

手動で設定した CTS リンクにポリシーを適用するには、次の手順を実行します。

ステップ 1　ASDM で、次のオプションから 1 つを選択します。

- [Configuration] > [Device Setup] > [Interfaces] > [Add Interface] > [Advanced]
- [Configuration] > [Device Setup] > [Interfaces] > [Add Redundant Interface] > [Advanced]
- [Configuration] > [Device Setup] > [Interfaces] > [Add Ethernet Interface] > [Advanced]

ステップ 2　[Secure Group Tagging] 領域で、[Enable secure group tagging for Cisco TrustSec] チェック ボックスをオンにします。

ステップ 3　[Tag egress packets with service group tags] チェック ボックスをオンにします。

ステップ 4　[Add a static secure group tag to all ingress packets] チェック ボックスをオンにします。

ステップ 5　セキュリティ グループ タグの番号を入力します。有効な値の範囲は 2 ～ 65519 です。

ステップ 6　[This is a trusted interface. Do not override existing secure group tags] チェック ボックスをオンにします。

ステップ 7　[OK] をクリックして設定を保存し、[Advanced] タブを閉じます。

IP-SGT バインディングの手動設定

IP-SGT バインディングを手動で設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall Identity by TrustSec] を選択します。

ステップ 2　[SGT Map Setup] 領域で、[Add] をクリックします （既存の IP-SGT バインディングを変更するには、対象のバインディングを選択して [Edit] をクリックします。既存の IP-SGT バインディングを削除するには、対象のバインディングを選択して [Delete] をクリックします）。

[Add SGT Map] ダイアログ ボックスが表示されます。

ステップ 3　SGT マップの IP アドレスと SGT 値を該当するフィールドに入力します。SGT 値の有効な値の範囲は 2 ～ 65519 です。

ステップ 4　[OK] をクリックし、続いて [Apply] をクリックします。

新たに設定した IP-SGT バインディングが [SGT Map Setup] 領域に表示されます。

Cisco TrustSec に対する AnyConnect VPN のサポート

ASA バージョン 9.3（1）は、VPN セッションのセキュリティ グループ タグを完全にサポートしています。セキュリティ グループ タグ（SGT）は、外部 AAA サーバを利用して VPN セッションに割り当てることができます。また、ローカル ユーザ データベースの設定によって割り当てることも可能です。さらに、レイヤ 2 イーサネット経由で、Cisco TrustSec システムを介してこのタグを伝搬することができます。AAA サーバが SGT を提供できない場合には、セキュリティ グループ タグをグループ ポリシーで利用したり、ローカル ユーザが利用したりすることができます。

AAA サーバの属性に、VPN ユーザに割り当てるための SGT が含まれていない場合、ASA はデフォルトのグループ ポリシーの SGT を使用します。グループ ポリシーに SGT が含まれていない場合は、タグ 0x0 が割り当てられます。

サーバに接続しているリモート ユーザのための一般的な手順

1. ユーザが ASA に接続します。

2. ASA が ISE の AAA 情報を要求します。この情報に SGT が含まれている場合があります。ASA は、ユーザのトンネル トラフィックに対する IP アドレスの割り当ても行います。
3. ASA が AAA 情報を使用して認証を行い、トンネルを作成します。
4. ASA が AAA 情報から取得した SGT と割り当て済みの IP アドレスを使用して、レイヤ 2 ヘッダー内に SGT を追加します。
5. SGT を含むパケットが Cisco TrustSec ネットワーク内の次のピア デバイスに渡されます。

ローカル ユーザおよびグループへの SGT の追加

SGT タグを追加するには、ASDM で、

- [Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] を選択します。ユーザの追加または編集を行い、[VPN Policy] パネルを選択して、セキュリティ グループ タグ（STG）の値を入力します。
- [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択し、[General] タブで [More Options] を展開して、[Security Group Tag (SGT)] に値を入力します。

Cisco TrustSec のモニタリング

ASA で Cisco TrustSec をモニタリングするには、ASDM で次のパスから 1 つを選択します。

パス	目的
[Monitoring] > [Properties] > [Identity By TrustSec] > [SXP Connections]	Cisco TrustSec インフラストラクチャおよび SXP コマンドの設定済みのデフォルト値を表示します。
[Monitoring] > [Properties] > [Connections]	すべての SXP 接続のデータを表示します。セキュリティ グループ テーブル値、セキュリティ グループの名前、IP アドレスでデータが表示されるように、IP アドレス セキュリティ グループのテーブル マップ エントリをフィルタリングします。
[Monitoring] > [Properties] > [Identity By TrustSec] > [Environment Data]	ASA のセキュリティ グループ テーブルに含まれる Cisco TrustSec 環境情報を表示します。

パス	目的
[Monitoring] > [Properties] > [Identity By TrustSec] > [IP Mapping]	データ パスに保持されている IP アドレス セキュリティ グループのテーブル マップ データベースから IP アドレス セキュリティ グループのテーブル マップ エントリを表示します。セキュリティ グループ テーブル値、セキュリティ グループの名前、IP アドレスでデータが表示されるように、IP アドレス セキュリティ グループのテーブル マップ エントリをフィルタリングします。 **ヒント**　選択したセキュリティ グループ オブジェクトが ACL で使用されている場所、もしくは別のセキュリティ グループ オブジェクトにネストされている場所を表示するには、[Where Used] をクリックします。
[Monitoring] > [Properties] > [Identity By TrustSec] > [PAC]	ISE から ASA にインポートされた PAC ファイルに関する情報を表示します。PAC ファイルの有効期限が切れた場合、または有効期限切れ 30 日以前を過ぎると警告メッセージが表示されます。

その他の関連資料

参照先	説明
http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html	企業向けの Cisco TrustSec システムおよびアーキテクチャが説明されています。
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_DesignZone_TrustSec.html	コンポーネントの設計ガイドへのリンクなど、Cisco TrustSec ソリューションを企業に導入する場合の手順が紹介されています。
http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/trustsec/solution_overview_c22-591771.pdf	Cisco TrustSec ソリューションを ASA、スイッチ、ワイヤレス LAN（WLAN）コントローラ、およびルータと共に使用する場合の概要が紹介されています。
http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html	Cisco TrustSec プラットフォームのサポート一覧が掲載されています。Cisco TrustSec ソリューションをサポートしているシスコ製品を確認できます。

Cisco TrustSec 統合の機能履歴

表 33-6 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定

の ASDM リリースは一覧には含まれていません。

表 33-6　Cisco TrustSec 統合の機能履歴

機能名	プラットフォーム リリース	機能情報
Cisco TrustSec の統合	9.0(1)	Cisco TrustSec は、既存の ID 認識型インフラストラクチャを基盤とするアクセス コントロールです。ネットワーク デバイス間のデータ機密性保持を目的としており、セキュリティ アクセス サービスを 1 つのプラットフォーム上で統合します。Cisco TrustSec 機能では、実行デバイスはユーザ属性とエンドポイント属性の組み合わせを使用して、ロールベースおよびアイデンティティベースのアクセス コントロールを決定します。 このリリースでは、ASA に Cisco TrustSec が統合されており、セキュリティ グループに基づいてポリシーが適用されます。Cisco TrustSec ドメイン内のアクセス ポリシーは、トポロジには依存しません。ネットワーク IP アドレスではなく、送信元および宛先のデバイスのロールに基づいています。 ASA は、セキュリティ グループに基づくその他のタイプのポリシー（アプリケーション インスペクションなど）に対しても Cisco TrustSec 機能を活用できます。たとえば、設定するクラス マップの中に、セキュリティ グループに基づくアクセス ポリシーを入れることができます。 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [Identity By TrustSec] [Configuration] > [Firewall] > [Objects] > [Security Groups Object Groups] [Configuration] > [Firewall] > [Access Rules] > [Add Access Rules] [Monitoring] > [Properties] > [Identity By Tag]
レイヤ 2 セキュリティ グループのタグ インポジション	9.3(1)	セキュリティ グループ タギングをイーサネット タギングと組み合わせて使用して、ポリシーを適用できるようになりました。SGT とイーサネット タギング（レイヤ 2 SGT インポジションとも呼ばれる）を利用すると、ASA でシスコ独自のイーサネット フレーミング（EtherType 0x8909）を使用して、イーサネット インターフェイスでセキュリティ グループ タグを送受信できます。これにより、送信元のセキュリティ グループ タグをプレーン テキストのイーサネット フレームに挿入できます。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Interfaces] > [Add Interface] > [Advanced] [Configuration] > [Device Setup] > [Interfaces] > [Add Redundant Interface] > [Advanced] [Configuration] > [Device Setup] > [Add Ethernet Interface] > [Advanced]

ASA および Cisco Mobile Enablement

ASA および Cisco Mobile Enablement

Cisco ASA は、Cisco Identity Services Engine（ISE）のコンポーネントである Cisco Mobile Enablement（ME）によって管理されるモバイル デバイスに企業ネットワークへの構外アクセスを提供するエッジ デバイスです。このロールでは、ASA は ISE ME のネットワーク アクセス デバイス（NAD）として、モバイル デバイスの認証、登録、定期的なチェックインのプロキシとして動作します。また、構外、リモート モバイル デバイス（AnyConnect Device Management クライアント）とモバイル デバイス マネージャ（ISE Mobile Enablement サーバ）間のセキュアな通信パスを提供します。この結果、構外モバイル デバイスが AnyConnect クライアント アプリケーションを実行し、構外モバイル デバイスとまったく同様にモバイル デバイス管理に参加できます。

この項では、ASA 固有の構成と動作のみについて説明します。

次を指定して ME プロキシ機能を ASA で設定します。

- AnyConnect ME クライアントが登録およびチェックイン要求に使用する ASA インターフェイスおよびポート
- クライアントの認証に使用する AAA サーバ 通常は ISE Mobile Enablement ソリューションの一部である RADIUS サーバ
- Mobile Enablement サーバに対する ASA の識別および認証に使用するトラスト ポイント

ASA MDM プロキシのガイドラインと制限事項

- ME プロキシ機能はシングル コンテキスト ルータ モードのみでサポートされます。
- ME プロキシには ASA ライセンス要件はありません。ME のライセンスは ISE で有効になります。

- モバイル デバイス上で実行される AnyConnect ME クライアントは、ユーザがオンプレミス（社内ネットワーク）か構外（パブリック ネットワーク）にかかわらず、同じ URI を使用して ME サーバと通信します。これをサポートするには、ネットワークの DNS 設定が、構外をサポートするには ME URI を ASA ゲートウェイに、オンプレミスをサポートするには ISE ポリシー サーバ ノード（PSN）に解決する必要があります。
- AnyConnect ME クライアントと ASA、ASA と ISE ME サーバの間の認証にはデジタル証明書が必要です。ASA ME プロキシを組み込む Mobile Enablement ソリューションを計画および設定する場合は、次の点を考慮してください。
  - ISE ポリシー サービス ノードに ASA を認証する証明書では、複数のプロキシ デバイスの表現を同時にイネーブルにする必要があります。
  - 登録時に SCEP の結果として取得するモバイル デバイスの AnyConnect クライアント証明書は、構外の場合は ASA に、オンプレミスの場合は ISE に認証するよう定義する必要があります。同様に、同じ方法で受け取った Applie iOS モバイル デバイスの追加 Apple iOS のクライアント証明書は同様に動作する必要があります。
  - [Subject Alternative Name (SAN)] フィールドで ASA と ISE の両方のサーバの FQDN を指定することで、両方のサーバをモバイル デバイスのクライアントに認証する 1 つの証明書を定義できます。
- ISE My Devices ポータルへのアクセスは、構外で管理されるモバイル デバイスでは利用できません。このポータルにアクセスするには、モバイル デバイスのユーザがオンプレミスである必要があります。

MDM プロキシとしての ASA の設定

はじめる前に

- 認証およびアカウンティングのために ISE AAA RADIUS サーバにアクセスするように RADIUS サーバ グループを設定する必要があります。
- AnyConnect クライアントに代わって ISE MDM サーバに ASA を認証するようにトラストポイントを設定する必要があります。

手順

ステップ 1　[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [MDM Server Groups] を選択します。

ステップ 2　[Access Interface] フィールドを設定します。

- **MDM サーバ アクセス インターフェイス**：クライアントから MDM プロキシ要求を保守するインターフェイスを選択します。
- **ポートの登録**：選択されたインターフェイスで MDM のクライアント認証および登録要求に使用するポートを指定します。デフォルトはポート 443 です。
- **チェックイン ポート**：（オプション）選択されたインターフェイスで MDM チェックイン要求に使用する 1 ～ 65535 のポートを指定します。このポートは、他のサービスが使用することはできません。

ステップ 3　[Radius Server Groups] フィールドを設定します。

- **認証サーバ グループ**：MDM クライアント認証に使用する認証サーバ グループを指定します。事前設定されているサーバ グループを選択するか、または新しいサーバ グループを指定します。

- **アカウンティング サーバ グループ**：さまざまな MDM クライアントのアクションの記録に使用するアカウンティング サーバ グループを指定します。事前設定されているサーバ グループを選択するか、または新しいサーバ グループを指定します。

ステップ 4　[MDM Server Authentication] フィールドを設定します。

- **デバイス証明書**：MDM サーバに対してそれ自体を認証するために ASA により使用されるトラストポイントを指定します（ISE）。事前設定されているサーバ グループを選択するか、[New] を選択して [Create Radius Server Group for MDM Proxy] ダイアログを開き、ISE MDM RADIUS サーバを設定します。
- **パスワードの期限切れ**：警告を発行するには、パスワードが失効するまでの日数を指定します。

ステップ 5　[OK] をクリックします。

Mobile Enablement プロキシのアクティビティのモニタリング

ASA の Mobile Enablement の統計情報を表示するには、ASDM で次のパスを選択します。

[Monitoring] > [VPN] > [VPN Statistics] > [MDM Proxy Statistics]

ASA Mobile Enablement プロキシの機能履歴

機能名	プラットフォーム リリース	機能情報
モバイル導入プロキシ	9.3(1)	モバイル導入プロキシ（ISE モバイル導入ソリューションのコンポーネント）を使用すると、オフプレミスのモバイル デバイスをオンプレミスのモバイル デバイスとまったく同じ方法で管理できるようになります。 画面、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [MDM Proxy] を導入しました。

デジタル証明書

この章では、デジタル証明書の設定方法について説明します。

デジタル証明書の概要

デジタル証明書は、認証に使用されるデジタル ID を保持しています。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。

デジタル証明書を使用して認証を行う場合は、ASA に 1 つ以上の ID 証明書と、その発行元の CA 証明書が必要です。この設定では、複数のアイデンティティ、ルート、および証明書の階層が許可されます。ASA では CRL（認証局の失効リストとも呼ばれます）に照らしてサードパーティの証明書を検証します。検証は、ID 証明書から下位証明書チェーンの認証局までさかのぼって行われます。

次に、使用可能な各種デジタル証明書について説明します。

- *CA 証明書*は、他の証明書に署名するために使用されます。これは自己署名され、*ルート証明書*と呼ばれます。別の CA 証明書により発行される証明書は、*下位証明書*と呼ばれます。
- *ID 証明書*は、特定のシステムまたはホストの証明書です。この証明書も CA により発行されます。

- *コード署名者証明書*は、コードに署名するためのデジタル署名を作成する際に使用される特殊な証明書であり、署名されたコードそのものが証明書の作成元を示しています。

ローカル CA は、ASA の独立認証局機能を統合したもので、証明書の配布と、発行された証明書に対するセキュアな失効チェックを行います。Web サイトのログイン ページからユーザ登録を行う場合には、ローカル CA により実現されるセキュアで設定可能な内部認証局機能によって、証明書の認証を行うことができます。

（注）CA 証明書および ID 証明書は、サイトツーサイト VPN 接続およびリモート アクセス VPN 接続の両方に適用されます。このマニュアルに記載の手順は、ASDM GUI でリモート アクセス VPN を使用する場合の手順です。

デジタル証明書は、認証に使用されるデジタル ID を保持しています。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。

デジタル証明書を使用して認証を行う場合は、ASA に 1 つ以上の ID 証明書と、その発行元の CA 証明書が必要です。この設定では、複数のアイデンティティ、ルート、および証明書の階層が許可されます。次に、使用可能な各種デジタル証明書について説明します。

- *CA 証明書*は、他の証明書に署名するために使用されます。これは自己署名され、*ルート証明書*と呼ばれます。
- 別の CA 証明書により発行される証明書は、*下位証明書*と呼ばれます。

CA は、証明書要求の管理とデジタル証明書の発行を行います。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。デジタル証明書には、ユーザまたはデバイスの公開キーのコピーも含まれています。CA は、信頼できるサードパーティ（VeriSign など）の場合もあれば、組織内に設置したプライベート CA（インハウス CA）の場合もあります。

ヒント　証明書コンフィギュレーションおよびロード バランシングの例は、次の URL を参照してください。https://supportforums.cisco.com/docs/DOC-5964

公開キー暗号化

デジタル署名は、公開キー暗号化によってイネーブルになり、デバイスおよびユーザを認証する手段です。RSA 暗号化システムなどの Public Key Cryptography では、各ユーザは、公開キーと秘密キーの両方を含むキー ペアを使用します。これらのキーは、補足として機能し、一方で暗号化されたものは、もう一方で復号化できます。

簡単に言えば、データが秘密キーで暗号化されたとき、署名が形成されます。署名はデータに付加されて受信者に送信されます。受信者は送信者の公開キーをデータに適用します。データとともに送信された署名が、公開キーをデータに適用した結果と一致した場合、メッセージの有効性が確立されます。

このプロセスは、受信者が送信者の公開キーのコピーを持っていること、およびその公開キーが送信者になりすました別人のものではなく、送信者本人のものであることを受信者が強く確信していることに依存しています。

通常、送信者の公開キーは外部で取得するか、インストール時の操作によって取得します。たとえば、ほとんどの Web ブラウザでは、いくつかの CA のルート証明書がデフォルトで設定されています。VPN の場合、IKE プロトコルは IPsec のコンポーネントであり、デジタル署名を使用してピア デバイスを認証した後で、セキュリティ アソシエーションをセットアップできます。

証明書のスケーラビリティ

デジタル証明書がない場合、通信するピアごとに各 IPsec ピアを手動で設定する必要があります。そのため、ネットワークにピアを新たに追加するたびに、安全に通信するために各ピアで設定変更を行わなければなりません。

デジタル証明書を使用している場合、各ピアは CA に登録されます。2 つのピアは、通信を試みるときに、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアがネットワークに追加された場合は、そのピアを CA に登録するだけで済みます。他のピアを修正する必要はありません。新しいピアが IPSec 接続を試みると、証明書が自動的に交換され、そのピアの認証ができます。

CA を使用した場合、ピアはリモート ピアに証明書を送り、公開キー暗号化を実行することによって、そのリモート ピアに対して自分自身を認証します。各ピアから、CA によって発行された固有の証明書が送信されます。このプロセスが機能を果たすのは、関連付けられているピアの公開キーが各証明書にカプセル化され、各証明書が CA によって認証され、参加しているすべてのピアによって CA が認証権限者として認識されるためです。このプロセスは、RSA 署名付きの IKE と呼ばれます。

ピアは、証明書が期限満了になるまで、複数の IPSec セッションに対して、および複数の IPSec ピア宛てに証明書を送り続けることができます。証明書が期限満了になったときは、ピアの管理者は新しい証明書を CA から入手する必要があります。

CA は、IPSec に参加しなくなったピアの証明書を無効にすることもできます。無効にされた証明書は、他のピアからは有効な証明書とは認識されなくなります。無効にされた証明書は CRL に記載され、各ピアは別のピアの証明書を受け取る前に、CRL をチェックします。

CA の中には、実装の一部として RA を持つものもあります。RA は CA のプロキシの役割を果たすサーバであるため、CA が使用できないときも CA 機能は継続しています。

キー ペア

キー ペアとは、次の特性を持つ RSA キーです。

- RSA キーは SSH や SSL に使用できます。
- SCEP 登録は、RSA キーの証明書をサポートしています。
- キー生成では、RSA キーの最大キー係数は 2048 ビットです。デフォルト サイズは 1024 です。1024 ビットを超える RSA キー ペアを持つ ID 証明書を使用している複数の SSL 接続によって、ASA での CPU 使用率が高くなり、クライアントレス ログインが拒否される可能性があります。
- 署名操作でサポートされているキーの最大サイズは 4096 ビットです。キー サイズは 2048 以上を使用することをお勧めします。
- 署名にも暗号化にも使用できる汎用 RSA キー ペアを生成することも、署名用と暗号化用に別々の RSA キー ペアを生成することもできます。SSL では署名用ではなく暗号化用のキーが使用されるので、署名用と暗号化用にキーを分けると、キーが公開される頻度を少なくすることができます。ただし、IKE では暗号化用ではなく署名用のキーが使用されます。キーを用途別に分けることで、キーの公開頻度が最小化されます。

トラストポイント

トラストポイントを使用すると、CA と証明書の管理とトレースができます。トラストポイントとは、CA または ID ペアを表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。

トラストポイントの定義が完了したら、CA の指定を必要とするコマンドで、名前によってトラストポイントを参照できます。トラストポイントは複数設定できます。

（注）　Cisco ASA に同じ CA を共有するトラストポイントが複数ある場合、CA を共有するトラストポイントのうち、ユーザ証明書の検証に使用できるのは 1 つだけです。CA を共有するどのトラストポイントを使用して、その CA が発行したユーザ証明書を検証するかを制御するには、**support-user-cert-validation** コマンドを使用します。

自動登録の場合は、登録 URL がトラストポイントに設定されている必要があり、また、トラストポイントが示す CA がネットワーク上で使用可能であり、SCEP をサポートしている必要があります。

キー ペアと、トラストポイントに関連付けられている発行済み証明書は、PKCS12 形式でエクスポートとインポートができます。この形式は、異なる ASA 上のトラストポイント コンフィギュレーションを手動でコピーする場合に便利です。

証明書の登録

ASA は、トラストポイントごとに 1 つの CA 証明書が必要で、セキュリティ アプライアンス自体には、トラストポイントで使用するキーのコンフィギュレーションに応じて 1 つまたは 2 つの証明書が必要です。トラストポイントが署名と暗号化に別々の RSA キーを使用する場合、ASA には署名用と暗号化用の 2 つの証明書が必要になります。署名用と暗号化用のキーが同じである場合、必要な証明書は 1 つだけです。

ASA は、SCEP を使用した自動登録と、base-64-encoded 証明書を直接端末に貼り付けられる手動登録をサポートしています。サイトツーサイト VPN の場合は、各 ASA を登録する必要があります。リモート アクセス VPN の場合は、各 ASA と各リモート アクセス VPN クライアントを登録する必要があります。

SCEP 要求のプロキシ

ASA は、AnyConnect とサードパーティ CA 間の SCEP 要求のプロキシとして動作することができます。プロキシとして動作する場合に必要なのは CA が ASA からアクセス可能であることのみです。ASA のこのサービスが機能するには、ASA が登録要求を送信する前に、ユーザが AAA でサポートされているいずれかの方法を使用して認証されている必要があります。また、ホスト スキャンおよびダイナミック アクセス ポリシーを使用して、登録資格のルールを適用することもできます。

ASA では、AnyConnect SSL または IKEv2 VPN セッションでのみこの機能をサポートしています。これは、Cisco IOS CS、Windows Server 2003 CA、および Windows Server 2008 CA を含む、すべての SCEP 準拠 CA をサポートしています。

クライアントレス（ブラウザベース）でのアクセスは SCEP プロキシをサポートしていませんが、WebLaunch（クライアントレス起動 AnyConnect）はサポートしていません。

ASA では、証明書のポーリングはサポートしていません。

ASA はこの機能に対するロード バランシングをサポートしています。

失効チェック

証明書は発行されると、一定期間有効です。CA は、安全上の問題や名前またはアソシエーションの変更などの理由で、期限が切れる前に証明書を無効にすることがあります。CA は、無効になった証明書の署名付きリストを定期的に発行します。失効確認をイネーブルにすることにより、CA が認証にその証明書を使用するたびに、その証明書が無効にされていないかどうか、ASA によってチェックされます。

失効確認をイネーブルにすると、PKI 証明書検証プロセス時に ASA によって証明書の失効ステータスがチェックされます。これには、CRL チェック、OCSP、またはその両方が使用されます。OCSP は、最初の方式がエラーを返した場合に限り使用されます（たとえば、サーバが使用不可であることを示すエラー）。

CRL チェックを使用すると、ASA によって、無効になった（および失効解除された）証明書とその証明書シリアル番号がすべてリストされている CRL が取得、解析、およびキャッシュされます。ASA では CRL（認証局の失効リストとも呼ばれます）に基づいて証明書を検証します。検証は、ID 証明書から下位証明書チェーンの認証局までさかのぼって行われます。

OCSP は、検証局に特定の証明書のステータスを問い合わせ、チェックを検証局が扱う範囲に限定するため、よりスケーラブルな方法を提供します。

サポート対象の CA サーバ

ASA は次の CA サーバをサポートしています。

Cisco IOS CS、ASA ローカル CA、およびサードパーティの X.509 準拠 CA ベンダー（次のベンダーが含まれますが、これらに限定はされません）。

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRL

CRL は、有効期間内の証明書が発行元の CA によって無効にされているかどうかを ASA が判断するための 1 つの方法です。CRL コンフィギュレーションは、トラストポイントのコンフィギュレーションの一部です。

証明書を認証するときに必ず **revocation-check crl** コマンドを使用して CRL チェックを行うように、ASA を設定できます。また、**revocation-check crl none** コマンドを使用することで、CRL チェックをオプションにすることもできます。こうすると、更新された CRL データが CA から提供されない場合でも、証明書認証は成功します。

ASA は HTTP、SCEP、または LDAP を使用して、CA から CRL を取得できます。トラストポイントごとに取得された CRL は、トラストポイントごとに設定可能な時間だけキャッシュされます。

ASA により、CRL のキャッシュに設定されている時間を超過してキャッシュされた CRL がある場合、ASA ではその CRL は古すぎて信頼できない、つまり「失効した」と見なされます。次回の証明書認証で失効した CRL のチェックが必要な場合に、ASA によってより新しいバージョンの CRL の取得が試みられます。

ASA によって CRL がキャッシュされる時間は、次の 2 つの要素によって決まります。

- **cache-time** コマンドで指定される分数。デフォルト値は 60 分です。
- 取得した CRL 中の NextUpdate フィールド。このフィールドが CRL にない場合もあります。ASA が NextUpdate フィールドを必要とするかどうか、およびこのフィールドを使用するかどうかは、**enforcenextupdate** コマンドで制御します。

ASA では、これらの 2 つの要素が次のように使用されます。

- NextUpdate フィールドが不要の場合、**cache-time** コマンドで指定された時間が経過すると、ASA は CRL に失効のマークを付けます。
- NextUpdate フィールドが必要な場合、ASA は、**cache-time** コマンドと NextUpdate フィールドで指定されている 2 つの時間のうち短い方の時間で、CRL に失効のマークを付けます。たとえば、**cache-time** コマンドによってキャッシュ時間が 100 分に設定され、NextUpdate フィールドによって次のアップデートが 70 分後に指定されている場合、ASA は 70 分後に CRL に失効のマークを付けます。

ASA がメモリ不足で、特定のトラストポイント用にキャッシュされた CRL をすべて保存することができない場合、使用頻度が最も低い CRL が削除され、新しく取得した CRL 用の空き領域が確保されます。

OCSP

OCSP は、有効期間内の証明書が発行元の CA によって無効にされているかどうかを ASA が判断するための 1 つの方法です。OCSP のコンフィギュレーションは、トラストポイントのコンフィギュレーションの一部です。

OCSP によって、証明書のステータスをチェックする範囲が検証局（OCSP サーバ、*応答側*とも呼ばれます）に限定され、ASA によって検証局に特定の証明書のステータスに関する問い合わせが行われます。これは、CRL チェックよりもスケーラブルで、最新の失効ステータスを確認できる方法です。この方法は、PKI の導入規模が大きい場合に便利で、安全なネットワークを拡大できます。

（注）　ASA では、OCSP 応答に 5 秒間のスキューを許可します。

証明書を認証するときに必ず **revocation-check ocsp** コマンドを使用して OCSP チェックを行うように、ASA を設定できます。また、**revocation-check ocsp none** コマンドを使用することで、OCSP チェックをオプションにすることもできます。こうすると、更新された OCSP データが検証局から提供されない場合でも、証明書認証は成功します。

OCSP を利用すると、OCSP サーバの URL を 3 つの方法で定義できます。ASA は、これらのサーバを次の順に使用します。

1. **match certificate** コマンドの使用による証明書の照合の上書きルールで定義されている OCSP サーバの URL
2. **ocsp url** コマンドを使用して設定されている OCSP サーバの URL
3. クライアント証明書の AIA フィールド

（注）トラストポイントで OCSP の応答側の自己署名した証明書を検証するように設定するには、信頼できる CA 証明書として、この自己署名した応答側の証明書をそのトラストポイントにインポートします。次に、クライアント証明書を検証するトラストポイントで **match certificate** コマンドを設定して、応答側の証明書を検証するために、OCSP の応答側の自己署名された証明書を含むトラストポイントを使用するようにします。クライアント証明書の検証パスの外部にある応答側の証明書を検証する場合も、同じ手順で設定します。

通常、OCSP サーバ（応答側）の証明書によって、OCSP 応答が署名されます。ASA が応答を受け取ると、応答側の証明書を検証しようとします。通常、CA は、侵害される危険性を最小限に抑えるために、OCSP レスポンダ証明書のライフタイムを比較的短い期間に設定します。CA は一般に、応答側証明書に ocsp-no-check 拡張を含めて、この証明書では失効ステータスチェックが必要ないことを示します。ただし、この拡張がない場合、ASA はトラストポイントで指定されている方法で失効ステータスをチェックします。応答側の証明書を検証できない場合、失効ステータスをチェックできなくなります。この可能性を防ぐには、**revocation-check none** コマンドを使用して応答側の証明書を検証するトラストポイントを設定し、**revocation-check ocsp** コマンドを使用してクライアント証明書を設定します。

ローカル CA

ローカル CA では、次のタスクが実行されます。

- ASA の基本的な認証局の動作を統合する。
- 証明書を導入する。
- 発行済み証明書のセキュアな失効チェックを実行する。
- ブラウザベースとクライアントベースの両方で SSL VPN 接続とともに使用するために、ASA 上に認証局を提供する。
- 外部の証明書認証に依存することなく、ユーザに信頼できるデジタル証明書を提供する。
- 証明書認証のためのセキュアな内部認証局を提供し、Web サイト ログインを使用した簡単なユーザ登録を実現する。

ローカル CA ファイル用のストレージ

ASA では、ユーザ情報、発行済み証明書、および失効リストへのアクセスと実装にローカル CA データベースが使用されます。このデータベースは、デフォルトでローカル フラッシュ メモリに存在するか、または、マウントされて ASA にアクセス可能な外部のファイル システム上に設定することもできます。

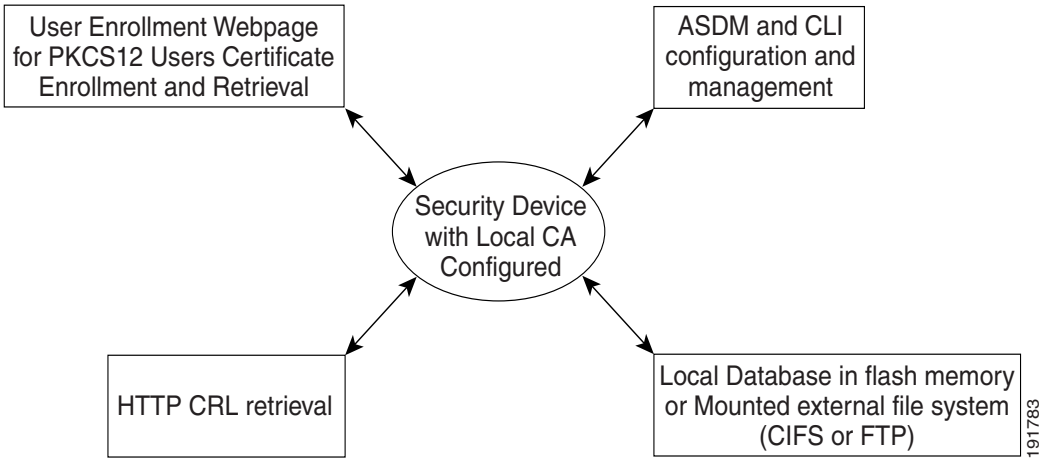
ローカル CA ユーザ データベースに保存できるユーザの数に制限はありませんが、フラッシュ メモリ ストレージに問題がある場合、管理者に対策を取るように警告する syslog が作成され、ローカル CA はストレージの問題が解決されるまでディセーブルになることがあります。フラッシュ メモリは、3500 人以下のユーザを持つデータベースを保存できますが、ユーザの数がそれを超えるデータベースでは外部ストレージが必要になります。

ローカル CA サーバ

ASA にローカル CA サーバを設定すると、ユーザは、Web サイトにログインし、ユーザの登録資格を検証するためにローカル CA 管理者によって与えられたユーザ名とワンタイム パスワードを入力することで、証明書を登録できます。

図 35-1 に示すように、ローカル CA サーバは ASA に常駐し、Web サイト ユーザからの登録要求や、その他の証明書を検証するデバイスおよび ASA から発信された CRL の問い合わせを処理します。ローカル CA データベースおよびコンフィギュレーション ファイルは、ASA のフラッシュ メモリ（デフォルトのストレージ）または個別のストレージ デバイスに保持されます。

図 35-1　　ローカル CA



証明書とユーザ ログイン クレデンシャル

この項では、認証と認可に証明書およびユーザ ログイン クレデンシャル（ユーザ名とパスワード）を使用する、さまざまな方法について説明します。これらの方式は、IPSec、AnyConnect、およびクライアントレス SSL VPN に適用されます。

すべての場合において、LDAP 認可では、パスワードをクレデンシャルとして使用しません。RADIUS 認可では、すべてのユーザの共通パスワード またはユーザ名のいずれかを、パスワードとして使用します。

ユーザ ログイン クレデンシャル

認証および認可のデフォルトの方法では、ユーザ ログイン クレデンシャルを使用します。

- 認証
  - トンネル グループ（ASDM 接続プロファイルとも呼ばれます）の認証サーバ グループ設定によりイネーブルにされます。
  - ユーザ名とパスワードをクレデンシャルとして使用します。
- 認可
  - トンネル グループ（ASDM 接続プロファイルとも呼ばれます）の認可サーバ グループ設定によりイネーブルにされます。
  - ユーザ名をクレデンシャルとして使用します。

証明書

ユーザ デジタル証明書が設定されている場合、ASA によって最初に証明書が検証されます。ただし、証明書の DN は認証用のユーザ名として使用されません。

認証と認可の両方がイネーブルになっている場合、ASA によって、ユーザの認証と認可の両方にユーザ ログイン クレデンシャルが使用されます。

- 認証
  - 認証サーバ グループ設定によってイネーブルにされます。
  - ユーザ名とパスワードをクレデンシャルとして使用します。
- 認可
  - 認可サーバ グループ設定によってイネーブルにされます。
  - ユーザ名をクレデンシャルとして使用します。

認証がディセーブルで認可がイネーブルになっている場合、ASA によって認可にプライマリ DN のフィールドが使用されます。

- 認証
  - 認証サーバ グループ設定によってディセーブル（[None] に設定）になります。
  - クレデンシャルは使用されません。
- 認可
  - 認可サーバ グループ設定によってイネーブルにされます。
  - 証明書のプライマリ DN フィールドのユーザ名の値をクレデンシャルとして使用します。

（注） 証明書にプライマリ DN のフィールドが存在しない場合、ASA では、セカンダリ DN のフィールド値が認可要求のユーザ名として使用されます。

次のサブジェクト DN フィールドと値が含まれるユーザ証明書を例に挙げます。

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

プライマリ DN = EA（電子メール アドレス）およびセカンダリ DN = CN（一般名）の場合、認可要求で使われるユーザ名は anyuser@example.com になります。

ローカル証明書の前提条件

ローカル証明書には、次の前提条件があります。

- 証明書をサポートするように ASA が正しく設定されていることを確認します。ASA の設定に誤りがあると、登録に失敗したり、不正確な情報を含む証明書が要求されたりする可能性があります。
- ASA のホスト名とドメイン名が正しく設定されていることを確認します。現在設定されているホスト名とドメイン名を表示するには、**show running-config** コマンドを入力します。
- CA を設定する前に、ASA のクロックが正しく設定されていることを確認します。証明書には、有効になる日時と満了になる日時が指定されています。ASA が CA に登録して証明書を取得するとき、ASA は現在の時刻が証明書の有効期間の範囲内であるかどうかをチェックします。現在の時刻が有効期間の範囲外の場合、登録は失敗します。

SCEP プロキシ サポートの前提条件

サードパーティ製証明書の要求を送信するために ASA をプロキシとして設定するには、次の要件があります。

- AnyConnect セキュア モビリティ クライアント 3.0 以降がエンドポイントで実行中である必要があります。
- グループ ポリシーの接続プロファイルで設定される認証方式は、AAA 認証と証明書認証の両方を使用するように設定する必要があります。
- SSL ポートが、IKEv2 VPN 接続用に開いている必要があります。
- CA は、自動許可モードになっている必要があります。

デジタル証明書のガイドライン

コンテキスト モードのガイドライン

- サードパーティ CA ではシングル コンテキスト モードでのみサポートされています。

フェールオーバーのガイドライン

- ステートフル フェールオーバーではセッションの複製はサポートされません。
- ローカル CA のフェールオーバーはサポートされません。

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドライン

- ASA が CA サーバまたはクライアントとして設定されている場合、推奨される終了日（2038 年 1 月 19 日 03:14:08 UTC）を超えないよう、証明書の有効期を制限してください。このガイドラインは、サードパーティ ベンダーからインポートした証明書にも適用されます。
- フェールオーバーがイネーブルになっている場合、ローカル CA は設定できません。ローカル CA サーバを設定できるのは、フェールオーバーのないスタンドアロン ASA のみです。詳細については、「CSCty43366」を参照してください。
- 証明書の登録が完了すると、ASA により、ユーザのキー ペアと証明書チェーンを含む PKCS12 ファイルが保存されます。これには、登録ごとに約 2 KB のフラッシュ メモリまたはディスク領域が必要です。実際のディスク領域の量は、設定されている RSA キー サイズと証明書フィールドによって異なります。使用できるフラッシュ メモリの量が限られている ASA に、保留中の証明書登録を多数追加する場合には、このガイドラインに注意してください。これらの PKCS12 ファイルは、設定されている登録の取得タイムアウトの間、フラッシュ メモリに保存されます。キー サイズは 2048 以上を使用することをお勧めします。
- **lifetime ca-certificate** コマンドは、ローカル CA サーバ証明書の初回生成時（初めてローカル CA サーバを設定し、**no shutdown** コマンドを発行するとき）に有効になります。CA 証明書の期限が切れると、設定されたライフタイム値を使用して新しい CA 証明書が生成されます。既存の CA 証明書のライフタイム値は変更できません。
- 管理インターフェイスに対する ASDM トラフィックおよび HTTPS トラフィックを保護するために、ID 証明書を使用するよう ASA を設定する必要があります。SCEP により自動的に生成される ID 証明書はリブートのたびに再生成されるため、必ず独自の ID 証明書を手動でインストールしてください。SSL のみに適用されるこの手順の例については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml

- ASA および AnyConnect クライアントで検証できるのは、[X520Serialnumber] フィールド（[Subject Name] のシリアル番号）が PrintableString 形式である証明書のみです。シリアル番号の形式に UTF8 などのエンコーディングが使用されている場合、証明書認証は失敗します。
- ASA でのインポート時は、有効な文字と値だけを証明書パラメータに使用してください。
- ワイルドカード（*）記号を使用するには、文字列値でこの文字を使用できるエンコードを CA サーバで使用していることを確認してください。RFC 5280 では UTF8String または PrintableString を使用することを推奨していますが、PrintableString ではこのワイルドカード文字を有効であると認識しないため UTF8String を使用する必要があります。ASA では、インポート時に無効な文字または値が見つかると、インポートした証明書を拒否します。次に例を示します。

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read
162*H÷ytes as CA certificate:0U0= \Ivr"phÕV°3é¼p0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

デジタル証明書の設定

この項では、ローカル CA 証明書を設定する方法を説明します。このタイプのデジタル証明書を正しく設定するためには、必ず記載されている順にタスクを実行してください。

- 「CA 証明書認証の設定」（P.35-11）
- 「失効に関する CA 証明書の設定」（P.35-14）
- 「CRL 取得ポリシーの設定」（P.35-14）
- 「CRL 取得方式の設定」（P.35-15）
- 「OCSP ルールの設定」（P.35-15）
- 「高度な CRL および OCSP の設定」（P.35-16）

CA 証明書認証の設定

[CA Certificates] ペインには、使用可能な証明書、発行先および発行元の CA サーバによる識別、証明書の有効期限日、関連付けられているトラストポイント、および証明書の使用法と目的が表示されます。[CA Certificates] ペインでは、次のタスクを実行できます。

- 自己署名または下位 CA 証明書を認証します。
- CA 証明書を ASA にインストールします。
- 新しい証明書コンフィギュレーションを作成します。
- 既存の証明書コンフィギュレーションを編集します。
- CA 証明書を手動で取得してインポートします。
- ASA が SCEP を使用して CA に接続して、自動的に証明書を取得およびインストールするようにします。

- 選択した証明書の詳細と発行元情報を表示します。
- 既存の CA 証明書の CRL にアクセスします。
- 既存の CA 証明書のコンフィギュレーションを削除します。
- 新規作成または修正した CA 証明書コンフィギュレーションを保存します。
- 変更内容をすべて破棄して、証明書コンフィギュレーションを元の設定に戻します。
- 「CA 証明書の追加またはインストール」（P.35-12）
- 「CA 証明書コンフィギュレーションの編集または削除」（P.35-13）
- 「CA 証明書の詳細の表示」（P.35-13）

CA 証明書の追加またはインストール

PEM 形式での証明書の手動による貼り付けや、SCEP を使用した自動登録により、既存のファイルから証明書コンフィギュレーションを新たに追加できます。SCEP は、ユーザの介入を最小限しか必要としない、セキュアなメッセージング プロトコルです。SCEP を使用すると、VPN Concentrator Manager のみを使用して証明書を登録およびインストールできます。

CA 証明書を追加またはインストールするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Remote Access VPN] > [Certificate Management] > [CA Certificates] の順に選択します。

ステップ 2　[Add] をクリックします。

[Install Certificate] ダイアログボックスが表示されます。選択されたトラストポイント名が読み取り専用形式で表示されます。

ステップ 3　既存のファイルから証明書コンフィギュレーションを追加するには、[Install from a file] オプション ボタンをクリックします（これがデフォルトの設定です）。

ステップ 4　パスおよびファイル名を入力するか、または [Browse] をクリックしてファイルを検索します。次に、[Install Certificate] をクリックします。

ステップ 5　[Certificate Installation] ダイアログボックスが表示され、証明書が正常にインストールされたことを示す確認メッセージが示されます。[OK] をクリックして、このダイアログボックスを閉じます。

ステップ 6　手動で登録するには、[Paste certificate in PEM format] オプション ボタンをクリックします。

ステップ 7　PEM 形式（base64 または 16 進数）の証明書をコピーして、指定の領域に貼り付け、[Install Certificate] をクリックします。

ステップ 8　[Certificate Installation] ダイアログボックスが表示され、証明書が正常にインストールされたことを示す確認メッセージが示されます。[OK] をクリックして、このダイアログボックスを閉じます。

ステップ 9　自動で登録するには、[Use SCEP] オプション ボタンをクリックします。ASA が、SCEP を使用して CA に接続し、証明書を取得して、証明書をデバイスにインストールします。SCEP を使用するには、インターネットを介して、SCEP をサポートする CA に登録する必要があります。SCEP を使用した自動登録では、ユーザは次の情報を入力する必要があります。

- 自動インストールする証明書のパスとファイル名。
- 証明書のインストールの最大再試行分数。デフォルトは 1 分です。
- 証明書のインストールの再試行回数。デフォルトは 0 です。この場合は、再試行時間内であれば何度でも再試行できます。

（注）　SCEP 方式を使用して証明書をインストールすることを選択する場合は、SCEP プロキシ サポートの前提条件を参照してください。

ステップ 10　新規および既存の証明書のその他のコンフィギュレーション オプションを表示するには、[More Options] をクリックします。

[Configuration Options for CA Certificates] ペインが表示されます。

ステップ 11　以降の手順については、「CA 証明書コンフィギュレーションの編集または削除」（P.35-13）を参照してください。

CA 証明書コンフィギュレーションの編集または削除

既存の CA 証明書コンフィギュレーションを変更または削除するには、次の手順を実行します。

ステップ 1　既存の CA 証明書コンフィギュレーションを変更するには、コンフィギュレーションを選択し、[Edit] をクリックします。

[Edit Options for CA Certificates] ペインが表示されます。これらのいずれかの設定を変更するには、後述の項で手順を参照してください。

- 「CRL 取得ポリシーの設定」（P.35-14）
- 「CRL 取得方式の設定」（P.35-15）
- 「OCSP ルールの設定」（P.35-15）
- 「高度な CRL および OCSP の設定」（P.35-16）

ステップ 2　CA 証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

（注）　証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Add] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

CA 証明書の詳細の表示

選択した CA 証明書に関する詳細情報を表示するには、[Show Details] をクリックして、次の 3 つの*表示専用タブ*が含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

失効に関する CA 証明書の設定

失効する CA 証明書を設定するには、シングルまたはマルチ コンテキスト モードで、次のサイト間タスクを実行します。

ステップ 1　ASDM アプリケーション ウィンドウで、[Configuration] > [Site-to-Site VPN] > [Certificate Management] > [CA Certificates] > [Add] の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2　[Configuration Options for CA Certificates] ペインで、[Revocation Check] タブをクリックします。

ステップ 3　証明書の失効チェックをディセーブルにするには、[Do not check certificates for revocation] オプション ボタンをクリックします。

ステップ 4　1 つ以上の失効チェック方式（CRL または OCSP）を選択するには、[Check certificates for revocation] オプション ボタンをクリックします。

ステップ 5　[Revocation Methods] 領域の左側に、選択可能な方式が表示されます。[Add] をクリックして方式を右側に移動すると、その方式が使用可能になります。[Move Up] または [Move Down] をクリックして、方式の順序を変更します。

選択した方式は、追加した順序で実装されます。方式からエラーが返された場合は、その次の失効チェック方式がアクティブになります。

ステップ 6　証明書の検証中に失効チェックのエラーを無視するには、[Consider certificate valid if revocation checking returns errors] チェックボックスをオンにします。

ステップ 7　[OK] をクリックして、[Revocation Check] タブを閉じます。また、続行する場合は、「CRL 取得ポリシーの設定」（P.35-14）を参照してください。

CRL 取得ポリシーの設定

CRL 取得ポリシーを設定するには、次の手順を実行します。

ステップ 1　ASDM アプリケーション ウィンドウで、[Configuration] > [Site-to-Site VPN] > [Certificate Management] > [CA Certificates] > [Add] の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2　[Use CRL Distribution Point from the certificate] チェックボックスをオンにして、チェック対象の証明書から CRL 分散ポイントに失効チェックを転送します。

ステップ 3　[Use Static URLs configured below] チェックボックスをオンにして、CRL の取得に使用する特定の URL を一覧表示します。選択した URL は、追加した順序で実装されます。指定した URL でエラーが発生した場合は、その次の URL が使用されます。

ステップ 4　[Static Configuration] 領域で、[Add] をクリックします。

[Add Static URL] ダイアログボックスが表示されます。

ステップ 5　[URL] フィールドに、CRL の分散に使用するスタティック URL を入力して、[OK] をクリックします。

入力した URL が [Static URLs] リストに表示されます。

ステップ 6　スタティック URL を変更するには、URL を選択し、[Edit] をクリックします。

ステップ 7　既存のスタティック URL を削除するには、URL を選択し、[Delete] をクリックします。

ステップ 8　スタティック URL の表示順序を変更するには、[Move Up] または [Move Down] をクリックします。

ステップ 9　[OK] をクリックして、このタブを閉じます。また、続行する場合は、「CRL 取得方式の設定」（P.35-15）を参照してください。

CRL 取得方式の設定

CRL 取得方式を設定するには、次の手順を実行します。

ステップ 1　ASDM アプリケーション ウィンドウで、[Configuration] > [Site-to-Site VPN] > [Certificate Management] > [CA Certificates] > [Add] の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2　[Configuration Options for CA Certificates] ペインで、[CRL Retrieval Methods] タブをクリックします。

ステップ 3　次の 3 つの取得方式のいずれかを選択します。

- CRL の取得で LDAP をイネーブルにするには、[Enable Lightweight Directory Access Protocol (LDAP)] チェックボックスをオンにします。LDAP を使用して CRL を取得する場合は、指定した LDAP サーバにパスワードを使用して接続することで、LDAP セッションが開始されます。デフォルトの場合、この接続には TCP ポート 389 を使用されます。次の必須パラメータを入力します。
  - 名前
  - パスワード
  - Confirm Password
  - デフォルト サーバ（サーバ名）
  - デフォルト ポート（389）
- CRL の取得で HTTP をイネーブルにするには、[Enable HTTP] チェックボックスをオンにします。

ステップ 4　[OK] をクリックして、このタブを閉じます。また、続行する場合は、「OCSP ルールの設定」（P.35-15）を参照してください。

OCSP ルールの設定

ASA では、プライオリティ順に OCSP ルールが検証され、最初に一致したルールが適用されます。CRL の代わりに X.509 デジタル証明書が使用されます。

（注）　OCSP ルールを追加する前に、必ず証明書マップを設定しておいてください。証明書マップが設定されていない場合、エラー メッセージが表示されます。証明書マップを設定するには、[Configuration] > [Site-to-Site VPN] > [Advanced] > [Certificate to Connection Profile Maps] > [Rules] > [Add] の順に選択します。

