Cisco ASA シリーズ CLI 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 9.3

リリース日：2014 年 7 月 24 日
更新日：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

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

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

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）
Copyright © 2014 Cisco Systems, Inc. All rights reserved.

このマニュアルについて xxix
マニュアルの目的 xxix
関連資料 xxix
表記法 xxx
マニュアルの入手方法およびテクニカル サポート xxxi

PART 1 ASA の開始

CHAPTER 1 Cisco ASA の概要 1-1
ハードウェアとソフトウェアの互換性 1-1
VPN の互換性 1-2
新機能 1-2
ASA 9.3(1) の新機能 1-2
スイッチにおける ASA サービス モジュールの動作 1-6
ファイアウォール機能の概要 1-8
セキュリティ ポリシーの概要 1-9
ファイアウォール モードの概要 1-11
ステートフル インスペクションの概要 1-12
VPN 機能の概要 1-13
セキュリティ コンテキストの概要 1-14
ASA クラスタリングの概要 1-14
特殊なレガシー サービス 1-14
特殊なサービスに関するガイド 1-15
レガシー サービス ガイド 1-15

CHAPTER 2 使用する前に 2-1
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 2-1
アプライアンス コンソールへのアクセス 2-2
ASA サービス モジュール コンソールへのアクセス 2-3
ASDM アクセスの設定 2-7
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した ASDM アクセス（アプライアンス、ASAv） 2-8
アプライアンスおよび ASAv の ASDM アクセスのカスタマイズ 2-8

ASA サービス モジュールの ASDM アクセスの設定 2-10
ASDM の起動 2-13
工場出荷時のデフォルト コンフィギュレーション 2-14
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 2-15
ASAv 導入設定の復元 2-16
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 2-16
ASAv の導入設定 2-17
コンフィギュレーションの処理 2-18
コンフィギュレーションの変更の保存 2-18
実行コンフィギュレーションへのスタートアップ コンフィギュレーションのコピー 2-20
コンフィギュレーションの表示 2-21
コンフィギュレーション設定のクリアと削除 2-21
オフラインでのテキスト コンフィギュレーション ファイルの作成 2-22
接続に対するコンフィギュレーションの変更の適用 2-22
ASA のリロード 2-23

CHAPTER 3 **Cisco ASA サービス モジュール向けのスイッチの設定 3-1**
スイッチに関する情報 3-1
サポートされているスイッチ ハードウェアおよびソフトウェア 3-1
バックプレーン接続 3-2
ASA と Cisco IOS 機能の相互作用 3-2
SVI に関する情報 3-2
ガイドラインと制限事項 3-3
モジュールの搭載確認 3-4
ASA サービス モジュールへの VLAN の割り当て 3-5
直接接続されたルータ（SVI）としての MSFC の使用 3-7
ASA フェールオーバーのスイッチの設定 3-9
セカンダリ ASA サービス モジュール への VLAN の割り当て 3-9
プライマリ スイッチとセカンダリ スイッチ間のトランクの追加 3-9
トランスペアレント ファイアウォール モードとの両立 3-9
高速リンク障害検出のための自動ステート メッセージングのイネーブル化 3-9
ASA サービス モジュールのリセット 3-10
ASA サービス モジュールのモニタリング 3-11
ASA サービス モジュールを使用するためのスイッチの機能履歴 3-13

CHAPTER 4 **機能ライセンス 4-1**
モデルごとにサポートされている機能のライセンス 4-1

モデルごとのライセンス 4-2
ライセンスの注釈 4-15
VPN ライセンスと機能の互換性 4-20
機能のライセンスに関する情報 4-21
事前インストールされているライセンス 4-21
永続ライセンス 4-21
時間ベース ライセンス 4-22
AnyConnect Premium（共有）ライセンス 4-25
フェールオーバーまたは ASA クラスタ ライセンス 4-28
ペイロード暗号化機能のないモデル 4-31
ライセンスの FAQ 4-32
ガイドラインと制限事項 4-33
ライセンスの設定 4-34
アクティベーション キーの取得 4-34
キーのアクティブ化および非アクティブ化 4-35
共有ライセンスの設定 4-37
ライセンスのモニタリング 4-40
現在のライセンスの表示 4-40
共有ライセンスのモニタリング 4-51
ライセンスの機能履歴 4-53

CHAPTER 5 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 5-1
ファイアウォール モードに関する情報 5-1
ルーテッド ファイアウォール モードに関する情報 5-2
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 5-2
ファイアウォール モードのライセンス要件 5-8
デフォルト設定 5-8
ガイドラインと制限事項 5-8
ファイアウォール モードの設定 5-10
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 5-11
ARP インスペクションの設定のタスク フロー 5-11
スタティック ARP エントリの追加 5-11
ARP インスペクションのイネーブル化 5-12
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 5-13
トランスペアレント ファイアウォールのモニタリング 5-14
ARP インスペクションのモニタリング 5-14
MAC アドレス テーブルのモニタリング 5-14

ファイアウォール モードの例 5-15
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 5-15
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 5-21
ファイアウォール モードの機能履歴 5-26

PART 2 ハイ アベイラビリティとスケーラビリティ

CHAPTER 6 マルチ コンテキスト モード 6-1
セキュリティ コンテキストに関する情報 6-1
セキュリティ コンテキストの一般的な使用方法 6-2
コンテキスト コンフィギュレーション ファイル 6-2
ASA によるパケットの分類方法 6-3
セキュリティ コンテキストのカスケード接続 6-7
セキュリティ コンテキストへの管理アクセス 6-7
リソース管理に関する情報 6-8
MAC アドレスに関する情報 6-12
マルチ コンテキスト モードのライセンス要件 6-14
前提条件 6-14
ガイドラインと制限事項 6-14
デフォルト設定 6-15
マルチ コンテキストの設定 6-16
マルチ コンテキスト モードの設定のタスク フロー 6-16
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 6-16
リソース管理のクラスの設定 6-18
セキュリティ コンテキストの設定 6-21
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 6-26
コンテキストとシステム実行スペースの切り替え 6-26
セキュリティ コンテキストの管理 6-27
セキュリティ コンテキストの削除 6-27
管理コンテキストの変更 6-28
セキュリティ コンテキスト URL の変更 6-28
セキュリティ コンテキストのリロード 6-30
セキュリティ コンテキストのモニタリング 6-31
コンテキスト情報の表示 6-31
リソース割り当ての表示 6-32
リソースの使用状況の表示 6-36
コンテキストでの SYN 攻撃のモニタリング 6-38
割り当てられた MAC アドレスの表示 6-40

マルチ コンテキスト モードの設定例 6-42
マルチ コンテキスト モードの機能履歴 6-43

CHAPTER 7 ハイ アベイラビリティのためのフェールオーバー 7-1
フェールオーバーについて 7-1
フェールオーバーの概要 7-2
フェールオーバーのシステム要件 7-2
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 7-3
MAC アドレスと IP アドレス 7-9
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 7-9
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 7-13
トランスペアレント ファイアウォール モードの要件 7-16
フェールオーバー ヘルスのモニタリング 7-17
フェールオーバー時間 7-19
コンフィギュレーション同期 7-20
アクティブ / スタンバイ フェールオーバーについて 7-22
アクティブ / アクティブ フェールオーバーについて 7-24
フェールオーバーのライセンス 7-27
フェールオーバーの前提条件 7-28
フェールオーバーのガイドライン 7-28
フェールオーバーのデフォルト 7-29
アクティブ / スタンバイ フェールオーバーの設定 7-29
アクティブ / スタンバイ フェールオーバーのプライマリ装置の設定 7-29
アクティブ / スタンバイ フェールオーバーのセカンダリ装置の設定 7-33
アクティブ / アクティブ フェールオーバーの設定 7-34
アクティブ / アクティブ フェールオーバーのプライマリ装置の設定 7-34
アクティブ / アクティブ フェールオーバーのセカンダリ装置の設定 7-38
オプションのフェールオーバー パラメータの設定 7-39
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 7-39
インターフェイス モニタリングの設定 7-42
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） 7-43
フェールオーバーの管理 7-47
リモート コマンドの実行 7-50
コマンドの送信 7-51
コマンド モードの変更 7-51
セキュリティの考慮事項 7-53
リモート コマンドの実行に関する制限事項 7-53

フェールオーバー動作のモニタ 7-53
フェールオーバー メッセージ 7-54
フェールオーバー動作のモニタ 7-55
フェールオーバーの機能履歴 7-55

CHAPTER 8 **ASA クラスタ 8-1**
ASA クラスタリングについて 8-1
ASA クラスタをネットワークに適合させる方法 8-2
パフォーマンス スケーリング係数 8-2
クラスタ メンバ 8-3
クラスタ インターフェイス 8-4
クラスタ制御リンク 8-6
ASA クラスタ内のハイ アベイラビリティ 8-9
コンフィギュレーションの複製 8-12
ASA クラスタ管理 8-12
ロード バランシングの方式 8-14
サイト間クラスタリング 8-19
ASA クラスタが接続を管理する方法 8-23
ASA の機能とクラスタリング 8-25
ASA クラスタリングのライセンス 8-32
ASA クラスタリングの前提条件 8-33
ASA クラスタリングのガイドライン 8-34
ASA クラスタリングのデフォルト 8-38
ASA クラスタリングの設定 8-38
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 8-39
各ユニットでのクラスタ インターフェイス モードの設定 8-41
マスター ユニットでのインターフェイスの設定 8-42
マスター ユニットのブートストラップの設定 8-49
スレーブ ユニットのブートストラップの設定 8-56
ASA クラスタ メンバの管理 8-58
非アクティブなメンバーになる 8-58
メンバの非アクティブ化 8-59
クラスタからの脱退 8-60
マスター ユニットの変更 8-61
クラスタ全体でのコマンドの実行 8-62
ASA クラスタのモニタリング 8-63
クラスタの状態のモニタリング 8-63
クラスタ全体のパケットのキャプチャ 8-64

クラスタ リソースのモニタリング 8-64
クラスタ トラフィックのモニタリング 8-65
クラスタのルーティングのモニタリング 8-67
クラスタリングのロギングの設定 8-67
クラスタのインターフェイスのモニタリング 8-68
クラスタリングのデバッグ 8-68
ASA クラスタリングの例 8-68
ASA およびスイッチのコンフィギュレーションの例 8-69
Firewall on a Stick 8-71
トラフィックの分離 8-73
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） 8-75
ASA クラスタリングの履歴 8-81

PART 3 インターフェイス

CHAPTER 9 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） 9-1
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 9-2
Auto-MDI/MDIX 機能 9-2
トランスペアレント モードのインターフェイス 9-2
管理インターフェイス 9-2
冗長インターフェイス 9-5
EtherChannel 9-5
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 9-8
ASA 5512-X 以降のインターフェイスのライセンス要件 9-10
ガイドラインと制限事項 9-12
デフォルト設定 9-14
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） 9-15
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 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 9-16
冗長インターフェイスの設定 9-19
EtherChannel の設定 9-21
VLAN サブインターフェイスと 802.1Q トランキングの設定 9-26
ジャンボ フレーム サポートのイネーブル化 9-28
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 9-29

インターフェイスのモニタリング 9-39
ASA 5512-X 以降のインターフェイスの設定例 9-39
物理インターフェイス パラメータの例 9-40
サブインターフェイス パラメータの例 9-40
マルチ コンテキスト モードの例 9-40
EtherChannel の例 9-40
次の作業 9-41
ASA 5512-X 以降のインターフェイスの機能履歴 9-41

CHAPTER 10 基本インターフェイスの設定（ASAv） 10-1
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 10-1
ASAv インターフェイスおよび仮想 NIC 10-2
トランスペアレント モードのインターフェイス 10-3
管理インターフェイス 10-3
冗長インターフェイス 10-4
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 10-5
ASAv インターフェイスのライセンス要件 10-7
ガイドラインと制限事項 10-8
デフォルト設定 10-8
インターフェイス コンフィギュレーションの開始（ASAv） 10-9
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 10-9
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 10-10
冗長インターフェイスの設定 10-12
VLAN サブインターフェイスと 802.1Q トランキングの設定 10-14
ジャンボ フレーム サポートのイネーブル化 10-15
インターフェイスのモニタリング 10-17
ASAv インターフェイスの設定例 10-17
物理インターフェイス パラメータの例 10-17
サブインターフェイス パラメータの例 10-17
次の作業 10-17
ASAv インターフェイスの機能履歴 10-17

CHAPTER 11 ルーテッド モードのインターフェイス 11-1
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 11-1
セキュリティ レベル 11-1

デュアル IP スタック（IPv4 および IPv6） 11-2
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 11-3
ガイドラインと制限事項 11-4
デフォルト設定 11-5
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 11-6
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 11-6
一般的なインターフェイス パラメータの設定 11-6
MAC アドレス、MTU、TCP MSS の設定 11-10
IPv6 アドレッシングの設定 11-12
同じセキュリティ レベルの通信の許可 11-16
インターフェイスのオン / オフ 11-18
インターフェイスのモニタリング 11-18
ルーテッド モードのインターフェイスの機能履歴 11-19

CHAPTER 12 トランスペアレント モードのインターフェイス 12-1
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 12-1
トランスペアレント モードのブリッジ グループ 12-2
セキュリティ レベル 12-2
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 12-3
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 12-5
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 12-6
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 12-7
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 12-7
ブリッジ グループの設定 12-8
一般的なインターフェイス パラメータの設定 12-9
管理インターフェイスの設定（ASA 5512-X 以降および ASAv） 12-11
MAC アドレス、MTU、TCP MSS の設定 12-13
IPv6 アドレッシングの設定 12-16
同じセキュリティ レベルの通信の許可 12-19
インターフェイスのオン / オフ 12-20
インターフェイスのモニタリング 12-21
トランスペアレント モードのインターフェイスの設定例 12-21
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 12-22

PART 4 基本設定

CHAPTER 13 基本設定 13-1
ホスト名、ドメイン名、イネーブル パスワード、Telnet パスワードの設定 13-1
イネーブル パスワードと Telnet パスワードの回復 13-3
ASA のパスワードの回復 13-3
ASA 5506、5506-W および ASA 5508 のパスワードの回復 13-5
ASAv のパスワードまたはイメージの回復 13-6
パスワード回復のディセーブル化 13-7
日時の設定 13-8
タイム ゾーンと夏時間の設定 13-8
NTP サーバを使用した日付と時刻の設定 13-9
手動での日付と時刻の設定 13-11
マスター パスフレーズの設定 13-11
マスター パスフレーズの追加または変更 13-12
マスター パスフレーズの無効化 13-14
マスター パスフレーズの削除 13-15
DNS サーバの設定 13-15
DNS サーバの設定 13-15
DNS キャッシュのモニタリング 13-16
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 13-17
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 13-17
ASP ロード バランシングのイネーブル化 13-18
基本設定の履歴 13-19

CHAPTER 14 ダイナミック DNS 14-1
DDNS について 14-1
DDNS アップデート コンフィギュレーション 14-1
UDP Packet Size 14-2
DDNS のガイドライン 14-2
DDNS の設定 14-2
スタティック IP アドレスの A RR と PTR RR の両方のアップデート 14-2
A RR と PTR RR の両方のアップデート 14-3
両方の RR へのアップデートを無視 14-4
PTR RR のみのアップデート 14-5
RR のクライアントによるアップデートと PTR RR のサーバによるアップデート 14-6
DDNS のモニタリング 14-7

DDNS の履歴 14-8

CHAPTER 15 DHCP サービス 15-1
DHCP サーバについて 15-1
DHCP リレー エージェントについて 15-2
DHCP サービスのライセンス要件 15-2
DHCP サービスのガイドライン 15-3
DHCP サーバの設定 15-4
DHCP サーバのイネーブル化 15-5
高度な DHCP オプションの設定 15-6
IP アドレスを返す 15-7
テキスト文字列を返す 15-7
16 進数値を返す 15-7
DHCP サーバによる Cisco IP Phone の設定 15-8
DHCPv4 リレー エージェントの設定 15-10
DHCPv6 リレー エージェントの設定 15-12
DHCP サービスのモニタリング 15-13
DHCP サービスの履歴 15-13

PART 5 オブジェクトと ACL

CHAPTER 16 アクセス コントロールのオブジェクト 16-1
オブジェクトのガイドライン 16-1
オブジェクトの設定 16-2
ネットワーク オブジェクトとグループの設定 16-2
サービス オブジェクトとサービス グループの設定 16-4
ローカル ユーザ グループの設定 16-7
セキュリティ グループ オブジェクト グループの設定 16-9
時間範囲の設定 16-10
オブジェクトのモニタリング 16-11
オブジェクトの履歴 16-12

CHAPTER 17 アクセス コントロール リスト 17-1
ACL について 17-1
ACL タイプ 17-1
ACL 名 17-3
ACE の順序 17-3
許可 / 拒否と 一致 / 不一致の比較 17-3

アクセス コントロールによる暗黙的な拒否 17-4
NAT 使用時に拡張 ACL で使用する IP アドレス 17-4
時間ベース ACE 17-5
ACL のガイドライン 17-5
ACL の設定 17-6
基本的な ACL 設定および管理オプション 17-6
拡張 ACL の設定 17-7
標準 ACL の設定 17-14
Webtype ACL の設定 17-15
EtherType ACL の設定 17-19
ACL のモニタリング 17-20
ACL の履歴 17-20

PART 6 IP ルーティング

CHAPTER 18 ルーティングの概要 18-1
ルーティングについて 18-1
スイッチング 18-1
パス判別 18-2
サポートされるルート タイプ 18-2
ASA 内でのルーティングの仕組み 18-4
出力インターフェイスの選択プロセス 18-4
ネクスト ホップの選択プロセス 18-5
ルーティングにサポートされているインターネット プロトコル 18-5
ルーティング テーブルについて 18-6
ルーティング テーブルの表示 18-6
ルーティング テーブルへの入力方法 18-7
転送の決定方法 18-9
ダイナミック ルーティングとフェールオーバー 18-10
ダイナミック ルーティングとクラスタリング 18-10
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 18-12
プロキシ ARP 要求のディセーブル化 18-13

CHAPTER 19 スタティック ルートとデフォルト ルート 19-1
スタティック ルートとデフォルト ルートについて 19-1
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 19-2
スタティック ルートの設定 19-2
スタティック null0 ルートの設定 19-3

デフォルト スタティック ルートの設定 19-4
デフォルト スタティック ルートの設定の制限事項 19-4
IPv6 デフォルト ルートおよびスタティック ルートの設定 19-5
スタティック ルートまたはデフォルト ルートのモニタ 19-6
スタティック ルートまたはデフォルト ルートの例 19-8
スタティック ルートおよびデフォルト ルートの履歴 19-9

CHAPTER 20 ルート マップ 20-1
ルート マップについて 20-1
permit 句と deny 句 20-2
match 句と set 句の値 20-2
BGP match 句および BGP set 句 20-3
ルート マップのガイドライン 20-4
ルート マップの定義 20-4
ルート マップのカスタマイズ 20-5
特定の宛先アドレスに一致するルートの定義 20-5
ルート アクションのメトリック値の設定 20-6
ルート マップの設定例 20-7
ルート マップの機能履歴 20-7

CHAPTER 21 BGP 21-1
BGP について 21-1
BGP を使用する状況 21-1
ルーティング テーブルの変更 21-2
BGP パスの選択 21-3
BGP のガイドライン 21-3
BGP の設定 21-4
BGP のイネーブル化 21-4
BGP ルーティング プロセスの最適なパスの定義 21-6
ポリシー リストの設定 21-7
AS パス フィルタの設定 21-8
コミュニティ ルールの設定 21-8
IPv4 アドレス ファミリの設定 21-9
BGP のモニタリング 21-21
BGP の設定例 21-23
BGP の履歴 21-24

CHAPTER 22 OSPF 22-1

OSPF について 22-1
fast hello パケットに対する OSPF のサポート 22-3
OSPFv2 および OSPFv3 間の実装の差異 22-4
OSPF のガイドライン 22-5
OSPFv2 の設定 22-7
OSPF fast hello パケットの設定 22-8
OSPFv2 のカスタマイズ 22-8
OSPFv2 へのルートの再配布 22-9
OSPFv2 にルートを再配布する場合のルート集約の設定 22-10
OSPFv2 エリア間のルート集約の設定 22-11
OSPFv2 インターフェイス パラメータの設定 22-12
OSPFv2 エリア パラメータの設定 22-15
OSPFv2 NSSA の設定 22-16
クラスタリングの IP アドレス プールの設定（OSPFv2 および OSPFv3） 22-17
スタティック OSPFv2 ネイバーの定義 22-18
ルート計算タイマーの設定 22-19
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 22-19
OSPFv3 の設定 22-20
OSPFv3 のイネーブル化 22-21
OSPFv3 インターフェイスのパラメータの設定 22-21
OSPFv3 ルータ パラメータの設定 22-27
OSPFv3 エリア パラメータの設定 22-29
OSPFv3 パッシブ インターフェイスの設定 22-32
OSPFv3 アドミニストレーティブ ディスタンスの設定 22-32
OSPFv3 タイマーの設定 22-33
スタティック OSPFv3 ネイバーの定義 22-36
OSPFv3 デフォルト パラメータのリセット 22-37
syslog メッセージの送信 22-38
syslog メッセージの抑止 22-38
サマリー ルート コストの計算 22-39
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 22-39
IPv6 サマリー プレフィックスの設定 22-40
IPv6 ルートの再配布 22-40
グレースフル リスタートの設定 22-42
機能の設定 22-42
OSPFv2 のグレースフル リスタートの設定 22-43
OSPFv3 のグレースフル リスタートの設定 22-44
OSPF 設定の削除 22-45

OSPFv2 の設定例 22-46
OSPFv3 の設定例 22-47
OSPF のモニタリング 22-48
その他の関連資料 22-51
RFC 22-51
OSPF の機能履歴 22-52

CHAPTER 23 EIGRP 23-1
EIGRP に関する情報 23-1
クラスタリングの使用 23-2
EIGRP のライセンス要件 23-3
ガイドラインと制限事項 23-3
EIGRP の設定 23-3
EIGRP のイネーブル化 23-4
EIGRP スタブ ルーティングのイネーブル化 23-4
EIGRP のカスタマイズ 23-5
EIGRP ルーティング プロセスのネットワークの定義 23-6
EIGRP のインターフェイスの設定 23-7
インターフェイスでのサマリー集約アドレスの設定 23-9
インターフェイス遅延値の変更 23-10
インターフェイスでの EIGRP 認証のイネーブル化 23-10
EIGRP ネイバーの定義 23-12
EIGRP へのルートの再配布 23-12
EIGRP でのネットワークのフィルタリング 23-14
EIGRP Hello 間隔と保持時間のカスタマイズ 23-15
自動ルート集約のディセーブル化 23-16
EIGRP でのデフォルト情報の設定 23-16
EIGRP スプリット ホライズンのディセーブル化 23-17
EIGRP プロセスの再始動 23-18
EIGRP のモニタリング 23-18
EIGRP の設定例 23-19
EIGRP の機能履歴 23-20

CHAPTER 24 マルチキャスト ルーティング 24-1
マルチキャスト ルーティングに関する情報 24-1
スタブ マルチキャスト ルーティング 24-2
PIM マルチキャスト ルーティング 24-2
マルチキャスト グループの概念 24-2

クラスタ 24-3
マルチキャスト ルーティングのライセンス要件 24-3
ガイドラインと制限事項 24-3
マルチキャスト ルーティングのイネーブル化 24-4
マルチキャスト ルーティングのカスタマイズ 24-4
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 24-5
スタティック マルチキャスト ルートの設定 24-5
IGMP 機能の設定 24-6
PIM 機能の設定 24-11
双方向ネイバー フィルタの設定 24-14
マルチキャスト境界の設定 24-15
マルチキャスト ルーティングの設定例 24-16
その他の関連資料 24-16
関連資料 24-16
RFC 24-16
マルチキャスト ルーティングの機能履歴 24-17

CHAPTER 25 IPv6 ネイバー探索 25-1
IPv6 ネイバー ディスカバリについて 25-1
ネイバー送信要求メッセージ 25-2
ネイバー到達可能時間 25-2
重複アドレス検出 25-2
ルータ アドバタイズメント メッセージ 25-3
スタティック IPv6 ネイバー 25-4
IPv6 ネイバー探索のライセンス要件 25-4
IPv6 ネイバー探索の前提条件 25-4
ガイドラインと制限事項 25-4
IPv6 ネイバー探索のデフォルト設定 25-6
IPv6 ネイバー探索の設定 25-7
インターフェイス コンフィギュレーション モードの開始 25-7
ネイバー送信要求メッセージの送信間隔の設定 25-8
ネイバー到達可能時間の設定 25-8
ルータ アドバタイズメントの送信間隔の設定 25-9
ルータ ライフタイム値の設定 25-9
DAD 設定の指定 25-10
ルータ アドバタイズメント メッセージの抑止 25-10
IPv6 DHCP リレーのアドレス設定フラグの設定 25-11
ルータ アドバタイズメントの IPv6 プレフィックスの設定 25-12

スタティック IPv6 ネイバーの設定 25-13
IPv6 ネイバー探索のモニタリング 25-14
その他の関連資料 25-14
IPv6 プレフィックスの関連資料 25-14
IPv6 プレフィックスとドキュメンテーションに関する RFC 25-15
IPv6 ネイバー探索の機能履歴 25-15

PART 7 AAA サーバおよびローカル データベース

CHAPTER 26 AAA について 26-1
認証 26-1
許可 26-2
アカウンティング 26-2
認証、許可、アカウンティング間の相互作用 26-2
AAA サーバ 26-2
AAA サーバ グループ 26-2
ローカル データベースのサポート 26-2

CHAPTER 27 AAA のローカル データベース 27-1
ローカル データベースについて 27-1
フォールバック サポート 27-2
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 27-2
ローカル データベースのガイドライン 27-3
ユーザ アカウントのローカル データベースへの追加 27-3
ローカル データベースのモニタリング 27-7
ローカル データベースの履歴 27-8

CHAPTER 28 AAA の RADIUS サーバ 28-1
RADIUS サーバに関する情報 28-1
サポートされている認証方式 28-2
VPN 接続のユーザ許可 28-2
RADIUS 属性のサポートされるセット 28-2
サポートされる RADIUS 許可属性 28-3
サポートされる IETF RADIUS 許可属性 28-13
RADIUS アカウンティング切断の理由コード 28-13
RADIUS サーバのライセンス要件 28-14
ガイドラインと制限事項 28-14

RADIUS サーバの設定 28-15
RADIUS サーバを設定するためのタスク フロー 28-15
RADIUS サーバ グループの設定 28-16
グループへの RADIUS サーバの追加 28-20
RADIUS サーバのモニタリング 28-22
その他の関連資料 28-22
RFC 28-22
RADIUS サーバの機能履歴 28-23

CHAPTER 29 AAA 用の TACACS+ サーバ 29-1
TACACS+ サーバに関する情報 29-1
TACACS+ 属性の使用 29-1
TACACS+ サーバのライセンス要件 29-3
ガイドラインと制限事項 29-3
TACACS+ サーバの設定 29-3
TACACS+ サーバを設定するためのタスク フロー 29-4
TACACS+ サーバ グループの設定 29-4
グループへの TACACS+ サーバの追加 29-6
TACACS+ サーバのモニタリング 29-6
TACACS+ サーバの機能履歴 29-7

CHAPTER 30 AAA の LDAP サーバ 30-1
LDAP および ASA に関する情報 30-1
LDAP サーバ ガイドライン 30-1
LDAP での認証方法 30-2
LDAP の階層について 30-2
LDAP サーバへのバインディングについて 30-4
LDAP サーバのライセンス要件 30-4
ガイドラインと制限事項 30-5
LDAP サーバの設定 30-5
LDAP サーバを設定するためのタスク フロー 30-5
LDAP 属性マップの設定 30-5
LDAP サーバ グループの設定 30-8
VPN のための LDAP での許可の設定 30-10
LDAP サーバのモニタリング 30-12
LDAP サーバの機能履歴 30-12

CHAPTER 31 アイデンティティ ファイアウォール 31-1
アイデンティティ ファイアウォールに関する情報 31-1
アイデンティティ ファイアウォールの概要 31-1
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 31-2
アイデンティティ ファイアウォールの機能 31-4
展開シナリオ 31-5
アイデンティティ ファイアウォールのライセンス 31-8
ガイドラインと制限事項 31-8
前提条件 31-10
アイデンティティ ファイアウォールの設定 31-11
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 31-11
Active Directory ドメインの設定 31-12
Active Directory エージェントの設定 31-14
アイデンティティ オプションの設定 31-15
アイデンティティに基づくセキュリティ ポリシーの設定 31-21
ユーザ統計の収集 31-23
設定例 31-23
AAA ルールとアクセス ルールの例 1 31-23
AAA ルールとアクセス ルールの例 2 31-24
VPN フィルタの例 31-24
アイデンティティ ファイアウォールのモニタリング 31-26
AD エージェントのモニタリング 31-26
グループのモニタリング 31-26
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 31-26
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 31-27
アイデンティティ ファイアウォールの機能履歴 31-28

CHAPTER 32 ASA と Cisco TrustSec 32-1
Cisco TrustSec と統合された ASA に関する情報 32-1
Cisco TrustSec の概要 32-2
Cisco TrustSec の SGT および SXP サポートについて 32-2
Cisco TrustSec 機能のロール 32-3
セキュリティ グループ ポリシーの適用 32-4
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 32-5
セキュリティ グループに対する変更が ISE に及ぼす影響 32-6
ASA での送信者および受信者のロール 32-7
SXP による頻繁な通信 32-8
SXP タイマー 32-8

IP-SGT マネージャ データベース 32-9
ASA-Cisco TrustSec 統合の機能 32-9
Cisco TrustSec のライセンス要件 32-11
Cisco TrustSec を使用するための前提条件 32-12
ASA の ISE への登録 32-12
ISE でのセキュリティ グループの作成 32-12
PAC ファイルの生成 32-13
ガイドラインと制限事項 32-13
Cisco TrustSec と統合するための ASA の設定 32-15
Cisco TrustSec と統合するための AAA サーバの設定 32-16
PAC ファイルのインポート 32-17
Security Exchange Protocol の設定 32-19
SXP 接続のピアの追加 32-22
環境データのリフレッシュ 32-23
セキュリティ ポリシーの設定 32-24
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 32-25
SGT とイーサネット タギングのイネーブル化 32-27
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 32-28
手動で設定した Cisco TrustSec リンクへのポリシーの適用 32-28
IP-SGT バインディングの手動設定 32-29
設定例 32-30
Cisco TrustSec に対する AnyConnect VPN のサポート 32-30
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 32-30
ローカル ユーザおよびグループへの SGT の追加 32-31
Cisco TrustSec のモニタリング 32-31
その他の関連資料 32-32
Cisco TrustSec 統合の機能履歴 32-33

CHAPTER 33 **ASA および Cisco Mobile Enablement 33-1**
ASA および Cisco Mobile Enablement について 33-1
ASA MDM プロキシのガイドラインと制限事項 33-2
MDM プロキシとしての ASA の設定 33-2
Mobile Enablement プロキシのアクティビティのモニタリング 33-3
ASA Mobile Enablement プロキシの機能履歴 33-3

CHAPTER 34 **デジタル証明書 34-1**
デジタル証明書の概要 34-1
公開キー暗号化 34-1

証明書のスケーラビリティ 34-2
キー ペア 34-2
トラストポイント 34-3
失効チェック 34-4
ローカル CA 34-6
証明書とユーザ ログイン クレデンシャル 34-7
ローカル証明書の前提条件 34-8
SCEP プロキシ サポートの前提条件 34-9
デジタル証明書のガイドライン 34-9
デジタル証明書の設定 34-10
キー ペアの設定 34-11
キー ペアの削除 34-11
トラストポイントの設定 34-12
トラストポイントの CRL の設定 34-15
トラストポイント コンフィギュレーションのエクスポート 34-17
トラストポイント コンフィギュレーションのインポート 34-17
CA 証明書マップ規則の設定 34-18
手動での証明書の取得 34-19
SCEP を使用した証明書の自動取得 34-21
SCEP 要求のプロキシ サポートの設定 34-22
ローカル CA サーバのイネーブル化 34-23
ローカル CA サーバの設定 34-25
ローカル CA サーバのカスタマイズ 34-26
ローカル CA サーバのデバッグ 34-27
ローカル CA サーバのディセーブル化 34-28
ローカル CA サーバの削除 34-28
ローカル CA 証明書の特性の設定 34-28
デジタル証明書のモニタリング 34-43
証明書管理の機能履歴 34-45

PART 8 システム管理

CHAPTER 35 管理アクセス 35-1
ASDM、Telnet、または SSH の ASA アクセスの設定 35-1
ASDM、Telnet、または SSH での ASA アクセスのライセンス要件 35-2
ガイドラインと制限事項 35-2
Telnet アクセスの設定 35-3
Telnet クライアントの使用 35-4
SSH アクセスの設定 35-4

SSH クライアントの使用 35-5
ASDM の HTTPS アクセスの設定 35-6
CLI パラメータの設定 35-6
CLI パラメータのライセンス要件 35-7
ガイドラインと制限事項 35-7
ログイン バナーの設定 35-7
CLI プロンプトのカスタマイズ 35-8
コンソール タイムアウトの変更 35-9
VPN トンネルを介した管理アクセスの設定 35-10
管理インターフェイスのライセンス要件 35-10
ガイドラインと制限事項 35-10
管理インターフェイスの設定 35-11
システム管理者用 AAA の設定 35-11
システム管理者用 AAA に関する情報 35-12
システム管理者用 AAA のライセンス要件 35-15
前提条件 35-15
ガイドラインと制限事項 35-16
デフォルト設定 35-17
CLI および ASDM アクセスの認証の設定 35-17
特権 EXEC モードにアクセスするための認証の設定（enable コマンド） 35-18
管理許可によるユーザ CLI および ASDM アクセスの制限 35-20
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 35-22
コマンド許可の設定 35-25
管理アクセス アカウンティングの設定 35-31
現在のログイン ユーザの表示 35-31
管理セッション割り当て量の設定 35-32
SSH セッションでのキーの交換 35-33
ロックアウトからの回復 35-34
管理アクセスの機能履歴 35-35

CHAPTER 36 ソフトウェアおよびコンフィギュレーション 36-1
ソフトウェアのアップグレード 36-1
アップグレード パスと移行 36-1
現在のバージョンの表示 36-3
Cisco.com からのソフトウェアのダウンロード 36-3
スタンドアロン ユニットのアップグレード 36-4
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 36-5
ファイルの管理 36-12
フラッシュ メモリ内のファイルの表示 36-12

フラッシュ メモリからのファイルの削除 36-13
フラッシュ ファイル システムの消去 36-13
ファイル アクセスの設定 36-13
ASA へのファイルのコピー 36-17
スタートアップ コンフィギュレーションまたは実行コンフィギュレーションへのファイルのコピー 36-20
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 36-22
イメージをロードするための ROM モニタの使用 36-23
ASA 5500-X シリーズに対する ROM モニタの使用 36-24
ASASM に対する ROM モニタの使用 36-25
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 36-27
シングル モード コンフィギュレーションまたはマルチ モード システム コンフィギュレーションのバックアップ 36-27
フラッシュ メモリ内のコンテキスト 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 36-28
コンテキスト内でのコンテキスト コンフィギュレーションのバックアップ 36-29
端末の表示からのコンフィギュレーションのコピー 36-29
export および import コマンドを使用した追加ファイルのバックアップ 36-29
スクリプトを使用したファイルのバックアップおよび復元 36-30
ソフトウェアのダウングレード 36-36
アクティベーション キーの互換性に関する情報 36-36
ダウングレードの実行 36-37
Auto Update の設定 36-38
Auto Update に関する情報 36-38
ガイドラインと制限事項 36-41
Auto Update サーバとの通信の設定 36-42
Auto Update サーバとしてのクライアント アップデートの設定 36-43
Auto Update ステータスの表示 36-44
ソフトウェアとコンフィギュレーションの機能履歴 36-45

CHAPTER 37 システム イベントに対する応答の自動化 37-1
EEM について 37-1
EEM のガイドライン 37-3
EEM の設定 37-3
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 37-3
アクションおよびアクションの出力先の設定 37-5
イベント マネージャ アプレットの実行 37-7
EEM の例 37-7
EEM のモニタリング 37-8

EEM の履歴 37-8

CHAPTER 38 トラブルシューティング 38-1
デバッグ メッセージの表示 38-1
パケットのキャプチャ 38-1
クラスタリング環境でのパケットのキャプチャ 38-3
クラッシュ ダンプの表示 38-6
コア ダンプの表示 38-6
ASAv の vCPU 使用率 38-6
CPU 使用率の例 38-6
VMware の CPU 使用率のレポート 38-7
ASAv のグラフと vCenter のグラフ 38-7

PART 9 ロギング、SNMP、および Smart Call Home

CHAPTER 39 ロギング 39-1
ロギングについて 39-1
マルチ コンテキスト モードでのロギング 39-2
syslog メッセージ分析 39-2
syslog メッセージ形式 39-3
重大度 39-3
メッセージ クラスと syslog ID の範囲 39-4
syslog メッセージのフィルタリング 39-4
カスタム メッセージ リスト 39-5
クラスタ 39-5
ロギングのガイドライン 39-5
ロギングの設定 39-6
ロギングのイネーブル 39-7
出力先の設定 39-7
ログのモニタリング 39-19
ロギングの例 39-20
ロギングの履歴 39-21

CHAPTER 40 SNMP 40-1
SNMP について 40-1
SNMP の用語 40-2
MIB およびトラップ 40-2
SNMP オブジェクト ID 40-4

物理ベンダー タイプ値 40-6
MIB でサポートされているテーブルとオブジェクト 40-12
サポートされているトラップ（通知） 40-13
インターフェイスの種類と例 40-16
SNMP バージョン 3 の概要 40-17
SNMP syslog メッセージ 40-19
アプリケーション サービスとサードパーティ ツール 40-19
SNMP のガイドライン 40-19
SNMP の設定 40-22
SNMP エージェントおよび SNMP サーバのイネーブル化 40-22
SNMP トラップの設定 40-22
CPU 使用率のしきい値の設定 40-23
物理インターフェイスのしきい値の設定 40-24
SNMP バージョン 1 または 2c のパラメータの設定 40-24
SNMP バージョン 3 のパラメータの設定 40-26
ユーザのグループの設定 40-29
ネットワーク オブジェクトへのユーザの関連付け 40-30
SNMP のモニタリング 40-30
SNMP バージョン 1 および 2c の例 40-32
SNMP バージョン 3 の例 40-32
SNMP の履歴 40-32

CHAPTER 41 **Anonymous Reporting および Smart Call Home 41-1**
Anonymous Reporting について 41-1
DNS 要件 41-2
Smart Call Home の概要 41-2
アラート グループへの登録 41-3
Anonymous Reporting および Smart Call Home のガイドライン 41-8
Anonymous Reporting および Smart Call Home の設定 41-9
Anonymous Reporting の設定 41-9
Smart Call Home の設定 41-10
Anonymous Reporting および Smart Call Home のモニタリング 41-19
Smart Call Home の例（CLI） 41-20
Anonymous Reporting および Smart Call Home の履歴 41-21

PART 10 参照先

CHAPTER 42 コマンドライン インターフェイスの使用 42-1
ファイアウォール モードとセキュリティ コンテキスト モード 42-1
コマンドのモードとプロンプト 42-2
構文の書式 42-3
コマンドの短縮形 42-4
コマンドラインの編集 42-4
コマンドの補完 42-4
コマンドのヘルプ 42-4
実行コンフィギュレーションの確認 42-5
show コマンドおよび more コマンドの出力のフィルタリング 42-5
コマンド出力のページング 42-6
コメントの追加 42-6
テキスト コンフィギュレーション ファイル 42-6
テキスト ファイルでコマンドと行が対応する仕組み 42-7
コマンド固有のコンフィギュレーション モード コマンド 42-7
自動テキスト入力 42-7
行の順序 42-7
テキスト コンフィギュレーションに含まれないコマンド 42-7
パスワード 42-8
マルチセキュリティ コンテキスト ファイル 42-8
サポートされている文字セット 42-8

CHAPTER 43 アドレス、プロトコル、およびポート 43-1
IPv4 アドレスとサブネット マスク 43-1
クラス 43-1
プライベート ネットワーク 43-2
サブネット マスク 43-2
IPv6 アドレス 43-5
IPv6 アドレス形式 43-5
IPv6 アドレス タイプ 43-6
IPv6 アドレス プレフィックス 43-10
プロトコルとアプリケーション 43-11
TCP ポートと UDP ポート 43-12
ローカル ポートとプロトコル 43-15
ICMP タイプ 43-16

このマニュアルについて

- 「マニュアルの目的」（P.xxix）
- 「関連資料」（P.xxix）
- 「表記法」（P.xxx）
- 「マニュアルの入手方法およびテクニカル サポート」（P.xxxi）

マニュアルの目的

このマニュアルの目的は、コマンドライン インターフェイスを使用した Cisco ASA シリーズ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。

また、Web ベースの GUI アプリケーションである Adaptive Security Device Manager（ASDM）を使用して ASA を設定、監視することもできます。ASDM では、コンフィギュレーション ウィザードを使用して、いくつかの一般的なコンフィギュレーションを設定できます。また、あまり一般的ではない事例には、オンラインのヘルプが用意されています。

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。

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。
`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、**`courier`** フォントで示しています。
`courier` フォント	ユーザが値を指定する引数は、***`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/c/en/us/td/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

リリース日：2014 年 7 月 24 日
更新日：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。

- 「ハードウェアとソフトウェアの互換性」（P.1-1）
- 「VPN の互換性」（P.1-2）
- 「新機能」（P.1-2）
- 「スイッチにおける ASA サービス モジュールの動作」（P.1-6）
- 「ファイアウォール機能の概要」（P.1-8）
- 「VPN 機能の概要」（P.1-13）
- 「セキュリティ コンテキストの概要」（P.1-14）
- 「ASA クラスタリングの概要」（P.1-14）
- 「特殊なレガシー サービス」（P.1-14）

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) の新機能」（P.1-2）

（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) の新機能

リリース日：2014 年 7 月 24 日

表 1-1 に、ASA バージョン 9.3(1) の新機能を示します。

表 1-1　ASA バージョン 9.3(1)

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。 変更されたコマンドはありません。
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）。 変更されたコマンドはありません。
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	イネーブルにすると、ルールのアップデートはルールのコンパイルが完了した後に適用され、ルール マッチングのパフォーマンスに影響しません。 次のコマンドが導入されました。**asp rule-engine transactional-commit**、**show running-config asp rule-engine transactional-commit**、**clear configure asp rule-engine transactional-commit**

表 1-1　ASA バージョン 9.3(1)（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。自動サインオンで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。 変更されたコマンドはありません。
Mobile Enablement プロキシ	Mobile Enablement プロキシ（ISE Mobile Enablement ソリューションのコンポーネント）を使用すると、構外モバイル デバイスがオンプレミス 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。 **（注）** Mobile Enablement プロキシには、2015 年の初めに予定されている ISE リリースでの ISE サポートが必要です。 config-mdm-proxy モードにするための **mdm-proxy** コマンドが導入されました。この新しいモードでは、次のコマンドが適用されます。**authentication-server-group**、**accounting-server-group**、**password-management**、**trusttpoint**、**port**、**session-limit**、**session-timeout**、**enable**
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。 次のコマンドが導入または変更されました。**anyconnect-custom-attr**、**anyconnect-custom-data**、および **anyconnect-custom**
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モバイル ポスチャとも呼ばれる）は、ASA にポスチャ情報を伝えるために AnyConnect VPN クライアントで使用される方式です。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。 変更されたコマンドはありません。

表 1-1　ASA バージョン 9.3(1)（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。 次の新しいコマンドが導入されました。**security-group-tag value**
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が強化されました。 次のコマンドが変更されました。**show cluster info health**
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、デフォルトでは ASA FirePOWER モジュールなどインストール済みハードウェア モジュールのヘルスをモニタします。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。 次のコマンドが変更されました。**monitor-interface service-module**
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は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のに役立ちます。 • フローの突発的なトラフィックの急増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の受信リングをオーバーサブスクライブするバルク フローによって発生するオーバーラン • シングルコアでは負荷に耐えられない非常に過負荷のインターフェイス受信リングが原因のオーバーラン 次のコマンドが導入または修正されました。**asp load-balance per-packet auto**、**show asp load-balance per-packet**、**show asp load-balance per-packet history**、および **clear asp load-balance history**
SNMP MIB	CISCO-REMOTE-ACCESS-MONITOR-MIB で ASASM がサポートされるようになりました。
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 グループの最大数を 250 に増加	ブリッジ グループの最大数が 8 個から 250 個のブリッジ グループに増加されました。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追加できます。 次のコマンドが変更されました。**interface bvi**、**bridge-group**

表 1-1　ASA バージョン 9.3(1)（続き）

機能	説明
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。 次の新しいコマンドが導入されました。**bgp router-id clusterpool**
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。 次の新しいコマンドが導入されました。**bgp graceful-restart**、**neighbor ha-mode graceful-restart**
アドバタイズされたマップに対する BGP のサポート	BGPv4 によってアドバタイズされたマップのサポートが追加されました。 次の新しいコマンドが導入されました。**neighbor advertise-map**
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。 次のコマンドが追加されました。**capability**、**nsf cisco**、**nsf cisco helper**、**nsf ietf**、**nsf ietf helper**、**nsf ietf helper strict-lsa-checking**、**graceful-restart**、**graceful-restart helper**、**graceful-restart helper strict-lsa-checking**
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。 次のコマンドが導入または変更されました。**cts manual**、**policy static sgt**、**propagate sgt**、**cts role-based sgt-map**、**show cts sgt-map**、**packet-tracer**、**capture**、**show capture**、**show asp drop**、**show asp table classify**、**show running-config all**、**clear configure all**、および **write memory**
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。 次のコマンドは廃止されました。**aaa-server protocol nt**

表 1-1　ASA バージョン 9.3(1)（続き）

機能	説明
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の集約トラフィックの情報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。

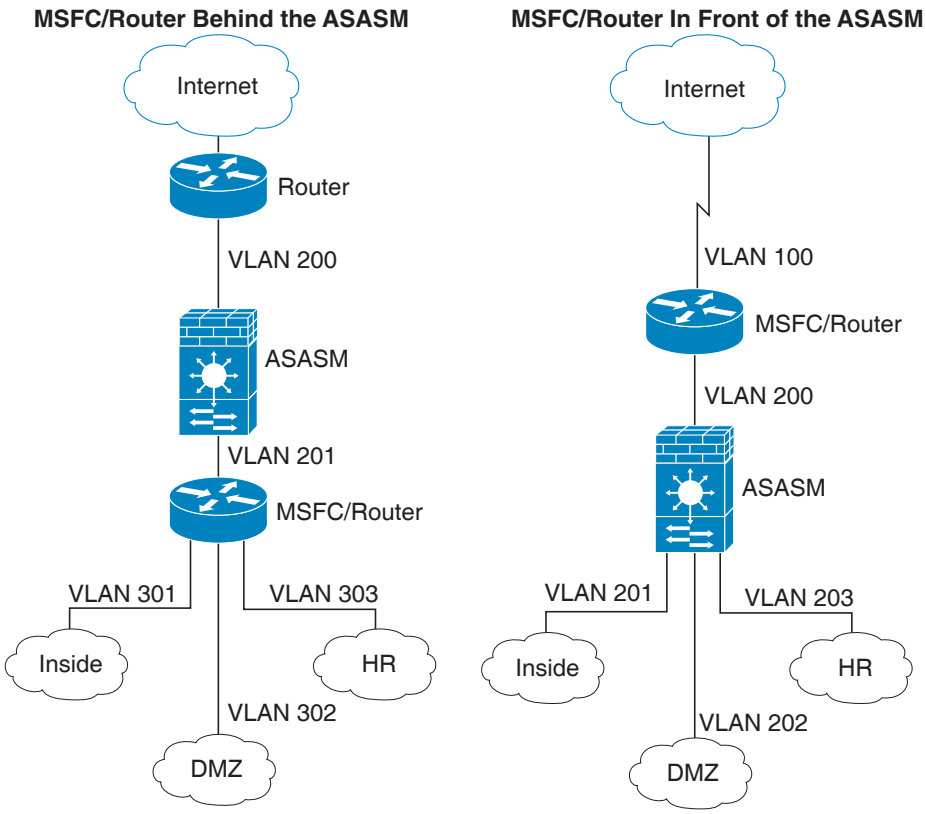
スイッチにはスイッチング プロセッサ（スーパーバイザ）とルータ（MSFC）が組み込まれています。MSFC はシステムの一部として必要ですが、使用しなくてもかまいません。使用する場合、MSFC に 1 つまたは複数の VLAN インターフェイスを割り当てることができます。MSFC の代わりに外部ルータを使用できます。

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。

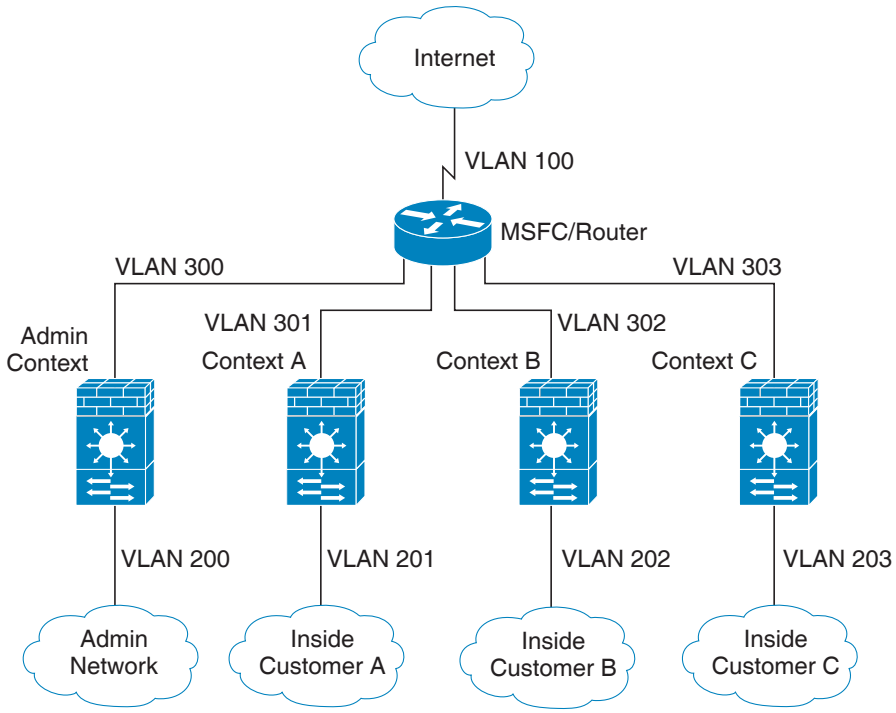
左側の例では、MSFC またはルータは VLAN 201、301、302、および 303 の間をルーティングします。宛先がインターネットの場合以外、内部トラフィックは ASASM を通過しません。右側の例では、ASASM は内部 VLAN 201、202、および 203 間のすべてのトラフィックを処理して保護します。

図 1-1　MSFC/ルータ 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/ルータ 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、認証または許可を義務づける、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、各種のインターフェイスに対してさまざまなセキュリティ ポリシーを設定できます。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.1-9）
- 「ファイアウォール モードの概要」（P.1-11）
- 「ステートフル インスペクションの概要」（P.1-12）

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 リストを使用）」（P.1-9）
- 「NAT の適用」（P.1-9）
- 「IP フラグメントからの保護」（P.1-9）
- 「通過トラフィックに対する AAA の使用」（P.1-10）
- 「HTTP、HTTPS、または FTP フィルタリングの適用」（P.1-10）
- 「アプリケーション インスペクションの適用」（P.1-10）
- 「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.1-10）
- 「QoS ポリシーの適用」（P.1-10）
- 「接続の制限と TCP 正規化の適用」（P.1-10）
- 「脅威検出のイネーブル化」（P.1-11）
- 「ボットネット トラフィック フィルタのイネーブル化」（P.1-11）
- 「Cisco Unified Communications の設定」（P.1-11）

トラフィックの許可または拒否（アクセス リストを使用）

アクセス リストは、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、認証と許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
  - 「高速パス」でのセッションの確立

  ASA は、TCP トラフィックの高速パスに転送フローとリバース フローを作成します。ASA は、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高速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「高速」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、メンバー ユニットに複製されます。

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.1-15）
- 「レガシー サービス ガイド」（P.1-15）

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は、別のガイドで説明します。

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」（P.2-1）
- 「ASDM アクセスの設定」（P.2-7）
- 「ASDM の起動」（P.2-13）
- 「工場出荷時のデフォルト コンフィギュレーション」（P.2-14）
- 「コンフィギュレーションの処理」（P.2-18）
- 「接続に対するコンフィギュレーションの変更の適用」（P.2-22）
- 「ASA のリロード」（P.2-23）

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

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 35 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」（P.2-2）
- 「ASA サービス モジュール コンソールへのアクセス」（P.2-3）

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、イネーブル パスワード、Telnet パスワードの設定」（P.13-1）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。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」（P.2-3）
- 「ASA サービス モジュールへのログイン」（P.2-4）
- 「コンソール セッションのログアウト」（P.2-6）
- 「アクティブなコンソール接続の終了」（P.2-6）
- 「Telnet セッションのログアウト」（P.2-7）

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.35-1）
- 「ホスト名、ドメイン名、イネーブル パスワード、Telnet パスワードの設定」（P.13-1）

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 コンフィギュレーション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。

- 「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した ASDM アクセス（アプライアンス、ASAv）」（P.2-8）
- 「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）

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した ASDM アクセス（アプライアンス、ASAv）

工場出荷時のデフォルト コンフィギュレーションでは、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 コンフィギュレーション」（P.2-14）
- 「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.6-16）
- 「ASDM の起動」（P.2-13）

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。
- 管理 IP アドレスを変更したい。
- 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、オプションで独自の管理 IP アドレスを設定し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.2-15）
- 「ファイアウォール 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.2-13）
- 第 6 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 を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 6 章「マルチ コンテキスト モード」
- 「ファイアウォール 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。

工場出荷時のデフォルト コンフィギュレーション

工場出荷時のデフォルト 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」（P.2-15）
- 「ASAv 導入設定の復元」（P.2-16）
- 「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」（P.2-16）
- 「ASAv の導入設定」（P.2-17）

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。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　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します。

configure factory-default [*ip_address* [*mask*]]

例：

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

ip_address を指定する場合は、デフォルトの IP アドレス 192.168.1.1 を使用する代わりに、お使いのモデルに応じて、内部または管理インターフェイスの IP アドレスを設定します。**http** コマンドでは、指定するサブネットが使用されます。同様に、**dhcpd address** コマンドの範囲は、指定したサブネット内のアドレスで構成されます。

このコマンドは、**boot system** コマンド（存在する場合）も、他のコンフィギュレーションとともにクリアします。**boot system** コマンドを使用すると、外部フラッシュ メモリ カードに保存されているイメージなどの、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 2　デフォルト コンフィギュレーションをフラッシュ メモリに保存します。

write memory

このコマンドでは、事前に **boot config** コマンドを設定して、別の場所を設定していた場合でも、実行コンフィギュレーションはスタートアップ 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がクリアされると、このパスもクリアされます。

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（management）。

- 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
failover
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
```

コンフィギュレーションの処理

この項では、コンフィギュレーションを処理する方法について説明します。ASA は、スタートアップ コンフィギュレーションと呼ばれるコンフィギュレーションをテキスト ファイルからロードします。このファイルは、デフォルトでは隠しファイルとして内部フラッシュ メモリに常駐しています。ただし、ユーザはスタートアップ コンフィギュレーションに異なるパスを指定することができます

コマンドを入力すると、メモリ上の実行コンフィギュレーションに対してだけ変更が適用されます。変更内容をリブート後も維持するには、実行コンフィギュレーションを手動でスタートアップ コンフィギュレーションに保存する必要があります。

この項で説明する内容は、特に指定がない限り、シングル モードとマルチ モードの両セキュリティ コンテキストに適用されます。

- 「コンフィギュレーションの変更の保存」（P.2-18）
- 「実行コンフィギュレーションへのスタートアップ コンフィギュレーションのコピー」（P.2-20）
- 「コンフィギュレーションの表示」（P.2-21）
- 「コンフィギュレーション設定のクリアと削除」（P.2-21）
- 「オフラインでのテキスト コンフィギュレーション ファイルの作成」（P.2-22）

コンフィギュレーションの変更の保存

この項では、コンフィギュレーションを保存する方法について説明します。

- 「シングル コンテキスト モードでのコンフィギュレーションの変更の保存」（P.2-18）
- 「マルチ コンテキスト モードでのコンフィギュレーションの変更の保存」（P.2-19）

シングル コンテキスト モードでのコンフィギュレーションの変更の保存

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保存するには、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スタートアップ コンフィギュレーションに保存します。

```
write memory
```

（注）　**copy running-config startup-config** コマンドは、**write memory** コマンドに相当します。

マルチ コンテキスト モードでのコンフィギュレーションの変更の保存

各コンテキスト（およびシステム）コンフィギュレーションを個別に保存することも、すべてのコンテキスト コンフィギュレーションを同時に保存することもできます。

- 「各コンテキストとシステムの個別保存」（P.2-19）
- 「すべてのコンテキスト コンフィギュレーションの同時保存」（P.2-19）

各コンテキストとシステムの個別保存

システムまたはコンテキストのコンフィギュレーションを保存するには、次の手順を使用します。

手順

ステップ 1　コンテキストまたはシステム内から、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保存します。

```
write memory
```

マルチ コンテキスト モードでは、コンテキストのスタートアップ コンフィギュレーションを外部サーバに置くことができます。この場合、そのコンフィギュレーションは、コンテキスト URL（HTTP URL および HTTPS URL を除く）に指定されているサーバに ASA によって戻され、保存されるため、サーバにコンフィギュレーションを保存する必要はありません。

（注）　**copy running-config startup-config** コマンドは、**write memory** コマンドに相当します。

すべてのコンテキスト コンフィギュレーションの同時保存

すべてのコンテキスト コンフィギュレーションとシステム コンフィギュレーションを同時に保存するには、次の手順を使用します。

手順

ステップ 1　システム実行スペースから、すべてのコンテキストとシステム コンフィギュレーション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保存します。

```
write memory all [/noconfirm]
```

/noconfirm キーワードを入力しない場合、次のプロンプトが表示されます。

```
Are you sure [Y/N]:
```

Y を入力すると、ASA によってシステム コンフィギュレーションと各コンテキストが保存されます。コンテキストのスタートアップ コンフィギュレーションは、外部サーバに配置できます。この場合、そのコンフィギュレーションは、コンテキスト URL（HTTP URL および HTTPS URL を除く）に指定されているサーバに ASA によって戻され、保存されるため、サーバにコンフィギュレーションを保存する必要はありません。

ASA によって各コンテキストが保存されると、次のメッセージが表示されます。

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

エラーのためにコンテキストが保存されない場合もあります。エラーについては、次の情報を参照してください。

- メモリ不足のためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- リモートの宛先に到達できないためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- コンテキストがロックされているために保存されない場合は、次のメッセージが表示されます。

  ```
  Unable to save the configuration for the following contexts as these contexts are
  locked.
  context ‘a’ , context ‘x’ , context ‘z’ .
  ```

  コンテキストがロックされるのは、別のユーザがすでにコンフィギュレーションを保存している場合、またはコンテキストを削除している場合のみです。

- スタートアップ コンフィギュレーションが読み取り専用であるために（たとえば、HTTP サーバで）コンテキストが保存されない場合は、他のすべてのメッセージの最後に次のメッセージ レポートが出力されます。

  ```
  Unable to save the configuration for the following contexts as these contexts have
  read-only config-urls:
  context ‘a’ , context ‘b’ , context ‘c’ .
  ```

- フラッシュ メモリのセクターが壊れているためコンテキストを保存できない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to Unknown errors
  ```

実行コンフィギュレーションへのスタートアップ コンフィギュレーションのコピー

新しいスタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーするには、次のいずれかのコマンドを使用します。

- **copy startup-config running-config**

  スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。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。

- **reload**

  ASA をリロードします。その結果、スタートアップ コンフィギュレーションがロードされ、実行コンフィギュレーションが破棄されます。

- **clear configure all**、続いて then**copy startup-config running-config**

  スタートアップ コンフィギュレーションをロードし、実行コンフィギュレーションを破棄します。リロードは不要です。

コンフィギュレーションの表示

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を表示するには、次のコマンドを使用します。

- **show running-config**

  実行コンフィギュレーションを表示します。

- **show running-config** *command*

  特定のコマンドの実行コンフィギュレーションを表示します。

- **show startup-config**

  スタートアップ コンフィギュレーションを表示します。

コンフィギュレーション設定のクリアと削除

設定を消去するには、次のいずれかのコマンドを入力します。

- **clear configure** *configurationcommand* [*level2configurationcommand*]

  指定されたコマンドのすべてのコンフィギュレーションをクリアします。コマンドの特定バージョンのコンフィギュレーションだけをクリアする場合は、*level2configurationcommand* に値を入力します。

  たとえば、すべての **aaa** コマンドのコンフィギュレーションをクリアするには、次のコマンドを入力します。

  ```
  ciscoasa(config)# clear configure aaa
  ```

  aaa authentication コマンドのコンフィギュレーションだけをクリアするには、次のコマンドを入力します。

  ```
  ciscoasa(config)# clear configure aaa authentication
  ```

- **no** *configurationcommand* [*level2configurationcommand*] *qualifier*

  コマンドの特定のパラメータまたはオプションをディセーブルにします。この場合、**no** コマンドを使用して、*qualifier* で特定されるコンフィギュレーションを削除します。

  たとえば、特定の **access-list** コマンドを削除するには、それを一意に特定するのに十分なコマンドを入力します。コマンド全体を入力しなければならない場合もあります。

  ```
  ciscoasa(config)# no access-list abc extended permit icmp any any object-group
  obj_icmp_1
  ```

- **write erase**

  スタートアップ コンフィギュレーションを消去します。

（注） ASAv の場合、このコマンドはリロード後に導入設定を復元します。コンフィギュレーションを完全に消去するには、**clear configure all** コマンドを使用します。

- **clear configure all**

  実行コンフィギュレーションを消去します。

（注）　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から **clear configure all** を入力すると、すべてのコンテキストを削除し、実行中のコンフィギュレーションを停止することにもなります。コンテキスト コンフィギュレーション ファイルは消去されず、元の場所に保持されます。

このコマンドは、**boot system** コマンド（存在する場合）も、他のコンフィギュレーションとともにクリアします。**boot system** コマンドを使用すると、外部フラッシュ メモリ カードに保存されているイメージなどの、特定のイメージからブートできます。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。

オフラインでのテキスト コンフィギュレーション ファイルの作成

このマニュアルでは、ASA を設定するための CLI の使用方法について説明しています。コマンドを保存すると、変更内容はテキスト ファイルに書き込まれます。一方、CLI を使用する代わりに、テキスト ファイルを PC で直接編集して、コンフィギュレーション モードのコマンドライン プロンプトから、コンフィギュレーションを全部または 1 行ずつペーストすることができます。また、ASA の内部フラッシュ メモリにテキスト ファイルをダウンロードできます。コンフィギュレーション ファイルを ASA にダウンロードする方法の詳細については、第 36 章「ソフトウェアおよびコンフィギュレーション」を参照してください。

ほとんどの場合、このマニュアルで説明するコマンドには、CLI プロンプトが先行します。次の例では、CLI プロンプトは「ciscoasa(config)#」です。

```
ciscoasa(config)# context a
```

コマンドの入力が要求されないテキスト コンフィギュレーション ファイルの場合は、プロンプトは次のように省略されます。

```
context a
```

テキスト コンフィギュレーション ファイルのフォーマッティングの詳細については、付録 42「コマンド ライン インターフェイスの使用」を参照してください。

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。

ASA のリロード

ASA をリロードするには、次の手順を実行します。

手順

ステップ 1　ASA をリロードします。

```
reload
```

（注）　マルチ コンテキスト モードでは、システム実行スペース以外からはリロードできません。

Cisco ASA サービス モジュール向けのスイッチの設定

この章では、Cisco ASA サービス モジュール（ASASM）と組み合わせて使用できるように、Catalyst 6500 シリーズまたは Cisco 7600 シリーズ スイッチを設定する方法について説明します。この章で説明する作業を行う前に、スイッチに付属のマニュアルに従って、スイッチ ポートへの VLAN 割り当てをはじめ、スイッチの基本的なプロパティを設定してください。

- 「スイッチに関する情報」（P.3-1）
- 「ガイドラインと制限事項」（P.3-3）
- 「モジュールの搭載確認」（P.3-4）
- 「ASA サービス モジュールへの VLAN の割り当て」（P.3-5）
- 「直接接続されたルータ（SVI）としての MSFC の使用」（P.3-7）
- 「ASA フェールオーバーのスイッチの設定」（P.3-9）
- 「ASA サービス モジュールのリセット」（P.3-10）
- 「ASA サービス モジュールのモニタリング」（P.3-11）
- 「ASA サービス モジュールを使用するためのスイッチの機能履歴」（P.3-13）

スイッチに関する情報

- 「サポートされているスイッチ ハードウェアおよびソフトウェア」（P.3-1）
- 「バックプレーン接続」（P.3-2）
- 「ASA と Cisco IOS 機能の相互作用」（P.3-2）

サポートされているスイッチ ハードウェアおよびソフトウェア

ASASM は、Catalyst 6500 シリーズおよび Cisco 7600 シリーズ スイッチにインストールできます。スイッチにはスイッチ（スーパーバイザ エンジン）とルータ（MSFC）が組み込まれています。

スイッチのスーパーバイザ エンジンと統合型の MSFC ルータの両方で Cisco IOS ソフトウェアがサポートされています。

（注） Catalyst オペレーティング システム ソフトウェアはサポートされていません。

ASASM は独自のオペレーティング システムで動作します。

（注）　ASASM は独自のオペレーティング システムで動作するので、Cisco IOS ソフトウェアをアップグレードしても ASASM の動作には影響ありません。

ASASM および Cisco IOS バージョンのハードウェアとソフトウェアの互換性については、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

バックプレーン接続

ASASM とスイッチは、単一の 20 GB インターフェイスで接続されています。

ASA と Cisco IOS 機能の相互作用

一部の ASASM の機能は Cisco IOS 機能と連携します。次の機能は、Cisco IOS ソフトウェアを必要とします。

- 仮想スイッチング システム（VSS）：ASASM 設定は必要ありません。
- 自動ステート：スーパーバイザは、指定 VLAN の最後のインターフェイスがダウンしたとき、ASASM に通知します。これは、フェールオーバー スイッチが必要かどうかの決定を支援します。
- フェールオーバー スイッチのスーパーバイザ MAC アドレス テーブルのエントリのクリア：ASASM 設定は必要ありません。
- バージョン互換性：スーパーバイザ/ASASM バージョン互換性マトリクス チェックが失敗した場合、ASASM は自動的に電源がオフになります。

SVI に関する情報

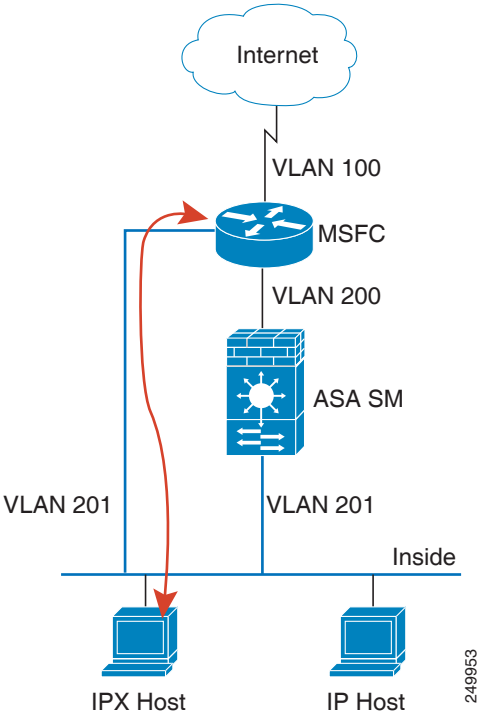
直接接続されたルータとして（たとえば、ASASM 外部インターフェイスに接続されているデフォルト ゲートウェイとして）MSFC を使用する場合は、スイッチ仮想インターフェイス（SVI）として MSFC に ASASM VLAN インターフェイスを追加します。

セキュリティ上の理由から、デフォルトでは、MSFC と ASASM の間の 1 つの SVI を設定できます。複数の SVI をイネーブルにできますが、誤ってネットワークの設定をしないよう注意してください。

たとえば、複数の SVI を設定した場合、MSFC に内部 VLAN と外部 VLAN の両方が割り当てられていることによって、トラフィックが偶発的に ASASM をバイパスする可能性があります

ネットワーク シナリオの中には、ASASM をバイパスする必要があるものもあります。図 3-1 に、IP ホストと同じイーサネット セグメント上にある IPX ホストを示します。ルーテッド ファイアウォール モードの ASASM は IP トラフィックしか処理せず、IPX などの他のプロトコル トラフィックを廃棄するため（トランスペアレント ファイアウォール モードでは IP 以外のトラフィックの通過が任意に許可されます）、IPX トラフィックで ASASM をバイパスする必要があります。この場合は、必ず VLAN 201 を通過できるのが IPX トラフィックに限定されるアクセス リストを使用して MSFC を設定してください。

図 3-1　IPX 対応の複数の SVI



トランスペアレント ファイアウォールがマルチ コンテキスト モードの場合、コンテキストごとに対応する外部インターフェイス上に固有の VLAN が必要なので、複数の SVI を使用する必要があります。ルーテッド モードの場合でも複数の SVI を使用できるので、外部インターフェイス用に 1 つの VLAN を共有する必要はありません。

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。

VLAN のガイドラインと制限事項

- VLAN ID 2 ～ 1001 を使用します。
- ASASM では、プライベート VLAN を使用できます。ASASM にプライマリ VLAN を割り当てると、ASASM は自動的にセカンダリ VLAN トラフィックを処理します。この機能は、ASASM 上での設定は必要ありません。詳細については、スイッチのコンフィギュレーション ガイドを参照してください。「ASA サービス モジュールへの VLAN の割り当て」（P.3-5）の例も参照してください。
- 予約済みの VLAN は使用できません。
- VLAN 1 は使用できません。
- 同一スイッチ シャーシ内で ASASM フェールオーバーを使用する場合は、フェールオーバーおよびステートフル通信のために確保してある VLAN（複数可）をスイッチ ポートに割り当てないでください。ただし、シャーシ間でフェールオーバーを使用する場合は、シャーシ間を結ぶトランク ポートに VLAN を組み込む必要があります。

- ASASM に VLAN を割り当てる前に、スイッチに VLAN を追加しなかった場合、VLAN はスーパーバイザ エンジンのデータベースに保管され、スイッチに追加された時点で ASASM に送信されます。
- VLAN がスイッチに割り当てられる前に、ASASM コンフィギュレーションに VLAN を設定できます。スイッチが VLAN を ASASM に送信すると、ASASM コンフィギュレーションでシャットダウンするかどうかにかかわらず、VLAN は ASASM 上で、デフォルトで管理上アップ状態になることに注意してください。この場合、再度シャットダウンする必要があります。

SPAN リフレクタのガイドライン

Cisco IOS ソフトウェア バージョン 12.2SXJ1 以前では、スイッチ内の ASASM ごとに SPAN リフレクタ機能がイネーブルになっています。この機能により、ASASM から送られてきたマルチキャスト トラフィック（および中央の書き換えエンジンを必要とする他のトラフィック）をスイッチングできます。SPAN リフレクタ機能は SPAN セッションを 1 つ使用します。この機能をディセーブルにするには、次のコマンドを入力します。

```
Router(config)# no monitor session servicemodule
```

モジュールの搭載確認

スイッチが ASASM を認識し、オンラインに移行させたことを確認するには、次のコマンドを入力します。

手順の詳細

コマンド	目的
show module [**switch** {**1** |**2**}] [*mod-num* | **all**] **例：** `Router# show module 1`	モジュール情報を表示します。VSS 内のスイッチの場合、**switch** キーワードを入力します。 [Status] 列で、ASASM に対して [Ok] が表示されることを確認します。

例

次に、**show module** コマンドの出力例を示します。

```
Router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
 2     3  ASA Service Module                     WS-SVC-ASA-SM1     SAD143502E8
 4     3  ASA Service Module                     WS-SVC-ASA-SM1     SAD135101Z9
 5     5  Supervisor Engine 720 10GE (Active)    VS-S720-10G        SAL12426KB1
 6    16  CEF720 16 port 10GE                    WS-X6716-10GE      SAL1442WZD1

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
 2  0022.bdd4.016f to 0022.bdd4.017e   0.201 12.2(2010080 12.2(2010121 Ok
 4  0022.bdd3.f64e to 0022.bdd3.f655   0.109 12.2(2010080 12.2(2010121 PwrDown
 5  0019.e8bb.7b0c to 0019.e8bb.7b13   2.0   8.5(2)       12.2(2010121 Ok
 6  f866.f220.5760 to f866.f220.576f   1.0   12.2(18r)S1  12.2(2010121 Ok
```

```
Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ------------ ------- -------
2/0 ASA Application Processor   SVC-APP-PROC-1     SAD1436015D  0.202  Other
4/0 ASA Application Processor   SVC-APP-INT-1      SAD141002AK  0.106  PwrDown
 5  Policy Feature Card 3       VS-F6K-PFC3C       SAL12437BM2  1.0    Ok
 5  MSFC3 Daughterboard         VS-F6K-MSFC3       SAL12426DE3  1.0    Ok
 6  Distributed Forwarding Card WS-F6700-DFC3C     SAL1443XRDC  1.4    Ok

Base PID:
Mod  Model            Serial No.
---- -----------      ----------
 2 WS-SVC-APP-HW-1    SAD143502E8
 4 TRIFECTA           SAD135101Z9

Mod  Online Diag Status
---- -------------------
 2  Pass
2/0 Not Applicable
 4  Not Applicable
4/0 Not Applicable
 5  Pass
 6  Pass
```

ASA サービス モジュールへの VLAN の割り当て

ここでは、ASASM に VLAN を割り当てる方法について説明します。ASASM には、外部物理インターフェイスが組み込まれていません。代わりに VLAN インターフェイスを使用します。ASASM への VLAN の割り当ては、スイッチ ポートへの VLAN の割り当てと同様です。ASASM には、スイッチ ファブリック モジュール（SFM）（搭載されている場合）または共有バスへの内部インターフェイスが組み込まれています。

前提条件

VLAN をスイッチに追加してスイッチ ポートに割り当てる方法については、スイッチのマニュアルを参照してください。

ガイドライン

- 各 ASASM に最大 16 個のファイアウォール VLAN グループを割り当てることができます（Cisco IOS ソフトウェアでは 17 個以上の VLAN グループを作成できますが、各 ASASM に割り当てることができるのは 16 個だけです）。たとえば、すべての VLAN を 1 つのグループに割り当てたり、内部グループと外部グループを作成したり、カスタマーごとにグループを作成したりすることができます。
- グループごとの VLAN の数に制限はありませんが、ASASM は VLAN を ASASM システム制限までしか使用できません（詳細については、ASASM ライセンス マニュアルを参照してください）。
- 同じ VLAN を複数のファイアウォール グループに関連付けることはできません。
- 複数の ASASM に単一のファイアウォール グループを割り当てることはできます。たとえば、複数の ASASM に割り当てる VLAN は、それぞれの ASASM に一意の VLAN とは別のグループに配置できます。
- 「VLAN のガイドラインと制限事項」（P.3-3）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	**firewall vlan-group** *firewall_group vlan_range* **例：** `Router(config)# firewall vlan-group 1 55-57`	VLAN をファイアウォール グループに割り当てます。 *firewall_group* 引数には、整数値を指定します。*vlan_range* 引数には、次のいずれかの形式で 1 つまたは複数の VLAN（2 ～ 1001）を指定できます。 • 個別の番号（*n*） • 範囲（*n-x*） 次の例のように、番号または範囲をカンマで区切ります。 **5,7-10,13,45-100**
ステップ 2	**firewall** [**switch** {**1** |**2**}] **module** *slot* **vlan-group** *firewall_group* **例：** `Router(config)# firewall module 5 vlan-group 1`	ASASM にファイアウォール グループを割り当てます。 VSS 内のスイッチの場合、**switch** 引数を入力します。 ASASM がインストールされているスロットを表示するには、**show module** コマンドを入力します。 *firewall_group* 引数には、次のいずれかの形式で 1 つ以上のグループ番号を指定します。 • 個別の番号（*n*） • 範囲（*n-x*） 次の例のように、番号または範囲をカンマで区切ります。 **5,7-10**

例

次に、3 つのファイアウォール VLAN グループ（各 ASASM 用のグループおよび両方の ASASM に割り当てられた VLAN を含むグループ）を作成する例を示します。

```
Router(config)# firewall vlan-group 10 55-57
Router(config)# firewall vlan-group 11 70-85
Router(config)# firewall vlan-group 12 100
Router(config)# firewall module 5 vlan-group 10,12
Router(config)# firewall module 8 vlan-group 11,12
```

次に、プライマリ VLAN を ASASM に割り当てて、スイッチでプライベート VLAN を設定する例を示します。

ステップ 1　プライマリ VLAN 200 をファイアウォール VLAN グループに追加し、グループを ASASM に割り当てます。

```
Router(config)# firewall vlan-group 10 200
Router(config)# firewall module 5 vlan-group 10
```

ステップ 2　VLAN 200 をプライマリ VLAN として指定します。

```
Router(config)# vlan 200
Router(config-vlan)# private-vlan primary
```

ステップ 3　セカンダリ独立 VLAN を 1 つだけ指定します。セカンダリ コミュニティ VLAN を 1 つ以上指定します。

```
Router(config)# vlan 501
Router(config-vlan)# private-vlan isolated
Router(config)# vlan 502
Router(config-vlan)# private-vlan community
Router(config)# vlan 503
Router(config-vlan)# private-vlan community
```

ステップ 4　セカンダリ VLAN をプライマリ VLAN に関連付けます。

```
Router(config)# vlan 200
Router(config-vlan)# private-vlan association 501-503
```

ステップ 5　ポート モードを分類します。インターフェイス f1/0/1 のモードは、ホストです。インターフェイス f1/0/2 のモードは、無差別です。

```
Router(config)# interface f1/0/1
Router(config-ifc)# switchport mode private-vlan host
Router(config)# interface f1/0/2
Router(config-ifc)# switchport mode private-vlan promiscuous
```

ステップ 6　VLAN メンバーシップをホスト ポートに割り当てます。インターフェイス f1/0/1 は、プライマリ VLAN 200 とセカンダリ独立 VLAN 501 のメンバです。

```
Router(config)# interface f1/0/1
Router(config-ifc)# switchport private-vlan host-association 200 501
```

ステップ 7　VLAN メンバーシップを無差別インターフェイスに割り当てます。インターフェイス f1/0/2 は、プライマリ VLAN 200 のメンバです。セカンダリ VLAN 501 ～ 503 は、プライマリ VLAN にマッピングされます。

```
Router(config)# interface f1/0/2
Router(config-ifc)# switchport private-vlan mapping 200 501-503
```

ステップ 8　VLAN 間ルーティングが必要な場合は、プライマリ SVI を設定し、セカンダリ VLAN をプライマリにマッピングします。

```
Router(config)# interface vlan 200
Router(config-ifc)# private-vlan mapping 501-503
```

直接接続されたルータ（SVI）としての MSFC の使用

直接接続されたルータとして（たとえば、ASASM 外部インターフェイスに接続されているデフォルト ゲートウェイとして）MSFC を使用する場合は、スイッチ仮想インターフェイス（SVI）として MSFC に ASASM VLAN インターフェイスを追加します。「SVI に関する情報」（P.3-2）を参照してください。

制限事項

セキュリティ上の理由から、デフォルトでは、MSFC と ASASM の間の 1 つの SVI を設定できます。複数の SVI をイネーブルにできますが、誤ってネットワークの設定をしないよう注意してください。

手順の詳細

	コマンド	目的
ステップ 1	（オプション） **firewall multiple-vlan-interfaces** **例：** `Router(config)# firewall multiple-vlan-interfaces`	ASASM に複数の SVI を追加できます。
ステップ 2	**interface vlan** *vlan_number* **例：** `Router(config)# interface vlan 55`	MSFC に VLAN インターフェイスを追加します。
ステップ 3	**ip address** *address mask* **例：** `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	MSFC でこのインターフェイスの IP アドレスを設定します。
ステップ 4	**no shutdown** **例：** `Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。

例

次に、複数の SVI を使用する一般的な設定例を示します。

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall module 8 vlan-group 50-51
Router(config)# firewall multiple-vlan-interfaces
Router(config)# interface vlan 55
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# interface vlan 56
Router(config-if)# ip address 10.1.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

ASA フェールオーバーのスイッチの設定

- 「セカンダリ ASA サービス モジュール への VLAN の割り当て」（P.3-9）
- 「プライマリ スイッチとセカンダリ スイッチ間のトランクの追加」（P.3-9）
- 「トランスペアレント ファイアウォール モードとの両立」（P.3-9）
- 「高速リンク障害検出のための自動ステート メッセージングのイネーブル化」（P.3-9）

セカンダリ ASA サービス モジュール への VLAN の割り当て

両方の装置が同じように内部ネットワークと外部ネットワークにアクセスできる必要があるため、スイッチ上の両方の ASASM に同じ VLAN を割り当てる必要があります。「セカンダリ ASA サービス モジュール への VLAN の割り当て」（P.3-9）を参照してください。

プライマリ スイッチとセカンダリ スイッチ間のトランクの追加

スイッチ間フェールオーバーを使用している場合、2 つのスイッチ間に 802.1Q VLAN トランクを設定してフェールオーバーとステート リンクを処理する必要があります。CoS 値が 5（ハイ プライオリティ）のフェールオーバー VLAN パケットがこれらのポートでハイ プライオリティとして処理されるように、トランクで QoS をイネーブルにしておく必要があります。

EtherChannel とトランクの設定については、スイッチのマニュアルを参照してください。

トランスペアレント ファイアウォール モードとの両立

トランスペアレント モードでフェールオーバーを使用した場合にループが発生しないように、BPDU の転送をサポートするスイッチ ソフトウェアを使用してください。ASASM がトランスペアレント モードの場合、スイッチでグローバルに LoopGuard をイネーブルにしないでください。LoopGuard は、スイッチと ASASM 間の内部 EtherChannel に自動的に適用されます。そのため、フェールオーバーおよびフェールバック後、EtherChannel がエラー ディセーブル ステートになるため、LoopGuard によりセカンダリ ユニットが切断されます。

高速リンク障害検出のための自動ステート メッセージングのイネーブル化

スーパーバイザ エンジンから ASASM に、ASASM VLAN に関連付けられている物理インターフェイスのステータスに関する自動ステート メッセージが送信されます。たとえば、VLAN に関連付けられたすべての物理インターフェイスが停止すると、VLAN が停止したことを示す自動ステート メッセージが ASASM に届きます。この情報に基づいて ASASM は VLAN が停止していると判断できます。この場合は、いずれの側でリンク障害が発生したかを判別するのに必要となるインターフェイス モニタリング テストが回避されます。自動ステート メッセージングにより、ASASM がリンク障害を検出するのに要する時間が大幅に短縮されます（自動ステートがサポートされていない場合は最長 45 秒あるのに対して、数ミリ秒になります）。

次の場合に、スイッチのスーパーバイザから ASASM に自動ステート メッセージが送信されます。

- VLAN に属している最後のインターフェイスが停止した
- VLAN に属している最初のインターフェイスが動作を開始した

手順の詳細

コマンド	目的
firewall autostate **例：** `Router(config)# firewall autostate`	Cisco IOS ソフトウェアで自動ステート メッセージングをイネーブルにします。デフォルトでは、自動ステート メッセージングはディセーブルになっています。

ASA サービス モジュールのリセット

ここでは、ASASM をリセットする方法について説明します。CLI または外部 Telnet セッションから ASASM にアクセスできない場合は、FWSM のリセットが必要となります。リセットすると、完了までに数分間かかることがあります。

手順の詳細

コマンド	目的
hw-module [**switch** {**1** |**2**}] **module** *slot* **reset** **例：** `Router# hw-module module 9 reset`	ASASM をリセットします。 VSS 内のスイッチの場合、**switch** 引数を入力します。 *slot* 引数は、モジュールがインストールされているスロット番号を示します。ASASM がインストールされているスロットを表示するには、**show module** コマンドを入力します。 **（注）** 現在ログイン済みの ASASM をリセットするには、**reload** コマンドまたは **reboot** コマンドを入力します。

例

次に、**hw-module module reset** コマンドの出力例を示します。

```
Router# hw-module module 9 reset

Proceed with reload of module?[confirm] y
% reset issued for module 9

Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down.Please wait ...
```

ASA サービス モジュールのモニタリング

ASA をモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
show firewall module [*mod-num*] **state**	ASA の状態を確認します。
show firewall module [*mod-num*] **traffic**	トラフィックが ASA を通過していることを確認します。
show firewall module [*mod-num*] **version**	ASA のソフトウェア バージョンを表示します。
show firewall multiple-vlan-interfaces	複数の VLAN インターフェイスのステータスを示します（イネーブルまたはディセーブル）。
show firewall vlan-group	設定されているすべての VLAN グループを表示します。
show interface vlan	設定されている VLAN インターフェイスに関するステータスおよび情報を表示します。

例

次に、**show firewall module** [*mod-num*] **state** コマンドの出力例を示します。

```
Router> show firewall module 11 state
Firewall module 11:
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 3,6,7,20-24,40,59,85,87-89,99-115,150,188-191,200,250,
     501-505,913,972
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:
Vlans allowed and active in management domain:
Vlans in spanning tree forwarding state and not pruned:
```

次に、**show firewall module** [*mod-num*] **traffic** コマンドの出力例を示します。

```
Router> show firewall module 11 traffic
Firewall module 11:

Specified interface is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0014.1cd5.bef6 (bia 0014.1cd5.bef6)
  MTU 1500 bytes, BW 6000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 1000Mb/s, media type is unknown
  input flow-control is on, output flow-control is on
  Members in this channel: Gi11/1 Gi11/2 Gi11/3 Gi11/4 Gi11/5 Gi11/6
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queuing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 10000 bits/sec, 17 packets/sec
     8709 packets input, 845553 bytes, 0 no buffer
     Received 745 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     18652077 packets output, 1480488712 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

次に、**show firewall multiple-vlan-interfaces** コマンドの出力例を示します。

```
Router# show firewall multiple-vlan-interfaces
Multiple firewall vlan interfaces feature is enabled
```

次に、**show firewall module state** コマンドの出力例を示します。

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

次に、**show firewall module** [*mod-num*] **version** コマンドの出力例を示します。

```
Router# show firewall module 2 version
ASA Service Module 2:

Sw Version: 100.7(8)19
```

次に、**show firewall vlan-group** コマンドの出力例を示します。

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

次に、**show interface vlan** コマンドの出力例を示します。

```
Router# show interface vlan 55
Vlan55 is up, line protocol is up
  Hardware is EtherSVI, address is 0008.20de.45ca (bia 0008.20de.45ca)
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched:ucast:196 pkt, 13328 bytes - mcast:4 pkt, 256 bytes
  L3 in Switched:ucast:0 pkt, 0 bytes - mcast:0 pkt, 0 bytes mcast
  L3 out Switched:ucast:0 pkt, 0 bytes
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     4 packets output, 256 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

ASA サービス モジュールを使用するためのスイッチの機能履歴

表 3-1 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。

表 3-1　ASASM を使用するためのスイッチの機能履歴

機能名	プラットフォーム リリース	機能情報
Catalyst 6500 スイッチでの ASA サービス モジュールのサポート	8.5(1)	ASASM は、Catalyst 6500 シリーズ スイッチ用の高性能セキュリティ サービス モジュールです。本章の手順に従って設定します。 **firewall transparent**、**mac-address auto**、**firewall autostate**（IOS）、**interface vlan** の各コマンドが導入または変更されました。
Cisco 7600 スイッチでの ASA サービス モジュールのサポート	9.0(1)	Cisco 7600 シリーズが、ASASM をサポートするようになりました。
プライベート VLAN のサポート	9.1(2)	ASASM では、プライベート VLAN を使用できます。ASASM にプライマリ VLAN を割り当てると、ASASM は自動的にセカンダリ VLAN トラフィックを処理します。この機能は、ASASM 上での設定は必要ありません。詳細については、スイッチのコンフィギュレーション ガイドを参照してください。

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」（P.4-1）
- 「機能のライセンスに関する情報」（P.4-21）
- 「ガイドラインと制限事項」（P.4-33）
- 「ライセンスの設定」（P.4-34）
- 「ライセンスのモニタリング」（P.4-40）
- 「ライセンスの機能履歴」（P.4-53）

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」（P.4-2）
- 「ライセンスの注釈」（P.4-15）
- 「VPN ライセンスと機能の互換性」（P.4-20）

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 5512-X」（P.4-2）
- 「ASA 5515-X」（P.4-4）
- 「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 X 1 を搭載）」（P.4-12）
- 「ASAv（仮想 CPU X 4 を搭載）」（P.4-13）

*イタリック体*で示された項目は、基本（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.4-31）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.4-15）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*

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					
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. エンドポイント アセスメント	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*				
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	*オプションの永続ライセンス*					2	*オプションの永続ライセンス*				
		10	*25*	*50*	*100*	*250*		*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	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. エンドポイント アセスメント	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	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. エンドポイント アセスメント	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	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. エンドポイント アセスメント	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	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. エンドポイント アセスメント	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	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. エンドポイント アセスメント	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									

表 4-6　ASA 5585-X（SSP-10）ライセンスの機能 （続き）

ライセンス	基本ライセンスと Security Plus ライセンス						
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	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. エンドポイント アセスメント	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											

表 4-7　ASA 5585-X（SSP-20）ライセンスの機能 （続き）

ライセンス	基本ライセンスと Security Plus ライセンス							
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	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. エンドポイント アセスメント	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*									

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

ライセンス	基本ライセンス										
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	*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. エンドポイント アセスメント	*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*									

表 4-9　ASASM ライセンス機能 （続き）

ライセンス	基本ライセンス										
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	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 X 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. エンドポイント アセスメント	**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

表 4-10　　1 つの vCPU ライセンスを持つ ASAv の機能 （続き）

ライセンス	標準および Premium ライセンス	
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	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 X 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. エンドポイント アセスメント	**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

表 4-11　4 つの vCPU ライセンスを持つ ASAv の機能 （続き）

ライセンス	標準および Premium ライセンス	
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.4-2）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	メモ
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 VPN 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.4-20）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	メモ
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 VPN
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	メモ
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。設定で定義されている各 **interface** コマンドは、この制限に対してカウントされます。たとえば、GigabitEthernet 0/0 インターフェイスがポートチャネル 1 の一部として定義されている場合でも、次のインターフェイスは両方ともカウントされます。
	`interface gigabitethernet 0/0`
	
	および
	`interface port-channel 1`

表 4-12　ライセンスの注釈（続き）

ライセンス	メモ
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。 • フェールオーバーについて、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、フェールオーバーの装置ごとに個別の IPS モジュール ライセンスを購入する必要があります。
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	メモ
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	メモ
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。次に例を示します。
	`interface gigabitethernet 0/0.100`
	`  VLAN 100`

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	×	**Yes**
AnyConnect for Mobile[2]	**Yes**	**Yes**
Advanced Endpoint Assessment	×	**Yes**
AnyConnect Premium Shared	×	**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	×	**Yes**
IPsec VPN	**Yes**	**Yes**
VPN ロード バランシング	**Yes**	**Yes**
Cisco Secure Desktop	×	**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、**webvpn** を表示し、次に **no anyconnect-essentials** コマンドを表示するか、。
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.4-15）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」（P.4-21）
- 「永続ライセンス」（P.4-21）
- 「時間ベース ライセンス」（P.4-22）
- 「AnyConnect Premium（共有）ライセンス」（P.4-25）
- 「フェールオーバーまたは ASA クラスタ ライセンス」（P.4-28）
- 「ペイロード暗号化機能のないモデル」（P.4-31）
- 「ライセンスの FAQ」（P.4-32）

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.4-40）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.4-23）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」（P.4-22）
- 「時間ベース ライセンス タイマーの動作」（P.4-22）
- 「永続ライセンスと時間ベース ライセンスの結合」（P.4-23）
- 「時間ベース ライセンスのスタッキング」（P.4-24）
- 「時間ベース ライセンスの有効期限」（P.4-24）

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.4-40）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 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.4-35）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.4-24）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.4-35）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。ここでは、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.4-25）
- 「参加システムとサーバの間の通信に関する問題」（P.4-26）
- 「共有ライセンス バックアップ サーバに関する情報」（P.4-26）
- 「フェールオーバーと共有ライセンス」（P.4-27）
- 「参加システムの最大数」（P.4-28）

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. 共有ライセンス サーバにする ASA を決定し、そのデバイス シリアル番号を使用して共有ライセンス サーバのライセンスを購入します。
2. 共有ライセンス参加者にする ASA を決定し（共有ライセンス バックアップ サーバを含む）、それぞれのデバイス 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の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の 3 倍の時間が経過した場合、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

ここでは、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.4-27）
- 「フェールオーバーと共有ライセンス参加システム」（P.4-28）

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 Gateway 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。

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.4-26）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」（P.4-28）
- 「ASA クラスタ ライセンスの要件および例外」（P.4-29）
- 「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.4-29）
- 「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」（P.4-30）
- 「フェールオーバー ペアのアップグレード」（P.4-31）

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：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：両方のユニットで IPS モジュール ライセンスが必要です。両方のユニットの 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。
  - 両方のユニットに 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、ユニットごとに個別の 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。ただし、IPS シグニチャ サブスクリプションの要件のため、ユニットごとに個別の 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 ユニットに割り当てられる vCPU の数をプライマリ ユニット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.4-40）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.4-35）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.4-40）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.4-27）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.4-28）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。
- 購入した後でライセンスを返却して、返金を受けたりライセンスをアップグレードしたりすることはできません。
- 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。**webvpn** を使用し、次に **no anyconnect-essentials** コマンドを使用する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」（P.4-34）
- 「キーのアクティブ化および非アクティブ化」（P.4-35）
- 「共有ライセンスの設定」（P.4-37）

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。

Product Authorization Key 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、次のコマンドを入力して取得します。

```
ciscoasa# show version | grep Serial
```

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。

- Product Authorization Key（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　Product Authorization Key がさらにある場合は、Product Authorization Key ごとにステップ 4 を繰り返します。すべての Product Authorization Key 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

	コマンド	目的
ステップ 1	**activation-key** *key* [**activate** | **deactivate**] **例：** `ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490`	アクティベーション キーを ASA に適用します。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。 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。 **activate** および **deactivate** キーワードは、時間ベース キーだけに使用できます。値を入力しない場合は、**activate** がデフォルトです。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。アクティブな時間ベース キーを非アクティブにするには、**deactivate** キーワードを入力します。キーの初回入力時で、**deactivate** を指定した場合、キーは ASA に非アクティブ ステートでインストールされます。詳細については、「時間ベース ライセンス」（P.4-22）を参照してください。

	コマンド	目的
ステップ 2	（場合によって必須） **reload** **例：** ciscoasa# reload	ASA をリロードします。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.4-35）を参照してください。リロードが必要な場合は、次のメッセージが表示されます。 WARNING: The running activation key was not updated with the requested key. The flash activation key was updated with the requested key, and will become active after the next reload.

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.4-25）を参照してください。

- 「共有ライセンス サーバの設定」（P.4-37）
- 「共有ライセンス バックアップ サーバの設定（オプション）」（P.4-39）
- 「共有ライセンス参加ユニット、の設定」（P.4-40）

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

	コマンド	目的
ステップ 1	**license-server secret** *secret* **例：** ciscoasa(config)# license-server secret farscape	共有秘密を 4 ～ 128 文字の ASCII 文字のストリングで設定します。この秘密を持つ参加システムが、ライセンス サーバを使用できます。
ステップ 2	（オプション） **license-server refresh-interval** *seconds* **例：** ciscoasa(config)# license-server refresh-interval 100	10 ～ 300 秒のリフレッシュ間隔を設定します。この値が、サーバと通信する頻度として参加システムに設定されます。デフォルトは 30 秒です。

	コマンド	目的
ステップ 3	（オプション） **license-server port** *port* **例：** ciscoasa(config)# license-server port 40000	参加ユニットからの SSL 接続をサーバがリッスンするポート（1 ～ 65535）を設定します。デフォルトは、TCP ポート 50554 です。
ステップ 4	（オプション） **license-server backup** *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*] **例：** ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id JMX1378N0W3	バックアップ サーバの IP アドレスとシリアル番号を指定します。バックアップ サーバがフェールオーバー ペアの一部である場合は、スタンバイ装置のシリアル番号も指定します。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 5	**license-server enable** *interface_name* **例：** ciscoasa(config)# license-server enable inside	この装置を共有ライセンス サーバとしてイネーブルにします。参加システムがサーバと通信するインターフェイスを指定します。このコマンドは必要なインターフェイスの数だけ繰り返せます。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバを設定し、このユニットを inside インターフェイスおよび dmz インターフェイスで共有ライセンス サーバとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

次の作業

「共有ライセンス バックアップ サーバの設定（オプション）」（P.4-39）のみ）または「共有ライセンス参加ユニット、の設定」（P.4-40）を参照してください。

共有ライセンス バックアップ サーバの設定（オプション）

この項では、共有ライセンスのメイン サーバがダウンした場合にバックアップ サーバとして機能する参加システムをイネーブルにします。

前提条件

バックアップ サーバには、共有ライセンス参加キーが必要です。

手順の詳細

	コマンド	目的
ステップ 1	**license-server address** *address* **secret** *secret* [**port** *port*] **例：** `ciscoasa(config)# license-server address 10.1.1.1 secret farscape`	共有ライセンス サーバの IP アドレスと共有秘密を指定します。デフォルト ポートをサーバ コンフィギュレーションで変更した場合は、同じポートをバックアップ サーバにも設定します。
ステップ 2	**license-server backup enable** *interface_name* **例：** `ciscoasa(config)# license-server backup enable inside`	この装置を共有ライセンス バックアップ サーバとしてイネーブルにします。参加システムがサーバと通信するインターフェイスを指定します。このコマンドは必要なインターフェイスの数だけ繰り返せます。

例

次に、ライセンス サーバと共有秘密を指定し、このユニットを内部インターフェイスと dmz インターフェイス上のバックアップ共有ライセンス サーバとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

次の作業

「共有ライセンス参加ユニット、の設定」（P.4-40）を参照してください。

共有ライセンス参加ユニット、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

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

	コマンド	目的
ステップ 1	**license-server address** *address* **secret** *secret* [**port** *port*] **例：** `ciscoasa(config)# license-server address 10.1.1.1 secret farscape`	共有ライセンス サーバの IP アドレスと共有秘密を指定します。デフォルト ポートをサーバ コンフィギュレーションで変更した場合は、同じポートを参加システムにも設定します。
ステップ 2	（オプション） **license-server backup address** *address* **例：** `ciscoasa(config)# license-server backup address 10.1.1.2`	バックアップ サーバを設定した場合は、バックアップ サーバのアドレスを入力します。

例

次に、ライセンス サーバの IP アドレスおよび共有秘密、ならびにバックアップ ライセンス サーバの IP アドレスの設定例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

ライセンスのモニタリング

- 「現在のライセンスの表示」（P.4-40）
- 「共有ライセンスのモニタリング」（P.4-51）

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.4-31）を参照してください。

手順の詳細

コマンド	目的
show activation-key [**detail**] **例：** ciscoasa# show activation-key detail	このコマンドは、永続ライセンス、アクティブな時間ベース ライセンス、および実行ライセンスを表示します。実行ライセンスとは、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す。**detail** キーワードを使用すると、非アクティブな時間ベース ライセンスも表示されます。 フェールオーバーまたはクラスタ ユニットでは、このコマンドは、すべてのユニットの結合キーである「クラスタ」ライセンスも示します。

例

例 4-1　show activation-key コマンドのスタンドアロン ユニットの出力

次に、実行ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）、およびアクティブな各時間ベース ライセンスを示す、スタンドアロン ユニットの **show activation-key** コマンドの出力例を示します。

```
ciscoasa# show activation-key

Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.
```

```
The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

例 4-2　show activation-key detail のスタンドアロン ユニットの出力

次に、実行ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）、および永続ライセンスとインストールされている各時間ベース ライセンス（アクティブおよび非アクティブ）を示す、スタンドアロン ユニットの **show activation-key detail** コマンドの出力例を示します。

```
ciscoasa# show activation-key detail

Serial Number:  88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5512-X Security Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
```

```
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days

Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers                   : 25     7 days
```

例 4-3　show activation-key detail のフェールオーバー ペアのプライマリ ユニットの出力

次に、プライマリ フェールオーバー ユニットの **show activation-key detail** コマンドの出力例を示します。次の内容が表示されています。

- プライマリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- プライマリ ユニットの永続ライセンス。
- プライマリ ユニットのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.
```

```
Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers       : 4           perpetual
AnyConnect Essentials            : Disabled       perpetual
Other VPN Peers                  : 750            perpetual
Total VPN Peers                  : 750            perpetual
Shared License                   : Disabled       perpetual
AnyConnect for Mobile            : Disabled       perpetual
AnyConnect for Cisco VPN Phone   : Disabled       perpetual
Advanced Endpoint Assessment     : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers         : 2              perpetual
AnyConnect Essentials            : Disabled       perpetual
Other VPN Peers                  : 750            perpetual
Total VPN Peers                  : 750            perpetual
Shared License                   : Disabled        perpetual
AnyConnect for Mobile            : Disabled       perpetual
AnyConnect for Cisco VPN Phone   : Disabled       perpetual
Advanced Endpoint Assessment     : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter          : Enabled    33 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts              : 2          7 days
AnyConnect Premium Peers                  : 100        7 days

0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions        : 100        14 days
```

例 4-4　show activation-key detail のフェールオーバー ペアのセカンダリ ユニットの出力

次に、セカンダリ フェールオーバー ユニットの **show activation-key detail** コマンドの出力例を示します。次の内容が表示されています。

セカンダリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。

- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- セカンダリ ユニットの永続ライセンス。
- セカンダリのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。このユニットには時間ベース ライセンスはないため、この出力例には何も表示されません。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 10             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
```

```
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
```

例 4-5　show activation-key のライセンスがない ASAv のスタンドアロン ユニットの出力

展開した 1 つの vCPU ASAv の次の出力は、空白のアクティベーション キー、ライセンスなしの状態、1 つの vCPU ライセンスをインストールするメッセージを示しています。

（注） コマンド出力には「This platform has an ASAv VPN Premium license.」が表示されます。このメッセージは、ASAv がペイロード暗号化を実行できることを示しており、ASAv の標準ライセンスと Premium ライセンスを示しているのではありません。

```
ciscoasa# show activation-key
Serial Number: 9APM1G4RV41
Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000

ASAv Platform License State: Unlicensed
*Install 1 vCPU ASAv platform license for full functionality.
The Running Activation Key is not valid, using default settings:

Licensed features for this platform:
Virtual CPUs                   : 0              perpetual
Maximum Physical Interfaces    : 10             perpetual
Maximum VLANs                  : 50             perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
Encryption-DES                 : Enabled        perpetual
Encryption-3DES-AES            : Enabled        perpetual
Security Contexts              : 0              perpetual
```

```
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

Failed to retrieve flash permanent activation key.
The flash permanent activation key is the SAME as the running permanent key.
```

例 4-6　show activation-key の vCPU 標準ライセンスを 4 つ所有する ASAv のスタンドアロン ユニットの出力

（注） コマンド出力には「This platform has an ASAv VPN Premium license.」が表示されます。このメッセージは、ASAv がペイロード暗号化を実行できることを示しており、ASAv の標準ライセンスと Premium ライセンスを示しているのではありません。

```
ciscoasa# show activation-key
Serial Number: 9ALQ8W1XCJ7
Running Permanent Activation Key: 0x0013e945 0x685a232c 0x1153fdac 0xeae8b068 0x4413f4ae

ASAv Platform License State: Compliant

Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

The flash permanent activation key is the SAME as the running permanent key.
```

例 4-7　show activation-key の vCPU Premium ライセンスを 4 つ所有する ASAv のスタンドアロン ユニットの出力

（注）　コマンド出力には「This platform has an ASAv VPN Premium license.」が表示されます。このメッセージは、ASAv がペイロード暗号化を実行できることを示しており、ASAv の標準ライセンスと Premium ライセンスを示しているのではありません。

```
ciscoasa# show activation-key
Serial Number: 9ALQ8W1XCJ7
Running Permanent Activation Key: 0x8224dd7d 0x943ed77c 0x9d71cdd0 0xd90474d0 0xcb04df82

ASAv Platform License State: Compliant

Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 750            perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Enabled        perpetual
AnyConnect for Cisco VPN Phone    : Enabled        perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

The flash permanent activation key is the SAME as the running permanent key.
ciscoasa#
```

例 4-8　show activation-key のフェールオーバー ペアでの ASA サービス モジュール プライマリ ユニットの出力

次に、プライマリ フェールオーバー ユニットの **show activation-key** コマンドの出力例を示します。次の内容が表示されています。

- プライマリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- プライマリ ユニットのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。

```
ciscoasa# show activation-key

erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter           : Enabled    330 days
```

例 4-9　show activation-key のフェールオーバー ペアでの ASA サービス モジュール セカンダリ ユニットの出力

次に、セカンダリ フェールオーバー ユニットの **show activation-key** コマンドの出力例を示します。次の内容が表示されています。

- セカンダリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- セカンダリのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。このユニットには時間ベース ライセンスはないため、この出力例には何も表示されません。

```
ciscoasa# show activation-key detail

Serial Number:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
```

```
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Disabled       perpetual
Botnet Traffic Filter             : Disabled       perpetual

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.
```

例 4-10　クラスタでの show activation-key の出力

```
ciscoasa# show activation-key
 Serial Number: JMX1504L2TD
 Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9

 Licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 2 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 2 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 2 perpetual
 Total UC Proxy Sessions : 2 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual

 This platform has an ASA 5585-X base license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
```

```
 Security Contexts : 4 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 4 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 4 perpetual
 Total UC Proxy Sessions : 4 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual

 This platform has an ASA 5585-X base license.

The flash permanent activation key is the SAME as the running permanent key.
```

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、次のいずれかのコマンドを入力します。

コマンド	目的
show shared license [**detail** | **client** [*hostname*] | **backup**]	共有ライセンス統計情報を表示します。オプション キーワードはライセンス サーバだけに使用できます。**detail** キーワードを使用すると、参加システムごとの統計情報が表示されます。表示内容を 1 台の参加システムに限定するには、**client** キーワードを使用します。**backup** キーワードを使用すると、バックアップ サーバに関する情報が表示されます。 共有ライセンスの統計情報をクリアするには、**clear shared license** コマンドを入力します。
show activation-key	ASA にインストールされているライセンスを表示します。**show version** コマンドでもライセンス情報が表示されます。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

例

次に、ライセンス参加ユニットでの **show shared license** コマンドの出力例を示します。

```
ciscoasa>  show shared license
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive

Shared license utilization:
SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
```

```
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
```

次に、ライセンス サーバ上での **show shared license detail** コマンドの出力例を示します。

```
ciscoasa>  show shared license detail
Backup License Server Info:

Device ID           : ABCD
Address: 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

Shared license utilization:
SSLVPN:
    Total for network :      500
    Available         :      500
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0


Client Info:

Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
...
```

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。

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。
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。

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 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。 **speed** コマンドを使用してインターフェイスの速度を変更します。また、**show interface** コマンドを使用して各インターフェイスの現在の設定速度を確認します。
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。

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
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。
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、**webvpn** を使用し、次に **no anyconnect-essentials** コマンド 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。

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
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。
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。 **show activation-key** および **show version** の各コマンドが変更されました。
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。 **show activation-key** および **show version** の各コマンドが変更されました。

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
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。 **activation-key** [**activate** | **deactivate**] コマンドが変更されました。
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。
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 Peers」から「AnyConnect Premium Peers」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 VPN	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
クラスタリングの ASA 5500-X のサポート	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、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、基本ライセンスにおいてデフォルトでイネーブルになります。ASA 5512-X の場合は、Security Plus ライセンスが必要です。
ASA 5585-X の 16 個のクラスタ メンバのサポート	9.2(1)	ASA 5585-X は、16 ユニットの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。

CHAPTER 5

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」（P.5-1）
- 「ファイアウォール モードのライセンス要件」（P.5-8）
- 「デフォルト設定」（P.5-8）
- 「ガイドラインと制限事項」（P.5-8）
- 「ファイアウォール モードの設定」（P.5-10）
- 「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」（P.5-11）
- 「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」（P.5-13）
- 「トランスペアレント ファイアウォールのモニタリング」（P.5-14）
- 「ファイアウォール モードの例」（P.5-15）
- 「ファイアウォール モードの機能履歴」（P.5-26）

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」（P.5-2）
- 「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」（P.5-2）

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。

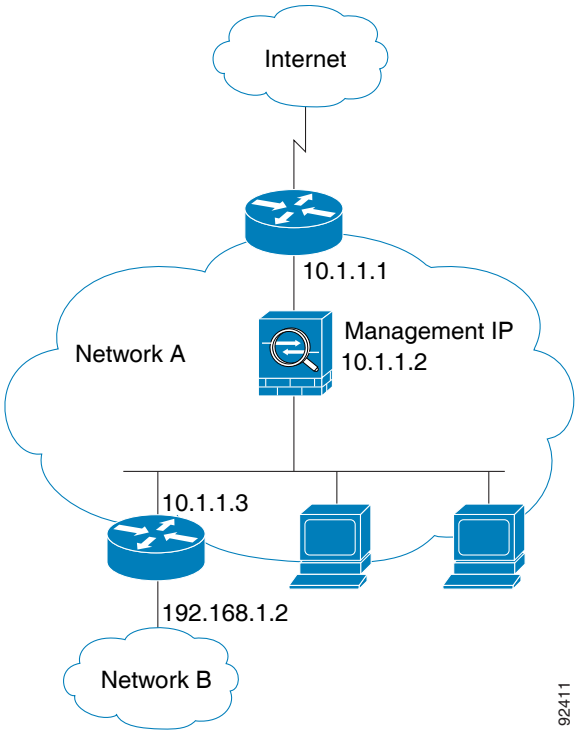
- 「ネットワークでのトランスペアレント ファイアウォールの使用」（P.5-2）
- 「ブリッジ グループ」（P.5-3）
- 「管理インターフェイス（ASA 5512-X 以降）」（P.5-4）
- 「レイヤ 3 トラフィックの許可」（P.5-4）
- 「許可される MAC アドレス」（P.5-5）
- 「ルーテッド モードで許可されないトラフィックの通過」（P.5-5）
- 「BPDU の処理」（P.5-6）
- 「MAC アドレス ルックアップと ルート ルックアップ」（P.5-6）
- 「ARP インスペクション」（P.5-7）
- 「MAC アドレス テーブル」（P.5-7）

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

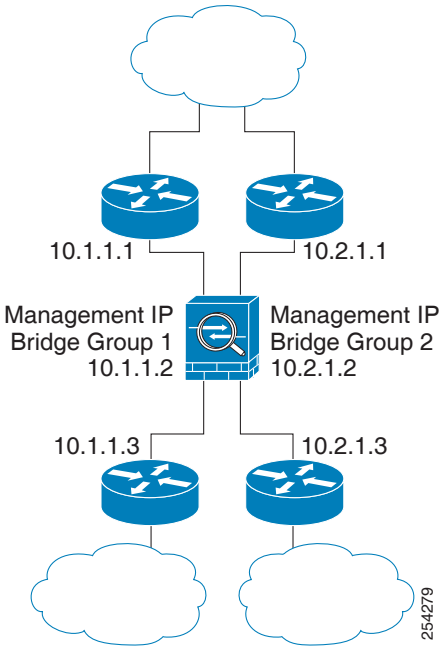


ブリッジ グループ

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、別の管理 *スロット/ポート* 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.9-2）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、HSRP や VRRP などのプロトコルも 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.7-16）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 インスペクション

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 スプーフィングが可能な場合、「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 アドレス テーブル

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 テーブルを学習し、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。このテーブルでは MAC アドレスと送信元インターフェイスが関連付けられているため、ASA はデバイスのアドレスが指定されたパケットを正しいインターフェイスに送信できます。

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ディング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学習します。
- 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学習します。

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ディングします。
- 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入力トラフィック の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。

ガイドラインと制限事項

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。

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に関するガイドラインと制限事項」（P.12-5）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。テキスト ファイルのダウンロードの詳細については、「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」（P.36-22）を参照してください。

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	—

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 （続き）

機能	説明
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 モードの設定

（注） この項では、ファイアウォール モードを変更する方法を説明します。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、「ガイドラインと制限事項」（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。「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.36-27）を参照してください。
- 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、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） コンフィギュレーションがクリア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、Customizing ASDM Access (ASA 5512-X and Higher, ASAv), page 2-9 または Customizing ASDM Access (ASA 5512-X and Higher, ASAv), page 2-9 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

ここでは、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」（P.5-11）
- 「スタティック ARP エントリの追加」（P.5-11）
- 「ARP インスペクションのイネーブル化」（P.5-12）

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

コマンド	目的
arp *interface_name ip_address mac_address* **例：** `ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100`	スタティック ARP エントリを追加します。

例

たとえば、外部インターフェイスで、IP アドレスが 10.1.1.1、MAC アドレスが 0009.7cbe.2100 のルータからの ARP 応答を許可するには、次のコマンドを入力します。

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

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

コマンド	目的
arp-inspection *interface_name* **enable** [**flood** | **no-flood**] **例：** `ciscoasa(config)# arp-inspection outside enable no-flood`	ARP インスペクションをイネーブルにします。 **flood** キーワードは、一致しない ARP パケットをすべてのインターフェイスに転送し、**no-flood** は、一致しないパケットをドロップします。 **（注）** デフォルト設定では、一致しないパケットはフラッディングします。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するには、このコマンドを **no-flood** に設定します。

例

たとえば、外部インターフェイスで ARP インスペクションをイネーブルにして、一致しないすべての ARP パケットをドロップするには、次のコマンドを入力します。

```
ciscoasa(config)# arp-inspection outside enable no-flood
```

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 タイムアウトの設定」（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、次のコマンドを入力します。

コマンド	目的
mac-address-table static *interface_name mac_address* **例：** `ciscoasa(config)# mac-address-table static inside 0009.7cbe.2100`	スタティック MAC アドレス エントリを追加します。 *interface_name* は、発信元インターフェイスです。

MAC アドレス タイムアウトの設定

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 分ですが、タイムアウトは変更できます。タイムアウトを変更するには、次のコマンドを入力します。

コマンド	目的
mac-address-table aging-time *timeout_value* **例：** `ciscoasa(config)# mac-address-table aging-time 10`	MAC アドレス エントリのタイムアウトを設定します。 *timeout_value*（分）は、5 ～ 720（12 時間）です。5 分がデフォルトです。

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入力トラフィックの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、次のコマンドを入力します。

コマンド	目的
mac-learn *interface_name* **disable** **例：** `ciscoasa(config)# mac-learn inside disable`	MAC アドレス ラーニングをディセーブルにします。 このコマンドの **no** 形式を使用すると、MAC アドレス ラーニングが再度イネーブルになります。**clear configure mac-learn** コマンドは、すべてのインターフェイスで MAC アドレス ラーニングを再度イネーブルにします。

トランスペアレント ファイアウォールのモニタリング

- 「ARP インスペクションのモニタリング」（P.5-14）
- 「MAC アドレス テーブルのモニタリング」（P.5-14）

ARP インスペクションのモニタリング

ARP インスペクションをモニタするには、次のタスクを実行します。

コマンド	目的
show arp-inspection	すべてのインターフェイスについて、ARP インスペクションの現在の設定を表示します。

MAC アドレス テーブルのモニタリング

MAC アドレス テーブル全体（両方のインターフェイスのスタティック エントリとダイナミック エントリを含む）を表示できます。または、あるインターフェイスの MAC アドレス テーブルを表示できます。MAC アドレス テーブルを表示するには、次のコマンドを入力します。

コマンド	目的
show mac-address-table [*interface_name*]	MAC アドレス テーブルを表示します。

例

すべてのテーブルを表示する **show mac-address-table** コマンドの出力例を示します。

```
ciscoasa# show mac-address-table
interface          mac address       type      Time Left
-----------------------------------------------------------------------
outside            0009.7cbe.2100    static      -
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