X.509 デジタル証明書の失効ステータスを取得するための OCSP ルールを設定するには、次の手順を実行します。

ステップ 1　ASDM アプリケーション ウィンドウで、[Configuration] > [Site-to-Site VPN] > [Certificate Management] > [CA Certificates] > [Add] の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2　[Configuration Options for CA Certificates] ペインで、[OCSP Rules] タブをクリックします。

ステップ 3　この OCSP ルールと照合する証明書マップを選択します。証明書マップにより、ユーザ権限と、証明書の特定のフィールドとの照合が行われます。[Certificate] フィールドに、ASA において応答側の証明書の検証に使用される CA の名前が表示されます。[Index] フィールドに、ルールのプライオリティ番号が表示されます。[URL] フィールドに、この証明書の OCSP サーバの URL が表示されます。

ステップ 4　新しい OCSP ルールを追加するには、[Add] をクリックします。

[Add OCSP Rule] ダイアログボックスが表示されます。

ステップ 5　使用する証明書マップをドロップダウン リストから選択します。

ステップ 6　使用する証明書をドロップダウン リストから選択します。

ステップ 7　ルールのプライオリティ番号を入力します。

ステップ 8　この証明書の OCSP サーバの URL を入力します。

ステップ 9　完了したら、[OK] をクリックして、このダイアログボックスを閉じます。

新しく追加された OCSP ルールがリストに表示されます。

ステップ 10　既存の OCSP ルールを編集するには、ルールを選択し、[Edit] をクリックします。

ステップ 11　OCSP ルールを削除するには、ルールを選択し、[Delete] をクリックします。

ステップ 12　[OK] をクリックして、このタブを閉じます。また、続行する場合は、「高度な CRL および OCSP の設定」（P.35-16）を参照してください。

高度な CRL および OCSP の設定

証明書は発行されると、一定期間有効です。CA は、安全上の問題や名前またはアソシエーションの変更などの理由で、期限が切れる前に証明書を無効にすることがあります。CA は、無効になった証明書の署名付きリストを定期的に発行します。失効チェックをイネーブルにすると、ASA では、検証中の証明書が CA により無効になっていないかについてのチェックが行われます。ASA では、失効ステータスに対して、CRL および OCSP という 2 つのチェック方法がサポートされています。

CRL および OCSP の追加設定を行うには、次の手順を実行します。

ステップ 1　ASDM アプリケーション ウィンドウで、[Configuration] > [Site-to-Site VPN] > [Certificate Management] > [CA Certificates] > [Add] の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2　[Configuration Options for CA Certificates] ペインで、[Advanced] タブをクリックします。

ステップ 3　[CRL Options] 領域で、キャッシュのリフレッシュを行う間隔を分数で入力します。デフォルトは 60 分です。範囲は 1 ～ 1440 分です。CA から同じ CRL を何度も受け取る必要のないように、ASA では、取得した CRL をローカルで保存できます。これを CRL キャッシングと呼びます。CRL キャッシュの容量はプラットフォームによって異なり、すべてのコンテキストについて累積されます。新たに取得した CRL をキャッシュすることで、保存制限を超える可能性がある場合は、ASA により使用頻度が最も低い CRL が削除され、使用可能な空き容量が確保されます。

ステップ 4　[Enforce next CRL update] チェックボックスをオンにして、Next Update 値の有効期限が切れていない CRL に限り、有効な CRL として使用できるようにします。[Enforce next CRL update] チェックボックスをオフにすると、Next Update 値がない場合や、Next Update 値の有効期限が切れている場合でも有効な CRL として使用できます。

ステップ 5　[OCSP Options] 領域で、OCSP サーバの URL を入力します。ASA で使用される OCSP サーバは、次の順に選択されます。

1. 一致証明書上書きルールの OCSP URL に対応するサーバ
2. 選択された [OCSP Options] 属性に設定した OCSP URL に対応するサーバ
3. ユーザ証明書の AIA フィールド

ステップ 6　デフォルトでは、[Disable nonce extension] チェックボックスがオンになっています。この設定では、暗号化によって要求を応答にバインドし、リプレイ アタックを回避します。このプロセスでは、要求と応答との間でそれぞれのナンス拡張を照合し、両者が同一であることを確認することで、リプレイ アタックを防ぐことができます。ただし、事前に生成した応答には、各要求と一致するナンス拡張は含まれていません。そのため、使用している OCSP サーバから、事前に生成した応答を送信する場合は、[Disable nonce extension] チェックボックスをオフにしてください。

ステップ 7　[Other Options] 領域で、次のオプションのいずれかを選択します。

- 指定した CA の証明書を ASA で受け入れるようにするには、[Accept certificates issued by this CA] チェックボックスをオンにします。
- 下位 CA の証明書を ASA で受け入れるようにするには、[Accept certificates issued by the subordinate CAs of this CA] チェックボックスをオンにします。

ステップ 8　[OK] をクリックしてこのタブを閉じ、[Apply] をクリックしてコンフィギュレーションの変更を保存します。

次の作業

「CRL のモニタリング」（P.35-32）を参照してください。

ID 証明書の認証の設定

ID 証明書は、ASA 経由の VPN アクセスの認証に使用できます。ASDM ランチャを使用して ASDM にアクセスするときに ID 証明書を使用することもできます。http://www.cisco.com/go/asdm-certificate で、ASDM ID 証明書ウィザードおよび手順を参照してください。

[Identity Certificates Authentication] ペインでは、次のタスクを実行できます。

- 新しい ID 証明書を追加またはインポートする。
- ID 証明書の詳細を表示する。
- 既存の ID 証明書を削除する。
- 既存の ID 証明書をエクスポートする。
- 既存の ID 証明書をインストールする。
- Entrust に ID 証明書を登録する。

- 「ID 証明書の追加またはインポート」（P.35-18）
- 「ID 証明書の詳細の表示」（P.35-20）

ID 証明書の追加またはインポート

新しい ID 証明書コンフィギュレーションを追加またはインポートするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Identity Certificates] の順に選択します。

ステップ 2　[Add] をクリックします。

選択されたトラストポイント名が上部に示された [Add Identity Certificate] ダイアログボックスが表示されます。

ステップ 3　既存のファイルから ID 証明書をインポートするには、[Import the identity certificate from a file (PKCS12 format with Certificate(s) + Private Key)] オプション ボタンをクリックします。

ステップ 4　PKCS12 ファイルの復号化に使用するパスフレーズを入力します。

ステップ 5　ファイルのパス名を入力するか、[Browse] をクリックして [Import ID Certificate File] ダイアログボックスを表示します。証明書ファイルを見つけて、[Import ID Certificate File] をクリックします。

ステップ 6　新しい ID 証明書を追加するには、[Add a new identity certificate] オプション ボタンをクリックします。

ステップ 7　[New] をクリックして、[Add Key Pair] ダイアログボックスを表示します。

ステップ 8　**RSA** または **ECDSA** キーのタイプを選択します。

ステップ 9　デフォルトのキー ペア名を使用する場合は、[Use default keypair name] オプション ボタンをクリックします。

ステップ 10　新しいキー ペア名を使用する場合は、[Enter a new key pair name] オプション ボタンをクリックし、新しい名前を入力します。ASA では、複数のキー ペアをサポートします。

ステップ 11　ドロップダウン リストから係数サイズを選択します。係数サイズが不明な場合は、Entrust にお問い合わせください。

ステップ 12　[General purpose] オプション ボタン（デフォルト）または [Special] オプション ボタンをクリックして、キー ペアの用途を選択します。[Special] オプション ボタンを選択すると、ASA により署名用と暗号化用の 2 つのキー ペアが生成されます。この選択は、対応する識別用に 2 つの証明書が必要なことを示します。

ステップ 13　[Generate Now] をクリックして新しいキー ペアを作成し、[Show] をクリックして [Key Pair Details] ダイアログボックスを表示します。ここには、次の*表示専用*の情報が示されます。

- 公開キーが認証の対象となるキー ペアの名前。
- キー ペアの生成日時。
- RSA キー ペアの用途。
- キー ペアの係数サイズ（512、768、1024、および 2048 ビット）。デフォルトは 1024 です。
- テキスト形式の特定のキー データを含むキー データ。

ステップ 14　完了したら [OK] をクリックして、[Key Pair Details] ダイアログボックスを閉じます。

ステップ 15　ID 証明書で DN を形成するための証明書サブジェクト DN を選択します。次に [Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

ステップ 16　ドロップダウン リストから追加する DN 属性を 1 つ以上選択し、値を入力し、[Add] をクリックします。証明書サブジェクト DN の使用可能な X.500 属性は、次のとおりです。

- Common Name（CN）
- Department（OU）
- Company Name（O）
- Country（C）
- State/Province（ST）
- Location（L）
- E-mail Address（EA）

ステップ 17　完了したら [OK] をクリックして、[Certificate Subject DN] ダイアログボックスを閉じます。

ステップ 18　自己署名証明書を作成するには、[Generate self-signed certificate] チェックボックスをオンにします。

ステップ 19　ID 証明書がローカル CA として動作するようにするには、[Act as local certificate authority and issue dynamic certificates to TLS proxy] チェックボックスをオンにします。

ステップ 20　追加の ID 証明書設定を行うには、[Advanced] をクリックします。

[Certificate Parameters]、[Enrollment Mode]、および [SCEP Challenge Password] の 3 つのタブを持つ [Advanced Options] ダイアログボックスが表示されます。

（注）　登録モード設定と SCEP チャレンジ パスワードは自己署名証明書では使用できません。

ステップ 21　[Certificate Parameters] タブをクリックし、次の情報を入力します。

- DNS ツリー階層内のノードの位置を示す FQDN（完全修飾ドメイン名）。
- ID 証明書に関連付けられている電子メール アドレス。
- 4 分割ドット付き 10 進表記の、ネットワーク上の ASA IP アドレスです。
- ASA シリアル番号を証明書パラメータに追加するには、[Include serial number of the device] チェックボックスをオンにします。

ステップ 22　[Enrollment Mode] タブをクリックし、次の情報を入力します。

- [Request by manual enrollment] オプション ボタンまたは [Request from a CA] オプション ボタンをクリックして、登録方式を選択します。
- SCEP を介して自動的にインストールされる証明書の登録 URL。
- ID 証明書のインストールに許可される最大再試行分数。デフォルトは 1 分です。
- ID 証明書のインストールに許可される最大再試行回数。デフォルトは 0 です。この場合は、再試行時間内であれば何度でも再試行できます。

ステップ 23　[SCEP Challenge Password] タブをクリックし、次の情報を入力します。

- SCEP パスワード
- SCEP パスワードを確認のために再入力

ステップ 24　完了したら [OK] をクリックして、[Advanced Options] ダイアログボックスを閉じます。

ステップ 25　[Add Identity Certificate] ダイアログボックスで、[Add Certificate] をクリックします。

[Identity Certificates] リストに新しい ID 証明書が表示されます。

ステップ 26　[Apply] をクリックし、新しい ID 証明書コンフィギュレーションを保存します。

ID 証明書の詳細の表示

選択した ID 証明書に関する詳細情報を表示するには、[Show Details] をクリックして、次の 3 つの*表示専用*タブが含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

ID 証明書の削除

ID 証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[**Delete**] をクリックします。

（注）　証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Add] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

ID 証明書のエクスポート

証明書コンフィギュレーションおよび関連付けられているすべてのキーと証明書を、公開キーの暗号化標準である PKCS12 形式でエクスポートできます。これには、base64 エンコードまたは 16 進数形式を使用できます。完全なコンフィギュレーションには、チェーン全体（ルート CA 証明書、ID 証明書、キー ペア）は含まれますが、登録設定（サブジェクト名、FQDN など）は含まれません。通常、この機能は、同じグループ内の ASA 間で証明書を複製するために行うフェールオーバーまたはロードバランシングの設定に使用されます。たとえば、リモート アクセス クライアントから中央処理装置への呼び出しが複数のユニットで処理されている場合、これらのユニット間では、証明書コンフィギュレーションが同一であることが必要となります。このような場合、管理者は、証明書コンフィギュレーションをエクスポートしたうえで、ASA のグループ全体にインポートできます。

ID 証明書をエクスポートするには、次の手順を実行します。

ステップ 1　[Export] をクリックし、[Export Certificate] ダイアログボックスを表示します。

ステップ 2　証明書コンフィギュレーションをエクスポートするときに使用する PKCS12 形式ファイルの名前を入力します。または、[Browse] をクリックして [Export ID Certificate File] ダイアログボックスを表示し、証明書コンフィギュレーションをエクスポートするファイルを探します。

ステップ 3　[PKCS12 Format] オプション ボタンまたは [PEM Format] オプション ボタンをクリックして、証明書の形式を選択します。

ステップ 4　PKCS12 ファイルをエクスポート用に暗号化するために使用するパスフレーズを入力します。

ステップ 5　暗号化パスフレーズを確認のために再入力します。

ステップ 6　[Export Certificate] をクリックして、証明書コンフィギュレーションをエクスポートします。

情報ダイアログボックスが表示され、証明書コンフィギュレーション ファイルが指定の場所に正常にエクスポートされたことが示されます。

証明書署名要求の生成

Entrust に送信する証明書署名要求を生成するには、次の手順を実行します。

ステップ 1　[Enroll ASA SSL VPN with Entrust] をクリックして、[Generate Certificate Signing Request] ダイアログボックスを表示します。

ステップ 2　[Key Pair] 領域で、次の手順を実行します。

- **a.** ドロップダウン リストから、設定されたキー ペアのいずれかを選択します。
- **b.** [Show] をクリックして [Key Details] ダイアログボックスを表示します。ここには、選択されたキー ペアの生成日時、用途（一般的または特殊な用途）、係数サイズ、およびキーデータといった情報が示されます。
- **c.** 完了したら [OK] をクリックして、[Key Details] ダイアログボックスを閉じます。
- **d.** [New] をクリックして、[Add Key Pair] ダイアログボックスを表示します。以降の手順については、「ID 証明書の追加またはインポート」（P.35-18）の手順 8 に進みます。生成したキー ペアは ASA に送信するか、ファイルに保存できます。

ステップ 3　[Certificate Subject DN] 領域で、次の情報を入力します。

- **a.** ASA の FQDN または IP アドレス。
- **b.** 会社の名前。
- **c.** 2 文字の国番号。

ステップ 4　[Optional Parameters] 領域で、次の手順を実行します。

- **a.** [Select] をクリックして、[Additional DN Attributes] ダイアログボックスを表示します。
- **b.** ドロップダウン リストから追加する属性を選択し、値を入力します。
- **c.** [Add] をクリックして、各属性を [attribute] テーブルに追加します。
- **d.** [Delete] をクリックして、[attribute] テーブルから属性を削除します。
- **e.** 完了したら [OK] をクリックして、[Additional DN Attributes] ダイアログボックスを閉じます。

  [Additional DN Attributes] フィールドに追加された属性が表示されます。

ステップ 5　CA から要求された場合は、完全修飾ドメイン名情報を追加で入力します。

ステップ 6　[Generate Request] をクリックして、証明書署名要求を生成します。生成した証明書署名要求については、Entrust に送信するか、ファイルに保存するか、または後で送信するかを選択できます。

CSR が示された [Enroll with Entrust] ダイアログボックスが表示されます。

ステップ 7　登録プロセスを完了するには、http://www.entrust.net/cisco/ にある [request a certificate from Entrust] リンクをクリックします。その際、示された CSR をコピーして貼り付け、それを Entrust Web フォームを使用して送信します。後で登録する場合は、生成された CSR をファイルに保存し、[Identity Certificates] ペインの [enroll with Entrust] リンクをクリックして登録プロセスを完了します。

ステップ 8　Entrust により、要求の認証が確認された後、証明書が発行されます。これには数日間かかる場合があります。次に、[Identity Certificate] ペインで保留中の要求を選択し、[Install] をクリックして、証明書をインストールする必要があります。[Close] をクリックして、[Enroll with Entrust] ダイアログボックスを閉じます。

アイデンティティ証明書のインストール

[Identity Certificates] ペインの [Install] ボタンは、保留中の登録がない場合はグレー表示されます。ASA が CSR を受信した場合は必ず、[Identity Certificates] ペインに保留中の ID 証明書が表示されます。保留中の ID 証明書を選択すると、[Install] ボタンがアクティブになります。

保留中の要求を CA に転送すると、CA はそのファイルを登録して証明書を ASA に返します。証明書を受信したら、[Install] をクリックし、該当する ID 証明書を選択して操作を完了します。

保留中の ID 証明書をインストールするには、次の手順を実行します。

ステップ 1　[Identity Certificates] ペインで、[Add] をクリックし、[Add Identity Certificate] ダイアログボックスを表示します。

ステップ 2　[Add Identity Certificate] ダイアログボックスで、[Add a new identity certificate] オプション ボタンをクリックします。

ステップ 3　（オプション）キー ペアを変更するか、新しいキー ペアを作成します。キー ペアは必須です。

ステップ 4　[Certificate Subject DN] に情報を入力し、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

ステップ 5　関係する CA で必要なサブジェクト DN 属性をすべて指定し、[OK] をクリックして [Certificate Subject DN] ダイアログボックスを閉じます。

ステップ 6　[Add Identity Certificate] ダイアログボックスで、[Advanced] をクリックして [Advanced Options] ダイアログボックスを表示します。

ステップ 7　以降の手順については、「ID 証明書の認証の設定」（P.35-17）の手順 17 ～ 23 を参照してください。

ステップ 8　[Add Identity Certificate] ダイアログボックスで、[Add Certificate] をクリックします。

[Identity Certificate Request] ダイアログボックスが表示されます。

ステップ 9　テキスト タイプの CSR ファイル名（c:\verisign-csr.txt など）を入力し、[OK] をクリックします。

ステップ 10　CSR テキスト ファイルを CA に送信します。送信する代わりに、CA の Web サイトにある CSR 登録ページにテキスト ファイルを貼り付けることもできます。

ステップ 11　CA から ID 証明書が返されたら、[Identity Certificates] ペインに移動し、保留中の証明書エントリを選択して、[Install] をクリックします。

[Install Identity Certificate] ダイアログボックスが表示されます。

ステップ 12　該当するオプション ボタンをクリックして、次のいずれかのオプションを選択します。

- Install from a file

  または、[Browse] をクリックし、ファイルを検索します。

- Paste the certificate data in base-64 format

  コピーした証明書データを指定された領域に貼り付けます。

ステップ 13　[Install Certificate] をクリックします。

ステップ 14　[Apply] をクリックし、新しくインストールした証明書とその ASA コンフィギュレーションを保存します。

次の作業

「コード署名者証明書の設定」（P.35-23）を参照してください。

コード署名者証明書の設定

コード署名により、デジタル署名が、実際の実行可能なコードに追加されます。このデジタル署名には、署名者を認証し、署名以降にそのコードが変更されていないことを保証するのに十分な情報が含まれています。

コード署名者証明書は、関連付けられている秘密キーがデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードが証明書の発生元を示します。[Code Signer] ペインで、または [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Java Code Signer] を選択して、コード署名者証明書をインポートできます。

[Code Signer] ペインでは、次のタスクを実行できます。

- コード署名者証明書の詳細を表示する。
- 既存のコード署名者証明書を削除する。
- 既存のコード署名者証明書をインポートする。
- 既存のコード署名者証明書をエクスポートする。
- Entrust にコード署名者証明書を登録する。

- 「コード署名者証明書の詳細の表示」（P.35-23）
- 「コード署名者証明書の削除」（P.35-24）
- 「コード署名者証明書のインポート」（P.35-24）
- 「コード署名者証明書のエクスポート」（P.35-24）

コード署名者証明書の詳細の表示

選択した ID 証明書に関する詳細情報を表示するには、[Show Details] をクリックして、次の 3 つの*表示専用*タブが含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

コード署名者証明書の削除

コード署名者証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

（注） 証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Import] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

コード署名者証明書のインポート

コード署名者証明書をインポートするには、次の手順を実行します。

ステップ 1　[Code Signer] ペインで、[Import] をクリックし、[Import Certificate] ダイアログボックスを表示します。

ステップ 2　PKCS12 形式ファイルの復号化に使用するパスフレーズを入力します。

ステップ 3　インポートするファイルの名前を入力するか、[Browse] をクリックして [Import ID Certificate File] ダイアログボックスを表示し、ファイルを検索します。

ステップ 4　インポートするファイルを選択し、[Import ID Certificate File] をクリックします。

[Import Certificate] ダイアログボックスに、選択した証明書ファイルが表示されます。

ステップ 5　[Import Certificate] をクリックします。

[Code Signer] ペインにインポートされた証明書が表示されます。

ステップ 6　[Apply] をクリックし、新しくインポートしたコード署名者証明書コンフィギュレーションを保存します。

コード署名者証明書のエクスポート

コード署名者証明書をエクスポートするには、次の手順を実行します。

ステップ 1　[Code Signer] ペインで、[Export] をクリックし、[Export Certificate] ダイアログボックスを表示します。

ステップ 2　証明書コンフィギュレーションをエクスポートするときに使用する PKCS12 形式ファイルの名前を入力します。

ステップ 3　公開キー暗号化標準（base64 エンコードまたは 16 進数形式を使用できます）を使用するには、[Certificate Format] 領域で [PKCS12 format] オプション ボタンをクリックします。使用しない場合は、[PEM format] オプション ボタンをクリックします。

ステップ 4　[Browse] をクリックして [Export ID Certificate File] ダイアログボックスを表示し、証明書コンフィギュレーションをエクスポートするファイルを探します。

ステップ 5　ファイルを選択し、[Export ID Certificate File] をクリックします。

[Export Certificate] ダイアログボックスに、選択した証明書ファイルが表示されます。

ステップ 6　エクスポート用の PKCS12 形式ファイルの復号化に使用するパスフレーズを入力します。

ステップ 7　復号化パスフレーズを確認のために再入力します。

ステップ 8　[Export Certificate] をクリックして、証明書コンフィギュレーションをエクスポートします。

次の作業

「ローカル CA を使用した認証」（P.35-25）を参照してください。

ローカル CA を使用した認証

ブラウザベースおよびクライアントベースの SSL VPN 接続では、ローカル CA により実現される、ASA 上に存在するセキュアで設定可能な内部認証局によって、証明書の認証を行うことができます。

ユーザの登録は、指定された Web サイトにログインすることによって行われます。ローカル CA は、ASA の基本認証局の動作を統合したもので、証明書の配布と、発行された証明書に対するセキュアな失効チェックを行います。

ローカル CA を使用すると、次のタスクを実行できます。

- ローカル CA サーバを設定する。
- ローカル CA 証明書の失効/失効解除を行う。
- CRL を更新する。
- ローカル CA ユーザを追加、編集、および削除する。

- 「ローカル CA サーバの設定」（P.35-25）
- 「ローカル CA サーバの削除」（P.35-28）

ローカル CA サーバの設定

ASA でローカル CA サーバを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Remote Access VPN] > [Certificate Management] > [Local Certificate Authority] > [CA Server] の順に選択します。

ステップ 2　ローカル CA サーバをアクティブにするには、[Enable Certificate Authority Server] チェックボックスをオンにします。デフォルト設定は、ディセーブル（オフ）です。ローカル CA サーバをイネーブルにすると、ASA によりローカル CA サーバ証明書、キー ペア、および必要なデータベース ファイルが生成され、ローカル CA サーバ証明書とキー ペアが PKCS12 ファイルにアーカイブされます。

（注）　設定済みのローカル CA をイネーブルにする前に、オプションのすべての設定を慎重に見直してください。イネーブルにした後で、証明書の発行者名とキー サイズ サーバ値を変更することはできません。

自己署名した証明書のキーの使用拡張により、キー暗号化、キー シグニチャ、CRL 署名、および証明書署名がイネーブルになります。

ステップ 3　ローカル CA を初めてイネーブルにするときには、英数字のイネーブル パスフレーズを入力し、確認のために再入力する必要があります。イネーブル パスフレーズは、7 文字以上の英数字である必要があります。このパスフレーズにより、ストレージにアーカイブされたローカル CA 証明書およびローカル CA 証明書のキー ペアが保護され、不正なシャットダウンや予期しないシャットダウンが発生しないようにローカル CA サーバが保護されます。ローカル CA 証明書またはキー ペアが失われ、その復元が必要となった場合、PKCS12 アーカイブのロックを解除するためには、このパスフレーズが必要です。

（注）　ローカル CA サーバをイネーブルにするには、イネーブル パスフレーズが必要です。イネーブル パスフレーズの記録は、必ず安全な場所に保管してください。

ステップ 4　ASA をリブートしてもコンフィギュレーションが失われないように、[Apply] をクリックして、ローカル CA 証明書とキー ペアを保存します。

ステップ 5　ローカル CA の初回設定後にローカル CA を変更または再設定する場合は、[Enable Certificate Authority Server] チェックボックスをオフにして、ASA 上のローカル CA サーバをシャットダウンする必要があります。この状態では、コンフィギュレーションおよびすべての関連ファイルはストレージ内に保持され、登録はディセーブルになっています。

設定したローカル CA がイネーブルになると、次の 2 つの設定が*表示専用*になります。

- [Issuer Name] フィールド。発行元のサブジェクト名とドメイン名がリストで示されます。これは、ユーザ名とサブジェクト名のデフォルト DN 設定により構成され、cn=FQDN という形式で示されます。ローカル CA サーバは、証明書を付与するエンティティです。証明書のデフォルト名は、cn=hostname.domainname という形式で表示されます。
- [CA Server Key Size] 設定。これは、ローカル CA サーバに生成されるサーバ証明書を対象とします。キー サイズには、キーごとに 512、768、1024、または 2048 ビットのいずれかを指定できます。デフォルトは、1 つのキーあたり 1024 ビットです。キー サイズは 2048 以上を使用することをお勧めします。

ステップ 6　ドロップダウン リストから、ローカル CA サーバが発行した各ユーザ証明書に対して生成されるキー ペアのクライアント キー サイズを選択します。キー サイズには、キーごとに 512、768、1024、または 2048 ビットのいずれかを指定できます。デフォルトは、1 つのキーあたり 1024 ビットです。キー サイズは 2048 以上を使用することをお勧めします。

ステップ 7　CA 証明書のライフタイム値を入力します。これは、CA サーバ証明書の有効期間を日数単位で指定するものです。デフォルトは、3650 日（10 年）です。推奨される終了日（2038 年 1 月 19 日 03:14:08 UTC）を超えないよう、証明書の有効期間を制限します。

ローカル CA サーバでは、CA 証明書の期限が切れる 30 日前に後継の CA 証明書が自動的に生成されます。この証明書をエクスポートし、他のデバイスにインポートすることにより、ローカル CA が発行したユーザ証明書のローカル CA 証明書検証を、期限が切れた後に行うことができます。

期限切れが近付いていることをユーザに通知するために、次の syslog メッセージが [Latest ASDM Syslog Messages] ペインに表示されます。

```
%ASA-1-717049: Local CA Server certificate is due to expire in days days and a replacement
certificate is available for export.
```

（注）　この自動ロールオーバーが通知されたら、管理者は、新しいローカル CA 証明書が有効期限の前に必要なすべてのデバイスにインポートされるようにする必要があります。

ステップ 8　クライアント証明書のライフタイム値を入力します。これは、CA サーバが発行したユーザ証明書の有効期間を日数単位で指定するものです。デフォルトは 365 日（1 年）です。推奨される終了日（2038 年 1 月 19 日 03:14:08 UTC）を超えないよう、証明書の有効期間を制限します。

[SMTP Server & Email Settings] 領域で、次の設定を指定して、ローカル CA サーバに対する電子メール アクセスを設定します。

a. SMTP メール サーバ名または IP アドレスを入力します。または、省略符号（[...]）をクリックして [Browse Server Name/IP Address] ダイアログボックスを表示し、ここからサーバ名または IP アドレスを選択します。完了したら [OK] をクリックして、[Browse Server Name/IP Address] ダイアログボックスを閉じます。

b. ローカル CA ユーザに電子メール メッセージを送信する際に使用する From アドレスを、「adminname@hostname.com」という形式で入力します。自動電子メール メッセージは、新規登録ユーザへのワンタイム パスワードの送信や、証明書の更新が必要なときの電子メール メッセージの発行に使用されます。

c. ローカル CA サーバからユーザに送信されるすべてのメッセージで使用される件名を入力します。件名を指定しない場合のデフォルトは「Certificate Enrollment Invitation」です。

ステップ 9　その他のオプションを設定するには、[More Options] ドロップダウン矢印をクリックします。

ステップ 10　CRL 分散ポイント（ASA 上の CRL の場所）を入力します。デフォルトの場所は、http://hostname.domain/+CSCOCA+/asa_ca.crl です。

ステップ 11　特定のインターフェイスおよびポートで、CRL に HTTP ダウンロードできるようにするには、ドロップダウン リストから publish-CRL インターフェイスを選択します。次に、1 ～ 65535 の任意のポート番号を入力します。デフォルトのポート番号は TCP ポート 80 です。

（注）　CRL の名前は変更できません。LOCAL-CA-SERVER.crl という名前が常に使用されます。

たとえば、http://10.10.10.100/user8/my_crl_file という URL を入力します。この場合、指定された IP アドレスを持つインターフェイスのみが動作します。要求を受信すると、ASA によってパス /user8/my_crl_file と設定済み URL が照合されます。パスが一致すると、ASA から、保存されている CRL ファイルが返されます。

ステップ 12　CRL の有効期間である CRL ライフタイムを時間単位で入力します。CA 証明書のデフォルトは 6 時間です。

ローカル CA では、ユーザ証明書が失効するたびまたは失効解除されるたびに、更新された CRL が再発行されますが、失効状態に変更がない場合、CRL の再発行は、そのライフタイムの中で 1 回しか行われません。[CA Certificates] ペインで [Request CRL] をクリックすると、CRL を即時に更新して再生成できます。

ステップ 13　データベース ストレージの場所を入力して、ローカル CA コンフィギュレーションとデータファイル用のストレージ領域を指定します。ASA では、ユーザ情報、発行済み証明書、および失効リストへのアクセスと実装にローカル CA データベースが使用されます。外部ファイルを指定する場合は、外部ファイルへのパス名を入力するか、[Browse] をクリックして [Database Storage Location] ダイアログボックスを表示します。

ステップ 14　表示されるフォルダのリストからストレージの場所を選択し、[OK] をクリックします。

（注）　フラッシュ メモリには、3500 人以下のユーザを持つデータベースを保存できます。ユーザの数がそれを超えるデータベースでは外部ストレージが必要になります。

ステップ 15　発行された証明書のユーザ名に追加されるデフォルト サブジェクト（DN 文字列）を入力します。次に示す DN 属性を指定できます。

- CN（一般名）
- SN（姓名の姓）

- O（組織名）
- L（地名）
- C（国）
- OU（組織ユニット）
- EA（電子メール アドレス）
- ST（州/都道府県）
- T（タイトル）

ステップ 16　登録されたユーザがユーザ証明書を登録および取得するための PKCS12 登録ファイルを取得できる期間を、時間単位で入力します。この登録期間は、ワンタイム パスワードの有効期間とは関係ありません。デフォルトは 24 時間です。

（注）　ローカル CA の証明書の登録は、クライアントレス SSL VPN 接続でのみサポートされます。このタイプの接続の場合、クライアントと ASA の通信は、標準の HTML を使用して Web ブラウザ経由で行われます。

ステップ 17　登録ユーザに電子メールで送信されたワンタイム パスワードの有効期間を入力します。デフォルトは 72 時間です。

ステップ 18　期限の何日前になったら、ユーザに期限切れ通知の電子メールを送信するかを入力します。デフォルトは、14 日です。

ステップ 19　[Apply] をクリックし、新しいまたは変更された CA 証明書コンフィギュレーションを保存します。変更を破棄して元の設定に戻す場合は、[Reset] をクリックします。

ローカル CA サーバの削除

ASA からローカル CA サーバを削除するには、次の手順を実行します。

ステップ 1　[CA Server] ペインで、[Delete Certificate Authority Server] をクリックします。

[Delete Certificate Authority] ダイアログボックスが表示されます。

ステップ 2　CA サーバを削除する場合は、[OK] をクリックします。CA サーバを保持する場合は、[Cancel] をクリックします。

（注）　削除したローカル CA サーバは、復元および復旧できません。削除した CA サーバ コンフィギュレーションを再作成する場合は、CA サーバ コンフィギュレーション情報をすべて再入力する必要があります。

次の作業

「ユーザ データベースの管理」（P.35-29）を参照してください。

ユーザ データベースの管理

ローカル CA ユーザ データベースには、ユーザ識別情報とユーザ ステータス（登録済み、許可、失効など）が格納されています。[Manage User Database] ペインでは、次のタスクを実行できます。

- ローカル CA データベースにユーザを追加する。
- 既存のユーザ識別情報を変更する。
- ローカル CA データベースからユーザを削除する。
- ユーザを登録する。
- CRL を更新する。
- ユーザに OTP を電子メールで送信する。
- OTP を表示または再生成（置換）する。

- 「ローカル CA ユーザの追加」（P.35-29）
- 「最初の OTP の送信または OTP の置換」（P.35-30）
- 「ローカル CA ユーザの編集」（P.35-30）
- 「ローカル CA ユーザの削除」（P.35-31）
- 「ユーザ登録の許可」（P.35-31）
- 「OTP の表示または再生成」（P.35-31）

ローカル CA ユーザの追加

ローカル CA ユーザを追加するには、次の手順を実行します。

ステップ 1　新しいユーザをローカル CA データベースに追加するには、[Add] をクリックして、[Add User] ダイアログボックスを表示します。

ステップ 2　有効なユーザ名を入力します。

ステップ 3　既存の有効な電子メール アドレスを入力します。

ステップ 4　サブジェクト（DN 文字列）を入力します。または、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

ステップ 5　ドロップダウン リストから追加する DN 属性を 1 つ以上選択し、値を入力し、[Add] をクリックします。証明書サブジェクト DN の使用可能な X.500 属性は、次のとおりです。

- Common Name（CN）
- Department（OU）
- Company Name（O）
- Country（C）
- State/Province（ST）

- Location（L）
- E-mail Address（EA）

ステップ 6　完了したら [OK] をクリックして、[Certificate Subject DN] ダイアログボックスを閉じます。

ステップ 7　[Allow enrollment] チェックボックスをオンにしてユーザを登録し、[Add User] をクリックします。

[Manage User Database] ペインに新しいユーザが表示されます。

最初の OTP の送信または OTP の置換

新規追加されたユーザに対して、一意の OTP とローカル CA 登録 URL が記載された登録許可の電子メール通知を自動的に送信するには、[Email OTP] をクリックします。

OTP が新規ユーザに送信されたことを示す [Information] ダイアログボックスが表示されます。

自動的に新しい OTP を再発行して、新しいパスワードが記載された電子メール通知を既存のユーザまたは新規ユーザに送信するには、[Replace OTP] をクリックします。

ローカル CA ユーザの編集

データベース内の既存のローカル CA ユーザに関する情報を変更するには、次の手順を実行します。

ステップ 1　特定のユーザを選択し、[Edit] をクリックして [Edit User] ダイアログボックスを表示します。

ステップ 2　有効なユーザ名を入力します。

ステップ 3　既存の有効な電子メール アドレスを入力します。

ステップ 4　サブジェクト（DN 文字列）を入力します。または、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

ステップ 5　ドロップダウン リストから変更する DN 属性を 1 つ以上選択し、値を入力し、[Add] または [Delete] をクリックします。証明書サブジェクト DN の使用可能な X.500 属性は、次のとおりです。

- Common Name（CN）
- Department（OU）
- Company Name（O）
- Country（C）
- State/Province（ST）
- Location（L）
- E-mail Address（EA）

ステップ 6　完了したら [OK] をクリックして、[Certificate Subject DN] ダイアログボックスを閉じます。

ステップ 7　[Allow enrollment] チェックボックスをオンにしてユーザを再登録し、[Edit User] をクリックします。

[Manage User Database] ペインに更新されたユーザ詳細が表示されます。

ローカル CA ユーザの削除

ユーザをデータベースから削除し、そのユーザに発行されたすべての証明書をローカル CA データベースから削除するには、ユーザを選択し、[Delete] をクリックします。

（注）　削除されたユーザは復元できません。削除したユーザ レコードを再作成するには、[Add] をクリックして、そのユーザの情報をすべて再入力します。

ユーザ登録の許可

選択したユーザを登録するには、[Allow Enrollment] をクリックします。

[Manage User Database] ペインに示されるユーザのステータスが [enrolled] に変わります。

（注）　ユーザがすでに登録されている場合は、エラー メッセージが表示されます。

OTP の表示または再生成

選択したユーザの OTP を表示または再生成するには、次の手順を実行します。

ステップ 1　[View/Regenerate OTP] をクリックして、[View & Regenerate OTP] ダイアログボックスを表示します。

現在の OTP が表示されます。

ステップ 2　完了したら [OK] をクリックし、[View & Regenerate OTP] ダイアログボックスを閉じます。

ステップ 3　OTP を再生成するには、[Regenerate OTP] をクリックします。

新しく生成された OTP が表示されます。

ステップ 4　[OK] をクリックして、[View & Regenerate OTP] ダイアログボックスを閉じます。

次の作業

「ユーザ証明書の管理」（P.35-32）を参照してください。

ユーザ証明書の管理

証明書のステータスを変更するには、次の手順を実行します。

ステップ 1　[Manage User Certificates] ペインで、ユーザ名または証明書のシリアル番号で特定の証明書を選択します。

ステップ 2　次のいずれかのオプションを選択します。

- ユーザ証明書のライフタイムが期限切れになった場合は、ユーザのアクセス権を削除するために、[Revoke] をクリックします。また、ローカル CA により、証明書データベース内にあるその証明書に失効のマークが付けられ、情報が自動的に更新されて、CRL が再発行されます。
- アクセス権を復元するには、失効した証明書を選択して、[Unrevoke] をクリックします。また、ローカル CA により、証明書データベース内にあるその証明書に失効解除のマークが付けられ、証明書の情報が自動的に更新された後、更新された CRL が再発行されます。

ステップ 3　完了したら [Apply] をクリックして、変更を保存します。

次の作業

「CRL のモニタリング」（P.35-32）を参照してください。

CRL のモニタリング

CRL をモニタにするには、次の手順を実行します。

ステップ 1　ASDM メイン アプリケーション ウィンドウで、[Monitoring] > [Properties] > [CRL] の順に選択します。

ステップ 2　[CRL] 領域で、ドロップダウン リストから CA 証明書名を選択します。

ステップ 3　CRL の詳細を表示するには、[View CRL] をクリックします。次に例を示します。

```
CRL Issuer Name:
    cn=asa4.cisco.com
    LastUpdate: 09:58:34 UTC Nov 11 2010
    NextUpdate: 15:58:34 UTC Nov 11 2010
    Cached Until: 15:58:34 UTC Nov 11 2010
    Retrieved from CRL Distribution Point:
      ** CDP Not Published - Retrieved via SCEP
    Size (bytes): 224
    Associated Trustpoints: LOCAL-CA-SERVER
```

ステップ 4　完了したら [Clear CRL] をクリックして CRL の詳細を削除し、表示する別の CA 証明書を選択します。

証明書管理の機能履歴

表 35-1　証明書管理の機能履歴

機能名	プラットフォーム リリース	機能情報
証明書管理	7.0(1)	デジタル証明書（CA 証明書、ID 証明書、およびコード署名者証明書など）は、認証用のデジタル ID を提供します。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。 次の画面が導入されました。 [Configuration] > [Remote Access VPN] > [Certificate Management] [Configuration] > [Site-to-Site VPN] > [Certificate Management] 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [Advanced]> [Certificate Management] > [CA Certificates] [Configuration] > [Device Management] > [Certificate Management] > [CA Certificates]。
証明書管理	7.2(1)	
証明書管理	8.0(2)	
SCEP プロキシ	8.4(1)	サードパーティ CA からのデバイス証明書を安全に構成できる機能を導入しました。

PART 8

システム管理

管理アクセス

この章では、Telnet、SSH、および HTTPS（ASDM を使用）を介してシステム管理のために Cisco ASA にアクセスする方法と、ユーザを認証および許可する方法とログイン バナーを作成する方法について説明します。

（注） また、ASA インターフェイスに管理アクセスの目的でアクセスするには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。必要なのは、この章の各項の説明に従って管理アクセスを設定することだけです。

ASDM、Telnet、または SSH の ASA アクセスの設定

この項では、ASDM、Telnet、または SSH を使用した ASA へのアクセスをクライアントに許可する方法を説明します。

ASDM、Telnet、または SSH での ASA アクセスのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

モデルのガイドライン

ASASM の場合、スイッチから ASASM へのセッションは Telnet セッションですが、このセクションに従って Telnet アクセスを設定する必要はありません。

その他のガイドライン

- VPN トンネル内で Telnet を使用する場合を除き、最も低いセキュリティ インターフェイスに対して Telnet は使用できません。
- ASA への通過ルートとなるインターフェイス以外のインターフェイスへの管理アクセスはサポートされません。たとえば、管理ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。このルールの例外は、VPN 接続を介した場合のみです。「VPN トンネルを介した管理アクセスの設定」（P.36-8）を参照してください。
- ASA では、以下のことが可能です。
  - コンテキストごとに最大 5 つの同時 Telnet 接続を許可し、可能な場合は、最大 100 の接続がすべてのコンテキストの間で分割されます。
  - コンテキストごとに最大 5 つの同時 SSH 接続を許可し、可能な場合は、最大 100 の接続がすべてのコンテキストの間で分割されます。
  - コンテキストごとに最大 5 つの同時 ASDM インスタンスを使用でき、全コンテキスト間で最大 32 の ASDM インスタンスの使用が可能です。
- ASA は SSH バージョン 1 および 2 で提供されている SSH リモート シェル機能をサポートし、DES 暗号および 3DES 暗号をサポートします。
- SSL および SSH での XML 管理はサポートされていません。

- （8.4 以降）SSH デフォルト ユーザ名はサポートされなくなりました。**pix** または **asa** ユーザ名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] を使用して AAA 認証を設定し、次に [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] を選択してローカル ユーザを定義する必要があります。ローカル データベースの代わりに AAA サーバを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。
- （9.1(2) 以降）デフォルトの Telnet ログイン パスワードが排除されました。Telnet を使用する前に手動でパスワードを設定する必要があります。「ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定」（P.14-1）を参照してください。
- ASA インターフェイスへの Telnet または SSH 接続を確立できない場合は、「ASDM、Telnet、または SSH の ASA アクセスの設定」（P.36-1）の手順に従って、ASA への Telnet または SSH をイネーブルにしていることを確認します。

管理アクセスの設定

クライアント IP アドレスを、ASA に Telnet、SSH、または ASDM を使用して接続できるよう指定するには、次の手順を実行します。

前提条件

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [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。

手順

ステップ 1　ASDM で、[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH] を選択して、[Add] をクリックします。

[Add Device Access Configuration] ダイアログボックスが表示されます。

ステップ 2　セッションのタイプとして、[ASDM/HTTPS]、[Telnet]、[SSH] のいずれかを選択します。

ステップ 3　管理インターフェイスを選択し、許可するホスト IP アドレス設定して、[OK] をクリックします。

ステップ 4　[Enable HTTP Server] チェックボックスがオンになっていることを確認します。この設定はデフォルトでイネーブルになっています。必要に応じて他の HTTP サーバ オプションを設定します。

ステップ 5　（オプション）Telnet の設定を行います。デフォルトのタイムアウト値は 5 分です。

ステップ 6　（オプション）SSH の設定を行います。[DH Key Exchange] で、該当するオプション ボタンをクリックして、Diffie-Hellman（DH）キー交換グループ 1 またはグループ 14 を選択します。ASA では、DH グループ 1 およびグループ 14 キー交換の両方の方法がサポートされます。DH グループ キー交換方式が指定されないと、DH グループ 1 のキー交換方式が使用されます。DH キー交換方法の使用方法の詳細については、RFC 4253 を参照してください。

ステップ 7　[Apply] をクリックします。

変更内容が実行コンフィギュレーションに保存されます。

ステップ 8　（Telnet に必要）Telnet で接続する前に、ログイン パスワードを設定します。デフォルトのパスワードはありません。

a.　[Configuration] > [Device Setup] > [Device Name/Password] を選択します。

b. [Telnet Password] 領域で、[Change the password to access the console of the security appliance] チェックボックスをオンにします。

c. 古いパスワード（新しい ASA の場合、このフィールドは空白にしておきます）、新しいパスワードを入力し、新しいパスワードを確認します。

d. [Apply] をクリックします。

ステップ 9　（SSH に必要）SSH ユーザ認証を設定します。

a. [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] を選択します。

b. [SSH] チェックボックスをオンにします。

c. [Server Group] ドロップダウン リストから、[LOCAL] データベースを選択します。AAA サーバを使用して認証を設定することもできます。

d. [Apply] をクリックします。

e. ローカル ユーザを追加します。[Configuration] > [Device Management] > [Users/AAA] **>** [User Accounts] の順に選択し、[Add] をクリックします。

   [Add User Account-Identity] ダイアログボックスが表示されます。

f. ユーザ名とパスワードを入力し、パスワードを確認します。

g. [OK] をクリックし、続いて [Apply] をクリックします。

HTTP リダイレクトの設定

HTTPS を使用して、ASDM を使用する ASA に接続します。利便性のために、HTTP 接続を HTTPS への管理インターフェイスにリダイレクトすることができます。たとえば、HTTP をリダイレクトすることによって、ユーザは、http://10.1.1.4/admin/ または https://10.1.8.4/admin/ と入力し、ASDM 起動ページで HTTPS アドレスにアクセスできます。

リダイレクトをイネーブルにするには、ASDM アクセスでサポートする各インターフェイスに対してこの手順を実行します。

ヒント　管理インターフェイスのアクセス ルールでは、HTTP と HTTPS の両方の接続が許可されている必要があり、これらのプロトコルは、通常、それぞれポート 80 と 443 を使用します。

ステップ 1　[Configuration] > [Device Management] > [HTTP Redirect] の順に選択します。

表には、現在設定されているインターフェイスと、リダイレクトがインターフェイスでイネーブルになっているかどうかを示しています。

ステップ 2　ASDM に使用するインターフェイスを選択し、[Edit] をクリックします。

ステップ 3　[Edit HTTP/HTTPS Settings] ダイアログボックスで、次のオプションを設定します。

- [Redirect HTTP to HTTPS]：HTTP リクエストを HTTPS にリダイレクトするかどうか。
- [HTTP Port]：インターフェイスが HTTP 接続のリダイレクトに使用するポートを指定します。デフォルトは 80 です。

ステップ 4　[OK] をクリックします。

Telnet クライアントの使用

ASA CLI に Telnet を使用してアクセスするには、ログイン パスワードを入力します。Telnet を使用する前に手動でパスワードを設定する必要があります。「ホスト名、ドメイン名、および イネーブル パスワードと Telnet パスワードの設定」（P.14-1）を参照してください。

Telnet 認証を設定している場合（「CLI、ASDM、および enable コマンド アクセスの認証の設定」（P.36-16）を参照）、AAA サーバまたはローカル データベースで定義したユーザ名とパスワードを入力します。

SSH クライアントの使用

管理ホストの SSH クライアントで、ユーザ名とパスワードを入力します。SSH セッションを開始すると、次の SSH ユーザ認証プロンプトが表示される前に、ASA コンソール上にドット（.）が表示されます。

```
ciscoasa(config)#.
```

ドットが表示されても、SSH の機能には影響を与えません。コンソールにドットが表示されるのは、ユーザ認証が始まる前で、サーバ キーを生成する場合か、または SSH キー交換中に秘密キーを使用してメッセージを暗号化する場合です。これらのタスクには 2 分以上かかることがあります。ドットは、ASA がビジー状態で、ハングしていないことを示す進捗インジケータです。

パスワードを使用する代わりに公開キーを設定できます。「ユーザ アカウントのローカル データベースへの追加」（P.28-3）を参照してください。

CLI パラメータの設定

CLI パラメータのライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

ログイン バナーの設定

ユーザが ASA に接続し、ユーザがログインする前または特権 EXEC モードに入る前に表示されるメッセージを設定できます。

制限事項

バナーが追加された後、次の場合は ASA に対する Telnet または SSH セッションが終了する可能性があります。

- バナー メッセージを処理するためのシステム メモリが不足している場合。
- バナー メッセージの表示を試みたときに、TCP 書き込みエラーが発生した場合。

ガイドライン

- セキュリティの観点から、バナーで不正アクセスを防止することが重要です。「ようこそ」や「どうぞ」など、侵入者を歓迎するような言葉は使用しないでください。次のバナーは、不正アクセスに対して適切な雰囲気を表しています。

  安全なデバイスにログインしました。このデバイスにアクセスする権限を持っていない場合は、すぐにログアウトしないと犯罪に巻き込まれる危険があります。

- バナー メッセージのガイドラインについては、RFC 2196 を参照してください。

ログイン バナーを設定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Banner] の順に選択し、CLI に対して作成するバナーのタイプに対応するフィールドに、バナー テキストを入力します。

- [session (exec)] バナーは、ユーザが CLI で特権 EXEC モードにアクセスした場合に表示されます。
- [login] バナーは、ユーザが CLI にログインした場合に表示されます。
- [message-of-the-day (motd)] バナーは、ユーザが CLI に初めて接続する場合に表示されます。
- [ASDM] バナーは、ユーザが認証を受けた後 ASDM に接続した場合に表示されます。ユーザは、次のいずれかのオプションを使用して、表示されたバナーを消去できます。
  - [Continue]：バナーを消去し、ログインできます。
  - [Disconnect]：バナーを消去し、接続を終了します。

- 使用できるのは、改行（Enter キー）も含めて ASCII 文字だけです。ただし、改行文字は 2 文字に相当します。
- また、タブ文字は、CLI バージョンでは無視されるため、バナーには使用しないでください。
- RAM およびフラッシュ メモリに関するもの以外、バナーに長さ制限はありません。
- ASA のホスト名またはドメイン名は、**$(hostname)** 文字列と **$(domain)** 文字列を組み込むことによって動的に追加できます。
- システム コンフィギュレーションでバナーを設定する場合は、コンテキスト コンフィギュレーションで **$(system)** 文字列を使用することによって、コンテキスト内でそのバナー テキストを使用できます。