内部インターフェイスのテーブルを表示する **show mac-address-table** コマンドの出力例を示します。

```
ciscoasa# show mac-address-table inside
interface          mac address       type      Time Left
-----------------------------------------------------------------------
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

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.5-15）
- 「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.5-21）

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

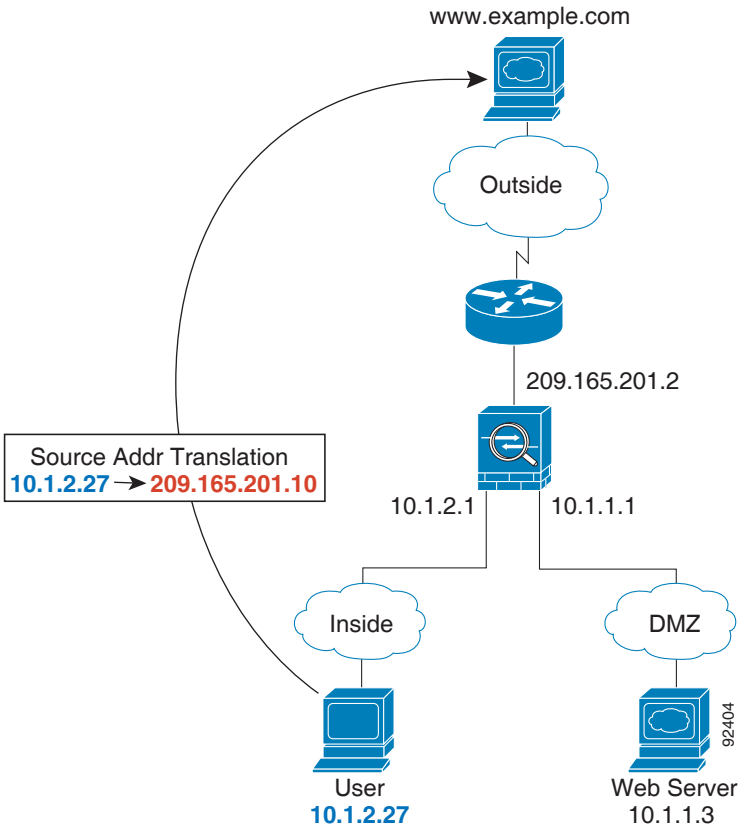
ここでは、ルーテッド ファイアウォール モードでデータが ASA をどのように通過するのかを説明します。

- 「内部ユーザが Web サーバにアクセスする」（P.5-16）
- 「外部ユーザが DMZ 上の Web サーバにアクセスする」（P.5-17）
- 「内部ユーザが DMZ 上の Web サーバにアクセスする」（P.5-18）
- 「外部ユーザが内部ホストにアクセスしようとする」（P.5-19）
- 「DMZ ユーザが内部ホストにアクセスしようとする」（P.5-20）

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。

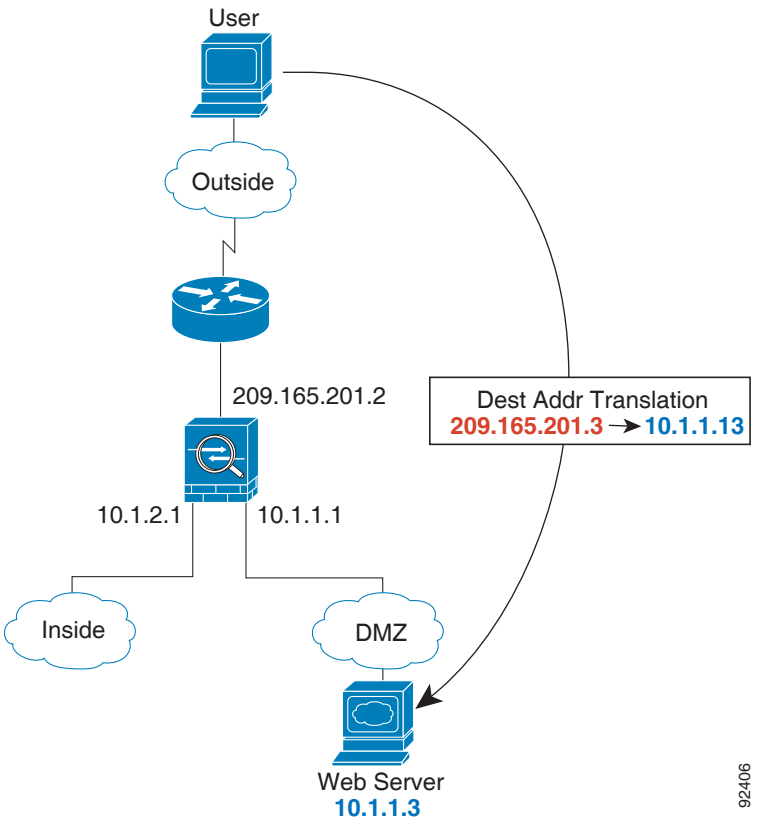
   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. ASA は、ローカル送信元アドレス（10.1.2.27）を、外部インターフェイス サブネット上のグローバル アドレス 209.165.201.10 に変換します。

   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）。

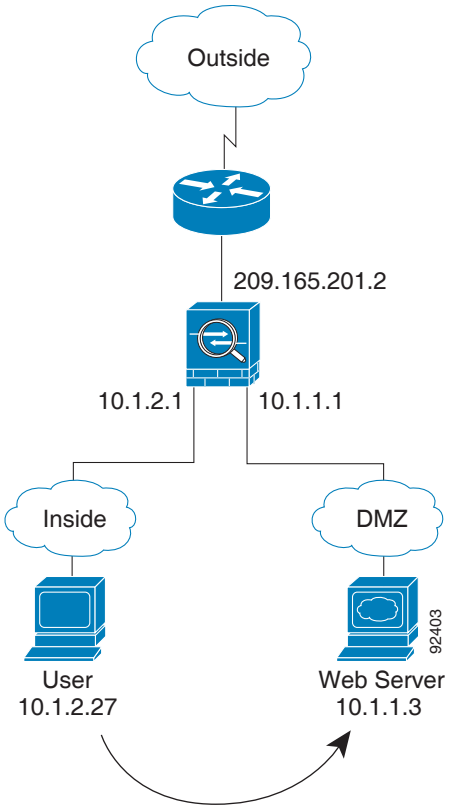
1. 外部ネットワーク上のユーザは、外部インターフェイス サブネット上にあるグローバル宛先アドレス 209.165.201.3 を使用して DMZ Web サーバから Web ページを要求します。
2. ASA は、パケットを受信し、宛先アドレスをローカル アドレスの 10.1.1.3 には変換しません。
3. 新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、ASA はパケットが許可されていることを確認します。

   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）。

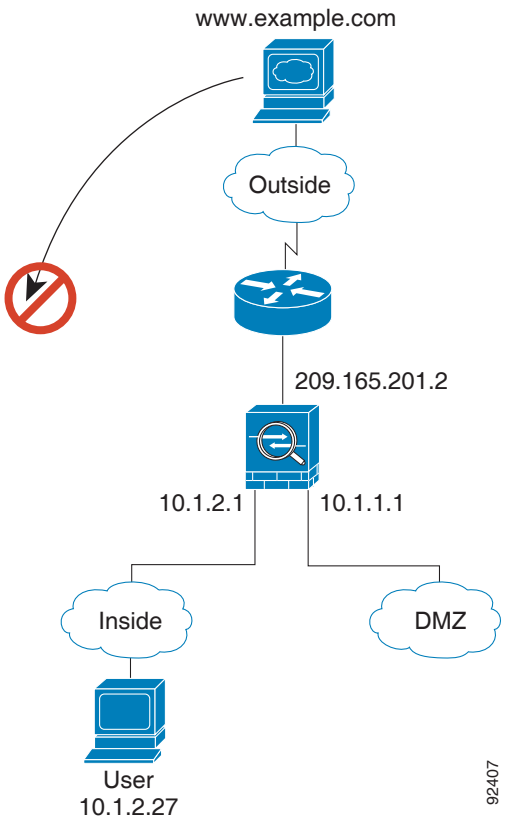
1. 内部ネットワーク上のユーザは、宛先アドレス 10.1.1.3 を使用して DMZ Web サーバから Web ページを要求します。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

   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。

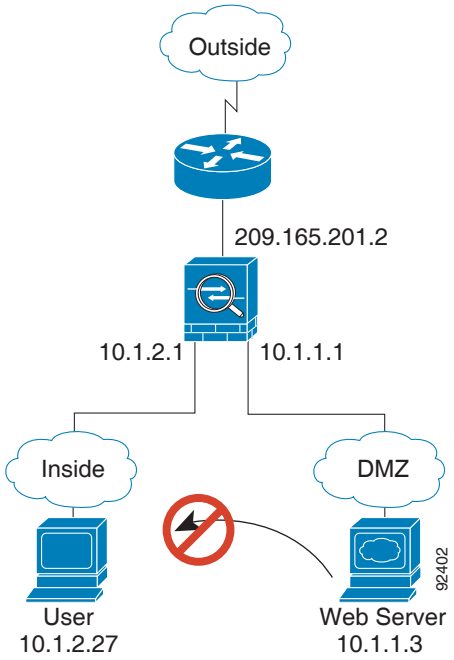
3. パケットが拒否され、ASA はパケットをドロップし、接続試行をログに記録します。

   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）。

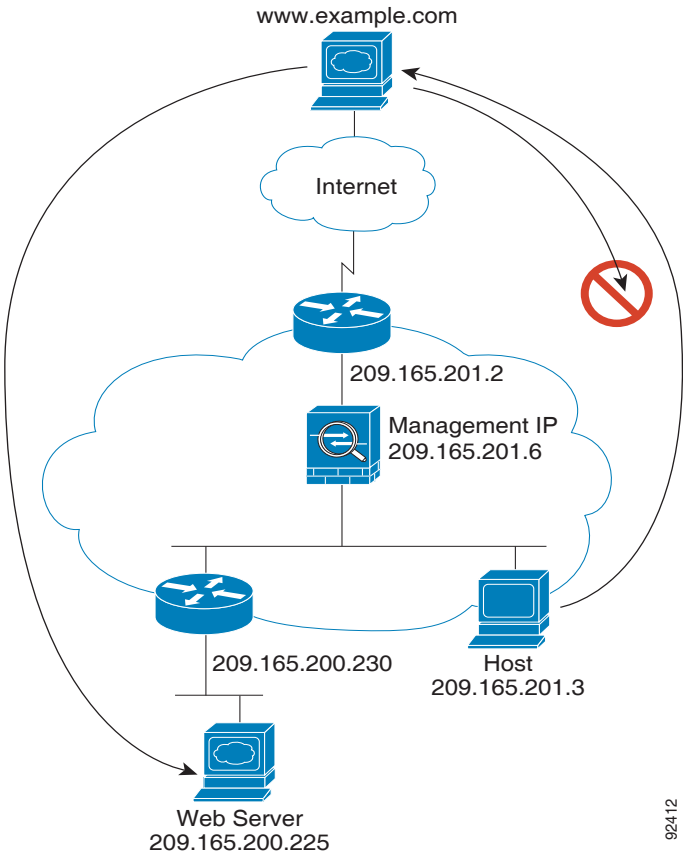
1. DMZ ネットワーク上のユーザが、内部ホストに到達しようとします。DMZ はインターネット上のトラフィックをルーティングする必要がないので、プライベート アドレッシング方式はルーティングを回避しません。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）に従って、パケットが許可されているかどうかを確認します。

   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



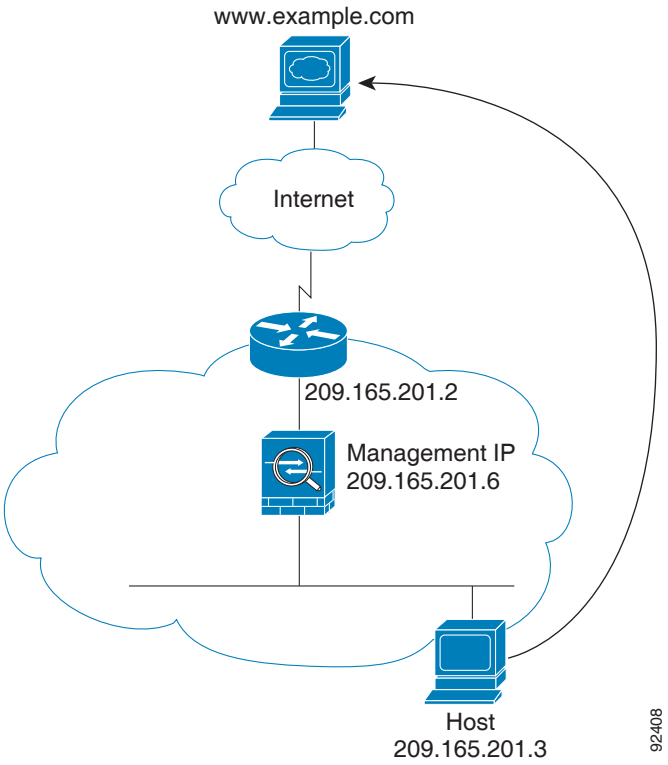
ここでは、データが ASA をどのように通過するかを示します。

- 「内部ユーザが Web サーバにアクセスする」（P.5-22）
- 「NAT を使用して内部ユーザが Web サーバにアクセスする」（P.5-23）
- 「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.5-24）
- 「外部ユーザが内部ホストにアクセスしようとする」（P.5-25）

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。

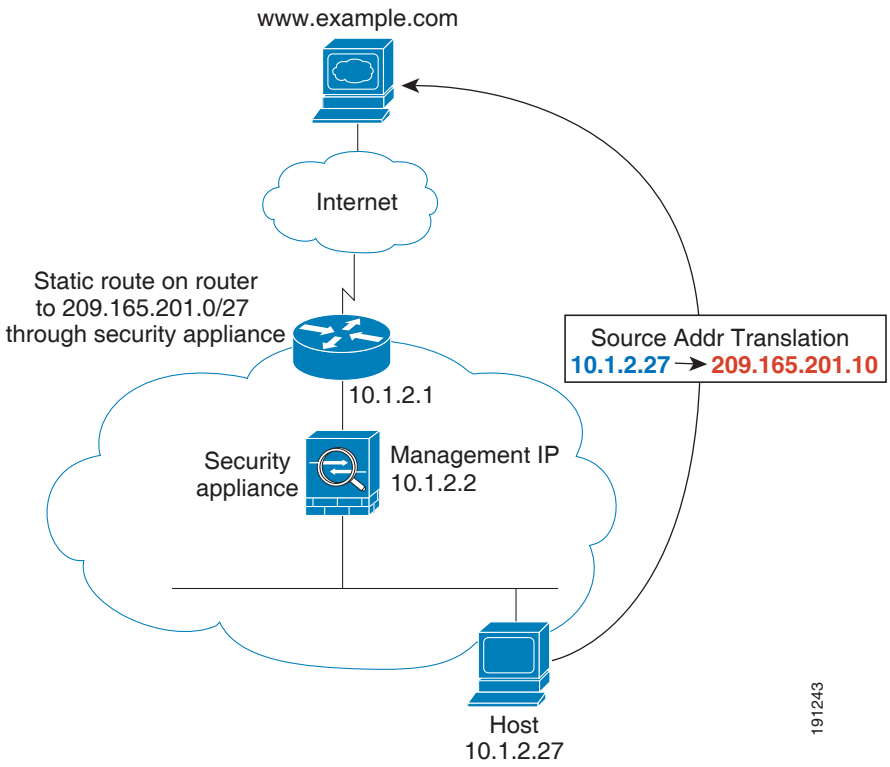
   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. ASA は、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、ASA は外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータのアドレス 209.165.201.2 です。

   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。

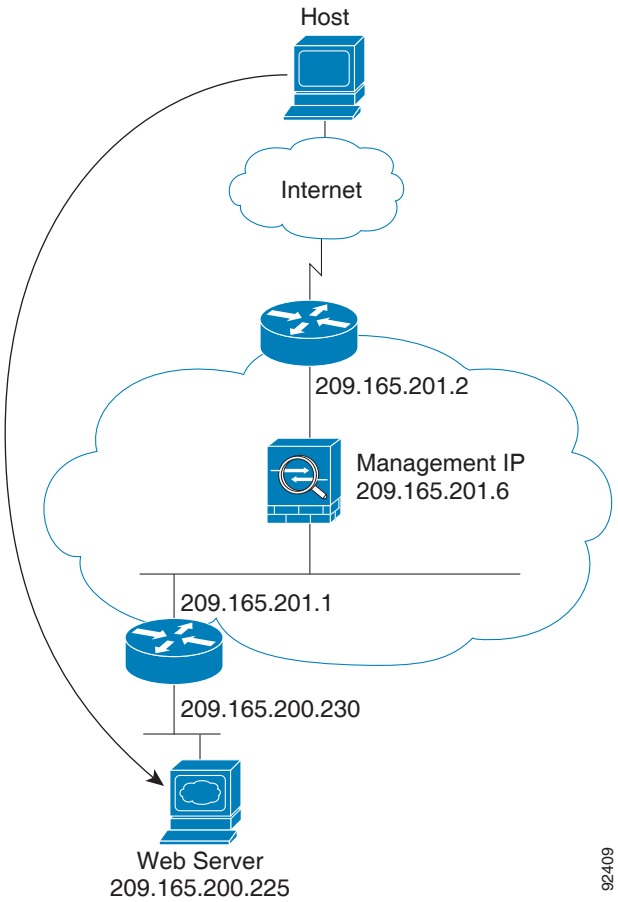
   宛先 MAC アドレスが ASA のテーブルにない場合、ASA は、ARP 要求と ping を送信して、MAC アドレスを検出しようとします。最初のパケットはドロップされます。

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。

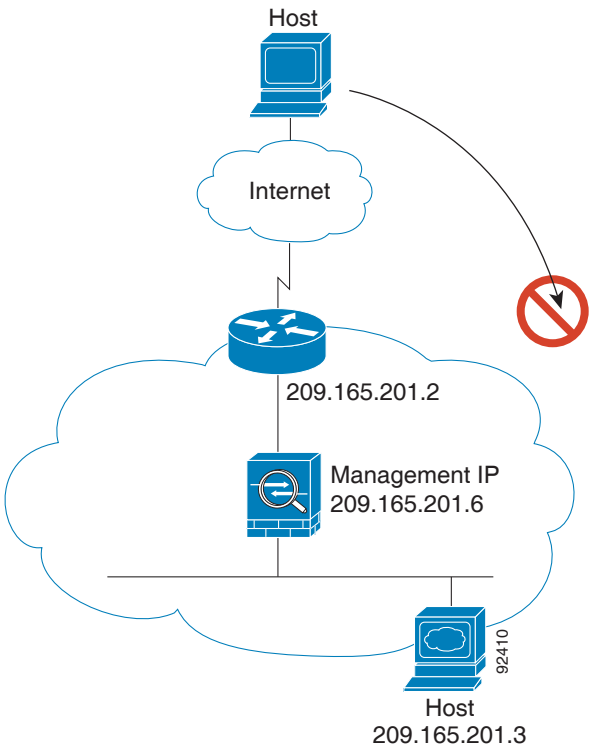
4. 宛先 MAC アドレスがテーブル内にある場合、ASA は内部インターフェイスからパケットを転送します。宛先 MAC アドレスは、ダウンストリーム ルータ 209.165.201.1 のアドレスです。

   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。

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。
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。 **interface bvi**、**bridge-group**、**show bridge-group** の各コマンドが導入されました。

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。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）攻撃を容易にする可能性があります。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ための隣接ルートのプロキシ ARP。 **arp permit-nonconnected** コマンドが導入されました。
マルチ コンテキスト モードのファイアウォール モードの混合をサポート	8.5(1)/9.0(1)	マルチ コンテキスト モードでのセキュリティ コンテキスト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。
トランスペアレント モードのブリッジ グループの最大数を 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 個のブリッジ グループに増加されました。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追加できます。 **interface bvi** および **bridge-group** コマンドが変更されました。

PART 2

ハイ アベイラビリティとスケーラビリティ

CHAPTER 6

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」（P.6-1）
- 「マルチ コンテキスト モードのライセンス要件」（P.6-14）
- 「ガイドラインと制限事項」（P.6-14）
- 「デフォルト設定」（P.6-15）
- 「マルチ コンテキストの設定」（P.6-16）
- 「コンテキストとシステム実行スペースの切り替え」（P.6-26）
- 「セキュリティ コンテキストの管理」（P.6-27）
- 「セキュリティ コンテキストのモニタリング」（P.6-31）
- 「マルチ コンテキスト モードの設定例」（P.6-42）
- 「マルチ コンテキスト モードの機能履歴」（P.6-43）

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、「ガイドラインと制限事項」（P.6-14）を参照してください。

ここでは、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」（P.6-2）
- 「コンテキスト コンフィギュレーション ファイル」（P.6-2）
- 「ASA によるパケットの分類方法」（P.6-3）
- 「セキュリティ コンテキストのカスケード接続」（P.6-7）
- 「セキュリティ コンテキストへの管理アクセス」（P.6-7）
- 「リソース管理に関する情報」（P.6-8）
- 「MAC アドレスに関する情報」（P.6-12）

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

ここでは、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.6-2）
- 「システム設定」（P.6-2）
- 「管理コンテキストの設定」（P.6-3）

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.6-3）
- 「分類の例」（P.6-4）

（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

ここでは、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.6-3）
- 「固有の MAC アドレス」（P.6-4）
- 「NAT コンフィギュレーション」（P.6-4）

（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。

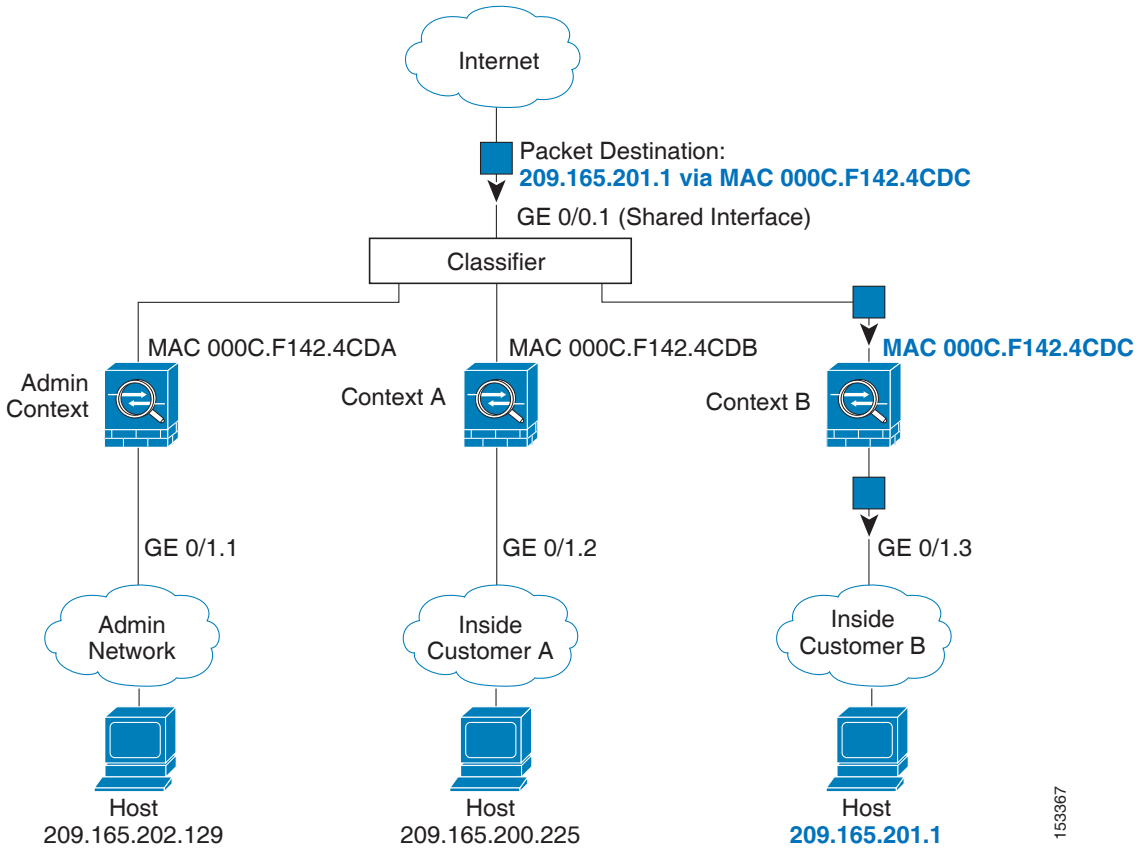
NAT コンフィギュレーション

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

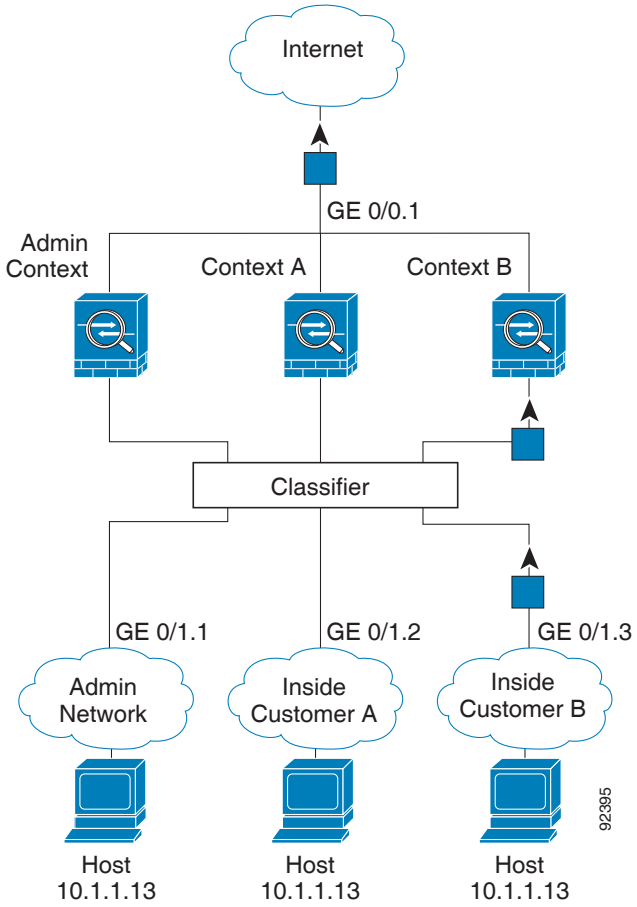
図 6-1 に、外部インターフェイスを共有するマルチ コンテキストを示します。コンテキスト B にはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをコンテキスト B に割り当てます。

図 6-1　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



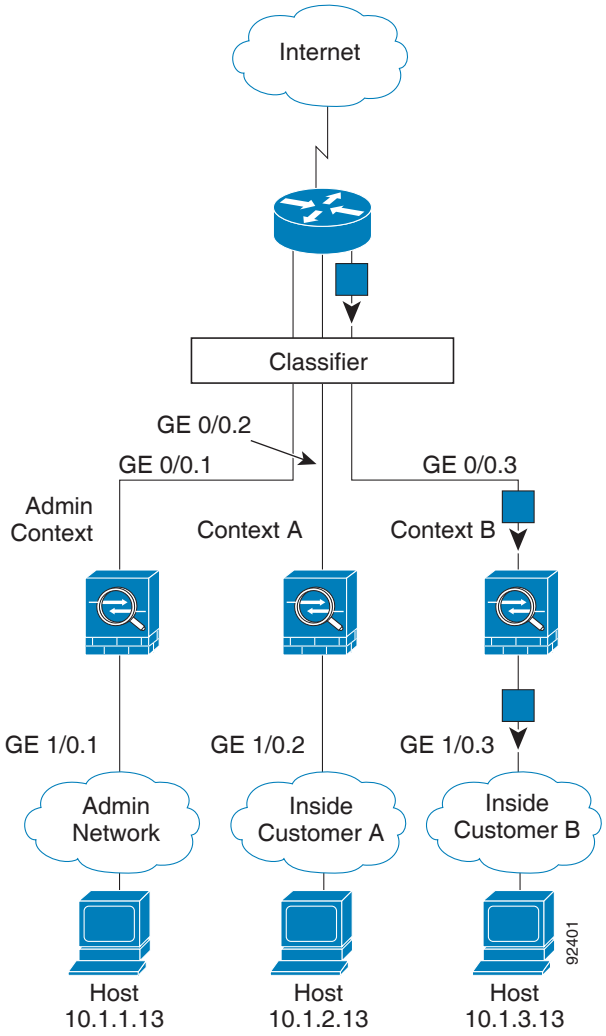
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。図 6-2 に、内部ネットワークのコンテキスト B 上のホストがインターネットにアクセスしている場合を示します。分類子は、パケットをコンテキスト B に割り当てます。これは、入力インターフェイスがギガビット イーサネット 0/1.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 6-2　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 6-3 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 6-3　トランスペアレント ファイアウォールのコンテキスト



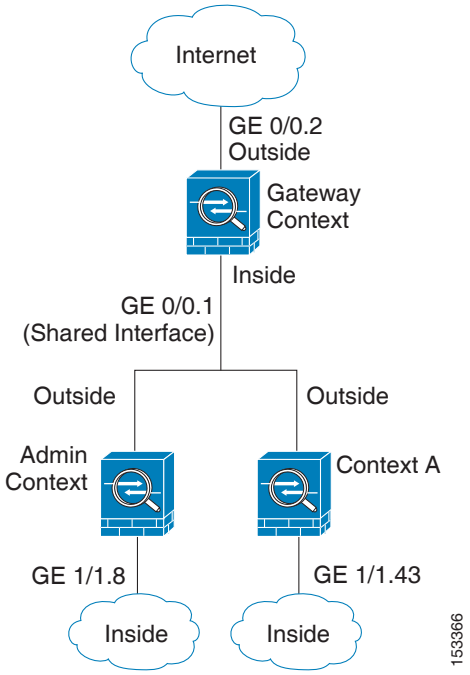
セキュリティ コンテキストのカスケード接続

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 6-4 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 6-4　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.6-8）
- 「コンテキスト管理者のアクセス」（P.6-8）

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する

  コンソールから*システム実行スペース*にアクセスします。この場合、入力したコマンドは、システム コンフィギュレーションまたはシステムの実行（run-time コマンド）だけに影響します。

- Telnet、SSH、または ASDM を使用して管理コンテキストにアクセスする

  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 35 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「enable_15」ユーザ名に変更されます。そのコンテキストでコマンド許可を設定した場合は、「enable_15」というユーザの許可特権を設定する必要があります。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 35 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」（P.6-9）
- 「リソース制限値」（P.6-9）
- 「デフォルト クラス」（P.6-9）
- 「オーバーサブスクライブ型リソースの使用」（P.6-10）
- 「無制限リソースの使用」（P.6-11）

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 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。

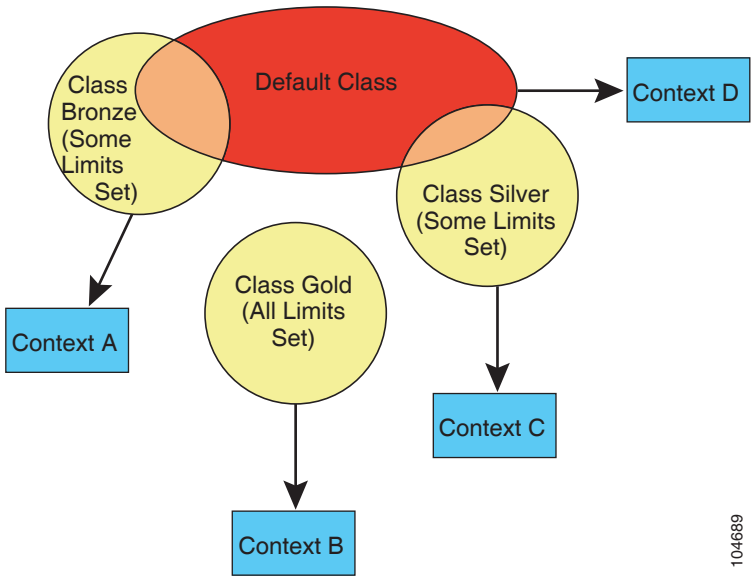
コンテキストがデフォルト クラス以外のクラスに属する場合、それらのクラス設定は常にデフォルト クラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバ コンテキストはそれらの制限にデフォルト クラスを使用します。たとえば、すべての同時接続に 2% の制限を設定したがその他の制限を設定せずにクラスを作成した場合、他のすべての制限はデフォルト クラスから継承されます。これとは逆に、すべてのリソースに対する制限値を設定してクラスを作成すると、そのクラスではデフォルト クラスの設定を何も使用しません。

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 6-5 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。

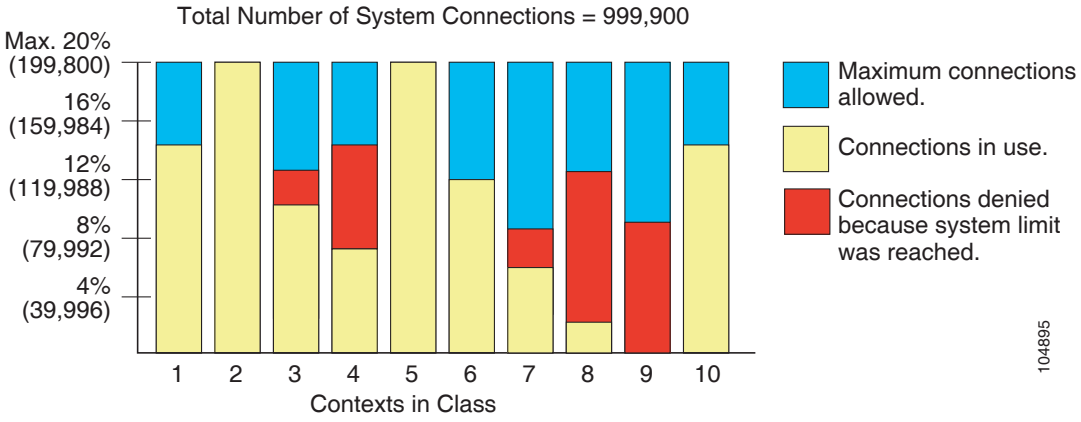
図 6-5　　リソース クラス



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 6-6 を参照）。

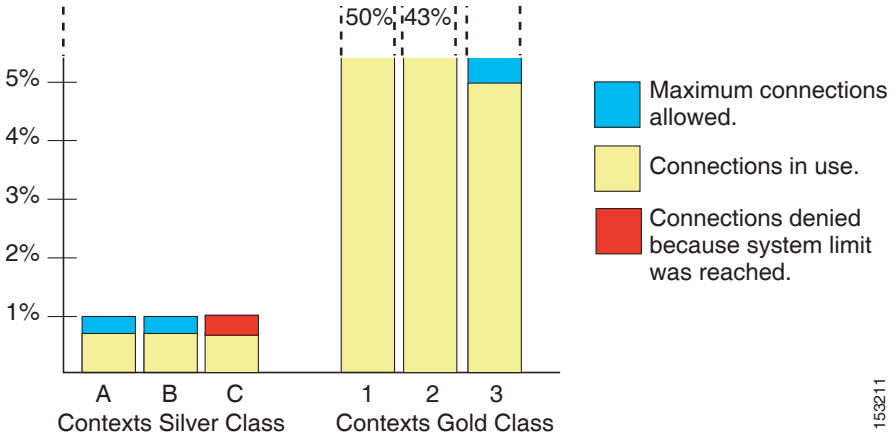
図 6-6　リソースのオーバーサブスクライブ



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 6-7 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 6-7　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、デフォルトでASA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.6-26）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.6-3）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、TCP MSS の設定」（P.11-10）を参照してください。

- 「デフォルトの MAC アドレス」（P.6-12）
- 「手動 MAC アドレスとの通信」（P.6-13）
- 「フェールオーバー用の MAC アドレス」（P.6-13）
- 「MAC アドレス形式」（P.6-13）

デフォルトの MAC アドレス

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.6-13）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.6-13）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としてたとえば、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 アドレスで使用されるときに、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：サポートしない • 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はシステムまたは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。

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。

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.6-9）を参照してください。
- 「デフォルトの MAC アドレス」（P.6-12）を参照してください。

マルチ コンテキストの設定

ここでは、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」（P.6-16）
- 「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.6-16）
- 「リソース管理のクラスの設定」（P.6-18）
- 「セキュリティ コンテキストの設定」（P.6-21）
- 「コンテキスト インターフェイスへの MAC アドレスの自動割り当て」（P.6-26）

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.6-16）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.6-18）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 9 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 3 章「Cisco ASA サービス モジュール向けのスイッチの設定」

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.6-21）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.6-26）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 11 章「ルーテッド モードのインターフェイス」または第 12 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。

- 「マルチ コンテキスト モードのイネーブル化」（P.6-17）
- 「シングルコンテキスト モードの復元」（P.6-17）

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。「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.36-27）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 6-1 に、リソース タイプと制限を示します。**show resource types** コマンドも参照してください。

表 6-1　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	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。
conns[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	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-addresses	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。

表 6-1　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
vpn burst other	同時接続数	該当なし	モデルに応じた Other VPN セッション数から、**vpn other** 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。	**vpn other** 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、**vpn other** 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 **vpn burst other** 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 **vpn other** とは異なり、**vpn burst other** 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。
vpn other	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	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

	コマンド	目的
ステップ 1	**class** *name* **例：** ciscoasa(config)# class gold	クラス名を指定して、クラス コンフィギュレーション モードを開始します。*name* は、最大 20 文字の文字列です。デフォルト クラスの制限値を設定するには、名前として **default** と入力します。
ステップ 2	**limit-resource** [**rate**] *resource_name number*[**%**] **例：** ciscoasa(config-class)# limit-resource rate inspects 10	リソース タイプのリソース制限を設定します。リソース タイプのリストについては、表 6-1 を参照してください。**all** を指定すると、すべてのリソースが同じ値に設定されます。特定のリソースの値も指定した場合は、その制限は **all** に対して設定された制限よりも優先されます。 **rate** 引数を入力して、特定のリソースの毎秒あたりのレートを設定します。 ほとんどのリソースについては、**0** を *number* に対して設定すると、そのリソースは無制限となるか、システム制限を上限とする（システム制限がある場合）ことになります。VPN のリソースについては、**0** を指定すると制限なしと設定されます。 システム制限がないリソースの場合は、パーセンテージ（**%**）を設定できません。絶対値のみを設定できます。

例

たとえば、conns のデフォルト クラス制限を無制限ではなく 10% に設定し、サイトツーサイト VPN トンネル 5 本と VPN バースト用のトンネル 2 本を許可するには、次のコマンドを入力します。

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 5
ciscoasa(config-class)# limit-resource vpn burst other 2
```

他のリソースはすべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 5000
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5
```

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 3 章「Cisco ASA サービス モジュール向けのスイッチの設定」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 9 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。
- 管理コンテキストがない場合（コンフィギュレーションをクリアした場合など）は、最初に次のコマンドを入力して管理コンテキスト名を指定する必要があります。

  ```
  ciscoasa(config)# admin-context name
  ```

  このコンテキストはコンフィギュレーション内にまだ存在しませんが、続いて **context** *name* コマンドを入力して管理コンテキスト コンフィギュレーションに進むことができます。

手順の詳細

	コマンド	目的
ステップ 1	**context** *name* **例：** `ciscoasa(config)# context administrator`	コンテキストを追加または編集します。*name* は最大 32 文字の文字列です。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。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンは使用できません。 「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 2	（オプション） **description** *text* **例：** `ciscoasa(config-ctx)# description Administrator Context`	このコンテキストの説明を追加します。

	コマンド	目的
ステップ 3	インターフェイスを割り当てるには： **allocate-interface** *interface_id* [*mapped_name*] [**visible** | **invisible**] 1 つまたは複数のサブインターフェイスを割り当てるには： **allocate-interface** *interface_id.subinterface*[-*interface_id.subinterface*] [*mapped_name*[-*mapped_name*]] [**visible** | **invisible**] **例：** ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1 ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2 ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305 int3-int8	コンテキストで使用できるインターフェイスを指定します。インターフェイス タイプとポート番号の間にスペースを含めないでください。 これらのコマンドを複数回入力して複数の範囲を指定します。このコマンドの **no** 形式を使用して割り当てを削除すると、このインターフェイスを含むコンテキスト コマンドすべてが実行コンフィギュレーションから削除されます。 トランスペアレント ファイアウォール モードでは、限られた数のインターフェイスのみがトラフィックを通過させることができます。ただし、専用の管理インターフェイスである管理*スロット/ポート*（物理、サブインターフェイス、冗長、または EtherChannel）を管理トラフィック用の追加インターフェイスとして使用できます。独立した管理インターフェイスは、ASASM では使用できません。 ルーテッド モードでは、必要に応じて同じインターフェイスを複数のコンテキストに割り当てることができます。トランスペアレント モードでは、インターフェイスを共有できません。 *mapped_name* は、インターフェイスの英数字のエイリアスで、インターフェイス ID の代わりにコンテキスト内で使用できます。マッピング名を指定しない場合、インターフェイス ID がコンテキスト内で使用されます。セキュリティ目的で、コンテキストがどのインターフェイスを使用しているかをコンテキスト管理者には知らせないようにすることができます。マッピング名はアルファベットで始まり、アルファベットまたは数字で終わる必要があります。その間の文字には、アルファベット、数字、または下線のみを使用できます。たとえば、次の名前を使用できます。 **int0、inta、int_0** サブインターフェイスの範囲を指定する場合は、マッピング名の一致範囲を指定できます。範囲については、次のガイドラインに従ってください。 • マッピング名は、アルファベット部分と、それに続く数値部分で構成する必要があります。マッピング名のアルファベット部分は、範囲の両端で一致している必要があります。たとえば、次のような範囲を入力します。 **int0-int10** たとえば、gig0/1.1-gig0/1.5 **happy**1-**sad**5 と入力した場合、コマンドは失敗します。 • マッピング名の数値部分には、サブインターフェイスの範囲と同じ個数の数値を含める必要があります。たとえば、次の例では、両方の範囲に 100 個のインターフェイスが含まれています。 **gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100** たとえば、gig0/0.**100**-gig0/0.**199** int**1**-int**15** と入力した場合、コマンドは失敗します。 マッピング名を設定している場合に **show interface** コマンドで実際のインターフェイス ID を参照するには、**visible** を指定します。デフォルトの **invisible** キーワードでは、マッピング名のみが表示されます。

	コマンド	目的

ステップ 4	**config-url** *url*
	
	例：
	`ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg`
		システムがコンテキスト コンフィギュレーションをダウンロードする URL を識別します。コンテキストの URL を追加すると、そのコンテキストをただちにロードし、コンフィギュレーションが使用可能であればコンテキストを実行できるようにします。
		
		（注） **config-url** コマンドを入力する前に、**allocate-interface** コマンドを入力します。最初に **config-url** コマンドを入力した場合、ASA はただちにコンテキスト コンフィギュレーションをロードします。そのコンテキストが（未設定）インターフェイスを参照するコマンドを含んでいる場合、それらのコマンドは失敗します。
		
		ファイル名にファイル拡張子は必要ありませんが、「.cfg」を使用することを推奨します。管理コンテキストからサーバにアクセス可能である必要があります。コンフィギュレーション ファイルが存在しない場合は、次のメッセージが表示されます。
		
		`WARNING: Could not fetch the URL url`
		`INFO: Creating context with default config`
		
		HTTP（S）以外の URL の場合、対象 URL にファイルを書き込むには、URL を指定した後、そのコンテキストに変更し、CLI に設定して、**write memory** コマンドを入力します。（HTTP（S）は読み取り専用です）。
		
		（注） 管理コンテキスト ファイルは内部フラッシュ メモリに保存する必要があります。
		
		使用可能な URL は次のタイプがあります。**disk***number*（フラッシュ メモリ用）、**ftp**、**http**、**https**、または **tftp**。
		
		URL を変更するには、新しい URL で **config-url** コマンドを再入力します。URL の変更の詳細については、「セキュリティ コンテキスト URL の変更」（P.6-28）を参照してください。

ステップ 5	（オプション） **member** *class_name* **例：** `ciscoasa(config-ctx)# member gold`	コンテキストをリソース クラスに割り当てます。クラスを指定しない場合、コンテキストはデフォルト クラスに属します。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。
ステップ 6	（オプション） **allocate-ips** *sensor_name* [*mapped_name*] [**default**] **例：** `ciscoasa(config-ctx)# allocate-ips sensor1 highsec`	このコンテキストに IPS 仮想センサーを割り当てます（IPS モジュールがインストールされている場合）。 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。

	コマンド	目的
ステップ 7	（オプション） **join-failover-group** {**1** | **2**) **例：** ciscoasa(config-ctx)# join-failover-group 2	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 グループにコンテキストを割り当てます。デフォルトでは、コンテキストはグループ 1 にあります。管理コンテキストは常にグループ 1 に置く必要があります。 フェールオーバー グループに関する詳細については、「オプションのフェールオーバー パラメータの設定」（P.7-39）を参照してください。
ステップ 8	（オプション） **scansafe** [**license** *key*] **例：** ciscoasa(config-ctx)# scansafe	このコンテキストに対してクラウド Web セキュリティをイネーブルにします。 **license** を指定しない場合は、システム コンフィギュレーションで設定されているライセンスがこのコンテキストで使用されます。ASA は、要求がどの組織からのものかを示すために、認証キーを クラウド Web セキュリティ プロキシ サーバに送信します。認証キーは 16 バイトの 16 進数です。 ScanSafe 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。

例

次の例では、管理コンテキストを「administrator」と設定し、「administrator」というコンテキストを内部フラッシュ メモリに作成してから、2 つのコンテキストを FTP サーバから追加します。

```
ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold


ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

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.6-12）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.6-40）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 **nameif** コマンドを設定すると、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、TCP MSS の設定」（P.11-10）を参照してください。

手順の詳細

コマンド	目的
mac-address auto [**prefix** *prefix*] **例：** `ciscoasa(config)# mac-address auto prefix 19`	プライベート MAC アドレスを各コンテキスト インターフェイスに自動的に割り当てます。 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。 手動でプレフィックスを入力する場合は、*prefix* に 0 ～ 65535 の 10 進数値を指定します。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.6-13）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、つまり **copy** コマンドや **write** コマンドで使用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。たとえば、**show running-config** コマンドを入力しても、すべての実行コンフィギュレーション（システム コンテキストとすべてのコンテキスト）を表示することはできません。現在のコンフィギュレーションだけが表示されます。

手順の詳細

コマンド	目的
changeto context *name*	コンテキストに変更します。プロンプトが次のように変化します。 ciscoasa/*name*#
changeto system	システム実行スペースに切り替えます。プロンプトが次のように変化します。 ciscoasa#

セキュリティ コンテキストの管理

ここでは、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.6-27）
- 「管理コンテキストの変更」（P.6-28）
- 「セキュリティ コンテキスト URL の変更」（P.6-28）
- 「セキュリティ コンテキストのリロード」（P.6-30）

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。ただし、**clear context** コマンドを使用してすべてのコンテキストを削除すれば、管理コンテキストも削除できます。

（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。アクティブ装置とスタンバイ装置の間でインターフェイス数が一致していないことを示すエラー メッセージが表示される場合があります。このエラーは一時的に表示されるもので、無視できます。

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

コマンド	目的
no context *name*	1 つの コンテキストを削除します。すべてのコンテキスト コマンドも削除されます。コンテキスト コンフィギュレーション ファイルがコンフィギュレーション URL の場所から削除されることはありません。
clear context	すべてのコンテキスト（管理コンテキストを含みます）を削除します。コンテキスト コンフィギュレーション ファイルがコンフィギュレーション URL の場所から削除されることはありません。

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。

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

コマンド	目的
admin-context *context_name* **例：** `ciscoasa(config)# admin-context administrator`	管理コンテキストを設定します。Telnet、SSH、HTTPS 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

	コマンド	目的

ステップ 1	（マージを実行しない場合は、任意）
	changeto context *name*
	clear configure all
	
	例：
	`ciscoasa(config)# changeto context ctx1`
	`ciscoasa/ctx1(config)# clear configure all`
		コンテキストに切り替えて、設定を削除します。マージを実行する場合は、ステップ 2 にスキップします。

ステップ 2	**changeto system**
	
	例：
	`ciscoasa/ctx1(config)# changeto system`
	`ciscoasa(config)#`
		システム実行スペースに切り替えます。

ステップ 3	**context** *name* **例：** `ciscoasa(config)# context ctx1`	変更するコンテキストのコンテキスト コンフィギュレーション モードを開始します。
ステップ 4	**config-url** *new_url* **例：** `ciscoasa(config)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/ctx1.cfg`	新しい URL を入力します。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.6-30）
- 「コンテキストの削除および再追加によるリロード」（P.6-30）

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

	コマンド	目的

ステップ 1	**changeto context** *name*
	
	例：
	`ciscoasa(config)# changeto context ctx1`
	`ciscoasa/ctx1(comfig)#`
		リロードするコンテキストに変更します。

ステップ 2	**clear configure all** **例：** `ciscoasa/ctx1(config)# clear configure all`	実行コンフィギュレーションをクリアします。このコマンドを実行するとすべての接続がクリアされます。
ステップ 3	**copy startup-config running-config** **例：** `ciscoasa/ctx1(config)# copy startup-config running-config`	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、次の各項の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.6-27）
2. 「セキュリティ コンテキストの設定」（P.6-21）

セキュリティ コンテキストのモニタリング

ここでは、コンテキスト情報を表示およびモニタする方法について説明します。

- 「コンテキスト情報の表示」（P.6-31）
- 「リソース割り当ての表示」（P.6-32）
- 「リソースの使用状況の表示」（P.6-36）
- 「コンテキストでの SYN 攻撃のモニタリング」（P.6-38）
- 「割り当てられた MAC アドレスの表示」（P.6-40）

コンテキスト情報の表示

システム実行スペースから、名前、割り当てられているインターフェイス、コンフィギュレーション ファイル URL を含むコンテキストのリストを表示できます。

システム実行スペースから次のコマンドを入力すると、すべてのコンテキストが表示されます。

コマンド	目的
show context [*name* | **detail**| **count**]	すべてのコンテキストを表示します。 特定のコンテキストの情報を表示する場合は、*name* にコンテキスト名を指定します。 **detail** オプションを指定すると、追加情報が表示されます。詳細については、次の出力例を参照してください。 **count** オプションを指定すると、コンテキストの合計数が表示されます。

次に、**show context** コマンドの出力例を示します。この出力例は、3 個のコンテキストを示しています。

```
ciscoasa# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      disk0:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      disk0:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      disk0:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

表 6-2 に、各フィールドの説明を示します。

表 6-2　　show context のフィールド

フィールド	説明
Context Name	すべてのコンテキスト名が表示されます。アスタリスク（*）の付いているコンテキスト名は、管理コンテキストです。
Interfaces	このコンテキストに割り当てられたインターフェイス。
URL	ASA がコンテキストのコンフィギュレーションをロードする URL。

次に、**show context detail** コマンドの出力例を示します。

```
ciscoasa# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk0:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
Real Interfaces:
Mapped Interfaces:
Flags: 0x00000009, ID: 258
```

detail の出力の詳細については、コマンド リファレンスを参照してください。

次に、**show context count** コマンドの出力例を示します。

```
ciscoasa# show context count
Total active contexts: 2
```

リソース割り当ての表示

システム実行スペースから、すべてのクラスおよびクラス メンバーに渡るリソースごとの割り当て状況を表示できます。

リソース割り当てを表示するには、次のコマンドを入力します。

コマンド	目的
show resource allocation [**detail**]	リソース割り当てを表示します。このコマンドは、リソース割り当てを表示しますが、実際に使用されているリソースは表示しません。実際のリソース使用状況の詳細については、「リソースの使用状況の表示」（P.6-36）を参照してください。 **detail** 引数を指定すると、追加情報が表示されます。詳細については、次の出力例を参照してください。

次の出力例には、各リソースの合計割り当て量が絶対値および使用可能なシステム リソースの割合として示されています。

```
ciscoasa# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000           30.50%
 Hosts                      78842           N/A
 SSH                           35           35.00%
 Routes                      5000           N/A
 Telnet                        35           35.00%
 Xlates                     91749           N/A
 Other VPN Sessions            20           2.66%
 Other VPN Burst               20           2.66%
 All                    unlimited
```

表 6-3 に、各フィールドの説明を示します。

表 6-3　　show resource allocation のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
Total	すべてのコンテキストで割り当てられるリソースの総量。この数量は、同時発生インスタンスまたは 1 秒あたりのインスタンスの絶対量です。クラス定義でパーセンテージを指定した場合、ASA はこの表示のためにパーセンテージを絶対数に変換します。
% of Avail	リソースにハードウェア システム制限がある場合に、コンテキスト全体に渡って割り当てられている合計システム リソースの割合。リソースにシステム制限がない場合、このカラムには N/A と表示されます。

次に、**show resource allocation detail** コマンドの出力例を示します。

```
ciscoasa# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A
```

```
Conns           default          all      CA  unlimited
                gold               1       C     200000     200000     20.00%
                silver             1      CA     100000     100000     10.00%
                bronze             0      CA      50000
                All Contexts:      3                        300000     30.00%

Hosts           default          all      CA  unlimited
                gold               1      DA  unlimited
                silver             1      CA      26214      26214      N/A
                bronze             0      CA      13107
                All Contexts:      3                         26214      N/A

SSH             default          all       C          5
                gold               1       D          5          5      5.00%
                silver             1      CA         10         10     10.00%
                bronze             0      CA          5
                All Contexts:      3                            20     20.00%

Telnet          default          all       C          5
                gold               1       D          5          5      5.00%
                silver             1      CA         10         10     10.00%
                bronze             0      CA          5
                All Contexts:      3                            20     20.00%

Routes          default          all       C  unlimited                N/A
                gold               1       D  unlimited          5      N/A
                silver             1      CA         10         10      N/A
                bronze             0      CA          5                 N/A
                All Contexts:      3                            20      N/A

Xlates          default          all      CA  unlimited
                gold               1      DA  unlimited
                silver             1      CA      23040      23040     N/A
                bronze             0      CA      11520
                All Contexts:      3                         23040     N/A

mac-addresses   default          all       C      65535
                gold               1       D      65535      65535    100.00%
                silver             1      CA       6553       6553      9.99%
                bronze             0      CA       3276
                All Contexts:      3                        137623    209.99%
```

表 6-4 に、各フィールドの説明を示します。

表 6-4　show resource allocation detail のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
Class	デフォルト クラスを含む、各クラスの名前。 All Contexts フィールドには、すべてのクラス全体での合計値が表示されます。
Mmbrs	各クラスに割り当てられているコンテキストの数。
Origin	リソース制限の生成元。値は次のとおりです。 • A：この制限は個々のリソースとしてではなく、**all** オプションを使用して設定されています。 • C：この制限はメンバー クラスから生成されています。 • D：この制限はメンバー クラスで定義されたのではなく、デフォルト クラスから生成されました。デフォルト クラスに割り当てられたコンテキストの場合、値は「D」ではなく「C」になります。 ASA では、「A」と「C」または「D」を組み合わせることができます。
Limit	コンテキストごとのリソース制限（絶対数として）。クラス定義でパーセンテージを指定した場合、ASA はこの表示のためにパーセンテージを絶対数に変換します。
Total	クラス内のすべてのコンテキストにわたって割り当てられているリソースの合計数。この数量は、同時発生インスタンスまたは 1 秒あたりのインスタンスの絶対量です。リソースが無制限の場合、この表示は空白です。
% of Avail	クラス内のコンテキスト全体に渡って割り当てられている合計システム リソースの割合。リソースが無制限の場合、この表示は空白です。リソースにシステム制限がない場合、このカラムの表示は N/A になります。

リソースの使用状況の表示

システム実行スペースで、コンテキストごとのリソースの使用状況やシステム リソースの使用状況を表示できます。

コマンド	目的
show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system**] [**resource** {*resource_name* | **all**} | **detail**] [**counter** *counter_name* [*count_threshold*]]	デフォルトでは、**all**（すべての）コンテキストの使用状況が表示されます。各コンテキストは個別にリスト表示されます。 指定したリソースの上位 **n** 人のユーザとなっているコンテキストを表示するには、*top n* キーワードを入力します。このオプションでは、**resource all** ではなく、リソース タイプを 1 つのみ指定する必要があります。 **summary** オプションを指定すると、すべてのコンテキストの使用状況がまとめて表示されます。 **system** オプションでは、すべてのコンテキストの使用状況がまとめて表示されますが、コンテキスト制限の合計数ではなく、リソースに対するシステムの制限が表示されます。 **resource** *resource_name* で使用可能なリソース名については、表 6-1 を参照してください。**show resource type** コマンドも参照してください。すべてのタイプを表示するには **all**（デフォルト）を指定します。 **detail** オプションを指定すると、管理できないリソースを含むすべてのリソースの使用状況が表示されます。たとえば、TCP 代行受信の数を表示できます。 **counter** *counter_name* には、次のいずれかのキーワードを指定します。 • **current**：リソースのアクティブな同時発生インスタンス数、またはリソースの現在のレートを表示します。 • **denied**：Limit カラムに示されるリソース制限を超えたため拒否されたインスタンスの数を表示します。 • **peak**：ピーク時のリソースの同時発生インスタンス数、またはピーク時のリソースのレートを表示します。これは、統計情報が **clear resource usage** コマンドまたはデバイスのリブートによって最後にクリアされた時点から計測されます。 • **all**：（デフォルト）すべての統計情報を表示します。 *count_threshold* は、表示するリソースの下限を設定します。デフォルトは 1 です。リソースの使用状況がここで設定する回数を下回っている場合、そのリソースは表示されません。カウンタ名に **all** を指定した場合、*count_threshold* は現在の使用状況に適用されます。 **（注）**　すべてのリソースを表示するには、*count_threshold* を **0** に設定します。

次に、**show resource usage context** コマンドの出力例を示します。ここでは、admin コンテキストのリソース使用状況を表示する例を示しています。

```
ciscoasa# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

次に、**show resource usage summary** コマンドの出力例を示します。ここでは、すべてのコンテキストとすべてのリソースのリソース使用状況を表示する例を示しています。ここでは、6 コンテキスト分の制限値が表示されています。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      N/A            0 Summary
Conns                     584          763      280000(S)      0 Summary
Xlates                   8526         8966      N/A            0 Summary
Hosts                     254          254      N/A            0 Summary
Conns [rate]              270          535      N/A         1704 Summary
Inspects [rate]           270          535      N/A            0 Summary
Other VPN Sessions        0            10       10           740 Summary
Other VPN Burst           0            10       10           730 Summary

S = System: Combined context limits exceed the system limit; the system limit is shown.
```

次に、**show resource usage summary** コマンドの出力例を示します。このコマンドでは、25 コンテキストの制限が示されます。Telnet 接続および SSH 接続のコンテキストの制限がコンテキストごとに 5 であるため、制限数の合計は 125 です。システムの制限数は 100 であるため、システムの制限が表示されています。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit    Denied   Context
Telnet                      1            1        100[S]      0   Summary
SSH                         2            2        100[S]      0   Summary
Conns                      56           90        130000(S)   0   Summary
Hosts                      89          102        N/A         0   Summary
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

次に、**show resource usage system** コマンドの出力例を示します。このコマンドは、すべてのコンテキストのリソース使用状況を表示しますが、コンテキストの制限数の合計ではなく、システムの制限を表示します。現在使用中でないリソースを表示するには、**counter all 0** オプションを指定します。Denied の統計情報は、システム制限がある場合に、その制限によってリソースが拒否された回数を示します。

```
ciscoasa# show resource usage system counter all 0

Resource              Current         Peak      Limit        Denied    Context
Telnet                      0            0        100               0    System
SSH                         0            0        100               0    System
ASDM                        0            0         32               0    System
Routes                      0            0        N/A               0    System
IPSec                       0            0          5               0    System
Syslogs [rate]              1           18        N/A               0    System
Conns                       0            1     280000               0    System
Xlates                      0            0        N/A               0    System
Hosts                       0            2        N/A               0    System
Conns [rate]                1            1        N/A               0    System
Inspects [rate]             0            0        N/A               0    System
Other VPN Sessions          0           10        750             740    System
Other VPN Burst             0           10        750             730    System
```

コンテキストでの SYN 攻撃のモニタリング

ASA は TCP 代行受信を使用して SYN 攻撃を阻止します。TCP 代行受信では、SYN クッキー アルゴリズムを使用して TCP SYN フラッディング攻撃を防ぎます。SYN フラッディング攻撃は、通常はスプーフィングされた IP アドレスから送信されてくる一連の SYN パケットで構成されています。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、接続要求に対してサービスを提供できなくなります。接続の初期接続しきい値を超えると、ASAはサーバのプロキシとして動作し、クライアント SYN 要求に対する SYN-ACK 応答を生成します。ASAがクライアントから ACK を受信すると、クライアントを認証し、サーバへの接続を許可できます。

次のコマンドを使用して SYN 攻撃をモニタします。

コマンド	目的
show perfmon	各コンテキストについて、攻撃の割合をモニタリングします。
show resource usage detail	個々のコンテキストの TCP 代行受信で使用されるリソースの量をモニタします。
show resource usage summary detail	システム全体の TCP 代行受信で使用されるリソースをモニタします。

次に、**show perfmon** コマンドの出力例を示します。このコマンドは、admin というコンテキストの TCP 代行受信レートを表示します。

```
ciscoasa/admin# show perfmon

Context:admin
PERFMON STATS:   Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept    322779/s     322779/s
```

次に、**show resource usage detail** コマンドの出力例を示します。このコマンドは、個々のコンテキストの TCP 代行受信で使用されるリソース量を表示します（**太字**のサンプル テキストは、TCP 代行受信情報を示します）。

```
ciscoasa(config)# show resource usage detail
Resource              Current         Peak      Limit         Denied Context
memory                 843732       847288  unlimited             0 admin
chunk:channels             14           15  unlimited             0 admin
chunk:fixup                15           15  unlimited             0 admin
chunk:hole                  1            1  unlimited             0 admin
chunk:ip-users             10           10  unlimited             0 admin
chunk:list-elem            21           21  unlimited             0 admin
chunk:list-hdr              3            4  unlimited             0 admin
chunk:route                 2            2  unlimited             0 admin
chunk:static                1            1  unlimited             0 admin
tcp-intercepts         328787       803610  unlimited             0 admin
np-statics                  3            3  unlimited             0 admin
```

```
statics                     1           1  unlimited            0 admin
ace-rules                   1           1  unlimited            0 admin
console-access-rul          2           2  unlimited            0 admin
fixup-rules                14          15  unlimited            0 admin
memory                 959872      960000  unlimited            0 c1
chunk:channels             15          16  unlimited            0 c1
chunk:dbgtrace              1           1  unlimited            0 c1
chunk:fixup                15          15  unlimited            0 c1
chunk:global                1           1  unlimited            0 c1
chunk:hole                  2           2  unlimited            0 c1
chunk:ip-users             10          10  unlimited            0 c1
chunk:udp-ctrl-blk          1           1  unlimited            0 c1
chunk:list-elem            24          24  unlimited            0 c1
chunk:list-hdr              5           6  unlimited            0 c1
chunk:nat                   1           1  unlimited            0 c1
chunk:route                 2           2  unlimited            0 c1
chunk:static                1           1  unlimited            0 c1
tcp-intercept-rate      16056       16254  unlimited            0 c1
globals                     1           1  unlimited            0 c1
np-statics                  3           3  unlimited            0 c1
statics                     1           1  unlimited            0 c1
nats                        1           1  unlimited            0 c1
ace-rules                   2           2  unlimited            0 c1
console-access-rul          2           2  unlimited            0 c1
fixup-rules                14          15  unlimited            0 c1
memory              232695716   232020648  unlimited            0 system
chunk:channels             17          20  unlimited            0 system
chunk:dbgtrace              3           3  unlimited            0 system
chunk:fixup                15          15  unlimited            0 system
chunk:ip-users              4           4  unlimited            0 system
chunk:list-elem          1014        1014  unlimited            0 system
chunk:list-hdr              1           1  unlimited            0 system
chunk:route                 1           1  unlimited            0 system
block:16384               510         885  unlimited            0 system
block:2048                 32          34  unlimited            0 system
```

次の出力例は、システム全体の TCP 代行受信で使用されるリソースを示します（**太字**のサンプル テキストは、TCP 代行受信情報を示します）。

```
ciscoasa(config)# show resource usage summary detail
Resource              Current         Peak      Limit        Denied Context
memory              238421312    238434336  unlimited            0 Summary
chunk:channels             46          48  unlimited            0 Summary
chunk:dbgtrace              4           4  unlimited            0 Summary
chunk:fixup                45          45  unlimited            0 Summary
chunk:global                1           1  unlimited            0 Summary
chunk:hole                  3           3  unlimited            0 Summary
chunk:ip-users             24          24  unlimited            0 Summary
chunk:udp-ctrl-blk          1           1  unlimited            0 Summary
chunk:list-elem          1059        1059  unlimited            0 Summary
chunk:list-hdr             10          11  unlimited            0 Summary
chunk:nat                   1           1  unlimited            0 Summary
chunk:route                 5           5  unlimited            0 Summary
chunk:static                2           2  unlimited            0 Summary
block:16384               510         885  unlimited            0 Summary
block:2048                 32          35  unlimited            0 Summary
tcp-intercept-rate     341306      811579  unlimited            0 Summary
globals                     1           1  unlimited            0 Summary
np-statics                  6           6  unlimited            0 Summary
statics                     2           2        N/A            0 Summary
nats                        1           1        N/A            0 Summary
ace-rules                   3           3        N/A            0 Summary
console-access-rul          4           4        N/A            0 Summary
fixup-rules                43          44        N/A            0 Summary
```

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.6-40）
- 「コンテキスト内の MAC アドレスの表示」（P.6-41）

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たときに自動生成もイネーブルになっている場合は、手動 MAC アドレスが使用されますが、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

コマンド	目的
show running-config all context [*name*]	システム実行スペースから割り当てられた MAC アドレスを表示します。 割り当てられた MAC アドレスを表示するには、**all** オプションが必要です。**mac-address auto** コマンドは、グローバル コンフィギュレーション モードに限りユーザ設定可能ですが、コンテキスト コンフィギュレーション モードでは、このコマンドは読み取り専用エントリとして、割り当てられた MAC アドレスとともに表示されます。コンテキスト内で **nameif** コマンドで設定される割り当て済みのインターフェイスだけに MAC アドレスが割り当てられます。

例

show running-config all context admin コマンドからの次の出力には、Management0/0 インターフェイスに割り当てられたプライマリおよびスタンバイ MAC アドレスが表示されます。

```
ciscoasa# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

show running-config all context コマンドからの次の出力には、すべてのコンテキスト インターフェイスのすべての MAC アドレス（プライマリおよびスタンバイ）が表示されます。GigabitEthernet0/0 と GigabitEthernet0/1 の各メイン インターフェイスはコンテキスト内部に **nameif** コマンドで設定されないため、それらのインターフェイスの MAC アドレスは生成されていないことに注意してください。

```
ciscoasa# show running-config all context

admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

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

コマンド	目的
show interface | include (Interface)|(MAC)	コンテキスト内で各インターフェイスに使用されている MAC アドレスを表示します。

例

次に例を示します。

```
ciscoasa/context# show interface | include (Interface)|(MAC)

Interface GigabitEthernet1/1.1 "g1/1.1", is down, line protocol is down
        MAC address a201.0101.0600, MTU 1500
Interface GigabitEthernet1/1.2 "g1/1.2", is down, line protocol is down
        MAC address a201.0102.0600, MTU 1500
Interface GigabitEthernet1/1.3 "g1/1.3", is down, line protocol is down
        MAC address a201.0103.0600, MTU 1500
...
```

（注）　**show interface** コマンドは、使用中の MAC アドレスを表示します。MAC アドレスを手動で割り当てた場合に、自動生成がイネーブルになっていたときは、システム コンフィギュレーション内の未使用の自動生成アドレスのみを表示できます。

マルチ コンテキスト モードの設定例

次に例を示します。

- 各コンテキストの MAC アドレスを、カスタム プレフィックスを使用して自動的に設定します。
- conns のデフォルト クラス制限を、無制限ではなく 10% に設定し、VPN other セッション数を 10、バーストを 5 に設定します。
- gold リソース クラスを作成します。
- 管理コンテキストを「administrator」と設定します。
- 「administrator」というコンテキストを、デフォルトのリソース クラスの一部になるように、内部フラッシュ メモリ上に作成します。
- gold リソース クラスの一部として FTP サーバから 2 個のコンテキストを追加します。

```
ciscoasa(config)# mac-address auto prefix 19

ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5

ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 700
ciscoasa(config-class)# limit-resource vpn other 100
ciscoasa(config-class)# limit-resource vpn burst other 50
```

```
ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member gold
```

マルチ コンテキスト モードの機能履歴

表 6-5 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。

表 6-5　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。 **context**、**mode**、**class** の各コマンドが導入されました。
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。 **mac-address auto** コマンドが導入されました。
リソース管理	7.2(1)	リソース管理が導入されました。 **class**、**limit-resource**、**member** の各コマンドが導入されました。

表 6-5　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
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。 **allocate-ips** コマンドが導入されました。
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場合は、A2 で始まる手動 MAC アドレスは指定できません。 **mac-address auto prefix** コマンドが変更されました。
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。 **mac-address auto** コマンドが変更されました。

表 6-5　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 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。**show running-config mac-address** コマンドを入力して、自動生成されたプレフィックスを表示できます。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。 **mac-address auto** コマンドが変更されました。
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 6-5　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。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各コマンドが変更されました。
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。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各コマンドが変更されました。

CHAPTER 7

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」（P.7-1）
- 「フェールオーバーのライセンス」（P.7-27）
- 「フェールオーバーの前提条件」（P.7-28）
- 「フェールオーバーのガイドライン」（P.7-28）
- 「フェールオーバーのデフォルト」（P.7-29）
- 「アクティブ/スタンバイ フェールオーバーの設定」（P.7-29）
- 「アクティブ/アクティブ フェールオーバーの設定」（P.7-34）
- 「オプションのフェールオーバー パラメータの設定」（P.7-39）
- 「フェールオーバーの管理」（P.7-47）
- 「フェールオーバー動作のモニタ」（P.7-53）
- 「フェールオーバーの機能履歴」（P.7-55）

フェールオーバーについて

- 「フェールオーバーの概要」（P.7-2）
- 「フェールオーバーのシステム要件」（P.7-2）
- 「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」（P.7-3）
- 「MAC アドレスと IP アドレス」（P.7-9）
- 「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」（P.7-9）
- 「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」（P.7-13）
- 「トランスペアレント ファイアウォール モードの要件」（P.7-16）
- 「フェールオーバー ヘルスのモニタリング」（P.7-17）
- 「フェールオーバー時間」（P.7-19）

- 「コンフィギュレーション同期」（P.7-20）
- 「アクティブ/スタンバイ フェールオーバーについて」（P.7-22）
- 「アクティブ/アクティブ フェールオーバーについて」（P.7-24）

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.7-2）
- 「ソフトウェア要件」（P.7-3）
- 「ライセンス要件」（P.7-3）

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.36-5）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.4-28）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.7-4）
- 「ステートフル フェールオーバー リンク」（P.7-5）
- 「フェールオーバーの中断の回避とデータ リンク」（P.7-6）

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.7-4）
- 「フェールオーバー リンクのインターフェイス」（P.7-4）
- 「フェールオーバー リンクの接続」（P.7-4）

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.7-5）
- 「フェールオーバー リンクと共有」（P.7-5）
- 「通常のデータ インターフェイスと共有（非推奨）」（P.7-6）

（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 7-1 および図 7-2 で示されている次の 2 つの接続方式は推奨しません。

図 7-1　単一のスイッチを使用した接続：非推奨

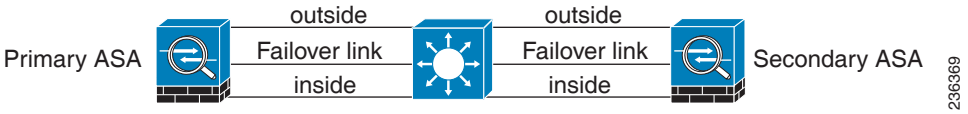
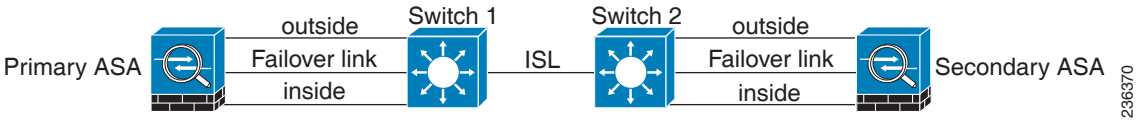


図 7-2　2 つのスイッチを使用した接続：非推奨



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 7-3 および図 7-4 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 7-3　異なるスイッチを使用した接続

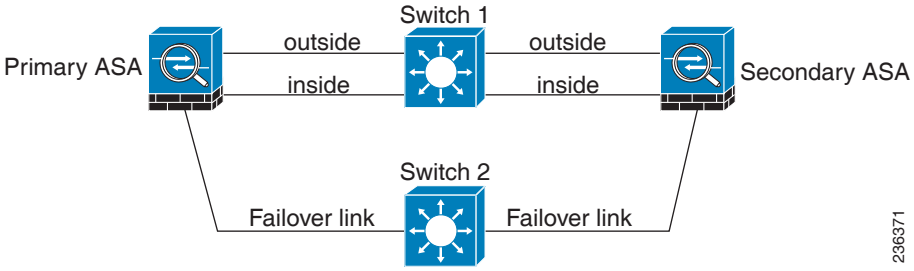
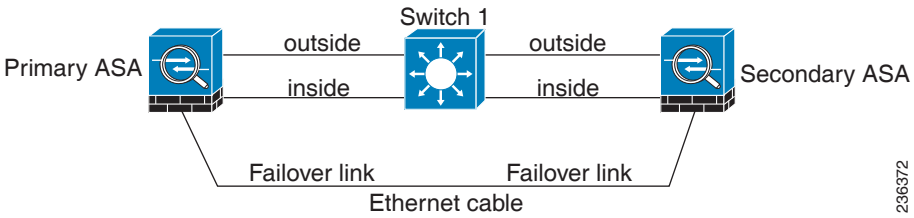


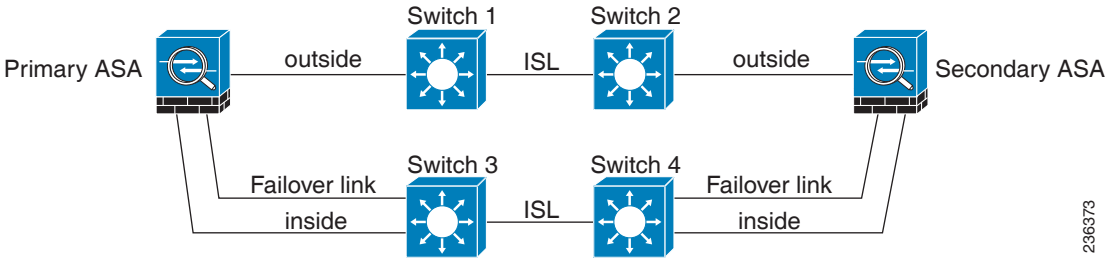
図 7-4　ケーブルを使用した接続



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 7-5 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 7-5　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 7-6 および図 7-7 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 7-6　冗長インターフェイスを使用した接続

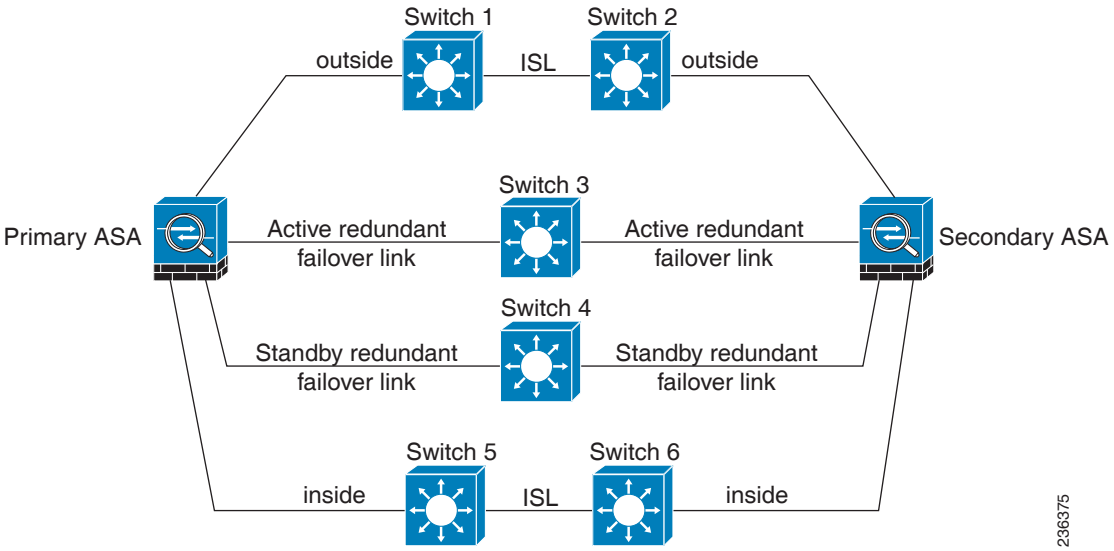
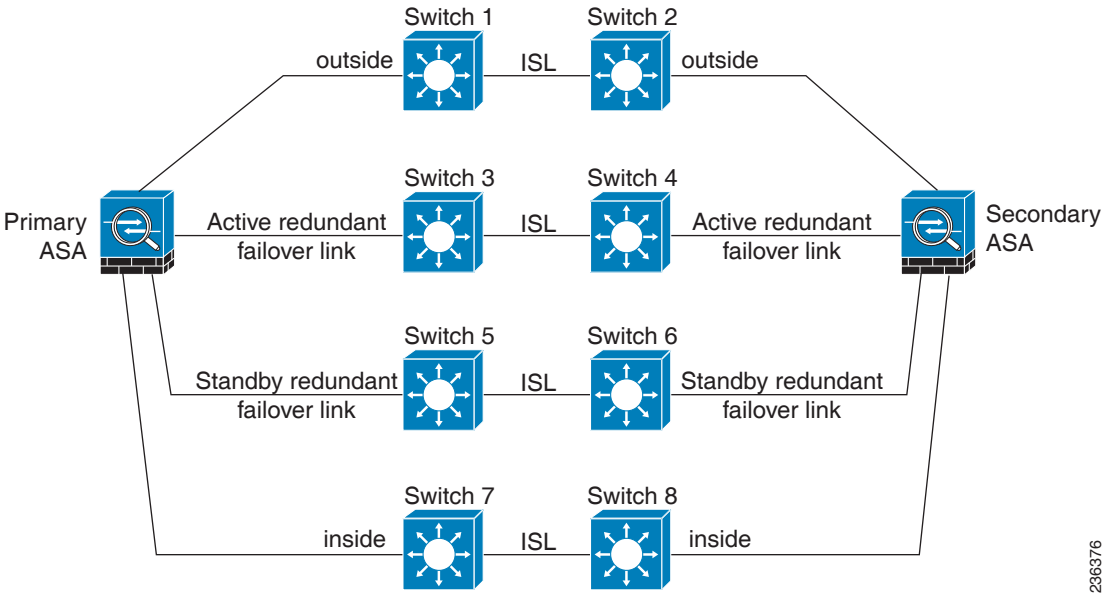


図 7-7　スイッチ間リンクを使用した接続



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.6-12）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.7-34）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 テーブルをクリアする必要がある場合があります。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.7-10）
- 「シャーシ間フェールオーバー」（P.7-10）

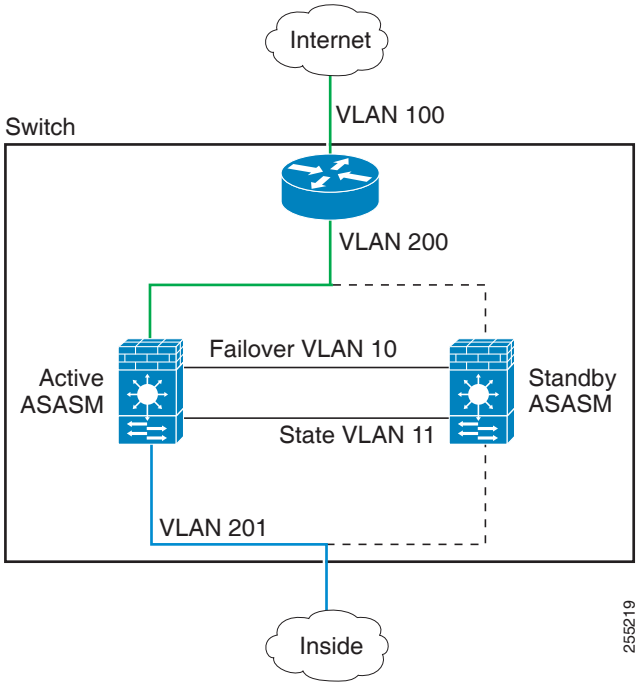
シャーシ内フェールオーバー

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.7-10）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 7-8 に、一般的なスイッチ内の構成を示します。

図 7-8　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。

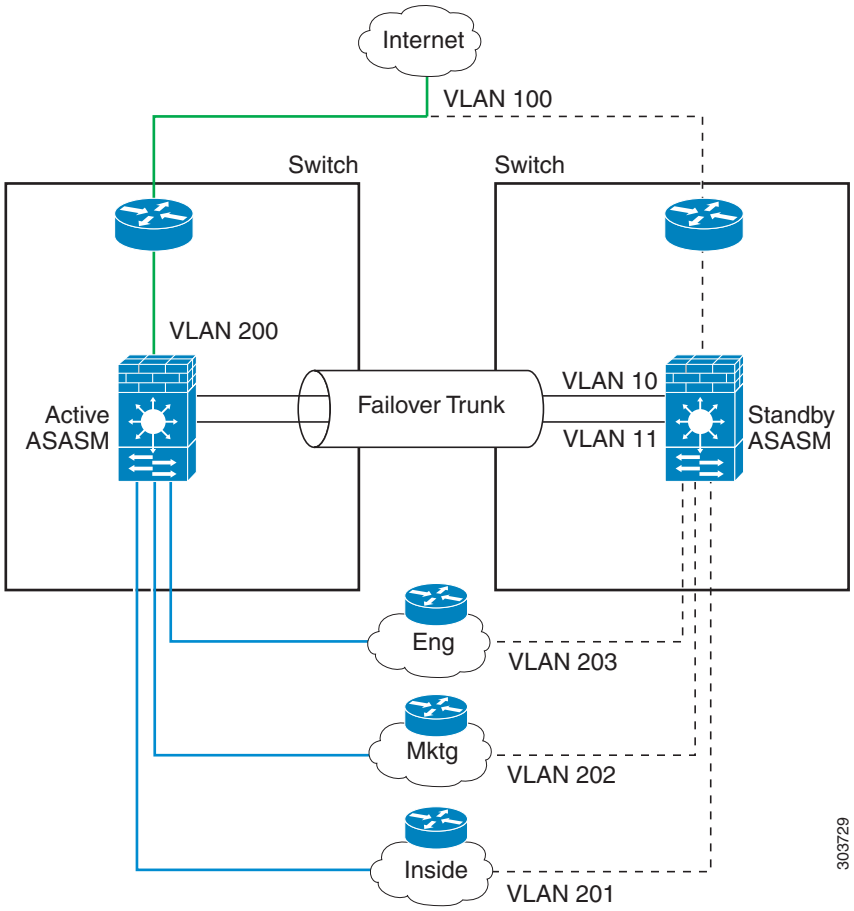
ASASM 間のフェールオーバー通信の信頼性を高めるために、2 台のスイッチ間に EtherChannel トランク ポートを設定して、フェールオーバーおよびステート VLAN を伝送することをお勧めします。

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 7-9 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。

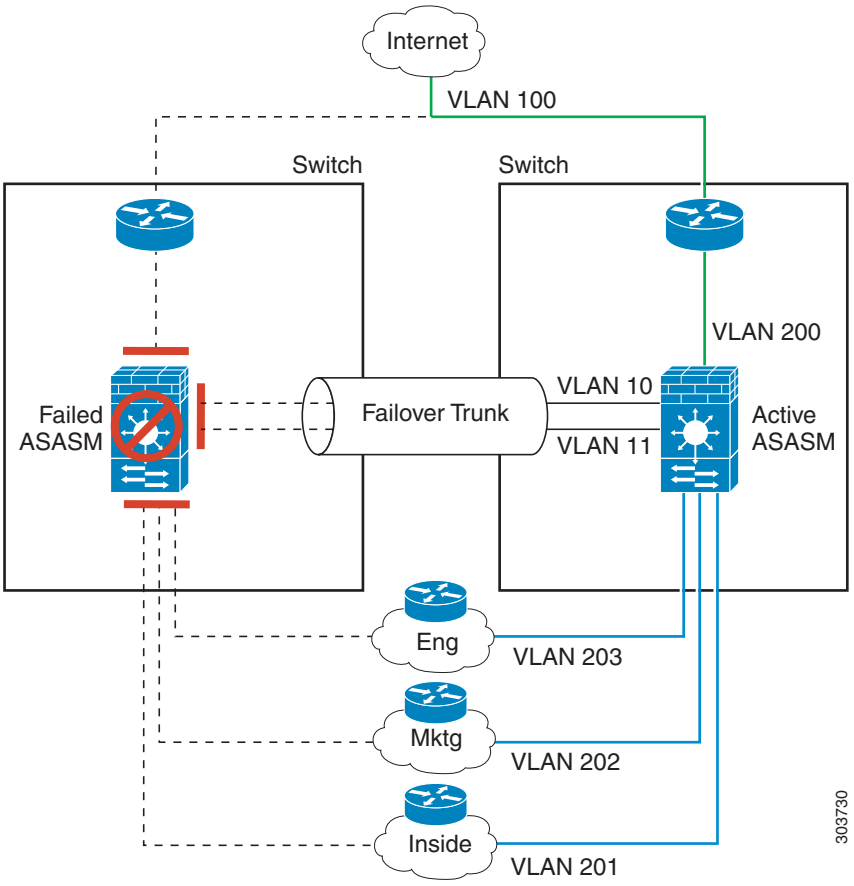
（注）　ASASM のフェールオーバーはスイッチのフェールオーバーに依存しない独立した機能ですが、スイッチのフェールオーバーが発生した場合には、ASASM もそれに対応します。

図 7-9　　通常の動作



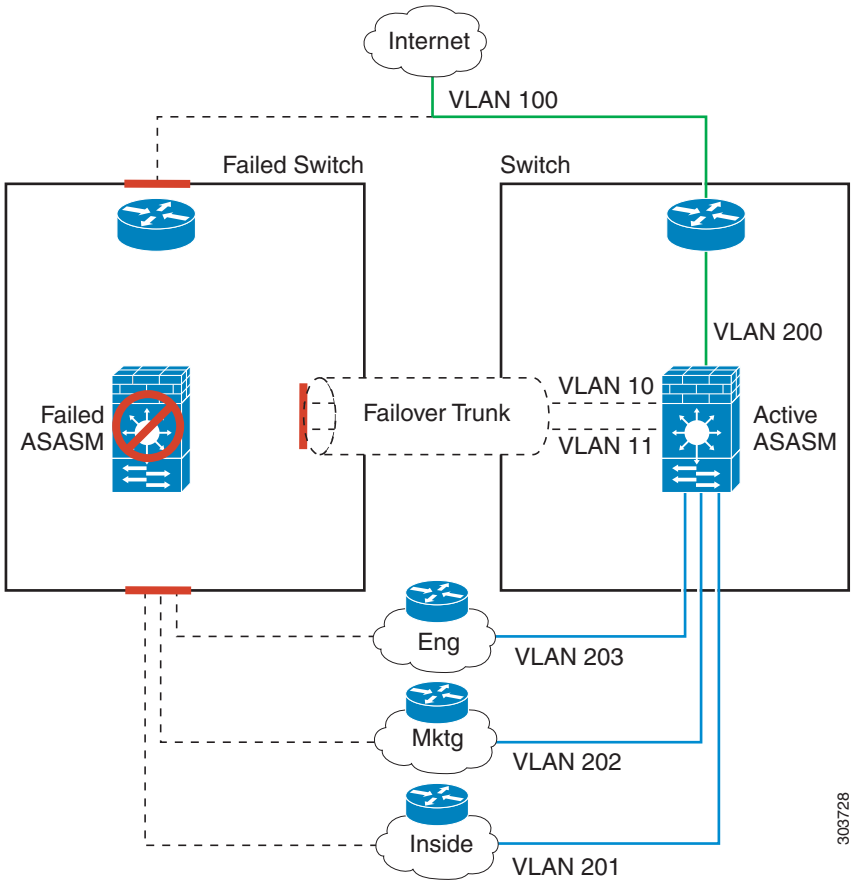
プライマリ ASASM に障害が発生すると、セカンダリ ASASM がアクティブになってファイアウォール VLAN を通過させます（図 7-10）。

図 7-10　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 7-11）。

図 7-11　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.7-14）
- 「ステートフル フェールオーバー」（P.7-14）

（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.7-14）
- 「サポートされていない機能」（P.7-15）

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」（P.7-16）
- 「モジュールのトランスペアレント モードの要件」（P.7-17）

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。

```
access-list id ethertype deny bpdu
access-group id in interface inside_name
access-group id in interface outside_name
```

  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。

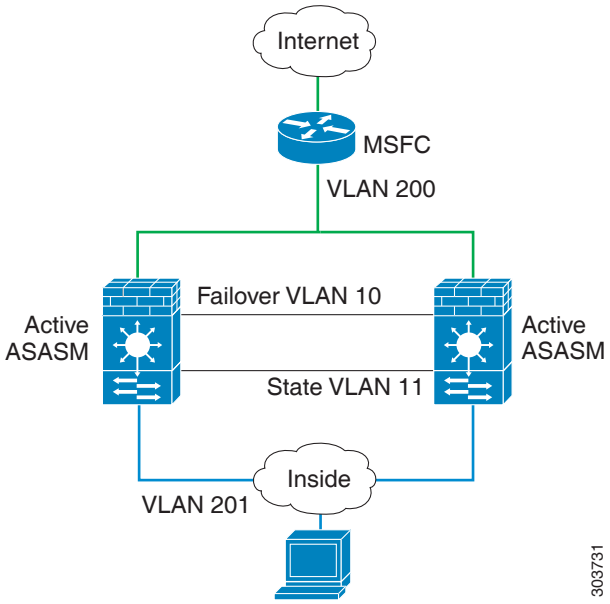
- インターフェイス モニタリングをディセーブルにします。
- ASA がフェールオーバーする前に、インターフェイスのホールド時間を STP が収束可能になる大きい値に増やします。
- STP がインターフェイスのホールド時間よりも速く収束するように、STP タイマーを減らします。

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する場合や、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になるときに、ループが発生することがあります。両方のASASM が 2 つの同じ VLAN 間でパケットをブリッジングするので、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 7-12 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 7-12　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.7-18）
- 「インターフェイスのモニタリング」（P.7-18）

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。装置は、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いときは、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検証します。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「未知」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 7-1 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 7-1　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

表 7-1　ASA のフェールオーバー時間 （続き）

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.7-20）
- 「コマンドの複製」（P.7-21）

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の変更の保存」（P.2-18）に従って、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）　複製の間は、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され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コマンドは、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コマンド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.7-22）
- 「起動時のアクティブ装置の判別」（P.7-22）
- 「フェールオーバー イベント」（P.7-23）

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 7-2 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 7-2　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	メモ
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。
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.7-24）
- 「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.7-24）
- 「フェールオーバー イベント」（P.7-25）

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のコンテキストでは必要でない場合、最もシンプルな設定は追加コンテキストを 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で設定されます。

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 グループがこの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 コンフィギュレーションでは、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 7-3 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 7-3　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	メモ
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 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 : 両方のユニットで IPS モジュール ライセンスが必要です。両方のユニットの 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。
  - 両方のユニットに 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、ユニットごとに個別の 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。ただし、IPS シグニチャ サブスクリプションの要件のため、ユニットごとに個別の 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 ユニットに割り当てられる vCPU の数をプライマリ ユニット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 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：両方のユニットで IPS モジュール ライセンスが必要です。両方のユニットの 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。
  - 両方のユニットに 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、ユニットごとに個別の 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。ただし、IPS シグニチャ サブスクリプションの要件のため、ユニットごとに個別の 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 ユニットに割り当てられる vCPU の数をプライマリ ユニット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.7-2）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.36-39）

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

- 「アクティブ/スタンバイ フェールオーバーのプライマリ装置の設定」（P.7-29）
- 「アクティブ/スタンバイ フェールオーバーのセカンダリ装置の設定」（P.7-33）

アクティブ/スタンバイ フェールオーバーのプライマリ装置の設定

この項の手順に従って、アクティブ/スタンバイ フェールオーバー構成のプライマリを設定します。この手順では、プライマリ装置でフェールオーバーをイネーブルにするために必要な最小のコンフィギュレーションが用意されています。

はじめる前に

- 第 11 章「ルーテッド モードのインターフェイス」または第 12 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、フェールオーバー リンクとステート リンクを除くすべてのインターフェイスのスタンバイ IP アドレスを設定します。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。

- 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。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1　この装置をプライマリ装置に指定します。

```
failover lan unit primary
```

ステップ 2　フェールオーバー リンクとして使用するインターフェイスを指定します。

```
failover lan interface if_name interface_id
```

例：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

このインターフェイスは、他の目的には使用できません（オプションのステート リンクは除く）。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、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、または EtherChannel インターフェイス ID を指定できます。ASASM では、*interface_id* には VLAN ID を指定します。

順序が不正なパケットを防ぐために、フェールオーバーまたはステート リンクとして EtherChannel を使用できますが、EtherChannel のインターフェイスは 1 個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。

ステップ 3　アクティブ IP アドレスとスタンバイ IP アドレスをフェールオーバー リンクに割り当てます。

```
failover interface ip failover_if_name {ip_address mask | ipv6_address/prefix} standby
ip_address
```

例：

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

または：

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

この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。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

ステップ 4　フェールオーバー リンクをイネーブルにします。

```
interface failover_interface_id
  no shutdown
```

例：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

ステップ 5　（オプション）ステート リンクとして使用するインターフェイスを指定します。

```
failover link if_name interface_id
```

例：

```
ciscoasa(config)# failover link statelink gigabitethernet0/4
```

フェールオーバー リンクまたはデータ インターフェイスとは異なるインターフェイスを指定することをお勧めします。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、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、または EtherChannel インターフェイス ID を指定できます。ASASM では、*interface_id* には VLAN ID を指定します。

順序が不正なパケットを防ぐために、フェールオーバーまたはステート リンクとして EtherChannel を使用できますが、EtherChannel のインターフェイスは 1 個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。

ステップ 6　別のステート リンクを指定した場合、ステート リンクにアクティブ IP アドレスとスタンバイ IP アドレスを割り当てます。

failover interface ip *state_if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

例：

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

または：

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

このアドレスは、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。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

ステート リンクを共有する場合は、この手順を省略してください。

ステップ 7　別のステート リンクを指定した場合、ステート リンクをイネーブルにします。

interface *state_interface_id*
  no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

ステート リンクを共有する場合は、この手順を省略してください。

ステップ 8　（オプション）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、次のいずれかを実行します。

- （推奨）すべてのフェールオーバー通信を暗号化するには、装置間のフェールオーバー リンクおよびステート リンクの IPsec LAN-to-LAN トンネルを確立します。

  failover ipsec pre-shared-key [**0** | **8**] *key*

  例：

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  key は最大 128 文字です。両方の装置に同じキーを指定します。キーは IKEv2 によってトンネルを確立するために使用されます。

マスター パスフレーズ（「マスター パスフレーズの設定」（P.13-11）を参照）を使用している場合、キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は（たとえば **more system:running-config** の出力からのコピー）、キーワード **8** を使用してキーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

show running-config の出力では、**failover ipsec pre-shared-key** 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。

フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信に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すべてのパスワードやキーも含まれます。

IPsec 暗号化とレガシーの **failover key** 暗号化の両方を使用することはできません。両方を設定した場合、IPsec が使用されます。ただし、マスター パスフレーズ（「マスター パスフレーズの設定」（P.13-11）を参照）を使用する場合、IPsec 暗号化を設定する前に **no failover key** コマンドを使用してフェールオーバー キーを削除する必要があります。

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。

- （オプション）フェールオーバー リンクおよびステート リンクのフェールオーバー通信を暗号化します。

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  例：

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  1 ～ 63 文字の *shared_secret* または 32 文字の **hex** *key*を使用します。*shared_secret* には、数字、文字、または句読点の任意の組み合わせを使用できます。共有秘密または 16 進数キーは暗号キーを生成するために使用されます。両方の装置に同じキーを指定します。

  マスター パスフレーズ（「マスター パスフレーズの設定」（P.13-11）を参照）を使用している場合、共有秘密または 16 進数キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は（たとえば **more system:running-config** の出力からのコピー）、キーワード **8** を使用して共有秘密または 16 進数キーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

  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。

  フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信に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すべてのパスワードやキーも含まれます。

ステップ 9　フェールオーバーをイネーブルにします。

```
failover
```

ステップ 10　システム コンフィギュレーションをフラッシュ メモリに保存します。

```
write memory
```

例

次に、プライマリ装置用のフェールオーバー パラメータの設定例を示します。

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4
failover interface ip statelink 172.27.49.1 255.255.255.0 standby 172.27.49.2
interface gigabitethernet 0/4
  no shutdown
failover ipsec pre-shared-key a3rynsun
failover
```

アクティブ/スタンバイ フェールオーバーのセカンダリ装置の設定

セカンダリ装置に必要なコンフィギュレーションは、フェールオーバー リンクのコンフィギュレーションだけです。セカンダリ装置には、プライマリ装置と初期に通信するために、これらのコマンドが必要です。プライマリ装置がセカンダリ装置にコンフィギュレーションを送信した後、2 つのコンフィギュレーション間で唯一、不変の相違点は **failover lan unit** コマンドです。このコマンドで各装置がプライマリかセカンダリかを識別します。

はじめる前に

- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- 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。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1　**failover lan unit primary** コマンドを*除いて*、プライマリ装置とまったく同じコマンドを再入力します。任意で **failover lan unit secondary** コマンドに置き換えることもできますが、**secondary** はデフォルト設定のため、必須ではありません。「アクティブ/スタンバイ フェールオーバーのプライマリ装置の設定」（P.7-29）を参照してください。

次に例を示します。

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its
sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
  no shutdown
ciscoasa(config)# failover link statelink gigabitethernet0/4
INFO: Non-failover interface config is cleared on GigabitEthernet0/4 and its
sub-interfaces
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
ciscoasa(config)# interface gigabitethernet 0/4
  no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

ステップ 2　フェールオーバー コンフィギュレーションが同期された後で、コンフィギュレーションをフラッシュ メモリに保存します。

```
ciscoasa(config)# write memory
```

アクティブ/アクティブ フェールオーバーの設定

- 「アクティブ/アクティブ フェールオーバーのプライマリ装置の設定」（P.7-34）
- 「アクティブ/アクティブ フェールオーバーのセカンダリ装置の設定」（P.7-38）

アクティブ/アクティブ フェールオーバーのプライマリ装置の設定

この項の手順に従って、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でプライマリ装置を設定します。この手順では、プライマリ装置でフェールオーバーをイネーブルにするために必要な最小のコンフィギュレーションが用意されています。

はじめる前に

- 「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.6-16）に従って、マルチ コンテキスト モードをイネーブルにします。
- 第 11 章「ルーテッド モードのインターフェイス」または第 12 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、フェールオーバー リンクとステート リンクを除くすべてのインターフェイスのスタンバイ IP アドレスを設定します。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- この手順はシステム実行スペースで実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1　この装置をプライマリ装置に指定します。

```
failover lan unit primary
```

ステップ 2　フェールオーバー リンクとして使用するインターフェイスを指定します。

```
failover lan interface if_name interface_id
```

例：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

このインターフェイスは、他の目的には使用できません（オプションのステート リンクは除く）。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、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、または EtherChannel インターフェイス ID を指定できます。ASASM では、*interface_id* には VLAN ID を指定します。

順序が不正なパケットを防ぐために、フェールオーバーまたはステート リンクとして EtherChannel を使用できますが、EtherChannel のインターフェイスは 1 個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。

ステップ 3　アクティブ IP アドレスとスタンバイ IP アドレスをフェールオーバー リンクに割り当てます。

failover interface ip *if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

例：

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

または：

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

この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。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

ステップ 4　フェールオーバー リンクをイネーブルにします。

interface *failover_interface_id*
  no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

ステップ 5　（オプション）ステート リンクとして使用するインターフェイスを指定します。

failover link *if_name interface_id*

例：

```
ciscoasa(config)# failover link statelink gigabitethernet0/4
```

フェールオーバー リンクまたはデータ インターフェイスとは異なるインターフェイスを指定することをお勧めします。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、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、または EtherChannel インターフェイス ID を指定できます。ASASM では、*interface_id* には VLAN ID を指定します。

順序が不正なパケットを防ぐために、フェールオーバーまたはステート リンクとして EtherChannel を使用できますが、EtherChannel のインターフェイスは 1 個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。

ステップ 6　別のステート リンクを指定した場合、ステート リンクにアクティブ IP アドレスとスタンバイ IP アドレスを割り当てます。

このアドレスは、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。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

ステート リンクを共有する場合は、この手順を省略してください。

failover interface ip *state_if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

例：

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

または：

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

ステップ 7　別のステート リンクを指定した場合、ステート リンクをイネーブルにします。

interface *state_interface_id*
no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

ステート リンクを共有する場合は、この手順を省略してください。

ステップ 8　（オプション）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、次のいずれかを実行します。

- （推奨）すべてのフェールオーバー通信を暗号化するには、装置間のフェールオーバー リンクおよびステート リンクの IPsec LAN-to-LAN トンネルを確立します。

  failover ipsec pre-shared-key [**0** | **8**] *key*

  例：

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  key は最大 128 文字です。両方の装置に同じキーを指定します。キーは IKEv2 によってトンネルを確立するために使用されます。

  マスター パスフレーズ（「マスター パスフレーズの設定」（P.13-11）を参照）を使用している場合、キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は（たとえば **more system:running-config** の出力からのコピー）、キーワード **8** を使用してキーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

  show running-config の出力では、**failover ipsec pre-shared-key** 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。

  フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信に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すべてのパスワードやキーも含まれます。

  IPsec 暗号化とレガシーの **failover key** 暗号化の両方を使用することはできません。両方を設定した場合、IPsec が使用されます。ただし、マスター パスフレーズ（「マスター パスフレーズの設定」（P.13-11）を参照）を使用する場合、IPsec 暗号化を設定する前に **no failover key** コマンドを使用してフェールオーバー キーを削除する必要があります。

  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。

- （オプション）フェールオーバー リンクおよびステート リンクのフェールオーバー通信を暗号化します。

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

例：

```
ciscoasa(config)# failover key johncr1cht0n
```

1 ～ 63 文字の *shared_secret* または 32 文字の **hex** *key*を使用します。

shared_secret には、数字、文字、または句読点の任意の組み合わせを使用できます。共有秘密または 16 進数キーは暗号キーを生成するために使用されます。両方の装置に同じキーを指定します。

マスター パスフレーズ（「マスター パスフレーズの設定」（P.13-11）を参照）を使用している場合、共有秘密または 16 進数キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は（たとえば **more system:running-config** の出力からのコピー）、キーワード **8** を使用して共有秘密または 16 進数キーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

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。

フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信に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すべてのパスワードやキーも含まれます。

ステップ 9　フェールオーバー グループ 1 を作成します。

```
failover group 1
```

デフォルトで、このグループはプライマリ装置に割り当てられます。通常、プライマリ装置にグループ 1 を割り当て、セカンダリ装置にグループ 2 を割り当てます。標準以外の設定が必要な場合は、**primary** サブコマンドまたは **secondary** サブコマンドを使用して、別の装置を優先するように指定できます。

ステップ 10　フェールオーバー グループ 2 を作成して、セカンダリ装置に割り当てます。

```
failover group 2
  secondary
```

ステップ 11　特定のコンテキストのコンテキスト コンフィギュレーション モードに入り、そのコンテキストをフェールオーバー グループに割り当てます。

```
context name
  join-failover-group {1 | 2}
```

例：

```
ciscoasa(config)# context Eng
ciscoasa(config-ctx)# join-failover-group 2
```

コンテキストごとにこのコマンドを繰り返します。

未割り当てのコンテキストはすべて、自動的にフェールオーバー グループ 1 に割り当てられます。管理コンテキストは常にフェールオーバー グループ 1 のメンバーです。グループ 2 に割り当てることはできません。

ステップ 12　フェールオーバーをイネーブルにします。

```
failover
```

ステップ 13　システム コンフィギュレーションをフラッシュ メモリに保存します。

```
write memory
```

例

次に、プライマリ装置用のフェールオーバー パラメータの設定例を示します。

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4
failover interface ip statelink 172.27.49.1 255.255.255.0 standby 172.27.49.2
interface gigabitethernet 0/4
  no shutdown
failover group 1
failover group 2
  secondary
context admin
  join-failover-group 1
failover ipsec pre-shared-key a3rynsun
failover
```

アクティブ/アクティブ フェールオーバーのセカンダリ装置の設定

セカンダリ装置に必要なコンフィギュレーションは、フェールオーバー リンクのコンフィギュレーションだけです。セカンダリ装置には、プライマリ装置と初期に通信するために、これらのコマンドが必要です。プライマリ装置がセカンダリ装置にコンフィギュレーションを送信した後、2 つのコンフィギュレーション間で唯一、不変の相違点は **failover lan unit** コマンドです。このコマンドで各装置がプライマリかセカンダリかを識別します。

はじめる前に

- 「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.6-16）に従って、マルチ コンテキスト モードをイネーブルにします。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- この手順はシステム実行スペースで実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1　**failover lan unit primary** コマンドを*除いて*、プライマリ装置とまったく同じコマンドを再入力します。任意で **failover lan unit secondary** コマンドに置き換えることもできますが、**secondary** はデフォルト設定のため、必須ではありません。また、プライマリ装置から複製されるので、**failover group** コマンドおよび **join-failover-group** コマンドを入力する必要もありません。「アクティブ/アクティブ フェールオーバーのプライマリ装置の設定」（P.7-34）を参照してください。

次に例を示します。

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its
sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
  no shutdown
ciscoasa(config)# failover link statelink gigabitethernet0/4
INFO: Non-failover interface config is cleared on GigabitEthernet0/4 and its
sub-interfaces
```

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
ciscoasa(config)# interface gigabitethernet 0/4
  no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

ステップ 2　フェールオーバー コンフィギュレーションがプライマリ装置と同期された後で、コンフィギュレーションをフラッシュ メモリに保存します。

```
ciscoasa(config)# write memory
```

ステップ 3　必要に応じて、フェールオーバー グループ 2 がセカンダリ装置でアクティブになるように設定します。

```
failover active group 2
```

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.7-39）
- 「インターフェイス モニタリングの設定」（P.7-42）
- 「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.7-43）

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.7-29）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。

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 1　装置のポーリング時間およびホールド時間を変更します。

アクティブ/アクティブ モードでは、システムに対してこのレートを設定します。フェールオーバー グループごとにこのレートを設定することはできません。

装置のポーリング時間の 3 倍未満の値をホールド時間の値として入力することはできません。ポーリング時間が短いほど、ASA は短時間で故障を検出し、フェールオーバーをトリガーできます。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。

1 回のポーリング期間中に、装置がフェールオーバー通信インターフェイスで hello パケットを検出しなかった場合、残りのインターフェイスで追加テストが実行されます。それでも保持時間内にピア装置から応答がない場合、その装置は故障していると見なされ、故障した装置がアクティブ装置の場合は、スタンバイ装置がアクティブ装置を引き継ぎます。

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

例：

```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

ステップ 2　HTTP 複製レートを、1 秒間の接続数で設定します。

8341 ～ 50000 の範囲でレートを設定します。デフォルトは 50000 です。アクティブ/アクティブ モードでは、システムに対してこのレートを設定します。フェールオーバー グループごとにこのレートを設定することはできません。

failover replication rate *conns*

例：

```
ciscoasa(config)# failover replication rate 20000
```

ステップ 3　（アクティブ/アクティブ モードのみ）カスタマイズするフェールオーバー グループを指定します。

failover group {**1** | **2**}

例：

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)#
```

ステップ 4　（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 1 のフェールオーバー グループ プリエンプションを設定します。

preempt [*delay*]

例：

```
ciscoasa(config-fover-group)# preempt 1200
```

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。このコマンドは、指定された装置が使用可能になったときに、フェールオーバー グループがその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。

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 5　HTTP ステート複製をイネーブルにします。

- アクティブ/スタンバイ モードの場合

  failover replication http

- アクティブ/アクティブ モードの場合

  replication http

HTTP 接続がステート情報複製に含まれるようにするには、HTTP 複製をイネーブルにする必要があります。HTTP 接続は通常は存続期間が短く、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 接続は複製されるステート情報に自動的には含まれません。

ステップ 6　インターフェイスに障害が発生したときのフェールオーバーのしきい値を設定します。

- アクティブ/スタンバイ モードの場合

  failover interface-policy *num*[%]

  例：

  ```
  ciscoasa (config)# failover interface-policy 20%
  ```

- アクティブ/アクティブ モードの場合

  interface-policy *num*[%]

  例：

  ```
  ciscoasa(config-fover-group)# interface-policy 20%
  ```

デフォルトでは、1 つ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具体的な数を指定するときは、*num* 引数に 1 ～ 250 を設定できます。

インターフェイスの割合を指定するときは、*num* 引数に 1 ～ 100 を設定できます。

ステップ 7　インターフェイスのポーリング時間とホールド時間を変更します。

- アクティブ/スタンバイ モードの場合

  failover polltime interface [**msec**] *time* [**holdtime** *time*]

  例：

  ```
  ciscoasa(config)# failover polltime interface msec 500 holdtime 5
  ```

- アクティブ/アクティブ モードの場合

  polltime interface [**msec**] *time* [**holdtime** *time*]

  例：

  ```
  ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
  ```

ポーリング時間の有効な値は 1 ～ 15 秒で、オプションの **msec** キーワードを使用すると、500 ～ 999 ミリ秒です。hello パケットを受信できなかったときからインターフェイスが失敗としてマークされるまでの時間が、保持時間によって決まります。保持時間に有効な値は、5 ～ 75 秒です。ポーリング時間の 5 倍に満たない保持時間は入力できません。

インターフェイス リンクがダウンしていると、インターフェイスのテストは実行されず、設定されたフェールオーバー基準に障害のあるインターフェイスの数が合致するか、または基準を超過している場合、スタンバイ装置は、1 つのインターフェイス ポーリング期間内でアクティブになります。

ステップ 8　インターフェイスの仮想 MAC アドレスを設定します。

- アクティブ/スタンバイ モードの場合

  failover mac address *phy_if active_mac standby_mac*

  例：

  ```
  ciscoasa(config)# failover mac address gigabitethernet0/2 00a0.c969.87c8
  00a0.c918.95d8
  ```

- アクティブ/アクティブ モードの場合

  mac address *phy_if active_mac standby_mac*

  例：

  ```
  ciscoasa(config-fover-group)# mac address gigabitethernet0/2 00a0.c969.87c8
  00a0.c918.95d8
  ```

phy_if 引数は、インターフェイスの物理名（gigabitethernet0/1 など）です。

active_mac および *standby_mac* 引数は、H.H.H 形式（H は 16 ビットの 16 進数）の MAC アドレスです。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。

active_mac アドレスはインターフェイスのアクティブ IP アドレスに関連付けられ、*standby_mac* はインターフェイスのスタンバイ IP アドレスに関連付けられます。

他のコマンドまたは方法を使用して 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。

show interface コマンドを使用して、インターフェイスが使用している MAC アドレスを表示します。

ステップ 9　（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

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。

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　インターフェイスのヘルス モニタリングをイネーブルまたはディゼーブルにします。

[**no**] **monitor-interface** {*if_name* | **service-module**}

例：

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)# no monitor-interface eng1
```

ASA FirePOWER モジュールなどの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、**no monitor-interface service-module** コマンドを使用してモジュールのモニタリングをディセーブルにできます。

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。

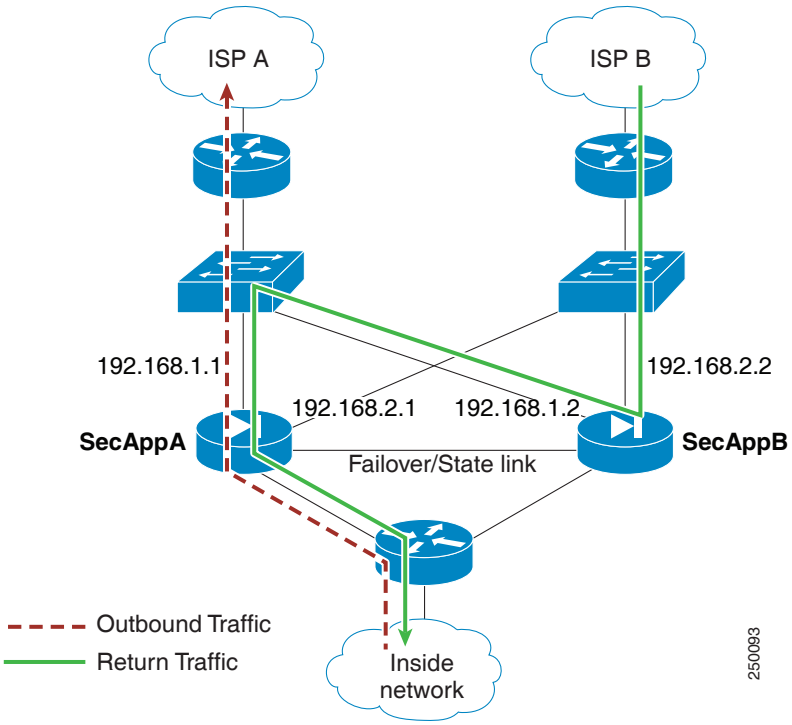
返送パケットのドロップは、非対称にルーティングされたパケットを許可することによって防ぐことができます。そのためには、それぞれの ASA の同様のインターフェイスを同じ ASR グループに割り当てます。たとえば、両方の ASA が、内部インターフェイスで内部ネットワークに接続しているが、外部インターフェイスでは別の ISP に接続しているとします。プライマリ装置で、アクティブ コンテキストの外部インターフェイスを ASR グループ 1 に割り当て、セカンダリ装置でも、アクティブ コンテキストの外部インターフェイスを同じ ASR グループ 1 に割り当てます。プライマリ装置の外部インターフェイスが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 コンテキストにある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で発信されたものの場合、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で発信されたものの場合、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 7-13 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 7-13　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。このセッションは、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 を持つ装置上でスタンバイ状態となっているインターフェイス 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

	コマンド	目的
ステップ 1	プライマリ装置で以下のコマンドを実行します。 **interface** *phy_if* **例：** `primary/admin(config)# interface gigabitethernet 0/0`	非対称にルーティングされたパケットを許可するプライマリ装置のインターフェイスを指定します。
ステップ 2	**asr-group** *num* **例：** `primary/admin(config-ifc)# asr-group 1`	インターフェイスの ASR グループ番号を設定します。*num* 範囲に有効な値は、1 ～ 32 です。
ステップ 3	セカンダリ装置で以下のコマンドを実行します。 **interface** *phy_if* **例：** `secondary/ctx1(config)# interface gigabitethernet 0/1`	非対称にルーティングされたパケットを許可するセカンダリ装置の同様のインターフェイスを指定します。
ステップ 4	**asr-group** *num* **例：** `secondary/ctx1(config-ifc)# asr-group 1`	インターフェイスの ASR グループ番号をプライマリ装置のインターフェイスに一致するように設定します。

例

2 つの装置に次のコンフィギュレーションが設定されます（コンフィギュレーションには関連するコマンドだけを示します）。図の「SecAppA」というラベルの付いたデバイスは、フェールオーバー ペアのプライマリ装置です。

例 7-1　プライマリ装置のシステム コンフィギュレーション

```
interface GigabitEthernet0/1
  description LAN/STATE Failover Interface
interface GigabitEthernet0/2
  no shutdown
interface GigabitEthernet0/3
  no shutdown
interface GigabitEthernet0/4
  no shutdown
```

```
interface GigabitEthernet0/5
  no shutdown
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/1
failover link folink
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
  primary
failover group 2
  secondary
admin-context SecAppA
context admin
  allocate-interface GigabitEthernet0/2
  allocate-interface GigabitEthernet0/3
  config-url flash:/admin.cfg
  join-failover-group 1
context SecAppB
  allocate-interface GigabitEthernet0/4
  allocate-interface GigabitEthernet0/5
  config-url flash:/ctx1.cfg
  join-failover-group 2
```

例 7-2　SecAppA コンテキスト コンフィギュレーション

```
interface GigabitEthernet0/2
  nameif outsideISP-A
  security-level 0
  ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  asr-group 1
interface GigabitEthernet0/3
  nameif inside
  security-level 100
  ip address 10.1.0.1 255.255.255.0 standby 10.1.0.11
monitor-interface outside
```

例 7-3　SecAppB コンテキスト コンフィギュレーション

```
interface GigabitEthernet0/4
  nameif outsideISP-B
  security-level 0
  ip address 192.168.2.2 255.255.255.0 standby 192.168.2.1
  asr-group 1
interface GigabitEthernet0/5
  nameif inside
  security-level 100
  ip address 10.2.20.1 255.255.255.0 standby 10.2.20.11
```

フェールオーバーの管理

- 「フェールオーバーの強制実行」（P.7-47）
- 「フェールオーバーのディセーブル化」（P.7-48）
- 「障害が発生した装置の復元」（P.7-49）
- 「コンフィギュレーションの再同期」（P.7-49）
- 「フェールオーバー機能のテスト」（P.7-50）

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

コマンド	目的

アクティブ / スタンバイ モードのスタンバイ装置の場合
failover active
 	
アクティブ / アクティブ モードのスタンバイ装置の場合
failover active [**group** *group_id*]
 	
例：
`standby# failover active`
 	
または
`standby# failover active group 1`
	*スタンバイ*装置で入力した場合、フェールオーバーが強制実行されます。スタンバイ装置はアクティブ装置になります。
	
	group *group_id* を指定する場合、指定するアクティブ / アクティブ フェールオーバー グループの*スタンバイ*装置でこのコマンドを入力すると、フェールオーバーが強制実行されます。スタンバイ装置はそのフェールオーバー グループのアクティブ装置になります。

アクティブ / スタンバイ モードのアクティブ装置の場合
no failover active
 	
アクティブ / アクティブ モードのアクティブ装置の場合
no failover active [**group** *group_id*]
 	
例：
`active# no failover active`
 	
または
`active# no failover active group 1`
	アクティブ装置で入力した場合、フェールオーバーが強制実行されます。アクティブ装置はスタンバイ装置になります。
	
	group *group_id* を指定する場合、指定するフェールオーバー グループのアクティブ装置でこのコマンドを入力すると、フェールオーバーが強制実行されます。アクティブ装置はそのフェールオーバー グループのスタンバイ装置になります。

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

コマンド	目的
no failover **例：** ciscoasa(config)# no failover	フェールオーバーをディセーブルにします。 アクティブ / スタンバイ ペアでフェールオーバーをディセーブルにすると、リロードするまで各装置のアクティブおよびスタンバイ状態が維持されます。たとえば、スタンバイ装置はスタンバイ モードのまま維持されるので、両方の装置はトラフィックの転送を開始しません。（フェールオーバーがディセーブルにされていても）スタンバイ装置をアクティブにするには、「フェールオーバーの強制実行」（P.7-47）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 ペアでフェールオーバーをディセーブル化すると、どの装置を優先するように設定されていようと、フェールオーバー グループはアクティブであるすべての装置でアクティブ状態のまま維持されます。

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

コマンド	目的
アクティブ / スタンバイ モードの場合 **failover reset** アクティブ / アクティブ モードの場合 **failover reset** [**group** *group_id*] **例：** ciscoasa(config)# failover reset または ciscoasa(config)# failover reset group 1	障害が発生したユニットを障害が発生していない状態に復元します。障害が発生した装置を障害のない状態に復元しても、その装置が自動的にアクティブになるわけではありません。復元された装置は、フェールオーバー（強制または性質）によってアクティブになるまではスタンバイ状態のままです。例外は、フェールオーバー グループ（アクティブ / アクティブ モードのみ）にフェールオーバー プリエンプションが設定されている場合です。以前アクティブであったフェールオーバー グループにプリエンプションが設定されており、障害が発生した装置が優先装置の場合、そのフェールオーバー グループはアクティブになります。 **group** *group_id* を指定した場合、このコマンドは障害が発生したアクティブ / アクティブ フェールオーバー グループを障害のない状態に復元します。

コンフィギュレーションの再同期

アクティブ装置に **write standby** コマンドを入力すると、スタンバイ装置で実行コンフィギュレーションが削除され（アクティブ装置との通信に使用するフェールオーバー コマンドを除く）、アクティブ装置のコンフィギュレーション全体がスタンバイ装置に送信されます。

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に **write standby** コマンドを入力すると、すべてのコンテキストが複製されます。あるコンテキスト内で **write standby** コマンドを入力すると、コマンドはそのコンテキスト コンフィギュレーションだけを複製します。

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。

フェールオーバー機能のテスト

フェールオーバー機能をテストするには、次の手順を実行します。

手順の詳細

ステップ 1　FTP などを使用して、異なるインターフェイス上のホスト間でファイルを送信し、アクティブ装置が予期したとおりにトラフィックを渡しているかどうかをテストします。

ステップ 2　アクティブ装置で次のコマンドを入力し、フェールオーバーを強制実行します。

アクティブ/スタンバイ モード

```
ciscoasa(config)# no failover active
```

アクティブ/アクティブ モード

```
ciscoasa(config)# no failover active group group_id
```

ステップ 3　FTP を使用して、2 つの同じホスト間で別のファイルを送信します。

ステップ 4　テストが成功しなかった場合は、**show failover** コマンドを入力してフェールオーバー ステータスを確認します。

ステップ 5　テストが終了したら、新しくアクティブになった装置で次のコマンドを入力すると、装置をアクティブ ステータスに復元できます。

アクティブ/スタンバイ モード

```
ciscoasa(config)# no failover active
```

アクティブ/アクティブ モード

```
ciscoasa(config)# failover active group group_id
```

（注）　ASA のインターフェイスの 1 つがダウンしたときも、フェールオーバーの観点からは、これも装置の問題と見なされます。インターフェイスの 1 つがダウンしていることを ASA が検出した場合は、インターフェイスのホールド時間を待たずに、フェールオーバーがただちに行われます。インターフェイスのホールド時間が有効であるのは、ASA が自身のステータスを OK と見なしているときだけです（ピアから hello パケットを受信していなくても）。インターフェイスのホールド時間をシミュレートするには、ピアが他のピアから hello パケットを受信するのを停止させるために、スイッチ上で VLAN をシャットダウンします。

リモート コマンドの実行

リモート コマンドを実行すると、コマンド ラインに入力されたコマンドを特定のフェールオーバー ピアに送信できます。

- 「コマンドの送信」（P.7-51）
- 「コマンド モードの変更」（P.7-51）
- 「セキュリティの考慮事項」（P.7-53）
- 「リモート コマンドの実行に関する制限事項」（P.7-53）

コマンドの送信

コンフィギュレーション コマンドはアクティブ装置またはコンテキストからスタンバイ装置またはコンテキストに複製されるため、いずれの装置にログインしているかにかかわらず、**failover exec** コマンドを使用して正しい装置にコンフィギュレーション コマンドを入力できます。たとえば、スタンバイ装置にログインしている場合、**failover exec active** コマンドを使用して、コンフィギュレーションの変更をアクティブ装置に送信できます。その後、これらの変更はスタンバイ装置に複製されます。スタンバイ装置またはコンテキストへのコンフィギュレーション コマンドの送信には、**failover exec** コマンドを使用しないでください。これらのコンフィギュレーションの変更はアクティブ装置に複製されないため、2 つのコンフィギュレーションが同期されなくなります。

コンフィギュレーション、exec、および **show** コマンドの出力は、現在のターミナル セッションで表示されます。したがって、**failover exec** コマンドを使用して、ピア装置で **show** コマンドを発行し、その結果を現在のターミナルに表示することができます。

ピア装置でコマンドを実行するには、ローカル装置でコマンドを実行できるだけの十分な権限を持っている必要があります。

手順の詳細

ステップ 1　マルチ コンテキスト モードの場合は、**changeto context** *name* コマンドを使用して、設定するコンテキストに変更します。**failover exec** コマンドを使用して、フェールオーバー ピアでコンテキストを変更することはできません。

ステップ 2　次のコマンドを使用して、所定のフェールオーバー装置にコマンドを送信します。

```
ciscoasa(config)# failover exec {active | mate | standby}
```

active または **standby** キーワードを使用すると、その装置が現在の装置であっても、コマンドは指定された装置で実行されます。**mate** キーワードを使用すると、コマンドはフェールオーバー ピアで実行されます。

コマンド モードを変更するコマンドによって、現在のセッションのプロンプトが変更されることはありません。コマンドが実行されるコマンド モードを表示するには、**show failover exec** コマンドを使用する必要があります。詳細については、「コマンド モードの変更」（P.7-51）を参照してください。

コマンド モードの変更

failover exec コマンドは、お使いのターミナル セッションのコマンド モードとは異なるコマンド モード状態を維持します。デフォルトでは、**failover exec** コマンド モードは、指定されたデバイスのグローバル コンフィギュレーション モードで開始されます。このコマンド モードを

変更するには、**failover exec** コマンドを使用して適切なコマンド（**interface** コマンドなど）を送信します。**failover exec** を使用してモードを変更しても、セッション プロンプトは変更されません。

たとえば、フェールオーバー ピアのアクティブ装置のグローバル コンフィギュレーション モードにログインし、**failover exec active** コマンドを使用してインターフェイス コンフィギュレーション モードを変更した場合、ターミナル プロンプトはグローバル コンフィギュレーション モードのままですが、**failover exec** を使用して入力されるコマンドは、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。

次の例は、ターミナル セッション モードと **failover exec** コマンド モードの違いを示しています。この例で、管理者はアクティブ装置の **failover exec** モードを、インターフェイス GigabitEthernet0/1 用のインターフェイス コンフィギュレーション モードに変更します。その後、**failover exec active** を使用して入力されたすべてのコマンドは、インターフェイス GigabitEthernet0/1 のインターフェイス コンフィギュレーション モードに送信されます。次に、管理者は failover exec active を使用して、そのインターフェイスに IP アドレスを割り当てます。プロンプトはグローバル コンフィギュレーション モードを示していますが、**failover exec active** モードはインターフェイス コンフィギュレーション モードです。

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# failover exec active ip address 192.168.1.1 255.255.255.0 standby
192.168.1.2
ciscoasa(config)# router rip
ciscoasa(config-router)#
```

デバイスとの現在のセッションのコマンド モードを変更しても、**failover exec** コマンドで使用されるコマンド モードには影響しません。たとえば、アクティブ装置のインターフェイス コンフィギュレーション モードで、**failover exec** コマンド モードを変更していない場合、次のコマンドはグローバル コンフィギュレーション モードで実行されます。その結果、デバイスとのセッションはインターフェイス コンフィギュレーション モードのままで、**failover exec active** を使用して入力されたコマンドは、指定されたルーティング プロセスを実行するためルータ コンフィギュレーション モードに送信されます。

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

show failover exec コマンドを使用すると、指定したデバイスにコマンド モードが表示されます。**failover exec** コマンドを使用して送信されたコマンドは、このモードで実行されます。**show failover exec** コマンドでは、**failover exec** コマンドと同じキーワード、つまり **active**、**mate**、または **standby** が使用されます。各デバイスの **failover exec** モードは個別に追跡されます。

次に、スタンバイ装置に入力された **show failover exec** コマンドの出力例を示します。

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# sh failover exec active
Active unit Failover EXEC is at interface sub-command mode

ciscoasa(config)# sh failover exec standby
Standby unit Failover EXEC is at config mode

ciscoasa(config)# sh failover exec mate
Active unit Failover EXEC is at interface sub-command mode
```

セキュリティの考慮事項

failover exec コマンドは、フェールオーバー リンクを使用してコマンドをピア装置に送信し、実行されたコマンドの出力をピア装置から受信します。盗聴や中間者攻撃を防ぐためには、フェールオーバー リンクの暗号化をイネーブルにする必要があります。

リモート コマンドの実行に関する制限事項

リモート コマンドの使用には、次の制限事項があります。

- ゼロダウンタイム アップグレード手順を使用して 1 台の装置だけをアップグレードする場合は、機能するコマンドとして **failover exec** コマンドをサポートしているソフトウェアが両方の装置で動作している必要があります。
- コマンドの完成およびコンテキスト ヘルプは、*cmd_string* 引数のコマンドでは使用できません。
- マルチ コンテキスト モードでは、ピア装置のピア コンテキストだけにコマンドを送信できます。異なるコンテキストにコマンドを送信するには、まずログインしている装置でそのコンテキストに変更する必要があります。
- 次のコマンドと **failover exec** コマンドを一緒に使用することはできません。
  - **changeto**
  - **debug**（**undebug**）
- スタンバイ装置が故障状態の場合、故障の原因がサービス カードの不具合であれば、**failover exec** コマンドからのコマンドは受信できます。それ以外の場合、リモート コマンドの実行は失敗します。
- **failover exec** コマンドを使用して、フェールオーバー ピアで特権 EXEC モードをグローバル コンフィギュレーション モードに切り替えることはできません。たとえば、現在の装置が特権 EXEC モードのときに **failover exec mate configure terminal** を入力すると、**show failover exec mate** の出力に、failover exec セッションがグローバル コンフィギュレーション モードであることが示されます。ただし、ピア装置で **failover exec** を使用してコンフィギュレーション コマンドを入力した場合、現在の装置でグローバル コンフィギュレーション モードを開始しない限り、その処理は失敗します。
- **failover exec mate failover exec mate** コマンドのような、再帰的な failover exec コマンドは入力できません。
- ユーザの入力または確認が必要なコマンドでは、**/nonconfirm** オプションを使用する必要があります。

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」（P.7-54）
- 「フェールオーバー動作のモニタ」（P.7-55）

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」（P.7-54）
- 「フェールオーバー デバッグ メッセージ」（P.7-54）
- 「SNMP のフェールオーバー トラップ」（P.7-54）

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 39 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 40 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

フェールオーバーをモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
`show failover`	装置のフェールオーバー状態についての情報を表示します。
`show failover group`	フェールオーバー グループのフェールオーバー状態に関する情報を表示します。表示される情報は、**show failover** コマンドの場合と似ていますが、指定されたグループに対象が限定されます。
`show monitor-interface`	モニタ対象インターフェイスの情報を表示します。
`show running-config failover`	実行コンフィギュレーション内のフェールオーバー コマンドを表示します。

モニタリング コマンドの出力の詳細については、コマンド リファレンスを参照してください。

フェールオーバーの機能履歴

表 7-4 に、この機能のリリース履歴を示します。

表 7-4　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。 **failover key hex** コマンドが変更されました。
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。 **failover key [0 | 8]** コマンドが変更されました。

表 7-4　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 （続き）

機能名	リリース	機能情報
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)	**failover interface ip**、**show failover**、**ipv6 address**、**show monitor-interface** の各コマンドが変更されました。
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（**failover key** コマンド）、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。 **failover ipsec pre-shared-key**、**show vpn-sessiondb** の各コマンドが導入または変更されました。
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、デフォルトでは ASA FirePOWER モジュールなどインストール済みハードウェア モジュールのヘルスをモニタします。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。 次のコマンドが変更されました。**monitor-interface service-module**

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.8-25）を参照してください。

- 「ASA クラスタリングについて」（P.8-1）
- 「ASA クラスタリングのライセンス」（P.8-32）
- 「ASA クラスタリングの前提条件」（P.8-33）
- 「ASA クラスタリングのガイドライン」（P.8-34）
- 「ASA クラスタリングのデフォルト」（P.8-38）
- 「ASA クラスタリングの設定」（P.8-38）
- 「ASA クラスタ メンバの管理」（P.8-58）
- 「ASA クラスタのモニタリング」（P.8-63）
- 「ASA クラスタリングの例」（P.8-68）
- 「ASA クラスタリングの履歴」（P.8-81）

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。

- 「ASA クラスタをネットワークに適合させる方法」（P.8-2）
- 「パフォーマンス スケーリング係数」（P.8-2）
- 「クラスタ メンバ」（P.8-3）
- 「クラスタ インターフェイス」（P.8-4）
- 「クラスタ制御リンク」（P.8-6）
- 「ASA クラスタ内のハイ アベイラビリティ」（P.8-9）
- 「コンフィギュレーションの複製」（P.8-12）
- 「ASA クラスタ管理」（P.8-12）

- 「ロード バランシングの方式」（P.8-14）
- 「サイト間クラスタリング」（P.8-19）
- 「ASA クラスタが接続を管理する方法」（P.8-23）
- 「ASA の機能とクラスタリング」（P.8-25）

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.8-32）
- 「クラスタ制御リンク」（P.8-6）
- 「ASA クラスタ管理」（P.8-12）
- 「スパンド EtherChannel（推奨）」（P.8-14）
- 「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.8-18）
- 「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.8-19）

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.8-3）
- 「マスターおよびスレーブ ユニットの役割」（P.8-3）
- 「マスター ユニット選定」（P.8-3）

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.8-26）

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

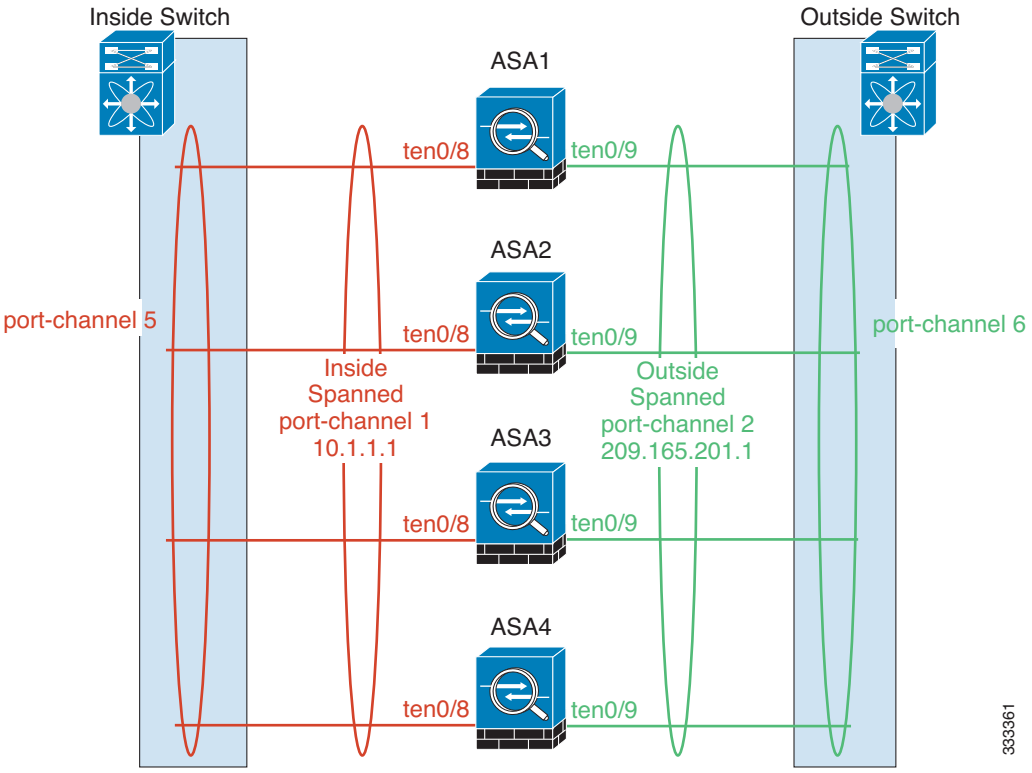
- 「クラスタリングの中央集中型機能」（P.8-26）

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）

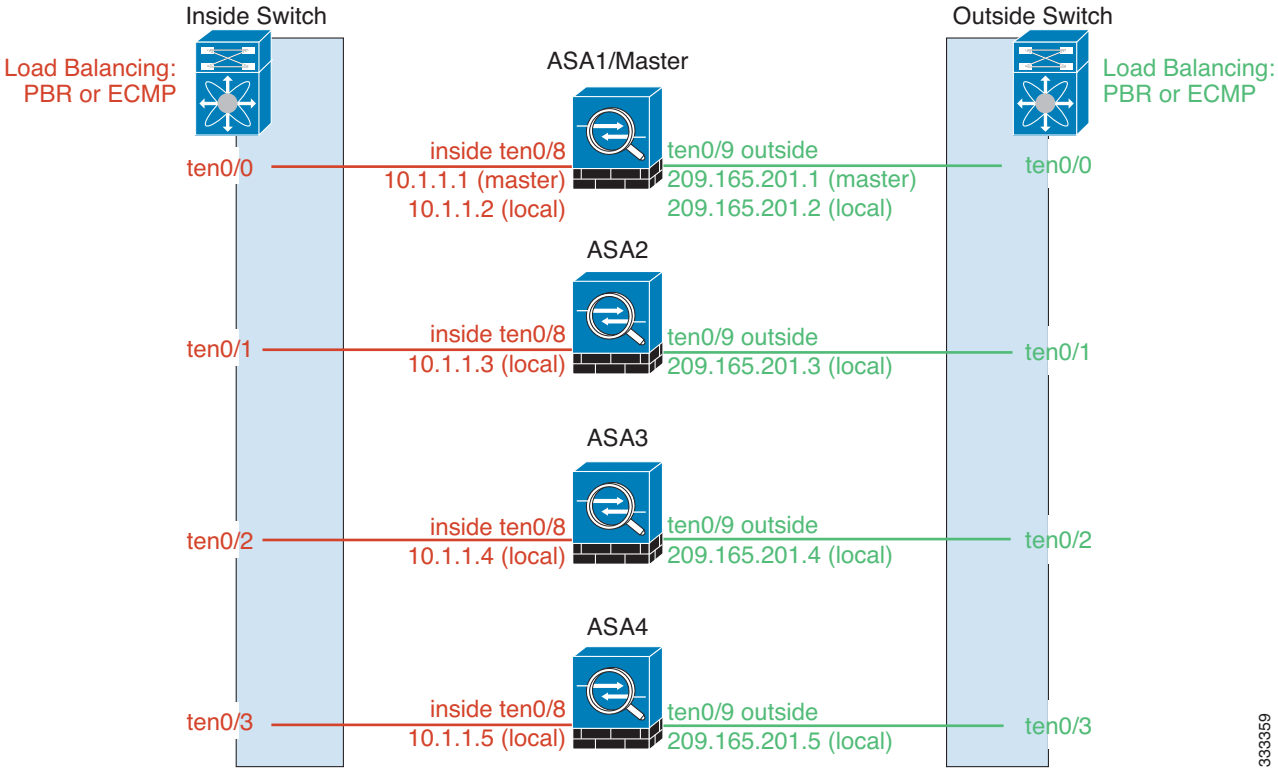
ユニットあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのユニットに広がる EtherChannel とすることができます。EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォール モードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはインターフェイスではなくブリッジ 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.8-14）

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.8-6）
- 「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.8-7）
- 「クラスタ制御リンクのサイジング」（P.8-8）
- 「クラスタ制御リンクの冗長性」（P.8-8）
- 「クラスタ制御リンクの信頼性」（P.8-9）
- 「クラスタ制御リンクの障害」（P.8-9）

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.8-3）
- 「コンフィギュレーションの複製」（P.8-12）
- 「ユニットのヘルス モニタリング」（P.8-10）
- 「データ パス接続状態の複製」（P.8-11）
- 「新しい TCP 接続のクラスタ全体での再分散」（P.8-25）

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。
- Management *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 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.8-8）
- 「クラスタ制御リンクのサイジング」（P.8-8）

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。

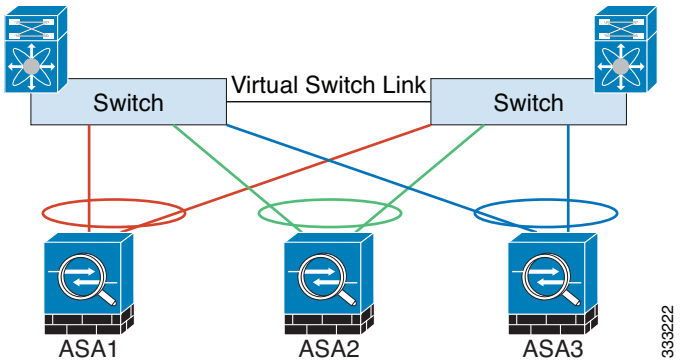
関連項目

- 「サイト間クラスタリング」（P.8-19）

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.8-11）

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」（P.8-10）
- 「インターフェイスのモニタ」（P.8-10）
- 「ユニットまたはインターフェイスの障害」（P.8-10）
- 「データ パス接続状態の複製」（P.8-11）

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 リンク集約制御プロトコル（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.8-11）

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、コンソール ポートで **cluster** *name* と入力してから **enable** と入力して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、コンソール ポートで **cluster** *name* と入力してから **enable** と入力して、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 **enable** コマンドで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

- 「マスター ユニットのブートストラップの設定」（P.8-49）

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 8-1　　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	メモ
アップ タイム	Yes	システム アップ タイムをトラッキングします。
ARP テーブル	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	×	—
VPN（サイト間）	×	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.8-12）
- 「管理インターフェイス」（P.8-12）
- 「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.8-13）
- 「RSA キー複製」（P.8-13）
- 「ASDM 接続証明書 IP アドレス不一致」（P.8-13）

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 34 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.8-14）
- 「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.8-18）
- 「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.8-19）

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.8-14）
- 「最大スループットのガイドライン」（P.8-14）
- 「ロード バランシング」（P.8-15）
- 「EtherChannel の冗長性」（P.8-15）
- 「VSS または vPC への接続」（P.8-15）

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.9-5）

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.9-24）
- 「ロード バランシング」（P.9-7）
- 「NAT とクラスタリング」（P.8-30）

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

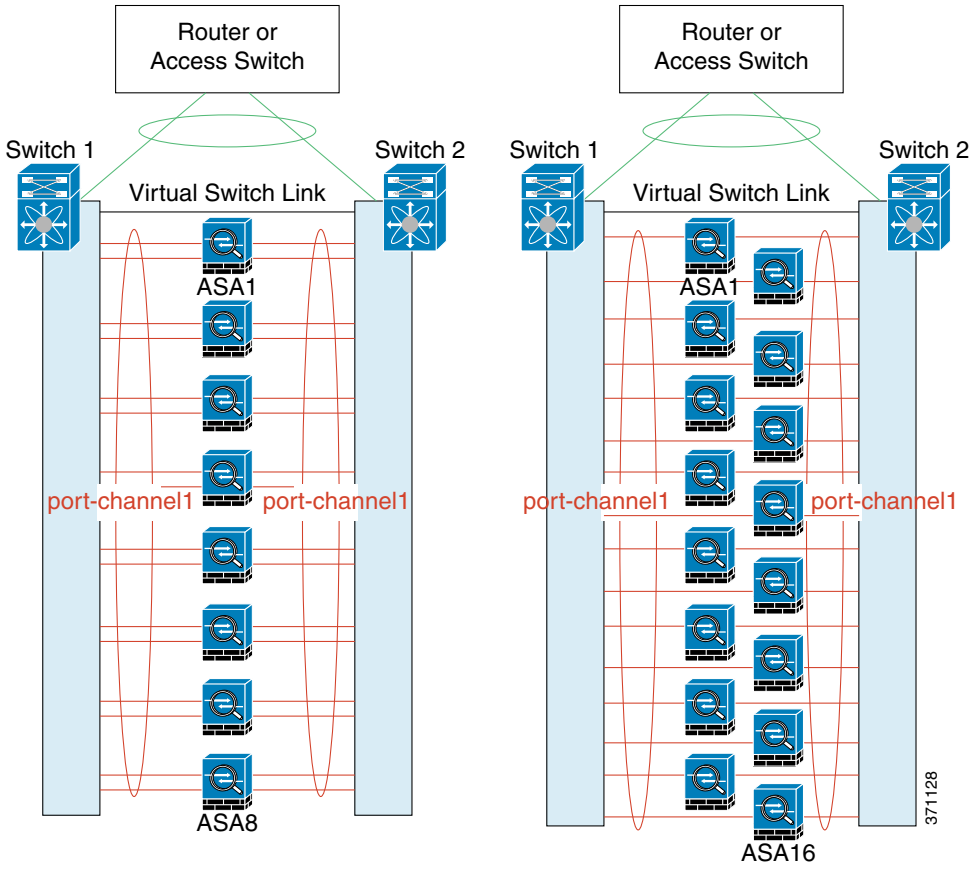
1 つの ASA につき複数のインターフェイスを、スパンド EtherChannel に入れることができます。1 つの ASA につき複数のインターフェイスが特に役立つのは、VSS または vPC の両方のスイッチに接続するときです。

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）。

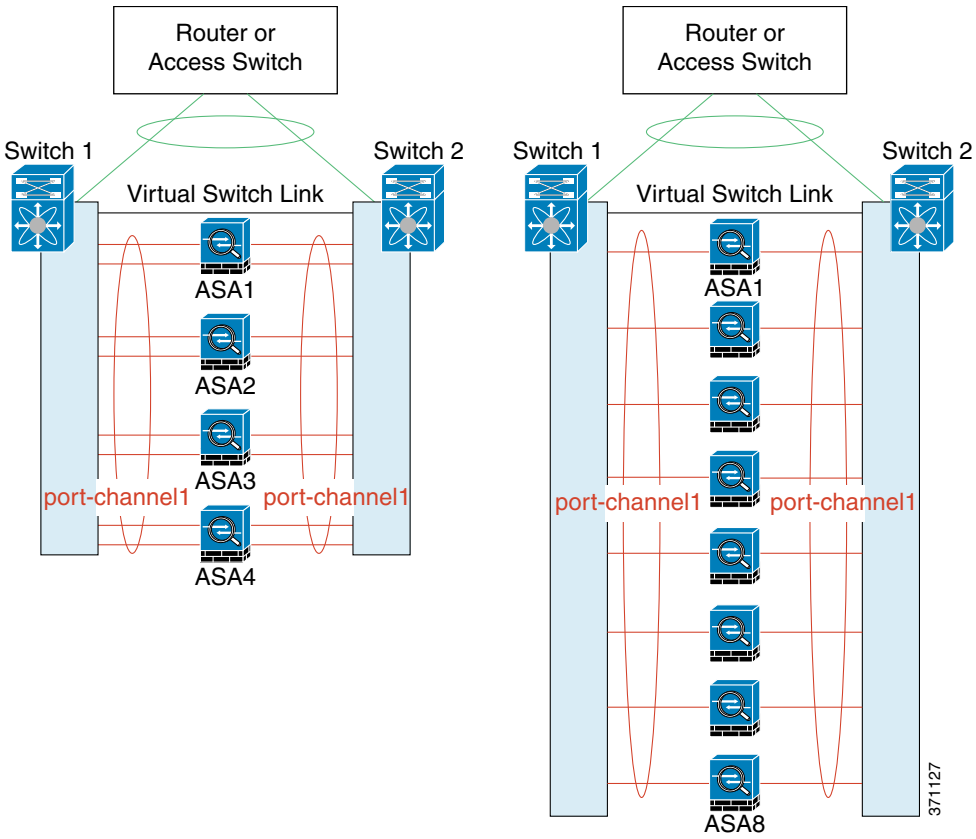
EtherChannel で 8 個のアクティブ リンクをサポートするスイッチの場合、VSS/vPC で 2 台のスイッチに接続すると、スパンド EtherChannel に最大 16 個のアクティブ リンクを設定できます。

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。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。

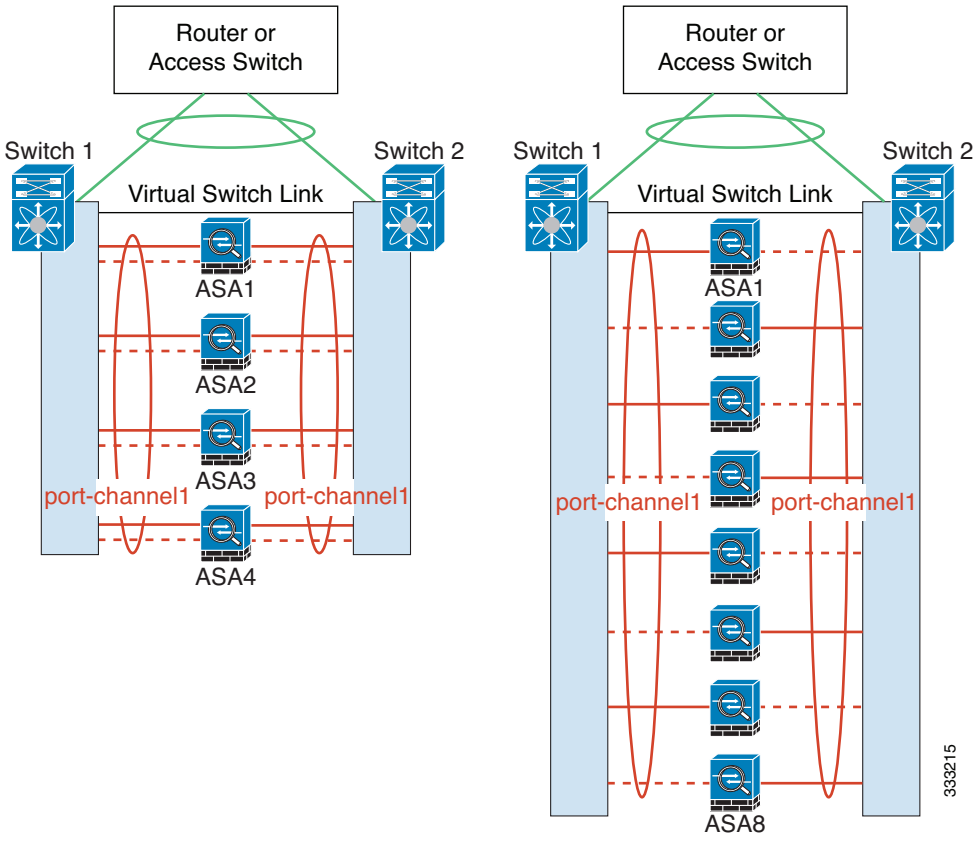
次の図では、8 ASA クラスタおよび 16 ASA クラスタでの 32 アクティブ リンクのスパンド EtherChannel を示します。



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。

サイト間クラスタリング

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。

- 「サイト間クラスタリングのガイドライン」（P.8-19）
- 「Data Center Interconnect のサイジング」（P.8-20）
- 「サイト間での例」（P.8-21）

サイト間クラスタリングのガイドライン

サイト間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 サイト間クラスタリングをサポートします。

インターフェイス モード	ファイアウォール 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	×	**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.8-25）
- 「接続のロール」（P.8-23）

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）。

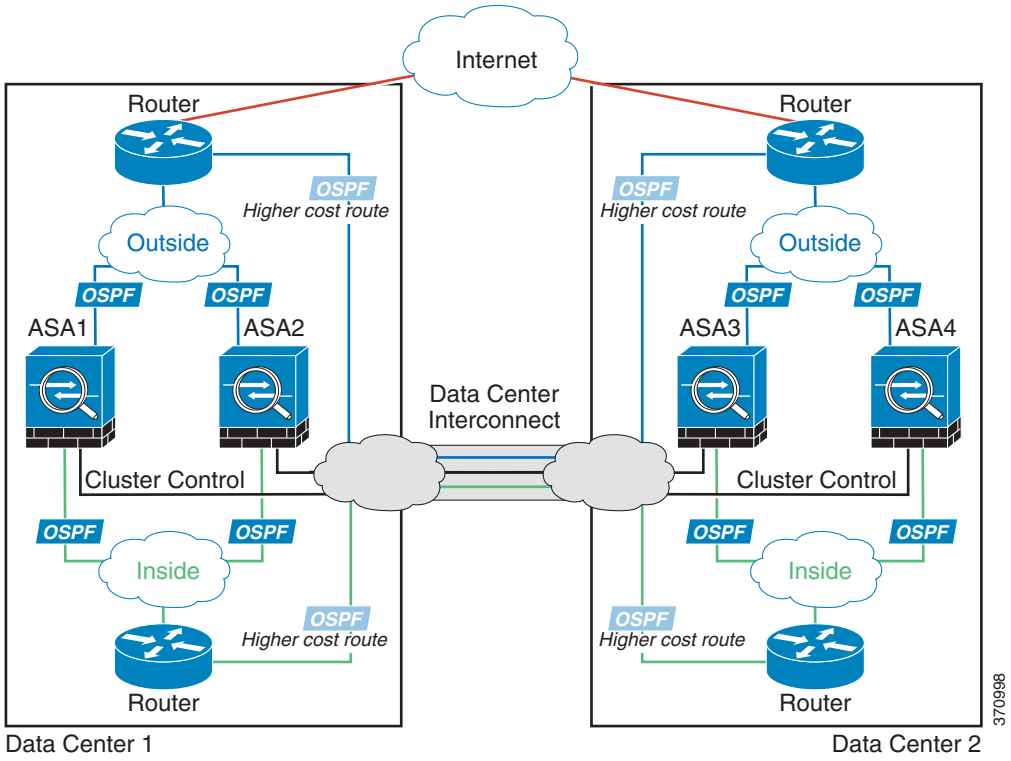
サイト間での例

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のサイト間 の例」（P.8-21）
- 「スパンド EtherChannel トランスペアレント モードのサイト間の例」（P.8-22）

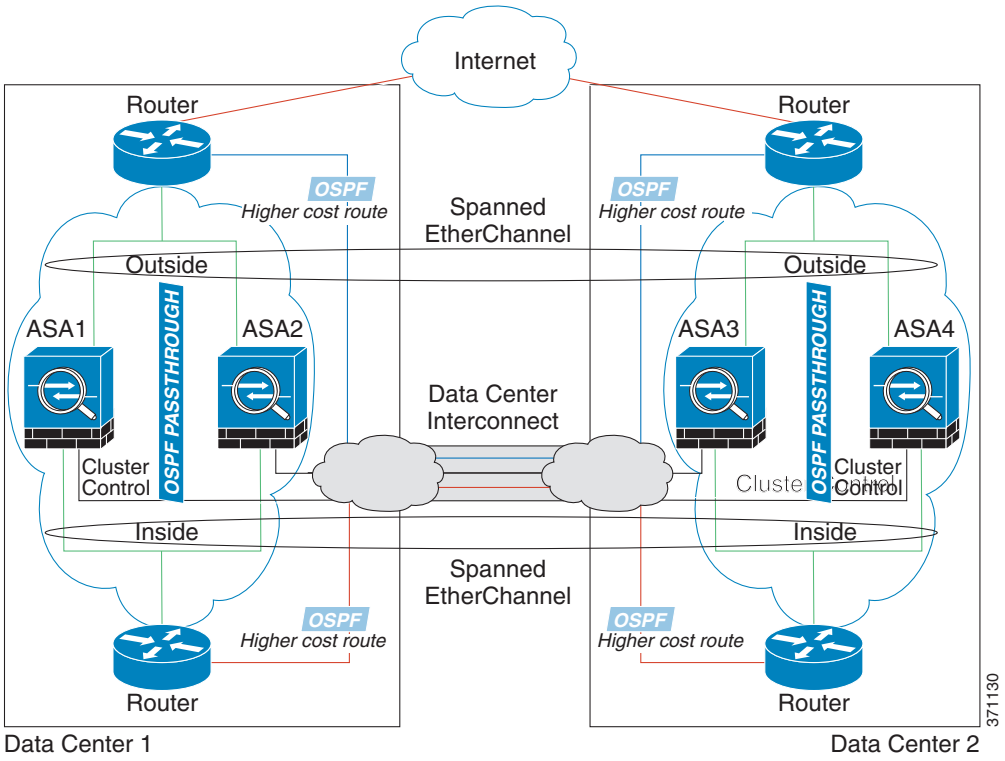
個別インターフェイスのサイト間 の例

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 モードのサイト間の例

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。

- サイト間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.8-23）
- 「新しい接続の所有権」（P.8-24）
- 「サンプル データ フロー」（P.8-24）
- 「新しい TCP 接続のクラスタ全体での再分散」（P.8-25）

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

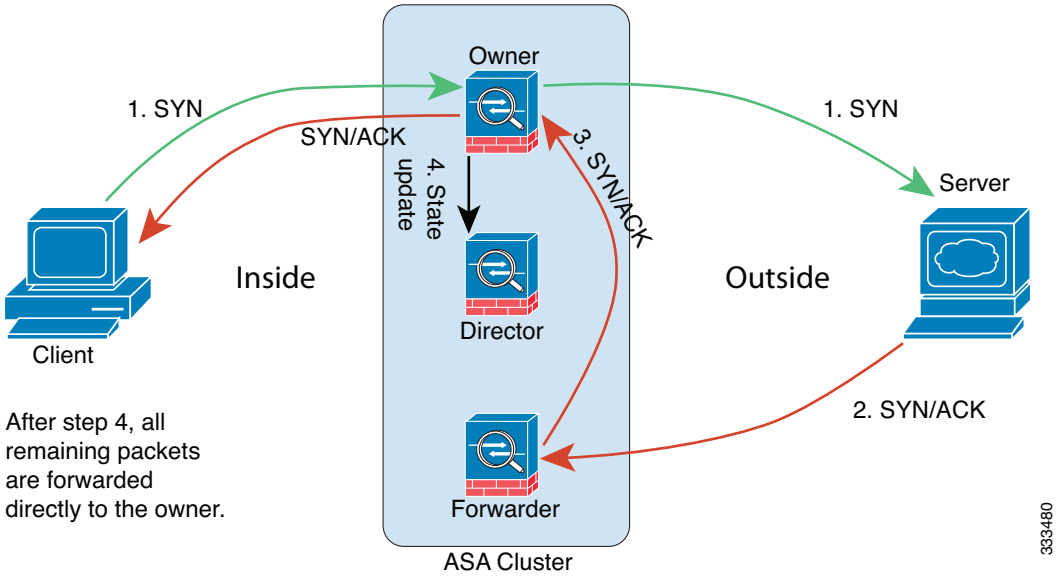
新しい接続がロード バランシング経由でクラスタのメンバに送信される場合は、そのユニットがその接続の両方向のオーナーとなります。接続のパケットが別のユニットに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナー ユニットに転送されます。最適なパフォーマンスを得るには、適切な外部ロード バランシングが必要です。1 つのフローの両方向が同じユニットに到着するとともに、フローがユニット間に均等に分散されるようにするためです。逆方向のフローが別のユニットに到着した場合は、元のユニットにリダイレクトされます。

関連項目

- 「ロード バランシングの方式」（P.8-14）

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」（P.8-25）
- 「クラスタリングの中央集中型機能」（P.8-26）
- 「個々のユニットに適用される機能」（P.8-27）
- 「ダイナミック ルーティングとクラスタリング」（P.8-28）
- 「マルチキャスト ルーティングとクラスタリング」（P.8-29）
- 「NAT とクラスタリング」（P.8-30）
- 「ネットワーク アクセス用の AAA とクラスタリング」（P.8-31）
- 「syslog および NetFlow とクラスタリング」（P.8-31）
- 「SNMP とクラスタリング」（P.8-31）
- 「VPN とクラスタリング」（P.8-31）
- 「FTP とクラスタリング」（P.8-32）
- 「Cisco TrustSec とクラスタリング」（P.8-32）

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.8-8）
- 「新しい TCP 接続のクラスタ全体での再分散」（P.8-25）

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。

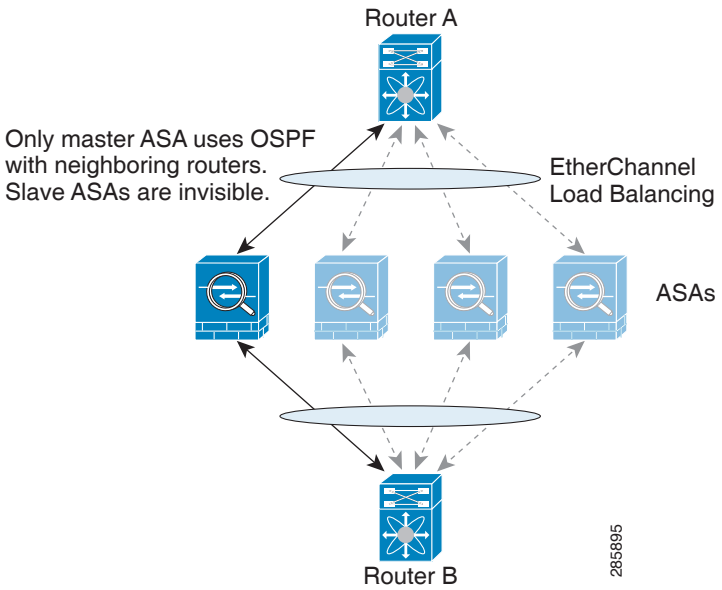
ダイナミック ルーティングとクラスタリング

- 「スパンド EtherChannel モードでのダイナミック ルーティング」（P.8-28）
- 「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.8-29）

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 8-1　スパンド EtherChannel モードでのダイナミック ルーティング



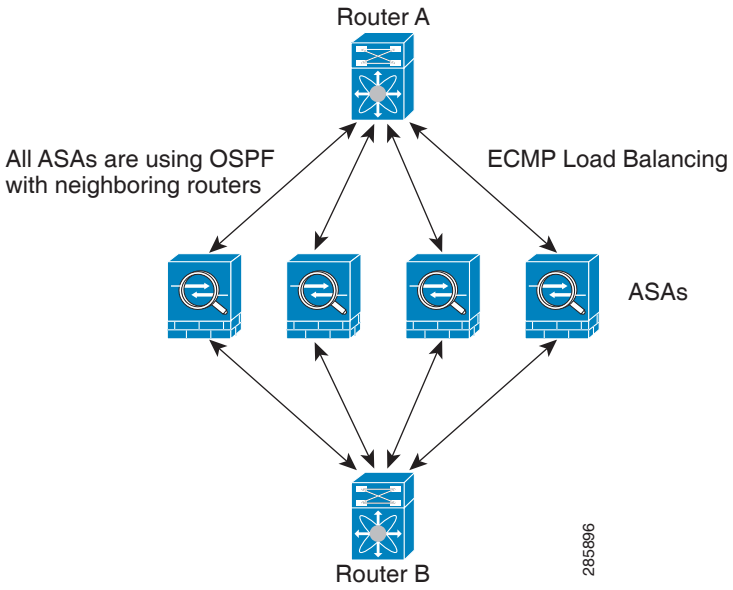
スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

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 8-2　　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.8-29）
- 「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.8-29）

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.39-17）

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 8-2　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 の前提条件

- 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.8-34）
- 「ジャンボ フレーム サポートのイネーブル化」（P.9-28）
- 「ブートストラップ コンフィギュレーション」（P.8-3）

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

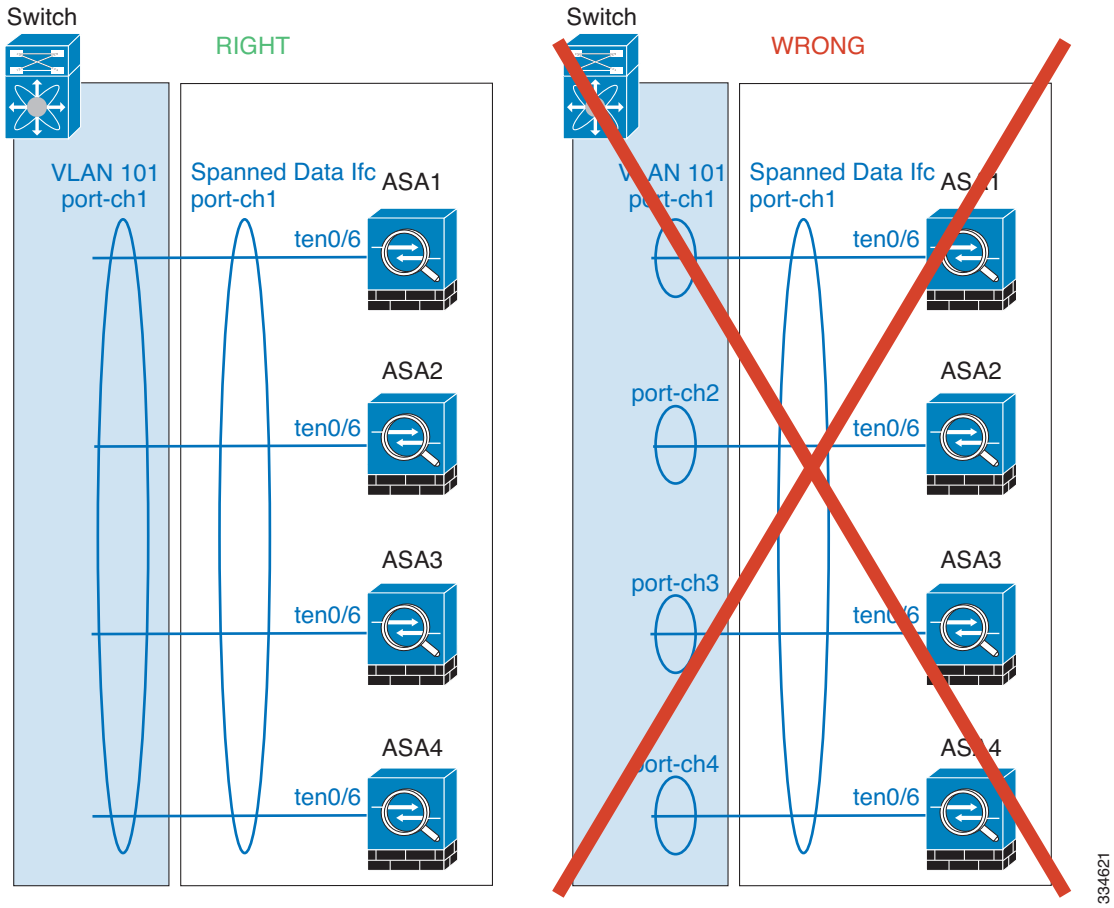
スイッチ

- 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。

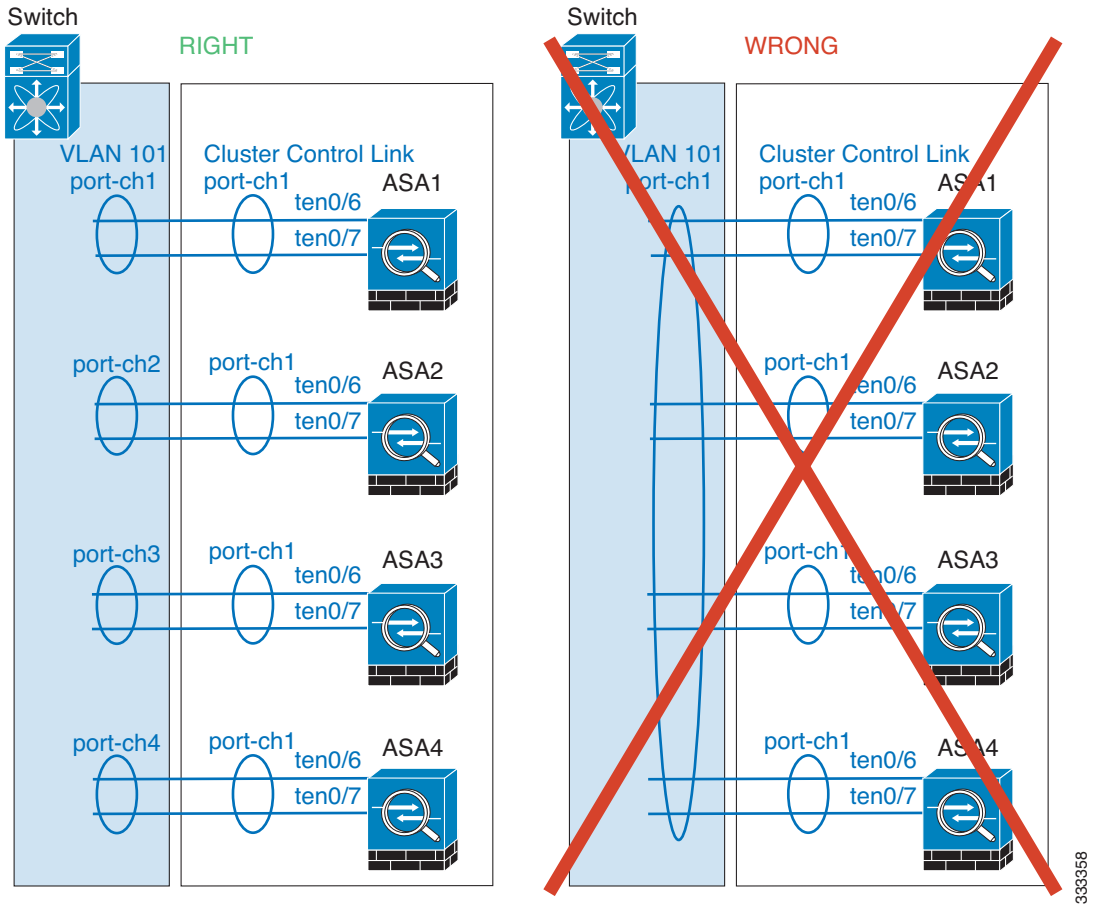
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタ内の ASA へのトラフィックが均等に分散されなくなることがあるため、ロードバランシング アルゴリズムでは、**vlan** キーワードを使用しないでください。ASA のデフォルトのロードバランシング アルゴリズムを変更*しないでください*（**port-channel load-balance** コマンド内）。
- 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.8-8）
- 「ブートストラップ コンフィギュレーション」（P.8-3）
- 「クラスタリングでサポートされない機能」（P.8-25）
- 「EtherChannel の設定」（P.9-21）
- 「EtherChannel のガイドライン」（P.9-13）

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.8-33）および「ASA クラスタリングのガイドライン」（P.8-34）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.8-39）

ステップ 3　「各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.8-41）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 4　「マスター ユニットでのインターフェイスの設定」（P.8-42）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。

ステップ 5　「マスター ユニットのブートストラップの設定」（P.8-49）

ステップ 6　「スレーブ ユニットのブートストラップの設定」（P.8-56）

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。

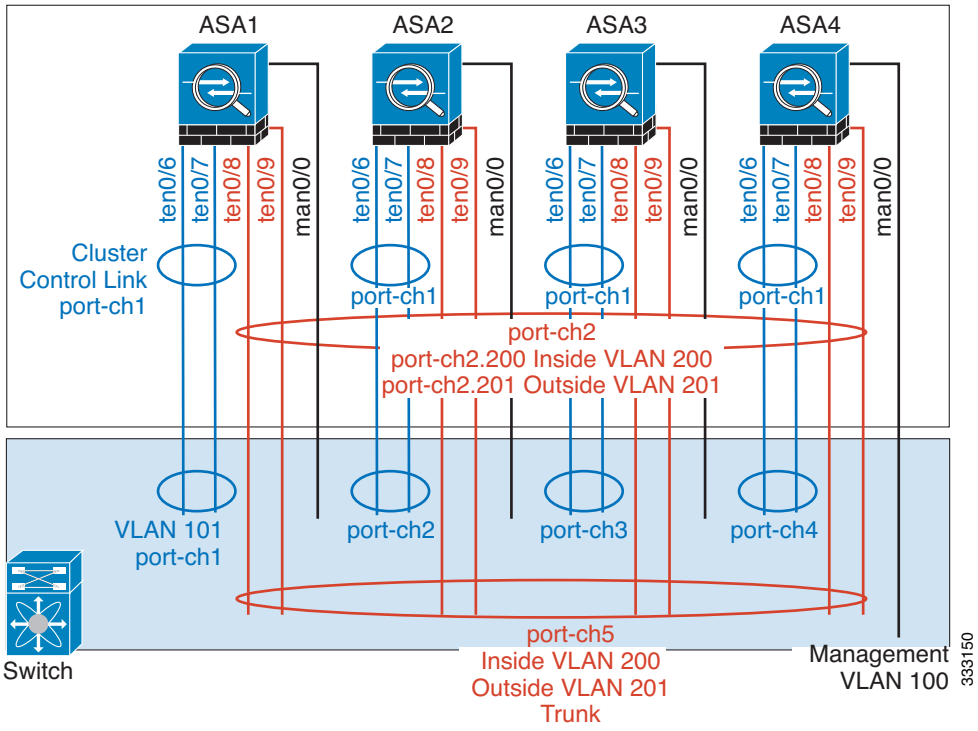
例

（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。

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
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。

各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。

はじめる前に

- モードの設定は、クラスタに追加する各 ASA で個別に行う必要があります。
- 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　互換性のないコンフィギュレーションを表示し、インターフェイス モードを強制した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：

```
ciscoasa(config)# cluster interface-mode spanned check-details
```

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：

```
ciscoasa(config)# cluster interface-mode spanned force
```

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。

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。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。

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.8-43）
- 「スパンド EtherChannel の設定」（P.8-45）

関連項目

- 「クラスタ インターフェイス」（P.8-4）

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、**changeto context** *name* コマンドを入力します。
- 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。

手順

ステップ 1　ローカル IP アドレス（IPv4 と IPv6 の一方または両方）のプールを設定します。このアドレスの 1 つが、このインターフェイス用に各クラスタ ユニットに割り当てられます。

（IPv4）

ip local pool *poolname first-address*—*last-address* [**mask** *mask*]

（IPv6）

ipv6 local pool *poolname ipv6-address/prefix-length number_of_addresses*

例：

```
ciscoasa(config)# ip local pool ins 192.168.1.2-192.168.1.9
ciscoasa(config-if)# ipv6 local pool insipv6 2001:DB8::1002/32 8
```

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。クラスタを拡張する予定の場合は、アドレスを増やします。現在のマスター ユニットに属するメイン クラスタ IP アドレスは、このプールの一部では*ありません*。必ず、同じネットワークの IP アドレスの 1 つをメイン クラスタ IP アドレス用に確保してください。

各ユニットに割り当てられるローカル アドレスを、事前に正確に特定することはできません。各ユニットで使用されているアドレスを表示するには、**show ip**[**v6**] **local pool** *poolname* コマンドを入力します。各クラスタ メンバには、クラスタに参加したときにメンバ ID が割り当てられます。この ID によって、プールから使用されるローカル IP が決定します。

ステップ 2　インターフェイス コンフィギュレーション モードを開始します。

interface *interface_id*

例：

```
ciscoasa(config)# interface tengigabitethernet 0/8
```

ステップ 3　（管理インターフェイスのみ）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。

management-only

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。

この設定は、クラスタ インターフェイス モードがスパンドの場合に必要です。

ステップ 4　インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。

ステップ 5　メイン クラスタの IP アドレスを設定し、クラスタ プールを指定します。

（IPv4）

ip address *ip_address* [*mask*] **cluster-pool** *poolname*

（IPv6）

ipv6 address *ipv6-address/prefix-length* **cluster-pool** *poolname*

例：

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ciscoasa(config-if)# ipv6 address 2001:DB8::1002/32 cluster-pool insipv6
```

この IP アドレスは、クラスタ プール アドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。IPv4 アドレスと IPv6 アドレスの一方または両方を設定できます。

DHCP、PPPoE、および IPv6 自動設定はサポートされません。IP アドレスを手動で設定する必要があります。

ステップ 6　セキュリティ レベルを設定します。*number* には、0（最低）～ 100（最高）の整数を指定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 100
```

ステップ 7　インターフェイスをイネーブルにします。

no shutdown

例

次の例では、Management 0/0 およびManagement 0/1 インターフェイスをデバイス ローカル EtherChannel として設定してから、この EtherChannel を個別インターフェイスとして設定します。

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8:45:1002/64 8

interface management 0/0
    channel-group 1 mode active
    no shutdown

interface management 0/1
    channel-group 1 mode active
    no shutdown

interface port-channel 1
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8:45:1001/64 cluster-pool mgmtipv6
    security-level 100
    management-only
```

関連項目

- 「管理インターフェイス」（P.8-12）
- 「各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.8-41）
- 「ロード バランシングの方式」（P.8-14）
- 「EtherChannel の設定」（P.9-21）
- 「冗長インターフェイスの設定」（P.9-19）
- 「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.9-26）
- 「セキュリティ レベル」（P.11-1）

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、**changeto system** コマンドを入力します。
- 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（**lacp max-bundle** コマンドと **port-channel min-bundle** コマンド）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（**port-channel load-balance** コマンドを参照）。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。
- **lacp port-priority** コマンドと **lacp system-priority** コマンドは、スパンド EtherChannel には使用されません。
- 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　チャネル グループに追加するインターフェイスを指定します。

```
interface physical_interface
```

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID には、タイプ、スロット、およびポート番号を *type slot/port* という形式で指定します。チャネル グループのこの最初のインターフェイスによって、グループ内の他のすべてのインターフェイスのタイプと速度が決まります。

ステップ 2　EtherChannel にこのインターフェイスを割り当てます。

```
channel-group channel_id mode active [vss-id {1 | 2}]
```

例：

```
ciscoasa(config-if)# channel-group 1 mode active
```

channel_id は 1 ～ 48 です。このチャネル ID のポートチャネル インターフェイスがコンフィギュレーションにまだ存在しない場合は、自動的に追加されます。

```
interface port-channel channel_id
```

active モードだけがスパンド EtherChannel に対してサポートされます。

VSS または vPC の 2 台のスイッチに ASA を接続する場合は、このインターフェイスをどのスイッチに接続するかを指定するために **vss-id** キーワードを設定します（1 または 2）。また、ステップ 6 で **port-channel span-cluster vss-load-balance** コマンドをポートチャネル インターフェイスに対して使用する必要があります。

ステップ 3　インターフェイスをイネーブルにします。

```
no shutdown
```

ステップ 4　（オプション）EtherChannel にさらにインターフェイスを追加するには、ステップ 1 からステップ 3 までを繰り返します。

例：

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# no shutdown
```

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）、**clacp static-port-priority** コマンドを使用してダイナミック 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。

ステップ 5　ポートチャネル インターフェイスを指定します。

interface port-channel *channel_id*

例：

```
ciscoasa(config)# interface port-channel 1
```

このインターフェイスは、チャネル グループにインターフェイスを追加したときに自動的に作成されたものです。

ステップ 6　この EtherChannel をスパンド EtherChannel として設定します。

port-channel span-cluster [**vss-load-balance**]

例：

```
ciscoasa(config-if)# port-channel span-cluster
```

ASA を VSS または vPC の 2 台のスイッチに接続する場合は、**vss-load-balance** キーワードを使用して 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。ロード バランシングをイネーブルにする前に、各メンバ インターフェイスに対して **channel-group** コマンドの **vss-id** キーワードを設定する必要があります（ステップ 2を参照）。

ステップ 7　（オプション）ポートチャネル インターフェイスのイーサネット プロパティを設定します。この設定は、個別インターフェイスに対して設定されたプロパティよりも優先されます。

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。

ステップ 8　（オプション）この EtherChannel 上に VLAN サブインターフェイスを作成する予定の場合は、この時点で作成します。

例：

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

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 9　（マルチ コンテキスト モード）コンテキストにインターフェイスを割り当てます。その後で、次のとおりに入力します。

```
changeto context name
interface port-channel channel_id
```

例：

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

マルチ 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の残りの部分は各コンテキスト内で行われます。

ステップ 10　インターフェイスの名前を指定します。

```
nameif name
```

例：

```
ciscoasa(config-if)# nameif inside
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。

ステップ 11　ファイアウォール モードに応じて、次のいずれかを実行します。

- ルーテッド モード：IPv4 アドレスと IPv6 アドレスの一方または両方を設定します。

  （IPv4）

  ```
  ip address ip_address [mask]
  ```

  （IPv6）

  ```
  ipv6 address ipv6-prefix/prefix-length
  ```

  例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
  ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
  ```

  DHCP、PPPoE、および IPv6 自動設定はサポートされません。

- トランスペアレント モード：インターフェイスをブリッジ グループに割り当てます。

  ```
  bridge-group number
  ```

  例：

  ```
  ciscoasa(config-if)# bridge-group 1
  ```

  number は、1 ～ 100 の整数です。ブリッジ グループには最大 4 個のインターフェイスを割り当てることができます。同一インターフェイスを複数のブリッジ グループに割り当てることはできません。BVI のコンフィギュレーションには IP アドレスが含まれていることに注意してください。

ステップ 12　セキュリティ レベルを設定します。

```
security-level number
```

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

ステップ 13　現在のマスター ユニットがクラスタから脱退しても MAC アドレスが変化しないように、スパンド EtherChannel の MAC アドレスを設定します。

mac-address *mac_address*

例：

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

MAC アドレスが手動設定されている場合、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。

mac_address は、H.H.H 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。

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。

関連項目

- 「各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.8-41）
- 「ブリッジ グループの設定」（P.12-8）
- 「マスター ユニットのブートストラップの設定」（P.8-49）
- 「EtherChannel の設定」（P.9-21）
- 「EtherChannel のガイドライン」（P.9-13）
- 「VSS または vPC への接続」（P.8-15）
- 「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.9-16）
- 「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.9-26）
- 「セキュリティ コンテキストの設定」（P.6-21）
- 「セキュリティ レベル」（P.11-1）
- 「ASA クラスタリングのガイドライン」（P.8-34）

マスター ユニットのブートストラップの設定

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。一般的には、クラスタに参加するように最初に設定したユニットがマスター ユニットとなります。クラスタリングをイネーブルにした後で、選定期間が経過すると、クラスタのマスター ユニットが選定されます。最初はクラスタ内のユニットが 1 つだけであるため、そのユニットがマスター ユニットになります。それ以降クラスタに追加されるユニットは、スレーブ ユニットとなります。

はじめる前に

- 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 ポートを使用する必要があります。Telnet または SSH を使用することはできません。
- コンフィギュレーションをバックアップします。後でクラスタから脱退する必要が生じたときに備えて、コンフィギュレーションを復元できるようにしておくためです。
- 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次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。
- クラスタ制御リンクで使用するためのジャンボ フレームの予約をイネーブルにすることを推奨します。
- クラスタ制御リンクを除いて、コンフィギュレーション内のインターフェイスはすべて、クラスタ IP プールを指定して設定されているか、スパンド EtherChannel として設定されている必要があります。この設定は、クラスタリングをイネーブルにする前に、インターフェイス モードに応じて行います。既存のインターフェイス コンフィギュレーションがある場合は、そのインターフェイス コンフィギュレーションをクリアすることも（**clear configure interface**）、インターフェイスをクラスタ インターフェイスに変換することもできます。これは、クラスタリングをイネーブルにする前に行います。
- 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。
- クラスタ制御リンクのサイズを決定します。

手順

ステップ 1　クラスタに参加する前に、クラスタ制御リンク インターフェイスをイネーブルにします。

後でクラスタリングをイネーブルにするときに、このインターフェイスをクラスタ制御リンクとして識別します。

十分な数のインターフェイスがある場合は、複数のクラスタ制御リンク インターフェイスを結合して 1 つの EtherChannel とすることを推奨します。この EtherChannel は ASA に対してローカルであり、スパンド EtherChannel ではありません。

クラスタ制御リンク インターフェイス コンフィギュレーションは、マスター ユニットからスレーブ ユニットには複製されませんが、同じコンフィギュレーションを各ユニットで使用する必要があります。このコンフィギュレーションは複製されないため、クラスタ制御リンク インターフェイスの設定は各ユニットで個別に行う必要があります。

- 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。
- Management *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。

a. インターフェイス コンフィギュレーション モードを開始します。

```
interface interface_id
```

例：

```
ciscoasa(config)# interface tengigabitethernet 0/6
```

b. （任意、EtherChannel の場合）EtherChannel にこの物理インターフェイスを割り当てます。

channel-group *channel_id* **mode on**

例：

```
ciscoasa(config-if)# channel-group 1 mode on
```

channel_id は 1 ～ 48 です。このチャネル ID のポートチャネル インターフェイスがコンフィギュレーションにまだ存在しない場合は、自動的に追加されます。

interface port-channel *channel_id*

クラスタ制御リンクでの不要なトラフィックを削減できるように、クラスタ制御リンクのメンバ インターフェイスに対しては On モードを使用することを推奨します。クラスタ制御リンクは LACP トラフィックのオーバーヘッドを必要としません。これは隔離された、安定したネットワークであるからです。**注：** データ EtherChannel を Active モードに設定することをお勧めします。

c. インターフェイスをイネーブルにします。

no shutdown

必要があるのはインターフェイスのイネーブル化だけです。インターフェイスの名前などのパラメータを設定しないでください。

d. （EtherChannel の場合）EtherChannel に追加するインターフェイスごとに繰り返します。

例：

```
ciscoasa(config)# interface tengigabitethernet 0/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

ステップ 2　（オプション）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指定します。

mtu cluster *bytes*

例：

```
ciscoasa(config)# mtu cluster 9000
```

MTU を 64 ～ 65,535 バイトの間で設定します。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、この手順を続ける前にジャンボ フレームの予約をイネーブルにする必要があります。ジャンボ フレームの予約には、ASA のリロードが必要です。

このコマンドはグローバル コンフィギュレーション コマンドですが、ユニット間で複製されないブートストラップ コンフィギュレーションの一部でもあります。

ステップ 3　クラスタに名前を付け、クラスタ コンフィギュレーション モードにします。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

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 グループはユニットあたり 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。

ステップ 4　クラスタのこのメンバの名前を指定します。

local-unit *unit_name*

```
ciscoasa(cfg-cluster)# local-unit unit1
```

1 ～ 38 文字の一意の ASCII 文字列を使用します。各ユニットに固有の名前が必要です。クラスタ内の他のユニットと同じ名前を付けることはできません。

ステップ 5　クラスタ制御リンク インターフェイス（EtherChannel を推奨）を指定します。

cluster-interface *interface_id* **ip** *ip_address mask*

例：

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.1 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

サブインターフェイスと管理インターフェイスは許可されません。

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。このインターフェイスには、**nameif** を設定することはできません。

ユニットごとに、同じネットワークにある別の IP アドレスを指定します。

ステップ 6　マスター ユニットの選択に対するこのユニットのプライオリティを設定します。

priority *priority_number*

例：

```
ciscoasa(cfg-cluster)# priority 1
```

プライオリティは 1 ～ 100 であり、1 が最高のプライオリティです。

ステップ 7　（オプション）クラスタ制御リンクの制御トラフィックの認証キーを設定します。

key *shared_secret*

例：

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このコマンドは、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。

ステップ 8　（オプション）クラスタのヘルス チェック機能（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 モニタリングを含む）をカスタマイズします。

health-check [**holdtime** *timeout*] [**vss-enabled**]

例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

holdime 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。holdtime 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。

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。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、**vss-enabled** 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 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-enabled** 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。

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。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。

ヘルス チェックはデフォルトでイネーブルです。このコマンドの **no** 形式を使用してディセーブルにできます。

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。

ステップ 9　（オプション）TCP トラフィックの接続再分散をイネーブルにします。

conn-rebalance [**frequency** *seconds*]

例：

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

このコマンドは、デフォルトでディセーブルになっています。イネーブルの場合は、ASA は負荷情報を定期的に交換し、新しい接続の負荷を高負荷のデバイスから低負荷のデバイスに移動します。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。デフォルトは 5 秒です。

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。

ステップ 10　（オプション）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。

console-replicate

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。

ステップ 11　（オプション）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。

clacp static-port-priority

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、このコマンド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）。このコマンドを使用しないと、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。このコマンド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。

ステップ 12　（オプション）cLACP システム ID およびシステムのプライオリティを手動で指定します。

clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

例：

```
ciscoasa(cfg-cluster)# clacp system-mac 000a.0000.aaaa
```

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。cLACP ネゴシエーションのパラメータの 1 つであるシステム ID は、MAC アドレスの形式をとります。クラスタ内のすべての 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、このコマンドを使用して *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 00-0A-00-00-AA-AA は 000A.0000.AAAA と入力されます）。MAC アドレスの手動設定が必要になるのは、たとえば、トラブルシューティング目的で、認識しやすい MAC アドレスを使用したい場合です。一般的には、自動生成された MAC アドレスを使用します。

システム プライオリティ（1 ～ 65535）は、どのユニットがバンドルの決定を行うかを決めるために使用されます。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。

このコマンドは、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 13　クラスタリングをイネーブルにします。

enable [**noconfirm**]

例：

```
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
 Would you like to remove these commands?[Y]es/[N]o:Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

enable コマンドが入力されると、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ように求められます。応答として **No** を入力した場合は、クラスタリングはイネーブルになりません。確認を省略し、互換性のないコマンドを自動的に削除するには、**noconfirm** キーワードを使用します。

最初にイネーブルにしたユニットについては、マスター ユニット選定が発生します。最初のユニットは、その時点でクラスタの唯一のメンバであるため、そのユニットがマスター ユニットになります。この期間中にコンフィギュレーション変更を実行しないでください。

クラスタリングをディセーブルにするには、**no enable** コマンドを入力します。

（注） クラスタリングをディセーブルにした場合は、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、管理専用インターフェイスだけがアクティブになります。

例

次の例では、管理インターフェイスを設定し、クラスタ制御リンク用のデバイス ローカル EtherChannel を設定し、その後で、「unit1」という名前の ASA のクラスタリングをイネーブルにします。これは最初にクラスタに追加されるユニットであるため、マスター ユニットになります。

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/32 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 0/6
    channel-group 1 mode on
    no shutdown

interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown

cluster group pod1
    local-unit unit1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

関連項目

- 「ジャンボ フレーム サポートのイネーブル化」（P.9-28）
- 「マスター ユニットでのインターフェイスの設定」（P.8-42）
- 「クラスタ制御リンクのサイジング」（P.8-8）
- 「マスター ユニット選定」（P.8-3）
- 「インターフェイスのモニタ」（P.8-10）
- 「クラスタからの脱退」（P.8-60）

スレーブ ユニットのブートストラップの設定

スレーブ ユニットを設定するには、次の手順に従います。

はじめる前に

- 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 ポートを使用する必要があります。Telnet または SSH を使用することはできません。
- コンフィギュレーションをバックアップします。後でクラスタから脱退する必要が生じたときに備えて、コンフィギュレーションを復元できるようにしておくためです。
- 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。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。
- クラスタ制御リンクで使用するためのジャンボ フレームの予約をイネーブルにすることを推奨します。
- コンフィギュレーション内に、クラスタリング用として設定されていないインターフェイスがある場合は（たとえば、デフォルト コンフィギュレーションのManagement 0/0 インターフェイス）、スレーブ ユニットとしてクラスタに参加させることができます（現在の選定でマスターになる可能性はありません）。
- 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　マスター ユニットに設定したものと同じクラスタ制御リンク インターフェイスを設定します。

例：

```
ciscoasa(config)# interface tengigabitethernet 0/6
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
ciscoasa(config)# interface tengigabitethernet 0/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

ステップ 2　マスター ユニットに設定したものと同じ MTU を指定します。

例：

```
ciscoasa(config)# mtu cluster 9000
```

ステップ 3　マスター ユニットに設定したものと同じクラスタ名を指定します。

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 4　クラスタのこのメンバに一意の文字列で名前を指定します。

local-unit *unit_name*

例：

```
ciscoasa(cfg-cluster)# local-unit unit2
```

1 ～ 38 文字の ASCII 文字列を指定します。

各ユニットに固有の名前が必要です。クラスタ内の他のユニットと同じ名前を付けることはできません。

ステップ 5　マスター ユニットに設定したものと同じクラスタ制御リンク インターフェイスを指定しますが、ユニットごとに同じネットワーク上の異なる IP アドレスを指定します。

cluster-interface *interface_id* **ip** *ip_address mask*

例：

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.2 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

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。このインターフェイスには、**nameif** を設定することはできません。

ステップ 6　マスター ユニットの選択に対するこのユニットのプライオリティを設定します。通常は、マスター ユニットより高い値にします。

priority *priority_number*

例：

```
ciscoasa(cfg-cluster)# priority 2
```

プライオリティを 1 ～ 100 に設定します。1 が最高のプライオリティです。

ステップ 7　マスター ユニットに設定したものと同じ認証キーを設定します。

例：

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

ステップ 8　クラスタリングをイネーブルにします。

enable as-slave

enable as-slave コマンドを使用することによって、コンフィギュレーションに関するすべての非互換性（主として、クラスタリングに対してまだ設定されていないインターフェイスの存在）を回避できます。このコマンドを実行すると、クラスタに参加させるスレーブが現在の選定においてマスターとなる可能性をなくすことができます。スレーブのコンフィギュレーションは、マスター ユニットから同期されたコンフィギュレーションによって上書きされます。

クラスタリングをディセーブルにするには、**no enable** コマンドを入力します。

（注）　クラスタリングをディセーブルにした場合は、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、管理インターフェイスだけがアクティブになります。

例

次の例には、スレーブ ユニット unit2 のコンフィギュレーションが含まれています。

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown

interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown

cluster group pod1
    local-unit unit2
    cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    enable as-slave
```

関連項目

- 「ジャンボ フレーム サポートのイネーブル化」（P.9-28）
- 「マスター ユニット選定」（P.8-3）
- 「クラスタからの脱退」（P.8-60）

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。

- 「非アクティブなメンバーになる」（P.8-58）
- 「メンバの非アクティブ化」（P.8-59）
- 「クラスタからの脱退」（P.8-60）
- 「マスター ユニットの変更」（P.8-61）
- 「クラスタ全体でのコマンドの実行」（P.8-62）

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

- コンソール ポートを使用する必要があります。クラスタリングのイネーブルまたはディセーブルを、リモート CLI 接続から行うことはできません。
- 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、**changeto system** コマンドを入力します。

手順

ステップ 1　クラスタ コンフィギュレーション モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 2　クラスタリングをディセーブルにします。

no enable

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.8-60）

メンバの非アクティブ化

任意のユニットから 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、**changeto system** コマンドを入力します。

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。

関連項目

- 「クラスタからの脱退」（P.8-60）

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。さらに、クラスタリングのイネーブルまたはディセーブルを、リモート CLI 接続から行うことはできません。

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、**changeto system** コマンドを入力します。

手順

ステップ 1　新しいユニットをマスター ユニットとして設定します。

```
cluster master unit unit_name
```

例：

```
ciscoasa(config)# cluster master unit asa2
```

メイン クラスタ IP アドレスへの再接続が必要になります。

メンバ名を一覧表示するには、**cluster master 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。

関連項目

- 「非アクティブなメンバーになる」（P.8-58）
- 「クラスタリングの中央集中型機能」（P.8-26）

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。

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：

```
ciscoasa# 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。

```
ciscoasa# 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。

```
ciscoasa# 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 クラスタのモニタリング

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.8-63）
- 「クラスタ全体のパケットのキャプチャ」（P.8-64）
- 「クラスタ リソースのモニタリング」（P.8-64）
- 「クラスタ トラフィックのモニタリング」（P.8-65）
- 「クラスタのルーティングのモニタリング」（P.8-67）
- 「クラスタリングのロギングの設定」（P.8-67）
- 「クラスタのインターフェイスのモニタリング」（P.8-68）
- 「クラスタリングのデバッグ」（P.8-68）

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、次のコマンドを参照してください。

- **show cluster info** [**health**]

  キーワードを指定しないで **show cluster info** コマンドを実行すると、クラスタ内のすべてのメンバのステータスが表示されます。

  show cluster info health コマンドは、インターフェイス、ユニットおよびクラスタ全体の現在の状態を表示します。

  show cluster info コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state SLAVE
      ID        : 0
      Version   : 100.8(0.52)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
```

```
Other members in the cluster:
Unit "D" in state SLAVE
      ID        : 1
      Version   : 100.8(0.52)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state MASTER
      ID        : 2
      Version   : 100.8(0.52)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state SLAVE
      ID        : 3
      Version   : 100.8(0.52)
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
      Last leave: 19:13:36 UTC Sep 23 2011
```

- **show cluster history**

  クラスタの履歴を表示します。

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、次のコマンドを参照してください。

cluster exec capture

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、**cluster exec capture** コマンドを使用してマスター 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

- 「パケットのキャプチャ」（P.38-1）

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、次のコマンドを参照してください。

show cluster {**cpu** | **memory** | **resource**} [*options*]

クラスタ全体の集約データを表示します。使用可能な *options* はデータのタイプによって異なります。

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、次のコマンドを参照してください。

- **show conn [detail]、cluster exec show conn**

  show conn コマンドは、フローがディレクタ、バックアップ、またはフォワーダのどのフローであるかを示します。**cluster exec show conn** コマンドを任意のユニットで使用すると、すべての接続が表示されます。このコマンドの表示からは、1 つのフローのトラフィックがクラスタ内のさまざまな ASA にどのように到達するかがわかります。クラスタのスループットは、ロード バランシングの効率とコンフィギュレーションによって異なります。このコマンドを利用すると、ある接続のトラフィックがクラスタ内をどのように流れるかが簡単にわかります。また、ロード バランサがフローのパフォーマンスにどのように影響を与えるかを理解するのに役立ちます。

  次に、**show conn detail** コマンドの出力例を示します。

```
ciscoasa/ASA2/slave# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
            B - initial SYN from outside, b - TCP state-bypass or nailed,
            C - CTIQBE media, c - cluster centralized,
            D - DNS, d - dump, E - outside back connection, F - outside FIN, f -
inside              FIN,
            G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
            i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
            k - Skinny media, M - SMTP data, m - SIP media, n - GUP
            O - outbound data, P - inside back connection, p - Phone-proxy TFTP
            connection,
            q - SQL*Net data, R - outside acknowledged FIN,
            R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
            s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
            V - VPN orphan, W - WAAS,
            X - inspected by service module,
            x - per session, Y - director stub flow, y - backup stub flow,
            Z - Scansafe redirection, z - forwarding stub flow
ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, , flags c, idle 0s,
uptime 1m21s, timeout 30s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255)
Traffic received at interface outside Locally received: 7544 (93 byte/s) Traffic
received at interface NP Identity Ifc Locally received: 0 (0 byte/s) UDP outside:
10.1.227.1/500 NP Identity Ifc: 10.1.226.1/500, flags -c, idle 1m22s, uptime 1m22s,
timeout 2m0s, bytes 1580, cluster sent/rcvd bytes 0/0, cluster sent/rcvd total bytes
0/0, owners (0,255) Traffic received at interface outside Locally received: 864 (10
byte/s) Traffic received at interface NP Identity Ifc Locally received: 716 (8 byte/s)
```

  接続フローのトラブルシューティングを行うには、最初にすべてのユニットの接続を一覧表示します。それには、任意のユニットで **cluster exec show conn** コマンドを入力します。ディレクタ（Y）、バックアップ（y）、およびフォワーダ（z）のフラグを持つフローを探します。次の例には、3 つのすべての ASA での 172.18.124.187:22 から 192.168.103.131:44727 への SSH 接続が表示されています。ASA1 には z フラグがあり、この接続のフォワーダであることを表しています。ASA3 には Y フラグがあり、この接続のディレクタであることを表しています。ASA2 には特別なフラグはなく、これがオーナーであることを表しています。アウトバウンド方向では、この接続のパケットは ASA2 の内部インターフェイスに入り、外部インターフェイスから出ていきます。インバウンド方向では、この接続のパケットは ASA1 および ASA3 の外部インターフェイスに入り、クラスタ制御リンクを介して ASA2 に転送され、次に ASA2 の内部インターフェイスから出ていきます。

```
ciscoasa/ASA1/master# cluster exec show conn
ASA1(LOCAL):**********************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:**********************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:**********************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0,
flags  Y
```

- **show cluster info** [**conn-distribution** | **packet-distribution** | **loadbalance**]

  show cluster info conn-distribution コマンドと **show cluster info packet-distribution** コマンドは、すべてのクラスタ ユニットへのトラフィック分散を表示します。これらのコマンドは、外部ロード バランサを評価し、調整するのに役立ちます。

  show cluster info loadbalance コマンドは、接続再分散の統計情報を表示します。

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity** | **xlate**} [*options*]

  クラスタ全体の集約データを表示します。使用可能な *options* はデータのタイプによって異なります。

  show cluster access-list コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
```

```
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

使用中の接続の、すべてのユニットでの合計数を表示するには、次のとおりに入力します。

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):**********************************************************
  100 in use, 100 most used

  cl1:*****************************************************************
  100 in use, 100 most used
```

- **show asp cluster counter**

  このコマンドは、データパスのトラブルシューティングに役立ちます。

関連項目

- 接続のロール（11 ～ 22 ページ）

クラスタのルーティングのモニタリング

クラスタのルーティング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 route cluster

debug route cluster

クラスタのルーティング情報を表示します。

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、次のコマンドを参照してください。

logging device-id

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。**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。

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.39-17）

クラスタのインターフェイスのモニタリング

クラスタのインターフェイス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 cluster interface-mode**

  クラスタ インターフェイスのモードを表示します。

- **show port-channel**

  ポートチャネルがスパンドかどうかに関する情報が含まれます。

- **show lacp cluster {system-mac | system-id}**

  cLACP システム ID およびプライオリティを表示します。

- **debug lacp cluster [all | ccp | misc | protocol]**

  cLACP のデバッグ メッセージを表示します。

クラスタリングのデバッグ

クラスタリングのデバッグについては、次のコマンドを参照してください。

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  クラスタリングのデバッグ メッセージを表示します。

- **show cluster info trace**

  show cluster info trace コマンドは、トラブルシューティングのためのデバッグ情報を表示します。

  show cluster info trace コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
MASTER
```

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.8-69）
- 「Firewall on a Stick」（P.8-71）
- 「トラフィックの分離」（P.8-73）
- 「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.8-75）

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.8-69）
- 「Cisco IOS スイッチのコンフィギュレーション」（P.8-70）

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

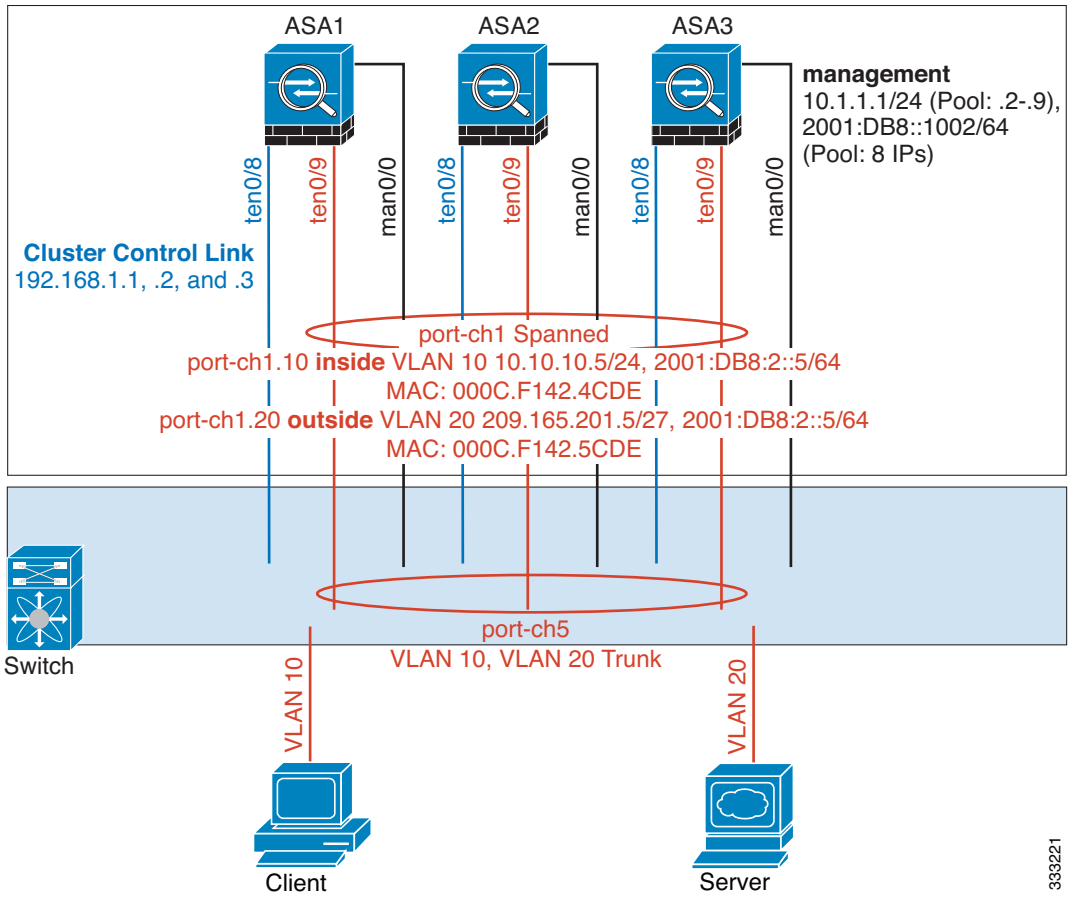
```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

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

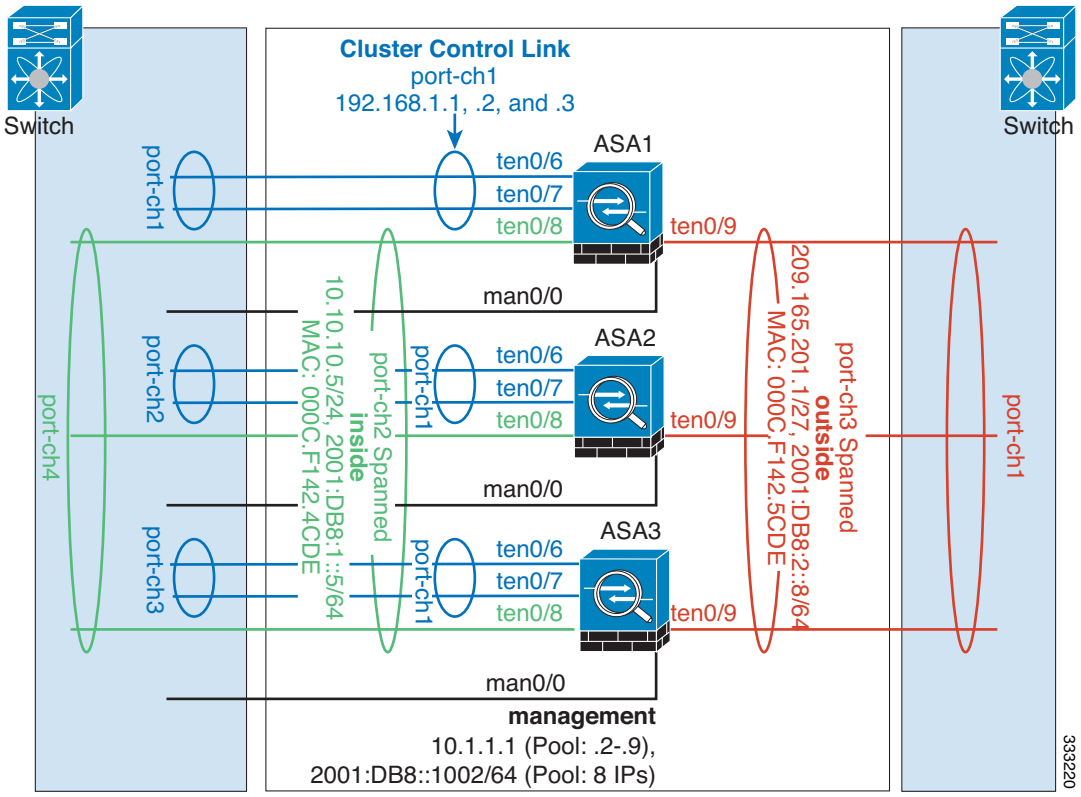
```
interface tengigabitethernet 0/8
    no shutdown
    description CCL

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

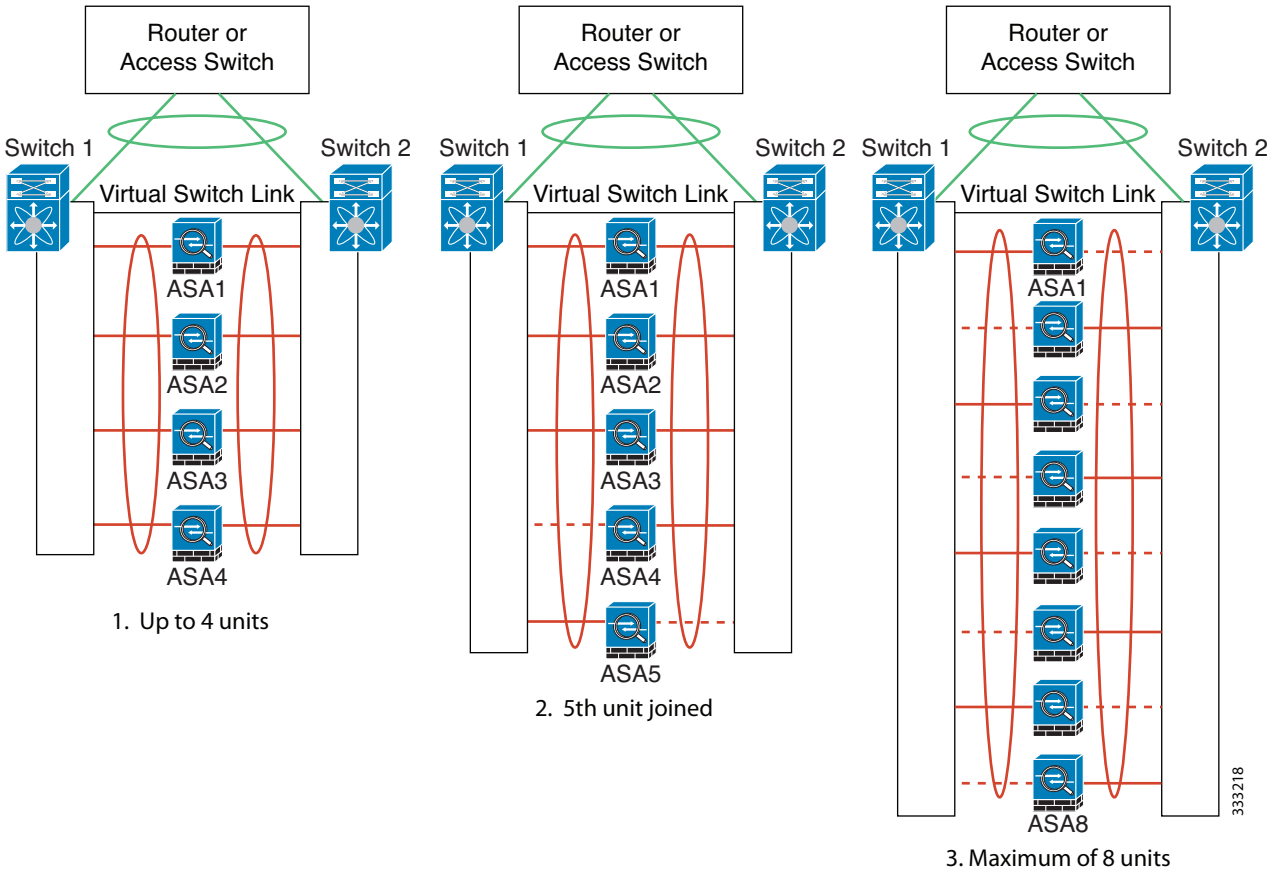
```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

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
```

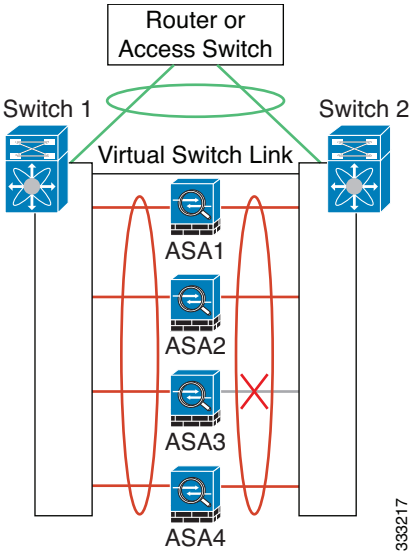
スパンド EtherChannel とバックアップ リンク（従来の 8 アクティブ /8 スタンバイ）

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。

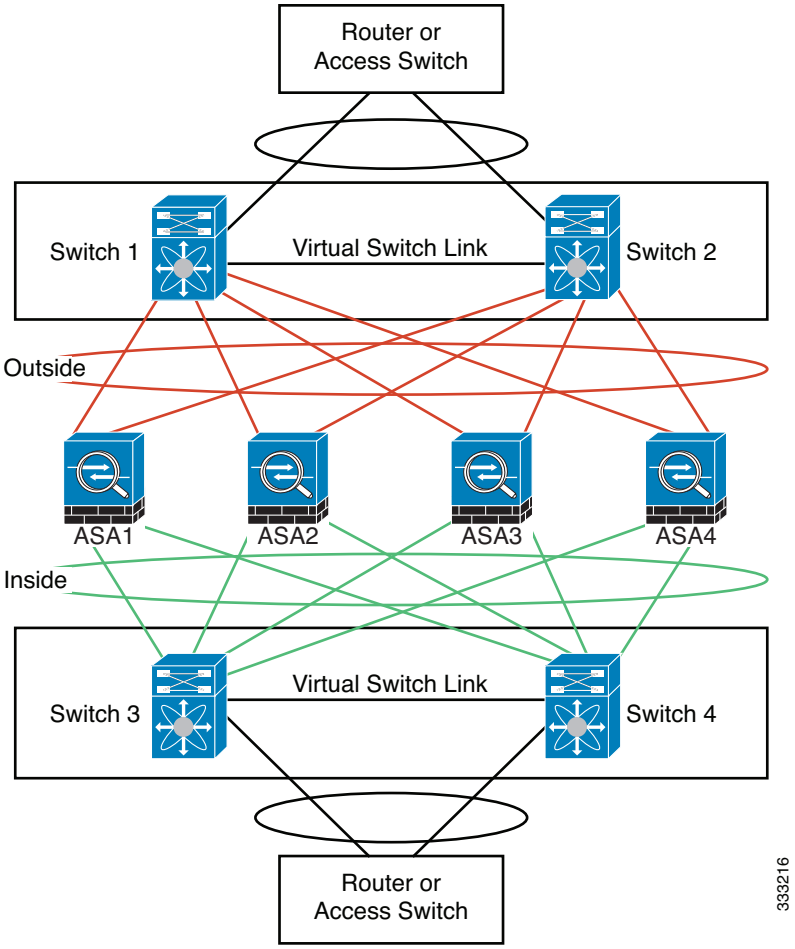


原則として、初めにチャネル内のアクティブ ポート数を最大化し、そのうえで、アクティブなプライマリ ポートとアクティブなセカンダリ ポートの数のバランスを保ちます。5 番目のユニットがクラスタに参加したときは、トラフィックがすべてのユニットに均等には分散されないことに注意してください。

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。 **channel-group**、**clacp system-mac**、**clear cluster info**、**clear configure cluster**、**cluster exec**、**cluster group**、**cluster interface-mode**、**cluster-interface**、**conn-rebalance**、**console-replicate**、**cluster master unit**、**cluster remove unit**、**debug cluster**、**debug lacp cluster**、**enable**（クラスタ グループ）、**health-check**、**ip address**、**ipv6 address**、**key**（クラスタ グループ）、**local-unit**、**mac-address**（インターフェイス）、**mac-address pool**、**mtu cluster**、**port-channel span-cluster**、**priority**（クラスタ グループ）、**prompt cluster-unit**、**show asp cluster counter**、**show asp table cluster chash-table**、**show cluster**、**show cluster info**、**show cluster user-identity**、**show lacp cluster**、**show running-config cluster** の各コマンドが導入または変更されました。
クラスタリングの ASA 5500-X のサポート	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、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、基本ライセンスにおいてデフォルトでイネーブルになります。ASA 5512-X の場合は、Security Plus ライセンスが必要です。 変更されたコマンドはありません。
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 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。 **health-check** [**vss-enabled**] コマンドが変更されました。

機能名	プラットフォーム リリース	機能情報
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。 変更されたコマンドはありません。
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 サイト間クラスタリングはサポートされません。 変更されたコマンドはありません。
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。 **clacp static-port-priority** コマンドが導入されました。
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。 **clacp static-port-priority** コマンドが導入されました。

機能名	プラットフォームリリース	機能情報
ASA 5585-X の 16 個のクラスタ メンバのサポート	9.2(1)	ASA 5585-X は、16 ユニットのクラスタをサポートするようになりました。 変更されたコマンドはありません。
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。 次の新しいコマンドが導入されました。**bgp router-id clusterpool**

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。コンテキストから実行スペースに変更するには、**changeto system** コマンドを入力します。。

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 8 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」（P.9-2）
- 「ASA 5512-X 以降のインターフェイスのライセンス要件」（P.9-10）
- 「ガイドラインと制限事項」（P.9-12）
- 「デフォルト設定」（P.9-14）
- 「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.9-15）
- 「インターフェイスのモニタリング」（P.9-39）
- 「ASA 5512-X 以降のインターフェイスの設定例」（P.9-39）
- 「次の作業」（P.9-41）
- 「ASA 5512-X 以降のインターフェイスの機能履歴」（P.9-41）

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」（P.9-2）
- 「トランスペアレント モードのインターフェイス」（P.9-2）
- 「管理インターフェイス」（P.9-2）
- 「冗長インターフェイス」（P.9-5）
- 「EtherChannel」（P.9-5）
- 「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.9-8）

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.12-2）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」（P.9-3）
- 「Management Slot/Portインターフェイス」（P.9-3）
- 「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」（P.9-3）
- 「トランスペアレント モードの管理インターフェイス」（P.9-4）
- 「冗長管理インターフェイスの非サポート」（P.9-4）
- 「ASA 5512-X ～ ASA 5555-X の Management 0/0 インターフェイス」（P.9-4）

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で使用できる場合）

第 35 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 9-1 に、モデルごとの管理インターフェイスを示します。

表 9-1　　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**	×	×	×	×	×
ASA 5515-X	**Yes**	×	×	×	×	×
ASA 5525-X	**Yes**	×	×	×	×	×
ASA 5545-X	**Yes**	×	×	×	×	×
ASA 5555-X	**Yes**	×	×	×	×	×
ASA 5585-X	**Yes**	**Yes**	**Yes**[3]	**Yes**[3]	**Yes**	**Yes**
ASASM	×	×	×	×	該当なし	該当なし
ASAv	**Yes**	×	×	×	×	×

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 コンフィギュレーション」（P.2-14）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（**management-only** コマンド）。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（**management-only** コマンドを参照）。

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の非サポート

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 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 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、TCP MSS の設定」（P.11-10）または「マルチ コンテキストの設定」（P.6-16）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.9-5）
- 「別のデバイスの EtherChannel への接続」（P.9-6）
- 「リンク集約制御プロトコル」（P.9-7）
- 「ロード バランシング」（P.9-7）
- 「EtherChannel MAC アドレス」（P.9-7）

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 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。

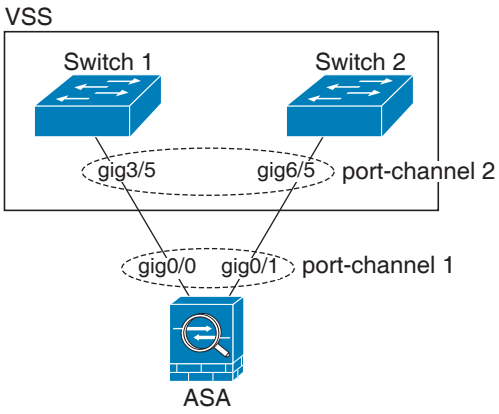
EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。インターフェイスは、送信元または宛先 MAC アドレス、IP アドレス、TCP および UDP ポート番号、および VLAN 番号に基づいて、専用のハッシュ アルゴリズムを使用して選択されます。

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。

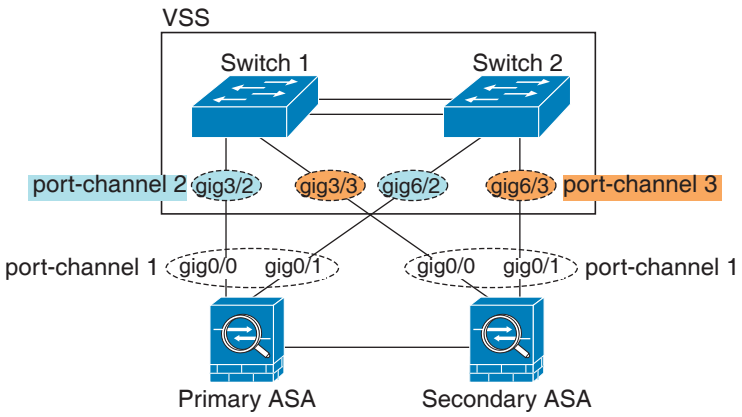
スイッチが仮想スイッチング システム（VSS）または 仮想ポート チャネル（vPC）の一部である場合、同じ EtherChannel 内の ASA インターフェイスを VSS/vPC 内の個別のスイッチに接続できます。個別のスイッチは単一のスイッチのように動作するため、スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです（図 9-1 を参照）。

図 9-1　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 9-1 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 9-2　アクティブ/スタンバイ フェールオーバーと VSS/vPC



リンク集約制御プロトコル

リンク集約制御プロトコル（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 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.9-24）を参照してください）。生成されたハッシュは、モジュロ演算によってアクティブ リンクの数で割られます。得られた剰余によってフローを保持するインターフェイスが決定されます。*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 の値が提供されます。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。障害はレイヤ 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」（P.9-8）
- 「デフォルト MTU」（P.9-9）
- 「パス MTU ディスカバリ」（P.9-9）
- 「MTU とジャンボ フレームの設定」（P.9-9）
- 「TCP 最大セグメント サイズの概要」（P.9-9）
- 「デフォルト TCP MSS」（P.9-9）
- 「VPN および非 VPN トラフィックの TCP MSS の設定」（P.9-10）
- 「例」（P.9-10）

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.9-9））。

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.9-28）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 の定義に従う）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、TCP MSS の設定」（P.11-10）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.9-28）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 フレームに対する対応：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、TCP MSS の設定」（P.11-10）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。

例

下記の例では、ジャンボ フレームをイネーブルにし、すべてのインターフェイスの MTU を増加し、非 VPN トラフィックの TCP MSS をディセーブルにします（TCP MSS を 0 に設定、すなわち無制限とすることによって行います）。

```
jumbo frame-reservation
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 0
```

下記の例では、ジャンボ フレームをイネーブルにし、すべてのインターフェイスの MTU を増加し、VPN トラフィックの TCP MSS を 9078 に変更します（MTU から 120 を差し引きます）。

```
jumbo frame-reservation
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 9078
```

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

モデル	ライセンス要件
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。次に例を示します。

```
interface gigabitethernet 0/0.100
  vlan 100
```

すべてのタイプのインターフェイスが、インターフェイス（VLAN、物理、冗長、ブリッジ グループ、EtherChannel インターフェイスなど）の最大数に含まれます。設定で定義されている各 **interface** コマンドは、この制限に対してカウントされます。たとえば、GigabitEthernet 0/0 インターフェイスがポートチャネル 1 の一部として定義されている場合でも、次のインターフェイスは両方ともカウントされます。

interface gigabitethernet 0/0
および
interface port-channel 1

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.9-15）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 11 章「ルーテッド モードのインターフェイス」または第 12 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。それには、**monitor-interface** コマンドを使用します。必ず、論理冗長インターフェイス名を指定してください。アクティブなメンバ 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 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

- 冗長または EtherChannel 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ときは、そのリンクをクラスタ内のすべてのユニットで事前に設定する必要があります。プライマリ装置だけで設定してもメンバ ユニットに複製されることはありません。*複製にはクラスタ制御リンクそのものが必要である*からです。
- スパンド EtherChannel を設定するには、「スパンド EtherChannel の設定」（P.8-45）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.8-43）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.9-12）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.9-13）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 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.9-12）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.9-13）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 コンフィギュレーション」（P.2-14）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、2 種類のコネクター、銅線 RJ-45 とファイバ SFP を含みます。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」（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.9-16）
- 「冗長インターフェイスの設定」（P.9-19）
- 「EtherChannel の設定」（P.9-21）
- 「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.9-26）
- 「ジャンボ フレーム サポートのイネーブル化」（P.9-28）
- 「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.9-29）

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、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.9-29）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。コンテキストからシステム実行スペースに変更するには **changeto system** コマンドを入力します。

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.9-16）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.9-19）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.9-21）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.9-26）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.9-28）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 6 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.6-21）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.6-26）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、TCP MSS の設定」（P.11-10）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 11 章「ルーテッド モードのインターフェイス」または第 12 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。コンテキストからシステム実行スペースに変更するには **changeto system** コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	**interface** *physical_interface* **例：** `ciscoasa(config)# interface gigabitethernet 0/0`	設定するインターフェイスを指定します。 *physical_interface* ID には、タイプ、スロット、およびポート番号を *type*[*slot*/]*port* という形式で指定します。 物理インターフェイスのタイプには、次のものがあります。 • **gigabitethernet** • **tengigabitethernet** • **management** タイプに続けて*スロット* / *ポート*を入力します。たとえば、**gigabitethernet0/1** というようになります。タイプとスロット / ポートの間のスペースは任意です。
ステップ 2	（オプション） **media-type sfp** **例：** `ciscoasa(config-if)# media-type sfp`	使用しているモデルで利用できる場合には、メディア タイプを SFP に設定します。デフォルトの RJ-45 に戻すには、**media-type rj45** コマンドを入力します。
ステップ 3	（オプション） **speed** {**auto** | **10** | **100** | **1000** | **nonegotiate**} **例：** `ciscoasa(config-if)# speed 100`	速度を設定します。 RJ-45 インターフェイスのデフォルト設定は **auto** です。 SFP インターフェイスのデフォルト設定は **no speed nonegotiate** です。この設定では、速度が最大速度に設定され、フロー制御パラメータとリモート障害情報のリンク ネゴシエーションがイネーブルになります。**nonegotiate** キーワードは、SFP インターフェイスで使用できる唯一のキーワードです。**speed nonegotiate** コマンドは、リンク ネゴシエーションをディセーブルにします。
ステップ 4	（オプション） **duplex** {**auto** | **full** | **half**} **例：** `ciscoasa(config-if)# duplex full`	RJ-45 インターフェイスの二重通信を設定します。**auto** 設定がデフォルトです。 **（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。

	コマンド	目的
ステップ 5	（オプション） **flowcontrol send on** [*low_water high_water pause_time*] [**noconfirm**] **例：** `ciscoasa(config-if)# flowcontrol send on 95 200 10000`	GigabitEthernet インターフェイスと TenGigabitEthernet 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。 このコマンドを使用すると、次の警告が表示されます。 `Changing flow-control parameters will reset the interface.Packets may be lost during the reset. Proceed with flow-control changes?` プロンプトを表示しないでパラメータを変更するには、**noconfirm** キーワードを使用します。 **（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	**no shutdown** **例：** `ciscoasa(config-if)# no shutdown`	インターフェイスをイネーブルにします。インターフェイスをディセーブルにするには、**shutdown** コマンドを入力します。**shutdown** コマンドを入力すると、すべてのサブインターフェイスもシャットダウンします。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、そのインターフェイスを共有しているすべてのコンテキストでシャットダウンします。

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.9-19）を参照してください。
- EtherChannel を設定します。「EtherChannel の設定」（P.9-21）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.9-26）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.9-28）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.6-16）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 11 章「ルーテッド モードのインターフェイス」または第 12 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.9-19）
- 「アクティブ インターフェイスの変更」（P.9-21）

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。

ガイドラインと制限事項

- 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 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.9-13）も参照してください。

前提条件

- 両方のメンバ 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、**no nameif** コマンドを使用して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。コンテキストからシステム実行スペースに変更するには **changeto system** コマンドを入力します。

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

	コマンド	目的
ステップ 1	**interface redundant** *number* **例：** `ciscoasa(config)# interface redundant 1`	論理冗長インターフェイスを追加します。*number* 引数は、1 ～ 8 の整数です。 **（注）**　冗長インターフェイスの名前などの論理パラメータを設定する前に、少なくとも 1 つのメンバー インターフェイスを冗長インターフェイスに追加する必要があります。
ステップ 2	**member-interface** *physical_interface* **例：** `ciscoasa(config-if)# member-interface gigabitethernet 0/0`	最初のメンバ インターフェイスを冗長インターフェイスに追加します。 物理インターフェイス ID の説明については、「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.9-16）を参照してください。 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。 インターフェイスを追加すると、インターフェイスのコンフィギュレーション（IP アドレスなど）はすべて削除されます。
ステップ 3	**member-interface** *physical_interface* **例：** `ciscoasa(config-if)# member-interface gigabitethernet 0/1`	2 番目のメンバ インターフェイスを冗長インターフェイスに追加します。 2 つ目のインターフェイスの物理タイプは、必ず最初のインターフェイスと同じにしてください。 メンバー インターフェイスを削除するには、**no member-interface** *physical_interface* コマンドを入力します。冗長インターフェイスから両方のメンバ インターフェイスは削除できません。冗長インターフェイスには、少なくとも 1 つのメンバ インターフェイスが必要です。

例

次の例では、2 つの冗長インターフェイスを作成します。

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

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.9-26）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.9-28）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.6-16）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 11 章「ルーテッド モードのインターフェイス」または第 12 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。

```
ciscoasa# show interface redundantnumber detail | grep Member
```

次に例を示します。

```
ciscoasa# 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。

```
ciscoasa# 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 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.9-22）
- 「EtherChannel のカスタマイズ」（P.9-24）

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。

ガイドラインと制限事項

- 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 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.8-45）を参照してください。
- 「EtherChannel のガイドライン」（P.9-13）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、**no nameif** コマンドを使用して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。コンテキストからシステム実行スペースに変更するには **changeto system** コマンドを入力します。

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

	コマンド	目的
ステップ 1	**interface** *physical_interface* **例：** `ciscoasa(config)# interface gigabitethernet 0/0`	チャネル グループに追加するインターフェイスを指定します。*physical_interface* ID では、タイプ、スロット、ポート番号を *type*[*slot*/]*port* の形式で指定します。チャネル グループのこの最初のインターフェイスによって、グループ内の他のすべてのインターフェイスのタイプと速度が決まります。 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。

	コマンド	目的
ステップ 2	**channel-group** *channel_id* **mode** {**active** | **passive** | **on**} **例：** `ciscoasa(config-if)# channel-group 1 mode active`	1 ～ 48 の *channel_id* を指定して、この物理インターフェイスを EtherChannel に割り当てます。このチャネル ID のポートチャネル インターフェイスがコンフィギュレーションにまだ存在しない場合、ポートチャネル インターフェイスが作成されます。 **interface port-channel** *channel_id* **active** モード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、「リンク集約制御プロトコル」（P.9-7）を参照してください。
ステップ 3	（オプション） **lacp port-priority** *number* **例：** `ciscoasa(config-if)# lacp port-priority 12345`	チャネル グループ内の物理インターフェイスのプライオリティを、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 **lacp port-priority** 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。「EtherChannel のカスタマイズ」（P.9-24）の **lacp system-priority** コマンドを参照してください。
ステップ 4	チャネル グループに追加するインターフェイスごとに、ステップ 1 ～ 3 を繰り返します。	チャネル グループの各インターフェイスのタイプと速度が同一であることが必要です。半二重はサポートされません。一致しないインターフェイスを追加すると、一時停止状態になります。

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.9-24）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.9-26）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.6-16）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 11 章「ルーテッド モードのインターフェイス」または第 12 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

	コマンド	目的
ステップ 1	**interface port-channel** *channel_id* **例：** `ciscoasa(config)# interface port-channel 1`	ポートチャネル 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、チャネル グループにインターフェイスを追加したときに自動的に作成されたものです。まだインターフェイスを追加していない場合は、このコマンドを実行するとポートチャネル インターフェイスが作成されます。 **（注）** 少なくとも 1 つのメンバ インターフェイスをポートチャネル インターフェイスに追加してからでなければ、インターフェイスの論理パラメータ（名前など）は設定できません。
ステップ 2	**lacp max-bundle** *number* **例：** `ciscoasa(config-if)# lacp max-bundle 6`	このチャネル グループ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 の範囲内で指定します。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。
ステップ 3	**port-channel min-bundle** *number* **例：** `ciscoasa(config-if)# port-channel min-bundle 2`	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブ インターフェイスの最小数を 1 ～ 16 の範囲で指定します。デフォルトは 1 です。チャネル グループ内のアクティブ インターフェイス数がこの値よりも小さい場合、ポートチャネル インターフェイスがダウンし、デバイスレベル フェールオーバーが開始されます。

	コマンド	目的
ステップ 4	**port-channel load-balance** {**dst-ip** | **dst-ip-port** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-ip-port** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-ip-port** | **src-mac** | **src-port** | **vlan-dst-ip** | **vlan-dst-ip-port** | **vlan-only** | **vlan-src-dst-ip** | **vlan-src-dst-ip-port** | **vlan-src-ip** | **vlan-src-ip-port**} **例：** `ciscoasa(config-if)# port-channel load-balance src-dst-mac`	ロードバランシング アルゴリズムを設定します。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（**src-dst-ip**）に従ってインターフェイスでのパケットの負荷を分散します。パケットの分類の基準となるプロパティを変更する場合は、このコマンドを使用します。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.9-7）を参照してください。
ステップ 5	**lacp system-priority** *number* **例：** `ciscoasa(config)# lacp system-priority 12345`	LACP システム 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。このコマンドは、ASA に対してグローバルです。 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。EtherChannel 内でのインターフェイス プライオリティについては、「EtherChannel へのインターフェイスの追加」（P.9-22）の **lacp port-priority** コマンドを参照してください。
ステップ 6	（オプション） ポートチャネル インターフェイスのイーサネット プロパティを設定します。この設定は、個別インターフェイスに対して設定されたプロパティよりも優先されます。	イーサネットのコマンドについては、「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.9-16）を参照してください。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。

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.9-26）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.9-28）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.6-16）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 11 章「ルーテッド モードのインターフェイス」または第 12 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。

ガイドラインと制限事項

- 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.9-10）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、**nameif** コマンドを除外してください。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 **nameif** コマンドを設定できます。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 11 章「ルーテッド モードのインターフェイス」または第 12 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。コンテキストからシステム実行スペースに変更するには **changeto system** コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ1	**interface** {*physical_interface* | **redundant** *number* | **port-channel** *number*}.*subinterface* **例：** `ciscoasa(config)# interface gigabitethernet 0/1.100`	新しいサブインターフェイスを指定します。物理インターフェイス ID 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.9-16）の説明を参照してください。 **redundant** *number* 引数には、冗長インターフェイス ID（**redundant 1** など）を指定します。 **port-channel** *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。 *subinterface* ID は、1 ～ 4294967293 の整数です。
ステップ2	**vlan** *vlan_id* **例：** `ciscoasa(config-subif)# vlan 101`	サブインターフェイスの VLAN アドレスを指定します。*vlan_id* は、1 ～ 4094 の整数です。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。 1 つの VLAN は 1 つのサブインターフェイスにだけ割り当てることができます。同じ VLAN を複数のサブインターフェイスに割り当てることはできません。VLAN を物理インターフェイスに割り当てることはできません。トラフィックがサブインターフェイスを通過するには、各サブインターフェイスに VLAN ID が必要となります。VLAN ID を変更するために **no** オプションで古い VLAN ID を削除する必要はありません。別の VLAN ID を指定して **vlan** コマンドを入力すると、ASA によって古い ID が変更されます。

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.9-28）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.6-16）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 11 章「ルーテッド モードのインターフェイス」または第 12 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.9-8）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、**mtu** コマンドを使用してデフォルト値の 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、TCP MSS の設定」（P.11-10）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（**sysopt connection tcpmss 0** コマンドを使用）、または「MAC アドレス、MTU、TCP MSS の設定」（P.11-10）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

コマンド	目的
jumbo-frame reservation **例：** `ciscoasa(config)# jumbo-frame reservation`	ジャンボ フレーム サポートをイネーブルにします。ジャンボ フレームをディセーブルにするには、このコマンドの **no** 形式を使用します。

例

次に、ジャンボ フレームの予約をイネーブルにし、コンフィギュレーションを保存して ASA をリロードする例を示します。

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted.Command accepted.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload?[confirm] Y
```

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.6-16）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 11 章「ルーテッド モードのインターフェイス」または第 12 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.9-19）と「EtherChannel の設定」（P.9-21）を参照してください。

- 「手順の詳細（シングル モード）」（P.9-29）
- 「手順の詳細（マルチ モード）」（P.9-35）

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する場合は、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する場合、**no failover** コマンドを入力して、フェールオーバーをディセーブルにします。

ステップ 3　**more system:running-config** コマンドを入力して、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。

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 コンフィグ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.9-21）を参照してください。

ステップ 8　ASA の CLI プロンプトで、接続（コンソールまたはリモート）に応じて次の手順を実行します。

- コンソール接続の場合
  a. 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クリップボードにコピーします。
  b. 実行コンフィギュレーションをクリアするために、次のとおりに入力します。

     ```
     ciscoasa(config)# clear configure all
     ```

     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。
  c. 新しいコンフィギュレーションをプロンプトで貼り付けます。

     ASA を通過するトラフィックが再開します。
- リモート接続：
  a. 新しいコンフィギュレーションを TFTP または FTP サーバに保存します。ASA のスタートアップ コンフィギュレーションにコピーできるようにするためです。たとえば、PC 上で TFTP サーバまたは FTP サーバを実行できます。
  b. 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クリアします。

     ```
     ciscoasa(config)# write erase
     ```

  c. 新しい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するために、次のとおりに入力します。

     ```
     ciscoasa(config)# copy url startup-config
     ```

     「ASA へのファイルのコピー」（P.36-17）を参照してください。
  d. **reload** コマンドを使用して ASA をリロードします。実行コンフィギュレーションを保存しないでください。

ステップ 9　**failover** コマンドを入力して、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する場合は、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する場合、**no failover** コマンドを入力して、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、**more system:running-config** コマンドを入力し、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ります。

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.36-27）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.9-19）または「EtherChannel の設定」（P.9-21）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.6-21）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、コンテキストが FTP サーバにある場合は、FTP を使用して既存のファイル（必要に応じてバックアップを作成します）に上書きコピーします。コンテキストがフラッシュ メモリ内にある場合、**copy** コマンドを使用し TFTP サーバまたは FTP サーバを PC 上で実行するか、セキュア コピーを使用します。「ASA へのファイルのコピー」（P.36-17）を参照してください。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　ASA のシステム CLI プロンプトで、接続（コンソールまたはリモート）に応じて次の手順を実行します。

- コンソール接続の場合
  - **a.** 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。
  - **b.** 実行コンフィギュレーション（システムおよびコンテキストの両方）をクリアするために、次のとおりに入力します。

    ```
    ciscoasa(config)# clear configure all
    ```

    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。

c. 新しいシステム コンフィギュレーションをプロンプトで貼り付けます。

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。

- リモート接続：

a. 新しいシステム コンフィギュレーションを TFTP または FTP サーバに保存します。ASA のスタートアップ コンフィギュレーションにコピーできるようにするためです。たとえば、PC 上で TFTP サーバまたは FTP サーバを実行できます。

b. 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クリアします。

```
ciscoasa(config)# write erase
```

c. 新しいシステム 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するために、次のとおりに入力します。

```
ciscoasa(config)# copy url startup-config
```

「ASA へのファイルのコピー」（P.36-17）を参照してください。

d. **reload** コマンドを使用して ASA をリロードします。実行コンフィギュレーションを保存しないでください。

ステップ 10　**failover** コマンドを入力して、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

コマンド	目的
show interface	インターフェイス統計情報を表示します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。
show lacp {[*channel_group_number*] {**counters** | **internal** | **neighbor**} | **sys-id**}	EtherChannel の場合は、LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。
show port-channel [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]	EtherChannel の場合は、EtherChannel 情報が、詳細な 1 行サマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel *channel_group_number* **load-balance** [**hash-result** {**ip** | **ipv6** | **l4port** | **mac** | **mixed** | **vlan-only**} *parameters*]	EtherChannel の場合は、ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバ インターフェイスとともに表示されます。

ASA 5512-X 以降のインターフェイスの設定例

- 「物理インターフェイス パラメータの例」（P.9-40）
- 「サブインターフェイス パラメータの例」（P.9-40）
- 「マルチ コンテキスト モードの例」（P.9-40）
- 「EtherChannel の例」（P.9-40）

物理インターフェイス パラメータの例

次に、シングル モードで物理インターフェイスのパラメータを設定する例を示します。

```
interface gigabitethernet 0/1
    speed 1000
    duplex full
    no shutdown
```

サブインターフェイス パラメータの例

次に、シングル モードでサブインターフェイスのパラメータを設定する例を示します。

```
interface gigabitethernet 0/1.1
    vlan 101
    no shutdown
```

マルチ コンテキスト モードの例

次に、システム コンフィギュレーション用にマルチ コンテキスト モードでインターフェイス パラメータを設定し、GigabitEthernet 0/1.1 サブインターフェイスをコンテキスト A に割り当てる例を示します。

```
interface gigabitethernet 0/1
    speed 1000
    duplex full
    no shutdown
interface gigabitethernet 0/1.1
    vlan 101
context contextA
    allocate-interface gigabitethernet 0/1.1
```

EtherChannel の例

次の例では、3 つのインターフェイスを EtherChannel の一部として設定します。また、システム プライオリティをより高く設定するとともに、GigabitEthernet 0/2 のプライオリティを他のインターフェイスよりも高く設定します。これは、8 個を超えるインターフェイスが EtherChannel に割り当てられた場合に備えるためです。

```
lacp system-priority 1234
interface GigabitEthernet0/0
    channel-group 1 mode active
interface GigabitEthernet0/1
    channel-group 1 mode active
interface GigabitEthernet0/2
    lacp port-priority 1234
    channel-group 1 mode passive
interface Port-channel1
    lacp max-bundle 4
    port-channel min-bundle 2
    port-channel load-balance dst-ip
```

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 6 章「マルチ コンテキスト モード」を参照してください。
  b. 第 11 章「ルーテッド モードのインターフェイス」または第 12 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 11 章「ルーテッド モードのインターフェイス」または第 12 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 9-2 に、この機能のリリース履歴を示します。

表 9-2　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。**speed** コマンドを使用してインターフェイスの速度を変更します。また、**show interface** コマンドを使用して各インターフェイスの現在の設定速度を確認します。

表 9-2　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
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。
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。 **jumbo-frame reservation** コマンドが導入されました。
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。
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。 **flowcontrol** コマンドが導入されました。
1 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 1 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。 **flowcontrol** コマンドが変更されました。

表 9-2　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。 **channel-group**、**lacp port-priority**、**interface port-channel**、**lacp max-bundle**、**port-channel min-bundle**、**port-channel load-balance**、**lacp system-priority**、**clear lacp counters**、**show lacp**、**show port-channel** の各コマンドが導入されました。 **（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（**lacp max-bundle** コマンド）。 次のコマンドが変更されました。**lacp max-bundle** および **port-channel min-bundle**。

CHAPTER 10

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」（P.10-1）
- 「ASAv インターフェイスのライセンス要件」（P.10-7）
- 「ガイドラインと制限事項」（P.10-8）
- 「デフォルト設定」（P.10-8）
- 「インターフェイス コンフィギュレーションの開始（ASAv）」（P.10-9）
- 「インターフェイスのモニタリング」（P.10-17）
- 「ASAv インターフェイスの設定例」（P.10-17）
- 「次の作業」（P.10-17）
- 「ASAv インターフェイスの機能履歴」（P.10-17）

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」（P.10-2）
- 「トランスペアレント モードのインターフェイス」（P.10-3）
- 「管理インターフェイス」（P.10-3）
- 「冗長インターフェイス」（P.10-4）
- 「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.10-5）

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。各 ASAv インターフェイスには仮想 NIC（vNIC）に該当します。

- 「ASAv インターフェイス」（P.10-2）
- 「サポートされる vNIC」（P.10-2）
- 「VMware における ASAv インターフェイスと vNIC の対応」（P.10-2）

ASAv インターフェイス

ASAv には、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	メモ
	VMware	KVM		
VMXNET3	**Yes**	×	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。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.12-2）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」（P.10-3）
- 「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」（P.10-3）
- 「トランスペアレント モードの管理インターフェイス」（P.10-4）
- 「通過トラフィックのサポートなし」（P.10-4）

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 35 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（**management-only** コマンドを参照）。

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 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 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、TCP MSS の設定」（P.11-10）または「マルチ コンテキストの設定」（P.6-16）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」（P.10-5）
- 「デフォルト MTU」（P.10-5）
- 「パス MTU ディスカバリ」（P.10-5）
- 「MTU とジャンボ フレームの設定」（P.10-6）
- 「TCP 最大セグメント サイズの概要」（P.10-6）
- 「デフォルト TCP MSS」（P.10-6）
- 「VPN および非 VPN トラフィックの TCP MSS の設定」（P.10-6）
- 「例」（P.10-7）

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.10-6）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.10-15）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 の定義に従う）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、TCP MSS の設定」（P.11-10）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.10-15）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 フレームに対する対応：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、TCP MSS の設定」（P.11-10）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。

例

下記の例では、ジャンボ フレームをイネーブルにし、すべてのインターフェイスの MTU を増加し、非 VPN トラフィックの TCP MSS をディセーブルにします（TCP MSS を 0 に設定、すなわち無制限とすることによって行います）。

```
jumbo frame-reservation
mtu inside 9000
mtu outside 9000
sysopt connection tcpmss 0
```

下記の例では、ジャンボ フレームをイネーブルにし、すべてのインターフェイスの MTU を増加し、VPN トラフィックの TCP MSS を 8880 に変更します（MTU から 120 を差し引きます）。

```
jumbo frame-reservation
mtu inside 9000
mtu outside 9000
sysopt connection tcpmss 8880
```

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 X 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 X 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。次に例を示します。

interface gigabitethernet 0/0.100
**　VLAN 100**

すべてのタイプのインターフェイスが、インターフェイス（VLAN、物理、冗長、ブリッジ グループなどのインターフェイス）の最大数に含まれます。設定で定義されている各 **interface** コマンドは、この制限に対してカウントされます。

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。

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。**monitor-interface** コマンドで、必ず論理冗長インターフェイス名を参照してください。アクティブなメンバ 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.10-8）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 コンフィギュレーション」（P.2-14）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」（P.10-9）
- 「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.10-10）
- 「冗長インターフェイスの設定」（P.10-12）
- 「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.10-14）
- 「ジャンボ フレーム サポートのイネーブル化」（P.10-15）

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.10-10）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.10-12）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.10-14）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.10-15）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

	コマンド	目的
ステップ 1	**interface** *physical_interface* **例：** `ciscoasa(config)# interface gigabitethernet 0/0`	設定するインターフェイスを指定します。 *physical_interface* ID には、タイプ、スロット、およびポート番号を *type*[*slot*/]*port* という形式で指定します。 物理インターフェイスのタイプには、次のものがあります。 • **gigabitethernet** • **管理** タイプに続けて*スロット / ポート*を入力します。たとえば、**gigabitethernet0/1** というようになります。タイプとスロット / ポートの間のスペースは任意です。
ステップ 2	（オプション） **speed** {**auto** | **10** | **100** | **1000**} **例：** `ciscoasa(config-if)# speed 100`	速度を設定します。**auto** 設定がデフォルトです。
ステップ 3	（オプション） **duplex** {**auto** | **full** | **half**} **例：** `ciscoasa(config-if)# duplex full`	二重通信を設定します。**auto** 設定がデフォルトです。

	コマンド	目的
ステップ 4	（オプション） **flowcontrol send on** [*low_water high_water pause_time*] [**noconfirm**] **例：** `ciscoasa(config-if)# flowcontrol send on 95 200 10000`	フロー制御のポーズ（XOFF）フレームのイネーブル化 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。 このコマンドを使用すると、次の警告が表示されます。 `Changing flow-control parameters will reset the interface.Packets may be lost during the reset. Proceed with flow-control changes?` プロンプトを表示しないでパラメータを変更するには、**noconfirm** キーワードを使用します。 **（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 5	**no shutdown** **例：** `ciscoasa(config-if)# no shutdown`	インターフェイスをイネーブルにします。インターフェイスをディセーブルにするには、**shutdown** コマンドを入力します。**shutdown** コマンドを入力すると、すべてのサブインターフェイスもシャットダウンします。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、そのインターフェイスを共有しているすべてのコンテキストでシャットダウンします。

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.10-12）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.10-14）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.10-15）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 11 章「ルーテッド モードのインターフェイス」または第 12 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.10-12）
- 「アクティブ インターフェイスの変更」（P.10-14）

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。

ガイドラインと制限事項

- 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 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.10-8）も参照してください。

前提条件

- 両方のメンバ 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、**no nameif** コマンドを使用して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

	コマンド	目的
ステップ 1	**interface redundant** *number* **例：** `ciscoasa(config)# interface redundant 1`	論理冗長インターフェイスを追加します。*number* 引数は、1 ～ 8 の整数です。 **（注）** 冗長インターフェイスの名前などの論理パラメータを設定する前に、少なくとも 1 つのメンバー インターフェイスを冗長インターフェイスに追加する必要があります。
ステップ 2	**member-interface** *physical_interface* **例：** `ciscoasa(config-if)# member-interface gigabitethernet 0/0`	最初のメンバ インターフェイスを冗長インターフェイスに追加します。インターフェイスを追加すると、インターフェイスのコンフィギュレーション（IP アドレスなど）はすべて削除されます。
ステップ 3	**member-interface** *physical_interface* **例：** `ciscoasa(config-if)# member-interface gigabitethernet 0/1`	2 番目のメンバ インターフェイスを冗長インターフェイスに追加します。 2 つ目のインターフェイスの物理タイプは、必ず最初のインターフェイスと同じにしてください。 メンバー インターフェイスを削除するには、**no member-interface** *physical_interface* コマンドを入力します。冗長インターフェイスから両方のメンバ インターフェイスは削除できません。冗長インターフェイスには、少なくとも 1 つのメンバ インターフェイスが必要です。

例

次の例では、2 つの冗長インターフェイスを作成します。

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

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.10-14）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.10-15）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 11 章「ルーテッド モードのインターフェイス」または第 12 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。

```
ciscoasa# show interface redundantnumber detail | grep Member
```

次に例を示します。

```
ciscoasa# 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。

```
ciscoasa# 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 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。

ガイドラインと制限事項

- 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.10-7）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、**nameif** コマンドを除外してください。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 **nameif** コマンドを設定できます。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 11 章「ルーテッド モードのインターフェイス」または第 12 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

	コマンド	目的
ステップ 1	**interface** {*physical_interface* | **redundant** *number*}.*subinterface* **例：** `ciscoasa(config)# interface gigabitethernet 0/1.100`	新しいサブインターフェイスを指定します。物理インターフェイス ID の説明については、「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.10-10）を参照してください。 **redundant** *number* 引数には、冗長インターフェイス ID（**redundant 1** など）を指定します。 *subinterface* ID は、1 ～ 4294967293 の整数です。
ステップ 2	**vlan** *vlan_id* **例：** `ciscoasa(config-subif)# vlan 101`	サブインターフェイスの VLAN アドレスを指定します。*vlan_id* は、1 ～ 4094 の整数です。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。 1 つの VLAN は 1 つのサブインターフェイスにだけ割り当てることができます。同じ VLAN を複数のサブインターフェイスに割り当てることはできません。VLAN を物理インターフェイスに割り当てることはできません。トラフィックがサブインターフェイスを通過するには、各サブインターフェイスに VLAN ID が必要となります。VLAN ID を変更するために **no** オプションで古い VLAN ID を削除する必要はありません。別の VLAN ID を指定して **vlan** コマンドを入力すると、ASA によって古い ID が変更されます。

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.10-15）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 11 章「ルーテッド モードのインターフェイス」または第 12 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.10-5）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。MTU は、**mtu** コマンドを使用して、デフォルト値の 1500 よりも大きい値（たとえば 9000）に設定します。「MAC アドレス、MTU、TCP MSS の設定」（P.11-10）を参照してください。
- 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（**sysopt connection tcpmss 0** コマンドを使用）、または「MAC アドレス、MTU、TCP MSS の設定」（P.11-10）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

コマンド	目的
jumbo-frame reservation **例：** `ciscoasa(config)# jumbo-frame reservation`	ジャンボ フレーム サポートをイネーブルにします。ジャンボ フレームをディセーブルにするには、このコマンドの **no** 形式を使用します。

例

次に、ジャンボ フレームの予約をイネーブルにし、コンフィギュレーションを保存して ASA をリロードする例を示します。

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted.Command accepted.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload?[confirm] Y
```

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 11 章「ルーテッド モードのインターフェイス」または第 12 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

インターフェイスをモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
`show interface`	インターフェイス統計情報を表示します。
`show interface ip brief`	インターフェイスの IP アドレスとステータスを表示します。

ASAv インターフェイスの設定例

- 「物理インターフェイス パラメータの例」（P.10-17）
- 「サブインターフェイス パラメータの例」（P.10-17）

物理インターフェイス パラメータの例

次に、物理インターフェイスのパラメータの設定例を示します。

```
interface gigabitethernet 0/1
    speed 1000
    duplex full
    no shutdown
```

サブインターフェイス パラメータの例

次に、サブインターフェイスのパラメータの設定例を示します。

```
interface gigabitethernet 0/1.1
    vlan 101
    no shutdown
```

次の作業

第 11 章「ルーテッド モードのインターフェイス」または第 12 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 10-1　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。

- 「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」（P.11-1）
- 「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」（P.11-3）
- 「ガイドラインと制限事項」（P.11-4）
- 「デフォルト設定」（P.11-5）
- 「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」（P.11-6）
- 「インターフェイスのオン/オフ」（P.11-18）
- 「インターフェイスのモニタリング」（P.11-18）
- 「ルーテッド モードのインターフェイスの機能履歴」（P.11-19）

（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。設定するコンテキストに切り替えるには、**changeto context** *name* コマンドを入力します。

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」（P.11-1）
- 「デュアル IP スタック（IPv4 および IPv6）」（P.11-2）

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.11-16）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することで、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.11-16）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。次に例を示します。
interface gigabitethernet 0/0.100
vlan 100

すべてのタイプのインターフェイスが、インターフェイス（VLAN、物理、冗長、ブリッジ グループ、EtherChannel インターフェイスなど）の最大数に含まれます。設定で定義されている各 **interface** コマンドは、この制限に対してカウントされます。たとえば、GigabitEthernet 0/0 インターフェイスがポートチャネル 1 の一部として定義されている場合でも、次のインターフェイスは両方ともカウントされます。
interface gigabitethernet 0/0
および
interface port-channel 1

モデル	ライセンス要件
ASASM	VLAN： 基本ライセンス：1000

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 9 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 3 章「Cisco ASA サービス モジュール向けのスイッチの設定」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.6-16）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 12 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 7 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 コンフィギュレーション」（P.2-14）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.11-10）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

- 「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」（P.11-6）
- 「一般的なインターフェイス パラメータの設定」（P.11-6）
- 「MAC アドレス、MTU、TCP MSS の設定」（P.11-10）
- 「IPv6 アドレッシングの設定」（P.11-12）
- 「同じセキュリティ レベルの通信の許可」（P.11-16）

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 9 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 3 章「Cisco ASA サービス モジュール向けのスイッチの設定」
- ASAv：第 10 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.6-16）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）設定するコンテキストに切り替えるには、**changeto context** *name* コマンドを入力します。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.11-6）を参照してください。

ステップ 4　（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.11-10）を参照してください。

ステップ 5　（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.11-12）を参照してください。

ステップ 6　（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.11-16）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

ガイドラインと制限事項

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 7 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 9 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 3 章「Cisco ASA サービス モジュール向けのスイッチの設定」
  - ASAv：第 10 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.6-16）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、**changeto context** *name* コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	ASA 5512-X 以降および ASAv： **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[.*subinterface*] | *mapped_name*} ASASM： ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **例：** ciscoasa(config)# interface gigabithethernet 0/0	まだインターフェイス コンフィギュレーション モードを開始していない場合は、インターフェイス コンフィギュレーション モードを開始します。 **redundant** *number* 引数には、冗長インターフェイス ID（**redundant 1** など）を指定します。 **port-channel** *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。 物理インターフェイス ID 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.9-16）の説明を参照してください。 *subinterface* ID は、物理インターフェイス ID または冗長インターフェイス ID の後ろに、ピリオド（.）で区切って付加します。 マルチ コンテキスト モードで、マッピング名を *allocate-interface* コマンドを使用して割り当てた場合、その名前を **mapped_name** に入力します。
ステップ 2	**nameif** *name* **例：** ciscoasa(config-if)# nameif inside	インターフェイスに名前を付けます。 *name* は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。
ステップ 3	次のいずれかを実行します。	
	ip address *ip_address* [*mask*] [**standby** *ip_address*] **例：** ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2	IP アドレスを手動で設定します。 **（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。 *ip_address* 引数および *mask* 引数には、インターフェイスの IP アドレスとサブネット マスクを設定します。 **standby** *ip_address* 引数は、フェールオーバーで使用します。詳細については、「アクティブ / スタンバイ フェールオーバーの設定」（P.7-29）または「アクティブ / アクティブ フェールオーバーの設定」（P.7-34）を参照してください。

	コマンド	目的
	ip address dhcp [**setroute**] **例：** ciscoasa(config-if)# ip address dhcp	DHCP サーバから IP アドレスを取得します。 **setroute** キーワードを指定すると、ASA が DHCP サーバから渡されたデフォルト ルートを使用できるようになります。 DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。 **ip address dhcp** コマンドを入力する前に、**no shutdown** コマンドを使用してインターフェイスをイネーブルにしなかった場合、DHCP 要求が送信されないことがあります。
	PPPoE サーバからの IP アドレスの取得については、VPN コンフィギュレーション ガイドを参照してください。	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。
ステップ 4	**security-level** *number* **例：** ciscoasa(config-if)# security-level 50	セキュリティ レベルを設定します。*number* には、0（最下位）～ 100（最上位）の整数を指定します。「セキュリティ レベル」（P.11-1）を参照してください。
ステップ 5	（オプション） **management-only** **例：** ciscoasa(config-if)# 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、管理インターフェイスは管理専用として設定されます。この設定をディセーブルにするには、**no management-only** コマンドを入力します。 （ASA 5512-X ～ ASA 5555-X）Management 0/0 インターフェイスの **management-only** をディセーブルにすることはできません。 **management-only** コマンドは、冗長インターフェイスではサポートされません。

例

次に、VLAN 101 のパラメータの設定例を示します。

```
ciscoasa(config)# interface vlan 101
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

次に、マルチコンテキスト モードでコンテキスト コンフィギュレーションにパラメータを設定する例を示します。インターフェイス ID はマップ名です。

```
ciscoasa/contextA(config)# interface int1
ciscoasa/contextA(config-if)# nameif outside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

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.11-10）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.11-12）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、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 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.6-3）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.6-26）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.9-8）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 9 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 3 章「Cisco ASA サービス モジュール向けのスイッチの設定」
  - ASAv：第 10 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.6-16）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、**changeto context** *name* コマンドを入力します。
- MTU を 1500 より多く増やすには、「ジャンボ フレーム サポートのイネーブル化」（P.9-28）に従って、ジャンボ フレームをイネーブルにします。ASASM 上でジャンボ フレームがデフォルトでサポートされている場合、この機能をイネーブルにする必要はありません。

手順の詳細

	コマンド	目的
ステップ 1	ASA 5512-X 以降および ASAv： **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[.*subinterface*] | *mapped_name*} ASASM： ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **例：** ciscoasa(config)# interface vlan 100	まだインターフェイス コンフィギュレーション モードを開始していない場合は、インターフェイス コンフィギュレーション モードを開始します。 **redundant** *number* 引数には、冗長インターフェイス ID（**redundant 1** など）を指定します。 **port-channel** *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。 物理インターフェイス ID 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.9-16）の説明を参照してください。 *subinterface* ID は、物理インターフェイス ID または冗長インターフェイス ID の後ろに、ピリオド（.）で区切って付加します。 マルチ コンテキスト モードで、マッピング名を *allocate-interface* コマンドを使用して割り当てた場合、その名前を **mapped_name** に入力します。

	コマンド	目的
ステップ 2	**mac-address** *mac_address* [**standby** *mac_address*] **例：** ciscoasa(config-if)# mac-address 000C.F142.4CDE	プライベート MAC アドレスをこのインターフェイスに割り当てます。*mac_address* は、H.H.H 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。 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。 フェールオーバーで使用する場合は、**スタンバイ** MAC アドレスを設定します。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 3	**mtu** *interface_name bytes* **例：** ciscoasa(config)# mtu inside 9200	300 ～ 9198 バイトの間（ASAv の場合は 9000）で MTU を設定します。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 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モデルでは、インターフェイスに 1500 よりも大きな値を入力する場合、ジャンボ フレームのサポートをイネーブルにする必要があります。「ジャンボ フレーム サポートのイネーブル化」（P.9-28）を参照してください。
ステップ 4	**sysopt connection tcpmss** [**minimum**] *bytes* **例：** ciscoasa(config)# sysopt connection tcpmss 8500 ciscoasa(config)# sysopt connection tcpmss minimum 1290	最大 TCP セグメント サイズをバイト単位で設定します（48 ～任意の最大値）。デフォルト値は 1380 バイトです。この機能をディセーブルにするには、bytes を **0** に設定します。 **minimum** キーワードには、最大セグメント サイズを 48 ～ 65535 の間で *bytes* 以上の値に設定してください。minimum 機能は、デフォルトでディセーブルです（0 に設定）。

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.11-12）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」（P.11-13）
- 「グローバル IPv6 アドレスの設定」（P.11-14）
- 「IPv6 ネイバー探索の設定」（P.11-15）

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.11-13）
- 「Modified EUI-64 インターフェイス ID」（P.11-13）

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。

（注）　リンクローカル アドレスの設定だけを行う場合は、コマンド リファレンスの **ipv6 enable** コマンド（自動設定）または **ipv6 address link-local** コマンド（手動設定）を参照してください。

Modified EUI-64 インターフェイス ID

RFC 3513「Internet Protocol Version 6 (IPv6) Addressing Architecture」（インターネット プロトコル バージョン 6 アドレッシング アーキテクチャ）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 9 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 3 章「Cisco ASA サービス モジュール向けのスイッチの設定」
  - ASAv：第 10 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.6-16）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、**changeto context** *name* コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	ASA 5512-X 以降および ASAv： **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[.*subinterface*] | *mapped_name*} ASASM： ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **例：** ciscoasa(config)# interface gigabithethernet 0/0	まだインターフェイス コンフィギュレーション モードを開始していない場合は、インターフェイス コンフィギュレーション モードを開始します。 **redundant** *number* 引数には、冗長インターフェイス ID（**redundant 1** など）を指定します。 **port-channel** *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。 物理インターフェイス ID の説明については、「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.9-16）を参照してください。 *subinterface* ID は、物理インターフェイス ID または冗長インターフェイス ID の後ろに、ピリオド（.）で区切って付加します。 マルチ コンテキスト モードで、マッピング名を *allocate-interface* コマンドを使用して割り当てた場合、その名前を **mapped_name** に入力します。

	コマンド	目的
ステップ 2	次のいずれかを実行します。	
	ipv6 address autoconfig **例：** `ciscoasa(config-if)# ipv6 address autoconfig`	インターフェイスでステートレスな自動設定をイネーブルにします。インターフェイスでステートレスな自動設定をイネーブルにすると、ルータ アドバタイズメント メッセージで受信したプレフィックスに基づいて IPv6 アドレスが設定されます。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。メッセージを抑制するには、**ipv6 nd suppress-ra** コマンドを参照してください。
	ipv6 address *ipv6-address/prefix-length* [**standby** *ipv6-address*] **例：** `ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48`	インターフェイスにグローバル アドレスを割り当てます。グローバル アドレスを割り当てると、インターフェイスのリンクローカル アドレスが自動的に作成されます。 **standby** は、フェールオーバー ペアのセカンダリ ユニットまたはフェールオーバー グループで使用されるインターフェイス アドレスを指定します。
	ipv6 address *ipv6-prefix/prefix-length* **eui-64** **例：** `ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98::/48 eui-64`	Modified EUI-64 形式を使用してインターフェイスの MAC アドレスから生成されたインターフェイス ID と、指定されたプレフィックスを結合することによって、インターフェイスにグローバル アドレスを割り当てます。グローバル アドレスを割り当てると、インターフェイスのリンクローカル アドレスが自動的に作成されます。 スタンバイ アドレスを指定する必要はありません。インターフェイス ID が自動的に生成されます。
ステップ 3	（オプション） **ipv6 enforce-eui64** *if_name* **例：** `ciscoasa(config)# ipv6 enforce-eui64 inside`	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します。 *if_name* 引数には、**nameif** コマンドで指定したインターフェイスの名前を指定します。このインターフェイスに対してアドレス形式を適用できます。 詳細については、「Modified EUI-64 インターフェイス ID」（P.11-13）を参照してください。

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 25 章「IPv6 ネイバー探索」を参照してください。

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。

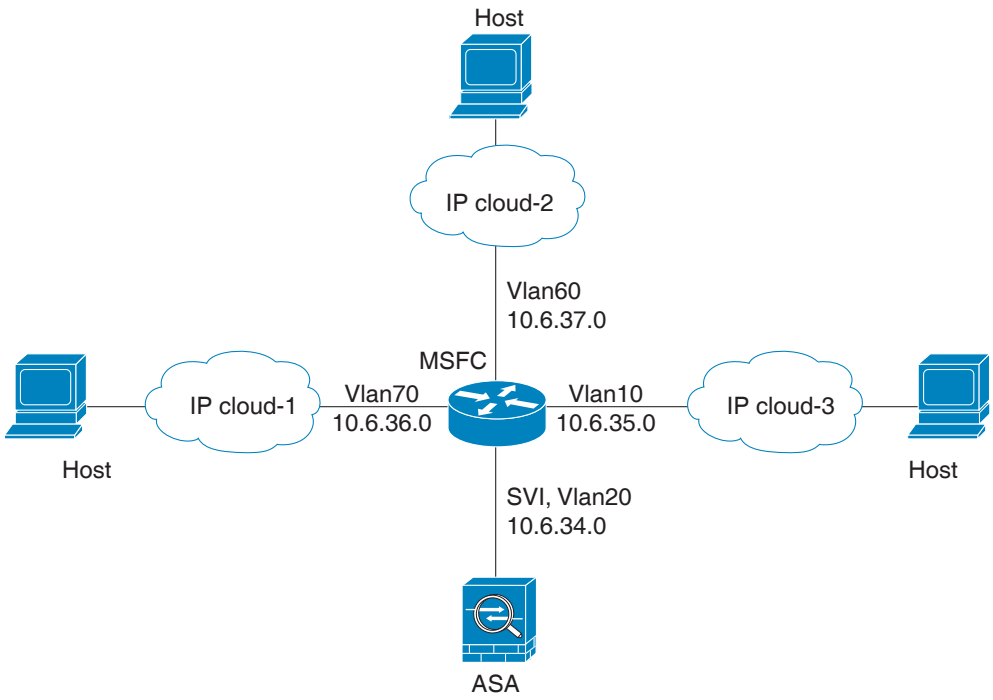
インターフェイス内通信に関する情報

インターフェイス内通信は、インターフェイスに入る VPN トラフィックが同じインターフェイスから出力される場合に役に立つことがあります。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 11-1 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 11-1　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 11-1 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

コマンド	目的
same-security-traffic permit inter-interface	相互通信を可能にするために同じセキュリティ レベルのインターフェイスをイネーブルにします。
same-security-traffic permit intra-interface	同じインターフェイスに接続されたホスト間の通信をイネーブルにします。

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

	コマンド	目的

ステップ 1	`ciscoasa(config)# interface {vlan number | mapped_name}`
	
	例：
	`ciscoasa(config)# interface vlan 100`
		まだインターフェイス コンフィギュレーション モードを開始していない場合は、インターフェイス コンフィギュレーション モードを開始します。
		
		マルチ コンテキスト モードで、マッピング名を *allocate-interface* コマンドを使用して割り当てた場合、その名前を **mapped_name** に入力します。

ステップ 2	**shutdown** **例：** `ciscoasa(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 3	**no shutdown** **例：** `ciscoasa(config-if)# no shutdown`	インターフェイスを再びイネーブルにします。

インターフェイスのモニタリング

インターフェイスをモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
show interface	インターフェイス統計情報を表示します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

ルーテッド モードのインターフェイスの機能履歴

表 11-1 に、この機能のリリース履歴を示します。

表 11-1　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。
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。**speed** コマンドを使用してインターフェイスの速度を変更します。また、**show interface** コマンドを使用して各インターフェイスの現在の設定速度を確認します。
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。 **switchport trunk native vlan** コマンドが導入されました。

表 11-1　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 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。 **jumbo-frame reservation** コマンドが導入されました。
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。
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。 **flowcontrol** コマンドが導入されました。

CHAPTER 12

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。

- 「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」（P.12-1）
- 「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」（P.12-3）
- 「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」（P.12-5）
- 「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.12-6）
- 「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」（P.12-7）
- 「インターフェイスのオン/オフ」（P.12-20）
- 「インターフェイスのモニタリング」（P.12-21）
- 「トランスペアレント モードのインターフェイスの設定例」（P.12-21）
- 「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」（P.12-22）

（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。設定するコンテキストに切り替えるには、**changeto context** *name* コマンドを入力します。

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」（P.12-2）
- 「セキュリティ レベル」（P.12-2）

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.9-2）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.12-19）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することで、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.12-19）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

モデル	ライセンス要件
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。次に例を示します。