ステップ 2　[**Apply**] をクリックします。

新しいバナーが、実行コンフィギュレーションに保存されます。

CLI プロンプトのカスタマイズ

[CLI Prompt] ペインで、CLI セッション時に使用するプロンプトをカスタマイズできます。デフォルトでは、プロンプトに ASA のホスト名が表示されます。マルチ コンテキスト モードでは、プロンプトにコンテキスト名も表示されます。CLI プロンプトには、次の項目を表示できます。

cluster-unit	（シングルおよびマルチ モード）クラスタ ユニット名を表示します。クラスタの各ユニットは一意の名前を持つことができます。
コンテキスト	（マルチ モードのみ）現在のコンテキストの名前を表示します。
domain	ドメイン名を表示します。
hostname	ホスト名を表示します。
priority	フェールオーバー プライオリティを [pri]（プライマリ）または [sec]（セカンダリ）として表示します。
state	装置のトラフィック通過状態を表示します。状態には次の値が表示されます。 • [act]：フェールオーバーがイネーブルであり、装置ではトラフィックをアクティブに通過させています。 • [stby]：フェールオーバーはイネーブルです。ユニットはトラフィックを通過させていません。スタンバイ、失敗、または他の非アクティブ状態です。 • [actNoFailove]：フェールオーバーはディセーブルであり、装置ではトラフィックをアクティブに通過させています。 • [stbyNoFailover]：フェールオーバーはディセーブルであり、装置ではトラフィックを通過させていません。この状況は、スタンバイ ユニットでしきい値を上回るインターフェイス障害が発生したときに生じることがあります。 クラスタのユニットのロール（マスターまたはスレーブ）を示します。たとえば、プロンプト ciscoasa/cl2/slave では、ホスト名は ciscoasa、ユニット名は cl2、状態名は slave です。

手順の詳細

CLI プロンプトをカスタマイズするには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [CLI Prompt] の順に選択し、次のいずれかの操作を行って、プロンプトをカスタマイズします。

- プロンプトに属性を追加する場合は、[Available Prompts] リストで目的の属性をクリックし、[Add] をクリックします。プロンプトには複数の属性を追加できます。属性が [Available Prompts] リストから [Selected Prompts] リストに移動します。
- プロンプトから属性を削除する場合は、[Selected Prompts] リストで属性をクリックし、[Delete] をクリックします。属性が [Selected Prompts] リストから [Available Prompts] リストに移動します。
- コマンド プロンプトに属性が表示される順序を変更する場合は、[Selected Prompts] リストで目的の属性をクリックし、[Move Up] または [Move Down] をクリックして順序を変更します。

変更されたプロンプトが [CLI Prompt Preview] フィールドに表示されます。

ステップ 2　[Apply] をクリックします。

変更されたプロンプトが、実行コンフィギュレーションに保存されます。

コンソール タイムアウトの変更

コンソール タイムアウトでは、接続を特権 EXEC モードまたはコンフィギュレーション モードにしておくことができる時間を設定します。タイムアウトに達すると、セッションはユーザ EXEC モードになります。デフォルトでは、セッションはタイムアウトしません。この設定は、コンソール ポートへの接続を保持できる時間には影響しません。接続がタイムアウトすることはありません。

コンソール タイムアウトを変更するには、次の手順を実行します。

手順の詳細

ステップ 1　新しいタイムアウト値を分単位で定義するには、[Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Console Timeout] の順に選択します。

ステップ 2　タイムアウトを設定しない場合は、**0** を入力します。デフォルト値は 0 です

ステップ 3　[Apply] をクリックします。

タイムアウト値が変更され、その変更内容が実行コンフィギュレーションに保存されます。

VPN トンネルを介した管理アクセスの設定

VPN トンネルがあるインターフェイスで終わっている場合に、別のインターフェイスにアクセスして ASA を管理する必要があれば、そのインターフェイスを管理アクセス インターフェイスとして識別できます。たとえば、外部インターフェイスから ASA に入る場合は、この機能を使用して、ASDM、SSH、Telnet、または SNMP 経由で内部インターフェイスに接続するか、

外部インターフェイスから入るときに内部インターフェイスに ping を実行できます。管理アクセスは、IPsec クライアント、IPsec site-to-site、AnyConnect SSL VPN クライアントの VPN トンネル タイプ経由で行えます。

- 「管理インターフェイスのライセンス要件」（P.36-9）
- 「注意事項と制約事項」（P.36-2）
- 「管理インターフェイスの設定」（P.36-10）

管理インターフェイスのライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル モードでだけサポートされています。

ファイアウォール モードのガイドライン

ルーテッド モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

その他のガイドライン

管理アクセス インターフェイスは 1 つだけ定義できます。

（注）その後の設定用には、192.168.10.0/24 が AnyConnect または IPSec VPN クライアントの VPN プールです。各設定によって、VPN クライアント ユーザは、管理インターフェイスの IP アドレスを使用して、ASA に対して ASDM または SSH に接続することができます。

VPN クライアント ユーザのみに ASDM または HTTP へのアクセスを許可（およびその他のユーザへのアクセスを拒否）するには、次のコマンドを入力します。

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.10.0 255.255.255.0 management_interface
```

VPN クライアント ユーザのみに SSH を使用した ASA へのアクセスを許可（およびその他のユーザへのアクセスを拒否）するには、次のコマンドを入力します。

```
ciscoasa(config)# ssh 192.168.10.0 255.255.255.0 management_interface
```

管理インターフェイスの設定

管理インターフェイスを設定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [Management Interface] ペインの [Management Access Interface] ドロップダウン リストから、セキュリティ レベルの最も高いインターフェイス（内部インターフェイス）を選択します。

ステップ 2　[Apply] をクリックします。

管理インターフェイスが割り当てられ、変更内容が実行コンフィギュレーションに保存されます。

システム管理者用 AAA の設定

この項では、システム管理者の認証とコマンド許可をイネーブルにする方法について説明します。

システム管理者用 AAA に関する情報

この項では、システム管理者用 AAA について説明します。

管理認証に関する情報

ここでは、管理アクセスの認証について説明します。

- 「認証がある場合とない場合の CLI アクセスの比較」（P.36-11）
- 「認証がある場合とない場合の ASDM アクセスの比較」（P.36-11）
- 「スイッチから ASA サービス モジュールへのセッションの認証」（P.36-11）

認証がある場合とない場合の CLI アクセスの比較

ASA へのログイン方法は、認証をイネーブルにしているかどうかによって異なります。

- 認証なし：Telnet の認証をイネーブルにしていない場合は、ユーザ名を入力しません。ログイン パスワードを入力します （SSH は認証なしでは使用できません）。ユーザ EXEC モードにアクセスします。
- 認証あり：この項の説明に従って Telnet または SSH 認証をイネーブルにした場合は、AAA サーバまたはローカル ユーザ データベースで定義されているユーザ名とパスワードを入力します。ユーザ EXEC モードにアクセスします。

ログイン後に特権 EXEC モードに入るには、**enable** コマンドを入力します。**enable** の動作は、認証をイネーブルにしているかどうかによって異なります。

- 認証なし：enable 認証を設定していない場合は、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力します。ただし、enable 認証を使用しない場合、**enable** コマンドを入力した後は、特定のユーザとしてログインしていません。ユーザ名を維持するには、enable 認証を使用してください。
- 認証あり：enable 認証を設定する場合は、ASA によってユーザ名とパスワードの入力を求めるプロンプトが再度表示されます。この機能は、ユーザが入力できるコマンドを判別するためにユーザ名が重要な役割を果たすコマンド許可を実行する場合に特に役立ちます。

ローカル データベースを使用する enable 認証の場合は、**enable** コマンドの代わりに **login** コマンドを使用できます。**login** によりユーザ名が維持されますが、認証をオンにするための設定は必要ありません。

認証がある場合とない場合の ASDM アクセスの比較

デフォルトでは、ブランクのユーザ名とイネーブル パスワードを使用して ASDM にログインできます。ログイン画面で（ユーザ名をブランクのままにしないで）ユーザ名とパスワードを入力した場合は、ASDM によってローカル データベースで一致がチェックされることに注意してください。

HTTP 認証を設定した場合は、ユーザ名をブランクのままにし、イネーブル パスワードを指定して ASDM を使用することはできなくなります。

スイッチから ASA サービス モジュールへのセッションの認証

スイッチから ASASM へのセッションの場合は（**session** コマンドを使用）、Telnet 認証を設定できます。スイッチから ASASM への仮想コンソール接続の場合は（**service-module session** コマンドを使用）、シリアル ポート認証を設定できます。

マルチ コンテキスト モードでは、システム コンフィギュレーションで AAA コマンドを設定できません。ただし、Telnet またはシリアル認証を管理コンテキストで設定した場合、認証はスイッチから ASASM へのセッションにも適用されます。この場合、管理コンテキストの AAA サーバまたはローカル ユーザ データベースが使用されます。

コマンド許可に関する情報

この項では、コマンド許可について説明します。

- 「サポートされるコマンド許可方式」（P.36-12）
- 「ユーザ クレデンシャルの維持について」（P.36-12）
- 「セキュリティ コンテキストとコマンド許可」（P.36-13）

サポートされるコマンド許可方式

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル：ASA でコマンド特権レベルを設定します。ローカル ユーザ、RADIUS ユーザ、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）を CLI アクセスについて認証する場合、ASA はそのユーザをローカル データベース、RADIUS、または LDAP サーバで定義されている特権レベルに所属させます。ユーザは、割り当てられた特権レベル以下のコマンドにアクセスできます。すべてのユーザは、初めてログインするときに、ユーザ EXEC モード（レベル 0 または 1 のコマンド）にアクセスします。ユーザは、特権 EXEC モード（レベル 2 以上のコマンド）にアクセスするために再び **enable** コマンドで認証するか、**login** コマンドでログイン（ローカル データベースに限る）できます。

（注）ローカル データベース内にユーザが存在しなくても、また CLI 認証や **enable** 認証がない場合でも、ローカル コマンド許可を使用できます。代わりに、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力すると、ASA によってレベル 15 に置かれます。次に、すべてのレベルのイネーブル パスワードを作成します。これにより、**enable** *n*（2 ～ 15）を入力したときに、ASA によってレベル *n* に置かれるようになります。これらのレベルは、ローカル コマンド許可をイネーブルにするまで使用されません（「ローカル コマンド許可の設定」（P.36-22）を参照）。**enable** コマンドの詳細については、コマンド リファレンスを参照してください。

- TACACS+ サーバ特権レベル：TACACS+ サーバで、ユーザまたはグループが CLI アクセスについて認証した後で使用できるコマンドを設定します。CLI でユーザが入力するすべてのコマンドは、TACACS+ サーバで検証されます。

ユーザ クレデンシャルの維持について

ユーザが ASA にログインする場合、ユーザ名とパスワードを入力して認証される必要があります。ASA は、同じセッションで後ほど認証が再び必要になる場合に備えて、これらのセッション クレデンシャルを保持します。

次の設定が行われている場合、ユーザはログイン時にローカル サーバだけで認証されればよいことになります。その後に続く認可では、保存されたクレデンシャルが使用されます。また、特権レベル 15 のパスワードの入力を求めるプロンプトが表示されます。特権モードを出るときに、ユーザは再び認証されます。ユーザのクレデンシャルは特権モードでは保持されません。

- ローカル サーバは、ユーザ アクセスの認証を行うように設定されます。
- 特権レベル 15 のコマンド アクセスは、パスワードを要求するように設定されます。
- ユーザのアカウントは、シリアル認可専用（コンソールまたは ASDM へのアクセスなし）として設定されます。
- ユーザのアカウントは、特権レベル 15 のコマンド アクセス用に設定されます。

次の表に、ASA でのクレデンシャルの使用方法を示します。

必要なクレデンシャル	ユーザ名とパスワードによる認証	シリアル（Serial）認可	特権モード コマンド許可	特権モード終了認可
ユーザ名	Yes	No	No	Yes
パスワード	Yes	No	No	Yes
特権モードのパスワード	No	No	Yes	No

セキュリティ コンテキストとコマンド許可

マルチ セキュリティ コンテキストでコマンド許可を実装する場合の重要な考慮点を次に示します。

- AAA 設定はコンテキストごとに個別であり、コンテキスト間で共有されません。

  コマンド許可を設定する場合は、各セキュリティ コンテキストを別々に設定する必要があります。この設定により、異なるセキュリティ コンテキストに対して異なるコマンド許可を実行できます。

  セキュリティ コンテキストを切り替える場合、管理者は、ログイン時に指定したユーザ名で許可されるコマンドが新しいコンテキスト セッションでは異なる可能性があることや、新しいコンテキストではコマンド許可がまったく設定されていない可能性があることを念頭に置いてください。コマンド許可がセキュリティ コンテキストによって異なる場合があることを管理者が理解していないと、混乱が生じる可能性があります。この動作は、次の仕組みによってさらに複雑になります。

- **changeto** コマンドによって開始された新しいコンテキスト セッションでは、前のコンテキスト セッションで使用されたユーザ名に関係なく、管理者 ID として常にデフォルトの「enable_15」ユーザ名が使用されます。これにより、enable_15 ユーザに対してコマンド許可が設定されていない場合や、enable_15 ユーザの認可が前のコンテキスト セッションでのユーザの認可と異なる場合に、混乱が生じる可能性があります。

  これは、発行される各コマンドを特定の管理者に正確に関連付けることができる場合に限り有効となる、コマンド アカウンティングにも影響します。**changeto** コマンドを使用する権限を持つすべての管理者は、enable_15 ユーザ名を他のコンテキストで使用できるため、誰が enable_15 ユーザ名としてログインしたかをコマンド アカウンティング レコードで識別することが困難になる場合があります。コンテキストごとに異なるアカウンティング サーバを使用する場合は、enable_15 ユーザ名を使用していたユーザを追跡するために数台のサーバのデータを相関させる必要が生じます。

  コマンド許可を設定する場合は、次の点を考慮します。

  - **changeto** コマンドの使用が許可されている管理者は、実質的に、他のコンテキストそれぞれで enable_15 ユーザに許可されているすべてのコマンドを使用する許可を持ちます。
  - コンテキストごとに別々にコマンドを認可する場合は、**changeto** コマンドの使用許可を持つ管理者に対しても拒否されるコマンドが enable_15 ユーザ名でも拒否されることを、各コンテキストで確認してください。

  セキュリティ コンテキストを切り替える場合、管理者は特権 EXEC モードを終了し、再度 **enable** コマンドを入力して必要なユーザ名を使用できます。

（注） システム実行スペースでは AAA コマンドがサポートされないため、システム実行スペースではコマンド許可を使用できません。

システム管理者用 AAA のライセンス要件

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

前提条件

AAA サーバまたはローカル データベースの前提条件

AAA サーバまたはローカル データベースでユーザを設定する必要があります。AAA サーバに、ASA と通信するように設定する必要があります。次の章を参照してください。

- AAA サーバ：該当する AAA サーバタイプの章を参照してください。
- ローカルデータベース：「ユーザ アカウントのローカル データベースへの追加」（P.28-3）を参照してください。

管理認証の前提条件

ASA において Telnet ユーザ、SSH ユーザ、または HTTP ユーザを認証できるようにするには、その前に ASA との通信を許可されている IP アドレスを特定する必要があります。ASASM の場合、マルチコンテキスト モードのシステムへのアクセスについては例外です。この場合、スイッチから ASASM へのセッションは Telnet セッションですが、Telnet アクセスの設定は不要です。詳細については、「ASDM、Telnet、または SSH の ASA アクセスの設定」（P.36-1）を参照してください。

ローカル コマンド許可の前提条件

- **enable** 認証を設定します （「CLI、ASDM、および enable コマンド アクセスの認証の設定」（P.36-16）を参照）。

  enable 認証は、ユーザが **enable** コマンドにアクセスした後にユーザ名を保持するためには不可欠です。

  あるいは、設定を必要としない **login** コマンド（これは、認証されている **enable** コマンドと同じでローカル データベースの場合に限る）を使用することもできます。このオプションは **enable** 認証ほど安全ではないため、お勧めしません。

  CLI 認証を使用することもできますが、必須ではありません。
- 次に示すユーザ タイプごとの前提条件を確認してください。
  - ローカル データベース ユーザ：ローカル データベース内の各ユーザの特権レベルを 0 ～ 15 で設定します。
  - RADIUS ユーザ：ユーザの Cisco VSA CVPN3000-Privilege-Level を、0 ～ 15 の値で設定します。
  - LDAP ユーザ：ユーザを特権レベル 0 ～ 15 の間で設定し、次に「LDAP 属性マップの設定」（P.31-5）の説明に従って、LDAP 属性を Cisco VSA CVPN3000-Privilege-Levelにマッピングします。

TACACS+ コマンド許可の前提条件

- CLI および **enable** 認証を設定します（「CLI、ASDM、および enable コマンド アクセスの認証の設定」（P.36-16）を参照）。

管理アカウンティングの前提条件

- CLI および **enable** 認証を設定します（「CLI、ASDM、および enable コマンド アクセスの認証の設定」（P.36-16）を参照）。

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

デフォルト設定

デフォルトのコマンド特権レベル

デフォルトでは、次のコマンドが特権レベル 0 に割り当てられます。その他のすべてのコマンドは特権レベル 15 に割り当てられます。

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

コンフィギュレーション モード コマンドを 15 より低いレベルに移動する場合は、**configure** コマンドも同じレベルに移動してください。このようにしないと、ユーザはコンフィギュレーション モードに入ることができません。

すべての特権レベルを表示する方法は、「ローカル コマンド特権レベルの表示」（P.36-24）を参照してください。

CLI、ASDM、および enable コマンド アクセスの認証の設定

CLI、ASDM、および enable コマンドの認証を要求することができます。

前提条件

- 「ASDM、Telnet、または SSH の ASA アクセスの設定」（P.36-1）に従って Telnet、SSH、または HTTP アクセスを設定します。
- SSH アクセスするためは、SSH 認証を設定する必要があります。デフォルトのユーザ名はありません。

手順の詳細

ステップ 1　**enable** コマンドを使用するユーザを認証する場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] の順に選択し、次のように設定を行います。

a. [Enable] チェックボックスを選択します。

b. [Server Group] ドロップダウン リストから、サーバ グループ名または LOCAL データベースを選択します。

c. （オプション）AAA サーバを選択する場合は、AAA サーバが使用不可になった場合のフォールバック方式としてローカル データベースが使用されるように ASA を設定できます。[Use LOCAL when server group fails] チェックボックスをオンにします。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、ASA のプロンプトでは、いずれの方式が使用されているかが示されないためです。

ステップ 2　CLI または ASDM にアクセスするユーザを認証する場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] の順に選択し、次のように設定を行います。

a. 次のチェックボックスをオンにします（複数可）。

- [HTTP/ASDM]：HTTPS を使用して ASDM にアクセスする ASA クライアントを認証します。HTTP 管理認証では、AAA サーバ グループの SDI プロトコルをサポートしていません。
- [Serial]：コンソール ポートを使用して ASA にアクセスするユーザを認証します。ASASM の場合、このパラメータは **service-module session** コマンドを使用してスイッチからアクセスする仮想コンソールにも影響します。マルチ モード アクセスについては、「スイッチから ASA サービス モジュールへのセッションの認証」（P.36-11）を参照してください。
- [SSH]：SSH を使用して ASA にアクセスするユーザを認証します。
- [Telnet]：Telnet を使用して ASA にアクセスするユーザを認証します。ASASM の場合、このパラメータは **session** コマンドを使用するスイッチからのセッションにも影響します。マルチ モード アクセスについては、「スイッチから ASA サービス モジュールへのセッションの認証」（P.36-11）を参照してください。

b. 対応するチェックボックスをオンにしたサービスごとに、[Server Group] ドロップダウン リストから、サーバ グループ名または LOCAL データベースを選択します。

c. （オプション）AAA サーバを選択する場合は、AAA サーバが使用不可になった場合のフォールバック方式としてローカル データベースが使用されるように ASA を設定できます。[Use LOCAL when server group fails] チェックボックスをオンにします。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、ASA のプロンプトでは、いずれの方式が使用されているかが示されないためです。

ステップ 3　[Apply] をクリックします。

管理認可によるユーザ CLI および ASDM アクセスの制限

ASA を使用すると、RADIUS、LDAP、TACACS+、またはローカル ユーザ データベースを使用して認証する場合に、管理ユーザとリモート アクセス ユーザを区別することができます。ユーザ ロールを区別することで、リモート アクセス VPN ユーザやネットワーク アクセス ユーザが ASA に管理接続を確立するのを防ぐことができます。

（注）　シリアル アクセスは管理認可に含まれないため、を設定している[Authentication] > [Serial] オプションをイネーブルにしている場合は、認証したユーザはすべてコンソール ポートにアクセスできます。

手順の詳細

ステップ 1　次のいずれかのオプションを選択します。

- 管理認可をイネーブルにする場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] の順に選択し、[Perform authorization for exec shell access] > [Enable] チェックボックスをオンにします。

  LOCAL オプションを設定するときは、ローカル ユーザのデータベースは入力したユーザ名と割り当てられた Service-Type および Privilege-Level 属性のソースとなります。

  このオプションを選択すると、RADIUS の管理ユーザ特権レベルのサポートもイネーブルになります。管理ユーザ特権レベルは、ローカル コマンド特権レベルと組み合わせて、コマンド許可に使用できます。詳細については、「ローカル コマンド許可の設定」（P.36-22）を参照してください。

  authentication-server オプションが設定されているときは、認証と許可の両方に同じサーバーを使用します。

- 管理認可をイネーブルにするには、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] の順に選択し、[Allow privileged users to enter into EXEC mode on login] チェックボックスをオンにします。

  auto-enable オプションによって、十分な特権を有するユーザは特権 EXEC モード内にログイン認証サーバーから直接入ることが可能となります。それ以外では、ユーザはユーザ EXEC モードになります。これらの特権は、各 EXEC モードに入るために必要な Service-Type および Privilege-Level 属性で決定されます。特権 EXEC モードを開始するには、ユーザは Administrative の Service-Type 属性およびそれらに割り当てられた 1 以上の Privilege Level 属性を有している必要があります。

  このオプションは、システム コンテキストではサポートされていません。ただし、Telnet またはシリアル認証を管理コンテキストで設定した場合、認証はスイッチから ASASM へのセッションにも適用されます。

aaa authorization exec コマンドを単独で入力しても効果はありません。

管理認可でシリアル認証を使用するときは、**auto-enable** オプションは含まれません。

aaa authentication http コマンドは **auto-enable** オプションの影響を受けません。

auto-enable オプションを設定する前に、プロトコル ログインと enable 認証の両方を設定し、以下の例で示すようにすべての認証要求が同じ AAA サーバ グループに向かうように設定することをお勧めします。

```
ciscoasa (config)# aaa authentication ssh console RADIUS
ciscoasa (config)# aaa authentication enable console RADIUS
ciscoasa (config)# aaa authorization exec authentication-server auto-enable
```

別のタイプの設定を使用することは推奨*されません*。

ステップ 2　ユーザを管理認証対象に設定するには、次の各 AAA サーバ タイプまたはローカル ユーザの要件を参照してください。

RADIUS または LDAP（マッピング済み）ユーザ

ユーザが LDAP 経由で認証される場合、ネイティブ LDAP 属性およびその値は Cisco ASA 属性にマッピングされ、特定の認可機能を提供します。Cisco VSA CVPN3000-Privilege-Level を、0 ～ 15 の値で設定します。次に、LDAP 属性を Cisco VAS CVPN3000-Privilege-Level にマッピングします。詳細については、「LDAP 属性マップの設定」（P.31-5）を参照してください。

RADIUS IETF の **service-type** 属性が、RADIUS 認証および許可要求の結果として access-accept メッセージで送信される場合、この属性は認証されたユーザにどのタイプのサービスを付与するかを指定するために使用されます。

- Service-Type 6（管理）: [Authentication] タブ オプションで指定されたサービスへのフル アクセスを許可します。
- Service-Type 7（NAS プロンプト）: Telnet または SSH 認証オプションを設定した場合は CLI へのアクセスを許可しますが、HTTP オプションを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。[Enable] オプションで **enable** 認証を設定している場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。Framed (2) および Login (1) サービス タイプは同様に扱われます。
- Service-Type 5（発信）: 管理アクセスを拒否します。ユーザは [Authentication] タブ オプションで指定されたサービスを使用できません（[Serial] オプションを除きます。シリアル アクセスは許可されます）。リモート アクセス（IPsec および SSL）ユーザは、引き続き自身のリモート アクセス セッションを認証および終了できます。他のすべてのサービス タイプ（ボイス、ファクスなど）も同様に処理されます。

RADIUS Cisco VSA **privilege-level** 属性（ベンダー ID 3076、サブ ID 220）が access-accept メッセージで送信される場合は、ユーザの権限レベルを指定するために使用されます。

認証されたユーザが ASDM、SSH、または Telnet を使用して ASA に管理アクセスを試みたものの、これを実行するために必要な特権レベルを持っていないと、ASA から syslog メッセージ 113021 が生成されます。このメッセージは、管理者権限が不適切であるためログインに失敗したことをユーザに通知するものです。

TACACS+ ユーザ

「service=shell」で許可が要求され、サーバは PASS または FAIL で応答します。

- PASS、特権レベル 1 : [Authentication] タブのオプションで指定されたすべてのサービスへのフル アクセスを許可します。

- PASS、特権レベル 2 以上：Telnet または SSH 認証オプションを設定した場合は CLI へのアクセスを許可しますが、HTTP オプションを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。[Enable] オプションで **enable** 認証を設定している場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。イネーブルの特権レベルが 14 以下に設定されている場合は、**enable** コマンドを使用して特権 EXEC モードにアクセスすることはできません。
- FAIL：管理アクセスを拒否します。[Authentication] タブ オプションで指定されたサービスを使用できません（[Serial] オプションを除きます。シリアル アクセスは許可されます）。

ローカル ユーザ

指定したユーザ名の [Access Restriction] オプションを設定します。アクセス制限のデフォルト値は [Full Access] です。この場合は、[Authentication] タブのオプションで指定されたすべてのサービスに対して、フル アクセスが許可されます。詳細については、「ユーザ アカウントのローカル データベースへの追加」（P.28-3）を参照してください。

ローカル データベース ユーザのパスワード ポリシーの設定

ローカル データベースを使用して CLI または ASDM アクセスの認証を設定する場合は、指定期間を過ぎるとユーザにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワード ポリシーを設定することができます。

パスワード ポリシーはローカル データベースを使用する管理ユーザに対してのみ適用されます。ローカル データベースを使用するその他のタイプのトラフィック（VPN や AAA によるネットワーク アクセスなど）や、AAA サーバによって認証されたユーザには適用されません。

- 「パスワード ポリシーの設定」（P.36-19）
- 「パスワードの変更」（P.36-21）

パスワード ポリシーの設定

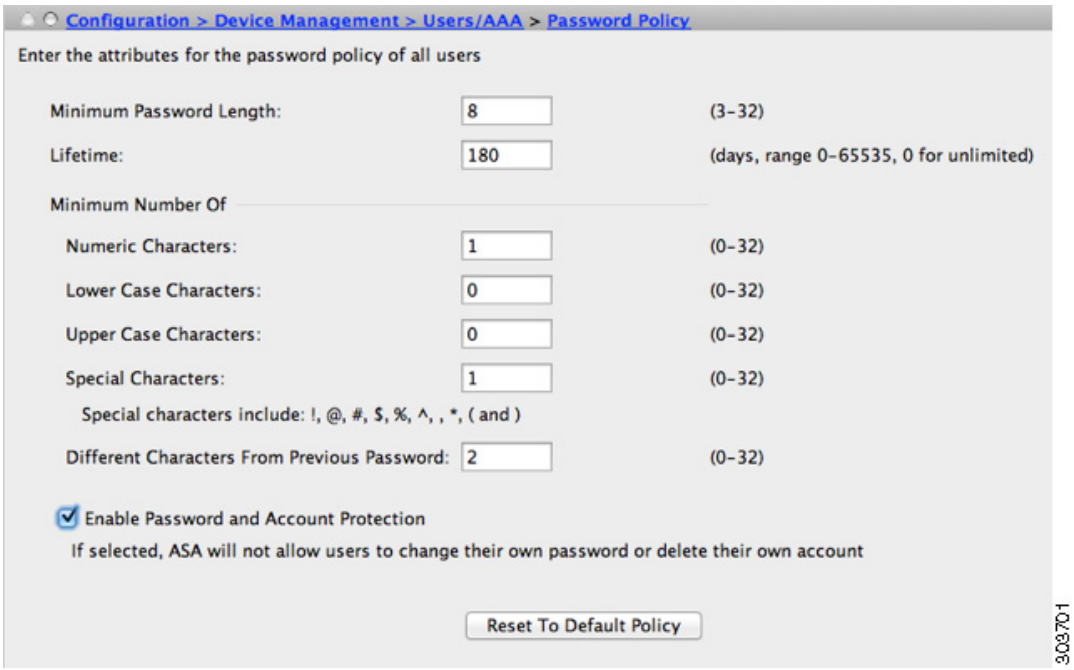
パスワード ポリシーの設定後は、自分または別のユーザのパスワードを変更すると、新しいパスワードに対してパスワード ポリシーが適用されます。あらゆる既存のパスワードは、対象外です。新しいポリシーは、[User Accounts] ペインおよび [Change My Password] ペインを使用したパスワードの変更に適用されます。

前提条件

- 「CLI、ASDM、および enable コマンド アクセスの認証の設定」（P.36-16）に従って、CLI/ASDM および enable 認証の両方を設定します。ローカル データベースの指定を忘れないでください。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [Password Policy] の順に選択します。



ステップ 2　次のオプションを任意に組み合わせて設定します。

- [Minimum Password Length]：パスワードの最短長を入力します。有効値の範囲は 3 ～ 64 文字です。推奨されるパスワードの最小長は 8 文字です。
- [Lifetime]：リモート ユーザ（SSH、Telnet、HTTP）のパスワードの有効期間を日数で指定します。コンソール ポートのユーザが、パスワードの有効期限切れでロックされることはありません。有効な値は、0 ～ 65536 です。デフォルト値は 0 日です。この場合、パスワードは決して期限切れになりません。

  パスワードの有効期限が切れる 7 日前に、警告メッセージが表示されます。パスワードの有効期限が切れると、リモート ユーザのシステム アクセスは拒否されます。有効期限が切れた後アクセスするには、次のいずれかの手順を実行します。

  – 他の管理者にパスワードを変更してもらいます。
  – 物理コンソール ポートにログインして、パスワードを変更します。
- [Minimum Number Of]：次のタイプの最短文字数を指定します。
  – [Numeric Characters]：パスワードに含まれなければならない数字の最短文字数を入力します。有効な値は、0 ～ 64 文字です。デフォルト値は 0 です
  – [Lower Case Characters]：パスワードに含まれなければならない小文字の最短文字数を入力します。有効値の範囲は 0 ～ 64 文字です。デフォルト値は 0 です
  – [Upper Case Characters]：パスワードに含まれなければならない大文字の最短文字数を入力します。有効値の範囲は 0 ～ 64 文字です。デフォルト値は 0 です
  – [Special Characters]：パスワードに含まれなければならない特殊文字の最短文字数を入力します。有効値の範囲は 0 ～ 64 文字です。特殊文字には、!、@、#、$、%、^、&、*、(、) が含まれます。デフォルト値は 0 です。
  – [Different Characters from Previous Password]：新しいパスワードと古いパスワードで違わなければならない最小文字数を入力します。有効な値は、0 ～ 64 文字です。デフォルト値は 0 です 文字マッチングは位置に依存しません。したがって、新しいパスワードで使用される文字が、現在のパスワードのどこにも使用されていない場合に限り、パスワードが変更されたとみなされます。

ステップ 3　（オプション）[Authentication Enable] チェックボックスをオンにして、ユーザが [User Accounts] ペインではなく、[Change My Password] ペインでパスワードを変更するようにします。デフォルト設定はディセーブルです。どちらの方法でも、ユーザはパスワードを変更することができます。

この機能をイネーブルにすると、[User Accounts] ペインでパスワードを変更しようとしても、次のエラー メッセージが表示されます。

```
ERROR: Changing your own password is prohibited
```

ステップ 4　パスワード ポリシーをデフォルトにリセットするには、[Reset to Default] をクリックします。

ステップ 5　[Apply] をクリックして、設定を適用します。

パスワードの変更

パスワード ポリシーでパスワードの有効期間を設定した場合、有効期間を過ぎるとパスワードを新しいパスワードに変更する必要があります。パスワード ポリシー認証をイネーブルにした場合は、このパスワード変更メソッドが必要です。パスワード ポリシー認証がイネーブルでない場合は、このメソッドを使用することも、[User Accounts] ペインを使用して直接ユーザ アカウントを変更することもできます。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [Change Password] の順に選択します。

ステップ 2　古いパスワードを入力します。

ステップ 3　新しいパスワードを入力します。

ステップ 4　確認のために新しいパスワードを再度入力します。

ステップ 5　[Make Change] をクリックします。

ステップ 6　[Save] アイコンをクリックして、実行コンフィギュレーションに変更を保存します。

コマンド許可の設定

コマンドへのアクセスを制御する場合、ASA ではコマンド許可を設定でき、ユーザが使用できるコマンドを決定できます。デフォルトでは、ログインするとユーザ EXEC モードにアクセスでき、最低限のコマンドだけが提供されます。**enable** コマンド（または、ローカル データベースを使用するときは **login** コマンド）を入力すると、特権 EXEC モードおよびコンフィギュレーション コマンドを含む高度なコマンドにアクセスできます。

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル
- TACACS+ サーバ特権レベル

このコマンド許可の詳細については、「コマンド許可に関する情報」（P.36-12）を参照してください。

- 「ローカル コマンド許可の設定」（P.36-22）
- 「ローカル コマンド特権レベルの表示」（P.36-24）
- 「TACACS+ サーバでのコマンドの設定」（P.36-24）
- 「TACACS+ コマンド許可の設定」（P.36-26）

ローカル コマンド許可の設定

ローカル コマンド許可を使用して、コマンドを 16 の特権レベル（0 ～ 15）の 1 つに割り当てることができます。デフォルトでは、各コマンドは特権レベル 0 または 15 に割り当てられます。各ユーザを特定の特権レベルに定義でき、各ユーザは割り当てられた特権レベル以下のコマンドを入力できます。ASA は、ローカル データベース、RADIUS サーバ、または LDAP サーバ（LDAP 属性を RADIUS 属性にマッピングする場合）に定義されているユーザ特権レベルをサポートしています。詳細については、次の項を参照してください。

- 「ユーザ アカウントのローカル データベースへの追加」（P.28-3）
- 「サポートされている認証方式」（P.29-2）
- 「LDAP 属性マップの設定」（P.31-5）

ローカル コマンド許可を設定するには、次の手順を実行します。

手順の詳細

ステップ 1　コマンド許可をイネーブルにする場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] の順に選択し、[Enable authorization for command access] > [Enable] チェックボックスをオンにします。

ステップ 2　[Server Group] ドロップダウン リストから、[LOCAL] を選択します。

ステップ 3　ローカル コマンド許可をイネーブルにすると、オプションで、特権レベルを個々のコマンドまたはコマンド グループに手動で割り当てたり、事前定義済みユーザ アカウント特権をイネーブルにしたりできます。

- 事前定義済みユーザ アカウント特権を使用する場合は、[Set ASDM Defined User Roles] をクリックします。

  [ASDM Defined User Roles Setup] ダイアログボックスに、コマンドとそのレベルが表示されます。[Yes] をクリックすると、事前定義済みユーザ アカウント特権を使用できるようになります。事前定義済みユーザ アカウント特権には、[Admin]（特権レベル 15、すべての

CLI コマンドへのフル アクセス権）、[Read Only]（特権レベル 5、読み取り専用アクセス権）、[Monitor Only]（特権レベル 3、[Monitoring] セクションへのアクセス権のみ）があります。

- コマンド レベルを手動で設定する場合は、[Configure Command Privileges] をクリックします。

  [Command Privileges Setup] ダイアログボックスが表示されます。[Command Mode] ドロップダウン リストから [--All Modes--] を選択すると、すべてのコマンドを表示できます。代わりに、コンフィギュレーション モードを選択し、そのモードで使用可能なコマンドを表示することもできます。たとえば、[context] を選択すると、コンテキスト コンフィギュレーション モードで使用可能なすべてのコマンドを表示できます。コンフィギュレーション モードだけでなく、ユーザ EXEC モードや特権 EXEC モードでも入力が可能で、かつモードごとに異なるアクションが実行されるようなコマンドを使用する場合は、これらのモードに対して別個に特権レベルを設定できます。

  [Variant] カラムには、[show]、[clear]、または [cmd] が表示されます。特権は、コマンドの show 形式、clear 形式、または configure 形式に対してのみ設定できます。コマンドの configure 形式は、通常、未修正コマンド（**show** または **clear** プレフィックスなしで）または **no** 形式として、コンフィギュレーションの変更を引き起こす形式です。

  コマンドのレベルを変更する場合は、コマンドをダブルクリックするか、[Edit] をクリックします。レベルは 0 ～ 15 の範囲で設定できます。設定できるのは、*main* コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルを個別に設定できません。

  表示されているすべてのコマンドのレベルを変更する場合は、[Select All] をクリックした後に、[Edit] をクリックします。

  [OK] をクリックして変更内容を確定します。

ステップ 4　RADIUS の管理ユーザ特権レベルをサポートする場合は、[Perform authorization for exec shell access] **>** [Enable] チェックボックスをオンにします。

このオプションを設定しないと、ASA ではローカル データベース ユーザの特権レベルだけがサポートされ、他のタイプのユーザにはデフォルトのレベル 15 がそのまま適用されます。

また、このオプションを設定すると、ローカル ユーザ、RADIUS ユーザ、マッピング済み LDAP ユーザ、TACACS+ ユーザに対する管理認可がイネーブルになります。詳細については、「管理認可によるユーザ CLI および ASDM アクセスの制限」（P.36-17）を参照してください。

ステップ 5　[Apply] をクリックします。

許可設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されます。

ローカル コマンド特権レベルの表示

次のコマンドを [Tools] > [Command Line Interface tool] に入力すると、コマンドの特権レベルを表示できます。

TACACS+ サーバでのコマンドの設定

グループまたは個々のユーザの共有プロファイル コンポーネントとしての Cisco Secure Access Control Server（ACS）TACACS+ サーバでコマンドを設定できます。サードパーティの TACACS+ サーバの場合は、コマンド許可サポートの詳細については、ご使用のサーバのマニュアルを参照してください。

Cisco Secure ACS バージョン 3.1 でコマンドを設定する場合は、次のガイドラインを参照してください。

- ASA は、「シェル」コマンドとして認可するコマンドを送信し、TACACS+ サーバでシェル コマンドとしてコマンドを設定します。

（注） Cisco Secure ACS には、「pix-shell」と呼ばれるコマンド タイプが含まれている場合があります。このタイプは ASA コマンド許可に使用しないでください。

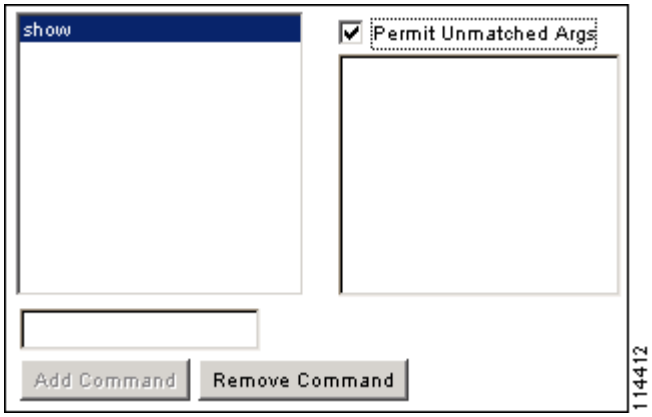
- コマンドの最初のワードは、メイン コマンドと見なされます。その他のワードはすべて引数と見なされます。これは、**permit** または **deny** の後に置く必要があります。

  たとえば、**show running-configuration aaa-server** コマンドを許可するには、コマンド フィールドに **show running-configuration** を追加し、引数フィールドに **permit aaa-server** を入力します。

- [Permit Unmatched Args] チェックボックスをオンにすると、明示的に拒否していないすべてのコマンド引数を許可できます。

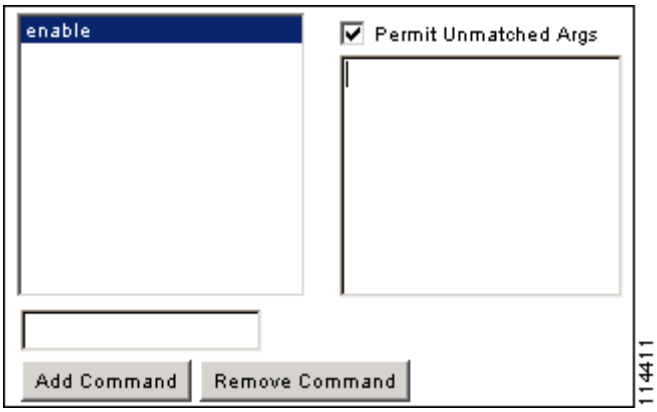
  たとえば、特定の **show** コマンドを設定するだけで、すべての **show** コマンドが許可されます。CLI の使用法を示す疑問符や省略形など、コマンドの変形をすべて予想する必要がなくなるので、この方法を使用することをお勧めします（図 36-1 を参照）。

図 36-1　　関連するすべてのコマンドの許可



- **enable** や **help** など、単一ワードのコマンドについては、そのコマンドに引数がない場合でも、一致しない引数を許可する*必要があります*（図 36-2 を参照）。

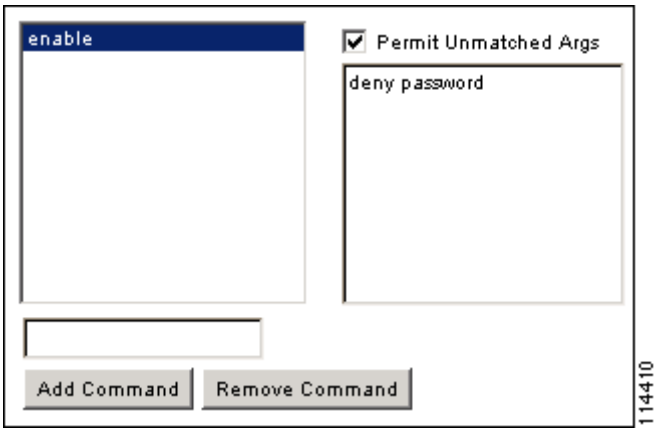
図 36-2　　単一ワードのコマンドの許可



- 引数を拒否するには、その引数の前に **deny** を入力します。

  たとえば、**enable** コマンドを許可し、**enable password** コマンドを許可しない場合には、コマンド フィールドに **enable** を入力し、引数フィールドに **deny password** を入力します。**enable** だけが許可されるように、必ず、[Permit Unmatched Args] チェックボックスを選択してください（図 36-3 を参照）。

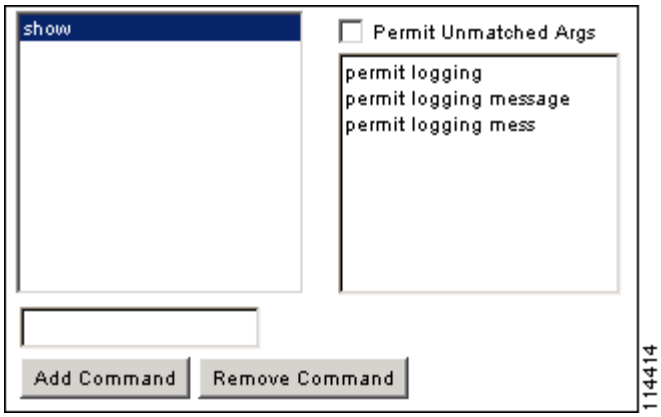
図 36-3　　引数の拒否



- コマンドラインでコマンドを省略形で入力した場合、ASA はプレフィックスとメイン コマンドを完全なテキストに展開しますが、その他の引数は入力したとおりに TACACS+ サーバに送信します。

  たとえば、**sh log** と入力すると、ASA は完全なコマンド **show logging** を TACACS+ サーバに送信します。一方、**sh log mess** と入力すると、ASA は展開されたコマンド **show logging message** ではなく、**show logging mess** を TACACS+ サーバに送信します。省略形を予想して同じ引数に複数のスペルを設定できます（図 36-4 を参照）。

図 36-4　省略形の指定



- すべてのユーザに対して次の基本コマンドを許可することをお勧めします。
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**
  - **logout**
  - **pager**
  - **show pager**
  - **clear pager**
  - **quit**
  - **show version**

TACACS+ コマンド許可の設定

TACACS+ コマンド許可をイネーブルにし、ユーザが CLI でコマンドを入力すると、ASA はそのコマンドとユーザ名を TACACS+ サーバに送信し、コマンドが認可されているかどうかを判別します。

TACACS+ コマンド許可をイネーブルにする前に、TACACS+ サーバで定義されたユーザとして ASA にログインしていること、および ASA の設定を続けるために必要なコマンド許可があることを確認してください。たとえば、すべてのコマンドが認可された管理ユーザとしてログインする必要があります。このようにしないと、意図せずロックアウトされる可能性があります。

意図したとおりに機能することが確認できるまで、設定を保存しないでください。間違いによりロック アウトされた場合、通常は ASA を再起動することによってアクセスを回復できます。それでもロックアウトされたままの場合は、「ロックアウトからの回復」（P.36-29）を参照してください。

TACACS+ システムが完全に安定して信頼できることを確認します。必要な信頼性レベルについて、通常は、完全冗長 TACACS+ サーバ システムと ASA への完全冗長接続が必要です。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続された 1 つのサーバとインターフェイス 2 に接続された別のサーバを含めます。TACACS+ サーバが使用できない場合に

フォールバック方式としてローカル コマンド許可を設定することもできます。この場合は、「コマンド許可の設定」（P.36-22）に示されている手順に従ってローカル ユーザとコマンド特権レベルを設定する必要があります。

TACACS+ コマンド許可を設定するには、次の手順を実行します。

手順の詳細

ステップ 1　TACACS+ サーバを使用したコマンド許可を実行する場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] の順に選択し、[Enable authorization for command access] > [Enable] チェックボックスをオンにします。

ステップ 2　[Server Group] ドロップダウン リストから、AAA サーバ グループ名を選択します。

ステップ 3　（オプション）AAA サーバが使用不可になった場合のフォールバック方式としてローカル データベースが使用されるように ASA を設定できます。設定するには、[Use LOCAL when server group fails] チェックボックスをオンにします。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、ASA のプロンプトでは、いずれの方式が使用されているかが示されないためです。必ずローカル データベースのユーザ（「ユーザ アカウントのローカル データベースへの追加」（P.28-3）を参照）とコマンド特権レベル（「ローカル コマンド許可の設定」（P.36-22）を参照）を設定してください。

ステップ 4　[Apply] をクリックします。

コマンド許可設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されます。

管理アクセス アカウンティングの設定

CLI で **show** コマンド以外のコマンドを入力する場合、アカウンティング メッセージを TACACS+ アカウンティング サーバに送信できます。ユーザがログインするとき、ユーザが **enable** コマンドを入力するとき、またはユーザがコマンドを発行するときのアカウンティングを設定できます。

コマンド アカウンティングに使用できるサーバは、TACACS+ だけです。

管理アクセスおよびイネーブル コマンド アカウンティングを設定するには、次の手順を実行します。

手順の詳細

ステップ 1　ユーザが **enable** コマンドを入力した場合にそのユーザのアカウンティングをイネーブルにするには、次の手順を実行します。

a.　[Configuration] > [Device Management] > [Users/AAA] >[AAA Access] > [Accounting] の順に選択し、[Require accounting to allow accounting of user activity] > [Enable] チェックボックスをオンにします。

b.　[Server Group] ドロップダウン リストから、RADIUS サーバ グループまたは TACACS+ サーバ グループの名前を選択します。

ステップ 2　ユーザが Telnet、SSH、またはシリアル コンソールを使用して ASA にアクセスした場合にそのユーザのアカウンティングをイネーブルにするには、次の手順を実行します。

a.　[Require accounting for the following types of connections] 領域で、[Serial]、[SSH]、[Telnet] の中から目的のチェックボックスをオンにします（複数可）。

b. 接続タイプごとに、[Server Group] ドロップダウン リストから RADIUS サーバ グループまたは TACACS+ サーバ グループの名前を選択します。

ステップ 3　コマンド アカウンティングを設定するには、次の手順を実行します。

a. [Require command accounting] 領域で、[Enable] チェックボックスをオンにします。

b. [Server Group] ドロップダウン リストから、TACACS+ サーバ グループの名前を選択します。RADIUS はサポートされていません。

CLI で **show** コマンド以外のコマンドを入力する場合、アカウンティング メッセージを TACACS+ アカウンティング サーバに送信できます。

c. [Command Privilege Setup] ダイアログボックスを使用してコマンド特権レベルをカスタマイズする際、[Privilege level] ドロップダウン リストで最小特権レベルを指定することで、ASA のアカウンティング対象となるコマンドを制限できます。最小特権レベルよりも下のコマンドは、ASA で処理の対象となりません。

ステップ 4　[Apply] をクリックします。

アカウンティング設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されます。

現在のログイン ユーザの表示

現在のログイン ユーザを表示するには、[Tools] > [Command Line Interface tool] で。

```
ciscoasa# show curpriv
```

例

次に、**show curpriv** コマンドの出力例を示します。

```
ciscoasa# show curpriv
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```

表 36-1 に、**show curpriv** コマンドの出力の説明を示します。

表 36-1　show curpriv コマンド出力の説明

フィールド	説明
Username	ユーザ名。デフォルト ユーザとしてログインすると、名前は enable_1（ユーザ EXEC）または enable_15（特権 EXEC）になります。
Current privilege level	レベルの範囲は 0 ～ 15 です。ローカル コマンド許可を設定してコマンドを中間特権レベルに割り当てない限り、使用されるレベルはレベル 0 と 15 だけです。
Current Modes	使用可能なアクセス モードは次のとおりです。 • P_UNPR：ユーザ EXEC モード（レベル 0 と 1） • P_PRIV：特権 EXEC モード（レベル 2 ～ 15） • P_CONF：コンフィギュレーション モード