```
interface gigabitethernet 0/0.100
  vlan 100
```

すべてのタイプのインターフェイスが、インターフェイス（VLAN、物理、冗長、ブリッジ グループ、EtherChannel インターフェイスなど）の最大数に含まれます。設定で定義されている各 **interface** コマンドは、この制限に対してカウントされます。たとえば、GigabitEthernet 0/0 インターフェイスがポートチャネル 1 の一部として定義されている場合でも、次のインターフェイスは両方ともカウントされます。

interface gigabitethernet 0/0
および
interface port-channel 1

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 9 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 3 章「Cisco ASA サービス モジュール向けのスイッチの設定」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、**allocate-interface** コマンドを使用してシステム 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。

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.9-2）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.12-8）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、ルーティングの観点からマルチ コンテキストを可能にするためには、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 7 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 コンフィギュレーション」（P.2-14）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.12-13）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」（P.12-7）
- 「ブリッジ グループの設定」（P.12-8）
- 「一般的なインターフェイス パラメータの設定」（P.12-9）
- 「管理インターフェイスの設定（ASA 5512-X 以降および ASAv）」（P.12-11）
- 「MAC アドレス、MTU、TCP MSS の設定」（P.12-13）
- 「IPv6 アドレッシングの設定」（P.12-16）
- 「同じセキュリティ レベルの通信の許可」（P.12-19）

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 9 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 3 章「Cisco ASA サービス モジュール向けのスイッチの設定」
- ASAv：第 10 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.6-16）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）設定するコンテキストを変更する場合は、**changeto context** *name* コマンドを入力します。

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.12-8）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.12-9）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.12-11）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.12-13）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.12-16）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.12-19）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。

ガイドラインと制限事項

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

	コマンド	目的
ステップ 1	**interface bvi** *bridge_group_number* **例：** `ciscoasa(config)# interface bvi 1`	ブリッジ グループを作成します。*bridge_group_number* は 1 ～ 250 の整数です。
ステップ 2	**ip address** *ip_address* [*mask*] [**standby** *ip_address*] **例：** `ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2`	ブリッジ グループの管理 IP アドレスを指定します。 ブリッジ グループにホスト 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で送受信されるすべての ARP パケットをドロップします。このため、/30 サブネットを使用し、このサブネットからアップストリーム ルータに予約済みアドレスを割り当てると、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。 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。 フェールオーバーには、**standby** キーワードおよびアドレスを使用します。

例

次に、ブリッジ グループ 1 の管理アドレスおよびスタンバイ アドレスを設定する例を示します。

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

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.12-9）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.12-11）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

ガイドラインと制限事項

- 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.12-2）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 7 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 9 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 3 章「Cisco ASA サービス モジュール向けのスイッチの設定」
  - ASAv：第 10 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.6-16）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、**changeto context** *name* コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	ASA 5512-X 以降および ASAv： **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[.*subinterface*] | *mapped_name*} **例：** `ciscoasa(config)# interface gigabitethernet 0/0`	まだインターフェイス コンフィギュレーション モードを開始していない場合は、インターフェイス コンフィギュレーション モードを開始します。 **redundant** *number* 引数には、冗長インターフェイス ID（**redundant 1** など）を指定します。 **port-channel** *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。 物理インターフェイス ID 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.9-16）の説明を参照してください。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.12-11）を参照してください。 *subinterface* ID は、物理インターフェイス ID または冗長インターフェイス ID の後ろに、ピリオド（.）で区切って付加します。 マルチ コンテキスト モードで、マッピング名を *allocate-interface* コマンドを使用して割り当てた場合、その名前を **mapped_name** に入力します。
ステップ 2	**bridge-group** *number* **例：** `ciscoasa(config-if)# bridge-group 1`	インターフェイスをブリッジ グループに割り当てます。*number* は 1 ～ 100 の範囲の整数です。ブリッジ グループには最大 4 個のインターフェイスを割り当てることができます。同一インターフェイスを複数のブリッジ グループに割り当てることはできません。
ステップ 3	**nameif** *name* **例：** `ciscoasa(config-if)# nameif inside`	インターフェイスに名前を付けます。 *name* は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。
ステップ 4	**security-level** *number* **例：** `ciscoasa(config-if)# security-level 50`	セキュリティ レベルを設定します。*number* には、0（最下位）～ 100（最上位）の整数を指定します。

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.12-11）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.12-13）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.12-16）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.9-2）を参照してください。

制限事項

- 「管理インターフェイス」（P.9-2）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 9 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.6-16）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、**changeto context** *name* コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	**interface** {{**port-channel** *number* | **management** *slot/port*}[*.subinterface*] | *mapped_name*} **例：** `ciscoasa(config)# interface management 0/0.1`	まだインターフェイス コンフィギュレーション モードを開始していない場合は、管理インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 **port-channel** *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。EtherChannel インターフェイスには、管理メンバ インターフェイスのみが設定されている必要があります。 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。 マルチ コンテキスト モードで、マッピング名を *allocate-interface* コマンドを使用して割り当てた場合、その名前を **mapped_name** に入力します。
ステップ 2	**nameif** *name* **例：** `ciscoasa(config-if)# nameif management`	インターフェイスに名前を付けます。 *name* は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。
ステップ 3	次のいずれかを実行します。	
	ip address *ip_address* [*mask*] [**standby** *ip_address*] **例：** `ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2`	IP アドレスを手動で設定します。 **（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。 *ip_address* 引数および *mask* 引数には、インターフェイスの IP アドレスとサブネット マスクを設定します。 **standby** *ip_address* 引数は、フェールオーバーで使用します。詳細については、「アクティブ / スタンバイ フェールオーバーの設定」（P.7-29）または「アクティブ / アクティブ フェールオーバーの設定」（P.7-34）を参照してください。

	コマンド	目的

	`ip address dhcp [setroute]`
	
	例：
	`ciscoasa(config-if)# ip address dhcp`
		DHCP サーバから IP アドレスを取得します。
		setroute キーワードを指定すると、ASA が DHCP サーバから渡されたデフォルト ルートを使用できるようになります。
		DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。
		ip address dhcp コマンドを入力する前に、**no shutdown** コマンドを使用してインターフェイスをイネーブルにしなかった場合、DHCP 要求が送信されないことがあります。

ステップ 4	`security-level` *number* **例：** `ciscoasa(config-if)# security-level 50`	セキュリティ レベルを設定します。*number* には、0（最下位）～ 100（最上位）の整数を指定します。

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.12-13）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.12-16）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、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 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.6-3）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.6-26）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.9-8）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 9 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 3 章「Cisco ASA サービス モジュール向けのスイッチの設定」
  - ASAv：第 10 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.6-16）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、**changeto context** *name* コマンドを入力します。
- MTU を 1500 より多く増やすには、「ジャンボ フレーム サポートのイネーブル化」（P.9-28）に従って、サポート対象モデル上でジャンボ フレームをイネーブルにします。ASASM 上でジャンボ フレームがデフォルトでサポートされている場合、この機能をイネーブルにする必要はありません。

手順の詳細

	コマンド	目的
ステップ 1	ASA 5512-X 以降および ASAv： **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[**.***subinterface*] | *mapped_name*} ASASM： ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **例：** ciscoasa(config)# interface vlan 100	まだインターフェイス コンフィギュレーション モードを開始していない場合は、インターフェイス コンフィギュレーション モードを開始します。 **redundant** *number* 引数には、冗長インターフェイス ID（**redundant 1** など）を指定します。 **port-channel** *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。 物理インターフェイス ID 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.9-16）の説明を参照してください。 *subinterface* ID は、物理インターフェイス ID または冗長インターフェイス ID の後ろに、ピリオド（.）で区切って付加します。 マルチ コンテキスト モードで、マッピング名を *allocate-interface* コマンドを使用して割り当てた場合、その名前を **mapped_name** に入力します。
ステップ 2	**mac-address** *mac_address* [**standby** *mac_address*] **例：** ciscoasa(config-if)# mac-address 000C.F142.4CDE	プライベート MAC アドレスをこのインターフェイスに割り当てます。*mac_address* は、H.H.H 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。 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。 フェールオーバーで使用する場合は、**スタンバイ** MAC アドレスを設定します。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。

	コマンド	目的
ステップ 3	**mtu** *interface_name bytes* **例：** `ciscoasa(config)# mtu inside 9200`	300 ～ 9198 バイトの間（ASAv の場合は 9000）で MTU を設定します。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 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モデルでは、インターフェイスに 1500 よりも大きな値を入力する場合、ジャンボ フレームのサポートをイネーブルにする必要があります。「ジャンボ フレーム サポートのイネーブル化」（P.9-28）を参照してください。

ステップ 4	**sysopt connection tcpmss** [**minimum**] *bytes*
	
	例：
	`ciscoasa(config)# sysopt connection tcpmss 8500`
	`ciscoasa(config)# sysopt connection tcpmss minimum 1290`
		最大 TCP セグメント サイズをバイト単位で設定します（48 ～任意の最大値）。デフォルト値は 1380 バイトです。この機能をディセーブルにするには、bytes を **0** に設定します。
		
		minimum キーワードには、最大セグメント サイズを 48 ～ 65535 の間で *bytes* 以上の値に設定してください。minimum 機能は、デフォルトでディセーブルです（0 に設定）。

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.12-16）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」（P.12-16）
- 「グローバル IPv6 アドレスの設定」（P.12-18）
- 「IPv6 ネイバー探索の設定」（P.12-19）

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.12-17）
- 「Modified EUI-64 インターフェイス ID」（P.12-17）
- 「サポートされていないコマンド」（P.12-18）

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。

（注） リンクローカル アドレスの設定だけを行う場合は、コマンド リファレンスの **ipv6 enable** コマンド（自動設定）または **ipv6 address link-local** コマンド（手動設定）を参照してください。

Modified EUI-64 インターフェイス ID

RFC 3513「Internet Protocol Version 6 (IPv6) Addressing Architecture」（インターネット プロトコル バージョン 6 アドレッシング アーキテクチャ）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 9 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 3 章「Cisco ASA サービス モジュール向けのスイッチの設定」
  - ASAv：第 10 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.6-16）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、**changeto context** *name* コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	ブリッジ グループの場合： **interface bvi** *bridge_group_id* 管理インターフェイスの場合： **interface** *management_interface_id* **例：** `ciscoasa(config)# interface bvi 1`	まだインターフェイス コンフィギュレーション モードを開始していない場合は、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 address** *ipv6-address/prefix-length* [**standby** *ipv6-address*] **例：** `ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48`	インターフェイスにグローバル アドレスを割り当てます。グローバル アドレスを割り当てると、（ブリッジ グループ、各メンバ インターフェイスの）インターフェイスに対してリンクローカル アドレスが自動的に作成されます。 **standby** は、フェールオーバー ペアのセカンダリ ユニットまたはフェールオーバー グループで使用されるインターフェイス アドレスを指定します。 **（注）** インターフェイス ID に Modified EUI-64 インターフェイス ID を使用する **eui-64** キーワードは、トランスペアレント モードではサポートされません。
ステップ 3	（オプション） **ipv6 enforce-eui64** *if_name* **例：** `ciscoasa(config)# ipv6 enforce-eui64 inside`	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します。 *if_name* 引数には、**nameif** コマンドで指定したインターフェイスの名前を指定します。このインターフェイスに対してアドレス形式を適用できます。 詳細については、「Modified EUI-64 インターフェイス ID」（P.12-17）を参照してください。

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 25 章「IPv6 ネイバー探索」を参照してください。

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

コマンド	目的
same-security-traffic permit inter-interface	相互通信を可能にするために同じセキュリティ レベルのインターフェイスをイネーブルにします。

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

	コマンド	目的
ステップ 1	ciscoasa(config)# **interface** {**vlan** *number* | *mapped_name*} **例：** ciscoasa(config)# interface vlan 100	まだインターフェイス コンフィギュレーション モードを開始していない場合は、インターフェイス コンフィギュレーション モードを開始します。 マルチ コンテキスト モードで、マッピング名を *allocate-interface* コマンドを使用して割り当てた場合、その名前を **mapped_name** に入力します。
ステップ 2	**shutdown** **例：** ciscoasa(config-if)# shutdown	インターフェイスをディセーブルにします。
ステップ 3	**no shutdown** **例：** ciscoasa(config-if)# no shutdown	インターフェイスを再びイネーブルにします。

インターフェイスのモニタリング

コマンド	目的
show interface	インターフェイス統計情報を表示します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。
show bridge-group	ブリッジ グループの情報を表示します。

トランスペアレント モードのインターフェイスの設定例

次の例では、3 つのインターフェイスそれぞれの 2 つのブリッジ グループと管理専用インターフェイスを示します。

```
interface gigabitethernet 0/0
    nameif inside1
    security-level 100
    bridge-group 1
    no shutdown
interface gigabitethernet 0/1
    nameif outside1
    security-level 0
    bridge-group 1
    no shutdown
interface gigabitethernet 0/2
    nameif dmz1
    security-level 50
    bridge-group 1
    no shutdown
interface bvi 1
    ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
    nameif inside2
    security-level 100
    bridge-group 2
    no shutdown
interface gigabitethernet 1/1
    nameif outside2
    security-level 0
    bridge-group 2
    no shutdown
interface gigabitethernet 1/2
    nameif dmz2
    security-level 50
    bridge-group 2
    no shutdown
interface bvi 2
    ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
    nameif mgmt
    security-level 100
    ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
    no shutdown
```

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 12-1 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。

表 12-1　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。**speed** コマンドを使用してインターフェイスの速度を変更します。また、**show interface** コマンドを使用して各インターフェイスの現在の設定速度を確認します。

表 12-1　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 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。 **switchport trunk native vlan** コマンドが導入されました。
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。 **jumbo-frame reservation** コマンドが導入されました。
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。
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。 **flowcontrol** コマンドが導入されました。
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。 **interface bvi**、**show bridge-group** コマンドが導入されました。

表 12-1　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 グループの最大数を 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 個のブリッジ グループに増加されました。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追加できます。 **interface bvi** および **bridge-group** コマンドが変更されました。

PART 4

基本設定

基本設定

この章では、ASA を機能させるため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、イネーブル パスワード、Telnet パスワードの設定」（P.13-1）
- 「イネーブル パスワードと Telnet パスワードの回復」（P.13-3）
- 「日時の設定」（P.13-8）
- 「マスター パスフレーズの設定」（P.13-11）
- 「DNS サーバの設定」（P.13-15）
- 「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」（P.13-17）

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、システム実行スペースとコンテキスト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、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 ASA またはコンテキストのホスト名を指定します。デフォルトのホスト名は「asa」です。

hostname *name*

例：

```
ciscoasa(config)# hostname myhostnamexample12345
```

名前には、63 文字以下の文字を使用できます。ホスト名はアルファベットまたは数字で開始および終了する必要があります。使用できるのはアルファベット、数字、ハイフンのみです。

ASA のホスト名を設定すると、そのホスト名がコマンド 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。

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。コンテキスト内で任意に設定したホスト名はコマンドラインには表示されませんが、**banner** コマンド **$(hostname)** トークンによって使用できます。

ステップ 2　ASA のドメイン名を指定します。デフォルト ドメイン名は default.domain.invalid です。

domain-name *name*

例：

```
ciscoasa(config)# domain-name example.com
```

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 3　イネーブル パスワードを変更します。デフォルトでは、イネーブル パスワードは空白です。

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。

enable password *password*

例：

```
ciscoasa(config)# enable passwd Pa$$w0rd
```

password 引数は、最大 16 文字の英数字および特殊文字からなるパスワードで、大文字と小文字は区別されます。パスワードには、疑問符とスペースを除いて、任意の文字を使用できます。

このコマンドによって最高の特権レベル（15）のパスワードが変更されます。ローカル コマンド許可を設定すると、次の構文を使用して 0 ～ 15 の各特権レベルにイネーブル パスワードを設定できます。

enable password *password* **level** *number*

パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。パスワードを指定せずに **enable password** コマンドを入力すると、パスワードはデフォルトの空白に設定されます。

ステップ 4　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。

{**passwd** | **password**} *password* [**encrypted**]

例：

```
ciscoasa(config)# password cisco12345
```

passwd または **password** と入力します。*password* は、大文字と小文字が区別されるパスワードです。英数字と特殊記号を 16 文字まで使用できます。パスワードには、疑問符とスペースを除いて、任意の文字を使用できます。

パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。何らかの理由で別の ASA にパスワードをコピーする必要があるにもかかわらず、元のパスワードが不明な場合、暗号化されたパスワードと、**encrypted** キーワードを指定して **passwd** コマンドを入力できます。通常、このキーワードは、**show running-config passwd** コマンドを入力するときにだけ表示されます。

関連項目

「特権 EXEC モードにアクセスするための認証の設定（enable コマンド）」（P.35-18）

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.13-3）
- 「ASA 5506、5506-W および ASA 5508 のパスワードの回復」（P.13-5）
- 「ASAv のパスワードまたはイメージの回復」（P.13-6）
- 「パスワード回復のディセーブル化」（P.13-7）

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、[<filename> with no configuration load] オプションを選択して Enter 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。

enable password

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。

- 「タイム ゾーンと夏時間の設定」（P.13-8）
- 「NTP サーバを使用した日付と時刻の設定」（P.13-9）
- 「手動での日付と時刻の設定」（P.13-11）

タイム ゾーンと夏時間の設定

タイム ゾーンと夏時間の日付範囲を設定するには、次の手順を実行します。

手順

ステップ 1　タイム ゾーンを設定します。デフォルトでは、タイム ゾーンは UTC（協定世界時）であり、夏時間の日付範囲は 4 月の第一日曜日の午前 2 時～ 10 月の最終日曜日の午前 2 時です。

```
clock timezone zone [-]hours [minutes]
```

例：

```
ciscoasa(config)# clock timezone PST -8
```

zone 引数は、タイム ゾーンを文字列で指定します。たとえば、PST は太平洋標準時（Pacific Standard Time）を表します。

[-]*hours* 値は、UTC との時差を時間で設定します。たとえば、PST は -8 時間です。

minutes 値は、UTC との時差を分で設定します。

ステップ 2　次のいずれかのコマンドを入力して、夏時間の日付範囲をデフォルトから変更します。定期的な日付範囲のデフォルト値は、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 時です。

- 夏時間の開始日と終了日を、特定の年の特定の日付として指定します。このコマンドを使用する場合は、日付を毎年再設定する必要があります。

  ```
  clock summer-time zone date {day month | month day} year hh:mm {day month | month day}
  year hh:mm [offset]
  ```

例：

```
ciscoasa(config)# clock summer-time PDT 1 April 2010 2:00 60
```

zone 値は、タイム ゾーンを文字列で指定します。たとえば、PDT は太平洋夏時間（Pacific Daylight Time）を表します。

day 値は、月の日付として 1 ～ 31 を設定します。標準の日付形式に応じて、月日を **April 1** または 1 April のように入力できます。

month 値は、月を文字列で設定します。標準の日付形式に応じて、月日を April 1 または 1 April のように入力できます。

year 値は、4 桁で年を設定します（2004 など）。年の範囲は 1993 ～ 2035 です。

hh:mm 値は、24 時間形式で、時間と分を設定します。

offset 値は、夏時間用に時間を変更する分数を設定します。デフォルト値は 60 分です。

- 夏時間の開始日と終了日を、年の特定の日付ではなく、月の日時の形式で指定します。このコマンドを使用すると、毎年変更する必要がない、繰り返される日付範囲を設定できます。

  clock summer-time *zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]

  例：

  ```
  ciscoasa(config)# clock summer-time PDT recurring first Monday April 2:00 60
  ```

  zone 値は、タイム ゾーンを文字列で指定します。たとえば、PDT は太平洋夏時間（Pacific Daylight Time）を表します。

  week 値は、月の特定の週を 1 から 4 までの整数で指定するか、first または last という単語で指定します。たとえば、日付が 5 週目に当たる場合は、last を指定します。

  weekday 値は、Monday、Tuesday、Wednesday などのように曜日を指定します。

  month 値は、月を文字列で設定します。

  hh:mm 値は、24 時間形式で、時間と分を設定します。

  offset 値は、夏時間用に変更する時間の長さを分単位で設定します。デフォルト値は 60 分です。

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　NTP サーバの認証をイネーブルにします。

ntp authenticate

例：

```
ciscoasa(config)# ntp authenticate
```

ステップ 2　認証キー ID が信頼できるキーであると指定します。この信頼できるキーは、NTP サーバの認証に必要です。

ntp trusted-key *key_id*

例：

```
ciscoasa(config)# ntp trusted-key 1
```

key_id 引数は、1 ～ 4294967295 の値です。複数のサーバで使用できるように複数の信頼できるキーを入力できます。

ステップ 3　NTP サーバの認証を行うためのキーを設定します。

ntp authentication-key *key_id* **md5** *key*

例：

```
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
```

key_id 引数は、ステップ 2 で **ntp trusted-key** コマンドを使用して設定した ID であり、*key* 引数は長さ 32 文字以下の文字列です。

ステップ 4　NTP サーバを指定します。

ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

例：

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
```

key_id 引数は、**ntp trusted-key** コマンドを使用して設定した ID です。

source *interface_name* キーワード引数ペアには、NTP パケットの発信インターフェイスを指定します（ルーティング テーブル内のデフォルトのインターフェイスを使用しない場合）。マルチ コンテキスト モードではシステムにインターフェイスが含まれないため、管理コンテキストに定義されているインターフェイス名を指定します。

prefer キーワードは、精度が類似する複数のサーバがある場合に、この NTP 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。サーバの精度に差がない場合は、**prefer** キーワードにどのサーバを使用するかを指定します。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。たとえば、ASA では、優先サーバの stratum 3 の代わりに、サーバ stratum 2 を使用します。

複数のサーバを識別できます。ASA では、最も正確なサーバを使用します。

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　日付と時刻を手動で設定します。

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

例：

```
ciscoasa# clock set 20:54:00 april 1 2004
```

hh:*mm*:*ss* 引数には、時、分、秒を 24 時間形式で設定します。たとえば、午後 8:54 の場合は、20:54:00 と入力します。

day 値は、月の日付として 1 ～ 31 を設定します。標準の日付形式に応じて、月日を april 1 または 1 april のように入力できます。

month 値は、月を設定します。標準の日付形式に応じて、月日を april 1 または 1 april のように入力できます。

year 値は、4 桁で年を設定します（2004 など）。年の範囲は 1993 ～ 2035 です。

デフォルトのタイム ゾーンは UTC です。**clock timezone** コマンドを使用して **clock set** コマンドを入力した後にタイム ゾーンを変更した場合、時間は自動的に新しいタイム ゾーンに調整されます。

このコマンドはハードウェア チップ内の時間を設定しますが、コンフィギュレーション ファイル内の時間は保存しません。この時間はリブート後も保持されます。他の **clock** コマンドとは異なり、このコマンドは特権 EXEC コマンドです。クロックをリセットするには、**clock set** コマンドを使用して新しい時刻を設定する必要があります。

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。

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、コンソール、SSH、HTTPS 経由の 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　暗号キーの生成に使用されるパスフレーズを設定します。パスフレーズの長さは、8 ～ 128 文字にする必要があります。パスフレーズには、バックスペースと二重引用符を除くすべての文字を使用できます。コマンドに新しいパスフレーズを入力しないと、入力を求めるプロンプトが表示されます。パスフレーズを変更するには、古いパスフレーズを入力する必要があります。

key config-key password-encryption [*new_passphrase* [*old_passphrase*]]

例：

```
ciscoasa(config)# key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
```

（注） インタラクティブ プロンプトを使用してパスワードを入力し、パスワードがコマンド履歴バッファに記録されないようにします。

暗号化されたパスワードがプレーン テキスト パスワードに変換されるため、**no key config-key password-encrypt** コマンドは注意して使用してください。パスワードの暗号化がサポートされていないソフトウェア バージョンにダウングレードするときは、このコマンドの **no** 形式を使用できます。

ステップ 2　パスワードの暗号化をイネーブルにします。

password encryption aes

例：

```
ciscoasa(config)# password encryption aes
```

パスワードの暗号化がイネーブルになり、マスター パスワードが使用可能になると、ただちにすべてのユーザ パスワードが暗号化されます。実行コンフィギュレーションには、パスワードは暗号化された形式で表示されます。

パスワードの暗号化をイネーブルにしたときに、パスフレーズが設定されていない場合、パスフレーズが将来的に使用可能になるものとしてコマンドは正常に実行されます。

後から **no password encryption aes** コマンドを使用して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　マスター パスフレーズのランタイム値と結果のコンフィギュレーションを保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

このコマンドを入力しなければ、スタートアップ コンフィギュレーションのパスワードは引き続き可読状態となります（過去に暗号化された状態で保存されていない場合）。また、マルチ コンテキスト モードでは、マスター パスフレーズはシステム コンテキスト コンフィギュレーション内で変更されます。その結果、すべてのコンテキスト内のパスワードが影響を受けます。すべてのユーザ コンテキストではなく、システム コンテキスト モードで **write memory** コマンドを入力しないと、ユーザ コンテキストで暗号化されたパスワードは失効する可能性があります。また、すべての設定を保存するには、システム コンテキストで **write memory all** コマンドを使用します。

例

次の例は、これまでにキーが何も存在していないことを示します。

```
ciscoasa(config)# key config-key password-encryption 12345678
```

次の例は、キーがすでに存在することを示します。

```
ciscoasa(config)# key config-key password-encryption 23456789
Old key: 12345678
```

次の例では、パラメータを指定しないでコマンドを入力して、キーの入力を求めるプロンプトが表示されるようにします。キーがすでに存在するため、入力を求めるプロンプトが表示されます。

```
ciscoasa(config)# key config-key password-encryption
Old key: 12345678
New key: 23456789
Confirm key: 23456789
```

次の例では、既存のキーがないため、入力を求めるプロンプトが表示されません。

```
ciscoasa(config)# key config-key password-encryption
New key: 12345678
Confirm key: 12345678
```

マスター パスフレーズの無効化

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.13-15）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　マスター パスフレーズを削除します。コマンドにパスフレーズを入力しないと、入力を求めるプロンプトが表示されます。

no key config-key password-encryption [*old_passphrase*]]

例：

```
ciscoasa(config)# no key config-key password-encryption

Warning!You have chosen to revert the encrypted passwords to plain text.This operation
will expose passwords in the configuration and therefore exercise caution while viewing,
storing, and copying configuration.

Old key: bumblebee
```

ステップ 2　マスター パスフレーズのランタイム値と結果のコンフィギュレーションを保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

パスフレーズを含む不揮発性メモリは消去され、0xFF パターンで上書きされます。

マルチ モードでは、システム コンテキスト コンフィギュレーション内のマスター パスフレーズが変更されます。その結果、すべてのコンテキスト内のパスワードが影響を受けます。すべてのユーザ コンテキストではなく、システム コンテキスト モードで **write memory** コマンドを入力すると、ユーザ コンテキストで暗号化されたパスワードは失効する可能性があります。また、すべての設定を保存するには、システム コンテキストで **write memory all** コマンドを使用します。

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.13-15）
- 「DNS キャッシュのモニタリング」（P.13-16）

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。たとえば、ほとんどのコマンドでは、IP アドレスを入力する必要があります。名前を使用できるのは、名前と IP アドレスを関連付けるように **name** コマンドを手動で設定し、**names** コマンドを使用して名前の使用をイネーブルにした場合だけです。

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　サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。

dns domain-lookup *interface_name*

例：

```
ciscoasa(config)# dns domain-lookup inside
```

ステップ 2　ASA が発信要求に使用する DNS サーバ グループを指定します。

dns server-group DefaultDNS

例：

```
ciscoasa(config)# dns server-group DefaultDNS
```

PN トンネル グループ用に他の DNS サーバ グループを設定できます。詳細については、コマンド リファレンスの **tunnel-group** コマンドを参照してください。

ステップ 3　1 つまたは複数の DNS サーバを指定します。同じコマンドで 6 つの IP アドレスすべてをスペースで区切って入力するか、各コマンドを別々に入力できます。ASA では、応答を受信するまで各 DNS サーバを順に試します。

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

例：

```
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```

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 や certificate コマンド用に送信された外部 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.13-17）
- 「ASP ロード バランシングのイネーブル化」（P.13-18）

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低下することはありません。次の表に動作の相違点を示します。

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、コンパイルの開始と終了をマークする 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、次のコマンドを使用します:

asp rule-engine transactional-commit *option*

オプションは次のとおりです。

- **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。

例：

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

ASP ロード バランシングのイネーブル化

ASP ロード バランシングのメカニズムによって、次の問題を回避しやすくなります。

- フローの突発的なトラフィックの急増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の受信リングをオーバーサブスクライブするバルク 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るようにします。システムがパケットをドロップしていて、**show cpu** コマンドの出力が 100% を大幅に下回っているときは、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向上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。

パケット単位のロード バランシングのオンとオフの自動切り替えをイネーブルにするには、次のコマンドを入力します。

```
ciscoasa(config)# asp load-balance per-packet auto
```

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。 **key config-key password-encryption**、**password encryption aes**、**clear configure password encryption aes**、**show running-config password encryption aes**、**show password encryption** コマンドが導入されました。
パスワード暗号化の可視性	8.4(1)	**show password encryption** コマンドが変更されました。
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）** ログイン パスワードが使用されるのは、Telnet ユーザ認証（**aaa authentication telnet console** コマンド）を設定しない場合の 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。 **passwd** コマンドが変更されました。
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 バランシングのメカニズムでは、CPU のマルチ コアがインターフェイスの受信リングからのパケットを受信して、それらを個別に処理できるようにすることで、パケット ドロップを削減してスループットを向上させます。 **asp load-balance per-packet-auto** コマンドが導入されました。

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」（P.14-1）
- 「DDNS のガイドライン」（P.14-2）
- 「DDNS の設定」（P.14-2）
- 「DDNS のモニタリング」（P.14-7）
- 「DDNS の履歴」（P.14-8）

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 アップデートを実行するための 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。

スタティック IP アドレスの A RR と PTR RR の両方のアップデート

クライアントを設定して、スタティック IP アドレスの A RR と PTR RR の両方をアップデートするように要求するには、次の手順を実行します。

手順

ステップ 1　DNS RR を動的にアップデートする DDNS アップデート方式を作成します。

ddns update method *name*

例：

```
ciscoasa(config)# ddns update method ddns-2
```

ステップ 2　クライアントが DNS の A RR と PTR RR の両方をアップデートすることを指定します。

ddns both

例：

```
ciscoasa(DDNS-update-method)# ddns both
```

ステップ 3　インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

interface *mapped_name*

例：

```
ciscoasa(DDNS-update-method)# interface eth1
```

ステップ 4　DDNS 方式とインターフェイスおよびアップデート ホスト名を関連付けます。

ddns update [*method-name* | **hostname** *hostname*]

例：

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

ステップ 5　インターフェイスのスタティック IP アドレスを設定します。

ip address *ip_address* [*mask*] [**standby** *ip_address*]

例：

```
ciscoasa(config-if)# ip address 10.0.0.40 255.255.255.0
```

A RR と PTR RR の両方のアップデート

DHCP クライアントを設定して、A RR と PTR RR の両方をアップデートするように要求するとともに、DHCP サーバがこれらの要求を受け取るように要求するには、次の手順を実行します。

手順

ステップ 1　DHCP サーバがアップデートを実行しないことを要求するように DHCP クライアントを設定します。

dhcp-client update dns [**server** {**both** | **none**}]

例：

```
ciscoasa(config)# dhcp-client update dns server none
```

ステップ 2　DNS RR を動的にアップデートする DDNS アップデート方式を作成します。

ddns update method *name*

例：

```
ciscoasa(config)# ddns update method ddns-2
```

ステップ 3　クライアントが DNS の A RR と PTR RR の両方をアップデートすることを指定します。

ddns both

例：

```
ciscoasa(DDNS-update-method)# ddns both
```

ステップ 4　インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

interface *mapped_name*

例：

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

ステップ 5　DDNS 方式とインターフェイスおよびアップデート ホスト名を関連付けます。

ddns update [*method-name* | **hostname** *hostname*]

例：

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

ステップ 6　DHCP を使用してインターフェイスの IP アドレスを取得します。

ip address dhcp

例：

```
ciscoasa(if-config)# ip address dhcp
```

ステップ 7　DDNS アップデートを実行するように DHCP サーバを設定します。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

例：

```
ciscoasa(if-config)# dhcpd update dns
```

両方の RR へのアップデートを無視

DHCP クライアントを設定して、DHCP サーバに A と PTR のどちらのアップデートも受け取らないように指示する FQDN オプションを含めるには、次の手順を実行します。

手順

ステップ 1　DNS RR を動的にアップデートする DDNS アップデート方式を作成します。

ddns update method *name*

例：

```
ciscoasa(config)# ddns update method ddns-2
```

ステップ 2　クライアントが DNS の A RR と PTR RR の両方をアップデートすることを指定します。

ddns both

例：

```
ciscoasa(DDNS-update-method)# ddns both
```

ステップ 3　インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

interface *mapped_name*

例：

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

ステップ 4　DDNS 方式とインターフェイスおよびアップデート ホスト名を関連付けます。

ddns update [*method-name* | **hostname** *hostname*]

例：

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

ステップ 5　DHCP サーバがアップデートを実行しないことを要求するように DHCP クライアントを設定します。

dhcp-client update dns [**server** {**both** | **none**}]

例：

```
ciscoasa(config)# dhcp-client update dns server none
```

ステップ 6　DHCP を使用してインターフェイスの IP アドレスを取得します。

ip address dhcp

例：

```
ciscoasa(if-config)# ip address dhcp
```

ステップ 7　クライアントのアップデート要求を上書きするように DHCP サーバを設定します。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

例：

```
ciscoasa(if-config)# dhcpd update dns both override
```

PTR RR のみのアップデート

サーバを設定して、デフォルトで PTR RR のアップデートのみを実行するには、次の手順を実行します。

手順

ステップ 1　インターフェイスを設定します。

interface *mapped_name*

例：

```
ciscoasa(config)# interface Ethernet0
```

ステップ 2　DHCP サーバが DNS の A RR と PTR RR の両方をアップデートすることを要求します。

dhcp-client update dns [**server** {**both** | **none**}]

例：

```
ciscoasa(config-if)# dhcp-client update dns both
```

ステップ 3　設定されたインターフェイスで DHCP クライアントを設定します。

ddns update [*method-name* | **hostname** *hostname*]

例：

```
ciscoasa(config-if)# ddns update hostname asa
```

ステップ 4　DDNS アップデートを実行するように DHCP サーバを設定します。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

例：

```
ciscoasa(config-if)# dhcpd update dns
```

ステップ 5　DHCP クライアントの DNS ドメイン名を定義します。

dhcpd domain *domain_name* [**interface** *if_name*]

例：

```
ciscoasa(config-if)# dhcpd domain example.com
```

RR のクライアントによるアップデートと PTR RR のサーバによるアップデート

クライアントを設定して A リソース レコードをアップデートするとともに、サーバを設定して PTR レコード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　DNS RR を動的にアップデートする DDNS アップデート方式を作成します。

ddns update method *name*

例：

```
ciscoasa(config)# ddns update method ddns-2
```

ステップ 2　DDNS のアップデート方式を指定します。

ddns both

例：

```
ciscoasa(DDNS-update-method)# ddns both
```

ステップ 3　インターフェイスを設定します。

interface *mapped_name*

例：

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

ステップ 4　DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。

dhcp-client update dns [**server** {**both** | **none**}]

例：

```
ciscoasa(config-if)# dhcp-client update dns
```

ステップ 5　DDNS 方式とインターフェイスおよびアップデート ホスト名を関連付けます。

ddns update [*method-name* | **hostname** *hostname*]

例：

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa
```

ステップ 6　DDNS アップデートを実行するように DHCP サーバを設定します。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

例：

```
ciscoasa(if-config)# dhcpd update dns
```

ステップ 7　DHCP クライアントの DNS ドメイン名を定義します。

dhcpd domain *domain_name* [**interface** *if_name*]

例：

```
ciscoasa(config-if)# dhcpd domain example.com
```

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、次のコマンドを参照してください。

- **show running-config ddns**

  このコマンドは、現在の DDNS コンフィギュレーションを表示します。
- **show running-config dns server-group**

  このコマンドは、現在の DNS サーバ グループのステータスを表示します。

DDNS の履歴

表 14-1　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。 **ddns**、**ddns update**、**dhcp client update dns**、**dhcpd update dns**、**show running-config ddns**、および **show running-config dns server-group** の各コマンドが導入されました。

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」（P.15-1）
- 「DHCP リレー エージェントについて」（P.15-2）
- 「DHCP サービスのライセンス要件」（P.15-2）
- 「DHCP サービスのガイドライン」（P.15-3）
- 「DHCP サーバの設定」（P.15-4）
- 「DHCP サービスのモニタリング」（P.15-13）
- 「DHCP サービスの履歴」（P.15-13）

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.15-4）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.15-5）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.15-10）または「DHCPv6 リレー エージェントの設定」（P.15-12）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　DHCP アドレス プールを作成します。ASA は、クライアントにこのプールのアドレスを 1 つ割り当てます。このアドレスは、一定時間だけ使用できます。これらのアドレスは、直接接続されているネットワークのための、変換されていないローカル アドレスです。

dhcpd address *ip_address if_name*

例：

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
```

アドレス プールは、ASA インターフェイスと同じサブネット内にある必要があります。

ステップ 2　（オプション）DNS サーバの IP アドレスを指定します。

dhcpd dns *dns1* [*dns2*]

例：

```
ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129
```

ステップ 3　（オプション）WINS サーバの IP アドレスを指定します。WINS サーバは最大 2 つまで指定できます。

dhcpd wins *wins1* [*wins2*]

例：

```
ciscoasa(config)# dhcpd wins 209.165.201.5
```

ステップ 4　（オプション）クライアントに許可するリース期間を変更します。リース期間とは、割り当てられた IP アドレスをクライアントが使用できる時間の長さ（秒）であり、この時間が経過するとリースは失効します。0 ～ 1,048,575 の範囲の数を入力してください。デフォルト値は 3600 秒です。

dhcpd lease *lease_length*

例：

```
ciscoasa(config)# dhcpd lease 3000
```

ステップ 5　（オプション）ドメイン名を設定します。

dhcpd domain *domain_name*

例：

```
ciscoasa(config)# dhcpd domain example.com
```

ステップ 6　（オプション）ICMP パケットの DHCP ping タイムアウト値を設定します。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。

dhcpd ping_timeout *milliseconds*

例：

```
ciscoasa(config)# dhcpd ping timeout 20
```

ステップ 7　DHCP クライアントに送信するデフォルト ゲートウェイを定義します。**dhcpd option 3** コマンドを使用してデフォルト ゲートウェイを定義しない場合、DHCP クライアントはデフォルトで DHCP クライアントに最も近い ASA インターフェイスの IP アドレスを使用します。ASA は管理インターフェイスの IP アドレスは使用しません。その結果、DHCP ACK にはこのオプションが含まれなくなります。

dhcpd option 3 ip *gateway_ip*

例：

```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

ステップ 8　ASA 内の DHCP デーモンをイネーブルにし、イネーブルになったインターフェイス上で DHCP クライアント要求をリッスンします。

dhcpd enable *interface_name*

例：

```
ciscoasa(config)# dhcpd enable outside
```

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。

IP アドレスを返す

1 つまたは 2 つの IP アドレスを返す DHCP オプ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　1 つまたは 2 つの IP アドレスを返す DHCP オプションを設定します。

dhcpd option *code* **ip** *addr_1* [*addr_2*]

例：

```
ciscoasa(config)# dhcpd option 2 ip 10.10.1.1 10.10.1.2
```

テキスト文字列を返す

テキスト文字列を返す DHCP オプ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　テキスト文字列を返す DHCP オプションを設定します。

dhcpd option *code* **ascii** *text*

例：

```
ciscoasa(config)# dhcpd option 2 ascii examplestring
```

16 進数値を返す

16 進数値を返す DHCP オプ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　16 進数値を返す DHCP オプションを設定します。

dhcpd option *code* **hex** *value*

例：

```
ciscoasa(config)# dhcpd option 2 hex 22.0011.01.FF1111.00FF.0000.AAAA.1111.1111.1111.11
```

（注）　ASA は、指定されたオプションのタイプおよび値が、RFC 2132 に定義されているオプション コードに対して期待されているタイプおよび値と一致するかどうかは確認しません。たとえば、**dhcpd option 46 ascii hello** というコマンドを入力することは可能であり、ASA はこのコンフィギュレーションを受け入れますが、RFC 2132 の定義では、オプション 46 には 1 桁の 16 進数値を指定することになっています。オプション コードと、コードに関連付けられたタイプおよび期待値の詳細については、RFC 2132 を参照してください。

表 15-1 に、**dhcpd option** コマンドでサポートされていない DHCP オプションを示します。

表 15-1　サポートされていない DHCP オプション

オプション コード	説明
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

DHCP オプション 3、66、および 150 は、Cisco IP フォンを設定するために使用します。オプションの設定の詳細については、「DHCP サーバによる Cisco IP Phone の設定」（P.15-8）を参照してください。

DHCP サーバによる Cisco IP Phone の設定

Cisco IP フォンは、コンフィギュレーションを TFTP サーバからダウンロードします。Cisco IP フォンの起動時に、IP アドレスと TFTP サーバの IP アドレスの両方が事前に設定されていない場合は、この情報を取得するために、オプション 150 または 66 を指定した要求が Cisco IP フォンから DHCP サーバに送信されます。

- DHCP オプション 150 では、TFTP サーバのリストの IP アドレスが提供されます。
- DHCP オプション 66 では、1 つの TFTP サーバの IP アドレスまたはホスト名が与えられます。

（注） Cisco IP フォンからの要求には、DHCP オプション 3 を含めることもできます。これは、デフォルト ルートを設定するためのものです。

1 つの要求にオプション 150 と 66 の両方が含まれている場合があります。この場合、両者が ASA ですでに設定されていると、ASA の DHCP サーバは、その応答で両方のオプションに対する値を提供します。

任意のオプション番号

任意のオプション番号に対して使用される情報を送信するには、次の手順を実行します。

手順

ステップ 1　RFC 2132 で指定されているオプション番号を含む DHCP 要求に対して情報を提供します。

dhcpd option *number value*

例：

```
ciscoasa(config)# dhcpd option 2
```

オプション 66

オプション 66 に対して使用される情報を送信するには、次の手順を実行します。

手順

ステップ 1　オプション 66 の TFTP サーバの IP アドレスまたは名前を提供します。

dhcpd option 66 ascii *server_name*

例：

```
ciscoasa(config)# dhcpd option 66 ascii exampleserver
```

オプション 150

オプション 150 に対して使用される情報を送信するには、次の手順を実行します。

手順

ステップ 1　オプション 150 の 1 台または 2 台の TFTP サーバの IP アドレスまたは名前を提供します。

dhcpd option 150 ip *server_ip1* [*server_ip2*]

例：

```
ciscoasa(config)# dhcpd option 150 ip 10.10.1.1
```

server_ip1 には、プライマリ TFTP サーバの IP アドレスまたは名前を、*server_ip2* には、セカンダリ TFTP サーバの IP アドレスまたは名前を指定します。オプション 150 を使用すると、最大 2 つの TFTP サーバが指定できます。

オプション 3

オプション 3 に対して使用される情報を送信するには、次の手順を実行します。

手順

ステップ 1　デフォルト ルートを設定します。

```
dhcpd option 3 ip router_ip1
```

例：

```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

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。

手順

ステップ 1　次のいずれかまたは両方を実行します。

- グローバル DHCP サーバの IP アドレスおよびそのサーバに到達可能なインターフェイスを指定します。

  ```
  dhcprelay server ip_address if_name
  ```

  例：

  ```
  ciscoasa(config)# dhcprelay server 209.165.201.5 outside
  ciscoasa(config)# dhcprelay server 209.165.201.8 outside
  ciscoasa(config)# dhcprelay server 209.165.202.150 it
  ```

- DHCP クライアント ネットワークに接続されているインターフェイス ID 、およびそのインターフェイスで受信した DHCP 要求に対して使用される DHCP サーバの IP アドレスを指定します。

  ```
  interface interface_id
    dhcprelay server ip_address
  ```

  例：

  ```
  ciscoasa(config)# interface gigabitethernet 0/0
  ciscoasa(config)# dhcprelay server 209.165.201.6
  ciscoasa(config)# dhcprelay server 209.165.201.7
  ciscoasa(config)# interface gigabitethernet 0/1
  ciscoasa(config)# dhcprelay server 209.165.202.155
  ciscoasa(config)# dhcprelay server 209.165.202.156
  ```

グローバルな **dhcprelay server** コマンド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。

ステップ 2　DHCP クライアントに接続された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します。複数のインターフェイス上で DHCP リレーをイネーブルにできます。

dhcprelay enable *interface*

例：

```
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# dhcprelay enable dmz
ciscoasa(config)# dhcprelay enable eng1
ciscoasa(config)# dhcprelay enable eng2
ciscoasa(config)# dhcprelay enable mktg
```

ステップ 3　（オプション）DHCP リレーのアドレス処理のために許容する時間を秒数で設定します。

dhcprelay timeout *seconds*

例：

```
ciscoasa(config)# dhcprelay timeout 25
```

ステップ 4　（オプション）DHCP サーバから送信されたパケットの最初のデフォルト ルータ アドレスを、ASA インターフェイスのアドレスに変更します。

dhcprelay setroute *interface_name*

例：

```
ciscoasa(config)# dhcprelay setroute inside
```

このアクションによって、DHCP サーバが別のルータを指定している場合でも、クライアントのデフォルト ルートが ASA を指すように設定できます。

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。

ステップ 5　（オプション）次のいずれかを行います。

- 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。

  interface *interface_id*
  dhcprelay information trusted

  例：

  ```
  ciscoasa(config)# interface gigabitethernet 0/0
  ciscoasa(config-if)# dhcprelay information trusted
  ```

  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。

- すべてのクライアント 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します。

  dhcprelay information trust-all

  例：

  ```
  ciscoasa(config)# dhcprelay information trust-all
  ```

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　クライアント メッセージの転送先となる IPv6 DHCP サーバの宛先アドレスを指定します。

ipv6 dhcprelay server *ipv6_address* [*interface*]

例：

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701
```

ipv6-address 引数には、リンク スコープのユニキャスト、マルチキャスト、サイト スコープのユニキャスト、またはグローバル IPv6 アドレスを指定できます。リレー宛先の指定は必須です。ループバックやノード ローカルのマルチキャスト アドレスは指定できません。オプションの *interface* 引数では、宛先に対する出力インターフェイスを指定します。クライアントのメッセージは、この出力インターフェイスが接続されたリンクを経由して宛先アドレスに転送されます。指定したアドレスがリンク スコープのアドレスである場合は、インターフェイスを指定する必要があります。

ステップ 2　クライアント インターフェイスで DHCPv6 リレー サービスをイネーブルにします。

ipv6 dhcprelay enable *interface*

例：

```
ciscoasa(config)# ipv6 dhcprelay enable inside
```

ステップ 3　（オプション）リレー アドレスの処理のために、リレー バインディングを通して DHCPv6 サーバからの応答を DHCPv6 クライアントに渡すときに許容する時間を秒数で指定します。

ipv6 dhcprelay timeout *seconds*

例：

```
ciscoasa(config)# ipv6 dhcprelay timeout 25
```

seconds 引数の有効な値の範囲は 1 ～ 3600 です。デフォルトは 60 秒です。

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、次のコマンドを参照してください。

- **show running-config dhcpd**

  このコマンドは、現在の DHCP コンフィギュレーションを表示します。
- **show running-config dhcprelay**

  このコマンドは、現在の DHCP リレー サービスのステータスを表示します。
- **show ipv6 dhcprelay binding**

  このコマンドは、リレー エージェントによって作成されたリレー バインディング エントリを表示します。
- **show ipv6 dhcprelay statistics**

  このコマンドは、IPv6 の DHCP リレー エージェントの統計情報を表示します。
- **clear config ipv6 dhcprelay**

  このコマンドは、IPv6 DHCP リレーのコンフィギュレーションを消去します。

DHCP サービスの履歴

表 15-2　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。 **dhcp client update dns**、**dhcpd address**、**dhcpd domain**、**dhcpd enable**、**dhcpd lease**、**dhcpd option**、**dhcpd ping timeout**、**dhcpd update dns**、**dhcpd wins**、**dhcp-network-scope**、**dhcprelay enable**、**dhcprelay server**、**dhcprelay setroute**、**dhcp-server** の各コマンドが導入されました。**show running-config dhcpd**、および **show running-config dhcprelay** の各コマンドが導入されました。
DHCP for IPv6（DHCPv6）	9.0(1)	IPv6 のサポートが追加されました。 **ipv6 dhcprelay server**、**ipv6 dhcprelay enable**、**ipv6 dhcprelay timeout**、**clear config ipv6 dhcprelay**、**ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag**、**debug ipv6 dhcp**、**debug ipv6 dhcprelay**、**show ipv6 dhcprelay binding**、**clear ipv6 dhcprelay binding**、**show ipv6 dhcprelay statistics**、**clear ipv6 dhcprelay statistics** の各コマンドが導入されました。

表 15-2　DHCP サービスの履歴 （続き）

機能名	プラットフォームリリース	説明
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。 **dhcprelay server**（インターフェイス設定モード）、**clear configure dhcprelay**、**show running-config dhcprelay** の各コマンドが導入または変更されました。
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。 **dhcprelay information trusted**、**dhcprelay information trust-all**、**show running-config dhcprelay** の各コマンドが導入または変更されました。
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。 導入または変更されたコマンドはありません。

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」（P.16-1）
- 「オブジェクトの設定」（P.16-2）
- 「オブジェクトのモニタリング」（P.16-11）
- 「オブジェクトの履歴」（P.16-12）

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。
- 前方参照（**forward-reference enable** コマンド）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.16-2）
- 「サービス オブジェクトとサービス グループの設定」（P.16-4）
- 「ローカル ユーザ グループの設定」（P.16-7）
- 「セキュリティ グループ オブジェクト グループの設定」（P.16-9）
- 「時間範囲の設定」（P.16-10）

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.16-2）
- 「ネットワーク オブジェクト グループの設定」（P.16-3）

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　オブジェクト名を使用して、ネットワーク オブジェクトを作成または編集します。

```
ciscoasa(config)# object network object_name
```

例

```
ciscoasa(config)# object network email-server
```

ステップ 2　次のいずれかのコマンドを使用して、オブジェクトにアドレスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **host** {*IPv4_address* | *IPv6_address*}：単一のホストの 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。

- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address*/*IPv6_prefix*}：ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。
- **range** *start_address end_address*：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** [**v4** | **v6**] *fully_qualified_domain_name*：完全修飾ドメイン名。つまり、www.example.com のようなホスト名。アドレスを IPv4 に制限するには **v4**、IPv6 に制限するには **v6** を指定します。アドレス タイプを指定しない場合、IPv4 が使用されます。

例

```
ciscoasa(config-network-object)# host 10.2.2.2
```

ステップ 3　（オプション）説明を追加します。

```
ciscoasa(config-network-object)# description string
```

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　オブジェクト名を使用して、ネットワーク オブジェクト グループを作成または編集します。

```
ciscoasa(config)# object-group network group_name
```

例

```
ciscoasa(config)# object-group network admin
```

ステップ 2　次のコマンドの 1 つまたは複数を使用して、ネットワーク オブジェクト グループにオブジェクトとアドレスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **network-object host** {*IPv4_address* | *IPv6_address*}：単一のホストの 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-object** {*IPv4_address IPv4_mask* | *IPv6_address*/*IPv6_prefix*}：ネットワークのアドレスまたはホスト。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。
- **network-object object** *object_name*：既存のネットワーク オブジェクトの名前。
- **group-object** *object_group_name*：既存のネットワーク オブジェクト グループの名前。

例

```
ciscoasa(config-network-object-group)# network-object 10.1.1.0 255.255.255.0
ciscoasa(config-network-object-group)# network-object 2001:db8:0:cd30::/60
ciscoasa(config-network-object-group)# network-object host 10.1.1.1
ciscoasa(config-network-object-group)# network-object host 2001:DB8::0DB8:800:200C:417A
ciscoasa(config-network-object-group)# network-object object existing-object-1
ciscoasa(config-network-object-group)# group-object existing-network-object-group
```

ステップ 3　（オプション）説明を追加します。

```
ciscoasa(config-network-object-group)# description string
```

例

3 人の管理者の IP アドレスを含むネットワーク グループを作成するには、次のコマンドを入力します。

```
hostname (config)# object-group network admins
hostname (config-protocol)# description Administrator Addresses
hostname (config-protocol)# network-object host 10.2.2.4
hostname (config-protocol)# network-object host 10.2.2.78
hostname (config-protocol)# network-object host 10.2.2.34
```

次のコマンドを入力して、さまざまな部門に所属する特権ユーザのネットワーク オブジェクト グループを作成します。

```
hostname (config)# object-group network eng
hostname (config-network)# network-object host 10.1.1.5
hostname (config-network)# network-object host 10.1.1.9
hostname (config-network)# network-object host 10.1.1.89

hostname (config)# object-group network hr
hostname (config-network)# network-object host 10.1.2.8
hostname (config-network)# network-object host 10.1.2.12

hostname (config)# object-group network finance
hostname (config-network)# network-object host 10.1.4.89
hostname (config-network)# network-object host 10.1.4.100
```

その後、3 つすべてのグループを次のようにネストします。

```
hostname (config)# object-group network admin
hostname (config-network)# group-object eng
hostname (config-network)# group-object hr
hostname (config-network)# group-object finance
```

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.16-5）
- 「サービス グループの設定」（P.16-6）

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　オブジェクト名を使用して、サービス オブジェクトを作成または編集します。

```
ciscoasa(config)# object service object_name
```

例

```
ciscoasa(config)# object service web
```

ステップ 2　次のいずれかのコマンドを使用して、オブジェクトにサービスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **service** *protocol*：IP プロトコルの名前または番号（0 ～ 255）。**ip** を指定すると、すべてのプロトコルに適用されます。サポートされるキーワードの一覧については、「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。
- **service** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]]：ICMP または ICMP バージョン 6 のメッセージ用。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.43-16）を参照してください。
- **service** {**tcp** | **udp**} [**source** *operator port*] [**destination** *operator port*]：TCP または UDP 用。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）。operator には次のいずれかを指定できます。
  - **lt**：小なり。
  - **gt**：大なり。
  - **eq**：等しい。
  - **neq**：等しくない。
  - **range**：値の包括的な範囲。この演算子を使用する場合は、2 つのポート番号を指定します（例：**range 100 200**）。

例

```
ciscoasa(config-service-object)# service tcp destination eq http
```

ステップ 3　（オプション）説明を追加します。

```
ciscoasa(config-service-object)# description string
```

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　オブジェクト名を使用して、サービス オブジェクト グループを作成または編集します。

```
ciscoasa(config)# object-group service group_name
```

例

```
ciscoasa(config)# object-group service general-services
```

ステップ 2　次のコマンドの 1 つまたは複数を使用して、サービス オブジェクト グループにオブジェクトとサービスを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **service-object** *protocol*：IP プロトコルの名前または番号（0 ～ 255）。**ip** を指定すると、すべてのプロトコルに適用されます。サポートされるキーワードの一覧については、「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。
- **service-object** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]]：ICMP または ICMP バージョン 6 のメッセージ用。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.43-16）を参照してください。
- **service-object** {**tcp** | **udp** | **tcp-udp**} [**source** *operator port*] [**destination** *operator port*]：TCP、UDP、またはその両方用。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）。operator には次のいずれかを指定できます。
  - **lt**：小なり。
  - **gt**：大なり。
  - **eq**：等しい。
  - **neq**：等しくない。
  - **range**：値の包括的な範囲。この演算子を使用する場合は、2 つのポート番号を指定します（例：**range 100 200**）。
- **service-object object** *object_name*：既存のサービス オブジェクトの名前。
- **group-object** *object_group_name*：既存のサービス オブジェクト グループの名前。

例

```
ciscoasa(config-service-object-group)# service-object ipsec
ciscoasa(config-service-object-group)# service-object tcp destination eq domain
ciscoasa(config-service-object-group)# service-object icmp echo
ciscoasa(config-service-object-group)# service-object object my-service
ciscoasa(config-service-object-group)# group-object Engineering_groups
```

ステップ 3　（オプション）説明を追加します。

```
ciscoasa(config-service-object-group)# description string
```

例

次の例では、TCP と UDP の両方のサービスを同じサービス オブジェクト グループに追加する方法を示します。

```
ciscoasa(config)# object-group service CommonApps
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq h323
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
```

次の例では、複数のサービス オブジェクトを同じサービス オブジェクト グループに追加する方法を示します。

```
ciscoasa(config)# object service SSH
ciscoasa(config-service-object)# service tcp destination eq ssh
ciscoasa(config)# object service EIGRP
ciscoasa(config-service-object)# service eigrp
ciscoasa(config)# object service HTTPS
ciscoasa(config-service-object)# service tcp source range 1 1024 destination eq https
ciscoasa(config)# object-group service Group1
ciscoasa(config-service-object-group)# service-object object SSH
ciscoasa(config-service-object-group)# service-object object EIGRP
ciscoasa(config-service-object-group)# service-object object HTTPS
```

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 31 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　オブジェクト名を使用して、ユーザ オブジェクト グループを作成または編集します。

```
ciscoasa(config)# object-group user group_name
```

例

```
ciscoasa(config)# object-group user admins
```

ステップ 2　次のコマンドの 1 つまたは複数を使用して、ユーザ オブジェクト グループにユーザとグループを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **user** [*domain_NETBIOS_name*\]*username*：ユーザ名。ドメイン名またはユーザ名にスペースが含まれている場合は、ドメイン名とユーザ名を引用符で囲む必要があります。ドメイン名には、LOCAL（ローカル データベースで定義されているユーザ向け）、または **user-identity domain** *domain_NetBIOS_name* **aaa-server** *aaa_server_group_tag* コマンドで指定されている Active Directory（AD）のドメイン名を指定できます。AD ドメインに定義されているユーザを追加する場合、*user_name* には、一意ではない可能性がある Common Name（CN）ではなく、一意の Active Directory sAMAccountName を指定する必要があります。ドメイン名を指定しない場合、デフォルト値が使用されます。デフォルト値は、LOCAL または **user-identity default-domain** コマンドで定義されている値のいずれかです。
- **user-group** [*domain_NETBIOS_name*\\]*username*：ユーザ グループ。ドメイン名またはグループ名にスペースが含まれている場合は、ドメイン名とグループ名を引用符で囲む必要があります。ドメイン名とグループ名を区切る二重の \\ に注意してください。
- **group-object** *object_group_name*：既存のユーザ オブジェクト グループの名前。

例

```
ciscoasa(config-user-object-group)# user EXAMPLE\admin
ciscoasa(config-user-object-group)# user-group EXAMPLE\\managers
ciscoasa(config-user-object-group)# group-object local-admins
```

ステップ 3　（オプション）説明を追加します。

```
ciscoasa(config-user-object-group)# description string
```

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 32 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　オブジェクト名を使用して、セキュリティ グループ オブジェクト グループを作成または編集します。

```
ciscoasa(config)# object-group security group_name
```

例

```
ciscoasa(config)# object-group security mktg-sg
```

ステップ 2　次のコマンドの 1 つまたは複数を使用して、サービス グループ オブジェクト グループにオブジェクトを追加します。オブジェクトを削除するには、コマンドの **no** 形式を使用します。

- **security-group** {**tag** *sgt_number* | **name** *sg_name*}：セキュリティ グループ タグ（SGT）または名前。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。

- **group-object** *object_group_name*：既存のセキュリティ グループ オブジェクト グループの名前。

例

```
ciscoasa(config-security-object-group)# security-group tag 1
ciscoasa(config-security-object-group)# security-group name mgkt
ciscoasa(config-security-object-group)# group-object local-sg
```

ステップ 3　（オプション）説明を追加します。

```
ciscoasa(config-security-object-group)# description string
```

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　時間範囲を作成します。

```
time-range name
```

ステップ 2　（オプション）時間範囲に開始時刻または終了時刻（または両方）を追加します。

```
absolute [start time date] [end time date]
```

開始時刻を指定しない場合、現在の時刻がデフォルトの開始時刻になります。

time は 24 時間形式（*hh*:*mm*）で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 と指定します。

date は *day month year* の形式で指定します（たとえば、**1 January 2014**）。

ステップ 3　（オプション）繰り返しの期間を追加します。

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

days-of-the-week には次の値を指定できます。最初の引数に曜日を 1 つ指定した場合にのみ、2 番目の曜日を指定できることに注意してください。

- **Monday**、**Tuesday**、**Wednesday**、**Thursday**、**Friday**、**Saturday**、または **Sunday**。最初の *days-of-the-week* 引数には、複数の曜日をスペースで区切って指定できます。
- **daily**
- **weekdays**
- **weekend**

time は 24 時間形式（*hh*:*mm*）で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 と指定します。

このコマンドを繰り返して、複数の繰り返し期間を設定できます。

例

次に、2006 年 1 月 1 日の午前 8 時に始まる絶対的な時間範囲の例を示します。終了時刻も終了日も指定されていないため、時間範囲は事実上無期限になります。

```
ciscoasa(config)# time-range for2006
ciscoasa(config-time-range)# absolute start 8:00 1 january 2006
```

次に、平日の午前 8 時～午後 6 時に毎週繰り返される定期的な時間範囲の例を示します。

```
ciscoasa(config)# time-range workinghours
ciscoasa(config-time-range)# periodic weekdays 8:00 to 18:00
```

次の例では、時間範囲の終了日を設定し、平日の期間を午前 8 時から 午後 5 時に設定します。さらに火曜日、木曜日と比較して、月曜日、水曜日、金曜日には 5 時以降に異なる時間を設定します。

```
asa4(config)# time-range contract-A-access
asa4(config-time-range)# absolute end 12:00 1 September 2025
asa4(config-time-range)# periodic weekdays 08:00 to 17:00
asa4(config-time-range)# periodic Monday Wednesday Friday 18:00 to 20:00
asa4(config-time-range)# periodic Tuesday Thursday 17:30 to 18:30
```

オブジェクトのモニタリング

オブジェクトおよびグループをモニタするには、次のコマンドを入力します。

- **show access-list**

  アクセス リストのエントリを表示します。オブジェクトを含むエントリは、オブジェクトのコンテンツに基づいて個々のエントリへも拡大しています。

- **show running-config object** [**id** *object_id*]

  現在のすべてのオブジェクトを表示します。**id** キーワードを使用すると、単一のオブジェクトを名前別に表示できます。

- **show running-config object** *object_type*

  現在のオブジェクトをタイプ、ネットワーク、またはサービス別に表示します。

- **show running-config object-group** [**id** *group_id*]

  現在のすべてのオブジェクト グループを表示します。**id** キーワードを使用すると、単一のオブジェクト グループを名前別に表示できます。

- **show running-config object-group** *grp_type*

  現在のオブジェクト グループをグループ タイプごとに表示します。

オブジェクトの履歴

機能名	プラットフォーム 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。 **object-group** *protocol*、**object-group** *network*、**object-group** *service*、**object-group** *icmp_type* コマンドを導入または変更しました。
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。 **object-network**、**object-service**、**object-group** *network*、**object-group** *service*、**network object**、**access-list extended**、**access-list webtype**、**access-list remark** の各コマンドが導入または変更されました。
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。 **object-network user**、**user** の各コマンドが導入されました。
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。 **object-network security**、**security** の各コマンドが導入されました。

機能名	プラットフォーム リリース	説明
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。 **object-group network** コマンドが変更されました。
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。 **access-list extended**、**service-object**、**service** の各コマンドが導入または変更されました。

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」（P.17-1）
- 「ACL のガイドライン」（P.17-5）
- 「ACL の設定」（P.17-6）
- 「ACL のモニタリング」（P.17-20）
- 「ACL の履歴」（P.17-20）

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。「拡張 ACL の設定」（P.17-7）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。「EtherType ACL の設定」（P.17-19）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.17-15）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.17-14）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 17-1　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 35 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 標準	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。
ルート フィルタリングおよび再配布の特定	標準 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 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。

拡張 ACL では、**access-list** コマンドで **line** *number* パラメータを使用して適切な場所にルールを挿入します。どの番号を使用すればよいか判断できるように ACL エントリとその行番号を表示するには、**show access-list** *name* コマンドを使用します。その他のタイプの ACL の場合は、ACL を作成（できれば ASDM を使用）して ACE の順序を変更します。

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

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を使用すると、NAT の設定が変更されても ACL を変更する必要はありません。

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。

```
ciscoasa(config)# object network server1
ciscoasa(config-network-object)# host 10.1.1.5
ciscoasa(config-network-object)# nat (inside,outside) static 209.165.201.5

ciscoasa(config)# access-list OUTSIDE extended permit tcp any host 10.1.1.5 eq www
ciscoasa(config)# access-group OUTSIDE in interface outside
```

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

時間ベース 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.16-10）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 ACL の設定方法について説明します。まず ACL の基本に関するセクションを読んで全体像を把握し、次に特定のタイプの ACL に関するセクションを読んで詳細を確認してください。

- 「基本的な ACL 設定および管理オプション」（P.17-6）
- 「拡張 ACL の設定」（P.17-7）
- 「標準 ACL の設定」（P.17-14）
- 「Webtype ACL の設定」（P.17-15）
- 「EtherType ACL の設定」（P.17-19）

基本的な ACL 設定および管理オプション

1 つの ACL は、同じ ACL ID または ACL 名を持つ 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。新しい ACL を作成するには、新しい ACL 名で ACE を作成します。作成した ACE は、新しい ACL の最初のルールになります。

ACL の操作では、次のことを実行できます。

- **ACL の内容を調べ、行番号とヒット カウントを確認する**：ACL の内容を表示するには、**show access-list** *name* コマンドを使用します。各行は ACE で、行番号を含みます。行番号は、拡張 ACL に新しいエントリを挿入する場合に知っておく必要があります。情報には、各 ACE のヒット カウントも含まれます。ヒット カウントは、トラフィックがルールに一致した回数です。次に例を示します。

```
ciscoasa# show access-list outside_access_in
access-list outside_access_in; 3 elements; name hash: 0x6892a938
access-list outside_access_in line 1 extended permit ip 10.2.2.0 255.255.255.0 any
(hitcnt=0) 0xcc48b55c
access-list outside_access_in line 2 extended permit ip host
2001:DB8::0DB8:800:200C:417A any (hitcnt=0) 0x79797f94
```

```
access-list outside_access_in line 3 extended permit ip user-group LOCAL\\usergroup
any any (hitcnt=0) 0xb0f5b1e1
```

- **ACE を追加する**：ACE を追加するためのコマンドは **access-list** *name* [**line** *line-num*] *type parameters* です。行番号引数は、拡張 ACL でのみ使用できます。行番号を指定すると、ACE は ACL のその場所に挿入されます。その場所にあった ACE は、残りの ACE とともに下に移動します（つまり、ある行番号の位置に ACE を挿入しても、その行にあった古い ACE は置き換えられません）。行番号を指定しない場合、ACE は ACL の末尾に追加されます。使用可能なパラメータは、ACL のタイプによって異なります。詳細については、各 ACL タイプのトピックを参照してください。
- **コメントを追加する（Webtype 以外のすべてのタイプ）**：ACE の目的を説明するのに役立つ注釈を ACL に追加するには、**access-list** *name* [**line** *line-num*] **remark** *text* コマンドを使用します。ベスト プラクティスは、ACE の前に注釈を挿入することです。ASDM で設定を表示すると、注釈は、その注釈に続く ACE に関連付けられます。ACE の前に複数の注釈を入力してコメントを拡張できます。各注釈は 100 文字に制限されます。先頭にスペースを置いて注釈を強調することができます。行番号を指定しない場合、注釈は ACL の末尾に追加されます。たとえば、各 ACE を追加する前に注釈を追加できます。

```
ciscoasa(config)# access-list OUT remark - this is the inside admin address
ciscoasa(config)# access-list OUT extended permit ip host 209.168.200.3 any
ciscoasa(config)# access-list OUT remark - this is the hr admin address
ciscoasa(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

- **ACE または注釈を編集または移動する**：ACE または注釈を編集または移動することはできません。代わりに、目的の値を持つ新しい ACE または注釈を（行番号を使用して）適切な場所に作成してから、古い ACE または注釈を削除します。ACE を挿入できるのは拡張 ACL だけなので、標準、Webtype、または EtherType の ACL の ACE を編集または移動する必要がある場合は、それらのタイプの ACL を再作成する必要があります。これは ASDM を使用して長い ACL を再編成するよりもはるかに簡単です。
- **ACE または注釈を削除する**：ACE または注釈を削除するには、**no access-list** *parameters* コマンドを使用します。入力する必要があるパラメータ文字列を表示するには、**show access-list** コマンドを使用します。この文字列は、削除する ACE または注釈に正確に一致する必要があります。ただし、**line** *line-num* 引数は除きます。この引数は、**no access-list** コマンドのオプションです。
- **コメントを含む ACL 全体を削除する**：**clear configure access-list** *name* コマンドを使用します。注意してください。このコマンドでは、確認は求められません。名前を指定しない場合、ASA のすべてのアクセス リストが削除されます。
- **ACL の名前を変更する**：**access-list** *name* **rename** *new_name* コマンドを使用します。
- **ポリシーに ACL を適用する**：ACL を作成しただけでは、トラフィックには何の処理も実行されません。ポリシーに ACL を適用する必要があります。たとえば、**access-group** コマンドを使用してインターフェイスに拡張 ACL を適用すると、このインターフェイスを通過するトラフィックを拒否または許可できます。ACL の使用例については、「ACL タイプ」（P.17-1）を参照してください。

拡張 ACL の設定

拡張 ACL は、同じ ACL ID または ACL 名を持つすべての ACE で構成されます。拡張 ACL は、最も複雑で機能豊富な ACL タイプで、さまざまな機能に使用できます。拡張 ACL の最も注目すべき用途は、グローバルに、またはインターフェイスに適用され、デバイスを通過するのを拒否または許可されるトラフィックを決定するアクセス グループとしての使用です。ただし、拡張 ACL は、その他のサービスの適用対象のトラフィックを決定するのにも使用されます。

拡張 ACL は複雑であるため、次の各セクションでは、ACE を作成して特定のタイプのトラフィック照合を提供することに焦点を当てます。最初のセクションでは、基本的なアドレスベースの ACE と TCP/UDP ACE について説明し、残りのセクションの基礎を作ります。

- 「IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加」（P.17-8）
- 「ポートを使用した TCP または UDP ベースの照合に使用する拡張 ACE の追加」（P.17-10）
- 「ICMP ベースの照合に使用する拡張 ACE の追加」（P.17-10）
- 「ユーザベースの照合（アイデンティティ ファイアウォール）に使用する拡張 ACE の追加」（P.17-11）
- 「セキュリティ グループ ベースの照合（Cisco TrustSec）に使用する拡張 ACE の追加」（P.17-12）
- 「拡張 ACL の例」（P.17-13）
- 「アドレスを拡張 ACL のオブジェクトに変換する例」（P.17-14）

IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加

基本的な拡張 ACE では、IPv4 および IPv6 アドレスや、www.example.com などの完全修飾ドメイン名（FQDN）を含む送信元アドレスと宛先アドレスに基づいてトラフィックを照合します。実際、どのタイプの拡張 ACE にも、送信元アドレスと宛先アドレスに関する詳細を含める必要があります。したがって、このトピックでは、最小限の拡張 ACE について説明します。

ヒント　FQDN に基づいてトラフィックを照合する場合は、各 FQDN を表すネットワーク オブジェクトを作成する必要があります。

IP アドレスまたは FQDN 照合に使用する ACE を追加するには、次のコマンドを使用します。

```
access-list access_list_name [line line_number] extended {deny | permit}
protocol_argument source_address_argument dest_address_argument
[log [[level] [interval secs] | disable | default]]
[time-range time_range_name]
[inactive]
```

例：

```
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

次のオプションがあります。

- *access_list_name*：新規または既存の ACL の名前。
- 行番号：**line** *line_number* オプションでは、ACE を挿入する位置の行番号を指定します。指定しない場合は、ACL の末尾に追加されます。
- 許可または拒否：**deny** キーワードを指定すると、条件に一致した場合にパケットが拒否または免除されます。**permit** キーワードを指定すると、条件に一致した場合にパケットが許可または包含されます。
- プロトコル：*protocol_argument* では、IP プロトコルを指定します。
  - *name* または *number*：プロトコルの名前または番号を指定します。**ip** を指定すると、すべてのプロトコルに適用されます。サポートされるキーワードの一覧については、「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。

  - **object-group** *protocol_grp_id*：**object-group protocol** コマンドを使用して作成されたプロトコル オブジェクト グループを指定します。「サービス オブジェクトとサービス グループの設定」（P.16-4）を参照してください。
  - **object** *service_obj_id*：**object service** コマンドを使用して作成されたサービス オブジェクトを指定します。TCP、UDP、または ICMP のサービス オブジェクトには、プロトコルに加えて、送信元や宛先のポートまたは ICMP タイプとコードも入れることができます。
  - **object-group** *service_grp_id*：**object-group service** コマンドを使用して作成されたサービス オブジェクト グループを指定します。
- 送信元アドレス、宛先アドレス：*source_address_argument* ではパケットの送信元の IP アドレスまたは FQDN を指定し、*dest_address_argument* ではパケットの送信先の IP アドレスまたは FQDN を指定します。
  - **host** *ip_address*：IPv4 ホスト アドレスを指定します。
  - *ip_address mask*：10.100.10.0 255.255.255.0 などの IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。
  - *ipv6-address/prefix-length*：IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。
  - **any**、**any4**、**any6**：**any** は IPv4 と IPv6 の両方のトラフィックを表し、**any4** は IPv4 トラフィックのみを表し、**any6** は IPv6 トラフィックのみを表します。
  - **interface** *interface_name*：ASA インターフェイスの名前を指定します。IP アドレスではなくインターフェイス名を使用し、どのインターフェイスがトラフィックの送信元または宛先であるかに基づいてトラフィックを照合します。
  - **object** *nw_obj_id*：**object network** コマンドを使用して作成されたネットワーク オブジェクトを指定します。「ネットワーク オブジェクトとグループの設定」（P.16-2）を参照してください。
  - **object-group** *nw_grp_id*：**object-group network** コマンドを使用して作成されたネットワーク オブジェクト グループを指定します。
- ロギング：**log** 引数では、ネットワーク アクセスに関して ACE に一致するパケットが見つかったとき（**access-group** コマンドで ACL が適用されます）のロギング オプションを設定します。引数を指定せずに **log** オプションを入力すると、syslog メッセージ 106100 はデフォルト レベル（6）とデフォルト間隔（300 秒）でイネーブルになります。ログ オプションは次のとおりです。
  - *level*：0 ～ 7 の重大度。デフォルトは 6（情報）です。アクティブな ACE でこのレベルを変更した場合、新しいレベルは新規接続に適用され、既存の接続は引き続き前のレベルでロギングされます。
  - **interval** *secs*：syslog メッセージ間の時間間隔（秒）。1 ～ 600 で指定します。デフォルト値は 300 です。この値は、ドロップ統計情報の収集に使用されるキャッシュからアクティブでないフローを削除するためのタイムアウト値としても使用されます。
  - **disable**：すべての ACE ロギングをディセーブルにします。
  - **default**：拒否されたパケットに関するメッセージ 106023 のロギングをイネーブルにします。この設定は、**log** オプションを指定しないのと同じです。
- 時間範囲：**time-range** *time_range_name* オプションでは、ACE がアクティブになっている時間帯と曜日を決定する時間範囲オブジェクトを指定します。時間範囲を指定しない場合、ACE は常にアクティブです。

- アクティベーション：ACE を削除せずにディセーブルにするには、**inactive** オプションを使用します。再度イネーブルにするには、inactive キーワードを使用せずに ACE 全体を入力します。

ポートを使用した TCP または UDP ベースの照合に使用する拡張 ACE の追加

TCP/UDP 拡張 ACE は、プロトコルが **tcp** または **udp** である基本的なアドレス照合 ACE です。これらのプロトコルではポートが使用されるため、ACE にポート仕様を追加できます。たとえば、TCP ポート 80 で HTTP トラフィックをターゲットにできます。

プロトコルが TCP または UDP である IP アドレスまたは FQDN 照合に使用する ACE を追加するには、次のコマンドを使用します。

```
access-list access_list_name [line line_number] extended {deny | permit}
{tcp | udp} source_address_argument [port_argument] dest_address_argument [port_argument]
[log [[level] [interval secs] | disable | default]]
[time-range time_range_name]
[inactive]
```

例：

```
ciscoasa(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
```

port_argument オプションでは、送信元ポートまたは宛先ポートを指定します。ポートを指定しない場合は、すべてのポートに一致します。使用可能な引数は次のとおりです。

- *operator port*：*operator* は次のいずれかです。
  - **lt**：より小さい
  - **gt**：より大きい
  - **eq**：等しい
  - **neq**：等しくない
  - **range**：値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。

    ```
    range 100 200
    ```

  port には、TCP または UDP ポートの番号（整数）または名前を指定できます。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。
- **object** *service_obj_id*：**object service** コマンドを使用して作成されたサービス オブジェクトを指定します。「サービス オブジェクトとサービス グループの設定」（P.16-4）を参照してください。
- **object-group** *service_grp_id*：**object-group service** コマンドを使用して作成されたサービス オブジェクト グループを指定します。

他のキーワードの説明については、「IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加」（P.17-8）を参照してください。

ICMP ベースの照合に使用する拡張 ACE の追加

ICMP 拡張 ACE は、プロトコルが **icmp** または **icmp6** である基本的なアドレス照合 ACE です。これらのプロトコルにはタイプおよびコード値があるため、ACE にタイプおよびコード仕様を追加できます。たとえば、ICMP エコー要求（ping）トラフィックをターゲットにできます。

プロトコルが ICMP または ICMP6 である IP アドレスまたは FQDN 照合に使用する ACE を追加するには、次のコマンドを使用します。

```
access-list access_list_name [line line_number] extended {deny | permit}
{icmp | icmp6} source_address_argument dest_address_argument [icmp_argument]
[log [[level] [interval secs] | disable | default]]
[time-range time_range_name]
[inactive]
```

例：

```
ciscoasa(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
ciscoasa(config)# access-list abc extended permit icmp any any echo
```

icmp_argument オプションでは、ICMP のタイプとコードを指定します。

- *icmp_type* [*icmp_code*]：ICMP タイプを名前または番号で指定し、そのタイプの ICMP コード（省略可能）を指定します。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.43-16）を参照してください。
- **object-group** *icmp_grp_id*：**object-group service** コマンドまたは（非推奨の）**object-group icmp** コマンドで作成された ICMP/ICMP6 のオブジェクト グループを指定します。

他のキーワードの説明については、「IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加」（P.17-8）を参照してください。

ユーザベースの照合（アイデンティティ ファイアウォール）に使用する拡張 ACE の追加

ユーザベースの拡張 ACE は、ユーザ名またはユーザ グループを送信元の一致条件に含める基本的なアドレス照合 ACE です。ユーザ ID に基づくルールを作成すると、ルールがスタティックなホストまたはネットワーク アドレスに縛られるのを回避できます。たとえば、user1 のルールを定義し、アイデンティティ ファイアウォール機能によってそのユーザがあるホストにマッピングされているとします。さらに、このホストにある日 10.100.10.3 が割り当てられ、その翌日に 192.168.1.5 が割り当てられたとします。この場合でも、ユーザベースのルールは適用されます。

送信元アドレスと宛先アドレスは引き続き指定する必要があります。そのため、送信元アドレスは、ユーザに（通常は DHCP 経由で）割り当てられる可能性があるアドレスが含まれるように広く設定してください。たとえば、ユーザ「LOCAL\user1 any」は、割り当てられているアドレスに関係なく LOCAL\user1 ユーザに一致しますが、「LOCAL\user1 10.100.1.0 255.255.255.0」は、アドレスが 10.100.1.0/24 ネットワーク上にある場合にのみユーザに一致します。

グループ名を使用すると、学生、教師、マネージャ、エンジニアなどユーザのクラス全体に基づいてルールを定義できます。

ユーザまたはグループ照合に使用する ACE を追加するには、次のコマンドを使用します。

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument
[user_argument] source_address_argument [port_argument]
dest_address_argument [port_argument]
[log [[level] [interval secs] | disable | default]]
[time-range time_range_name]
[inactive]
```

例：

```
ciscoasa(config)# access-list v1 extended permit ip user LOCAL\idfw
any 10.0.0.0 255.255.255.0
```

user_argument オプションでは、送信元アドレスに加えて、トラフィックを照合するユーザまたはグループを指定します。使用可能な引数は次のとおりです。

- **object-group-user** *user_obj_grp_id* : **object-group user** コマンドを使用して作成されたユーザ オブジェクト グループを指定します。
- **user** {[*domain_nickname*\]*name* | **any** | **none**} : ユーザ名を指定します。ユーザ資格情報を持つすべてのユーザに一致させるには、**any** を選択します。ユーザ名にマッピングされていないアドレスに一致させるには、**none** を選択します。これらのオプションが特に役立つのは、**access-group** と **aaa authentication match** のポリシーを結合する場合です。
- **user-group** [*domain_nickname*\\]*user_group_name* : ユーザ グループ名を指定します。\\ はドメインとグループ名の区切りです。

他のキーワードの説明については、「IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加」（P.17-8）を参照してください。

ヒント　特定の ACE にユーザと Cisco Trustsec セキュリティ グループの両方を含めることができます。「セキュリティ グループ ベースの照合（Cisco TrustSec）に使用する拡張 ACE の追加」（P.17-12）を参照してください。

セキュリティ グループ ベースの照合（Cisco TrustSec）に使用する拡張 ACE の追加

セキュリティ グループ拡張 ACE は、セキュリティ グループまたはタグを送信元または宛先の一致条件に含める基本的なアドレス照合 ACE です。セキュリティ グループに基づくルールを作成すると、ルールがスタティックなホストまたはネットワーク アドレスに縛られるのを回避できます。送信元アドレスと宛先アドレスは引き続き指定する必要があります。そのため、アドレスは、ユーザに（通常は DHCP 経由で）割り当てられる可能性があるアドレスが含まれるように広く設定してください。

ヒント　このタイプの ACE を追加する前に、第 32 章「ASA と Cisco TrustSec」の説明に従って Cisco TrustSec 設定してください。

セキュリティ グループ照合に使用する ACE を追加するには、次のコマンドを使用します。

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument
[security_group_argument] source_address_argument [port_argument]
[security_group_argument] dest_address_argument [port_argument] [log [[level]
[interval secs] | disable | default]] [inactive | time-range time_range_name]
```

例：

```
ciscoasa(config)# access-list INSIDE_IN extended permit ip
security-group name my-group any any
```

security_group_argument オプションでは、送信元または宛先アドレスに加えて、トラフィックを照合するセキュリティ グループを指定します。使用可能な引数は次のとおりです。

- **object-group-security** *security_obj_grp_id* : **object-group security** コマンドを使用して作成されたセキュリティ オブジェクト グループを指定します。
- **security-group** {**name** *security_grp_id* | **tag** *security_grp_tag*} : セキュリティ グループの名前またはタグを指定します。

他のキーワードの説明については、「IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加」（P.17-8）を参照してください。

ヒント　特定の ACE にユーザと Cisco Trustsec セキュリティ グループの両方を含めることができます。「ユーザベースの照合（アイデンティティ ファイアウォール）に使用する拡張 ACE の追加」（P.17-11）を参照してください。

拡張 ACL の例

次に示す ACL は ASA を通るすべてのホスト（ACL を適用するインターフェイス上の）を許可します。

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

次の ACL は、192.168.1.0/24 のホストが TCP ベースのトラフィックで 209.165.201.0/27 のネットワークにアクセスすることを拒否します。その他のアドレスはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

選択したホストだけにアクセスを制限する場合は、限定的な許可 ACE を入力します。デフォルトでは、明示的に許可しない限り、他のトラフィックはすべて拒否されます。

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

次の ACL では、すべてのホスト（この ACL を適用するインターフェイス上の）からアドレス 209.165.201.29 の Web サイトへのアクセスを禁止しています。他のトラフィックはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

オブジェクト グループを使用する次のアクセス リストでは、内部ネットワーク上のさまざまなホストについて、さまざまな Web サーバへのアクセスを禁止しています。他のトラフィックはすべて許可されます。

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

次の例では、あるネットワーク オブジェクト グループ（A）から別のネットワーク オブジェクト グループ（B）へのトラフィックを許可する ACL を一時的にディセーブルにします。

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

時間ベース ACE を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended** コマンドを使用して、時間範囲を ACE にバインドします。次の例では、「Sales」ACL の ACE を「New_York_Minute」という時間範囲にバインドしています。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
```

次の例では、IPv4/IPv6 混在 ACL が表示されています。

```
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 10.2.2.0
255.255.255.0
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 2001:DB8:2::/64
hostname(config)# access-list demoacl extended permit ip host 10.3.3.3 host 10.4.4.4
```

アドレスを拡張 ACL のオブジェクトに変換する例

次に示す、オブジェクト グループを使用しない通常の ACL では、内部ネットワーク上のさまざまなホストについて、さまざまな Web サーバへのアクセスを禁止しています。他のトラフィックはすべて許可されます。

```
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.29
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.29
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.29
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.16
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.16
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.16
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.78
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.78
eq www
ciscoasa(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.78
eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
ciscoasa(config)# access-group ACL_IN in interface inside
```

2 つのネットワーク オブジェクト グループ（内部ホスト用に 1 つ、Web サーバ用に 1 つ）を作成すると、コンフィギュレーションが簡略化され、簡単に修正してホストを追加できるようになります。

```
ciscoasa(config)# object-group network denied
ciscoasa(config-network)# network-object host 10.1.1.4
ciscoasa(config-network)# network-object host 10.1.1.78
ciscoasa(config-network)# network-object host 10.1.1.89

ciscoasa(config-network)# object-group network web
ciscoasa(config-network)# network-object host 209.165.201.29
ciscoasa(config-network)# network-object host 209.165.201.16
ciscoasa(config-network)# network-object host 209.165.201.78

ciscoasa(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
ciscoasa(config)# access-group ACL_IN in interface inside
```

標準 ACL の設定

標準 ACL は、同じ ACL ID または ACL 名を持つすべての ACE で構成されます。標準 ACL は、ルート マップや VPN フィルタなどの限られた数の機能に使用されます。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。

標準アクセス リスト エントリを追加するには、次のコマンドを使用します。

```
ciscoasa(config)# access-list access_list_name standard {deny | permit}
{any4 | host ip_address | ip_address mask}
```

例：

```
ciscoasa(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

次のオプションがあります。

- 名前：*access_list_name* 引数には、ACL の名前または番号を指定します。標準 ACL の従来の数値は 1 ～ 99 または 1300 ～ 1999 ですが、任意の名前または数値を使用できます。ACL がまだ存在しない場合は、新しい ACL を作成します。ACL が存在する場合、エントリは ACL の末尾に追加されます。
- 許可または拒否：**deny** キーワードを指定すると、条件に一致した場合にパケットが拒否または免除されます。**permit** キーワードを指定すると、条件に一致した場合にパケットが許可または包含されます。
- 宛先アドレス：**any4** キーワードは、すべての IPv4 アドレスに一致します。**host** *ip_address* 引数は、ホストの IPv4 アドレスに一致します。*ip_address ip_mask* 引数は、IPv4 サブネット（10.1.1.0 255.255.255.0 など）に一致します。

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、同じ ACL ID または ACL 名を持つすべての ACE で構成されます。

Webtype ACL では、URL または宛先アドレスに基づいてトラフィックを照合できます。単一の ACE でこれらの仕様を組み合わせることはできません。次の各セクションでは、各タイプの ACE について説明します。

- 「URL 照合に使用する Webtype ACE の追加」（P.17-15）
- 「IP アドレス照合に使用する Webtype ACE の追加」（P.17-17）
- 「Webtype ACL の例」（P.17-17）

URL 照合に使用する Webtype ACE の追加

ユーザがアクセスしようとしている URL に基づいてトラフィックを照合するには、次のコマンドを使用します。

```
access-list access_list_name webtype {deny | permit} url {url_string | any}
[log [[level] [interval secs] | disable | default]]
[time_range time_range_name]]
[inactive]
```

例：

```
ciscoasa(config)# access-list acl_company webtype deny url http://*.example.com
```

次のオプションがあります。

- *access_list_name*：新規または既存の ACL の名前。ACL がすでに存在する場合は、ACL の末尾に ACE が追加されます。
- 許可または拒否：**deny** キーワードを指定すると、条件に一致した場合にパケットが拒否または免除されます。**permit** キーワードを指定すると、条件に一致した場合にパケットが許可または包含されます。

- URL：**url** キーワードでは、照合する URL を指定します。すべての URL ベースのトラフィックに一致させるには、**url any** を使用します。そうでない場合は、URL 文字列を入力します。URL 文字列には、ワイルドカードを含めることができます。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** を指定します。
  - 「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。
- ロギング：**log** 引数では、パケットが ACE に一致した場合のロギング オプションを設定します。引数を指定せずに **log** オプションを入力すると、syslog メッセージ 106102 はデフォルト レベル（6）とデフォルト間隔（300 秒）でイネーブルになります。ログ オプションは次のとおりです。
  - *level*：0 ～ 7 の重大度。デフォルト値は 6 です。
  - **interval** *secs*：syslog メッセージ間の時間間隔（秒）。1 ～ 600 で指定します。デフォルト値は 300 です。
  - **disable**：すべての ACL ロギングをディセーブルにします。
  - **default**：メッセージ 106103 のロギングをイネーブルにします。この設定は、**log** オプションを指定しないのと同じです。
- 時間範囲：**time-range** *time_range_name* オプションでは、ACE がアクティブになっている時間帯と曜日を決定する時間範囲オブジェクトを指定します。時間範囲を指定しない場合、ACE は常にアクティブです。
- アクティベーション：ACE を削除せずにディセーブルにするには、**inactive** オプションを使用します。再度イネーブルにするには、inactive キーワードを使用せずに ACE 全体を入力します。

IP アドレス照合に使用する Webtype ACE の追加

ユーザがアクセスしようとしている宛先アドレスに基づいてトラフィックを照合するには、次のコマンドを使用します。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。

IP アドレス照合に使用する Webtype ACE を追加するには、次のコマンドを使用します。

```
access-list access_list_name webtype {deny | permit}
tcp dest_address_argument [operator port]
[log [[level] [interval secs] | disable | default]]
[time_range time_range_name]]
[inactive]
```

例：

```
ciscoasa(config)# access-list acl_company webtype permit tcp any
```

ここで説明していないキーワードの説明については、「URL 照合に使用する Webtype ACE の追加」（P.17-15）を参照してください。このタイプの ACE に固有のキーワードと引数は次のとおりです。

- **tcp**：TCP プロトコル。Webtype ACL では、TCP トラフィックのみを照合します。
- 宛先アドレス：*dest_address_argument* では、パケットの送信先の IP アドレスを指定します。
  - **host** *ip_address*：IPv4 ホスト アドレスを指定します。
  - *dest_ip_address mask*：10.100.10.0 255.255.255.0 などの IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。
  - *ipv6-address/prefix-length*：IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。
  - **any**、**any4**、**any6**：**any** は IPv4 と IPv6 の両方のトラフィックを表し、**any4** は IPv4 トラフィックのみを表し、**any6** は IPv6 トラフィックのみを表します。
- *operator port*：宛先ポート。ポートを指定しない場合は、すべてのポートに一致します。*operator* には次のいずれかを指定できます。
  - **lt**：より小さい
  - **gt**：より大きい
  - **eq**：等しい
  - **neq**：等しくない
  - **range**：値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。

    ```
    range 100 200
    ```

  port には、TCP ポートの整数または名前を指定できます。

Webtype ACL の例

次の例は、特定の企業の URL へのアクセスを拒否する方法を示しています。

```
ciscoasa(config)# access-list acl_company webtype deny url http://*.example.com
```

次の例は、特定の Web ページへのアクセスを拒否する方法を示しています。

```
ciscoasa(config)# access-list acl_file webtype deny url
https://www.example.com/dir/file.html
```

次の例は、特定のサーバ上の任意の URL へのポート 8080 経由の HTTP アクセスを拒否する方法を示しています。

```
ciscoasa(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

次の例は、Webtype ACL でワイルドカードを使用する方法を示しています。

- 次に、http://www.example.com/layouts/1033 などの URL に一致させる例を示します。

  ```
  access-list VPN-Group webtype permit url http://www.example.com/*
  ```

- 次に、http://www.example.com/ や http://www.example.net/ などの URL に一致させる例を示します。

  access-list test webtype permit url http://www.example.*

- 次に、http://www.example.com や ftp://wwz.example.com などの URL に一致させる例を示します。

  ```
  access-list test webtype permit url *://ww?.e*co*/
  ```

- 次の例は、http://www.cisco.com:80 や https://www.cisco.com:81 などの URL に一致します。

  ```
  access-list test webtype permit url *://ww?.c*co*:8[01]/
  ```

  上記の例の範囲演算子「[ ]」は、文字 **0** または **1** がその場所で出現する可能性があることを示しています。

- 次に、http://www.example.com や http://www.example.net などの URL に一致させる例を示します。

  ```
  access-list test webtype permit url http://www.[a-z]xample?*/
  ```

  上記の例の範囲演算子「[ ]」は、**a** ～ **z** の任意の文字が出現する可能性があることを示しています。

- 次に、ファイル名またはパスのどこかに「cgi」が含まれる http または https URL に一致させる例を示します。

  ```
  access-list test webtype permit url htt*://*/*cgi?*
  ```

（注） すべての http URL に一致させるには、「 http://*」ではなく「**http://*/***」と入力する必要があります。

次の例は、Webtype ACL を適用して、特定の CIFS 共有へのアクセスをディセーブルにする方法を示しています。

このシナリオでは、「shares」というルート フォルダに「Marketing_Reports」および「Sales_Reports」という 2 つのサブフォルダが格納されており、「shares/Marketing_Reports」フォルダへのアクセスを明示的に拒否しようとしています。

```
access-list CIFS_Avoid webtype deny url cifs://172.16.10.40/shares/Marketing_Reports.
```

ただし、ACL の末尾に暗黙的な「deny all」があるため、上記の ACL を指定すると、ルート フォルダ（「shares」）とすべてのサブ フォルダ（「shares/Sales Reports」と「shares/Marketing Reports」）にアクセスできなくなります。

この問題を修正するには、ルート フォルダと残りのサブフォルダへのアクセスを許可する新しい ACL を追加します。

```
access-list CIFS_Allow webtype permit url cifs://172.16.10.40/shares*
```

EtherType ACL の設定

EtherType ACL は、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、ASA を通過する非 IP トラフィック フローを制御できます。802.3 形式フレームでは、type フィールドではなく length フィールドが使用されるため、ACL では処理されません。

EtherType ACE を追加するには、次のコマンドを使用します。

access-list *access_list_name* **ethertype** {**deny** | **permit**}
{**ipx** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **isis** | **any** | *hex_number*}

例：

```
ciscoasa(config)# access-list ETHER ethertype deny ipx
```

次のオプションがあります。

- *access_list_name*：新規または既存の ACL の名前。ACL がすでに存在する場合は、ACL の末尾に ACE が追加されます。
- 許可または拒否：**deny** キーワードを指定すると、条件に一致した場合にパケットが拒否されます。**permit** キーワードは、条件が一致した場合にパケットを許可します。
- トラフィック一致条件：次のオプションを使用してトラフィックを照合できます。
  - **ipx**：Internetwork Packet Exchange（IPX）。
  - **bpdu**：デフォルトで許可されるブリッジ プロトコル データ ユニット。
  - **mpls-multicast**：MPLS マルチキャスト。
  - **mpls-unicast**：MPLS ユニキャスト。
  - **isis**：Intermediate System to Intermediate System（IS-IS）。
  - **any**：すべてのトラフィックに一致します。
  - *hex_number*：16 ビットの 16 進数 0x600 ～ 0xffff で指定できる任意の EtherType。EtherType のリストについては、http://www.ietf.org/rfc/rfc1700.txt にアクセスして、RFC 1700「Assigned Numbers」を参照してください。

EtherType ACL の例

次の例は、EtherType ACL の設定方法（インターフェイスへの適用方法を含む）を示しています。

次のサンプル ACL では、内部インターフェイスで発信される一般的なトラフィックが許可されます。

```
ciscoasa(config)# access-list ETHER ethertype permit ipx
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
ciscoasa(config)# access-group ETHER in interface inside
```

次の ACL では、一部の EtherType は ASA を通過することが許可されますが、IPX は拒否されます。

```
ciscoasa(config)# access-list ETHER ethertype deny ipx
ciscoasa(config)# access-list ETHER ethertype permit 1234
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
ciscoasa(config)# access-group ETHER in interface inside
ciscoasa(config)# access-group ETHER in interface outside
```

次の ACL では、両方のインターフェイスで EtherType 0x1256 のトラフィックが拒否されますが、他のトラフィックはすべて許可されます。

```
ciscoasa(config)# access-list nonIP ethertype deny 1256
ciscoasa(config)# access-list nonIP ethertype permit any
ciscoasa(config)# access-group ETHER in interface inside
ciscoasa(config)# access-group ETHER in interface outside
```

ACL のモニタリング

ACL をモニタするには、次のいずれかのコマンドを入力します。

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。 **access-list extended**、**access-list standard**、**access-list webtype**、**access-list ethertype** の各コマンドが導入されました。
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を使用すると、NAT の設定が変更されても ACL を変更する必要はありません。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.17-4）を参照してください。

機能名	リリース	説明
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、VPN 認証に使用できます。 **access-list extended** コマンドが変更されました。
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。 **access-list ethertype {permit | deny} isis** コマンドが変更されました。
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。 **access-list extended** コマンドが変更されました。
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。 **access-list extended**、**access-list webtype** の各コマンドが変更されました。 **ipv6 access-list**、**ipv6 access-list webtype**、**ipv6-vpn-filter** の各コマンドが削除されました。
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。 **access-list extended**、**service-object**、**service** の各コマンドが導入または変更されました。

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」（P.18-1）
- 「ASA 内でのルーティングの仕組み」（P.18-4）
- 「ルーティングにサポートされているインターネット プロトコル」（P.18-5）
- 「ルーティング テーブルについて」（P.18-6）
- 「プロキシ ARP 要求のディセーブル化」（P.18-13）

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」（P.18-1）
- 「パス判別」（P.18-2）
- 「サポートされるルート タイプ」（P.18-2）

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）レイヤ）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。他のすべてのルータからのルーティング アップデートを分析することで、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.18-3）
- 「シングルパスとマルチパスの比較」（P.18-3）
- 「フラットと階層型の比較」（P.18-3）
- 「リンクステートと距離ベクトル型の比較」（P.18-4）

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ディングします。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.18-4）
- 「ネクスト ホップの選択プロセス」（P.18-5）

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.23-3）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.22-7）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。顧客は ISP に接続し、ISP は BGP を使用して顧客および 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.21-4）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」（P.18-6）
- 「ルーティング テーブルへの入力方法」（P.18-7）
- 「転送の決定方法」（P.18-9）
- 「ダイナミック ルーティングとフェールオーバー」（P.18-10）
- 「ダイナミック ルーティングとクラスタリング」（P.18-10）
- 「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」（P.18-12）

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 テーブルのエントリを表示します。

```
ciscoasa# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

```
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

S    10.1.1.0 255.255.255.0 [3/0] via 10.86.194.1, outside
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

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。メトリックス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に複数の異なるルートがある場合に、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 18-1 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 18-1　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（Unknown）	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 テーブルに次のルートを持つ 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.19-2）を参照してください。

ダイナミック ルーティングとクラスタリング

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たときにのみ、マスター ユニットから参加ユニットに対して行われます。

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 18-2 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、「x」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 18-2　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	×	Yes
RIP（レイヤ 2）	Yes	Yes	×

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 8 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
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　プロキシ ARP 要求をディセーブルにします。

sysopt noproxyarp *interface*

例：

```
ciscoasa(config)# sysopt noproxyarp exampleinterface
```

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」（P.19-1）
- 「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」（P.19-2）
- 「スタティック ルートの設定」（P.19-2）
- 「デフォルト スタティック ルートの設定」（P.19-4）
- 「IPv6 デフォルト ルートおよびスタティック ルートの設定」（P.19-5）
- 「スタティック ルートまたはデフォルト ルートのモニタ」（P.19-6）
- 「スタティック ルートまたはデフォルト ルートの例」（P.19-8）
- 「スタティック ルートおよびデフォルト ルートの履歴」（P.19-9）

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 8 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。複数インターフェイス間での等コスト 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。ブラック ホールのスタティック ルートに最も一致する宛先アドレスを持つ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、次の項を参照してください。

- 「スタティック ルートの追加または編集」（P.19-3）

スタティック ルートの追加または編集

手順

ステップ 1　スタティック ルートを追加または編集します。

route *if_name dest_ip mask gateway_ip* [*distance*]

例：

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 [1]
```

dest_ip および *mask* 引数は宛先ネットワークの IP アドレスであり、*gateway_ip* 引数はネクストホップ ルータのアドレスです。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。

distance 引数は、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。

例

次に、外部インターフェイス上の 3 台のゲートウェイにトラフィックを転送する、コストの等しいスタティック ルートの例を示します。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。

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.2
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.3
```

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) 以降では、異なるインターフェイス上で異なるメトリックを持つ 2 つのデフォルト ルートが設定されている場合、大きい方の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、小さい方の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　トンネル デフォルト スタティック ルートを追加または編集します。

route *if_name* 0.0.0.0 0.0.0.0 *gateway_ip* [*distance* | *tunneled*]

例：

```
ciscoasa(config)# route outside 0 0 192.168.2.4 tunneled
```

dest_ip および *mask* 引数は宛先ネットワークの IP アドレスであり、*gateway_ip* 引数はネクスト ホップ ルータのアドレスです。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。

distance 引数は、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。

ヒント　宛先ネットワーク アドレスおよびマスクとして、0.0.0.0 0.0.0.0 の代わりに 0 0 と入力することができます。たとえば、次のように入力します。

```
ciscoasa(config)# route outside 0 0 192.168.1 1
```

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 に対応しており、IPv6 ACL でトラフィックが許可されている場合、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　デフォルトの IPv6 ルートを追加します。

ipv6 route *if_name* **::/0** *next_hop_ipv6_addr*

例：

```
ciscoasa(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1
```

この例では、ネットワーク 7fff::0/32 のパケットを、3FFE:1100:0:CC00::1 の内部インターフェイス上のネットワーキング デバイスにルーティングします。

アドレス ::/0 は任意の IPv6 に相当します。

ステップ 2　IPv6 ルーティング テーブルに IPv6 スタティック ルートを追加します。

ipv6 route *if_name destination next_hop_ipv6_addr* [*admin_distance*]

例：

```
ciscoasa(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 [110]
```

この例では、ネットワーク 7fff::0/32 のパケットを、3FFE:1100:0:CC00::1 の内部インターフェイス上のネットワーキング デバイスにルーティングします。アドミニストレーティブ ディスタンスは 110 です。

（注）　**ipv6 route** コマンドは、**route** コマンド（IPv4 スタティック ルートの定義に使用）と同じように動作しです。

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。ルート トラッキングが設定されている複数インターフェイス上の PPPoE クライアントのみをイネーブルにできます。

手順

ステップ 1　モニタリング プロセスを定義することにより、追跡されるオブジェクトのモニタリング パラメータを設定します。

sla monitor *sla_id*

例：

```
ciscoasa(config)# sla monitor 5
```

タイプが定義済みでスケジュールが未設定のモニタリング プロセスのモニタリング パラメータを変更する場合は、自動的に SLA プロトコル コンフィギュレーション モードに入ります。

ステップ 2　モニタリング プロトコルを指定します。

type echo protocol ipIcmpEcho *target_ip* **interface** *if_name*

例：

```
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 172.29.139.134
```

タイプが定義済みでスケジュールが未設定のモニタリング プロセスのモニタリング パラメータを変更する場合は、自動的に SLA プロトコル コンフィギュレーション モードに入り、この設定は変更できません。

target_ip 引数は、トラッキング プロセスによって使用可能かどうかをモニタされるネットワーク オブジェクトの IP アドレスです。このオブジェクトが使用可能な場合、トラッキング プロセス 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。このオブジェクトが使用できない場合、トラッキング プロセスがルートを削除し、代わりにバックアップ ルートが使用されます。

ステップ 3　モニタリング プロセスのスケジュールを設定します。

sla monitor schedule *sla_id* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | *pending* | *now* | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]

例：

```
ciscoasa(config)# sla monitor schedule 5 start-time now
```

一般に、モニタリング スケジュールには **sla monitor schedule** *sla_id* **life forever start-time now** コマンドを使用し、モニタリング コンフィギュレーションがテスト頻度を判別できるようにします。

ただし、このモニタリング プロセスを将来開始するようにしたり、指定した時刻だけに実行されるようにスケジュールを設定したりできます。

ステップ 4　追跡するスタティック ルートを SLA モニタリング プロセスに関連付けます。

track *track_id* **rtr** *sla_id* **reachability**

例：

```
ciscoasa(config)# track 6 rtr 5 reachability
```

track_id 引数は、このコマンドで割り当てるトラッキング番号です。*sla_id* 引数は SLA プロセスの ID 番号です。

ステップ 5　スタティック ルートを追跡します。

route *if_name dest_ip mask gateway_ip* [*admin_distance*] **track** *track_id*

例：

```
ciscoasa(config)# route if_name dest_ip mask gateway_ip [admin_distance] track track_id
```

スタティック ルート トラッキングでは、**route** コマンドに **tunneled** オプションを使用できません。

ステップ 6　DHCP から取得したデフォルト ルートを追跡します。

```
ciscoasa(config)# interface phy_if
ciscoasa(config-if)# dhcp client route track track_id
ciscoasa(config-if)# ip address dhcp setroute
ciscoasa(config-if)# exit
```

DHCP を使用してデフォルト ルートを取得するには、**ip address dhcp** コマンドで **setroute** キーワードを使用する必要があることに注意してください。

ステップ 7　PPPoE から取得したデフォルト ルートを追跡します。

```
ciscoasa(config)# interface phy_if
ciscoasa(config-if)# pppoe client route track track_id
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config-if)# exit
```

PPPoE を使用してデフォルト ルートを取得するには、**ip address pppoe** コマンドで **setroute** キーワードを使用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。

```
ciscoasa(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.1
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.2
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.3
ciscoasa(config)# route outside 0 0 192.168.2.4 tunneled
```

ASA で受信した非暗号化トラフィックは、スタティック ルートも既知のルートも指定されていない場合、IP アドレスが 192.168.2.1、192.168.2.2、192.168.2.3 のゲートウェイの間に分散されます。ASA で受信した暗号化されたトラフィックは、スタティック ルートも既知のルートも指定されていない場合、IP アドレス 192.168.2.4 のゲートウェイに転送されます。

次に、10.1.1.0/24 宛てのすべてのトラフィックを、内部インターフェイスに接続されたルータ（10.1.2.45）に送信するスタティック ルートを作成する例を示します。

```
ciscoasa(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
```

スタティック ルートおよびデフォルト ルートの履歴

表 19-1　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。 **route** コマンドが導入されました。
クラスタ	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されます。この機能は、BGP の Remotely Triggered Black Hole (RTBH) の設定に役立ちます。 **route** コマンドが変更されました。

CHAPTER 20

ルート マップ

- 「ルート マップについて」（P.20-1）
- 「ルート マップのガイドライン」（P.20-4）
- 「ルート マップの定義」（P.20-4）
- 「ルート マップのカスタマイズ」（P.20-5）
- 「ルート マップの設定例」（P.20-7）
- 「ルート マップの機能履歴」（P.20-7）

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.20-4）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.20-2）
- 「match 句と set 句の値」（P.20-2）
- 「BGP match 句および BGP set 句」（P.20-3）

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。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。

手順

ステップ 1　ルート マップのエントリを作成します。

route-map *name* {**permit** | **deny**} [*sequence_number*]

例：

```
ciscoasa(config)# route-map name {permit} [12]
```

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、*sequence_number* 引数を使用して指定できます。この引数で指定しなければ、ルート マップ エントリを追加した順序が ASA で使用されます。

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」（P.20-5）
- 「ルート アクションのメトリック値の設定」（P.20-6）

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　ルート マップのエントリを作成します。

route-map *name* {**permit** | **deny**} [*sequence_number*]

例：

```
ciscoasa(config)# route-map name {permit} [12]
```

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、*sequence_number* オプションを使用して指定できます。このオプションで指定しなければ、ルート マップ エントリを追加した順序が ASA で使用されます。

ステップ 2　標準 ACL またはプレフィックス リストに一致する宛先ネットワークを持つ任意のルートを照合します。

match ip address *acl_id* [*acl_id*] [...] [prefix-list]

例：

```
ciscoasa(config-route-map)# match ip address acl1
```

複数の ACL を指定する場合、ルートは任意の ACL を照合できます。

ステップ 3　指定したメトリックを持つ任意のルートを照合します。

match metric *metric_value*

例：

```
ciscoasa(config-route-map)# match metric 200
```

metric_value には、0 ～ 4294967295 の範囲が指定できます。

ステップ 4　標準 ACL と一致するネクスト ホップ ルータ アドレスを持つ任意のルートを照合します。

match ip next-hop *acl_id* [*acl_id*] [...]

例：

```
ciscoasa(config-route-map)# match ip next-hop acl2
```

複数の ACL を指定する場合、ルートは任意の ACL を照合できます。

ステップ 5　指定されたネクスト ホップ インターフェイスを持つ任意のルートを照合します。

match interface *if_name*

例：

```
ciscoasa(config-route-map)# match interface if_name
```

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。

ステップ 6　標準の ACL と一致するルータによってアドバタイズされた任意のルートを照合します。

match ip route-source *acl_id* [*acl_id*] [...]

例：

```
ciscoasa(config-route-map)# match ip route-source acl_id [acl_id] [...]
```

複数の ACL を指定する場合、ルートは任意の ACL を照合できます。

ステップ 7　ルート タイプを照合します。

match route-type {**internal** | **external** [**type-1** | **type-2**]}

ルート アクションのメトリック値の設定

ルートが **match** コマンドで一致する場合は、次の **set** コマンドによって、ルートを再配布する前にルートで実行するアクションが決まります。

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　ルート マップのエントリを作成します。

route-map *name* {**permit** | **deny**} [*sequence_number*]

例：

```
ciscoasa(config)# route-map name {permit} [12]
```

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、*sequence_number* 引数を使用して指定できます。この引数で指定しなければ、ルート マップ エントリを追加した順序が ASA で使用されます。

ステップ 2　ルート マップのメトリック値を設定します。

set metric *metric_value*

例：

```
ciscoasa(config-route-map)# set metric 200
```

metric_value の引数は、0～294967295 の範囲で指定できます。

ステップ 3　ルート マップのメトリック タイプを設定します。

set metric-type {**type-1** | **type-2**}

例：

```
ciscoasa(config-route-map)# set metric-type type-2
```

metric-type 引数には type-1 と type-2 があります。

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。

ASA は、これらのルートをメトリック 5、メトリック タイプ 1 で外部 LSA として再配布します。

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
```

次に、メトリック値が設定された EIGRP プロセス 1 に 10.1.1.0 のスタティック ルートを再配布する例を示します。

```
ciscoasa(config)# route outside 10.1.1.0 255.255.255.0 192.168.1.1
ciscoasa(config-route-map)# access-list mymap2 line 1 permit 10.1.1.0 255.255.255.0
ciscoasa(config-route-map)# route-map mymap2 permit 10
ciscoasa(config-route-map)# match ip address mymap2
ciscoasa(config-route-map)# router eigrp 1
ciscoasa(config-router)# redistribute static metric 250 250 1 1 1 route-map mymap2
```

ルート マップの機能履歴

表 20-1　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。 **route-map** コマンドが導入されました。
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。
ダイナミック ルーティング プロトコル（EIGRP、OSPF、RIP）のステートフル フェールオーバーと一般的なルーティング関連動作のデバッグのサポート	8.4(1)	**debug route**、および **show debug route** コマンドが導入されました。 **show route** コマンドが変更されました。
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。

表 20-1　ルート マップの機能履歴 （続き）

機能名	プラットフォームリリース	機能情報
BGP のサポート	9.2(1)	この機能が導入されました。 **router bgp** コマンドが導入されました。
		次のコマンドを導入しました。

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」（P.21-1）
- 「BGP のガイドライン」（P.21-3）
- 「BGP の設定」（P.21-4）
- 「BGP のモニタリング」（P.21-21）
- 「BGP の設定例」（P.21-23）
- 「BGP の履歴」（P.21-24）

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」（P.21-1）
- 「ルーティング テーブルの変更」（P.21-2）

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。顧客は ISP に接続し、ISP は BGP を使用して顧客および 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　CLI で、BGP をイネーブルにして、一般的な BGP パラメータを設定します。

ステップ 2　BGP ルーティング プロセスの最適なパスを定義し、最適なパスのコンフィギュレーション パラメータを設定します。

ステップ 3　ポリシー リストを追加および設定します。

ステップ 4　AS パス フィルタを追加および設定します。

ステップ 5　コミュニティ ルールを追加および設定します。

ステップ 6　IPv4 アドレス ファミリを設定します。

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　BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

autonomous-num の有効な値は 1 ～ 4294967295 および 1.0 ～ XX.YY です。

ステップ 2　指定値を超えている AS パス セグメントを含むルートを破棄します。

bgp maxas-limit *number*

例：

```
ciscoasa(config-router)# bgp maxas-limit 15
```

number 引数には、自律システム セグメントの最大許容数を指定します。有効な値は 1 ～ 254 です。

ステップ 3　BGP ネイバーのリセットをログに記録します。

bgp log-neighbor-changes

ステップ 4　BGP で各 BGP セッションの最適な TCP パス MTU を自動検出できるようにします。

bgp transport path-mtu-discovery

ステップ 5　BGP が、ピアに到達するために使用されているリンクがダウンした場合に、ホールドダウン タイマーが期限切れになるのを待たずに、直接隣接するいずれかのピアの外部 BGP セッションを終了できるようにします。

bgp fast-external-fallover

ステップ 6　BGP ルーティング プロセスで、自律システム（AS）番号を着信ルートの AS_path 属性の 1 つ目の AS パス セグメントとしてリストしていない外部 BGP（eBGP）ピアから受信したアップデートを破棄できるようにします。

bgp enforce-first-as

ステップ 7　デフォルトの表示を変更し、BGP 4 バイト自律システム番号の正規表現一致形式を、asplain（10 進数の値）からドット付き表記にします。

bgp asnotation dot

ステップ 8　BGP ネットワーク タイマーを調整します。

timers bgp *keepalive holdtime* [*min-holdtime*]

例：

```
ciscoasa(config-router)# timers bgp 80 120
```

- *keepalive：*ASA がキープアライブ メッセージをピアに送信する頻度（秒）。デフォルト値は 60 秒です。
- *holdtime：*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）。デフォルト値は 180 秒です。
- （オプション）*min-holdtime：*ネイバーからキープアライブ メッセージを受信できない状態が継続して、ネイバーがデッドであると ASA が宣言するまでの時間（秒）。

ステップ 9　BGP グレースフル リスタート機能をイネーブルにします。

bgp graceful-restart [**restart-time** *seconds*|**stalepath-time** *seconds*] [**all**]

例：

```
ciscoasa(config-router)# bgp graceful-restart restart-time 200
```

- **restart-time**：リスタート イベントが発生した後、グレースフル リスタート対応ネイバーが通常の動作に戻るまで ASA が待機する最大時間（秒）。デフォルトは 120 秒です。有効な値は 1 ～ 3600 秒です。
- **stalepath-time**：リスタートしているピアの古いパスを ASA が保持する最大時間（秒）。すべての古いパスは、このタイマーが期限切れになった後に削除されます。デフォルト値は 360 秒です。有効な値は 1 ～ 3600 秒です。

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.21-3）を参照してください。

手順

ステップ 1　BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2　デフォルトの Local preference 値を変更します。

bgp default local-preference *number*

例：

```
ciscoasa(config-router)# bgp default local-preference 500
```

number 引数は、0 ～ 4294967295 の値です。値が大きいほど、優先度が高いことを示します。デフォルト値は 100 です。

ステップ 3　さまざまな自律システムのネイバーから学習したパス間での Multi-exit discriminator（MED）比較をイネーブルにします。

bgp always-compare-med

ステップ 4　最適なパスの選択プロセス中に外部 BGP （eBGP）ピアから受信した類似ルートを比較し、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。

bgp bestpath compare-routerid

ステップ 5　隣接 AS からアドバタイズされた最適な MED パスを選択します。

bgp deterministic-med

ステップ 6　MED 属性が欠落しているパスを最も優先度の低いパスとして設定します。

bgp bestpath med missing-as-worst

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 リストを設定できます。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　ポリシー マップ コンフィギュレーション モードをイネーブルにし、BGP ポリシー リストを作成できるようにします。

policy-list *policy_list_name* {**permit** | **deny**}

例：

```
ciscoasa(config)# policy-list Example-policy-list1 permit
```

permit キーワードを指定すると、条件が一致した場合にアクセスが許可されます。

deny キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。

ステップ 2　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ます。

match interface [*...interface_name*]

例：

```
ciscoasa(config-policy-list)# match interface outside
```

ステップ 3　宛先アドレス、ネクスト ホップ ルータ アドレス、ルータ/アクセス サーバ ソースのいずれかまたはすべてを一致させてルートを再配布します。

match ip {**address** | **next-hop** | **route-source**}

ステップ 4　BGP 自律システム パスを一致させます。

match as-path

ステップ 5　BGP コミュニティを一致させます。

match community {*community-list_name* | **exact-match**}

例：

```
ciscoasa(config-policy-list)# match community ExampleCommunity1
```

- *community-list_name* ：1 つ以上のコミュニティ リスト。
- **exact-match**：完全に一致する必要があることを示します。指定されたすべてのコミュニティのみが存在する必要があります。

ステップ 6　指定したメトリックを持つルートを再配布します。

match metric

ステップ 7　指定されたタグと一致するルーティング テーブルのルートを再配布します。

match tag

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　グローバル コンフィギュレーション モードで正規表現を使用して自律システム パス フィルタを設定します。

as-path access-list *acl-number* {**permit**|**deny**} *regexp*

例：

```
ciscoasa(config)# as-path access-list 35 permit testaspath
```

- *acl-number*：AS パス アクセス リストの番号。有効な値は、1 ～ 500 です。
- *regexp*：AS パス フィルタを定義する正規表現。自律システム番号は 1 ～ 65535 の範囲で表されます。

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　BGP コミュニティ リストを作成または設定して、そのリストへのアクセスを制御します。

community-list {**standard**| *community list-name* {**deny**|**permit**} [*community-number*] [*AA:NN*] [**internet**] [**no-advertise**][**no-export**]}| {**expanded**|*expanded list-name* {**deny**| **permit**}*regexp*}

例：

```
ciscoasa(config)# community-list standard excomm1 permit 100 internet no-advertise
no-export
```

- **standard**：1 ～ 99 の数字を使用して標準のコミュニティ リストを設定し、1 つ以上の許可または拒否コミュニティ グループを識別します。
- （オプション）*community-number*：1 ～ 4294967200 の 32 ビットの数値で表わされたコミュニティ。1 つのコミュニティ、または複数のコミュニティをそれぞれスペースで区切って入力できます。

- *AA:NN*：4 バイトの新コミュニティ形式で入力された自律システム番号およびネットワーク番号。この値は、コロンで区切られた 2 バイトの数 2 つで設定されます。2 バイトの数ごとに 1 ～ 65535 の数を入力できます。1 つのコミュニティ、または複数のコミュニティをそれぞれスペースで区切って入力できます。
- （オプション）**internet**：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。
- （オプション）**no-advertise**：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。
- （オプション）**no-export**：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。
- （オプション）**expanded**：100 ～ 500 の拡張コミュニティ リスト番号を設定し、1 つ以上の許可または拒否コミュニティ グループを識別します。
- *regexp*：AS パス フィルタを定義する正規表現。自律システム番号は 1 ～ 65535 の範囲で表されます。

（注） 正規表現を使用できるのは拡張コミュニティ リストだけです。

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.21-10）
- 「IPv4 ファミリ集約アドレスの設定」（P.21-12）
- 「IPv4 ファミリのフィルタリング設定」（P.21-13）
- 「IPv4 ファミリの BGP ネイバーの設定」（P.21-14）
- 「IPv4 ネットワークの設定」（P.21-19）
- 「再配布の設定」（P.21-20）
- 「ルート注入の設定」（P.21-21）

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　BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2　アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [**unicast**]

キーワード **unicast** では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3　（オプション）ローカル BGP ルーティング プロセスの固定ルータ ID を設定します。

bgp router-id *A.B.C.D*

例：

```
ciscoasa(config-router-af)# bgp router-id 10.86.118.3
```

引数 *A.B.C.D* には、ルータ ID を IP アドレス形式で指定します。ルータ ID を指定しない場合、自動的に割り当てられます。

ステップ 4　（オプション）個別インターフェイス（L3）モードで IP アドレスのクラスタ プールを設定します。

bgp router-id *cluster-pool*

例：

```
ciscoasa(config-router-af)# bgp router-id cp
```

（注）　L3 クラスタでは、BGP ネイバーをクラスタ プールの IP アドレスの 1 つとして定義できません。

ステップ 5　BGP ルートのアドミニストレーティブ ディスタンスを設定します。

distance bgp *external-distance internal-distance local-distance*

例：

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- *external-distance*：外部 BGP ルートのアドミニストレーティブ ディスタンス。ルートは、外部自律システムから学習された場合は外部になります。この引数の値の範囲は 1 ～ 255 です。
- *internal-distance*：内部 BGP ルートのアドミニストレーティブ ディスタンス。ルートは、ローカル自律システムのピアから学習された場合は内部です。この引数の値の範囲は 1 ～ 255 です。

- *local-distance*：ローカル BGP ルートのアドミニストレーティブ ディスタンス。ローカル ルートは、別のプロセスから再配布されているルータまたはネットワークの、多くの場合バック ドアとして、ネットワーク ルータ コンフィギュレーション コマンドによりリストされるネットワークです。この引数の値の範囲は 1 ～ 255 です。

ステップ 6　BGP で学習されたルートを使用して IP ルーティング テーブルが更新されたときに、メトリックおよびタグ値を変更します。

table-map {**WORD**|*route-map_name*}

例：

```
ciscoasa(config-router-af)# table-map example1
```

引数 *route-map_name* には **route-map** コマンドのルート マップ名を指定します。

ステップ 7　BGP ルーティング プロセスを設定し、デフォルト ルート（ネットワーク 0.0.0.0）を配布します。

default-information originate

ステップ 8　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。

auto-summary

ステップ 9　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のアドバタイズメントを抑制します。

bgp suppress-inactive

ステップ 10　BGP と Interior Gateway Protocol（IGP）システム間で同期します。

synchronization

ステップ 11　OSPF などの IGP への iBGP の再配布を設定します。

bgp redistribute-internal

ステップ 12　ネクスト ホップの検証用に BGP ルータのスキャン間隔を設定します。

bgp scan-time *scanner-interval*

例：

```
ciscoasa(config-router-af)# bgp scan-time 15
```

引数 *scanner-interval* には BGP ルーティング情報のスキャン間隔を指定します。有効な値は 5 ～ 60 秒です。デフォルトは 60 秒です。

ステップ 13　BGP ネクスト ホップ アドレス トラッキングを設定します。

bgp nexthop trigger {**delay** *seconds*|**enable**}

例：

```
ciscoasa(config-router-af)# bgp nexthop trigger delay 15
```

- **trigger**：BGP ネクスト ホップ アドレス トラッキングの使用を指定します。ネクスト ホップ トラッキングの遅延を変更するには、このキーワードを **delay** キーワードとともに使用します。ネクスト ホップ アドレス トラッキングをイネーブルにするには、このキーワードを **enable** キーワードとともに使用します。
- **delay**：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変更します。

- *seconds*：遅延を秒数で指定します。値の範囲は 0 ～ 100 です。デフォルトは 5 です。
- **enable**：BGP ネクスト ホップ アドレス トラッキングをすぐにイネーブルにします。

ステップ 14　ルーティング テーブルにインストールできる並列 iBGP ルートの最大数を制御します。

maximum-paths {*number_of_paths*|ibgp *number_of_paths*}

例：

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

（注）　*number_of_paths* 引数には、ルーティング テーブルにインストールするルートの数を指定します。ASA 9.3(1) では、有効な値は 1 ～ 3 です。
ibgp キーワードを使用しない場合、*number_of_paths* 引数は、並列 EBGP ルートの最大数を制御します。

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　BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2　アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [**unicast**]

キーワード **unicast** では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3　BGP データベースで集約エントリを作成します。

aggregate-address *address mask* [**as-set**][**summary-only**][**suppress-map** *map-name*][**advertise-map** *map-name*][**attribute-map** *map-name*]

例：

```
ciscoasa(config-router-af) aggregate-address 10.86.118.0 255.255.255.0 as-set summary-only
suppress-map example1 advertise-map example1 attribute-map example1
```

- *address*：集約アドレス。
- *mask*：集約マスク。
- *map-name*：ルート マップ。

- （オプション）**as-set**：自律システムの設定パス情報を生成します。
- （オプション）**summary-only**：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。
- （オプション）**Suppress-map** ***map-name***：抑制するルートを選択するために使用するルートマップの名前を指定します。
- （オプション）**Advertise-map** ***map-name***：AS_SET 発信コミュニティを作成するためのルートを選択するために使用するルート マップの名前を指定します。
- （オプション）**Attribute-map** ***map-name***：集約ルートの属性を設定するために使用するルート マップの名前を指定します。

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　BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2　アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [**unicast**]

キーワード **unicast** では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3　着信 BGP アップデートで受信したルータまたはネットワーク、あるいは発信 BGP アップデートでアドバタイズされたルータまたはネットワークをフィルタリングします。

distribute-list *acl-number* **in**|**out**[]

例：

```
ciscoasa(config-router-af)# distribute-list ExampleAcl in bgp 2
```

引数 *acl-number* には、IP アクセス リストの番号を指定します。アクセス リストは、ルーティング アップデートで受信されるネットワークと抑制されるネットワークを定義します。

キーワード **in** はフィルタを着信 BGP アップデートに適用する必要があることを指定し、**out** はフィルタを発信 BGP アップデートに適用する必要があることを指定します。

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　BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2　アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [**unicast**]

キーワード **unicast** では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3　エントリを BGP ネイバー テーブルに追加します。

neighbor *ip-address* **remote-as** *autonomous-number*

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remote-as 3
```

ステップ 4　（オプション）ネイバーまたはピア グループをディセーブルにします。

neighbor *ip-address* **shutdown**

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 shutdown 3
```

ステップ 5　BGP ネイバーと情報を交換します。

neighbor *ip-address* **activate**

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 activate
```

ステップ 6　BGP ネイバーの 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。

neighbor *ip-address* **ha-mode graceful-restart** [**disable**]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ha-mode graceful-restart
```

（オプション）**disable** を指定すると、ネイバーの BGP グレースフル リスタート機能がディセーブルなります。

ステップ 7　アクセス リストで指定された BGP ネイバー情報を配布します。

neighbor {*ip-address*} **distribute-list** {*access-list-name*}{**in**|**out**}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 distribute-list ExampleAcl in
```

- *access-list-number*：標準アクセス リストまたは拡張アクセス リストの番号。標準アクセス リストの番号の範囲は 1 ～ 99 です。拡張アクセス リストの番号の範囲は 100 ～ 199 です。
- *expanded-list-number*：拡張アクセス リストの番号。拡張アクセス リストの範囲は 1300 ～ 2699 です。
- *access-list-name*：標準アクセス リストまたは拡張アクセス リストの名前。
- *prefix-list-name*：BGP プレフィックス リストの名前。
- **in :** アクセス リストはそのネイバーへの着信アドバタイズメントに適用されます。
- **out**：アクセス リストはそのネイバーへの発信アドバタイズメントに適用されます。

ステップ 8　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。

neighbor {*ip-address*} **route-map** *map-name* {**in**|**out**}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 route-map example1 in
```

キーワード **in** を指定すると、ルート マップは着信ルートに適用されます。

キーワード **out** を指定すると、ルート マップは発信ルートに適用されます。

ステップ 9　プレフィックス リストで指定された BGP ネイバー情報を配布します。

neighbor {*ip-address*} **prefix-list** *prefix-list-name* {**in**|**out**}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 prefix-list NewPrefixList in
```

キーワード **in** は、プレフィックス リストがそのネイバーからの着信アドバタイズメントに適用されることを意味します。

キーワード **out** は、プレフィックス リストがそのネイバーへの発信アドバタイズメントに適用されることを意味します。

ステップ 10　フィルタ リストを設定します。

neighbor {*ip-address*} **filter-list** *access-list-number* {**in**|**out**}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 filter-list 5 in
```

- *access-list-name*：自律システム パスのアクセス リストの番号を指定します。**ip as-path access-list** コマンドを使用して、このアクセス リストを定義します。
- **in**：アクセス リストはそのネイバーからの着信アドバタイズメントに適用されます。
- **out**：アクセス リストはそのネイバーへの発信アドバタイズメントに適用されます。

ステップ 11　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。

neighbor {*ip-address*} **maximum-prefix** *maximum* [*threshold*][**restart** *restart interval*][**warning-only**]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 maximum-prefix 7 75 restart 12
```

- *maximum*：このネイバーからの許可される最大プレフィックス数。
- （オプション）*threshold*：最大数の何パーセントになったらルータが警告メッセージの生成を開始するかを指定する整数。指定できる範囲は 1 ～ 100 です。デフォルト値は 75（%）です。
- （オプション）*restart interval*：BGP ネイバーが再起動するまでの時間を指定する整数値（分）。
- （オプション）**warning-only**：プレフィックスの最大数を超えた場合に、ピアリングを終了する代わりに、ルータでログ メッセージを生成できます。

ステップ 12　BGP スピーカー（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。

neighbor {*ip-address*} **default-originate** [**route-map** *map-name*]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 default-originate route-map example1
```

引数 *map-name* はルート マップの名前です。ルート マップにより、ルート 0.0.0.0 が条件に応じて注入されます。

ステップ 13　BGP ルーティング アップデートの最小送信間隔を設定します。

neighbor {*ip-address*} **advertisement-interval** *seconds*

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 advertisement-interval 15
```

引数 *seconds* は時間（秒）です。有効な値は 0 ～ 600 です。

ステップ 14　設定されているルート マップと一致する BGP テーブル内のルートをアドバタイズします。

neighbor {*ip-address*} **advertise-map** *map-name* {**exist-map** *map-name* |**non-exist-map** *map-name*}[**check-all-paths**]

例：

```
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
```

- **advertise-map** *map name*：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 マップの名前。
- **exist-map** *map name*：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る exist-map の名前。
- **non-exist-map** *map name*：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る non-exist-map の名前。
- （オプション）**check all paths**：BGP テーブル内のプレフィックスを持つ exist-map によるすべてのパスのチェックをイネーブルにします。

ステップ 15　プライベート自律システム番号を発信ルーティング アップデートから削除します。

neighbor {*ip-address*} **remove-private-as**

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remove-private-as
```

ステップ 16　特定の BGP ピアまたは BGP ピア グループのタイマーを設定します。

neighbor {*ip-address*} **timers** *keepalive holdtime min holdtime*

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 timers 15 20 12
```

- *keepalive*：ASA がキープアライブ メッセージをピアに送信する頻度（秒）。デフォルトは 60 秒です。有効な値は、0 ～ 65535 です。
- *holdtime :* 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）。デフォルト値は 180 秒です。
- *min holdtime*：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）。

ステップ 17　2 つの BGP ピア間の TCP 接続で Message Digest 5（MD5）認証をイネーブルにします。

neighbor {*ip-address*} **password** *string*

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 password test
```

引数 *string* は大文字と小文字を区別するパスワードで、**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。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。

（注）　最初の文字を数値にはできません。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 18　BGP ネイバーに送信する Community 属性を指定します。

neighbor {*ip-address*} **send-community**[**both**|**standard**|**extended**]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 send-community
```

- （オプション）**both** キーワード：標準コミュニティと拡張コミュニティの両方が送信されます。
- （オプション）**standard** キーワード：標準コミュニティのみ送信されます。
- （オプション）**extended** キーワード：拡張コミュニティのみ送信されます。

ステップ 19　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。

neighbor {*ip-address*}**next-hop-self**

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 next-hop-self
```

ステップ 20　直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。

neighbor {*ip-address*} **ebgp-multihop** [*ttl*]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ebgp-multihop 5
```

引数 *ttl* には、1 ～ 255 ホップの範囲の存続可能時間を指定します。

ステップ 21　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。

neighbor {*ip-address*} **disable-connected-check**

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 disable-connected-check
```

ステップ 22　BGP ピアリング セッションを保護し、2 つの外部 BGP （eBGP）ピアを区切るホップの最大数を設定します。

neighbor {*ip-address*} **ttl-security hops** *hop-count*

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

引数 *hop-count* は、eBGP ピアを区切るホップの数です。TTL 値は、設定された hop-count 引数に基づいてルータにより計算されます。有効な値は 1 ～ 254 です。

ステップ 23　ネイバー接続に重みを割り当てます。

neighbor {*ip-address*} **weight** *number*

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 weight 30
```

引数 *number* は、ネイバー接続に割り当てる重みです。有効な値は、0 ～ 65535 です。

ステップ 24　特定の BGP バージョンだけを受け入れるように ASA を設定します。

neighbor {*ip-address*} **version** *number*

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 version 4
```

引数 *number* には、BGP バージョン番号を指定します。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 25　BGP セッションの TCP トランスポート セッション オプションをイネーブルにします。

neighbor {*ip-address*} **transport** {**connection-mode**{**active**|**passive**}|
path-mtu-discovery[**disable**]}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 transport path-mtu-discovery
```

- **connection-mode**：接続のタイプ（**active または passive**）。
- **path-mtu-discovery**：TCP トランスポート パスの最大伝送ユニット（MTU）ディスカバリをイネーブルにします。TCP パス MTU ディスカバリは、デフォルトではイネーブルです。
- （オプション）**disable**：TCP パス MTU ディスカバリをディセーブルにします。

ステップ 26　External Border Gateway Protocol（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。

neighbor {*ip-address*} **local-as** [*autonomous-system-number*[**no-prepend**]]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- （オプション）*autonomous-system-number*：AS_path 属性の前に追加する自律システムの番号。この引数の値の範囲は、1 ～ 4294967295 または 1.0 ～ XX.YY の有効な任意の自律システム番号です。
- （オプション）**no-prepend**：eBGP ネイバーから受信したルートの前にローカル自律システム番号を追加しません。

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　BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2　アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

キーワード **unicast** では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3　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指定します。

network {*network-number* *[***mask** *network-mask]}[***route-map** *map-tag]*

例：

```
ciscoasa(config-router-af)# network 10.86.118.13 mask 255.255.255.255 route-map example1
```

- *network-number*：BGP がアドバタイズするネットワーク。
- （オプション）*network-mask*：マスク アドレスを持つネットワーク マスクまたはサブネットワーク マスク。
- （オプション）*map-tag*：設定されているルート マップの ID。ルート マップは、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があります。この値を指定しない場合、すべてのネットワークがアドバタイズされます。

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　BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2　アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

キーワード **unicast** では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3　別のルーティング ドメインから BGP 自律システムにルートを再配布します。

redistribute *protocol [process-id] [metric] [***route-map [map-tag]]**

例：

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- *protocol :* ルートの再配布元となるソース プロトコル。Connected、EIGRP、OSPF、RIP または [Static] のいずれかを指定できます。
- （オプション）*process-id*：特定のルーティング プロセスの名前。
- （オプション）*metric*：再配布されるルートのメトリック。
- （オプション）*map-tag*：設定されているルート マップの ID。

（注）　ルート マップは、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があります。この値を指定しない場合、すべてのネットワークが再配布されます。

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　BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2　アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

```
address-family ipv4 [unicast]
```

例：

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

キーワード **unicast** では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3　BGP ルーティング テーブルに固有性の強いルートを注入するよう条件付きルート注入を設定します。

bgp inject-map *inject-map* **exist-map** *exist-map* [**copy-attributes**]

例：

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- *inject-map*：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 マップの名前。
- *exist-map*：BGP スピーカーが追跡するプレフィックスを含むルート マップの名前。
- （オプション）**copy-attributes**：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。

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、次のコマンドの 1 つを入力します。

- **show bgp** [*ip-address* [*mask* [*longer-prefixes* [*injected*] | *shorter-prefixes* [*length*]]]| **prefix-list** *name* | **route-map** *name*]

  BGP ルーティング テーブル内のエントリを表示します。

- **show bgp cidr-only**

  ナチュラル ネットワーク マスク以外を使用するルート（つまり、クラスレス ドメイン間ルーティング（CIDR））を表示します。
- **show bgp community** *community-number* [**exact-match**][**no-advertise**][**no-export**]

  指定された BGP コミュニティに属するルートを表示します。
- **show bgp community-list** *community-list-name* [**exact-match**]

  BGP コミュニティ リストによって許可されたルートを表示します。
- **show bgp filter-list** *access-list-number*

  指定されたフィルタ リストと一致するルートを表示します。
- **show bgp injected-paths**

  BGP ルーティング テーブルに注入されたすべてのパスを表示します。
- **show bgp ipv4 unicast**

  ユニキャスト セッションの IPv4 BGP ルーティング テーブルのエントリを表示します。
- **show bgp neighbors** *ip_address*

  ネイバーに対する BGP 接続と TCP 接続に関する情報を表示します。
- **show bgp paths** [LINE]

  データベース内のすべての BGP パスを表示します。
- **show bgp pending-prefixes**

  削除が保留されているプレフィックスを表示します。
- **show bgp prefix-list** *prefix_list_name* [WORD]

  指定のプレフィックス リストに一致するルートを表示します。
- **show bgp regexp** *regexp*

  自律システム パスの正規表現と一致するルートを表示します。
- **show bgp replication** [*index-group* | *ip-address*]

  BGP アップデート グループのアップデートのレプリケーション統計情報を表示します。
- **show bgp rib-failure**

  ルーティング情報ベース（RIB）テーブルにインストールできなかった BGP ルートを表示します。
- **show bgp route-map** *map-name*

  指定されたルート マップに基づいて、BGP ルーティング テーブルのエントリを表示します。
- **show bgp summary**

  すべての BGP 接続のステータスを表示します。
- **show bgp system-config**

  マルチ コンテキスト モードでシステム コンテキスト固有の BGP 設定を表示します。

  このコマンドは、マルチ コンテキスト モードのすべてのユーザ コンテキストで使用できます。
- **show bgp update-group**

  BGP アップデート グループに関する情報を表示します。

（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。

BGP 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 BGPv4 をイネーブルにし、設定する方法を示します。

ステップ 1　ルーティング プロトコル間のルートの再配布に対する条件を定義します。または、ポリシー ルーティングをイネーブルにします。

```
ciscoasa(config)# route-map mymap2 permit 10
```

ステップ 2　指定されたアクセス リストのいずれかによって渡されるルート アドレスまたは一致パケットを持つルートを再配布します。

```
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

ステップ 3　ポリシー ルーティング用のルート マップの match 節を通過したパケットの送出先を指定します。

```
ciscoasa(config-route-map)# set ip next-hop peer address
```

ステップ 4　グローバル コンフィギュレーション モードで BGP ルーティング プロセスをイネーブルにします。

```
ciscoasa(config)# router bgp 2
```

ステップ 5　アドレス ファミリ コンフィギュレーション モードでローカル Border Gateway Protocol（BGP）ルーティング プロセスの固定ルータ ID を設定します。

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

ステップ 6　エントリを BGP ネイバー テーブルに追加します。

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 remote-as 65
```

ステップ 7　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。

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 route-map mymap2 in
```

BGP の履歴

表 21-1 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。

表 21-1　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。 次のコマンドが導入されました。**router bgp**、**bgp maxas-limitbgp maxas-limit**、**bgp log-neighbor-changes**、**bgp transport path-mtu-discovery**、**bgp fast-external-fallover**、**bgp enforce-first-as**、**bgp asnotation dot**、**timers bgp**、**bgp default local-preference**、**bgp always-compare-med**、**bgp bestpath compare-routerid**、**bgp deterministic-med**、**bgp bestpath med missing-as-worst**、**policy-list**、**match as-path**、**match community**、**match metric**、**match tag**、**as-path access-list**、**community-list**、**address-family ipv4**、**bgp router-id**、**distance bgp**、**table-map**、**bgp suppress-inactive**、**bgp redistribute-internal**、**bgp scan-time**、**bgp nexthop**、**aggregate-address**、**neighbor**、**bgp inject-map**、**show bgp**、**show bgp cidr-only**、**show bgp all community**、**show bgp all neighbors**、**show bgp community**、**show bgp community-list**、**show bgp filter-list**、**show bgp injected-paths**、**show bgp ipv4 unicast**、**show bgp neighbors**、**show bgp paths**、**show bgp pending-prefixes**、**show bgp prefix-list**、**show bgp regexp**、**show bgp replication**、**show bgp rib-failure**、**show bgp route-map**、**show bgp summary**、**show bgp system-config**、**show bgp update-group**、**clear route network**、**maximum-path**、**network**。 次のコマンドが変更されました。**show route**、**show route summary**、**show running-config router**、**clear config router**、**clear route all**、**timers lsa arrival**、**timers pacing**、**timers throttle**、**redistribute bgp**。

表 21-1　BGP 機能の履歴 （続き）

機能名	プラットフォームリリース	機能情報
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。 次の新しいコマンドが導入されました。**bgp router-id clusterpool**
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 フォワーディングに対するサポートが追加されました。 次の新しいコマンドが導入されました。**bgp graceful-restart**、**neighbor ha-mode graceful-restart**
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)	BGPv4 によってアドバタイズされたマップのサポートが追加されました。 次の新しいコマンドが導入されました。**neighbor advertise-map**

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」（P.22-1）
- 「OSPF のガイドライン」（P.22-5）
- 「OSPFv2 の設定」（P.22-7）
- 「OSPF fast hello パケットの設定」（P.22-8）
- 「OSPFv2 のカスタマイズ」（P.22-8）
- 「OSPFv3 の設定」（P.22-20）
- 「グレースフル リスタートの設定」（P.22-42）
- 「OSPFv2 の設定例」（P.22-46）
- 「OSPFv3 の設定例」（P.22-47）
- 「OSPF のモニタリング」（P.22-48）
- 「その他の関連資料」（P.22-51）
- 「OSPF の機能履歴」（P.22-52）

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.22-3）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）の物理層およびデータリンク層で検出されない可能性がある LAN セグメントで特に有効です。

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 アドレスはルータ 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.20-4）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.19-2）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.22-8）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　OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ASA上で OSPF プロセスが 1 つしかイネーブルになっていないと、そのプロセスがデフォルトで選択されます。既存のエリアを編集する場合、OSPF プロセス ID を変更できません。

ステップ 2　OSPF を実行する IP アドレスを定義し、そのインターフェイスのエリア ID を定義します。

network *ip_address mask* **area** *area_id*

例：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

新しいエリアを追加する場合、そのエリア ID を入力します。このエリア ID には、10 進数か IP アドレスを指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。既存のエリアを編集する場合、エリア ID は変更できません。

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

ステップ 1　インターフェイスを設定します。

interface port-channel *number*

例：

```
ciscoasa(config)# interface port-channel 10
```

number 引数は、ポートチャネル インターフェイスの番号を示します。

ステップ 2　少なくとも 1 個の hello パケットの受信が必要なインターバルを設定します。受信されなければ、ネイバーがダウンしていると判断されます。

ospf dead-interval minimal hello-multiplier *no.of times*

例：

```
ciscoasa(config-if)# ospf dead-interval minimal hell0-multiplier 5
ciscoasa
```

no.of time 引数は、毎秒送信される hello パケットの数を示します。有効な値は、3 ～ 20 です。

ここでは、minimal キーワードおよび hello-multiplier キーワードと値を指定することにより、fast hello パケットに対する OSPF のサポートがイネーブルになっています。multiplier キーワードが 5 に設定されているため、hello パケットが毎秒 5 回送信されます。

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」（P.22-9）
- 「OSPFv2 にルートを再配布する場合のルート集約の設定」（P.22-10）
- 「OSPFv2 エリア間のルート集約の設定」（P.22-11）
- 「OSPFv2 インターフェイス パラメータの設定」（P.22-12）
- 「OSPFv2 エリア パラメータの設定」（P.22-15）
- 「OSPFv2 NSSA の設定」（P.22-16）
- 「クラスタリングの IP アドレス プールの設定（OSPFv2 および OSPFv3）」（P.22-17）
- 「スタティック OSPFv2 ネイバーの定義」（P.22-18）
- 「ルート計算タイマーの設定」（P.22-19）
- 「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」（P.22-19）

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.19-2）を参照し、その後に「ルート マップの定義」（P.20-4）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　OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2　接続済みルートを OSPF ルーティング プロセスに再配布します。

redistribute connected [[**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

例：

```
ciscoasa(config)# redistribute connected 5 type-1 route-map-practice
```

ステップ 3　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。

redistribute static [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*

例：

```
ciscoasa(config)# redistribute static 5 type-1 route-map-practice
```

ステップ 4　ルートを OSPF ルーティング プロセスから別の OSPF ルーティング プロセスに再配布します。

redistribute ospf *pid* [**match {internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

例：

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

このコマンドに **match** オプションを使用してルート プロパティを照合および設定することも、ルート マップを使用することもできます。**subnets** オプションは、**route-map** コマンドで使用する場合と同じではありません。**redistribute** コマンドでルート マップと **match** オプションの両方を使用した場合、これらは一致している必要があります。

この例では、ルートをメトリック 1 に照合することによる、OSPF プロセス 1 から OSPF プロセス 2 へのルートの再配布を示しています。ASA は、これらのルートをメトリック 5、メトリック タイプ 1 で外部 LSA として再配布します。

ステップ 5　ルートを RIP ルーティング プロセスから OSPF ルーティング プロセスに再配布します。

redistribute rip [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

例：

```
ciscoasa(config)# redistribute rip 5
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

ステップ 6　ルートを EIGRP ルーティング プロセスから OSPF ルーティング プロセスに再配布します。

redistribute eigrp *as-num* [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

例：

```
ciscoasa(config)# redistribute eigrp 2
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

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抑制できます。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.22-11）

ルート サマリー アドレスの追加

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　OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2　サマリー アドレスを設定します。

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

例：

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

この例のサマリー アドレスの 10.1.0.0 には、10.1.1.0、10.1.2.0、10.1.3.0 などのアドレスが含まれます。外部のリンクステート アドバタイズメントでは、アドレス 10.1.0.0 だけがアドバタイズされます。

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　OSPF ルーティング プロセスを作成して、この OSPF プロセスのルータ コンフィギュレーション モードを開始します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2　アドレス範囲を設定します。

```
area area-id range ip-address mask [advertise | not-advertise]
```

例：

```
ciscoasa(config-rtr)# area 17 range 12.1.0.0 255.255.0.0
```

この例では、アドレス範囲は OSPF エリア間で設定されます。

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、**ospf hello-interval**、**ospf dead-interval**、**ospf authentication-key** 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

ステップ 1　OSPF ルーティング プロセスを作成します。

```
router ospf process_id
```

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2　OSPF を実行する IP アドレスを定義し、そのインターフェイスのエリア ID を定義します。

```
network ip_address mask area area_id
```

例：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

ステップ 3　インターフェイス コンフィギュレーション モードを開始します。

```
interface interface_name
```

例：

```
ciscoasa(config)# interface my_interface
```

ステップ 4　インターフェイスの認証タイプを指定します。

ospf authentication [**message-digest** | **null**]

例：

```
ciscoasa(config-interface)# ospf authentication message-digest
```

ステップ 5　OSPF 簡易パスワード認証を使用しているネットワーク セグメント上で近接する OSPF ルータが使用するパスワードを割り当てます。

ospf authentication-key *key*

例：

```
ciscoasa(config-interface)# ospf authentication-key cisco
```

key 引数には、最大 8 バイトの連続する文字列が指定できます。

このコマンドで作成するパスワードはキーとして使用され、このキーはASAのソフトウェアによるルーティング プロトコル パケットの発信時に OSPF ヘッダーに直接挿入されます。各ネットワークにはインターフェイスごとに個別のパスワードを割り当てることができます。OSPF 情報を交換するには、同じネットワーク上のすべての隣接ルータが同じパスワードを持っている必要があります。

ステップ 6　OSPF インターフェイスでパケットを送信するコストを明示的に指定します。

ospf cost *cost*

例：

```
ciscoasa(config-interface)# ospf cost 20
```

cost は、1 ～ 65535 の整数です。

この例では、cost は 20 に設定されています。

ステップ 7　デバイスが hello パケットを受信していないためネイバー OSPF ルータがダウンしていることを宣言するまでデバイスが待機する秒数を設定します。

ospf dead-interval *seconds*

例：

```
ciscoasa(config-interface)# ospf dead-interval 40
```

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。

ステップ 8　ASA が OSPF インターフェイスから hello パケットを送信する時間間隔を指定します。

ospf hello-interval *seconds*

例：

```
ciscoasa(config-interface)# ospf hello-interval 10
```

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。

ステップ 9　OSPF MD5 認証を有効にします。

ospf message-digest-key *key_id* **md5** *key*

例：

```
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
```

次の引数を設定できます。

key_id：範囲 1 ～ 255 の識別子

key：最大 16 バイトの英数字パスワード

通常は、インターフェイスあたり 1 つのキーを使用して、パケット送信時に認証情報を生成するとともに着信パケットを認証します。隣接ルータの同一キー識別子は、キー値を同一にする必要があります。

1 インターフェイスで 2 つ以上のキーを保持しないことをお勧めします。新しいキーを追加したらその都度古いキーを削除して、ローカル システムが古いキー情報を持つ悪意のあるシステムと通信を続けることのないようにしてください。古いキーを削除すると、ロールオーバー中のオーバーヘッドを減らすことにもなります。

ステップ 10　ネットワークに対して、OSPF で指定されたルータを判別するときに役立つプライオリティを設定します。

ospf priority *number_value*

例：

```
ciscoasa(config-interface)# ospf priority 20
```

number_value の引数の範囲は 0 ～ 255 です。

ステップ 11　OSPF インターフェイスに属する隣接ルータに LSA を再送信する間隔を秒単位で指定します。

ospf retransmit-interval *seconds*

例：

```
ciscoasa(config-interface)# ospf retransmit-interval seconds
```

seconds の値は、接続されているネットワーク上の任意の 2 ルータ間で予想されるラウンドトリップ遅延よりも長い秒数でなければなりません。範囲は 1 ～ 8192 秒です。デフォルト値は 5 秒です。

ステップ 12　OSPF 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ために必要な予想時間を秒単位で設定します。

ospf transmit-delay *seconds*

例：

```
ciscoasa(config-interface)# ospf transmit-delay 5
```

seconds の値は、1 ～ 8192 秒です。デフォルト値は 1 秒です。

ステップ 13　1 秒間に送信される hello パケットの数を設定します。

ospf dead-interval minimal hello-interval *multiplier*

例：

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 6
```

有効な値は 3 ～ 20 の整数です。

ステップ 14　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 ネットワークとして指定します。

```
ospf network point-to-point non-broadcast
```

例：

```
ciscoasa(config-interface)# ospf network point-to-point non-broadcast
```

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には、手動で OSPF ネイバーを定義する必要があります。ダイナミック ネイバー探索はできません。詳細については、「スタティック OSPFv2 ネイバーの定義」（P.22-18）を参照してください。さらに、そのインターフェイスに定義できる OSPF ネイバーは 1 つだけです。

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。スタブ エリアに送信される LSA の数をさらに減らすには、ABR で実行する **area stub** コマンドで **no-summary** キーワードを使用して、スタブ エリアにサマリー リンク アドバタイズメント（LSA タイプ 3）が送信されないようにします。

手順

ステップ 1　OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2　OSPF エリアの認証をイネーブルにします。

area *area-id* **authentication**

例：

```
ciscoasa(config-rtr)# area 0 authentication
```

ステップ 3　OSPF エリアの MD5 認証をイネーブルにします。

area *area-id* **authentication message-digest**

例：

```
ciscoasa(config-rtr)# area 0 authentication message-digest
```

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　OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2　NSSA エリアを定義します。

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate**]

例：

```
ciscoasa(config-rtr)# area 0 nssa
```

ステップ 3　サマリー アドレスを設定します。これは、ルーティング テーブルのサイズを小さくするために役立ちます。

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

例：

```
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

OSPF でこのコマンドを使用すると、このアドレスでカバーされる再配布ルートすべての集約として、1 つの外部ルートが OSPF ASBR からアドバタイズされます。

この例のサマリー アドレスの 10.1.0.0 には、10.1.1.0、10.1.2.0、10.1.3.0 などのアドレスが含まれます。外部のリンクステート アドバタイズメントでは、アドレス 10.1.0.0 だけがアドバタイズされます。

（注） OSPF は summary-address 0.0.0.0 0.0.0.0 をサポートしません。

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 および 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 プールの IPv4 アドレスの範囲を割り当てるには、次のコマンドを入力します。

ステップ 1　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 プールを指定します。

router-id cluster-pool hostname | **A.B.C.D** *ip_pool*

例：

```
hostname(config)# ip local pool rpool 1.1.1.1-1.1.1.4
hostname(config)# router ospf 1
hostname(config-rtr)# router-id cluster-pool rpool
hostname(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
hostname(config-rtr)# log-adj-changes
```

cluster-pool キーワードは、個別インターフェイス クラスタリングが設定されている場合に、IP アドレス プールのコンフィギュレーションをイネーブルにします。**hostname | A.B.C.D.**キーワードは、この OSPF プロセスの OSPF ルータ ID を指定します。*ip_pool* 引数には、IP アドレス プールの名前を指定します。

（注） 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。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 19 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

手順の詳細

	目的	コマンド
ステップ 1	OSPFv2 ルーティング プロセスを作成して、この OSPFv2 プロセスのルータ コンフィギュレーション モードを開始します。 *process_id* 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。	**router ospf** *process_id* `ciscoasa(config)# router ospf 2`
ステップ 2	OSPFv2 ネイバーフッドを定義します。 *addr* 引数には OSPFv2 ネイバーの IP アドレスを指定します。*if_name* 引数は、ネイバーとの通信に使用するインターフェイスです。OSPFv2 ネイバーが直接接続されているインターフェイスのいずれとも同じネットワーク上にない場合、interface を指定する必要があります。	**neighbor** *addr* [**interface** *if_name*] `ciscoasa(config-rtr)# neighbor 255.255.0.0 [interface my_interface]`

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。

手順の詳細

	コマンド	目的
ステップ 1	**router ospf** *process_id* **例：** `ciscoasa(config)# router ospf 2`	OSPFv2 ルーティング プロセスを作成して、この OSPFv2 プロセスのルータ コンフィギュレーション モードを開始します。 *process_id* 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
ステップ 2	**timers throttle spf** *spf-start spf-hold spf-maximum* **例：** `ciscoasa(config-router)# timers throttle spf 500 500 600`	ルート計算時間を設定します。 *spf-start* 引数は、OSPF によるトポロジ変更受信と SPF 計算開始との間の遅延時間（ミリ秒）です。0 ～ 600000 の整数に設定できます。 *spf-hold* 引数は、2 回の連続する SPF 計算間の最小時間（ミリ秒）です。0 ～ 600000 の整数に設定できます。 *spf-maximum* 引数は、2 回の連続する SPF 計算間の最大時間（ミリ秒）です。0 ～ 600000 の整数に設定できます。

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 ネイバーについて、**debug ospf adjacency** コマンドを実行せずに確認する必要がある場合に、**log-adj-changes** コマンドを設定します。**log-adj-changes** コマンドでは、少ない出力によってピアの関係が高いレベルで表示されます。それぞれの状態変化メッセージを確認する場合は、**log-adj-changes detail** コマンドを設定します。

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。

手順の詳細

	コマンド	目的
ステップ 1	**router ospf** *process_id* **例：** `ciscoasa(config)# router ospf 2`	OSPFv2 ルーティング プロセスを作成して、この OSPFv2 プロセスのルータ コンフィギュレーション モードを開始します。 *process_id* 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
ステップ 2	**log-adj-changes** [**detail**] **例：** `ciscoasa(config-rtr)# log-adj-changes [detail]`	アップ状態またはダウン状態になったネイバーに対するロギングを設定します。

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.22-21）
- 「OSPFv3 インターフェイスのパラメータの設定」（P.22-21）
- 「OSPFv3 ルータ パラメータの設定」（P.22-27）
- 「OSPFv3 エリア パラメータの設定」（P.22-29）
- 「OSPFv3 パッシブ インターフェイスの設定」（P.22-32）
- 「OSPFv3 アドミニストレーティブ ディスタンスの設定」（P.22-32）
- 「OSPFv3 タイマーの設定」（P.22-33）
- 「スタティック OSPFv3 ネイバーの定義」（P.22-36）
- 「OSPFv3 デフォルト パラメータのリセット」（P.22-37）
- 「syslog メッセージの送信」（P.22-38）
- 「syslog メッセージの抑止」（P.22-38）
- 「サマリー ルート コストの計算」（P.22-39）
- 「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」（P.22-39）
- 「IPv6 サマリー プレフィックスの設定」（P.22-40）
- 「IPv6 ルートの再配布」（P.22-40）

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、次のコマンドを入力するか、次の手順を実行します。

コマンド	目的
ipv6 router ospf *process-id* **例：** `ciscoasa(config)# ipv6 router ospf 10`	OSPFv3 ルーティング プロセスを作成し、IPv6 ルータ コンフィギュレーション モードを開始します。 *process-id* 引数は、このルーティング プロセス内部で使用されるタグです。任意の正の整数が使用できます。このタグは内部専用のため、他のどのデバイス上のタグとも照合する必要はありません。最大 2 つのプロセスが使用できます。

	コマンド	目的
ステップ 1	**interface** *interface_name* **例：** `ciscoasa(config)# interface Gigabitethernet0/0`	インターフェイスをイネーブルにします。
ステップ 2	**ipv6 ospf** *process-id* **area** *area_id* **例：** `ciscoasa(config)# ipv6 ospf 200 area 100`	特定のプロセス ID を持つ OSPFv3 ルーティング プロセスおよび指定したエリア ID を持つ OSPFv3 のエリアを作成します。

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、**ipv6 ospf hello-interval** および **ipv6 ospf dead-interval** 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。

手順の詳細

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process-id* **例：** `ciscoasa(config-if)# ipv6 router ospf 10`	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process-id* 引数は、このルーティング プロセス内部で使用されるタグです。任意の正の整数が使用できます。このタグは内部専用のため、他のどのデバイス上のタグとも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2	**ipv6 ospf area** [*area-num*] [**instance**]
	
	例：
	`ciscoasa(config-if)# interface GigabitEthernet3/2.200`
	`vlan 200`
	`nameif outside`
	`security-level 100`
	`ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31`
	`ipv6 address 3001::1/64 standby 3001::8`
	`ipv6 address 6001::1/64 standby 6001::8`
	`ipv6 enable`
	`ospf priority 255`
	`ipv6 ospf cost 100`
	`ipv6 ospf 100 area 10 instance 200`
		OSPFv3 エリアを作成します。
		
		area-num 引数は、認証がイネーブルになるエリアであり、10 進数値または IP アドレスを指定できます。**instance** キーワードは、インターフェイスに割り当てられるエリア 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 3	次のいずれかの手順を実行し、OSPFv3 インターフェイス パラメータを設定します。	

	ipv6 ospf cost *interface-cost*
	
	例：
	`ciscoasa(config-if)# interface GigabitEthernet3/2.200`
	`vlan 200`
	`nameif outside`
	`security-level 100`
	`ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31`
	`ipv6 address 3001::1/64 standby 3001::8`
	`ipv6 address 6001::1/64 standby 6001::8`
	`ipv6 enable`
	`ospf priority 255`
	`ipv6 ospf cost 100`
	`ipv6 ospf 100 area 10 instance 200`
		インターフェイス上でパケットを送信するコストを明示的に指定します。*interface-cost* 引数は、リンクステート メトリックとして表される符号なし整数値を指定します。値の範囲は、1 ～ 65535 です。デフォルトのコストは帯域幅に基づきます。

コマンド	目的
ipv6 ospf database-filter all out **例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf database-filter all out	OSPFv3 インターフェイスへの発信 LSA をフィルタリングします。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。
ipv6 ospf dead-interval *seconds* **例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf dead-interval 60	hello パケットが確認されない場合に、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設定します。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。デフォルト値は、**ipv6 ospf hello-interval** コマンドで設定された間隔の 4 倍です。

コマンド	目的
ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [[*key-encryption-type*] *key* | **null**} **例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf encryption ipsec spi 1001 esp null sha1 123456789A123456789B123456789C123456789D	インターフェイスに暗号化タイプを指定します。**ipsec** キーワードは、IP セキュリティ プロトコルを指定します。**spi** *spi* キーワード引数のペアは、セキュリティ ポリシー インデックスを指定します。値の範囲は 256 ～ 42949667295 である必要があり、10 進数で入力する必要があります。**esp** キーワードは、カプセル化セキュリティ ペイロードを指定します。*encryption-algorithm* 引数は、ESP で使用される暗号化アルゴリズムを指定します。有効な値は次のとおりです。 • aes-cdc：AES-CDC 暗号化をイネーブルにします。 • 3des：トリプル DES 暗号化をイネーブルにします。 • des：DES 暗号化をイネーブルにします。 • null：暗号化なしの ESP を指定します。 *key-encryption-type* 引数に、次の 2 つのうちいずれかの値を指定します。 • 0：キーは暗号化されません。 • 7：キーは暗号化されます。 *key* 引数は、メッセージ ダイジェストの計算で使用される番号を指定します。この番号の長さは 32 桁の 16 進数（16 バイト）です。キーのサイズは、使用される暗号化アルゴリズムによって異なります。AES-CDC など、一部のアルゴリズムでは、キーのサイズを選択することができます。*authentication-algorithm* 引数は、使用される次のいずれかの暗号化認証アルゴリズムを指定します。 • md5：Message Digest 5（MD5）をイネーブルにします。 • sha1：SHA-1 をイネーブルにします。 **null** キーワードはエリアの暗号化より優先されます。 **（注）** インターフェイスで OSPFv3 暗号化がイネーブルになっており、ネイバーが異なるエリア（たとえば、エリア 0）にあり、ASA がそのエリアとの隣接関係を形成する場合は、ASA のエリアを変更する必要があります。ASA のエリアを 0 に変更すると、OSPFv3 の隣接関係が確立される前に 2 分の遅延が発生します。

コマンド	目的
ipv6 ospf flood-reduction **例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf flood reduction	インターフェイスに LSA のフラッディング削減を指定します。
ipv6 ospf hello-interval *seconds* **例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf hello-interval 15	インターフェイス上で送信される hello パケット間の間隔（秒数）を指定します。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。
ipv6 ospf mtu-ignore **例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf mtu-ignore	DBD パケットを受信した場合の 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。

コマンド	目的
ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**} **例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf network point-to-point non-broadcast	ネットワーク タイプに依存するデフォルト以外のタイプに OSPF ネットワーク タイプを設定します。**point-to-point non-broadcast** キーワードは、ネットワーク タイプをポイントツーポイント、非ブロードキャストに設定します。**broadcast** キーワードは、ネットワーク タイプをブロードキャストに設定します。
ipv6 ospf priority *number-value* **例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf priority 4	ルータ プライオリティを設定します。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。有効値の範囲は 0 ～ 255 です。
ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**] **例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01	非ブロードキャスト ネットワークへの OSPFv3 ルータの相互接続を設定します。

コマンド	目的
ipv6 ospf retransmit-interval *seconds* **例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf retransmit-interval 8	インターフェイスに属する隣接関係の LSA 再送信間の時間を秒単位で指定します。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。
ipv6 ospf transmit-delay *seconds* **例：** ciscoasa(config-if)# interface GigabitEthernet3/2.200 vlan 200 nameif outside security-level 100 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31 ipv6 address 3001::1/64 standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf retransmit-delay 3	インターフェイス上でリンクステート更新パケットを送信する時間を秒単位で設定します。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。

OSPFv3 ルータ パラメータの設定

IPv6 の OSPFv3 ルータ パラメータを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process-id* **例：** ciscoasa(config)# ipv6 router ospf 10	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process-id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

コマンド	目的
ステップ 2 次のいずれかの手順を実行し、オプションの OSPFv3 ルータ パラメータを設定します。	

`area`
 	
例：
`ciscoasa(config-rtr)# area 10`
	OSPFv3 エリア パラメータを設定します。サポートされているパラメータには、0 ～ 4294967295 の 10 進数値のエリア ID、**A.B.C.D** の IP アドレス形式のエリア ID などがあります。

default **例：** `ciscoasa(config-rtr)# default originate`	コマンドをデフォルト値に設定します。**originate** パラメータはデフォルト ルートを配布します。
default-information **例：** `ciscoasa(config-rtr)# default-information`	デフォルト情報の配布を制御します。
distance **例：** `ciscoasa(config-rtr)# distance 200`	ルート タイプに基づいて、OSPFv3 ルート アドミニストレーティブ ディスタンスを定義します。サポートされるパラメータには、1 ～ 254 の値のアドミニストレーティブ ディスタンス、OSPFv3 ディスタンスの **ospf** などがあります。

`exit`
 	
例：
`ciscoasa(config-rtr)# exit`
	IPv6 ルータ コンフィギュレーション モードを終了します。

ignore **例：** `ciscoasa(config-rtr)# ignore lsa`	ルータがタイプ 6 Multicast OSPF（MOSPF）パケットのリンクステート アドバタイズメント（LSA）を受信した場合に、**lsa** パラメータが指定されている syslog メッセージの送信を抑止します。
log-adjacency-changes **例：** `ciscoasa(config-rtr)# log-adjacency-changes detail`	OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。**detail** パラメータによって、すべての状態変更がログに記録されます。
passive-interface [*interface_name*] **例：** `ciscoasa(config-rtr)# passive-interface inside`	インターフェイスでのルーティング アップデートの送受信を抑止します。*interface_name* 引数は、OSPFv3 プロセスが実行されているインターフェイスの名前を指定します。
redistribute **例：** `ciscoasa(config-rtr)# redistribute ospf`	次のパラメータに基づいて 1 つのルーティング ドメインから別のルーティング ドメインへのルートの再配布を設定します。 • **connected**：接続ルートを指定します。 • **ospf**：OSPFv3 ルートを指定します。 • **static**：スタティック ルートを指定します。

コマンド	目的
router-id **例：** `ciscoasa(config-rtr)# router-id 10.1.1.1`	次のパラメータを使用して、指定されたプロセスの固定ルータ ID を作成します。 • **A.B.C.D**：IP アドレス形式の OSPF ルータ ID を指定します。 • **cluster-pool**：個別インターフェイス クラスタリングが設定されている場合に、IP アドレス プールを設定します。クラスタリングで使用される IP アドレス プールの詳細については、「クラスタリングの IP アドレス プールの設定（OSPFv2 および OSPFv3）」（P.22-17）を参照してください。

summary-prefix
 	
例：
`ciscoasa(config-if)# ipv6 router ospf 1`
`ciscoasa(config-router)# router-id 192.168.3.3`
`ciscoasa(config-router)# summary-prefix FECO::/24`
`ciscoasa(config-router)# redistribute static`
	0 ～ 128 の有効な値で IPv6 アドレス サマリーを設定します。**X:X:X:X::X/** パラメータは、IPv6 プレフィックスを指定します。

timers
 	
例：
`ciscoasa(config)# ipv6 router ospf 10`
`ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000`
	ルーティング タイマーを調整します。ルーティング タイマー パラメータは次のとおりです。
	• **lsa**：OSPFv3 LSA タイマーを指定します。
	• **pacing**：OSPFv3 ペーシング タイマーを指定します。
	• **throttle**：OSPFv3 スロットル タイマーを指定します。

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。

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process-id* **例：** `ciscoasa(config)# ipv6 router ospf 1`	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process-id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
ステップ 2	次のいずれかの手順を実行し、オプションの OSPFv3 エリア パラメータを設定します。	
	area *area-id* **default-cost** *cost* **例：** `ciscoasa(config-rtr)# area 1 default-cost nssa`	NSSA エリアまたはスタブ エリアのサマリー デフォルト コストを設定します。

コマンド	目的
area *area-id* **range** *ipv6-prefix/prefix-length* [**advertise** | **not advertise**] [**cost** *cost*] **例：** `ciscoasa(config-rtr)# area 1 range FE01:1::1/64`	アドレスおよび境界ルータ専用のマスクと一致するルートを集約します。 *area-id* 引数は、ルートが集約されるエリアを識別します。値には、10 進数または IPv6 プレフィックスを指定できます。*ipv6-prefix* 引数は、IPv6 プレフィックスを指定します。*prefix-length* 引数は、プレフィックス長を指定します。**advertise** キーワードは、アドレス範囲ステータスをアドバタイズに設定し、Type 3 サマリー LSA を生成します。**not-advertise** キーワードはアドレス範囲ステータスを DoNotAdvertise に設定します。Type 3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。**cost** *cost* キーワード引数のペアは、宛先への最短パスを決定するために OSPF SPF 計算で使用されるサマリー ルートのメトリックまたはコストを指定します。有効な値の範囲は 0 ～ 16777215 です。
area *area-id* **nssa** **例：** `ciscoasa(config-rtr)# area 1 nssa`	NSSA エリアを指定します。
area *area-id* **stub** **例：** `ciscoasa(config-rtr)# area 1 stub`	スタブ エリアを指定します。

コマンド	目的
area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*] **例：** `ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello-interval 5`	仮想リンクとそのパラメータを定義します。 *area-id* 引数は、ルートが集約されるエリアを識別します。**virtual link** キーワードは、仮想リンク ネイバーの作成を指定します。*router-id* 引数は、仮想リンク ネイバーに関連付けられたルータ ID を指定します。ルータ ID を表示するには、**show ospf** コマンドまたは **show ipv6 ospf** コマンドを入力します。デフォルト値はありません。**hello-interval** キーワードは、インターフェイス上で送信される hello パケット間の時間を秒単位で指定します。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。**retransmit-interval** *seconds* キーワード引数のペアは、インターフェイスに属する隣接関係の LSA 再送信間の時間を秒単位で指定します。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。**transmit-delay** *seconds* キーワード引数のペアは、インターフェイス上でリンクステート更新パケットを送信するために必要とされる時間を秒単位で設定します。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。**dead-interval** *seconds* キーワード引数のペアは、hello パケットが確認されない場合に、ルータがダウンしたとネイバーが判断するまでの時間を秒単位で指定します。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。**ttl-security hops** キーワードは仮想リンクの存続可能時間（TTL）セキュリティを設定します。*hop-count* 引数の値は 1 ～ 254 の範囲で指定できます。

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。

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process_id* **例：** ciscoasa(config-if)# ipv6 router ospf 1	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process_id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
ステップ 2	**passive-interface** [*interface_name*] **例：** ciscoasa(config-rtr)# passive-interface inside	インターフェイスでのルーティング アップデートの送受信を抑止します。*interface_name* 引数は、OSPFv3 プロセスが実行されているインターフェイスの名前を指定します。*interface_name* 引数を指定しない場合は、OSPFv3 プロセス *process_id* のすべてのインターフェイスがパッシブとなります。

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。

手順の詳細

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process_id* **例：** ciscoasa(config-if)# ipv6 router ospf 1	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process_id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
ステップ 2	**distance** [**ospf** {**external** | **inter-area** | **intra-area**}] *distance* **例：** ciscoasa(config-rtr)# distance ospf external 200	OSPFv3 ルートのアドミニストレーティブ ディスタンスを設定します。 **ospf** キーワードは、OSPFv3 ルートを指定します。**external** キーワードは、OSPFv3 の外部タイプ 5 およびタイプ 7 ルートを指定します。**inter-area** キーワードは、OSPVv3 のエリア間ルートを指定します。**intra-area** キーワードは、OSPFv3 のエリア内ルートを指定します。*distance* 引数は、10 ～ 254 の整数であるアドミニストレーティブ ディスタンスを指定します。

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。

手順の詳細

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process-id* **例：** `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process-id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
ステップ 2	**timers lsa arrival** *milliseconds* **例：** `ciscoasa(config-rtr)# timers lsa arrival 2000`	ASA が OSPF ネイバーから同一の LSA を受け入れる最小間隔を設定します。 *milliseconds* 引数は、ネイバーから到着する同じ LSA の受け入れの間で経過する最小遅延をミリ秒単位で指定します。有効な範囲は 0 ～ 6,000,000 ミリ秒です。デフォルトは 1000 ミリ秒です。

LSA フラッディング 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。

手順の詳細

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process-id* **例：** `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process-id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
ステップ 2	**timers pacing flood** *milliseconds* **例：** `ciscoasa(config-rtr)# timers lsa flood 20`	LSA フラッディング パケット ペーシングを設定します。 *milliseconds* 引数は、フラッディング キュー内の LSA が更新と更新の間にペーシングされる時間（ミリ秒）を指定します。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。

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。

手順の詳細

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process-id* **例：** `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process-id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
ステップ 2	**timers pacing lsa-group** *seconds* **例：** `ciscoasa(config-rtr)# timers pacing lsa-group 300`	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、またはエージングを行う間隔を変更します。 *seconds* 引数は、LSA がグループ化、リフレッシュ、チェックサム計算、またはエージングされる間隔を秒単位で指定します。有効な範囲は 10 ～ 1800 秒です。デフォルト値は 240 秒です。

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。

手順の詳細

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process-id* **例：** `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process-id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
ステップ 2	**timers pacing retransmission** *milliseconds* **例：** `ciscoasa(config-rtr)# timers pacing retransmission 100`	LSA 再送信パケット ペーシングを設定します。 *milliseconds* 引数は、再送信キュー内の LSA がペーシングされる時間（ミリ秒）を指定します。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 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可能にするダイナミック 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。

手順の詳細

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process-id* **例：** `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process-id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
ステップ 2	次のいずれかのオプションを選択します。	
	timers throttle lsa *milliseconds1 milliseconds2 milliseconds3* **例：** `ciscoasa(config-rtr)# timers throttle lsa 500 6000 8000`	OSPFv3 LSA スロットリングを設定します。 *milliseconds1* 引数は、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。*milliseconds2* 引数は、同じ LSA を送信する最大遅延をミリ秒単位で指定します。*milliseconds3* 引数は、同じ LSA を送信する最小遅延をミリ秒単位で指定します。 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、指定された最大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。 LSA スロットリングのデフォルト値は次のとおりです。 • *milliseconds1* の場合、デフォルト値は 0 ミリ秒です。 • *milliseconds2* および *milliseconds3* の場合、デフォルト値は 5000 ミリ秒です。
	timers throttle spf *milliseconds1 milliseconds2 milliseconds3* **例：** `ciscoasa(config-rtr)# timers throttle spf 5000 12000 16000`	OSPFv3 SPF スロットリングを設定します。 *milliseconds1* 引数は、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。*milliseconds2* 引数は、最初と 2 番目の SPF 計算の間の遅延をミリ秒単位で指定します。*milliseconds3* 引数は、SPF 計算の最大待機時間をミリ秒単位で指定します。 SPF スロットリングでは、*milliseconds2* または *milliseconds3* が *milliseconds1* よりも小さい場合、OSPFv3 が自動的に *milliseconds1* の値に修正します。同様に、*milliseconds3* が *milliseconds2* より小さい場合、OSPFv3 が自動的に *milliseconds2* の値に修正します。 SPF スロットリングのデフォルト値は次のとおりです。 • *milliseconds1* の場合、デフォルト値は 5000 ミリ秒です。 • *milliseconds2* および *milliseconds3* の場合、デフォルト値は 10000 ミリ秒です。

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 19 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。

手順の詳細

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process-id* **例：** `ciscoasa(config)# ipv6 router ospf 1`	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process-id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2	**ipv6 ospf neighbor** *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]
	
	例：
	`ciscoasa(config-if)# interface ethernet0/0`
	`ipv6 ospf neighbor`
	`FE80::A8BB:CCFF:FE00:C01`
		非ブロードキャスト ネットワークへの OSPFv3 ルータの相互接続を設定します。

OSPFv3 デフォルト パラメータのリセット

OSPFv3 パラメータをデフォルト値に戻すには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process-id* **例：** `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process_id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
ステップ 2	**default** [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **discard-route** | **distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**] **例：** `ciscoasa(config-rtr)# default metric 5`	オプションのパラメータをデフォルト値に戻します。 **area** キーワードは、OSPFv3 エリア パラメータを指定します。**auto-cost** キーワードは、帯域幅に従って OSPFv3 インターフェイス コストを指定します。**default-information** キーワードはデフォルト情報を配布します。**default-metric** キーワードは再配布ルートのメトリックを指定します。**discard-route** キーワードは、廃棄ルートのインストールをイネーブルまたはディセーブルにします。**distance** キーワードはアドミニストレーティブ ディスタンスを指定します。**distribute-list** キーワードは、ルーティング アップデートのネットワークをフィルタリングします。**Ignore** キーワードは、特定のイベントを無視します。**log-adjacency-changes** キーワードは、隣接状態の変更をログに記録します。**maximum-paths** キーワードは、複数のパスを介して複数のパケットを転送します。**passive-interface** キーワードは、インターフェイス上のルーティング アップデートを抑止します。**redistribute** キーワードは、別のルーティング プロトコルからの IPv6 プレフィックスを再配布します。**router-id** キーワードは、指定されたルーティング プロセスのルータ ID を指定します。**summary-prefix** キーワードは、IPv6 サマリー プレフィックスを指定します。**timers** キーワードは、OSPFv3 タイマーを指定します。

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。

手順の詳細

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process-id* **例：** `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process-id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
ステップ 2	**log-adjacency-changes** [**detail**] **例：** `ciscoasa(config-rtr)# log-adjacency-changes detail`	OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。 **detail** キーワードは、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。

手順の詳細

	コマンド	目的
ステップ 1	**router ospf** *process_id* **例：** `ciscoasa(config-if)# router ospf 1`	OSPFv2 ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。 *process_id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
ステップ 2	**ignore lsa mospf** **例：** `ciscoasa(config-rtr)# ignore lsa mospf`	ルータが、サポートされていない LSA タイプ 6 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、次のコマンドを入力します。

コマンド	目的
compatible rfc1583 **例：** `ciscoasa (config-rtr)# compatible rfc1583`	RFC 1583 に従ってサマリー ルート コストを計算する方式に復元します。

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。

手順の詳細

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process-id* **例：** `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process-id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
ステップ 2	**default-information originate** [**always**] **metric** *metric-value* [**metric-type** *type-value*] [**route-map** *map-name*] **例：** `ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2`	OSPFv3 ルーティング ドメインへのデフォルトの外部ルートを生成します。 **always** キーワードは、デフォルト ルートがあるかどうかにかかわらず、デフォルト ルートをアドバタイズします。**metric** *metric-value* キーワード引数のペアは、デフォルト ルートの生成に使用するメトリックを指定します。**default-metric** コマンドを使用して値を指定しない場合、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。**metric-type** *type-value* キーワード引数のペアは、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る外部リンク タイプを指定します。有効な値は次のいずれかになります。 • 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。**route-map** *map-name* キーワード引数のペアは、ルート マップが一致し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 プロセスを指定します。

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。

手順の詳細

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process-id* **例：** `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process_id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2	**summary-prefix** *prefix* [**not-advertise** | **tag** *tag-value*]
	
	例：
	`ciscoasa(config-if)# ipv6 router ospf 1`
	`ciscoasa(config-rtr)# router-id 192.168.3.3`
	`ciscoasa(config-rtr)# summary-prefix FECO::/24`
	`ciscoasa(config-rtr)# redistribute static`
		IPv6 サマリー プレフィックスを設定します。
		
		prefix 引数は、宛先の IPv6 ルート プレフィックスです。**not-advertise** キーワードは、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抑止します。このキーワードは OSPFv3 だけに適用されます。**tag** *tag-value* キーワード引数のペアは、ルート マップで再配布を制御するために一致値として使用できるタグ値を指定します。このキーワードは OSPFv3 だけに適用されます。

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。

手順の詳細

	コマンド	目的
ステップ 1	**ipv6 router ospf** *process-id* **例：** `ciscoasa(config-if)# ipv6 router ospf 1`	OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。 *process-id* 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

	コマンド	目的
ステップ 2	**redistribute** *source-protocol* [*process-id*] [**include-connected** {[**level-1** | **level-2**}] [*as-number*] [**metric** [*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**external** [**1**|**2**] | **internal** | **nssa-external** [**1**|**2**]}] [**tag** *tag-value*] [**route-map** *map-tag*] **例：** `ciscoasa(config-rtr)# redistribute connected 5 type-1`	ある OSPFv3 プロセスから別の OSPFv3 プロセスに IPv6 ルートを再配布します。 *source-protocol* 引数は、ルートの再配布元となるソース プロトコルを指定します。これは、スタティック、接続済み、または OSPFv3 にすることができます。*process-id* 引数は、OSPFv3 ルーティング プロセスがイネーブルになったときに管理目的で割り当てられる番号です。**include-connected** キーワードは、ソース プロトコルから学習したルートと、ソース プロトコルが動作しているインターフェイス上の接続先プレフィックスを、ターゲット プロトコルが再配布できるようにします。**level-1** キーワードは、Intermediate System-to-Intermediate System（IS-IS）用に、レベル 1 ルートが他の IP ルーティング プロトコルに個別に再配布されることを指定します。**level-1-2** キーワードは、IS-IS 用に、レベル 1 とレベル 2 の両方のルートが他の IP ルーティング プロトコルに再配布されることを指定します。**level-2** キーワードは、IS-IS 用に、レベル 2 ルートが他の IP ルーティング プロトコルに個別に再配布されることを指定します。**metric** *metric-value* キーワード引数のペアでは、ある OSPFv3 プロセスのルートを同じルータ上の別の OSPFv3 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 OSPFv3 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。**metric transparent** キーワードにより、RIP は RIP メトリックとして再配布ルートのルーティング テーブル メトリックを使用します。**metric-type** *type-value* キーワード引数のペアは、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る外部リンク タイプを指定します。有効な値は、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。**metric-type** キーワードに値が指定されていない場合、ASA は、タイプ 2 外部ルートを受け入れます。IS-IS の場合、リンク タイプは、63 未満の IS-IS メトリックの場合は内部、64 を超えて 128 未満の IS-IS メトリックの場合は外部となります。デフォルトは、内部です。**match** キーワードは、他のルーティング ドメインにルートを再配布し、次のいずれかのオプションとともに使用されます。自律システムの外部であり、タイプ 1 またはタイプ 2 の外部ルートとして OSPFv3 にインポートされるルートの場合は **external** [**1**|**2**]、特定の自律システムの内部にあるルートの場合は **internal**、自律システムの外部であり、タイプ 1 またはタイプ 2 の外部ルートとして IPv6 の NSSA で OSPFv3 にインポートされるルートの場合は **nssa-external** [**1**|**2**]。**tag** *tag-value* キーワード引数のペアは、ASBR 間で情報を通信するために使用できる、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。有効値の範囲は、0 ～ 4294967295 です。**route-map** キーワードは、送信元ルーティング 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チェックするルート マップを指定します。このキーワードを指定しない場合、すべてのルートが再配布されます。このキーワードを指定し、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。*map-tag* 引数は、設定されたルート マップを識別します。

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（クティブ ユニットがクラッシュしてスタンバイ ユニットがフェールオーバー（HA）モードで処理を引き継ぐ場合や、マスター ユニットがクラッシュしてクラスタ モードでスレーブ ユニットが新しいマスターとして選択される場合など）、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。

機能の設定

Cisco NSF グレースフル リスタート メカニズムは、リスタート アクティビティを示すために、Hello パケットで RS ビットが設定された LLS ブロックを送信するため、LLS 機能に依存しています。IETF NSF メカニズムは、リスタート アクティビティを示すために、タイプ 9 の opaque LSA を送信するため、opaque LSA 機能に依存しています。機能を設定するには、次のコマンドを入力します。

コマンド	目的
router ospf *process_id* **例：** ciscoasa(config)# router ospf 2	OSPF ルーティング プロセスを作成し、再配布する OSPF プロセスのルータ コンフィギュレーション モードに入ります。 *process_id* 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。
capability {**lls**|**opaque**} **例：** ciscoasa(config-router)# capability lls	LLS データ ブロックまたは opaque LSA の使用をイネーブルにして、NSF をイネーブルにします。 **lls** キーワードは、Cisco NSF グレースフル リスタート メカニズムに対して、LLS 機能をイネーブルにするために使用されます。 **opaque** キーワードは、IETF NSF グレースフル リスタート メカニズムに対して、opaque LSA 機能をイネーブルにするために使用されます。

OSPFv2 のグレースフル リスタートの設定

OSPFv2 には、Cisco NSF と IETF NSF の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、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、次のコマンドを入力します。

コマンド	目的
nsf cisco [**enforce global**] **例：** ciscoasa(config-router)# nsf cisco	NSF 対応デバイスで Cisco NSF をイネーブルにします。 **enforce global** キーワードは、非 NSF 認識ネイバー デバイスが検出されると、NSF リスタートをキャンセルします。
capability {**lls**|**opaque**} **例：** ciscoasa(config-router)# capability lls	（オプション）NSF 認識デバイスで、Cisco NSF ヘルパー モードをイネーブルにします。 このコマンドは、デフォルトでイネーブルになっています。このコマンドの no 形式を使用すると、ディセーブルになります。

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、次のコマンドを入力します。

コマンド	目的
nsf ietf [**restart interval** *seconds*] **例：** `ciscoasa(config-router)# nsf ietf restart interval 80`	NSF 対応デバイスで IETF NSF を有効にします。 （オプション）**restart interval** *seconds* は、グレースフル リスタート間隔の長さを秒単位で指定します。有効な値は 1 ～ 1800 秒です。デフォルト値は 120 秒です。 **（注）** 隣接関係が有効になるまでにかかる時間よりもリスタート間隔が小さい値に設定されている場合、グレースフル リスタートは終了することがあります。たとえば 30 秒以下の再起動間隔は、サポートされていません。
nsf ietf helper [**strict-lsa-checking**] **例：** `ciscoasa(config-router)# nsf ietf helper`	（オプション）NSF 認識デバイスで、IETF NSF ヘルパー モードをイネーブルにします。 （オプション）**strict-LSA-checking** キーワードは、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。 **（注）** このコマンドは、デフォルトでイネーブルになっています。このコマンドの no 形式を使用すると、ディセーブルになります。

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、次のコマンドを入力します。

コマンド	目的

interface *physical_interface*
ipv6 enable
 	
例：
`ciscoasa(config)# interface ethernet 0/0`
`ciscoasa(config-if)# ipv6 enable`
	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
	physical_interface 引数は、OSPFv3 NSF に参加するインターフェイスを識別します。

コマンド	目的
graceful-restart [**restart interval** *seconds*] **例：** ciscoasa(config-router)# graceful-restart restart interval 80	NSF 対応デバイスで OSPFv3 のグレースフル リスタートをイネーブルにします。 （オプション）**restart interval** *seconds* は、グレースフル リスタート間隔の長さを秒単位で指定します。有効な値は 1 ～ 1800 秒です。デフォルト値は 120 秒です。 **（注）** 隣接関係が有効になるまでにかかる時間よりもリスタート間隔が小さい値に設定されている場合、グレースフル リスタートは終了することがあります。たとえば 30 秒以下の再起動間隔は、サポートされていません。
graceful-restart helper [**strict-lsa-checking**] **例：** ciscoasa(config-router)# graceful-restart helper strict-lsa-checking	NSF 認識デバイスで OSPFv3 のグレースフル リスタートをイネーブルにします。 （オプション）**strict-LSA-checking** キーワードは、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。 **（注）** グレースフル リスタート ヘルパー モードは、デフォルトでイネーブルになっています。

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、次のコマンドを入力します。

コマンド	目的
clear configure router ospf *pid* **例：** ciscoasa(config)# clear configure router ospf 1000	イネーブルにした OSPFv2 設定全体を削除します。設定をクリアした後、**router ospf** コマンドを使用して OSPF を再設定する必要があります。

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、次のコマンドを入力します。

コマンド	目的
clear configure ipv6 router ospf *process-id* **例：** ciscoasa(config)# clear configure ipv6 router ospf 1000	イネーブルにした OSPFv3 設定全体を削除します。設定をクリアした後、**ipv6 router ospf** コマンドを使用して OSPFv3 を再設定する必要があります。

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　OSPFv2 をイネーブルにするには、次のコマンドを入力します。

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

ステップ 2　（オプション）1 つの OSPFv2 プロセスから別の OSPFv2 プロセスにルートを再配布するには、次のコマンドを入力します。

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

ステップ 3　（オプション）OSPFv2 インターフェイス パラメータを設定するには、次のコマンドを入力します。

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
ciscoasa(config-rtr)# interface inside
ciscoasa(config-interface)# ospf cost 20
ciscoasa(config-interface)# ospf retransmit-interval 15
ciscoasa(config-interface)# ospf transmit-delay 10
ciscoasa(config-interface)# ospf priority 20
ciscoasa(config-interface)# ospf hello-interval 10
ciscoasa(config-interface)# ospf dead-interval 40
ciscoasa(config-interface)# ospf authentication-key cisco
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
ciscoasa(config-interface)# ospf authentication message-digest
```

ステップ 4　（オプション）OSPFv2 エリア パラメータを設定するには、次のコマンドを入力します。

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# area 0 authentication
ciscoasa(config-rtr)# area 0 authentication message-digest
ciscoasa(config-rtr)# area 17 stub
ciscoasa(config-rtr)# area 17 default-cost 20
```

ステップ 5　（オプション）ルート計算タイマーを設定し、ログにネイバーのアップおよびダウンのメッセージを表示するには、次のコマンドを入力します。

```
ciscoasa(config-rtr)# timers spf 10 120
ciscoasa(config-rtr)# log-adj-changes [detail]
```

ステップ 6　（オプション）現在の OSPFv2 の設定を表示するには、**show ospf** コマンドを入力します。

次に、**show ospf** コマンドの出力例を示します。

```
ciscoasa(config)# show ospf

Routing Process "ospf 2" with ID 10.1.89.2 and Domain ID 0.0.0.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs.Minimum LSA arrival 1 secs
Number of external LSA 5.Checksum Sum 0x 26da6
Number of opaque AS LSA 0.Checksum Sum 0x     0
```

```
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1.1 normal 0 stub 0 nssa
External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm executed 2 times
        Area ranges are
        Number of LSA 5.Checksum Sum 0x 209a3
        Number of opaque link LSA 0.Checksum Sum 0x     0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

ステップ 7　OSPFv2 設定をクリアするには、次のコマンドを入力します。

```
ciscoasa(config)# clear configure router ospf pid
```

OSPFv3 の設定例

次に、インターフェイス レベルで OSPFv3 をイネーブルにして設定する例を示します。

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf 1 area 1
```

次に、**show running-config ipv6** コマンドの出力例を示します。

```
ciscoasa (config)# show running-config ipv6
ipv6 router ospf 1
 log-adjacency-changes
```

次に、**show running-config interface** コマンドの出力例を示します。

```
ciscoasa (config-if)# show running-config interface GigabitEthernet3/1
interface GigabitEthernet3/1
 nameif fda
 security-level 100
 ip address 1.1.11.1 255.255.255.0 standby 1.1.11.2
 ipv6 address 9098::10/64 standby 9098::11
 ipv6 enable
 ipv6 ospf 1 area 1
```

次に、OSPFv3 専用インターフェイスを設定する例を示します。

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# nameif fda
ciscoasa (config-if)# security-level 100
ciscoasa (config-if)# ip address 10.1.11.1 255.255.255.0 standby 10.1.11.2
ciscoasa (config-if)# ipv6 address 9098::10/64 standby 9098::11
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf cost 900
ciscoasa (config-if)# ipv6 ospf hello-interval 20
ciscoasa (config-if)# ipv6 ospf network broadcast
ciscoasa (config-if)# ipv6 ospf database-filter all out
ciscoasa (config-if)# ipv6 ospf flood-reduction
ciscoasa (config-if)# ipv6 ospf mtu-ignore
ciscoasa (config-if)# ipv6 ospf 1 area 1 instance 100
```

```
ciscoasa (config-if)# ipv6 ospf encryption ipsec spi 890 esp null md5
123456789012345678901234567890123456
ciscoasa (config)# ipv6 router ospf 1
ciscoasa (config)# area 1 nssa
ciscoasa (config)# distance ospf intra-area 190 inter-area 100 external 100
ciscoasa (config)# timers lsa arrival 900
ciscoasa (config)# timers pacing flood 100
ciscoasa (config)# timers throttle lsa 900 900 900
ciscoasa (config)# passive-interface fda
ciscoasa (config)# log-adjacency-changes
ciscoasa (config)# redistribute connected metric 100 metric-type 1 tag 700
```

OSPFv3 仮想リンクを設定する方法の例については、次の URL を参照してください。

http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080b8fd06.shtml

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。

さまざまな OSPFv2 ルーティング統計情報をモニタまたは表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
show ospf [*process-id* [*area-id*]]	OSPFv2 ルーティング プロセスに関する一般情報を表示します。
show ospf border-routers	ABR および ASBR までの内部 OSPFv2 ルーティング テーブル エントリを表示します。
show ospf [*process-id* [*area-id*]] **database**	特定のルータの OSPFv2 データベースに関係する情報のリストを表示します。

コマンド	目的
show ospf flood-list *if-name*	（OSPFv2 パケット ペーシングの観察のため）インターフェイスへのフラッディングを待機している LSA のリストを表示します。 OSPFv2 アップデート パケットは、自動的にペーシングされるため、各パケットの送信間隔が 33 ミリ秒未満になることはありません。ペーシングを行わないと、リンクが低速の状態でアップデート パケットの一部が失われたり、ネイバーがアップデートを十分すばやく受信できなくなったり、あるいは、ルータがバッファ スペースを使い切ってしまったりすることがあります。たとえば、ペーシングを行わないと、次のいずれかのトポロジが存在する場合にパケットがドロップされる可能性があります。 • 高速ルータがポイントツーポイント リンクを介して低速のルータと接続している。 • フラッディング中に、複数のネイバーから 1 つのルータに同時にアップデートが送信される。 ペーシングは、再送信間でも、送信効率を高めて再送信パケットの損失を最小にするために利用されます。インターフェイスからの送信を待機している LSA を表示することもできます。ペーシングの利点は、OSPFv2 アップデートおよび再送信パケットの送信の効率をよくすることです。 この機能を設定するタスクはありません。自動的に行われます。
show ospf interface [*if_name*]	OSPFv2 関連のインターフェイス情報を表示します。
show ospf neighbor [*interface-name*] [*neighbor-id*] [**detail**]	OSPFv2 ネイバー情報をインターフェイスごとに表示します。
show ospf request-list *neighbor if_name*	ルータで要求されるすべての LSA のリストを表示します。
show ospf retransmission-list *neighbor if_name*	再送信を待機しているすべての LSA のリストを表示します。
show ospf [*process-id*] **summary-address**	OSPFv2 プロセスで設定されているサマリー アドレスのすべての再配布情報のリストを表示します。
show ospf [*process-id*] **traffic**	特定の OSPFv2 インスタンスで送信または受信されたパケットのさまざまなタイプのリストを表示します。
show ospf [*process-id*] **virtual-links**	OSPFv2 関連の仮想リンク情報を表示します。
show route cluster	クラスタリングの追加 OSPFv2 ルートの同期情報を表示します。

さまざまな OSPFv3 ルーティング統計情報をモニタまたは表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
show ipv6 ospf [*process-id* [*area-id*]]	OSPFv3 ルーティング プロセスに関する一般的な情報を表示します。
show ipv6 ospf [*process-id*] **border-routers**	ABR および ASBR までの内部 OSPFv3 ルーティング テーブル エントリを表示します。
show ipv6 ospf [*process-id* [*area-id*]] **database** [**external** | **inter-area prefix** | **inter-area-router** | **network** | **nssa-external** | **router** | **area** | **as** | **ref-lsa** | [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*]] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] | **self-originate**] [**internal**] [**database-summary**]	特定のルータの OSPFv3 データベースに関する情報のリストを表示します。
show ipv6 ospf [*process-id* [*area-id*]] **events**	OSPFv3 イベント情報を表示します。
show ipv6 ospf [*process-id*] [*area-id*] **flood-list** *interface-type interface-number*	（OSPFv3 パケット ペーシングの観察のため）インターフェイスへのフラッディングを待機している LSA のリストを表示します。 OSPFv3 アップデート パケットは、自動的にペーシングされるため、各パケットの送信間隔が 33 ミリ秒未満になることはありません。ペーシングを行わないと、リンクが低速の状態でアップデート パケットの一部が失われたり、ネイバーがアップデートを十分すばやく受信できなくなったり、あるいは、ルータがバッファ スペースを使い切ってしまったりすることがあります。たとえば、ペーシングを行わないと、次のいずれかのトポロジが存在する場合にパケットがドロップされる可能性があります。 • 高速ルータがポイントツーポイント リンクを介して低速のルータと接続している。 • フラッディング中に、複数のネイバーから 1 つのルータに同時にアップデートが送信される。 ペーシングは、再送信間でも、送信効率を高めて再送信パケットの損失を最小にするために利用されます。インターフェイスからの送信を待機している LSA を表示することもできます。ペーシングの利点は、OSPFv3 アップデートおよび再送信パケットの送信の効率をよくすることです。 この機能を設定するタスクはありません。自動的に行われます。

コマンド	目的
show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] [**brief**]	OSPFv3 関連のインターフェイス情報を表示します。
show ipv6 ospf neighbor [*process-id*] [*area-id*] [*interface-type interface-number*] [*neighbor-id*] [**detail**]	OSPFv3 ネイバー情報をインターフェイスごとに表示します。
show ipv6 ospf [*process-id*] [*area-id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]	ルータで要求されるすべての LSA のリストを表示します。
show ipv6 ospf [*process-id*] [*area-id*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]	再送信を待機しているすべての LSA のリストを表示します。
show ipv6 ospf statistic [*process-id*] [**detail**]	さまざまな OSPFv3 統計情報を表示します。
show ipv6 ospf [*process-id*] **summary-prefix**	OSPFv3 プロセスで設定されているサマリー アドレスのすべての再配布情報のリストを表示します。
show ipv6 ospf [*process-id*] **timers** [**lsa-group** | **rate-limit**]	OSPFv3 タイマー情報を表示します。
show ipv6 ospf [*process-id*] **traffic** [*interface_name*]	OSPFv3 トラフィック関連の統計情報を表示します。
show ipv6 ospf virtual-links	OSPFv3 関連の仮想リンク情報を表示します。
show ipv6 route cluster [**failover**] [**cluster**] [**interface**] [**ospf**] [**summary**]	クラスタ内の IPv6 ルーティング テーブルのシーケンス番号、IPv6 再コンバージェンス タイマーのステータス、および IPv6 ルーティング エントリのシーケンス番号を表示します。

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 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。

表 22-1　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。 **route ospf** コマンドが導入されました。
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)	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。
クラスタ		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。 **show route cluster**、**show ipv6 route cluster**、**debug route cluster**、**router-id cluster-pool** の各コマンドが導入または変更されました。
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。 **ipv6 ospf**、**ipv6 ospf area**、**ipv6 ospf cost**、**ipv6 ospf database-filter all out**、**ipv6 ospf dead-interval**、**ipv6 ospf encryption**、**ipv6 ospf hello-interval**、**ipv6 ospf mtu-ignore**、**ipv6 ospf neighbor**、**ipv6 ospf network**、**ipv6 ospf flood-reduction**、**ipv6 ospf priority**、**ipv6 ospf retransmit-interval**、**ipv6 ospf transmit-delay**、**ipv6 router ospf**、**ipv6 router ospf area**、**ipv6 router ospf default**、**ipv6 router ospf default-information**、**ipv6 router ospf distance**、**ipv6 router ospf exit**、**ipv6 router ospf ignore**、**ipv6 router ospf log-adjacency-changes**、**ipv6 router ospf no**、**ipv6 router ospf passive-interface**、**ipv6 router ospf redistribute**、**ipv6 router ospf router-id**、**ipv6 router ospf summary-prefix**、**ipv6 router ospf timers**、**area encryption**、**area range**、**area stub**、**area nssa**、**area virtual-link**、**default**、**default-information originate**、**distance**、**ignore lsa mospf**、**log-adjacency-changes**、**redistribute**、**router-id**、**summary-prefix**、**timers lsa arrival**、**timers pacing flood**、**timers pacing lsa-group**、**timers pacing retransmission**、**timers throttle**、**show ipv6 ospf**、**show ipv6 ospf border-routers**、**show ipv6 ospf database**、**show ipv6 ospf events**、**show ipv6 ospf flood-list**、**show ipv6 ospf graceful-restart**、**show ipv6 ospf interface**、**show ipv6 ospf neighbor**、**show ipv6 ospf request-list**、**show ipv6 ospf retransmission-list**、**show ipv6 ospf statistic**、**show ipv6 ospf summary-prefix**、**show ipv6 ospf timers**、**show ipv6 ospf traffic**、**show ipv6 ospf virtual-links**、**show ospf**、**show running-config ipv6 router**、**clear ipv6 ospf**、**clear configure ipv6 router**、**debug ospfv3**、**ipv6 ospf neighbor** の各コマンドが導入または変更されました。

表 22-1　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。 次のコマンドが変更されました。**ospf dead-interval**
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。 次のコマンドが導入されました。**timers lsa arrival**、**timers pacing**、**timers throttle** 次のコマンドが削除されました。**Timers spf**、**timers lsa-grouping-pacing**
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。 次のコマンドが導入されました。**distribute-list** 次の画面が導入されました。
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。 次のコマンドが変更されました。**show ospf events**、**show ospf rib**、**show ospf statistics**、**show ospf border-routers [detail]**、**show ospf interface brief**
OSPF 再配布 BGP		OSPF 再配布機能が追加されました。 次のコマンドが追加されました。**redistribute bgp**
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。 次のコマンドが追加されました。**capability**、**nsf cisco**、**nsf cisco helper**、**nsf ietf**、**nsf ietf helper**、**nsf ietf helper strict-lsa-checking**、**graceful-restart**、**graceful-restart helper**、**graceful-restart helper strict-lsa-checking**

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」（P.23-1）
- 「EIGRP のライセンス要件」（P.23-3）
- 「ガイドラインと制限事項」（P.23-3）
- 「EIGRP の設定」（P.23-3）
- 「EIGRP のカスタマイズ」（P.23-5）
- 「EIGRP のモニタリング」（P.23-18）
- 「EIGRP の設定例」（P.23-19）
- 「EIGRP の機能履歴」（P.23-20）

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 ルーティングとクラスタリング」（P.18-10）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

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

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 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.23-4）
- 「EIGRP スタブ ルーティングのイネーブル化」（P.23-4）

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。

手順の詳細

	コマンド	目的
ステップ 1	**router eigrp** *as-num* **例：** `ciscoasa(config)# router eigrp 2`	EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。 *as-num* 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2	**network** *ip-addr* [*mask*]
	
	例：
	`ciscoasa(config)# router eigrp 2`
	`ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`
		EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。このコマンドで、1 つ以上の **network** 文を設定できます。
		
		直接接続されているネットワークとスタティックなネットワークが定義されたネットワークに含まれていれば、ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。
		
		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、「EIGRP のインターフェイスの設定」（P.23-7）を参照してください。

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をすべての隣接ルータに送信します。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。

手順の詳細

	コマンド	目的
ステップ 1	**router eigrp** *as-num* **例：** ciscoasa(config)# router eigrp *2*	EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。 *as-num* 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。
ステップ 2	**network** *ip-addr* [*mask*] **例：** ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0	EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。このコマンドで、1 つ以上の **network** 文を設定できます。 直接接続されているネットワークとスタティックなネットワークが定義されたネットワークに含まれていれば、ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。 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、「受動インターフェイスの設定」（P.23-8）の項を参照してください。
ステップ 3	**eigrp stub** {**receive-only** | [**connected**] [**redistributed**] [**static**] [**summary**]} **例：** ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0 ciscoasa(config-router)# eigrp stub {receive-only | [connected] [redistributed] [static] [summary]}	スタブ ルーティング プロセスを設定します。スタブ ルーティング プロセスから配布ルータにアドバタイズされるネットワークを指定する必要があります。スタティック ルートおよび接続されているネットワークが、自動的にスタブ ルーティング プロセスに再配布されることはありません。

（注） スタブ ルーティング プロセスでは、完全なトポロジ テーブルは維持されません。スタブ ルーティングには、ルーティングの決定を行うために、少なくとも配布ルータへのデフォルト ルートが必要です。

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」（P.23-6）
- 「EIGRP のインターフェイスの設定」（P.23-7）
- 「インターフェイスでのサマリー集約アドレスの設定」（P.23-9）
- 「インターフェイス遅延値の変更」（P.23-10）

- 「インターフェイスでの EIGRP 認証のイネーブル化」（P.23-10）
- 「EIGRP ネイバーの定義」（P.23-12）
- 「EIGRP へのルートの再配布」（P.23-12）
- 「EIGRP でのネットワークのフィルタリング」（P.23-14）
- 「EIGRP Hello 間隔と保持時間のカスタマイズ」（P.23-15）
- 「自動ルート集約のディセーブル化」（P.23-16）
- 「EIGRP でのデフォルト情報の設定」（P.23-16）
- 「EIGRP スプリット ホライズンのディセーブル化」（P.23-17）
- 「EIGRP プロセスの再始動」（P.23-18）

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。

手順の詳細

	コマンド	目的
ステップ 1	**router eigrp** *as-num* **例：** `ciscoasa(config)# router eigrp 2`	EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。 *as-num* 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2	**network** *ip-addr* [*mask*]
	
	例：
	`ciscoasa(config)# router eigrp 2`
	`ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`
		EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。このコマンドで、1 つ以上の **network** 文を設定できます。
		
		直接接続されているネットワークとスタティックなネットワークが定義されたネットワークに含まれていれば、ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。
		
		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、「受動インターフェイスの設定」（P.23-8）を参照してください。

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 **network** コマンドを設定し、**passive-interface** コマンドを使用して、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。

手順の詳細

	コマンド	目的
ステップ 1	**router eigrp** *as-num* **例：** `ciscoasa(config)# router eigrp 2`	EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。 *as-num* 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2	`ciscoasa(config-router)#` **network** *ip-addr* [*mask*]
	
	例：
	`ciscoasa(config)# router eigrp 2`
	`ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`
		EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。このコマンドで、1 つ以上の network 文を設定できます。
		
		直接接続されているネットワークとスタティックなネットワークが定義されたネットワークに含まれていれば、ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。
		
		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、「EIGRP ルーティング プロセスのネットワークの定義」（P.23-6）を参照してください。

ステップ 3	（オプション）EIGRP ルーティングに参加するインターフェイスをカスタマイズするには、次のいずれかの手順を実行します。	

	no default-information {**in** | **out** | **WORD**}
	
	例：
	`ciscoasa(config)# router eigrp 2`
	`ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`
	`ciscoasa(config-router)# no default-information {in | out | WORD}`
		候補となるデフォルト ルート情報の送受信を制御できます。
		
		no default-information in コマンドを入力すると、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。**no default-information out** コマンドを入力すると、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。
		
		このオプションの詳細については、「EIGRP でのデフォルト情報の設定」（P.23-16）を参照してください。

コマンド	目的
authentication mode eigrp *as-num* **md5** **例：** `ciscoasa(config)# authentication mode eigrp 2 md5`	EIGRP パケットの MD5 認証をイネーブルにします。 *as-num* 引数には、ASA に設定されている EIGRP ルーティング プロセスの自律システム番号を指定します。EIGRP がイネーブルになっていないか、誤った番号を入力した場合、ASA は次のエラー メッセージを返します。 `% Asystem(100) specified does not exist` このオプションの詳細については、「インターフェイスでの EIGRP 認証のイネーブル化」（P.23-10）を参照してください。
delay *value* **例：** `ciscoasa(config-if)# delay 200`	*value* 引数は 10 マイクロ秒単位で入力します。2000 マイクロ秒の遅延を設定するには、*value* に 200 を入力します。 インターフェイスに割り当てられている遅延値を表示するには、**show interface** コマンドを使用します。 このオプションの詳細については、「インターフェイス遅延値の変更」（P.23-10）を参照してください。
hello-interval eigrp *as-num seconds* **例：** `ciscoasa(config)# hello-interval eigrp 2 60`	hello 間隔を変更できます。このオプションの詳細については、「EIGRP Hello 間隔と保持時間のカスタマイズ」（P.23-15）を参照してください。
hold-time eigrp *as-num seconds* **例：** `ciscoasa(config)# hold-time eigrp 2 60`	保持時間を変更できます。このオプションの詳細については、「EIGRP Hello 間隔と保持時間のカスタマイズ」（P.23-15）を参照してください。

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。

手順の詳細

	コマンド	目的
ステップ 1	**router eigrp** *as-num* **例：** `ciscoasa(config)# router eigrp 2`	EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。 *as-num* 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

	コマンド	目的
ステップ 2	ciscoasa(config-router)# **network** *ip-addr* [*mask*] **例：** ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0	EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。このコマンドで、1 つ以上の **network** 文を設定できます。 直接接続されているネットワークとスタティックなネットワークが定義されたネットワークに含まれていれば、ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。 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、「EIGRP ルーティング プロセスのネットワークの定義」（P.23-6）を参照してください。
ステップ 3	**passive-interface** {**default** | *if-name*} **例：** ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0 ciscoasa(config-router)# passive-interface {default}	インターフェイスが EIGRP ルーティング メッセージを送受信しなくなります。 **default** キーワードを使用すると、すべてのインターフェイスで EIGRP ルーティング アップデートがディセーブルになります。**nameif** コマンドで定義したインターフェイス名を指定すると、指定したインターフェイスで EIGRP ルーティング アップデートがディセーブルになります。EIGRP ルータ コンフィギュレーション内で、複数の **passive-interface** コマンドを使用できます。

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。

手順の詳細

	コマンド	目的
ステップ 1	**interface** *phy_if* **例：** ciscoasa(config)# interface inside	EIGRP で使用される遅延値を変更するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。
ステップ 2	**summary-address eigrp** *as-num address mask* [*distance*] **例：** ciscoasa(config-if)# summary-address eigrp 2 address mask [20]	サマリー アドレスを作成します。 デフォルトでは、定義する EIGRP サマリー アドレスのアドミニストレーティブ ディスタンスは 5 になります。この値は、**summary-address** コマンドにオプションの引数 *distance* を指定して変更できます。

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。

手順の詳細

	コマンド	目的
ステップ 1	**interface** *phy_if* **例：** `ciscoasa(config)# interface inside`	EIGRP で使用される遅延値を変更するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。
ステップ 2	**delay** *value* **例：** `ciscoasa(config-if)# delay 200`	*value* 引数は 10 マイクロ秒単位で入力します。2000 マイクロ秒の遅延を設定するには、*value* に 200 を入力します。 インターフェイスに割り当てられている遅延値を表示するには、**show interface** コマンドを使用します。

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。

手順の詳細

	コマンド	目的
ステップ 1	**router eigrp** *as-num* **例：** `hostname(config)# router eigrp 2`	EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。 *as-num* 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

	コマンド	目的
ステップ 2	**network** *ip-addr* [*mask*] **例：** hostname(config)# router eigrp 2 hostname(config-router)# network 10.0.0.0 255.0.0.0	EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。このコマンドで、1 つ以上の network 文を設定できます。 直接接続されているネットワークとスタティックなネットワークが定義されたネットワークに含まれていれば、ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。 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、「EIGRP の設定」（P.23-3）を参照してください。
ステップ 3	**interface** *phy_if* **例：** hostname(config)# interface inside	EIGRP メッセージ認証を設定するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。
ステップ 4	**authentication mode eigrp** *as-num* **md5** **例：** hostname(config)# authentication mode eigrp 2 md5	EIGRP パケットの MD5 認証をイネーブルにします。 *as-num* 引数には、ASA に設定されている EIGRP ルーティング プロセスの自律システム番号を指定します。EIGRP がイネーブルになっていないか、誤った番号を入力した場合、ASA は次のエラー メッセージを返します。 `% Asystem(100) specified does not exist`
ステップ 5	**authentication key eigrp** *as-num key* **key-id** *key-id* **例：** hostname(config)# authentication key eigrp 2 cisco key-id 200	MD5 アルゴリズムで使用するキーを設定します。 *as-num* 引数には、ASA に設定されている EIGRP ルーティング プロセスの自律システム番号を指定します。EIGRP がイネーブルになっていないか、誤った番号を入力した場合、ASA は次のエラー メッセージを返します。 `% Asystem(100) specified does not exist%` *key* 引数には、アルファベット、数字、特殊文字を含む最大 16 文字を含めることができます。 **（注）** key 引数には空白は使用できません。 *key-id* 引数には、0 ～ 255 の範囲の数字を指定できます。

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。

手順の詳細

	コマンド	目的
ステップ 1	**router eigrp** *as-num* **例：** `ciscoasa(config)# router eigrp 2`	EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。 *as-num* 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2	**neighbor** *ip-addr* **interface** *if_name*
	
	例：
	`ciscoasa(config)# router eigrp 2`
	`ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1`
		スタティック ネイバーを定義します。
		
		ip-addr 引数には、ネイバーの IP アドレスを指定します。
		
		if-name 引数には、インターフェイスの名前を指定します。ネイバーを使用可能にしている **nameif** コマンドで指定した名前を使用します。1 つの EIGRP ルーティング プロセスに対して複数のネイバーを定義できます。

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 20 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。

手順の詳細

	コマンド	目的
ステップ 1	**router eigrp** *as-num* **例：** `ciscoasa(config)# router eigrp 2`	EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。 *as-num* 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

	コマンド	目的
ステップ 2	**default-metric** *bandwidth delay reliability loading mtu* **例：** ciscoasa(config)# router eigrp **2** ciscoasa(config-router)# default-metric *bandwidth delay reliability loading mtu*	（オプション）EIGRP ルーティング プロセスに再配布するルートに適用するデフォルト メトリックを指定します。 EIGRP ルータ コンフィギュレーション内にデフォルト メトリックを指定しない場合、各 **redistribute** コマンドにメトリック値を指定する必要があります。**redistribute** コマンドで EIGRP メトリックを指定し、EIGRP ルータ コンフィギュレーション内に **default-metric** コマンドが含まれている場合、**redistribute** コマンドのメトリックが使用されます。
ステップ 3	選択したルート タイプを EIGRP ルーティング プロセスに再配布するには、次のいずれかの手順を実行します。	
	redistribute connected [**metric** *bandwidth delay reliability loading mtu*] [**route-map** *map_name*] **例：** ciscoasa(config-router): redistribute connected [metric *bandwidth delay reliability loading mtu*] [route-map *map_name*]	接続済みルートを EIGRP ルーティング プロセスに再配布します。 EIGRP ルータ コンフィギュレーション内に **default-metric** コマンドが含まれていない場合、**redistribute** コマンドに EIGRP メトリック値を指定する必要があります。
	redistribute static [**metric** *bandwidth delay reliability loading mtu*] [**route-map** *map_name*] **例：** ciscoasa(config-router): redistribute static [metric *bandwidth delay reliability loading mtu*] [route-map *map_name*]	スタティック ルートを EIGRP ルーティング プロセスに再配布します。
	redistribute ospf *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**metric** *bandwidth delay reliability loading mtu*] [**route-map** *map_name*] **例：** ciscoasa(config-router): redistribute ospf *pid* [match {internal | external [1 | 2] | nssa-external [1 | 2]}] [metric *bandwidth delay reliability loading mtu*] [route-map *map_name*]	ルートを OSPF ルーティング プロセスから EIGRP ルーティング プロセスに再配布します。
	redistribute rip [**metric** bandwidth delay reliability load mtu] [**route-map map_name**] **例：** (config-router): redistribute rip [metric bandwidth delay reliability load mtu] [route-map map_name]	ルートを RIP ルーティング プロセスから EIGRP ルーティング プロセスに再配布します。

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。

手順の詳細

	コマンド	目的
ステップ 1	**router eigrp** *as-num* **例：** `ciscoasa(config)# router eigrp 2`	EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。 *as-num* 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2	`ciscoasa(config-router)#` **network** *ip-addr* [*mask*]
	
	例：
	`ciscoasa(config)# router eigrp 2`
	`ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`
		EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。このコマンドで、1 つ以上の network 文を設定できます。
		
		直接接続されているネットワークとスタティックなネットワークが定義されたネットワークに含まれていれば、ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。
		
		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、「EIGRP のインターフェイスの設定」（P.23-7）を参照してください。

ステップ 3	EIGRP ルーティング アップデートで送信または受信するネットワークをフィルタリングするには、次のいずれかの手順を実行します。	

	distribute-list *acl* **out** [**connected** | **ospf** | **rip** | **static** | **interface** *if_name*]
	
	例：
	`ciscoasa(config)# router eigrp 2`
	`ciscoasa(config-router)# network 10.0.0.0 255.0.0.0`
	`ciscoasa(config-router): distribute-list acl out [connected]`
		EIGRP ルーティング アップデートで送信するネットワークをフィルタリングします。
		
		インターフェイスを指定して、そのインターフェイスが送信するアップデートだけにフィルタを適用することができます。
		
		EIGRP ルータ コンフィギュレーション内に、複数の **distribute-list** コマンドを入力できます。

コマンド	目的
distribute-list *acl* **in** [**interface** *if_name*] **例：** ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0 ciscoasa(config-router): distribute-list acl in [interface interface1]	EIGRP ルーティング アップデートで受信するネットワークをフィルタリングします。 インターフェイスを指定して、そのインターフェイスが受信するアップデートだけにフィルタを適用することができます。

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。

手順の詳細

	コマンド	目的
ステップ 1	**interface** *phy_if* **例：** ciscoasa(config)# interface inside	hello 間隔またはアドバタイズされる保持時間を設定するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。
ステップ 2	**hello-interval eigrp** *as-num seconds* **例：** ciscoasa(config)# hello-interval eigrp 2 60	hello 間隔を変更します。
ステップ 3	**hold-time eigrp** *as-num seconds* **例：** ciscoasa(config)# hold-time eigrp 2 60	保持時間を変更します。

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。

自動ルート集約をディセーブルにするには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**router eigrp** *as-num*	EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。
	例： `ciscoasa(config)# router eigrp 2`	*as-num* 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。
ステップ 2	**no auto-summary**	この値は設定できません。自動サマリー アドレスのアドミニストレーティブ ディスタンスは 5 です。
	例： `ciscoasa(config-router)# no auto-summary`	

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。

デフォルト ルーティング情報を設定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**router eigrp** *as-num*	EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。
	例： `ciscoasa(config)# router eigrp 2`	*as-num* 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

	コマンド	目的
ステップ 2	ciscoasa(config-router)# **network** *ip-addr* [*mask*] **例：** ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0	EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。このコマンドで、1 つ以上の network 文を設定できます。 直接接続されているネットワークとスタティックなネットワークが定義されたネットワークに含まれていれば、ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。 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、「EIGRP のインターフェイスの設定」（P.23-7）を参照してください。
ステップ 3	**no default-information** {**in** | **out** | **WORD**} **例：** ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0 ciscoasa(config-router)# no default-information {in | out | WORD}	候補となるデフォルト ルート情報の送受信を制御します。 **no default-information in** コマンドを入力すると、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。**no default-information out** コマンドを入力すると、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。

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。

手順の詳細

	コマンド	目的
ステップ 1	**interface** *phy_if* **例：** `ciscoasa(config)# interface phy_if`	EIGRP で使用される遅延値を変更するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。
ステップ 2	**no split-horizon eigrp** *as-number* **例：** `ciscoasa(config-if)# no split-horizon eigrp 2`	スプリット ホライズンをディセーブルにします。

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、次のコマンドを入力します。

コマンド	目的
clear eigrp pid {**1-65535** | **neighbors** | **topology** | **events**)} **例：** `ciscoasa(config)# clear eigrp pid 10 neighbors`	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、次のいずれかのコマンドを入力します。

コマンド	目的
EIGRP ルーティングのモニタリング	
router-id	EIGRP プロセスの router-id を表示します。
show eigrp [*as-number*] **events** [{*start end*} | **type**]	EIGRP イベント ログを表示します。
show eigrp [*as-number*] **interfaces** [*if-name*] [**detail**]	EIGRP ルーティングに参加するインターフェイスを表示します。
show eigrp [*as-number*] **neighbors** [**detail** | **static**] [*if-name*]	EIGRP ネイバー テーブルを表示します。

コマンド （続き）	目的 （続き）
show eigrp [*as-number*] **topology** [*ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]	EIGRP トポロジ テーブルを表示します。
show eigrp [*as-number*] **traffic**	EIGRP トラフィックの統計情報を表示します。
show mfib cluster	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。
show route cluster	クラスタリングに関する追加ルートの同期の詳細を表示します。
EIGRP ロギング メッセージのディセーブル化	
no eigrp log-neighbor-changes	ネイバー変更メッセージのロギングをディセーブルにします。EIGRP 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。
no eigrp log-neighbor-warnings	ネイバー警告メッセージのロギングをディセーブルにします。

（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 EIGRP をイネーブルにし、設定する方法を示します。

ステップ 1　EIGRP をイネーブルにするには、次のコマンドを入力します。

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

ステップ 2　EIGRP ルーティング メッセージの送信または受信からインターフェイスを設定するには、次のコマンドを入力します。

```
ciscoasa(config-router)# passive-interface {default}
```

ステップ 3　EIGRP ネイバーを定義するには、次のコマンドを入力します。

```
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

ステップ 4　EIGRP ルーティングに参加するインターフェイスとネットワークを設定するには、次のコマンドを入力します。

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

ステップ 5　EIGRP ディスタンス計算で使用されるインターフェイス遅延値を変更するには、次のコマンドを入力します。

```
ciscoasa(config-router)# exit
ciscoasa(config)# interface phy_if
ciscoasa(config-if)# delay 200
```

EIGRP 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。

表 23-1　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。 **route eigrp** コマンドが導入されました。
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)	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。
クラスタ	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。 **show route cluster**、**debug route cluster**、**show mfib cluster**、**debug mfib cluster** の各コマンドが導入または変更されました。
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。

CHAPTER 24

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」（P.24-1）
- 「マルチキャスト ルーティングのライセンス要件」（P.24-3）
- 「ガイドラインと制限事項」（P.24-3）
- 「マルチキャスト ルーティングのイネーブル化」（P.24-4）
- 「マルチキャスト ルーティングのカスタマイズ」（P.24-4）
- 「マルチキャスト ルーティングの設定例」（P.24-16）
- 「その他の関連資料」（P.24-16）
- 「マルチキャスト ルーティングの機能履歴」（P.24-17）

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」（P.24-2）
- 「PIM マルチキャスト ルーティング」（P.24-2）
- 「マルチキャスト グループの概念」（P.24-2）
- 「クラスタ」（P.24-3）

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 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

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 8 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

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

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、次のコマンドを入力します。

コマンド	目的

`multicast-routing`
 	
例：
`ciscoasa(config)# multicast-routing`
	マルチキャスト ルーティングをイネーブルにします。
	マルチキャスト ルーティング テーブルのエントリの数は、ASA に搭載されているメモリの量によって制限されます。

表 24-1 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 24-1　マルチキャスト テーブルのエントリ数の上限

テーブル	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.24-5）
- 「スタティック マルチキャスト ルートの設定」（P.24-5）
- 「IGMP 機能の設定」（P.24-6）
- 「PIM 機能の設定」（P.24-11）
- 「双方向ネイバー フィルタの設定」（P.24-14）
- 「マルチキャスト境界の設定」（P.24-15）

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、スタブ エリアに接続されているインターフェイスから次のコマンドを入力します。

コマンド	目的
igmp forward interface *if_name* **例：** ciscoasa(config-if)# igmp forward interface *interface1*	スタブ マルチキャスト ルーティングを設定し、IGMP メッセージを転送します。

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、次のいずれかのコマンドを入力します。

コマンド	目的
mroute *src_ip src_mask* {*input_if_name* | *rpf_neighbor*} [*distance*] **例：** ciscoasa(config)# mroute *src_ip src_mask* {*input_if_name* | *rpf_neighbor*} [*distance*]	スタティック マルチキャスト ルートを設定します。

コマンド	目的
mroute *src_ip src_mask input_if_name* [**dense** *output_if_name*] [*distance*] **例：** ciscoasa(config)# mroute *src_ip src_mask input_if_name* [dense *output_if_name*] [*distance*]	スタブ エリアのスタティック マルチキャスト ルートを設定します。 **dense** *output_if_name* キーワードと引数のペアは、スタブ マルチキャスト ルーティングだけでサポートされます。

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.24-7）
- 「IGMP グループ メンバーシップの設定」（P.24-7）
- 「スタティック加入した IGMP グループの設定」（P.24-7）
- 「マルチキャスト グループへのアクセスの制御」（P.24-8）
- 「インターフェイスにおける IGMP 状態の数の制限」（P.24-9）
- 「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」（P.24-9）
- 「IGMP バージョンの変更」（P.24-10）

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、次のコマンドを入力します。

コマンド	目的
no igmp **例：** `ciscoasa(config-if)# no igmp`	インターフェイスの IGMP をディセーブルにします。 インターフェイスで IGMP を再度イネーブルにするには、**igmp** コマンドを使用します。

（注） 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。

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.24-7）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、次のコマンドを入力します。

コマンド	目的
igmp join-group *group-address* **例：** `ciscoasa(config-if)# igmp join-group mcast-group`	ASA をマルチキャスト グループのメンバとして設定します。 *group-address* 引数はグループの IP アドレスです。

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。

igmp static-group コマンドを入力します。ASA は、マルチキャスト パケットを受け入れずに、指定したインターフェイスに転送します。

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、次のコマンドを入力します。

コマンド	目的
igmp static-group **例：** ciscoasa(config-if)# **igmp static-group** *group-address*	インターフェイスのマルチキャスト グループにスタティック加入するように、ASA を設定します。 *group-address* 引数はグループの IP アドレスです。

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。

手順の詳細

	コマンド	目的
ステップ 1	標準 ACL または拡張 ACL を作成するには、次のいずれかを実行します。	
	access-list *name* **standard** [**permit** | **deny**] *ip_addr mask* **例：** ciscoasa(config)# access-list *acl1* standard permit *192.52.662.25*	マルチキャスト トラフィックの標準 ACL を作成します。 1 つの ACL に複数のエントリを作成することができます。標準 ACL または拡張 ACL を使用できます。 *ip_addr mask* 引数は、許可または拒否されるマルチキャスト グループの IP アドレスです。
	access-list *name* **extended** [**permit** | **deny**] *protocol src_ip_addr src_mask dst_ip_addr dst_mask* **例：** ciscoasa(config)# access-list *acl2* extended permit *protocol src_ip_addr src_mask dst_ip_addr dst_mask*	拡張 ACL を作成します。 *dst_ip_addr* 引数は、許可または拒否されるマルチキャスト グループの IP アドレスです。
ステップ 2	**igmp access-group** *acl* **例：** ciscoasa(config-if)# igmp access-group *acl*	ACL をインターフェイスに適用します。 *acl* 引数は、標準 IP ACL または拡張 IP ACL の名前です。

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、次のコマンドを入力します。

コマンド	目的
igmp limit *number* **例：** `ciscoasa(config-if)# igmp limit 50`	インターフェイスにおける IGMP 状態の数を制限します。 有効値の範囲は 0 ～ 500 で、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、（**igmp join-group** コマンドおよび **igmp static-group** コマンドを使用して）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。このコマンドの **no** 形式を使用すると、デフォルト値に戻ります。

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

（注） **igmp query-timeout** コマンドおよび **igmp query-interval** コマンドを実行するには、IGMP バージョン 2 が必要です。

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。

手順の詳細

	コマンド	目的
ステップ 1	**igmp query-interval** *seconds* **例：** ciscoasa(config-if)# igmp query-interval *30*	クエリー間隔を秒単位で設定します。 有効値の範囲は 0 ～ 500 で、デフォルト値は 125 です。 指定されたタイムアウト値（デフォルトは 255 秒）の間にインターフェイス上でクエリー メッセージが ASA によって検出されないと、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 2	**igmp query-timeout** *seconds* **例：** ciscoasa(config-if)# igmp query-timeout *30*	クエリーのタイムアウト値を変更します。 有効値の範囲は 0 ～ 500 で、デフォルト値は 225 です。
ステップ 3	**igmp query-max-response-time** *seconds* **例：** ciscoasa(config-if)# igmp query-max-response-time *30*	最大クエリー応答時間を変更します。

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、**igmp query-timeout** コマンドや **igmp query-interval** コマンドなどの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、次のコマンドを入力します。

コマンド	目的
igmp version {**1** | **2**} **例：** ciscoasa(config-if)# igmp version 2	インターフェイスで実行する IGMP のバージョンを制御します。

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.24-11）
- 「スタティック ランデブー ポイント アドレスの設定」（P.24-12）
- 「指定ルータのプライオリティの設定」（P.24-12）
- 「PIM 登録メッセージの設定とフィルタリング」（P.24-13）
- 「PIM メッセージ間隔の設定」（P.24-13）
- 「PIM ネイバーのフィルタリング」（P.24-13）

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。

手順の詳細

	コマンド	目的

ステップ 1	`pim`
	
	例：
	`ciscoasa(config-if)# pim`
		特定のインターフェイスで PIM をイネーブルにする、または再度イネーブルにします。

ステップ 2	`no pim`
	
	例：
	`ciscoasa(config-if)# no pim`
		特定のインターフェイス上の PIM をディセーブルにします。

（注）　インターフェイス コンフィギュレーションには、**no pim** コマンドだけが表示されます。

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。RP アドレスを指定するには、**pim rp-address** コマンドを使用する必要があります。

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、次のコマンドを入力します。

コマンド	目的
pim rp-address *ip_address* [*acl*] [**bidir**] **例：** `ciscoasa(config)# pim rp-address 10.86.75.23 [acl1] [bidir]`	特定のインターフェイスで PIM をイネーブルにする、または再度イネーブルにします。 *ip_address* 引数は、PIM RP となるように割り当てられたルータのユニキャスト IP アドレスです。 *acl* 引数は、RP とともに使用する必要があるマルチキャスト グループを定義している標準 ACL の名前または番号です。このコマンドではホスト ACL を使用しないでください。 **bidir** キーワードを除外すると、グループは PIM スパース モードで動作するようになります。

（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。

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、次のコマンドを入力します。

コマンド	目的
pim dr-priority *num* **例：** `ciscoasa(config-if)# pim dr-priority 500`	指定ルータのプライオリティを変更します。 *num* 引数は、1 ～ 4294967294 の任意の数字にできます。

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、未許可の送信元が 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、次のコマンドを入力します。

コマンド	目的
pim accept-register {**list** *acl* | **route-map** *map-name*} **例：** `ciscoasa(config)# pim accept-register {list acl1 | route-map map2}`	PIM 登録メッセージをフィルタリングするように ASA を設定します。 この例では、ASA によって PIM 登録メッセージ *acl1* とルート マップ *map2* がフィルタリングされます。

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。

手順の詳細

	コマンド	目的
ステップ 1	**pim hello-interval** *seconds* **例：** `ciscoasa(config-if)# pim hello-interval 60`	ルータ クエリー メッセージを送信します。 *seconds* 引数の有効な値は 1 ～ 3600 秒です。
ステップ 2	**pim join-prune-interval** *seconds* **例：** `ciscoasa(config-if)# pim join-prune-interval 60`	ASA が PIM 加入メッセージまたはプルーニング メッセージを送信する時間（秒）を変更します。 *seconds* 引数の有効な値は 10 ～ 600 秒です。

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。
- 接続されたスタブ 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。

手順の詳細

	コマンド	目的
ステップ 1	**access-list pim_nbr deny** *router-IP_addr PIM neighbor* **例：** `ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255`	標準 ACL を使用して、PIM に参加させるルータを定義します。 この例では、次の ACL を **pim neighbor-filter** コマンドと使用すると、10.1.1.1 ルータを PIM ネイバーとして設定できなくなります。

ステップ 2	**pim neighbor-filter pim_nbr**
	
	例：
	`ciscoasa(config)# interface GigabitEthernet0/3`
	`ciscoasa(config-if)# pim neighbor-filter pim_nbr`
		隣接ルータをフィルタします。
		
		この例では、インターフェイス GigabitEthernet0/3 で 10.1.1.1 ルータを PIM ネイバーとして設定できなくなります。

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。

手順の詳細

	コマンド	目的
ステップ 1	**access-list pim_nbr deny** *router-IP_addr PIM neighbor* **例：** `ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255`	標準 ACL を使用して、PIM に参加させるルータを定義します。 この例では、次の ACL を **pim neighbor-filter** コマンドと使用すると、10.1.1.1 ルータを PIM ネイバーとして設定できなくなります。

ステップ 2	**pim bidirectional-neighbor-filter pim_nbr**
	
	例：
	`ciscoasa(config)# interface GigabitEthernet0/3`
	`ciscoasa(config-if)# pim bidirectional neighbor-filter pim_nbr`
		隣接ルータをフィルタします。
		この例では、10.1.1.1 ルータが、インターフェイス GigabitEthernet0/3 上で PIM 双方向ネイバーとして設定できなくなります。

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、**multicast boundary** コマンドを入力します。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。

filter-autorp キーワードを入力することにより、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、次のコマンドを入力します。

コマンド	目的
multicast boundary *acl* [**filter-autorp**] **例：** `ciscoasa(config-if)# multicast boundary acl1 [filter-autorp]`	マルチキャスト境界を設定します。

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　マルチキャスト ルーティングをイネーブルにします。

```
ciscoasa(config)# multicast-routing
```

ステップ 2　スタティック マルチキャスト ルートを設定します。

```
ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
ciscoasa(config)# exit
```

ステップ 3　ASA をマルチキャスト グループのメンバとして設定します。

```
ciscoasa(config)# interface
ciscoasa(config-if)# igmp join-group group-address
```

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.24-16）
- 「RFC」（P.24-16）

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	IGMPv2
RFC 2362	PIM-SM
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 24-2 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。

表 24-2　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、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。 **multicast-routing** コマンドが導入されました。
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。 **debug mfib cluster**、**show mfib cluster** の各コマンドが導入されました。

IPv6 ネイバー探索

- 「IPv6 ネイバー ディスカバリについて」（P.25-1）
- 「IPv6 ネイバー探索のライセンス要件」（P.25-4）
- 「IPv6 ネイバー探索の前提条件」（P.25-4）
- 「ガイドラインと制限事項」（P.25-4）
- 「IPv6 ネイバー探索のデフォルト設定」（P.25-6）
- 「IPv6 ネイバー探索の設定」（P.25-7）
- 「IPv6 ネイバー探索のモニタリング」（P.25-14）
- 「その他の関連資料」（P.25-14）
- 「IPv6 ネイバー探索の機能履歴」（P.25-15）

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、接続リンク上に存在することがわかっているネイバーのリンク層アドレスの特定や、無効になったキャッシュ値の迅速なパージを行います。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われると、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」（P.25-2）
- 「ネイバー到達可能時間」（P.25-2）
- 「重複アドレス検出」（P.25-2）
- 「ルータ アドバタイズメント メッセージ」（P.25-3）
- 「スタティック IPv6 ネイバー」（P.25-4）

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。

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。

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は、ルータ送信要求メッセージへの応答でも送信されます（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.11-12）に従って、IPv6 アドレッシングを設定します。

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

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 25-1 に、IPv6 ネイバー探索のデフォルト設定を示します。

表 25-1　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。

表 25-1　IPv6 ネイバー探索のデフォルト パラメータ （続き）

パラメータ	デフォルト
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

- 「インターフェイス コンフィギュレーション モードの開始」（P.25-7）
- 「ネイバー送信要求メッセージの送信間隔の設定」（P.25-8）
- 「ネイバー到達可能時間の設定」（P.25-8）
- 「ルータ アドバタイズメントの送信間隔の設定」（P.25-9）
- 「ルータ ライフタイム値の設定」（P.25-9）
- 「DAD 設定の指定」（P.25-10）
- 「ルータ アドバタイズメント メッセージの抑止」（P.25-10）
- 「IPv6 DHCP リレーのアドレス設定フラグの設定」（P.25-11）
- 「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.25-12）
- 「スタティック IPv6 ネイバーの設定」（P.25-13）

インターフェイス コンフィギュレーション モードの開始

インターフェイスごとのネイバー探索設定を行います。インターフェイス コンフィギュレーション モードを開始するには、次の手順を実行します。

手順の詳細

コマンド	目的

interface *name*
 	
例：
`hostname(config)# interface gigabitethernet 0/0`
`hostname(config-if)#`
	インターフェイス コンフィギュレーション モードを開始します。

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、次のコマンドを入力します。

手順の詳細

コマンド	目的
ipv6 nd ns-interval *value* **例：** `hostname (config-if)# ipv6 nd ns-interval 9000`	インターフェイスに IPv6 ネイバー送信要求の再送信する間隔を設定します。 value 引数の有効な値は、1000 ～ 3600000 ミリ秒です。 この情報は、ルータ アドバタイズメント メッセージでも送信されます。

例

次の例では、GigabitEthernet 0/0 での IPv6 ネイバー送信要求の送信間隔を 9000 ミリ秒に設定します。

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ns-interval 9000
```

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、次のコマンドを入力します。

手順の詳細

コマンド	目的
ipv6 nd reachable-time *value* **例：** `hostname (config-if)# ipv6 nd reachable-time 1700000`	リモートの IPv6 ノードに到達可能な時間を設定します。 *value* 引数の有効な値は、0 ～ 3600000 ミリ秒です。 value に 0 を使用すると、到達可能時間が未定のまま送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。

例

次の例では、選択したインターフェイス、GigabitEthernet 0/0 で 1700000 ミリ秒の IPv6 到達可能時間を設定します。

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd reachable-time 1700000
```

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、次のコマンドを入力します。

手順の詳細

コマンド	目的
ipv6 nd ra-interval [**msec**] *value* **例：** hostname (config-if)# ipv6 nd ra-interval 201	IPv6 ルータ アドバタイズメントの送信間隔を設定します。 オプションの **msec** キーワードは、この値がミリ秒単位で指定されることを示します。このキーワードが存在しない場合、値は秒単位で指定されます。 *value* 引数の有効な値の範囲は 3 ～ 1800 秒、**msec** キーワードが指定されている場合は 500 ～ 1800000 ミリ秒です。 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 ライフタイム以下にする必要があります。詳細については、「ルータ ライフタイム値の設定」（P.25-9）を参照してください。他の IPv6 ノードと同期しないようにするには、使用する実際値を必要値の 20 % 以内にランダムに調整します。

例

次の例では、選択したインターフェイス、GigabitEthernet 0/0 で 201 秒の IPv6 ルータ アドバタイズメント間隔を設定します。

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ra-interval 201
```

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、次のコマンドを入力します。

手順の詳細

コマンド	目的
ipv6 nd ra-lifetime [**msec**] *value* **例：** hostname (config-if)# ipv6 nd ra-lifetime 2000	ローカル リンク上のノードが、ASA をリンク上のデフォルト ルータと見なす時間の長さを指定します。 オプションの **msec** キーワードは、この値がミリ秒単位で指定されることを示します。このキーワードが存在しない場合、値は秒単位で指定されます。 *value* 引数の有効な値は 0 ～ 9000 秒です。 0 を入力すると、ASA は選択したインターフェイスのデフォルト ルータと見なされません。

例

次の例では、選択したインターフェイス GigabitEthernet 0/0 で 2000 秒の IPv6 ルータ ライフタイム値を設定します。

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ra-lifetime 2000
```

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、次のコマンドを入力します。

手順の詳細

コマンド	目的
ipv6 nd dad attempts *value* **例：** `hostname (config-if)# ipv6 nd dad attempts 20`	割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を指定し、ネットワークに重複する IPv6 アドレスが検出されていないかをリンクベースで確認します。 *value* 引数の有効な値の範囲は 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。

例

次の例では、選択したインターフェイス GigabitEthernet 0/0 で DAD の試行の値を 20 に設定します。

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd dad attempts 20
```

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、次のコマンドを入力します。

手順の詳細

コマンド	目的
ipv6 nd suppress-ra *seconds* **例：** `hostname (config-if)# ipv6 nd suppress-ra 900`	ルータ ライフタイム値を抑制します。 *seconds* 引数は、ASA の有効性をこのインターフェイスのデフォルトのルータとして指定します。有効な値の範囲は、0 ～ 9000 秒です。0 を入力すると、ASA は指定したインターフェイス上のデフォルト ルータと見なされません。 このコマンドを入力すると、ASA がリンク上では IPv6 ルータではなく、通常の IPv6 ネイバーのように見えるようになります。

例

次の例では、指定したインターフェイス GigabitEthernet 0/0 で、IPv6 ルータ アドバタイズメントの送信を抑制します。

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd suppress-ra 900
```

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

コマンド	目的
ipv6 nd managed-config-flag **例：** `hostname (config-if)# ipv6 nd managed-config-flag`	IPv6 ルータ アドバタイズメント パケットの管理対象アドレス設定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。
ipv6 nd other-config-flag **例：** `hostname (config-if)# ipv6 nd other-config-flag`	IPv6 ルータ アドバタイズメント パケットのその他のアドレス設定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、次のコマンドを入力します。

手順の詳細

コマンド	目的
ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**] **例：** `hostname (config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900`	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します。ネイバー デバイスは、プレフィックス アドバタイズメントを使用して、そのインターフェイス アドレスを自動設定できます。ステートレス自動設定では、ルータ アドバタイズメント メッセージで提供される IPv6 プレフィックスを使用して、リンクローカル アドレスからグローバル ユニキャスト アドレスを作成します。 **at** *valid-date preferred-date* 構文は、ライフタイムとプリファレンスが期限切れになる日付と時刻を示します。プレフィックスは、この指定された日付と時刻に達するまで有効です。日付は *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* の形式で表されます。 **default** キーワードは、デフォルト値が使用されることを示します。 オプションの **infinite** キーワードは、有効なライフタイムが期限切れにならないように指定します。 *ipv6-prefix* 引数には、IPv6 ネットワーク番号にルータ アドバタイズメントが含まれることを指定します。この引数は、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。 オプションの **no-advertise** キーワードは、指定したプレフィックスを IPv6 の自動設定に使用しないことをローカル リンク上のホストに示します。 オプションの **no-autoconfig** キーワードは、指定したプレフィックスを IPv6 の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示します。 オプションの **off-link** キーワードは、指定したプレフィックスをオンリンクの指定に使用しないことを示します。 *preferred-lifetime* 引数には、指定した IPv6 プレフィックスを推奨するものとしてアドバタイズする時間を（秒単位で）指定します。有効値の範囲は 0 ～ 4294967295 秒です。最大値は無限ですが、これは infinite を使用して指定もできます。デフォルトは 604800（7 日間）です。 *prefix-length* 引数には IPv6 プレフィックスの長さを指定します。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ（/）を使用する必要があります。 *valid-lifetime* 引数には、指定した IPv6 プレフィックスを有効なものとしてアドバタイズする時間を指定します。有効値の範囲は 0 ～ 4294967295 秒です。最大値は無限ですが、これは infinite を使用して指定もできます。デフォルトは、2592000（30 日）です。

例

次の例では、指定したインターフェイス GigabitEthernet 0/0 で送信されるルータ アドバタイズメントの、有効ライフタイムが 1000 秒、推奨ライフタイムが 900 秒の IPv6 プレフィックス 2001:DB8::/32 を示します。

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900
```

スタティック IPv6 ネイバーの設定

IPv6 ネイバー探索キャッシュにスタティック エントリを設定するには、次のコマンドを入力します。

手順の詳細

コマンド	目的
ipv6 neighbor *ipv6_address if_name mac_address* **例：** `hostname(config-if)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472`	IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。 *ipv6_address* 引数にはネイバーのリンクローカル IPv6 アドレス、*if_name* 引数にはネイバーを使用可能にするためのインターフェイス、*mac_address* 引数にはネイバー インターフェイスの MAC アドレスを指定します。

例

次の例では、IPv6 アドレスが 3001:1::45A、MAC アドレスが 002.7D1a.9472 の内部ホストのスタティック エントリをネイバー探索キャッシュに追加します。

```
hostname(config-if)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472
```

IPv6 ネイバー探索のモニタリング

IPv6 ネイバー探索パラメータをモニタするには、次のコマンドを入力します。

コマンド	目的
`show ipv6 interface`	IPv6 向けに設定されたインターフェイスの使用状況を表示します。「outside」などのインターフェイス名を含めると、指定したインターフェイスの設定が表示されます。コマンドに名前を含めないと、IPv6 がイネーブルになっているすべてのインターフェイスの設定が表示されます。コマンドの出力では、次の項目が表示されます。 • インターフェイスの名前とステータス • リンクローカルおよびグローバルなユニキャスト アドレス • インターフェイスが属するマルチキャスト グループ • ICMP リダイレクトおよびエラー メッセージの設定 • ネイバー探索の設定 • コマンドが 0 に設定されているときの実際の時間 • 使用されているネイバー探索の到達可能時間

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.25-14）
- 「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.25-15）

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 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。

表 25-2　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。 **ipv6 nd ns-interval**、**ipv6 nd ra-lifetime**、**ipv6 nd suppress-ra**、**ipv6 neighbor**、**ipv6 nd prefix**、**ipv6 nd dad-attempts**、**ipv6 nd reachable-time**、**ipv6 address**、および **ipv6 enforce-eui64** コマンドが導入されました。
IPv6 DHCP リレーのアドレス設定フラグ	9.0(1)	コマンド **ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag** が導入されました。

PART 7

AAA サーバおよびローカル データベース

CHAPTER 26

AAA について

この章では、認証、許可、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」（P.26-1）
- 「許可」（P.26-2）
- 「アカウンティング」（P.26-2）
- 「認証、許可、アカウンティング間の相互作用」（P.26-2）
- 「AAA サーバ」（P.26-2）
- 「AAA サーバ グループ」（P.26-2）
- 「ローカル データベースのサポート」（P.26-2）

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
- VPN アクセス

許可

許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許可される可能性があります。

次の項目を許可するように、ASA を設定できます。

- 管理コマンド
- ネットワーク アクセス
- 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、許可、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、許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。許可では必ず、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、認証および許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。許可は、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、許可、アカウンティングを提供することもできます。

CHAPTER 27

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」（P.27-1）
- 「ローカル データベースのガイドライン」（P.27-3）
- 「ユーザ アカウントのローカル データベースへの追加」（P.27-3）
- 「ローカル データベースのモニタリング」（P.27-7）
- 「ローカル データベースの履歴」（P.27-8）

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。

- ユーザごとの ASDM 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。
- 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 アクセス許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許可するためにローカル データベースが使用されます。
- VPN 認証および許可：VPN 認証および許可は、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許可に使用する場合、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.35-34）

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　ユーザ アカウントを作成します。

username *username* {**nopassword** | **password** *password*} [**privilege** *priv_level*]

例：

```
ciscoasa(config)# username exampleuser1 privilege 1
```

username *user*name キーワードは、4 ～ 64 文字の文字列です。**password** *password* キーワードは、3 ～ 32 文字の文字列です。**privilege** *priv_level* キーワードでは、0 ～ 15 の特権レベルを設定します。デフォルト値は 2 です。この特権レベルは、コマンド許可で使用されます。

注意　コマンド許可（**aaa authorization console LOCAL** コマンド）を使用していない場合、デフォルトのレベル 2 を使用して特権 EXEC モードにアクセスできます。特権 EXEC モードへのアクセスを制限する場合、特権レベルを 0 または 1 に設定するか、**service-type** コマンドを使用します。

nopassword キーワードは、パスワードを指定しないユーザ アカウントを作成します。**encrypted** キーワードは、パスワードが暗号化されていることを示します。**username** コマンド内のパスワードを定義すると、ASA はセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するときに暗号化します。**show running-config** コマンドを入力すると、**username** コマンドでは実際のパスワードは示されません。暗号化されたパスワードとそれに続けて **encrypted** キーワードが示されます。たとえば、パスワードに「test」と入力すると、**show running-config** の出力には次のように表示されます。

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

実際に CLI で **encrypted** キーワードを入力するのは、同じパスワードを使用していて、あるコンフィギュレーション ファイルを他の ASA にカット アンド ペーストする場合だけです。

ステップ 2　（オプション）ユーザ名属性を設定します。

username *username* **attributes**

例：

```
ciscoasa(config)# username exampleuser1 attributes
```

username 引数は、最初の手順で作成したユーザ名です。

デフォルトでは、このコマンドで追加した VPN ユーザには属性またはグループ ポリシーが関連付けられません。**username attributes** コマンドを使用して、明示的にすべての値を設定する必要があります。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。

ステップ 3　（オプション）管理許可を設定している場合は、**aaa authorization exec** コマンドを使用して、ユーザ レベルを設定します。

service-type {**admin** | **nas-prompt** | **remote-access**}

例：

```
ciscoasa(config-username)# service-type admin
```

admin キーワードは、**aaa authentication console LOCAL** コマンドによって指定されたサービスへのフル アクセスを許可します。デフォルトは **admin** キーワードです。

nas-prompt キーワードは、**aaa authentication {telnet | ssh | serial} console** コマンドを設定しているときに CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定しているときは ASDM への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。**aaa authentication enable console** コマンドを使用して認証をイネーブルにしている場合、ユーザは、**enable** コマンド（または **login** 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。

remote-access キーワードは管理アクセスを拒否します。**aaa authentication console** コマンドで指定されたサービスは使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。

ステップ 4　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します。

ssh authentication {**pkf** | **publickey** *key* [**hashed**]}

例：

```
ciscoasa(config-username)# ssh authentication pkf

Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+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/7K77II==
---- END SSH2 PUBLIC KEY ----quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config-username)#
```

公開キー ファイル (PKF) でフォーマットされたキー（**pkf** キーワード）、または Base64 キー（**publickey** キーワード）を指定できます。**publickey** の場合、キーは Base64 でエンコードされた公開キーです。SSH-RSA raw キーを生成（証明書なし）する任意の 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。

pkf キーの場合、PKF でフォーマットされたキーを最大 4096 ビット貼り付けるよう求められます。Base64 形式でインライン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 keygen を使って4096 ビットのキーを生成してから PKF に変換し、そのキーに対して **pkf** キーワードが求められるようにすることができます。

（注）　フェールオーバーで **pkf** オプションを使用できますが、PKF キーは、スタンバイ システムに自動的に複製されません。PKF キーを同期するには、**write standby** コマンドを入力する必要があります。

show running-config username コマンドを使用して ASA 上でキーを表示した場合、キーは、SHA-256 ハッシュを使用して暗号化されます。キーを **pkf** として入力した場合でも、ASA はキーをハッシュし、ハッシュ化された **publickey** として表示します。**show** の出力からキーをコピーする必要がある場合、**hashed** キーワードを使って、**publickey** タイプを指定します。

ステップ 5　（オプション）VPN 認証にこのユーザ名を使用している場合、そのユーザに多くの VPN 属性を設定できます。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。

例

次の例では、admin ユーザ アカウントに対して特権レベル 15 を割り当てます。

```
ciscoasa(config)# username admin password password privilege 15
```

次の例では、パスワードを指定しないユーザ アカウントを作成します。

```
ciscoasa(config)# username user34 nopassword
```

次の例では、管理許可をイネーブルにし、パスワードを指定するユーザ アカウントを作成し、ユーザ名コンフィギュレーション モードを開始して、**nas-prompt** の **service-type** を指定します：

```
ciscoasa(config)# aaa authorization exec authentication-server
ciscoasa(config)# username user1 password gOgeOus
ciscoasa(config)# username user1 attributes
ciscoasa(config-username)# service-type nas-prompt
```

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　ASA CLI に接続し、ユーザ名に公開キーを追加します。

```
ciscoasa(config)# username test attributes
ciscoasa(config-username)# ssh authentication pkf
Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- 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 ----
quit
INFO: Import of an SSH public key formatted file completed successfully.
```

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、次のコマンドを参照してください。

- **show aaa-server**

  このコマンドは、設定されたデータベースの統計情報を表示します。AAA サーバ コンフィギュレーションをクリアするには、**clear aaa-server statistics** コマンドを入力します。

- **show running-config aaa-server**

  このコマンドは、AAA サーバの実行コンフィギュレーションを表示します。AAA サーバの統計情報をクリアするには、**clear configure aaa-server** コマンドを入力します。

ローカル データベースの履歴

表 27-1　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。 次のコマンドを導入しました。 **username**、**aaa authorization exec authentication-server**、**aaa authentication console LOCAL**、**aaa authorization exec LOCAL**、**service-type, aaa authentication {telnet | ssh | serial} console LOCAL**、**aaa authentication http console LOCAL**、**aaa authentication enable console LOCAL**、**show running-config aaa-server**、**show aaa-server**、**clear configure aaa-server**、**clear aaa-server statistics**。
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。 次のコマンドを導入しました。**ssh authentication** *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」（P.28-1）
- 「RADIUS サーバのライセンス要件」（P.28-14）
- 「ガイドラインと制限事項」（P.28-14）
- 「RADIUS サーバの設定」（P.28-15）
- 「RADIUS サーバのモニタリング」（P.28-22）
- 「その他の関連資料」（P.28-22）
- 「RADIUS サーバの機能履歴」（P.28-23）

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」（P.28-2）
- 「VPN 接続のユーザ許可」（P.28-2）
- 「RADIUS 属性のサポートされるセット」（P.28-2）
- 「サポートされる RADIUS 許可属性」（P.28-3）
- 「サポートされる IETF RADIUS 許可属性」（P.28-13）
- 「RADIUS アカウンティング切断の理由コード」（P.28-13）

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。
- CHAP および MS-CHAPv1：L2TP-over-IPsec 接続。
- MS-CHAPv2：L2TP-over-IPsec 接続、およびパスワード管理機能がイネーブルの場合の通常の IPsec リモート アクセス接続。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な 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
- RADIUS ベンダー ID 9 によって識別される Cisco IOS ベンダー固有属性（VSA）
- 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 許可属性

許可では、権限または属性を使用するプロセスを参照します。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 28-1 に、ユーザ許可に使用可能な、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 28-1 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 28-1　サポートされる RADIUS 許可属性

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 28-1　サポートされる RADIUS 許可属性 （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 28-1　サポートされる RADIUS 許可属性 （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（許可のみ） 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 28-1　サポートされる RADIUS 許可属性 （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 28-1　サポートされる RADIUS 許可属性 （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： `Engineering, Sales` 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 28-1　サポートされる RADIUS 許可属性 （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 28-1　サポートされる RADIUS 許可属性 （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 は相互排他値。 0 ～ 11、16 ～ 27、32 ～ 43、48 ～ 59 は有効値。

表 28-1　サポートされる RADIUS 許可属性 （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 その他の値 = 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 = JavaScript 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 28-1　サポートされる RADIUS 許可属性 （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（「Corporate-Apps」など）。 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 28-1　サポートされる RADIUS 許可属性 （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 許可属性

表 28-2 に、サポートされている IETF RADIUS 属性を示します。

表 28-2　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 28-1 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

切断の理由コード （続き）
ACCT_DISC_ADMIN_REBOOT = 7
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

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

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場合は、「フォールバック サポート」（P.27-2）および「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.27-2）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.35-34）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」（P.28-15）
- 「RADIUS サーバ グループの設定」（P.28-16）
- 「グループへの RADIUS サーバの追加」（P.28-20）

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.28-16）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.28-20）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

	コマンド	目的

ステップ 1	**aaa-server** *server_tag* **protocol radius**
	
	例：
	`ciscoasa(config)# aaa-server servergroup1 protocol radius`
	`ciscoasa(config-aaa-server-group)#`
		サーバ グループ名とプロトコルを識別します。
		
		aaa-server protocol コマンドを入力すると、コンフィギュレーション モードに入ります。

ステップ 2	**merge-dacl** {**before-avpair** | **after-avpair**}
	
	例：
	`ciscoasa(config)# aaa-server servergroup1 protocol radius`
	`ciscoasa(config-aaa-server-group)# merge-dacl before-avpair`
		ダウンロード可能 ACL と、RADIUS パケットから Cisco AV ペアで受信した ACL を結合します。デフォルト設定は **no merge dacl** で、ダウンロード可能な ACL は Cisco AV ペア ACL と結合されません。AV ペアおよびダウンロード可能な ACL の両方を受信した場合は、AV ペアが優先し、使用されます。
		
		before-avpair オプションは、ダウンロード可能な ACL エントリが Cisco AV ペアエントリの前に配置されるように指定します。
		
		after-avpair オプションは、ダウンロード可能な ACL エントリが Cisco AV ペアエントリの後に配置されるように指定します。このオプションは、VPN 接続にのみ適用されます。VPN ユーザの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および ASA で設定される ACL の形式になります。このオプションでは、ダウンロード可能 ACL と AV ペア ACL を結合するかどうかを決定します。ASA で設定されている ACL には適用されません。

	コマンド	目的
ステップ 3	**max-failed-attempts** *number* **例：** ciscoasa(config-aaa-server-group)# max-failed-attempts 2	次のサーバを試す前にグループ内の RADIUS サーバに送信する要求の最大数を指定します。*number* 引数の範囲は 1 ～ 5 です。デフォルト値は 3 です。 ローカル データベースを使用してフォールバック方式（管理アクセス専用）を設定している場合で、グループ内のすべてのサーバが応答しないとき、グループは応答なしと見なされ、フォールバック方式が試行されます。このサーバ グループは 10 分間（デフォルト）非応答としてマークされるため、その期間内の追加の AAA 要求については、サーバ グループへのアクセスを試みることなく、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。 フォールバック方式が設定されていない場合、ASA は引き続きグループ内のサーバへのアクセスを試みます。
ステップ 4	**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**} **例：** ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20	グループ内で障害の発生したサーバを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。 **depletion** キーワードを指定すると、グループ内のすべてのサーバが非アクティブになった後に、障害の発生したサーバが再度アクティブ化されます。 **deadtime** *minutes* キーワード引数のペアには、グループ内の最後のサーバをディセーブルにしてから、次にすべてのサーバを再度イネーブルにするまでの経過時間を分単位で 0 ～ 1440 から指定します。デフォルトは 10 分です。 **timed** キーワードは、30 秒間のダウンタイムの後に障害が発生したサーバを再度アクティブ化します。
ステップ 5	**accounting-mode simultaneous** **例：** ciscoasa(config-aaa-server-group)# accounting-mode simultaneous	グループ内のすべてのサーバにアカウンティング メッセージを送信します。 アクティブ サーバにのみメッセージを送信するデフォルトに戻すには、**accounting-mode single** コマンドを入力します。
ステップ 6	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **例：** ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1	サーバと、そのサーバが属する AAA サーバ グループを識別します。 **aaa-server host** コマンドを入力すると、AAA サーバのホスト コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 7	**dynamic-authorization** {port *port-number*} **例：** (config-aaa-server-group)# dynamic-authorization port 1700	AAA サーバ グループの RADIUS の動的許可（CoA）サービスをイネーブルにします。 定義されると、対応する RADIUS サーバ グループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー更新用ポートをリッスンします。 CoA のリスニング *ポート番号*の有効な範囲は、1 ～ 65535 です。 このコマンドの「no」形式で指定されたポート番号またはインターフェイスが現在のコンフィギュレーションの行に一致しない場合は、エラー メッセージが表示されます。
ステップ 8	**authorize-only** **例：** (config-aaa-server-group)# authorize-only	RADIUS サーバ グループ用の許可専用モードをイネーブルにします。これで、このサーバ グループが許可に使用されている場合に RADIUS アクセス要求メッセージが現在利用可能になっている設定済みのパスワード方式ではなく、「許可専用」要求として構築されることが示されます。許可専用要求には値 Authorize-Only（17）を持つサービス タイプ属性と、アクセス要求内のメッセージ認証子が含まれます。 許可専用モードのサポートにより、アクセス要求に RADIUS 共通パスワードを含める必要がなくなります。したがって、AAA サーバ ホスト モードで radius Common pw CLI を使用して共通パスワードを設定する必要はありません。 **（注）** 許可専用モードはサーバ グループに対して設定されますが、共通パスワードはホストに固有です。したがって、許可専用モードを設定すると、個々の AAA サーバに設定された共通パスワードは無視されるようになります。
ステップ 9	**without-csd** {**anyconnect**} **例：** (config-tunnel-webvpn)# without-csd anyconnect	特定のトンネル グループに行われる接続のホスト スキャン処理をオフに切り替えます。この設定は現在、クライアントレスおよび L3 接続に適用されます。このコマンドは、この設定を AnyConnect 接続にのみ適用するように変更されています。

	コマンド	目的
ステップ 10	**interim-accounting-update** {periodic *interval*} **例：** (config-aaa-server-group)# interim-accounting-update periodic 12	RADIUS 中間アカウンティング アップデート メッセージの生成をイネーブルにします。現在、これらのメッセージは、VPN トンネル接続がクライアントレス VPN セッションに追加された場合にだけ生成されます。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウンティング アップデートが生成されます。現在の機能を許可する、またはアカウンティング メッセージを指示されたサーバ グループに送信するように設定されたすべてのセッションに対して定期的なアカウンティング アップデートの生成を許可する設定ができるように、このコマンドにキーワードが追加されています。 *[periodic]*：このオプションのキーワードは、対象のサーバ グループにアカウンティング レコードを送信するように設定されたすべての VPN セッションのアカウンティング レコードの定期的な生成と伝送をイネーブルにします。 *[interval]*：定期的なアカウンティング アップデート間の間隔の長さを時間単位で表す数値です。有効な範囲は 1 ～ 120 で、デフォルト値は 24 です。

例

次に、1 つのサーバを含む 1 つの RADIUS グループを追加する例を示します。

```
ciscoasa(config)# aaa-server AuthOutbound protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key RadUauthKey
ciscoasa(config-aaa-server-host)# exit
```

次に、許可専用の動的許可（CoA）の更新と時間ごとの定期的なアカウンティングの ISE サーバ オブジェクトを設定する例を示します。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
```

次に、ISE でパスワード認証用のトンネル グループを設定する例を示します。

```
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

次に、ISE でローカル証明書の検証と許可用のトンネル グループを設定する例を示します。

```
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

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

	コマンド	目的
ステップ 1	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **例：** `ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1`	RADIUS サーバと、そのサーバが属する AAA サーバ グループを識別します。 **aaa-server host** コマンドを入力すると、AAA サーバのホスト コンフィギュレーション モードを開始します。
ステップ 2	**acl-netmask-convert** {**auto-detect** | **standard** | **wildcard**} **例：** `ciscoasa(config-aaa-server-host)#` **acl-netmask-convert standard**	RADIUS サーバ（**aaa-server host** コマンドを使用してアクセスします）からダウンロード可能 ACL で受け取ったネットマスクを ASA が処理する方法について指定します。 **auto-detect** キーワードは、使用されているネットマスク表現のタイプの判別を ASA が試みる必要があることを指定します。ASA によってワイルドカード ネットマスク表現が検出された場合は、標準ネットマスク表現に変換されます。 **standard** キーワードは、RADIUS サーバから受信したダウンロード可能 ACL には、標準ネットマスク表現のみが含まれていると ASA が見なすように指定します。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** キーワードは、RADIUS サーバから受信したダウンロード可能 ACL には、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 ASA が見なし、ACL をダウンロードしたときにそれらすべてを標準ネットマスク表現に変換するように指定します。
ステップ 3	**radius-common-pw** *string* **例：** `ciscoasa(config-aaa-server-host)# radius-common-pw examplepassword123abc`	ASA を介して RADIUS 許可サーバにアクセスするすべてのユーザが使用する共通パスワードを指定します。 *string* 引数は、大文字と小文字が区別される最大 127 文字の英数字キーワードです。RADIUS サーバとのすべての許可トランザクションで共通パスワードとして使用されます。