管理セッション割り当て量の設定

同時に実行できる管理セッションの最大数を設定できます。この最大値に達すると、それ以降のセッションは許可されず、syslog メッセージが生成されます。システム ロックアウトを回避するために、管理セッション割り当て量のメカニズムではコンソール セッションをブロックできません。

管理セッション割り当て量を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [Management Session Quota] の順に選択します。

ステップ 2　ASA で許可される ASDM、SSH、および Telnet の同時セッションの最大数を入力します。有効値の範囲は 0 ～ 10000 です。

（注）　クォータ管理セッション数を超えた場合、エラー メッセージが表示され、ASDM が閉じます。

ステップ 3　設定の変更を保存するには、[Apply] をクリックします。

ロックアウトからの回復

状況によっては、コマンド許可や CLI 認証をオンにすると、ASA CLI からロックアウトされる場合があります。通常は、ASA を再起動することによってアクセスを回復できます。ただし、すでにコンフィギュレーションを保存した場合は、ロックアウトされたままになる可能性があります。表 36-2 に、一般的なロックアウト条件と回復方法を示します。

表 36-2　CLI 認証およびコマンド許可のロックアウト シナリオ

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
ローカル CLI 認証	ローカル データベースにユーザが設定していない。	ローカル データベース内にユーザが存在しない場合は、ログインできず、ユーザの追加もできません。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザを追加することができます。

表 36-2　CLI 認証およびコマンド許可のロックアウト シナリオ （続き）

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
TACACS+ コマンド許可 TACACS+ CLI 認証 RADIUS CLI 認証	サーバがダウンしているか到達不能で、フォールバック方式を設定していない。	サーバが到達不能である場合は、ログインもコマンドの入力もできません。	1. ログインし、パスワードと AAA コマンドをリセットします。 2. サーバがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。	1. ASA でネットワーク コンフィギュレーションが正しくないためサーバが到達不能である場合は、スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてネットワークを再設定することができます。 2. サーバがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。
TACACS+ コマンド許可	十分な特権のないユーザまたは存在しないユーザとしてログインした。	コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できなくなります。	TACACS+ サーバのユーザ アカウントを修正します。 TACACS+ サーバへのアクセス権がなく、ASA をすぐに設定する必要がある場合は、メンテナンス パーティションにログインして、パスワードと **aaa** コマンドをリセットします。	スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてコンフィギュレーションの変更を完了することができます。また、TACACS+ コンフィギュレーションを修正するまでコマンド許可をディセーブルにすることもできます。
ローカル コマンド許可	十分な特権のないユーザとしてログインしている。	コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できなくなります。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザ レベルを変更することができます。

デバイス アクセスのモニタリング

デバイス アクセスをモニタするには、次のペインを参照してください。

パス	目的
[Monitoring] > [Properties] > [Device Access] > [ASDM/HTTPS/Telnet/SSH Sessions]	上部ペインには、ASDM、HTTPS、および Telnet のセッションを介して接続するユーザの接続タイプ、セッション ID、および IP アドレスが示されます。特定のセッションを切断するには、[Disconnect] をクリックします。 下部ペインには、クライアント、ユーザ名、接続ステータス、ソフトウェア バージョン、入力暗号化タイプ、出力暗号化タイプ、入力 HMAC、出力 HMAC、SSH セッション ID、残りのキー再生成データ、残りのキー再生成時間、データベースのキー再生成、時間ベースのキー再生成、最後のキー再生成の時間が表示されます。特定のセッションを切断するには、[Disconnect] をクリックします。
[Monitoring] > [Properties] > [Device Access] > [Authenticated Users]	AAA サーバによって認証されるユーザのユーザ名、IP アドレス、ダイナミック ACL、非アクティブ タイムアウト（ある場合）、および絶対タイムアウトが示されます。
[Monitoring] > [Properties] > [Device Access] > [AAA Local Locked Out Users]	ロックアウトされた AAA ローカル ユーザのユーザ名、失敗した認証の試行回数、およびユーザがロックアウトされた回数が示されます。ロックアウトされた特定のユーザをクリアするには、[Clear Selected Lockout] をクリックします。ロックアウトされたすべてのユーザをクリアするには、[Clear All Lockouts] をクリックします。

管理アクセスの機能履歴

表 36-3 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 36-3　管理アクセスの機能履歴

機能名	プラットフォーム リリース	機能情報
管理アクセス	7.0(1)	この機能が導入されました。 次の画面が導入されました。 [Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]。 [Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Banner]。 [Configuration] > [Device Management] > [Management Access] > [CLI Prompt]。 [Configuration] > [Device Management] > [Management Access] > [ICMP]。 [Configuration] > [Device Management] > [Management Access] > [File Access] > [FTP Client]。 [Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP) Server]。 [Configuration] > [Device Management] > [Management Access] > [File Access] > [Mount-Points]。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication]。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization]。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Accounting]。
SSH セキュリティが向上し、SSH デフォルト ユーザ名はサポートされなくなりました。	8.4(2)	8.4(2) 以降、pix または asa ユーザ名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、**aaa authentication ssh console LOCAL** コマンド（CLI）または [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication (ASDM)] を使用して AAA 認証を設定してから、ローカル ユーザを定義する必要があります。定義するには、**username** コマンド（CLI）を入力するか、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts (ASDM)] を選択します。ローカル データベースの代わりに AAA サーバを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。

表 36-3　管理アクセスの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
ローカル データベースを使用する場合の管理者パスワード ポリシーのサポート	8.4(4.1)、9.1(2)	ローカル データベースを使用して CLI または ASDM アクセスの認証を設定する場合は、指定期間を過ぎるとユーザにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワード ポリシーを設定することができます。 次の画面が導入されました。[Configuration] > [Device Management] > [Users/AAA] > [Password Policy]。
SSH 公開キー認証のサポート	8.4(4.1)、9.1(2)	ASA への SSH 接続の公開キー認証は、ユーザ単位でイネーブルにできます。公開キー ファイル（PKF）でフォーマットされたキーまたは Base64 キーを指定できます。PKF キーは、4096 ビットまで使用できます。Base64 形式（最大 2048 ビット）の ASA サポートには大きすぎるキーには、PKF 形式を使用します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Authentication] [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Using PKF]。 *PKF キー形式のサポートは 9.1(2) 以降のみです。*
SSH キー交換の Diffie-Hellman グループ 14 のサポート	8.4(4.1)、9.1(2)	SSH キー交換に Diffie-Hellman グループ 14 が追加されました。これまでは、グループ 1 だけがサポートされていました。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]。
管理セッションの最大数のサポート	8.4(4.1)、9.1(2)	同時 ASDM、SSH、Telnet セッションの最大数を設定することができます。 次の画面が導入されました。[Configuration] > [Device Management] > [Management Access] > [Management Session Quota]。
マルチ コンテキスト モードの ASASM において、スイッチからの Telnet 認証および仮想コンソール認証をサポートしました。	8.5(1)	マルチ コンテキスト モードのスイッチから ASASM への接続はシステム実行スペースに接続しますが、これらの接続を制御するために管理コンテキストでの認証を設定できます。
SSH の AES-CTR 暗号化	9.1(2)	ASA での SSH サーバの実装が、AES-CTR モードの暗号化をサポートするようになりました。
SSH キー再生成間隔の改善		SSH 接続は、接続時間 60 分間またはデータ トラフィック 1 GB ごとに再生成されます。 。

表 36-3　管理アクセスの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
改善されたワンタイム パスワード認証	9.2(1)	十分な認可特権を持つ管理者は、認証クレデンシャルを一度入力すると特権 EXEC モードに移行できます。**auto-enable** オプションが **aaa authorization exec** コマンドに追加されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization]。

ソフトウェアおよびコンフィギュレーション

この章では、Cisco ASA ソフトウェアおよびコンフィギュレーションの管理方法について説明します。

ソフトウェアのアップグレード

アップグレード パスと移行

- ACL 移行のために 9.0 より前のリリースからアップグレードする場合、後でダウングレードすることはできません。ダウングレードする場合に備え、コンフィギュレーション ファイルのバックアップを確実に行ってください。詳細については、9.0 アップグレード ガイドの ACL の移行の項を参照してください。

- 9.1(2.8) より前のバージョンの場合、9.1(2.8) 以降にアップグレードするには、次のバージョンのいずれかを実行している必要があります。
  - 8.4(5) 以降
  - 9.0(2) 以降
  - 9.1(2)

  *旧*バージョンを実行している場合、*最初に*上記のバージョンのいずれかにアップグレードしないと 9.1(2.8) 以降に直接アップグレードすることはできません。次に例を示します。

9.1(2.8) より前の ASA バージョン	最初のアップグレード先:	次のアップグレード先:
8.2(1)	8.4(7)	9.3(1) 以降
8.4(4)	8.4(7)	9.3(1) 以降
9.0(1)	9.0(4)	9.3(1) 以降
9.1(1)	9.1(2)	9.3(1) 以降

- 8.3 より前のバージョンからアップグレードする場合
  - 設定の移行に関する重要な情報については、『*Cisco ASA 5500 Migration Guide to Version 8.3*』を参照してください。
  - 9.0 以降に直接アップグレードすることはできません。移行を成功させるためには、まずバージョン 8.4 にアップグレードする必要があります。
- ゼロダウンタイム アップグレードのためのソフトウェア バージョン要件

  フェールオーバー構成や ASA クラスタのすべての装置の、ソフトウェアのメジャー バージョン（最初の番号）とマイナー バージョン（2 番目の番号）が同じである必要があります。ただし、アップグレード プロセス中に装置のバージョン パリティを維持する必要はありません。それぞれの装置で実行されるソフトウェアのバージョンが異なっていても、フェールオーバーのサポートを維持できます。長期の互換性および安定性を確保するために、すべての装置をできるだけ早く同じバージョンにアップグレードすることをお勧めします。

  表 37-1 に、ゼロダウンタイム アップグレードの実行がサポートされるシナリオを示します。

表 37-1　ゼロダウンタイム アップグレードのサポート

アップグレードのタイプ	サポート
メンテナンス リリース	任意のメンテナンス リリースを、マイナー リリース内の他のメンテナンス リリースにアップグレードできます。 たとえば、中間のメンテナンス リリースをあらかじめインストールしなくても、9.1(1) から 9.1(5) にアップグレードできます。
マイナー リリース	マイナー リリースから次のマイナー リリースにアップグレードできます。マイナー リリースはスキップできません。 たとえば、9.0 から 9.1 にアップグレードできます。ただし、ゼロダウンタイム アップグレードでは 9.0 から 9.2 への直接のアップグレードはサポートされておらず、まず 9.1 にアップグレードする必要があります。 **（注）** ゼロダウンタイム アップグレードは機能の構成が移行されていても可能です。

表 37-1　ゼロダウンタイム アップグレードのサポート （続き）

アップグレードのタイプ	サポート
メジャー リリース	前のバージョンの最後のマイナー リリースから次のメジャー リリースにアップグレードできます。 たとえば、8.6 がモデルの 8.x リリース シリーズの最後のマイナー バージョンであれば、8.6 から 9.0 にアップグレードできます。ただし、ゼロダウンタイム アップグレードでは 8.6 から 9.1 への直接のアップグレードはサポートされておらず、まず 9.0 にアップグレードする必要があります。特定のマイナー リリースでサポートされないモデルの場合は、そのマイナー リリースをスキップできます。たとえば ASA 5585-X の場合は、8.4 から 9.0 にアップグレードできます（このモデルは 8.5 または 8.6 ではサポートされません）。 **（注）** ゼロダウンタイム アップグレードは機能の構成が移行されていても可能です。

現在のバージョンの表示

ソフトウェア バージョンは ASDM ホーム ページに表示されます。ご使用の ASA のソフトウェア バージョンを確認するには、ホーム ページを参照してください。

Cisco.com からのソフトウェアのダウンロード

ASDM アップグレード ウィザードを使用している場合は、ソフトウェアを事前にダウンロードする必要ありません。フェールオーバー アップグレードなど手動でのアップグレードの場合は、ローカル コンピュータにイメージをダウンロードします。

Cisco.com のログインをお持ちの場合は、次の Web サイトから OS および ASDM のイメージを入手できます。

http://www.cisco.com/go/asa-software

スタンドアロン ユニットのアップグレード

この項では、ASDM およびオペレーティング システム（OS）のイメージをインストールする方法について説明します。

- 「ローカル コンピュータからのアップグレード」（P.37-4）
- 「Cisco.com ウィザードを使用したアップグレード」（P.37-5）

ローカル コンピュータからのアップグレード

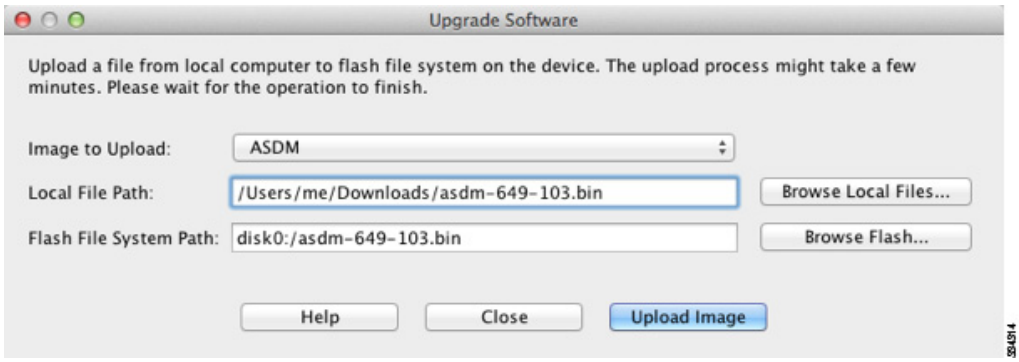
Upgrade Software from Local Computer ツールにより、コンピュータからフラッシュ メモリにイメージ ファイルをアップロードし、ASA をアップグレードできます。

手順

ステップ 1　（設定の移行の場合）ASDM で、[Tools] > [Backup Configurations] ツールにより、現在の設定をバック アップします。

ステップ 2　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Upgrade Software from Local Computer] の順に選択します。

[Upgrade Software] ダイアログボックスが表示されます。



ステップ 3　[Image to Upload] ドロップダウン リストから、[ASDM] を選択します。

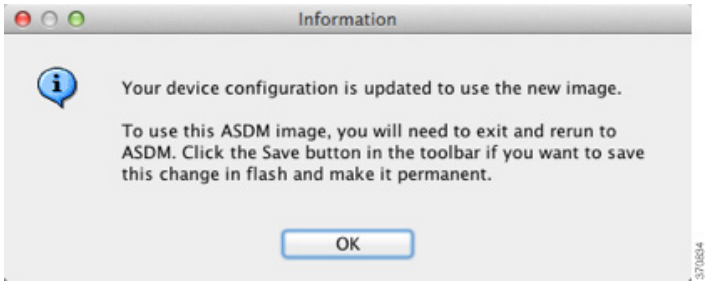
ステップ 4　[Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを検索します。

ステップ 5　[Flash File System Path] フィールドにフラッシュ ファイル システムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュ ファイル システム上のディレクトリまたはファイルを検索します。

ステップ 6　[Upload Image] をクリックします。アップグレード プロセスには数分かかる場合があります。

ステップ 7　このイメージを ASDM イメージとして設定するように求められます。[Yes] をクリックします。

ステップ 8　ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。アップグレード ツールを終了します。**注：**ASA ソフトウェアをアップグレードした*後*で、設定を保存し、ASDM をリロードします。



ステップ 9　ステップ 2 からステップ 8 を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。この手順は、その他のタイプのファイルのアップロードでも同じです。

ステップ 10　[Tools] > [System Reload] を選択して、ASA をリロードします。

リロードの詳細の確認を求める新しいウィンドウが表示されます。

a.　[Save the running configuration at the time of reload] オプション ボタン（デフォルト）をクリックします。

b.　リロードする時刻を選択します（たとえば、デフォルトの [Now]）。

c.　[Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションも表示されます。

ステップ 11　ASA のリロード後、ASDM を再起動します。

Cisco.com ウィザードを使用したアップグレード

Upgrade Software from Cisco.com Wizard により、ASDM および ASA を最新のバージョンに自動的にアップグレードできます。

このウィザードでは、次の操作を実行できます。

- アップグレード用の ASA イメージ ファイルまたは ASDM イメージ ファイルを選択する。

（注）　ASDM は最新のイメージ バージョンをダウンロードし、そこにはビルド番号が含まれています。たとえば、9.2(1) をダウンロードした場合、そのダウンロードは 9.2(1.2) になります。この動作は想定されているため、計画したアップグレードを続行できます。

- 実行したアップグレードの変更点を確認する。
- イメージをダウンロードし、インストールする。
- インストールのステータスを確認する。
- インストールが正常に完了した場合は、ASA を再起動して、コンフィギュレーションを保存し、アップグレードを完了する。

手順

ステップ 1　（設定の移行の場合）ASDM で、[Tools] > [Backup Configurations] ツールにより、現在の設定をバック アップします。

ステップ 2　[Tools] > [Check for ASA/ASDM Updates] を選択します。

マルチ コンテキスト モードでは、システムからこのメニューにアクセスします。

[Cisco.com Authentication] ダイアログボックスが表示されます。

ステップ 3　Cisco.com のユーザ ID とパスワードを入力して、[Login] をクリックします。

[Cisco.com Upgrade Wizard] が表示されます。

（注）　利用可能なアップグレードがない場合は、ダイアログボックスが表示されます。ウィザードを終了するには、[OK] をクリックします。

ステップ 4　[Next] をクリックして [Select Software] 画面を表示します。

現在の ASA バージョンおよび ASDM バージョンが表示されます。

ステップ 5　ASA バージョンおよび ASDM バージョンをアップグレードするには、次の手順を実行します。

a.　[ASA] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASA バージョンをドロップダウン リストから選択します。

b.　[ASDM] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASDM バージョンをドロップダウン リストから選択します。

ステップ 6　[Next] をクリックして [Review Changes] 画面を表示します。

ステップ 7　次の項目を確認します。

- ダウンロードした ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
- アップロードする ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
- 正しい ASA ブート イメージが選択されていること。

ステップ 8　[Next] をクリックして、アップグレード インストールを開始します。

アップグレード インストールの進行状況を示すステータスを表示できます。

[Results] 画面が表示され、アップグレード インストール ステータス（成功または失敗）など、追加の詳細が示されます。

ステップ 9　アップグレード インストールが成功した場合に、アップグレード バージョンを有効にするには、[Save configuration and reload device now] チェックボックスをオンにして、ASA を再起動し、ASDM を再起動します。

ステップ 10　[Finish] をクリックして、ウィザードを終了し、コンフィギュレーションに対して行った変更を保存します。

（注）　次に高いバージョン（存在する場合）にアップグレードするには、ウィザードを再起動する必要があります。

フェールオーバー ペアまたは ASA クラスタのアップグレード

アクティブ/スタンバイ フェールオーバー ペアのアップグレード

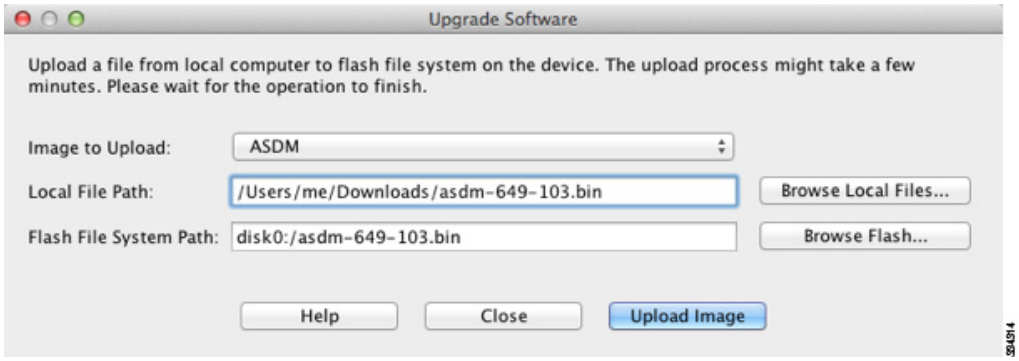
アクティブ/スタンバイ フェールオーバー ペアをアップグレードするには、次の手順を実行します。

手順

ステップ 1　（設定の移行の場合）ASDM で、[Tools] > [Backup Configurations] ツールにより、現在の設定をバック アップします。

ステップ 2　アクティブ装置のメイン ASDM アプリケーション ウィンドウで、[Tools] > [Upgrade Software from Local Computer] を選択します。

[Upgrade Software] ダイアログボックスが表示されます。



ステップ 3　[Image to Upload] ドロップダウン リストから、[ASDM] を選択します。

ステップ 4　[Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを検索します。

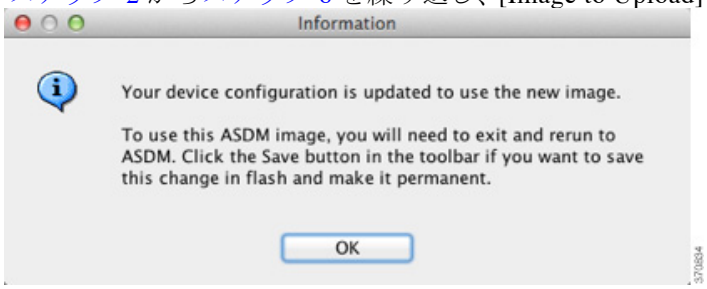
ステップ 5　[Flash File System Path] フィールドにフラッシュ ファイル システムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュ ファイル システム上のディレクトリまたはファイルを検索します。

ステップ 6　[Upload Image] をクリックします。アップグレード プロセスには数分かかる場合があります。

ステップ 7　このイメージを ASDM イメージとして設定するように求められます。[Yes] をクリックします。

ステップ 8　ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。アップグレード ツールを終了します。**注：**ASA ソフトウェアをアップグレードした*後*で、設定を保存し、ASDM をリロードします。

ステップ 9　ステップ 2 からステップ 8 を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。



ステップ 10　コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。

ステップ 11　ASDM を*スタンバイ*装置に接続し、ステップ 2 からステップ 9 に従って ASA および ASDM ソフトウェアをアップロードします。このとき、アクティブ装置と同じ場所にファイルを置きます。

ステップ 12　[Tools] > [System Reload] を選択して、スタンバイ ASA をリロードします。

リロードの詳細の確認を求める新しいウィンドウが表示されます。

a.　[Save the running configuration at the time of reload] オプション ボタン（デフォルト）をクリックします。

b.　リロードする時刻を選択します（たとえば、デフォルトの [Now]）。

c.　[Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションも表示されます。

ステップ 13　スタンバイ ASA のリロード後、ASDM を再起動し、スタンバイ装置に接続して、実行中であることを確認します。

ステップ 14　再度 ADSM をアクティブ装置に接続します。

ステップ 15　[Monitoring] > [Properties] > [Failover] > [Status] を選択して、アクティブ装置をスタンバイ装置にフェールオーバーし、[Make Standby] をクリックします。

ステップ 16　[Tools] > [System Reload] を選択して、（旧）アクティブ ASA をリロードします。

リロードの詳細の確認を求める新しいウィンドウが表示されます。

a.　[Save the running configuration at the time of reload] オプション ボタン（デフォルト）をクリックします。

b.　リロードする時刻を選択します（たとえば、デフォルトの [Now]）。

c.　[Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションも表示されます。

ASA を起動すると、スタンバイ装置になります。

アクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

はじめる前に

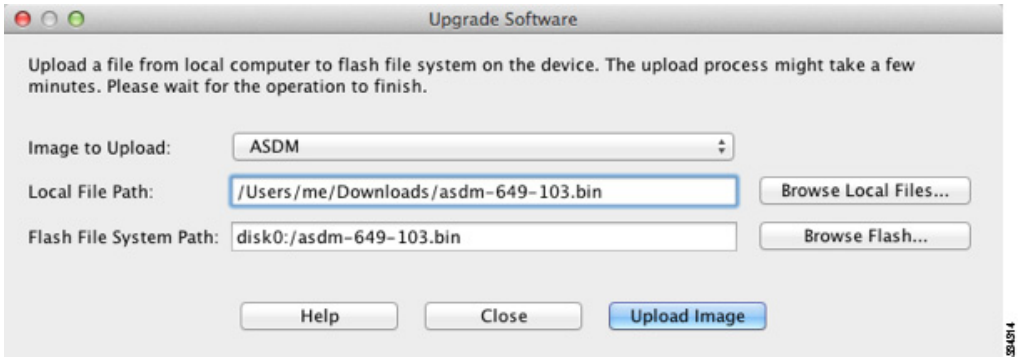
これらの手順をシステム実行スペースで実行します。

手順

ステップ 1　（設定の移行の場合）ASDM で、[Tools] > [Backup Configurations] ツールにより、現在の設定をバック アップします。

ステップ 2　プライマリ装置のメイン ASDM アプリケーション ウィンドウで、[Tools] > [Upgrade Software from Local Computer] を選択します。

[Upgrade Software] ダイアログボックスが表示されます。



ステップ 3　[Image to Upload] ドロップダウン リストから、[ASDM] を選択します。

ステップ 4　[Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを検索します。

ステップ 5　[Flash File System Path] フィールドにフラッシュ ファイル システムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュ ファイル システム上のディレクトリまたはファイルを検索します。

ステップ 6　[Upload Image] をクリックします。アップグレード プロセスには数分かかる場合があります。

ステップ 7　このイメージを ASDM イメージとして設定するように求められます。[Yes] をクリックします。

ステップ 8　ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。アップグレード ツールを終了します。**注：**ASA ソフトウェアをアップグレードした*後*で、設定を保存し、ASDM をリロードします。

ステップ 9　ステップ 2 からステップ 8 を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。

ステップ 10　コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。

ステップ 11　[Monitoring] > [Failover] > [Failover Group #] を選択して、プライマリ装置上の両方のフェールオーバー グループをアクティブにします。ここで # は、プライマリ装置に移動するフェールオーバー グループ数です。[Make Active] をクリックします。

ステップ 12　ASDM を*セカンダリ*装置に接続し、ステップ 2 からステップ 9 に従って ASA および ASDM ソフトウェアをアップロードします。このとき、アクティブ装置と同じ場所にファイルを置きます。

ステップ 13　[Tools] > [System Reload] を選択して、セカンダリ ASA をリロードします。

リロードの詳細の確認を求める新しいウィンドウが表示されます。

a.　[Save the running configuration at the time of reload] オプション ボタン（デフォルト）をクリックします。

b.　リロードする時刻を選択します（たとえば、デフォルトの [Now]）。

c.　[Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションも表示されます。

ステップ 14　ASDM を*プライマリ*装置に接続して、[Monitoring] > [Failover] > [System] の順に選択し、セカンダリ装置がリロードされたことを確認します。

ステップ 15　セカンダリ装置が起動したら、[Monitoring] > [Properties] > [Failover] > [System] の順に選択して、プライマリ装置をセカンダリ装置にフェールオーバーし、[Make Standby] をクリックします。

ステップ 16　[Tools] > [System Reload] を選択して、（旧）アクティブ ASA をリロードします。

リロードの詳細の確認を求める新しいウィンドウが表示されます。

a.　[Save the running configuration at the time of reload] オプション ボタン（デフォルト）をクリックします。

b.　リロードする時刻を選択します（たとえば、デフォルトの [Now]）。

c. [Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションも表示されます。

フェールオーバー グループは、[Preempt Enabled] を使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。[Preempt Enabled] でフェールオーバー グループが設定されていない場合は、[Monitoring] > [Failover] > [Failover Group #] ペインを使用して、指定された装置上でアクティブ ステータスに戻すことができます。

ASA クラスタのアップグレード

ASA クラスタ内のすべての装置をアップグレードするには、マスター装置で次の手順を実行します。マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。

手順

ステップ 1　マスター装置で ASDM を起動します。

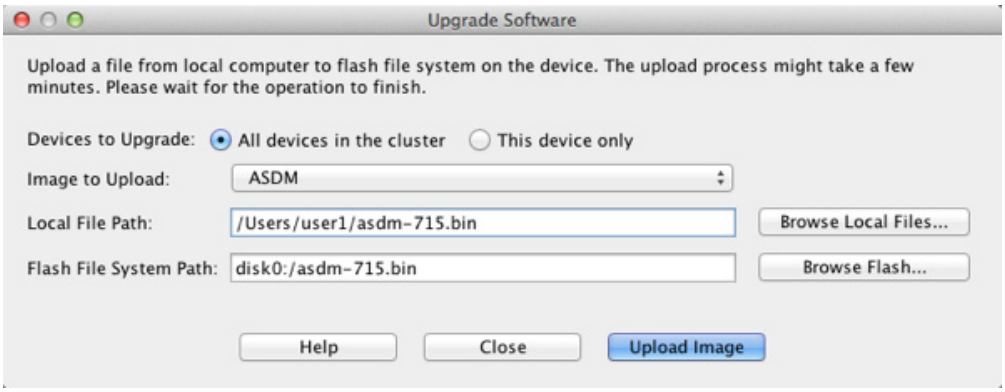
ステップ 2　（設定の移行の場合）ASDM で、[Tools] > [Backup Configurations] ツールにより、現在の設定をバック アップします。

ステップ 3　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Upgrade Software from Local Computer] の順に選択します。

[Upgrade Software from Local Computer] ダイアログボックスが表示されます。

ステップ 4　[All devices in the cluster] オプション ボタンをクリックします。

[Upgrade Software] ダイアログボックスが表示されます。



ステップ 5　[Image to Upload] ドロップダウン リストから、[ASDM] を選択します。

ステップ 6　[Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを検索します。

ステップ 7　[Flash File System Path] フィールドにフラッシュ ファイル システムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュ ファイル システム上のディレクトリまたはファイルを検索します。

ステップ 8　[Upload Image] をクリックします。アップグレード プロセスには数分かかる場合があります。

ステップ 9　このイメージを ASDM イメージとして設定するように求められます。[Yes] をクリックします。

ステップ 10　ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。アップグレード ツールを終了します。**注：**ASA ソフトウェアをアップグレードした*後*で、設定を保存し、ASDM をリロードします。

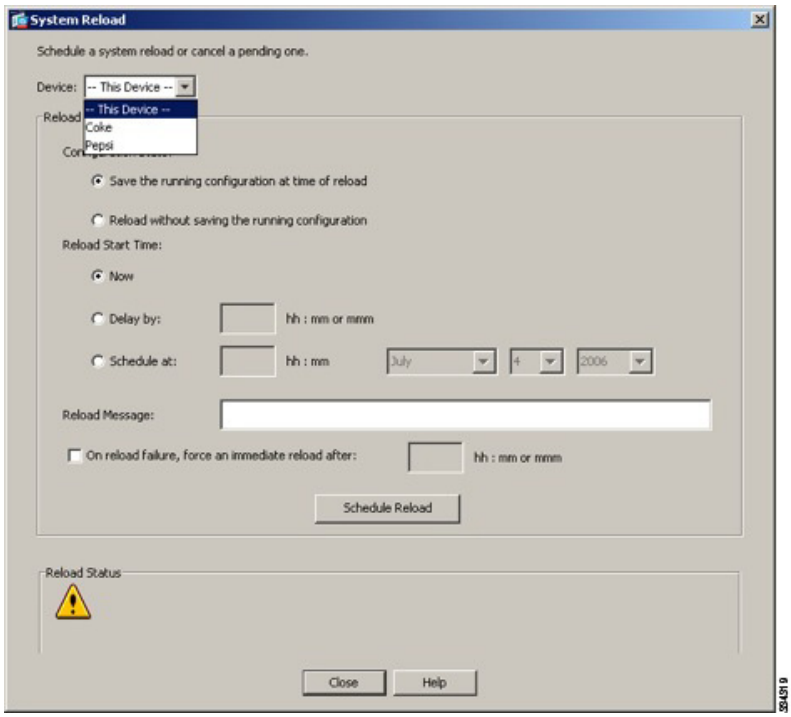
ステップ 11　ステップ 3 からステップ 10 を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。

ステップ 12　コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。

ステップ 13　[Tools] > [System Reload] を選択します。

[System Reload] ダイアログボックスが表示されます。

ステップ 14　[Device] ドロップダウン リストからスレーブ装置名を選択して、スレーブ装置を 1 台ずつリロードし、続いて [Schedule Reload] をクリックして装置をすぐにリロードします。



接続損失を回避しトラフィックを安定させるために、各装置が起動するまで（約 5 分）次の装置のリロードを待ちます。装置がクラスタに再接続したことを確認するには、[Monitoring] > [ASA Cluster] > [Cluster Summary] ペインを表示します。

ステップ 15　すべてのスレーブ装置のリロードが完了したら、[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] を選択して、マスター装置のクラスタリングをディセーブルにします。続いて [Participate ASA cluster] チェックボックスをオフにして、[Apply] をクリックします。

新しいマスターが選択されトラフィックが安定するまでに、5 分間かかります。それまでマスターであった装置がクラスタに再参加すると、その装置はスレーブとなります。

設定は保存しないでください。マスター装置がリロードしたら、そこでクラスタリングをイネーブルにします。

ステップ 16　[Tools] > [System Reload] を選択し、[Device] ドロップダウン リストから [--This Device--] を選択して [System Reload] ダイアログボックスからマスター装置をリロードします。

ステップ 17　ASDM を停止および再起動します。新しいマスター装置に再接続できます。

ファイルの管理

ASDM には、基本的なファイル管理タスクを実行するのに便利なファイル管理ツール セットが用意されています。ファイル管理ツールにより、フラッシュ メモリに保存されているファイルの表示、移動、コピー、および削除、ファイルの転送、およびリモート ストレージ デバイス（マウント ポイント）のファイルの管理を行うことができます。

（注）　マルチコンテキスト モードの場合、このツールはシステムのセキュリティ コンテキストでだけ使用できます。

- 「ファイル アクセスの設定」（P.37-14）
- 「ファイル管理ツールへのアクセス」（P.37-18）
- 「ファイル転送」（P.37-19）

ファイル アクセスの設定

- 「FTP クライアント モードの設定」（P.37-14）
- 「セキュア コピー サーバとしての ASA の設定　」（P.37-15）
- 「ASA セキュア コピー クライアントのカスタマイズ」（P.37-15）
- 「ASA TFTP クライアントのパス設定」（P.37-16）
- 「マウント ポイントの追加」（P.37-17）

FTP クライアント モードの設定

ASA では、FTP サーバとの間で、イメージ ファイルやコンフィギュレーション ファイルのアップロードおよびダウンロードを実行できます。パッシブ FTP では、クライアントは制御接続およびデータ接続の両方を開始します。パッシブ モードではデータ接続の受け入れ側となるサーバは、今回の特定の接続においてリッスンするポート番号を応答として返します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [File Access] > [FTP Client] ペインで、[Specify FTP mode as passive] チェックボックスをオンにします。

ステップ 2　[Apply] をクリックします。

FTP クライアントのコンフィギュレーションが変更され、その変更内容が実行コンフィギュレーションに保存されます。

セキュア コピー サーバとしての ASA の設定

ASA 上でセキュア コピー（SCP）サーバをイネーブルにできます。SSH による ASA へのアクセスを許可されたクライアントだけが、セキュア コピー接続を確立できます。

制限事項

- サーバにはディレクトリ サポートがありません。そのため、リモート クライアント アクセスで ASA の内部ファイル参照はできません。
- サーバではバナーがサポートされません。
- サーバではワイルドカードがサポートされません。

前提条件

- 「管理アクセスの設定」（P.36-3）に従って、ASA で SSH をイネーブルにします。
- SSH バージョン 2 接続をサポートするには、ASA のライセンスに強力な暗号化（3DES/AES）ライセンスが必要です。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP) Server] の順に選択して、[Enable secure copy server] チェックボックスをオンにします。

ステップ 2　[Apply] をクリックします。

例

外部ホストのクライアントから、SCP ファイル転送を実行します。たとえば、Linux では次のコマンドを入力します。

```
scp -v -pw password source_filename username@asa_address:{disk0|disk1}:/dest_filename
```

-v は冗長を表します。**-pw** が指定されていない場合は、パスワードの入力を求めるプロンプトが表示されます。

ASA セキュア コピー クライアントのカスタマイズ

オンボード SCP クライアントを使用して ASA 間でファイルをコピーすることができます（「ファイル管理ツールへのアクセス」（P.37-18）を参照）。ここでは、SCP クライアントの動作をカスタマイズすることができます。

前提条件

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。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、[Configuration] > [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。

手順の詳細

ステップ 1　コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP)] の順に選択します。
- マルチ モードの場合、[Configuration] > [Device Management] > [Device Administration] > [Secure Copy] の順に選択します。

ステップ 2　ASA は接続先の各 SCP サーバの SSH ホストキーを保存します。必要に応じて、ASA データベースから手動でサーバとそのキーを追加または削除できます。

キーを追加するには、次の手順を実行します。

a. 新しいサーバの [Add] をクリックするか、または信頼できる SSH ホストのテーブルからサーバを選択し、[Edit] をクリックします。

b. 新しいサーバの [Host] フィールドに、サーバの IP アドレスを入力します。

c. [Add public key for the trusted SSH host] チェックボックスをオンにします。

d. 次のいずれかのキーを指定します。

- フィンガープリント：すでにハッシュされているキーを入力します。たとえば、**show** コマンドの出力からコピーしたキーです。
- キー：SSH ホストの公開キーまたはハッシュ値を入力します。キー ストリングはリモート ピアの Base64 で符号化された RSA 公開キーです。オープン SSH クライアントから（言い換えると .ssh/id_rsa.pub ファイルから）公開キー値を取得できます。Base64 で符号化された公開キーを送信した後、SHA-256 によってそのキーがハッシュされます。

キーを削除するには、次の手順を実行します。

a. 信頼できる SSH ホストのテーブルからサーバを選択し、[Delete] をクリックします。

ステップ 3　新しいホストキーが検出されたときに通知を受け取るには、[Inform me when a new host key is detected] チェックボックスをオンにします。

デフォルトで、このオプションは有効になっています。このオプションがイネーブルになっている場合、ASA にまだ格納されていないホストキーを許可または拒否するように求められます。このオプションがディセーブルになっている場合、ASA は過去に保存されたことがないホストキーを自動的に許可します。

ステップ 4　[Apply] をクリックします。

ASA TFTP クライアントのパス設定

TFTP は、単純なクライアント/サーバ ファイル転送プロトコルで、RFC 783 および RFC 1350 Rev で規定されています。2.TFTP サーバとの間でファイルをコピーできるように、ASA を TFTP クライアントとして設定できます（「ファイル転送」（P.37-19）を参照）。これにより、コンフィギュレーション ファイルをバックアップし、それらを複数の ASA にプロパゲートできます。

ここでは、TFTP サーバへのパスを事前定義できるため、**copy** および **configure net** などのコマンドで入力する必要がなくなります。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [File Access] > [TFTP Client] の順に選択して、[Enable] チェックボックスをオンにします。

ステップ 2　[Interface Name] ドロップダウン リストから、TFTP クライアントとして使用するインターフェイスを選択します。

ステップ 3　コンフィギュレーション ファイルの保存先とする TFTP サーバの IP アドレスを [IP Address] フィールドに入力します。

ステップ 4　コンフィギュレーション ファイルの保存先とする TFTP サーバへのパスを [Path] フィールドに入力します。

例：/tftpboot/asa/config3

ステップ 5　[Apply] をクリックします。

マウント ポイントの追加

- 「CIFS マウント ポイントの追加」（P.37-17）
- 「FTP マウント ポイントの追加」（P.37-18）

CIFS マウント ポイントの追加

共通インターネット ファイル システム（CIFS）マウント ポイントを定義するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [File Access] > [Mount-Points] の順に選択して、[Add] > [CIFS Mount Point] をクリックします。

[Add CIFS Mount Point] ダイアログボックスが表示されます。

ステップ 2　[Enable mount point] チェックボックスをオンにします。

これにより、ASA 上の CIFS ファイル システムが UNIX のファイル ツリーに接続されます。

ステップ 3　[Mount Point Name] フィールドに、既存の CIFS が存在する位置の名前を入力します。

ステップ 4　[Server Name] フィールドまたは [IP Address] フィールドに、マウント ポイントを配置するサーバの名前または IP アドレスを入力します。

ステップ 5　[Share Name] フィールドに、CIFS サーバ上のフォルダの名前を入力します。

ステップ 6　[NT Domain Name] フィールドに、サーバが常駐する NT ドメインの名前を入力します。

ステップ 7　サーバに対するファイル システムのマウントを認可されているユーザの名前を、[User Name] フィールドに入力します。

ステップ 8　サーバに対するファイル システムのマウントを認可されているユーザのパスワードを、[Password] フィールドに入力します。

ステップ 9　[Confirm Password] フィールドにパスワードを再入力します。

ステップ 10　[OK] をクリックします。

[Add CIFS Mount Point] ダイアログボックスが閉じます。

ステップ 11　[Apply] をクリックします。

FTP マウント ポイントの追加

（注）　FTP マウント ポイントの場合、FTP サーバには UNIX のディレクトリ リスト スタイルが必要です。Microsoft FTP サーバには、デフォルトで MS-DOS ディレクトリ リスト スタイルがあります。

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [File Access] > [Mount-Points] の順に選択して、[Add] > [FTP Mount Point] をクリックします。

[Add FTP Mount Point] ダイアログボックスが表示されます。

ステップ 2　[Enable] チェックボックスを選択します。

これにより、ASA 上の FTP ファイル システムが UNIX のファイル ツリーに接続されます。

ステップ 3　[Mount Point Name] フィールドに、既存の FTP が存在する位置の名前を入力します。

ステップ 4　[Server Name] フィールドまたは [IP Address] フィールドに、マウント ポイントを配置するサーバの名前または IP アドレスを入力します。

ステップ 5　[Mode] フィールドで、オプション ボタン（[Active] または [Passive]）をクリックして FTP モードを選択します。[Passive] モードを選択した場合、クライアントでは、FTP コントロール接続とデータ接続がともに起動します。サーバは、この接続をリッスンするポートの番号で応答します。

ステップ 6　FTP ファイル サーバへのディレクトリ パス名を [Path to Mount] フィールドに入力します。

ステップ 7　サーバに対するファイル システムのマウントを認可されているユーザの名前を、[User Name] フィールドに入力します。

ステップ 8　サーバに対するファイル システムのマウントを認可されているユーザのパスワードを、[Password] フィールドに入力します。

ステップ 9　[Confirm Password] フィールドにパスワードを再入力します。

ステップ 10　[OK] をクリックします。

[Add FTP Mount Point] ダイアログボックスが閉じます。

ステップ 11　[Apply] をクリックします。

ファイル管理ツールへのアクセス

ファイル管理ツールを使用するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [File Management] の順に選択します。

[File Management] ダイアログボックスが表示されます。

- [Folders] ペインには、ディスク上にあるフォルダが表示されます。
- [Flash Space] は、フラッシュ メモリの合計容量と、使用可能なメモリ容量を示します。
- [Files] 領域には、選択したフォルダのファイルについて次の情報が表示されます。
  - パス
  - ファイル名

- サイズ（バイト単位）
- 修正時刻
- 選択したファイルの種類（ブート コンフィギュレーション、ブート イメージ ファイル、ASDM イメージ ファイル、SVC イメージ ファイル、CSD イメージ ファイル、または APCF イメージ ファイル）を示す、ステータス

ステップ 2　選択したファイルをブラウザに表示するには、[View] をクリックします。

ステップ 3　選択したファイルを切り取って別のディレクトリに貼り付けるには、[Cut] をクリックします。

ステップ 4　選択したファイルをコピーして別のディレクトリに貼り付けるには、[Copy] をクリックします。

ステップ 5　コピーしたファイルを選択した場所に貼り付けるには、[Paste] をクリックします。

ステップ 6　選択したファイルをフラッシュ メモリから削除するには、[Delete] をクリックします。

ステップ 7　ファイルの名前を変更するには、[Rename] をクリックします。

ステップ 8　ファイルを保存するディレクトリを新規作成するには、[New Directory] をクリックします。

ステップ 9　[File Transfer] ダイアログボックスを開くには、[File Transfer] をクリックします。詳細については、「ファイル転送」（P.37-19）を参照してください。

ステップ 10　[Manage Points] ダイアログボックスを開くには、[Mount Points] をクリックします。詳細については、「マウント ポイントの追加」（P.37-17）を参照してください。

ファイル転送

File Transfer ツールにより、ローカルにあるファイルとリモートにあるファイルを転送できます。PC またはフラッシュ ファイル システムのローカル ファイルを ASA との間で転送できます。HTTP、HTTPS、TFTP、FTP、または SMB を使用して、ASA との間でファイルを転送できます。

（注）　IPS SSP ソフトウェア モジュールの場合、IPS ソフトウェアを disk0 にダウンロードする前に、フラッシュ メモリに少なくとも 50% の空きがあることを確認してください。IPS をインストールするときに、IPS のファイル システム用に内部フラッシュ メモリの 50% が予約されます。

- 「ローカル PC とフラッシュ間でのファイル転送」（P.37-19）
- 「リモート サーバとフラッシュ間でのファイル転送」（P.37-20）

ローカル PC とフラッシュ間でのファイル転送

ローカル PC とフラッシュ ファイル システムとの間でファイルを転送するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [File Management] の順に選択します。

[File Management] ダイアログボックスが表示されます。

ステップ 2　[File Transfer] の横にある下矢印をクリックし、続いて [Between Local PC and Flash] をクリックします。

[File Transfer] ダイアログボックスが表示されます。

ステップ 3　ローカル PC またはフラッシュ ファイル システムのどちらかで、アップロードまたはダウンロードしたいファイルを選択し、目的の場所にドラッグします。または、ローカル PC またはフラッシュ ファイル システムのどちらかで、アップロードまたはダウンロードしたいファイルを選択し、右矢印または左矢印をクリックし、目的の場所にファイルを転送します。

ステップ 4　完了したら [Close] をクリックします。

リモート サーバとフラッシュ間でのファイル転送

リモート サーバとフラッシュ ファイル システムとの間でファイルを転送するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [File Management] の順に選択します。

[File Management] ダイアログボックスが表示されます。

ステップ 2　[File Transfer] ドロップダウン リストで下矢印をクリックし、[Between Remote Server and Flash] をクリックします。

[File Transfer] ダイアログボックスが表示されます。

ステップ 3　リモート サーバからファイルを転送するには、[Remote server] オプションをクリックします。

ステップ 4　転送対象になるソース ファイルを定義します。

a.　サーバの IP アドレスを含めたファイルの場所へのパスを選択します。

（注）　ファイル転送は IPv4 および IPv6 のアドレスをサポートしています。

b.　FTP の場合はリモート サーバのタイプを、HTTP または HTTPS の場合はリモート サーバのポート番号を入力します。有効な FTP タイプは次のとおりです。

- ap：パッシブ モードの ASCII ファイル
- an：非パッシブ モードの ASCII ファイル
- ip：パッシブ モードのバイナリ イメージ ファイル
- in：非パッシブ モードのバイナリ イメージ ファイル

ステップ 5　フラッシュ ファイル システムからファイルを転送するには、[Flash file system] オプションを選択します。

ステップ 6　ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。

ステップ 7　また、CLI により、スタートアップ コンフィギュレーション、実行コンフィギュレーション、または SMB ファイル システムからファイルをコピーすることもできます。**copy** コマンドの使用方法については、『CLI 設定ガイド』を参照してください。

ステップ 8　転送するファイルの宛先を定義します。

a.　フラッシュ ファイル システムにファイルを転送するには、[Flash file system] オプションを選択します。

b.　ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。

ステップ 9　リモート サーバにファイルを転送するには、[Remote server] オプションを選択します。

a. ファイルの場所へのパスを入力します。

b. FTP 転送の場合はタイプを入力します。有効なタイプは次のとおりです。

- ap：パッシブ モードの ASCII ファイル
- an：非パッシブ モードの ASCII ファイル
- ip：パッシブ モードのバイナリ イメージ ファイル
- in：非パッシブ モードのバイナリ イメージ ファイル

ステップ 10　[Transfer] をクリックしてファイル転送を開始します。

[Enter Username and Password] ダイアログボックスが表示されます。

ステップ 11　リモート サーバのユーザ名、パスワード、ドメイン（必要な場合）が表示されます。

ステップ 12　[OK] をクリックし、ファイル転送を続行します。

ファイル転送プロセスには数分かかる場合があります。必ず終了するまでお待ちください。

ステップ 13　ファイル転送が完了したら [Close] をクリックします。

使用するイメージおよびスタートアップ コンフィギュレーションの設定

複数の ASA または ASDM イメージがある場合は、ブートするイメージを指定する必要があります。イメージを設定しない場合はデフォルトのブート イメージが使用され、そのイメージは意図されたものではない可能性があります。スタートアップ コンフィギュレーションでは、コンフィギュレーション ファイルを任意で指定できます。

デフォルト設定

ASA イメージ

- 物理 ASA：内部フラッシュ メモリ内で見つかった最初のアプリケーション イメージをブートします。
- ASAv：最初に展開したときに作成された、読み取り専用の boot:/ パーティションにあるイメージをブートします。フラッシュ メモリ内のイメージをアップグレードし、そのイメージからブートするように ASAv を設定できます。後でコンフィギュレーションをクリアすると、ASAv は元の展開のイメージをロードするようになることに注意してください。

ASDM イメージ

すべての ASA：内部フラッシュ メモリ内で見つかった（またはここにイメージがない場合は、外部フラッシュ メモリ内で見つかった）最初の ASDM イメージをブートします。

スタートアップ コンフィギュレーション

デフォルトでは、ASA は、隠しファイルであるスタートアップ コンフィギュレーションからブートします。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [System Image/Configuration] > [Boot Image/Configuration] を選択します。

起動イメージとして使用するバイナリ イメージ ファイルは、ローカルから 4 つまで指定できます。また TFTP サーバのイメージを 1 つ指定し、そこからデバイスをブートできます。TFTP サーバに格納されているイメージを指定する場合は、そのファイルをリスト内の先頭に配置する必要があります。デバイスが、イメージのロード元の TFTP サーバに到達できない場合は、フラッシュ メモリに保存されているリスト内の次のイメージ ファイルのロードが試行されます。

ステップ 2　[Boot Image/Configuration] ペインで [Add] をクリックします。

ステップ 3　ブートするイメージを参照します。TFTP イメージの場合は、[File Name] フィールドに TFTP URL を入力します。[OK] をクリックします。

ステップ 4　上へ移動ボタンと下へ移動ボタンを使用してイメージの順番を並べ替えます。

ステップ 5　（オプション）[Boot Configuration File Path] フィールドで、[Browse Flash] をクリックしてコンフィギュレーションを選択してスタートアップ コンフィギュレーション ファイルを指定します。[OK] をクリックします。

ステップ 6　[ASDM Image File Path] フィールドで、[Browse Flash] をクリックしてイメージを選択して ASDM イメージを指定します。[OK] をクリックします。

ステップ 7　[Apply] をクリックします。

コンフィギュレーションまたはその他のファイルのバックアップおよび復元

[Tools] メニューの [Backup and Restore] オプションを使用して、ASA の実行コンフィギュレーション、スタートアップ コンフィギュレーション、インストールされたアドオン イメージ、および SSL VPN クライアントのイメージとプロファイルをバックアップおよび復元できます。

ASDM の [Backup Configurations] 画面では、バックアップするファイル タイプを選択し、それらを単一の zip ファイルに圧縮し、その zip ファイルをコンピュータ上の選択したディレクトリに転送できます。同様に、ファイルを復元するには、コンピュータ上で転送元となる zip ファイルを選択し、復元するファイル タイプを選択します。

- 「ローカル CA サーバのバックアップ」（P.37-26）
- 「ローカル CA サーバのバックアップ」（P.37-26）
- 「TFTP サーバへの実行コンフィギュレーションの保存」（P.37-27）

完全なシステム バックアップまたは復元を実行します。

次の手順では、コンフィギュレーションおよびイメージの zip ファイルへのバックアップおよび復元方法と、そのファイルのローカル コンピュータへの転送方法について説明します。

- 「はじめる前に」（P.37-23）
- 「システムのバックアップ」（P.37-24）
- 「バックアップの復元」（P.37-25）

はじめる前に

- ASA はシングル コンテキスト モードである必要があります。
- バックアップ中またはバックアップ後にコンフィギュレーションの変更を行うと、その変更はバックアップされません。バックアップの作成後にコンフィギュレーションを変更してから復元を実行すると、このコンフィギュレーションへの変更は上書きされます。その結果、ASA の動作が異なる可能性があります。
- 一度に開始できるバックアップまたは復元は 1 つだけです。
- 元のバックアップを実行したときと同じ ASA バージョンに対してのみコンフィギュレーションを復元できます。復元ツールは、1 つの ASA バージョンから別のバージョンへコンフィギュレーションを移行するためには使用できません。コンフィギュレーションの移行が必要な場合、ASA が新しい ASA OS をロードするときに、常駐するスタートアップ コンフィギュレーションが自動的にアップグレードされます。
- クラスタリングを使用する場合、バックアップまたは復元できるのはスタートアップ コンフィギュレーション、実行コンフィギュレーション、およびマスター装置の ID 証明書だけです。
- フェールオーバーを使用する場合、アクティブ装置とスタンバイ装置のバックアップを個別に作成して復元する必要があります。
- ASA にマスター パスフレーズを設定している場合は、この手順で作成したバックアップ コンフィギュレーションの復元時にそのマスター パスフレーズが必要となります。ASA のマスター パスフレーズが不明な場合は、「マスター パスフレーズの設定」（P.14-9）を参照して、バックアップを続行する前に、マスター パスフレーズをリセットする方法を確認してください。
- PKCS12 データをインポート（**crypto ca trustpoint** コマンドを使用）する際にトラストポイントが RSA キーを使用している場合、インポートされたキー ペアにはトラストポイントと同じ名前が割り当てられます。この制限のため、ASDM コンフィギュレーションを復元した後でトラストポイントとそのキー ペアに別の名前を指定すると、スタートアップ コンフィギュレーションは元のコンフィギュレーションと同じになりますが、実行コンフィギュレーションのキー ペア名は異なります。これは、キー ペアとトラストポイントに別の名前を使用する場合は、元のコンフィギュレーションを復元できなくなります。この問題を回避するには、トラストポイントとキー ペアに同じ名前を使用していることを確認してください。
- 各バックアップ ファイルには次の内容が含まれます。
  - 実行コンフィギュレーション
  - スタートアップ コンフィギュレーション
  - すべてのセキュリティ イメージ

    Cisco Secure Desktop およびホスト スキャン イメージ

    Cisco Secure Desktop およびホスト スキャンの設定

    AnyConnect（SVC）クライアント イメージおよびプロファイル

    AnyConnect（SVC）のカスタマイズおよび変換
  - ID 証明書（ID 証明書に関連する RSA キー ペアが含まれ、スタンドアロン キーは除外されます）
  - VPN 事前共有キー
  - SSL VPN のコンフィギュレーション
  - アプリケーション プロファイルのカスタム フレームワーク（APCF）

- Bookmarks
- Customizations
- ダイナミック アクセス ポリシー（DAP）
- プラグイン
- 接続プロファイル用の事前入力スクリプト
- Proxy Auto-Config
- 変換テーブル
- Web コンテンツ
- バージョン情報

システムのバックアップ

この手順では、完全なシステム バックアップを実行する方法について説明します。

手順

ステップ 1　コンピュータ上にフォルダを作成し、バックアップ ファイルを保存します。こうすると、後で復元するときに探しやすくなります。

ステップ 2　[Tools] > [Backup Configurations] を選択します。

[Backup Configurations] ダイアログボックスが表示されます。[SSL VPN Configuration] 領域の下矢印をクリックし、SSL VPN コンフィギュレーションのバックアップ オプションを確認します。デフォルトでは、すべてのコンフィギュレーション ファイルがチェックされ、利用できる場合にはバックアップされます。リスト内のすべてのファイルをバックアップするには、手順 5 に進みます。

ステップ 3　バックアップするコンフィギュレーションを選択する場合は、[Backup All] チェックボックスをオフにします。

ステップ 4　バックアップするオプションの横にあるチェックボックスをオンにします。

ステップ 5　[Browse Local] をクリックして、バックアップ .zip ファイルのディレクトリおよびファイル名を指定します。

ステップ 6　[Select] ダイアログボックスで、バックアップ ファイルを格納するディレクトリを選択します。

ステップ 7　[Select] をクリックします。[Backup File] フィールドにパスが表示されます。

ステップ 8　ディレクトリ パスの後にバックアップ ファイルの宛先の名前を入力します。バックアップ ファイルの名前の長さは、3 ～ 232 文字の間である必要があります。

ステップ 9　[Backup] をクリックします。証明書をバックアップする場合や、ASA でマスター パスフレーズを使用している場合を除き、すぐにバックアップが続行されます。

ステップ 10　ASA でマスター パスフレーズを設定し、イネーブルにしている場合、バックアップを続行する前に、マスター パスフレーズが不明な場合は変更することを推奨する警告メッセージが表示されます。マスター パスフレーズがわかっている場合は、[Yes] をクリックしてバックアップを続行します。ID 証明書をバックアップする場合を除き、すぐにバックアップが続行されます。

ステップ 11　ID 証明書をバックアップする場合は、証明書を PKCS12 形式でエンコーディングするために使用する別のパスフレーズを入力するように求められます。パスフレーズを入力するか、またはこの手順をスキップすることができます。

（注）　このプロセスで ID 証明書はバックアップされますが、認証局の証明書はバックアップされません。CA 証明書のバックアップ手順については、「ローカル CA サーバのバックアップ」（P.37-26）を参照してください。

- 証明書を暗号化するには、[Certificate Passphrase] ダイアログボックスで証明書のパスフレーズを入力および確認し、[OK] をクリックします。証明書の復元時に必要となるため、このダイアログボックスに入力したパスワードを覚えておく必要があります。
- [Cancel] をクリックすると、この手順がスキップされ、証明書はバックアップされません。

[OK] または [Cancel] をクリックすると、すぐにバックアップが開始されます。

ステップ 12　バックアップが完了すると、ステータス ウィンドウが閉じ、[Backup Statistics] ダイアログボックスが表示され、成功または失敗のメッセージが示されます。

（注）　バックアップの「失敗」メッセージは多くの場合、指定されたタイプの既存のコンフィギュレーションが存在しない場合に表示されます。

ステップ 13　[OK] をクリックし、[Backup Statistics] ダイアログボックスを閉じます。

バックアップの復元

zip ファイルからローカル PC に復元するコンフィギュレーションやイメージを指定します。

手順

ステップ 1　[Tools] > [Restore Configurations] を選択します。

ステップ 2　[Restore Configurations] ダイアログボックスで、[Browse Local Directory] をクリックし、ローカルコンピュータ上の、復元するコンフィギュレーションが含まれている zip ファイルを選択し、[Select] をクリックします。[Local File] フィールドにパスと zip ファイル名が表示されます。

復元する zip ファイルは、[Tools] > [Backup Configurations] オプションを選択して作成したものである必要があります。

ステップ 3　[Next] をクリックします。2 つ目の [Restore Configuration] ダイアログボックスが表示されます。復元するコンフィギュレーションの横にあるチェックボックスをオンにします。使用可能なすべての SSL VPN コンフィギュレーションがデフォルトで選択されています。

ステップ 4　[Restore] をクリックします。

ステップ 5　バックアップ ファイルの作成時に、証明書の暗号化に使用する証明書パスフレーズを指定している場合は、このパスフレーズを入力するように ASDM から求められます。

ステップ 6　実行コンフィギュレーションの復元を選択した場合、実行コンフィギュレーションを結合するか、実行コンフィギュレーションを置換するか、または復元プロセスのこの部分をスキップするかを尋ねられます。

- コンフィギュレーションの結合では、現在の実行コンフィギュレーションとバックアップされた実行コンフィギュレーションが結合されます。
- 実行コンフィギュレーションの置換では、バックアップされた実行コンフィギュレーションのみが使用されます。

- この手順をスキップすると、バックアップされた実行コンフィギュレーションは復元されません。

ASDM では、復元操作が完了するまでステータス ダイアログボックスが表示されます。

ステップ 7　実行コンフィギュレーションを置換または結合した場合は、ASDM を閉じてから再起動します。実行コンフィギュレーションを復元しなかった場合は、ASDM セッションをリフレッシュして、変更を有効にします。

ローカル CA サーバのバックアップ

ASDM バックアップを実行した場合、ローカル CA サーバ データベースは含まれていないため、サーバ上の CA 証明書はバックアップされません。ローカル CA サーバをバックアップする場合は、ASA CLI による次の手動プロセスを使用します。

ステップ 1　**show run crypto ca server** コマンドを入力します。

```
crypto ca server
 keysize server 2048
 subject-name-default OU=aa,O=Cisco,ST=ca,
 issuer-name CN=xxx,OU=yyy,O=Cisco,L=Bxb,St=Mass
 smtp from-address abcd@cisco.com
 publish-crl inside 80
 publish-crl outside 80
```

ステップ 2　**crypto ca import** コマンドを使用して、ローカル CA PKCS12 ファイルをインポートして LOCAL-CA-SERVER トラストポイントを作成し、キーペアを復元します。

```
crypto ca import LOCAL-CA-SERVER pkcs12 <passphrase> (paste the pkcs12
base64 data here)
```

（注）　この手順では、正確な名前「LOCAL-CA-SERVER」を必ず使用してください。

ステップ 3　LOCAL-CA-SERVER ディレクトリが存在しない場合、**mkdir LOCAL-CA-SERVER** を入力して作成する必要があります。

ステップ 4　ローカル CA ファイルを LOCAL-CA-SERVER ディレクトリにコピーします。

```
copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.ser
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.cdb
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.udb
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.crl
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.p12
disk0:/LOCAL-CA-SERVER/
```

ステップ 5　**crypto ca server** コマンドを入力して、ローカル CA サーバをイネーブルにします。

```
crypto ca server
 no shutdown
```

ステップ 6　**show crypto ca server** コマンドを入力して、ローカル CA サーバが起動し、動作していることを確認します。

ステップ 7　設定を保存します。

TFTP サーバへの実行コンフィギュレーションの保存

この機能により、現在の実行コンフィギュレーション ファイルのコピーを TFTP サーバに保存します。

実行コンフィギュレーションを TFTP サーバに保存するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[File] > [Save Running Configuration to TFTP Server] の順に選択します。

[Save Running Configuration to TFTP Server] ダイアログボックスが表示されます。

ステップ 2　TFTP サーバの IP アドレスと、コンフィギュレーション ファイルの保存先となる TFTP サーバ上のファイル パスを入力して、[Save Configuration] をクリックします。

（注）　デフォルトの TFTP 設定を行うには、[Configuration] > [Device Management] > [Management Access] > [File Access] > [TFTP Client] の順に選択します。この設定を行った後は、このダイアログボックスに、TFTP サーバの IP アドレスと TFTP サーバ上でのファイル パスが自動的に表示されます。

システム再起動のスケジュール

System Reload ツールにより、システムの再起動をスケジュールしたり、現在の再起動をキャンセルしたりできます。

再起動をスケジュールするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [System Reload] の順に選択します。

ステップ 2　[Reload Scheduling] 領域で、次の設定を定義します。

a.　[Configuration State] では、再起動時に実行コンフィギュレーションを保存するか、破棄するかのどちらかを選択します。

b.　[Reload Start Time] では、次のオプションから選択します。

- 再起動をただちに実行するには、[Now] をクリックします。
- 指定した時間だけ再起動を遅らせるには、[Delay by] をクリックします。再起動開始までの時間を、時間と分単位、または分単位だけで入力します。

– 指定した時刻と日付に再起動を実行するようにスケジュールするには、[Schedule at] をクリックします。再起動の実行時刻を入力し、再起動のスケジュール日を選択します。

c. [Reload Message] フィールドに、再起動時に ASDM の開いているインスタンスに送信するメッセージを入力します。

d. 再起動を再試行するまでの経過時間を時間と分単位で、または分単位だけで表示するには、[On reload failure force immediate reload after] チェックボックスをオンにします。

e. 設定に従って再起動をスケジュールするには、[Schedule Reload] をクリックします。

[Reload Status] 領域には、再起動のステータスが表示されます。

ステップ 3　次のいずれかを選択します。

- スケジュールされた再起動を停止するには、[Cancel Reload] をクリックします。
- スケジュールされた再起動の終了後に [Reload Status] 表示をリフレッシュするには、[Refresh] をクリックします。
- スケジュールされた再起動の詳細を表示するには、[Details] をクリックします。

ソフトウェアのダウングレード

バージョン 8.3 にアップグレードすると、コンフィギュレーションが移行されます。既存のコンフィギュレーションは、自動的にフラッシュ メモリに保存されます。たとえば、バージョン 8.2(1) から 8.3(1) にアップグレードすると、古い 8.2(1) コンフィギュレーションはフラッシュ メモリ内の 8_2_1_0_startup_cfg.sav というファイルに保存されます。

（注）　ダウングレードする前に、古いコンフィギュレーションを手動で復元する必要があります。

ここでは、ダウングレードする方法について説明します。

- 「アクティベーション キーの互換性に関する情報」（P.37-28）
- 「ダウングレードの実行」（P.37-29）

アクティベーション キーの互換性に関する情報

任意の旧バージョンから最新バージョンにアップグレードした場合、アクティベーション キーの互換性は存続します。ただし、ダウングレード機能の維持には問題が生じる場合があります。

- バージョン 8.1 以前のバージョンにダウングレードする場合：アップグレード後に、*8.2 よりも前*に導入された追加の機能ライセンスをアクティブ化すると、ダウングレードした場合でも旧バージョンに対するアクティベーション キーの互換性は存続します。ただし、バージョン 8.2 以降のバージョンで導入された機能ライセンスをアクティブ化した場合は、アクティベーション キーの下位互換性がなくなります。互換性のないライセンス キーがある場合は、次のガイドラインを参照してください。
  - 旧バージョンでアクティベーション キーを入力した場合は、そのキーが ASA で使用されます（バージョン 8.2 以降のバージョンでアクティブ化した新しいライセンスがない場合）。
  - 新しいシステムで、以前のアクティベーション キーがない場合は、旧バージョンと互換性のある新しいアクティベーション キーを要求する必要があります。

- バージョン 8.2 以前のバージョンにダウングレードする場合：バージョン 8.3 では、よりロバストな時間ベース キーの使用およびフェールオーバー ライセンスの変更が次のとおり導入されました。
  - 複数の時間ベースのアクティベーション キーがアクティブな場合、ダウングレード時には一番最近アクティブ化された時間ベース キーのみがアクティブになれます。他のキーはすべて非アクティブ化されます。
  - フェールオーバー ペアに不一致のライセンスがある場合、ダウングレードによりフェールオーバーはディセーブルになります。キーが一致した場合でも、使用するライセンスは、結合されたライセンスではなくなります。

ダウングレードの実行

コンフィギュレーションの移行の詳細については、「[Tools] メニューの [Backup and Restore] オプションを使用して、ASA の実行コンフィギュレーション、スタートアップ コンフィギュレーション、インストールされたアドオン イメージ、および SSL VPN クライアントのイメージとプロファイルをバックアップおよび復元できます。」（P.37-22）を参照してください。

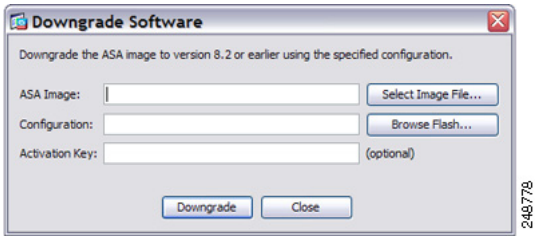
バージョン 8.3 からダウングレードするには、次の手順を実行します。

手順の詳細

ステップ 1　[Tools] > [Downgrade Software] を選択します。

[Downgrade Software] ダイアログボックスが表示されます。

図 37-1　Downgrade Software



ステップ 2　ASA イメージの場合、[Select Image File] をクリックします。

[Browse File Locations] ダイアログボックスが表示されます。

ステップ 3　次のいずれかのオプション ボタンをクリックします。

- [Remote Server]：ドロップダウン リストで [ftp]、[smb]、[http] のいずれかを選択し、以前のイメージ ファイルのパスを入力します。
- [Flash File System]：[Browse Flash] をクリックして、ローカル フラッシュ ファイル システムにある以前のイメージ ファイルを選択します。

ステップ 4　[Configuration] で [Browse Flash] をクリックし、移行前の設定ファイルを選択します（デフォルトでは disk0 に保存されています）。

ステップ 5　（オプション）バージョン 8.3 よりも前のアクティベーション キーに戻す場合は、[Activation Key] フィールドで以前のアクティベーション キーを入力します。

詳細については、「アクティベーション キーの互換性に関する情報」（P.37-28）を参照してください。

ステップ 6　[Downgrade] をクリックします。

このツールは、次の機能を実行するためのショートカットです。

1. ブート イメージ コンフィギュレーションのクリア（**clear configure boot**）。
2. 古いイメージへのブート イメージの設定（**boot system**）。
3. （オプション）新たなアクティベーション キーの入力（**activation-key**）。
4. 実行コンフィギュレーションのスタートアップ コンフィギュレーションへの保存（**write memory**）。これにより、BOOT 環境変数を古いイメージに設定します。このため、リロードすると古いイメージがロードされます。
5. 古いコンフィギュレーションのスタートアップ コンフィギュレーションへのコピー（**copy** *old_config_url* **startup-config**）。
6. リロード（**reload**）。

Auto Update の設定

Auto Update に関する情報

Auto Update は、Auto Update サーバがコンフィギュレーションおよびソフトウェア イメージを多数の ASA にダウンロードすることを許可し、中央からの ASA の基本的なモニタリングを提供するプロトコル仕様です。

Auto Update クライアントまたはサーバ

ASA は、クライアントまたはサーバとして設定できます。Auto Update クライアントとして動作する場合は、ソフトウェア イメージおよびコンフィギュレーション ファイルへのアップデートのため、Auto Update サーバを定期的にポーリングします。Auto Update サーバとして動作する場合は、Auto Update クライアントとして設定された ASA のアップデートを発行します。

自動更新の利点

Auto Update は、次のように、管理者が ASA の管理で直面するさまざまな問題を解決できる便利な機能です。

- ダイナミック アドレッシングおよび NAT に関する問題点の解決。
- コンフィギュレーションの変更を 1 つのアクションでコミット。
- ソフトウェア更新用の信頼度の高い方式の提供。

- ハイ アベイラビリティ用の十分実績のある方式の活用（フェールオーバー）。
- オープン インターフェイスによる柔軟性の提供。
- サービス プロバイダー環境のセキュリティ ソリューションの簡素化。

Auto Update 仕様は、中央、または複数の場所から、リモート管理アプリケーションにより ASA のコンフィギュレーションやソフトウェア イメージをダウンロードしたり、基本的な監視機能を実行したりする場合に必要なインフラストラクチャです。

Auto Update 仕様に従うと、Auto Update サーバから ASA にコンフィギュレーション情報をプッシュしたり、要求を送信して情報を取得したりすることも、ASA から Auto Update サーバに定期的にポーリングすることによって、最新のコンフィギュレーション情報を引き出す（プルする）こともできます。また、Auto Update サーバはいつでも ASA にコマンドを送信し、ただちにポーリング要求を送信させることもできます。Auto Update サーバと ASA の通信では、通信パスとローカル CLI コンフィギュレーションをすべての ASA に設定する必要があります。

フェールオーバー コンフィギュレーションでの Auto Update サーバ サポート

Auto Update サーバを使用して、ソフトウェア イメージとコンフィギュレーション ファイルを、アクティブ/スタンバイ フェールオーバー コンフィギュレーションの ASA に配置できます。アクティブ/スタンバイ フェールオーバー コンフィギュレーションで Auto Update をイネーブルにするには、フェールオーバー ペアのプライマリ装置に Auto Update サーバのコンフィギュレーションを入力します。

フェールオーバー コンフィギュレーションの Auto Update サーバ サポートには、次の制限と動作が適用されます。

- アクティブ/スタンバイ コンフィギュレーションがサポートされるのは、シングル モードだけです。
- 新しいプラットフォーム ソフトウェア イメージをロードする際、フェールオーバー ペアはトラフィックの転送を停止します。
- LAN ベースのフェールオーバーを使用する場合、新しいコンフィギュレーションによってフェールオーバー リンクのコンフィギュレーションが変更されてはいけません。フェールオーバー リンクのコンフィギュレーションが変更されると、装置間の通信は失敗します。
- Auto Update サーバへの Call Home を実行するのはプライマリ装置だけです。Call Home を実行するには、プライマリ装置がアクティブ状態である必要があります。そうでない場合、ASA は自動的にプライマリ装置にフェールオーバーします。
- ソフトウェア イメージまたはコンフィギュレーション ファイルをダウンロードするのは、プライマリ装置だけです。その後、ソフトウェア イメージまたはコンフィギュレーション ファイルはセカンダリ装置にコピーされます。
- インターフェイス MAC アドレスとハードウェアのシリアル番号は、プライマリ装置のものです。
- Auto Update サーバまたは HTTP サーバに保存されたコンフィギュレーション ファイルは、プライマリ装置専用です。

Auto Update プロセスの概要

次に、フェールオーバー コンフィギュレーションでの Auto Update プロセスの概要を示します。このプロセスは、フェールオーバーがイネーブルであり、動作していることを前提としています。装置がコンフィギュレーションを同期化している場合、SSM カードの不具合以外の理由でスタンバイ装置に障害が発生している場合、または、フェールオーバー リンクがダウンしている場合、Auto Update プロセスは実行できません。

1. 両方の装置は、プラットフォームおよび ASDM ソフトウェア チェックサムとバージョン情報を交換します。
2. プライマリ装置は Auto Update サーバにアクセスします。プライマリ装置がアクティブ状態でない場合、ASA はプライマリ装置にフェールオーバーした後、Auto Update サーバにアクセスします。
3. Auto Update サーバは、ソフトウェア チェックサムと URL 情報を返します。
4. プライマリ装置が、アクティブまたはスタンバイ装置のプラットフォーム イメージ ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
   a. プライマリ装置は、Auto Update サーバの URL を使用して、HTTP サーバから適切なファイルを取得します。
   b. プライマリ装置は、そのイメージをスタンバイ装置にコピーしてから、自身のイメージをアップデートします。
   c. 両方の装置に新しいイメージがある場合は、セカンダリ（スタンバイ）装置が最初にリロードされます。
   – セカンダリ装置のブート時にヒットレス アップグレードが可能な場合は、セカンダリ装置がアクティブ装置になり、プライマリ装置がリロードされます。リロードが終了すると、プライマリ装置がアクティブ装置になります。
   – スタンバイ装置のブート時にヒットレス アップグレードができない場合は、両方の装置が同時にリロードされます。
   d. セカンダリ（スタンバイ）装置だけに新しいイメージがある場合は、セカンダリ装置だけがリロードされます。プライマリ装置は、セカンダリ装置のリロードが終了するまで待機します。
   e. プライマリ（アクティブ）装置だけに新しいイメージがある場合は、セカンダリ装置がアクティブ装置になり、プライマリ装置がリロードされます。
   f. もう一度アップデート プロセスが手順 1 から開始されます。
5. ASA が、プライマリまたはセカンダリ装置の ASDM ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
   a. プライマリ装置は、Auto Update サーバから提供された URL を使用して、HTTP サーバから ASDM イメージ ファイルを取得します。
   b. プライマリ装置は、必要に応じてそのイメージをスタンバイ装置にコピーします。
   c. プライマリ装置は、自身の ASDM イメージをアップデートします。
   d. もう一度アップデート プロセスが手順 1 から開始されます。
6. プライマリ装置が、コンフィギュレーション ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
   a. プライマリ装置は、指定された URL を使用して、からコンフィギュレーション ファイルを取得します。
   b. 両方の装置で同時に、古いコンフィギュレーションが新しいコンフィギュレーションに置換されます。
   c. もう一度アップデート プロセスが手順 1 から開始されます。

7. チェックサムがすべてのイメージおよびコンフィギュレーション ファイルと一致している場合、アップデートは必要ありません。このプロセスは、次のポーリング時間まで中断されます。

Auto Update プロセスのモニタリング

debug auto-update client または **debug fover cmd-exe** コマンドを使用して、Auto Update プロセスで実行される処理を表示できます。次に、**debug auto-update client** コマンドの出力例を示します。ターミナル セッションから **debug** コマンドを実行します。

```
Auto-update client: Sent DeviceDetails to /cgi-bin/dda.pl of server 192.168.0.21
Auto-update client: Processing UpdateInfo from server 192.168.0.21
   Component: asdm, URL: http://192.168.0.21/asdm.bint, checksum:
0x94bced0261cc992ae710faf8d244cf32
   Component: config, URL: http://192.168.0.21/config-rms.xml, checksum:
0x67358553572688a805a155af312f6898
   Component: image, URL: http://192.168.0.21/cdisk73.bin, checksum:
0x6d091b43ce96243e29a62f2330139419
Auto-update client: need to update img, act: yes, stby yes
name
ciscoasa(config)# Auto-update client: update img on stby unit...
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 9001, len = 1024
auto-update: Fover file copy waiting at clock tick 6129280
fover_parse: Rcvd file copy ack, ret = 0, seq = 4
auto-update: Fover filecopy returns value: 0 at clock tick 6150260, upd time 145980 msecs
Auto-update client: update img on active unit...
fover_parse: Rcvd image info from mate
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
Beginning configuration replication: Sending to mate.
auto-update: HA safe reload: reload active waiting with mate state: 50
```

```
auto-update: HA safe reload: reload active waiting with mate state: 50

auto-update: HA safe reload: reload active waiting with mate state: 80
        Sauto-update: HA safe reload: reload active unit at clock tick: 6266860
Auto-update client: Succeeded: Image, version: 0x6d091b43ce96243e29a62f2330139419
```

Auto Update プロセスが失敗すると、次の syslog メッセージが生成されます。

```
%ASA4-612002: Auto Update failed: file version: version reason: reason
```

The *file* is “image”, “asdm”, or “configuration”, depending on which update failed.*version* は、アップデートのバージョン番号です。*reason* は、アップデートが失敗した原因です。

注意事項と制約事項

- ASA のコンフィギュレーションが Auto Update で更新されても、ASDM には通知されません。[Refresh] または [File] > [Refresh ASDM with the Running Configuration on the Device] を選択して、最新のコンフィギュレーションを取得する必要があります。また、ASDM でコンフィギュレーションに加えた変更は失われます。
- Auto Update サーバと通信するためのプロトコルとして HTTPS が選択されている場合は、ASA は SSL を使用します。これは、ASA が DES または 3DES ライセンスを保有していることを必要とします。
- Auto Update は、シングル コンテキスト モードでのみサポートされます。

Auto Update サーバとの通信の設定

手順の詳細

Auto Update 機能を設定するには、[Configuration] > [Device Management] > [System Image/Configuration] > [Auto Update] を選択します。[Auto Update] ペインには、[Auto Update Servers] テーブルの他に [Timeout] 領域と [Polling] 領域があります。

[Auto Update Servers] テーブルで、Auto Update サーバにすでに設定されているパラメータを確認できます。ASA は、テーブルの一番上にあるサーバを最初にポーリングします。テーブル内のサーバの順序を変更するには、[Move Up] または [Move Down] をクリックします。[Auto Update Servers] テーブルには次のカラムがあります。

- [Server]：Auto Update サーバの名前または IP アドレス。
- [User Name]：Auto Update サーバのアクセス時に使用されるユーザ名。
- [Interface]：Auto Update サーバへの要求送信時に使用されるインターフェイス。
- [Verify Certificate]：Auto Update サーバが返した証明書を、ASA で CA のルート証明書と照合して確認するかどうかを指定します。Auto Update サーバおよび ASA は同じ CA を使用する必要があります。

[Auto Update Server] テーブルの行のいずれかをダブルクリックすると、[Edit Auto Update Server] ダイアログボックスが開き、Auto Update サーバのパラメータを変更できます。ここで行った変更はただちにテーブルに反映されますが、コンフィギュレーションに保存するには [Apply] をクリックする必要があります。

[Timeout] エリアでは、ASA が Auto Update サーバのタイムアウトを待つ時間を設定できます。[Timeout] 領域には次のフィールドがあります。

- [Enable Timeout Period]：ASA が Auto Update サーバから応答を受信しなかった場合にタイムアウトするには、オンにします。
- [Timeout Period (Minutes)]：Auto Update サーバから応答がなかった場合の ASA のタイムアウト時間（分単位）を指定します。

[Polling] エリアで、ASA から Auto Update サーバの情報をポーリングする頻度を設定できます。[Polling] 領域には次のフィールドがあります。

- [Polling Period (minutes)] : ASA から Auto Update サーバに新しい情報をポーリングするときの待ち時間（分単位）。
- [Poll on Specified Days]：ポーリングのスケジュールを指定します。
- [Set Polling Schedule]：[Set Polling Schedule] ダイアログボックスが表示され、Auto Update サーバをポーリングする日付と時刻を設定できます。
- [Retry Period (minutes)]：サーバのポーリングに失敗した場合、ASA から Auto Update サーバに新しい情報をポーリングするまでの待ち時間（分単位）。
- [Retry Count]：ASA から Auto Update サーバに新しい情報をポーリングするときの再試行回数。

Auto Update サーバの追加または編集

[Add/Edit Auto Update Server] ダイアログボックスには次のフィールドがあります。

- [URL]：Auto Update サーバが ASA と通信する際に使用する HTTP または HTTPS のプロトコルと Auto Update サーバへのパスです。
- [Interface]：Auto Update サーバに要求を送信する際に使用するインターフェイス。
- [Do not verify server's SSL certificate]：CA のルート証明書をもつ Auto Update サーバによって返される証明書の検証をディセーブルにする場合はオンにします。Auto Update サーバおよび ASA は同じ CA を使用する必要があります。

[User] 領域には次のフィールドがあります。

- [User Name (Optional)]：Auto Update サーバのアクセス時に必要なユーザ名を入力します。
- [Password]：Auto Update サーバのユーザ パスワードを入力します。
- [Confirm Password]：Auto Update サーバのユーザ パスワードを再入力します。
- [Use Device ID to uniquely identify the ASA]: デバイス ID による認証をイネーブルにします。デバイス ID により、ASA が Auto Update サーバを一意に識別できます。
- [Device ID]：使用するデバイス ID のタイプ。
  - [Hostname]：ホストの名前。
  - [Serial Number]：デバイスのシリアル番号。
  - [IP Address on interface]：選択したインターフェイスの IP アドレス。ASA を Auto Update サーバが一意に識別する場合に使用します。
  - [MAC Address on interface] : 選択したインターフェイスの MAC アドレス。ASA を Auto Update サーバが一意に識別する場合に使用します。
  - [User-defined value]：一意のユーザ ID。

ポーリング スケジュールの設定

[Set Polling Schedule] ダイアログボックスでは、ASA から Auto Update サーバをポーリングする特定の日付と時刻を設定できます。

[Set Polling Schedule] ダイアログボックスには次のフィールドがあります。

[Days of the Week]：ASA から Auto Update サーバをポーリングする曜日のチェックボックスを選択します。

[Daily Update] ペイン グループでは、ASA が Auto Update サーバをポーリングする時刻を設定できます。次のフィールドがあります。

- [Start Time]：Auto Update のポーリング開始時刻を入力します。
- [Enable randomization] : ASA から Auto Update サーバをランダムに選択した時刻にポーリングするには、オンにします。

ソフトウェアと設定の機能履歴

表 37-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 37-2　ソフトウェアと設定の機能履歴

機能名	プラットフォーム リリース	機能情報
セキュア コピー クライアント	9.1(5)/9.2(1)	現在、ASA では SCP サーバとの間でファイルを転送するために Secure Copy（SCP）クライアントがサポートされています。 次の画面が変更されました。 [Tools] > [File Management] > [File Transfer] > [Between Remote Server and Flash] [Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP) Server]
デフォルトでイネーブルになっている Auto Update サーバ証明書の検証	9.2(1)	Auto Update サーバ証明書の検証がデフォルトでイネーブルになりました。新しいコンフィギュレーションでは証明書の検証を明示的にディセーブルにする必要があります。以前のリリースからアップグレードする場合に証明書の検証がイネーブルになっていないと、証明書の検証がイネーブルにならずに次の警告が表示されます。 `WARNING: The certificate provided by the auto-update servers will not be verified.` この証明書を検証するには `verify-certificate` オプションを使用します。 コンフィギュレーションの移行では、検証を行わないように明示的に設定されます。 次の画面が変更されました。[Configuration] > [Device Management] > [System/Image Configuration] > [Auto Update] > [Add Auto Update Server]。

システム イベントに対する応答の自動化

この章では、Embedded Event Manager（EEM）を設定する方法について説明します。

EEM について

EEM サービスを利用することで、問題をデバッグし、トラブルシューティングに対して汎用ロギングを提供できます。EEM サービスには 2 つのコンポーネント、つまり EEM が応答またはリッスンするイベント、およびアクションと EEM が応答するイベントを定義するイベント マネージャ アプレットがあります。さまざまなイベントに応答し、さまざまなアクションを実行するために、複数のイベント マネージャ アプレットを設定できます。

サポートされるイベント

EEM は次のイベントをサポートします。

- Syslog：ASA は、syslog メッセージの ID を使用して、イベント マネージャ アプレットをトリガーする syslog メッセージを識別します。複数の syslog イベントを設定できますが、単一のイベント マネージャ アプレット内で syslog メッセージの ID が重複することはできません。
- タイマー：タイマーを使用して、イベントをトリガーできます。各タイマーは、各イベント マネージャ アプレットに対して一度だけ設定できます。各イベント マネージャ アプレットには最大で 3 つのタイマーがあります。3 種類のタイマーは次のとおりです。
  - ウォッチドッグ（定期的）タイマーは、アプレット アクションの完了後に指定された期間が経過するとイベント マネージャ アプレットをトリガーし、自動的にリスタートします。
  - カウントダウン（ワンショット）タイマーは、指定された期間が経過するとイベント マネージャ アプレットを 1 回トリガーします。削除および再追加されない限りはリスタートしません。
  - 絶対（1 日 1 回）タイマーは、イベントを 1 日 1 回指定された時刻に発生させ、自動的にリスタートします。時刻の形式は hh:mm:ss です。

各イベント マネージャ アプレットに対して、各タイプのタイマー イベントを 1 つだけ設定できます。

- なし：CLI または ASDM を使用してイベント マネージャ アプレットを手動で実行する場合、イベントはトリガーされません。
- クラッシュ：ASA がクラッシュした場合、クラッシュ イベントがトリガーされます。**output** コマンドの値に関係なく、**action** コマンドはクラッシュ情報ファイルを対象とします。出力は **show tech** コマンドの前に生成されます。

イベント マネージャ アプレットのアクション

イベント マネージャ アプレットがトリガーされると、そのイベント マネージャ アプレットのアクションが実行されます。各アクションには、アクションの順序を指定するために使用される番号があります。このシーケンス番号は、イベント マネージャ アプレット内で一意である必要があります。イベント マネージャ アプレットには複数のアクションを設定できます。コマンドは典型的な CLI コマンドです（**show blocks** など）。

出力先

output コマンドを使用すると、アクションの出力を指定した場所に送信できます。一度にイネーブルにできる出力値は 1 つだけです。デフォルト値は **output none** です。この値は、**action** コマンドによるすべての出力を破棄します。このコマンドは、特権レベル 15（最高）を持つユーザとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けません。**action** CLI コマンドの出力を次の 3 つの場所のいずれかに送信できます。

- なし：これがデフォルトです。出力を破棄します。
- コンソール：出力を ASA コンソールに送信します。
- ファイル：出力をファイルに送信します。次の 4 つのファイル オプションを使用できます。
  - 一意のファイルを作成する：イベント マネージャ アプレットが呼び出されるたびに、一意の名前を持つ新しいファイルを作成します。
  - ファイルを作成する/ファイルを上書きする：イベント マネージャ アプレットが呼び出されるたびに、指定されたファイルを上書きします。
  - ファイルを作成する/ファイルに付加する：イベント マネージャ アプレットが呼び出されるたびに、指定されたファイルに付加します。ファイルがまだ存在しない場合は作成されます。
  - 一連のファイルを作成する：イベント マネージャ アプレットが呼び出されるたびにローテーションされる、一意の名前を持つ一連のファイルを作成します。

EEM のガイドライン

コンテキスト モードのガイドライン

マルチ コンテキスト モードではサポートされません。

その他のガイドライン

- 通常、クラッシュ時は ASA の状態が不明です。こうした状況では、一部のコマンドの実行は安全ではない可能性があります。
- イベント マネージャ アプレットの名前にはスペースを含めることができません。

- None イベントおよび Crashinfo イベント パラメータは変更できません。
- syslog メッセージが EEM に送信されて処理されるため、パフォーマンスが影響を受ける可能性があります。
- 各イベント マネージャ アプレットのデフォルトの出力は、**output none** です。この設定を変更するには、異なる出力値を入力する必要があります。
- 各イベント マネージャ アプレットに定義できる出力オプションは 1 つだけです。

EEM の設定

EEM の設定は、次のタスクで構成されています。

ステップ 1　イベント マネージャ アプレットを作成してから、さまざまなイベントを設定します。「イベント マネージャ アプレットの作成とイベントの設定」（P.38-3）を参照してください。

ステップ 2　イベント マネージャ アプレットにアクションを設定し、続いてアクションからの出力先を設定します。「アクションおよびアクションからの出力先の設定」（P.38-4）を参照してください。

ステップ 3　イベント マネージャ アプレットを実行します。「イベント マネージャ アプレットの実行」（P.38-5）を参照してください。

イベント マネージャ アプレットの作成とイベントの設定

イベント マネージャ アプレットを作成してイベントを設定するには、次の手順を実行します。

手順

ステップ 1　ASDM で、[Configuration] > [Device Management] > [Advanced] > [Embedded Event Manager] を選択します。

ステップ 2　[Add] をクリックして、[Add Event Manager Applet] ダイアログボックスを表示します。

ステップ 3　アプレット名（スペースを含まない）を入力し、そのアプレットに関する説明を入力します。説明の長さは最大 256 文字です。引用符内であれば、説明テキストにスペースを含めることができます。

ステップ 4　[Events] 領域にある [Add] をクリックして、[Add Event Manager Applet Event] ダイアログボックスを表示します。

ステップ 5　[Type] ドロップダウン リストから設定したいイベント タイプを選択します。使用可能なオプションは、[Crashinfo]、[None]、[Syslog]、[Once-a-day timer]、[One-shot timer]、および [Periodic timer] です。

- [Syslog]：単一の syslog メッセージまたは syslog メッセージの範囲を入力します。指定された個々の syslog メッセージまたは syslog メッセージの範囲に一致する syslog メッセージが発生すると、イベント マネージャ アプレットがトリガーされます。（オプション）イベント マネージャ アプレットを呼び出すために syslog メッセージが発生する必要がある回数を [Occurrences] フィールドに入力します。デフォルトの発生回数は 0 秒ごとに 1 回です。有効な値は 1 ～ 4294967295 です。（オプション）アクションを呼び出すために syslog メッセージが発生しなければならない許容時間（秒数）を [Period] フィールドに入力します。

この値によって、イベント マネージャ アプレットが設定された期間に 1 回呼び出される際の最大の間隔が制限されます。有効な値は 0 ～ 604800 です。値 0 は、期間が定義されていないことを示しています。

- [Periodic]：期間を秒単位で入力します。秒数は、1 ～ 604800 の範囲で設定してください。
- [Once-a-day timer]：時刻を hh:mm:ss の形式で入力します。時刻の範囲は 00:00:00（真夜中）から 23:59:59 です。
- [One-shot timer]：期間を秒単位で入力します。秒数は、1 ～ 604800 の範囲で設定してください。
- [None]：イベント マネージャ アプレットを手動で呼び出すには、このオプションを選択します。
- [Crashinfo]：ASA のクラッシュ時にクラッシュ イベントをトリガーするには、このオプションを選択します。

アクションおよびアクションからの出力先の設定

アクションおよびアクションからの出力を送信する特定の宛先を設定するには、次の手順を実行します。

手順

ステップ 1　[Add] をクリックして、[Add Event Manager Applet] ダイアログボックスを表示します。

ステップ 2　アプレット名（スペースを含まない）を入力し、そのアプレットに関する説明を入力します。説明の長さは最大 256 文字です。

ステップ 3　[Actions] 領域にある [Add] をクリックして、[Add Event Manager Applet Action] ダイアログボックスを表示します。

ステップ 4　[Sequence #] フィールドに一意のシーケンス番号を入力します。有効なシーケンス番号の範囲は 0 ～ 4294967295 です。

ステップ 5　CLI コマンドを [CLI Command] フィールドに入力します。このコマンドは、特権レベル 15（最高）を持つユーザとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けない場合があります。

ステップ 6　[OK] をクリックして、[Add Event Manager Applet Action] ダイアログボックスを閉じます。

新しく追加されたアクションが [Actions] リストに表示されます。

ステップ 7　[Add] をクリックして、[Add Event Manager Applet] ダイアログボックスを開きます。

ステップ 8　使用可能な出力先オプションを 1 つ選択します。

- **action** コマンドからの出力を破棄するには、[Output Location] ドロップダウン リストから [None] オプションを選択します。これがデフォルト設定です。
- **action** コマンドの出力をコンソールに送信するには、[Output Location] ドロップダウン リストから [Console] オプションを選択します。

（注）　このコマンドを実行すると、パフォーマンスに影響を及ぼします。

- **action** コマンドの出力を呼び出された各イベント マネージャ アプレットの新しいファイルに送信するには、[Output Location] ドロップダウン リストから [File] オプションを選択します。[Create a unique file] オプションがデフォルトとして自動的に選択されます。

  ファイル名の形式は、eem-*applet*-*timestamp*.log です。ここで、*applet* はイベント マネージャ アプレットの名前、*timestamp* は日付のタイム スタンプ（形式は YYYYMMDD-hhmmss）を示しています。

- ローテーションされる一連のファイルを作成するには、[Output Location] ドロップダウン リストから [File] オプションを選択し、続いてドロップダウン リストから [Create a set of files] オプションを選択します。

  新しいファイルが書き込まれる場合、最も古いファイルが削除され、最初のファイルが書き込まれる前に後続のすべてのファイルに番号が再度割り振られます。最も新しいファイルが 0 で示され、最も古いファイルが最大数で示されます。有効なローテーションの値の範囲は 2 ～ 100 です。ファイル名の形式は、eem-*applet*-*x*.log です。ここで、*applet* はアプレットの名前、*x* はファイル番号を示しています。

- **action** コマンドの出力を毎回上書きされる単一のファイルに書き込むには、[Output Location] ドロップダウン リストから [File] オプションを選択し、続いてドロップダウン リストから [Create/overwrite a file] オプションを選択します。

- **action** コマンドの出力を毎回付加される単一のファイルに書き込むには、[Output Location] ドロップダウン リストから [File] オプションを選択し、続いてドロップダウン リストから [Create/append a file] オプションを選択します。

ステップ 9　[OK] をクリックして、[Add Event Manager Applet] ダイアログボックスを閉じます。

指定した出力先は [Embedded Event Manager] ペインに表示されます。

イベント マネージャ アプレットの実行

イベント マネージャ アプレットを実行するには、次の手順を実行します。

手順

ステップ 1　[Embedded Event Manager] ペインで、**None** イベントで設定されたイベント マネージャ アプレットをリストから選択します。

ステップ 2　[Run] をクリックします。

EEM の例

次に、ブロックの漏えい情報を 1 時間ごとに記録し、その出力をローテーションされる一連のログ ファイルに書き込み、1 日分のログを保持するイベント マネージャ アプレットの例を示します。

```
ciscoasa(config)# event manager applet blockcheck
ciscoasa(config-applet)# description "Log block usage"
ciscoasa(config-applet)# event timer watchdog time 3600
ciscoasa(config-applet)# output rotate 24
ciscoasa(config-applet)# action 1 cli command "show blocks old"
```

次に、毎日午前 1 時に ASA をリブートし、必要に応じて設定を保存するイベント マネージャ アプレットの例を示します。

```
ciscoasa(config)# event manager applet dailyreboot
ciscoasa(config-applet)# description "Reboot every night"
ciscoasa(config-applet)# event timer absolute time 1:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "reload save-config noconfirm"
```

次に、真夜中から午前 3 時の間に特定のインターフェイスをディセーブルにするイベント マネージャ アプレットの例を示します。

```
ciscoasa(config)# event manager applet disableintf
ciscoasa(config-applet)# description "Disable the interface at midnight"
ciscoasa(config-applet)# event timer absolute time 0:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"

ciscoasa(config)# event manager applet enableintf
ciscoasa(config-applet)# description "Enable the interface at 3am"
ciscoasa(config-applet)# event timer absolute time 3:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "no shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"
```

EEM のモニタリング

EEM をモニタするには、次の画面を参照してください。

- **[Monitoring] > [Properties] > [EEM Applets]**

  このペインでは、EEM アプレットとそのヒット カウント値のリストを表示します。

- **[Tools] > [Command Line Interface]**

  非対話形式の各種コマンドを発行して結果を表示できます。

EEM の履歴

表 38-1　EEM の履歴

機能名	プラットフォーム リリース	説明
Embedded Event Manager（EEM）	9.2(1)	EEM サービスを利用することで、問題をデバッグし、トラブルシューティングに対して汎用ロギングを提供できます。EEM サービスには 2 つのコンポーネント、つまり EEM が応答またはリッスンするイベント、およびアクションと EEM が応答するイベントを定義するイベント マネージャ アプレットがあります。さまざまなイベントに応答し、さまざまなアクションを実行するために、複数のイベント マネージャ アプレットを設定できます。 次の画面が導入されました。[Configuration] > [Device Management] > [Advanced] > [Embedded Event Manager]、[Monitoring] > [Properties] > [EEM Applets]。

トラブルシューティング

この章では、Cisco ASA のトラブルシューティングを行う方法について説明します。

Packet Capture Wizard を使用したキャプチャの設定と実行

Packet Capture Wizard を使用して、エラーのトラブルシューティングを行う場合のキャプチャを設定および実行できます。キャプチャでは ACL を使用して、キャプチャされるトラフィックのタイプを、送信元と宛先のアドレスとポート、および 1 つ以上のインターフェイスで制限できます。このウィザードは、入出力インターフェイスのそれぞれでキャプチャを 1 回実行します。キャプチャしたパケットは、PC に保存してパケット アナライザで分析できます。

（注） このツールは、クライアントレス SSL VPN キャプチャをサポートしていません。

キャプチャを設定および実行するには、次の手順を実行します。

手順

ステップ 1 [Wizards] > [Packet Capture Wizard] を選択します。

[Overview of Packet Capture] 画面には、ウィザードを完了するまでに行うタスクの一覧が表示されます。これらのタスクには、以下が含まれます。

- 入力インターフェイスの選択。
- 出力インターフェイスの選択。
- バッファ パラメータの設定。
- キャプチャの実行。
- （オプション）キャプチャ データの PC への保存。

ステップ 2 [Next] をクリックします。

クラスタ環境では、[Cluster Option] 画面が表示されます。ステップ 3 に進みます。

非クラスタ環境では、[Ingress Traffic Selector] 画面が表示されます。ステップ 4 に進みます。

ステップ 3　[Cluster Option] 画面で、キャプチャの実行対象について、[This device only] または [The whole cluster] のいずれかのオプションを選択します。[Next] をクリックして [Ingress Selector] 画面を表示します。

ステップ 4　インターフェイスでパケットをキャプチャするには、[Select Interface] オプション ボタンをクリックします。ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。

ステップ 5　[Packet Match Criteria] 領域で、次のいずれかを実行します。

- パケットの照合に使用する ACL を指定するには、[Specify access-list] オプション ボタンをクリックし、[Select ACL] ドロップダウン リストから ACL を選択します。以前設定した ACL を現在のドロップダウン リストに追加するには、[Manage] をクリックして [ACL Manager] ペインを表示します。ACL を選択して [OK] をクリックします。
- [Specify Packet Parameters] オプション ボタンをクリックして、パケット パラメータを指定します。

ステップ 6　以降の手順については、「Ingress Traffic Selector」（P.39-3）を参照してください。

ステップ 7　[Next] をクリックして、[Egress Traffic Selector] 画面を表示します。以降の手順については、「Egress Traffic Selector」（P.39-4）を参照してください。

（注）　送信元ポートのサービス、宛先ポートのサービスおよび ICMP タイプは読み取り専用であり、[Ingress Traffic Selector] 画面での選択に基づきます。