	コマンド	目的
ステップ 4	**mschapv2-capable** **例：** ciscoasa(config-aaa-server-host)# mschapv2-capable	RADIUS サーバへの MS-CHAPv2 認証要求をイネーブルにします。
ステップ 5	**timeout** *hh:mm:ss* **例：** ciscoasa(config-aaa-server-host)# timeout 15	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	**retry-interval** *seconds* **例：** ciscoasa(config-aaa-server-host)# retry-interval 8	前に **aaa-server host** コマンドで指定した特定の AAA サーバに対して、再試行間隔を設定します。 *seconds* 引数に要求の再試行間隔（1 ～ 10 秒）を指定します。これは、接続要求を再試行するまでに ASA が待機する時間です。 **（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 7	**accounting-mode simultaneous** **例：** ciscoasa(config-aaa-server-group)# accounting-mode simultaneous	グループ内のすべてのサーバにアカウンティング メッセージを送信します。 アクティブ サーバにのみメッセージを送信するデフォルトに戻すには、**accounting-mode single** コマンドを入力します。
ステップ 8	**authentication-port** *port* **例：** ciscoasa(config-aaa-server-host)# authentication-port 1645	認証ポートをポート番号 1645 に指定するか、またはユーザ認証に使用するサーバ ポートを指定します。
ステップ 9	**accounting-port** *port* **例：** ciscoasa(config-aaa-server-host)# accounting-port 1646	アカウンティング ポートをポート番号 1646 に指定するか、またはこのホスト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。
ステップ 10	**key** **例：** ciscoasa(config-aaa-host)# key myexamplekey1	ASA に対する RADIUS サーバの認証に使用されるサーバ秘密値を指定します。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。サーバ秘密キーの値が不明の場合は、RADIUS サーバの管理者に問い合わせてください。最大長は、64 文字です。

例

次に、既存の RADIUS サーバ グループに RADIUS サーバを追加する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa(config-aaa-server-host)# radius-common-pw myexaplepasswordabc123
ciscoasa(config-aaa-server-host)# mschapv2-capable
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# accounting-mode simultaneous
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# authorization-port 1645
ciscoasa(config-aaa-server-host)# key mysecretkeyexampleiceage2
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

RADIUS サーバのモニタリング

RADIUS サーバをモニタするには、次のコマンドのいずれかを入力します。

コマンド	目的
show aaa-server	設定した RADIUS サーバの統計情報を表示します。 RADIUS サーバのコンフィギュレーションを消去するには、**clear aaa-server statistics** コマンドを入力します。
show running-config aaa-server	RADIUS サーバの実行コンフィギュレーションを表示します。 RADIUS サーバの統計情報を消去するには、**clear configure aaa-server** コマンドを入力します。

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.28-22）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 28-3 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。

表 28-3　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の記述。 次のコマンドを導入しました。 **aaa-server protocol**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**show aaa-server**、**show running-config aaa-server**、**clear aaa-server statistics**、**authentication-port**、**accounting-port**、**retry-interval**、**acl-netmask-convert**、**clear configure aaa-server**、**merge-dacl**、**radius-common-pw**、**key**。
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る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、許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。

CHAPTER 29

AAA 用の TACACS+ サーバ

この章では、AAA で使用される 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」（P.29-1）
- 「TACACS+ サーバのライセンス要件」（P.29-3）
- 「ガイドラインと制限事項」（P.29-3）
- 「TACACS+ サーバの設定」（P.29-3）
- 「TACACS+ サーバのモニタリング」（P.29-6）
- 「TACACS+ サーバの機能履歴」（P.29-7）

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 29-1 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+ 許可応答属性の一覧を示します。表 29-2 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 29-1　サポートされる TACACS+ 許可応答属性

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 29-2　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た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た出力バイト数を指定します（ストップ レコードのみ）。
cmd	実行された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	トンネル接続のためにクライアントが接続した 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た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た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	使用された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

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

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場合は、「フォールバック サポート」（P.27-2）および「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.27-2）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.35-34）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」（P.29-4）
- 「TACACS+ サーバ グループの設定」（P.29-4）
- 「グループへの TACACS+ サーバの追加」（P.29-6）

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.29-4）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.29-6）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

	コマンド	目的

ステップ 1	**aaa-server** *server_tag* **protocol tacacs+**
	
	例：
	`ciscoasa(config)# aaa-server servergroup1 protocol tacacs+`
	`ciscoasa(config-aaa-server-group)#`
		サーバ グループ名とプロトコルを識別します。
		
		aaa-server protocol コマンドを入力すると、コンフィギュレーション モードに入ります。

ステップ 2	**max-failed-attempts** *number* **例：** `ciscoasa(config-aaa-server-group)# max-failed-attempts 2`	次のサーバを試す前にグループ内の AAA サーバに送信する要求の最大数を指定します。*number* 引数の範囲は 1 ～ 5 です。デフォルト値は 3 です。 ローカル データベースを使用してフォールバック方式（管理アクセス専用）を設定している場合で、グループ内のすべてのサーバが応答しないとき、グループは応答なしと見なされ、フォールバック方式が試行されます。このサーバ グループは 10 分間（デフォルト）非応答としてマークされるため、その期間内の追加の AAA 要求については、サーバ グループへのアクセスを試みることなく、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。 フォールバック方式が設定されていない場合、ASA は引き続きグループ内のサーバへのアクセスを試みます。

	コマンド	目的
ステップ 3	**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**} **例：** ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20	グループ内で障害の発生したサーバを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。 **depletion** キーワードを指定すると、グループ内のすべてのサーバが非アクティブになった後に、障害の発生したサーバが再度アクティブ化されます。 **deadtime** *minutes* キーワード引数のペアには、グループ内の最後のサーバをディセーブルにしてから、次にすべてのサーバを再度イネーブルにするまでの経過時間を分単位で 0 ～ 1440 から指定します。デフォルトは 10 分です。 **timed** キーワードは、30 秒間のダウンタイムの後に障害が発生したサーバを再度アクティブ化します。
ステップ 4	**accounting-mode simultaneous** **例：** ciscoasa(config-aaa-server-group)# accounting-mode simultaneous	グループ内のすべてのサーバにアカウンティング メッセージを送信します。 アクティブ サーバにのみメッセージを送信するデフォルトに戻すには、**accounting-mode single** コマンドを入力します。

例

次の例では、1 台のプライマリ サーバと 1 台のバックアップ サーバで構成された 1 つの TACACS+ グループを追加する例を示します。

```
ciscoasa(config)# aaa-server AuthInbound protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.1
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.2
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey2
ciscoasa(config-aaa-server-host)# exit
```

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

	コマンド	目的
ステップ 1	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **例：** `ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1`	TACACS+ サーバと、そのサーバが属するサーバ グループを識別します。 **aaa-server host** コマンドを入力すると、AAA サーバのホスト コンフィギュレーション モードを開始します。
ステップ 2	**timeout** *hh:mm:ss* **例：** `ciscoasa(config-aaa-server-host)# timeout 15`	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 3	**server-port** *port_number* **例：** `ciscoasa(config-aaa-server-host)# server-port 49`	サーバ ポートに対して、ポート番号 49、または ASA によって TACACS+ サーバとの通信に使用される TCP ポート番号を指定します。
ステップ 4	**key** **例：** `ciscoasa(config-aaa-host)# key myexamplekey1`	TACACS+ サーバに対する NAS の認証に使用されるサーバ秘密値を指定します。この値は大文字と小文字が区別される、最大 127 文字の英数字から成るキーワードで、TACACS+ サーバ上のキーと同じ値です。127 を超える文字は無視されます。このキーはクライアントとサーバ間でデータを暗号化するために使用され、クライアントとサーバ両方のシステムで同じである必要があります。このキーにスペースを含めることはできませんが、他の特殊文字は使用できます。

TACACS+ サーバのモニタリング

TACACS+ サーバをモニタするには、次のコマンドのいずれかを入力します。

コマンド	目的
show aaa-server	設定した TACACS+ サーバの統計情報を表示します。 TACACS+ サーバ コンフィギュレーションをクリアするには、**clear aaa-server statistics** コマンドを入力します。
show running-config aaa-server	TACACS+ サーバ実行コンフィギュレーションを表示します。 TACACS+ サーバの統計情報をクリアするには、**clear configure aaa-server** コマンドを入力します。

TACACS+ 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。

表 29-3　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。 次のコマンドを導入しました。 **aaa-server protocol**、**ax-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**aaa authorization exec authentication-server**、**server-port**、**key**、**clear aaa-server statistics**、**clear configure aaa-server**、**show aaa-server**、**show running-config aaa-server**、**username**、**service-type**、**timeout**。

CHAPTER 30

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」（P.30-1）
- 「LDAP サーバのライセンス要件」（P.30-4）
- 「ガイドラインと制限事項」（P.30-5）
- 「LDAP サーバの設定」（P.30-5）
- 「LDAP サーバのモニタリング」（P.30-12）
- 「LDAP サーバの機能履歴」（P.30-12）

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 Distinguished Name（DN; 識別者名）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許可を行うため、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許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。

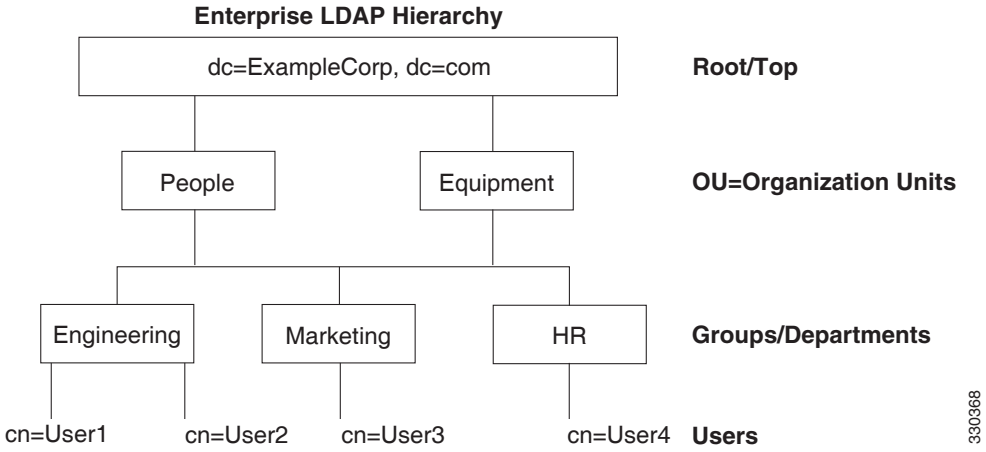
（注）　LDAP プロトコルの詳細については、RFC 1777、2251、および 2849 を参照してください。

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 30-1 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 30-1　　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 から許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 30-1 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 30-1 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 許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 30-1　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、ログインDN には、AD の「Member Of」の指定が Domain Users 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、ログインDN にはより高い特権が必要となり、AD の Account Operators グループに含まれている必要があります。

次に、ログイン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

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

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」（P.30-5）
- 「LDAP 属性マップの設定」（P.30-5）
- 「LDAP サーバ グループの設定」（P.30-8）「VPN のための LDAP での許可の設定」（P.30-10）

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.30-8）を参照してください。

ステップ 2　（オプション）認証メカニズムとは別の異なる LDAP サーバからの許可を設定します。「VPN のための LDAP での許可の設定」（P.30-10）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.30-5）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）：ディレクトリの部門名またはユーザ 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

	コマンド	目的
ステップ 1	**ldap attribute-map** *map-name* **例：** `ciscoasa(config)# ldap attribute-map att_map_1`	空の LDAP 属性マップ テーブルを作成します。
ステップ 2	**map-name** *user-attribute-name Cisco-attribute-name* **例：** `ciscoasa(config-ldap-attribute-map)# map-name department IETF-Radius-Class`	ユーザ定義の属性名 department を、シスコの属性にマッピングします。
ステップ 3	**map-value** *user-attribute-name Cisco-attribute-name* **例：** `ciscoasa(config-ldap-attribute-map)# map-value department Engineering group1`	ユーザ定義のマップ値である department をユーザ定義の属性値とシスコの属性値にマッピングします。

	コマンド	目的
ステップ 4	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **例：** ciscoasa(config)# aaa-server ldap_dir_1 host 10.1.1.4	サーバと、そのサーバが属する AAA サーバ グループを識別します。
ステップ 5	**ldap-attribute-map** *map-name* **例：** ciscoasa(config-aaa-server-host)# ldap-attribute-map att_map_1	属性マップを LDAP サーバにバインドします。

例

次の例は、accessType という名前の LDAP 属性に基づいて ASA への管理セッションを制限する方法を示しています。accessType 属性には、以下の値のいずれかが含まれる可能性があります。

- VPN
- admin
- helpdesk

次の例では、各値が、ASA でサポートされる有効な IETF-Radius-Service-Type 属性のいずれかにマッピングされる方法を示します。有効なタイプには、remote-access（Service-Type 5）発信、admin（Service-Type 6）管理、および nas-prompt（Service-Type 7）NAS プロンプトがあります。

```
ciscoasa(config)# ldap attribute-map MGMT
ciscoasa(config-ldap-attribute-map)# map-name accessType IETF-Radius-Service-Type
ciscoasa(config-ldap-attribute-map)# map-value accessType VPN 5
ciscoasa(config-ldap-attribute-map)# map-value accessType admin 6
ciscoasa(config-ldap-attribute-map)# map-value accessType helpdesk 7

ciscoasa(config-ldap-attribute-map)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 10.1.254.91
ciscoasa(config-aaa-server-host)# ldap-base-dn CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-password test
ciscoasa(config-aaa-server-host)# ldap-login-dn
CN=Administrator,CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# server-type auto-detect
ciscoasa(config-aaa-server-host)# ldap-attribute-map MGMT
```

次の例では、シスコの LDAP 属性名の全リストを表示します。

```
ciscoasa(config)# ldap attribute-map att_map_1
ciscoasa(config-ldap-attribute-map)# map-name att_map_1?

ldap mode commands/options:
cisco-attribute-names:
Access-Hours
  Allow-Network-Extension-Mode
  Auth-Service-Type
  Authenticated-User-Idle-Timeout
  Authorization-Required
  Authorization-Type
    :
    :
  X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

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（管理認証および許可限定）。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。

	コマンド	目的

ステップ 1	**aaa-server** *server_tag* **protocol ldap**
	
	例：
	`ciscoasa(config)# aaa-server servergroup1 protocol ldap`
	`ciscoasa(config-aaa-server-group)#`
		サーバ グループ名とプロトコルを識別します。**aaa-server protocol** コマンドを入力すると、コンフィギュレーション モードに入ります。

ステップ 2	**max-failed-attempts** *number* **例：** `ciscoasa(config-aaa-server-group)# max-failed-attempts 2`	次のサーバを試す前にグループ内の LDAP サーバに送信する要求の最大数を指定します。*number* 引数の範囲は 1 ～ 5 です。デフォルト値は 3 です。 ローカル データベースを使用してフォールバック方式を設定し（管理アクセスだけの場合）、グループ内のすべてのサーバが応答できなかった場合、グループは非応答と見なされ、フォールバック方式が試行されます。このサーバ グループは 10 分間（デフォルト）非応答としてマークされるため、その期間内の追加の AAA 要求については、サーバ グループへのアクセスを試みることなく、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。 フォールバック方式が設定されていない場合、ASA は引き続きグループ内のサーバへのアクセスを試みます。

	コマンド	目的
ステップ 3	**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**} **例：** ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20	グループ内で障害の発生したサーバを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。 **depletion** キーワードを指定すると、グループ内のすべてのサーバが非アクティブになった後に、障害の発生したサーバが再度アクティブ化されます。 **deadtime** *minutes* キーワード引数のペアには、グループ内の最後のサーバをディセーブルにしてから、次にすべてのサーバを再度イネーブルにするまでの経過時間を分単位で 0 ～ 1440 から指定します。デフォルトは 10 分です。 **timed** キーワードは、30 秒間のダウンタイムの後に障害が発生したサーバを再度アクティブ化します。
ステップ 4	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **例：** ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1 グループにサーバを追加するための新しい手順への移動	LDAP サーバと、そのサーバが属する AAA サーバグループを識別します。 **aaa-server host** コマンドを入力すると、AAA サーバのホスト コンフィギュレーション モードを開始します。必要に応じて、ホスト コンフィギュレーション モード コマンドを使用して、さらに AAA サーバを設定します。 LDAP サーバで使用できるコマンドと、新しい LDAP サーバ定義にそのコマンドのデフォルト値があるかどうかを、表 30-2 に示します。デフォルト値が指定されていない場合（「—」で表示）、コマンドを使用して値を指定します。

表 30-2　ホスト モード コマンドとデフォルト値

コマンド	デフォルト値	説明
ldap-attribute-map	—	**aaa server host** コマンドで手順内のステップを区切ります
ldap-base-dn	—	—
ldap-login-dn	—	—
ldap-login-password	—	—
ldap-naming-attribute	—	—
ldap-over-ssl	636	設定されていない場合は、ASA では LDAP 要求に sAMAccountName を使用します。SASL とプレーン テキストのどちらを使用する場合でも、ASA と LDAP サーバの間での通信のセキュリティは SSL で確保されます。SASL を設定しない場合、SSL で LDAP 通信を保護することを強くお勧めします。
ldap-scope	—	—
sasl-mechanism	—	—
server-port	389	—

表 30-2　ホスト モード コマンドとデフォルト値（続き）

コマンド	デフォルト値	説明
server-type	自動検出	自動検出により LDAP サーバのタイプが特定できなくても、そのサーバが、Microsoft Active Directory、Sun LDAP ディレクトリ サーバ、それ以外の LDAP サーバのいずれであるかがわかっている場合は、そのサーバ タイプを手動で設定できます。
timeout	10 秒	—

例

次の例では、watchdogs という名前の LDAP サーバ グループを設定し、そのグループに LDAP サーバを追加する方法を示します。この例では、リトライ インターバルや LDAP サーバがリスンするポートを定義しないため、ASA はこの 2 つのサーバ固有パラメータにデフォルト値を使用します。

```
ciscoasa(config)# aaa-server watchdogs protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

VPN のための LDAP での許可の設定

VPN アクセスのためのユーザ LDAP 認証が成功すると、ASA は、LDAP 属性を返す LDAP サーバのクエリーを実行します。通常これらの属性には、VPN セッションに適用される許可データが含まれます。このように LDAP を使用すると、1 つのステップで認証および許可を完了できます。

ただし、場合によっては、許可メカニズムとは別の異なる許可を LDAP ディレクトリ サーバから取得する必要があります。たとえば、認証に SDI または証明書サーバを使用している場合、許可情報は返されません。この場合、ユーザ許可では、認証の成功後に LDAP ディレクトリのクエリーを実行するため、認証と許可は 2 つのステップで行われます。

LDAP を使用した VPN ユーザ許可を設定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**tunnel-group** *groupname* **例：** ciscoasa(config)# tunnel-group remotegrp	「remotegrp」という名前の IPsec リモート アクセス トンネル グループを作成します。
ステップ 2	**tunnel-group** *groupname* **general-attributes** **例：** ciscoasa(config)# tunnel-group remotegrp general-attributes	サーバ グループとトンネル グループを関連付けます。
ステップ 3	**authorization-server-group** *group-tag* **例：** ciscoasa(config-general)# authorization-server-group ldap_dir_1	以前作成した認証のための AAA サーバ グループに新しいトンネル グループを割り当てます。

例

特定の要件で使用できる許可関連のコマンドとオプションは他にもありますが、次の例では、LDAP でのユーザ許可をイネーブルにするコマンドを示します。この例では、remote-1 という名前の IPsec リモートアクセス トンネルグループを作成し、すでに作成してある許可用の ldap_dir_1 AAA サーバ グループにその新しいトンネルグループを割り当てています。

```
ciscoasa(config)# tunnel-group remote-1 type ipsec-ra
ciscoasa(config)# tunnel-group remote-1 general-attributes
ciscoasa(config-general)# authorization-server-group ldap_dir_1
ciscoasa(config-general)#
```

この設定が完了したら、次のコマンドを入力して、ディレクトリ パスワード、ディレクトリ検索の開始点、ディレクトリ検索の範囲など、追加の LDAP 許可パラメータを設定できます。

```
ciscoasa(config)# aaa-server ldap_dir_1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
ciscoasa(config-aaa-server-host)# ldap-login-dn obscurepassword
ciscoasa(config-aaa-server-host)# ldap-base-dn starthere
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)#
```

LDAP サーバのモニタリング

LDAP サーバを監視するには、次のいずれかのコマンドを入力します。

コマンド	目的
show aaa-server	設定済みの AAA サーバの統計情報を表示します。 AAA サーバ コンフィギュレーションをクリアするには、**clear aaa-server statistics** コマンドを入力します。
show running-config aaa-server	AAA サーバ実行コンフィギュレーションを表示します。 AAA サーバの統計情報をクリアするには、**clear configure aaa-server** コマンドを入力します。

LDAP 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。

表 30-3　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。 次のコマンドを導入しました。 **username**、**aaa authorization exec authentication-server**、**aaa authentication console LOCAL**、**aaa authorization exec LOCAL**、**service-type**、**ldap attribute-map**、**aaa-server protocol**、**aaa authentication {telnet | ssh | serial} console LOCAL**、**aaa authentication http console LOCAL**、**aaa authentication enable console LOCAL**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**authorization-server-group**、**tunnel-group**、**tunnel-group general-attributes**、**map-name**、**map-value**、**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」（P.31-1）
- 「アイデンティティ ファイアウォールのライセンス」（P.31-8）
- 「ガイドラインと制限事項」（P.31-8）
- 「前提条件」（P.31-10）
- 「アイデンティティ ファイアウォールの設定」（P.31-11）
- 「アイデンティティ ファイアウォールのモニタリング」（P.31-26）
- 「アイデンティティ ファイアウォールの機能履歴」（P.31-28）

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」（P.31-1）
- 「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」（P.31-2）
- 「アイデンティティ ファイアウォールの機能」（P.31-4）
- 「展開シナリオ」（P.31-5）

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、特定の IP アドレスに対する現在のユーザのアイデンティティ情報を取得する情報元として Windows Active Directory を使用し、Active Directory ユーザのトランスペアレント認証を実現します。

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、制約を受けることなく従来の IP アドレス ベースのルールと混在させることができます。

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。

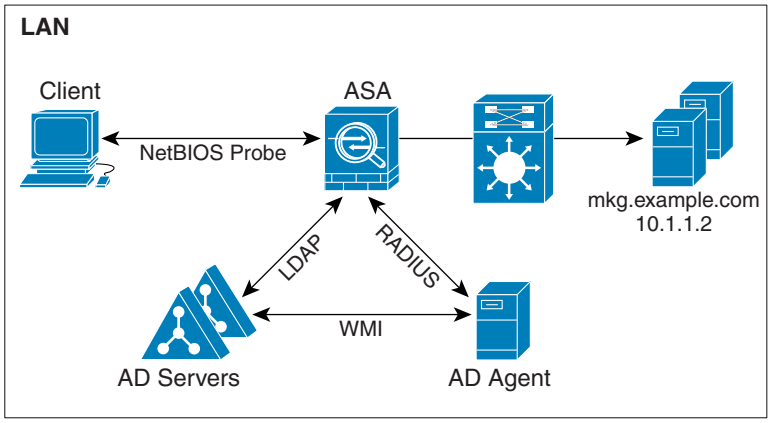
- Active Directory（AD）エージェント

  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 31-1 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 31-1　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 エージェントに対して 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間での分散 IP アドレス/ユーザ マッピング データベースが可能です。

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 31-2 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 31-2　冗長性のない展開シナリオ

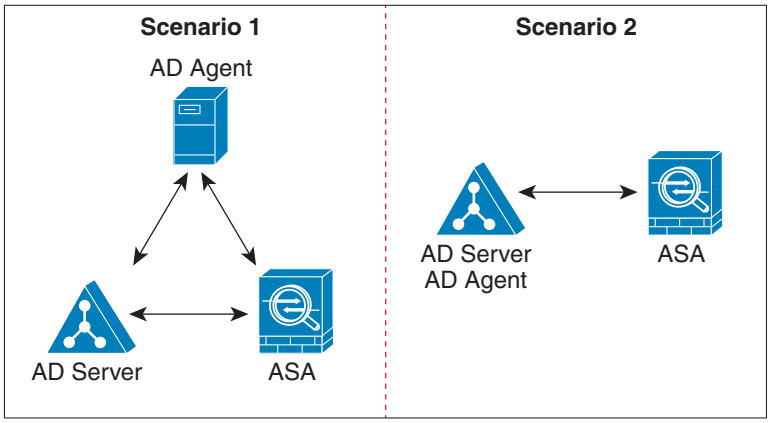


図 31-3 は、冗長性をサポートするためのアイデンティティ ファイアウォールのコンポーネントの展開方法を示しています。シナリオ 1 では、複数の Active Directory サーバと、AD エージェントをインストールした 1 台の Windows サーバを配置しています。シナリオ 2 では、複数の Active Directory サーバと、それぞれ AD エージェントがインストールされた複数の Windows サーバを配置しています。

図 31-3　　冗長コンポーネントのある展開シナリオ

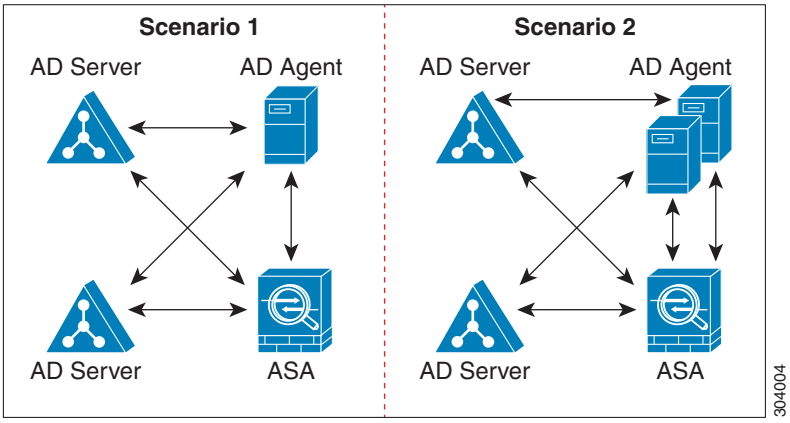


図 31-4は、LAN 上にすべてのアイデンティティ ファイアウォール コンポーネント（Active Directory サーバ、AD エージェント、クライアント）がインストールされ通信する方法を示しています。

図 31-4　　LAN ベースの展開

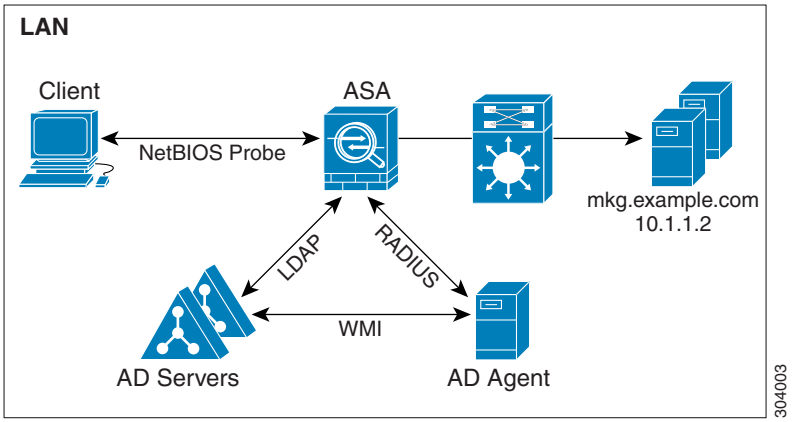


図 31-5 は、WAN を使用してリモート サイトと接続した展開方法を示しています。Active Directory サーバと AD エージェントはメイン サイトの LAN 上に配置されています。クライアントはリモート サイトに配置されており、WAN 経由でアイデンティティ ファイアウォール コンポーネントに接続しています。

図 31-5　WAN ベースの展開

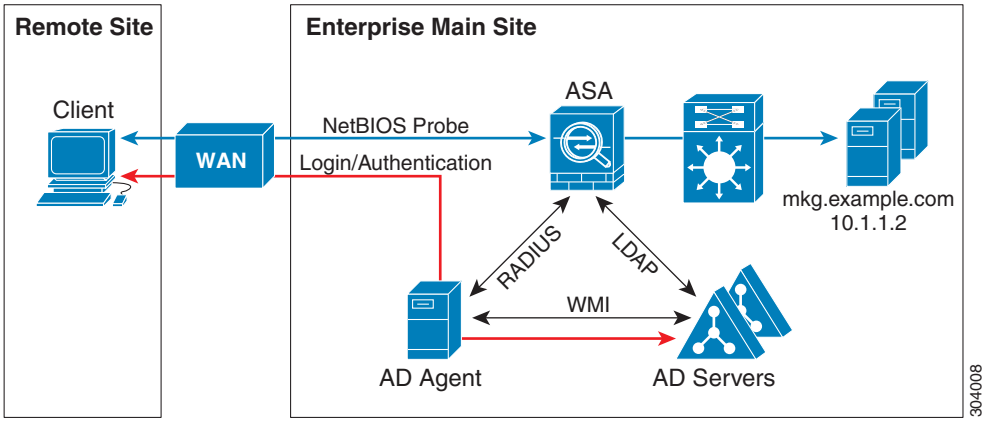


図 31-6 も WAN を使用したリモート サイトにまたがる展開方法を示しています。Active Directory サーバはメイン サイトの LAN にインストールされています。一方、AD エージェントはリモート サイトに配置され、同じサイト内のクライアントからアクセスされます。リモート クライアントは、WAN 経由でメイン サイトの Active Directory サーバに接続します。

図 31-6　リモート AD エージェントを使用した WAN ベースの展開

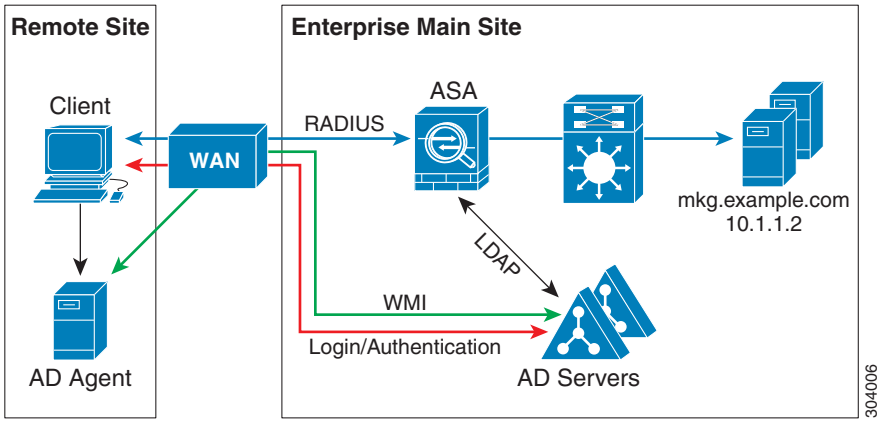
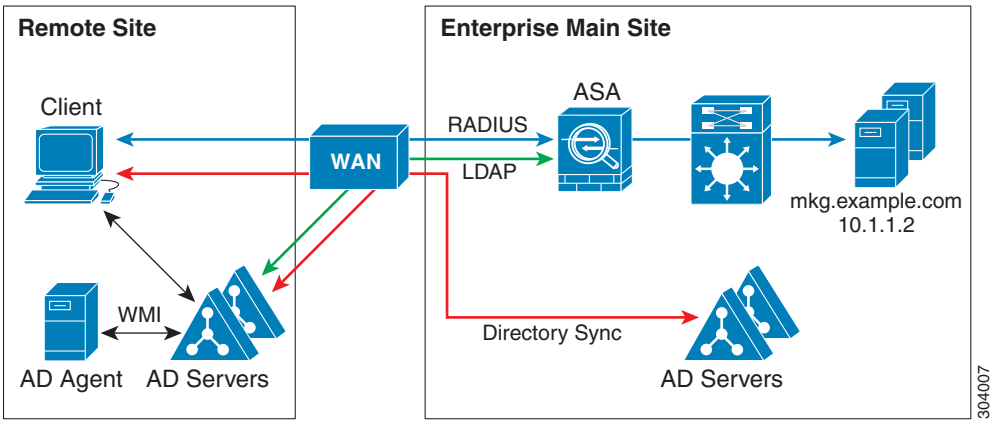


図 31-7 は、リモート サイトを拡張した WAN ベースの展開を示しています。AD エージェントと Active Directory サーバがリモート サイトに配置されています。クライアントは、メイン サイトに配置されているネットワーク リソースにログインする際に、これらのコンポーネントにローカルでアクセスします。リモート Active Directory サーバは、メイン サイトに配置された Active Directory サーバとの間でデータを同期する必要があります。

図 31-7　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

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

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。

  「ERROR: one update active-user-database is already in progress.」

  前のセッションが完全に終了するまで待機する必要があります。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 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 ファイアウォールの設定のタスク フロー」（P.31-11）
- 「Active Directory ドメインの設定」（P.31-12）
- 「Active Directory エージェントの設定」（P.31-14）
- 「アイデンティティ オプションの設定」（P.31-15）
- 「アイデンティティに基づくセキュリティ ポリシーの設定」（P.31-21）
- 「ユーザ統計の収集」（P.31-23）

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.31-12）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.31-5）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 エージェントの設定」（P.31-14）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.31-5）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.31-15）を参照してください。

ステップ 4　アイデンティティに基づくセキュリティ ポリシーを設定します。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。

「アイデンティティに基づくセキュリティ ポリシーの設定」（P.31-21）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するときに、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。

	コマンド	目的
ステップ 1	**aaa-server** *server-tag* **protocol ldap** **例：** `ciscoasa(config)# aaa-server adserver protocol ldap`	AAA サーバ グループを作成し、Active Directory サーバの AAA サーバ パラメータを設定します。
ステップ 2	**aaa-server** *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*] **例：** `ciscoasa(config-aaa-server-group)# aaa-server adserver (mgmt) host 172.168.224.6`	Active Directory サーバに対し、AAA サーバを AAA サーバ グループの一部として設定し、ホスト固有の AAA サーバ パラメータを設定します。
ステップ 3	**ldap-base-dn** *string* **例：** `ciscoasa(config-aaa-server-host)# ldap-base-dn DC=SAMPLE,DC=com`	サーバが許可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。 **ldap-base-dn** コマンドの指定は任意です。このコマンドを指定しなかった場合、ASA は Active Directory から defaultNamingContext を取得し、それをベース DN として使用します。

	コマンド	目的
ステップ 4	**ldap-scope subtree** **例：** `ciscoasa(config-aaa-server-host)# ldap-scope subtree`	サーバが許可要求を受信した場合に検索する LDAP 階層の範囲を指定します。
ステップ 5	**ldap-login-password** *string* **例：** `ciscoasa(config-aaa-server-host)# ldap-login-password obscurepassword`	LDAP サーバのログイン パスワードを指定します。
ステップ 6	**ldap-login-dn** *string* **例：** `ciscoasa(config-aaa-server-host)# ldap-login-dn SAMPLE\user1`	システムがバインドするディレクトリ オブジェクトの名前を指定します。ASA は、ログイン DN フィールドをユーザ認証要求にアタッチして、認証済みバインディングに対して識別情報を示します。ログイン DN フィールドには、ASA の認証特性が記述されます。 *string* 引数は、LDAP 階層内のディレクトリ オブジェクトの名前を指定する、最大 128 文字の文字列です。大文字と小文字は区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。 従来の形式と簡易形式のどちらでも指定できます。 一般的な **ldap-login-dn** コマンドの形式は次のとおりです。 CN=username,OU=Employees,OU=Sample Users,DC=sample,DC=com
ステップ 7	**server-type microsoft** **例：** `ciscoasa(config-aaa-server-host)# server-type microsoft`	Microsoft Active Directory サーバの LDAP サーバ モデルを設定します。
ステップ 8	**ldap-group-base-dn** *string* **例：** `ciscoasa(config-aaa-server-host)# ldap-group-base-dn OU=Sample Groups,DC=SAMPLE,DC=com`	Active Directory ドメイン コントローラにおける Active Directory グループ設定の場所を指定します。指定しないと、**ldap-group-base-dn** コマンドの値が使用されます。 **ldap-group-base-dn** コマンドの指定は任意です。

	コマンド	目的
ステップ 9	**ldap-over-ssl enable** **例：** ciscoasa(config-aaa-server-host)# ldap-over-ssl enable	ASA が SSL 上で Active Directory ドメイン コントローラとアクセスできるようにします。LDAP over SSL をサポートするには、Active Directory サーバがこのサポートを確保するように設定する必要があります。 デフォルトでは、Active Directory に SSL は設定されていません。Active Directory に SSL が設定されていない場合は、アイデンティティ ファイアウォールのために ASA に SSL を設定する必要はありません。
ステップ 10	**server-port** *port-number* **例：** ciscoasa(config-aaa-server-host)# server-port 389 ciscoasa(config-aaa-server-host)# server-port 636	デフォルトでは、**ldap-over-ssl** コマンドがイネーブルになっていない場合、デフォルトのポート サーバは 389 になり、**ldap-over-ssl** コマンドがイネーブルになっている場合、デフォルトのサーバ ポートは 636 になります。
ステップ 11	**group-search-timeout** *seconds* **例：** ciscoasa(config-aaa-server-host)# group-search-timeout 300	LDAP クエリー がタイムアウトになるまでの時間を設定します。

Active Directory エージェントの設定

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。

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。

	コマンド	目的
ステップ 1	**aaa-server** *server-tag* **protocol radius** **例：** ciscoasa(config)# aaa-server adagent protocol radius	AAA サーバ グループを作成し、AD エージェントの AAA サーバ パラメータを設定します。
ステップ 2	**ad-agent-mode** **例：** ciscoasa(config)# ad-agent-mode	AD エージェント モードをイネーブルにします。

	コマンド	目的
ステップ 3	**aaa-server** *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*] **例：** `ciscoasa(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101`	AD エージェントに対し、AAA サーバを AAA サーバ グループの一部として設定し、ホスト固有の AAA サーバ パラメータを設定します。
ステップ 4	**key** *key* **例：** `ciscoasa(config-aaa-server-host)# key mysecret`	AD エージェント サーバに対する ASA の認証に使用されるサーバ秘密値を指定します。
ステップ 5	**user-identity ad-agent aaa-server** *aaa_server_group_tag* **例：** `ciscoasa(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent`	AD エージェントのサーバ グループを定義します。 *aaa_server_group_tag* 引数に定義する最初のサーバがプライマリ AD エージェントとなり、次に定義するサーバがセカンダリ AD エージェントとなります。 アイデンティティ ファイアウォールでは、2 つの AD エージェント ホストのみ定義できます。 プライマリ AD エージェントが停止していることを 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、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 AAA サーバは通信プロトコルとして RADIUS を使用するため、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。
ステップ 6	**test aaa-server ad-agent** **例：** `ciscoasa(config-aaa-server-host)# test aaa-server ad-agent`	ASA と AD エージェント サーバとの通信をテストします。

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。「アイデンティティに基づくセキュリティ ポリシーの設定」（P.31-21）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

この手順を実行して、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.31-10）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。

	コマンド	目的
ステップ 1	**user-identity enable** **例：** `ciscoasa(config)# user-identity enable`	アイデンティティ ファイアウォール機能をイネーブルにします。
ステップ 2	**user-identity default-domain** *domain_NetBIOS_name* **例：** `ciscoasa(config)# user-identity default-domain SAMPLE`	アイデンティティ ファイアウォールのデフォルト ドメインを指定します。 *domain_NetBIOS_name* 引数には、[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、名前全体を引用符で囲みます。ドメイン名では、大文字と小文字が区別されません。 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。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。 **（注）** 指定するデフォルト 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 アイデンティティと IP アドレスのマッピング エントリを 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。 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に対して LOCAL ドメインを使用します。Web ポータル（カットスルー プロキシ）経由でログインしたユーザは、認証された Active Directory ドメインに属すると見なされます。VPN が Active Directory で LDAP により認証されていない限り、VPN 経由でログインしたユーザは、ローカル ドメインに属すると見なされます。この場合は、アイデンティティ ファイアウォールは、Active Directory ドメインとユーザを関連付けることができます。

	コマンド	目的
ステップ 3	**user-identity domain** *domain_nickname* **aaa-server** *aaa_server_group_tag* **例：** `ciscoasa(config)# user-identity domain SAMPLE aaa-server ds`	AAA サーバでユーザ グループ クエリーのインポート用に定義された LDAP パラメータをドメイン名に関連付けます。 *domain_nickname* 引数には、[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。
ステップ 4	**user-identity logout-probe netbios local-system probe-time minutes** *minutes* **retry-interval seconds** *seconds* **retry-count** *times* [**user-not-needed** | **match-any** | **exact-match**] **例：** `ciscoasa(config)# user-identity logout-probe netbios local-system probe-time minutes 10 retry-interval seconds 10 retry-count 2 user-not-needed`	NetBIOS プローブをイネーブルにします。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 クライアント IP アドレスのプローブによって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。デフォルトでは、NetBIOS プローブはディセーブルになっています。 NetBIOS パケットを最小限に抑えるために、ASA は、ユーザが指定された分数を超えて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。 • **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。 • **User-not-needed**：ASA がクライアントから 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。 アイデンティティ ファイアウォールは、少なくとも 1 つのセキュリティ ポリシーに存在するアクティブ状態のユーザ アイデンティティに対してのみ NetBIOS プローブを実行します。ASA は、ユーザがカットスルー プロキシ経由または VPN を使用してログインするクライアントについては、NetBIOS プローブを実行しません。

	コマンド	目的
ステップ 5	**user-identity inactive-user-timer minutes** *minutes* **例：** `ciscoasa(config)# user-identity inactive-user-timer minutes 120`	ユーザがアイドル状態であると見なされるまでの時間を指定します。これは、ASA が指定された時間にわたりユーザの IP アドレスからトラフィックを受信しなかった場合を意味します。 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 キャッシュ内のユーザ アイデンティティと IP アドレスのマッピング データベースから削除されます。ASA は、この IP アドレスを 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。このコマンドを指定すると、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。 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。 **（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 6	**user-identity poll-import-user-group-timer hours** *hours* **例：** `ciscoasa(config)# user-identity poll-import-user-group-timer hours 1`	ASA が Active Directory サーバにユーザ グループ情報を問い合わせるまでの時間を指定します。 Active Directory グループでユーザが追加または削除されると、ASA はグループ インポート タイマーの実行後に更新されたユーザ グループを受け取ります。 デフォルトでは、**poll-import-user-group-timer hours** の値は 8 時間です。 ユーザ グループ情報をただちに更新するには、**user-identity update import-user** コマンドを入力します。
ステップ 7	**user-identity action netbios-response-fail remove-user-ip** **例：** `ciscoasa(config)# user-identity action netbios-response-fail remove-user-ip`	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を指定します。このような状況には、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などがあります。 **user-identity action remove-user-ip** コマンドを設定すると、ASA はそのクライアントのユーザ アイデンティティと IP アドレスのマッピングを削除します。 デフォルトでは、このコマンドはディセーブルです。

	コマンド	目的
ステップ 8	**user-identity action domain-controller-down** *domain_nickname* **disable-user-identity-rule** **例：** ciscoasa(config)# user-identity action domain-controller-down SAMPLE disable-user-identity-rule	Active Directory ドメイン コントローラが応答しないためにドメインがダウンしている場合のアクションを指定します。 ドメインがダウンし、**disable-user-identity-rule** キーワードが設定されている場合、ASA はそのドメインのユーザ アイデンティティと IP アドレスのマッピングをディセーブルにします。さらに、**show user-identity user** コマンドによって表示される出力では、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。 デフォルトでは、このコマンドはディセーブルです。
ステップ 9	**user-identity user-not-found enable** **例：** ciscoasa(config)# **user-identity user-not-found enable**	user-not-found トラッキングをイネーブルにします。最後の 1024 個の IP アドレスだけがトラッキングされます。 デフォルトでは、このコマンドはディセーブルです。
ステップ 10	**user-identity action ad-agent-down disable-user-identity-rule** **例：** ciscoasa(config)# user-identity action ad-agent-down disable-user-identity-rule	AD エージェントが応答していない場合のアクションを指定します。 AD エージェントがダウンし、**user-identity action ad-agent-down** コマンドが設定されている場合、ASA はそのドメインのユーザに関連付けられたユーザ アイデンティティ ルールをディセーブルにします。さらに、**show user-identity user** コマンドによって表示される出力では、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。 デフォルトでは、このコマンドはディセーブルです。
ステップ 11	**user-identity action mac-address-mismatch remove-user-ip** **例：** ciscoasa(config)# user-identity action mac-address-mismatch remove-user-ip	ユーザの MAC アドレスが、そのアドレスに現在マッピングされている ASA IP アドレスと一致しないことが明らかになった場合のアクションを指定します。 **user-identity action mac-address-mismatch** コマンドが設定されている場合、ASA はそのクライアントのユーザ アイデンティティと IP アドレスのマッピングを削除します。 デフォルトでは、このコマンドが指定されている場合、ASA は **remove-user-ip** キーワードを使用します。

	コマンド	目的
ステップ 12	**user-identity ad-agent active-user-database** {**on-demand** | **full-download**} **例：** `ciscoasa(config)# user-identity ad-agent active-user-database full-download`	ASA が 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情報を取得する方法を定義します。 • **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 マッピング情報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。 • **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。 デフォルトでは、ASA は full-download オプションを使用します。 フル ダウンロードはイベント ドリブンです。つまり、2 回目以降のデータベース ダウンロード要求があった場合、ユーザ アイデンティティと IP アドレス マッピング データベースの更新内容だけが送信されます。 ASA が変更要求を AD エージェントに登録すると、AD エージェントは新しいイベントを ASA に送信します。
ステップ 13	**user-identity ad-agent hello-timer seconds** *seconds* **retry-times** *number* **例：** `ciscoasa(config)# user-identity ad-agent hello-timer seconds 20 retry-times 3`	ASA と AD エージェントとの間の Hello タイマーを定義します。 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。 デフォルトでは、Hello タイマーは間隔が 30 秒、リトライ回数が 5 回に設定されます。

	コマンド	目的
ステップ 14	**user-identity ad-agent event-timestamp-check** **例：** `ciscoasa(config)# user-identity ad-agent event-timestamp-check`	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 をイネーブルにできます。 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 15	**user-identity ad-agent aaa-server** *aaa_server_group_tag* **例：** `ciscoasa(config)# user-identity ad-agent aaa-server adagent`	AD エージェントのサーバ グループを定義します。 *aaa_server_group_tag* 引数には、**aaa-server** コマンドで定義された値を入力します。

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.31-12）を参照してください。

AD エージェントを設定します。「Active Directory エージェントの設定」（P.31-14）を参照してください。

アイデンティティに基づくセキュリティ ポリシーの設定

アイデンティティに基づく 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（「ガイドラインと制限事項」（P.31-8）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。

- 拡張 ACL を設定するには、第 17 章「アクセス コントロール リスト」を参照してください。
- ACL で使用できるローカル ユーザ グループを設定するには、「ローカル ユーザ グループの設定」（P.16-7）を参照してください。

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。

ユーザ統計の収集

モジュラ ポリシー フレームワークによるユーザの統計情報の収集とアイデンティティ ファイアウォールの一致ルックアップ アクションをアクティブにするには、次のコマンドを入力します。

コマンド	目的
user-statistics [**accounting** | **scanning**] **例：** ciscoasa(config)# class-map c-identity-example-1 ciscoasaciscoasa(config-cmap)# match access-list identity-example-1 ciscoasaciscoasa(config-cmap)# exit ciscoasaciscoasa(config)# policy-map p-identity-example-1 ciscoasaciscoasa(config-pmap)# class c-identity-example-1 ciscoasaciscoasa(config-pmap)# user-statistics accounting ciscoasaciscoasa(config-pmap)# exit ciscoasaciscoasa(config)# service-policy p-identity-example-1 interface outside	モジュラ ポリシー フレームワークによるユーザ統計情報の収集と、アイデンティティ ファイアウォールの一致ルックアップ アクションをアクティブにします。 **accounting** キーワードは、ASA が送信パケット カウント、送信ドロップ カウント、受信パケット カウントを収集することを指定します。**scanning** キーワードは、ASA が送信ドロップ カウントだけを収集することを指定します。 ユーザ統計情報を収集するようポリシー マップを設定すると、ASA は選択したユーザの詳細な統計情報を収集します。**user-statistics** コマンドを **accounting** または **scanning** キーワードなしで指定すると、ASA はアカウティング統計とスキャニング統計の両方を収集します。

設定例

- 「AAA ルールとアクセス ルールの例 1」（P.31-23）
- 「AAA ルールとアクセス ルールの例 2」（P.31-24）
- 「VPN フィルタの例」（P.31-24）

AAA ルールとアクセス ルールの例 1

次の例は、ユーザが ASA を介してログインすることを可能にする典型的なカットスルー プロキシ設定を示します。この例は次の条件に基づいています。

- ASA の IP アドレスは 172.1.1.118 です。
- Active Directory ドメイン コントローラの IP アドレスは 71.1.2.93 です。
- エンド ユーザ クライアントは、IP アドレスが 172.1.1.118 であり、HTTPS を使用して Web ポータル経由でログインします。
- ユーザは、LDAP を介して Active Directory ドメイン コントローラにより認証されます。
- ASA は、Inside インターフェイスを使用して企業ネットワーク上の Active Directory ドメイン コントローラに接続します。

```
ciscoasa(config)# access-list AUTH extended permit tcp any 172.1.1.118 255.255.255.255 eq http
ciscoasa(config)# access-list AUTH extended permit tcp any 172.1.1.118 255.255.255.255 eq https
ciscoasa(config)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 171.1.2.93
ciscoasa(config-aaa-server-host)# ldap-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-group-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-dn cn=kao,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
```

```
ciscoasa(config-aaa-server-host)# ldap-login-password *****
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)# server-type microsoft
ciscoasa(config-aaa-server-host)# aaa authentication match AUTH inside LDAP
ciscoasa(config)#
ciscoasa(config)# http server enable
ciscoasa(config)# http 0.0.0.0 0.0.0.0 inside
ciscoasa(config)#
ciscoasa(config)# auth-prompt prompt Enter Your Authentication
ciscoasa(config)# auth-prompt accept You are Good
ciscoasa(config)# auth-prompt reject Goodbye
```

AAA ルールとアクセス ルールの例 2

この例には、次のガイドラインが適用されます。

- **access list** コマンドでは、未認証の着信ユーザが AAA カットスルー プロキシをトリガーできるように、**access-list 100 ex deny any any** コマンドを入力する前に permit user NONE ルールを設定する必要があります。
- **auth access-list** コマンドでは、permit user NONE ルールにより、未認証のユーザだけがカットスルー プロキシをトリガーします。これらを最後の行に指定することが理想的です。

```
ciscoasa(config)# access-list listenerAuth extended permit tcp any any
ciscoasa(config)# aaa authentication match listenerAuth inside ldap
ciscoasa(config)# aaa authentication listener http inside port 8888
ciscoasa(config)# access-list 100 ex permit ip user SAMPLE\user1 any any
ciscoasa(config)# access-list 100 ex deny ip user SAMPLE\user2 any any
ciscoasa(config)# access-list 100 ex permit ip user NONE any any
ciscoasa(config)# access-list 100 ex deny any any
ciscoasa(config)# access-group 100 in interface inside
ciscoasa(config)# aaa authenticate match 200 inside user-identity
```

VPN フィルタの例

一部のトラフィックでアイデンティティ ファイアウォールをバイパスすることが必要となる場合があります。

ASA は、VPN 認証または Web ポータル（カットスルー プロキシ）によってログインしたユーザを AD エージェントに報告し、AD エージェントがユーザ情報を登録されているすべての ASA デバイスに配布します。具体的には、認証されたユーザの IP とユーザのマッピングが、HTTP/HTTPS パケットを受信して認証する入力インターフェイスを含むすべての ASA コンテキストに転送されます。ASA は、VPN 経由でログインするユーザを LOCAL ドメインに属するユーザと見なします。

VPN ユーザにアイデンティティ ファイアウォール（IDFW）のルールを適用するには 2 種類の方法があります。

- アクセスリスト チェックのバイパスをディセーブルにして VPN フィルタを適用する
- アクセスリスト チェックのバイパスをイネーブルにして VPN フィルタを適用する

IDFW ルール -1 を使用する VPN の例

デフォルトでは **sysopt connection permit-vpn** コマンドがイネーブルになり、VPN トラフィックはアクセス リスト チェックの対象外となります。VPN トラフィックにインターフェイスに基づく ACL ルールを適用するには、VPN トラフィックのアクセス リスト バイパスをディセーブルにする必要があります。

この例では、ユーザが外部インターフェイスからログインすると、IDFW ルールはアクセス可能なネットワーク リソースを制御します。すべての VPN ユーザは LOCAL ドメインに保存されます。したがって、LOCAL ユーザまたは LOCAL ユーザを含むオブジェクト グループへのルールの適用のみが意味を持ちます。

```
!Apply VPN-Filter with bypassing access-list check disabled
no sysopt connection permit-vpn
access-list v1 extended deny ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v1 extended permit ip user LOCAL\idfw any 20.0.0.0 255.255.255.0
access-group v1 in interface outside
```

IDFW ルール -2 を使用する VPN の例

デフォルトでは、**sysopt connection permit-vpn** コマンドがイネーブルになり、VPN トラフィックのアクセス バイパスもイネーブルになります。VPN フィルタを使用することにより、VPN トラフィックに IDFW ルールを適用できます。IDFW ルールを指定した VPN フィルタは、CLI ユーザ名とグループ ポリシーで定義できます。

この例では、ユーザ idfw がログインすると、ユーザは、10.0.00/24 サブネットのネットワーク リソースにアクセスできます。これに対し、ユーザ user1 がログインした場合は、10.0.00/24 サブネット内のネットワーク リソースへのアクセスは拒否されます。すべての VPN ユーザが LOCAL ドメインに保存されることに注意してください。したがって、LOCAL ユーザまたは LOCAL ユーザを含むオブジェクト グループへのルールの適用のみが意味を持ちます。

（注） IDFW ルールはグループ ポリシーに基づく VPN フィルタにのみ適用でき、他のグループ ポリシー機能では使用できません。

```
!Apply VPN-Filter with bypassing access-list check enabled
sysopt connection permit-vpn
access-list v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v2 extended deny ip user LOCAL\user1 any 10.0.0.0 255.255.255.0
username user1 password QkBIIYVi6IFLEsYv encrypted privilege 0 username user1 attributes
    vpn-group-policy group1 vpn-filter value v2
username idfw password eEm2dmjMaopcGozT encrypted
username idfw attributes
    vpn-group-policy testgroup vpn-filter value v1

sysopt connection permit-vpn
access-list v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0 access-list
v1 extended deny ip user LOCAL\user1 any 10.0.0.0 255.255.255.0 group-policy group1
internal
group-policy group1 attributes

    vpn-filter value v1
    vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-client ssl-clientless
```

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」（P.31-26）
- 「グループのモニタリング」（P.31-26）
- 「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」（P.31-26）
- 「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」（P.31-27）

AD エージェントのモニタリング

AD エージェントのトラブルシューティング情報を取得するには、次のコマンドの 1 つを使用します。

- **show user-identity ad-agent**
- **show user-identity ad-agent statistics**

これらのコマンドによって、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 グループのトラブルシューティング情報を取得するには、**show user-identity group** コマンドを使用します。

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

アイデンティティ ファイアウォールのメモリ使用率に関するトラブルシューティング情報を取得するには、**show user-identity memory** コマンドを使用します。

このコマンドによって、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.31-15）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

AD エージェントのトラブルシューティング情報を取得するには、次のコマンドの 1 つを入力します。

- **show user-identity user all list**
- **show user-identity user active user** *domain\user-name* **list detail**

これらのコマンドによって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）
domain\user_name	アクティブなコネクション	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。

コマンド **user-identity action domain-controller-down** *domain_name* **disable-user-identity-rule** が設定されていて、指定されたドメインがダウンした場合、または **user-identity action ad-agent-down disable-user-identity-rule** コマンドが設定されていて、AD エージェントがダウンした場合には、ログオンしたすべてのユーザのステータスがディセーブルとなります。

アイデンティティ ファイアウォールの機能履歴

表 31-1 に、この機能のリリース履歴を示します。

\

表 31-1　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。 **user-identity enable**、**user-identity default-domain**、**user-identity domain**、**user-identity logout-probe**、**user-identity inactive-user-timer**、**user-identity poll-import-user-group-timer**、**user-identity action netbios-response-fail**、**user-identity user-not-found**、**user-identity action ad-agent-down**、**user-identity action mac-address-mismatch**、**user-identity action domain-controller-down**、**user-identity ad-agent active-user-database**、**user-identity ad-agent hello-timer**、**user-identity ad-agent aaa-server**、**user-identity update import-user**、**user-identity static user**、**dns domain-lookup**、**dns poll-timer**、**dns expire-entry-timer**、**object-group user**、**show user-identity**、**show dns, clear configure user-identity**、**clear dns**、**debug user-identity** の各コマンドが導入または変更されました。

ASA と Cisco TrustSec

- 「Cisco TrustSec と統合された ASA に関する情報」（P.32-1）
- 「Cisco TrustSec のライセンス要件」（P.32-11）
- 「Cisco TrustSec を使用するための前提条件」（P.32-12）
- 「ガイドラインと制限事項」（P.32-13）
- 「Cisco TrustSec と統合するための ASA の設定」（P.32-15）
- 「設定例」（P.32-30）
- 「Cisco TrustSec に対する AnyConnect VPN のサポート」（P.32-30）
- 「その他の関連資料」（P.32-32）
- 「Cisco TrustSec 統合の機能履歴」（P.32-33）

Cisco TrustSec と統合された ASA に関する情報

- 「Cisco TrustSec の概要」（P.32-2）
- 「Cisco TrustSec の SGT および SXP サポートについて」（P.32-2）
- 「Cisco TrustSec 機能のロール」（P.32-3）
- 「セキュリティ グループ ポリシーの適用」（P.32-4）
- 「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」（P.32-5）
- 「セキュリティ グループに対する変更が ISE に及ぼす影響」（P.32-6）
- 「ASA での送信者および受信者のロール」（P.32-7）
- 「SXP による頻繁な通信」（P.32-8）
- 「SXP タイマー」（P.32-8）
- 「IP-SGT マネージャ データベース」（P.32-9）
- 「ASA-Cisco TrustSec 統合の機能」（P.32-9）

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.32-32）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 スイッチ、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

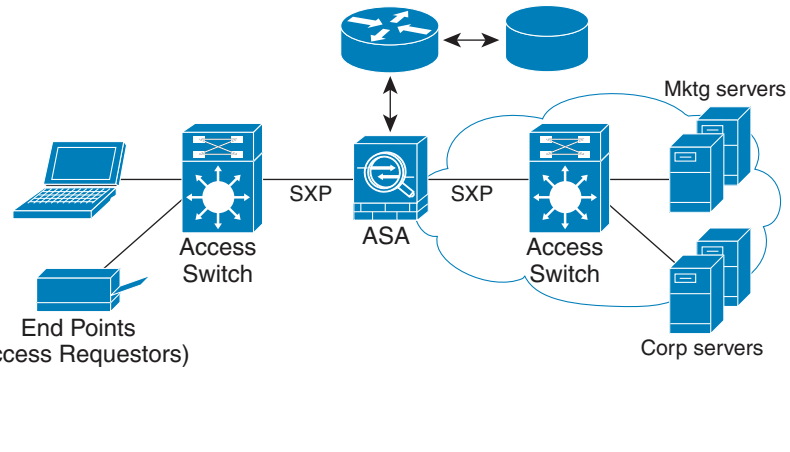
セキュリティ ポリシーの適用はセキュリティ グループの名前に基づきます。エンドポイント デバイスは、データセンターのリソースへのアクセスを試行します。ファイアウォールで設定された従来の IP ベースのポリシーと比較して、アイデンティティベースのポリシーは、ユーザおよびデバイス アイデンティティに基づいて設定されます。たとえば、mktg-contractor が mktg-server にアクセスできるとします。mktg-corp-user は、mktg-server および corp-server にアクセスできます。

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 32-1 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 32-1　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 31 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。

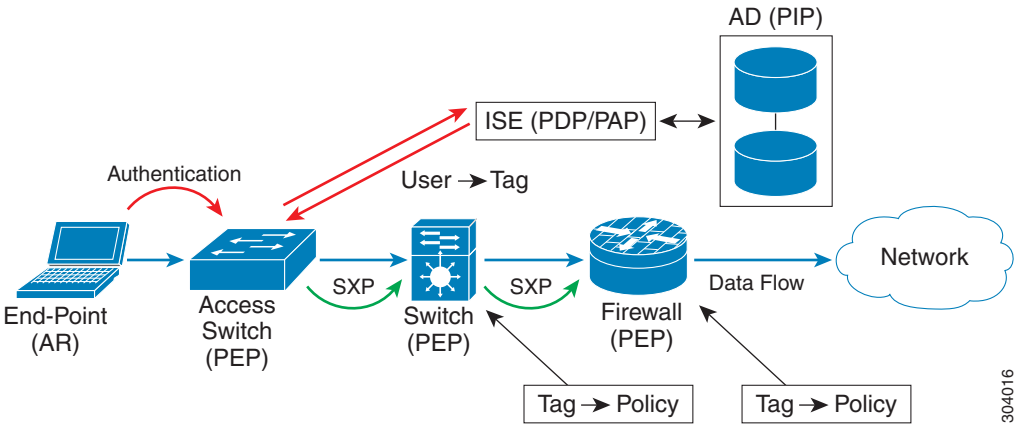
Cisco TrustSec と連携するように ASA を設定するには、ISE から Protected Access Credential（PAC）ファイルをインポートする必要があります。詳細については、「PAC ファイルのインポート」（P.32-17）を参照してください。

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 32-2 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 32-2　　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.32-7）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 による頻繁な通信

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 による頻繁な通信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 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 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 テーブルを更新するように 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

- 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 32-1 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 32-1　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 32-2 に、ASA がサポートする SXP 接続の数を示します。

表 32-2　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.32-12）
- 「ISE でのセキュリティ グループの作成」（P.32-12）
- 「PAC ファイルの生成」（P.32-13）

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.32-17）を参照してください。

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

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.32-13）と「PAC ファイルのインポート」（P.32-17）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.32-23）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」（P.32-16）
- 「PAC ファイルのインポート」（P.32-17）
- 「Security Exchange Protocol の設定」（P.32-19）
- 「SXP 接続のピアの追加」（P.32-22）
- 「環境データのリフレッシュ」（P.32-23）
- 「セキュリティ ポリシーの設定」（P.32-24）
- 「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」（P.32-25）

- 「SGT とイーサネット タギングのイネーブル化」（P.32-27）
- 「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」（P.32-28）
- 「手動で設定した Cisco TrustSec リンクへのポリシーの適用」（P.32-28）
- 「IP-SGT バインディングの手動設定」（P.32-29）

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。

ASA で ISE の AAA サーバ グループを設定するには、次の手順を実行します。

	コマンド	目的

ステップ 1	`ciscoasa(config)# aaa-server server-tag protocol radius`
	
	例：
	`ciscoasa(config)# aaa-server ISEserver protocol radius`
		AAA サーバ グループを作成し、ISE サーバと通信するように ASA の AAA サーバ パラメータを設定します。
		
		server-tag にはサーバ グループ名を指定します。
		
		詳細については、「ISE でのセキュリティ グループの作成」（P.32-12）を参照してください。

ステップ 2	`ciscoasa(config-aaa-server-group)# exit`	AAA サーバ グループ コンフィギュレーション モードを終了します。

ステップ 3	`ciscoasa(config)# aaa-server server-tag (interface-name) host server-ip`
	
	例：
	`ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1`
		AAA サーバを AAA サーバ グループの一部として設定し、ホスト固有の接続データを設定します。
		
		interface-name には、ISE サーバが配置されているネットワーク インターフェイスを指定します。このパラメータにはカッコが必要です。
		
		server-tag は、AAA サーバ グループの名前です。
		
		server-ip には、ISE サーバの IP アドレスを指定します。

ステップ 4	`ciscoasa(config-aaa-server-host)# key key`
	
	例：
	`ciscoasa(config-aaa-server-host)# key myexclusivemumblekey`
		ISE サーバで ASA の認証に使用されるサーバ秘密値を指定します。
		
		key は、最大 127 文字の英数字キーワードです。
		
		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入力します。
		
		詳細については、「ASA の ISE への登録」（P.32-12）を参照してください。

	コマンド	目的
ステップ 5	`ciscoasa(config-aaa-server-host)# exit`	AAA サーバ ホスト コンフィギュレーション モードを終了します。
ステップ 6	`ciscoasa(config)# cts server-group` *AAA-server-group-name* **例：** `ciscoasa(config)# cts server-group ISEserver`	環境データ取得のために Cisco TrustSec によって使用される AAA サーバ グループを識別します。 *AAA-server-group-name* は、ステップ 1 で *server-tag* 引数に指定した AAA サーバ グループの名前です。 ASA では、サーバ グループの 1 つのインスタンスだけを Cisco TrustSec 用に設定できます。

例

次に、Cisco TrustSec との統合のために ISE サーバと通信するように ASA を設定する例を示します。

```
ciscoasa(config)# aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# cts server-group ISEserver
```

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。

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.32-12）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、次のコマンドを入力します。

コマンド	目的
`ciscoasaciscoasa(config)# cts import-pac` *filepath* **password** *value* **例：** `ciscoasaciscoasa(config)# cts import-pac disk0:/xyz.pac password IDFW-pac99`	Cisco TrustSec PAC ファイルをインポートします。 *filepath* には、次の EXEC モード コマンドおよびオプションのいずれか 1 つを入力します。 **シングル モード** • **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 • **ftp**：FTP のパスおよびファイル名 • **http**：HTTP のパスおよびファイル名 • **https**：HTTPS のパスおよびファイル名 • **smb**：SMB のパスおよびファイル名 • **tftp**：TFTP のパスおよびファイル名 **マルチ モード** • **http**：HTTP のパスおよびファイル名 • **https**：HTTPS のパスおよびファイル名 • **smb**：SMB のパスおよびファイル名 • **tftp**：TFTP のパスおよびファイル名 *value* には、PAC ファイルの暗号化に使用するパスワードを指定します。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。

例

次に、PAC ファイルを ASA にインポートする例を示します。

```
ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme
PAC file successfully imported
```

次に、端末を使用して PAC ファイルを ASA にインポートする例を示します。

```
ciscoasa(config)# cts import-pac terminal password A9875Za551
Enter the PAC file data in ASCII hex format
End with the word "quit" on a line by itself.
ciscoasa(exec_pac_hex)# 0100290405000001000000000000000
ciscoasa(exec_pac_hex)# 00000000000000001111111111111111
ciscoasa(exec_pac_hex)# 11111111111111112222222222222222
ciscoasa(exec_pac_hex)# 222222222222222776d7d64b6be4804b
ciscoasa(exec_pac_hex)# 0b4fdca3aeee11950ecd0e47c34157e5
ciscoasa(exec_pac_hex)# 25f4964ed75835cde0adb7e198e0bcdb
ciscoasa(exec_pac_hex)# 6aa8e363b0e4f9b4ac241be9ab576d0b
ciscoasa(exec_pac_hex)# a1fcd34e5dd05dbe1312cbfea072fdb9
ciscoasa(exec_pac_hex)# ee356fb61fe987d2d8f0ac3ef0467627
ciscoasa(exec_pac_hex)# 7f8b137da2b840e16da520468b039bae
ciscoasa(exec_pac_hex)# 36a4d844acc85cdefd7cb2cc58787590
ciscoasa(exec_pac_hex)# ef123882a69b6c37bdbc9320e403024f
ciscoasa(exec_pac_hex)# 354d42f404ec2d67ef3606575014584b
ciscoasa(exec_pac_hex)# 2796e65ccd6e6c8d14d92448a8b24f6e
ciscoasa(exec_pac_hex)# 47015a21f4f66cf6129d352bdfd4520f
ciscoasa(exec_pac_hex)# 3f0c6f340a80715df4498956efe15dec
ciscoasa(exec_pac_hex)# c08bb9a58cb6cb83ac91a3c40ce61de0
ciscoasa(exec_pac_hex)# 284b743e52fd68e848685e2d78c33633
ciscoasa(exec_pac_hex)# f2b4c5824138fc7bac9d9b83ac58ff9f
ciscoasa(exec_pac_hex)# 1dbc84c416322f1f3c5951cf2132994a
ciscoasa(exec_pac_hex)# a7cf20409df1d0d6621eba2b3af83252
ciscoasa(exec_pac_hex)# 70d0130650122bdb13a83b2dae55533a
ciscoasa(exec_pac_hex)# 4a394f21b441e164
ciscoasa(exec_pac_hex)# quit
PAC Imported Successfully
ciscoasa(config)#
```

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。

SXP を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	ciscoasa(config)# **cts sxp enable**	必要に応じて、ASA で 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 2	ciscoasa(config)# **cts sxp default source-ip** *ipaddress* **例：** ciscoasa(config)# cts sxp default source-ip 192.168.1.100	SXP 接続のデフォルトの送信元 IP アドレスを設定します。 *ipaddress* は、IPv4 または IPv6 アドレスです。 SXP 接続のデフォルトの送信元 IP アドレスを設定する場合は、ASA 発信インターフェイスと同じアドレスを指定する必要があります。送信元 IP アドレスが発信インターフェイスのアドレスと一致しない場合、SXP 接続は失敗します。 SXP 接続の送信元 IP アドレスが設定されていない場合、ASA は、route/ARP 検索を実行して、SXP 接続用の発信インターフェイスを判別します。詳細については、「SXP 接続のピアの追加」（P.32-22）を参照してください。
ステップ 3	ciscoasa(config)# **cts sxp default password** [**0** | **8**] *password* **例：** ciscoasa(config)# cts sxp default password 8 IDFW-TrustSec-99	SXP ピアでの TCP MD5 認証のデフォルト パスワードを設定します。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 *password* には、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 ストリングを指定します。

	コマンド	目的
ステップ 4	ciscoasa(config)# **cts sxp retry period** *timervalue* **例：** ciscoasa(config)# cts sxp retry period 60	ASA が SXP ピア間での新しい SXP 接続の設定を試行するデフォルトの時間間隔を指定します。ASA は、成功した接続が確立されるまで接続を試み続けます。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。 *timervalue* の範囲は 0 ～ 64000 秒です。デフォルトでは、*timervalue* は 120 秒です。 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。 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。 再試行タイマーは、SXP ピア デバイスとは異なる値に設定することを推奨します。
ステップ 5	ciscoasa(config)# **cts sxp reconciliation period** *timervalue* **例：** ciscoasa(config)# cts sxp reconciliation period 60	デフォルトの調整タイマーの値を指定します。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。 *timervalue* の範囲は 1 ～ 64000 秒です。デフォルトでは、*timervalue* は 120 秒です。 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。

例

次に、SXP のデフォルト値を設定する例を示します。

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

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。

	コマンド	目的
ステップ 1	`ciscoasa(config)# cts sxp enable`	必要に応じて、ASA で 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。

ステップ 2	`ciscoasa(config)# cts sxp connection peer peer_ip_address [source source_ip_address] password {default | none} [mode {local | peer}] {speaker | listener}`
	
	例：
	`ciscoasaciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker`
		SXP ピアへの SXP 接続を設定します。SXP 接続は IP アドレスごとに設定されます。単一デバイスのペアは複数の SXP 接続に対応できます。
		
		peer_ip_address は、SXP ピアの IPv4 または IPv6 アドレスです。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。
		
		source_ip_address は、SXP 接続のローカル IPv4 または IPv6 アドレスです。送信元 IP アドレスは ASA 発信インターフェイスと同じである必要があります。そうでなければ、接続が失敗します。
		
		SXP 接続の送信元 IP アドレスを設定せずに、ASA が route/ARP 検索を実行して SXP 接続の送信元 IP アドレスを決定できるようにすることを推奨します。
		
		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.32-19）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。
		
		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。
		
		SXP 接続で、ASA が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。「ASA での送信者および受信者のロール」（P.32-7）を参照してください。
		• **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。

例

次に、ASA で SXP ピアを設定する例を示します。

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker
ciscoasa(config)# cts sxp connection peer 192.168.1.101 password default mode peer
ciscoasa(config)# no cts sxp connection peer 192.168.1.100
ciscoasa(config)# cts sxp connection peer 192.168.1.100 source 192.168.1.1 password default mode peer speaker
ciscoasa(config)# no cts sxp connection peer 192.168.1.100 source 192.168.1.1 password default mode peer
speaker
```

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 のポリシー設定の変更および 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、次のコマンドを入力します。

コマンド	目的
cts refresh environment-data **例：** ciscoasaciscoasa(config)# cts refresh environment-data	ISE からの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。

- 拡張 ACL 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.16-9）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。

例

次に、ローカルで定義されたセキュリティ オブジェクト グループを使用する ACL を作成する例を示します。

```
object-group security objgrp-it-admin
   security-group name it-admin-sg-name
   security-group tag 1
object-group security objgrp-hr-admin
   security-group name hr-admin-sg-name  // single sg_name
   group-object it-admin     // locally defined object-group as nested object
object-group security objgrp-hr-servers
    security-group name hr-servers-sg-name
object-group security objgrp-hr-network
    security-group tag 2
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
```

前の例で設定した ACL をアクティブにするには、アクセス グループまたはモジュラ ポリシー フレームワークを設定します。

その他の例：

```
!match src hr-admin-sg-name from any network to dst host 172.23.59.53
    access-list idw-acl permit ip security-group name hr-admin-sg-name any host 172.23.59.53
!match src hr-admin-sg-name from host 10.1.1.1 to dst any
    access-list idfw-acl permit ip security-group name hr-admin-sg-name host 10.1.1.1 any
!match src tag 22 from any network to dst hr-servers-sg-name any network
    access-list idfw-acl permit ip security-group tag 22 any security-group name hr-servers-sg-name any
!match src user mary from any host to dst hr-servers-sg-name any network
    access-list idfw-acl permit ip user CSCO\mary any security-group name hr-servers-sg-name any
!match src objgrp-hr-admin from any network to dst objgrp-hr-servers any network
    access-list idfw-acl permit ip object-group-security objgrp-hr-admin any object-group-security
    objgrp-hr-servers any
!match src user Jack from objgrp-hr-network and ip subnet 10.1.1.0/24 to dst objgrp-hr-servers any network
    access-list idfw-acl permit ip user CSCO\Jack object-group-security objgrp-hr-network 10.1.1.0
    255.255.255.0 object-group-security objgrp-hr-servers any
!match src user Tom from security-group mktg any google.com
object network net-google
    fqdn google.com
    access-list sgacl permit ip sec name mktg any object net-google
!If user Tom or object_group security objgrp-hr-admin needs to be matched, multiple ACEs can be defined as
follows:
    access-list idfw-acl2 permit ip user CSCO\Tom 10.1.1.0 255.255.255.0 object-group-security
    objgrp-hr-servers any
    access-list idfw-acl2 permit ip object-group-security objgrp-hr-admin 10.1.1.0 255.255.255.0
    object-group-security objgrp-hr-servers any
```

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。

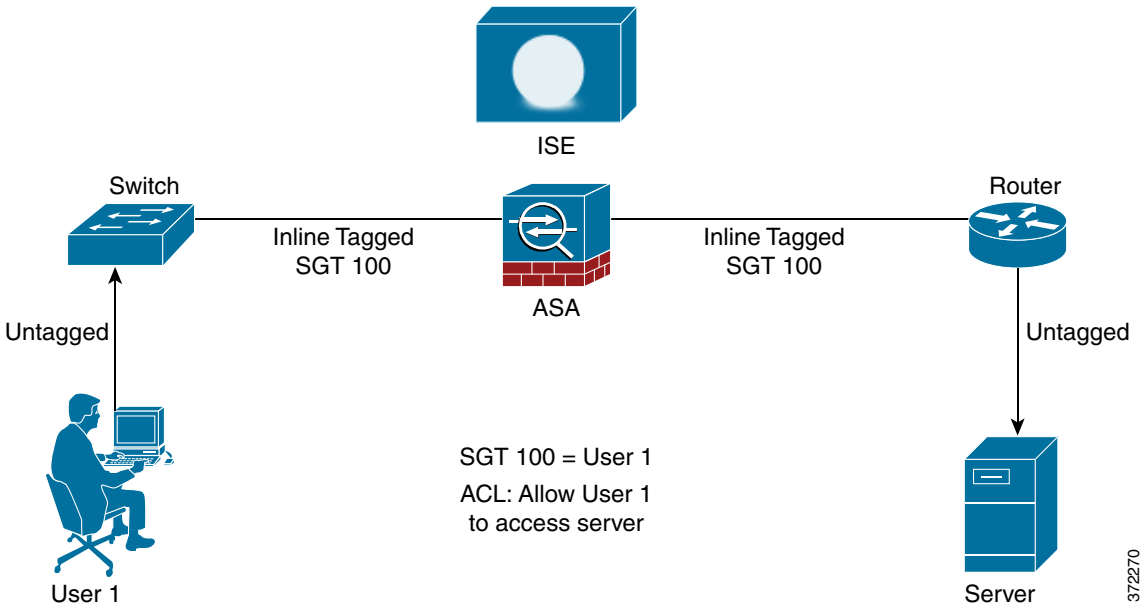
SGT とイーサネット タギング（レイヤ 2 SGT インポジションとも呼ばれる）を利用すると、ASA でシスコ独自のイーサネット フレーミング（EtherType 0x8909）を使用して、イーサネット インターフェイスでセキュリティ グループ タグを送受信できます。これにより、送信元のセキュリティ グループ タグをプレーン テキストのイーサネット フレームに挿入できます。ASA は、インターフェイスごとの手動設定に基づいて、発信パケットにセキュリティ グループ タグを挿入し、着信パケットのセキュリティ グループ タグを処理します。この機能を使用することで、ネットワーク デバイス間におけるエンドポイント 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 32-3 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 32-3　レイヤ 2 SGT インポジション



使用シナリオ

表 32-3 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 32-3　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。
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 32-4 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 32-4　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 32-5 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 32-5　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、次のコマンドを入力します。

コマンド	目的

`ciscoasa(config-if)# cts manual`
 	
例：
`ciscoasaciscoasa(config-if)# cts manual`
`ciscoasa(config-if-cts-manual)#`
	レイヤ 2 SGT インポジションをイネーブルにして、CTS 手動インターフェイス コンフィギュレーション モードを開始します。レイヤ 2 SGT インポジションをディセーブルにするには、**no cts manual** コマンドを入力します。

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。

	コマンド	目的
ステップ 1	ciscoasa(config-if)# **cts manual** **例：** ciscoasa(config-if)# cts manual ciscoasa(config-if-cts-manual)#	レイヤ 2 SGT インポジションをイネーブルにして、CTS 手動インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	ciscoasa(config-if-cts-manual)# **propagate sgt** **例：** ciscoasa(config-if-cts-manual)# propagate sgt	インターフェイスでのセキュリティ グループ タグ（**sgt** と呼ばれる）の伝搬をイネーブルにします。伝搬はデフォルトでイネーブルになっています。インターフェイスでのセキュリティ グループ タグ（**sgt** と呼ばれる）の伝搬をディセーブルにするには、**no propagate sgt** コマンドを使用します。

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。

	コマンド	目的
ステップ 1	ciscoasa(config-if)# **cts manual** **例：** ciscoasa(config-if)# cts manual ciscoasa(config-if-cts-manual)#	レイヤ 2 SGT インポジションをイネーブルにして、CTS 手動インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	ciscoasa(config-if-cts-manual)# **policy static sgt** *sgt_number* [**trusted**] **例：** ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted	手動で設定した CTS リンクにポリシーを適用します。 **static** で、リンクの着信トラフィックに適用する SGT ポリシーを指定します。 **sgt** *sgt_number* には、ピアからの着信トラフィックに適用する SGT 値を指定します。有効な値の範囲は 2 ～ 65519 です。 **trusted** は、コマンドで SGT が指定されたインターフェイスの入力トラフィックでは、SGT を上書きしてはいけないことを示します。デフォルトは untrusted です。

例

次に、レイヤ 2 SGT インポジション用のインターフェイスをイネーブルにし、インターフェイスが信頼できるかどうかを定義する例を示します。

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)# propagate sgt
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

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、次のコマンドを入力します。

コマンド	目的
ciscoasa(config)# **cts role-based sgt-map** [*IPv4_addr* | *IPv6_addr*] **sgt** *sgt_value* **例：** ciscoasa(config)# cts role-based sgt-map 10.2.1.2 sgt 50	IP-SGT バインディングは手動で設定できます。 **sgt** *sgt_value* には SGT 値を指定します。有効な値の範囲は 2 ～ 65519 です。

トラブルシューティングのヒント

特定のセッションが許可または拒否された理由、使用されている SGT 値（パケットの SGT 値、IP-SGT マネージャから取得した SGT 値、またはインターフェイスで設定した **policy static sgt** コマンドで取得した SGT 値）、および適用されたセキュリティ グループベースのセキュリティ ポリシーを確認するには、**packet-tracer** コマンドを使用します。

次に、**packet-tracer** コマンドの出力例を示します。この出力から、セキュリティ グループ タグと IP アドレスの対応付けがわかります。

```
ciscoasa# packet-tracer input inside tcp inline-tag 100 security-group name alpha 30
security-group tag 31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside....
----------------More---------------------
```

特定の SGT 値を指定するかどうかにかかわらず、Cisco CMD パケット（EtherType 0x8909）のみをキャプチャするには、**capture** *capture-name* **type inline-tag** *tag* コマンドを使用します。

次に、SGT 値を指定した場合の **show capture** コマンドの出力例を示します。

```
ciscoasa# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
```

設定例

次に、Cisco TrustSec を使用するように ASA を設定する方法の例を示します。

```
// Import an encrypted CTS PAC file
    cts import-pac asa.pac password Cisco
// Configure ISE for environment data download
    aaa-server cts-server-list protocol radius
    aaa-server cts-server-list host 10.1.1.100 cisco123
    cts server-group cts-server-list
// Configure SXP peers
    cts sxp enable
    cts sxp connection peer 192.168.1.100 password default mode peer speaker
//Configure security-group based policies
    object-group security objgrp-it-admin
          security-group name it-admin-sg-name
          security-group tag 1
    object-group security objgrp-hr-admin
        security-group name hr-admin-sg-name
        group-object it-admin
    object-group security objgrp-hr-servers
        security-group name hr-servers-sg-name
    access-list hr-acl permit ip object-group-security objgrp-hr-admin any
    object-group-security objgrp-hr-servers
//Configure security group tagging plus Ethernet tagging
   interface gi0/1
   cts manual
   propagate sgt
   policy static sgt 100 trusted10.1.1.100 sgt 50
```

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

ローカル ユーザ データベースおよびグループ ポリシーの SGT 属性を設定するには、次のコマンドを入力します。

コマンド	目的
ciscoasa(config-group-policy# **[no] security-group-tag value** *sgt* **例：** ciscoasa(config-group-policy# **security-group-tag value 101**	名前付きグループ ポリシーまたはローカル ユーザ名の属性セットで SGT 属性を設定します。 このコマンドのデフォルトの形式は、**security-group-tag none** です。つまり、この属性セットにはセキュリティ グループ タグが含まれていません。 **[no] security-group-tag value** *sgt* コマンドを実行すると、設定がデフォルトに戻ります。

Cisco TrustSec のモニタリング

ASA で Cisco TrustSec をモニタリングするには、次のコマンドの 1 つまたは複数を入力します。

コマンド	目的
show running-config cts	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。
show running-config [all] cts role-based [sgt-map]	ユーザが定義した IP-SGT バインディング テーブル エントリを表示します。
show cts sxp connections	マルチ コンテキスト モードが使用されている場合の、特定のユーザ コンテキストに対する ASA の SXP 接続を表示します。
show conn security-group	すべての SXP 接続のデータを表示します。
show cts 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。
show cts sgt-map	制御パスの IP アドレス セキュリティ グループ テーブル マネージャ エントリを表示します。
show asp table cts sgt-map	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。
show cts 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 32-6 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。

表 32-6　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。 **access-list extended**、**cts sxp enable**、**cts server-group**、**cts sxp default**、**cts sxp retry period**、**cts sxp reconciliation period**、**cts sxp connection peer**、**cts import-pac**、**cts refresh environment-data**、**object-group security**、**security-group**、**show running-config cts**、**show running-config object-group**、**clear configure cts**、**clear configure object-group**、**show cts pac**、**show cts environment-data**、**show cts environment-data sg-table**、**show cts sxp connections**、**show object-group**、**show configure security-group**、**clear cts environment-data**、**debug cts**、および **packet-tracer** の各コマンドが導入または変更されました。
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。 **cts manual**、**policy static sgt**、**propagate sgt**、**cts role-based sgt-map**、**show cts sgt-map**、**packet-tracer**、**capture**、**show capture**、**show asp drop**、**show asp table classify**、**show running-config all**、**clear configure all**、および **write memory** の各コマンドが導入または変更されました。

ASA および Cisco Mobile Enablement

- ASA および Cisco Mobile Enablement について
- ASA MDM プロキシのガイドラインと制限事項
- MDM プロキシとしての ASA の設定
- Mobile Enablement プロキシのアクティビティのモニタリング
- ASA Mobile Enablement プロキシの機能履歴

ASA および Cisco Mobile Enablement について

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、オンプレミス 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には、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　MDM プロキシ機能を設定し、イネーブルにするには、コンフィギュレーション モードから config-mdm-proxy モードにします。

```
asa(config)# mdm-proxy
```

ステップ 2　AnyConnect Device Management の登録とチェックイン用のポートを設定します。

デフォルトの登録ポートは 443 です。MDM チェックイン要求に使用するポートを指定する必要があります。ポートは 1 ～ 65535 の範囲でなければなりません。

```
asa (config-mdm-proxy)# port enrollment 443 checkin 8906
```

ステップ 3　MDM プロキシ セッションの事前に定義された認証およびアカウンティング サーバ グループを設定します。

```
asa (config-mdm-proxy)# accounting-server-group ISE-AAA
asa (config-mdm-proxy)# authentication-server-group ISE-AAA
```

ステップ 4　すべての AnyConnect Device Management セッションのために ISE MDM サーバへの MDM プロキシ アクセスの事前定義されたトラストポイントを設定します。

```
asa (config-mdm-proxy)# trustpoint ASAtoISEMDM
```

ステップ 5　（オプション）警告を表示するには、パスワードの期限切れまでの日数を指定します。

```
asa (config-mdm-proxy)# password-management 5
```

ステップ 6　（オプション）MDM プロキシ セッションの制限を指定します。

a.　並列 MDM セッション数を設定します（1 ～ 10000、デフォルトは 1000）。

```
asa (config-mdm-proxy)# session-limit 5000
```

b.　登録およびチェックインの最大セッション期間を設定します（デフォルトは 300）。

```
asa (config-mdm-proxy)# session-timeout enrollment 600 checkin 600
```

ステップ 7　外部インターフェイスの MDM プロキシ設定を有効にします。

```
asa (config-mdm-proxy)# enable outside
```

Mobile Enablement プロキシのアクティビティのモニタリング

ASA の Mobile Enhancement の統計情報を表示するには、次のコマンドを入力します。

show mdm-proxy statistics

現在の Mobile Enablement の設定を表示するには、次のコマンドを入力します。

show running-config phone-proxy

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
Mobile Enablement プロキシ	9.3(1)	Mobile Enablement プロキシ（ISE Mobile Enablement ソリューションのコンポーネント）を使用すると、構外モバイル デバイスがオンプレミス 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。 config-mdm-proxy モードにするための **mdm-proxy** コマンドが導入されました。この新しいモードでは、コマンド **authentication-server-group**、**accounting-server-group**、**password-management**、**trusttpoint**、**port**、**session-limit**、**session-timeout**、**enable** が適用されます。

CHAPTER 34

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」（P.34-1）
- 「ローカル証明書の前提条件」（P.34-8）
- 「デジタル証明書のガイドライン」（P.34-9）
- 「デジタル証明書の設定」（P.34-10）
- 「デジタル証明書のモニタリング」（P.34-43）
- 「証明書管理の機能履歴」（P.34-45）

デジタル証明書の概要

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 公開キー暗号化 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、相互に補完し合い、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す。

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して失効ステータスをチェックする、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。

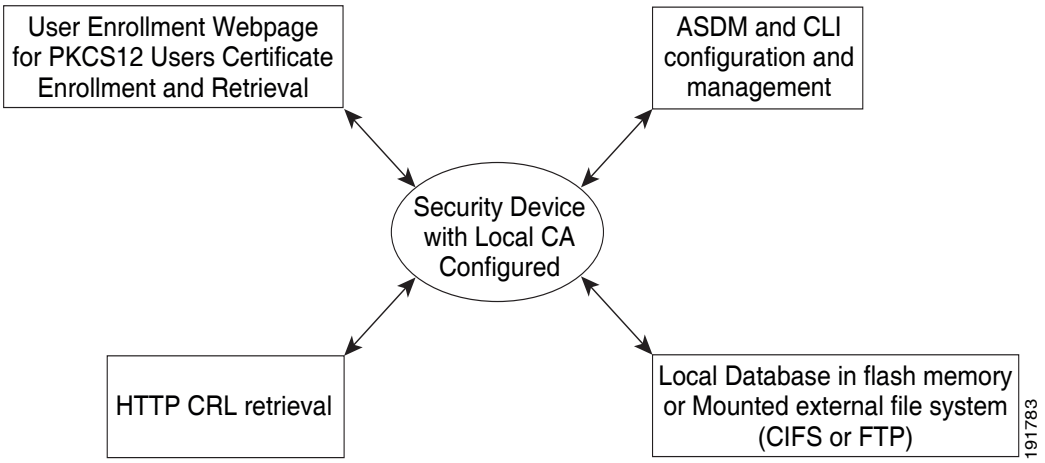
ローカル CA ユーザ データベースに保存できるユーザの数に制限はありませんが、フラッシュ メモリ ストレージに問題がある場合、管理者に対策を取るように警告する syslog が作成され、ローカル CA はストレージの問題が解決されるまでディセーブルになることがあります。フラッシュ メモリは、3500 人以下のユーザを持つデータベースを保存できますが、ユーザの数がそれを超えるデータベースでは外部ストレージが必要になります。

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 34-1 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 34-1　　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、認証と許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 許可では、パスワードをクレデンシャルとして使用しません。RADIUS 許可では、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

認証および許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。
- 許可
  - トンネル グループ（ASDM 接続プロファイルとも呼ばれます）の許可サーバ 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。

認証と許可の両方がイネーブルになっている場合、ASA によって、ユーザの認証と許可の両方にユーザ 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。
- 許可
  - 許可サーバ 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許可がイネーブルになっている場合、ASA によって許可にプライマリ 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。
- 許可
  - 許可サーバ 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 のフィールド値が許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、許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、証明書の有効期間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。

- 「キー ペアの設定」（P.34-11）
- 「キー ペアの削除」（P.34-11）
- 「トラストポイントの設定」（P.34-12）
- 「トラストポイントの CRL の設定」（P.34-15）
- 「トラストポイント コンフィギュレーションのエクスポート」（P.34-17）
- 「トラストポイント コンフィギュレーションのインポート」（P.34-17）
- 「CA 証明書マップ規則の設定」（P.34-18）
- 「手動での証明書の取得」（P.34-19）
- 「SCEP を使用した証明書の自動取得」（P.34-21）
- 「SCEP 要求のプロキシ サポートの設定」（P.34-22）
- 「ローカル CA サーバのイネーブル化」（P.34-23）
- 「ローカル CA サーバの設定」（P.34-25）
- 「ローカル CA サーバのカスタマイズ」（P.34-26）

- 「ローカル CA サーバのデバッグ」（P.34-27）
- 「ローカル CA サーバのディセーブル化」（P.34-28）
- 「ローカル CA サーバの削除」（P.34-28）
- 「ローカル CA 証明書の特性の設定」（P.34-28）

キー ペアの設定

キー ペアを生成するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**crypto key generate rsa** **例：** ciscoasa/contexta(config)# crypto key generate rsa	1 つの汎用 RSA キー ペアを生成します。デフォルトのキー係数は 1024 です。その他の係数サイズを指定するには、**modulus** キーワードを使用します。 **（注）** 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。
ステップ 2	**crypto key generate rsa label** *key-pair-label* **例：** ciscoasa/contexta(config)# crypto key generate rsa label exchange	（オプション）ラベルを各キー ペアに割り当てます。このラベルは、キー ペアを使用するトラストポイントによって参照されます。ラベルを割り当てなかった場合、キー ペアには *Default-RSA-Key* というラベルが自動的に付けられます。
ステップ 3	**show crypto key** *name of key* **例：** ciscoasa/contexta(config)# show crypto key examplekey	生成したキー ペアを検証します。
ステップ 4	**write memory** **例：** ciscoasa(config)# write memory	生成したキー ペアを保存します。

キー ペアの削除

キー ペアを削除するには、次の手順を実行します。

コマンド	目的
crypto key zeroize rsa **例：** ciscoasa(config)# crypto key zeroize rsa	キー ペアを削除します。

例

次に、キー ペアを削除する例を示します。

```
ciscoasa(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All device certs issued using these keys will also be removed.

Do you really want to remove these keys?[yes/no] y
```

トラストポイントの設定

トラストポイントを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**crypto ca trustpoint** *trustpoint-name* **例：** ciscoasa/contexta(config)# crypto ca trustpoint Main	ASA が証明書を受け取る必要のある CA に対応するトラストポイントを作成します。crypto ca トラストポイント コンフィギュレーション モードに入り、ステップ 3 から設定できる CA 固有のトラストポイント パラメータを制御します。 **（注）** 接続しようとすると、トラストポイントからの ID 証明書の取得の試行時にそのトラストポイントに ID 証明書が含まれていないことを示す警告が表示されます。
ステップ 2	次のいずれかのオプションを選択します。	
	enrollment url *url* **例：** ciscoasa/contexta(config-ca-trustpoint)# enrollment url http://10.29.67.142:80/certsrv/mscep/mscep.dll	SCEP と指定のトラストポイントを使用して自動登録を要求し、登録用 URL を設定します。
	enrollment terminal **例：** ciscoasa/contexta(config-ca-trustpoint)# enrollment terminal	CA から取得した証明書を端末に貼り付けることによって、指定したトラストポイントで手動登録を要求します。
ステップ 3	**revocation-check crl none** revocation-check crl revocation-check none **例：** ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl none ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl ciscoasa/contexta(config-ca-trustpoint)# revocation-check none	使用可能な CRL コンフィギュレーション オプションを指定します。 **（注）** 必須または任意の CRL チェックをイネーブルにするには、証明書を取得してから、CRL 管理用のトラストポイントを設定します。

	コマンド	目的
ステップ 4	**crl configure** **例：** ciscoasa/contexta(config-ca-trustpoint)# crl configure	CRL コンフィギュレーション モードを開始します。
ステップ 5	**email** *address* **例：** ciscoasa/contexta(config-ca-trustpoint)# email example.com	登録時に、指定された電子メール アドレスを、証明書の Subject Alternative Name 拡張子に含めるように CA に要求します。
ステップ 6	**enrollment retry period** **例：** ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 5	（オプション）再試行時間を分単位で指定し、SCEP 登録だけに適用します。
ステップ 7	**enrollment retry count** **例：** ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 2	（オプション）許可される再試行の最大数を指定し、SCEP 登録だけに適用します。
ステップ 8	**fqdn** *fqdn* **例：** ciscoasa/contexta(config-ca-trustpoint)# fqdn example.com	登録時に、指定された完全修飾ドメイン名を証明書の Subject Alternative Name 拡張子に含めるように CA に要求します。
ステップ 9	**ip-address** *ip-address* **例：** ciscoasa/contexta(config-ca-trustpoint)# ip-address 10.10.100.1	登録時に、ASA の IP アドレスを証明書に含めるように CA に要求します。
ステップ 10	**keypair** *name* **例：** ciscoasa/contexta(config-ca-trustpoint)# keypair exchange	公開キーが認証の対象となるキー ペアを指定します。
ステップ 11	**match certificate map-name override ocsp** **例：** ciscoasa/contexta(config-ca-trustpoint)# match certificate examplemap override ocsp	OCSP の URL の上書きと、OCSP の応答側の証明書の検証に使用するトラストポイントを設定します。
ステップ 12	**ocsp disable-nonce** **例：** ciscoasa/contexta(config-ca-trustpoint)# ocsp disable-nonce	OCSP 要求の nonce 拡張をディセーブルにします。nonce 拡張は、リプレイ攻撃を防ぐために、要求と応答を暗号化してバインドします。

	コマンド	目的
ステップ 13	**ocsp url** **例：** ciscoasa/contexta(config-ca-trustpoint)# ocsp url	ASA で、トラストポイントに関連するすべての証明書をチェックするときに使用する OCSP サーバを設定します。クライアント証明書の AIA 拡張で指定されているサーバは使用しません。
ステップ 14	**password** *string* **例：** ciscoasa/contexta(config-ca-trustpoint)# password mypassword	登録時に CA に登録されるチャレンジ フレーズを指定します。CA は、通常、このフレーズを使用して、その後の失効要求を認証します。
ステップ 15	**revocation check** **例：** ciscoasa/contexta(config-ca-trustpoint)# revocation check	失効チェックの方法（CRL、OCSP、および none）を 1 つまたは複数設定します。
ステップ 16	**subject-name** *X.500 name* **例：** ciscoasa/contexta(config-ca-trustpoint)# myname X.500 examplename	登録時に、指定されたサブジェクト DN を証明書に含めるように CA に要求します。DN 文字列にカンマが含まれている場合、この値文字列を二重引用符で囲みます（例：O="Company, Inc."）。
ステップ 17	**serial-number** **例：** ciscoasa/contexta(config-ca-trustpoint)# serial number JMX1213L2A7	登録時に、ASA のシリアル番号を証明書に含めるように CA に要求します。
ステップ 18	**write memory** **例：** ciscoasa/contexta(config)# write memory	実行コンフィギュレーションを保存します。

トラストポイントの CRL の設定

証明書の認証時に必須またはオプションの CRL チェックを行うには、トラストポイントごとに CRL を設定する必要があります。トラストポイントの CRL を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**crypto ca trustpoint** *trustpoint-name* **例：** `ciscoasa (config)# crypto ca trustpoint Main`	CRL コンフィギュレーションを変更するトラストポイントに対して、crypto ca trustpoint コンフィギュレーション モードに入ります。 **（注）** このコマンドを入力する前に、CRL がイネーブルであることを確認してください。また、認証が成功するためには、CRL が使用可能である必要があります。
ステップ 2	**crl configure** **例：** `ciscoasa (config-ca-trustpoint)# crl configure`	現在のトラストポイントで、crl コンフィギュレーション モードを開始します。 **ヒント** すべての CRL コンフィギュレーションのパラメータをデフォルト値に設定するには、**default** コマンドを使用します。CRL の設定中は、いつでもこのコマンドを入力して手順をやり直すことができます。
ステップ 3	次のいずれかを実行します。	
	policy cdp **例：** `ciscoasa (config-ca-crl)# policy cdp`	取得ポリシーを設定します。CRL は、認証済みの証明書で指定されている CRL 分散ポイントだけから取得できます。 **（注）** SCEP の取得は、証明書で指定されている分散ポイントではサポートされていません。 続行するには、ステップ 5 に進みます。
	policy static **例：** `ciscoasa (config-ca-crl)# policy static`	取得ポリシーを設定します。CRL は、設定した URL だけから取得できます。 続行するには、ステップ 4 に進みます。
	policy both **例：** `ciscoasa (config-ca-crl)# policy both`	取得ポリシーを設定します。CRL は、認証済みの証明書で指定されている CRL 分散ポイントと、設定した URL の両方から取得できます。 続行するには、ステップ 4 に進みます。
ステップ 4	**url** *n url* **例：** `ciscoasa (config-ca-crl)# url 2 http://www.example.com`	CRL ポリシーの設定時に **static** または **both** キーワードを使用する場合、CRL 取得用の URL を設定する必要があります。1 ～ 5 のランクを付けて、最大 5 つの URL を入力できます。*n* は、URL に割り当てるランクです。URL を削除するには、**no url** *n* コマンドを使用します。

	コマンド	目的
ステップ 5	**protocol http** | **ldap** | **scep** **例：** ciscoasa (config-ca-crl)# protocol http	取得方法を設定します。CRL 取得方式として HTTP、LDAP、または SCEP を指定します。
ステップ 6	**cache-time** *refresh-time* **例：** ciscoasa (config-ca-crl)# cache-time 420	ASA が現在のトラストポイントの CRL をキャッシュしている時間を設定します。*refresh-time* は、CRL を失効と判断するまで ASA が待機する時間（分）です。
ステップ 7	次のどちらかを実行します。	
	enforcenextupdate **例：** ciscoasa (config-ca-crl)# enforcenextupdate	CRL の NextUpdate フィールドを要求します。これがデフォルト設定です。
	no enforcenextupdate **例：** ciscoasa (config-ca-crl)# no enforcenextupdate	CRL に NextUpdate フィールドが存在しないことを許可します。
ステップ 8	**ldap-defaults** *server* **例：** ciscoasa (config-ca-crl)# ldap-defaults ldap1	LDAP が取得プロトコルとして指定されている場合に ASA に LDAP サーバを指定します。LDAP サーバは、DNS ホスト名または IP アドレスで指定できます。LDAP サーバがデフォルトの 389 以外のポートで LDAP クエリーを受信する場合は、ポート番号も指定できます。 **（注）** LDAP サーバを指定するために、IP アドレスの代わりにホスト名を使用する場合は、ASA が DNS を使用するように設定されていることを確認します。
ステップ 9	**ldap-dn** *admin-DN password* **例：** ciscoasa (config-ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering c00lRunZ	LDAP サーバでクレデンシャルを必要としている場合に、CRL の取得を許可します。
ステップ 10	**crypto ca crl request** *trustpoint* **例：** ciscoasa (config-ca-crl)# crypto ca crl request Main	指定したトラストポイントによって示される CA から現在の CRL を取得し、現在のトラストポイントの CRL コンフィギュレーションをテストします。
ステップ 11	**write memory** **例：** ciscoasa (config)# write memory	実行コンフィギュレーションを保存します。

トラストポイント コンフィギュレーションのエクスポート

トラスト ポイント設定をエクスポートするには、次のコマンドを入力します。

コマンド	目的
crypto ca export *trustpoint* **例：** ciscoasa(config)# crypto ca export Main	トラスト ポイント設定を関連するすべてのキーと PKCS12 形式の証明書とともにエクスポートします。ASA は PKCS12 データを端末に表示します。この表示されたデータはコピーできます。トラストポイント データはパスワードで保護されますが、このデータをファイルに保存する場合は、そのファイルがセキュアな場所にあることを確認してください。

例

次の例では、トラストポイント Main の PKCS12 データをパスフレーズ Wh0zits とともにエクスポートしています。

```
ciscoasa (config)# crypto ca export Main pkcs12 Wh0zits

Exported pkcs12 follows:

[ PKCS12 data omitted ]

---End - This line not part of the pkcs12---
```

トラストポイント コンフィギュレーションのインポート

トラスト ポイント設定をインポートするには、次のコマンドを入力します。

コマンド	目的
crypto ca import *trustpoint* **pkcs12** **例：** ciscoasa(config)# crypto ca import Main pkcs12	キー ペアと、トラスト ポイント設定に関連付けられている発行済み証明書をインポートします。ASA では、Base-64 形式で端末にテキストを貼り付けるように要求されます。トラストポイントとともにインポートされるキー ペアには、作成するトラストポイントの名前と一致するラベルが割り当てられます。 **（注）** 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で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** キーワードを使用します。

例

次の例では、パスフレーズ Wh0zits とともに PKCS12 データを手動でトラストポイント Main にインポートしています。

```
ciscoasa (config)# crypto ca import Main pkcs12 Wh0zits

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
```

次に、トラストポイント Main の証明書を手動でインポートする例を示します。

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

CA 証明書マップ規則の設定

証明書の [Issuer] フィールドと [Subject] フィールドに基づいて、ルールを設定できます。作成した規則を使用すると、**tunnel-group-map** コマンドによって、IPSec ピアの証明書をトンネルグループにマッピングできます。ASA は CA 証明書マップを 1 つサポートしています。これには、複数の規則を設定できます。

CA 証明書マップ規則を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**crypto ca certificate map** *sequence-number* **例：** `ciscoasa(config)# crypto ca certificate map 1`	設定するルールの CA 証明書マップ コンフィギュレーション モードを開始し、ルール インデックス番号を指定します。
ステップ 2	**issuer-name** *DN-string* **例：** `ciscoasa(config-ca-cert-map)# issuer-name cn=asa.example.com`	すべての発行済み証明書の識別名を指定します。これは自己署名 CA 証明書のサブジェクト名 DN でもあります。属性と値のペアを区切るには、カンマを使用します。カンマを含む値は、引用符で囲んでください。発行者名は、英数字で 500 文字未満にする必要があります。デフォルトの発行者名は cn=*hostame.domain-name* です。

	コマンド	目的
ステップ 3	**subject-name attr** *tag* **eq** | **co** | **ne** | **nc** *string* **例：** `ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert`	ASA が証明書の [Subject] フィールドの値に適用できるテストを指定します。テストは、特定の属性または全体のフィールドに適用できます。ルールごとに複数のテストを設定できますが、これらのコマンドで指定するすべてのテストは、証明書と一致するルールで真である必要があります。有効な演算子は次のとおりです。 • eq：フィールドまたは属性が所定の値と一致する。 • ne：フィールドまたは属性が所定の値と一致しない。 • co：フィールドまたは属性の一部または全部が所定の値と一致する。 • nc：フィールドまたは属性の全部が所定の値と一致しない。
ステップ 4	**write memory** **例：** `ciscoasa (config)# write memory`	実行コンフィギュレーションを保存します。

手動での証明書の取得

証明書を手動で取得するには、次の手順を実行します。

	コマンド	目的

ステップ 1	**crypto ca authenticate** *trustpoint*
	
	例：
	`ciscoasa(config)# crypto ca authenticate Main`
	`Enter the base 64 encoded CA certificate.`
	`End with a blank line or the word "quit" on a line by itself`
	`MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG 9w0BAQUFADCB`
	`[ certificate data omitted ]`
	`/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==`
	`quit`
	
	`INFO: Certificate has the following attributes:`
	`Fingerprint:  24b81433 409b3fd5 e5431699 8d490d34`
	`Do you accept this certificate?[yes/no]: y`
	`Trustpoint CA certificate accepted.`
	
	`% Certificate successfully imported`
		設定したトラストポイントの CA 証明書をインポートします。
		（注） この手順は、トラストポイントで示されている CA から、base-64 encoded CA 証明書を取得済みであることを前提としています。
		
		トラストポイントが手動で証明書を取得する必要があるかどうかは、そのトラストポイントを設定するときに **enrollment terminal** コマンドを使用するかどうかによって決まります。詳細については、「トラストポイントの設定」（P.34-12）を参照してください。

	コマンド	目的
ステップ 2	**crypto ca enroll** *trustpoint* **例：** ciscoasa(config)# crypto ca enroll Main % Start certificate enrollment .. % The fully-qualified domain name in the certificate will be: securityappliance.example.com % Include the device serial number in the subject name?[yes/no]: **n** Display Certificate Request to terminal?[yes/no]: **y** Certificate Request follows: MIIBoDCCAQkCAQAwIzEhMB8GCSqGSIb3DQEJAhYSRmVyYWxQaXguY2lzY28uY29t *[certificate request data omitted]* jF4waw68eOxQxVmdgMWeQ+RbIOYmvt8g6hnBTrd0GdqjjVLt ---End - This line not part of the certificate request--- Redisplay enrollment request?[yes/no]: **n**	このトラストポイントを持つ ASA を登録します。署名データの証明書を生成し、設定したキーのタイプによっては暗号化データの証明書も生成します。 署名と暗号化に別々の RSA キーを使用する場合、**crypto ca enroll** コマンドは各キーに対する 2 つの証明書要求を表示します。署名と暗号化の両方に汎用の RSA キーを使用する場合、**crypto ca enroll** コマンドでは証明書要求が 1 つ表示されます。 登録を完了するには、該当するトラストポイントで示される CA から **crypto ca enroll** コマンドで生成されたすべての証明書要求に対する証明書を取得します。証明書が base-64 形式であることを確認してください。
ステップ 3	**crypto ca import** *trustpoint* **certificate** **例：** ciscoasa (config)# crypto ca import Main certificate % The fully-qualified domain name in the certificate will be: securityappliance.example.com Enter the base 64 encoded certificate. End with a blank line or the word “quit” on a line by itself *[certificate data omitted]* quit INFO: Certificate successfully imported	CA から受信する各証明書をインポートします。証明書を base-64 形式で端末に貼り付けることが求められます。
ステップ 4	**show crypto ca server certificate** **例：** ciscoasa(config)# show crypto ca server certificate Main	ASA に発行された証明書の詳細とトラストポイントの CA 証明書を表示して、登録プロセスが成功したことを確認します。
ステップ 5	**write memory** **例：** ciscoasa(config)# write memory	実行コンフィギュレーションを保存します。 手動登録を設定したトラストポイントごとに、これらの手順を繰り返します。

SCEP を使用した証明書の自動取得

SCEP を使用して証明書を自動的に取得するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**crypto ca authenticate** *trustpoint* **例：** ciscoasa/contexta(config)# crypto ca authenticate Main	設定したトラストポイントの CA 証明書を取得します。 **（注）** この手順は、トラストポイントで示されている CA から、base-64 encoded CA 証明書を取得済みであることを前提としています。 トラスト ポイントを設定するときに、**enrollment url** コマンドを使用すると、SCEP を使用して証明書を自動的に取得する必要があるかどうかを判断できます。詳細については、「トラストポイントの設定」（P.34-12）を参照してください。
ステップ 2	**crypto ca enroll** *trustpoint* **例：** ciscoasa/contexta(config)# crypto ca enroll Main	このトラストポイントを持つ ASA を登録します。署名データの証明書を取得し、設定したキーのタイプによっては暗号化データの証明書も取得します。CA の管理者は、CA が証明書を付与する前に手動で登録要求を認証しなければならない場合があるため、このコマンドを入力する前に CA の管理者に連絡してください。 ASA が証明書要求を送信してから 1 分（デフォルト）以内に CA から証明書を受け取らなかった場合は、証明書要求が再送信されます。ASA によって、証明書を受信するまで 1 分ごとに証明書要求が送信されます。 トラストポイントの完全修飾ドメイン名が ASA の完全修飾ドメイン名と一致しなかった場合（完全修飾ドメイン名が文字の場合も含む）、警告が表示されます。この問題を解決するには、登録プロセスを終了し、必要な修正を行ってから、**crypto ca enroll** コマンドを再入力します。 **（注）** **crypto ca enroll** コマンドを発行した後、証明書を受信する前に ASA がリブートされた場合は、**crypto ca enroll** コマンドを再入力して、CA 管理者に連絡してください。

	コマンド	目的
ステップ 3	**show crypto ca server certificate** **例：** `ciscoasa/contexta(config)# show crypto ca server certificate Main`	ASA に発行された証明書の詳細とトラストポイントの CA 証明書を表示して、登録プロセスが成功したことを確認します。
ステップ 4	**write memory** **例：** `ciscoasa/contexta(config)# write memory`	実行コンフィギュレーションを保存します。

SCEP 要求のプロキシ サポートの設定

サードパーティの CA を使用してリモート アクセスのエンド ポイントを認証するように ASA を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**crypto ikev2 enable outside client-services port** *portnumber* **例：** `ciscoasa(config-tunnel-ipsec)# crypto ikev2 enable outside client-services`	クライアント サービスをイネーブルにします。 **（注）** IKEv2 をサポートする場合にのみ必要です。 このコマンドをトンネル グループ ipsec 属性コンフィギュレーション モードで入力します。 デフォルトのポート番号は 443 です。

ステップ 2	**scep-enrollment enable**
	
	例：
	`ciscoasa(config-tunnel-general)# scep-enrollment enable`
	`INFO: 'authentication aaa certificate' must be configured to complete setup of this option.`
		トンネル グループの SCEP 登録をイネーブルにします。
		このコマンドを tunnel-group general-attributes コンフィギュレーション モードで入力します。

ステップ 3	**scep-forwarding-url value** *URL* **例：** `ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/`	グループ ポリシー用の SCEP CA を登録します。 このコマンドは、サードパーティのデジタル証明書をサポートするグループ ポリシーごとに 1 回入力します。また、このコマンドはグループ ポリシー一般属性コンフィギュレーション モードで入力します。 *URL* は CA の SCEP URL です。

	コマンド	目的

ステップ 4	**secondary-pre-fill-username clientless hide use-common-password** *password*
	
	例：
	`ciscoasa(config)# tunnel-group remotegrp webvpn-attributes`
	`ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide use-common-password secret`
		証明書が SCEP プロキシの WebLaunch のサポートに使用できない場合は、共通のセカンダリ パスワードを使用します。
		
		SCEP プロキシをサポートするには、**hide** キーワードを使用する必要があります。
		
		たとえば、証明書は、それを要求するエンド ポイントでは使用できません。エンド ポイントに証明書が存在する場合、AnyConnect は ASA への接続を切断し、その後再接続して、内部ネットワーク リソースへのアクセスを提供する DAP ポリシーに適合するようにします。

ステップ 5	**secondary-pre-fill-username ssl-client hide use-common-password** *password* **例：** `ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide use-common-password secret`	AnyConnect VPN セッションの事前入力されているセカンダリ ユーザ名を非表示にします。 以前のリリースから継承した **ssl-client** キーワードに関係なく、IKEv2 または SSL を使用する AnyConnect セッションをサポートするには、このコマンドを使用します。 SCEP プロキシをサポートするには、**hide** キーワードを使用する必要があります。
ステップ 6	**secondary-username-from-certificate** {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**] **例：** `ciscoasa(config-tunnel-webvpn)# secondary-username-from-certificate CN no-certificate-fallback cisco-secure-desktop machine-unique-id`	証明書が使用できないときにはユーザ名を指定します。

ローカル CA サーバのイネーブル化

ローカル CA サーバをイネーブルにする前に、7 文字以上からなるパスフレーズを作成して、生成されるローカル CA 証明書とキー ペアを含む PKCS12 ファイルを符号化し、アーカイブしておく必要があります。CA 証明書またはキー ペアが失われた場合は、パスフレーズを使用して PKCS12 アーカイブをロック解除します。

ローカル CA サーバをイネーブルにするには、次のコマンドを実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** ciscoasa (config)# crypto ca server	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**no shutdown** **例：** ciscoasa (config-ca-server)# no shutdown	ローカル CA サーバをイネーブルにします。ローカル CA サーバの証明書、キー ペア、および必要なデータベース ファイルを生成し、ローカル CA サーバの証明書とキー ペアを PKCS12 ファイル内のストレージにアーカイブします。8 ～ 65 文字の英数字のパスワードが必要になります。初期スタートアップ後、パスフレーズを求めるプロンプトを表示せずにローカル CA をディセーブルにすることができます。 **（注）** ローカル CA サーバをイネーブルにしたら、コンフィギュレーションを保存して、リブート後にローカル CA 証明書とキー ペアが失われないようにします。

例

次の例では、ローカル CA サーバをイネーブルにします。

```
hostname (config)# crypto ca server
ciscoasa (config-ca-server)# no shutdown

% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password: caserver

Re-enter password: caserver

Keypair generation process begin.Please wait...
```

次に、ローカル CA サーバのコンフィギュレーションとステータスを表示するサンプル出力を示します。

```
Certificate Server LOCAL-CA-SERVER:
    Status: enabled
    State: enabled
    Server's configuration is locked (enter "shutdown" to unlock it)
    Issuer name: CN=wz5520-1-16
    CA certificate fingerprint/thumbprint: (MD5)
        76dd1439 ac94fdbc 74a0a89f cb815acc
    CA certificate fingerprint/thumbprint: (SHA1)
        58754ffd 9f19f9fd b13b4b02 15b3e4be b70b5a83
    Last certificate issued serial number: 0x6
    CA certificate expiration timer: 14:25:11 UTC Jan 16 2008
    CRL NextUpdate timer: 16:09:55 UTC Jan 24 2007
    Current primary storage dir: flash:
```

ローカル CA サーバの設定

ローカル CA サーバを設定するには、次のコマンドを実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** ciscoasa (config)# crypto ca server	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA を作成します。
ステップ 2	**smtp from-address** *e-mail_address* **例：** ciscoasa (config-ca-server) # smtp from-address SecurityAdmin@example.com	SMTP from-address を指定します。これはローカル CA がユーザに登録案内用の OTP を送る電子メール メッセージを送信するときに、発信元アドレスとして使用する有効な電子メール アドレスを指定です。
ステップ 3	**subject-name-default** *dn* **例：** hostname (config-ca-server)# subject-name-default cn=engineer, o=asc systems, c="US"	（オプション）発行された証明書のユーザ名に付加する subject-name DN を指定します。 subject-name DN とユーザ名は結合して、ローカル CA サーバによって発行されたすべてのユーザ証明書の DN を形成します。subject-name DN を指定しない場合、ユーザ データベースにユーザを追加するたびに、ユーザ証明書に含めるサブジェクト名 DN を正確に指定する必要があります。 **（注）** ローカル CA をイネーブルにした後は、issuer-name 値および keysize server 値は変更できないため、設定したローカル CA をイネーブルにする前に、オプションのすべてのパラメータを慎重に見直してください。
ステップ 4	**no shutdown** **例：** hostname (config-ca-server)# no shutdown	自己署名した証明書を作成し、ASA のローカル CA に関連付けます。自己署名した証明書のキーの使用拡張には、キー暗号化、キー シグニチャ、CRL 署名、および証明書署名機能があります。 **（注）** 自己署名したローカル CA 証明書が生成された後、特性を変更するには、既存のローカル CA サーバを削除して、完全に作成し直す必要があります。 ローカル CA サーバはユーザ証明書を把握しているため、管理者は、必要に応じて特権を無効にしたり元に戻したりできます。

例

次の例は、必要なパラメータすべてで事前定義済みのデフォルト値を使用してローカル CA サーバを設定する方法を示しています。

```
hostname (config)# crypto ca server
hostname (config-ca-server) # smtp from-address SecurityAdmin@example.com
hostname (config-ca-server)# subject-name-default cn=engineer, o=asc Systems, c=US
hostname (config-ca-server)# no shutdown
```

ローカル CA サーバのカスタマイズ

カスタマイズされたローカル CA グループ サーバを設定するには、次のコマンドを実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** ciscoasa (config)# crypto ca server	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**issuer-name** *DN-string* **例：** hostname (config-ca-server)# issuer-name cn=xx5520,cn=30.132.0.25,ou=DevTest,ou=QA,o=ASC Systems	デフォルト値のないパラメータを指定します。
ステップ 3	**smtp subject** *subject-line* **例：** hostname (config-ca-server) # smtp subject Priority E-Mail: Enclosed Confidential Information is Required for Enrollment	ローカル CA サーバから送信されるすべての電子メールの件名フィールドに表示するテキストをカスタマイズします。
ステップ 4	**smtp from-address** *e-mail_address* **例：** hostname (config-ca-server) # smtp from-address SecurityAdmin@example.com	ローカル CA サーバによって生成されるすべての電子メールの [From:] フィールドに使用する電子メール アドレスを指定します。

	コマンド	目的
ステップ 5	**subject-name-default** *dn* **例：** `hostname (config-ca-server) # subject-name default cn=engineer, o=ASC Systems, c=US`	発行された証明書のユーザ名に追加するオプションの subject-name DN を指定します。デフォルトの subject-name DN は、ローカル CA サーバによって発行されたすべてのユーザ証明書でユーザ名の一部になります。 許可される DN 属性キーワードは次のとおりです。 • C = 国 • CN = 通常名 • EA = 電子メール アドレス • L = 地名 • O = 組織名 • OU = 組織ユニット • ST = 州/都道府県 • SN = 姓名の姓 • ST = 州/都道府県 **（注）** subject-name-default を標準の subject-name のデフォルト値として機能するように指定しない場合、ユーザを追加するたびに DN を指定する必要があります。

ローカル CA サーバのデバッグ

新たに設定されたローカル CA サーバをデバッグするには、次のコマンドを実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** `ciscoasa (config)# crypto ca server`	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**debug crypto ca server** **例：** `ciscoasa (config-ca-server)# debug crypto ca server`	ローカル CA サーバを設定およびイネーブルにするときに、デバッグ メッセージを表示します。レベル 1 のデバッグ機能を実行します。レベル 1 ～ 255 を使用できます。 **（注）** デバッグ コマンドによって、ビジー状態のネットワークのトラフィックが低速化することがあります。レベル 5 以上は、未加工データのダンプのために予約されており、出力が多くなりすぎるため、通常のデバッグ時は避ける必要があります。

ローカル CA サーバのディセーブル化

ローカル CA サーバをディセーブルにするには、次のコマンドを実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** ciscoasa (config)# crypto ca server	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**shutdown** **例：** ciscoasa (config-ca-server)# shutdown INFO: Local CA Server has been shutdown.	ローカル CA サーバをディセーブルにします。Web サイト登録をディセーブルにして、ローカル CA サーバ コンフィギュレーションの修正を可能にします。現在のコンフィギュレーションと関連付けられたファイルを保存します。初期スタートアップ後、パスフレーズを求めるプロンプトを表示せずにローカル CA を再びイネーブルにすることができます。

ローカル CA サーバの削除

既存のローカル CA サーバ（イネーブル状態またはディセーブル状態）を削除するには、次のいずれかのコマンドを入力します。

コマンド	目的
次のどちらかを実行します。	
no crypto ca server **例：** ciscoasa (config)# no crypto ca server	既存のローカル CA サーバ（イネーブル状態またはディセーブル状態）を削除します。 **（注）** ローカル CA サーバを削除すると、ASA からコンフィギュレーションが削除されます。削除されたコンフィギュレーションは元に戻せません。 関連付けられたローカル CA サーバのデータベースとコンフィギュレーション ファイル（つまり、ワイルドカード名が LOCAL-CA-SERVER.* のすべてのファイル）も必ず削除してください。
clear configure crypto ca server **例：** ciscoasa (config)# clear config crypto ca server	

ローカル CA 証明書の特性の設定

次のローカル CA 証明書の特性を設定できます。

- すべてのユーザ証明書に表示されるとおりの証明書発行元の名前。
- ローカル CA 証明書（サーバおよびユーザ）および CRL のライフタイム。
- ローカル CA とユーザ証明書に関連付けられている公開キーと秘密キーペアの長さ。

- 「発行元名の設定」（P.34-29）
- 「CA 証明書のライフタイムの設定」（P.34-30）
- 「ユーザ証明書のライフタイムの設定」（P.34-31）
- 「CRL のライフタイムの設定」（P.34-31）
- 「サーバのキーサイズの設定」（P.34-32）
- 「外部ローカル CA ファイル ストレージの設定」（P.34-33）
- 「CRL のダウンロード」（P.34-35）
- 「CRL の保存」（P.34-36）
- 「登録パラメータの設定」（P.34-37）
- 「ユーザの追加と登録」（P.34-38）
- 「ユーザの更新」（P.34-40）
- 「ユーザの復元」（P.34-41）
- 「ユーザの削除」（P.34-41）
- 「証明書の無効化」（P.34-42）
- 「ローカル CA 証明書データベースのメンテナンス」（P.34-42）
- 「ローカル CA 証明書のロールオーバー」（P.34-42）
- 「ローカル CA サーバ証明書およびキー ペアのアーカイブ」（P.34-43）

発行元名の設定

証明書の発行元名を設定するには、次のコマンドを実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** ciscoasa (config)# crypto ca server	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**issuer-name** *DN-string* **例：** hostname (config-ca-server)# issuer-name CN=xx5520,CN=30.132.0.25,ou=DevTest,ou=QA,O=ABC Systems	ローカル CA 証明書のサブジェクト名を指定します。設定した証明書発行元名は、自己署名したローカル CA 証明書のサブジェクト名および発行元名の両方であり、発行済みクライアント証明書すべておよび発行済み CRL の発行元名でもあります。ローカル CA のデフォルトの発行元名の形式は、*hostname.domainname* です。 **（注）** ローカル CA が最初にイネーブルになった後に発行元名の値を変更することはできません。

CA 証明書のライフタイムの設定

ローカル CA サーバ証明書のライフタイムを設定するには、次のコマンドを実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** `ciscoasa (config)# crypto ca server`	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**lifetime ca-certificate** *time* **例：** `hostname (config-ca-server)# lifetime ca-certificate 365`	証明書に含まれる有効期限を指定します。ローカル CA 証明書のデフォルトのライフタイムは 3 年間です。 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。
ステップ 3	**no lifetime ca-certificate** **例：** `hostname (config-ca-server)# no lifetime ca-certificate`	（オプション）ローカル CA 証明書のライフタイムをデフォルトの 3 年にリセットします。 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 証明書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。次のような preexpiration syslog メッセージが生成されます。 `%ASA-1-717049: Local CA Server certificate is due to expire in 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。

ユーザ証明書のライフタイムの設定

ユーザ証明書のライフタイムを設定するには、次のコマンドを実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** `ciscoasa (config)# crypto ca server`	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**lifetime certificate** *time* **例：** `hostname (config-ca-server)# lifetime certificate 60`	ユーザ証明書の有効期間の時間の長さを設定します。 **（注）** ユーザ証明書の期限が満了になる前に、ローカル CA サーバは、証明書の有効期限の数日前にそのユーザに登録特権を付与し、更新の注意を設定し、証明書更新用の登録ユーザ名および OTP を電子メールで配信することで、証明書の更新プロセスを自動的に開始します。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。

CRL のライフタイムの設定

CRL ライフタイムを設定するには、次のコマンドを実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** `ciscoasa (config)# crypto ca server`	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**lifetime crl** *time* **例：** `hostname (config-ca-server)# lifetime crl 10`	CRL の有効期間の時間の長さを設定します。 ローカル CA では、ユーザ証明書が失効または失効解除されるたびに CRL をアップデートおよび再発行しますが、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 回だけ自動的に行われます。CRL のライフタイムを指定しない場合、デフォルトの期間は 6 時間になります。

ステップ 3	**crypto ca server crl issue**
	
	例：
	`ciscoasa(config)# crypto ca server crl issue`
	`A new CRL has been issued.`
		CRL を任意のタイミングで強制的に発行します。現在の CRL がただちに更新および再生成され、既存の CRL が上書きされます。
		
		（注） CRL ファイルがエラーで削除されたり、壊れたりして、再生成が必要になった場合以外は、このコマンドを使用しないでください。

サーバのキーサイズの設定

サーバのキーサイズを設定するには、次のコマンドを実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** `ciscoasa (config)# crypto ca server`	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**keysize server** **例：** `hostname (config-ca-server)# keysize server 2048`	ユーザ証明書登録で生成される公開キーと秘密キーのサイズを指定します。キーペア サイズのオプションは 512、768、1024、2048 ビットで、デフォルト値は 1024 ビットです。 **（注）** ローカル CA をイネーブルにした後でローカル CA のキーサイズを変更することはできません。発行済み証明書すべてが無効になるためです。ローカル CA キーサイズを変更するには、現在のローカル CA を削除して新しいローカル CA を再設定する必要があります。

例

次は、データベースの 2 つのユーザ証明書の出力例です。

```
Username: user1
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 12:45:52 UTC Fri Jan 4 2017
Certificates Issued:
serial:   0x71
issued:   12:45:52 UTC Thu Jan 3 2008
expired:  12:17:37 UTC Sun Dec 31 2017
status:   Not Revoked
Username: user2
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 12:27:59 UTC Fri Jan 4 2008
Certificates Issued:
serial:   0x2
issued:   12:27:59 UTC Thu Jan 3 2008
expired:  12:17:37 UTC Sun Dec 31 2017
status:   Not Revoked
<--- More --->
```

外部ローカル CA ファイル ストレージの設定

ローカル CA サーバ データベースのローカル CA サーバ設定、ユーザ、発行済み証明書、CRL をフラッシュ メモリまたは外部ローカル CA ファイル システムのいずれかに保存できます。外部ローカル CA ファイル ストレージを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**mount** *name* **type** **例：** `hostname (config)# mount mydata type cifs`	特定のファイル システム タイプで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	**mount** *name* **type cifs**
	
	例：
	`hostname (config-mount-cifs)# mount mydata type cifs`
	`server 10.1.1.10 share myshare`
	`domain example.com`
	`username user6`
	`password ********`
	`status enable`
		CIFS ファイル システムをマウントします。
		（注） ファイル システムをマウントするユーザだけが、**no mount** コマンドを使ってアンマウントできます。

ステップ 3	**crypto ca server** **例：** `ciscoasa (config)# crypto ca server`	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。

ステップ 4	**database path** *mount-name directory-path*
	
	例：
	`hostname (config-ca-server)# database path`
	`mydata:newuser`
		ローカル CA サーバ データベースで使用するマウント済みの CIFS ファイル システムである *mydata* の場所を指定します。サーバへのパスを確立して、ストレージおよび取得に使用するローカル CA ファイルまたはフォルダ名を指定します。ローカル CA ファイル ストレージを ASA フラッシュ メモリに戻すには、**no database path** コマンドを使用します。
		（注） 外部サーバに保存されているローカル CA ファイルを保護するには、ユーザ名とパスワードが保護されているファイル タイプが CIFS または FTP のマウント済みファイル システムが必要です。

ステップ 5	**write memory** **例：** `ciscoasa (config)# write memory`	実行コンフィギュレーションを保存します。 外部ローカル CA ファイル ストレージでは、ASA 設定を保存するたびに、ユーザ情報が ASA からマウント済みのファイル システムおよびファイルの場所である *mydata:newuser* に保存されます。 フラッシュ メモリ ストレージの場合、ユーザ情報は、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自動的に保存されます。

例

次の例は、フラッシュ メモリまたは外部ストレージにあるローカル CA ファイルの一覧を表示します。