ステップ 8　[Next] をクリックして [Buffers & Captures] 画面を表示します。以降の手順については、「Buffers」（P.39-4）を参照してください。

ステップ 9　最新のキャプチャを 10 秒ごとに自動的に取得するように、[Capture Parameters] 領域で [Get capture every 10 seconds] チェックボックスをオンにします。デフォルトでは、このキャプチャは循環バッファを使用します。

ステップ 10　[Buffer Parameters] 領域で、バッファ サイズとパケット サイズを指定します。バッファ サイズは、キャプチャがパケットを保存するために使用可能なメモリの最大容量です。パケット サイズは、キャプチャが保持できる最長のパケットです。できる限り多くの情報をキャプチャするため、最長パケット サイズを使用することを推奨します。

a. パケット サイズを入力します。有効なサイズ範囲は 14 ～ 1522 バイトです。
b. バッファ サイズを入力します。有効なサイズ範囲は 1534 ～ 33554432 バイトです。
c. キャプチャされたパケットを保存するには、[Use circular buffer] チェックボックスをオンにします。

（注）　この設定を選択すると、すべてのバッファ ストレージが使用されている場合、キャプチャは最も古いパケットへの上書きを始めます。

ステップ 11　[Next] をクリックして、入力したクラスタ内の全装置のクラスタ オプション（クラスタを使用している場合）、トラフィック セレクタ、バッファ パラメータを表示する [Summary] 画面を表示します。以降の手順については、「概要」（P.39-5）を参照してください。

ステップ 12　[Next] をクリックして [Run Captures] 画面を表示し、次に [Start] をクリックしてパケットのキャプチャを開始します。[Stop] をクリックしてキャプチャを終了します。以降の手順については、「キャプチャの実行」（P.39-5）を参照してください。クラスタリングを使用している場合は、ステップ 14 に進みます。

ステップ 13　残りのバッファ スペースを確認するには、[Get Capture Buffer] をクリックします。現在のパケットの内容を削除して、バッファに別のパケットをキャプチャするスペースを確保するには、[Clear Buffer on Device] をクリックします。

ステップ 14　クラスタ環境では、[Run Captures] 画面で、次の手順の 1 つ以上を実行します。

- [Get Cluster Capture Summary] をクリックすると、クラスタ内の全装置のパケット キャプチャ情報のサマリーに続いて、各装置のパケット キャプチャ情報が表示されます。
- [Get Capture Buffer] をクリックすると、クラスタの各装置にどの程度バッファ スペースが残っているかが表示されます。[Capture Buffer from Device] ダイアログボックスが表示されます。
- [Clear Capture Buffer] をクリックすると、クラスタ内の特定の装置またはすべての装置の現在のコンテンツを削除し、さらにパケットをキャプチャするためのバッファ容量を確保します。

ステップ 15　[Save captures] をクリックして、[Save Capture] ダイアログボックスを表示します。入力キャプチャ、出力キャプチャ、またはその両方を保存するオプションを選択できます。以降の手順については、「キャプチャの保存」（P.39-5）を参照してください。

ステップ 16　[Save Ingress Capture] をクリックして、[Save capture file] ダイアログボックスを表示します。PC 上の保存場所を指定して、[Save] をクリックします。

ステップ 17　[Launch Network Sniffer Application] をクリックして、[Tools] > [Preferences] で指定したパケット分析アプリケーションを起動し、入力キャプチャを分析します。

ステップ 18　[Save Egress Capture] をクリックして、[Save capture file] ダイアログボックスを表示します。PC 上の保存場所を指定して、[Save] をクリックします。

ステップ 19　[Launch Network Sniffer Application] をクリックして、[Tools] > [Preferences] で指定したパケット分析アプリケーションを起動し、出力キャプチャを分析します。

ステップ 20　[Close] をクリックし、次に [Finish] をクリックしてウィザードを終了します。

Ingress Traffic Selector

パケット キャプチャの入力インターフェイス、送信元と宛先のホストまたはネットワーク、およびプロトコルを設定するには、次の手順を実行します。

手順

ステップ 1　ドロップダウン リストから入力インターフェイス名を選択します。

ステップ 2　入力送信元ホストおよびネットワークを入力します。ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。

ステップ 3　入力宛先ホストおよびネットワークを入力します。

ステップ 4　キャプチャするプロトコル タイプを指定します。指定できるプロトコルは、ah、eigrp、esp、gre、icmp、icmp6、igmp、igrp、ip、ipinip、nos、ospf、pcp、pim、snp、tcp、または udp です。

a. ICMP にのみ ICMP タイプを入力します。指定できるタイプは、all、alternate address、conversion-error、echo、echo-reply、information-reply、information-request、mask-reply、mask-request、mobile-redirect、parameter-problem、redirect、router-advertisement、router-solicitation、source-quench、time-exceeded、timestamp-reply、timestamp-request、traceroute、または unreachable です。

b. TCP および UDP プロトコルだけの送信元および宛先ポートのサービスを指定します。指定できるオプションは次のとおりです。
   - すべてのサービスを含めるには、[All Services] を選択します。
   - サービス グループを含めるには、[Service Groups] を選択します。

     特定のサービスを含めるには、aol、bgp、chargen、cifx、citrix-ica、ctiqbe、daytime、discard、domain、echo、exec、finger、ftp、ftp-data、gopher、h323、hostname、http、https、ident、imap4、irc、kerberos、klogin、kshell、ldap、ldaps、login、lotusnotes、lpd、netbios-ssn、nntp、pcanywhere-data、pim-auto-rp、pop2、pop3、pptp、rsh、rtsp、sip、smtp、sqlnet、ssh、sunrpc、tacacs、talk、telnet、uucp、または whois のいずれかを指定します。

ステップ 5　Cisco TrustSec サービスのパケット キャプチャをイネーブルにするには、[Security Group Tagging] 領域の [SGT number] チェックボックスをオンにして、セキュリティ グループ タグ番号を入力します。有効なセキュリティ グループ タグ番号は 2 ～ 65519 です。

Egress Traffic Selector

パケット キャプチャでの出力インターフェイス、送信元と宛先のホストとネットワーク、および送信元と宛先ポートのサービスを設定するには、次の手順を実行します。

手順

ステップ 1　インターフェイスでパケットをキャプチャするには、[Select Interface] オプション ボタンをクリックします。ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。

ステップ 2　ドロップダウン リストから出力インターフェイス名を選択します。

ステップ 3　出力送信元ホストおよびネットワークを入力します。

ステップ 4　出力宛先ホストおよびネットワークを入力します。

入力設定時に選択したプロトコル タイプがすでにリストされています。

Buffers

パケット キャプチャのパケット サイズ、バッファ サイズ、および循環バッファを使用するかどうかを設定するには、次の手順を実行します。

手順

ステップ 1　キャプチャが保持できる最長のパケットを入力します。できるだけ多くの情報をキャプチャするために、指定可能な最長サイズを使用してください。

ステップ 2　パケットを保存するためにキャプチャが使用できるメモリの最大容量を入力します。

ステップ 3　パケットの保存には循環バッファを使用します。循環バッファのバッファ ストレージがすべて使い尽くされると、キャプチャは最も古いパケットから上書きを始めます。

概要

[Summary] 画面には、前のウィザード画面で選択したパケット キャプチャのためのクラスタ オプション（クラスタリングを使用している場合）、トラフィック セレクタ、バッファ パラメータが表示されます。

キャプチャの実行

キャプチャ セッションの開始および停止、キャプチャ バッファの表示、ネットワーク アナライザ アプリケーションの起動、パケット キャプチャの保存、およびバッファのクリアを行うには、次の手順を実行します。

手順

ステップ 1　[Start] をクリックして、選択したインターフェイス上でパケット キャプチャ セッションを開始します。

ステップ 2　[Stop] をクリックして、選択したインターフェイス上のパケット キャプチャ セッションを停止します。

ステップ 3　[Get Capture Buffer] をクリックして、インターフェイス上でキャプチャされたパケットのスナップショットを取得します。

ステップ 4　[Ingress] をクリックして、入力インターフェイスのキャプチャ バッファを表示します。

ステップ 5　[Egress] をクリックして、出力インターフェイスのキャプチャ バッファを表示します。

ステップ 6　[Clear Buffer on Device] をクリックして、デバイス上のバッファを消去します。

ステップ 7　[Launch Network Sniffer Application] をクリックして、[Tools] > [Preferences] で指定した、入力キャプチャまたは出力キャプチャを分析するためのパケット分析アプリケーションを起動します。

ステップ 8　[Save Captures] をクリックして、入力キャプチャおよび出力キャプチャを ASCII または PCAP 形式で保存します。

キャプチャの保存

パケットをさらに分析するために、入力および出力パケット キャプチャを ASCII または PCAP ファイル形式で保存するには、次の手順を実行します。

手順

ステップ 1　キャプチャ バッファを ASCII 形式で保存するには、[ASCII] をクリックします。

ステップ 2　キャプチャ バッファを PCAP 形式で保存するには、[PCAP] をクリックします。

ステップ 3　入力パケット キャプチャを保存するファイルを指定するには、[Save ingress capture] をクリックします。

ステップ 4　出力パケット キャプチャを保存するファイルを指定するには、[Save egress capture] をクリックします。

ASAv の vCPU 使用率

ASAv の vCPU 使用率では、データ パス、制御ポイント、および外部プロセスで使用されている vCPU の量を表示します。

vSphere で報告される vCPU の使用率には、この ASAv の使用率に加えて、次のものが含まれます。

- ASAv のアイドル時間
- ASAv VM に使用される %SYS オーバーヘッド
- vSwitch、vNIC および pNIC の間を移動するパケットのオーバーヘッド。このオーバーヘッドは非常に大きくなる場合があります。

CPU 使用率の例

報告された vCPU の使用率が大幅に異なる例を次に示します。

- ASAv のレポート：40%
- DP：35%
- 外部プロセス：5%
- vSphere のレポート：95%
- ASA（ASAv レポートとして）：40%
- ASA アイドル ポーリング：10%
- オーバーヘッド：45%

オーバーヘッドは、ハイパーバイザ機能の実行、および vSwitch を使用した NIC と vNIC の間のパケット転送に使用されています。

ASAv のためのオーバーヘッドとして、ESXi サーバが追加のコンピューティング リソースを使用する場合があるため、使用率は 100% を超えることがあります。

VMware の CPU 使用率のレポート

vSphere で [VM Performance] タブをクリックし、[Advanced] をクリックすると [Chart Options] ドロップダウンリストが表示されます。ここには VM の各ステート（%USER、%IDLE、%SYS など）の vCPU 使用率が表示されます。この情報は、VMware の観点から CPU リソースが使用されている場所を理解するのに役立ちます。

ESXi サーバのシェル（ホストへの接続に SSH を使用してシェルにアクセスします）では、esxtop を使用できます。Esxtop は Linux の **top** コマンドに似た操作性と外観を持ち、次の内容を含む vSphere のパフォーマンスに関する VM のステート情報を提供します。

- vCPU、メモリ、ネットワーク使用率の詳細

- 各 VM のステートごとの vCPU 使用率
- メモリ（実行中に「M」と入力）とネットワーク（実行中に「N」と入力）に加えて、統計情報と RX ドロップ数

ASAv のグラフと vCenter のグラフ

ASAv と vCenter の間で CPU 使用率の数字に違いがあります。

- vCenter のグラフの数値は常に ASAv の数値よりも大きくなります。
- vCenter ではこの値は「%CPU usage」と呼ばれ、ASAv ではこの値は「%CPU utilization」と呼ばれます。

用語「%CPU utilization」と「%CPU usage」は別のものを意味しています。

- CPU utilization は、物理 CPU の統計情報を提供します。
- CPU usage は CPU のハイパースレッディングに基づいた論理 CPU の統計情報を提供します。しかし、1 つの vCPU のみが使用されるため、ハイパースレッディングは動作しません。

vCenter は CPU % usage を次のように計算します。

アクティブに使用された仮想 CPU の量。使用可能な CPU の合計に対する割合として指定されます。

この計算は、ホストから見た CPU 使用率であり、ゲスト オペレーティング システムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率の計算は次のとおりです。

MHz 単位での使用率 / 仮想 CPU の数 x コアの周波数

使用率を MHz で比較すると、vCenter と ASAv の両方の数値は一致します。vCenter のグラフによると、MHz % CPU usage は次のように計算されます。

60/(2499 x 1 vCPU) = 2.4

PART 9

ロギング、SNMP、および Smart Call Home

ロギング

この章では、システム メッセージを記録して、トラブルシューティングに使用する方法について説明します。

ロギングについて

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央の syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。シスコ デバイスでは、これらのログ メッセージを UNIX スタイルの syslog サービスに送信できます。syslog サービスは、シンプル コンフィギュレーション ファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、保護された長期的な保存場所をログに提供します。ログは、ルーチン トラブルシューティングおよびインシデント処理の両方で役立ちます。

Cisco ASA システム ログにより、ASA のモニタリングおよびトラブルシューティングで必要な情報を得ることができます。ロギング機能を使用して、次の操作を実行できます。

- ログに記録する syslog メッセージを指定する。
- syslog メッセージの重大度をディセーブルにする、または変更する。
- syslog メッセージの送信場所を 1 つ以上指定する。送信先には、内部バッファ、1 つ以上の syslog サーバ、ASDM、SNMP 管理ステーション、指定された電子メール アドレス、Telnet および SSH セッションなどがあります。
- syslog メッセージを、メッセージの重大度やクラスなどのグループで設定および管理する。
- syslog の生成にレート制限を適用するかどうかを指定する。
- 内部ログ バッファがいっぱいになった場合に、その内容に対して実行する処理（バッファを上書きする、バッファの内容を FTP サーバに送信する、または内容を内部フラッシュ メモリに保存する）を指定する。
- 場所、重大度、クラス、またはカスタム メッセージ リストを基準にフィルタリングする。

マルチ コンテキスト モードでのロギング

それぞれのセキュリティ コンテキストには、独自のロギング コンフィギュレーションが含まれており、独自のメッセージが生成されます。システム コンテキストまたは管理コンテキストにログインし、別のコンテキストに変更した場合、セッションで表示されるメッセージは現在のコンテキストに関連するメッセージに限定されます。

システム実行スペースで生成されるフェールオーバー メッセージなどの syslog メッセージは、管理コンテキストで生成されるメッセージとともに管理コンテキストで表示できます。システム実行スペースでは、ロギングの設定やロギング情報の表示はできません。

ASA および ASASM は、それぞれのメッセージとともにコンテキスト名を含めるように設定できます。これによって、単一の syslog サーバに送信されるコンテキスト メッセージを区別できます。この機能は、管理コンテキストから送信されたメッセージとシステムから送信されたメッセージの判別にも役立ちます。これが可能なのは、送信元がシステム実行スペースであるメッセージでは**システム**のデバイス ID が使用され、管理コンテキストが送信元であるメッセージではデバイス ID として管理コンテキストの名前が使用されるからです。

syslog メッセージ分析

次に、さまざまな syslog メッセージを確認することで取得できる情報タイプの例を示します。

- ASA および ASASM のセキュリティ ポリシーで許可された接続。これらのメッセージは、セキュリティ ポリシーで開いたままのホールを発見するのに役立ちます。
- ASA および ASASM のセキュリティ ポリシーで拒否された接続。これらのメッセージは、セキュアな内部ネットワークに転送されているアクティビティのタイプを示します。
- ACE 拒否率ロギング機能を使用すると、使用している ASA または ASA サービス モジュールに対して発生している攻撃が表示されます。
- IDS アクティビティ メッセージには、発生した攻撃が示されます。
- ユーザ認証とコマンドの使用により、セキュリティ ポリシーの変更を監査証跡することができます。
- 帯域幅使用状況メッセージには、確立および切断された各接続のほか、使用された時間とトラフィック量が示されます。
- プロトコル使用状況メッセージには、各接続で使用されたプロトコルとポート番号が示されます。
- アドレス変換監査証跡メッセージは、確立または切断されている NAT または PAT 接続を記録します。この情報は、内部ネットワークから外部に送信される悪意のあるアクティビティのレポートを受信した場合に役立ちます。

syslog メッセージ形式

syslog メッセージは、パーセント記号（%）から始まり、次のような構造になっています。

```
%ASA Level Message_number: Message_text
```

次の表に、フィールドの説明を示します。

ASA	ASA および ASASM が生成するメッセージの syslog メッセージ ファシリティ コード。この値は常に ASA です。
レベル	1 ～ 7。レベルは、syslog メッセージに記述されている状況の重大度を示します。値が低いほどその状況の重大度は高くなります。
Message_number	syslog メッセージを特定する 6 桁の固有の番号。
Message_text	状況を説明するテキスト文字列。syslog メッセージのこの部分には、IP アドレス、ポート番号、またはユーザ名が含まれていることがあります。

重大度

表 40-1 に、syslog メッセージの重大度の一覧を示します。それぞれの重大度にカスタム カラーを割り当て、ASDM ログ ビューアで重大度を識別しやすくすることができます。syslog メッセージの色設定を行うには、[Tools] > [Preferences] > [Syslog] タブを選択するか、またはログ ビューア自体のツールバーで [Color Settings] をクリックします。

表 40-1　syslog メッセージの重大度

レベル番号	重大度	説明
0	**emergencies**	システムが使用不可能な状態。
1	**alert**	すぐに措置する必要があります。
2	**critical**	深刻な状況です。
3	**error**	エラー状態です。
4	**warning**	警告状態。
5	**notification**	正常ですが、注意を必要とする状況です。
6	**informational**	情報メッセージです。
7	**debugging**	デバッグ メッセージです。

（注） ASA および ASASM は、重大度 0（emergencies）の syslog メッセージを生成しません。このレベルは、UNIX の syslog 機能との互換性を保つために **logging** コマンドで使用できますが、ASA では使用されません。

メッセージ クラスと syslog ID の範囲

各クラスに関連付けられている syslog メッセージ クラスと syslog メッセージ ID の範囲のリストについては、syslog メッセージ ガイドを参照してください。

syslog メッセージのフィルタリング

生成される syslog メッセージは、特定の syslog メッセージだけが特定の出力先に送信されるようにフィルタリングできます。たとえば、ASA および ASASM を設定して、すべての syslog メッセージを 1 つの出力先に送信し、それらの syslog メッセージのサブセットを別の出力先に送信することができます。

具体的には、syslog メッセージが次の基準に従って出力先に転送されるように、ASA および ASASM を設定できます。

- syslog メッセージの ID 番号
- syslog メッセージの重大度
- syslog メッセージのクラス（ASA および ASASM の機能領域と同等）

これらの基準は、出力先を設定するときに指定可能なメッセージ リストを作成して、カスタマイズできます。あるいは、メッセージ リストとは無関係に、特定のメッセージ クラスを各タイプの出力先に送信するように ASA または ASASM を設定することもできます。

syslog メッセージのクラスは次の 2 つの方法で使用できます。

- **logging class** コマンドを使用して、syslog メッセージの 1 つのカテゴリ全体の出力先を指定する。
- **logging list** コマンドを使用して、メッセージ クラスを指定するメッセージ リストを作成する。

syslog メッセージのクラスは、タイプごとに syslog メッセージを分類する方法の 1 つであり、ASA および ASASM の機能に相当します。たとえば、vpnc クラスは VPN クライアントを意味します。

特定のクラスに属する syslog メッセージの ID 番号はすべて、最初の 3 桁が同じです。たとえば、611 で始まるすべての syslog メッセージ ID は、vpnc（VPN クライアント）クラスに関連付けられています。VPN クライアント機能に関連付けられている syslog メッセージの範囲は、611101 ～ 611323 です。

また、ほとんどの ISAKMP syslog メッセージには先頭に付加されたオブジェクトの共通セットが含まれているため、トンネルを識別するのに役立ちます。これらのオブジェクトは、使用可能なときに、syslog メッセージの説明テキストの前に付加されます。syslog メッセージの生成時にこのオブジェクトが存在しない場合、特定の ***heading = value*** の組み合わせは表示されません。

オブジェクトは次のように先頭に付加されます。

Group = ***groupname***, Username = ***user***, IP = ***IP_address***

Group はトンネル グループ、Username はローカル データベースまたは AAA サーバから取得したユーザ名、IP アドレスはリモート アクセス クライアントまたはレイヤ 2 ピアのパブリック IP アドレスです。

ログ ビューアのメッセージのソート

すべての ASDM ログ ビューア（Real-Time Log Viewer、Log Buffer Viewer、および Latest ASDM Syslog Events Viewer）でメッセージをソートできます。複数のカラムでテーブルをソートするには、ソートの基準とする、最初のカラムのヘッダーをクリックし、**Ctrl** キーを押したまま、同時にソート順に含める他のカラムのヘッダーをクリックします。時間順にメッセージをソートするには、日付と時刻のカラムを両方選択します。どちらか一方だけを選択した場合は、（時刻に関係なく）日付のみまたは（日付に関係なく）時刻のみでメッセージがソートされます。

Real-Time Log Viewer および Latest ASDM Syslog Events Viewer でメッセージをソートすると、記録された新しいメッセージは通常の表示位置となる一番上ではなく、ソートされた順序で表示されます。つまり、メッセージはその他のメッセージの中に混ざって表示されます。

カスタム メッセージ リスト

カスタム メッセージ リストを作成して、送信する syslog メッセージとその出力先を柔軟に制御できます。カスタム syslog メッセージ リストでは、重大度、メッセージ ID、syslog メッセージ ID の範囲、メッセージ クラスのいずれかまたはすべてを基準として、syslog メッセージのグループを指定できます。

たとえば、メッセージ リストを使用して次の操作を実行できます。

- 重大度が 1 および 2 の syslog メッセージを選択し、1 つ以上の電子メール アドレスに送信する。
- メッセージ クラス（「ha」など）に関連付けられたすべての syslog メッセージを選択し、内部バッファに保存する。

メッセージ リストには、メッセージを選択するための複数の基準を含めることができます。ただし、メッセージ選択基準の追加は、それぞれ個別のコマンド エントリで行う必要があります。重複したメッセージ選択基準を含むメッセージ リストが作成される可能性もあります。メッセージ リストの 2 つの基準によって同じメッセージが選択される場合、そのメッセージは一度だけログに記録されます。

クラスタリング

syslog メッセージは、クラスタリング環境でのアカウンティング、モニタリング、およびトラブルシューティングのための非常に重要なツールです。クラスタ内の各 ASA ユニット（最大 8 ユニットを使用できます）は、syslog メッセージを個別に生成します。特定の **logging** コマンドを使用すると、タイム スタンプおよびデバイス ID を含むヘッダー フィールドを制御できます。syslog サーバは、syslog ジェネレータを識別するためにデバイス ID を使用します。**logging device-id** コマンドを使用すると、同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。

（注） クラスタの装置から syslog メッセージをモニタするには、モニタする各装置に対して ASDM セッションを開く必要があります。

ロギングのガイドライン

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドライン

- syslog サーバでは、syslogd というサーバ プログラムを実行する必要があります。Windows（Windows 95 および Windows 98 を除く）では、オペレーティング システムの一部として syslog サーバを提供しています。Windows 95 および Windows 98 の場合は、別のベンダーから syslogd サーバを入手する必要があります。
- ASA または ASASM が生成したログを表示するには、ロギングの出力先を指定する必要があります。ロギングの出力先を指定せずにロギングをイネーブルにすると、ASA および ASASM はメッセージを生成しますが、それらのメッセージは後で表示できる場所に保存されません。各ロギングの出力先は個別に指定する必要があります。たとえば、出力先として複数の syslog サーバを指定する場合は、syslog サーバごとに [Syslog Server] ペインで個別のエントリを指定します。
- TCP での syslog の送信は、スタンバイ ASA ではサポートされていません。

- ASA は、シングル コンテキスト モードの **logging host** コマンドで 16 の syslog サーバのコンフィギュレーションをサポートします。マルチ コンテキスト モードでは、1 コンテキストあたり 4 つのサーバという制限があります。
- syslog サーバは、ASA と ASASM を介して到達可能である必要があります。そのインターフェイスを介して syslog サーバに到達できるインターフェイス上で、ICMP 到達不能メッセージを拒否し、同じサーバに対して syslog を送信するように、ASASM を設定する必要があります。すべての重大度に対してロギングがイネーブルであることを確認します。syslog サーバがクラッシュしないようにするため、syslog 313001、313004、および 313005 の生成を抑制します。
- アクセス リストのヒット数だけを照合するためにカスタム メッセージ リストを使用すると、ロギング重大度がデバッグ（レベル 7）のアクセス リストに対しては、アクセス リストのログは生成されません。**logging list** コマンドのロギング重大度のデフォルトは、6 に設定されています。このデフォルト動作は設計によるものです。アクセス リスト コンフィギュレーションのロギング重大度をデバッグに明示的に変更する場合は、ロギング コンフィギュレーション自体も変更する必要があります。

  ロギング重大度がデバッグに変更されたため、アクセス リストのヒットが含まれていない **show running-config logging** コマンドの出力例を次に示します。

  ```
  ciscoasa# show running-config logging
  logging enable
  logging timestamp
  logging list test message 106100
  logging buffered test
  ```

  次に、アクセス リスト ヒットを含む **show running-config logging** コマンドの出力例を示します。

  ```
  ciscoasa# show running-config logging
  logging enable
  logging timestamp
  logging buffered debugging
  ```

  この場合、アクセス リスト コンフィギュレーションは変更せず、アクセス リスト ヒット数が次の例のように表示されます。

  ```
  ciscoasa(config)# access-list global line 1 extended permit icmp any host 4.2.2.2 log
  debugging interval 1 (hitcnt=7) 0xf36b5386
  ciscoasa(config)# access-list global line 2 extended permit tcp host 10.1.1.2 any eq
  www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
  ciscoasa(config)# access-list global line 3 extended permit ip any any (hitcnt=543)
  0x25f9e609
  ```

ロギングの設定

ここでは、ロギングの設定方法について説明します。

ステップ 1　ロギングをイネーブルにします。「ロギングのイネーブル」（P.40-7）を参照してください。

ステップ 2　syslog メッセージの出力先を設定します。「出力先の設定」（P.40-7）を参照してください。

（注）　最小コンフィギュレーションは、ASA および ASASM で syslog メッセージを処理するために実行する操作および要件によって異なります。

ロギングのイネーブル

ロギングをイネーブルにするには、次の手順を実行します。

手順

ステップ 1　ASDM で、次のいずれかを選択します。

- [Home] > [Latest ASDM Syslog Messages] > [Enable Logging]
- [Configuration] > [Device Management] > [Logging] > [Logging Setup]
- [Monitoring] > [Real-Time Log Viewer] > [Enable Logging]
- [Monitoring] > [Log Buffer] > [Enable Logging]

ステップ 2　[Enable logging] チェックボックスをオンにして、ロギングをオンにします。

出力先の設定

トラブルシューティングおよびパフォーマンスのモニタリング用に syslog メッセージの使用状況を最適化するには、syslog メッセージの送信先（内部ログ バッファ、1 つまたは複数の外部 syslog サーバ、ASDM、SNMP 管理ステーション、コンソール ポート、指定した電子メール アドレス、または Telnet および SSH セッションなど）を 1 つまたは複数指定することをお勧めします。

外部 syslog サーバへの syslog メッセージの送信

外部 syslog サーバで利用可能なディスク領域に応じてメッセージをアーカイブし、その保存後、ロギング データを操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたり、ログからデータが抽出されてレポート用の別のファイルにその記録が保存されたり、あるいはサイト固有のスクリプトを使用して統計情報が追跡されたりした場合に、特別なアクションが実行されるように指定できます。

外部 syslog サーバに syslog メッセージを送信するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Logging Setup] を選択します。

ステップ 2　[Enable logging] チェックボックスをオンにして、ASA に対するロギングを有効にします。

ステップ 3　[Enable logging on the failover standby unit] チェックボックスをオンにして、スタンバイASAに対するロギングを有効にします（可能な場合）。

ステップ 4　[Send debug messages as syslogs] チェックボックスをオンにして、すべてのデバッグ トレース出力がシステム ログにリダイレクトされるようにします。このオプションがイネーブルになっている場合、syslog メッセージはコンソールには表示されません。そのため、デバッグ メッセージを表示するには、コンソールでロギングをイネーブルにし、デバッグ syslog メッセージ番号および重大度レベルの宛先としてコンソールを設定する必要があります。使用する syslog メッセージ番号は、**711001** です。この syslog メッセージに対するデフォルトの重大度レベルは、[Debugging] です。

ステップ 5　[Send syslogs in EMBLEM format] チェックボックスをオンにして、EMBLEM 形式をイネーブルにします。これにより、syslog サーバを除くロギングの宛先すべてに対して EMBLEM 形式が使用されます。

ステップ 6　ロギング バッファがイネーブルの場合、syslog メッセージを保存する内部ログ バッファのサイズを指定します。バッファの空き容量がなくなると、FTP サーバまたは内部フラッシュ メモリにログを保存していない限り、メッセージは上書きされます。デフォルトのバッファ サイズは 4096 バイトです。有効な範囲は 4096 ～ 1048576 です。

ステップ 7　バッファ内のデータが上書きされる前に、それらを FTP サーバに保存する場合は、[Save Buffer To FTP Server] チェックボックスをオンします。バッファ内のデータが上書きされるようにする場合は、このチェックボックスをオフにします。

ステップ 8　[Configure FTP Settings] をクリックして、FTP サーバを指定し、バッファ内のデータを保存する際に使用する FTP パラメータを設定します。

ステップ 9　[Save Buffer To Flash] チェックボックスをオンにして、上書きする前に内部フラッシュ メモリにバッファの内容を保存します。

（注）　このオプションは、ルーテッドまたはトランスペアレント シングル モードだけで使用できます。

ステップ 10　[Configure Flash Usage] をクリックし、ロギングに使用する内部フラッシュ メモリの最大容量、および最低限維持すべき空き容量を KB 単位で指定します。このオプションをイネーブルにすると、メッセージが格納されるデバイス ディスク上に、「syslog」という名前のディレクトリが作成されます。

（注）　このオプションは、単一ルーテッド モードまたはトランスペアレント モードでだけ使用できます。

ステップ 11　ASA または ASASM で表示するシステム ログのキュー サイズを指定します。

FTP の設定

ログ バッファの内容の保存に使用する FTP サーバのコンフィギュレーションを指定するには、次の手順を実行します。

手順

ステップ 1　[Enable FTP client] チェックボックスをオンにして、FTP クライアントのコンフィギュレーションをイネーブルにします。

ステップ 2　FTP サーバの IP アドレスを指定します。

ステップ 3　保存済みログ バッファ データの格納先となる FTP サーバ上のディレクトリ パスを指定します。

ステップ 4　FTP サーバにログインするためのユーザ名を指定します。

ステップ 5　FTP サーバへログインするためのユーザ名に関連付けられたパスワードを指定します。

ステップ 6　パスワードを確認し、[OK] をクリックします。

ロギングに使用するフラッシュ メモリの設定

ログ バッファの内容を内部フラッシュ メモリに保存する場合の制限事項を指定するには、次の手順を実行します。

手順

ステップ 1　ロギングに使用できる内部フラッシュ メモリの最大容量を指定します（KB 単位）。

ステップ 2　維持する内部フラッシュ メモリの容量を指定します（KB 単位）。内部フラッシュメモリがこの制限値に近づくと、新しいログが保存されなくなります。

ステップ 3　[OK] をクリックして、[Configure Logging Flash Usage] ダイアログボックスを閉じます。

syslog メッセージの設定

syslog メッセージを設定するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Syslog Setup] を選択します。

ステップ 2　ファイル メッセージのベースとして使用する syslog サーバのシステム ログ機能を選択します。デフォルトは LOCAL(4)20 です。これは、ほとんどの UNIX システムで必要となるコードです。ただし、ネットワーク デバイス間では 8 つのファシリティが共用されているため、システム ログではこの値を変更しなければならない場合があります。

ステップ 3　[Include timestamp in syslogs] チェックボックスをオンにして、送信される各 syslog メッセージに日付と時刻を追加します。

ステップ 4　[Syslog ID] テーブルに表示する情報を選択します。使用可能なオプションは、次のとおりです。

- [Syslog ID] テーブルにすべての syslog メッセージ ID を表示するように指定するには、[Show all syslog IDs] を選択します。
- [Syslog ID] テーブルに明示的にディセーブルにした syslog メッセージ ID だけを表示するように指定するには、[Show disabled syslog IDs] を選択します。
- [Syslog ID] テーブルにデフォルト値から変更された重大度を含む syslog メッセージ ID だけを表示するように指定するには、[Show syslog IDs with changed logging] を選択します。
- [Syslog ID] テーブルに重大度が変更された syslog メッセージ ID と、明示的にディセーブルにされた syslog メッセージ ID だけを表示するように指定するには、[Show syslog IDs that are disabled or with a changed logging level] を選択します。

ステップ 5　[Syslog ID Setup] テーブルには、その設定内容に基づいて、syslog メッセージのリストが表示されます。変更する個々のメッセージ ID またはメッセージ ID の範囲を選択します。選択したメッセージ ID は、ディセーブルにすることも、その重大度レベルを変更することもできます。リストから複数のメッセージ ID を選択する場合は、その範囲の先頭にあたる ID を選択し、Shift キーを押しながらその範囲の最後にあたる ID をクリックします。

ステップ 6　syslog メッセージにデバイス ID が含まれるよう設定する場合は、[Advanced] をクリックします。

syslog ID 設定の編集

syslog メッセージの設定を変更するには、次の手順を実行します。

（注）　[Syslog ID(s)] フィールドは表示専用です。この領域に表示される値は、[Syslog Setup] ペインにある [Syslog ID] テーブルで選択されたエントリにより決まります。

手順

ステップ 1　[Disable Message(s)] チェックボックスをオンにして、[Syslog ID(s)] リストに ID が表示されている syslog メッセージをディセーブルにします。

ステップ 2　[Syslog ID(s)] リストに表示される syslog メッセージ ID に送信するメッセージの重大度のロギング レベルを選択します。重大度レベルは次のように定義されています。

- Emergency（レベル 0、システムが使用不能）

  （注）　重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

ステップ 3　[OK] をクリックして [Edit Syslog ID Settings] ダイアログボックスを閉じます。

非 EMBLEM 形式の syslog メッセージへのデバイス ID の出力

デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるには、次の手順を実行します。

手順

ステップ 1　[Enable syslog device ID] チェックボックスをオンにして、非 EMBLEM 形式の syslog メッセージすべてにデバイス ID が含まれるように指定します。

ステップ 2　次のいずれかのオプションを選択して、どのようなデバイス ID を使用するかを指定します。

- ASA のホスト名
- インターフェイス IP アドレス

  選択した IP アドレスに対応するインターフェイス名を、ドロップダウン リストから選択します。

  クラスタリングを使用する場合は、[In an ASA cluster, always use master’s IP address for the selected interface] チェックボックスをオンにします。

- 文字列

  英数字のユーザ定義文字列を入力します。
- ASA クラスタ名

ステップ 3　[OK] をクリックして、[Advanced Syslog Configuration] ダイアログボックスを閉じます。

内部ログ バッファへの syslog メッセージの送信

一時的な保存場所となる内部ログ バッファに送信する syslog メッセージを指定する必要があります。新しいメッセージは、リストの最後に追加されます。バッファがいっぱいになったとき、つまりバッファ ラップが発生した場合は、ASA および ASASM がいっぱいになったバッファを別の場所に保存するように設定されていない限り、古いメッセージは生成される新しいメッセージによって上書きされます。

syslog メッセージを内部ログ バッファに送信するには、次の手順を実行します。

手順

ステップ 1　次のいずれかのオプションを選択して、内部ログ バッファに送信する syslog メッセージを指定します。

- [Home] > [Latest ASDM Syslog Messages] > [Configure ASDM Syslog Filters]
- [Configuration] > [Device Management] > [Logging] > [Logging Filters]

ステップ 2　[Monitoring] > [Logging] > [Log Buffer] > [View] の順に選択します。次に [Log Buffer] ペインで [File] > [Clear Internal Log Buffer] の順に選択して、内部ログ バッファを空にします。

ステップ 3　[Configuration] > [Device Management] > [Logging] > [Logging Setup] の順に選択して、内部ログ バッファのサイズを変更します。デフォルトのバッファ サイズは 4 KB です。

ASA および ASASM は、新しいメッセージを引き続き内部ログ バッファに保存し、いっぱいになったログ バッファの内容を内部フラッシュ メモリに保存します。バッファの内容を別の場所に保存するとき、ASA および ASASM は、次のタイムスタンプ形式を使用する名前でログ ファイルを作成します。

LOG-YYYY-MM-DD-HHMMSS.TXT

YYYY は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

ステップ 4　別の場所に新しいメッセージを保存するには、次のオプションから 1 つを選択します。

- 内部フラッシュ メモリに新しいメッセージを送信するには、[Flash] チェックボックスをオンにして、[Configure Flash Usage] をクリックします。[Configure Logging Flash Usage] ダイアログボックスが表示されます。
  - **a.** ロギングに使用するフラッシュ メモリの最大容量を KB で指定します。
  - **b.** ロギングをフラッシュ メモリに保持する最小空き領域量を KB で指定します。
  - **c.** [OK] をクリックして、このダイアログボックスを閉じます。
- FTP サーバに新しいメッセージを送信するには、[FTP Server] チェックボックスをオンにし、[Configure FTP Settings] をクリックします。[Configure FTP Settings] ダイアログボックスが表示されます。
  - **a.** [Enable FTP Client] チェックボックスをオンにします。

b. 表示されたフィールドに、FTP サーバ IP アドレス、パス、ユーザ名、パスワードを入力します。

c. パスワードを確認し、[OK] をクリックしてこのダイアログボックスを閉じます。

内部ログ バッファのフラッシュへの保存

内部ログ バッファをフラッシュ メモリに保存するには、次の手順を実行します。

手順

ステップ 1　[File] > [Save Internal Log Buffer to Flash] の順に選択します。

[Enter Log File Name] ダイアログボックスが表示されます。

ステップ 2　最初のオプションを選択し、LOG-YYYY-MM-DD-hhmmss.txt 形式のデフォルト ファイル名でログ バッファを保存します。

ステップ 3　2 番目のオプションを選択し、そのログ バッファのファイル名を指定します。

ステップ 4　ログ バッファのファイル名を入力して [OK] をクリックします。

ASDM Java Console による記録されたエントリの参照とコピー

ASDM Java コンソールを使用して、ASDM エラーのトラブルシューティングに役立つ、記録されたエントリをテキスト形式で表示およびコピーできます。

ASDM Java Console にアクセスするには、次の手順を実行します。

手順

ステップ 1　[Tools] > [ASDM Java Console] の順に選択します。

ステップ 2　コンソールで **m** と入力して、仮想マシンのメモリ統計情報を表示します。

ステップ 3　コンソールで **g** と入力して、ガベージ コレクションを実行します。

ステップ 4　Windows タスク マネージャを開き、**asdm_launcher.exe** ファイルをダブルクリックして、メモリ使用量を監視します。

（注）　メモリ割り当ての最大値は 256 MB です。

電子メール アドレスへの syslog メッセージの送信

syslog メッセージを電子メール アドレスに送信するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [E-Mail Setup] を選択します。

ステップ 2　電子メール メッセージとして送信される syslog メッセージの送信元アドレスとして使用する電子メール アドレスを指定します。

ステップ 3　[Add] をクリックして、指定した syslog メッセージの受信者の電子メール アドレスを入力します。

ステップ 4　その受信者に送信する syslog メッセージの重大度レベルを、ドロップダウン リストから選択します。宛先の電子メール アドレスに対して適用される syslog メッセージの重大度フィルタにより、指定された重大度レベル以上のメッセージが送信されます。[Logging Filters] ペインで指定されたグローバル フィルタも、各電子メール受信者に適用されます。

ステップ 5　[Edit] をクリックして、この受信者へ送信する syslog メッセージの現在の重大度を変更します。

ステップ 6　[OK] をクリックして、[Add E-mail Recipient] ダイアログボックスを閉じます。

電子メール受信者の追加または編集

電子メールの受信者および重大度を追加または編集するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [E-mail Setup] を選択します。

ステップ 2　[Add] または [Edit] をクリックして、[Add/Edit E-Mail Recipient] ダイアログボックスを表示します。

ステップ 3　宛先の電子メール アドレスを入力し、ドロップダウン リストから syslog 重大度を選択します。重大度レベルは次のように定義されています。

- Emergency（レベル 0、システムが使用不能）

  （注）　重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

（注）　宛先電子メール アドレスへのメッセージをフィルタリングする場合は、[Add/Edit E-Mail Recipient] ダイアログボックスで指定した重大度と、[Logging Filters] ペインですべての電子メール受信者に対して設定したグローバル フィルタの重大度のうち、上位にある方が使用されます。

ステップ 4　[OK] をクリックして、[Add/Edit E-Mail Recipient] ダイアログボックスを閉じます。

追加または修正されたエントリが [E-mail Recipients] ペインに表示されます。

ステップ 5　[Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

リモート SMTP サーバの設定

特定のイベントに対する電子メール アラートおよび通知の送信先となるリモート SMTP サーバを設定するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Setup] > [Logging] > [SMTP] を選択します。

ステップ 2　プライマリ SMTP サーバの IP アドレスを入力します。

ステップ 3　（オプション）スタンバイ SMTP サーバの IP アドレスを入力し、[Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

ASDM での syslog メッセージの表示

ステップ 1　[Home] > [Latest ASDM Syslog Messages] の順に選択して、ASDM に送信された最新の syslog メッセージを表示します。

ASA または ASASM は、ASDM への送信を待つ syslog メッセージのためにバッファ領域を確保し、メッセージが発生するとバッファに保存します。ASDM ログ バッファは、内部ログ バッファとは別のバッファです。ASDM のログ バッファがいっぱいになると、ASA または ASASM は最も古い syslog メッセージを削除し、新しい syslog メッセージ用にバッファ領域を確保します。最も古い syslog メッセージを削除して新しいメッセージ用に領域を確保する設定は、ASDM のデフォルト設定です。

ロギングの宛先へのメッセージ フィルタの適用

ロギングの宛先にメッセージ フィルタを適用するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Logging Filters] を選択します。

ステップ 2　フィルタを適用するロギングの宛先の名前を選択します。選択できるロギングの宛先は次のとおりです。

- ASDM
- コンソール ポート
- 電子メール
- 内部バッファ
- SNMP サーバ
- Syslog サーバ
- Telnet または SSH セッション

  このほか、2 番目のカラム [Syslogs From All Event Classes] と 3 番目のカラム [Syslogs From Specific Event Classes] でも選択操作を行います。2 番目のカラムでは、ロギングの宛先へのメッセージをフィルタリングする場合に使用する重大度やイベント クラスが表示されるほか、すべてのイベント クラスに対してロギングをディセーブルにするかを選択することもできます。3 番目のカラムには、選択したロギングの宛先へのメッセージをフィルタリングする場合に使用するイベント クラスが表示されます。

ステップ 3　[Edit] をクリックして、[Edit Logging Filters] ダイアログボックスを表示します。フィルタを適用、編集、またはディセーブルにする手順については、「ロギング フィルタの適用」（P.40-15）を参照してください。

ロギング フィルタの適用

フィルタを適用するには、次の手順を実行します。

手順

ステップ 1　重大度レベルに基づいて syslog メッセージのフィルタリングを行う場合は、[Filter on severity] オプションを選択します。

ステップ 2　イベント リストに基づいて syslog メッセージのフィルタリングを行う場合は、[Use event list] オプションを選択します。

ステップ 3　選択した宛先に対するロギングをすべてディセーブルにする場合は、[Disable logging from all event classes] オプションを選択します。

ステップ 4　[New] をクリックして、新しいイベント リストを追加します。イベント リストを新たに追加する手順については、「カスタム イベント リストの作成」（P.40-17）を参照してください。

ステップ 5　ドロップダウン リストからイベント クラスを選択します。使用できるイベント クラスは、使用しているデバイス モードによって異なります。

ステップ 6　ドロップダウン リストから、ロギング メッセージの重大度レベルを選択します。重大度レベルは次のとおりです。

- Emergency（レベル 0、システムが使用不能）

  （注）　重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）

- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

ステップ 7　[Add] をクリックして、イベント クラスおよび重大度レベルを追加し、[OK] をクリックします。

ダイアログボックスの上部には、フィルタに対して選択したロギングの宛先が表示されます。

メッセージ クラスと重大度フィルタの追加または編集

メッセージのフィルタリングに使用するメッセージ クラスおよび重大度レベルを追加または編集するには、次の手順を実行します。

手順

ステップ 1　ドロップダウン リストからイベント クラスを選択します。使用できるイベント クラスは、使用しているデバイス モードによって異なります。

ステップ 2　ドロップダウン リストから、ロギング メッセージの重大度レベルを選択します。重大度レベルは次のとおりです。

- Emergency（レベル 0、システムが使用不能）

（注）　重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

ステップ 3　選択が終了したら、[OK] をクリックします。

syslog メッセージ ID フィルタの追加または編集

syslog メッセージ ID フィルタを作成または編集する手順については、「syslog ID 設定の編集」（P.40-10）を参照してください。

コンソール ポートへの syslog メッセージの送信

syslog メッセージをコンソール ポートに送信するには、次の手順を実行します。

手順

ステップ 1　次のいずれかのオプションを選択します。

- [Home] > [Latest ASDM Syslog Messages] > [Configure ASDM Syslog Filters]
- [Configuration] > [Device Management] > [Logging] > [Logging Filters]

ステップ 2　[Logging Destination] カラムでコンソールを選択し、[Edit] をクリックします。

[Edit Logging Filters] ダイアログボックスが表示されます。

ステップ 3　すべてのイベント クラスまたは特定のイベント クラスのいずれかから syslog を選択して、コンソール ポートに送信する syslog メッセージを指定します。

Telnet または SSH セッションへの syslog メッセージの送信

syslog メッセージを Telnet または SSH セッションに送信するには、次の手順を実行します。

手順

ステップ 1　次のいずれかのオプションを選択します。

- [Home] > [Latest ASDM Syslog Messages] > [Configure ASDM Syslog Filters]
- [Configuration] > [Device Management] > [Logging] > [Logging Filters]

ステップ 2　[Logging Destination] カラムの [Telnet and SSH Sessions] を選択し、[Edit] をクリックします。

[Edit Logging Filters] ダイアログボックスが表示されます。

ステップ 3　すべてのイベント クラスまたは特定のイベント クラスのいずれかから syslog を選択して、Telnet または SSH セッションに送信する syslog メッセージを指定します。

ステップ 4　[Configuration] > [Device Management] > [Logging] > [Logging Setup] の順に選択して、現在のセッションのロギングだけをイネーブルにします。

ステップ 5　[Enable logging] チェックボックスをオンにし、[Apply] をクリックします。

カスタム イベント リストの作成

イベント リストの定義には、次の 3 つの基準を使用します。

- イベント クラス
- Severity
- メッセージ ID

特定のロギングの宛先（SNMP サーバなど）に送信するカスタム イベント リストを作成するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Event Lists] を選択します。

ステップ 2　[Add] をクリックして、[Add Event List] ダイアログボックスを表示します。

ステップ 3　イベント リストの名前を入力します。スペースは使用できません。

ステップ 4　[Add] をクリックして、[Add Class and SeverityFilter] ダイアログボックスを表示します。

ステップ 5　ドロップダウン リストからイベント クラスを選択します。使用できるイベント クラスは、使用しているデバイス モードによって異なります。

ステップ 6　ドロップダウン リストから重大度レベルを選択します。重大度レベルは次のとおりです。

- Emergency（レベル 0、システムが使用不能）

（注）　重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

ステップ 7　[OK] をクリックして、[Add Event List] ダイアログボックスを閉じます。

ステップ 8　[Add] をクリックして、[Add Syslog Message ID Filter] ダイアログボックスを表示します。

ステップ 9　フィルタに含める syslog メッセージ ID または syslog メッセージ ID の範囲（101001 ～ 199012 など）を入力します。

ステップ 10　[OK] をクリックして、[Add Event List] ダイアログボックスを閉じます。

目的のイベントがリストに表示されます。

syslog サーバに送信する EMBLEM 形式の syslog メッセージの生成

syslog サーバへの EMBLEM 形式の syslog メッセージを生成するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Syslog Server] を選択します。

ステップ 2　[Add] をクリックして、新しい syslog サーバを追加します。

[Add Syslog Server] ダイアログボックスが表示されます。

（注）　1 つのセキュリティ コンテキストに対して設定できる syslog サーバの数は最大で 4 です（合計で 16 まで）。

ステップ 3　syslog サーバがビジー状態の場合、ASA または ASASM でキューに入れることができるメッセージ数を指定します。値がゼロの場合は、キューに入れられるメッセージ数が無制限になります。

ステップ 4　[Allow user traffic to pass when TCP syslog server is down] チェックボックスをオンにして、いずれかの syslog サーバがダウンした場合にすべてのトラフィックを制限するかどうかを指定します。TCP を指定すると、ASA または ASASM は syslog サーバの障害を検出し、セキュリティ保護として ASA を経由する新しい接続をブロックします。UDP を指定すると、ASA または ASASM は、syslog サーバが動作しているかどうかに関係なく新しい接続を許可し続けます。有効なポート値は、どちらのプロトコルでも 1025 ～ 65535 です。デフォルトの UDP ポートは 514 です。デフォルトの TCP ポートは 1470 です。

（注）　TCP での syslog の送信は、スタンバイ ASA ではサポートされていません。

syslog サーバの設定の追加または編集

syslog サーバ設定を追加または編集するには、次の手順を実行します。

手順

ステップ 1　syslog サーバとの通信に使用するインターフェイスを、ドロップダウン リストから選択します。

ステップ 2　syslog サーバとの通信に使用する IP アドレスを入力します。

syslog サーバが ASA または ASASM との通信に使用するプロトコル（TCP または UDP）を選択します。UDP または TCP のいずれかを使用して syslog サーバにデータを送信するように ASA および ASASM を設定することはできますが、両方を使用するように設定することはできません。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。

ステップ 3　syslog サーバにおいて、ASA または ASASM との通信に使用されるポート番号を入力します。

ステップ 4　[Log messages in Cisco EMBLEM format (UDP only)] チェックボックスをオンにして、シスコの EMBLEM 形式でメッセージをログに記録するかどうかを指定します（プロトコルとして UDP が選択されている場合に限る）。