```
ciscoasa (config-ca-server)# dir LOCAL* //
Directory of disk0:/LOCAL*

75     -rwx  32          13:07:49 Jan 20 2007  LOCAL-CA-SERVER.ser
77     -rwx  229         13:07:49 Jan 20 2007  LOCAL-CA-SERVER.cdb
69     -rwx  0           01:09:28 Jan 20 2007  LOCAL-CA-SERVER.udb
81     -rwx  232         19:09:10 Jan 20 2007  LOCAL-CA-SERVER.crl
72     -rwx  1603        01:09:28 Jan 20 2007  LOCAL-CA-SERVER.p12

127119360 bytes total (79693824 bytes free)
```

CRL のダウンロード

特定のインターフェイスまたはポートで、CRL を HTTP ダウンロードできるようにするには、次のコマンドを実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** `ciscoasa (config)# crypto ca server`	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**publish-crl interface** *interface* **port** *portnumber* **例：** `hostname (config-ca-server)# publish-crl outside 70`	インターフェイスのポートを開き、CRL をインターフェイスからアクセスできるようにします。指定したインターフェイスおよびポートを使用して、CRL の着信要求をリッスンします。選択できるインターフェイスと任意のポートは、次のとおりです。 • inside：interface/GigabitEthernet0/1 の名前 • management：interface/Management0/0 の名前 • outside：interface/GigabitEthernet0/0 の名前 • ポート番号の範囲は 1 ～ 65535 です。TCP ポート 80 は、HTTP のデフォルト ポート番号です。 **（注）** インターフェイスを開いて CRL ファイルをダウンロードするにはこのコマンドが必要であるため、このコマンドを指定しないと、CDP の場所から CRL にアクセスできません。 CDP URL でインターフェイスの IP アドレスを使用するように設定し、CDP URL およびファイル名のパスも設定できます（http://10.10.10.100/user8/my_crl_file など）。 この場合、その IP アドレスが設定されたインターフェイスだけが CRL 要求をリッスンします。要求を受信すると、ASA によってパス /user8/my_crl_file と設定済み CDP 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。 **（注）** プロトコルは必ず HTTP にします。したがって、プレフィックスは http:// です。

CRL の保存

自動的に生成されるローカル CA の CRL に特定の場所を設定するには、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 モードで次のサイト間タスクを実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** ciscoasa (config)# crypto ca server	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**cdp-url** *url* **例：** ciscoasa(config-ca-server)# cdp-url http://172.16.1.1/pathname/myca.crl	対象となるすべての証明書に含まれる Cisco Discovery Protocol（CDP）を指定します。CDP に特定の場所を設定しない場合、デフォルトの URL は http://*hostname.domain*/+CSCOCA+/asa_ca.crl になります。 ローカル CA は、ユーザ証明書が無効化または無効化解除されるたびに、CRL を更新および再発行します。無効化に変更がない場合、CRL のライフタイムごとに 1 回 CRL が再発行されます。 このコマンドがローカル CA ASA から直接 CRL を処理するように設定されている場合に、インターフェイスのポートを開き、CRL をインターフェイスからアクセスできるようにする手順については、「CRL のダウンロード」（P.34-35）を参照してください。 CRL は、ローカル CA によって発行された証明書の失効を検証する他のデバイスのためにあります。また、ローカル CA は、自らの証明書データベース内にあるすべての発行済み証明書とステータスを追跡します。検証する機関が、外部サーバから失効ステータスを取得してユーザ証明書を検証する必要がある場合、失効チェックが行われます。この場合、外部サーバは、証明書を発行した CA、または CA が指定したサーバである可能性があります。

登録パラメータの設定

登録パラメータを設定するには、次のコマンドを実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** ciscoasa (config)# crypto ca server	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**otp expiration** *timeout* **例：** ciscoasa(config-ca-server)# otp expiration 24	ローカル CA 登録ページに対して発行された OTP が有効である期間を時間数で指定します。デフォルトの有効期間は 72 時間です。 **（注）** 登録 Web サイトで証明書に登録するためのユーザ OTP をパスワードとして使用して、指定したユーザの発行済み証明書およびキーペアが含まれる PKCS12 ファイルをロック解除することもできます。
ステップ 3	**enrollment-retrieval** *timeout* **例：** ciscoasa(config-ca-server)# enrollment-retrieval 120	登録済みユーザが PKCS12 登録ファイルを取得できる期間を時間単位で指定します。この期間は、ユーザが正常に登録されたときに開始します。デフォルトの取得期間は 24 時間です。取得期間の有効値の範囲は 1 ～ 720 時間です。登録取得期間は、OTP の有効期間とは関係ありません。 登録取得期間が過ぎた後、ユーザ証明書とキーペアは無効になります。ユーザが証明書を受け取る唯一の方法は、管理者が証明書の登録を再開し、ユーザの再ログインを許可することです。

ユーザの追加と登録

ローカル CA データベースに登録できるユーザを追加するには、次のコマンドを実行します。

	コマンド	目的
ステップ 1	**crypto ca server user-db add** *username* [**dn** *dn*] [**email** *emailaddress*] **例：** `hostname (config-ca-server)# crypto ca server user-db add user1 dn user1@example.com, Engineer, Example Company, US, email user1@example.com`	ローカル CA サーバ ユーザ データベースに新規ユーザを追加します。オプションは次のとおりです。 • *username*：4 ～ 64 文字の文字列で、追加するユーザの単純なユーザ名です。ユーザ名には、電子メール アドレスを指定できます。この電子メール アドレスを使用して、登録案内の際に必要に応じてユーザに連絡を取ることができます。 • *dn*：識別名。OSI ディレクトリ（X.500）内のグローバルな正規のエントリ名です（たとえば、cn=user1@example.com, cn=Engineer, o=Example Company, c=US のようになります）。 • *e-mail-address*：ワンタイム パスワード（OTP）および通知が送信される、新しいユーザの電子メール アドレスです。
ステップ 2	**crypto ca server user-db allow** *user* **例：** `hostname (config-ca-server)# crypto ca server user-db allow user6`	新たに追加したユーザにユーザ特権を付与します。
ステップ 3	**crypto ca server user-db email-otp** *username* **例：** `hostname (config-ca-server)# crypto ca server user-db email-otp exampleuser1`	ローカル CA データベースのユーザに、ユーザ証明書を登録およびダウンロードするように通知します。そのユーザには、OTP が自動的に電子メールで送信されます。 **（注）** 管理者は、電子メールでのユーザ通知が必要である場合、ユーザを追加するときに、ユーザ名フィールドまたは電子メール フィールドに電子メール アドレスを指定する必要があります。
ステップ 4	**crypto ca server user-db show-otp** **例：** `hostname (config-ca-server)# crypto ca server user-db show-otp`	対象の OTP を表示します。

	コマンド	目的
ステップ 5	**otp expiration** *timeout* **例：** `hostname (config-ca-server)# otp expiration 24`	登録の時間制限を時間単位で設定します。デフォルトの有効期間は 72 時間です。**otp expiration** コマンドは、OTP がユーザ登録に有効な期間を定義します。この期間は、ユーザが登録を許可されたときに開始します。 ユーザが正しい OTP を使って時間制限内に正常に登録すると、ローカル CA サーバによって PKCS12 ファイルが作成されます。これには、そのユーザのキー ペア、生成されたキー ペアの公開キーに基づいたユーザ証明書、およびユーザを追加したときに指定した subject-name DN が含まれます。PKCS12 ファイルの内容は、OTP と呼ばれるパスフレーズによって保護されます。OTP は手動で処理できます。または、管理者が登録を許可した後、このファイルをローカル CA からユーザに電子メールで送信し、ダウンロードすることもできます。 PKCS12 ファイルは、*username.p12* という名前で一時的なストレージに保存されます。ストレージ内の PKCS12 ファイルを使用して、登録取得期間内に戻り、PKCS12 ファイルを必要な回数だけダウンロードすることができます。登録取得期間が過ぎると、PKCS12 ファイルがストレージから自動的に削除され、ダウンロードできなくなります。 **（注）** ユーザ証明書が含まれる PKCS12 ファイルを取得する前に登録の有効期間が切れた場合、登録は許可されません。

ユーザの更新

更新通知のタイミングを指定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** `ciscoasa (config)# crypto ca server`	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**renewal-reminder** *time* **例：** `ciscoasa (config-ca-server)# renewal-reminder 7`	ローカル CA 証明書の有効期限までの日数（1 ～ 90）を指定します。この日数が経過すると、再登録に関する最初の通知が証明書所有者に送信されます。証明書は、有効期限を過ぎると無効になります。 電子メールでユーザに送信される更新通知のタイプや送信時機の設定は各種あり、ローカル CA サーバの設定中に管理者が設定できます。 3 種類の通知が送信されます。ユーザ データベースに電子メール アドレスが指定されている場合、3 種類ある通知ごとに、電子メールが自動的に証明書所有者に送信されます。ユーザの電子メール アドレスを指定していない場合、syslog メッセージが更新要件を警告します。 ユーザがユーザ データベース内に存在する限り、ASA によって、有効期限間近の有効な証明書を持つすべてのユーザに、証明書の更新特権が自動的に付与されます。したがって、管理者がユーザに自動更新を許可しない場合、更新期間の前にそのユーザをデータベースから削除する必要があります。

ユーザの復元

ローカル CA サーバによって発行され、以前無効にした証明書とユーザを復元するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** `ciscoasa (config)# crypto ca server`	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**crypto ca server unrevoke** *cert-serial-no* **例：** `ciscoasa (config)# crypto ca server unrevoke 782ea09f`	ユーザを復元し、ローカル CA サーバによって発行され、以前無効にした証明書を無効化解除します。 ローカル CA では、CRL は、無効になったすべてのユーザ証明書のシリアル番号で保持されます。このリストは外部デバイスで使用でき、**cdp-url** コマンドや **publish-crl** コマンドなどで設定されている場合に、ローカル CA から直接取得することができます。証明書のシリアル番号で、現在の証明書を無効化（または無効化解除）すると、CRL にはそれらの変更が自動的に反映されます。

ユーザの削除

ユーザ データベースからユーザ名によってユーザを削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** `ciscoasa (config)# crypto ca server`	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**crypto ca server user-db remove** *username* **例：** `ciscoasa (config)# crypto ca server user-db remove user1`	ユーザ データベースからユーザを削除し、そのユーザに発行された有効な証明書の無効化を許可します。

証明書の無効化

ユーザ証明書を無効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	**crypto ca server** **例：** `ciscoasa (config)# crypto ca server`	ローカル CA サーバ コンフィギュレーション モードに入ります。ローカル CA の設定と管理を許可します。
ステップ 2	**crypto ca server revoke** *cert-serial-no* **例：** `ciscoasa (config-ca-server)# crypto ca server revoke 782ea09f`	16 進数の形式で証明書のシリアル番号を入力します。ローカル CA サーバ上の証明書データベースと CRL で証明書に無効のマークを付けます。CRL は、自動的に再発行されます。 **（注）** ASA の証明書を無効にするには、パスワードも必要なので、パスワードは必ず記録し、安全な場所に保管してください。

ローカル CA 証明書データベースのメンテナンス

ローカル CA 証明書データベースを維持するため、データベースに変更が加えられるたびに **write memory** コマンドを使用して、証明書データベース ファイル LOCAL-CA-SERVER.cdb を保存してください。ローカル CA 証明書データベースには、次のファイルが含まれます。

- LOCAL-CA-SERVER.p12 ファイルは、ローカル CA サーバを最初にイネーブルにしたときに生成されたローカル CA 証明書とキー ペアのアーカイブです。
- LOCAL-CA-SERVER.crl ファイルは、実際の CRL です。
- LOCAL-CA-SERVER.ser ファイルでは、発行済み証明書のシリアル番号が追跡されます。

ローカル CA 証明書のロールオーバー

ローカル CA 証明書の有効期限の 30 日前に、ロールオーバー代替証明書が生成され、syslog メッセージ情報で管理者にローカル CA のロールオーバーの時期であることが知らされます。新しいローカル CA 証明書は、現在の証明書が有効期限に達する前に、必要なすべてのデバイスにインポートする必要があります。管理者が、新しいローカル CA 証明書としてロールオーバー証明書をインストールして対応しない場合、検証が失敗する可能性があります。

ローカル CA 証明書は、同じキー ペアを使用して期限満了後に自動的にロールオーバーします。ロールオーバー証明書は、base 64 形式でエクスポートに使用できます。

例

次に、base 64 で符号化されたローカル CA 証明書の例を示します。

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHAYJKo
ZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3SDOiDwZG9
n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZTS1E4L0fSaC3
uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZPrzoG1J8BFqdPa1j
BGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYYbP86tvbZ2yOVZR6aKFVI
0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmuBeGDKOncTknfgy0XM+fG5rb3
qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

ローカル CA サーバ証明書およびキー ペアのアーカイブ

ローカル CA サーバ認証とキー ペアをアーカイブするには、次のコマンドを入力します。

コマンド	目的
copy **例：** `hostname# copy LOCAL-CA-SERVER_0001.pl2 tftp://10.1.1.22/user6/`	FTP または TFTP を使用して、ローカル CA サーバ証明書とキー ペア、および ASA からのすべてのファイルをコピーします。 **（注）** すべてのローカル CA ファイルをできるだけ頻繁にバックアップしてください。

デジタル証明書のモニタリング

証明書のコンフィギュレーションとデータベース情報を表示するには、次のコマンドの 1 つまたは複数を入力します。

コマンド	目的
show crypto ca server	ローカル CA のコンフィギュレーションとステータスを表示します。
show crypto ca server cert-db	ローカル CA によって発行されたユーザ証明書を表示します。
show crypto ca server certificate	コンソールに base 64 形式でローカル CA 証明書を表示し、使用可能な場合は、他のデバイスへのインポート時に新しい証明書の検証に使うためのロールオーバー証明書のサムプリントを含むロールオーバー証明書の情報を表示します。
show crypto ca server crl	CRL を表示します。
show crypto ca server user-db	ユーザとユーザのステータスを表示します。この情報に次の修飾子を使用して、表示されるレコード数を減らすことができます。 • allowed：現在登録が許可されているユーザだけを表示します。 • enrolled：登録され、有効な証明書を持つユーザだけを表示します。 • expired：期間満了になった証明書を持つユーザだけを表示します。 • on-hold：証明書を持たず現在登録が許可されていないユーザだけを表示します。
show crypto ca server user-db allowed	登録できるユーザを表示します。
show crypto ca server user-db enrolled	有効な証明書を持つ登録済みユーザを表示します。
show crypto ca server user-db expired	期間満了した証明書を持つユーザを表示します。
show crypto ca server user-db on-hold	証明書がなく、登録が許可されていないユーザを表示します。
show crypto key *name of key*	生成したキー ペアを表示します。
show running-config	ローカル CA 証明書マップ ルールを表示します。

例

次の例では、汎用 RSA キーを表示します。

```
ciscoasa/contexta(config)# show crypto key mypubkey
Key pair was generated at: 16:39:47 central Feb 10 2010
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 1024
 Key Data:

30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ea51b7
  0781848f 78bccac2 4a1b5b8d 2f3e30b4 4cae9f86 f4485207 159108c9 f5e49103
  9eeb0f5d 45fd1811 3b4aafce 292b3b64 b4124a6f 7a777b08 75b88df1 8092a9f8
  5508e9e5 2c271245 7fd1c0c3 3aaf1e04 c7c4efa4 600f4c4a 6afe56ad c1d2c01c
  e08407dd 45d9e36e 8cc0bfef 14f9e6ac eca141e4 276d7358 f7f50d13 79020301 0001
Key pair was generated at: 16:34:54 central Feb 10 2010
```

次に、ローカル CA CRL を表示する例を示します。

```
hostname (config)# show crypto ca server crl
Certificate Revocation List:
    Issuer: cn=xx5520-1-3-2007-1
    This Update: 13:32:53 UTC Jan 4 2010
    Next Update: 13:32:53 UTC Feb 3 2010
    Number of CRL entries: 2
    CRL size: 270 bytes
Revoked Certificates:
    Serial Number: 0x6f
    Revocation Date: 12:30:01 UTC Jan 4 2010
    Serial Number: 0x47
    Revocation Date: 13:32:48 UTC Jan 4 2010
```

次に、1 人の保留中のユーザを表示する例を示します。

```
hostname (config)# show crypto ca server user-db on-hold
username: wilma101
email:    <None>
dn:       <None>
allowed:  <not allowed>
notified: 0
hostname (config)#
```

次に、**show running-config** コマンドの出力例を示します。この出力には、ローカル CA 証明書マップ ルールが表示されています。

```
crypto ca certificate map 1
 issuer-name co asc
 subject-name attr ou eq Engineering
```

証明書管理の機能履歴

表 34-1　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。
証明書管理	7.2(1)	次のコマンドを導入しました。 **issuer-name** *DN-string*、**revocation-check crl none**、**revocation-check crl**、**revocation-check none**。 **crl** {**required** | **optional** | **nocheck**} コマンドが非推奨になりました。
証明書管理	8.0(2)	次のコマンドを導入しました。 **cdp-url**、**crypto ca server**、**crypto ca server crl issue**、**crypto ca server revoke** *cert-serial-no*、**crypto ca server unrevoke** *cert-serial-no*、**crypto ca server user-db add** *user* [**dn** *dn*] [**email** *e-mail-address*]、**crypto ca server user-db allow** {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp**]、**crypto ca server user-db email-otp** {*username* | **all-unenrolled** | **all-certholders**}、**crypto ca server user-db remove** *username*、**crypto ca server user-db show-otp** {*username* | **all-certholders** | **all-unenrolled**}、**crypto ca server user-db write**、**[no] database path** *mount-name directory-path*、**debug crypto ca server** [*level*]、**lifetime {ca-certificate** | **certificate** | **crl**} *time*、no shutdown、**otp expiration** *timeout*、**renewal-reminder** *time*、**show crypto ca server**、**show crypto ca server cert-db [user** *username* | **allowed** | **enrolled** | **expired** | **on-hold] [serial** *certificate-serial-number*]、**show crypto ca server certificate**、**show crypto ca server crl**、**show crypto ca server user-db** [**expired** | **allowed** | **on-hold** | **enrolled**]、**show crypto key** *name of key*、**show running-config**、**shutdown**。

表 34-1　証明書管理の機能履歴 （続き）

機能名	プラットフォームリリース	機能情報
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。 次のコマンドを導入しました。 **crypto ikev2 enable outside client-services port** *portnumber*、**scep-enrollment enable**、**scep-forwarding-url value** *URL*、**secondary-pre-fill-username clientless hide use-common-password** *password*、**secondary-pre-fill-username ssl-client hide use-common-password** *password*、**secondary-username-from-certificate** {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**]。

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。

- 「ASDM、Telnet、または SSH の ASA アクセスの設定」（P.35-1）
- 「CLI パラメータの設定」（P.35-6）
- 「VPN トンネルを介した管理アクセスの設定」（P.35-10）
- 「システム管理者用 AAA の設定」（P.35-11）
- 「管理アクセスの機能履歴」（P.35-35）

（注） 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」（P.35-2）
- 「ガイドラインと制限事項」（P.35-2）
- 「Telnet アクセスの設定」（P.35-3）
- 「Telnet クライアントの使用」（P.35-4）
- 「SSH アクセスの設定」（P.35-4）
- 「SSH クライアントの使用」（P.35-5）
- 「ASDM の HTTPS アクセスの設定」（P.35-6）

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

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

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.35-10）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、**aaa authentication ssh console LOCAL** コマンドを使用して AAA 認証を設定し、次に **username** コマンドを入力してローカル 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、イネーブル パスワード、Telnet パスワードの設定」（P.13-1）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.35-1）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。

Telnet アクセスの設定

クライアント IP アドレスを、ASA に Telnet 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。

手順の詳細

	コマンド	目的
ステップ 1	**telnet** *source_IP_address mask source_interface* **例：** `ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside`	アドレスまたはサブネットごとに、ASA が接続を許可する IP アドレスを指定します。 インターフェイスが 1 つしかない場合は、インターフェイスのセキュリティ レベルが 100 である限り、そのインターフェイスにアクセスするように Telnet を設定することができます。
ステップ 2	**telnet timeout** *minutes* **例：** `ciscoasa(config)# telnet timeout 30`	ASA がセッションを切断するまでに Telnet がアイドル状態を維持する時間の長さを設定します。 タイムアウトは 1 ～ 1440 分に設定します。デフォルトは 5 分です。デフォルトの期間では一般に短すぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定しておいてください。

例

次の例は、アドレスが 192.168.1.2 の内部インターフェイスのホストで ASA にアクセスする方法を示しています。

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

次の例は、192.168.3.0 のネットワーク上のすべてのユーザが内部インターフェイス上の ASA にアクセスできるようにする方法を示しています。

```
ciscoasa(config)# telnet 192.168.3.0 255.255.255.0 inside
```

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、**password** コマンドで設定したログイン 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、イネーブル パスワード、Telnet パスワードの設定」（P.13-1）を参照してください。

Telnet 認証を設定している場合（「CLIおよび ASDM アクセスの認証の設定」（P.35-17）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 アクセスの設定

クライアント IP アドレスを指定して、ASA に SSH を使用して接続できるユーザを定義するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**crypto key generate rsa modulus** *modulus_size* **例：** `ciscoasa(config)# crypto key generate rsa modulus 1024`	SSH に必要な RSA キー ペアが生成されます（物理 ASA の場合のみ）。 **（注）** ASAv 用の RSA キー ペアは、展開後に自動的に作成されます。 係数の値（ビット単位）は 512、768、1024、または 2048 です。指定するキー係数のサイズが大きいほど、RSA キー ペアの生成にかかる時間は長くなります。値は 1024 にすることをお勧めします。
ステップ 2	**write memory** **例：** `ciscoasa(config)# write memory`	RSA キーを永続的なフラッシュ メモリに保存します。
ステップ 3	**aaa authentication ssh console LOCAL**	SSH アクセスのローカル認証をイネーブルにします。AAA サーバを使用して認証を設定することもできます。詳細については、「CLI および ASDM アクセスの認証の設定」（P.35-17）を参照してください。
ステップ 4	**username** *username* **password** *password*	SSH アクセスに使用できるユーザをローカル データベースに作成します。
ステップ 5	**ssh** *source_IP_address mask source_interface* **例：** `ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside`	アドレスまたはサブネットごとに、ASA が接続を許可する IP アドレスと、SSH を実行するインターフェイスを指定します。Telnet と異なり、SSH は最も低いセキュリティ レベルのインターフェイスで実行できます。

	コマンド	目的
ステップ 6	**ssh timeout** *minutes* **例：** ciscoasa(config)# ssh timeout 30	（オプション）ASA がセッションを切断するまでに SSH がアイドル状態を維持する時間の長さを設定します。 タイムアウトは 1 ～ 60 分に設定します。デフォルトは 5 分です。デフォルトの期間では一般に短すぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定しておいてください。
ステップ 7	**ssh version** *version_number* **例：** ciscoasa(config)# ssh version 2	（オプション）SSH バージョン 1 または 2 へのアクセスを制限します。デフォルトでは、SSH はバージョン 1 と 2 の両方を許可します。

例

次の例は、RSA キーを生成し、アドレスが 192.168.1.2 の内部インターフェイス上のホストで ASA にアクセスする方法を示しています。

```
ciscoasa(config)# crypto key generate rsa modulus 1024
ciscoasa(config)# write memory
ciscoasa(config)# aaa authentication ssh console LOCAL
WARNING: local database is empty!Use 'username' command to define local users.
ciscoasa(config)# username exampleuser1 password examplepassword1
ciscoasa(config)# ssh 192.168.1.2 255.255.255.255 inside
ciscoasa(config)# ssh timeout 30
```

次の例は、192.168.3.0/24 のネットワーク上のすべてのユーザが内部インターフェイス上の ASA にアクセスできるようにする方法を示しています。

```
ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside
```

SSH クライアントの使用

管理ホストの SSH クライアントで、「SSH アクセスの設定」（P.35-4）で設定した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.27-3）を参照してください。

ASDM の HTTPS アクセスの設定

ASDM を使用するには、HTTPS サーバをイネーブルにし、ASA への HTTPS 接続を許可する必要があります。HTTPS アクセスは、工場出荷時のデフォルト コンフィギュレーションの一部として、または **setup** コマンドを使用したときにイネーブルになっています。この項では、ASDM アクセスを手動で設定する方法について説明します。

手順の詳細

	コマンド	目的
ステップ 1	**http** *source_IP_address mask source_interface* **例：** `ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside`	アドレスまたはサブネットごとに、ASA が HTTPS 接続を許可する IP アドレスを指定します。
ステップ 2	**http server enable** [*port*] **例：** `ciscoasa(config)# http server enable 443`	HTTPS サーバをイネーブルにします。 デフォルトでは、*port* は 443 です。ポート番号を変更する場合は、必ず ASDM アクセス URL に変更したポート番号を含めてください。たとえば、ポート番号を 444 に変更する場合は、次のように入力します。 **https://10.1.1.1:444**
ステップ 3	**http redirect** *interface* [*port*] **例：** `ciscoasa(config)# http redirect inside`	（オプション）HTTP リクエストを HTTPS リクエストにリダイレクトします。これにより、ユーザは ASDM URL 内に「http://」と入力し、https URL にエラーなしで移動できるようになります。

例

次の例は、HTTPS サーバをイネーブルにし、アドレスが 192.168.1.2 の内部インターフェイス上のホストで ASDM にアクセスする方法を示しています。

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

次の例は、192.168.3.0/24 のネットワーク上のすべてのユーザが内部インターフェイス上の ASDM にアクセスできるようにする方法を示しています。

```
ciscoasa(config)# http 192.168.3.0 255.255.255.0 inside
```

CLI パラメータの設定

- 「CLI パラメータのライセンス要件」（P.35-7）
- 「ガイドラインと制限事項」（P.35-7）
- 「ログイン バナーの設定」（P.35-7）
- 「CLI プロンプトのカスタマイズ」（P.35-8）
- 「コンソール タイムアウトの変更」（P.35-9）

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

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

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

コマンド	目的
banner {**exec** | **login** | **motd**} *text* **例：** ciscoasa(config)# banner motd Welcome to $(hostname).	ユーザが最初に接続したとき（「今日のお知らせ」（**motd**））、ユーザがログインしたとき（**login**）、ユーザが特権 EXEC モードにアクセスしたとき（**exec**）のいずれかに表示するバナーを追加します。ユーザが ASA に接続すると、まず「今日のお知らせ」バナーが表示され、その後にログイン バナーとプロンプトが表示されます。ユーザが ASA に正常にログインすると、exec バナーが表示されます。 複数の行を追加する場合は、各行の前に **banner** コマンドを置きます。 バナー テキストに関する注意事項： • スペースは使用できますが、CLI を使用してタブを入力することはできません。 • バナーの長さの制限は、RAM およびフラッシュ メモリに関するもの以外はありません。 • ASAのホスト名またはドメイン名は、**$(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。

例

次は、「今日のお知らせ」バナーの追加方法の例です。

```
ciscoasa(config)# banner motd Welcome to $(hostname).
ciscoasa(config)# banner motd Contact me at admin@example.com for any
ciscoasa(config)# banner motd issues.
```

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。
context	（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、次のコマンドを入力します。

コマンド	目的
prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]} **例：** `ciscoasa(config)# firewall transparent`	CLI プロンプトをカスタマイズします。

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。接続時間によって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

コマンド	目的
console timeout *number* **例：** `ciscoasa(config)# console timeout 0`	特権セッションが終了するまでのアイドル時間を分単位（0 ～ 60）で指定します。デフォルトのタイムアウトは 0 であり、セッションがタイムアウトしないことを示します。

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端している場合、別のインターフェイスにアクセスして ASA を管理するために、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指定できます。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.35-10）
- 「ガイドラインと制限事項」（P.35-2）
- 「管理インターフェイスの設定」（P.35-11）

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

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

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）　この後の設定では、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

コマンド	目的
management-access *management_interface* **例：** `ciscoasa(config)# management-access inside`	*management_interface* は、別のインターフェイスから ASA に入るときにアクセスする管理インターフェイスの名前を指定します。

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」（P.35-12）
- 「システム管理者用 AAA のライセンス要件」（P.35-15）
- 「前提条件」（P.35-15）
- 「ガイドラインと制限事項」（P.35-16）
- 「デフォルト設定」（P.35-17）
- 「CLIおよび ASDM アクセスの認証の設定」（P.35-17）
- 「特権 EXEC モードにアクセスするための認証の設定（enable コマンド）」（P.35-18）
- 「管理許可によるユーザ CLI および ASDM アクセスの制限」（P.35-20）
- 「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」（P.35-22）
- 「コマンド許可の設定」（P.35-25）
- 「管理アクセス アカウンティングの設定」（P.35-31）
- 「現在のログイン ユーザの表示」（P.35-31）
- 「管理セッション割り当て量の設定」（P.35-32）
- 「SSH セッションでのキーの交換」（P.35-33）
- 「ロックアウトからの回復」（P.35-34）

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」（P.35-12）
- 「コマンド許可に関する情報」（P.35-13）

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.35-12）
- 「認証がある場合とない場合の ASDM アクセスの比較」（P.35-12）
- 「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.35-13）

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（**password** コマンドで設定）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（**enable password** コマンドで設定）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（「特権 EXEC モードにアクセスするための認証の設定（enable コマンド）」（P.35-18）を参照）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。詳細については、「login コマンドによるユーザの認証」（P.35-19）を参照してください。

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 **enable password** コマンドによって設定されたイネーブル 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.35-13）
- 「ユーザ クレデンシャルの維持について」（P.35-14）
- 「セキュリティ コンテキストとコマンド許可」（P.35-14）

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.35-25）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。その後に続く許可では、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、シリアル許可専用（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 許可	特権モード コマンド許可	特権 モード終了 許可
ユーザ名	Yes	×	×	Yes
パスワード	Yes	×	×	Yes
特権モードのパスワード	×	×	Yes	×

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 ユーザの許可が前のコンテキスト セッションでのユーザの許可と異なる場合に、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許可する場合は、**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.27-3）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.35-1）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および ASDM アクセスの認証の設定」（P.35-17）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.30-5）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 を設定します（「CLIおよび ASDM アクセスの認証の設定」（P.35-17）を参照）。
- **enable** 認証を設定します（「特権 EXEC モードにアクセスするための認証の設定（enable コマンド）」（P.35-18）を参照）。

管理アカウンティングの前提条件

- CLI を設定します（「CLIおよび ASDM アクセスの認証の設定」（P.35-17）を参照）。
- **enable** 認証を設定します（「特権 EXEC モードにアクセスするための認証の設定（enable コマンド）」（P.35-18）を参照）。

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

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.35-28）を参照してください。

CLIおよび ASDM 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.35-1）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

	コマンド	目的
ステップ 1	**aaa authentication** {**telnet** | **ssh** | **http** | **serial**} **console** {**LOCAL** | *server_group* [**LOCAL**]} **例：** ciscoasa(config)# aaa authentication ssh console radius_1 LOCAL ciscoasa(config)# aaa authentication http console radius_1 LOCAL ciscoasa(config)# aaa authentication serial console LOCAL	管理アクセス用のユーザを認証します。**telnet** キーワードを使用すると、Telnet アクセスを制御できます。ASASM の場合、このキーワードは **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.35-13）を参照してください。 **ssh** キーワードを使用すると、SSH アクセスを制御できます。 **http** キーワードを使用すると、ASDM アクセスを制御できます。 **serial** キーワードを使用すると、コンソール ポート アクセスを制御できます。ASASM の場合、このキーワードは **service-module** 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.35-13）を参照してください。 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。 認証に AAA サーバ グループを使用する場合は、AAA サーバが使用できないときにローカル データベースをフォールバック方式として使用するように ASA を設定できます。サーバ グループ名の後ろに **LOCAL** を指定します（**LOCAL** は大文字と小文字を区別します）。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。 **LOCAL** だけを入力して、ローカル データベースを認証の主要方式として（フォールバックなしで）使用することもできます。
ステップ 2	**http authentication-certificate** *interface* **例：** http authentication-certificate inside	指定したインターフェイス上で HTTP 経由で接続している ASDM クライアントからの証明書を要求します。ASDM 用の **aaa authentication** コマンドに加えて、このコマンドも使用できます。 このコマンドは ASDM アクセス専用であり、コマンド **ssl certificate-authentication** を使用して、カットスルー プロキシなどその他のすべての SSL トラフィックの証明書を要求します。

特権 EXEC モードにアクセスするための認証の設定（enable コマンド）

ユーザが **enable** コマンドを入力したときに AAA サーバまたはローカル データベースでそれらのユーザを認証するようにASAを設定することができます。あるいは、ユーザは **login** コマンドを入力したときにローカル データベースで自動的に認証されます。この場合も、ローカル データベース内のユーザ レベルに応じて特権 EXEC モードにアクセスします。

- 「enable コマンドの認証の設定」（P.35-19）
- 「login コマンドによるユーザの認証」（P.35-19）

enable コマンドの認証の設定

ユーザが **enable** コマンドを入力したときに認証されるように、ASAを設定できます。詳細については、「認証がある場合とない場合の CLI アクセスの比較」（P.35-12）を参照してください。

enable コマンドの入力時にユーザを認証するには、次のコマンドを入力します。

コマンド	目的
aaa authentication enable console {**LOCAL** | *server_group* [**LOCAL**]} **例：** `ciscoasa(config)# aaa authentication enable console LOCAL`	**enable** コマンドを入力したユーザを認証します。ユーザ名とパスワードの入力を求めるプロンプトがユーザに対して表示されます。 認証に AAA サーバ グループを使用する場合は、AAA サーバが使用できないときにローカル データベースをフォールバック方式として使用するように ASA を設定できます。サーバ グループ名の後ろに **LOCAL** を指定します（**LOCAL** は大文字と小文字を区別します）。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。 **LOCAL** だけを入力して、ローカル データベースを認証の主要方式として（フォールバックなしで）使用することもできます。

login コマンドによるユーザの認証

ユーザ EXEC モードから、**login** コマンドを使用してローカル データベース内のユーザ名でログインすることができます。

この機能を使用すると、ユーザは独自のユーザ名とパスワードでログインして特権 EXEC モードにアクセスすることができるので、システム イネーブル パスワードを全員に提供する必要がなくなります。ユーザがログイン時に特権 EXEC モード（およびすべてのコマンド）にアクセスできるようにするには、ユーザの特権レベルを 2（デフォルト）～ 15 に設定します。ローカル コマンド許可を設定した場合、ユーザは、その特権レベル以下のレベルに割り当てられているコマンドのみを入力できます。詳細については、「ローカル コマンド許可の設定」（P.35-25）を参照してください。

注意　CLI にアクセスできるユーザや特権 EXEC モードを開始できないようにするユーザをローカル データベースに追加する場合は、コマンド許可を設定する必要があります。コマンド許可がない場合、特権レベルが 2 以上（2 がデフォルト）のユーザは、CLI で自分のパスワードを使用して特権 EXEC モード（およびすべてのコマンド）にアクセスできます。あるいは、認証処理で AAA サーバを使用するか、またはすべてのローカル ユーザをレベル 1 に設定することにより、システム イネーブル パスワードを使用して特権 EXEC モードにアクセスできるユーザを制御できます。

ローカル データベースからユーザとしてログインするには、次のコマンドを入力します。

コマンド	目的
login **例：** `ciscoasa# login`	ローカル データベースからユーザとしてログインします。ASA により、ユーザ名とパスワードの入力を求めるプロンプトが表示されます。パスワードを入力すると、ASA により、ユーザはローカル データベースで指定されている特権レベルに置かれます。

管理許可によるユーザ 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 アクセスは管理許可に含まれないため、**aaa authentication serial console**コマンドを設定している場合は、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　ローカル、RADIUS、LDAP（マッピング済み）、および TACACS+ ユーザの管理許可をイネーブルとするには、次のコマンドを入力します。

```
ciscoasa(config)# aaa authorization exec {authentication-server | LOCAL} [auto-enable]
```

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.35-25）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。

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。

管理許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　ユーザを管理許可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、特定の許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 map-attributes** コマンドを使用して 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.30-5）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）: **aaa authentication console** コマンド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）: **aaa authentication {telnet | ssh} console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は 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。**aaa authentication enable console** コマンド **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 **aaa authentication console** コマンドで指定されたサービスを使用できません（**serial** キーワードを除きます。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。

次の例は、LDAP 属性マップを定義する方法を示しています。この例では、セキュリティ ポリシーによって、LDAP によって認証されているユーザが、ユーザ レコードのフィールドまたはパラメータの title と company を、IETF-RADIUS service-type と privilege-level にそれぞれマップすることを指定しています。

```
ciscoasa(config)# ldap attribute-map admin-control
ciscoasa(config-ldap-attribute-map)# map-name title IETF-RADIUS-Service-Type
ciscoasa(config-ldap-attribute-map)# map-name company Privilege-Level
```

次の例では、LDAP 属性マップを LDAP AAA サーバに適用します。

```
ciscoasa(config)# aaa-server ldap-server (dmz1) host 10.20.30.1
ciscoasa(config-aaa-server-host)# ldap-attribute-map admin-control
```

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：設定およびモニタリング セクションへの限定的な読み取り専用アクセス権で ASDM へのアクセスと、権限レベル 1 の **show** コマンドのみへのアクセスを許可します。
- PASS、特権レベル 2 以上：**aaa authentication {telnet | ssh} console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は 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。**aaa authentication enable console** コマンド **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。**aaa authentication console** コマンドで指定されたサービスを使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。

ローカル ユーザ

指定したユーザ名に対する **service-type** コマンドを設定します。デフォルトの **service-type** は **admin** で、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。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.27-3）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.35-22）
- 「パスワードの変更」（P.35-24）

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、**username** コマンドおよび **change-password** コマンド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および ASDM アクセスの認証の設定」（P.35-17）に従って、CLI/ASDM 認証を設定します。ローカル データベースの指定を忘れないでください。
- 「特権 EXEC モードにアクセスするための認証の設定（enable コマンド）」（P.35-18）にしたがって、enable 認証を設定します。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

	コマンド	目的
ステップ 1	**password-policy lifetime** *days* **例：** ciscoasa(config)# password-policy lifetime 180	（オプション）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設定します。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 **username** コマンドを使用して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。
ステップ 2	**password-policy minimum-changes** *value* **例：** ciscoasa(config)# password-policy minimum-changes 2	（オプション）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設定します。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	**password-policy minimum-length** *value* **例：** ciscoasa(config)# password-policy minimum-length 8	（オプション）パスワードの最小長を設定します。有効な値は、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。
ステップ 4	**password-policy minimum-uppercase** *value* **例：** ciscoasa(config)# password-policy minimum-uppercase 3	（オプション）パスワードに含める大文字の最小個数を設定します。有効な値は、0 ～ 64 文字です。デフォルト値は、最小個数がないことを意味する 0 です。
ステップ 5	**password-policy minimum-lowercase** *value* **例：** ciscoasa(config)# password-policy minimum-lowercase 6	（オプション）パスワードに含める小文字の最小個数を設定します。有効な値は、0 ～ 64 文字です。デフォルト値は、最小個数がないことを意味する 0 です。

	コマンド	目的
ステップ 6	**password-policy minimum-numeric** *value* **例：** ciscoasa(config)# password-policy minimum-numeric 1	（オプション）パスワードに含める数字の最小個数を設定します。有効な値は、0 ～ 64 文字です。デフォルト値は、最小個数がないことを意味する 0 です。
ステップ 7	**password-policy minimum-special** *value* **例：** ciscoasa(config)# password-policy minimum-special 2	（オプション）パスワードに含める特殊文字の最小個数を設定します。有効な値は、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、最小個数がないことを意味する 0 です。

ステップ 8	**password-policy authenticate enable**
	
	例：
	ciscoasa(config)# password-policy authenticate enable
		（オプション）ユーザが自分のパスワードの変更に **username** コマンドではなく **change-password** コマンドを使用する必要があるかを設定します。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した場合、**username** コマンドを使用してパスワードを変更しようとすると、次のエラー メッセージが表示されます。
		
		`ERROR: Changing your own password is prohibited`
		
		clear configure username コマンドを使用して自分のアカウントを消去することもできません。消去を試みた場合は、次のエラー メッセージが表示されます。
		
		`ERROR: You cannot delete all usernames because you are not allowed to delete yourself`

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 **username** 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（**password-policy authenticate enable** コマンド）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、**username** コマンド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

コマンド	目的
change-password [**old-password** *old_password* [**new-password** *new_password*]] **例：** hostname# change-password old-password j0hncr1chton new-password a3rynsun	自分の **username** パスワードを変更します。コマンドに新旧のパスワードを入力していない場合は、ASA によって入力が求められます。

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.35-13）を参照してください。

- 「ローカル コマンド許可の設定」（P.35-25）
- 「ローカル コマンド特権レベルの表示」（P.35-28）
- 「TACACS+ サーバでのコマンドの設定」（P.35-29）
- 「TACACS+ コマンド許可の設定」（P.35-30）

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.27-3）
- 「サポートされている認証方式」（P.28-2）
- 「LDAP 属性マップの設定」（P.30-5）

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

	コマンド	目的
ステップ 1	**privilege** [**show** | **clear** | **cmd**] **level** *level* [**mode** {**enable** | **cmd**}] **command** *command* **例：** `ciscoasa(config)# privilege show level 5 command filter`	特権レベルにコマンドを割り当てます。 再割り当てする各コマンドに対してこのコマンドを繰り返します。 このコマンドのオプションは、次のとおりです。 • **show | clear | cmd**：これらのオプション キーワードを使用すると、コマンドの show、clear、または configure 形式に対してだけ特権を設定できます。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。これらのキーワードのいずれかを使用しない場合は、コマンドのすべての形式が影響を受けます。 • **level** *level*：0 ～ 15 のレベル。 • **mode** {**enable | configure**}：ユーザ EXEC モードまたは特権 EXEC モードおよびコンフィギュレーション モードでコマンドを入力することができ、そのコマンドが各モードで異なるアクションを実行する場合は、それらのモードの特権レベルを個別に設定することができます。 – **enable**：ユーザ EXEC モードと特権 EXEC モードの両方を指定します。 – **configure**：**configure terminal** コマンドを使用してアクセスされるコンフィギュレーション モードを指定します。 • **command** *command*：設定しているコマンド。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。

	コマンド	目的
ステップ 2	**aaa authorization exec authentication-server** **例：** ciscoasa(config)# aaa authorization exec authentication-server	RADIUS からの管理ユーザ特権レベルをサポートします。 管理アクセスを認証するユーザに、ユーザ固有のアクセス レベルを強制します（**aaa authentication console LOCAL** コマンドを参照）。 このコマンドを入力しない場合、ASA は、ローカル データベース ユーザの特権レベルだけをサポートし、他のタイプのユーザをすべてデフォルトでレベル 15 に割り当てます。 このコマンドは、ローカル、RADIUS、LDAP（マッピング済み）、および TACACS+ の各ユーザの管理許可もイネーブルにします。 **aaa authorization exec LOCAL** コマンドを使用して、ローカル データベースから属性を取得できるようにします。管理許可が有効になるように AAA サーバのユーザを設定する方法については、「管理許可によるユーザ CLI および ASDM アクセスの制限」（P.35-20）を参照してください。
ステップ 3	**aaa authorization command LOCAL** **例：** ciscoasa(config)# aaa authorization command LOCAL	ローカル コマンドの特権レベルの使用をイネーブルにします。ローカル コマンドの特権レベルを使用すると、ローカル データベース、RADIUS サーバ、または LDAP サーバ（マッピングされた属性を持つ）のユーザの特権レベルと比較して検査できます。 コマンド特権レベルを設定する場合は、このコマンドでコマンド許可を設定しない限り、コマンド許可は実行されません。

例

filter コマンドの形式は次のとおりです。

- **filter**（**configure** オプションで表されます）
- **show running-config filter**
- **clear configure filter**

特権レベルを形式ごとに個別に設定することができます。または、このオプションを省略してすべての形式に同じ特権レベルを設定することもできます。次は、各形式を個別に設定する方法の例です。

```
ciscoasa(config)# privilege show level 5 command filter
ciscoasa(config)# privilege clear level 10 command filter
ciscoasa(config)# privilege cmd level 10 command filter
```

また、次の例では、すべての filter コマンドを同じレベルに設定する例を示します。

```
ciscoasa(config)# privilege level 5 command filter
```

show privilege コマンドは、形式を分けて表示します。

次の例では、**mode** キーワードの使用方法を示します。**enable** コマンドは、ユーザ EXEC モードから入力する必要があります。一方、**enable password** コマンドは、コンフィギュレーション モードでアクセスでき、最も高い特権レベルが必要です。

```
ciscoasa(config)# privilege cmd level 0 mode enable command enable
ciscoasa(config)# privilege cmd level 15 mode cmd command enable
ciscoasa(config)# privilege show level 15 mode cmd command enable
```

次に、**mode** キーワードを使用して、**configure** コマンドにレベルを設定する例を示します。

```
ciscoasa(config)# privilege show level 5 mode cmd command configure
ciscoasa(config)# privilege clear level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode enable command configure
```

（注）　この最後の行は、**configure terminal** コマンドで使用します。

ローカル コマンド特権レベルの表示

次のコマンドをコマンドの特権レベルを表示できます。

コマンド	目的
show running-config all privilege all	すべてのコマンドを表示します。
show running-config privilege level *level*	特定のレベルのコマンドを表示します。*level* は 0 ～ 15 の整数です。
show running-config privilege command *command*	特定のコマンドのレベルを表示します。

例

たとえば、**show running-config all privilege all** コマンドの場合、ASA は特権レベルに対する各 CLI コマンドの現在の割り当てを表示します。次に、このコマンドの出力例を示します。

```
ciscoasa(config)# show running-config all privilege all
privilege show level 15 command aaa
privilege clear level 15 command aaa
privilege configure level 15 command aaa
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
privilege show level 15 command activation-key
privilege configure level 15 command activation-key
....
```

次の例は、特権レベル 10 に対するコマンド割り当てを示しています。

```
ciscoasa(config)# show running-config privilege level 10
privilege show level 10 command aaa
```

次の例は、**access-list** コマンドに対するコマンド割り当てを示しています。

```
ciscoasa(config)# show running-config privilege command access-list
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
```

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」コマンドとして許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、**show** コマンドのみを設定と、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。

- **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*。

- 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。

- 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。

- 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、コマンドが許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許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.35-34）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.35-25）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、次のコマンドを入力します。

手順の詳細

コマンド	目的
aaa authorization command *tacacs+_server_group* [**LOCAL**] **例：** `ciscoasa(config)# aaa authorization command group_1 LOCAL`	TACACS+ サーバを使用してコマンド許可を実行します。 TACACS+ サーバを使用できない場合は、ローカル データベースをフォールバック方式として使用するように ASA を設定できます。フォールバックをイネーブルにするには、サーバ グループ名の後ろに **LOCAL** を指定します（**LOCAL** は大文字と小文字を区別します）。ASA は、どちらの方式を使用しているかを示すプロンプトを表示しないため、ローカル データベースと TACACS+ サーバで同じユーザ名とパスワードを使用することをお勧めします。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.27-3）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.35-25）を参照）を設定してください。

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

	コマンド	目的
ステップ 1	**aaa accounting** {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag* **例：** `ciscoasa(config)# aaa accounting telnet console group_1`	管理アクセスに対する AAA アカウンティングのサポートをイネーブルにします。 有効なサーバ グループ プロトコルは RADIUS と TACACS+ です。
ステップ 2	**aaa accounting command** [**privilege** *level*] *server-tag* **例：** `ciscoasa(config)# aaa accounting command privilege 15 group_1`	コマンド アカウンティングをイネーブルにします。TACACS+ サーバだけがコマンド アカウンティングをサポートします。 **privilege** *level* は最小特権レベルで、*server-tag* は、ASA がコマンド アカウンティング メッセージを送信する TACACS+ サーバ グループの名前です。

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、次のコマンドを入力します。

```
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 35-1 に、**show curpriv** コマンドの出力の説明を示します。

表 35-1　　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、次のコマンドを入力します。

コマンド	目的
quota management-session *number* **例：** `hostname(config)# quota management-session 1000`	ASA で許可する ASDM、SSH、および Telnet の同時最大セッション数を設定します。このコマンドの **no** 形式を使用すると、クォータ値が 0 に設定されます。これは、セッション数の制限がないことを意味します。

SSH セッションでのキーの交換

Diffie-Hellman（DH）キー交換は、いずれかの当事者単独では決定できない共有秘密を提供します。キー交換は署名とホストキーを組み合わせてホスト認証を提供します。このキー交換方式により、明示的なサーバ認証が可能となります。

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。

SSH セッションでキーを交換するには、次のコマンドを入力します。

コマンド	目的

ssh key-exchange group {**dh-group1** | **dh-group14**} **sha-1**
 	
例：
`ciscoasa(config)# ssh key-exchange group dh-group14 sha-1`
`ciscoasa# show running-config key-exchange`
`ssh key-exchange dh-group14-sha1`
	DH グループ 1 または DH グループ 14 のキー交換方式を使用してキーを交換します。
	
	key-exchange キーワードは、DH グループ 1 または DH グループ 14 キー交換方式のいずれかが続き、キーを交換するときにこれを使用する必要があることを指定します。
	
	group キーワードは、DH グループ 1 キー交換方式または DH グループ 14 キー交換方式のいずれかが続き、キーを交換するときにこれを使用する必要があることを示します。
	
	dh-group1 キーワードは、DH グループ 1 キー交換方式が続き、キーを交換するときにこれを使用する必要があることを示します。DH グループ 2 は、レガシーの理由で DH グループ 1 と呼ばれます。
	
	dh-group14 キーワードは、DH グループ 14 キー交換方式が続き、キーを交換するときにこれを使用する必要があることを示します。
	
	sha-1 キーワードは、SHA-1 暗号化アルゴリズムを使用する必要があることを示します。
	
	現在使用されている DH グループ キー交換方式を表示するには、**show running-config ssh key-exchange** コマンドを使用します。

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 35-2 に、一般的なロックアウト条件と回復方法を示します。

表 35-2　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。
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。

表 35-2　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	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。

管理アクセスの機能履歴

表 35-3 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。

表 35-3　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。 次のコマンドを導入しました。 **show running-config all privilege all、show running-config privilege level、show running-config privilege command、telnet、telnet timeout、ssh、ssh timeout、http、http server enable、asdm image disk、banner、console timeout、icmp、ipv6 icmp、management access、aaa authentication console、aaa authentication enable console、aaa authentication telnet | ssh console、service-type、login、privilege、aaa authentication exec authentication-server、aaa authentication command LOCAL、aaa accounting serial | telnet | ssh | enable console、show curpriv、aaa accounting command privilege**。

表 35-3　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
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。
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。 次のコマンドが導入されました。**change-password**、**password-policy lifetime**、**password-policy minimum changes**、**password-policy minimum-length**、**password-policy minimum-lowercase**、**password-policy minimum-uppercase**、**password-policy minimum-numeric**、**password-policy minimum-special**、**password-policy authenticate enable**、**clear configure password-policy**、**show running-config 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。 次のコマンドを導入しました。**ssh authentication** *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。 次のコマンドが導入されました。**ssh key-exchange**。

表 35-3　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
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。 次のコマンドが導入されました。**quota management-session**、**show running-config quota management-session**、**show quota management-session**。
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。 次のコマンドが導入されました。**show ssh sessions detail**。
改善されたワンタイム パスワード認証	9.2(1)	十分な許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。 次のコマンドが変更されました。**aaa authorization exec**。

CHAPTER 36

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」（P.36-1）
- 「ファイルの管理」（P.36-12）
- 「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」（P.36-22）
- 「イメージをロードするための ROM モニタの使用」（P.36-23）
- 「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.36-27）
- 「ソフトウェアのダウングレード」（P.36-36）
- 「Auto Update の設定」（P.36-38）
- 「ソフトウェアとコンフィギュレーションの機能履歴」（P.36-45）

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」（P.36-1）
- 「現在のバージョンの表示」（P.36-3）
- 「Cisco.com からのソフトウェアのダウンロード」（P.36-3）
- 「スタンドアロン ユニットのアップグレード」（P.36-4）
- 「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.36-5）

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（Cisco ASA 5500 バージョン 8.3 への移行ガイド）*』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 36-1 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 36-1　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。
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

ご使用の ASA のソフトウェア バージョンを確認するには、**show version** コマンドを使用します。

Cisco.com からのソフトウェアのダウンロード

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

この手順は、イメージを TFTP サーバに置くことを前提としていますが、その他のサーバ タイプもサポートされます。

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。

手順

この手順では、TFTP を使用します。FTP または HTTP の場合は、**copy** コマンドを参照してください。

ステップ 1　（コンフィギュレーション移行がある場合）コンフィギュレーションをバックアップできるようにするために、コンフィギュレーションを端末に表示します。

more system:running-config

このコマンドの出力をコピーし、テキスト ファイルにコンフィギュレーションを貼り付けます。その他のバックアップ方法については、コンフィギュレーション ガイドを参照してください。

ステップ 2　ASA ソフトウェアをアクティブ装置のフラッシュ メモリにコピーします。

copy tftp://*server*[/*path*]/*asa_image_name* {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

例：

```
ciscoasa# copy tftp://10.1.1.1/asa931-smp-k8.bin disk0:/asa931-smp-k8.bin
```

TFTP 以外の方法の場合は、**copy** コマンドを参照してください。

ステップ 3　ASDM イメージをアクティブ装置のフラッシュ メモリにコピーします。

copy tftp://*server*[/*path*]/*asdm_image_name* {**disk0:/** | **disk1:/**}[*path*/]*asdm_image_name*

例：

```
ciscoasa# copy tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

ステップ 4　まだグローバル コンフィギュレーション モードを開始していない場合は、グローバル コンフィギュレーション モードを開始します。

configure terminal

ステップ 5　設定されている現在のブート イメージを表示します（最大 4 個）。

show running-config boot system

例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa914-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭になるように指定するには、既存のエントリをすべて削除してから、ステップ 6 およびステップ 7 に従ってイメージの URL を目的の順序で入力します。

ステップ 6　既存のブート イメージ コンフィギュレーションがある場合は削除します。新しいブート イメージを最初の選択肢として入力できるようにするためです。

no boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

例：

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa914-smp-k8.bin
```

ステップ 7　ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

例：

```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、前のステップ 6 で削除したイメージを再入力できます。

ステップ 8　使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image {**disk0:/** | **disk1:/**}[*path*/]*asdm_image_name*

例：

```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```

使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 9　新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

ステップ 10　ASA をリロードします。

reload

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」（P.36-5）
- 「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」（P.36-8）
- 「ASA クラスタのアップグレード」（P.36-10）

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。

はじめる前に

アクティブ装置で次の手順を実行します。

手順

ステップ 1　（コンフィギュレーション移行がある場合）コンフィギュレーションをバックアップできるようにするために、コンフィギュレーションを端末に表示します。

more system:running-config

例：

```
active# more system:running-config
```

このコマンドの出力をコピーし、テキスト ファイルにコンフィギュレーションを貼り付けます。その他のバックアップ方法については、コンフィギュレーション ガイドを参照してください。

ステップ 2　ASA ソフトウェアをアクティブ装置のフラッシュ メモリにコピーします。

copy tftp://*server*[/*path*]/*asa_image_name* {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

例：

```
active# copy tftp://10.1.1.1/asa931-smp-k8.bin disk0:/asa931-smp-k8.bin
```

TFTP 以外の方法の場合は、**copy** コマンドを参照してください。

ステップ 3　ソフトウェアをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm tftp://*server*[/*path*]/*filename* {**disk0:/** | **disk1:/**}[*path*/]*filename*

例：

```
active# failover exec mate copy /noconfirm tftp://10.1.1.1/asa931-smp-k8.bin
disk0:/asa931-smp-k8.bin
```

ステップ 4　ASDM イメージをアクティブ装置のフラッシュ メモリにコピーします。

copy tftp://*server*[/*path*]/*asdm_image_name* {**disk0:/** | **disk1:/**}[*path*/]*asdm_image_name*

例：

```
active# copy tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

ステップ 5　ASDM イメージをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm tftp://*server*[/*path*]/*asdm_image_name* {**disk0:/** | **disk1:/**}[*path*/]*asdm_image_name*

例：

```
active# failover exec mate copy /noconfirm tftp://10.1.1.1/asdm-731.bin
disk0:/asdm-731.bin
```

ステップ 6　まだグローバル コンフィギュレーション モードを開始していない場合は、グローバル コンフィギュレーション モードを開始します。

configure terminal

ステップ 7　設定されている現在のブート イメージを表示します（最大 4 個）。

show running-config boot system

例：

```
ciscoasa(config)# show running-config boot system
```

```
boot system disk0:/cdisk.bin
boot system disk0:/asa921-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭になるように指定するには、既存のエントリをすべて削除してから、ステップ 8 およびステップ 9 に従ってイメージの URL を目的の順序で入力します。

ステップ 8　既存のブート イメージ コンフィギュレーションがある場合は削除します。新しいブート イメージを最初の選択肢として入力できるようにするためです。

no boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

例：

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa921-smp-k8.bin
```

ステップ 9　ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

例：

```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、前のステップ 8 で削除したイメージを再入力できます。

ステップ 10　使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image {**disk0:/** | **disk1:/**}[*path*/]*asdm_image_name*

例：

```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```

使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 11　新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

ステップ 12　スタンバイ装置をリロードして新しいイメージを起動します。

failover reload-standby

スタンバイ装置のロードが完了するまで待ちます。**show failover** コマンドを使用して、スタンバイ装置が Standby Ready 状態かどうかを検証します。

ステップ 13　強制的にアクティブ装置からスタンバイ装置へのフェールオーバーを行います。

no failover active

ステップ 14　以前アクティブであった装置（現在は新しいスタンバイ装置）をリロードします。

reload

リロード後にこの装置を再びアクティブにする場合は、**failover active** コマンドを入力します。

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。また、これらの手順を*プライマリ*装置で実行します。

手順

ステップ 1　（コンフィギュレーション移行がある場合）コンフィギュレーションをバックアップできるようにするために、コンフィギュレーションを端末に表示します。

more system:running-config

このコマンドの出力をコピーし、テキスト ファイルにコンフィギュレーションを貼り付けます。その他のバックアップ方法については、コンフィギュレーション ガイドを参照してください。

ステップ 2　ASA ソフトウェアをプライマリ装置のフラッシュ メモリにコピーします。

copy tftp://*server*[**/***path*]**/***asa_image_name* {**disk0:/** | **disk1:/**}[*path***/**]*asa_image_name*

例：

```
primary# copy tftp://10.1.1.1/asa931-smp-k8.bin disk0:/asa931-smp-k8.bin
```

TFTP 以外の方法の場合は、**copy** コマンドを参照してください。

ステップ 3　ソフトウェアをセカンダリ装置にコピーします。プライマリ装置で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm tftp://*server*[**/***path*]**/***filename* {**disk0:/** | **disk1:/**}[*path***/**]*filename*

例：

```
primary# failover exec mate copy /noconfirm tftp://10.1.1.1/asa931-smp-k8.bin
disk0:/asa931-smp-k8.bin
```

ステップ 4　ASDM イメージをプライマリ装置のフラッシュ メモリにコピーします。

copy tftp://*server*[**/***path*]**/***asdm_image_name* {**disk0:/** | **disk1:/**}[*path***/**]*asdm_image_name*

例：

```
primary# copy tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

ステップ 5　ASDM イメージをセカンダリ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm tftp://*server*[**/***path*]**/***asdm_image_name* {**disk0:/** | **disk1:/**}[*path***/**]*asdm_image_name*

例：

```
primary# failover exec mate copy /noconfirm tftp://10.1.1.1/asdm-731.bin
disk0:/asdm-731.bin
```

ステップ 6　プライマリ装置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。

```
failover active group 1
failover active group 2
```

ステップ 7　まだグローバル コンフィギュレーション モードを開始していない場合は、グローバル コンフィギュレーション モードを開始します。

configure terminal

例：

```
primary(config)# configure terminal
```

ステップ 8　設定されている現在のブート イメージを表示します（最大 4 個）。

show running-config boot system

例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa921-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭になるように指定するには、既存のエントリをすべて削除してから、ステップ 9 およびステップ 10 に従ってイメージの URL を目的の順序で入力します。

ステップ 9　既存のブート イメージ コンフィギュレーションがある場合は削除します。新しいブート イメージを最初の選択肢として入力できるようにするためです。

no boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

例：

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa921-smp-k8.bin
```

ステップ 10　ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

例：

```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、前のステップ 9 で削除したイメージを再入力できます。

ステップ 11　使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image {**disk0:/** | **disk1:/**}[*path*/]*asdm_image_name*

例：

```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```

使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 12　新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

ステップ 13　セカンダリ装置をリロードして新しいイメージを起動します。

failover reload-standby

セカンダリ装置のロードが完了するまで待ちます。**show failover** コマンドを使用して、両方のフェールオーバー グループが Standby Ready 状態であることを確認します。

ステップ 14　セカンダリ装置で、両方のフェールオーバー グループを強制的にアクティブにします。

```
no failover active group 1
no failover active group 2
```

ステップ 15　プライマリ装置をリロードします。

```
reload
```

フェールオーバー グループは、**preempt** コマンド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。フェールオーバー グループが **preempt** コマンドによって設定されていない場合は、**failover active group** コマンドを使用して、指定された装置でそれらのステータスをアクティブ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　（コンフィギュレーション移行がある場合）コンフィギュレーション ファイルをバックアップします。

```
more system:running-config
```

このコマンドの出力をコピーし、テキスト ファイルにコンフィギュレーションを貼り付けます。その他のバックアップ方法については、一般的な操作の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 2　ASA ソフトウェアをクラスタ内のすべての装置にコピーします。

cluster exec copy /noconfirm tftp://*server*[*/path*]*/asa_image_name* {**disk0:/** | **disk1:/**}[*path/*]*asa_image_name*

例：

```
master# cluster exec copy /noconfirm tftp://10.1.1.1/asa931-smp-k8.bin
disk0:/asa931-smp-k8.bin
```

TFTP 以外の方法の場合は、**copy** コマンドを参照してください。

ステップ 3　ASDM イメージをクラスタ内のすべての装置にコピーします。

cluster exec copy /noconfirm tftp://*server*[*/path*]*/asdm_image_name* {**disk0:/** | **disk1:/**}[*path/*]*asdm_image_name*

例：

```
master# cluster exec copy /noconfirm tftp://10.1.1.1/asdm-731.bin disk0:/asdm-731.bin
```

ステップ 4　まだグローバル コンフィギュレーション モードを開始していない場合は、グローバル コンフィギュレーション モードを開始します。

```
configure terminal
```

ステップ 5　設定されている現在のブート イメージを表示します（最大 4 個）。

show running-config boot system

例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa921-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭になるように指定するには、既存のエントリをすべて削除してから、ステップ 6 およびステップ 7 に従ってイメージの URL を目的の順序で入力します。

ステップ 6　既存のブート イメージ コンフィギュレーションがある場合は削除します。新しいブート イメージを最初の選択肢として入力できるようにするためです。

no boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

例：

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa921-smp-k8.bin
```

ステップ 7　ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system {**disk0:/** | **disk1:/**}[*path*/]*asa_image_name*

例：

```
ciscoasa(config)# boot system disk0://asa931-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、前のステップ 6 で削除したイメージを再入力できます。

ステップ 8　使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image {**disk0:/** | **disk1:/**}[*path*/]*asdm_image_name*

例：

```
ciscoasa(config)# asdm image disk0:/asdm-731.bin
```

使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 9　新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

ステップ 10　各ユニット名に対してこのコマンドを繰り返す場合は、スレーブ装置を 1 台ずつリロードします。

cluster exec unit *slave-unit* **reload noconfirm**

例：

```
master# cluster exec unit unit2 reload noconfirm
```

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。メンバ名を一覧表示するには、**cluster exec unit ?** と入力するか、**show cluster info** コマンドを入力します。

ステップ 11　マスター装置でクラスタリングをディセーブルにします。

```
no enable
```

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。**write memory** を入力しないでください。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 12　マスター装置をリロードします。

```
reload noconfirm
```

新しいマスターの選定が実行されて、新しいマスター装置が決定します。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。

ファイルの管理

- 「フラッシュ メモリ内のファイルの表示」（P.36-12）
- 「フラッシュ メモリからのファイルの削除」（P.36-13）
- 「フラッシュ ファイル システムの消去」（P.36-13）
- 「ファイル アクセスの設定」（P.36-13）
- 「ASA へのファイルのコピー」（P.36-17）
- 「スタートアップ コンフィギュレーションまたは実行コンフィギュレーションへのファイルのコピー」（P.36-20）

フラッシュ メモリ内のファイルの表示

次のように、フラッシュ メモリ内のファイルを表示して、そのファイルに関する情報を表示することもできます。

- フラッシュ メモリ内のファイルを表示するには、次のコマンドを入力します。

  ```
  ciscoasa# dir [disk0: | disk1:]
  ```

  内部フラッシュ メモリの場合、**disk0:** と入力します。**disk1:** キーワードは外部フラッシュ メモリを表します。デフォルトは、内部フラッシュ メモリです。

  次に例を示します。

  ```
  hostname# dir

  Directory of disk0:/
  500    -rw-  4958208     22:56:20 Nov 29 2004  cdisk.bin
  2513   -rw-  4634        19:32:48 Sep 17 2004  first-backup
  2788   -rw-  21601       20:51:46 Nov 23 2004  backup.cfg
  2927   -rw-  8670632     20:42:48 Dec 08 2004  asdmfile.bin
  ```

- 特定のファイルに関する拡張情報を表示するには、次のコマンドを入力します。

  ```
  hostname# show file information [path:/]filename
  ```

  デフォルト パスは、内部フラッシュ メモリのルート ディレクトリ（disk0:/）です。

次に例を示します。

```
hostname# show file information cdisk.bin

disk0:/cdisk.bin:
type is image (XXX) []
  file size is 4976640 bytes version 7.0(1)
```

示されているファイル サイズは例にすぎません。

フラッシュ メモリからのファイルの削除

不要になったファイルはフラッシュ メモリから削除できます。フラッシュ メモリからファイルを削除するには、次のコマンドを入力します。

```
hostname# delete disk0: filename
```

パスを指定しないと、デフォルトでは、ファイルは現在の作業ディレクトリから削除されます。ファイルを削除するときは、ワイルドカードを使用できます。削除するファイル名が表示されます。その後、削除を確定する必要があります。

フラッシュ ファイル システムの消去

フラッシュ ファイル システムを消去するには、次の手順を実行します。

ステップ 1　「ASA サービス モジュール コンソールへのアクセス」（P.2-3）または「アプライアンス コンソールへのアクセス」（P.2-2）に従って、ASA のコンソール 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　スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。

ステップ 4　非表示のシステム ファイルを含め、すべてのファイルを上書きしてファイル システムを消去する **erase** コマンドを入力します。

```
rommon #1> erase [disk0: | disk1: | flash:]
```

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.36-14）
- 「セキュア コピー サーバとしての ASA の設定　」（P.36-14）
- 「ASA セキュア コピー クライアントのカスタマイズ」（P.36-15）
- 「ASA TFTP クライアントのパス設定」（P.36-17）

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

コマンド	目的
ftp mode passive **例：** `ciscoasa(config)# ftp mode passive`	FTP モードをパッシブに設定します。

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

- 「SSH アクセスの設定」（P.35-4）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

コマンド	目的
ssh scopy enable **例：** `ciscoasa(config)# ssh scopy enable`	SCP サーバをイネーブルにします。

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（「ASA へのファイルのコピー」（P.36-17）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。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	**[no] ssh stricthostkeycheck** **例：** ciscoasa# ssh stricthostkeycheck ciscoasa# copy x scp://cisco@10.86.95.9/x The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established. RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a. Are you sure you want to continue connecting (yes/no)?**yes** Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts. Source filename [x]? Address or name of remote host [10.86.95.9]? Destination username [cisco]? Destination password []?cisco123 Destination filename [x]?	SSH ホスト キー チェックをイネーブルまたはディセーブルにします。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。

コマンド	目的
ステップ 2 **ssh pubkey-chain** **[no] server** *ip_address* {**key-string** *key_string* **exit**| **key-hash** {**md5** | **sha256**} *fingerprint*} **例：** ciscoasa(config)# ssh pubkey-chain ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9 ciscoasa(config-ssh-pubkey-server)# key-string Enter the base 64 encoded RSA public key. End with the word "exit" on a line by itself ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87 ciscoasa(config-ssh-pubkey-server-string)# exit ciscoasa(config-ssh-pubkey-server)# show running-config ssh pubkey-chain ssh pubkey-chain server 10.7.8.9 key-hash sha256 f1:22:49:47:b6:76:74:b2:db:26:fb:13:65:d8:99:19:e7:9e:24:46:59:be:13:7f:25:27:70:9b:0e:d2:86:12	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。 各サーバについて、SSH ホストの **key-string**（公開キー）または **key-hash**（ハッシュ値）を指定できます。 *key_string* 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登録した後、SHA-256 によってそのキーがハッシュされます。 **key-hash** {**md5** | **sha256**} *fingerprint* では、たとえば、**show** コマンドの出力からコピーしたキーなどの、すでにハッシュされているキー（MD5 または SHA-256 キーを使用）が入力されます。

例

次の例では、10.86.94.170 にあるサーバの、すでにハッシュされているホストキーを追加します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

次の例では、10.7.8.9 にあるサーバのホストの文字列キーを追加します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

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. 2 で規定されています。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（「ASA へのファイルのコピー」（P.36-17）および「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.36-27）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

コマンド	目的

tftp-server *interface_name server_ip filename*
 	
例：
`ciscoasa(config)# tftp-server inside 10.1.4.7 files/config1.cfg`
`ciscoasa(config)# copy tftp: test.cfg`
 	
`Address or name of remote host [10.1.4.7]?`
 	
`Source filename [files/config1.cfg]?`**`config2.cfg`**
 	
`Destination filename [test.cfg]?`
 	
`Accessing tftp://10.1.4.7/files/config2.cfg;int=outside...`
	configure net および **copy** コマンドで使用するために、TFTP サーバのアドレスおよびファイル名を事前定義します。コマンドを入力するとファイル名を上書きできます。たとえば、**copy** コマンドを使用するときに事前定義された TFTP サーバのアドレスを利用できますが、インタラクティブ プロンプトでファイル名を入力することもできます。
	
	copy コマンドに、**tftp:**//*url* ではなく **tftp:** を入力して tftp-server の値を使用します。

ASA へのファイルのコピー

この項では、TFTP、FTP、SMB、HTTP、HTTPS、または SCP サーバから内部または外部フラッシュ メモリにダウンロードする必要がある、アプリケーション イメージ、ASDM ソフトウェア、コンフィギュレーション ファイル、またはその他のファイルをコピーする方法について説明します。

ガイドライン

- 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。
- 文字の大文字と小文字が異なっていても、同じ名前の 2 つのファイルをフラッシュ メモリの同じディレクトリに保存できません。たとえば、config.cfg というファイルが存在する場所に Config.cfg というファイルをダウンロードしようとすると、次のエラー メッセージが表示されます。

```
%Error opening disk0:/Config.cfg (File exists).
```

- Cisco SSL VPN Client をインストールする方法の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*（*Cisco AnyConnect VPN クライアント管理者ガイド*）』を参照してください。ASA に Cisco Secure Desktop をインストールする方法の詳細については、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*（*Cisco ASA 5500 シリーズ管理者向け Cisco Secure Desktop コンフィギュレーション ガイド*）』を参照してください。
- 複数のイメージがインストールされている場合、または外部フラッシュ メモリにイメージがインストールされている場合に特定のアプリケーション イメージまたは ASDM イメージを使用するように ASA を設定する場合は、「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」（P.36-22）を参照してください。
- マルチ コンテキスト モードの場合は、システム実行スペース内にいる必要があります。

手順の詳細

コマンド	目的
copy [/noconfirm] tftp://*server*[*/path*]*/src_filename* **{disk0|disk1}:/[***path***/]***dest_filename* **例：** ciscoasa# copy tftp://10.1.1.67/files/context1.cfg disk0:/context1.cfg Address or name of remote host [10.1.1.67]? Source filename [files/context1.cfg]? Destination filename [context1.cfg]? Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b !!!!!!!!!!! 11143 bytes copied in 5.710 secs (2228 bytes/sec)	TFTP サーバからコピーします。
copy [/noconfirm] ftp://[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dest_filename* **例：** ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/context1.cfg disk0:/contexts/context1.cfg Address or name of remote host [10.1.1.67]? Source username [jcrichton]? Source password [aeryn]? Source filename [files/context1.cfg]? Destination filename [contexts/context1.cfg]? Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b !!!!!!!!!!! 11143 bytes copied in 5.710 secs (2228 bytes/sec)	FTP サーバからコピーします。

コマンド	目的
copy [**/noconfirm**] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*]**/***path*]**/***src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dest_filename* **例：** ciscoasa# copy https://asun:john@10.1.1.67/files/moya.cfg disk0:/contexts/moya.cfg Address or name of remote host [10.1.1.67]? Source username [asun]? Source password [john]? Source filename [files/moya.cfg]? Destination filename [contexts/moya.cfg]? Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b !!!!!!!!!!! 11143 bytes copied in 5.710 secs (2228 bytes/sec)	HTTP（S）サーバからコピーします。
copy [**/noconfirm**] **smb://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dest_filename* **例：** ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/test.xml disk0:/test.xml Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b !!!!!!!!!!! 11143 bytes copied in 5.710 secs (2228 bytes/sec)	SMB サーバからコピーします。

コマンド	目的
copy [**/noconfirm**] **scp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***src_filename*[**;int=***interface_name*] {**disk0**|**disk1**}**:/**[*path/*]*dest_filename* **例：** ciscoasa# copy scp://pilot@10.86.94.170/test.cfg disk0:/test.cfg Address or name of remote host [10.86.94.170]? Source username [pilot]? Destination filename [test.cfg]? The authenticity of host '10.86.94.170 (10.86.94.170)' can't be established. RSA key fingerprint is <65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d: 2d:bf:a9:2b:85:2e:19>(SHA256). Are you sure you want to continue connecting (yes/no)?yes Please use the following commands to add the hash key to the configuration: ssh pubkey-chain server 10.86.94.170 key-hash sha256 65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2 d:bf:a9:2b:85:2e:19 Password: <type in password> !!!!!! 6006 bytes copied in 8.160 secs (750 bytes/sec)	SCP サーバからコピーします。**;int=***interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバに到達します。

スタートアップ コンフィギュレーションまたは実行コンフィギュレーションへのファイルのコピー

テキスト ファイルは、TFTP、FTP、SMB、HTTP（S）、または SCP サーバから、またはフラッシュ メモリから、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにダウンロードできます。

スタートアップ コンフィギュレーションとして特定のコンフィギュレーションを使用するように ASA を設定する場合は、「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」（P.36-22）を参照してください。

ガイドライン

コンフィギュレーションを実行コンフィギュレーションにコピーすると、2 つのコンフィギュレーションがマージされます。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。

手順の詳細

スタートアップ コンフィギュレーションまたは実行コンフィギュレーションにファイルをコピーするには、適切なダウンロード サーバに対して次のコマンドのいずれかを入力します。

コマンド	目的
copy [/noconfirm] tftp://*server[/path]/src_filename* **{startup-config | running-config}** **例：** ciscoasa# copy tftp://10.1.1.67/files/old-running.cfg running-config	TFTP サーバからコピーします。
copy [**/noconfirm**] **ftp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***src_filename* {**startup-config** | **running-config**} **例：** ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/old-startup.cfg startup-config	FTP サーバからコピーします。
copy [**/noconfirm**] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][**/***path*]**/***src_filename* {**startup-config** | **running-config**} **例：** ciscoasa# copy https://asun:john@10.1.1.67/files/new-running.cfg running-config	HTTP（S）サーバからコピーします。
copy [**/noconfirm**] **smb://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***src_filename* {**startup-config** | **running-config**} **例：** ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/new-running.cfg running-config	SMB サーバからコピーします。
copy [**/noconfirm**] **scp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***src_filename*[**;int=***interface_name*] {**startup-config** | **running-config**} **例：** ciscoasa# copy scp://pilot:moya@10.86.94.170/new-startup.cfg startup-config	SCP サーバからコピーします。**;int=***interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバに到達します。

例

たとえば、TFTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
ciscoasa# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

FTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
ciscoasa# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg startup-config
```

HTTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
ciscoasa# copy http://209.165.200.228/configs/startup.cfg startup-config
```

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（**clear configure all**）、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

	コマンド	目的
ステップ 1	**boot system** *url* **例：** `ciscoasa(config)# boot system disk:/images/asa921.bin`	ASA ブート イメージの場所を設定します。URL は次のようになります。 • {**disk0:/** | **disk1:/**}[*path/*]*filename* • **tftp:**//[*user*[**:*password***]**@**]*server*[:*port*]/[*path/*]*filename* TFTP オプションは、すべてのモデルでサポートされるわけではありません。 最大 4 つの **boot system** コマンド エントリを入力して、複数のイメージをブートする順番に指定することができます。ASA は、最初に検出に成功したイメージをブートします。**boot system** コマンドを入力すると、エントリがリストの最後に追加されます。ブート エントリの順序を変更するには、**clear configure boot system** コマンドを使用してすべてのエントリを削除してから、エントリを目的の順序で再入力する必要があります。設定できる **boot system tftp** コマンドは 1 つだけです。これは、最初に設定する必要があります。 **（注）** ASA が連続ブートのサイクルから抜け出せない場合は、ASA を ROMMON モードにリブートします。ROMMON モードの詳細については、「デバッグ メッセージの表示」（P.38-1）を参照してください。
ステップ 2	**asdm image** {**disk0:/** | **disk1:/**}[*path/*]*filename* **例：** `ciscoasa(config)# asdm image disk0:/images/asdm721.bin`	ブートする ASDM イメージを設定します。ブートするイメージを指定しないと、インストールされているイメージが 1 つしかなくても、ASA によって **asdm image** コマンドが実行コンフィギュレーションに挿入されます。Auto Update（設定されている場合）の問題を避けるため、また起動時ごとのイメージ検索を回避するため、ブートする ASDM イメージをスタートアップ コンフィギュレーションで指定する必要があります。
ステップ 3	（オプション） **boot config** {**disk0:/** | **disk1:/**}[*path/*]*filename* **例：** `ciscoasa(config)# boot config disk0:/configs/startup1.cfg`	スタートアップ コンフィギュレーションをデフォルトの隠しファイルではなく既知のファイルになるように設定します。

イメージをロードするための ROM モニタの使用

- 「ASA 5500-X シリーズに対する ROM モニタの使用」（P.36-24）
- 「ASASM に対する ROM モニタの使用」（P.36-25）

ASA 5500-X シリーズに対する ROM モニタの使用

TFTP を使用して ROM モニタ モードから ASA へソフトウェア イメージをロードするには、次の手順を実行します。

ステップ 1　「アプライアンス コンソールへのアクセス」（P.2-2）の手順に従って、ASA のコンソール 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　スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。

ステップ 4　ROMMOM モードで、IP アドレス、TFTP サーバ アドレス、ゲートウェイ アドレス、ソフトウェア イメージ ファイル、およびポートを含む、ASA に対するインターフェイス設定を次のように定義します。

（注）　ASA 5506、ASA 5506-W、および ASA 5508 の場合は、PORT=Ethernet0/0 エントリを含める必要はありません。使用できるのは管理ポートだけです。

```
rommon #1> ADDRESS=10.132.44.177
rommon #2> SERVER=10.129.0.30
rommon #3> GATEWAY=10.132.44.1
rommon #4> IMAGE=f1/asa800-232-k8.bin
rommon #5> PORT=Ethernet0/0
Ethernet0/0
Link is UP
MAC Address: 0012.d949.15b8
```

（注）　ネットワークへの接続がすでに存在することを確認してください。

ステップ 5　設定を検証するには、**set** コマンドを入力します。

```
rommon #6> set
ROMMON Variable Settings:
ADDRESS=10.132.44.177
  SERVER=10.129.0.30
  GATEWAY=10.132.44.1
  PORT=Ethernet0/0
  VLAN=untagged
  IMAGE=f1/asa840-232-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

ステップ 6　**ping server** コマンドを入力して、TFTP サーバを ping します。

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.129.0.30, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

ステップ 7　**tftp** コマンドを入力して、ソフトウェア イメージをロードします。

```
rommon #8> tftp
ROMMON Variable Settings:
ADDRESS=10.132.44.177
  SERVER=10.129.0.30
```

```
  GATEWAY=10.132.44.1
  PORT=Ethernet0/0
  VLAN=untagged
  IMAGE=f1/asa840-232-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp f1/asa840-232-k8.bin@10.129.0.30 via 10.132.44.1

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2011

Loading...N
```

ソフトウェア イメージが正常にロードされると、ASA は自動的に ROMMON モードを終了します。

ステップ 8　正しいソフトウェア イメージが ASA にロードされたことを検証するには、次のコマンドを入力して、ASA 内のバージョンを確認します。

```
ciscoasa# show version
```

ASASM に対する ROM モニタの使用

TFTP を使用して ROM モニタ モードから ASASM へソフトウェア イメージをロードするには、次の手順を実行します。

ステップ 1　「ASA サービス モジュール コンソールへのアクセス」（P.2-3）の手順に従って、ASA のコンソール ポートに接続します。

ステップ 2　ASASM イメージをリロードすることを確認します。

ステップ 3　スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。

ステップ 4　ROMMOM モードで、IP アドレス、TFTP サーバ アドレス、ゲートウェイ アドレス、ソフトウェア イメージ ファイル、ポートおよび VLAN を含む、ASASM に対するインターフェイス設定を次のように定義します。

```
rommon #1> ADDRESS=172.16.145.149
rommon #2> SERVER=172.16.171.125
rommon #3> GATEWAY=172.16.145.129
rommon #4> IMAGE=f1/asa851-smp-k8.bin
rommon #5> PORT=Data0
rommon #6> VLAN=1
Data0
Link is UP
MAC Address: 0012.d949.15b8
```

（注）　ネットワークへの接続がすでに存在することを確認してください。

ステップ 5　設定を検証するには、**set** コマンドを入力します。

```
rommon #7> set
```

```
ROMMON Variable Settings:
ADDRESS=172.16.145.149
  SERVER=172.16.171.125
  GATEWAY=172.16.145.129
  PORT=Data0
  VLAN=1
  IMAGE=f1/asa851-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
  RETRY=20
```

ステップ 6　**ping server** コマンドを入力して、TFTP サーバを ping します。

```
rommon #8> ping server
Sending 20, 100-byte ICMP Echoes to server 172.16.171.125, timeout is 2 seconds:

Success rate is 100 percent (20/20)
```

ステップ 7　**tftp** コマンドを入力して、ソフトウェア イメージをロードします。

```
rommon #9> tftp
Clearing EOBC receive queue ...
cmostime_set = 1
ROMMON Variable Settings:
ADDRESS=172.16.145.149
  SERVER=172.16.171.125
  GATEWAY=172.16.145.129
  PORT=Data0
  VLAN=1
  IMAGE=f1/asa851-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
  RETRY=20

tftp f1/asa851-smp-k8.bin@172.16.171.125 via 172.16.145.129
Starting download.Press ESC to abort.
```

ソフトウェア イメージが正常にロードされると、ASASM は自動的に ROMMON モードを終了します。

（注）　ROMMON のブート完了後に、システム フラッシュにイメージを個別にダウンロードする必要があります。ROMMON モードにモジュールをブートすると、リロード時にシステム イメージが維持されません。

ステップ 8　正しいソフトウェア イメージが ASASM にロードされたことを検証するには、次のコマンドを入力して、バージョンを確認します。

```
hostname# show version
```

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

- 「シングル モード コンフィギュレーションまたはマルチ モード システム コンフィギュレーションのバックアップ」（P.36-27）
- 「フラッシュ メモリ内のコンテキスト 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」（P.36-28）
- 「コンテキスト内でのコンテキスト コンフィギュレーションのバックアップ」（P.36-29）
- 「端末の表示からのコンフィギュレーションのコピー」（P.36-29）
- 「export および import コマンドを使用した追加ファイルのバックアップ」（P.36-29）
- 「スクリプトを使用したファイルのバックアップおよび復元」（P.36-30）

シングル モード コンフィギュレーションまたはマルチ モード システム コンフィギュレーションのバックアップ

シングルコンテキスト モードで、またはマルチモードのシステム コンフィギュレーションから、スタートアップ コンフィギュレーションまたは実行コンフィギュレーションを外部サーバまたはローカル フラッシュ メモリにコピーできます。

手順の詳細

コマンド	目的
copy [**/noconfirm**] {**startup-config** | **running-config**} **tftp://***server*[*/path*]*/dst_filename* **例：** ciscoasa# copy running-config tftp://10.1.1.67/files/new-running.cfg	TFTP サーバにコピーします。
copy [**/noconfirm**] {**startup-config** | **running-config**} **ftp://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename* **例：** ciscoasa# copy startup-config ftp://jcrichton:aeryn@10.1.1.67/files/new-startup.cfg	FTP サーバにコピーします。
copy [**/noconfirm**] {**startup-config** | **running-config**} **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename* **例：** ciscoasa# copy /noconfirm running-config smb://chiana:dargo@10.1.1.67/new-running.cfg	SMB サーバにコピーします。

コマンド	目的
copy [**/noconfirm**] {**startup-config** | **running-config**} **scp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***dst_filename*[**;int=***interface_name*] **例：** ciscoasa# copy startup-config scp://pilot:moya@10.86.94.170/new-startup.cfg	SCP サーバにコピーします。**;int=***interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバに到達します。
copy [**/noconfirm**] {**startup-config** | **running-config**} {**disk0**|**disk1**}**:/**[*path/*]*dst_filename* **例：** ciscoasa# copy /noconfirm running-config disk0:/new-running.cfg	ローカル フラッシュ メモリにコピーします。宛先ディレクトリが存在することを確認してください。存在しない場合は、まず **mkdir** コマンドを使用してディレクトリを作成します。

フラッシュ メモリ内のコンテキスト 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

システム実行スペースで次のいずれかのコマンドを入力することによって、ローカル フラッシュ メモリにあるコンテキスト コンフィギュレーションまたは他のファイルをコピーします。

手順の詳細

コマンド	目的
copy [/noconfirm] {disk0|disk1}:/[*path/]src_filename* **tftp://***server[/path]/dst_filename*** **例：** ciscoasa# copy disk0:/asa-os.bin tftp://10.1.1.67/files/asa-os.bin	フラッシュから TFTP サーバにコピーします。
copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path/*]*src_filename* **ftp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***dst_filename* **例：** ciscoasa# copy disk0:/asa-os.bin ftp://jcrichton:aeryn@10.1.1.67/files/asa-os.bin	フラッシュから FTP サーバにコピーします。
copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path/*]*src_filename* **smb://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***dst_filename* **例：** ciscoasa# copy /noconfirm copy disk0:/asdm.bin smb://chiana:dargo@10.1.1.67/asdm.bin	フラッシュから SMB サーバにコピーします。

コマンド	目的
copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **scp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***dst_filename*[**;int=***interface_name*] **例：** ciscoasa# copy disk0:/context1.cfg scp://pilot:moya@10.86.94.170/context1.cfg	フラッシュから SCP サーバにコピーします。**;int=***interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバに到達します。
copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dst_filename* **例：** ciscoasa# copy /noconfirm disk1:/file1.cfg disk0:/file1.cfgnew-running.cfg	フラッシュからローカル フラッシュ メモリにコピーします。宛先ディレクトリが存在することを確認してください。存在しない場合は、まず **mkdir** コマンドを使用してディレクトリを作成します。

コンテキスト内でのコンテキスト コンフィギュレーションのバックアップ

マルチ コンテキスト モードでは、コンテキスト内から次のバックアップを実行できます。

- （admin コンテキストに接続された）スタートアップ コンフィギュレーション サーバに実行コンフィギュレーションをコピーするには、次のコマンドを入力します。

  ciscoasa/contexta# **copy running-config startup-config**

- コンテキスト ネットワークに接続された TFTP サーバに実行コンフィギュレーションをコピーするには、次のコマンドを入力します。

  ciscoasa/contexta# **copy running-config tftp:/***server*[/*path*]/*filename*

端末の表示からのコンフィギュレーションのコピー

コンフィギュレーションを端末に表示するには、次のコマンドを入力します。

ciscoasa# **show running-config**

コマンドから出力をコピーして、コンフィギュレーションをテキスト ファイルに貼り付けます。

export および import コマンドを使用した追加ファイルのバックアップ

コンフィギュレーションに欠かせない追加ファイルは次のとおりです。

- **import webvpn** コマンドを使用してインポートするファイル。現在これらのファイルには、カスタマイゼーション、URL リスト、Web コンテンツ、プラグイン、および言語翻訳などがあります。
- DAP ポリシー（dap.xml）。
- CSD コンフィギュレーション（data.xml）。
- デジタル キーおよびデジタル証明書。
- ローカル CA ユーザ データベース ファイルと証明書ステータス ファイル。

CLI では、**export** コマンドと **import** コマンドを使用して、コンフィギュレーションの個々の要素をバックアップおよび復元できます。

たとえば **import webvpn** コマンドを使用してインポートしたこれらのファイル、または証明書をバックアップするには、次の手順を実行します。

ステップ 1　次のように、適用可能な **show** コマンドを実行します。

```
ciscoasa # show import webvpn plug-in
ica
rdp
ssh、telnet
vnc
```

ステップ 2　バックアップするファイルに対して **export** コマンドを発行します（この例では rdp ファイルです）。

```
ciscoasa # export webvpn plug-in protocol rdp tftp://tftpserver/backupfilename
```

スクリプトを使用したファイルのバックアップおよび復元

スクリプトを使用して、ASA のコンフィギュレーション ファイルをバックアップおよび復元できます。これには、**import webvpn** CLI によってインポートする拡張機能のすべて、CSD コンフィギュレーションの XML ファイル、および DAP コンフィギュレーションの XML ファイルが含まれます。セキュリティ上の理由により、デジタル キーと証明書、またはローカル CA キーの自動バックアップを実行することはお勧めしません。

この項では、自動バックアップの手順について説明します。また、そのまま使用することも、環境要件に合わせて修正することもできるサンプル スクリプトを示します。サンプル スクリプトは Linux システムに固有のスクリプトです。Microsoft Windows システムで使用するには、サンプルのロジックを使用して修正する必要があります。

（注）　既存の CLI では、**copy**、**export**、および **import** コマンドを使用して個々のファイルをバックアップおよび復元できます。ただし、1 回の操作ですべての ASA コンフィギュレーション ファイルをバックアップする機能はありません。スクリプトを実行すると、複数の CLI を使用できます。

- 「前提条件」（P.36-30）
- 「スクリプトの実行」（P.36-31）
- 「サンプル スクリプト」（P.36-31）

前提条件

スクリプトを使用して ASA コンフィギュレーションをバックアップおよび復元するには、まず次の作業を実行します。

- Expect モジュールとともに Perl をインストールする。
- ASA に到達可能な SSH クライアントをインストールする。
- TFTP サーバをインストールして、ASA からバックアップ サイトにファイルを送信する。

別の選択肢としては、市販のツールを使用します。このスクリプトのロジックをそれらのツールに取り入れることができます。

スクリプトの実行

バックアップおよび復元のスクリプトを実行するには、次の手順を実行します。

ステップ 1　システムの任意の場所に、スクリプト ファイルをダウンロードまたはカットアンドペーストします。

ステップ 2　コマンド ラインで、**Perl** *scriptname* と入力します。*scriptname* はスクリプト ファイルの名前です。

ステップ 3　Enter を押します。

ステップ 4　オプションごとに値を入力するように、プロンプトが表示されます。あるいは、**Perl** *scriptname* コマンドを入力するときにオプションの値を入力してから、**Enter** を押すことができます。どちらの方法でも、スクリプトによりオプションごとに値を入力するよう求められます。

ステップ 5　このスクリプトが実行され、発行されるコマンドが出力されます。この出力は CLI の記録となります。これらの CLI は後で行われる復元に使用できます。特に、ファイルを 1 つまたは 2 つだけ復元する場合に便利です。

サンプル スクリプト

```
#!/usr/bin/perl
#Function: Backup/restore configuration/extensions to/from a TFTP server.
#Description: The objective of this script is to show how to back up
configurations/extensions before the backup/restore command is developed.
# It currently backs up the running configuration, all extensions imported via "import
webvpn" command, the CSD configuration XML file, and the DAP configuration XML file.
#Requirements: Perl with Expect, SSH to the ASA, and a TFTP server.
#Usage: backupasa -option option_value
#       -h: ASA hostname or IP address
#       -u: User name to log in via SSH
#       -w: Password to log in via SSH
#       -e: The Enable password on the security appliance
#       -p: Global configuration mode prompt
#       -s: Host name or IP address of the TFTP server to store the configurations
#       -r: Restore with an argument that specifies the file name.This file is produced
during backup.
#If you don't enter an option, the script will prompt for it prior to backup.
#
#Make sure that you can SSH to the ASA.

use Expect;
use Getopt::Std;

#global variables
%options=();
$restore = 0; #does backup by default
$restore_file = '';
$asa = '';
$storage = '';
$user = '';
$password = '';
$enable = '';
$prompt = '';
$date = `date +%F`;
chop($date);
my $exp = new Expect();
```

```
getopts("h:u:p:w:e:s:r:",\%options);
do process_options();

do login($exp);
do enable($exp);
if ($restore) {
   do restore($exp,$restore_file);
}
else {
   $restore_file = "$prompt-restore-$date.cli";
   open(OUT,">$restore_file") or die "Can't open $restore_file\n";
   do running_config($exp);
   do lang_trans($exp);
   do customization($exp);
   do plugin($exp);
   do url_list($exp);
   do webcontent($exp);
   do dap($exp);
   do csd($exp);
   close(OUT);
}
do finish($exp);

sub enable {
   $obj = shift;
   $obj->send("enable\n");
   unless ($obj->expect(15, 'Password:')) {
      print "timed out waiting for Password:\n";
   }
   $obj->send("enable\n");
   unless ($obj->expect(15, "$prompt#")) {
      print "timed out waiting for $prompt#\n";
   }
}

sub lang_trans {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn translation-table\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /Translation Tables/;
     next unless (/^.+\s+.+$/);
     ($lang, $transtable) = split(/\s+/,$_);
     $cli = "export webvpn translation-table $transtable language $lang
$storage/$prompt-$date-$transtable-$lang.po";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub running_config {
  $obj = shift;
  $obj->clear_accum();
  $cli ="copy /noconfirm running-config $storage/$prompt-$date.cfg";
```

```
  print "$cli\n";
  $obj->send("$cli\n");
  $obj->expect(15, "$prompt#" );
}


sub customization {
  $obj = shift;
  $obj->clear_accum();
  $obj->send("show import webvpn customization\n");
  $obj->expect(15, "$prompt#" );
  $output = $obj->before();
  @items = split(/\n+/, $output);

  for (@items) {
    chop;
    next if /^Template/ or /show import/ or /^\s*$/;
    $cli = "export webvpn customization $_ $storage/$prompt-$date-cust-$_.xml";
    $ocli = $cli;
    $ocli =~ s/^export/import/;
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
  }
}

sub plugin {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn plug-in\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/;
     $cli = "export webvpn plug-in protocol $_ $storage/$prompt-$date-plugin-$_.jar";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub url_list {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn url-list\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/ or /No bookmarks/;
     $cli="export webvpn url-list $_ $storage/$prompt-$date-urllist-$_.xml";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
```

```
      $obj->send("$cli\n");
      $obj->expect(15, "$prompt#" );
    }
}

sub dap {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("dir dap.xml\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm dap.xml $storage/$prompt-$date-dap.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-dap.xml disk0:/dap.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub csd {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("dir sdesktop\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm sdesktop/data.xml $storage/$prompt-$date-data.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-data.xml disk0:/sdesktop/data.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub webcontent {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn webcontent\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /No custom/;
     next unless (/^.+\s+.+$/);
     ($url, $type) = split(/\s+/,$_);
     $turl = $url;
     $turl =~ s/\/\+//;
     $turl =~ s/\+\//-/;
     $cli = "export webvpn webcontent $url $storage/$prompt-$date-$turl";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
```

```
}

sub login {
    $obj = shift;
    $obj->raw_pty(1);
    $obj->log_stdout(0); #turn off console logging.
    $obj->spawn("/usr/bin/ssh $user\@$asa") or die "can't spawn ssh\n";
    unless ($obj->expect(15, "password:" )) {
        die "timeout waiting for password:\n";
    }

    $obj->send("$password\n");

    unless ($obj->expect(15, "$prompt>" )) {
        die "timeout waiting for $prompt>\n";
    }
}

sub finish {
    $obj = shift;
    $obj->hard_close();
    print "\n\n";

}

sub restore {
   $obj = shift;
   my $file = shift;
   my $output;
   open(IN,"$file") or die "can't open $file\n";
   while (<IN>) {
      $obj->send("$_");
      $obj->expect(15, "$prompt#" );
      $output = $obj->before();
      print "$output\n";
   }
   close(IN);
}

sub process_options {
  if (defined($options{s})) {
      $tstr= $options{s};
      $storage = "tftp://$tstr";
  }
  else {
      print "Enter TFTP host name or IP address:";
      chop($tstr=<>);
      $storage = "tftp://$tstr";
  }
  if (defined($options{h})) {
      $asa = $options{h};
  }
  else {
      print "Enter ASA host name or IP address:";
      chop($asa=<>);
  }

  if (defined ($options{u})) {
      $user= $options{u};
  }
  else {
      print "Enter user name:";
      chop($user=<>);
  }
```

```
  if (defined ($options{w})) {
      $password= $options{w};
  }
  else {
      print "Enter password:";
      chop($password=<>);
  }
  if (defined ($options{p})) {
      $prompt= $options{p};
  }
  else {
      print "Enter ASA prompt:";
      chop($prompt=<>);
  }
  if (defined ($options{e})) {
      $enable = $options{e};
  }
  else {
      print "Enter enable password:";
      chop($enable=<>);
  }

  if (defined ($options{r})) {
     $restore = 1;
     $restore_file = $options{r};
  }
}
```

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.36-36）
- 「ダウングレードの実行」（P.36-37）

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

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　次のコマンドを入力します。

```
ciscoasa(config)# downgrade [/noconfirm] old_image_url old_config_url [activation-key old_key]
```

/noconfirm オプションを指定すると、プロンプトは表示されずにダウングレードされます。*image_url* は、disk0、disk1、tftp、ftp、または smb 上の古いイメージへのパスです。*old_config_url* は、保存されている移行前の設定へのパスです（デフォルトでは、この設定は disk0 に保存されます）。8.3 よりも前のアクティベーション キーに戻る必要がある場合は、そのアクティベーション キーを入力できます。

このコマンドは、次の機能を完了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**）。

次に例を示します。

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

Auto Update の設定

- 「Auto Update に関する情報」（P.36-38）
- 「ガイドラインと制限事項」（P.36-41）
- 「Auto Update サーバとの通信の設定」（P.36-42）
- 「Auto Update サーバとしてのクライアント アップデートの設定」（P.36-43）
- 「Auto Update ステータスの表示」（P.36-44）

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」（P.36-38）
- 「自動更新の利点」（P.36-38）
- 「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.36-39）

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、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。

```
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
```

file は「イメージ」、「ASDM」または「コンフィギュレーション」で、アップデートの失敗に応じて異なります。*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。

ガイドラインと制限事項

- 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

ASA を Auto Update クライアントとして設定するには、次の手順を実行します。

ステップ 1　Auto Update サーバの URL を指定するには、次のコマンドを入力します。

```
ciscoasa(config)# auto-update server url [source interface] [verify-certificate |
no-verification]
```

ここで、*url* には次の構文があります。

```
http[s]://[user:password@]server_ip[:port]/pathname
```

source *interface* キーワードおよび引数は、Auto Update サーバに要求を送信するときに使用するインターフェイスを指定します。**management-access** コマンドで指定したインターフェイスと同じインターフェイスを指定すると、Auto Update 要求は管理アクセスに使用されるのと同じ IPsec VPN トンネルを通過します。

HTTPS の場合、**verify-certificate キーワード**（デフォルト）は、Auto Update Server が返す証明書を検証します。検証をディセーブルにするには（推奨されません）、**no-verification** キーワードを指定します。

ステップ 2　（オプション）Auto Update サーバと通信する際に送信するデバイス ID を識別するには、次のコマンドを入力します。

```
ciscoasa(config)# auto-update device-id {hardware-serial | hostname | ipaddress [if-name] |
mac-address [if-name] | string text}
```

使用する ID は、次のいずれかのパラメータによって決まります。

- *hardware-serial* 引数は、ASA のシリアル番号を指定します。
- *hostname* 引数は、ASA のホスト名を指定します。
- **ipaddress** キーワードは、指定のインターフェイスの IP アドレスを指定します。インターフェイス名を指定しない場合、Auto Update サーバとの通信に使用するインターフェイスの IP アドレスが使用されます。
- **mac-address** キーワードは、指定のインターフェイスの MAC アドレスを指定します。インターフェイス名を指定しない場合、Auto Update サーバとの通信に使用するインターフェイスの MAC アドレスが使用されます。
- **string** キーワードは、指定のテキスト識別子を指定します。空白や '、"、>、&、? は使用できません。

ステップ 3　（オプション）コンフィギュレーション、またはイメージのアップデートを要求するために Auto Update サーバにポーリングする回数を指定するには、次のコマンドを入力します。

```
ciscoasa(config)# auto-update poll-period poll-period [retry-count [retry-period]]
```

poll-period 引数は、更新を確認する間隔（分単位）を指定します。デフォルトは 720 分（12 時間）です。

retry-count 引数は、サーバへの最初の接続に失敗した場合に、再試行する回数を指定します。デフォルトは 0 です。

retry-period 引数は、リトライの間の待機時間（分単位）を指定します。デフォルトは 5 分です。

ステップ 4　（オプション）ASA から Auto Update サーバにポーリングする特定の時刻をスケジュールするには、次のコマンドを入力します。

```
ciscoasa(config)# auto-update poll-at days-of-the-week time [randomize minutes]
[retry_count [retry_period]]
```

days-of-the-week 引数は、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、および Sunday の中の任意の曜日または曜日の組み合わせです。それ以外に、daily（月曜日から日曜日）、weekdays（月曜日から金曜日）、および weekend（土曜日と日曜日）の値が設定可能です。

time 引数は、ポーリングの開始時刻を HH:MM 形式で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 と指定します。

randomize *minutes* キーワードおよび引数は、指定した開始時刻に続いてポーリングをランダムに実行する期間を指定します。範囲は 1 ～ 1439 分です。

retry_count 引数は、最初の接続に失敗したときに、Auto Update サーバへの再接続を試みる回数を指定します。デフォルトは 0 です。

retry_period 引数は、接続の試行から次の試行までの待機時間を指定します。デフォルトは 5 分です。範囲は 1 ～ 35791 分です。

ステップ 5　（オプション）Auto Update サーバに一定期間アクセスがなかった場合にトラフィックの通過を中断するには、次のコマンドを入力します。

```
ciscoasa(config)# auto-update timeout period
```

period 引数は、1 ～ 35791 の範囲で分単位のタイムアウト期間を指定します。デフォルトはタイムアウトなし（0 分）です。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

最新のイメージとコンフィギュレーションが ASA にあることを確認するには、**auto-update timeout** コマンドを使用します。この状態は、システム ログ メッセージ 201008 で報告されます。

次の例では、ASA が外部インターフェイスから証明書の検証付きで、IP アドレス 209.165.200.224、ポート番号 1742 で Auto Update サーバをポーリングするように設定されています。

また、ASA は、デバイス ID としてホスト名を使用し、Auto Update サーバへのポーリングを毎週金曜日と土曜日の 10:00 p.m から 11:00 p.m. の間の任意の時刻に実行するように設定されます。次の例のように、ポーリングに失敗した場合は、ASA によって Auto Update サーバへの再接続が 10 回試みられます。再接続と再接続の間は、3 分間の待機時間が設定されます。

```
ciscoasa(config)# auto-update server
https://jcrichton:farscape@209.165.200.224:1742/management source outside
verify-certificate
ciscoasa (config)# auto-update device-id hostname
hostname (config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
```

Auto Update サーバとしてのクライアント アップデートの設定

client-update コマンドを入力すると、Auto Update クライアントとして設定された ASA のアップデートがイネーブルになり、ソフトウェア コンポーネントのタイプ（ASDM またはブートイメージ）、ASA のタイプまたはファミリ、アップデートが適用されるリビジョン番号、アップデートを取得した URL または IP アドレスを指定できるようになります。

ASA を Auto Update サーバとして設定するには、次の手順を実行します。

ステップ 1　クライアント アップデートをイネーブルにするには、次のコマンドを入力します。

```
ciscoasa(config)# client-update enable
```

ステップ 2　ASA に適用する **client-update** コマンドに、次のパラメータを設定します。

client-update {**component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} **url** *url-string* **rev-nums** *rev-nums*}

component {**asdm** | **image**} パラメータは、ASDM または ASA のブート イメージのいずれかをソフトウェア コンポーネントとして指定します。

device-id *dev_string* パラメータは、Auto Update クライアントが自身を識別するために使用する固有の文字列を指定します。最大で 63 文字です。

family *family_name* パラメータは、Auto Update クライアントが自身を識別するために使用するファミリ名を指定します。asa、pix、または 7 文字以内のテキスト文字列を指定します。

rev-nums *rev-nums* パラメータは、このクライアントのソフトウェアまたはファームウェア イメージを指定します。最大 4 個のイメージを、任意の順序でカンマで区切って指定します。

type *type* パラメータは、クライアント アップデートを通知するクライアントのタイプを指定します。このコマンドは、Windows クライアントのアップデートでも使用されるため、クライアントのリストには Windows オペレーティング システムも複数含まれています。

url *url-string* パラメータは、ソフトウェア / ファームウェア イメージの URL を指定します。この URL は、クライアントに適合するファイルを指している必要があります。すべての Auto Update クライアントでは、URL のプレフィックスとしてプロトコル「http://」または「https://」を使用する必要があります。

特定のタイプの ASA すべてに適用するクライアント アップデートのパラメータを設定します。つまり、ASA のタイプと、アップデートされたイメージの取得元 URL または IP アドレスを指定します。また、リビジョン番号も指定する必要があります。リモートの ASA のリビジョン番号が、指定したリビジョン番号の 1 つと一致する場合は、クライアントのアップデートは不要です。アップデートは無視されます。

Cisco 5525-X ASA にクライアント アップデートを設定するには、次のコマンドを入力します。

```
ciscoasa(config)# client-update type asa5525 component asdm url
http://192.168.1.114/aus/asdm601.bin rev-nums 8.0(1)
```

Auto Update ステータスの表示

Auto Update のステータスを表示するには、次のコマンドを入力します。

```
ciscoasa(config)# show auto-update
```

次に、**show auto-update** コマンドの出力例を示します。

```
ciscoasa(config)# show auto-update

Server: https://********@209.165.200.224:1742/management.cgi?1276
Certificate will be verified
Poll period: 720 minutes, retry count: 2, retry period: 5 minutes
Timeout: none
Device ID: host name [corporate]
Next poll in 4.93 minutes
Last poll: 11:36:46 PST Tue Nov 13 2004
Last PDM update: 23:36:46 PST Tue Nov 12 2004
```

ソフトウェアとコンフィギュレーションの機能履歴

表 36-2 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。

表 36-2　ソフトウェアとコンフィギュレーションの機能履歴

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セキュア コピー（SCP）クライアントがサポートされています。 **ssh pubkey-chain**、**server (ssh pubkey-chain)**、**key-string**、**key-hash**、**ssh stricthostkeycheck** の各コマンドが導入されました。 **copy scp** コマンドが変更されました。
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.In order to verify this certificate please use the verify-certificate option.` 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。次のコマンドを使用します。 **auto-update server no-verification** **auto-update server {verify-certificate | no-verification}** コマンドが変更されました。

CHAPTER 37

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」（P.37-1）
- 「EEM のガイドライン」（P.37-3）
- 「EEM の設定」（P.37-3）
- 「EEM の例」（P.37-7）
- 「EEM のモニタリング」（P.37-8）
- 「EEM の履歴」（P.37-8）

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用に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 を重複させ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 つのタイマーを設定できます。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ない場合があります。**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**：デフォルトの設定です。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.37-3）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の出力先の設定」（P.37-5）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.37-7）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　イベント マネージャ アプレットを作成し、イベント マネージャ アプレットのコンフィギュレーション モードを開始します。

event manager applet *name*

例：

```
ciscoasa(config)# event manager applet exampleapplet1
```

name 引数は、最大 32 文字の英数字です。スペースは使用できません。

イベント マネージャ アプレットを削除するには、このコマンドを **no** 形式で入力します。

ステップ 2　イベント マネージャ アプレットの説明を入力します。

description *text*

例：

```
ciscoasa(config-applet)# description applet1example
```

text 引数は、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 3　指定されたイベントを設定するには、次のコマンドのいずれかを入力します。設定されたイベントを削除するには、それぞれのコマンドを **no** 形式で入力します。

- syslog イベントを設定するには、イベント マネージャ アプレットをトリガーする単一の syslog メッセージまたは syslog メッセージの範囲を指定します。

  event syslog id *nnnnnn*[*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]

  例：

  ```
  ciscoasa(config-applet)# event syslog id 106201
  ```

  nnnnnn 引数には、syslog メッセージの ID を指定します。キーワードと引数のペアである **occurs** *n* は、イベント マネージャ アプレットを呼び出すために syslog メッセージが発生しなければならない回数を示しています。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。キーワードと引数のペアである **period** *seconds* は、イベントが発生する際の許容時間（秒数）を示しています。また、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を制限します。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表します。

- イベントを設定された期間ごとに 1 回発生させ、自動的にリスタートするように設定します。

  event timer watchdog time *seconds*

  例：

  ```
  ciscoasa(config-applet)# event timer watchdog time 30
  ```

  秒数は、1 ～ 604800 の範囲で設定してください。

- イベントを 1 回発生させ、削除および再追加されない限りはリスタートしないように設定します。

  event timer countdown time *seconds*

  例：

  ```
  ciscoasa(config-applet)# event timer countdown time 60
  ```

  秒数は、1 ～ 604800 の範囲で設定してください。カウントダウン タイマー イベントを削除するには、このコマンドの **no** 形式を使用します。

（注）　スタートアップ コンフィギュレーションである場合、このタイマーはリブート時に再実行されます。

- 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するように設定します。

  event timer absolute time *hh:mm:ss*

  例：

  ```
  ciscoasa(config-applet)# event timer absolute time 10:30:20
  ```

  時刻の形式は hh:mm:ss です。時刻の範囲は 00:00:00（午前 0 時）から 23:59:59 です。
- ASA のクラッシュ時にクラッシュ イベントをトリガーします。

  event crashinfo

  例：

  ```
  ciscoasa(config-applet)# event crashinfo
  ```

  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。

アクションおよびアクションの出力先の設定

アクションおよびアクション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　イベント マネージャ アプレットにアクションを設定します。

action *n* **cli command** "*command*"

例：

```
ciscoasa(config-applet)# action 1 cli command "show version"
```

n オプションはアクション ID です。有効な ID の範囲は、0 ～ 4294967295 です。*command* オプションの値は、引用符で囲む必要があります。引用符で囲んでいない場合、コマンドが 2 つ以上の単語で構成されているとエラーが発生します。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。コマンドで使用可能な場合は、**noconfirm** オプションを使用します。

ステップ 2　使用可能な出力先オプションを 1 つ選択します。出力先を削除するには、各コマンドの **no** 形式を使用します。

- **None** オプションは、**action** コマンドからのあらゆる出力を破棄します。これがデフォルト設定です。

  output none

  例：

  ```
  ciscoasa(config-applet)# output none
  ```

- **Console** オプションは、**action** コマンドの出力をコンソールに送信します。

  output console

  例：

  ```
  ciscoasa(config-applet)# output console
  ```

  （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。

- **New File** オプションは、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 **action** コマンドの出力を送信します。

  output file new

  例：

  ```
  ciscoasa(config-applet)# output file new
  ```

  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。

- **New Set of Rotated Files** オプションは、ローテーションで使用される一連のファイルを作成します。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。

  output file rotate *n*

  例：

  ```
  ciscoasa(config-applet)# output file rotate 50
  ```

  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（*n* -1）で示されます。*n* オプションはローテーションの値です。有効な値の範囲は 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。

- **Single Overwritten File** オプションは、**action** コマンドの出力を単一のファイルに書き込みます。このファイルは毎回上書きされます。

  output file overwrite *filename*

  例：

  ```
  ciscoasa(config-applet)# output file overwrite examplefile1
  ```

  filename 引数は、（ASA に対して）ローカルのファイル名です。このコマンドは、FTP、TFTP、および SMB のターゲット ファイルを使用する場合もあります。

- **Single Appended File** オプションは、**action** コマンドの出力を単一のファイルに書き込みますが、このファイルは毎回付加されます。

  output file append *filename*

  例：

  ```
  ciscoasa(config-applet)# output file append examplefile1
  ```

  filename 引数は、（ASA に対して）ローカルのファイル名です。

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　イベント マネージャ アプレットを実行します。

event manager run *applet*

例：

```
ciscoasa# event manager run exampleapplet1
```

event none コマンドで設定されていないイベント マネージャ アプレットを実行すると、エラーが発生します。*applet* 引数は、イベント マネージャ アプレットの名前です。

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、午前 0 時から午前 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、次のコマンド参照してください。

- **clear configure event manager**

  このコマンドは、イベント マネージャの実行コンフィギュレーションを削除します。

- **clear configure event manager applet** *appletname*

  このコマンドは、コンフィギュレーションから指定のイベント マネージャ アプレットを削除します。

- **show counters protocol eem**

  このコマンドは、イベント マネージャのカウンタを表示します。

- **show event manager**

  このコマンドは、ヒット カウントやイベント マネージャ アプレットが最後に呼び出されたのはいつかなど、設定されたイベント マネージャ アプレットに関する情報を表示します。

- **show running-config event manager**

  このコマンドは、イベント マネージャの実行コンフィギュレーションを表示します。

EEM の履歴

表 37-1　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。 **event manager applet**、**description**、**event syslog id**、**event none**、**event timer** {**watchdog time** *seconds* | **countdown time** *seconds* | **absolute time** *hh:mm:ss*}、**event crashinfo**、**action cli command**、**output** {**none** | **console** | **file** {**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*}}、**show running-config event manager**、**event manager run**、**show event manager**、**show counters protocol eem**、**clear configure event manager**、**debug event manager**、**debug menu eem** の各コマンドが導入または変更されました。

CHAPTER 38

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。

- 「デバッグ メッセージの表示」（P.38-1）
- 「パケットのキャプチャ」（P.38-1）
- 「クラッシュ ダンプの表示」（P.38-6）
- 「コア ダンプの表示」（P.38-6）
- 「ASAv の vCPU 使用率」（P.38-6）

デバッグ メッセージの表示

デバッグ出力は CPU プロセスで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が使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。デバッグ メッセージをイネーブルにするには、コマンド リファレンスの **debug** コマンドを参照してください。

パケットのキャプチャ

パケットのキャプチャは、接続の問題のトラブルシューティングや不審なアクティビティのモニタを行うときに役立つ可能性があります。パケット キャプチャ サービスを使用する場合は、Cisco TAC に連絡することをお勧めします。

パケットをキャプチャするには、次の手順を実行します。

手順

ステップ 1 パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。

[cluster exec] capture *capture_name* **[type {asp-drop all** *[drop-code]* **| tls-proxy | raw-data | lacp | isakmp [ikev1 | ikev2] | inline-tag** *[tag]* **| webvpn user** *webvpn-user*}] **[access-list** *access_list_name*] **[interface asa_dataplane] [buffer** *buf_size*] **[ethernet-type** *type*] **[interface** *interface_name*] **[reinject-hide] [packet-length** *bytes*] **[circular-buffer]**

[**trace** *trace_count*] [**real-time**] [**trace**] [**match prot** {**host** *source-ip* | *source-ip mask* |**any**}{**host** *destination-ip* |*destination-ip mask* | **any**} [*operator* **port**]

例：

```
ciscoasa# capture captest interface inside
```

構文の詳細な説明については、コマンド リファレンスまたは CLI ヘルプ（**help capture**）を参照してください。すべてのオプションが 1 つのコマンドで指定できるわけではありません。可能な組み合わせについては、CLI ヘルプを参照してください。

複数のタイプのトラフィックをキャプチャするには、複数の **capture** ステートメントで同じ *capture_name* を使用します。

type asp-drop キーワードは、高速セキュリティ パスでドロップされるパケットをキャプチャします。クラスタでは、ドロップされた、ユニット間の転送データ パケットもキャプチャされます。マルチ コンテキスト モードでは、このオプションがシステム コンテキストで発行されると、すべてのドロップされたデータ パケットがキャプチャされます。このオプションがユーザ コンテキストで発行されたときは、ドロップされたデータ パケットのうち、そのユーザ コンテキストに属するインターフェイスから入ったものだけがキャプチャされます。

inline-tag *tag* のキーワードと引数のペアは、特定の SGT 値のタグを指定します。指定しない場合は、任意の SGT 値を持つタグ付きパケットをキャプチャします。

buffer キーワードは、パケットを保存するために使用するバッファ サイズを定義します。このバイト バッファがいっぱいになると、パケット キャプチャは停止します。クラスタ内で使用されるときは、これはユニットあたりのサイズです（全ユニットの合計ではありません）。**circular-buffer** キーワードを指定すると、バッファがいっぱいになったときに、バッファが先頭から順に上書きされます。

interface キーワードは、パケット キャプチャを使用するインターフェイスの名前を設定します。キャプチャするすべてのパケットのインターフェイスを設定する必要があります。

データプレーン上のパケットをキャプチャするには、**asa_dataplane** キーワードを使用します。ASA CX バックプレーンでキャプチャされたパケットをフィルタするには、**asa_dataplane** オプションを使用し、次のガイドラインに従ってください。シングル モードでは、バックプレーン制御パケットはアクセス リストをバイパスしてキャプチャされます。マルチ コンテキスト モードでは、制御パケットのみがシステム コンテキストでキャプチャされます。データ パケットは、ユーザ コンテキストでキャプチャされます。**access-list** と **match** オプションは、ユーザ コンテキストでのみ使用できます。

クラスタ制御リンクのトラフィックをキャプチャするには、**cluster** キーワードを使用します。**type lacp** を設定する場合は、nameif name の代わりに物理インターフェイス ID を指定します。

match キーワードは、一致するプロトコルおよび送信元と宛先 IP アドレス、およびオプションのポートをキャプチャします。このキーワードは、1 つのコマンドで 3 回まで使用できます。*operator* には次のいずれかを指定できます。

- **lt**：より小さい
- **gt**：より大きい
- **eq**：等しい

type raw-data キーワードは、着信パケットと発信パケットをキャプチャします。この設定は、デフォルトです。

real-time キーワードを指定すると、キャプチャしたパケットがリアルタイムで連続して表示されます。リアルタイムのパケット キャプチャを終了するには、**Ctrl+C** を押します。キャプチャを完全に削除するには、このコマンドの **no** 形式を使用します。このオプションは、**raw-data** キャプチャおよび **asp-drop** キャプチャにだけ適用されます。このオプションは、**cluster exec capture** コマンドを使用するときはサポートされません。

reinject hide キーワードを指定すると、再注入されたパケットはキャプチャされません。これは、クラスタリング環境だけで適用されます。

（注） ACL の最適化が設定されている場合、キャプチャで **access-list** コマンドは使用できません。**access-group** コマンドのみを使用できます。この場合、**access-list** コマンドを使用しようとするとエラーが表示されます。

クラスタリング環境でのパケットのキャプチャ

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、**cluster exec capture** コマンドを使用してマスター 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。**cluster exec** キーワードは新しいキーワードであり、**capture** コマンドの前に置くとクラスタ全体のキャプチャがイネーブルになります。

「cluster」というインターフェイス名はクラスタ制御リンクのデフォルト名であり、変更できません。インターフェイス名として「cluster」を指定すると、クラスタ制御リンク インターフェイス上のトラフィックがキャプチャされます。クラスタ制御リンク上のパケットには、コントロール プレーン パケットとデータ プレーン パケットの 2 種類があり、どちらも、転送されたデータ トラフィックとクラスタ LU メッセージが含まれています。IP アドレス ヘッダーの TTL フィールドは、この 2 種類のパケットを区別できるように符号化されます。転送されたデータ パケットがキャプチャされるときは、デバッグのためにクラスタリング トレーラもキャプチャ ファイルに出力されます。

マルチ コンテキスト モードでは、クラスタ インターフェイスはシステム コンテキストに属していますが、そのインターフェイスを認識できるので、クラスタ リンクでのキャプチャをユーザ コンテキストで設定できます。システム コンテキストでは、コントロール プレーンとデータ プレーンの両方のパケットが使用できます。データ プレーンでは LU パケットがキャプチャされ、データ パケットのうち、システム コンテキストだけに属するものが転送されます。ユーザ コンテキストでは、コントロール プレーン パケットは認識されません。指定のユーザ コンテキストに属する転送されたデータ パケットと、LU パケットだけがキャプチャされます。セキュリティのために、各コンテキストが認識するのは、そのコンテキストに属するパケットだけとなっています。

パケット キャプチャのガイドライン

- ASA が不正な形式の TCP ヘッダーを持つパケットを受信し、ASP のドロップ理由が *invalid-tcp-hdr-length* でパケットがドロップされた場合、それらのパケットを受信したインターフェイスでの **show capture** コマンドの出力では、それらのパケットは表示されません。
- IP トラフィックだけをキャプチャできます。ARP などの非 IP パケットはキャプチャできません。
- マルチ コンテキスト モードでのクラスタ制御リンク キャプチャの場合は、クラスタ制御リンクで送信されるコンテキストに関連付けられたパケットだけがキャプチャされます。
- インライン SGT タグ付きパケットについては、キャプチャされたパケットに PCAP ビューアが認識できない追加の CMD ヘッダーが含まれます。

- マルチ コンテキスト モードでは、**copy capture** コマンドは、システム スペースでのみ使用できます。構文は次のようになります。

  copy /pcap capture:*Context-name*/*in-cap* **tftp**

  in-cap は、コンテキスト *context-name* で設定されたキャプチャです。

- **cluster exec capture realtime** コマンドはサポートされません。次のエラー メッセージが表示されます。

  ```
  Error: Real-time capture can not be run in cluster exec mode.
  ```

- 共有 VLAN には、次のガイドラインが適用されます。
  - VLAN ごとに設定できるキャプチャは 1 つだけです。共有 VLAN の複数のコンテキストでキャプチャを設定した場合は、最後に設定したキャプチャだけが使用されます。
  - 最後に設定した（アクティブ）キャプチャを削除した場合は、別のコンテキストで事前に設定したキャプチャがあっても、アクティブになるキャプチャはありません。キャプチャをアクティブにするには、キャプチャを削除して追加し直す必要があります。
  - キャプチャを指定したインターフェイスに着信するすべてのトラフィックがキャプチャされます。これには、共有 VLAN 上の他のコンテキストへのトラフィックも含まれます。
  - したがって、ある VLAN のコンテキスト A でのキャプチャをイネーブルにしたときに、その VLAN がコンテキスト B でも使用される場合は、コンテキスト A とコンテキスト B の両方の入力トラフィックがキャプチャされます。
- 出力トラフィックの場合は、アクティブ キャプチャのあるコンテキストのトラフィックだけがキャプチャされます。唯一の例外は、ICMP 検査をイネーブルにしない（したがって、ICMP トラフィックのセッションが高速パスにない）場合です。この場合は、共有 VLAN のすべてのコンテキストで入力と出力の ICMP トラフィックがキャプチャされます。
- キャプチャを設定する場合、通常は、キャプチャする必要のあるトラフィックを照合する ACL を設定します。トラフィック パターンを照合する ACL の設定後に、キャプチャを定義し、キャプチャを設定する必要があるインターフェイスとともに、この ACL をキャプチャに関連付ける必要があります。
- クラスタ全体のキャプチャを実行した後で、同じクラスタ全体のキャプチャ ファイルを 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。

  ```
  ciscoasa (cfg-cluster)# cluster exec copy /pcap capture: cap_name
  tftp://location/path/filename.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、filename_A.pcap、filename_B.pcap などとなります。この例では、A と B がクラスタ ユニット名です。ファイル名の末尾にユニット名を追加すると、別の宛先名が生成されます。
- 指定したインターフェイスでのクラスタ全体のキャプチャをイネーブルにするには、例に示したコマンドそれぞれの前に **cluster exec** キーワードを追加します。これらの **capture** コマンドは、マスター ユニットからスレーブ ユニットへの複製だけが可能です。ただし、指定したインターフェイスでのローカル ユニットのキャプチャを、これらの **capture** コマンドを使用して設定することは可能です。

例

次の例では、クラスタ全体の LACP キャプチャを作成する方法を示します。

```
ciscoasa (config)# cluster exec capture lacp type lacp interface gigabitEthernet0/0
```

次の例では、クラスタリング リンクでの制御パス パケットのキャプチャを作成する方法を示します。

```
ciscoasa (config)# capture cp interface cluster match udp any eq 49495 any
ciscoasa (config)# capture cp interface cluster match udp any any eq 49495
```

次の例では、クラスタリング リンクでのデータ パス パケットのキャプチャを作成する方法を示します。

```
ciscoasa (config)# access-list cc1 extended permit udp any any eq 4193
ciscoasa (config)# access-list cc1 extended permit udp any eq 4193 any
ciscoasa (config)# capture dp interface cluster access-list ccl
```

次の例では、クラスタを通過するデータ パス トラフィックをキャプチャする方法を示します。

```
ciscoasa (config)# capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
ciscoasa (config)# capture abc interface inside match udp host 1.1.1.1 any
ciscoasa (config)# capture abc interface inside access-list xxx
```

次の例では、指定した実際の発信元から実際の宛先へのフローに対する論理更新メッセージをキャプチャし、指定した実際の発信元から実際の宛先へ CCL を介して転送されるパケットをキャプチャする方法を示します。

```
ciscoasa (config)# access-list dp permit ip real_src real_dst
```

次の例では、特定タイプのデータ プレーン メッセージ（たとえば ICMP エコー要求/応答）のうち、ある ASA から別の ASA に転送されたものを、メッセージ タイプに応じた **match** キーワードまたは ACL を使用してキャプチャする方法を示します。

```
ciscoasa (config)# capture capture_name interface cluster access-list match icmp any any
```

次の例では、クラスタ制御リンク上で ACL 103 を使用してキャプチャを作成する方法を示します。

```
ciscoasa (config)# access-list 103 permit ip A B
ciscoasa (config)# capture example1 interface cluster access-list 103
```

前の例で、A と B が CCL インターフェイスの IP アドレスである場合は、この 2 つのユニット間で送信されるパケットだけがキャプチャされます。

A および B が、デバイスを通過するトラフィックの IP アドレスである場合は、次のことが当てはまります。

- 転送されたパケットは通常どおりにキャプチャされます。ただし、送信元および宛先の IP アドレスが ACL に一致することが条件です。
- データ パス ロジック更新メッセージがキャプチャされるのは、そのメッセージが A と B の間のフローに対するものであるか、特定の ACL（たとえば、access-list 103）に対するものである場合です。埋め込まれたフローの 5 タプルが一致するものがキャプチャされます。

UDP パケットの送信元と宛先のアドレスは CCL のアドレスですが、このパケットがフローを更新するためのものであり、そのフローにアドレス A および B が関連付けられている場合は、このパケットもキャプチャされます。つまり、パケットに埋め込まれているアドレス A および B が一致している限り、そのパケットもキャプチャされます。

クラッシュ ダンプの表示

ASA または ASAv がクラッシュした場合に、クラッシュ ダンプ情報を表示できます。クラッシュ ダンプの内容を調べる必要がある場合は、Cisco TAC に連絡することを推奨します。コマンド リファレンスの **show crashdump** コマンドを参照してください。

コア ダンプの表示

コア ダンプは、プログラムが異常終了（クラッシュ）したときの、実行中のプログラムのスナップショットです。コア ダンプは、エラーを診断またはデバッグするため、および障害を後からオフサイトで分析できるよう、クラッシュを保存するために使用されます。Cisco TAC では、ASA または ASAv のアプリケーションまたはシステムのクラッシュをトラブルシューティングするために、ユーザにコア ダンプ機能をイネーブルにするよう求める場合があります。コマンド リファレンスの **coredump** コマンドを参照してください。

ASAv の vCPU 使用率

ASAv の vCPU 使用率では、データ パス、コントロール 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

報告される 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（SSH を使用しホストに接続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** コマンドと似ており、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 では 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ている仮想 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」（P.39-1）
- 「ロギングのガイドライン」（P.39-5）
- 「ロギングの設定」（P.39-6）
- 「ログのモニタリング」（P.39-19）
- 「ロギングの例」（P.39-20）
- 「ロギングの履歴」（P.39-21）

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メッセージを収集する方法です。中央の syslog サーバへのロギングは、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、簡単な 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、日常的な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向けら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状況により、セキュリティ ポリシーの変更の監査証跡を得ることができます。
- 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。
Level	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 39-1 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 39-1　　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。

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

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。

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 サーバごとに新しいコマンドを入力します。
- 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.39-7）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.39-7）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　ロギングをイネーブルにします。

logging enable

例：

```
ciscoasa(config)# logging enable
```

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ときに特別なアクションが実行されるように指定したり、ログからデータを抽出してレポート用の別のファイルにその記録を保存したり、サイト固有のスクリプトを使用して統計情報を追跡したりできます。

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　syslog サーバにメッセージを送信するように、ASA および ASASM を設定します。

logging host *interface_name syslog_ip* [**tcp**[*/port*] | **udp**[*/port*] [**format emblem**]]

例：

```
ciscoasa(config)# logging host dmz1 192.168.1.5 udp 1026 format emblem
```

format emblem キーワードは、UDP 限定で syslog サーバでの EMBLEM 形式ロギングをイネーブルにします。*interface_name* 引数には、syslog サーバにアクセスするときのインターフェイスを指定します。*syslog_ip* 引数には、syslog サーバの IP アドレスを指定します。**tcp**[*/port*] または **udp**[*/port*] キーワードと引数のペアは、ASA および ASASM は、syslog サーバに syslog メッセージを送信するために TCP または UDP を使用する必要があることを指定します。

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 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。

TCP を指定すると、ASA および 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 および ASA サービス モジュール を経由する接続をブロックします。TCP syslog サーバへの接続に関係なく新しい接続を許可するには、手順 3 を参照してください。UDP を指定すると、ASA および 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。

ステップ 2　syslog サーバに送信する syslog メッセージを指定します。

logging trap {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging trap errors
```

重大度として、値（1 ～ 7）または名前を指定できます。たとえば重大度を 3 に設定すると、ASA および ASASM は、重大度が 3、2、および 1 の syslog メッセージを送信します。syslog サーバに送信する syslog メッセージを特定したカスタム メッセージ リストを指定することもできます。

ステップ 3　（オプション）TCP 接続された syslog サーバがダウンした場合、新しい接続をブロックする機能をディセーブルにします。

logging permit-hostdown

例：

```
ciscoasa(config)# logging permit-hostdown
```

ASA または ASASM が syslog メッセージを TCP ベースの syslog サーバに送信するように設定されている場合、および syslog サーバがダウンしているかログ キューがいっぱいの場合、新しい接続はブロックされます。新しい接続は、syslog サーバがバック アップされ、ログ キューがいっぱいでなくなった後に再度許可されます。

ステップ 4　（オプション）ロギング ファシリティを 20 以外の値に設定します。これは、ほとんどの UNIX システムで想定されています。

logging facility *number*

例：

```
ciscoasa(config)# logging facility 21
```

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　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 メッセージを指定します。

logging buffered {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging buffered critical

ciscoasa(config)# logging buffered level 2

ciscoasa(config)# logging buffered notif-list
```

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。内部ログ バッファを空にするには、**clear logging buffer** コマンドを入力します。

ステップ 2　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。

logging buffer-size *bytes*

例：

```
ciscoasa(config)# logging buffer-size 16384
```

ステップ 3　次のいずれかのオプションを選択します。

- 新しいメッセージを内部ログ 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。

  logging flash-bufferwrap

  例：

  ```
  ciscoasa(config)# logging flash-bufferwrap
  ```

- 新しいメッセージを内部ログ 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 FTP サーバに保存します。

  logging ftp-bufferwrap

  例：

  ```
  ciscoasa(config)# logging flash-bufferwrap
  ```

  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。

- ログ バッファの内容を保存する FTP サーバを指定します。

  logging ftp-server *server path username password*

  例：

  ```
  ciscoasa(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
  ```

  server 引数には、外部 FTP サーバの IP アドレスを指定します。*path* 引数には、ログ バッファのデータを保存する FTP サーバへのディレクトリ パスを指定します。このパスは、FTP ルート ディレクトリに対する相対パスです。*username* 引数には、FTP サーバへのロギングで有効なユーザ名を指定します。*password* 引数は、指定したユーザ名に対するパスワードを示します。

- 現在のログ バッファの内容を内部フラッシュ メモリに保存します。

  logging savelog [*savefile*]

  例：

  ```
  ciscoasa(config)# logging savelog latest-logfile.txt
  ```

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　電子メール アドレスに送信する syslog メッセージを指定します。

logging mail {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging mail high-priority
```

電子メールで送信される場合、syslog メッセージは電子メール メッセージの件名行に表示されます。このため、このオプションでは、critical、alert、および emergency など、重大度の高い syslog メッセージを管理者に通知するように設定することをお勧めします。

ステップ 2　電子メール アドレスに syslog メッセージを送信するときに使用する送信元電子メール アドレスを指定します。

logging from-address *email_address*

例：

```
ciscoasa(config)# logging from-address xxx-001@example.com
```

ステップ 3　電子メール アドレスに syslog メッセージを送信するときに使用する宛先の電子メール アドレスを指定します。

logging recipient-address *e-mail_address* [*severity_level*]

例：

```
ciscoasa(config)# logging recipient-address admin@example.com
```

ステップ 4　電子メール アドレスに syslog メッセージを送信するときに使用する SMTP サーバを指定します。

smtp-server *ip_address*

例：

```
ciscoasa(config)# smtp-server 10.1.1.1
```

ASDM への syslog メッセージの送信

syslog メッセージを ASDM に送信するには、次の手順を実行します。

手順

ステップ 1　ASDM に送信する syslog メッセージを指定します。

logging asdm {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging asdm 2
```

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 syslog メッセージのためのスペースを確保するのは、ASDM のデフォルト設定です。ASDM ログ バッファに保持される syslog メッセージの数を制御するために、バッファのサイズを変更できます。

ステップ 2　ASDM ログ バッファに保持される syslog メッセージの数を指定します。

logging asdm-buffer-size *num_of_msgs*

例：

```
ciscoasa(config)# logging asdm-buffer-size 200
```

ASDM ログ バッファの現在の内容を空にするには、**clear logging asdm** コマンドを入力します。

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　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。

logging console {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging console errors
```

SNMP サーバへの syslog メッセージの送信

SNMP サーバへの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。

ステップ 1　SNMP ロギングをイネーブルにし、SNMP サーバに送信するメッセージを指定します。

logging history [*logging_list* | *level*]

例：

```
ciscoasa(config)# logging history errors
```

SNMP ロギングをディセーブルにするには、**no logging history** コマンドを入力します。

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　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。

logging monitor {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging monitor 6
```

ステップ 2　現在のセッションへのロギングだけをイネーブルにします。

terminal monitor

例：

```
ciscoasa(config)# terminal monitor
```

一度ログアウトして再びログインする場合は、このコマンドを再入力する必要があります。現在のセッションへのロギングをディセーブルにするには、**terminal no monitor** コマンドを入力します。

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
- 重大度
- 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　内部ログ バッファに保存されるメッセージの選択基準を指定します。たとえば重大度を 3 に設定すると、ASA は、重大度が 3、2、および 1 の syslog メッセージを送信します。

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[**-***end_id*]}

例：

```
ciscoasa(config)# logging list notif-list level 3
```

name 引数には、リストの名前を指定します。**level** *level* キーワードと引数のペアは、重大度を指定します。**class** *message_class* キーワードと引数のペアは、特定のメッセージ クラスを指定します。**message** *start_id*[**-***end_id*] キーワードと引数のペアは、個々の syslog メッセージ番号または番号の範囲を指定します。

（注）　重大度の名前を syslog メッセージ リストの名前として使用しないでください。使用禁止の名前には、emergencies、alert、critical、error、warning、notification、informational、および debugging が含まれます。同様に、イベント リスト名の先頭にこれらの単語の最初の 3 文字は使用しないでください。たとえば、「err」で始まるイベント リスト名は使用しないでください。

ステップ 2　（オプション）リストにメッセージの選択基準をさらに追加します。

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[**-***end_id*]}

例：

```
ciscoasa(config)# logging list notif-list message 104024-105999

ciscoasa(config)# logging list notif-list level critical

ciscoasa(config)# logging list notif-list level warning class ha
```

前回の手順で使用したものと同じコマンドを入力し、既存のメッセージ リストの名前と追加基準を指定します。リストに追加する基準ごとに、新しいコマンドを入力します。たとえば、リストに追加される syslog メッセージの基準として、次の基準を指定できます。

- ID が 104024 ～ 105999 の範囲の syslog メッセージ。
- 重大度が critical 以上（emergency、alert、または critical）のすべての syslog メッセージ。
- 重大度が warning 以上（emergency、alert、critical、error、または warning）のすべての ha クラスの syslog メッセージ。

（注）　syslog メッセージは、これらの条件のいずれかを満たす場合にログに記録されます。syslog メッセージが複数の条件を満たす場合、そのメッセージは一度だけログに記録されます。

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　EMBLEM 形式の syslog メッセージを、UDP のポート 514 を使用して syslog サーバに送信します。

logging host *interface_name ip_address* {**tcp**[*/port*] | **udp**[*/port*]} [**format emblem**]

例：

```
ciscoasa(config)# logging host interface_1 127.0.0.1 udp format emblem
```

format emblem キーワードは、syslog サーバでの EMBLEM 形式ロギングをイネーブルにします（UDP 限定）。*interface_name* 引数には、syslog サーバにアクセスするときのインターフェイスを指定します。*ip_address* 引数には、syslog サーバの IP アドレスを指定します。**tcp[***/port***]** または **udp[***/port***]** キーワードと引数のペアは、syslog サーバに syslog メッセージを送信するために ASA および ASASM で TCP を使用するか、UDP を使用するかを指定します。

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。

複数の **logging host** コマンドを使用して、追加サーバを指定できます。それらすべてで syslog メッセージが受信されます。2 つ以上のロギング サーバを設定する場合は、必ず、すべてのロギング サーバにおいて、ロギングの重大度の上限を warnings にしてください。

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。

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　syslog サーバ以外の出力先（たとえば、Telnet または SSH セッション）に EMBLEM 形式の syslog メッセージを送信します。

logging emblem

例：

```
ciscoasa(config)# logging emblem
```

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　ログ ファイルの保存で使用可能な内部フラッシュ メモリの最大容量を指定します。

logging flash-maximum-allocation *kbytes*

例：

```
ciscoasa(config)# logging flash-maximum-allocation 1200
```

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 2　ASA または ASASM でログ ファイル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を指定します。

logging flash-minimum-free *kbytes*

例：

```
ciscoasa(config)# logging flash-minimum-free 4000
```

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　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 メッセージの数を指定します。

logging queue *message_count*

例：

```
ciscoasa(config)# logging queue 300
```

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。

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　指定した出力先コマンドでコンフィギュレーションを上書きします。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。

logging class *message_class* {**buffered** | **console** | **history** | **mail** | **monitor** | **trap**} [*severity_level*]

例：

```
ciscoasa(config)# logging class ha buffered alerts
```

buffered、**history**、**mail**、**monitor**、および **trap** キーワードは、このクラスの syslog メッセージの出力先を指定します。**history** キーワードは、SNMP でのロギングをイネーブルにします。**monitor** キーワードは、Telnet および SSH でのロギングをイネーブルにします。**trap** キーワードは、syslog サーバへのロギングをイネーブルにします。コマンドライン エントリあたり 1 つの出力先を指定します。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、出力先ごとに新しいコマンドを入力します。

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　セキュア ロギングをイネーブルにします。

logging host *interface_name syslog_ip* [**tcp**/port | **udp**/*port*] [**format emblem**] [**secure**]

例：

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure
```

interface_name 引数には、syslog サーバが常駐する *インターフェイス*を指定します。*syslog_ip* 引数*には*、syslog サーバの IP アドレスを指定します。*port* 引数には、syslog サーバが syslog メッセージをリスンするポート（TCP または UDP）を指定します。**tcp** キーワードは、ASA または ASASM が TCP を使用して syslog メッセージを syslog サーバに送信するように指定します。**udp** キーワードは、ASA または ASASM が UDP を使用して syslog メッセージを syslog サーバに送信するように指定します。**format emblem** キーワードは、syslog サーバでの EMBLEM 形式ロギングをイネーブルにします。**secure** キーワードは、リモート ロギング ホストへの接続で、TCP の場合にだけ SSL/TLS を使用するように指定します。

（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。

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　デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるように ASA または ASASM を設定します。syslog メッセージに対して指定できるデバイス ID のタイプは 1 つだけです。

logging device-id {**cluster-id** |**context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

例：

```
ciscoasa(config)# logging device-id hostname

ciscoasa(config)# logging device-id context-name
```

context-name キーワードは、現在のコンテキストの名前を装置 ID として使用することを示します（マルチコンテキスト モードにだけ適用されます）。マルチ コンテキスト モードの管理コンテキストでデバイス ID のロギングをイネーブルにすると、そのシステム実行スペースで生成されるメッセージは**システム**のデバイス ID を使用し、管理コンテキストで生成されるメッセージは管理コンテキストの名前をデバイス ID として使用します。

（注）　ASA クラスタでは、常に、選択したインターフェイスのマスター ユニットの IP アドレスを使用します。

cluster-id キーワードがデバイス ID としてクラスタの個別の ASA ユニットのブート設定に一意の名前を指定します。**hostname** キーワードは、ASA のホスト名をデバイス ID として使用するように指定します。**ipaddress** *interface_name* キーワード引数のペアは、*interface_name* として指定されたインターフェイスの IP アドレスをデバイス ID として使用することを指定します。**ipaddress** キーワードを使用すると、syslog メッセージの送信元となるインターフェイスに関係なく、そのデバイス ID は指定された ASA のインターフェイス IP アドレスとなります。クラスタ環境では、**system** キーワードは、デバイス ID がインターフェイスのシステム IP アドレスとなることを指定します。このキーワードにより、デバイスから送信されるすべての syslog メッセージに単一の一貫したデバイス ID を指定できます。**string** *text* キーワード引数のペアは、テキスト文字列をデバイス ID として使用することを指定します。文字列の長さは、最大で 16 文字です。

空白スペースを入れたり、次の文字を使用したりすることはできません。

- &（アンパサンド）
- '（一重引用符）
- "（二重引用符）
- <（小なり記号）
- >（大なり記号）
- ?（疑問符）

（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。

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　syslog メッセージにメッセージが生成された日付と時刻が含まれるように指定します。

logging timestamp

例：

```
ciscoasa(config)# logging timestamp
LOG-2008-10-24-081856.TXT
```

syslog メッセージから日付と時刻を削除するには、**no logging timestamp** コマンドを入力します。

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　ASA または ASASM が特定の syslog メッセージを生成しないように指定します。

no logging message *syslog_id*

例：

```
ciscoasa(config)# no logging message 113019
```

ディセーブルされた syslog メッセージを再度イネーブルにするには、**logging message** *syslog_id* コマンド（たとえば、**logging message 113019** など）を入力します。ディセーブルされたすべての syslog メッセージのロギングを再度イネーブルにするには、**clear configure logging disabled** コマンドを入力します。

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　syslog メッセージの重大度を指定します。

logging message *syslog_id* **level** *severity_level*

例：

```
ciscoasa(config)# logging message 113019 level 5
```

syslog メッセージの重大度をその設定にリセットするには、**no logging message** *syslog_id* **level** *severity_level* コマンド（たとえば、**no logging message 113019 level 5** など）を入力します。変更されたすべての syslog メッセージの重大度をそれらの設定にリセットするには、**clear configure logging level** コマンドを入力します。

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　指定された重大度（1 ～ 7）を、指定の時間内でメッセージ セットまたは個々のメッセージ（出力先ではない）に適用します。

logging rate-limit {unlimited | {*num* [*interval*]}} message *syslog_id* | level *severity_level*

例：

```
ciscoasa(config)# logging rate-limit 1000 600 level 6
```

レート制限は、すべての設定された出力先に送信されるメッセージの量に影響します。ロギングのレート制限をデフォルト値にリセットするには、**clear running-config logging rate-limit** コマンドを入力します。ロギングのレート制限をリセットするには、**clear configure logging rate-limit** コマンドを入力します。

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、次のコマンドを参照してください。

- **show logging**

  このコマンドは、重大度を含む syslog メッセージを表示します。

  （注）　表示できる syslog メッセージの最大数は、1000 です。これはデフォルト設定です。表示できる syslog メッセージの最大数は、2000 です。

- **show logging message**

  このコマンドは、変更された重大度とディセーブルにされた syslog メッセージを含む syslog メッセージのリストを表示します。

- **show logging message** *message_ID*

  このコマンドは、特定の syslog メッセージの重大度を表示します。

- **show logging queue**

  このコマンドは、ロギング キューとキュー統計情報を表示します。

- **show logging rate-limit**

  このコマンドは、禁止された syslog メッセージを表示します。

- **show running-config logging rate-limit**

  このコマンドは、現在のロギング レート制限の設定を表示します。

ロギングの例

次の例は、**show logging** コマンドで表示されるロギング情報を示しています。

```
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address “10.1.1.1”
    Mail logging: disabled
    ASDM logging: disabled
```

次の例は、syslog メッセージをイネーブルにするかどうかを制御する方法と、指定した syslog メッセージの重大度を制御する方法を示しています。

```
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)

ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (disabled)

ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)
```

ロギングの履歴

表 39-2　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。
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。 **logging rate-limit** コマンドが導入されました。
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。 **logging list** コマンドが導入されました。
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。 **logging host** コマンドが変更されました。
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。 **logging class** コマンドが変更されました。
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。 **logging class** コマンドが変更されました。 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。 **clear logging queue bufferwrap** コマンドが導入されました。
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。 **logging ftp server** コマンドが変更されました。

表 39-2　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
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、**logging permit-hostdown** コマンドを使用します。 **show logging** コマンドが変更されました。 414005、414006、414007、414008 の各 syslog メッセージが導入されました。
クラスタ	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。 **logging device-id** コマンドが変更されました。

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」（P.40-1）
- 「SNMP のガイドライン」（P.40-19）
- 「SNMP の設定」（P.40-22）
- 「SNMP バージョン 1 および 2c の例」（P.40-32）
- 「SNMP バージョン 3 の例」（P.40-32）
- 「SNMP のモニタリング」（P.40-30）
- 「SNMP の履歴」（P.40-32）

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。

NMS 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 の管理情報ベース（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 40-1 に、SNMP で頻繁に使用される用語を示します。

表 40-1　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。
Trap	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。

MIB およびトラップ

MIB は、標準またはエンタープライズ固有です。標準 MIB はインターネット技術特別調査委員会（IETF）によって作成され、さまざまな Request for Comment（RFC）に記載されています。トラップは、ネットワーク デバイスで発生する重要なイベント（多くの場合、エラーまたは障害）を報告します。SNMP トラップは、標準またはエンタープライズ固有の MIB のいずれかで定義されます。標準トラップは IETF によって作成され、さまざまな RFC に記載されています。SNMP トラップは、ASA、ASAv、または ASASM ソフトウェアにコンパイルされています。

必要に応じて、次の場所から RFC、標準 MIB、および標準トラップをダウンロードすることもできます。

http://www.ietf.org/

ftp://ftp-sj.cisco.com/pub/mibs

次の場所から Cisco MIB、トラップ、および OID の完全なリストをダウンロードしてください。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

また、Cisco OID を次の場所から FTP でダウンロードしてください。

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

（注）　ソフトウェア バージョン 7.2(1)、8.0(2) 以降では、SNMP を介してアクセスされるインターフェイス情報は 5 秒ごとにリフレッシュされます。そのため、連続するポーリングの間に少なくとも 5 秒間は待機することをお勧めします。

MIB のすべての OID がサポートされているわけではありません。特定の ASA または ASASM に対してサポートされている SNMP MIB および OID のリストを取得するには、次のコマンドを入力します。

```
ciscoasa(config)# show snmp-server oidlist
```

（注）　**oidlist** キーワードは **show snmp-server** コマンドのヘルプのオプション リストには表示されませんが、使用できます。ただし、このコマンドは Cisco TAC でのみ使用されます。このコマンドを使用する前に TAC にお問い合わせください。

次に、**show snmp-server oidlist** コマンドの出力例を示します。

```
ciscoasa(config)# show snmp-server oidlist
[0]     1.3.6.1.2.1.1.1.        sysDescr
[1]     1.3.6.1.2.1.1.2.        sysObjectID
[2]     1.3.6.1.2.1.1.3.        sysUpTime
[3]     1.3.6.1.2.1.1.4.        sysContact
[4]     1.3.6.1.2.1.1.5.        sysName
[5]     1.3.6.1.2.1.1.6.        sysLocation
[6]     1.3.6.1.2.1.1.7.        sysServices
[7]     1.3.6.1.2.1.2.1.        ifNumber
[8]     1.3.6.1.2.1.2.2.1.1.    ifIndex
[9]     1.3.6.1.2.1.2.2.1.2.    ifDescr
[10]    1.3.6.1.2.1.2.2.1.3.    ifType
[11]    1.3.6.1.2.1.2.2.1.4.    ifMtu
[12]    1.3.6.1.2.1.2.2.1.5.    ifSpeed
[13]    1.3.6.1.2.1.2.2.1.6.    ifPhysAddress
[14]    1.3.6.1.2.1.2.2.1.7.    ifAdminStatus
[15]    1.3.6.1.2.1.2.2.1.8.    ifOperStatus
[16]    1.3.6.1.2.1.2.2.1.9.    ifLastChange
[17]    1.3.6.1.2.1.2.2.1.10.   ifInOctets
[18]    1.3.6.1.2.1.2.2.1.11.   ifInUcastPkts
[19]    1.3.6.1.2.1.2.2.1.12.   ifInNUcastPkts
[20]    1.3.6.1.2.1.2.2.1.13.   ifInDiscards
[21]    1.3.6.1.2.1.2.2.1.14.   ifInErrors
[22]    1.3.6.1.2.1.2.2.1.16.   ifOutOctets
[23]    1.3.6.1.2.1.2.2.1.17.   ifOutUcastPkts
[24]    1.3.6.1.2.1.2.2.1.18.   ifOutNUcastPkts
[25]    1.3.6.1.2.1.2.2.1.19.   ifOutDiscards
[26]    1.3.6.1.2.1.2.2.1.20.   ifOutErrors
[27]    1.3.6.1.2.1.2.2.1.21.   ifOutQLen
[28]    1.3.6.1.2.1.2.2.1.22.   ifSpecific
[29]    1.3.6.1.2.1.4.1.        ipForwarding
[30]    1.3.6.1.2.1.4.20.1.1.   ipAdEntAddr
[31]    1.3.6.1.2.1.4.20.1.2.   ipAdEntIfIndex
[32]    1.3.6.1.2.1.4.20.1.3.   ipAdEntNetMask
[33]    1.3.6.1.2.1.4.20.1.4.   ipAdEntBcastAddr
[34]    1.3.6.1.2.1.4.20.1.5.   ipAdEntReasmMaxSize
[35]    1.3.6.1.2.1.11.1.       snmpInPkts
[36]    1.3.6.1.2.1.11.2.       snmpOutPkts
[37]    1.3.6.1.2.1.11.3.       snmpInBadVersions
[38]    1.3.6.1.2.1.11.4.       snmpInBadCommunityNames
[39]    1.3.6.1.2.1.11.5.       snmpInBadCommunityUses
[40]    1.3.6.1.2.1.11.6.       snmpInASNParseErrs
```

```
[41]    1.3.6.1.2.1.11.8.       snmpInTooBigs
[42]    1.3.6.1.2.1.11.9.       snmpInNoSuchNames
[43]    1.3.6.1.2.1.11.10.      snmpInBadValues
[44]    1.3.6.1.2.1.11.11.      snmpInReadOnlys
[45]    1.3.6.1.2.1.11.12.      snmpInGenErrs
[46]    1.3.6.1.2.1.11.13.      snmpInTotalReqVars
[47]    1.3.6.1.2.1.11.14.      snmpInTotalSetVars
[48]    1.3.6.1.2.1.11.15.      snmpInGetRequests
[49]    1.3.6.1.2.1.11.16.      snmpInGetNexts
[50]    1.3.6.1.2.1.11.17.      snmpInSetRequests
[51]    1.3.6.1.2.1.11.18.      snmpInGetResponses
[52]    1.3.6.1.2.1.11.19.      snmpInTraps
[53]    1.3.6.1.2.1.11.20.      snmpOutTooBigs
[54]    1.3.6.1.2.1.11.21.      snmpOutNoSuchNames
[55]    1.3.6.1.2.1.11.22.      snmpOutBadValues
[56]    1.3.6.1.2.1.11.24.      snmpOutGenErrs
[57]    1.3.6.1.2.1.11.25.      snmpOutGetRequests
[58]    1.3.6.1.2.1.11.26.      snmpOutGetNexts
[59]    1.3.6.1.2.1.11.27.      snmpOutSetRequests
[60]    1.3.6.1.2.1.11.28.      snmpOutGetResponses
[61]    1.3.6.1.2.1.11.29.      snmpOutTraps
[62]    1.3.6.1.2.1.11.30.      snmpEnableAuthenTraps
[63]    1.3.6.1.2.1.11.31.      snmpSilentDrops
[64]    1.3.6.1.2.1.11.32.      snmpProxyDrops
[65]    1.3.6.1.2.1.31.1.1.1.1.ifName
[66]    1.3.6.1.2.1.31.1.1.1.2.ifInMulticastPkts
[67]    1.3.6.1.2.1.31.1.1.1.3.ifInBroadcastPkts
[68]    1.3.6.1.2.1.31.1.1.1.4.ifOutMulticastPkts
[69]    1.3.6.1.2.1.31.1.1.1.5.ifOutBroadcastPkts
[70]    1.3.6.1.2.1.31.1.1.1.6.ifHCInOctets
--More--
```

SNMP オブジェクト ID

シスコのシステムレベルの各製品には、MIB-II の sysObjectID として使用される SNMP オブジェクト ID（OID）があります。CISCO-PRODUCTS-MIB には SNMPv2-MIB の sysObjectID オブジェクトで報告可能な OID が含まれます。モデル タイプを識別するためにこの値を使用できます。表 40-2 に、ASA モデルの sysObjectID OID を示します。

表 40-2　SNMP オブジェクト ID

製品 ID	sysObjectID	モデル番号
ASA5585-SSP10	ciscoASA5585Ssp10（ciscoProducts 1194）	ASA 5585-X SSP-10
ASA5585-SSP20	ciscoASA5585Ssp20（ciscoProducts 1195）	ASA 5585-X SSP-20
ASA5585-SSP40	ciscoASA5585Ssp40（ciscoProducts 1196）	ASA 5585-X SSP-40
ASA5585-SSP60	ciscoASA5585Ssp60（ciscoProducts 1197）	ASA 5585-X SSP-60
ASA5585-SSP10	ciscoASA5585Ssp10sc（ciscoProducts 1198）	ASA 5585-X SSP-10 セキュリティ コンテキスト
ASA5585-SSP20	ciscoASA5585Ssp20sc（ciscoProducts 1199）	ASA 5585-X SSP-20 セキュリティ コンテキスト

表 40-2　SNMP オブジェクト ID （続き）

ASA5585-SSP40	ciscoASA5585Ssp40sc（ciscoProducts 1200）	ASA 5585-X SSP-40 セキュリティ コンテキスト
ASA5585-SSP60	ciscoASA5585Ssp60sc（ciscoProducts 1201）	ASA 5585-X SSP-60 セキュリティ コンテキスト
ASA5585-SSP10	ciscoASA5585Ssp10sy（ciscoProducts 1202）	ASA 5585-X SSP-10 システム コンテキスト
ASA5585-SSP20	ciscoASA5585Ssp20sy（ciscoProducts 1203）	ASA 5585-X SSP-20 システム コンテキスト
ASA5585-SSP40	ciscoASA5585Ssp40sy（ciscoProducts 1204）	ASA 5585-X SSP-40 システム コンテキスト
ASA5585-SSP60	ciscoASA5585Ssp60sy（ciscoProducts 1205）	ASA 5585-X SSP-60 システム コンテキスト
Catalyst スイッチ /7600 ルータ向け ASA サービス モジュール	ciscoAsaSm1（ciscoProducts 1277）	Catalyst スイッチ /7600 ルータ向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
Catalyst スイッチ /7600 ルータのセキュリティ コンテキスト向け ASA サービス モジュール	ciscoAsaSm1sc（ciscoProducts 1275）	Catalyst スイッチ /7600 ルータのセキュリティ コンテキスト向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
ペイロード暗号化なし Catalyst スイッチ /7600 ルータのセキュリティ コンテキスト向け ASA サービス モジュール	ciscoAsaSm1K7sc（ciscoProducts 1334）	ペイロード暗号化なし Catalyst スイッチ /7600 ルータのセキュリティ コンテキスト向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
Catalyst スイッチ /7600 ルータ システム コンテキスト向け ASA サービス モジュール	ciscoAsaSm1sy（ciscoProducts 1276）	Catalyst スイッチ /7600 ルータのシステム コンテキスト向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
ペイロード暗号化なし Catalyst スイッチのシステム コンテキスト /7600 ルータ向け ASA サービス モジュール	ciscoAsaSm1K7sy（ciscoProducts 1335）	ペイロード暗号化なし Catalyst スイッチ /7600 ルータのシステム コンテキスト向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
ペイロード暗号化なし Catalyst スイッチ /7600 ルータのシステム コンテキスト向け ASA サービス モジュール	ciscoAsaSm1K7（ciscoProducts 1336）	ペイロード暗号化なし Catalyst スイッチ /7600 ルータ向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
ASA 5512	ciscoASA5512（ciscoProducts 1407）	ASA 5512 適応型セキュリティ アプライアンス
ASA 5525	ciscoASA5525（ciscoProducts 1408）	ASA 5525 適応型セキュリティ アプライアンス
ASA 5545	ciscoASA5545（ciscoProducts 1409）	ASA 5545 適応型セキュリティ アプライアンス
ASA 5555	ciscoASA5555（ciscoProducts 1410）	ASA 5555 適応型セキュリティ アプライアンス

表 40-2　SNMP オブジェクト ID （続き）

ASA 5512 セキュリティ コンテキスト	ciscoASA5512sc（ciscoProducts 1411）	ASA 5512 適応型セキュリティ アプライアンスのセキュリティ コンテキスト
ASA 5525 セキュリティ コンテキスト	ciscoASA5525sc（ciscoProducts 1412）	ASA 5525 適応型セキュリティ アプライアンスのセキュリティ コンテキスト
ASA 5545 セキュリティ コンテキスト	ciscoASA5545sc（ciscoProducts 1413）	ASA 5545 適応型セキュリティ アプライアンスのセキュリティ コンテキスト
ASA 5555 セキュリティ コンテキスト	ciscoASA5555sc（ciscoProducts 1414）	ASA 5555 適応型セキュリティ アプライアンスのセキュリティ コンテキスト
ASA 5512 システム コンテキスト	ciscoASA5512sy（ciscoProducts 1415）	ASA 5512 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5515 システム コンテキスト	ciscoASA5515sy（ciscoProducts 1416）	ASA 5515 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5525 システム コンテキスト	ciscoASA5525sy（ciscoProducts1417）	ASA 5525 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5545 システム コンテキスト	ciscoASA5545sy（ciscoProducts 1418）	ASA 5545 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5555 システム コンテキスト	ciscoASA5555sy（ciscoProducts 1419）	ASA 5555 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5515 セキュリティ コンテキスト	ciscoASA5515sc（ciscoProducts 1420）	ASA 5515 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5515	ciscoASA5515（ciscoProducts 1421）	ASA 5515 適応型セキュリティ アプライアンス
ASAv	ciscoASAv（ciscoProducts 1902）	Cisco 適応型セキュリティ仮想アプライアンス（ASAv）
ASAv システム コンテキスト	ciscoASAvsy（ciscoProducts 1903）	Cisco 適応型セキュリティ仮想アプライアンス（ASAv）のシステム コンテキスト
ASAv セキュリティ コンテキスト	ciscoASAvsc（ciscoProducts 1904）	Cisco 適応型セキュリティ仮想アプライアンス（ASAv）のセキュリティ コンテキスト

物理ベンダー タイプ値

シスコの各シャーシまたはスタンドアロン システムには、SNMP で使用する一意のタイプ番号があります。entPhysicalVendorType OID は CISCO-ENTITY-VENDORTYPE-OID-MIB で定義されます。この値は、ASA、ASAv、または ASASM SNMP エージェントから entPhysicalVendorType オブジェクトで返されます。この値を使用してコンポーネントのタイプ（モジュール、電源装置、ファン、センサー、CPU など）を識別できます。表 40-3 に、ASA および ASASM モデルの物理ベンダー タイプ値を示します。

表 40-3　物理ベンダー タイプ値

項目	entPhysicalVendorType OID の説明
Catalyst スイッチ /7600 ルータ向け ASA サービス モジュール	cevCat6kWsSvcAsaSm1（cevModuleCat6000Type 169）
ペイロード暗号化なし Catalyst スイッチ /7600 ルータ向け ASA サービス モジュール	cevCat6kWsSvcAsaSm1K7（cevModuleCat6000Type 186）
Cisco Adaptive Security Appliance（ASA）5512 適応型セキュリティ アプライアンス	cevChassisASA5512（cevChassis 1113）
Cisco Adaptive Security Appliance（ASA）5512 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5512K7（cevChassis 1108）
Cisco Adaptive Security Appliance（ASA）5515 適応型セキュリティ アプライアンス	cevChassisASA5515（cevChassis 1114）
Cisco Adaptive Security Appliance（ASA）5515 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5515K7（cevChassis 1109）
Cisco Adaptive Security Appliance（ASA）5525 適応型セキュリティ アプライアンス	cevChassisASA5525（cevChassis 1115）
Cisco Adaptive Security Appliance（ASA）5525 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5525K7（cevChassis 1110）
Cisco Adaptive Security Appliance（ASA）5545 適応型セキュリティ アプライアンス	cevChassisASA5545（cevChassis 1116）
Cisco Adaptive Security Appliance（ASA）5545 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5545K7（cevChassis 1111）
Cisco Adaptive Security Appliance（ASA）5555 適応型セキュリティ アプライアンス	cevChassisASA5555（cevChassis 1117）
Cisco Adaptive Security Appliance（ASA）5555 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5555K7（cevChassis 1112）
Cisco Adaptive Security Appliance（ASA）5512 向け中央演算処理装置	cevCpuAsa5512（cevModuleCpuType 229）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5512 向け中央演算処理装置	cevCpuAsa5512K7（cevModuleCpuType 224）
Cisco Adaptive Security Appliance（ASA）5515 向け中央演算処理装置	cevCpuAsa5515（cevModuleCpuType 230）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5515 向け中央演算処理装置	cevCpuAsa5515K7（cevModuleCpuType 225）
Cisco Adaptive Security Appliance（ASA）5525 向け中央演算処理装置	cevCpuAsa5525（cevModuleCpuType 231）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5525 向け中央演算処理装置	cevCpuAsa5525K7（cevModuleCpuType 226）
Cisco Adaptive Security Appliance（ASA）5545 向け中央演算処理装置	cevCpuAsa5545（cevModuleCpuType 232）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5545 向け中央演算処理装置	cevCpuAsa5545K7（cevModuleCpuType 227）

表 40-3　物理ベンダー タイプ値 （続き）

Cisco Adaptive Security Appliance（ASA）5555 向け中央演算処理装置	cevCpuAsa5555（cevModuleCpuType 233）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5555 向け中央演算処理装置	cevCpuAsa5555K7（cevModuleCpuType 228）
ASA 5585 SSP-10 向け CPU	cevCpuAsa5585Ssp10（cevModuleCpuType 204）
ペイロード暗号化なし ASA 5585 SSP-10 向け CPU	cevCpuAsa5585Ssp10K7（cevModuleCpuType 205）
ASA 5585 SSP-20 向け CPU	cevCpuAsa5585Ssp20（cevModuleCpuType 206）
ペイロード暗号化なし ASA 5585 SSP-20 向け CPU	cevCpuAsa5585Ssp20K7（cevModuleCpuType 207）
ASA 5585 SSP-40 向け CPU	cevCpuAsa5585Ssp40（cevModuleCpuType 208）
ペイロード暗号化なし ASA 5585 SSP-40 向け CPU	cevCpuAsa5585Ssp40K7（cevModuleCpuType 209）
ASA 5585 SSP-60 向け CPU	cevCpuAsa5585Ssp60（cevModuleCpuType 210）
ペイロード暗号化なし ASA 5585 SSP-60 向け CPU	cevCpuAsa5585Ssp60K（cevModuleCpuType 211）
Catalyst スイッチ /7600 ルータ向け Cisco ASA サービス モジュール向け CPU	cevCpuAsaSm1（cevModuleCpuType 222）
Catalyst スイッチ /7600 ルータ向けペイロード暗号化なし Cisco ASA サービス モジュール向け CPU	cevCpuAsaSm1K7（cevModuleCpuType 223）
適応型セキュリティ アプライアンス 5512 シャーシ冷却ファン	cevFanASA5512ChassisFan（cevFan 163）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5512 シャーシ冷却ファン	cevFanASA5512K7ChassisFan（cevFan 172）
適応型セキュリティ アプライアンス 5515 シャーシ冷却ファン	cevFanASA5515ChassisFan（cevFan 164）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5515 シャーシ冷却ファン	cevFanASA5515K7ChassisFan（cevFan 171）
適応型セキュリティ アプライアンス 5525 シャーシ冷却ファン	cevFanASA5525ChassisFan（cevFan 165）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5525 シャーシ冷却ファン	cevFanASA5525K7ChassisFan（cevFan 170）
適応型セキュリティ アプライアンス 5545 シャーシ冷却ファン	cevFanASA5545ChassisFan（cevFan 166）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 シャーシ冷却ファン	cevFanASA5545K7ChassisFan（cevFan 169）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 電源ファン	cevFanASA5545K7PSFan（cevFan 161）
適応型セキュリティ アプライアンス 5545 電源ファン	cevFanASA5545PSFan（cevFan 159）
適応型セキュリティ アプライアンス 5555 シャーシ冷却ファン	cevFanASA5555ChassisFan（cevFan 167）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 シャーシ冷却ファン	cevFanASA5555K7ChassisFan（cevFan 168）
適応型セキュリティ アプライアンス 5555 電源ファン	cevFanASA5555PSFan（cevFan 160）

表 40-3　物理ベンダー タイプ値 （続き）

ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 電源ファン	cevFanASA5555PSFanK7（cevFan 162）
ASA 5585-X 向け電源ファン	cevFanASA5585PSFan（cevFan 146）
10 ギガビット イーサネット インターフェイス	cevPort10GigEthernet（cevPort 315）
ギガビット イーサネット ポート	cevPortGe（cevPort 109）
適応型セキュリティ アプライアンス 5545 電源装置	cevPowerSupplyASA5545PSInput（cevPowerSupply 323）
適応型セキュリティ アプライアンス 5545 電源入力のプレゼンス センサー	cevPowerSupplyASA5545PSPresence（cevPowerSupply 321）
適応型セキュリティ アプライアンス 5555 電源装置	cevPowerSupplyASA5555PSInput（cevPowerSupply 324）
適応型セキュリティ アプライアンス 5555 電源入力のプレゼンス センサー	cevPowerSupplyASA5555PSPresence（cevPowerSupply 322）
ASA 5585 向け電源入力	cevPowerSupplyASA5585PSInput（cevPowerSupply 304）
Cisco Adaptive Security Appliance（ASA）5512 シャーシ ファン センサー	cevSensorASA5512ChassisFanSensor（cevSensor 120）
Cisco Adaptive Security Appliance（ASA）5512 向けシャーシ周囲温度センサー	cevSensorASA5512ChassisTemp（cevSensor 107）
Cisco Adaptive Security Appliance（ASA）5512 向け中央演算処理装置温度センサー	cevSensorASA5512CPUTemp（cevSensor 96）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5512 シャーシ ファン センサー	cevSensorASA5512K7ChassisFanSensor（cevSensor 125）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5512 向け中央演算処理装置温度センサー	cevSensorASA5512K7CPUTemp（cevSensor 102）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5512 シャーシ冷却ファンのセンサー	cevSensorASA5512K7PSFanSensor（cevSensor 116）
適応型セキュリティ アプライアンス 5512 シャーシ冷却ファンのセンサー	cevSensorASA5512PSFanSensor（cevSensor 119）
Cisco Adaptive Security Appliance（ASA）5515 シャーシ ファン センサー	cevSensorASA5515ChassisFanSensor（cevSensor 121）
Cisco Adaptive Security Appliance（ASA）5515 向けシャーシ周囲温度センサー	cevSensorASA5515ChassisTemp（cevSensor 98）
Cisco Adaptive Security Appliance（ASA）5515 向け中央演算処理装置温度センサー	cevSensorASA5515CPUTemp（cevSensor 97）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5515 シャーシ ファン センサー	cevSensorASA5515K7ChassisFanSensor（cevSensor 126）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5515 向け中央演算処理装置温度センサー	cevSensorASA5515K7CPUTemp（cevSensor 103）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5515 シャーシ冷却ファンのセンサー	cevSensorASA5515K7PSFanSensor（cevSensor 115）
適応型セキュリティ アプライアンス 5515 シャーシ冷却ファンのセンサー	cevSensorASA5515PSFanSensor（cevSensor 118）
Cisco Adaptive Security Appliance（ASA）5525 シャーシ ファン センサー	cevSensorASA5525ChassisFanSensor（cevSensor 122）

表 40-3　物理ベンダー タイプ値 （続き）

Cisco Adaptive Security Appliance（ASA）5525 向け シャーシ周囲温度センサー	cevSensorASA5525ChassisTemp（cevSensor 108）
Cisco Adaptive Security Appliance（ASA）5525 向け中央演算処理装置温度センサー	cevSensorASA5525CPUTemp（cevSensor 99）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5525 シャーシ ファン センサー	cevSensorASA5525K7ChassisFanSensor（cevSensor 127）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5525 向け中央演算処理装置温度センサー	cevSensorASA5525K7CPUTemp（cevSensor 104）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5525 シャーシ冷却ファンのセンサー	cevSensorASA5525K7PSFanSensor（cevSensor 114）
適応型セキュリティ アプライアンス 5525 シャーシ冷却ファンのセンサー	cevSensorASA5525PSFanSensor（cevSensor 117）
Cisco Adaptive Security Appliance（ASA）5545 シャーシ ファン センサー	cevSensorASA5545ChassisFanSensor（cevSensor 123）
Cisco Adaptive Security Appliance（ASA）5545 向け シャーシ周囲温度センサー	cevSensorASA5545ChassisTemp（cevSensor 109）
Cisco Adaptive Security Appliance（ASA）5545 向け中央演算処理装置温度センサー	cevSensorASA5545CPUTemp（cevSensor 100）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5545 シャーシ ファン センサー	cevSensorASA5545K7ChassisFanSensor（cevSensor 128）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5545 向けシャーシ周囲温度センサー	cevSensorASA5545K7ChassisTemp（cevSensor 90）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5545 向け中央演算処理装置温度センサー	cevSensorASA5545K7CPUTemp（cevSensor 105）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 シャーシ冷却ファンのセンサー	cevSensorASA5545K7PSFanSensor（cevSensor 113）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 電源入力のプレゼンス センサー	cevSensorASA5545K7PSPresence（cevSensor 87）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 電源ファンの温度センサー	cevSensorASA5545K7PSTempSensor（cevSensor 94）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 電源ファンのセンサー	cevSensorASA5545PSFanSensor（cevSensor 89）
適応型セキュリティ アプライアンス 5545 電源入力のプレゼンス センサー	cevSensorASA5545PSPresence（cevSensor 130）
適応型セキュリティ アプライアンス 5555 電源入力のプレゼンス センサー	cevSensorASA5545PSPresence（cevSensor 131）
適応型セキュリティ アプライアンス 5545 電源ファンの温度センサー	cevSensorASA5545PSTempSensor（cevSensor 92）
Cisco Adaptive Security Appliance（ASA）5555 シャーシ ファン センサー	cevSensorASA5555ChassisFanSensor（cevSensor 124）
Cisco Adaptive Security Appliance（ASA）5555 向け シャーシ周囲温度センサー	cevSensorASA5555ChassisTemp（cevSensor 110）

表 40-3　物理ベンダー タイプ値 （続き）

Cisco Adaptive Security Appliance（ASA）5555 向け中央演算処理装置温度センサー	cevSensorASA5555CPUTemp（cevSensor 101）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5555 シャーシ ファン センサー	cevSensorASA5555K7ChassisFanSensor（cevSensor 129）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5555 向けシャーシ周囲温度センサー	cevSensorASA5555K7ChassisTemp（cevSensor 111）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5555 向け中央演算処理装置温度センサー	cevSensorASA5555K7CPUTemp（cevSensor 106）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 シャーシ冷却ファンのセンサー	cevSensorASA5555K7PSFanSensor（cevSensor 112）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 電源入力のプレゼンス センサー	cevSensorASA5555K7PSPresence（cevSensor 88）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 電源ファンの温度センサー	cevSensorASA5555K7PSTempSensor（cevSensor 95）
適応型セキュリティ アプライアンス 5555 電源ファンのセンサー	cevSensorASA5555PSFanSensor（cevSensor 91）
適応型セキュリティ アプライアンス 5555 電源ファンの温度センサー	cevSensorASA5555PSTempSensor（cevSensor 93）
ASA 5585-X 向け電源ファン	cevSensorASA5585PSFanSensor（cevSensor 86）
ASA 5585-X 向け電源入力のセンサー	cevSensorASA5585PSInput（cevSensor 85）
ASA 5585 SSP-10 向け CPU 温度センサー	cevSensorASA5585SSp10CPUTemp（cevSensor 77）
ペイロード暗号化なし ASA 5585 SSP-10 向け CPU 温度センサー	cevSensorASA5585SSp10K7CPUTemp（cevSensor 78）
ASA 5585 SSP-20 向け CPU 温度センサー	cevSensorASA5585SSp20CPUTemp（cevSensor 79）
ペイロード暗号化なし ASA 5585 SSP-20 向け CPU 温度センサー	cevSensorASA5585SSp20K7CPUTemp（cevSensor 80）
ASA 5585 SSP-40 向け CPU 温度センサー	cevSensorASA5585SSp40CPUTemp（cevSensor 81）
ペイロード暗号化なし ASA 5585 SSP-40 向け CPU 温度センサー	cevSensorASA5585SSp40K7CPUTemp（cevSensor 82）
ASA 5585 SSP-60 向け CPU 温度センサー	cevSensorASA5585SSp60CPUTemp（cevSensor 83）
ペイロード暗号化なし ASA 5585 SSP-60 向け CPU 温度センサー	cevSensorASA5585SSp60K7CPUTemp（cevSensor 84）
適応型セキュリティ アプライアンス 5555-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5555XFRSSD (cevModuleCommonCards 396)
適応型セキュリティ アプライアンス 5545-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5545XFRSSD (cevModuleCommonCards 397)
適応型セキュリティ アプライアンス 5525-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5525XFRSSD (cevModuleCommonCards 398)

表 40-3　物理ベンダー タイプ値 （続き）

適応型セキュリティ アプライアンス 5515-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5515XFRSSD (cevModuleCommonCards 399)
適応型セキュリティ アプライアンス 5512-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5512XFRSSD (cevModuleCommonCards 400)
Cisco 適応型セキュリティ仮想アプライアンス	cevChassisASAv（cevChassis 1451）

MIB でサポートされているテーブルとオブジェクト

表 40-4 に、指定された MIB でサポートされるテーブルおよびオブジェクトを示します。

表 40-4　MIB でサポートされているテーブルとオブジェクト

MIB 名	サポートされているテーブルとオブジェクト
CISCO-ENHANCED-MEMPOOL-MIB	cempMemPoolTable、cempMemPoolIndex、cempMemPoolType、cempMemPoolName、cempMemPoolAlternate、cempMemPoolValid、cempMemPoolUsed、cempMemPoolFree、cempMemPoolUsedOvrflw、cempMemPoolHCUsed、cempMemPoolFreeOvrflw、cempMemPoolHCFree
CISCO-ENTITY-SENSOR-EXT-MIB （注）　Catalyst 6500 スイッチ /7600 ルータ向け ASA サービス モジュールではサポートされていません。	ceSensorExtThresholdTable
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB	ciscoL4L7ResourceLimitTable
CISCO-TRUSTSEC-SXP-MIB （注）　Cisco 適応型セキュリティ仮想アプライアンス（ASAv）ではサポートされていません。	ctsxSxpGlobalObjects、ctsxSxpConnectionObjects、ctsxSxpSgtObjects
DISMAN-EVENT-MIB	mteTriggerTable、mteTriggerThresholdTable、mteObjectsTable、mteEventTable、mteEventNotificationTable
DISMAN-EXPRESSION-MIB （注）　Catalyst 6500 スイッチ /7600 ルータ向け ASA サービス モジュールではサポートされていません。	expExpressionTable、expObjectTable、expValueTable
ENTITY-SENSOR-MIB （注）　Catalyst 6500 スイッチ /7600 ルータ向け ASA サービス モジュールではサポートされていません。	entPhySensorTable
NAT-MIB	natAddrMapTable、natAddrMapIndex、natAddrMapName、natAddrMapGlobalAddrType、natAddrMapGlobalAddrFrom、natAddrMapGlobalAddrTo、natAddrMapGlobalPortFrom、natAddrMapGlobalPortTo、natAddrMapProtocol、natAddrMapAddrUsed、natAddrMapRowStatus

サポートされているトラップ（通知）

表 40-5 に、サポートされているトラップ（通知）および関連する MIB を示します。

表 40-5　サポートされているトラップ（通知）

トラップおよび MIB 名	変数バインド リスト	説明
authenticationFailure （SNMPv2-MIB）	—	SNMP バージョン 1 または 2 の場合は、SNMP 要求で指定されたコミュニティ ストリングが正しくありません。SNMP バージョン 3 では、auth または priv パスワードまたはユーザ名が間違っている場合、レポート PDU がトラップの代わりに生成されます。 **snmp-server enable traps snmp authentication** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
cefcFRUInserted （CISCO-ENTITY-FRU-CONTROL-MIB）	—	**snmp-server enable traps entity fru-insert** コマンドはこの通知をイネーブルにするために使用されます。
cefcFRURemoved （CISCO-ENTITY-FRU-CONTROL-MIB）	—	**snmp-server enable traps entity fru-remove** コマンドはこの通知をイネーブルにするために使用されます。

表 40-5　サポートされているトラップ（通知）（続き）

ceSensorExtThresholdNotification （CISCO-ENTITY-SENSOR-EXT-MIB） （注）　Catalyst 6500 スイッチ /7600 ルータ向け ASA サービス モジュールではサポートされていません。	ceSensorExtThresholdValue、entPhySensorValue、entPhySensorType、entPhysicalName	**snmp-server enable traps entity [power-supply-failure | fan-failure | cpu-temperature]** コマンドは、エンティティしきい値通知の伝送をイネーブルにするために使用されます。この通知は、電源障害に対して送信されます。送信されるオブジェクトは、ファンおよび CPU の温度を指定します。 **snmp-server enable traps entity fan-failure** コマンドは、ファン障害トラップの送信をイネーブルにするために使用されます。 **snmp-server enable traps entity power-supply-failure** コマンドは、電源障害トラップの送信をイネーブルにするために使用されます。 **snmp-server enable traps entity chassis-fan-failure** コマンドは、シャーシファン障害トラップの送信をイネーブルにするために使用されます。 **snmp-server enable traps entity cpu-temperature** コマンドは、高 CPU 温度トラップの送信をイネーブルにするために使用されます。 **snmp-server enable traps entity power-supply-presence** コマンドは、電源プレゼンス障害トラップの送信をイネーブルにするために使用されます。 **snmp-server enable traps entity power-supply-temperature** コマンドは、電源温度しきい値トラップの送信をイネーブルにするために使用されます。 **snmp-server enable traps entity chassis-temperature** コマンドは、シャーシ周囲温度トラップの送信をイネーブルにするために使用されます。
cipSecTunnelStart （CISCO-IPSEC-FLOW-MONITOR-MIB）	cipSecTunLifeTime、cipSecTunLifeSize	**snmp-server enable traps ipsec start** コマンドは、このトラップの送信をイネーブルにするために使用されます。
cipSecTunnelStop （CISCO-IPSEC-FLOW-MONITOR-MIB）	cipSecTunActiveTime	**snmp-server enable traps ipsec stop** コマンドは、このトラップの送信をイネーブルにするために使用されます。
ciscoRasTooManySessions （CISCO-REMOTE-ACCESS-MONITOR-MIB）	crasNumSessions、crasNumUsers、crasMaxSessionsSupportable、crasMaxUsersSupportable、crasThrMaxSessions	**snmp-server enable traps remote-access session-threshold-exceeded** コマンドは、これらのトラップの送信をイネーブルにするために使用されます。

表 40-5　サポートされているトラップ（通知）（続き）

clogMessageGenerated （CISCO-SYSLOG-MIB）	clogHistFacility、clogHistSeverity、clogHistMsgName、clogHistMsgText、clogHistTimestamp	syslog メッセージが生成されます。 clogMaxSeverity オブジェクトの値は、トラップとして送信する syslog メッセージを決定するために使用されます。 **snmp-server enable traps syslog** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
clrResourceLimitReached （CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB）	crlResourceLimitValueType、crlResourceLimitMax、clogOriginIDType、clogOriginID	**snmp-server enable traps connection-limit-reached** コマンドは、接続制限に達した通知の送信をイネーブルにするために使用されます。clogOriginID オブジェクトには、トラップを発信したコンテキスト名が含まれています。
coldStart （SNMPv2-MIB）	—	SNMP エージェントが起動されました。 **snmp-server enable traps snmp coldstart** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
cpmCPURisingThreshold （CISCO-PROCESS-MIB）	cpmCPURisingThresholdValue、cpmCPUTotalMonIntervalValue、cpmCPUInterruptMonIntervalValue, cpmCPURisingThresholdPeriod、cpmProcessTimeCreated、cpmProcExtUtil5SecRev	**snmp-server enable traps cpu threshold rising** コマンドは、cpu threshold rising 通知の送信をイネーブルにするために使用されます。cpmCPURisingThresholdPeriod オブジェクトは、他のオブジェクトとともに送信されます。
entConfigChange （ENTITY-MIB）	—	**snmp-server enable traps entity config-change fru-insert fru-remove** コマンドは、この通知をイネーブルにするために使用されます。 **（注）** この通知は、セキュリティ コンテキストが作成または削除された場合にマルチ モードでのみ送信されます。
linkDown （IF-MIB）	ifIndex、ifAdminStatus、ifOperStatus	インターフェイスのリンクダウン トラップ。 **snmp-server enable traps snmp linkdown** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
linkUp （IF-MIB）	ifIndex、ifAdminStatus、ifOperStatus	インターフェイスのリンクアップ トラップ。 **snmp-server enable traps snmp linkup** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。

表 40-5　サポートされているトラップ（通知）（続き）

mteTriggerFired （DISMAN-EVENT-MIB）	mteHotTrigger、 mteHotTargetName、 mteHotContextName、mteHotOID、 mteHotValue、 cempMemPoolName、 cempMemPoolHCUsed	**snmp-server enable traps memory-threshold** コマンドは、memory threshold 通知をイネーブルにするために使用されます。mteHotOID が cempMemPoolHCUsed に設定されます。cempMemPoolName および cempMemPoolHCUsed オブジェクトは、他のオブジェクトとともに送信されます。
mteTriggerFired （DISMAN-EVENT-MIB） （注）　Catalyst 6500 スイッチ /7600 ルータ向け ASA サービス モジュールではサポートされていません。	mteHotTrigger、 mteHotTargetName、 mteHotContextName、mteHotOID、 mteHotValue、ifHCInOctets、 ifHCOutOctets、ifHighSpeed、 entPhysicalName	**snmp-server enable traps interface-threshold** コマンドは、interface threshold 通知をイネーブルにするために使用されます。entPhysicalName オブジェクトは、他のオブジェクトと共に送信されます。
natPacketDiscard （NAT-MIB）	ifIndex	**snmp-server enable traps nat packet-discard** コマンドは、NAT packet discard 通知をイネーブルにするために使用されます。この通知は、マッピング スペースを使用できないため、5 分間にレート制限され、IP パケットが NAT により廃棄された場合に生成されます。ifIndex は、マッピング インターフェイスの ID を提供します。
warmStart （SNMPv2-MIB）	—	**snmp-server enable traps snmp warmstart** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。

インターフェイスの種類と例

SNMP トラフィック統計情報を生成するインターフェイスの種類には次のものがあります。

- 論理：物理統計情報のサブセットであり、ソフトウェア ドライバによって収集される統計情報。
- 物理：ハードウェア ドライバによって収集される統計情報。物理的な名前の付いた各インターフェイスは、それに関連付けられている論理統計情報と物理統計情報のセットを 1 つ持っています。各物理インターフェイスは、関連付けられている VLAN インターフェイスを複数持っている場合があります。VLAN インターフェイスは論理統計情報だけを持っています。

（注）　複数の VLAN インターフェイスが関連付けられている物理インターフェイスでは、ifInOctets と ifOutoctets の OID の SNMP カウンタがその物理インターフェイスの集約トラフィック カウンタと一致していることに注意してください。

- VLAN だけ：SNMP は ifInOctets と ifOutOctets に対して論理統計情報を使用します。

表 40-6 の例で、SNMP トラフィック統計情報における差異を示します。例 1 では、**show interface** コマンドと **show traffic** コマンドの物理出力統計情報と論理出力統計情報の差異を示します。例 2 では、**show interface** コマンドと **show traffic** コマンドの VLAN だけのインターフェイスに対する出力統計情報を示します。この例は、統計情報が **show traffic** コマンドに対して表示される出力に近いことを示しています。

表 40-6　物理インターフェイスと VLAN インターフェイスの SNMP トラフィック統計情報

例 1

```
ciscoasa# show interface GigabitEthernet3/2
interface GigabitEthernet3/2
    description fullt-mgmt
    nameif mgmt
    security-level 10
    ip address 10.7.14.201 255.255.255.0
    management-only

ciscoasa# show traffic
(Condensed output)

Physical Statistics
GigabitEthernet3/2:
    received (in 121.760 secs)
        36 packets       3428 bytes
        0 pkts/sec       28 bytes/sec

Logical Statistics
mgmt:
    received (in 117.780 secs)
        36 packets       2780 bytes
        0 pkts/sec       23 bytes/sec
```

次の例は、管理インターフェイスと物理インターフェイスの SNMP 出力統計情報を示しています。ifInOctets 値は、**show traffic** コマンド出力で表示される物理統計情報出力に近くなりますが、論理統計情報出力には近くなりません。

mgmt インターフェイスの ifIndex：

```
IF_MIB::ifDescr.6 = Adaptive Security Appliance 'mgmt'
interface
```

物理インターフェイス統計情報に対応する ifInOctets：

```
IF-MIB::ifInOctets.6 = Counter32:3246
```

例 2

```
ciscoasa# show interface GigabitEthernet0/0.100
interface GigabitEthernet0/0.100
    vlan 100
    nameif inside
    security-level 100
    ip address 10.7.1.101 255.255.255.0 standby
    10.7.1.102

ciscoasa# show traffic
inside
    received (in 9921.450 secs)
        1977 packets       126528 bytes
        0 pkts/sec       12 bytes/sec
    transmitted (in 9921.450 secs)
        1978 packets       126556 bytes
        0 pkts/sec       12 bytes/sec
```

内部の VLAN の ifIndex：

```
IF-MIB::ifDescr.9 = Adaptive Security Appliance
'inside' interface
IF-MIB::ifInOctets.9 = Counter32: 126318
```

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-server host** コマンドを追加した後に、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。
- 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。

トラブルシューティングのヒント

- NMS からの着信パケットを受信する SNMP プロセスが実行されていることを確認するには、次のコマンドを入力します。

```
ciscoasa(config)# show process | grep snmp
```

- SNMP からの syslog メッセージをキャプチャし、それらを ASA、ASAv、または ASASM コンソールに表示するには、次のコマンドを入力します。

```
ciscoasa(config)# logging list snmp message 212001-212015
ciscoasa(config)# logging console snmp
```

- SNMP プロセスがパケットを送受信していることを確認するには、次のコマンドを入力します。

```
ciscoasa(config)# clear snmp-server statistics
ciscoasa(config)# show snmp-server statistics
```

  出力は SNMPv2-MIB の SNMP グループに基づきます。

- SNMP パケットが ASA、ASAv、または ASASM を通過し、SNMP プロセスに送信されていることを確認するには、次のコマンドを入力します。

```
ciscoasa(config)# clear asp drop
ciscoasa(config)# show asp drop
```

- NMS が正常にオブジェクトを要求できない場合、または ASA、ASAv、または ASASM からの着信トラップを正しく処理していない場合は、次のコマンドを入力して問題を分離するためにパケット キャプチャを使用します。

```
ciscoasa (config)# access-list snmp permit udp any eq snmptrap any
ciscoasa (config)# access-list snmp permit udp any any eq snmp
ciscoasa (config)# capture snmp type raw-data access-list snmp interface mgmt
ciscoasa (config)# copy /pcap capture:snmp tftp://192.0.2.5/exampledir/snmp.pcap
```

- ASA、ASAv、または ASASM が予期したとおりに実行していない場合は、次の操作を実行して、ネットワーク トポロジとトラフィックに関する情報を取得します。
  - NMS の設定について、次の情報を取得します。

    タイムアウトの回数

    リトライ回数

    エンジン ID キャッシング

    使用されるユーザ名とパスワード
  - 次のコマンドを発行します。

    show block

    show interface

    show process

    show cpu

    show vm

- 重大エラーが発生した場合は、エラーの再現を支援するために、Cisco TAC にトレースバック ファイルと **show tech-support** コマンドの出力を送信します。
- SNMP トラフィックが ASA、ASAv、または ASASM インターフェイスを通過できない場合、**icmp permit** コマンドを使用して、リモート SNMP サーバから ICMP トラフィックを許可しなければならないことがあります。

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.40-22）を参照してください。

ステップ 2　SNMP トラップを設定します。「SNMP トラップの設定」（P.40-22）を参照してください。

ステップ 3　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.40-24）または「SNMP バージョン 3 のパラメータの設定」（P.40-26）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　ASA、ASAv、または ASASM で SNMP エージェントおよび SNMP サーバをイネーブルにします。デフォルトでは、SNMP サーバはイネーブルになっています。

```
snmp-server enable
```

例：

```
ciscoasa(config)# snmp-server enable
```

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　個別のトラップ、トラップのセット、またはすべてのトラップを NMS に送信します。

```
snmp-server enable traps [all | syslog | snmp [authentication | linkup | linkdown |
coldstart | warmstart] |  | entity [config-change | fru-insert | fru-remove | fan-failure
| cpu-temperature | chassis-fan- failure | power-supply-failure] | chassis-temperature |
power-supply-presence | power-supply-temperature |] | ikev2 [start | stop] |ipsec [start |
stop] | remote-access [session-threshold-exceeded]| connection-limit-reached | cpu
threshold rising | interface-threshold | memory-threshold | nat [packet-discard]
```

例：

```
ciscoasa(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart
warmstart
```

このコマンドでは、トラップとして NMS に送信する syslog メッセージをイネーブルにしています。デフォルト コンフィギュレーションでは、例に示すように、すべての SNMP 標準トラップがイネーブルになっています。これらのトラップをディセーブルにするには、**no snmp-server enable traps snmp** コマンドを使用します。このコマンドを入力するときにトラップ 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。デフォルトでは、**syslog** トラップはイネーブルになっています。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。syslog MIB からのトラップを生成するには、**logging history** コマンドと **snmp-server enable traps syslog** コマンドの両方を設定する必要があります。SNMP トラップがイネーブルにされたデフォルトの状態を復元するには、**clear configure snmp-server** コマンドを使用します。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。

管理コンテキストでのみ使用できるトラップ：

- **connection-limit-reached**
- **entity**
- **memory-threshold**

システム コンテキストの物理的に接続されたインターフェイスに対してだけ管理コンテキストを介して生成されたトラップ：

- **interface-threshold**

（注）　**interface-threshold** トラップは Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。

その他すべてのトラップは、シングル モードの管理およびユーザ コンテキストで使用できます。

マルチ コンテキスト モードでは、**fan-failure** トラップ、**power-supply-failure** トラップ、および **cpu-temperature** トラップは、ユーザ コンテキストではなく管理コンテキストからのみ生成されます（ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X にのみ適用されます）。

CPU 使用率が、設定されたモニタリング期間の設定されたしきい値を超える場合、**cpu threshold rising** トラップが生成されます。

使用されたシステム コンテキストのメモリが総システム メモリの 80 % に達すると、**memory-threshold** トラップが管理コンテキストから生成されます。他のすべてのユーザ コンテキストでは、このトラップは使用メモリが特定のコンテキストの総システム メモリの 80 % に到達した場合に生成されます。

（注）　SNMP は電圧センサーをモニタしません。

CPU 使用率のしきい値の設定

CPU 使用率のしきい値を設定するには、次の手順を実行します。

手順

ステップ 1　高 CPU しきい値の値とモニタリング期間を設定します。

snmp cpu threshold rising *threshold_value monitoring_period*

例：

```
ciscoasa(config)# snmp cpu threshold rising 75% 30 minutes
```

CPU 使用率のしきい値およびモニタリング期間をクリアするには、このコマンドの **no** 形式を使用します。**snmp cpu threshold rising** コマンドが設定されていない場合、上限しきい値レベルのデフォルトは 70 % を超え、クリティカルしきい値レベルのデフォルトは 95 % を超えます。デフォルトのモニタリング期間は 1 分に設定されます。

CPU のクリティカルしきい値レベルは設定できません。この値は 95 % に固定されています。高 CPU しきい値の有効値の範囲は 10 ～ 94 % です。モニタリング期間の有効値は 1～60 分です。

物理インターフェイスのしきい値の設定

物理インターフェイスのしきい値を設定するには、次の手順を実行します。

手順

ステップ 1　SNMP 物理インターフェイスのしきい値を設定します。

snmp interface threshold *threshold_value*

例：

```
ciscoasa(config)# snmp interface threshold 75%
```

SNMP 物理インターフェイスのしきい値をクリアするには、このコマンドの **no** 形式を使用します。しきい値は、インターフェイス帯域幅利用率の割合として定義されます。有効なしきい値の範囲は 30～99 % です。デフォルト値は 70 % です。

snmp interface threshold コマンドは、管理コンテキストでのみ使用できます。

物理インターフェイスの使用状況はシングル モードおよびマルチ モードでモニタされ、システム コンテキストの物理インターフェイスのトラップは管理コンテキストを通して送信されます。物理インターフェイスだけがしきい値の使用状況を計算するために使用されます。

（注）　このコマンドは、Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。

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　SNMP 通知の受信者を指定し、トラップの送信元のインターフェイスを指定し、ASA に接続できる NMS または SNMP マネージャの名前および IP アドレスを指定します。

snmp-server host {*interface hostname* | *ip_address*} [**trap** | **poll**] [**community** *community-string*] [**version** {*1* | **2c** *username*}] [**udp-port** *port*]

例：

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 2

ciscoasa(config)# snmp-server host corp 172.18.154.159 community public
```

trap キーワードは、NMS をトラップの受信だけに制限します。**poll** キーワードは、NMS を要求の送信（ポーリング）だけに制限します。デフォルトでは、SNMP トラップはイネーブルになっています。デフォルトでは、UDP ポートは 162 です。コミュニティ ストリングは、ASA、ASAv、または ASASM と NMS の間の共有秘密キーです。キーは、大文字と小文字が区別される最大 32 文字の英数字の値です。スペースは使用できません。デフォルトのコミュニティ ストリングは public です。ASA では、このキーを使用して着信 SNMP 要求が有効かどうかを判別します。たとえば、コミュニティ ストリングを使用してサイトを指定すると、ASA と管理ステーションを同じストリングを使用して設定できます。ASA、ASAv、および ASASM は指定したストリングを使用し、無効なコミュニティ ストリングでの要求には応答しません。暗号化されたコミュニティ ストリングを使用した後は、暗号化された形式だけがすべてのシステム（CLI、ASDM、CSM など）に表示されます。クリア テキストのパスワードは表示されません。暗号化されたコミュニティ ストリングは常に ASA によって生成されます。通常は、クリア テキストの形式で入力します。

（注） ASA ソフトウェアをバージョン 8.3(1) から下のバージョンにダウングレードし、暗号化されたパスワードを設定した場合、まず **no key config-key password encryption** コマンドを使用して暗号化されたパスワードをクリア テキストに戻してから結果を保存する必要があります。

トラップを受信するには、**snmp-server host** コマンドを追加した後に、ASA、ASAv、および ASASM で設定されたクレデンシャルと同じクレデンシャルを使用して NMS でユーザを確実に設定するようにします。

ステップ 2　SNMP バージョン 1 または 2c *だけ*で使用するコミュニティ ストリングを設定します。

snmp-server community *community-string*

例：

```
ciscoasa(config)# snmp-server community onceuponatime
```

ステップ 3　SNMP サーバの場所または担当者情報を設定します。

snmp-server [**contact** | **location**] *text*

例：

```
ciscoasa(config)# snmp-server location building 42

ciscoasa(config)# snmp-server contact EmployeeA
```

text 引数には、担当者または ASA システム管理者の名前を指定します。名前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 4　SNMP 要求のリスニング ポートを設定します。

snmp-server listen-port *lport*

例：

```
ciscoasa(config)# snmp-server lport 192
```

lport 引数には、着信要求を受け取るポートを指定します。デフォルトのリスニング ポートは 161 です。**snmp-server listen-port** コマンドは管理コンテキストでのみ使用でき、システム コンテキストでは使用できません。現在使用中のポートで **snmp-server listen-port** コマンドを設定すると、次のメッセージが表示されます。

警告　The UDP port *port* is in use by another feature.SNMP requests to the device will fail until the snmp-server listen-port command is configured to use a different port.

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

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　SNMP バージョン 3 *だけ*で使用する、新しい SNMP グループを指定します。

```
snmp-server group group-name v3 [auth | noauth | priv]
```

例：

```
ciscoasa(config)# snmp-server group testgroup1 v3 auth
```

コミュニティ ストリングが設定されている場合は、コミュニティ ストリングに一致する名前を持つ 2 つの追加グループが自動生成されます。1 つはバージョン 1 のセキュリティ モデルのグループであり、もう 1 つはバージョン 2 のセキュリティ モデルのグループです。セキュリティ モデルの詳細については、「セキュリティ モデル」（P.40-18）を参照してください。**auth** キーワードは、パケット認証をイネーブルにします。**noauth** キーワードは、パケット認証または暗号化が使用されていないことを示します。**priv** キーワードは、パケット暗号化と認証をイネーブルします。**auth** または **priv** キーワードには、デフォルト値はありません。

ステップ 2　SNMP バージョン 3 だけで使用する、SNMP グループの新しいユーザを設定します。

```
snmp-server user username group-name {v3 [encrypted]] [auth {md5 | sha]} auth-password
[priv] [des | 3des | aes] [128 | 192 | 256] priv-password
```

例：

```
ciscoasa(config)# snmp-server user testuser1 testgroup1 v3 auth md5 testpassword aes 128
mypassword

ciscoasa(config)# snmp-server user testuser1 public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

username 引数は、SNMP エージェントに属するホスト上のユーザの名前です。*group-name* 引数は、ユーザが属するグループの名前です。**v3** キーワードは、SNMP バージョン 3 のセキュリティ モデルを使用することを指定し、**encrypted**、**priv**、および **auth** キーワードの使用をイネーブルにします。**encrypted** キーワードは、暗号化された形式でパスワードを指定します。暗号化されたパスワードは、16 進数の形式である必要があります。**auth** キーワードは、使用する認証レベル（**md5** または **sha**）を指定します。**priv** キーワードは、暗号化レベルを指定します。**auth** または **priv** キーワードのデフォルト値はありません。また、デフォルト パスワードもありません。暗号化アルゴリズムには、**des**、**3des**、または **aes** のキーワードを指定できます。使用する AES 暗号化アルゴリズムのバージョンとして、**128**、**192**、**256** のいずれかを指定することもできます。*auth-password* 引数は、認証ユーザ パスワードを指定します。*priv-password* 引数は、暗号化ユーザ パスワードを指定します。

（注） パスワードを忘れた場合は、回復できないため、ユーザを再設定する必要があります。プレーン テキストのパスワードまたはローカライズされたダイジェストを指定できます。ローカライズされたダイジェストは、ユーザに対して選択した認証アルゴリズム（MD5 または SHA にすることができます）に一致する必要があります。ユーザ設定がコンソールに表示される場合、またはファイル（スタートアップ コンフィギュレーション ファイルなど）に書き込まれる場合、ローカライズされた認証ダイジェストとプライバシー ダイジェストが常にプレーン テキストのパスワードの代わりに表示されます（2 番目の例を参照してください）。パスワードの最小長は、英数字 1 文字です。ただし、セキュリティを確保するために 8 文字以上の英数字を使用することを推奨します。

クラスタリング環境では、クラスタ化されたそれぞれの ASA について手動で SNMPv3 ユーザを更新する必要があります。これを行うには、マスター ユニットに対する **snmp-server user** *username group-name* **v3** コマンドを入力し、ローカライズされていない形式で *priv-password* オプションおよび *auth-password* オプションを指定します。

クラスタリングでの複製やコンフィギュレーションの実行時に SNMPv3 ユーザのコマンドが複製されないことを示すエラー メッセージが表示されます。この場合、SNMPv3 ユーザおよびグループのコマンドをスレーブの ASA に対して個別に設定します。また、複製の実行時に既存の SNMPv3 ユーザおよびグループのコマンドがクリアされない場合にもメッセージが表示されます。この場合は、クラスタのすべてのスレーブに対して SNMPv3 ユーザおよびグループのコマンドを入力します。次に例を示します。

マスター ユニットに対するコマンドで入力したキーがすでにローカライズされている場合：

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a priv aes 256
cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:f6:86:cf:18:c0:f0:47:d6:94:e5:
da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

スレーブ ユニットでクラスタ複製を実行した場合（コンフィギュレーションに **snmp-server user** コマンドがある場合のみ）

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

ステップ 3　SNMP 通知の受信者を指定します。トラップの送信元となるインターフェイスを指定します。ASA に接続できる NMS または SNMP マネージャの名前と IP アドレスを指定します。

```
snmp-server host interface {hostname | ip_address} [trap | poll] [community
community-string] [version {1 | 2c | 3 username}] [udp-port port]
```

例：

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 3 testuser1

ciscoasa(config)# snmp-server host mgmt 10.7.26.5 version 3 testuser2
```

trap キーワードは、NMS をトラップの受信だけに制限します。**poll** キーワードは、NMS を要求の送信（ポーリング）だけに制限します。デフォルトでは、SNMP トラップはイネーブルになっています。デフォルトでは、UDP ポートは 162 です。コミュニティ ストリングは、ASA と NMS の間の共有秘密キーです。キーは、大文字と小文字が区別される最大 32 文字の英数字の値です。スペースは使用できません。デフォルト コミュニティ ストリングは public です。ASA、ASAv、および ASASM では、このキーを使用して着信 SNMP 要求が有効かどうかを判別します。たとえば、コミュニティ ストリングを使用してサイトを指定すると、ASA、ASAv、または ASASM と NMS を同じストリングを使用して設定できます。ASA、ASAv、および ASASM は指定したストリングを使用し、無効なコミュニティ ストリングでの要求には応答しません。暗号化されたコミュニティ ストリングを使用した後は、暗号化された形式だけがすべてのシステム（CLI、ASDM、CSM など）に表示されます。クリア テキストのパスワードは表示されません。暗号化されたコミュニティ ストリングは常に ASA によって生成されます。通常は、クリア テキストの形式で入力します。

（注）　ASA ソフトウェアをバージョン 8.3(1) から下のバージョンにダウングレードし、暗号化されたパスワードを設定した場合、まず **no key config-key password encryption** コマンドを使用して暗号化されたパスワードをクリア テキストに戻してから結果を保存する必要があります。

version キーワードは、SNMP トラップのバージョンを指定します。ASA では、SNMP 要求（ポーリング）に基づくフィルタリングはサポートされません。

SNMP バージョン 3 のホストを ASA、ASAv、および ASASM に設定する場合は、ユーザをそのホストに関連付ける必要があります。

トラップを受信するには、**snmp-server host** コマンドを追加した後に、ASA、ASAv、または ASASM で設定されたクレデンシャルと同じクレデンシャルを使用して NMS でユーザを確実に設定するようにします。SNMP ホストの詳細については、「SNMP ホスト」（P.40-18）を参照してください。

ステップ 4　SNMP サーバの場所または担当者情報を設定します。

```
snmp-server [contact | location] text
```

例：

```
ciscoasa(config)# snmp-server location building 42

ciscoasa(config)# snmp-server contact EmployeeA
```

text 引数には、担当者または ASA システム管理者の名前を指定します。名前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　SNMP 要求のリスニング ポートを設定します。

snmp-server listen-port *lport*

例：

```
ciscoasa(config)# snmp-server lport 192
```

lport 引数には、着信要求を受け取るポートを指定します。デフォルトのリスニング ポートは 161 です。**snmp-server listen-port** コマンドは管理コンテキストでのみ使用でき、システム コンテキストでは使用できません。現在使用中のポートで **snmp-server listen-port** コマンドを設定すると、次のメッセージが表示されます。

警告　**The UDP port *port* is in use by another feature.SNMP requests to the device will fail until the snmp-server listen-port command is configured to use a different port.**

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

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　SNMP ユーザ リストを設定します。

snmp-server user-list *list_name* **username** *user_name*

例：

```
ciscoasa(config)# snmp-server user-list engineering username user1
```

listname 引数には、ユーザ リストの名前を指定します。最大 33 文字まで指定できます。**username** キーワードと *user_name* 引数で、ユーザ リストで設定するユーザを指定します。ユーザ リストのユーザは、**snmp-server user** *username* コマンドで設定します。このコマンドは、SNMP バージョン 3 を使用している場合にのみ使用できます。ユーザ リストには複数のユーザを含める必要があり、ホスト名または IP アドレスの範囲に関連付けることができます。

ネットワーク オブジェクトへのユーザの関連付け

ユーザ リストの単一のユーザまたはユーザのグループをネットワーク オブジェクトに関連付けるには、次の手順を実行します。

手順

ステップ 1　ユーザ リストの単一のユーザまたはユーザのグループをネットワーク オブジェクトに関連付けます。

snmp-server host-group *net_obj_name* [**trap** | **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}] [**udp-port** *port*]

例：

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1

ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c

ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1

ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

net_obj_name 引数には、ユーザまたはユーザ グループを関連付けるインターフェイスのネットワーク オブジェクト名を指定します。**trap** キーワードは、トラップの送信のみが可能であり、このホストはブラウズ（ポーリング）できないことを指定します。**poll** キーワードは、ホストでブラウズ（ポーリング）が可能だが、トラップの送信はできないことを指定します。**community** キーワードは、NMS からの要求に対して、または NMS に送信されるトラップを生成するときに、デフォルト以外のストリングが必要であることを指定します。このキーワードは、SNMP バージョン 1 または 2c でのみ使用できます。*community-string* 引数には、通知または NMS からの要求で送信されるコミュニティ ストリングを指定します。コミュニティ ストリングはパスワードのような役割を果たします。このコミュニティ ストリングは最大 32 文字です。**version** キーワードは、トラップの送信に使用する SNMP 通知のバージョン（バージョン 1、2c、または 3）を設定します。*username* 引数には、SNMP バージョン 3 を使用する場合にユーザの名前を指定します。**user-list** キーワードと *list_name* 引数で、ユーザ リストの名前を指定します。**udp-port** キーワードと *port* 引数では、NMS ホストへの SNMP トラップの送信にデフォルト以外のポートを使用する場合に、NMS ホストの UDP ポート番号を設定します。デフォルトの UDP ポートは 162 です。デフォルトのバージョンは 1 です。SNMP トラップはデフォルトでイネーブルになっています。

SNMP のモニタリング

SNMP は次のコマンドでモニタリングできます。

- **show running-config snmp-server [default]**

  すべての SNMP サーバのコンフィギュレーション情報を表示します。

- **show running-config snmp-server group**

  SNMP グループのコンフィギュレーション設定を表示します。

- **show running-config snmp-server host**

  リモート ホストに送信されるメッセージと通知を制御するために SNMP によって使用されているコンフィギュレーション設定を表示します。

- **show running-config snmp-server host-group**

  SNMP ホスト グループのコンフィギュレーションを表示します。

- **show running-config snmp-server user**

  SNMP ユーザベースのコンフィギュレーション設定を表示します。

- **show running-config snmp-server user-list**

  SNMP ユーザ リストのコンフィギュレーションを表示します。

- **show snmp-server engineid**

  設定されている SNMP エンジンの ID を表示します。

- **show snmp-server group**

  設定されている SNMP グループの名前を表示します。コミュニティ ストリングがすでに設定されている場合、デフォルトでは 2 つの別のグループが出力に表示されます。この動作は通常のものです。

- **show snmp-server statistics**

  SNMP サーバの設定済み特性を表示します。すべての SNMP カウンタをゼロにリセットするには、**clear snmp-server statistics** コマンドを使用します。

- **show snmp-server user**

  ユーザの設定済み特性を表示します。

例

次の例は、SNMP サーバの統計情報を表示する方法を示しています。

```
ciscoasa(config)# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

次の例は、SNMP サーバの実行コンフィギュレーションを表示する方法を示しています。

```
ciscoasa(config)# show running-config snmp-server
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

SNMP バージョン 1 および 2c の例

次の例は、どのホストにも SNMP syslog 要求を送信せずに、ASA が内部インターフェイスでホスト 192.0.2.5 からの SNMP 要求を受信する方法を示しています。

```
ciscoasa(config)# snmp-server host 192.0.2.5
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
ciscoasa(config)# snmp-server community ohwhatakeyisthee
```

SNMP バージョン 3 の例

次の例は、ASA が SNMP バージョン 3 のセキュリティ モデルを使用して SNMP 要求を受信する方法を示しています。このモデルでは、グループ、ユーザ、ホストという一定の順序で設定する必要があります。

```
ciscoasa(config)# snmp-server group v3 vpn-group priv
ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

SNMP の履歴

表 40-7　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。
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。 **show snmp-server engineid**、**show snmp-server group**、**show snmp-server user**、**snmp-server group**、**snmp-server user**、**snmp-server host** コマンドが導入または変更されました。
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。 **snmp-server community**、**snmp-server host** コマンドが変更されました。

表 40-7　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。 **snmp cpu threshold rising**、**snmp interface threshold**、**snmp-server enable traps** コマンドが導入または変更されました。
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 40-7　SNMP の履歴 （続き）

機能名	プラットフォームリリース	説明
VPN 関連の 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。 **snmp-server host-group**、**snmp-server user-list**、**show running-config snmp-server**、**clear configure snmp-server** の各コマンドが導入または変更されました。
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 OID		ASA で cpmCPUTotal5minRev OID がサポートされるようになりました。 SNMP の sysObjectID OID および entPhysicalVendorType OID に、新しい製品として ASAv が追加されました。 新しいプラットフォームである ASAv 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。 VPN 共有ライセンスの使用状況をモニタするための新しい SNMP MIB が追加されました。

表 40-7　SNMP の履歴 （続き）

機能名	プラットフォームリリース	説明
SNMP の MIB および OID	9.3(1)	ASASM 用に CISCO-REMOTE-ACCESS-MONITOR-MIB（OID 1.3.6.1.4.1.9.9.392）のサポートが追加されました。
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。 次のコマンドが変更されました。**snmp-server enable traps**。

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」（P.41-1）
- 「Smart Call Home の概要」（P.41-2）
- 「Anonymous Reporting および Smart Call Home のガイドライン」（P.41-8）
- 「Anonymous Reporting および Smart Call Home の設定」（P.41-9）
- 「Anonymous Reporting および Smart Call Home のモニタリング」（P.41-19）
- 「Smart Call Home の例（CLI）」（P.41-20）
- 「Anonymous Reporting および Smart Call Home の履歴」（P.41-21）

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。

アラート グループへの登録

アラート グループは、ASA でサポートされる Smart Call Homeの定義済みサブセットです。Smart Call Home アラートにはさまざまなタイプがあり、タイプに応じてさまざまなアラート グループにグループ化されます。各アラート グループは、特定の CLI の出力を報告します。サポートされる Smart Call Home アラート グループは次のとおりです。

- syslog
- 診断
- 環境
- インベントリ
- コンフィギュレーション
- 脅威
- スナップショット
- テレメトリ
- テスト

アラート グループの属性

アラート グループには次の属性があります。

- イベントはまず 1 個のアラート グループに登録します。
- 1 個のグループを、複数のイベントに関連付けることができます。
- 個々のアラート グループに登録できます。
- 個々のアラート グループをイネーブルまたはディセーブルにできます。デフォルト設定では、すべてのアラート グループに対してイネーブルです。
- 診断および環境アラート グループは定期的なメッセージのサブスクリプションをサポートします。
- syslog アラート グループは、メッセージ ID ベースのサブスクリプションをサポートします。
- 環境アラート グループの CPU とメモリの使用率のしきい値を設定できます。特定のパラメータが定義済みしきい値を超えると、メッセージが送信されます。しきい値のほとんどは、プラットフォームによって決まっており、変更できません。
- 指定する CLI 出力を送信するようスナップショット アラート グループを設定します。

アラート グループによってシスコに送信されるメッセージ

メッセージは、定期的に、および ASA がリロードされるたびにシスコに送信されます。これらのメッセージは、アラート グループによって分類されます。

インベントリ アラートは、次のコマンドによる出力で構成されます。

- **show version**：ASA ソフトウェア バージョン、ハードウェア構成、ライセンス キー、および関連するデバイスの稼働時間を表示します。
- **show inventory**：ネットワーキング デバイスにインストールされている各シスコ製品のインベントリ情報を取得および表示します。各製品は UDI と呼ばれる一意のデバイス情報で識別されます。UDI は、製品 ID（PID）、バージョン ID（VID）、およびシリアル番号（SN）の 3 つの異なるデータ要素の組み合わせです。

- **show failover state**：フェールオーバー ペアの両方のユニット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、ユニットのプライマリまたはセカンダリ ステータス、ユニットのアクティブ/スタンバイ ステータス、最後にレポートされたフェールオーバーの理由などがあります。
- **show module**：ASA 5585-X にインストールされている SSP に関する情報、ASA 5585-X にインストールされている IPS SSP に関する情報など、ASA にインストールされているすべてのモジュールに関する情報を表示します。
- **show environment**：シャーシ、ドライバ、ファン、および電源のハードウェア動作ステータスや、温度ステータス、電圧、CPU 使用率などの、ASA システム コンポーネントのシステム環境情報を表示します。

コンフィギュレーション アラートは、次のコマンドによる出力で構成されます。

- **show context**：割り当てられているインターフェイスとコンフィギュレーション ファイルの URL、設定済みコンテキストの数を表示します。または、システム実行スペースで Anonymous Reporting をイネーブルにしている場合には、全コンテキストのリストを表示します。
- **show call-home registered-module status**：登録されているモジュールのステータスを表示します。システム コンフィギュレーション モードを使用している場合、コマンドによって、コンテキストごとではなく、デバイス全体に基づくシステム モジュールのステータスが表示されます。
- **show running-config**：ASA で現在実行されている設定を表示します。
- **show startup-config**：スタートアップ コンフィギュレーションを表示します。
- **show access-list | include elements**：アクセス リストのヒット カウンタおよびタイム スタンプ値を表示します。

診断アラートは、次のコマンドによる出力で構成されます。

- **show failover**：ユニットのフェールオーバー ステータスに関する情報を表示します。
- **show interface**：インターフェイス統計情報を表示します。
- **show cluster info**：クラスタ情報を表示します。
- **show cluster history**：クラスタの履歴を表示します。
- **show crashinfo**（切り捨て）：予期しないソフトウェアのリロード後に、デバイスは、変更されたクラッシュ情報ファイルをファイルのトレースバック セクションだけを含めて送信します。したがって、ファンクション コール、レジスタ値、およびスタック ダンプだけがシスコに報告されます。
- **show tech-support no-config**：テクニカル サポート アナリストによる診断に使用される情報を表示します。

環境アラートは、次のコマンドによる出力で構成されます。

- **show environment**：シャーシ、ドライバ、ファン、および電源のハードウェア動作ステータスや、温度ステータス、電圧、CPU 使用率などの、ASA システム コンポーネントのシステム環境情報を表示します。
- **show cpu usage**：CPU 使用率情報を表示します。
- **show memory detail**：空きおよび割り当て済みのシステム メモリの詳細情報を表示します。

脅威アラートは、次のコマンドによる出力で構成されます。

- **show threat-detection rate**：脅威検出統計情報を表示します。
- **show threat-detection shun**：現在排除されているホストを表示します。
- **show shun**：排除情報を表示します。
- **show dynamic-filter reports top**：ボットネット トラフィック フィルタによって分類された上位 10 のマルウェア サイト、ポート、および感染ホストのレポートを生成します。

スナップショット アラートは、次のコマンドによる出力で構成されます。

- **show conn count**：アクティブな接続の数を表示します。
- **show asp drop**：高速セキュリティ パスでドロップされたパケットまたは接続を表示します。

テレメトリ アラートは、次のコマンドによる出力で構成されます。

- **show perfmon detail**：ASA パフォーマンスの詳細を表示します。
- **show traffic**：インターフェイスの送受信アクティビティを表示します。
- **show conn count**：アクティブな接続の数を表示します。
- **show vpn-sessiondb summary**：VPN セッションのサマリー情報を表示します。
- **show vpn load-balancing**：VPN ロード バランシングの仮想クラスタ コンフィギュレーションの実行時統計情報を表示します。
- **show local-host | include interface**：ローカル ホストのネットワーク状態を表示します。
- **show memory**：物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について要約を表示します。
- **show context**：割り当てられているインターフェイスとコンフィギュレーション ファイルの URL、設定済みコンテキストの数を表示します。または、システム実行スペースで Anonymous Reporting をイネーブルにしている場合には、全コンテキストのリストを表示します。
- **show access-list | include elements**：アクセス リストのヒット カウンタおよびタイム スタンプ値を表示します。
- **show interface**：インターフェイス統計情報を表示します。
- **show threat-detection statistics protocol**：IP プロトコルの統計情報を表示します。
- **show phone-proxy media-sessions count**：電話プロキシによって保存されている、対応するメディア セッションの数を表示します。
- **show phone-proxy secure-phones count**：データベースに保存されているセキュア モード対応の電話機の数を表示します。
- **show route**：ルーティング テーブルを表示します。
- **show xlate count**：NAT セッション（xlates）の数を表示します。

メッセージ重大度しきい値

特定のアラート グループに宛先プロファイルを登録すると、メッセージの重大度に基づいてアラート グループ メッセージを送信するしきい値を設定できます。宛先プロファイルに指定したしきい値より低い値のメッセージは、宛先に送信されません。

表 41-1 にメッセージの重大度と syslog の重大度のマッピングを示します。

表 41-1　メッセージの重大度と syslog レベルのマッピング

レベル	メッセージ 重大度	Syslog 重大度	説明
9	Catastrophic	該当なし	ネットワーク全体に壊滅的な障害が発生しています。
8	Disaster	該当なし	ネットワークに重大な影響が及びます。
7	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	0	Emergency。システムが使用不可能な状態。
6	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	1	Alert。クリティカルな状態。ただちに注意が必要。
5	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	2	Critical。重大な状態。
4	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	3	Error。軽微な状態。
3	Warning	4	警告状態。
2	Notification	5	基本的な通知および情報メッセージです。他と関係しない、重要性の低い障害です。
1	Normal	6	Information。通常のイベント。通常の状態に戻ることを意味します。
0	Debugging	7	デバッグ メッセージ（デフォルト設定）。

サブスクリプション プロファイル

サブスクリプション プロファイルを使用すると宛先受信者と関心のあるグループを関連付けることができます。プロファイルにあるサブスクライブされたグループに登録されているイベントがトリガーされると、イベントに関連付けられたメッセージが設定された受信者に送信されます。サブスクリプション プロファイルには次の属性があります。

- 複数のプロファイルを作成および設定できます。
- 1 個のプロファイルに複数の電子メールまたは HTTPS の受信者を設定できます。
- 1 個のプロファイルで、指定した重大度に複数のグループを登録できます。
- 1 個のプロファイルで、3 種類のメッセージ フォーマット（ショート テキスト、ロング テキスト、XML）をサポートします。
- 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できます。デフォルトでは、プロファイルはディセーブルです。
- 最大メッセージ サイズを指定できます。デフォルトは 3 MB です。

デフォルト プロファイル「Cisco TAC」が提供されました。デフォルト プロファイルには、事前定義されたモニタ対象グループ（診断、環境、インベントリ、コンフィギュレーション、テレメトリ）のセットと、事前定義された宛先電子メールおよび HTTPS URL があります。デフォルト プロファイルは、Smart Call Home を初めて設定するときに自動的に作成されます。宛先電子メールは callhome@cisco.com で、宛先 URL は https://tools.cisco.com/its/service/oddce/services/DDCEService です。

（注） デフォルト プロファイルの宛先電子メールと宛先 URL は変更できません。

コンフィギュレーション、インベントリ、テレメトリ、またはスナップショット アラート グループに宛先プロファイルを登録すると、アラート グループ メッセージを非同期に、または定期的に指定の時間に受信するよう選択できます。

表 41-2 に、デフォルトのアラート グループと重大度のサブスクリプションおよび期間（該当する場合）のマッピングを示します。

表 41-2　アラート グループと重大度のサブスクリプションのマッピング

アラート グループ	重大度	期間
コンフィギュレーション	Informational	毎月
診断	Informational 以上	該当なし
環境	Notification 以上	該当なし
インベントリ	Informational	毎月
スナップショット	Informational	該当なし
Syslog	同等の syslog	該当なし
テレメトリ	Informational	毎日
テスト	該当なし	該当なし
脅威	Notification	該当なし

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 形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.41-2）
- 「DNS サーバの設定」（P.13-15）

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。

コンフィギュレーション モードに入ると、次のガイドラインに従って Anonymous Reporting および Smart Call Home サービスをイネーブルにすることを要求するプロンプトが出ます。

- このプロンプトで、[Y]es、[N]o、[A]sk later を選択できます。[A]sk later を選択した場合、7 日後または ASA をリロードしたときに再度通知されます。[A]sk later を連続で選択すると、さらに ASA で 7 日ごとに 2 回プロンプトが表示されたのち、[N]o という答えだと見なされて再度表示されることはなくなります。
- プロンプトが表示されない場合は、「Anonymous Reporting の設定」（P.41-9）または「Smart Call Home の設定」（P.41-10）の手順を実行して、Anonymous Reporting または Smart Call Home をイネーブルにすることができます。

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　Anonymous Reporting 機能をイネーブルにし、新しい匿名のプロファイルを作成します。

```
call-home reporting anonymous
```

例：

```
ciscoasa(config)# call-home reporting anonymous
```

このコマンドを入力すると、トラスト ポイントが作成され、シスコの Web サーバのアイデンティティを検証するために使用する証明書がインストールされます。

ステップ 2　（オプション）このサーバへの接続があり、システムがメッセージを送信できることを確認します。

```
call-home test reporting anonymous
```

例：

```
ciscoasa(config)# call-home test reporting anonymous

INFO: Sending test message to
https://tools.cisco.com/its/service/oddce/services/DDCEService...
INFO: Succeeded
```

成功またはエラーのメッセージが、テスト結果として返されます。

Smart Call Home の設定

ASA で Smart Call Home サービスを設定するには、次のタスクを実行します。

ステップ 1　Smart Call Home サービスをイネーブルにします。「Smart Call Home のイネーブル化」（P.41-10）を参照してください。

ステップ 2　Smart Call Home メッセージがサブスクライバに配信される際に通過するメール サーバを設定します。「メール サーバの設定」（P.41-15）を参照してください。

ステップ 3　Smart Call Home メッセージの連絡先情報を設定します。「顧客連絡先情報の設定」（P.41-13）を参照してください。

ステップ 4　処理できるイベントの最大レートなどのアラート処理パラメータを定義します。「アラート グループ サブスクリプションの設定」（P.41-12）を参照してください。

ステップ 5　アラート サブスクリプション プロファイルを設定します。「宛先プロファイルの設定」（P.41-17）を参照してください。

個々のアラート サブスクリプション プロファイルによって、次の内容が特定されます。

- シスコの Smart Call Home サーバや電子メール受信者のリストなど、Smart Call Home メッセージの送信先となるサブスクライバ。
- コンフィギュレーション情報またはインベントリ情報など、受信するアラートの情報カテゴリ。

Smart Call Home のイネーブル化

Smart Call Home をイネーブルにして、Call Home プロファイルをアクティブにするには、次の手順を実行します。

手順

ステップ 1　Smart Call Home サービスをイネーブルにします。

```
service call-home
```

例：

```
ciscoasa(config)# service call-home
```

ステップ 2　Call Home コンフィギュレーション モードを開始します。

```
call-home
```

例：

```
ciscoasa(config)# call home
```

認証局のトラスト ポイントの宣言および認証

HTTPS 経由で Web サーバにメッセージを送信するように Smart Call Home が設定されている場合、Web サーバの証明書または証明書を発行した認証局（CA）の証明書を信頼するように ASA を設定する必要があります。Cisco Smart Call Home 実稼働サーバ証明書は、Verisign によって発行されます。Cisco Smart Call Home Staging サーバの証明書は Digital Signature Trust Company によって発行されます。

（注）　VPN 検証に使用されないために、no client-types および no validation-usage 用のトラスト ポイントを設定する必要があります。

Cisco サーバ セキュリティの証明書を宣言および認証し、Smart Call Home サービス用に Cisco HTTPS サーバとの通信を確立するには、次の手順を実行します。

手順

ステップ 1　（マルチ コンテキスト モードのみ）管理コンテキストで証明書をインストールします。

changeto context *admincontext*

例：

```
ciscoasa(config)# changeto context contextA
```

ステップ 2　トラスト ポイントを設定し、証明書登録の準備を整えます。

crypto ca trustpoint *trustpoint-name*

例：

```
ciscoasa(config)# crypto ca trustpoint cisco
```

（注）　転送方法として HTTP を使用する場合は、セキュリティ証明書をトラスト ポイント経由でインストールする必要があります。HTTPS には、これが必須です。次の URL で、インストールする指定の証明書を探します。

http://www.cisco.com/en/US/docs/switches/lan/smart_call_home/SCH31_Ch6.html#wp1035380

ステップ 3　証明書登録に、手動でのカットアンドペースト方式を指定します。

enroll terminal

例：

```
ciscoasa(ca-trustpoint)# enroll terminal
```

ステップ 4　指定した CA を認証します。CA の名前は、**crypto ca trustpoint** コマンドで指定したトラストポイント名と一致している必要があります。プロンプトで、セキュリティ証明書のテキストを貼り付けます。

crypto ca authenticate *trustpoint*

例：

```
ciscoasa(ca-trustpoint)# crypto ca authenticate cisco
```

ステップ 5　セキュリティ証明書のテキストの終わりを指定し、入力されたセキュリティ証明書の受け入れを確認します。

quit

例：

```
ciscoasa(ca-trustpoint)# quit

%Do you accept this certificate [yes/no]:

yes
```

環境およびスナップショット アラート グループの設定

環境およびスナップショット アラート グループを設定するには、次の手順を実行します。

手順

ステップ 1　アラート グループ コンフィギュレーション モードを開始します。

alert-group-config {**environment** | **snapshot**}

例：

```
ciscoasa(config)# alert-group-config environment
```

アラート グループ サブスクリプションの設定

宛先プロファイルをアラート グループに登録するには、次の手順を実行します。

手順

ステップ 1　Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2　指定した Smart Call Home アラート グループをイネーブルにします。

alert-group {**all** | **configuration** | **diagnostic** | **environment** | **inventory** | **syslog**}

例：

```
ciscoasa(cfg-call-home)# alert-group syslog
```

すべてのアラート グループをイネーブルにするには、**all** キーワードを使用します。デフォルトでは、すべてのアラート グループがイネーブルになります。

ステップ 3　指定された宛先プロファイルに対するプロファイル コンフィギュレーション モードを開始します。

profile *profile-name*

例：

```
ciscoasa(cfg-call-home)# profile CiscoTAC-1
```

ステップ 4　使用可能なすべてのアラート グループに登録します。

subscribe-to-alert-group all

例：

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group all
```

ステップ 5　この宛先プロファイルをコンフィギュレーション アラート グループに登録します。

subscribe-to-alert-group configuration periodic {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}

例：

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
```

periodic キーワードを指定すると、定期的に通知するようにコンフィギュレーション アラート グループが設定されます。デフォルトの間隔は daily です。

daily キーワードでは、送信する時刻を 24 時間制の *hh:mm* 形式（例：14:30）で指定します。

weekly キーワードでは、曜日と時刻を *day hh:mm* 形式で指定します。曜日は英語でスペルアウトします（例：Monday）。

monthly キーワードでは、1 ～ 31 の日付と時刻を *date hh:mm* 形式で指定します。

顧客連絡先情報の設定

顧客連絡先情報を設定するには、次の手順を実行します。

手順

ステップ 1　Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2　顧客電話番号を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

phone-number *phone-number-string*

例：

```
ciscoasa(cfg-call-home)# phone-number 8005551122
```

ステップ 3　顧客の住所（自由形式の文字列、最長 255 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

street-address *street-address*

例：

```
ciscoasa(cfg-call-home)# street-address “1234 Any Street, Any city, Any state, 12345”
```

ステップ 4　顧客名（最長 128 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

contact-name *contact-name*

例：

```
ciscoasa(cfg-call-home)# contact-name contactname1234
```

ステップ 5　シスコ カスタマー ID（最長 64 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

customer-id *customer-id-string*

例：

```
ciscoasa(cfg-call-home)# customer-id customer1234
```

ステップ 6　顧客サイト ID（最長 64 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

site-id *site-id-string*

例：

```
ciscoasa(cfg-call-home)# site-id site1234
```

ステップ 7　顧客連絡先 ID（最長 128 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

contract-id *contract-id-string*

例：

```
ciscoasa(cfg-call-home)# contract-id contract1234
```

例

次に、連絡先情報を設定する例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# contact-email-addr username@example.com
ciscoasa(cfg-call-home)# phone-number 8005551122
ciscoasa(cfg-call-home)# street-address “1234 Any Street, Any city, Any state, 12345”
ciscoasa(cfg-call-home)# contact-name contactname1234
ciscoasa(cfg-call-home)# customer-id customer1234
ciscoasa(cfg-call-home)# site-id site1234
ciscoasa(cfg-call-home)# contract-id contract1234
```

メール サーバの設定

メッセージの転送には、最もセキュアな HTTPS を使用することをお勧めします。ただし、Smart Call Home 宛ての電子メールを設定し、電子メール メッセージ転送を使用するようメール サーバを設定できます。

電子メール 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　Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2　SMTP メール サーバを指定します。

mail-server *ip-address* **name priority** [**1-100**] [**all**]

例：

```
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 smtp.example.com priority 1
```

最大 5 つのメール サーバを指定できます。その場合は、コマンドを 5 回実行します。Smart Call Home メッセージの電子メール転送を使用するには、最低 1 つのメール サーバを設定する必要があります。

番号が小さいほどメール サーバの優先順位が高くなります。

ip-address 引数には、IPv4 と IPv6 のどちらのメール サーバ アドレスも指定できます。

例

次にプライマリ メール サーバ（smtp.example.com）および IP アドレス 10.10.1.1 にあるセカンダリ メール サーバを設定する例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# mail-server smtp.example.com priority 1
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 priority 2
ciscoasa(cfg-call-home)# exit
ciscoasa(config)#
```

トラフィック レートの制限の設定

トラフィック レートの制限を設定するには、次の手順を実行します。

手順

ステップ 1　Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2　Smart Call Home が 1 分間に送信できるメッセージの数を指定します。デフォルト値は、1 分間に 10 のメッセージです。

rate-limit *msg-count*

```
ciscoasa(cfg-call-home)# rate-limit 5
```

Smart Call Home 通信の送信

Smart Call Home テスト メッセージを手動で送信するには、次の手順を実行します。

手順

ステップ 1　プロファイル コンフィギュレーションを使用して、テスト メッセージを送信します。

call-home test [*test-message*] **profile** *profile-name*

例：

```
ciscoasa# call-home test [testing123] profile CiscoTAC-1
```

アラート グループ メッセージを手動でトリガーするには、次の手順を実行します。

手順

ステップ 1　アラート グループ メッセージを 1 つの宛先プロファイルに送信します（指定されている場合）。プロファイルが指定されていない場合は、インベントリ、コンフィギュレーション、スナップショット、またはテレメトリ アラート グループの通知を受け取るように設定されたすべてのプロファイルにメッセージが送信されます。

call-home send alert-group {**inventory** | **configuration** | **snapshot** | **telemetry**} [**profile** *profile-name*]

例：

```
ciscoasa# call-home send alert-group inventory
```

CLI コマンドを発行してコマンド出力を電子メールで Cisco TAC に、または指定した電子メール 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　コマンド出力を電子メールアドレスに送信します。指定する CLI コマンドは、どのようなコマンドでもかまいません。これには、すべての登録済みモジュールのコマンドも含まれます。

call-home send *cli command* [**email** *email*]

例：

```
ciscoasa# call-home send cli destination email username@example.com
```

電子メール アドレスを指定した場合、コマンド出力はそのアドレスに送信されます。電子メール アドレスを指定していない場合、出力は Cisco TAC に送信されます。電子メールは、件名行にサービス番号を付けて（指定した場合）ログ テキスト形式で送信されます。

電子メール アドレスを指定しない場合、または Cisco TAC 電子メール アドレスを指定した場合に限り、サービス番号が必要になります。

宛先プロファイルの設定

電子メールまたは HTTP の宛先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　Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2　指定された宛先プロファイルに対するプロファイル コンフィギュレーション モードを開始します。指定された宛先プロファイルが存在しない場合、作成されます。

profile *profile-name*

例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

最大 10 個のアクティブ プロファイルを作成できます。デフォルト プロファイルは、Cisco TAC に報告するように設定されています。Call Home 情報を別の場所（たとえば、自社のサーバ）に送信するには、別のプロファイルを設定します。

ステップ 3　宛先、メッセージのサイズ、メッセージの形式、および Smart Call Home メッセージ受信者への転送方法を設定します。デフォルトのメッセージ形式は XML です。デフォルトでイネーブルになっている転送方法は、電子メールです。

destination {**email** *address* | **http** *url*} | **message-size-limit** *size* | **preferred-msg-format** {**long-text** | **short-text** | **xml**} **transport-method** {**email** | **http**}}

例：

```
ciscoasa(cfg-call-home-profile)# destination address email username@example.com

ciscoasa(cfg-call-home-profile)# destination preferred-msg-format long-text
```

電子メール アドレスは、Smart Call Home のメッセージを受け取る電子メール アドレスです（最長 100 文字）。デフォルトの最大 URL サイズは 5 MB です。

モバイル デバイスでメッセージを送信し、読み取るにはショート テキスト形式を使用し、コンピュータでメッセージを送信し、読み取るにはロング テキスト形式を使用します。

メッセージを受信するのが Smart Call Home バックエンド サーバの場合は、**preferred-msg-format** の値が XML であることを確認してください。バックエンド サーバが受け入れるメッセージは、XML 形式のものだけであるからです。

転送方式を HTTP に設定するには、「Smart Call Home のイネーブル化」（P.41-10）を参照してください。電子メールの転送方式をメールに戻すには、このコマンドを使用します。

宛先プロファイルのコピー

既存の宛先プロファイルをコピーして新しい宛先プロファイルを作成するには、次の手順を実行します。

手順

ステップ 1　Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2　コピーするプロファイルを指定します。

profile *profile-name*

例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

ステップ 3　既存のプロファイルの内容を新しいプロファイルにコピーします。

copy profile *src-profile-name dest-profile-name*

例：

```
ciscoasa(cfg-call-home)# copy profile newprofile profile1
```

既存のプロファイル（*src-profile-name*）と新しいプロファイル（*dest-profile-name*）は最大 23 文字です。

例

次に、既存のプロファイルをコピーする例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# copy profile newprofile profile1
```

宛先プロファイルの名前の変更

既存のプロファイルの名前を変更するには、次の手順を実行します。

手順

ステップ 1　Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2　名前を変更するプロファイルを指定します。

profile *profilename*

例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

ステップ 3　既存のプロファイルの名前を変更します。

rename profile *src-profile-name dest-profile-name*

例：

```
ciscoasa(cfg-call-home)# rename profile newprofile profile1
```

既存のプロファイル（*src-profile-name*）と新しいプロファイル（*dest-profile-name*）は最大 23 文字です。

例

次に、既存のプロファイルの名前を変更する例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# rename profile newprofile profile1
```

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、次のコマンドを参照してください。

- **show call-home detail**

  このコマンドは、現在の Smart Call Home の詳細設定を表示します。

- **show call-home mail-server status**

  このコマンドは、現在のメール サーバのステータスを表示します。

- **show call-home profile** {*profile name* | **all**}

  このコマンドは、Smart Call Home プロファイルのコンフィギュレーションを表示します。

- **show call-home registered-module status [all]**

  このコマンドは、登録されているモジュールのステータスを表示します。
- **show call-home statistics**

  このコマンドは、Call Home の詳細ステータスを表示します。
- **show call-home**

  このコマンドは、現在の Smart Call Home のコンフィギュレーションを表示します。
- **show running-config call-home**

  このコマンドは、現在の Smart Call Home の実行コンフィギュレーションを表示します。
- **show smart-call-home alert-group**

  このコマンドは、Smart Call Home アラート グループの現在のステータスを表示します。
- **show running-config all**

  このコマンドは、Anonymous Reporting ユーザ プロファイルに関する詳細を表示します。

Smart Call Home の例（CLI）

次の例は、Smart Call Home サービスを設定する方法を示しています。

```
ciscoasa (config)# service call-home
ciscoasa (config)# call-home
ciscoasa (cfg-call-home)# contact-email-addr customer@example.com
ciscoasa (cfg-call-home)# profile CiscoTAC-1
ciscoasa (cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService
ciscoasa (cfg-call-home-profile)# destination address email callhome@example.com
ciscoasa (cfg-call-home-profile)# destination transport-method http
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group environment
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group diagnostic
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group telemetry periodic weekly
Monday 23:30
```

Anonymous Reporting および Smart Call Home の履歴

表 41-3　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、ネットワークのアベイラビリティおよび運用効率を向上させます。 次のコマンドを導入または変更しました。 **active (call home)**、**call-home**、**call-home send alert-group**、**call-home test**、**contact-email-addr**、**customer-id (call home)**、**destination (call home)**、**profile**、**rename profile**、**service call-home**、**show call-home**、**show call-home detail**、**show smart-call-home alert-group**、**show call-home profile**、**show call-home statistics**、**show call-home mail-server status**、**show running-config call-home**、**show call-home registered-module status all**、**site-id**、**street-address**、**subscribe-to-alert-group all**、**alert-group-config**、**subscribe-to-alert-group configuration**、**subscribe-to-alert-group diagnostic**、**subscribe-to-alert-group environment**、**subscribe-to-alert-group inventory periodic**、**subscribe-to-alert-group snapshot periodic**、**subscribe-to-alert-group syslog**、**subscribe-to-alert-group telemetry periodic**。
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。 **call-home reporting anonymous**、**call-home test reporting anonymous** コマンドが導入されました。

表 41-3　Anonymous Reporting および Smart Call Home の履歴 （続き）

機能名	プラットフォームリリース	説明
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

CHAPTER 42

コマンドライン インターフェイスの使用

この章では、Cisco ASA での CLI の使用方法について説明します。

- 「ファイアウォール モードとセキュリティ コンテキスト モード」（P.42-1）
- 「コマンドのモードとプロンプト」（P.42-2）
- 「構文の書式」（P.42-3）
- 「コマンドの短縮形」（P.42-4）
- 「コマンドラインの編集」（P.42-4）
- 「コマンドの補完」（P.42-4）
- 「コマンドのヘルプ」（P.42-4）
- 「実行コンフィギュレーションの確認」（P.42-5）
- 「show コマンドおよび more コマンドの出力のフィルタリング」（P.42-5）
- 「コマンド出力のページング」（P.42-6）
- 「コメントの追加」（P.42-6）
- 「テキスト コンフィギュレーション ファイル」（P.42-6）
- 「サポートされている文字セット」（P.42-8）

（注） この CLI では構文など、Cisco IOS CLI と類似した表記法を使用しますが、ASA のオペレーティング システムが Cisco IOS ソフトウェアのいずれかのバージョンに該当するわけではありません。Cisco IOS CLI コマンドが ASA で動作するわけでも、同じ機能を使用できるわけでもありませんので注意してください。

ファイアウォール モードとセキュリティ コンテキスト モード

ASA は、次のモードの組み合わせで動作します。

- トランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モード

  ファイアウォール モードは、ASA がレイヤ 2 ファイアウォールまたはレイヤ 3 ファイアウォールとして動作するかどうかを決定します。

- マルチ コンテキスト モードまたはシングル コンテキスト モード

  セキュリティ コンテキスト モードは、ASA が単一のデバイスとして動作するか、またはマルチセキュリティ コンテキストとして動作する（仮想デバイスのように動作する）かを決定します。

特定のモードでしか使用できないコマンドもあります。

コマンドのモードとプロンプト

ASA の CLI にはコマンド モードが含まれています。特定のモードでしか入力できないコマンドもあります。たとえば、機密情報を表示するコマンドを入力するには、パスワードを入力して特権モードに入る必要があります。次に、コンフィギュレーション変更が誤って入力されないようにするために、コンフィギュレーション モードに入る必要があります。下位のコマンドはすべて、高位のモードで入力できます。たとえば、グローバル コンフィギュレーション モードで特権 EXEC コマンドを入力することができます。

（注） さまざまなタイプのプロンプトはすべてデフォルトで、別々のプロンプトとして設定できます。

- システム コンフィギュレーション モードまたはシングル コンテキスト モードに入っている場合、プロンプトはホスト名で始まります。

  ```
  ciscoasa
  ```

- プロンプト文字列を表示するときに、プロンプト コンフィギュレーションが解析され、設定されたキーワード値が **prompt** コマンドで設定された順に表示されます。キーワード引数は、ホスト名、ドメイン、コンテキスト、プライオリティ、状態のいずれかで、任意の順になります。

  ```
  asa(config)# prompt hostname context priority state
  ```

- コンテキスト内に入っている場合、プロンプトはホスト名で始まり、その後にコンテキスト名が続きます。

  ```
  ciscoasa/context
  ```

プロンプトは、アクセス モードに応じて変化します。

- ユーザ EXEC モード

  ユーザ EXEC モードでは、最小限の ASA 設定が表示されます。ユーザ EXEC モードのプロンプトは、初めて ASA にアクセスしたときに次のように表示されます。

  ```
  ciscoasa>

  ciscoasa/context>
  ```

- 特権 EXEC モード

  特権 EXEC モードでは、ユーザの特権レベルまでの現在の設定がすべて表示されます。すべてのユーザ EXEC モード コマンドは、特権 EXEC モードで動作します。特権 EXEC モードを開始するには、ユーザ EXEC モードで **enable** コマンドを入力します。これにはパスワードが必要です。プロンプトにはシャープ記号（#）が含まれています。

  ```
  ciscoasa#

  ciscoasa/context#
  ```

- グローバル コンフィギュレーション モード

  グローバル コンフィギュレーション モードでは、ASA コンフィギュレーションを変更できます。このモードでは、ユーザ EXEC、特権 EXEC、およびグローバルの各コンフィギュレーション コマンドをすべて使用できます。グローバル コンフィギュレーション モードを開始するには、特権 EXEC モードで **configure terminal** コマンドを入力します。プロンプトが次のように変化します。

  ```
  ciscoasa(config)#

  ciscoasa/context(config)#
  ```

- コマンド固有のコンフィギュレーション モード

  いくつかのコマンドは、グローバル コンフィギュレーション モードから、コマンド固有のコンフィギュレーション モードに移行します。このモードでは、ユーザ EXEC、特権 EXEC、グローバルの各コンフィギュレーション コマンド、およびコマンド固有のコンフィギュレーション コマンドをすべて使用できます。たとえば、**interface** 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 モードに入ります。プロンプトが次のように変化します。

  ```
  ciscoasa(config-if)#

  ciscoasa/context(config-if)#
  ```

構文の書式

コマンド構文の説明では、表 42-1 に記載されている表記法を使用します。

表 42-1　　構文の表記法

表記法	説明
太字	記載されているとおりに入力するコマンドおよびキーワードは、太字で示しています。
イタリック体	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。
|	省略可能または必須のキーワードや引数の中から選択する場合は、縦棒で区切って示しています。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	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や引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。

コマンドの短縮形

ほとんどのコマンドは、コマンドに固有の最小文字数まで短縮できます。たとえば、コンフィギュレーションを表示するには、完全なコマンド **write terminal** を入力する代わりに、**wr t** と入力できます。または、特権モードを開始するには **en**、コンフィギュレーション モードを開始するには **conf t** と入力できます。さらに、**0** を入力して、**0.0.0.0** を表すことができます。

コマンドラインの編集

ASA では、Cisco IOS ソフトウェアと同じコマンドライン編集ルールが使用されます。**show history** コマンドを使用して以前入力した全コマンドを表示することも、↑キーまたは **^p** コマンドで 1 つずつ前のコマンドを表示することもできます。前に入力したコマンドを確認したら、↓キーまたは **^n** コマンドでリスト内で前に進むことができます。再利用するコマンドに到達したら、そのコマンドを編集することも、Enter キーを押して実行することもできます。**^w** でカーソルの左側にある単語を削除することも、**^u** でカーソルのある行を消去することもできます。

ASA では、1 つのコマンドに 512 文字まで入力できます。512 文字を超えて入力した文字は無視されます。

コマンドの補完

部分的な文字列を入力してからコマンドまたはキーワードを完成させるには、Tab キーを押します。ASA は、部分的な文字列がコマンドまたはキーワード 1 つだけと一致する場合に限り、コマンドまたはキーワードを完成させます。たとえば、**s** と入力して Tab キーを押した場合は、一致するコマンドが複数あるため、ASA はコマンドを完成させません。一方、**dis** と入力して Tab キーを押すと、コマンド **disable** が完成します。

コマンドのヘルプ

次のコマンドを入力すると、コマンドラインからヘルプ情報を利用できます。

- **help** *command_name*

  特定のコマンドのヘルプを表示します。

- *command_name* **?**

  使用可能な引数のリストを表示します。

- *string***?**（スペースなし）

  その文字列で始まるコマンドをリストします。

- **?**および **+?**

  使用できるすべてのコマンドをリストします。**?** と入力すると、ASA は現在のモードで使用できるコマンドだけを表示します。下位モードのコマンドも含め、使用できるすべてのコマンドを表示するには、**+?** と入力します。

（注） コマンド文字列に疑問符（?）を組み込む場合は、誤って CLI ヘルプを起動しないよう、疑問符を入力する前に Ctrl+V を押す必要があります。

実行コンフィギュレーションの確認

実行コンフィギュレーションを確認するには、次のいずれかのコマンドを使用します。

- **show running-config** [**all**] [*command*]

  all を指定すると、デフォルト設定を含めすべてのコンフィギュレーションが表示されます。*command* を指定すると、指定コマンドに関連するコンフィギュレーションのみ表示されます。

  （注）　パスワードの多くは ***** と表示されます。パスワードをプレーン テキストまたは暗号化された形式（マスター パスフレーズをイネーブルにしている場合）で表示するには、**more** コマンドを使用します。

- **more system:running-config**

関連項目

「マスター パスフレーズの設定」（P.13-11）

show コマンドおよび more コマンドの出力のフィルタリング

縦棒（|）はどの **show** コマンドでも使用できます。これには、フィルタ オプションとフィルタリング式を組み込むことができます。フィルタリングは、Cisco IOS ソフトウェアと同様に、各出力行を正規表現と照合することによって行われます。選択するフィルタ オプションによって、正規表現に一致するすべての出力を含めたり除外したりできます。また、正規表現に一致する行で始まるすべての出力を表示することもできます。

show コマンドでフィルタリング オプションを使用する場合の構文は、次のとおりです。

```
ciscoasa# show command | {include | exclude | begin | grep [-v]} regexp
```

または

```
ciscoasa# more system:running-config | {include | exclude | begin | grep [-v]} regexp
```

（注）　**more** コマンドを入力すると、実行コンフィギュレーションだけでなく、すべてのファイルの内容を表示することができます。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。

このコマンド文字列の最初の縦棒（|）は演算子であり、コマンド内に含める必要があります。この演算子は、**show** コマンドの出力をフィルタに誘導します。構文内に含まれるその他の縦棒（|）は代替オプションを示すものであり、コマンドの一部ではありません。

include オプションを指定すると、正規表現に一致するすべての出力行が表示されます。**-v** を付けずに **grep** オプションを使用する場合も、同じ結果となります。**exclude** オプションを指定すると、正規表現に一致するすべての出力行が除外されます。**-v** を付けて **grep** オプションを使用する場合も、同じ結果となります。**begin** オプションを指定すると、正規表現に一致する行で始まるすべての出力行が表示されます。

regexp には、Cisco IOS の正規表現を指定します。正規表現は一重引用符または二重引用符で囲まれていません。したがって、末尾の空白スペースが正規表現の一部と解釈されるため、末尾の空白スペースに注意してください。

正規表現を作成する場合は、照合する任意の文字または数字を使用できます。また、*メタ文字*と呼ばれるキーボード文字は、正規表現で使用されると特別な意味を持ちます。

疑問符（?）やタブなど、CLI の特殊文字をすべてエスケープするには、**Ctrl+V** を使用します。たとえば、コンフィギュレーションで **d?g** と入力するには、**d[Ctrl+V]?g** とキー入力します。

コマンド出力のページング

help または **?**、**show**、**show xlate** など、長いリストが出力されるコマンドでは、1 画面分ずつ表示して停止させるか、リストの最後まで表示させるかを決めることができます。**pager** コマンドを使用すると、画面上に表示する行数を選択して、その行数を表示した後に More プロンプトを表示するようにできます。

ページングがイネーブルになっているときには、次のプロンプトが表示されます。

```
<--- More --->
```

More プロンプトの構文は、UNIX の **more** コマンドと似ています。

- 次の 1 画面を表示するには、**Space** バーを押します。
- 次の行を表示するには、**Enter** キーを押します。
- コマンドラインに戻るには、**q** キーを押します。

コメントの追加

行の先頭にコロン（:）を置いて、コメントを作成できます。しかし、コメントが表示されるのはコマンド ヒストリ バッファだけで、コンフィギュレーションには表示されません。したがって、コメントは、**show history** コマンドを使用するか、矢印キーを押して前のコマンドを取得することによって表示できますが、コンフィギュレーションには含まれないので、**write terminal** コマンドでは表示できません。

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 にダウンロードできるテキスト コンフィギュレーション ファイルをフォーマットする方法について説明します。

- 「テキスト ファイルでコマンドと行が対応する仕組み」（P.42-7）
- 「コマンド固有のコンフィギュレーション モード コマンド」（P.42-7）
- 「自動テキスト入力」（P.42-7）
- 「行の順序」（P.42-7）
- 「テキスト コンフィギュレーションに含まれないコマンド」（P.42-7）
- 「パスワード」（P.42-8）
- 「マルチセキュリティ コンテキスト ファイル」（P.42-8）

テキスト ファイルでコマンドと行が対応する仕組み

テキスト コンフィギュレーション ファイルには、このガイドで説明するコマンドに対応する行が含まれています。

例では、コマンドの前に CLI プロンプトがあります。次の例では、CLI プロンプトは「ciscoasa(config)#」です。

```
ciscoasa(config)# context a
```

テキスト コンフィギュレーション ファイルでは、コマンドの入力を求めるプロンプトが表示されないので、プロンプトは省略されています。

```
context a
```

コマンド固有のコンフィギュレーション モード コマンド

コマンド固有のコンフィギュレーション モード コマンドは、コマンドラインで入力されたときに、メイン コマンドの下に字下げして表示されます。テキスト ファイルの行は、コマンドがメイン コマンドのすぐ後に表示される限り、字下げする必要はありません。たとえば、次のテキストは字下げされていませんが、字下げしたテキストと同じように読み取られます。

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
    nameif outside
```

自動テキスト入力

コンフィギュレーションを ASA にダウンロードすると、それにより一部の行が自動的に挿入されます。たとえば、ASA は、デフォルト設定のため、またはコンフィギュレーションが変更されたときのための行を挿入します。テキスト ファイルを作成するときは、これらの自動入力を行う必要はありません。

行の順序

ほとんどの場合、コマンドはファイル内で任意の順序に置くことができます。ただし、ACE などいくつかの行は表示された順に処理されるので、順序がアクセス リストの機能に影響する場合があります。その他のコマンドでも、順序の要件がある場合があります。たとえば、あるインターフェイスの名前を多数の後続コマンドが使用する場合は、そのインターフェイスの **nameif** コマンドをまず入力する必要があります。また、コマンド固有のコンフィギュレーション モードのコマンドは、メイン コマンドの直後に置く必要があります。

テキスト コンフィギュレーションに含まれないコマンド

いくつかのコマンドは、コンフィギュレーションに行を挿入しません。たとえば、**show running-config** などのランタイム コマンドは、テキスト ファイル内に対応する行がありません。

パスワード

ログイン パスワード、イネーブル パスワード、およびユーザ パスワードは、コンフィギュレーションに保存される前に自動的に暗号化されます。たとえば、パスワード「cisco」の暗号化された形式は jMorNbK0514fadBh のようになります。コンフィギュレーション パスワードは暗号化された形式で別の ASA にコピーできますが、そのパスワードの暗号を解読することはできません。

暗号化されていないパスワードをテキスト ファイルに入力した場合、コンフィギュレーションを ASA にコピーしても、ASA は自動的にパスワードを暗号化しません。ASA がパスワードを暗号化するのは、**copy running-config startup-config** コマンドまたは **write memory** コマンドを使用して、コマンドラインから実行コンフィギュレーションを保存した場合のみです。

マルチセキュリティ コンテキスト ファイル

マルチ セキュリティ コンテキストの場合、コンフィギュレーション全体は次に示す複数の部分で構成されます。

- セキュリティ コンテキスト コンフィギュレーション
- コンテキストのリストなど、ASA の基本設定を示すシステム コンフィギュレーション
- システム コンフィギュレーション用のネットワーク インターフェイスを提供する管理コンテキスト

  システム コンフィギュレーションには、それ自体のインターフェイスまたはネットワーク設定は含まれていません。代わりに、システムは、ネットワーク リソースにアクセスする必要があるときに（サーバからコンテキストをダウンロードするときなど）、管理コンテキストとして指定されたコンテキストを使用します。

各コンテキストは、シングル コンテキスト モード コンフィギュレーションに似ています。システム コンフィギュレーションにはシステム限定のコマンド（全コンテキストのリストなど）が含まれており、その他の一般的なコマンド（多数のインターフェイス パラメータなど）は存在しない点で、システム コンフィギュレーションは、コンテキスト コンフィギュレーションとは異なっています。

サポートされている文字セット

ASA CLI は、現在 UTF-8 の符号化方式だけをサポートしています。UTF-8 は Unicode 文字の特定の符号化スキームであり、ASCII 文字のサブセットと互換性を持つように設計されています。ASCII 文字は UTF-8 で 1 バイト文字として表現されます。その他のすべての文字は、UTF-8 でマルチバイト文字として表現されます。

ASCII の印刷可能文字（0x20 ～ 0x7e）はすべてサポートされています。印刷可能な ASCII 文字は、ISO 8859-1 の文字と同じです。UTF-8 は ISO 8859-1 のスーパーセットであるため、最初の 256 文字（0 ～ 255）は ISO 8859-1 の文字と同じになります。ASA CLI は、ISO 8859-1 の文字を 255 文字（マルチバイト文字）までサポートしています。

CHAPTER 43

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」（P.43-1）
- 「IPv6 アドレス」（P.43-5）
- 「プロトコルとアプリケーション」（P.43-11）
- 「TCP ポートと UDP ポート」（P.43-12）
- 「ローカル ポートとプロトコル」（P.43-15）
- 「ICMP タイプ」（P.43-16）

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存在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決定します。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すると、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 進数マスクの場合、各バイナリ オクテットを 10 進数に変換して 255.255.255.0 にします。*/ビット* マスクの場合は、1 の数である /24 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字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 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.11-12）

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。

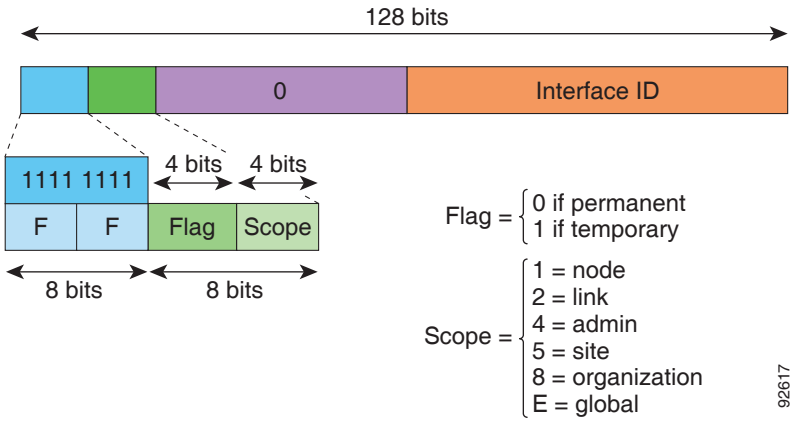
たとえば、MAC アドレスが 00E0.b601.3B7A のインターフェイスの場合、64 ビット インターフェイス ID は 02E0:B6FF:FE01:3B7A になります。

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
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。

表 43-6　プロトコルのリテラル値（続き）

リテラル	値	説明
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

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
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
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

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
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 フラッディング、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
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	ポート番号	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
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	—

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	ポート番号	注
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
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