ステップ 5　[Enable secure logging using SSL/TLS (TCP only)] チェックボックスをオンにして、syslog サーバへの接続が SSL/TLS over TCP の使用により保護され、syslog メッセージの内容が暗号化されるよう指定します。

ステップ 6　[OK] をクリックして設定を完了します。

他の出力先への EMBLEM 形式の syslog メッセージの生成

他の出力先への EMBLEM 形式の syslog メッセージを生成するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Logging Setup] を選択します。

ステップ 2　[Send syslogs in EMBLEM format] チェックボックスをオンにします。

ログを記録可能な内部フラッシュ メモリの容量の変更

ログの記録で使用可能な内部フラッシュ メモリの容量を変更するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Logging Setup] を選択します。

ステップ 2　[Enable Logging] チェックボックスをオンにします。

ステップ 3　[Logging to Internal Buffer] 領域の [Save Buffer to Flash] チェックボックスをオンにします。

ステップ 4　[Configure Flash Usage] をクリックします。

[Configure Logging Flash Usage] ダイアログボックスが表示されます。

ステップ 5　ログインに使用できるフラッシュ メモリの最大容量を KB で入力します。

デフォルトでは、ASA は、内部フラッシュ メモリの最大 1 MB をログ データに使用できます。ASA および ASASM でログ データを保存するために必要な内部フラッシュ メモリの最小空き容量は、3 MB です。内部フラッシュ メモリの空き容量が、内部フラッシュ メモリに保存するログ ファイルのために設定された最小限の容量を下回る場合、ASA または ASASM は最も古いログ ファイルを削除し、その新しいログ ファイルが保存されたとしても最小限の容量が確保されるようにします。削除するファイルがなかったり、古いファイルすべてを削除しても最小限の容量を確保できなかったりする場合、ASA または ASASM はその新しいログ ファイルを保存できません。

ステップ 6　フラッシュ メモリにロギングするために維持する空き領域の最小容量を KB で入力します。

ステップ 7　[OK] をクリックして、[Configure Logging Flash Usage] ダイアログボックスを閉じます。

ロギング キューの設定

ロギング キューを設定するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Logging Setup] を選択します。

ステップ 2　[Enable logging] チェックボックスをオンにします。

ステップ 3　設定された出力先に送信されるまでの間、ASA および ASASM がそのキューに保持できる syslog メッセージの数を入力します。

ASA および ASASM のメモリ内には、設定された出力先への送信を待機している syslog メッセージをバッファするために割り当てられる、固定された数のブロックがあります。必要なブロックの数は、syslog メッセージ キューの長さと、指定した syslog サーバの数によって異なります。デフォルトのキューのサイズは 512 syslog メッセージです。キューのサイズは、使用可能なブロック メモリのサイズが上限です。有効値は 0 ～ 8192 メッセージです。値はプラットフォームによって異なります。ロギング キューをゼロに設定した場合、そのキューは設定可能な最大サイズ（8192 メッセージ）になります。

ステップ 4　[Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

指定した出力先へのクラス内のすべての syslog メッセージの送信

クラス内のすべての syslog メッセージを指定した出力先に送信するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Logging Filters] を選択します。

ステップ 2　指定した出力先の設定をオーバーライドするには、変更する出力先を選択してから [Edit] をクリックします。

[Edit Logging Filters] ダイアログボックスが表示されます。

ステップ 3　[Syslogs from All Event Classes] または [Syslogs from Specific Event Classes] 領域のいずれかで設定を変更し、[OK] をクリックしてこのダイアログボックスを閉じます。

たとえば、重大度 7 のメッセージが内部ログ バッファに送信されるように指定し、重大度 3 の ha クラスのメッセージが内部ログ バッファに送信されるように指定すると、後のコンフィギュレーションが優先されます。

1 つのクラスが複数の出力先に送信されるように指定する場合は、出力先ごとに異なるフィルタリング オプションを選択します。

セキュア ロギングのイネーブル

セキュア ロギングをイネーブルにするには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Syslog Server] を選択します。

ステップ 2　セキュア ロギングをイネーブルにする syslog サーバを選択し、[Edit] をクリックします。

[Edit Syslog Server] ダイアログボックスが表示されます。

ステップ 3　[TCP] オプション ボタンをクリックします。

（注）　セキュア ロギングでは UDP をサポートしていないため、このプロトコルを使用しようとするとエラーが発生します。

ステップ 4　[Enable secure syslog with SSL/TLS] チェックボックスをオンにして、[OK] をクリックします。

非 EMBLEM 形式の syslog メッセージへのデバイス ID の出力

デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Syslog Setup] > [Advanced] > [Advanced Syslog Configuration] の順に選択します。

ステップ 2　[Enable syslog device ID] チェックボックスをオンにします。

ステップ 3　[Device ID] 領域で、[Hostname]、[Interface IP Address] または [String] オプション ボタンをクリックします。

- [Interface IP Address] オプションを選択した場合は、ドロップダウン リストで正しいインターフェイスが選択されていることを確認します。
- [String] オプションを選択した場合は、[User-Defined ID] フィールドにデバイス ID を入力します。文字列の長さは、最大で 16 文字です。

（注）　イネーブルにすると、EMBLEM 形式の syslog メッセージや SNMP トラップにデバイス ID は表示されません。

ステップ 4　[OK] をクリックして、[Advanced Syslog Configuration] ダイアログボックスを閉じます。

syslog メッセージへの日付と時刻の出力

syslog メッセージに日付と時刻を含めるには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Syslog Setup] を選択します。

ステップ 2　[Syslog ID Setup] 領域で [Include timestamp in syslogs] チェックボックスをオンにします。

ステップ 3　[Apply] をクリックして変更内容を保存します。

syslog メッセージのディセーブル

指定した syslog メッセージをディセーブルにするには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Syslog Setup] を選択します。

ステップ 2　テーブルからディセーブルにする syslog を選択して、[Edit] をクリックします。

[Edit Syslog ID Settings] ダイアログボックスが表示されます。

ステップ 3　[Disable messages] チェックボックスをオンにし、[OK] をクリックします。

syslog メッセージの重大度の変更

syslog メッセージの重大度を変更するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Syslog Setup] を選択します。

ステップ 2　重大度を変更する syslog をテーブルから選択して、[Edit] をクリックします。

[Edit Syslog ID Settings] ダイアログボックスが表示されます。

ステップ 3　適切な重大度を [Logging Level] ドロップダウン リストから選択し、[OK] をクリックします。

syslog メッセージの生成レートの制限

syslog メッセージの生成レートを制限するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Rate Limit] を選択します。

ステップ 2　レート制限を割り当てるロギング レベル（メッセージの重大度）を選択します。重大度レベルは次のように定義されています。

説明	重大度
Emergency	0：システムが使用不能
Alert	1：即時対処が必要
Critical	2：クリティカル条件
Error	3：エラー条件
Warning	4：警告条件
Notification	5：通常の状態だが、重要な状態
Informational	6：情報メッセージだけ
Debugging	7：デバッグ メッセージだけ

ステップ 3　送信されるメッセージの数が [No of Messages] フィールドに表示されます。また、選択したロギング レベルで送信できるメッセージ数を制限する際の基準となる時間間隔（秒単位）が [Interval (Seconds)] フィールドに表示されます。テーブルからロギング レベルを選択し、[Edit] をクリックして [Edit Rate Limit for Syslog Logging Level] ダイアログボックスを表示します。

ステップ 4　以降の手順については、「個々の syslog メッセージに対するレート制限の割り当てまたは変更」（P.40-24）を参照してください。

個々の syslog メッセージに対するレート制限の割り当てまたは変更

個々の syslog メッセージにレート制限を割り当てる、またはメッセージごとにレート制限を変更するには、次の手順を実行します。

手順

ステップ 1　特定の syslog メッセージにレート制限を割り当てる場合は、[Add] をクリックして、[Add Rate Limit for Syslog Message] ダイアログボックスを表示します。

ステップ 2　以降の手順については、「syslog メッセージに対するレート制限の追加または編集」（P.40-24）を参照してください。

ステップ 3　特定の syslog メッセージに対するレート制限を変更する場合は、[Edit] をクリックして、[Edit Rate Limit for Syslog Message] ダイアログボックスを表示します。

ステップ 4　以降の手順については、「syslog 重大度に対するレート制限の編集」（P.40-24）を参照してください。

syslog メッセージに対するレート制限の追加または編集

特定の syslog メッセージに対するレート制限を追加または変更するには、次の手順を実行します。

手順

ステップ 1　特定の syslog メッセージに対するレート制限を追加する場合は、[Add] をクリックして、[Add Rate Limit for Syslog Message] ダイアログボックスを表示します。特定の syslog メッセージに対するレート制限を変更する場合は、[Edit] をクリックして、[Edit Rate Limit for Syslog Message] ダイアログボックスを表示します。

ステップ 2　レートを制限する syslog メッセージの ID を入力します。

ステップ 3　指定した時間内に送信できるメッセージの最大数を入力します。

ステップ 4　指定したメッセージのレートを制限する際の基準となる時間間隔を秒単位で入力し、[OK] をクリックします。

（注）　メッセージ数を制限なしにする場合は、[Number of Messages] フィールドおよび [Time Interval] フィールドをともにブランクのままにします。

syslog 重大度に対するレート制限の編集

指定した syslog 重大度のレート制限を変更するには、次の手順を実行します。

手順

ステップ 1　指定した重大度で送信可能なメッセージの最大数を指定します。

ステップ 2　指定した重大度のメッセージに対するレートを制限する基準となる時間間隔を秒単位で入力し、[OK] をクリックします。

選択したメッセージ重大度が表示されます。

（注）　メッセージ数を制限なしにする場合は、[Number of Messages] フィールドおよび [Time Interval] フィールドをともにブランクのままにします。

ログのモニタリング

ロギング ステータスの監視については、次の画面を参照してください。

- [Monitoring] > [Logging] > [Log Buffer] > [View]
- [Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]
- [Tools] > [Command Line Interface]

  非対話形式の各種コマンドを発行して結果を表示できます。

ログ ビューアを使用した syslog メッセージのフィルタリング

Real-Time Log Viewer および Log Buffer Viewer の任意のカラムに対応する 1 つ以上の値に基づいて、syslog メッセージをフィルタリングできます。

ログ ビューアのいずれかを使用して syslog メッセージをフィルタリングするには、次の手順を実行します。

手順

ステップ 1　次のいずれかのオプションを選択します。

- [Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]
- [Monitoring] > [Logging] > [Log Buffer] > [View]

ステップ 2　[Real-Time Log Viewer] または [Log Buffer Viewer] ダイアログボックスのいずれかで、ツールバーの [Build Filter] をクリックします。

ステップ 3　[Build Filter] ダイアログボックスで、syslog メッセージに適用するフィルタリング基準を指定します。

a.　[Date and Time] 領域で、リアルタイム、特定時刻、時間範囲の 3 つのオプションから 1 つを選択します。特定時刻を選択した場合は、数値を入力してドロップダウン リストから時または分を選択し、時刻を指定します。時間範囲を選択した場合、[Start Time] フィールドのドロップダウン矢印をクリックすると、カレンダーが表示されます。ドロップダウン リストから開始日と開始時刻を選択し、[OK] をクリックします。[End Time] フィールドのドロップダウン矢印をクリックすると、カレンダーが表示されます。ドロップダウン リストから終了日と終了時刻を選択し、[OK] をクリックします。

b. [Severity] フィールドに有効な重大度を入力します。または、[Severity] フィールドの右側で [Edit] アイコンをクリックします。フィルタリングする重大度をリストでクリックします。重大度 1 ～ 7 を含めるには、[All] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Severity] フィールドの右側にある [Info] アイコンをクリックします。

c. [Syslog ID] フィールドに有効な syslog ID を入力します。または、[Syslog ID] フィールドの右側の [Edit] アイコンをクリックします。ドロップダウン リストからフィルタ対象の条件を選択し、[Add] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Syslog ID] フィールドの右側にある [Info] アイコンをクリックします。

d. [Source IP Address] フィールドに有効な送信元 IP アドレスを入力するか、または [Source IP Address] フィールドの右側で [Edit] アイコンをクリックします。単一の IP アドレスまたは IP アドレスの特定の範囲を選択し、[Add] をクリックします。特定の IP アドレスまたは IP アドレスの範囲を除外するには、[Do not include (exclude) this address or range] チェックボックスをオンにして、[OK] をクリックし、[Build Filter] ダイアログボックスにこれらの設定を表示します。使用する正しい入力形式に関する詳細な情報については、[Source IP Address] フィールドの右側にある [Info] アイコンをクリックします。

e. [Source Port] フィールドに有効な送信元ポートを入力するか、または [Source Port] フィールドの右側の [Edit] アイコンをクリックします。ドロップダウン リストからフィルタ対象の条件を選択し、[Add] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Source Port] フィールドの右側にある [Info] アイコンをクリックします。

f. [Destination IP Address] フィールドに有効な宛先 IP アドレスを入力するか、または [Destination IP Address] フィールドの右側で [Edit] アイコンをクリックします。単一の IP アドレスまたは IP アドレスの特定の範囲を選択し、[Add] をクリックします。特定の IP アドレスまたは IP アドレスの範囲を除外するには、[Do not include (exclude) this address or range] チェックボックスをオンにします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Destination IP Address] フィールドの右側にある [Info] アイコンをクリックします。

g. [Destination Port] フィールドに有効な宛先ポートを入力するか、または [Destination Port] フィールドの右側の [Edit] アイコンをクリックします。ドロップダウン リストからフィルタ対象の条件を選択し、[Add] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Destination Port] フィールドの右側にある [Info] アイコンをクリックします。

h. [Description] フィールドにフィルタリング テキストを入力します。このテキストには、正規表現を含む、1 つ以上の文字からなる任意の文字列を指定できます。ただし、セミコロンは有効な文字ではありません。また、この設定では大文字と小文字が区別されます。複数のエントリを指定する場合は、カンマで区切ります。

i. [OK] をクリックして、指定したフィルタリング設定をログ ビューアの [Filter By] ドロップダウン リストに追加します。フィルタ文字列は特定の形式に従います。FILTER: プレフィックスは、[Filter By] ドロップダウン リストに表示されるすべてのカスタム フィルタを示します。このフィールドにはランダムなテキストを入力することもできます。

次の表に、使用される形式の例を示します。

Build Filter の例	フィルタ文字列形式
Source IP = 192.168.1.1 または 0.0.0.0 Source Port = 67	FILTER: srcIP=192.168.1.1,0.0.0.0;srcPort=67;

Severity = Informational Destination IP = 1.1.1.1 ～ 1.1.1.10	FILTER: sev=6;dstIP=1.1.1.1-1.1.1.10;
725001 ～ 725003 の範囲外の syslog ID	FILTER: sysID=!725001-725003;
Source IP = 1.1.1.1 Description = Built outbound	FILTER: srcIP=1.1.1.1;descr=Built outbound

ステップ 4　[Filter By] ドロップダウン リストの設定の 1 つを選択し、ツールバーの [Filter] をクリックして、syslog メッセージをフィルタリングします。この設定は、これ以降のすべての syslog メッセージにも適用されます。すべてのフィルタをクリアするには、ツールバーにある [Show All] をクリックします。

（注）　[Build Filter] ダイアログボックスを使用して指定したフィルタは保存できません。これらのフィルタは、そのフィルタが作成された ASDM セッションのみで有効です。

フィルタリング設定の編集

[Build Filter] ダイアログボックスを使用して作成したフィルタリング設定を編集するには、次の手順を実行します。

手順

ステップ 1　次のいずれかのオプションを選択します。

- [Filter By] ドロップダウン リストで変更を入力して、フィルタを直接修正します。
- [Filter By] ドロップダウン リストでフィルタを選択し、[Build Filter] をクリックして [Build Filter] ダイアログボックスを表示します。[Clear Filter] をクリックして、現在のフィルタ設定を削除し、新しい値を入力します。それ以外の場合は、表示された設定を変更して [OK] をクリックします。

  （注）　これらのフィルタリング設定は、[Build Filter] ダイアログボックスで定義されたフィルタのみに適用されます。

- ツールバーの [Show All] をクリックすると、フィルタリングが停止し、すべての syslog メッセージが表示されます。

ログ ビューアを使用した特定のコマンドの発行

ログ ビューアのいずれかを使用して、**ping**、**traceroute**、**whois**、および **dns lookup** のコマンドを発行できます。

これらのコマンドのいずれかを実行するには、次の手順を実行します。

手順

ステップ 1　次のいずれかのオプションを選択します。

- [Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]
- [Monitoring Logging] > [Log Buffer] > [View]

ステップ 2　[Real-Time Log Viewer] または [Log Buffer] ペインから [Tools] をクリックし、実行するコマンドを選択します。または、表示された特定の syslog メッセージを右クリックしてコンテキスト メニューを表示し、実行するコマンドを選択します。

[Entering command] ダイアログボックスが表示され、選択したコマンドが自動的にドロップダウン リストに表示されます。

ステップ 3　選択した syslog メッセージの送信元 IP アドレスまたは宛先 IP アドレスのいずれかを [Address] フィールドに入力し、[Go] をクリックします。

指定した領域にコマンド出力が表示されます。

ステップ 4　[Clear] をクリックして出力を削除し、実行する別のコマンドをドロップダウン リストから選択します。必要に応じてステップ 3 を繰り返します。完了したら [Close] をクリックします。

ロギングの履歴

表 40-2　ロギングの履歴

機能名	プラットフォーム リリース	説明
ロギング	7.0(1)	さまざまな出力先を通して ASA ネットワーク ロギング情報を提供します。ログ ファイルを表示して保存するオプションも含まれています。 次の画面が導入されました。[Configuration] > [Device Management] > [Logging] > [Logging Setup]。
レート制限	7.0(4)	syslog メッセージが生成されるレートを制限します。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Rate Limit]。
ロギング リスト	7.2(1)	さまざまな基準（ロギング レベル、イベント クラス、およびメッセージ ID）でメッセージを指定するために他のコマンドで使用されるロギング リストを作成します。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Event Lists]。

表 40-2　　ロギングの履歴 （続き）

機能名	プラットフォーム リリース	説明
セキュア ロギング	8.0(2)	リモート ロギング ホストへの接続に SSL/TLS を使用するように指定します。このオプションは、選択されたプロトコルが TCP の場合にだけ有効です。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Syslog Server]。
ロギング クラス	8.0(4)、8.1(1)	ロギング メッセージの ipaa イベント クラスに対するサポートが追加されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Logging Filters]。
ロギング クラスと保存されたロギング バッファ	8.2(1)	ロギング メッセージの dap イベント クラスに対するサポートが追加されました。 保存されたロギング バッファ（ASDM、内部、FTP、およびフラッシュ）をクリアする追加サポート。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Logging Setup]。
パスワードの暗号化	8.3(1)	パスワードの暗号化に対するサポートが追加されました。
ログ ビューア	8.3(1)	送信元 IP アドレスおよび宛先 IP アドレスがログ ビューアに追加されました。
拡張ロギングと接続ブロック	8.3(2)	TCP を使用するように syslog サーバを設定したときに syslog サーバを利用できない場合、ASA はサーバが再び利用可能になるまで syslog メッセージを生成する新しい接続をブロックします（VPN、ファイアウォール、カットスルー プロキシの接続など）。この機能は拡張され、ASA のロギング キューがいっぱいの場合にも新しい接続をブロックするようになりました。ロギング キューがクリアされると接続が再開されます。 この機能は、Common Criteria EAL4+ への準拠のために追加されました。必要でない限り、syslog メッセージを送受信できない場合でも接続を許可することを推奨します。接続を許可するには、[Configuration] > [Device Management] > [Logging] > [Syslog Servers] ペインで [Allow user traffic to pass when TCP syslog server is down] チェックボックスをオンにします。 414005、414006、414007、414008 の各 syslog メッセージが導入されました。 変更された ASDM 画面はありません。

表 40-2　　ロギングの履歴 （続き）

機能名	プラットフォーム リリース	説明
syslog メッセージのフィルタリングとソート	8.4(1)	次のサポートが追加されました。 • さまざまなカラムに対応する複数のテキスト文字列に基づく syslog メッセージ フィルタリング。 • カスタム フィルタの作成。 • メッセージのカラムによるソート。詳細については、ASDM 設定ガイドを参照してください。 次の画面が変更されました。 [Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]。 [Monitoring] > [Logging] > [Log Buffer Viewer] > [View]。 この機能は、すべての ASA バージョンと相互運用性があります。
クラスタリング	9.0(1)	ASA 5580 および 5585-X でのクラスタリング環境における syslog メッセージ生成のサポートが追加されました。 次の画面が変更されました。[Configuration] > [Logging] > [Syslog Setup] > [Advanced] > [Advanced Syslog Configuration]。

SNMP

この章では、Cisco ASA をモニタするように簡易ネットワーク管理プロトコル（SNMP）を設定する方法について説明します。

SNMP について

SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルで、TCP/IP プロトコル スイートの一部です。ASA、ASAv、および ASASM は SNMP バージョン 1、2c、および 3 を使用したネットワーク モニタリングに対するサポートを提供し、3 つのバージョンの同時使用をサポートします。ASA インターフェイス上で実行される SNMP エージェントは、HP OpenView などのネットワーク管理システム（NMS）を介して ASA および ASASM をモニタできるようにします。ASA、ASAv、および ASASM は GET 要求の発行を通じた SNMP 読み取り専用アクセスをサポートします。SNMP 書き込みアクセスは許可されていないため、SNMP を使用して変更することはできません。さらに、SNMP SET 要求はサポートされていません。

管理情報ベース（MIB）への特定のイベントの管理ステーションに対する管理対象デバイスからの要求外のメッセージ（イベント通知）であるトラップを送信するように ASA、ASAv、および ASASM を設定したり、NMS を使用して ASA の MIB をブラウズしたりできます。MIB は定義の集合で、ASA、ASAv、および ASASM は各定義の値のデータベースを保持します。MIB をブラウズすることは、NMS から MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して値を決定することを意味します。

ASA、ASAv、および ASASM には SNMP エージェントが含まれています。SNMP エージェントは、通知を必要とすることが事前に定義されているイベント（たとえば、ネットワーク内のリンクがアップ状態またはダウン状態になる）が発生すると、指定した管理ステーションに通知します。このエージェントが送信する通知には、管理ステーションに対して自身を識別する SNMP OID が含まれています。ASA、ASAv、または ASASM SNMP エージェントは、管理ステーションが情報を要求した場合にも応答します。

SNMP の用語

表 41-1 に、SNMP で頻繁に使用される用語を示します。

表 41-1　SNMP の用語

用語	説明
エージェント	ASA で稼働する SNMP サーバ。SNMP エージェントは、次の機能を搭載しています。 • ネットワーク管理ステーションからの情報の要求およびアクションに応答する。 • 管理情報ベース（SNMP マネージャが表示または変更できるオブジェクトの集合）へのアクセスを制御する。 • SET 操作を許可しない。
ブラウジング	デバイス上の SNMP エージェントから必要な情報をポーリングすることによって、ネットワーク管理ステーションからデバイスのヘルスをモニタすること。このアクティビティには、ネットワーク管理ステーションから MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して、値を決定することが含まれる場合があります。
管理情報ベース（MIB）	パケット、接続、バッファ、フェールオーバーなどに関する情報を収集するための標準化されたデータ構造。MIB は、大部分のネットワーク デバイスで使用される製品、プロトコル、およびハードウェア標準によって定義されます。SNMP ネットワーク管理ステーションは、MIB をブラウズし、特定のデータまたはイベントの発生時にこれらを要求できます。
ネットワーク管理ステーション（NMS）	SNMP イベントのモニタや ASA、ASAv、ASASM などのデバイスの管理用に設定されている、PC またはワークステーション。
オブジェクト ID（OID）	NMS に対してデバイスを識別し、モニタおよび表示される情報の源をユーザに示すシステム。
トラップ	SNMP エージェントから NMS へのメッセージを生成する、事前定義済みのイベント。イベントには、リンクアップ、リンクダウン、コールドスタート、ウォームスタート、認証、syslog メッセージなどのアラーム状態が含まれます。

SNMP バージョン 3 の概要

SNMP バージョン 3 は SNMP バージョン 1 またはバージョン 2c では使用できなかったセキュリティ拡張機能を提供します。SNMP バージョン 1 とバージョン 2c は SNMP サーバと SNMP エージェント間でデータをクリア テキストで転送します。SNMP バージョン 3 は認証とプライバシー オプションを追加してプロトコル オペレーションをセキュリティ保護します。また、このバージョンはユーザベース セキュリティ モデル（USM）とビューベース アクセス コントロール モデル（VACM）を通して SNMP エージェントと MIB オブジェクトへのアクセスをコントロールします。ASA および ASASM は、SNMP グループとユーザの作成、およびセキュアな SNMP 通信の転送の認証と暗号化をイネーブルにするために必要なホストの作成もサポートします。

セキュリティ モデル

設定上の目的のために、認証とプライバシーのオプションはセキュリティ モデルにまとめられます。セキュリティ モデルはユーザとグループに適用され、次の 3 つのタイプに分けられます。

- NoAuthPriv：認証もプライバシーもありません。メッセージにどのようなセキュリティも適用されないことを意味します。

- AuthNoPriv：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
- AuthPriv：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

SNMP グループ

SNMP グループはユーザを追加できるアクセス コントロール ポリシーです。各 SNMP グループはセキュリティ モデルを使用して設定され、SNMP ビューに関連付けられます。SNMP グループ内のユーザは、SNMP グループのセキュリティ モデルに一致する必要があります。これらのパラメータは、SNMP グループ内のユーザがどのタイプの認証とプライバシーを使用するかを指定します。各 SNMP グループ名とセキュリティ モデルのペアは固有である必要があります。

SNMP ユーザ

SNMP ユーザは、指定されたユーザ名、ユーザが属するグループ、認証パスワード、暗号化パスワード、および使用する認証アルゴリズムと暗号化アルゴリズムを持ちます。認証アルゴリズムのオプションは MD5 と SHA です。暗号化アルゴリズムのオプションは DES、3DES、および AES（128、192、および 256 バージョンで使用可能）です。ユーザを作成した場合は、それを SNMP グループに関連付ける必要があります。その後、そのユーザはグループのセキュリティ モデルを継承します。

SNMP ホスト

SNMP ホストは SNMP 通知とトラップの送信先となる IP アドレスです。トラップは設定されたユーザだけに送信されるため、ターゲット IP アドレスとともに SNMP バージョン 3 のホストを設定するには、ユーザ名を設定する必要があります。SNMP ターゲット IP アドレスとターゲット パラメータ名は ASA および ASA サービス モジュールで固有である必要があります。各 SNMP ホストはそれぞれに関連付けられているユーザ名を 1 つだけ持つことができます。SNMP トラップを受信するには、SNMP NMS を設定し、NMS のユーザ クレデンシャルが ASA および ASASM のクレデンシャルと一致するように設定してください。

ASA、ASA サービス モジュール、および Cisco IOS ソフトウェア間の実装の差異

ASA および ASASM での SNMP バージョン 3 の実装は、Cisco IOS ソフトウェアでの SNMP バージョン 3 の実装とは次のように異なります。

- ローカル エンジン ID とリモート エンジン ID は設定できません。ローカル エンジン ID は、ASA または ASASM が起動されたとき、あるいはコンテキストが作成されたときに生成されます。
- ビューベースのアクセス コントロールに対するサポートはないため、結果として MIB のブラウジングは無制限になります。
- サポートは、USM、VACM、FRAMEWORK、および TARGET という MIB に制限されます。
- 正しいセキュリティ モデルを使用してユーザとグループを作成する必要があります。
- 正しい順序でユーザ、グループ、およびホストを削除する必要があります。
- **snmp-server host** コマンドを使用すると、着信 SNMP トラフィックを許可する ASA、ASAv、または ASASM のルールが作成されます。

SNMP syslog メッセージ

SNMP では、212*nnn* という番号が付いた詳細な syslog メッセージが生成されます。syslog メッセージは、SNMP 要求のステータス、SNMP トラップ、SNMP チャネル、ASA または ASASM から指定インターフェイスの指定ホストに対する SNMP 応答を表示します。

syslog メッセージの詳細については、syslog メッセージ ガイドを参照してください。

（注）　SNMP syslog メッセージがレート制限（毎秒約 4000）を超えた場合、SNMP ポーリングは失敗します。

アプリケーション サービスとサードパーティ ツール

SNMP サポートについては、次の URL を参照してください。

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

SNMP バージョン 3 MIB をウォークするためのサードパーティ ツールの使い方については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

SNMP のガイドライン

フェールオーバーのガイドライン

各 ASA、ASAv、または ASASM の SNMP クライアントはそれぞれのピアとエンジン データを共有します。エンジン データには、SNMP-FRAMEWORK-MIB の engineID、engineBoots、および engineTime オブジェクトが含まれます。エンジン データは flash:/snmp/*contextname* にバイナリ ファイルとして書き込まれます。

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドライン

- SNMP トラップを受信するか MIB をブラウズするには、CiscoWorks for Windows か別の SNMP MIB-II 互換ブラウザを持っている必要があります。
- ビューベースのアクセス コントロールはサポートされませんが、ブラウジングに VACM MIB を使用してデフォルトのビュー設定を決定できます。
- ENTITY-MIB は管理外コンテキストでは使用できません。代わりに IF-MIB を使用して、管理外コンテキストでクエリーを実行します。
- AIP SSM または AIP SSC では、SNMP バージョン 3 はサポートされません。
- SNMP デバッグはサポートされません。
- ARP 情報の取得はサポートされません。
- SNMP SET コマンドはサポートされません。
- NET-SNMP バージョン 5.4.2.1 を使用する場合、暗号化アルゴリズム バージョン AES128 だけがサポートされます。暗号化アルゴリズム バージョンの AES256 または AES192 はサポートされません。

- 結果として SNMP 機能の整合性が取れない状態になる場合、既存の設定への変更は拒否されます。
- SNMP バージョン 3 の設定は、グループ、ユーザ、ホストの順に行う必要があります。
- グループを削除する前に、そのグループに関連付けられているすべてのユーザが削除されていることを確認する必要があります。
- ユーザを削除する前に、そのユーザ名に関連付けられているホストが設定されていないことを確認する必要があります。
- 特定のセキュリティ モデルを使用して特定のグループに属するようにユーザが設定されている場合にそのグループのセキュリティ レベルを変更する場合は、次の順に操作を実行する必要があります。
  - そのグループからユーザを削除します。
  - グループのセキュリティ レベルを変更します。
  - 新しいグループに属するユーザを追加します。
- MIB オブジェクトのサブセットへのユーザ アクセスを制限するためのカスタム ビューの作成はサポートされていません。
- すべての要求とトラップは、デフォルトの読み取り/通知ビューだけで使用できます。
- connection-limit-reached トラップは管理コンテキストで生成されます。このトラップを生成するには、接続制限に達したユーザ コンテキストで設定された SNMP サーバ ホストが少なくとも 1 つ必要です。
- ASA 5585 SSP-40（NPE）のシャーシ温度を問い合わせることはできません。
- NMS が正常にオブジェクトを要求できない場合、または ASA からの着信トラップを処理していない場合は、パケット キャプチャの実行が問題を判別する最も有効な方法となります。[Wizards] > [Packet Capture Wizard] を選択して、画面に表示される指示に従います。
- 最大 4000 個までホストを追加できます。ただし、トラップの対象として設定できるのはそのうちの 128 個だけです。
- サポートされるアクティブなポーリング先の総数は 128 個です。
- ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。
- 1 つのホストに複数のユーザを関連付けることができます。
- ネットワーク オブジェクトは、別の **host-group** コマンドと重複して指定することができます。異なるネットワーク オブジェクトの共通のホストに対しては、最後のホスト グループに指定した値が適用されます。
- ホスト グループや他のホスト グループと重複するホストを削除すると、設定済みのホスト グループで指定されている値を使用してホストが再設定されます。
- ホストで取得される値は、コマンドの実行に使用するように指定したシーケンスによって異なります。
- SNMP で送信できるメッセージのサイズは 1472 バイトまでです。
- SNMPv3 エンジン ID はクラスタのメンバー間で同期されません。そのため、SNMPv3 については、クラスタの各ユニットでそれぞれ設定する必要があります。

SNMP の設定

ここでは、SNMP の設定方法について説明します。

ステップ 1　SNMP エージェントおよび SNMP サーバをイネーブルにします。「SNMP エージェントおよび SNMP サーバのイネーブル化」（P.41-6）を参照してください。

ステップ 2　ASA から要求を受信するように SNMP 管理ステーションを設定します。「SNMP 管理ステーションの設定」（P.41-6）を参照してください。

ステップ 3　SNMP トラップを設定します。「SNMP トラップの設定」（P.41-7）を参照してください。

ステップ 4　SNMP バージョン 1 および 2c のパラメータまたは SNMP バージョン 3 のパラメータを設定します。「SNMP バージョン 1 または 2c のパラメータの設定」（P.41-8）または「SNMP バージョン 3 のパラメータの設定」（P.41-9）を参照してください。

SNMP エージェントおよび SNMP サーバのイネーブル化

SNMP エージェントおよび SNMP サーバをイネーブルにするには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [SNMP] を選択します。デフォルトでは、SNMP サーバはイネーブルになっています。

ステップ 2　以降の手順については、「SNMP 管理ステーションの設定」（P.41-6）を参照してください。

SNMP 管理ステーションの設定

SNMP 管理ステーションを設定するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [SNMP] を選択します。

ステップ 2　[SNMP Management Stations] ペインで [Add] をクリックします。

[Add SNMP Host Access Entry] ダイアログボックスが表示されます。

ステップ 3　SNMP ホストが存在するインターフェイスを選択します。

ステップ 4　SNMP ホストの IP アドレスを入力します。

ステップ 5　SNMP ホストの UDP ポートを入力します。デフォルトのポート 162 をそのまま使用することもできます。

ステップ 6　SNMP ホストのコミュニティ ストリングを追加します。管理ステーションに対してコミュニティ ストリングが指定されていない場合は、[SNMP Management Stations] ペインの [Community String (default)] フィールドに設定されている値が使用されます。

ステップ 7　SNMP ホストで使用される SNMP のバージョンを選択します。

ステップ 8　前の手順で SNMP バージョン 3 を選択した場合は、設定済みユーザの名前を選択します。

ステップ 9　[Poll] チェックボックスまたは [Trap] チェックボックスのいずれかをオンにして、NMS との通信に使用する方式を指定します。

ステップ 10　[OK] をクリックします。

[Add SNMP Host Access Entry] ダイアログボックスが閉じます。

ステップ 11　[Apply] をクリックします。

NMS が設定され、その変更内容が実行コンフィギュレーションに保存されます。SNMP バージョン 3 の NMS ツールの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa82/snmp/snmpv3_tools.html

SNMP トラップの設定

SNMP エージェントが生成するトラップ、およびそのトラップを収集し、NMS に送信する方法を指定するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [SNMP] を選択します。

ステップ 2　[Configure Traps] をクリックします。

[SNMP Trap Configuration] ダイアログボックスが表示されます。

ステップ 3　[SNMP Server Traps Configuration] チェックボックスをオンにします。

トラップは、[standard]、[IKEv2]、[entity MIB]、[IPsec]、[remote access]、[resource]、[NAT]、[syslog]、[CPU utilization]、[CPU utilization and monitoring interval]、および [SNMP interface threshold and interval] のカテゴリに分類されます。SNMP トラップを介して通知を発行するための SNMP イベントを指定するため、目的のチェックボックスをオンにします。デフォルトの設定では、すべての SNMP 標準トラップがイネーブルです。トラップ タイプを指定しない場合、デフォルトでは syslog トラップになります。デフォルトの SNMP トラップは、syslog トラップとともにイネーブルの状態を続けます。デフォルトでは他のトラップはすべてディセーブルです。トラップをディセーブルにするには、該当するチェックボックスをオフにします。syslog トラップの重大度レベルを設定するには、[Configuration] > [Device Management] > [Logging] > [Logging Filters] を選択します。

ステップ 4　[OK] をクリックして、[SNMP Trap Configuration] ダイアログボックスを閉じます。

ステップ 5　[Apply] をクリックします。

SNMP トラップが設定され、その変更内容が実行コンフィギュレーションに保存されます。

SNMP バージョン 1 または 2c のパラメータの設定

SNMP バージョン 1 または 2c のパラメータを設定するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [SNMP] を選択します。

ステップ 2　SNMP バージョン 1 または 2c を使用する場合は、[Community String (default)] フィールドにデフォルトのコミュニティ ストリングを入力します。要求を ASA に送信するときに SNMP NMS で使用されるパスワードを入力します。SNMP コミュニティ ストリングは、SNMP NMS と管理対象のネットワーク ノード間の共有秘密です。ASA では、パスワードを基にして、受信する SNMP 要求が有効かどうかの判断が行われます。パスワードは、大文字と小文字が区別される、最大 32 文字の英数字です。スペースは使用できません。デフォルトは public です。SNMP バージョン 2c では、NMS ごとに、別々のコミュニティ ストリングを設定できます。コミュニティ ストリングがどの NMS にも設定されていない場合、ここで設定した値がデフォルトとして使用されます。

ステップ 3　ASA システム管理者の名前を入力します。テキストは、大文字と小文字が区別される、最大 127 文字の英数字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

ステップ 4　SNMP で管理している ASA の場所を入力します。テキストは、大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

ステップ 5　NMS からの SNMP 要求をリッスンする ASA ポートの番号を入力します。デフォルトのポート番号 161 をそのまま使用することもできます。

ステップ 6　[SNMP Host Access List] ペインで [Add] をクリックします。

[Add SNMP Host Access Entry] ダイアログボックスが表示されます。

ステップ 7　トラップの送信元となるインターフェイスの名前をドロップダウン リストから選択します。

ステップ 8　ASA に接続できる NMS または SNMP マネージャの IP アドレスを入力します。

ステップ 9　UDP のポート番号を入力します。デフォルトは 162 です。

ステップ 10　使用する SNMP のバージョンをドロップダウン リストから選択します。バージョン 1 または 2c を選択した場合は、コミュニティ ストリングを入力する必要があります。バージョン 3 を選択した場合は、ドロップダウン リストからユーザ名を選択する必要があります。

ステップ 11　要求の送信（ポーリング）だけに NMS を制限する場合は、[Server Poll/Trap Specification] 領域の [Poll] チェックボックスをオンにします。トラップの受信だけに NMS を制限する場合は、[Trap] チェックボックスをオンにします。両方のチェックボックスをオンにすると、SNMP ホストの両方の機能が実行されます。

ステップ 12　[OK] をクリックして、[Add SNMP Host Access Entry] ダイアログボックスを閉じます。

新しいホストが [SNMP Host Access List] ペインに表示されます。

ステップ 13　[Apply] をクリックします。

SNMP バージョン 1、2c、または 3 のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。

SNMP バージョン 3 のパラメータの設定

SNMP バージョン 3 のパラメータを設定するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [SNMP] を選択します。

ステップ 2　[SNMPv3 Users] ペインの [SNMPv3 User/Group] タブで [Add] > [SNMP User] の順にクリックして、設定済みのユーザまたは新規ユーザをグループに追加します。グループ内に残る最後のユーザを削除すると、そのグループは ASDM により削除されます。

（注）　ユーザが作成された後は、そのユーザが属するグループは変更できません。

[Add SNMP User Entry] ダイアログボックスが表示されます。

ステップ 3　SNMP ユーザが属するグループを選択します。選択できるグループは次のとおりです。

- [Auth&Encryption]：このグループに属するユーザには、認証と暗号化が設定されます。
- [Authentication_Only]：このグループに属するユーザには、認証だけ設定されます。
- [No_Authentication]：このグループに属するユーザには、認証も暗号化も設定されません。

（注）　グループ名は変更できません。

ステップ 4　ユーザ セキュリティ モデル（USM）グループを使用する場合は、[**USM Model**]タブをクリックします。

ステップ 5　[Add] をクリックします。

[Add SNMP USM Entry] ダイアログボックスが表示されます。

ステップ 6　グループ名を入力します。

ステップ 7　ドロップダウン リストからセキュリティ レベルを選択します。設定済みの USM グループをセキュリティ レベルとして SNMPv3 ユーザに割り当てることができます。

ステップ 8　設定済みユーザまたは新規ユーザの名前を入力します。ユーザ名は、選択した SNMP サーバ グループ内で一意であることが必要です。

ステップ 9　[Encrypted] と [Clear Text] のいずれかのオプション ボタンをクリックして、使用するパスワードのタイプを指定します。

ステップ 10　[MD5] と [SHA] のいずれかのオプション ボタンをクリックして、使用する認証のタイプを指定します。

ステップ 11　認証に使用するパスワードを入力します。

ステップ 12　[DES]、[3DES]、[AES] の中からいずれかのオプション ボタンをクリックして、使用する暗号化のタイプを指定します。

ステップ 13　AES 暗号化を選択した場合は、使用する AES 暗号化のレベルとして、**128**、**192**、**256** のいずれかを選択します。

ステップ 14　暗号化に使用するパスワードを入力します。パスワードの長さは、英数字で最大 64 文字です。

ステップ 15　[OK] をクリックすると、グループが作成され（指定したユーザがそのグループに属する最初のユーザである場合）、[Group Name] ドロップダウン リストにそのグループが表示されます。またそのグループ内にユーザが作成されます。

[Add SNMP User Entry] ダイアログボックスが閉じます。

ステップ 16　[Apply] をクリックします。

SNMP バージョン 3 のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。

ユーザのグループの設定

指定したユーザのグループからなる SNMP ユーザ リストを設定するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [SNMP] を選択します。

ステップ 2　[SNMPv3 Users] ペインの [SNMPv3 User/Group] タブで [Add] > [SNMP User Group] の順にクリックして、設定済みのユーザ グループまたは新規ユーザ グループを追加します。グループ内に残る最後のユーザを削除すると、そのグループは ASDM により削除されます。

[Add SNMP User Group] ダイアログボックスが表示されます。

ステップ 3　ユーザ グループ名を入力します。

ステップ 4　既存のユーザまたはユーザ グループを選択する場合は、[Existing User/User Group] オプション ボタンをクリックします。

ステップ 5　新規ユーザを作成する場合は、[Create new user] オプション ボタンをクリックします。

ステップ 6　SNMP ユーザが属するグループを選択します。選択できるグループは次のとおりです。

- [Auth&Encryption]：このグループに属するユーザには、認証と暗号化が設定されます。
- [Authentication_Only]：このグループに属するユーザには、認証だけ設定されます。
- [No_Authentication]：このグループに属するユーザには、認証も暗号化も設定されません。

ステップ 7　設定済みユーザまたは新規ユーザの名前を入力します。ユーザ名は、選択した SNMP サーバ グループ内で一意であることが必要です。

ステップ 8　[Encrypted] と [Clear Text] のいずれかのオプション ボタンをクリックして、使用するパスワードのタイプを指定します。

ステップ 9　[MD5] と [SHA] のいずれかのオプション ボタンをクリックして、使用する認証のタイプを指定します。

ステップ 10　認証に使用するパスワードを入力します。

ステップ 11　認証に使用するパスワードを確認のためにもう一度入力します。

ステップ 12　[DES]、[3DES]、[AES] の中からいずれかのオプション ボタンをクリックして、使用する暗号化のタイプを指定します。

ステップ 13　暗号化に使用するパスワードを入力します。パスワードの長さは、英数字で最大 64 文字です。

ステップ 14　暗号化に使用するパスワードを確認のためにもう一度入力します。

ステップ 15　[Members in Group] ペインの指定したユーザ グループに新規ユーザを追加するには、[Add] をクリックします。[Members in Group] ペインから既存のユーザを削除するには、[Remove] をクリックします。

ステップ 16　[OK] をクリックすると、指定したユーザ グループに新規ユーザが作成されます。

[Add SNMP User Group] ダイアログボックスが閉じます。

ステップ 17　[Apply] をクリックします。

SNMP バージョン 3 のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。

SNMP のモニタリング

SNMP は次の画面でモニタリングできます。

- [Tools] > [Command Line Interface]

  非対話形式の各種コマンドを発行して結果を表示できます。

SNMP の履歴

表 41-2　SNMP の履歴

機能名	プラットフォーム リリース	説明
SNMP バージョン 1 および 2c	7.0(1)	クリア テキスト コミュニティ ストリングを使用した SNMP サーバと SNMP エージェントの間でのデータ送信によって、ASA、ASAv、および ASASM ネットワーク モニタリングとイベント情報を提供します。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。
SNMP バージョン 3	8.2(1)	3DES または AES 暗号化、およびサポートされているセキュリティ モデルの中で最もセキュアな形式である SNMP バージョン 3 のサポートを提供します。このバージョンでは、USM を使用して、ユーザ、グループ、ホスト、および認証の特性を設定できます。さらに、このバージョンでは、エージェントと MIB オブジェクトへのアクセス コントロールが許可され、追加の MIB サポートが含まれます。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。
パスワードの暗号化	8.3(1)	パスワードの暗号化がサポートされます。

表 41-2　SNMP の履歴（続き）

機能名	プラットフォーム リリース	説明
SNMP トラップと MIB	8.4(1)	追加のキーワードとして、**connection-limit-reached**、**cpu threshold rising**、**entity cpu-temperature**、**entity fan-failure**、**entity power-supply**、**ikev2 stop | start**、**interface-threshold**、**memory-threshold**、**nat packet-discard**、**warmstart** をサポートします。 entPhysicalTable によって、センサー、ファン、電源、および関連コンポーネントのエントリがレポートされます。 追加の MIB として、CISCO-ENTITY-SENSOR-EXT-MIB、CISCO-ENTITY-FRU-CONTROL-MIB、CISCO-PROCESS-MIB、CISCO-ENHANCED-MEMPOOL-MIB、CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB、DISMAN-EVENT-MIB、DISMAN-EXPRESSION-MIB、ENTITY-SENSOR-MIB、NAT-MIB をサポートします。 さらに ceSensorExtThresholdNotification、clrResourceLimitReached、cpmCPURisingThreshold、mteTriggerFired、natPacketDiscard、warmStart トラップをサポートしています。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。
IF-MIB ifAlias OID のサポート	8.2(5)/8.4(2)	ASA で ifAlias OID がサポートされるようになりました。IF-MIB をブラウズする際、fAlias OID はインターフェイスの記述に設定済みの値に設定されます。
ASA サービス モジュール（ASASM）	8.5(1)	ASASM は、次を除く 8.4(1) にあるすべての MIB およびトラップをサポートします。 8.5(1) のサポートされていない MIB： • CISCO-ENTITY-SENSOR-EXT-MIB（entPhySensorTable グループのオブジェクトだけがサポートされます）。 • ENTITY-SENSOR-MIB（entPhySensorTable グループのオブジェクトだけがサポートされます）。 • DISMAN-EXPRESSION-MIB（expExpressionTable、expObjectTable、および expValueTable グループのオブジェクトだけがサポートされます）。 8.5(1) のサポートされていないトラップ： • ceSensorExtThresholdNotification（CISCO-ENTITY-SENSOR-EXT-MIB）。このトラップは、電源障害、ファン障害および高 CPU 温度のイベントだけに使用されます。 • InterfacesBandwidthUtilization。
SNMP トラップ	8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X の追加のキーワードとして、**entity power-supply-presence**、**entity power-supply-failure**、**entity chassis-temperature**、**entity chassis-fan-failure, entity power-supply-temperature** をサポートします。 次のコマンドが変更されました。**snmp-server enable traps**。

表 41-2　SNMP の履歴 （続き）

機能名	プラットフォーム リリース	説明
VPN-related MIB	9.0(1)	CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB の更新バージョンが、次世代の暗号化機能をサポートするために実装されました。 ASASM では、次の MIB がイネーブルになりました。 • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	CISCO-TRUSTSEC-SXP-MIB のサポートが追加されました。
SNMP OID	9.1(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X をサポートするために 5 つの新しい SNMP 物理ベンダー タイプ OID が追加されました。
NAT MIB	9.1(2)	cnatAddrBindNumberOfEntries および cnatAddrBindSessionCount OID が、xlate_count および max_xlate_count エントリをサポートするようになりました。これは、**show xlate count** コマンドを使用したポーリングの許可と同等です。
SNMP のホスト、ホスト グループ、ユーザ リスト	9.1(5)	最大 4000 個までホストを追加できるようになりました。サポートされるアクティブなポーリング先の数は 128 個です。ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。1 つのホストに複数のユーザを関連付けることができます。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。
SNMP メッセージのサイズ	9.2(1)	SNMP で送信できるメッセージのサイズが 1472 バイトまでに増えました。
SNMP の MIB およびトラップ	9.3(2)	新しい ASA 5506-X、ASA 5506W-X、および ASA 5508-X をサポートするように CISCO-PRODUCTS-MIB および CISCO-ENTITY-VENDORTYPE-OID-MIB が更新されました。 SNMP の sysObjectID OID および entPhysicalVendorType OID の表に、新しい製品として ASA 5506-X と ASA 5508-X が追加されました。 ASA で CISCO-CONFIG-MAN-MIB がサポートされるようになりました。以下が可能です。 • 特定のコンフィギュレーションについて入力されたコマンドを確認する。 • 実行コンフィギュレーションに変更が発生したときに NMS に通知する。 • 実行コンフィギュレーションが最後に変更または保存されたときのタイム スタンプを追跡する。 • 端末の詳細やコマンドのソースなど、コマンドに対するその他の変更を追跡する。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP] > [Configure Traps] > [SNMP Trap Configuration]。

Anonymous Reporting および Smart Call Home

この章では、Anonymous Reporting および Smart Call Home サービスを設定する方法について説明します。

Anonymous Reporting について

Anonymous Reporting をイネーブルにして、Cisco ASA プラットフォームを強化することができます。Anonymous Reporting により、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに安全に送信できます。この機能をイネーブルにした場合、お客様のアイデンティティは匿名のままとなり、識別情報は送信されません。

Anonymous Reporting をイネーブルにすると、トラスト ポイントが作成され、証明書がインストールされます。CA 証明書は、ASA でメッセージを安全に送信できるように、Smart Call Home Web サーバ上のサーバ証明書を検証して、HTTPS セッションを形成するために必要です。ソフトウェアに事前定義済みの証明書が、シスコによってインポートされます。Anonymous Reporting をイネーブルにする場合は、ハードコードされたトラスト ポイント名の _SmartCallHome_ServerCA で証明書が ASA にインストールされます。Anonymous Reporting をイネーブルにすると、このトラスト ポイントが作成され、適切な証明書がインストールされて、このアクションに関するメッセージが表示されます。これで、証明書が設定の中に存在するようになります。

Anonymous Reporting をイネーブルにしたときに、適切な証明書がすでに設定に存在する場合、トラスト ポイントは作成されず、証明書はインストールされません。

（注） Anonymous Reporting をイネーブルにすると、指定されたデータをシスコまたはシスコの代わりに運用するベンダー（米国以外の国を含む）に転送することに同意することになります。シスコでは、すべてのお客様のプライバシーを保護しています。シスコの個人情報の取り扱いに関する詳細については、次の URL にあるシスコのプライバシー声明を参照してください。
http://www.cisco.com/web/siteassets/legal/privacy.html

DNS 要件

ASA が Cisco Smart Call Home サーバに到達してシスコにメッセージを送信できるように DNS サーバを正しく設定する必要があります。ASA をプライベート ネットワークに配置し、パブリック ネットワークにはアクセスできないようにすることが可能なため、シスコでは DNS 設定を検証し、必要な場合には次の手順を実行して、ユーザの代わりにこれを設定します。

1. **設定されているすべての DNS サーバに対して DNS ルックアップを実行します。**
2. 最もセキュリティレベルの高いインターフェイスで DHCPINFORM メッセージを送信して、DHCP サーバから DNS サーバを取得します。
3. ルックアップにシスコの DNS サーバを使用します。
4. tools.cisco.com に対してランダムに静的 IP アドレスを使用します。

これらの作業は、現在の設定を変更せずに実行されます。（たとえば、DHCP から学習された DNS サーバは設定には追加されません）。

設定されている DNS サーバがなく、ASA が Cisco Smart Call Home サーバに到達できない場合は、各 Smart Call Home メッセージに対して、重大度「warning」の syslog メッセージが生成されます。これは、DNS を適切に設定するようお願いするためです。

syslog メッセージについては、syslog メッセージ ガイドを参照してください。

Smart Call Home の概要

完全に設定が終わると、Smart Call Home は設置場所での問題を検出し、多くの場合はそのような問題があることにユーザが気付く前に、シスコにレポートを返すか、別のユーザ定義のチャネル（ユーザ宛の電子メールまたはユーザに直接など）を使用してレポートを返します。シスコでは、これらの問題の重大度に応じて次のサービスを提供することにより、システム コンフィギュレーションの問題、製品ライフサイクル終了通知の発表、セキュリティ勧告問題などに対応します。

- 継続的モニタリング、リアルタイムの予防的なアラート、および詳細な診断により、問題を迅速に識別する。
- サービス要求が開かれ、すべての診断データが添付された Smart Call Home 通知を使用して、潜在的な問題をユーザに認識させる。
- Cisco TAC の専門家に自動的に直接アクセスすることにより、重大な問題を迅速に解決する。
- トラブルシューティングに必要な時間を短縮することにより、スタッフ リソースを効率よく使用する。
- Cisco TAC へのサービス リクエストを自動的に生成し（サービス契約がある場合）、適切なサポート チームに提出する。問題解決の時間を短縮する、詳細な診断情報を提供します。

Smart Call Home ポータルを使用すると必要な情報に迅速にアクセスできるため、以下の事項が実現されます。

- すべての Smart Call Home メッセージ、診断、および推奨事項を一箇所で確認する。
- サービス リクエスト ステータスを確認する。
- すべての Smart Call Home 対応デバイスに関する最新のインベントリ情報およびコンフィギュレーション情報を表示する。

Anonymous Reporting および Smart Call Home のガイドライン

Anonymous Reporting

- DNS が設定されていること。
- Anonymous Reporting のメッセージを最初の試行で送信できなかった場合、ASA はメッセージをドロップする前にさらに 2 回試行します。
- Anonymous Reporting は、既存の設定を変更せずに、他の Smart Call Home 設定と共存させることができます。たとえば、Anonymous Reporting をイネーブルにする前に Smart Call Home がディセーブルになっている場合、Anonymous Reporting をイネーブルにした後でも、ディセーブルのままです。
- Anonymous Reporting をイネーブルにしている場合、トラスト ポイントを削除することはできません。また、Anonymous Reporting をディセーブルにした場合、トラスト ポイントはそのまま残ります。Anonymous Reporting がディセーブルの場合は、トラスト ポイントを削除できますが、Anonymous Reporting をディセーブルにしてもトラスト ポイントは削除されません。
- マルチ コンテキスト モード設定を使用している場合は、**dns**、**interface**、**trustpoint** コマンドは管理コンテキストにあり、**call-home** コマンドはシステム コンテキストにあります。

Smart Call Home

- マルチ コンテキスト モードでは、**subscribe-to-alert-group snapshot periodic** コマンドは 2 つのコマンドに分割されます。1 つは情報をシステム コンフィギュレーションから取得するものであり、もう 1 つは情報をユーザ コンテキストから取得します。
- Smart Call Home のバックエンド サーバは、XML 書式のメッセージのみ受け取ることができます。
- Smart Call Home メッセージは、クラスタリングをイネーブルにしており、クリティカルな重大度を持つ診断アラート グループに登録するように Smart Call Home を設定してある場合に、重要なクラスタ イベントをレポートするためにシスコに送信されます。Smart Call Home クラスタリング メッセージは、次のイベントに対してのみ送信されます。
  - ユニットがクラスタに参加したとき
  - ユニットがクラスタから脱退したとき
  - クラスタ ユニットがクラスタ マスターになったとき
  - クラスタのセカンダリ ユニットが故障したとき

  送信される各メッセージには次の情報が含まれています。
  - アクティブ クラスタのメンバ数
  - クラスタ マスターでの **show cluster info** コマンドおよび **show cluster history** コマンドの出力

関連項目

- 「DNS 要件」（P.42-2）
- 「DNS サーバの設定」（P.14-12）

Anonymous Reporting および Smart Call Home の設定

Anonymous Reporting は Smart Call Home サービスの一部であり、これを使用すると、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに匿名で送信できます。一方、Smart Call Home サービスは、システム ヘルスのサポートをカスタマイズする機能です。Cisco TAC がお客様のデバイスをモニタして、問題があるときにケースを開くことができるようになります。多くの場合は、お客様がその問題に気付く前に発見できます。

両方のサービスをシステム上で同時に設定できますが、Smart Call Home サービスを設定すれば、Anonymous Reporting と同じ機能に加えて、カスタマイズされたサービスも使用できるようになります。

Anonymous Reporting の設定

Anonymous Reporting を設定するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Smart Call Home] の順に選択します。

ステップ 2　[Enable Anonymous Reporting] チェックボックスをオンにします。

ステップ 3　[Test Connection] をクリックして、システムでメッセージを送信できることを確認します。

ASDM は成功メッセージまたはエラー メッセージを返して、テスト結果を通知します。

ステップ 4　[Apply] をクリックして設定を保存し、Anonymous Reporting をイネーブルにします。

Smart Call Home の設定

Smart Call Home サービス、システム セットアップ、およびアラート サブスクリプション プロファイルを設定するには、次の手順を実行します。

手順

ステップ 1　[Configuration] > [Device Management] > [Smart Call Home] の順に選択します。

ステップ 2　[Enable Registered Smart Call Home] チェックボックスをオンにして、Smart Call Home をイネーブルにし、ASA を Cisco TAC に登録します。

ステップ 3　[Advanced System Setup] をダブルクリックします。この領域は、3 個のペインで構成されています。各ペインは、タイトル行をダブルクリックすると展開または縮小できます。

a. [Mail Servers] ペインで、Smart Call Home メッセージを電子メールのサブスクライバに配信する際に通過するメール サーバを設定できます。

b. ASA の [Contact Information] ペインで、Smart Call Home メッセージに表示される担当者の個人情報を入力できます。このペインには、次の情報が含まれます。

- 連絡先担当者の名前。
- 連絡先の電話番号。
- 連絡先担当者の住所。

- 連絡先の電子メール アドレス。
- Smart Call Home 電子メールの「from」電子メール アドレス。
- Smart Call Home 電子メールの「reply-to」電子メール アドレス。
- カスタマー ID。
- サイト ID。
- 連絡先 ID。

c. [Alert Control] ペインで、アラートの制御パラメータを調整できます。このペインには、[Alert Group Status] ペインが含まれ、ここには次のアラート グループのステータス（イネーブルまたはディセーブル）がリストされます。

- 診断アラート グループ。
- コンフィギュレーション アラート グループ。
- 環境アラート グループ。
- インベントリ アラート グループ。
- スナップショット アラート グループ。
- syslog アラート グループ。
- テレメトリ アラート グループ。
- 脅威アラート グループ。
- 1 分間に処理される Smart Call Home メッセージの最大数。
- Smart Call Home 電子メールの「from」電子メール アドレス。

ステップ 4　[Alert Subscription Profiles] をダブルクリックします。指定した各サブスクリプション プロファイルによって、サブスクライバおよび対象とするアラート グループが特定されます。

a. [Add] または [Edit] をクリックして、**サブスクリプション プロファイル エディタ**を表示します。ここでは、新規サブスクリプション プロファイルを作成したり、既存のサブスクリプション プロファイルを編集したりできます。

b. [Delete] をクリックして、選択したプロファイルを削除します。

c. [Active] チェックボックスをオンにして、選択されたサブスクリプション プロファイルの Smart Call Home メッセージをサブスクライバに送信します。

ステップ 5　[Add] または [Edit] をクリックして、[Add Alert Subscription Profile] ダイアログボックスまたは [Edit Alert Subscription Profile] ダイアログ ボックスを表示します。

a. [Name] フィールドは読み取り専用であり、編集できません。

b. [Enable this subscription profile] チェックボックスをオンにして、この特定のプロファイルをイネーブルまたはディセーブルにします。

c. [Alert Delivery Method] 領域で、[HTTP] または [Email] オプション ボタンのいずれかをクリックします。

d. [Subscribers] フィールドに電子メール アドレスまたは Web アドレスを入力します。

e. [Alert Dispatch] 領域では、管理者が、サブスクライバに送信する Smart Call Home 情報の種類と送信の条件を指定できます。時間ベースとイベントベースの 2 種類のアラートがあり、アラートのトリガー方法に応じて選択します。コンフィギュレーション、インベントリ、スナップショット、およびテレメトリの各アラート グループは時間ベースです。診断、環境、Syslog、および脅威の各アラート グループはイベントベースです。

f. [Message Parameters] 領域では、優先されるメッセージ形式や最大メッセージ サイズなど、サブスクライバに送信されるメッセージを制御するパラメータを調整できます。

ステップ 6　時間ベースのアラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Add Configuration Alert Dispatch Condition] または [Edit Configuration Alert Dispatch Condition] ダイアログボックスを表示します。

a. [Alert Dispatch Frequency] 領域で、サブスクライバに情報を送信する頻度を指定します。

- 毎月のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎週のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎日のサブスクリプションには、情報を送信する時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 時間単位のサブスクリプションには、情報を送信する時間（分単位）を指定します。この指定がない場合は、ASA が適切な値を選択します。時間単位のサブスクリプションが適切なのは、スナップショットおよびテレメトリ アラート グループのみです。

b. [Basic] または [Detailed] オプション ボタンをクリックして、サブスクライバに必要な情報のレベルを指定します。

c. [OK] をクリックして、コンフィギュレーションを保存します。

ステップ 7　イベントベースの診断、環境、および脅威アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Diagnostic Alert Dispatch Condition] または [Edit Diagnostic Alert Dispatch Condition] ダイアログボックスを表示します。

ステップ 8　[Event Severity] ドロップダウン リストで、サブスクライバへのアラートのディスパッチをトリガーするイベントの重大度を指定し、[OK] をクリックします。

ステップ 9　時間ベースのインベントリ アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Inventory Alert Dispatch Condition] または [Edit Inventory Alert Dispatch Condition] ダイアログボックスを表示します。

ステップ 10　[Alert Dispatch Frequency] ドロップダウン リストで、サブスクライバにアラートをディスパッチする頻度を指定し、[OK] をクリックします。

ステップ 11　時間ベースのスナップショット アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Snapshot Alert Dispatch Condition] または [Edit Snapshot Alert Dispatch Condition] ダイアログボックスを表示します。

a. [Alert Dispatch Frequency] 領域で、サブスクライバに情報を送信する頻度を指定します。

- 毎月のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎週のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎日のサブスクリプションには、情報を送信する時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 時間単位のサブスクリプションには、情報を送信する時間（分単位）を指定します。この指定がない場合は、ASA が適切な値を選択します。時間単位のサブスクリプションが適切なのは、スナップショットおよびテレメトリ アラート グループのみです。
- 間隔サブスクリプションの場合、サブスクライバに情報を送信する頻度を分単位で指定します。この要件は、スナップショット アラート グループにのみ適用されます。

b. [OK] をクリックして、コンフィギュレーションを保存します。

ステップ 12　イベントベースの syslog アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Syslog Alert Dispatch Condition] または [Edit Syslog Alert Dispatch Condition] ダイアログボックスを表示します。

a. [Specify the event severity which triggers the dispatch of alert to subscribers] チェックボックスをオンにして、ドロップダウン リストからイベントの重大度を選択します。

b. [Specify the message IDs of syslogs which trigger the dispatch of alert to subscribers] チェックボックスをオンにします。

c. 画面の指示に従って、サブスクライバへのアラートのディスパッチをトリガーする syslog メッセージ ID を指定します。

d. [OK] をクリックして、コンフィギュレーションを保存します。

ステップ 13　イベントベースのテレメトリ アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Telemetry Alert Dispatch Condition] または [Edit Telemetry Alert Dispatch Condition] ダイアログボックスを表示します。

a. [Alert Dispatch Frequency] 領域で、サブスクライバに情報を送信する頻度を指定します。

- 毎月のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎週のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎日のサブスクリプションには、情報を送信する時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 時間単位のサブスクリプションには、情報を送信する時間（分単位）を指定します。この指定がない場合は、ASA が適切な値を選択します。時間単位のサブスクリプションが適切なのは、スナップショットおよびテレメトリ アラート グループのみです。

b. [OK] をクリックして、コンフィギュレーションを保存します。

ステップ 14　[Test] をクリックして、設定したアラートが正しく動作しているかどうかを判別します。

Anonymous Reporting および Smart Call Home のモニタリング

Anonymous Reporting および Smart Call Home サービスのモニタリングについては、次の画面を参照してください。

- [Tools] > [Command Line Interface]

  非対話形式の各種コマンドを発行して結果を表示できます。

Anonymous Reporting および Smart Call Home の履歴

表 42-1　Anonymous Reporting および Smart Call Home の履歴

機能名	プラットフォーム リリース	説明
Smart Call Home	8.2(2)	Smart Call Home サービスは、ASA に関する予防的診断およびリアルタイム アラートを提供し、ネットワークの可用性および運用効率を向上させます。 次の画面が導入されました。 [Configuration] > [Device Management] > [Smart Call Home]。
Anonymous Reporting	9.0(1)	Anonymous Reporting をイネーブルにして、ASA プラットフォームを強化することができます。Anonymous Reporting により、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに安全に送信できます。 次の画面が変更されました。[Configuration] > [Device Monitoring] > [Smart Call Home]。
Smart Call Home	9.1(2)	テレメトリ アラート グループ レポートのための **show local-host** コマンドは、**show local-host | include interface** コマンドに変更になりました。
Smart Call Home	9.1(3)	Smart Call Home メッセージは、クラスタリングをイネーブルにしており、クリティカルな重大度を持つ診断アラート グループに登録するように Smart Call Home を設定してある場合に、重要なクラスタ イベントをレポートするためにシスコに送信されます。Smart Call Home クラスタリング メッセージは、次の 3 種類のイベントに対してのみ送信されます。 • ユニットがクラスタに参加したとき • ユニットがクラスタから脱退したとき • クラスタ ユニットがクラスタ マスターになったとき 送信される各メッセージには次の情報が含まれています。 • アクティブ クラスタのメンバ数 • クラスタ マスターでの **show cluster info** コマンドおよび **show cluster history** コマンドの出力

PART 10

参照先

アドレス、プロトコル、およびポート

この章では、IP アドレス、プロトコル、およびアプリケーションのクイック リファレンスを提供します。

IPv4 アドレスとサブネット マスク

この項では、Cisco ASA で IPv4 アドレスを使用する方法について説明します。IPv4 アドレスはドット付き 10 進数表記の 32 ビットの数値であり、バイナリから 10 進数に変換されドットで区切られた 4 つの 8 ビット フィールド（オクテット）で構成されます。IP アドレスの最初の部分はホストが常駐するネットワークを示し、2 番目の部分は所定のネットワーク上の特定のホストを示します。ネットワーク番号フィールドは、ネットワーク プレフィックスと呼ばれます。所定のネットワーク上のホストはすべて、同じネットワーク プレフィックスを共有しますが、固有のホスト番号を持つ必要があります。クラスフル IP では、アドレスのクラスがネットワーク プレフィックスとホスト番号の間の境界を決定します。

クラス

IP ホスト アドレスは、Class A、Class B、および Class C の 3 つの異なるアドレス クラスに分割されます。各クラスは、32 ビット アドレス内の異なるポイントで、ネットワーク プレフィックスとホスト番号の間の境界を修正します。Class D アドレスは、マルチキャスト IP 用に予約されています。

- Class A アドレス（1.xxx.xxx.xxx ～ 126.xxx.xxx.xxx）は、最初のオクテットだけをネットワーク プレフィックスとして使用します。
- Class B アドレス（128.0.xxx.xxx ～ 191.255.xxx.xxx）は、最初の 2 つのオクテットをネットワーク プレフィックスとして使用します。
- Class C アドレス（192.0.0.xxx ～ 223.255.255.xxx）は、最初の 3 つのオクテットをネットワーク プレフィックスとして使用します。

Class A アドレスには 16,777,214 個のホスト アドレス、Class B アドレスには 65,534 個のホストがあるので、サブネット マスクを使用してこれらの膨大なネットワークを小さいサブネットに分割することができます。

プライベート ネットワーク

ネットワーク上に多数のアドレスが必要な場合、それらをインターネットでルーティングする必要がないときは、インターネット割り当て番号局（IANA）が推奨するプライベート IP アドレスを使用できます（RFC 1918 を参照）。次のアドレス範囲が、アドバタイズされないプライベート ネットワークとして指定されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

サブネット マスク

サブネット マスクを使用すると、単一の Class A、B、または C ネットワークを複数のネットワークに変換できます。サブネット マスクを使用して、ホスト番号からネットワーク プレフィックスにビットを追加する拡張ネットワーク プレフィックスを作成することができます。たとえば、Class C ネットワーク プレフィックスは常に、IP アドレスの最初の 3 つのオクテットで構成されます。一方、Class C 拡張ネットワーク プレフィックスは、4 番目のオクテットの一部も使用します。

ドット付き 10 進数の代わりにバイナリ表記を使用している場合は、サブネット マスクを容易に理解できます。サブネット マスク内のビットには、インターネット アドレスとの 1 対 1 の対応関係があります。

- IP アドレス内の対応するビットが拡張ネットワーク プレフィックスの一部である場合、ビットは 1 に設定されます。
- ビットがホスト番号の一部である場合、ビットは 0 に設定されます。

例 1 : Class B アドレスが 129.10.0.0 の場合に 3 番目のオクテット全体をホスト番号ではなく拡張ネットワーク プレフィックスの一部として使用するには、サブネット マスクとして 11111111.11111111.11111111.00000000 を指定する必要があります。このサブネット マスクによって、Class B アドレスは、ホスト番号が最後のオクテットだけで構成される Class C アドレスに相当するものに変換されます。

例 2 : 3 番目のオクテットの一部だけを拡張ネットワーク プレフィックスに使用する場合は、11111111.11111111.11111000.00000000 のようなサブネット マスクを指定する必要があります。ここでは、3 番目のオクテットのうち 5 ビットだけが拡張ネットワーク プレフィックスに使用されます。

サブネット マスクは、ドット付き 10 進数マスクまたは */ビット*（「スラッシュ *ビット*」）マスクとして記述できます。例 1 では、ドット付き 10 進数マスクに対して、各バイナリ オクテットを 10 進数の 255.255.255.0 に変換します。*/ビット* マスクの場合は、1s: /24 の数値を追加します。例 2 では、10 進数は 255.255.248.0 で、/ビットは /21 です。

3 番目のオクテットの一部を拡張ネットワーク プレフィックスに使用して、複数の Class C ネットワークを大規模なネットワークにスーパーネット化することもできます。たとえば、192.168.0.0/20 と指定します。

サブネット マスクの決定

必要なホストの数に基づいてサブネット マスクを決定するには、表 43-1 を参照してください。

（注）　単一のホストを示す /32 を除き、サブネットの最初と最後の数は予約されています。

表 43-1　ホスト、ビット、およびドット付き 10 進数マスク

ホスト	/ビット マスク	ドット付き 10 進数マスク
16,777,216	/8	255.0.0.0 Class A ネットワーク
65,536	/16	255.255.0.0 Class B ネットワーク
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8192	/19	255.255.224.0
4096	/20	255.255.240.0
2048	/21	255.255.248.0
1024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	255.255.255.0 Class C ネットワーク
128	/25	255.255.255.128
64	/26	255.255.255.192
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
使用不可	/31	255.255.255.254
1	/32	255.255.255.255 単一ホスト アドレス

サブネット マスクで使用するアドレスの判別

次の各項では、Class C サイズおよび Class B サイズのネットワークに対してサブネット マスクで使用するネットワーク アドレスを判別する方法について説明します。

Class C サイズのネットワーク アドレス

2 ～ 254 のホストを持つネットワークの場合、4 番目のオクテットは、0 から始まるホスト アドレスの数の倍数になります。例として、表 43-2 に 8 個のホストを持つサブネット（/29）、192.168.0.x を示します。

（注）　サブネットの最初と最後のアドレスは予約されています。最初のサブネットの例では、192.168.0.0 と 192.168.0.7 は使用できません。

表 43-2　Class C サイズのネットワーク アドレス

マスク /29（255.255.255.248）でのサブネット	アドレス範囲
192.168.0.0	192.168.0.0 ～ 192.168.0.7
192.168.0.8	192.168.0.8 ～ 192.168.0.15
192.168.0.16	192.168.0.16 ～ 192.168.0.31
—	—
192.168.0.248	192.168.0.248 ～ 192.168.0.255

Class B サイズのネットワーク アドレス

254 ～ 65,534 のホストを持つネットワークのサブネット マスクで使用するネットワーク アドレスを判別するには、可能な拡張ネットワーク プレフィックスそれぞれについて 3 番目のオクテットの値を判別する必要があります。たとえば、10.1.*x*.0 のようなアドレスをサブネット化することができます。ここで、最初の 2 つのオクテットは拡張ネットワーク プレフィックスで使用されるため固定されています。4 番目のオクテットは、すべてのビットがホスト番号に使用されるため、0 です。

3 番目のオクテットの値を判別するには、次の手順を実行します。

ステップ 1　65,536（3 番目と 4 番目のオクテットを使用するアドレスの合計）を必要なホスト アドレスの数で割って、ネットワークから作成できるサブネットの数を計算します。

たとえば、65,536 を 4096 のホストで割ると、16 になります。

したがって、Class B サイズのネットワークでは、それぞれ 4096 個のアドレスを持つサブネットが 16 個できます。

ステップ 2　256（3 番目のオクテットの値の数）をサブネットの数で割って、3 番目のオクテット値の倍数を判別します。

この例では、256/16 = 16 です。

3 番目のオクテットは、0 から始まる 16 の倍数になります。

ネットワーク 10.1 の 16 個のサブネットを表 43-3 に示します。

（注）　サブネットの最初と最後のアドレスは予約されています。最初のサブネットの例では、10.1.0.0 と 10.1.15.255 は使用できません。

表 43-3　ネットワークのサブネット

マスク /20（255.255.240.0）でのサブネット	アドレス範囲
10.1.0.0	10.1.0.0 ～ 10.1.15.255
10.1.16.0	10.1.16.0 ～ 10.1.31.255
10.1.32.0	10.1.32.0 ～ 10.1.47.255
—	—
10.1.240.0	10.1.240.0 ～ 10.1.255.255

IPv6 形式のアドレス

IPv6 は、IPv4 後の次世代インターネット プロトコルです。これにより、アドレス空間の拡張、ヘッダー形式の簡略化、拡張子とオプションのサポートの向上、フロー ラベル機能、および認証とプライバシーの機能が提供されます。IPv6 については RFC 2460 で説明されています。IPv6 アドレッシング アーキテクチャについては RFC 3513 で説明されています。

この項では、IPv6 のアドレス形式とアーキテクチャについて説明します。

関連項目

「IPv6 アドレッシングの設定」（P.12-15）

IPv6 アドレス形式

IPv6 アドレスは、x:x:x:x:x:x:x:x のように、コロン（:）で区切られた 8 つの一連の 16 ビット 16 進数フィールドとして表されます。次に、IPv6 アドレスの例を 2 つ示します。

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A

（注） IPv6 アドレスの 16 進文字は大文字と小文字が区別されません。

アドレスの個々のフィールドに先行ゼロを入れる必要はありませんが、各フィールドに 1 個以上の桁が含まれている必要があります。したがって、例のアドレス 2001:0DB8:0000:0000:0008:0800:200C:417A は、左から 3 番目～ 6 番目のフィールドから先行ゼロを削除して、2001:0DB8:0:0:8:800:200C:417A のように短縮することができます。ゼロだけを含むフィールド（左から 3 番目と 4 番目のフィールド）は、単一のゼロに短縮されています。左から 5 番目のフィールドでは、3 つの先行ゼロが削除され、単一の 8 がフィールドに残されています。左から 6 番目のフィールドでは、1 つの先行ゼロが削除され、800 がフィールドに残されています。

IPv6 アドレスには、ゼロの 16 進数フィールドがいくつか連続して含まれていることがよくあります。IPv6 アドレスの先頭、中間、または末尾で 2 つのコロン（::）を使用して、ゼロの連続フィールドを圧縮することができます（コロンは、ゼロの 16 進数フィールドが連続していることを表します）。表 43-4 に、さまざまなタイプの IPv6 アドレスでのアドレス圧縮の例をいくつか示します。

表 43-4　IPv6 アドレスの圧縮例

アドレス タイプ	標準形式	圧縮形式
ユニキャスト	2001:0DB8:0:0:0:BA98:0:3210	2001:0DB8::BA98:0:3210
マルチキャスト	FF01:0:0:0:0:0:0:101	FF01::101
ループバック	0:0:0:0:0:0:0:1	::1
未指定	0:0:0:0:0:0:0:0	::

（注） ゼロのフィールドが連続することを表す 2 つのコロン（::）は、IPv6 アドレスの中で一度だけ使用できます。

IPv4 アドレスと IPv6 アドレスの両方を含む環境に対処するため、別の IPv6 形式がよく使用されます。その形式は x:x:x:x:x:x:y.y.y.y です。ここで、x は IPv6 アドレスの 6 つの高次の部分の 16 進数値を表し、y はアドレスの 32 ビット IPv4 部分（IPv6 アドレスの残りの 2 つの 16 ビット部分を占める）の 10 進数値を表します。たとえば、IPv4 アドレス 192.168.1.1 は、IPv6 アドレス 0:0:0:0:0:0:FFFF:192.168.1.1 または ::FFFF:192.168.1.1 として表すことができます。

IPv6 アドレス タイプ

次に、IPv6 アドレスの 3 つの主なタイプを示します。

- **ユニキャスト**：ユニキャスト アドレスは、単一インターフェイスの識別子です。ユニキャスト アドレスに送信されたパケットは、そのアドレスで示されたインターフェイスに送信されます。1 つのインターフェイスに複数のユニキャスト アドレスが割り当てられている場合もあります。
- **マルチキャスト**：マルチキャスト アドレスは、インターフェイスのセットを表す識別子です。マルチキャスト アドレスに送信されたパケットは、そのアドレスで示されたすべてのアドレスに送信されます。
- **エニーキャスト**：エニーキャスト アドレスは、インターフェイスのセットを表す識別子です。マルチキャスト アドレスと違い、エニーキャスト アドレスに送信されたパケットは、ルーティング プロトコルの距離測定によって判別された「最も近い」インターフェイスにだけ送信されます。

（注）　IPv6 にはブロードキャスト アドレスはありません。マルチキャスト アドレスにブロードキャスト機能があります。

ユニキャスト アドレス

この項では、IPv6 ユニキャスト アドレスについて説明します。ユニキャスト アドレスは、ネットワーク ノード上のインターフェイスを識別します。

グローバル アドレス

IPv6 グローバル ユニキャスト アドレスの一般的な形式では、グローバル ルーティング プレフィックス、サブネット ID、インターフェイス ID の順に並んでいます。グローバル ルーティング プレフィックスは、別の IPv6 アドレス タイプによって予約されていない任意のプレフィックスです。

バイナリ 000 で始まるものを除くすべてのグローバル ユニキャスト アドレスが、Modified EUI-64 形式で 64 ビットのインターフェイス ID を持っています。

バイナリ 000 で始まるグローバル ユニキャスト アドレスには、アドレスのインターフェイス ID 部分のサイズまたは構造に対する制約がありません。このタイプのアドレスの一例として、IPv4 アドレスが埋め込まれた IPv6 アドレスがあります。

関連項目

- 「IPv6 アドレス プレフィックス」（P.43-10）
- 「インターフェイス識別子」（P.43-8）
- 「IPv4 互換 IPv6 アドレス」（P.43-7）

サイトローカル アドレス

サイトローカル アドレスは、サイト内のアドレッシングに使用されます。このアドレスを使用すると、グローバルで一意のプレフィックスを使用せずにサイト全体をアドレッシングすることができます。サイトローカル アドレスでは、プレフィックス FEC0::/10、54 ビット サブネット ID、64 ビット インターフェイス ID（Modified EUI-64 形式）の順に並んでいます。

サイトローカル ルータは、サイト外の送信元または宛先にサイトローカル アドレスを持つパケットを転送しません。したがって、サイトローカル アドレスは、プライベート アドレスと見なされます。

リンクローカル アドレス

すべてのインターフェイスに、少なくとも 1 つのリンクローカル アドレスが必要です。インターフェイスごとに複数の IPv6 アドレスを設定できますが、設定できるリンクローカル アドレスは 1 つだけです。

リンクローカル アドレスは、Modified EUI-64 形式でリンクローカル プレフィックス FE80::/10 とインターフェイス識別子を使用して任意のインターフェイスで自動的に設定できる IPv6 ユニキャスト アドレスです。リンクローカル アドレスは、ネイバー探索プロトコルとステートレス自動設定プロセスで使用されます。リンクローカル アドレスを持つノードは、通信が可能です。これらのノードは通信にサイトローカル アドレスまたはグローバルに固有なアドレスを必要としません。

ルータは、送信元または宛先にリンクローカル アドレスを持つパケットを送信しません。したがって、リンクローカル アドレスは、プライベート アドレスと見なされます。

IPv4 互換 IPv6 アドレス

IPv4 アドレスを組み込むことができる IPv6 アドレスのタイプは 2 つあります。

最初のタイプは、IPv4 互換 IPv6 アドレスです。IPv6 移行メカニズムには、IPv4 ルーティングインフラストラクチャ上で IPv6 パケットを動的にトンネリングさせるためのホストおよびルータの技術が実装されています。この技術を使用する IPv6 ノードには、低次 32 ビットでグローバル IPv4 アドレスを伝送する特別な IPv6 ユニキャスト アドレスが割り当てられます。このタイプのアドレスは「IPv4 互換 IPv6 アドレス」と呼ばれ、形式は ::y.y.y.y です。この y.y.y.y は IPv4 ユニキャスト アドレスになります。

（注） 「IPv4 互換 IPv6 アドレス」で使用する IPv4 アドレスは、グローバルに固有な IPv4 ユニキャスト アドレスである必要があります。

2 つ目のタイプの IPv6 アドレスは、IPv4 アドレスが埋め込まれたもので、「IPv4 マッピング IPv6 アドレス」と呼ばれます。このアドレス タイプは、IPv4 ノードのアドレスを IPv6 アドレスとして表すために使用されます。このタイプのアドレス形式は ::FFFF:y.y.y.y です。ここで、y.y.y.y は IPv4 ユニキャスト アドレスです。

未指定アドレス

未指定アドレス 0:0:0:0:0:0:0:0 は、IPv6 アドレスがないことを示しています。たとえば、IPv6 ネットワーク上で新しく初期化されたノードは、IPv6 アドレスを受信するまで、パケットで未指定アドレスを送信元アドレスとして使用できます。

（注）　IPv6 未指定アドレスは、インターフェイスに割り当てることができません。未指定 IPv6 アドレスを IPv6 パケットまたは IPv6 ルーティング ヘッダーで宛先アドレスとして使用することはできません。

ループバック アドレス

ループバック アドレス 0:0:0:0:0:0:0:1 は、ノードが IPv6 パケットをそれ自体に送信するために使用できます。IPv6 のループバック アドレスは、IPv4 のループバック アドレス（127.0.0.1）と同じように機能します。

（注）　IPv6 ループバック アドレスは、物理インターフェイスに割り当てることができません。IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットは、そのパケットを作成したノード内に留まっている必要があります。IPv6 ルータは、IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットを転送しません。

インターフェイス識別子

IPv6 ユニキャスト アドレス内のインターフェイス識別子は、リンク上でインターフェイスを識別するために使用されます。これらの識別子は、サブネット プレフィックス内で固有である必要があります。多くの場合、インターフェイス識別子はインターフェイス リンク層アドレスから導出されます。各インターフェイスが異なるサブネットに接続されていれば、単一ノードの複数のインターフェイスで同一のインターフェイス識別子を使用することもできます。

バイナリ 000 で始まるものを除くすべてのユニキャスト アドレスで、インターフェイス識別子は、64 ビットの長さで Modified EUI-64 形式で構築されている必要があります。Modified EUI-64 形式は、アドレス内のユニバーサル/ローカル ビットを逆にし、MAC アドレスの上の 3 つのバイトと下の 3 つのバイトの間に 16 進数 FFFE を挿入することによって、48 ビット MAC アドレスから作成されます。

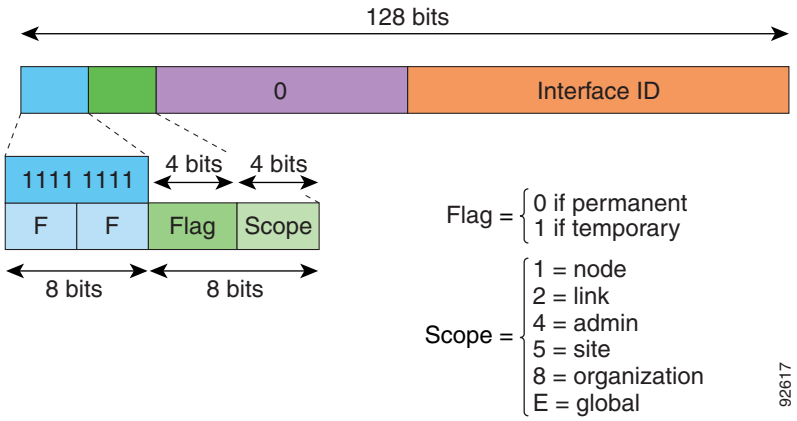
たとえば、MAC アドレスが 00E0.b601.3B7A のインターフェイスの場合、64 ビット インターフェイス ID は 02E0:B6FF:FE01:3B7A になります。

マルチキャスト アドレス

IPv6 マルチキャスト アドレスは、通常は異なるノード上にある、インターフェイスのグループの識別子です。マルチキャスト アドレスに送信されたパケットは、マルチキャスト アドレスが示すすべてのインターフェイスに配信されます。1 つのインターフェイスが任意の数のマルチキャスト グループに属すことができます。

IPv6 マルチキャスト アドレスのプレフィックスは FF00::/8（1111 1111）です。オクテットとそれに続くプレフィックスは、マルチキャスト アドレスのタイプとスコープを定義します。永続的に割り当てられた（周知の）マルチキャスト アドレスには、0 に等しいフラグ パラメータがあり、一時的な（過渡）マルチキャスト アドレスには 1 に等しいフラグ パラメータがあります。ノード、リンク、サイト、組織のスコープ、またはグローバル スコープを持つマルチキャスト アドレスのスコープ パラメータは、それぞれ 1、2、5、8、または E です。たとえば、プレフィックスが FF02::/16 のマルチキャスト アドレスは、リンク スコープを持つ永続マルチキャスト アドレスです。図 43-1に、IPv6 マルチキャスト アドレスの形式を示します。

図 43-1　　IPv6 マルチキャスト アドレス形式



IPv6 ノード（ホストとルータ）は、次のマルチキャスト グループに参加する必要があります。

- All Nodes マルチキャスト アドレス：
  - FF01::（インターフェイスローカル）
  - FF02::（リンクローカル）
- ノード FF02:0:0:0:0:1:FFXX:XXXX/104 上の各 IPv6 ユニキャスト アドレスおよびエニーキャスト アドレスの送信要求ノード アドレス。ここで、XX:XXXX は低次 24 ビットのユニキャスト アドレスまたはエニーキャスト アドレスです。

（注） 送信要求ノード アドレスは、ネイバー送信要求メッセージで使用されます。

IPv6 ルータは、次のマルチキャスト グループに参加する必要があります。

- FF01::2（インターフェイスローカル）
- FF02::2（リンクローカル）
- FF05::2（サイトローカル）

マルチキャスト アドレスは、IPv6 パケットで送信元アドレスとして使用できません。

（注） IPv6 にはブロードキャスト アドレスはありません。ブロードキャスト アドレスの代わりに IPv6 マルチキャスト アドレスが使用されます。

エニーキャスト アドレス

IPv6 エニーキャスト アドレスは、複数のインターフェイス（通常は異なるノードに属す）に割り当てられたユニキャスト アドレスです。エニーキャスト アドレスにルーティングされたパケットは、そのアドレスを持ち、有効なルーティング プロトコルによって最も近いと判別されたインターフェイスにルーティングされます。

エニーキャスト アドレスは、ユニキャスト アドレス空間から割り当てられます。エニーキャスト アドレスは、複数のインターフェイスに割り当てられたユニキャスト アドレスにすぎません。インターフェイスは、アドレスをエニーキャスト アドレスとして認識するように設定されている必要があります。

エニーキャスト アドレスには次の制限が適用されます。

- エニーキャスト アドレスは、IPv6 パケットの送信元アドレスとして使用できません。
- エニーキャスト アドレスは、IPv6 ホストに割り当てることはできません。IPv6 ルータにだけ割り当てるこができます。

（注）　エニーキャスト アドレスは、ASA ではサポートされていません。

必須アドレス

IPv6 ホストには、少なくとも次のアドレスが（自動または手動で）設定されている必要があります。

- 各インターフェイスのリンクローカル アドレス
- ループバック アドレス
- All-Nodes マルチキャスト アドレス
- 各ユニキャスト アドレスまたはエニーキャスト アドレスの送信要求ノード マルチキャスト アドレス

IPv6 ルータには、少なくとも次のアドレスが（自動または手動で）設定されている必要があります。

- 必須ホスト アドレス
- このルータがルータとして動作するように設定されているすべてのインターフェイスのサブネットルータ エニーキャスト アドレス
- All-Routers マルチキャスト アドレス

IPv6 アドレス プレフィックス

ipv6-prefix/prefix-length 形式の IPv6 アドレス プレフィックスを使用すると、アドレス空間全体のビット単位の連続ブロックを表現できます。IPv6-prefix は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス（アドレスのネットワーク部分）を構成しているかを指定する 10 進数値です。たとえば、2001:0DB8:8086:6502::/32 は有効な IPv6 プレフィックスです。

IPv6 プレフィックスは、IPv6 アドレスのタイプを特定します。表 43-5 に、各 IPv6 アドレス タイプのプレフィックスを示します。

表 43-5　IPv6 アドレス タイプのプレフィックス

アドレス タイプ	バイナリ プレフィックス	IPv6 表記
未指定	000...0（128 ビット）	::/128
ループバック	000...1（128 ビット）	::1/128
マルチキャスト	11111111	FF00::/8
リンクローカル（ユニキャスト）	1111111010	FE80::/10
サイトローカル（ユニキャスト）	1111111111	FEC0::/10

表 43-5　IPv6 アドレス タイプのプレフィックス （続き）

アドレス タイプ	バイナリ プレフィックス	IPv6 表記
グローバル（ユニキャスト）	その他すべてのアドレス。	
エニーキャスト	ユニキャスト アドレス空間から取得。	

プロトコルとアプリケーション

表 43-6 に、プロトコルのリテラル値とポート番号を示します。いずれも ASA のコマンドで入力できます。

表 43-6　プロトコルのリテラル値

リテラル	値	説明
ah	51	IPv6 の認証ヘッダー（RFC 1826）。
eigrp	88	Enhanced Interior Gateway Routing Protocol（Enhanced IGRP）。
esp	50	IPv6 の暗号ペイロード（RFC 1827）。
gre	47	総称ルーティング カプセル化。
icmp	1	インターネット制御メッセージ プロトコル（RPC 792）。
icmp6	58	IPv6 のインターネット制御メッセージ プロトコル（RFC 2463）。
igmp	2	インターネット グループ管理プロトコル（RFC 1112）。
igrp	9	Interior Gateway Routing Protocol。
ip	0	インターネット プロトコル。
ipinip	4	IP-in-IP カプセル化。
ipsec	50	IP セキュリティ。ipsec プロトコル リテラルを入力すると、esp プロトコル リテラルを入力した場合と同じ結果が得られます。
nos	94	ネットワーク オペレーティング システム（Novell の NetWare）。
ospf	89	OSPF ルーティング プロトコル（RFC 1247）。
pcp	108	ペイロード圧縮プロトコル。
pim	103	プロトコル独立型マルチキャスト。
pptp	47	ポイントツーポイント トンネリング プロトコル。pptp プロトコル リテラルを入力すると、gre プロトコル リテラルを入力した場合と同じ結果が得られます。
snp	109	Sitara Networks Protocol。
tcp	6	伝送制御プロトコル（RFC 793）。
udp	17	ユーザ データグラム プロトコル（RFC 768）。

IANA の Web サイトでオンラインでプロトコル番号を確認できます。

http://www.iana.org/assignments/protocol-numbers

TCP ポートと UDP ポート

表 43-7 に、リテラル値とポート番号を示します。いずれも ASA のコマンドで入力できます。次の警告を参照してください。

- ASA は、SQL*Net 用にポート 1521 を使用します。これは、Oracle が SQL*Net に使用するデフォルトのポートです。ただし、この値は IANA ポート割り当てとは一致しません。
- ASA は、ポート 1645 と 1646 で RADIUS をリスンしています。RADIUS サーバが標準ポート 1812 と 1813 を使用している場合は、**authentication-port** コマンドと **accounting-port** コマンドを使用して、それらのポートでリスンするように ASA を設定できます。
- DNS アクセスにポートを割り当てるには、**dns** ではなく **domain** リテラル値を使用します。**dns** を使用した場合、ASA では、**dnsix** リテラル値を使用すると見なされます。

IANA の Web サイトでオンラインでポート番号を確認できます。

http://www.iana.org/assignments/port-numbers

表 43-7　　ポートのリテラル値

リテラル	TCP または UDP?	値	説明
aol	TCP	5190	America Online
bgp	TCP	179	ボーダー ゲートウェイ プロトコル（RFC 1163）
biff	UDP	512	新しいメールの受信をユーザに通知するために、メール システムが使用
bootpc	UDP	68	ブートストラップ プロトコル クライアント
bootps	UDP	67	ブートストラップ プロトコル サーバ
chargen	TCP	19	キャラクタ ジェネレータ
citrix-ica	TCP	1494	Citrix Independent Computing Architecture（ICA）プロトコル
cmd	TCP	514	**cmd** は自動認証機能がある点を除いて、**exec** と同様
ctiqbe	TCP	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	TCP	13	Day time（日時）（RFC 867）
discard	TCP、UDP	9	廃棄
domain	TCP、UDP	53	DNS
dnsix	UDP	195	DNSIX Session Management Module Audit Redirector
echo	TCP、UDP	7	Echo
exec	TCP	512	リモート プロセスの実行
finger	TCP	79	Finger
ftp	TCP	21	ファイル転送プロトコル（コンソール ポート）
ftp-data	TCP	20	ファイル転送プロトコル（データ ポート）
gopher	TCP	70	Gopher

表 43-7　　ポートのリテラル値 （続き）

リテラル	TCP または UDP?	値	説明
https	TCP	443	HTTP over SSL
h323	TCP	1720	H.323 発呼信号
hostname	TCP	101	NIC ホスト ネーム サーバ
ident	TCP	113	ID 認証サービス
imap4	TCP	143	Internet Message Access Protocol バージョン 4
irc	TCP	194	インターネット リレー チャット プロトコル
isakmp	UDP	500	Internet Security Association and Key Management Protocol
kerberos	TCP、UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn シェル
ldap	TCP	389	Lightweight Directory Access Protocol。
ldaps	TCP	636	ライトウェイト ディレクトリ アクセス プロトコル（SSL）
lpd	TCP	515	ライン プリンタ デーモン（プリンタ スプーラー）
login	TCP	513	リモート ログイン
lotusnotes	TCP	1352	IBM Lotus Notes
mobile-ip	UDP	434	モバイル IP-Agent
nameserver	UDP	42	ホスト ネーム サーバ
netbios-ns	UDP	137	NetBIOS ネーム サービス
netbios-dgm	UDP	138	NetBIOS データグラム サービス
netbios-ssn	TCP	139	NetBIOS セッション サービス
nntp	TCP	119	Network News Transfer Protocol
ntp	UDP	123	ネットワーク タイム プロトコル
pcanywhere-status	UDP	5632	pcAnywhere ステータス
pcanywhere-data	TCP	5631	pcAnywhere データ
pim-auto-rp	TCP、UDP	496	Protocol Independent Multicast、逆パス フラッド、デンス モード
pop2	TCP	109	Post Office Protocol（POP）Version 2
pop3	TCP	110	Post Office Protocol - Version 3
pptp	TCP	1723	ポイントツーポイント トンネリング プロトコル
radius	UDP	1645	リモート認証ダイヤルイン ユーザ サービス
radius-acct	UDP	1646	リモート認証ダイヤルイン ユーザ サービス（アカウンティング）
rip	UDP	520	ルーティング情報プロトコル
secureid-udp	UDP	5510	SecureID over UDP

表 43-7　　ポートのリテラル値 （続き）

リテラル	TCP または UDP?	値	説明
smtp	TCP	25	シンプル メール転送プロトコル
snmp	UDP	161	簡易ネットワーク管理プロトコル
snmptrap	UDP	162	簡易ネットワーク管理プロトコル（トラップ）
sqlnet	TCP	1521	構造化照会言語ネットワーク
ssh	TCP	22	セキュア シェル
sunrpc (rpc)	TCP、UDP	111	Sun Remote Procedure Call
syslog	UDP	514	システム ログ
tacacs	TCP、UDP	49	Terminal Access Controller Access Control System Plus
talk	TCP、UDP	517	Talk
Telnet	TCP	23	Telnet（RFC 854）
tftp	UDP	69	Trivial File Transfer Protocol
time	UDP	37	時刻
uucp	TCP	540	UNIX 間コピー プログラム
who	UDP	513	Who
whois	TCP	43	Who Is
www	TCP	80	ワールドワイド ウェブ
xdmcp	UDP	177	X Display Manager Control Protocol

ローカル ポートとプロトコル

表 43-8 に、ASA に向かうトラフィックを処理するために ASA が開くプロトコル、TCP ポート、および UDP ポートを示します。表 43-8 に記載されている機能とサービスをイネーブルにしない限り、ASA は、TCP または UDP ポートでローカル プロトコルを*開きません*。ASA がデフォルトのリスニング プロトコルまたはポートを開くように機能またはサービスを設定する必要があります。多くの場合、機能またはサービスをイネーブルにすると、デフォルト ポート以外のポートを設定できます。

表 43-8　　機能とサービスによって開かれるプロトコルとポート

機能またはサービス	プロトコル	Port Number	注
DHCP	UDP	67、68	—
フェールオーバー制御	105	該当なし	—
HTTP	TCP	80	—
HTTPS	TCP	443	—
ICMP	1	該当なし	—
IGMP	2	該当なし	プロトコルは宛先 IP アドレス 224.0.0.1 でだけ開かれます

表 43-8　機能とサービスによって開かれるプロトコルとポート （続き）

機能またはサービス	プロトコル	Port Number	注
ISAKMP/IKE	UDP	500	設定可能。
IPsec（ESP）	50	該当なし	—
IPsec over UDP（NAT-T）	UDP	4500	—
IPsec over UDP（Cisco VPN 3000 シリーズ互換）	UDP	10000	設定可能。
IPsec over TCP（CTCP）	TCP	—	デフォルト ポートは使用されません。IPsec over TCP の設定時にポート番号を指定する必要があります。
NTP	UDP	123	—
OSPF	89	該当なし	プロトコルは宛先 IP アドレス 224.0.0.5 および 224.0.0.6 でだけ開かれます
PIM	103	該当なし	プロトコルは宛先 IP アドレス 224.0.0.13 でだけ開かれます
RIP	UDP	520	—
RIPv2	UDP	520	ポートは宛先 IP アドレス 224.0.0.9 でだけ開かれます
SNMP	UDP	161	設定可能。
SSH	TCP	22	—
ステートフル アップデート	8（ノンセキュア）9（セキュア）	該当なし	—
Telnet	TCP	23	—
VPN ロード バランシング	UDP	9023	設定可能。
VPN 個別ユーザ認証プロキシ	UDP	1645、1646	ポートは VPN トンネルでだけアクセスできます。

ICMP タイプ

表 43-9 に、ASA のコマンドで入力できる ICMP タイプの番号と名前を示します。

表 43-9　ICMP タイプ

ICMP 番号	ICMP 名
0	echo-reply
3	unreachable
4	source-quench
5	redirect

表 43-9　ICMP タイプ（続き）

ICMP 番号	ICMP 名
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect