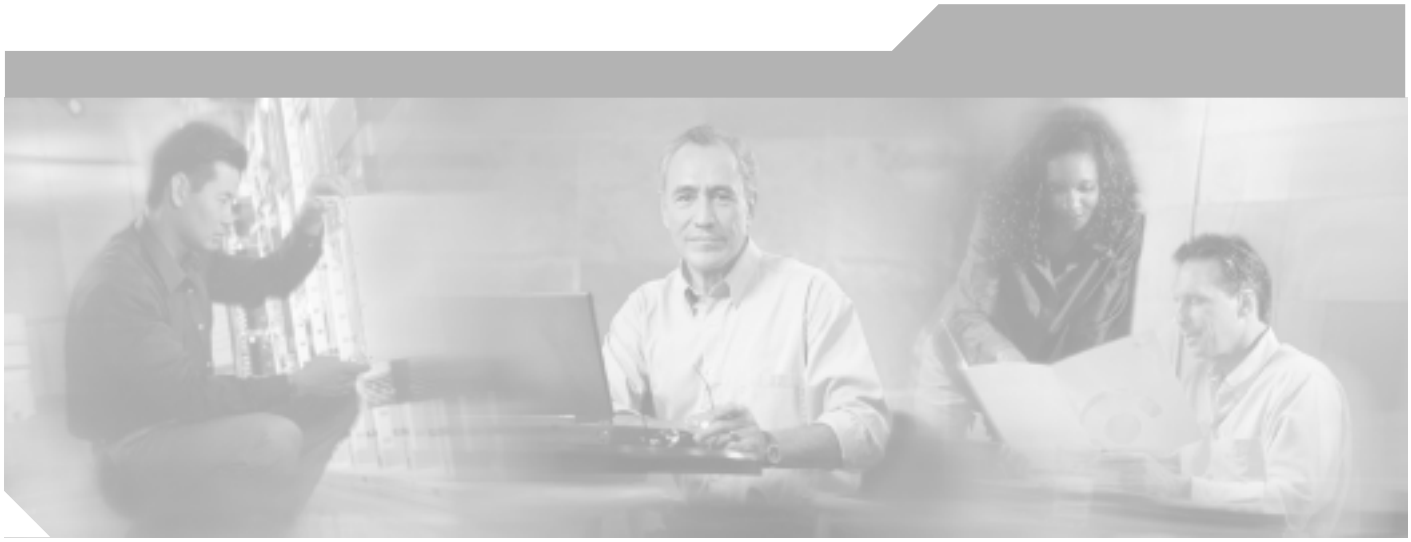


Catalyst 6500 シリーズ スイッチ /Cisco 7600 シリーズ ルータ Firewall Services Module コンフィギュレーション ガイド

Release 3.1(1)

Text Part Number: OL-8123-01-J

CONTENTS

マニュアルの概要 xxiii
- 対象読者 xxiv
- 目的 xxiv
- マニュアルの構成 xxv
- 表記法 xxvii
- 関連資料 xxvii
- マニュアルの入手方法 xxviii
  - Cisco.com xxviii
  - Documentation DVD xxviii
  - マニュアルの発注方法 xxviii
- シスコ製品のセキュリティ xxix
  - シスコ製品のセキュリティ問題の報告 xxix
- テクニカル サポート xxx
  - Cisco Technical Support Web サイト xxx
  - Japan TAC Web サイト xxx
  - Service Request ツールの使用 xxxi
  - 問題の重大度の定義 xxxi
- その他の資料および情報の入手方法 xxxii

クイック スタート手順 xxxiii
- ルーテッド ファイアウォールの最小限の設定手順 xxxiv
- 透過ファイアウォールの最小限の設定手順 xxxv

CHAPTER 1

FWSM について 1-1
- セキュリティ ポリシーの概要 1-2
  - アクセス リストでのトラフィックの許可または拒否 1-2
  - NAT の適用 1-2
  - 通過トラフィックに対する AAA の使用 1-2
  - インターネット フィルタリングの適用 1-2
  - アプリケーション検査の適用 1-3
  - 接続制限の適用 1-3
- スイッチにおける Firewall Services Module の動作 1-4

MSFC の使用方法 1-4
ファイアウォール モードの概要 1-6
ステートフル インスペクションの概要 1-7
セキュリティ コンテキストの概要 1-8

CHAPTER 2 Firewall Services Module を使用するためのスイッチの設定 2-1
スイッチの概要 2-2
モジュールの搭載確認 2-3
Firewall Services Module への VLAN 割り当て 2-4
VLAN の注意事項 2-4
Cisco IOS ソフトウェアで FWSM に VLAN を割り当てる場合 2-4
Catalyst OS ソフトウェアで FWSM に VLAN を割り当てる場合 2-6
MSFC への SVI の追加 2-7
SVI の概要 2-7
SVI の設定（スーパーバイザ エンジンで Cisco IOS ソフトウェアを実行している場合） 2-9
SVI の設定（スーパーバイザ エンジンで Catalyst OS ソフトウェアを実行している場合） 2-10
FWSM の内部インターフェイスのカスタマイズ 2-12
フェールオーバーを使用するためのスイッチの設定 2-13
セカンダリ Firewall Services Module への VLAN 割り当て 2-13
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 2-13
透過ファイアウォール モードとの両立 2-13
Firewall Services Module ブート パーティションの管理 2-14
フラッシュ メモリの概要 2-14
デフォルト ブート パーティションの設定 2-14
FWSM のリセットまたは特定のパーティションからの起動 2-15
Cisco IOS ソフトウェアで FWSM をリセットする場合 2-16
Catalyst OS ソフトウェアで FWSM をリセットする場合 2-16

CHAPTER 3 Firewall Services Module の接続および設定の管理 3-1
Firewall Services Module との接続 3-2
FWSM へのログイン 3-2
FWSM からのログアウト 3-3
設定の管理 3-4
変更した設定の保存 3-4
変更した設定の保存（シングルコンテキスト モードの場合） 3-4
変更した設定の保存（マルチコンテキスト モードの場合） 3-4
スタートアップ 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へのコピー 3-6

設定の表示 3-6
設定内の設定値の消去および削除 3-6
テキスト コンフィギュレーション ファイルをオフラインで作成する方法 3-7

CHAPTER 4 セキュリティ コンテキストの設定 4-1
セキュリティ コンテキストの概要 4-2
セキュリティ コンテキストの一般的な使用方法 4-2
サポートされていない機能 4-2
コンテキスト コンフィギュレーション ファイル 4-3
FWSM によるパケットの分類方法 4-3
コンテキスト間でのインターフェイスの共有 4-7
共有インターフェイスの注意事項 4-7
セキュリティ コンテキストのカスケード 4-9
マルチコンテキスト モードの FWSM へのログイン 4-10
マルチコンテキスト モードのイネーブル化またはディセーブル化 4-11
シングルモード コンフィギュレーションのバックアップ 4-11
マルチコンテキスト モードのイネーブル化 4-11
シングルコンテキスト モードの復元 4-12
リソース管理の設定 4-13
クラスおよびクラス メンバーの概要 4-13
リソース限度 4-13
デフォルト クラス 4-14
クラス メンバー 4-15
クラスの設定 4-16
メモリ パーティションの設定 4-18
セキュリティ コンテキストの設定 4-20
コンテキストとシステム実行スペース間の切り替え 4-24
セキュリティ コンテキストの管理 4-25
セキュリティ コンテキストの削除 4-25
管理コンテキストの変更 4-25
セキュリティ コンテキストの URL の変更 4-26
セキュリティ コンテキストのリロード 4-27
設定の消去によるリロード 4-27
コンテキストの削除および再追加によるリロード 4-28
セキュリティ コンテキストのモニタリング 4-28
コンテキスト情報の表示 4-28
リソース割り当ての表示 4-30
リソース使用状況の表示 4-32

コンテキストでの SYN 攻撃のモニタリング 4-34

CHAPTER 5 ファイアウォール モードの設定 5-1
ルーテッド モードの概要 5-2
IP ルーティング サポート 5-2
NAT 5-2
ルーテッド ファイアウォール モードで FWSM を通過するデータ 5-3
内部ユーザによる Web サーバ アクセス 5-4
外部ユーザによる DMZ 上の Web サーバ アクセス 5-5
内部ユーザによる DMZ 上の Web サーバ アクセス 5-6
外部ユーザによる内部ホストへのアクセス試行 5-7
DMZ ユーザによる内部ホストへのアクセス試行 5-8
透過モードの概要 5-9
透過ファイアウォールの機能 5-9
ネットワークでの透過ファイアウォールの使用例 5-10
透過ファイアウォールの注意事項 5-11
透過モードでサポートされていない機能 5-12
透過ファイアウォールを通過するデータ 5-13
内部ユーザによる Web サーバ アクセス 5-14
外部ユーザによる内部ネットワーク上の Web サーバ アクセス 5-15
外部ユーザによる内部ホストへのアクセス試行 5-16
透過ファイアウォール モードまたはルーテッド ファイアウォール モードの設定 5-17

CHAPTER 6 インターフェイス パラメータの設定 6-1
セキュリティ レベルの概要 6-2
ルーテッド ファイアウォール モードのインターフェイスの設定 6-3
透過ファイアウォール モードのインターフェイスの設定 6-5
透過ファイアウォール インターフェイスのパラメータの設定 6-5
IP アドレスのブリッジ グループへの割り当て 6-7
同じセキュリティ レベルのインターフェイス間の通信の許可 6-8
インターフェイスのオン / オフ 6-8

CHAPTER 7 基本設定 7-1
パスワードの変更 7-2
ログイン パスワードの変更 7-2
イネーブル パスワードの変更 7-2
メンテナンス ソフトウェア パスワードの変更 7-3
ホスト名の設定 7-5

ドメイン名の設定 7-5
プロンプトの設定 7-6
ログイン バナーの設定 7-7
透過ファイアウォール モードと NAT を設定しない場合の接続制限の設定 7-8

CHAPTER 8 IP ルーティングおよび DHCP サービスの設定 8-1
スタティック ルートおよびデフォルト ルートの設定 8-2
スタティック ルートの設定 8-3
デフォルト ルートの設定 8-4
OSPF の設定 8-5
OSPF の概要 8-5
OSPF のイネーブル化 8-6
OSPF プロセス間でのルートの再分配 8-7
ルート マップの追加 8-7
OSPF プロセスへのスタティック ルート、接続ルート、または OSPF ルートの再分配 8-8
OSPF インターフェイス パラメータの設定 8-9
OSPF エリア パラメータの設定 8-11
OSPF NSSA の設定 8-12
OSPF エリア間のルート集約の設定 8-13
OSPF へのルート再分配時のルート集約の設定 8-14
デフォルト ルートの生成 8-14
ルート計算タイマーの設定 8-15
ネイバのアップまたはダウンのロギング 8-16
OSPF アップデート パケット ペーシングの表示 8-16
OSPF のモニタリング 8-17
OSPF プロセスの再起動 8-17
RIP の設定 8-18
RIP の概要 8-18
RIP のイネーブル化 8-18
マルチキャスト ルーティングの設定 8-20
マルチキャスト ルーティングの概要 8-20
マルチキャスト ルーティングのイネーブル化 8-20
IGMP 機能の設定 8-21
インターフェイス上での IGMP のディセーブル化 8-21
グループ メンバーシップの設定 8-22
静的に加入するグループの設定 8-22
マルチキャスト グループへのアクセスの制御 8-22
インターフェイス上の IGMP ステート数の制限 8-23

クエリー間隔とクエリー タイムアウトの変更 8-23
クエリー応答時間の変更 8-24
IGMP バージョンの変更 8-24
スタブ マルチキャスト ルーティングの設定 8-24
スタティック マルチキャスト ルートの設定 8-24
PIM 機能の設定 8-25
インターフェイス上での PIM のディセーブル化 8-25
スタティック RP アドレスの設定 8-26
指定ルータのプライオリティの設定 8-26
PIM Register メッセージのフィルタリング 8-26
PIM メッセージ間隔の設定 8-27
マルチキャスト ルーティングの詳細について 8-27
非対称ルーティング サポートの設定 8-28
インターフェイスの ASR グループへの追加 8-28
非対称ルーティング サポートの例 8-29
DHCP の設定 8-30
DHCP サーバの設定 8-30
DHCP サーバのイネーブル化 8-30
DHCP オプションの設定 8-32
DHCP サーバで Cisco IP Phone を使用する方法 8-33
DHCP リレー サービスの設定 8-34
DHCP クライアントの設定 8-35

CHAPTER 9
IPv6 の設定 9-1
IPv6 対応 コマンド 9-2
インターフェイス上での IPv6 の設定 9-3
インターフェイス上でのデュアル IP スタックの設定 9-4
IPv6 重複アドレス検出の設定 9-5
IPv6 デフォルト / スタティック ルートの設定 9-6
IPv6 アクセス リストの設定 9-7
IPv6 ネイバ検出の設定 9-8
ネイバ送信要求メッセージの設定 9-8
ネイバ送信要求メッセージの間隔の設定 9-9
ネイバ到達可能時間の設定 9-9
ルータ アドバタイズメント メッセージの設定 9-9
ルータ アドバタイズメント送信間隔の設定 9-10
ルータのライフタイム値の設定 9-11
IPv6 プレフィクスの設定 9-11
ルータ アドバタイズメント メッセージのディセーブル 9-11

スタティック IPv6 ネイバの設定 9-12
IPv6 コンフィギュレーションの確認 9-13
IPv6 インターフェイス設定の表示 9-13
IPv6 ルートの表示 9-14

CHAPTER 10 アクセス リストでのトラフィックの識別 10-1
アクセス リストの概要 10-2
アクセス リストのタイプ 10-2
ACE の順序 10-3
アクセス リストの暗黙拒否 10-3
NAT 使用時のアクセス リスト用 IP アドレス 10-3
アクセス リストのコミット 10-5
ACE の最大数 10-6
拡張アクセス リストの追加 10-7
拡張アクセス リストの概要 10-7
透過ファイアウォールを通過できる特殊な IP トラフィック 10-7
拡張 ACE の追加 10-8
EtherType アクセス リストの追加 10-10
EtherType アクセス リストの概要 10-10
EtherType ACE の追加 10-11
標準アクセス リストの追加 10-12
オブジェクトのグループ化によるアクセス リストの簡素化 10-13
オブジェクト グループ化の機能 10-13
オブジェクト グループの追加 10-13
プロトコル オブジェクト グループの追加 10-14
ネットワーク オブジェクト グループの追加 10-14
サービス オブジェクト グループの追加 10-15
ICMP タイプ オブジェクト グループの追加 10-16
オブジェクト グループのネスト 10-17
アクセス リストでオブジェクト グループを使用する方法 10-18
オブジェクト グループの表示 10-19
オブジェクト グループの削除 10-19
アクセス リストへのコメントの追加 10-20
拡張アクセス リストのアクティベーションのスケジューリング 10-21
時間範囲の追加 10-21
時間範囲の ACE への適用 10-22
アクセス リスト アクティビティのロギング 10-23
アクセス リスト ロギングの概要 10-23
ACE ロギングの設定 10-24

拒否フローの管理 10-25

CHAPTER 11 ネットワーク アクセスの許可または拒否 11-1
着信および発信アクセス リストの概要 11-2
アクセス リストのインターフェイスへの適用 11-5

CHAPTER 12 NAT の設定 12-1
NAT の概要 12-2
NAT の説明 12-2
NAT 制御 12-3
NAT のタイプ 12-5
ダイナミック NAT 12-5
PAT 12-7
スタティック NAT 12-7
スタティック PAT 12-8
NAT 制御をイネーブルにした場合の NAT のバイパス 12-9
ポリシー NAT 12-10
NAT および同一セキュリティ レベルのインターフェイス 12-13
実アドレス照合用 NAT コマンドの順序 12-13
NAT ステートメントの最大数 12-13
マップ アドレスに関する注意事項 12-14
DNS および NAT 12-14
NAT 制御の設定 12-16
ダイナミック NAT および PAT の使用方法 12-17
ダイナミック NAT および PAT の実装 12-17
ダイナミック NAT または PAT の設定 12-23
スタティック NAT の使用方法 12-27
スタティック PAT の使用方法 12-29
NAT のバイパス 12-32
アイデンティティ NAT の設定 12-32
スタティック アイデンティティ NAT の設定 12-33
NAT 除外の設定 12-34
NAT の例 12-36
重複したネットワーク 12-36
ポートのリダイレクション 12-37

CHAPTER 13 フェールオーバーの設定 13-1
フェールオーバーの概要 13-2
フェールオーバーのシステム要件 13-2

ソフトウェア要件 13-2
ライセンス要件 13-2
フェールオーバー リンクとステート リンク 13-3
フェールオーバー リンク 13-3
ステート リンク 13-4
シャーシ内およびシャーシ間のモジュール配置 13-4
シャーシ内フェールオーバー 13-4
シャーシ間フェールオーバー 13-5
透過ファイアウォールの要件 13-8
アクティブ / スタンバイ フェールオーバーとアクティブ / アクティブ フェールオーバー 13-9
アクティブ / スタンバイ フェールオーバー 13-9
アクティブ / アクティブ フェールオーバー 13-13
使用するフェールオーバー タイプの決定 13-17
標準フェールオーバーとステートフル フェールオーバー 13-17
標準フェールオーバー 13-18
ステートフル フェールオーバー 13-18
フェールオーバーのヘルス モニタ 13-18
装置のヘルス モニタ 13-19
インターフェイスのモニタ 13-19
フェールオーバーの設定 13-21
アクティブ / スタンバイ フェールオーバーの使用 13-21
前提条件 13-21
アクティブ / スタンバイ フェールオーバーの設定 13-21
任意のアクティブ / スタンバイ フェールオーバーの設定 13-25
アクティブ / アクティブ フェールオーバーの使用 13-26
前提条件 13-26
アクティブ / アクティブ フェールオーバーの設定 13-26
アクティブ / アクティブ フェールオーバーの任意の設定 13-30
フェールオーバー通信の認証 / 暗号化の設定 13-31
フェールオーバーの設定の確認 13-32
フェールオーバー ステータスの表示 13-32
モニタ対象インターフェイスの表示 13-40
フェールオーバーの設定の表示 13-41
フェールオーバー機能のテスト 13-41
フェールオーバーの制御とモニタ 13-42
フェールオーバーの強制実行 13-42
フェールオーバーのディセーブル化 13-42
設定の同期化のディセーブル化 13-43

障害が発生した装置またはフェールオーバー グループの復元 13-43
フェールオーバー動作のモニタ 13-43
フェールオーバー システム メッセージ 13-43
デバッグ メッセージ 13-44
SNMP 13-44

CHAPTER 14 AAA サーバとローカル データベースの設定 14-1
AAA の概要 14-2
認証の概要 14-2
許可の概要 14-3
アカウンティングの概要 14-3
AAA サーバおよびローカル データベースのサポート 14-4
サポートの概要 14-4
RADIUS サーバのサポート 14-5
認証方法 14-5
属性のサポート 14-5
RADIUS の機能 14-5
TACACS+ サーバのサポート 14-6
SDI サーバのサポート 14-7
SDI バージョンのサポート 14-7
2 段階の認証プロセス 14-8
SDI プライマリ サーバとレプリカ サーバ 14-8
NT サーバのサポート 14-8
Kerberos サーバのサポート 14-8
LDAP サーバのサポート 14-8
ローカル データベースのサポート 14-9
ユーザ プロファイル 14-9
ローカル データベースの機能 14-9
フォールバックのサポート 14-10
ローカル データベースの設定 14-11
AAA サーバ グループおよびサーバの識別 14-13

CHAPTER 15 ネットワーク アクセスへの AAA の適用 15-1
AAA パフォーマンス 15-1
ネットワーク アクセスの認証の設定 15-2
認証の概要 15-2
ネットワーク アクセス認証のイネーブル化 15-3
Web クライアントのセキュア認証のイネーブル化 15-4
プロトコル単位の認証チャレンジのディセーブル化 15-6

ネットワーク アクセスの許可の設定 15-7
TACACS+ 許可の設定 15-7
RADIUS 許可の設定 15-8
RADIUS サーバからユーザごとの ACL をダウンロードする設定 15-9
RADIUS サーバからユーザごとの ACL 名をダウンロードする設定 15-11
ネットワーク アクセスのアカウンティングの設定 15-12
MAC アドレスを使用した認証および許可からのトラフィックの除外 15-13

CHAPTER 16 フィルタリング サービスの適用 16-1
フィルタリングの概要 16-1
ActiveX オブジェクトのフィルタリング 16-2
ActiveX フィルタリングの概要 16-2
ActiveX フィルタリングのイネーブル化 16-2
Java アプレットのフィルタリング 16-4
外部サーバによる URL および FTP 要求のフィルタリング 16-5
URL フィルタリングの概要 16-5
フィルタリング サーバの指定 16-5
コンテンツ サーバの応答のバッファリング 16-6
サーバ アドレスのキャッシング 16-7
HTTP URL のフィルタリング 16-8
HTTP フィルタリングの設定 16-8
長い HTTP URL のフィルタリングのイネーブル化 16-8
長い HTTP URL の短縮 16-9
フィルタリングから除外するトラフィックを指定 16-9
HTTPS URL のフィルタリング 16-9
FTP 要求のフィルタリング 16-10
フィルタリングの統計情報とフィルタリング設定の表示 16-11
フィルタリング サーバの統計情報の表示 16-11
バッファ設定とバッファ統計情報の表示 16-11
キャッシングの統計情報の表示 16-12
フィルタリング パフォーマンスの統計情報の表示 16-12
フィルタリング設定の表示 16-12

CHAPTER 17 ARP 検査およびブリッジング パラメータの設定 17-1
ARP 検査の設定 17-2
ARP 検査の概要 17-2
スタティック ARP エントリの追加 17-2
ARP 検査のイネーブル化 17-3

MAC アドレス テーブルのカスタマイズ 17-4
MAC アドレス テーブルの概要 17-4
スタティック MAC アドレスの追加 17-4
MAC アドレス タイムアウトの設定 17-5
MAC アドレス学習のディセーブル化 17-5
MAC アドレス テーブルの表示 17-5

CHAPTER 18 モジュラ ポリシー フレームワークの使用 18-1
モジュラ ポリシー フレームワークの概要 18-2
デフォルトのグローバル ポリシー 18-2
クラス マップを使用したトラフィックの識別 18-3
ポリシー マップを使用した動作の定義 18-5
ポリシー マップの概要 18-5
デフォルトのポリシー マップ 18-6
ポリシー マップの追加 18-6
サービス ポリシーを使用したインターフェイスへのポリシーの適用 18-8
モジュラ ポリシー フレームワークの例 18-9
HTTP トラフィックへの検査の適用 18-9
HTTP トラフィックへの検査のグローバルな適用 18-10
特定のサーバに対する HTTP トラフィックの検査および接続制限の適用 18-11
NAT を使用した HTTP トラフィックへの検査の適用 18-12

CHAPTER 19 ネットワーク攻撃の回避 19-1
接続制限とタイムアウトの設定 19-2
IP スプーフィングの回避 19-4
フラグメント サイズの設定 19-4
不正な接続のブロック 19-5

CHAPTER 20 アプリケーション レイヤ プロトコル検査の適用 20-1
アプリケーション インスペクション エンジンの概要 20-2
インスペクション エンジンの機能 20-3
NAT、PAT、アプリケーション検査 20-4
サポート対象プロトコル 20-4
アプリケーション エンジンのデフォルト 20-5
アプリケーション検査コンフィギュレーションの概要 20-7
デフォルトのアプリケーション検査 20-8
CTIQBE 検査 20-9
CTIQBE 検査の概要 20-9

制限事項および制約事項 20-9
CTIQBE 検査のイネーブル化および設定 20-10
CTIQBE 検査の確認およびモニタ 20-11
DNS 検査 20-13
DNS アプリケーション検査の動作 20-13
DNS Rewrite の動作 20-14
DNS Rewrite の設定 20-15
DNS Rewrite の alias コマンドの使用 20-15
DNS Rewrite の static コマンドの使用 20-15
2 つの NAT ゾーンを使用した DNS Rewrite の設定 20-16
3 つの NAT ゾーンを使用した DNS Rewrite 20-17
3 つの NAT ゾーンを使用した DNS Rewrite の設定 20-19
DNS 検査の設定 20-20
DNS 検査の確認およびモニタ 20-21
FTP 検査 20-22
FTP 検査の概要 20-22
strict オプションの使用 20-22
request-command deny コマンド 20-23
FTP 検査の設定 20-24
FTP 検査の確認およびモニタ 20-27
GTP 検査 20-28
GTP 検査の概要 20-28
GTP マップおよびコマンド 20-29
GTP 検査のイネーブル化および設定 20-30
GTP 検査の確認およびモニタ 20-32
H.323 検査 20-34
H.323 検査の概要 20-34
H.323 の動作 20-34
制限事項および制約事項 20-35
H.225 設定を必要とするトポロジー 20-36
H.225 マップ コマンド 20-37
H.323 検査のイネーブル化および設定 20-37
H.323 および H.225 タイムアウト値の設定 20-40
H.323 検査の確認およびモニタ 20-40
H.225 セッションのモニタ 20-40
H.245 セッションのモニタ 20-41
H.323 RAS セッションのモニタ 20-41
HTTP 検査 20-42

HTTP 検査の概要 20-42
拡張 HTTP 検査コマンド 20-43
拡張 HTTP 検査のイネーブル化および設定 20-43
ICMP 検査 20-45
ILS 検査 20-45
MGCP 検査 20-46
MGCP 検査の概要 20-46
MGCP コール エージェントおよびゲートウェイの設定 20-48
MGCP 検査の設定およびイネーブル化 20-48
MGCP タイムアウト値の設定 20-51
MGCP 検査の確認およびモニタ 20-51
NetBIOS 検査 20-52
PPTP 検査 20-52
RSH 検査 20-52
RTSP 検査 20-53
RTSP 検査の概要 20-53
RealPlayer の使用 20-54
制限事項および制約事項 20-54
RTSP 検査のイネーブル化および設定 20-54
SIP 検査 20-57
SIP 検査の概要 20-57
SIP インスタント メッセージング 20-57
IP アドレス プライバシー 20-58
SIP 検査のイネーブル化および設定 20-59
SIP タイムアウト値の設定 20-61
SIP 検査の確認およびモニタ 20-61
Skinny（SCCP）検査 20-63
SCCP 検査の概要 20-63
Cisco IP Phone のサポート 20-63
制限事項および制約事項 20-64
SCCP 検査の設定およびイネーブル化 20-64
SCCP 検査の確認およびモニタ 20-66
SMTP および拡張 SMTP 検査 20-67
SMTP および拡張 SMTP 検査の概要 20-67
SMTP および拡張 SMTP アプリケーション検査の設定およびイネーブル化 20-68
SNMP 検査 20-70
SNMP 検査の概要 20-70
SNMP アプリケーション検査のイネーブル化および設定 20-70

SQL*Net 検査 20-72
Sun RPC 検査 20-73
Sun RPC 検査の概要 20-73
Sun RPC 検査のイネーブル化および設定 20-73
Sun RPC サービスの管理 20-75
Sun RPC 検査の確認およびモニタ 20-76
TFTP 検査 20-77
XDMCP 検査 20-77

CHAPTER 21 管理アクセスの設定 21-1
Telnet アクセスの許可 21-2
SSH アクセスの許可 21-3
SSH アクセスの設定 21-3
SSH クライアントの使用 21-4
ASDM 用の HTTPS アクセスの許可 21-5
VPN 管理接続の許可 21-6
全トンネルの基本的な設定 21-6
VPN クライアント アクセスの設定 21-8
サイトツーサイト トンネルの設定 21-10
FWSM との ICMP 送受信の許可 21-12
システム管理者用の AAA 21-13
CLI アクセスの認証の設定 21-13
イネーブル EXEC モード アクセス認証の設定 21-14
enable コマンドの認証の設定 21-14
login コマンドを使用したユーザ認証 21-14
コマンド許可の設定 21-15
コマンド許可の概要 21-15
ローカル コマンド許可の設定 21-16
TACACS+ コマンド許可の設定 21-20
コマンド アカウンティングの設定 21-23
現在のログイン ユーザの表示 21-24
ロックアウトからの回復 21-25

CHAPTER 22 ソフトウェア、ライセンス、および設定の管理 22-1
ライセンスの管理 22-2
アクティベーション キーの取得 22-2
新しいアクティベーション キーの入力 22-3
アプリケーションまたは ASDM ソフトウェアのインストール 22-4
インストレーションの概要 22-4

FWSM CLI からのアプリケーション ソフトウェアのインストール 22-4
メンテナンス パーティションからのアプリケーション ソフトウェアのインストール 22-6
FWSM CLI からの ASDM のインストール 22-10
フェールオーバー ペアのアップグレード 22-11
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 22-12
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 22-13
メンテナンス ソフトウェアのインストール 22-14
メンテナンス ソフトウェア リリースの確認 22-14
メンテナンス ソフトウェアのアップグレード 22-15
コンフィギュレーション ファイルのダウンロードおよびバックアップ 22-17
フラッシュ メモリ内のファイルの確認 22-17
スタートアップまたは実行コンフィギュレーションへのテキスト コンフィギュレーションのダウンロード 22-17
ディスクへのコンテキスト コンフィギュレーションのダウンロード 22-18
設定のバックアップ 22-19
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 22-19
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のバックアップ 22-19
コンテキスト内のコンテキスト コンフィギュレーションのバックアップ 22-20
端末ディスプレイからの設定のコピー 22-20
自動アップデート サポートの設定 22-21
自動アップデート サーバとの通信の設定 22-21
自動アップデート ステータスの表示 22-22

CHAPTER 23 FWSM のモニタリング 23-1
SNMP の設定 23-2
SNMP の概要 23-2
SNMP のイネーブル化 23-4
ログの設定および管理 23-6
ロギングの概要 23-6
マルチコンテキスト モードでのロギング 23-7
ロギングのイネーブル化およびディセーブル化 23-7
設定された全出力先へのロギングのイネーブル化 23-7
設定された全出力先へのロギングのディセーブル化 23-8
ログ設定の表示 23-8
ログの出力先の設定 23-9
ログの出力先の概要 23-9

出力先としての Syslog サーバの指定 23-10
出力先としての電子メール アドレスの指定 23-12
出力先としての ASDM の指定 23-13
Telnet セッションを使用したログの表示 23-15
出力先としてのログ バッファの指定 23-16
出力先に送信するシステム ログ メッセージのフィルタリング 23-19
メッセージのフィルタリングの概要 23-19
クラスによるシステム ログ メッセージのフィルタリング 23-19
カスタム メッセージ リストによるシステム ログ メッセージのフィルタリング 23-21
ログ設定のカスタマイズ 23-22
ロギング キューの設定 23-22
システム ログ メッセージへの日付および時刻の記載 23-23
システム ログ メッセージへの装置 ID の記載 23-23
EMBLEM フォーマットのシステム ログ メッセージの生成 23-24
システム ログ メッセージのディセーブル化 23-24
システム ログ メッセージの重大度の変更 23-25
ログに使用する内部フラッシュ メモリの容量の変更 23-26
システム ログ メッセージの内容 23-27
システム ログ メッセージのフォーマット 23-27
重大度 23-28
システム ログ メッセージで使用される変数 23-28
logging コマンドのリスト 23-31

CHAPTER 24 FWSM のトラブルシューティング 24-1
設定のテスト 24-2
ICMP デバッグ メッセージおよびシステム メッセージのイネーブル化 24-2
FWSM のインターフェイスへの ping の実行 24-3
FWSM 経由の ping の実行 24-5
テスト設定のディセーブル化 24-6
FWSM のリロード 24-7
パスワード復旧の実行 24-8
アプリケーション パーティションのパスワードおよび AAA 設定の消去 24-8
メンテナンス パーティション パスワードのリセット 24-9
その他のトラブルシューティング ツール 24-10
デバッグ メッセージの表示 24-10
パケットのキャプチャ 24-10

クラッシュ ダンプの表示 24-10
一般的な問題 24-11

APPENDIX A
仕様 A-1
スイッチ ハードウェアおよびソフトウェアの互換性 A-2
ライセンス対象機能 A-2
物理仕様 A-3
機能の制限 A-3
管理対象のシステム リソース A-4
固定システム リソース A-5
ルールの制限 A-6

APPENDIX B
設定例 B-1
ルーテッド モードの設定例 B-1
例 1：外部からアクセスのあるマルチモード ファイアウォール B-1
システム コンフィギュレーション（例 1） B-3
admin コンテキスト コンフィギュレーション（例 1） B-4
カスタマー A のコンテキスト コンフィギュレーション（例 1） B-4
カスタマー B のコンテキスト コンフィギュレーション（例 1） B-5
カスタマー C のコンテキスト コンフィギュレーション（例 1） B-5
スイッチの設定（例 1） B-6
例 2：同じセキュリティ レベルを使用するシングル モード ファイアウォールの例 B-6
FWSM の設定（例 2） B-7
スイッチの設定（例 2） B-8
例 3：マルチコンテキストの共有リソースの例 B-8
システム コンフィギュレーション（例 3） B-10
admin コンテキスト コンフィギュレーション（例 3） B-11
部門 1 のコンテキスト コンフィギュレーション（例 3） B-12
部門 2 のコンテキスト コンフィギュレーション（例 3） B-13
スイッチの設定（例 3） B-13
例 4：IPv6 の設定例 B-14
透過モードでの設定例 B-15
例 5：外部からのアクセスのあるマルチモードの透過ファイアウォールの例 B-15
システム コンフィギュレーション（例 5） B-17
admin コンテキスト コンフィギュレーション（例 5） B-18
カスタマー A のコンテキスト コンフィギュレーション（例 5） B-18
カスタマー B のコンテキスト コンフィギュレーション（例 5） B-19

カスタマー C のコンテキスト コンフィギュレーション（例 5） B-19
フェールオーバーの設定例 B-20
例 6：ルーテッド モードのフェールオーバー B-20
プライマリ FWSM の設定（例 6） B-21
セカンダリ FWSM のシステム コンフィギュレーション（例 6） B-23
スイッチの設定（例 6） B-23
例 7：透過モードのフェールオーバー B-24
プライマリ FWSM の設定（例 7） B-24
セカンダリ FWSM のシステム コンフィギュレーション（例 7） B-27
スイッチの設定（例 7） B-28
例 8：非対称ルーティング サポートを使用したアクティブ / アクティブのフェールオーバー B-28
前提条件 B-29
プライマリ FWSM の設定（例 8） B-29
セカンダリ FWSM の設定（例 8） B-32
スイッチの設定（例 8） B-33

APPENDIX C
CLI の使用 C-1
ファイアウォール モードおよびセキュリティ コンテキスト モード C-1
コマンド モードおよびプロンプト C-2
構文の形式 C-3
コマンドの短縮形 C-3
コマンドラインの編集 C-3
コマンドの補完 C-4
コマンド ヘルプ C-4
show コマンド出力のフィルタリング C-5
コマンド出力のページング C-6
コメントの追加 C-6
テキスト コンフィギュレーション ファイル C-7
テキスト ファイル内の行とコマンドの対応 C-7
コマンド固有コンフィギュレーション モードのコマンド C-7
自動テキスト エントリ C-7
行の順序 C-8
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 C-8
パスワード C-8
複数のセキュリティ コンテキスト ファイル C-8

APPENDIX D
アドレス、プロトコル、およびポート D-1
IPv4 アドレスおよびサブネット マスク D-2

クラス D-2
プライベート ネットワーク D-2
サブネット マスク D-3
サブネット マスクの判別 D-3
サブネット マスクで使用するアドレスの判別 D-4
IPv6 アドレス D-6
IPv6 アドレス フォーマット D-6
IPv6 アドレス タイプ D-7
ユニキャスト アドレス D-7
マルチキャスト アドレス D-10
エニーキャスト アドレス D-11
必須アドレス D-11
IPv6 アドレス プレフィクス D-12
プロトコルおよびアプリケーション D-13
TCP ポートおよび UDP ポート D-14
ローカル ポートおよびプロトコル D-16
ICMP のタイプ D-17

GLOSSARY 用語集

INDEX 索引

マニュアルの概要

ここでは、マニュアルの目的および構成を示し、関連する製品およびサービスに関する追加情報を探す方法について説明します。

この章で説明する内容は、次のとおりです。

- 対象読者（p.xxiv）
- 目的（p.xxiv）
- マニュアルの構成（p.xxv）
- 表記法（p.xxvii）
- 関連資料（p.xxvii）
- マニュアルの入手方法（p.xxviii）
- シスコ製品のセキュリティ（p.xxix）
- テクニカル サポート（p.xxx）
- その他の資料および情報の入手方法（p.xxxii）

対象読者

このマニュアルは、次の作業を担当するネットワーク管理者が対象です。

- ネットワーク セキュリティの管理
- ファイアウォールのインストールおよび設定
- デフォルト ルート、スタティック ルート、TCP サービス、および UDP サービスの管理

目的

このマニュアルでは、Cisco 6500 スイッチおよび Cisco 7600 ルータでサポートされている単一幅のサービス モジュール、Firewall Services Module（FWSM）3.1 をコマンドライン インターフェイスを使用して設定する方法および手順について説明します。FWSM はお使いのネットワークを不正使用から守ります。このマニュアルではすべての機能を扱うわけではなく、最も標準的なコンフィギュレーション シナリオのみを説明します。

Web ベースの GUI アプリケーション、ASDM を使用して FWSM を設定およびモニタすることもできます。ASDM には、一般的なコンフィギュレーション シナリオのためのコンフィギュレーション ウィザード、およびあまり一般的ではないシナリオのためのオンライン ヘルプが組み込まれています。詳細については、次の URL を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/netsec/secmgmt/asdm/index.htm

マニュアルの構成

このマニュアルは、次の章で構成されています。

章	タイトル	説明
1	FWSM について	FWSM の高レベルな概要を提供します。
2	Firewall Services Module を使用するためのスイッチの設定	FWSM と組み合わせて使用するスイッチの設定方法について説明します。
3	Firewall Services Module の接続および設定の管理	コマンドライン インターフェイスへのアクセス方法および設定の管理方法について説明します。
4	セキュリティ コンテキストの設定	セキュリティ コンテキストの使用方法およびマルチコンテキスト モードをイネーブルにする方法について説明します。
5	ファイアウォール モードの設定	FWSM の 2 つの動作モード、ルーテッド モードと透過モードについて、および各モードでのデータ処理の違いについて詳しく説明します。
6	インターフェイス パラメータの設定	インターフェイス名、セキュリティ レベル、IP アドレスの設定方法について説明します。透過ファイアウォール モード インターフェイスにブリッジ グループを設定する方法についても説明します。
7	基本設定	コンフィギュレーションを機能させるために通常必要な基本設定について説明します。
8	IP ルーティングおよび DHCP サービスの設定	IP ルーティングおよび DHCP の設定方法について説明します。
9	IPv6 の設定	IPv6 をイネーブルにして設定する方法について説明します。
10	アクセス リストでのトラフィックの識別	アクセス リストでトラフィックを識別する方法について説明します。
11	ネットワーク アクセスの許可または拒否	アクセス リストを使用して FWSM を通過するネットワーク アクセスを制御する方法を説明します。
12	NAT の設定	アドレス変換の実行方法について説明します。
13	フェールオーバーの設定	フェールオーバー機能について説明します。この機能により、2 つの FWSM を設定して 1 つで障害が発生した場合にもう 1 つに操作を引き継がせることができます。
14	AAA サーバとローカル データベースの設定	AAA サーバおよびローカル データベースの設定方法について説明します。
15	ネットワーク アクセスへの AAA の適用	AAA のネットワーク アクセスをイネーブルにする方法について説明します。
16	フィルタリング サービスの適用	Web トラフィックをフィルタリングして、セキュリティ リスクを軽減したり不正使用を防ぐ方法について説明します。
17	ARP 検査およびブリッジング パラメータの設定	ARP インスペクションをイネーブルにする方法、およびブリッジング操作をカスタマイズする方法について説明します。

章	タイトル	説明
18	モジュラ ポリシー フレームワークの使用	Modular Policy Framework を使用して TCP、一般的な接続設定、およびインスペクションのセキュリティ ポリシーを作成する方法について説明します。
19	ネットワーク攻撃の回避	ネットワーク攻撃の遮断および対処を行う保護機能の設定方法について説明します。
20	アプリケーション レイヤ プロトコル検査の適用	アプリケーション検査を使用および設定する方法について説明します。
21	管理アクセスの設定	システム管理のために Telnet、SSH、HTTPS、および VPN を経由して FWSM にアクセスする方法について説明します。
22	ソフトウェア、ライセンス、および設定の管理	ライセンス キーを入力してソフトウェアおよびコンフィギュレーション ファイルをダウンロードする方法について説明します。
23	FWSM のモニタリング	FWSM のモニタ方法について説明します。
24	FWSM のトラブルシューティング	FWSM のトラブルシューティングについて説明します。
A	仕様	FWSM の仕様について説明します。
B	設定例	FWSM の一般的な実装方法をいくつか説明します。
C	CLI の使用	CLI を使用して FWSM を設定する方法について説明します。
D	アドレス、プロトコル、およびポート	IP アドレス、プロトコル、アプリケーションへのクイック リファレンスを提供します。
	GLOSSARY	このマニュアルで使用する用語の用語集です。
	Index	このマニュアルの索引です。

表記法

FWSM コマンド構文の記述には、次の表記法を使用しています。

コマンドの説明では、次の表記法を使用しています。

- 波カッコ（{ }）は必須の選択肢です。
- 角カッコ（[ ]）は省略可能な要素です。
- 縦棒（|）は選択要素の区切りです。
- **太字**は表示どおりにユーザが入力しなければならないコマンドおよびキーワードです。
- *イタリック体*はユーザが値を指定する引数です。

例では、次の表記法を使用しています。

- 画面表示およびコマンドラインは `screen` フォントで示しています。
- 例でユーザが入力すべき情報は、**太字**の **`screen`** フォントで示しています。
- ユーザが値を指定する変数は、*イタリック体*の *`screen`* フォントで示しています。
- 例にはさまざまなプラットフォームの出力が含まれている可能性があります。たとえば、ご使用のプラットフォームには存在しないインターフェイス タイプであるために、そのインターフェイス タイプを認識できないことがあります。ただし、大きな相違はないはずです。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

モード、プロンプト、構文の詳細については、付録 C「CLI の使用」を参照してください。

関連資料

詳細については、次のマニュアルを参照してください。

- 『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』
- 『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages*』
- 『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Installation Note*』
- 『*Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module to Release 3.1*』
- 『*Release Notes for the Catalyst 6500 Series and Cisco 7600 Series Firewall Services Module, Software Release 3.1*』

マニュアルの入手方法

シスコ製品のマニュアルおよびその他の資料は、Cisco.com で入手することができます。また、テクニカル サポートおよびその他のテクニカル リソースは、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

シスコの最新のマニュアルは、次の URL からアクセスしてください。

http://www.cisco.com/univercd/home/home.htm

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

http://www.cisco.com/jp

シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Documentation DVD パッケージでご利用いただけます。Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。この DVD パッケージは、単独で入手することができます。

Cisco.com（Cisco Direct Customers）に登録されている場合、Ordering ツールまたは Cisco Marketplace から Cisco Documentation DVD（Customer Order Number DOC-DOCDVD=）を発注できます。

Cisco Ordering ツール：

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace：

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

マニュアルの発注方法

マニュアルの発注方法については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

シスコ製品のマニュアルは、次の方法でご発注いただけます。

- Cisco.com（Cisco Direct Customers）に登録されている場合、Ordering ツールからシスコ製品のマニュアルを発注できます。次の URL にアクセスしてください。

  http://www.cisco.com/en/US/partner/ordering/
- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合わせください。

シスコ製品のセキュリティ

シスコでは、無償の Security Vulnerability Policy ポータルを次の URL で提供しています。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトから、以下のタスクを実行できます。

- シスコ製品における脆弱性を報告する。
- シスコ製品のセキュリティ問題に対する支援を受ける。
- シスコからのセキュリティ情報を入手するために登録を行う。

シスコ製品に関するセキュリティ勧告および注意のリストが以下の URL で確認できます。

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

勧告および注意事項が変更された際に、リアルタイムで確認したい場合は、以下の URL から Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）にアクセスできます。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、安全な製品を提供することを目指しています。製品のリリース前に社内でテストを実施し、すべての脆弱性を迅速に修正するように努めております。お客様がシスコ製品の脆弱性を発見したと思われる場合は、次の PSIRT にご連絡ください。

- 緊急度の高い問題 — security-alert@cisco.com
- 緊急度の低い問題 — psirt@cisco.com

ヒント お客様が第三者に知られたくない情報をシスコに送信する場合、Pretty Good Privacy（PGP）または PGP と互換性のある製品を使用して情報を暗号化することを推奨します。PSIRT は、PGP バージョン 2.*x* ～ 8.*x* と互換性のある暗号化情報を取り扱うことができます。

無効な暗号鍵または失効した暗号鍵は使用しないでください。PSIRT と通信する際は、次の公開鍵サーバの一覧に記載されている有効な公開鍵を使用してください。

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

緊急度の高い問題の場合、次の電話番号で PSIRT に問い合わせることができます。

- 1 877 228-7302
- 1 408 525-6532

テクニカル サポート

Cisco Technical Support では、シスコシステムズとサービス契約を結んでいるお客様、パートナー、リセラー、販売店を対象として、評価の高い 24 時間体制のテクニカル サポートを提供しています。Cisco.com の Cisco Technical Support Web サイトでは、広範囲にわたるオンラインでのサポート リソースを提供しています。さらに、Technical Assistance Center（TAC）では、電話でのサポートも提供しています。シスコシステムズとサービス契約を結んでいない場合は、リセラーにお問い合わせください。

Cisco Technical Support Web サイト

Cisco Technical Support Web サイトでは、オンラインで資料やツールを利用して、トラブルシューティングやシスコ製品およびテクノロジーに関する技術上の問題の解決に役立てることができます。Cisco Technical Support Web サイトは、1 年中いつでも利用することができます。次の URL にアクセスしてください。

http://www.cisco.com/techsupport

Cisco Technical Support Web サイト上のツールにアクセスする際は、いずれも Cisco.com のログイン ID およびパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、次の URL で登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注）テクニカル サポートにお問い合わせいただく前に、Cisco Product Identification（CPI）ツールを使用して、製品のシリアル番号をご確認ください。CPI ツールへは、Documentation & Tools の下にある **Tools & Resources** リンクをクリックして、Cisco Technical Support Web サイトからアクセスできます。Alphabetical Index ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下にある **Cisco Product Identification Tool** リンクをクリックしてください。CPI ツールは、製品 ID またはモデル名、ツリー表示、または特定の製品に対する **show** コマンド出力のコピー＆ペーストによる 3 つの検索オプションを提供します。検索結果には、シリアル番号のラベルの場所がハイライトされた製品の説明図が表示されます。テクニカル サポートにお問い合わせいただく前に、製品のシリアル番号のラベルを確認し、メモなどに控えておいてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register/

Service Request ツールの使用

オンラインの TAC Service Request ツールを使えば、S3 および S4 の問題について最も迅速にテクニカル サポートを受けられます（ネットワークの障害が軽微である場合、あるいは製品情報が必要な場合）。状況をご説明いただくと、TAC Service Request ツールが推奨される解決方法を提供します。これらの推奨リソースを使用しても問題が解決しない場合は、TAC の技術者が対応します。TAC Service Request ツールは次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

問題が S1 または S2 であるか、インターネットにアクセスできない場合は、電話で TAC にご連絡ください（運用中のネットワークがダウンした場合、あるいは重大な障害が発生した場合）。S1 および S2 の問題には TAC の技術者がただちに対応し、業務を円滑に運営できるよう支援します。

電話でテクニカル サポートを受ける際は、次の番号のいずれかをご使用ください。

アジア太平洋：+61 2 8446 7411（オーストラリア：1 800 805 227）
EMEA：+32 2 704 55 55
米国：1 800 553-2447

TAC の連絡先一覧については、次の URL にアクセスしてください。

http://www.cisco.com/techsupport/contacts

問題の重大度の定義

すべての問題を標準形式で報告するために、問題の重大度を定義しました。

重大度 1（S1）— ネットワークがダウンし、業務に致命的な損害が発生する場合。24 時間体制であらゆる手段を使用して問題の解決にあたります。

重大度 2（S2）— ネットワークのパフォーマンスが著しく低下、またはシスコ製品のパフォーマンス低下により業務に重大な影響がある場合。通常の業務時間内にフルタイムで問題の解決にあたります。

重大度 3（S3）— ネットワークのパフォーマンスが低下しているが、ほとんどの業務運用が機能している場合。通常の業務時間内にサービスの復旧を行います。

重大度 4（S4）— シスコ製品の機能、インストレーション、基本的なコンフィギュレーションについて、情報または支援が必要で、業務への影響がほとんどまたはまったくない場合。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手することができます。

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、およびロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスしてください。

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

- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を幅広く発行しています。初心者から上級者まで、さまざまな読者向けの出版物があります。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』は、シスコシステムズが発行するテクニカル ユーザ向けの季刊誌で、インターネットやネットワークへの投資を最大限に活用するのに役立ちます。『*Packet*』には、ネットワーク分野の最新動向、テクノロジーの進展、およびシスコの製品やソリューションに関する記事をはじめ、ネットワークの配置やトラブルシューティングのヒント、設定例、お客様の事例研究、認定やトレーニングに関する情報、および多数の詳細なオンライン リソースへのリンクが盛り込まれています。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

- 『*iQ Magazine*』は、シスコのテクノロジーを使って収益の増加、ビジネス効率の向上、およびサービスの拡大を図る方法について学ぶことを目的とした、シスコシステムズが発行する成長企業向けの季刊誌です。この季刊誌は、実際の事例研究や事業戦略を用いて、これら企業が直面するさまざまな課題や、問題解決の糸口となるテクノロジーを明確化し、テクノロジーの投資に関して読者が正しい決断を行う手助けをします。『*iQ Magazine*』には、次の URL からアクセスしてください。

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

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコシステムズが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコシステムズは最高水準のネットワーク関連のトレーニングを実施しています。トレーニングの最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

クイック スタート手順

ここでは、FWSM をルーテッド モードまたは透過モードで動作させるために最小限必要な設定について説明します。

- ルーテッド ファイアウォールの最小限の設定手順（p.xxxiv）
- 透過ファイアウォールの最小限の設定手順（p.xxxv）

ルーテッド ファイアウォールの最小限の設定手順

FWSM をルーテッド モードで設定するための手順は、次のとおりです。

	作業	説明
ステップ 1	Firewall Services Module への VLAN 割り当て（p.2-4）	FWSM がスイッチ上でトラフィックを送受信できるように、スイッチ上で FWSM に VLAN を割り当てる必要があります。
ステップ 2	（場合によって必要）MSFC への SVI の追加（p.2-7）	MSFC を使用して、FWSM に割り当てられた VLAN 間でルーティングを行う場合は、この作業が必要です。
ステップ 3	Firewall Services Module との接続（p.3-2）	スイッチの CLI から FWSM とのセッションを開始すると、FWSM の CLI にアクセスできます。
ステップ 4	（場合によって必要、マルチコンテキスト モード限定）マルチコンテキスト モードのイネーブル化またはディセーブル化（p.4-11）	マルチコンテキスト モードを使用するが、FWSM がマルチコンテキスト モード用にまだ設定されていない場合、またはシングル モードに戻す場合、この作業が必要です。
ステップ 5	（マルチコンテキスト モード限定）セキュリティ コンテキストの設定（p.4-20）	セキュリティ コンテキストを追加します。
ステップ 6	（マルチコンテキスト モード限定）コンテキストとシステム実行スペース間の切り替え（p.4-24）	システム実行スペースで必要な設定およびコンテキスト内で必要な設定があるので、コンテキストとシステム実行スペース間の切り替え方法を理解する必要があります。
ステップ 7	ルーテッド ファイアウォール モードのインターフェイスの設定（p.6-3）	各 VLAN インターフェイスについて、名前（内部または外部）、セキュリティ レベル、および IP アドレスを設定する必要があります。
ステップ 8	デフォルト ルートの設定（p.8-4）	アップストリーム ルータへのデフォルト ルートを作成します。
ステップ 9	次のいずれかの方法によるルーティングの設定 • スタティック ルートの設定（p.8-3） • （シングルコンテキスト モード限定）OSPF の設定（p.8-5） • （シングルコンテキスト モード限定）RIP の設定（p.8-18）	マルチコンテキスト モードで使用できるルーティング方式は、スタティック ルーティングだけです。シングル モードでは、スタティック、RIP、または OSPF を選択できます。RIP のサポートはパッシブ モードに限定されます。
ステップ 10	（場合によって必要）次の NAT 方式から 1 つまたは複数を使用 • ダイナミック NAT および PAT の使用方法（p.12-17） • スタティック NAT の使用方法（p.12-27） • スタティック PAT の使用方法（p.12-29）	プライベート アドレスを使用する場合、またはセキュリティを強化する場合は、NAT を設定します。
ステップ 11	拡張 ACE の追加（p.10-8）	トラフィックが FWSM を通過するためには、事前にトラフィックを許可するアクセス リストを作成する必要があります。
ステップ 12	アクセス リストのインターフェイスへの適用（p.11-5）	アクセス リストをインターフェイスに適用します。

透過ファイアウォールの最小限の設定手順

FWSM を透過モードで設定するための手順は、次のとおりです。

	作業	説明
ステップ 1	Firewall Services Module への VLAN 割り当て（p.2-4）	FWSM がスイッチ上でトラフィックを送受信できるように、スイッチ上で FWSM に VLAN を割り当てる必要があります。
ステップ 2	（場合によって必要）MSFC への SVI の追加（p.2-7）	MSFC を使用して、FWSM に割り当てられた VLAN 間でルーティングを行う場合は、この作業が必要です。
ステップ 3	Firewall Services Module との接続（p.3-2）	スイッチの CLI から FWSM とのセッションを開始すると、FWSM の CLI にアクセスできます。
ステップ 4	（場合によって必要、マルチコンテキスト モード限定）マルチコンテキスト モードのイネーブル化またはディセーブル化（p.4-11）	マルチコンテキスト モードを使用するが、FWSM がマルチコンテキスト モード用にまだ設定されていない場合、またはシングル モードに戻す場合、この作業が必要です。
ステップ 5	（マルチコンテキスト モード限定）セキュリティ コンテキストの設定（p.4-20）	セキュリティ コンテキストを追加します。
ステップ 6	（マルチコンテキスト モード限定）コンテキストとシステム実行スペース間の切り替え（p.4-24）	システム実行スペースで必要な設定およびコンテキスト内で必要な設定があるので、コンテキストとシステム実行スペース間の切り替え方法を理解する必要があります。
ステップ 7	透過ファイアウォール モードまたはルーテッド ファイアウォール モードの設定（p.5-17）	値を設定する前に、ファイアウォールのモードを透過モードに設定する必要があります。モードを変更すると、設定が消去されます。マルチコンテキスト モードでは、各コンテキストでモードを設定します。
ステップ 8	透過ファイアウォール インターフェイスのパラメータの設定（p.6-5）	各 VLAN インターフェイスについて、名前（内部または外部）、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必要があります。
ステップ 9	IP アドレスのブリッジ グループへの割り当て（p.6-7）	各ブリッジ グループに IP アドレスを割り当てます。
ステップ 10	デフォルト ルートの設定（p.8-4）	管理トラフィックを戻すために、アップストリーム ルータへのデフォルト ルートを作成します。
ステップ 11	拡張 ACE の追加（p.10-8）	トラフィックが FWSM を通過するためには、事前にトラフィックを許可するアクセス リストを作成する必要があります。
ステップ 12	アクセス リストのインターフェイスへの適用（p.11-5）	アクセス リストをインターフェイスに適用します。

FWSM について

Firewall Services Module（FWSM）は、Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータに搭載する、高性能でコンパクトなステートフル ファイアウォール モジュールです。

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。ファイアウォールを使用すると、たとえば、人事ネットワークとユーザ ネットワークを切り離しておくなどといった形で、内部ネットワーク相互間の保護も実現できます。Web、FTP サーバなど、外部ユーザが利用できるようにしなければならないネットワーク リソースがある場合は、ファイアウォールの背後の *Demilitarized Zone*（DMZ; 非武装地帯）と呼ばれる独立したネットワークに配置できます。ファイアウォールは DMZ への限定的なアクセスを認めますが、DMZ にあるのはパブリック サーバだけなので、攻撃を受けても影響を受けるのはサーバだけであり、他の内部ネットワークに影響はありません。認証または許可を要求したり、外部の URL フィルタリング サーバと連動させたりして、特定のアドレスだけを許可することによって、内部ユーザから外部ネットワークへのアクセス（インターネット アクセスなど）も制御できます。

FWSM には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）、透過（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、何百ものインターフェイス、およびその他の最先端の機能が多数組み込まれています。

ファイアウォールに接続されたネットワークについて述べる場合、*外部*ネットワークはファイアウォールの向こう側にあり、*内部*ネットワークはファイアウォールの手前にあって保護されています。*DMZ* はファイアウォールの手前にありますが、外部ユーザから一定のアクセスが可能です。FWSM では、多数の内部インターフェイス、多数の DMZ、さらに必要に応じて多数の外部インターフェイスを含め、多数のインターフェイスにさまざまなセキュリティ ポリシーを設定するので、このような用語はあくまでも一般的な用語として使用されます。

この章で説明する内容は、次のとおりです。

- セキュリティ ポリシーの概要（p.1-2）
- スイッチにおける Firewall Services Module の動作（p.1-4）
- ファイアウォール モードの概要（p.1-6）
- ステートフル インスペクションの概要（p.1-7）
- セキュリティ コンテキストの概要（p.1-8）

セキュリティ ポリシーの概要

セキュリティ ポリシーによって、ファイアウォールを通過して別のネットワークにアクセスさせるトラフィックを決定します。FWSM はアクセス リストで明示的に許可されていないかぎり、どのようなトラフィックも通過させません。トラフィックに、セキュリティ ポリシーをカスタマイズする処理を適用できます。ここでは、次の内容について説明します。

- アクセス リストでのトラフィックの許可または拒否（p.1-2）
- NAT の適用（p.1-2）
- 通過トラフィックに対する AAA の使用（p.1-2）
- インターネット フィルタリングの適用（p.1-2）
- アプリケーション検査の適用（p.1-3）
- 接続制限の適用（p.1-3）

アクセス リストでのトラフィックの許可または拒否

アクセス リストを適用して、トラフィックにインターフェイスの通過を許可できます。透過ファイアウォール モードの場合、EtherType アクセス リストを適用して、IP 以外のトラフィックを通過させることもできます。

NAT の適用

NAT の利点の一部は、次のとおりです。

- 内部ネットワーク上でプライベート 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上でルーティングできません。
- NAT は他のネットワークに対してローカル アドレスを隠すので、攻撃側はホストの実アドレスを突き止めることができません。
- NAT は IP アドレスのオーバーラップをサポートすることによって、IP ルーティングに伴う問題を解決します。

通過トラフィックに対する AAA の使用

HTTP など特定タイプのトラフィックに、認証または許可あるいはその両方を要求できます。FWSM は RADIUS または TACACS+ サーバにもアカウンティング情報を送信します。

インターネット フィルタリングの適用

アクセス リストを使用すれば特定の Web サイトまたは FTP サーバへの発信アクセスを阻止できますが、インターネットの規模およびダイナミック特性を考慮すると、この方法での Web 使用の設定および管理は実質的ではありません。FWSM と、次のインターネット フィルタリング製品の 1 つを実行する別途サーバを併用することを推奨します。

- Websense Enterprise
- Sentian（N2H2）

アプリケーション検査の適用

ユーザ データ パケットに IP アドレス情報が組み込まれているサービス、またはダイナミックに割り当てられるポート上でセカンダリ チャネルを開始するサービスには、インスペクション エンジンが必要です。これらのプロトコルは、ディープ パケット インスペクションを実行するために FWSM が必要です。

接続制限の適用

TCP/UDP 接続および初期接続を制限できます。接続数および初期接続数を制限することで、DoS 攻撃からシステムを保護できます。FWSM は初期制限によって TCP 代行受信をトリガーします。TCP 代行受信は、TCP SYN パケットでインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先間で所定のハンドシェイクが完了していない接続要求です。

スイッチにおける Firewall Services Module の動作

FWSM は、Cisco 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータに搭載できます。どちらのシリーズも、次の点の除いて構成は同じです。

- Catalyst 6500 シリーズ スイッチは、2 種類のソフトウェア モードをサポートします。
  - スイッチのスーパバイザおよび内蔵 Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）の両方で、Cisco IOS ソフトウェア（「スーパバイザ IOS」）を使用
  - スーパバイザ上で Catalyst Operating System（OS; オペレーティング システム）、MSFC 上で Cisco IOS ソフトウェアを使用

  スイッチ本体で実行するコマンドと設定は、両方のモードについて説明します。
- Cisco 7600 シリーズ ルータがサポートするのは、Cisco IOS ソフトウェアだけです。

このマニュアルでは両方のシリーズの総称として、「スイッチ」を使用します。

FWSM は独自の OS で動作します。

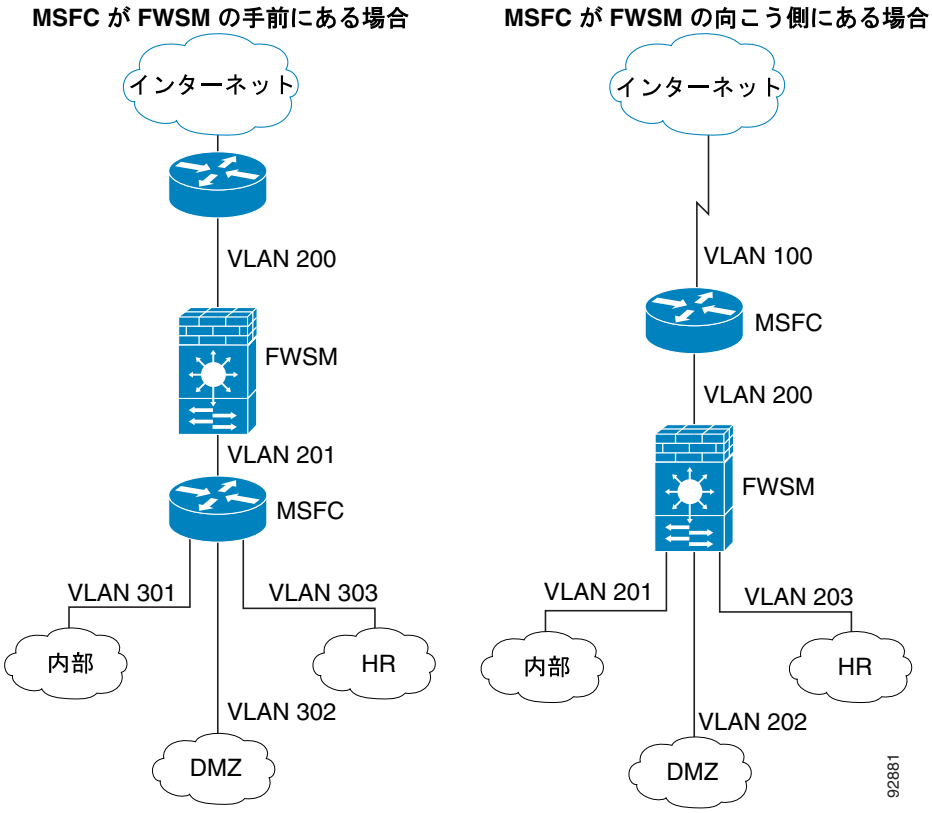
MSFC の使用方法

スイッチにはスイッチング プロセッサ（スーパバイザ）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。使用する場合は、1 つまたは複数の VLAN インターフェイスを MSFC に割り当てることができます（スイッチのソフトウェア バージョンが複数の Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）をサポートする場合は、表 A-1 [p.A-2] を参照）。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 MSFC 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）。

MSFC 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、FWSM の内部インターフェイスに VLAN 201 を割り当てているので、MSFC 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、FWSM の外部インターフェイスに VLAN 200 を割り当てているので、MSFC はファイアウォールの向こう側になります。

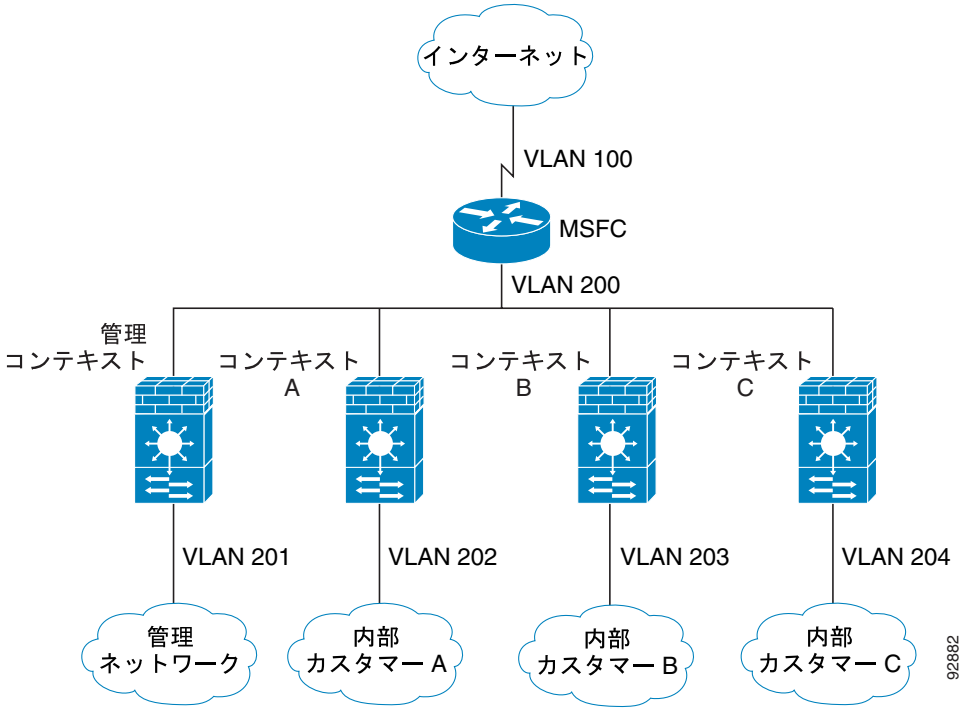
左側の例では、MSFC は VLAN 201、301、302、および 303 の間をルーティングします。宛先がインターネットの場合以外、内部トラフィックは FWSM を通過しません。右側の例では、FWSM は内部 VLAN 201、202、および 203 間のすべてのトラフィックを処理して保護します。

図 1-1　MSFC の配置



マルチコンテキスト モードでは、FWSM より手前に MSFC 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。MSFC を複数のコンテキストに接続すると、MSFC 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。マルチコンテキストの場合は通常、あらゆるコンテキストが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される前に、MSFC 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 の配置



ファイアウォール モードの概要

FWSM は、2 種類のファイアウォール モードで動作可能です。

- ルーテッド
- 透過

ルーテッド モードの場合、FWSM はネットワーク上のルータ ホップとみなされます。

透過モードの場合、FWSM は「ワイヤの凹凸」、すなわち「ステルス ファイアウォール」のように動作し、ルータ ホップにはなりません。FWSM は内部および外部インターフェイスの同一ネットワークに接続します。最大 8 ペアのインターフェイス（ブリッジ グループ）を設定して、コンテキストごとに 8 つの異なるネットワークに接続できます。

ネットワーク構成を簡素化する場合は、透過ファイアウォールを使用します。攻撃側にファイアウォールが見えないようにする場合も、透過モードが便利です。ルーテッド モードでブロックされるトラフィックに透過ファイアウォールを使用することもできます。たとえば、透過ファイアウォールはサポート対象外のルーティング プロトコルを許可できます。

マルチコンテキスト モードでは、各コンテキストに対して別個にモードを選択できるため、あるコンテキストを透過モードで実行し、別のコンテキストをルーテッド モードで実行できます。

ステートフル インスペクションの概要

ファイアウォールを通過するあらゆるトラフィックは、Adaptive Security Algorithm（ASA; アダプティブ セキュリティ アルゴリズム）を使用して点検され、通過が許可されるか、または廃棄されるかのどちらかになります。単純なパケット フィルタでも、送信元アドレス、宛先アドレス、およびポートを確認できますが、パケット シーケンスやフラグは確認できません。フィルタの場合はさらに、個々のパケットをフィルタと突き合わせるので、処理が遅くなる可能性があります。

ただし、FWSM などのステートフル ファイアウォールは、次のようにパケットの状態を考慮します。

- 新しい接続かどうか

  新しい接続の場合、ファイアウォールはパケットをアクセス リストと照合し、その他の作業を実行して、パケットを許可するのか拒否するのかを決定する必要があります。この確認を行うために、セッションの最初のパケットは「セッション管理パス」をたどり、さらにトラフィックのタイプによっては、「制御プレーン パス」もたどります。

  セッション管理パスは、次の作業を担当します。

  — アクセス リスト チェックの実行

  — ルート検索の実行

  — NAT 変換（xlate）の割り当て

  — 「高速パス」でのセッション確立

  （パケット ペイロードを点検または変更しなければならない）レイヤ 7 インスペクションが必要なパケットは、さらに制御プレーン パスへ送られます。2 つ以上のチャネルを使用するプロトコルには、レイヤ 7 インスペクション エンジンが必要です。この場合のチャネルとは、well-known ポートの番号を使用するデータ チャネルとセッションごとに異なるポート番号を使用する制御チャネルです。これに該当するプロトコルは、FTP、H.323、および SNMP です。

（注） FWSM は、3 つの特殊なネットワーキング プロセッサ上でセッション管理パスおよび高速パスの処理を実行します。制御プレーン パスの処理は、FWSM へのトラフィックを処理し、設定および管理作業も行う、汎用プロセッサで実行されます。

- 確立された接続かどうか

  接続がすでに確立されている場合、ファイアウォールがパケットを再チェックする必要はありません。一致する大部分のパケットは双方向とも、高速パスを通過します。高速パスは、次の作業を担当します。

  — IP チェックサム検証

  — セッション検査

  — TCP シーケンス番号の検査

  — 既存セッションに基づいた NAT 変換

  — レイヤ 3 およびレイヤ 4 のヘッダー調整

  UDP または他のコネクションレス プロトコルの場合、FWSM は高速パスも使用できるように接続ステート情報を作成します。

  レイヤ 7 のインスペクションを必要とするプロトコルのデータ パケットも、高速パスを通過します。

  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制御プレーン パスを通過させなければならないものがあります。セッション管理パスへ送られるパケットには、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。制御プレーン パスへ送られるパケットには、レイヤ 7 のインスペクションを必要とするプロトコルの制御パケットが含まれます。

（注）QoS の互換性を確保するために、FWSM は FWSM を通過するすべてのトラフィックの DSCP ビットを保存します。

セキュリティ コンテキストの概要

1 つの FWSM をセキュリティ コンテキストと呼ばれる複数の仮想デバイスに分割できます。各コンテキストには独自のセキュリティ ポリシー、インターフェイス、および管理者が与えられます。マルチコンテキストは、スタンドアロンのデバイスを複数使用することと同様です。マルチコンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、管理など数多くの機能がサポートされています。ダイナミック ルーティング プロトコルなど一部の機能はサポートされていません。

マルチコンテキスト モードでは、FWSM にはコンテキストごとに、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ぼすべてのオプションのコンフィギュレーションが含まれます。システム管理者は、システム コンフィギュレーション（シングル モード 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に相当します）でコンテキストを設定することによって、コンテキストを追加および管理します。システム コンフィギュレーションには FWSM の基本設定が含まれます。システム コンフィギュレーションには、システムそのもののネットワーク インターフェイスまたはネットワーク設定値は含みません。システムがネットワーク リソースにアクセスする必要がある場合に（サーバからコンテキストをダウンロードする場合など）、管理（admin）コンテキストとして指定されたコンテキストの 1 つを使用します。

管理コンテキストは、ユーザが管理コンテキストにログインすると、システム管理者の権限でシステムとその他のすべてのコンテキストにアクセスできるという点を除き、他のコンテキストとまったく同じです。

（注）マルチコンテキスト モードがサポートするのは、スタティック ルーティングだけです。

Firewall Services Module を使用するためのスイッチの設定

この章では、FWSM と組み合わせて使用できるように、Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータ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、インターフェイスへの 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。

この章で説明する内容は、次のとおりです。

- スイッチの概要（p.2-2）
- モジュールの搭載確認（p.2-3）
- Firewall Services Module への VLAN 割り当て（p.2-4）
- MSFC への SVI の追加（p.2-7）
- FWSM の内部インターフェイスのカスタマイズ（p.2-12）
- フェールオーバーを使用するためのスイッチの設定（p.2-13）
- Firewall Services Module ブート パーティションの管理（p.2-14）

スイッチの概要

FWSM は、Cisco 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータに搭載できます。どちらのシリーズもコンフィギュレーションは同じです。このマニュアルでは両方のシリーズをまとめて「スイッチ」と呼びます。スイッチには、スイッチ（スーパーバイザ エンジン）とともにルータ（Multilayer Switch Feature Card［MSFC; マルチレイヤ スイッチ フィーチャ カード］）が搭載されています。

スイッチは 2 種類のソフトウェア モードをサポートします。

- スイッチのスーパーバイザ エンジンおよび内蔵 MSFC ルータの両方で、Cisco IOS ソフトウェアを使用
- スーパーバイザ エンジンで Catalyst Operating System（OS; オペレーティング システム）ソフトウェア、MSFC 上で Cisco IOS ソフトウェアを使用

このマニュアルでは、両方のモードについて説明します。

FWSM は独自の OS で動作します。

MSFC の詳細については、「MSFC の使用方法」（p.1-4）を参照してください。

（注） スイッチでは、各 FWSM で SPAN リフレクタ機能がイネーブルです。この機能によって、FWSM 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が必要な他のトラフィック）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 FWSM を認識してオンラインにしているかどうかを確認するには、OS に応じてモジュール情報を表示します。

- Cisco IOS ソフトウェア

  Router> **show module** [*mod-num* | **all**]

  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.
--- ----- ------------------------------------- ------------------ -----------
  1    2  Catalyst 6000 supervisor 2 (Active)   WS-X6K-SUP2-2GE    SAD0444099Y
  2   48  48 port 10/100 mb RJ-45 ethernet      WS-X6248-RJ-45     SAD03475619
  3    2  Intrusion Detection System            WS-X6381-IDS       SAD04250KV5
  4    6  Firewall Module                       WS-SVC-FWM-1       SAD062302U4
```

- Catalyst OS ソフトウェア

  Console> **show module** [*mod-num*]

  次に、**show module** コマンドの出力例を示します。

```
Console> show module
Mod Slot Ports Module-Type                Model                Sub Status
--- ---- ----- ------------------------- ------------------- --- ------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
4   4    2     Intrusion Detection Syste WS-X6381-IDS        no  ok
5   5    6     Firewall Module           WS-SVC-FWM-1        no  ok
6   6    8     1000BaseX Ethernet        WS-X6408-GBIC       no  ok
```

(注) **show module** コマンドの出力に FWSM の 6 ポートが示されています。これは、EtherChannel としてひとまとめにされた内部ポートです。詳細については、「FWSM の内部インターフェイスのカスタマイズ」（p.2-12）を参照してください。

Firewall Services Module への VLAN 割り当て

ここでは、FWSM に VLAN を割り当てる方法について説明します。FWSM に外部物理インターフェイスは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。FWSM への VLAN 割り当ては、スイッチ ポートへの VLAN 割り当てと同様です。FWSM には Switch Fabric Module（SFM; スイッチ ファブリック モジュール）（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あります。

（注）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。

ここでは、次の内容について説明します。

- VLAN の注意事項（p.2-4）
- Cisco IOS ソフトウェアで FWSM に VLAN を割り当てる場合（p.2-4）
- Catalyst OS ソフトウェアで FWSM に VLAN を割り当てる場合（p.2-6）

VLAN の注意事項

FWSM で VLAN を使用する際の注意事項は、次のとおりです。

- FWSM でプライベート VLAN を使用できます。FWSM にプライマリ VLAN を割り当てると、FWSM は自動的にセカンダリ VLAN トラフィックを処理します。
- 予約済み VLAN を使用することはできません。
- VLAN 1 を使用することはできません。
- 同一スイッチ シャーシ内で FWSM 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。
- FWSM 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 FWSM に送信されます。
- MSFC に割り当てる前に、FWSM に VLAN を割り当てます。

  この条件を満たしていない VLAN は、FWSM 上で割り当てる VLAN の範囲から破棄されます。詳細については、「MSFC への SVI の追加」（p.2-7）を参照してください。

Cisco IOS ソフトウェアで FWSM に VLAN を割り当てる場合

Cisco IOS ソフトウェアでは、1 つまたは複数のファイアウォール VLAN グループを作成し、FWSM にグループを割り当てます。たとえば、すべての VLAN を 1 つのグループに割り当てる、内部グループと外部グループを作成する、またはカスタマーごとにグループを 1 つずつ作成するといったことが可能です。

1 つの VLAN を複数のファイアウォール グループに割り当てることはできませんが、複数のファイアウォール グループを 1 つの FWSM に割り当てたり、1 つのファイアウォール グループを複数の FWSM に割り当てることはできます。複数の FWSM に割り当てる VLAN は、各 FWSM に固有な VLAN とは別個のグループに配置できます。

VLAN を FWSM に 割り当てる手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、ファイアウォール グループに VLAN を割り当てます。

```
Router(config)# firewall vlan-group firewall_group vlan_range
```

vlan_range には、次のどちらかの形式で、1 つまたは複数の VLAN（1 ～ 1000 および 1025 ～ 4094）を指定できます。

- 個別の番号（*n*）
- 範囲（*n-x*）

番号または範囲はカンマで区切ります。番号の入力例を示します。

```
5,7-10,13,45-100
```

（注）　ルーテッド ポートと WAN ポートは内部 VLAN を使用するので、1020 ～ 1100 の範囲に含まれる番号は、すでに使用されている可能性があります。

ステップ 2　次のコマンドを入力して、FWSM にファイアウォール グループを割り当てます。

```
Router(config)# firewall module module_number vlan-group firewall_group
```

firewall_group は、1 つまたは複数のグループ番号です。

- 個別の番号（*n*）
- 範囲（*n-x*）

番号または範囲はカンマで区切ります。番号の入力例を示します。

```
5,7-10
```

次に、3 つのファイアウォール VLAN グループ（各 FWSM 用のグループ、および両方の FWSM 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 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall vlan-group 52 100
Router(config)# firewall module 5 vlan-group 50,52
Router(config)# firewall module 8 vlan-group 51,52
```

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、すべての VLAN グループを示す **show firewall module** 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
```

Catalyst OS ソフトウェアで FWSM に VLAN を割り当てる場合

Catalyst OS ソフトウェアで、FWSM に VLAN リストを割り当てます。必要であれば、複数の FWSM に同じ VLAN を割り当ててもかまいません。

次のコマンドを入力して、FWSM に VLAN を割り当てます。

```
Console> (enable) set vlan vlan_list firewall-vlan mod_num
```

vlan_list には、次のいずれかの形式で、1 つまたは複数の VLAN（2 ～ 1000 および 1025 ～ 4094）を指定できます。

- 個別の番号（*n*）
- 範囲（*n-x*）

番号または範囲はカンマで区切ります。次に例を示します。

```
5,7-10,13,45-100
```

（注） ルーテッド ポートと WAN ポートは内部 VLAN を使用するので、1020 ～ 1100 の範囲に含まれる番号は、すでに使用されている可能性があります。

次に、一般的な設定例を示します。

```
Console> (enable) set vlan 55-57,100 firewall-vlan 5
Console> (enable) set vlan 70-85,100 firewall-vlan 8
```

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

```
Console> show vlan firewall-vlan 5
Secured vlans by firewall module 5
55-57, 100
```

MSFC への SVI の追加

MSFC 上で定義された VLAN を Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）といいます。FWSM に SVI 用の VLAN を割り当てると（「Firewall Services Module への VLAN 割り当て」[p.2-4] を参照）、MSFC は FWSM と他のレイヤ 3 VLAN 間でルーティングを行います。

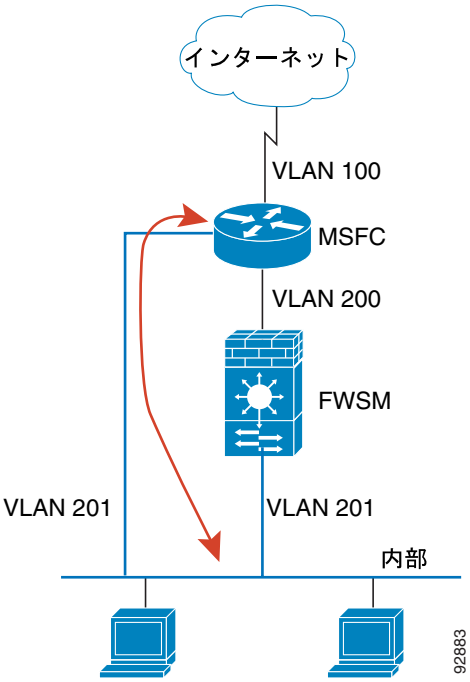
ここでは、次の内容について説明します。

- SVI の概要（p.2-7）
- SVI の設定（スーパーバイザ エンジンで Cisco IOS ソフトウェアを実行している場合）（p.2-9）
- SVI の設定（スーパーバイザ エンジンで Catalyst OS ソフトウェアを実行している場合）（p.2-10）

SVI の概要

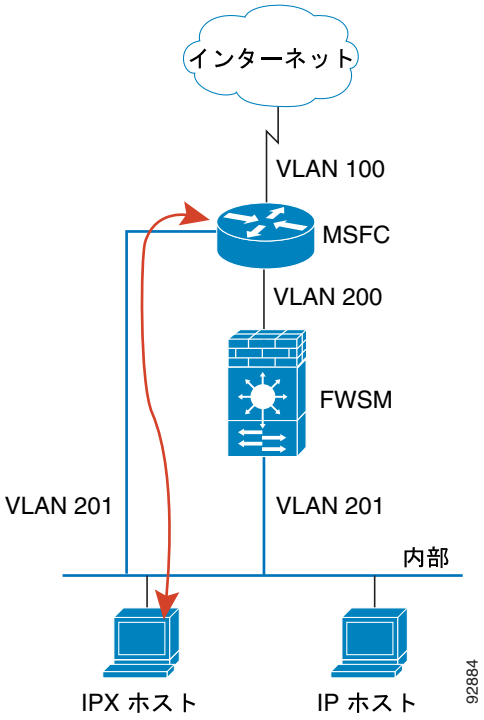
セキュリティ上の理由から、デフォルトでは MSFC と FWSM 間に存在できる SVI は 1 つだけです。たとえば、誤って複数の SVI を指定してシステムを設定した場合、MSFC に内部 VLAN と外部 VLAN の両方を割り当てることによって、トラフィックが偶発的に FWSM をバイパスしてしまう可能性があります（図 2-1 を参照）。

図 2-1　誤設定による複数の SVI



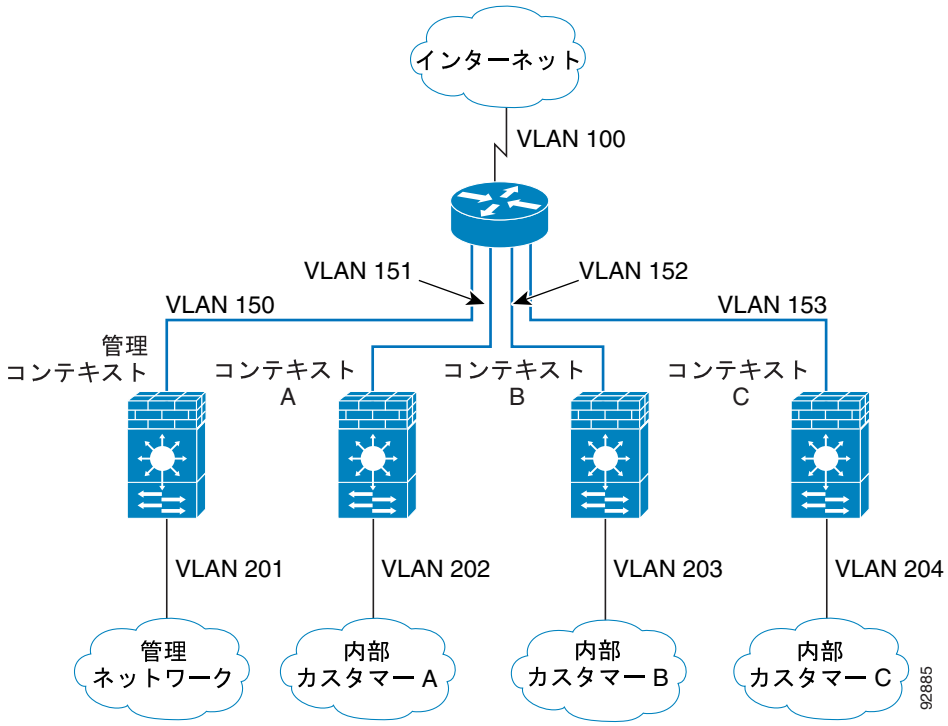
ただし、ネットワークの状況によっては、FWSM をバイパスしなければならないこともあります。図 2-2 に、IP ホストと同じイーサネット セグメント上に IPX ホストが配置されている例を示します。ルーテッド ファイアウォール モードの FWSM が処理できるのは IP トラフィックだけであり、IPX などの他のトラフィックは廃棄されるので（透過ファイアウォール モードでは任意で IP 以外のトラフィックの通過が可能）、IPX トラフィックは FWSM をバイパスさせる必要があります。この場合、必ず、VLAN 201 を通過できるのが IPX トラフィックに限定されるアクセス リストを使用して MSFC を設定してください。

図 2-2　IPX 対応の複数の SVI



透過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（図 2-3 を参照）。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。

図 2-3　マルチコンテキスト モードでの複数の SVI



SVI の設定（スーパーバイザ エンジンで Cisco IOS ソフトウェアを実行している場合）

スーパーバイザ エンジンで Cisco IOS ソフトウェアを実行している場合、次の手順で MSFC に SVI を追加します。

ステップ 1　（任意）次のコマンドを入力して、FWSM に複数の SVI を追加できるようにします。

```
Router(config)# firewall multiple-vlan-interfaces
```

ステップ 2　次のコマンドを入力して、MSFC に VLAN インターフェイスを追加します。

```
Router(config)# interface vlan vlan_number
```

ステップ 3　次のコマンドを入力して、MSFC 上でこのインターフェイスに対応する IP アドレスを設定します。

```
Router(config-if)# ip address address mask
```

ステップ 4　次のコマンドを入力して、インターフェイスをイネーブルにします。

```
Router(config-if)# no shutdown
```

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#
```

次に、**show interface** 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 55.1.1.1/24
  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
```

SVI の設定（スーパーバイザ エンジンで Catalyst OS ソフトウェアを実行している場合）

スーパーバイザ エンジンで Catalyst OS ソフトウェアを実行している場合、次の手順で MSFC に SVI を追加します。

ステップ 1　（任意）次のコマンドを入力して、FWSM に複数の SVI を追加できるようにします。

```
Console> (enable) set firewall multiple-vlan-interfaces enable
```

この設定をディセーブルにするには、次のコマンドを入力します。

```
Console> (enable) set firewall multiple-vlan-interfaces disable
```

ステップ 2　次のコマンドのいずれかを入力して、MSFC インターフェイスにアクセスします。

```
Console> (enable) switch console
```

または

```
Console> (enable) session {15 | 16}
```

Telnet または Secure Shell（SSH; セキュア シェル）を使用してスイッチにアクセスしている場合は、**session** コマンドを使用する必要があります。

ステップ 3　次のコマンドを入力して、MSFC 上でイネーブル モードを開始し、さらにコンフィギュレーション モードを開始します。

```
Router> enable
Router# configure terminal
```

ステップ 4　次のコマンドを入力して、MSFC に VLAN インターフェイスを追加します。

```
Router(config)# interface vlan vlan_number
```

ステップ 5　次のコマンドを入力して、MSFC 上でこのインターフェイスに対応する IP アドレスを設定します。

```
Router(config-if)# ip address address mask
```

ステップ 6　次のコマンドを入力して、インターフェイスをイネーブルにします。

```
Router(config-if)# no shutdown
```

ステップ 7　次のコマンドを入力して、イネーブル EXEC モードに戻ります。

```
Router(config-if)# end
```

ステップ 8　**Ctrl-C** を 3 回入力して、スイッチの CLI に戻ります。

次に、一般的な設定例を示します。

```
Console> (enable) set vlan 55-57,70-85 firewall-vlan 8
Console> (enable) set firewall multiple-vlan-interfaces enable
Console> (enable) switch console
Router> enable
Password: ******
Router# configure terminal
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# ^C^C^C
Console> (enable)
```

次に、MSFC プロンプトに入力する **show interface** 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 55.1.1.1/24
  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
```

FWSM の内部インターフェイスのカスタマイズ

FWSM とスイッチ間の接続は 6 GB の 802.1Q トランキング EtherChannel です。この EtherChannel は、FWSM を搭載した時点で自動的に作成されます。FWSM 側では、2 つの NP のそれぞれが 3 つのギガビット イーサネット インターフェイスに接続し、これらのインターフェイスが EtherChannel を形成します。スイッチはセッション情報に基づき、分散アルゴリズムに従って EtherChannel 内のインターフェイスにトラフィックを分散させます。負荷分散はパケット単位ではなく、フロー単位で行われます。アルゴリズムがインターフェイス間、したがって 2 つの NP 間でトラフィックを均等に割り当てない場合もあります。恒常的な不均衡は、FWSM の処理能力がフル活用されないだけではなく、複数のコンテキストにリソース管理を適用したときに予想外の動作を引き起こす可能性があります（詳細については、「クラスの設定」[p.4-16] を参照）。

- Cisco IOS ソフトウェア

  ```
  Router(config)# port-channel load-balance {dst-ip | dst-mac | dst-port | src-dst-ip
  | src-dst-mac | src-dst-port | src-ip | src-mac | src-port}
  ```

  デフォルトは **src-dst-ip** です。

- Catalyst OS ソフトウェア

  ```
  Console> (enable) set port channel all distribution {ip | mac | session |
  ip-vlan-session} [source | destination | both]
  ```

  デフォルトは **ip both** です。

フェールオーバーを使用するためのスイッチの設定

フェールオーバー対応としてスイッチを設定する場合は、次の項を参照してください。

- セカンダリ Firewall Services Module への VLAN 割り当て（p.2-13）
- 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.2-13）
- 透過ファイアウォール モードとの両立（p.2-13）

セカンダリ Firewall Services Module への VLAN 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なければならないので、スイッチ上の両方の FWSM に同じ VLAN を割り当てる必要があります。「Firewall Services Module への VLAN 割り当て」（p.2-4）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（「シャーシ内およびシャーシ間のモジュール配置」[p.13-4] を参照）、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 プライオリティで処理されるように、トランクで Quality of Service（QoS; サービス品質）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。

透過ファイアウォール モードとの両立

透過モードでフェールオーバーを使用したときにループが発生しないように、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）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。透過ファイアウォール モードでのスイッチのサポートの詳細については、「スイッチ ハードウェアおよびソフトウェアの互換性」（p.A-2）を参照してください。

Firewall Services Module ブート パーティションの管理

ここでは、スイッチから FWSM をリセットする方法とフラッシュ メモリ カード上のブート パーティションを管理する方法について説明します。ここでは、次の内容について説明します。

- フラッシュ メモリの概要（p.2-14）
- デフォルト ブート パーティションの設定（p.2-14）
- FWSM のリセットまたは特定のパーティションからの起動（p.2-15）

フラッシュ メモリの概要

FWSM には、OS、コンフィギュレーション、およびその他のデータを保管する 128 MB のフラッシュ メモリ カードがあります。フラッシュ メモリにはパーティションが 6 つあります。Cisco IOS および Catalyst OS ソフトウェアのコマンドでは、**cf:***n* で指定します。

- メンテナンス パーティション（**cf:1**）— メンテナンス ソフトウェアが格納されています。メンテナンス ソフトウェアを使用して、アプリケーション パーティションの起動ができない場合に、アプリケーション イメージをアップグレードまたはインストールしたり、アプリケーション イメージのパスワードをリセットしたり、クラッシュ ダンプ情報を表示したりします。
- ネットワーク コンフィギュレーション パーティション（**cf:2**）— メンテナンス ソフトウェアのネットワーク コンフィギュレーションが格納されています。FWSM が TFTP サーバにアクセスしてアプリケーション ソフトウェア イメージをダウンロードできるように、メンテナンス ソフトウェアには IP の設定値が必要です。
- クラッシュ ダンプ パーティション（**cf:3**）— クラッシュ ダンプ情報が保管されます。
- アプリケーション パーティション（**cf:4** および **cf:5**）— アプリケーション ソフトウェア イメージ、システム コンフィギュレーション、および ASDM を保管します。デフォルトで、イメージは **cf:4** にインストールされます。**cf:5** はテスト パーティションとして使用できます。たとえば、ソフトウェアをアップグレードする場合、新しいソフトウェアを **cf:5** にインストールし、問題が発生した場合のバックアップとして旧ソフトウェアを維持することもできます。各パーティションには独自のスタートアップ コンフィギュレーションが設定されています。
- セキュリティ コンテキスト パーティション（**cf:6**）— このパーティション専用として 64 MB が確保されます。ここにはセキュリティ コンテキスト コンフィギュレーション（必要に応じて）とナビゲーション可能なファイル システムの RSA キーを保管します。他のパーティションには、ファイルのリスト表示などの一般的な作業を実行できるファイル システムはありません。**copy** コマンドの使用時には、このパーティションを**ディスク**といいます。

デフォルト ブート パーティションの設定

FWSM はデフォルトで、**cf:4** アプリケーション パーティションから起動します。**cf:5** アプリケーション パーティションからの起動または **cf:1** メンテナンス パーティションでの起動を選択することもできます。デフォルト ブート パーティションを変更するには、OS に応じたコマンドを入力します。

- Cisco IOS ソフトウェア

  ```
  Router(config)# boot device module mod_num cf:n
  ```

  n は 1（メンテナンス）、4（アプリケーション）、または 5（アプリケーション）です。
- Catalyst OS ソフトウェア

  ```
  Console> (enable) set boot device cf:n mod_num
  ```

  n は 1（メンテナンス）、4（アプリケーション）、または 5（アプリケーション）です。

現在のブート パーティションを表示するには、OS に応じたコマンドを入力します。

- Cisco IOS ソフトウェア

  ```
  Router# show boot device [mod_num]
  ```

  次に例を示します。

  ```
  Router# show boot device
  [mod:1 ]:
  [mod:2 ]:
  [mod:3 ]:
  [mod:4 ]: cf:4
  [mod:5 ]: cf:4
  [mod:6 ]:
  [mod:7 ]: cf:4
  [mod:8 ]:
  [mod:9 ]:
  ```

- Catalyst OS ソフトウェア

  ```
  Console> (enable) show boot device mod_num
  ```

  次に例を示します。

  ```
  Console> (enable) show boot device 6
  Device BOOT variable = cf:5
  ```

FWSM のリセットまたは特定のパーティションからの起動

ここでは、FWSM をリセットする方法または特定のパーティションから起動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 FWSM にアクセスできない場合は、FWSM のリセットが必要です。メンテナンス パーティションにアクセスしなければならない場合、またはバックアップのアプリケーション パーティションに保管されている別のソフトウェア イメージから起動しなければならない場合は、デフォルト以外のブート パーティションからの起動が必要になります。メンテナンス パーティションは、トラブルシューティング時に役立ちます。

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。

Cisco IOS ソフトウェアの場合、FWSM のリセット時に、フルメモリ テストの実行を選択することもできます。FWSM の初回起動時には、部分的なメモリ テストが実行されるだけです。フルメモリ テストには、6 分ほどかかります。

FWSM をリセットする場合は、使用する OS に応じた項を参照してください。

- Cisco IOS ソフトウェアで FWSM をリセットする場合（p.2-16）
- Catalyst OS ソフトウェアで FWSM をリセットする場合（p.2-16）

（注） FWSM にログインするときに FWSM をリロードする場合は、**reload** コマンドまたは **reboot** コマンドを入力します。これらのコマンドで、デフォルト以外のブート パーティションから起動することはできません。

Cisco IOS ソフトウェアで FWSM をリセットする場合

FWSM をリセットするには、次のコマンドを入力します。

```
Router# hw-module module mod_num reset [cf:n] [mem-test-full]
```

引数 **cf:***n* はパーティションで、1（メンテナンス）、4（アプリケーション）、または 5（アプリケーション）のいずれかです。パーティションを指定しなかった場合、デフォルトのパーティションが使用されます（通常は **cf:4**）。

mem-test-full オプションを指定すると、フルメモリ テストが実行されます。所要時間は約 6 分です。

次に、スロット 9 に搭載された FWSM をリセットする例を示します。デフォルトのブート パーティションが使用されます。

```
Router# hw-mod 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 ...
```

Catalyst OS ソフトウェアで FWSM をリセットする場合

次のコマンドを入力して、スイッチの CLI から FWSM をリセットします。

```
Console> (enable) reset mod_num [cf:n]
```

cf:*n* はパーティションで、1（メンテナンス）、4（アプリケーション）、または 5（アプリケーション）のいずれかです。パーティションを指定しなかった場合、デフォルトのパーティションが使用されます（通常は cf:4）。

Firewall Services Module の接続および設定の管理

この章では、コマンドライン インターフェイスへのアクセス方法および設定の管理方法について説明します。この章で説明する内容は、次のとおりです。

- Firewall Services Module との接続（p.3-2）
- 設定の管理（p.3-4）

Firewall Services Module との接続

ここでは、スイッチのコマンドラインから FWSM に接続または「セッション」を開始する方法について説明します。FWSM からログアウトしてスイッチの CLI にアクセスする方法についても説明します。ここでは、次の内容について説明します。

- FWSM へのログイン（p.3-2）
- FWSM からのログアウト（p.3-3）

FWSM へのログイン

FWSM には外部コンソール ポートがないので、FWSM とのセッションを開始して初期設定を行う必要があります。FWSM 本体のインターフェイスと IP アドレスを設定してからであれば、FWSM のインターフェイスを介して FWSM の CLI にリモート アクセスできます。詳細については、第 21 章「管理アクセスの設定」を参照してください。

ユーザ認証に関する他の設定がない場合、ログイン方式はデフォルト ユーザとしてのログインです。

1. ログイン パスワードを使用してユーザ EXEC モードにアクセスします。
2. コンフィギュレーション コマンドにアクセスするには、イネーブル EXEC モードを開始する必要があります。それには、第 2 パスワードが必要です。
3. イネーブル EXEC モードからグローバル コンフィギュレーション モードにアクセスできます。この場合、パスワードは不要です。

注意　FWSM への管理アクセスの実行は、パフォーマンスが低下する原因になります。高いネットワーク パフォーマンスを保持する必要がある場合には、FWSM にアクセスしないことを推奨します。

スイッチから FWSM とのセッションを開始してログインし、イネーブル モードにアクセスし、コンフィギュレーション モードを開始する手順は次のとおりです。

ステップ 1　スイッチの OS（オペレーティング システム）に応じたコマンドを使用して、スイッチから FWSM とのセッションを開始します。

- Cisco IOS ソフトウェア

```
Router# session slot number processor 1
```

- Catalyst OS ソフトウェア

```
Console> (enable) session module_number
```

マルチコンテキスト モードの場合、FWSM とのセッションを開始すると、システム コンフィギュレーションにアクセスすることになります。詳細については、第 4 章「セキュリティ コンテキストの設定」を参照してください。

ステップ 2　次のプロンプトにログイン パスワードを入力して、FWSM にログインします。

```
hostname passwd:
```

デフォルトのパスワードは、**cisco** です。

パスワードの変更については、「パスワードの変更」（p.7-2）を参照してください。

ステップ 3　次のコマンドを入力して、イネーブル EXEC モードにアクセスします。

```
hostname> enable
```

このコマンドによって、最上位の権限レベルにアクセスできます。

次のプロンプトが表示されます。

```
Password:
```

ステップ 4　プロンプトにイネーブル パスワードを入力します。

パスワードはデフォルトでブランクです。**Enter** キーを押すと、処理を継続します。イネーブル パスワードの変更については、「パスワードの変更」（p.7-2）を参照してください。

プロンプトが次のように変わります。

```
hostname#
```

イネーブル モードを終了する場合は、**disable** を入力します。**exit** または **quit** を入力して現在のアクセス モード（イネーブル EXEC モード、グローバル コンフィギュレーション モードなど）を終了することもできます。

ステップ 5　次のコマンドを入力して、コンフィギュレーション モードにアクセスします。

```
hostname# configure terminal
```

プロンプトが次のように変わります。

```
hostname(config)#
```

FWSM からのログアウト

FWSM 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、次のコマンドを入力します。

```
hostname# exit

Logoff

[Connection to 127.0.0.31 closed by foreign host]
Router#
```

コンフィギュレーション モードを使用している場合、**exit** コマンドを複数回入力しなければならないことがあります。

設定の管理

ここでは、設定の管理方法について説明します。FWSM は、スタートアップ コンフィギュレーションというテキスト ファイルから設定をロードします。

コマンドを入力したときに変更されるのは、メモリ内の実行コンフィギュレーションだけです。再起動後も変更を維持するには、スタートアップ コンフィギュレーションに実行コンフィギュレーションを手動で保存する必要があります。

この項の情報は、シングル セキュリティ コンテキストとマルチセキュリティ コンテキストの両方に当てはまります。例外については、そのつど明記します。コンテキストの詳細については、第 4 章「セキュリティ コンテキストの設定」を参照してください。

ここでは、次の内容について説明します。

- 変更した設定の保存（p.3-4）
- スタートアップ 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へのコピー（p.3-6）
- 設定の表示（p.3-6）
- 設定内の設定値の消去および削除（p.3-6）
- テキスト コンフィギュレーション ファイルをオフラインで作成する方法（p.3-7）

変更した設定の保存

ここでは、設定の保存方法について説明します。内容は次のとおりです。

- 変更した設定の保存（シングルコンテキスト モードの場合）（p.3-4）
- 変更した設定の保存（マルチコンテキスト モードの場合）（p.3-4）

変更した設定の保存（シングルコンテキスト モードの場合）

スタートアップ コンフィギュレーションに実行コンフィギュレーションを保存するには、次のコマンドを入力します。

```
hostname# write memory
```

（注）　**copy running-config startup-config** コマンドは **write memory** コマンドと同じです。

変更した設定の保存（マルチコンテキスト モードの場合）

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別々に保存することも、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。次のコマンドを参照してください。

- システムまたはコンテキスト コンフィギュレーションを保存するには、システムまたはコンテキスト内に次のコマンドを入力します。

  ```
  hostname# write memory
  ```

（注）　**copy running-config startup-config** コマンドは **write memory** コマンドと同じです。

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保管できます。その場合、FWSM はコンテキストの URL で指定されたサーバに設定を戻します。ただし、HTTP または HTTPS URL の場合は、サーバに設定を保存できません。

- すべてのコンテキスト コンフィギュレーションおよびシステム コンフィギュレーションを同時に保存するには、システム実行スペースに次のコマンドを入力します。

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

/noconfirm キーワードを入力しないと、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、FWSM はシステム コンフィギュレーションおよび各コンテキストを保存します。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を外部サーバに保管できます。その場合、FWSM はコンテキストの URL で指定されたサーバに設定を戻します。ただし、HTTP または HTTPS URL の場合は、サーバに設定を保存できません。

FWSM が各コンテキストを保存すると、次のメッセージが表示されます。

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

エラーによりコンテキストが保存されないことがあります。次のエラー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を保存できない場合、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を保存できない場合、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コンテキストを保存できない場合、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、他のユーザがすでに設定を保存している場合またはコンテキスト削除プロセスを実行している場合だけです。

— 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（HTTP サーバ上にある場合など）であるためにコンテキストを保存できない場合、他のすべてのメッセージの最後に次のメッセージ レポートが印刷されます。

```
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 メモリの不良セクタが原因でコンテキストを保存できない場合、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
```

スタートアップ 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へのコピー

次のいずれかのオプションを使用して、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します。

- スタートアップ　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結合するには、次のコマンドを入力します。

  ```
  hostname(config)# copy startup-config running-config
  ```

- 実行コンフィギュレーションを廃棄してスタートアップ　コンフィギュレーションをロードするには、次のコマンドを入力して、FWSM を再起動します。

  ```
  hostname# reload
  ```

  次のコマンドを使用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、再起動せずに実行コンフィギュレーションを廃棄することもできます。

  ```
  hostname(config)# clear configure all
  hostname(config)# copy startup-config running-config
  ```

設定の表示

次のコマンドを使用すると、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できます。

- 実行コンフィギュレーションを表示するには、次のコマンドを入力します。

  ```
  hostname# show running-config
  ```

- 特定コマンドの実行コンフィギュレーションを表示するには、次のコマンドを入力します。

  ```
  hostname# show running-config command
  ```

- 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、次のコマンドを入力します。

  ```
  hostname# show startup-config
  ```

設定内の設定値の消去および削除

設定値を削除するには、次のいずれかのコマンドを入力します。

- 指定したコマンドのすべての設定を消去するには、次のコマンドを入力します。

  ```
  hostname(config)# clear configure configurationcommand [level2configurationcommand]
  ```

  このコマンドによって、指定したコンフィギュレーション コマンドの現在のすべての設定が消去されます。特定バージョンのコマンドの設定のみを消去する場合、*level2configurationcommand* の値を入力できます。

  たとえば、すべての **aaa** コマンドの設定を消去するには、次のコマンドを入力します。

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

  aaa authentication コマンドの設定だけを消去するには、次のコマンドを入力します。

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

- 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するには、次のコマンドを入力します。

  ```
  hostname(config)# no configurationcommand [level2configurationcommand] qualifier
  ```

  この場合、***no*** コマンドを使用して、*qualifier* で指定した特定の設定を削除します。

たとえば、特定の **nat** コマンドを削除するには、次のように、固有のものとして識別できるだけのコマンドを入力します。

```
hostname(config)# no nat (inside) 1
```

- スタートアップ コンフィギュレーションを削除するには、次のコマンドを入力します。

```
hostname(config)# write erase
```

- 実行コンフィギュレーションを削除するには、次のコマンドを入力します。

```
hostname(config)# clear configure all
```

(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が削除されて実行が中止されます。

テキスト コンフィギュレーション ファイルをオフラインで作成する方法

このマニュアルでは、CLI を使用して FWSM を設定する方法について説明しています。この場合、コマンドを保存すると、変更内容がテキスト ファイルに書き込まれます。ただし、CLI を使用する代わりに、テキスト ファイルを自分の PC で直接編集し、コンフィギュレーション モードのコマンドライン プロンプトに、設定全体をペーストしたり、1 行ずつペーストしたりすることもできます。FWSM 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することもできます。FWSM にコンフィギュレーション ファイルをダウンロードする場合の詳細については、第 22 章「ソフトウェア、ライセンス、および設定の管理」を参照してください。

このマニュアルに記載されているコマンドは、ほとんどの場合、先頭に CLI プロンプトがあります。次に、「hostname(config)#」プロンプトの例を示します。

```
hostname(config)# context a
```

テキスト コンフィギュレーション ファイルでは、コマンド入力が要求されないので、プロンプトは次のように省略されます。

```
context a
```

ファイルのフォーマットの詳細については、付録 C「CLI の使用」を参照してください。

セキュリティ コンテキストの設定

この章では、複数のセキュリティ コンテキストを設定する方法について説明します。内容は次のとおりです。

- セキュリティ コンテキストの概要（p.4-2）
- マルチコンテキスト モードのイネーブル化またはディセーブル化（p.4-11）
- リソース管理の設定（p.4-13）
- メモリ パーティションの設定（p.4-18）
- セキュリティ コンテキストの設定（p.4-20）
- コンテキストとシステム実行スペース間の切り替え（p.4-24）
- セキュリティ コンテキストの管理（p.4-25）

セキュリティ コンテキストの概要

1 つの FWSM をセキュリティ コンテキストと呼ばれる複数の仮想デバイスに分割できます。各コンテキストには独自のセキュリティ ポリシー、インターフェイス、および管理者が与えられます。マルチコンテキストは、スタンドアロンのデバイスを複数使用することと同様です。ルーティング テーブル、ファイアウォール機能、管理などマルチコンテキスト モードでサポートされている機能は数多くあります。ダイナミック ルーティング プロトコルなど一部の機能はサポートされていません。

マルチコンテキスト モードの場合、FWSM にはコンテキストごとに、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ぼすべてのオプションのコンフィギュレーションが含まれます。システム管理者は、システム コンフィギュレーション（シングルモード 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に相当します）でコンテキストを設定することによって、コンテキストを追加および管理します。システム コンフィギュレーションには FWSM の基本設定が含まれます。システム コンフィギュレーションには、システムそのもののネットワーク インターフェイスまたはネットワーク設定値は含みません。システムがネットワーク リソースにアクセスする必要がある場合に（サーバからコンテキストをダウンロードする場合など）、管理（admin）コンテキストとして指定されたコンテキストの 1 つを使用します。

管理コンテキストは、ユーザが管理コンテキストにログインすると、システム管理者の権限でシステムとその他のすべてのコンテキストにアクセスできるという点を除き、他のコンテキストとまったく同じです。

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。内容は次のとおりです。

- セキュリティ コンテキストの一般的な使用方法（p.4-2）
- サポートされていない機能（p.4-2）
- コンテキスト コンフィギュレーション ファイル（p.4-3）
- FWSM によるパケットの分類方法（p.4-3）
- コンテキスト間でのインターフェイスの共有（p.4-7）
- マルチコンテキスト モードの FWSM へのログイン（p.4-10）

セキュリティ コンテキストの一般的な使用方法

複数のセキュリティ コンテキストを使用する状況として考えられるものは、次のとおりです。

- サービス プロバイダーが多数のカスタマーにセキュリティ サービスを販売する場合。FWSM 上でマルチセキュリティ コンテキストを使用できるようにすると、すべてのカスタマー トラフィックが切り離され、セキュアで設定の容易な、コスト効率が高く、しかも場所を取らないソリューションを実現できます。
- 大企業または大学構内で、各部門を完全に切り離しておく必要がある場合
- 企業で、部門ごとにセキュリティ ポリシーを区別して提供する場合
- 複数のファイアウォールが必要なネットワークを使用する場合

サポートされていない機能

マルチコンテキスト モードでは、次の機能はサポートしません。

- ダイナミック ルーティング プロトコル

  セキュリティ コンテキストがサポートするのは、スタティック ルートだけです。マルチコンテキスト モードで OSPF または Routing Information Protocol（RIP）をイネーブルにすることはできません。
- マルチキャスト

コンテキスト コンフィギュレーション ファイル

コンテキストごとに、セキュリティ ポリシー、インターフェイス、およびサポートされている機能についてスタンドアロン デバイスで設定できるすべてのオプションを指定した、専用のコンフィギュレーション ファイルを使用します。コンテキスト コンフィギュレーションは内部フラッシュ メモリに保存できます。または TFTP、FTP、HTTP（S）サーバからダウンロードできます。

個々のセキュリティ コンテキストのほかに、FWSM にはコンテキストのリストを含め、FWSM の基本設定を指定したシステム コンフィギュレーションも組み込まれます。シングルモード コンフィギュレーションと同様、この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として常時設定されます。

システム コンフィギュレーションには、システムそのもののネットワーク インターフェイスまたはネットワーク設定値は含みません。システムがネットワーク リソースにアクセスする必要がある場合に（サーバからコンテキストをダウンロードする場合など）、管理（admin）コンテキストとして指定されたコンテキストの 1 つを使用します。システム コンフィギュレーションには、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 インターフェイスは含みません。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切り替える場合、内部フラッシュ メモリ上に、admin.cfg というファイルとして管理コンテキストが自動的に作成されます。このコンテキストの名前は「admin」です。admin.cfg を管理コンテキストとして使用しない場合は、管理コンテキストを変更できます。

FWSM によるパケットの分類方法

FWSM がパケットの送信先コンテキストを判別できるように、FWSM に入ってくるパケットごとに分類が必要です。分類機能では次のルールを使用して、パケットをコンテキストに割り当てます。

1. 入力側インターフェイスに対応付けられるコンテキストが 1 つのみの場合、FWSM はパケットをそのコンテキストに分類します。

   透過ファイアウォール モードではコンテキスト固有のインターフェイスが必要であるため、常にこの方法でパケットを分類します。

2. 入力側インターフェイスに対応付けられるコンテキストが複数ある場合、FWSM は宛先アドレスを次のいずれかのコンテキスト コンフィギュレーションと照合することによって、パケットをコンテキストに分類します。

   a. インターフェイス IP アドレス（**ip address** コマンド）

      分類機能は、管理トラフィックなどインターフェイス宛てのトラフィックのインターフェイス IP アドレスを調べます。

   b. スタティック Network Address Translation（NAT; ネットワーク アドレス変換）ステートメントのマップ アドレス（**static** コマンド）

      分類機能は、マップ インターフェイスがパケットの入力側インターフェイスと一致する **static** コマンドのみを調べます。

   c. アクティブなダイナミック アドレス変換のマップ アドレス（**global** コマンドによって設定）

      分類機能は、入力側インターフェイスの変換テーブルのマップ IP アドレスを調べます。

（注） 分類機能は、分類目的では NAT 除外コンフィギュレーションを使用しません。NAT 除外はマップ インターフェイスを識別しないためです。

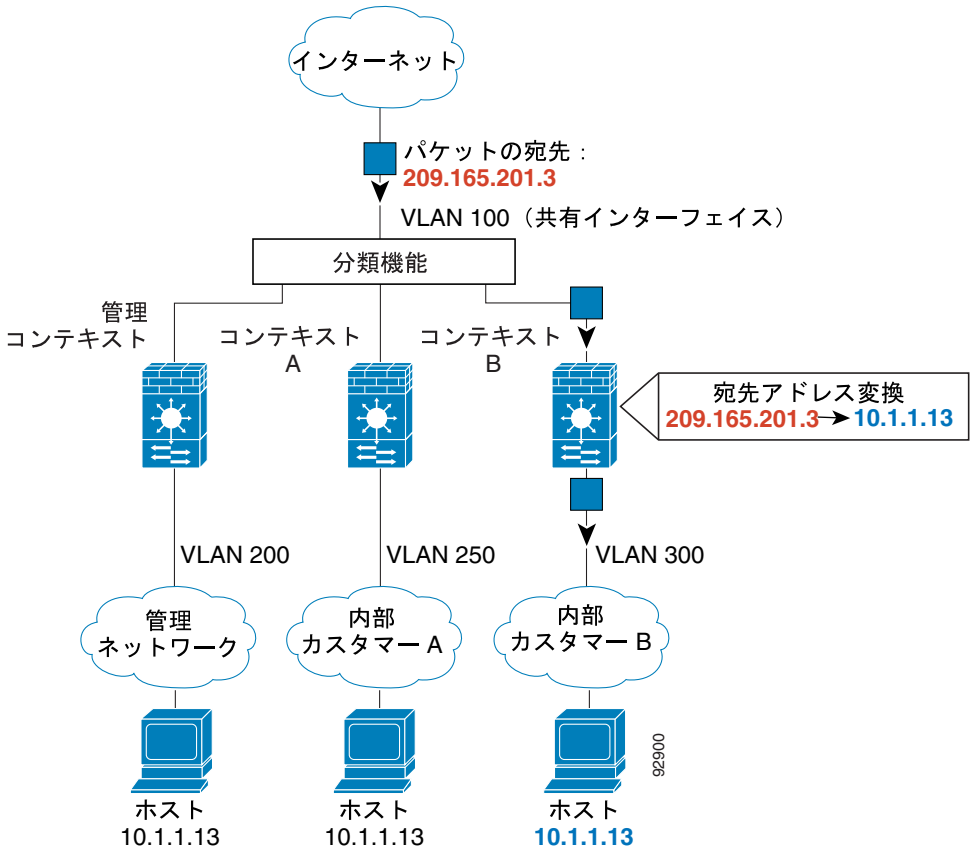
パケットは、上述のいずれかの方法に基づいてコンテキストに分類する必要があります。たとえば、コンテキストにサブネットへのネクストホップとして外部ルータをポイントするスタティック ルートが含まれる場合、および異なるコンテキストに同一サブネットの **static** コマンドが含まれる場合、分類機能では **static** コマンドを使用してそのサブネット宛てのパケットを分類し、スタティック ルートは無視します。

たとえば、各コンテキストが固有のインターフェイスを持つ場合、分類機能では入力側インターフェイスに基づいてパケットをコンテキストに対応付けます。ただし、コンテキスト間でインターフェイスを共有する場合、分類機能は宛先アドレスを使用します。

宛先アドレスの分類には NAT が必要であるため（転送トラフィックのために）、NAT を使用しない場合は、各コンテキストに固有のインターフェイスを使用してください。

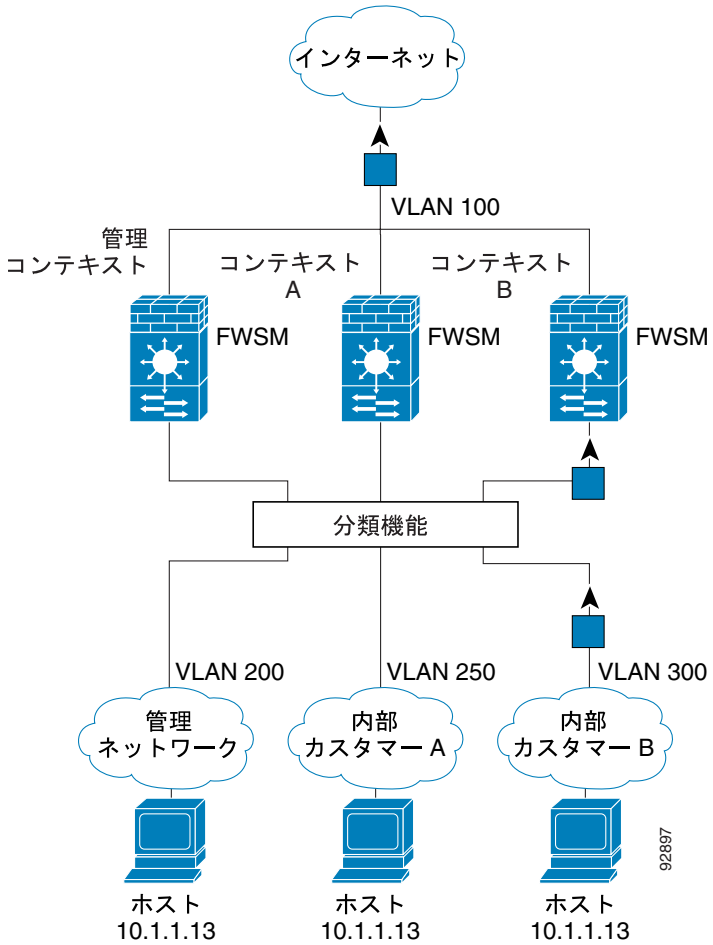
図 4-1 は、内部インターフェイスが固有であるのに対し、外部インターフェイスを複数のコンテキストで共有し、IP アドレスのオーバーラップを認めている状態を示しています。コンテキスト B には宛先アドレスと一致するアドレス変換が含まれるため、分類機能はパケットをコンテキスト B に割り当てています。

図 4-1　共有インターフェイスを使用したパケット分類



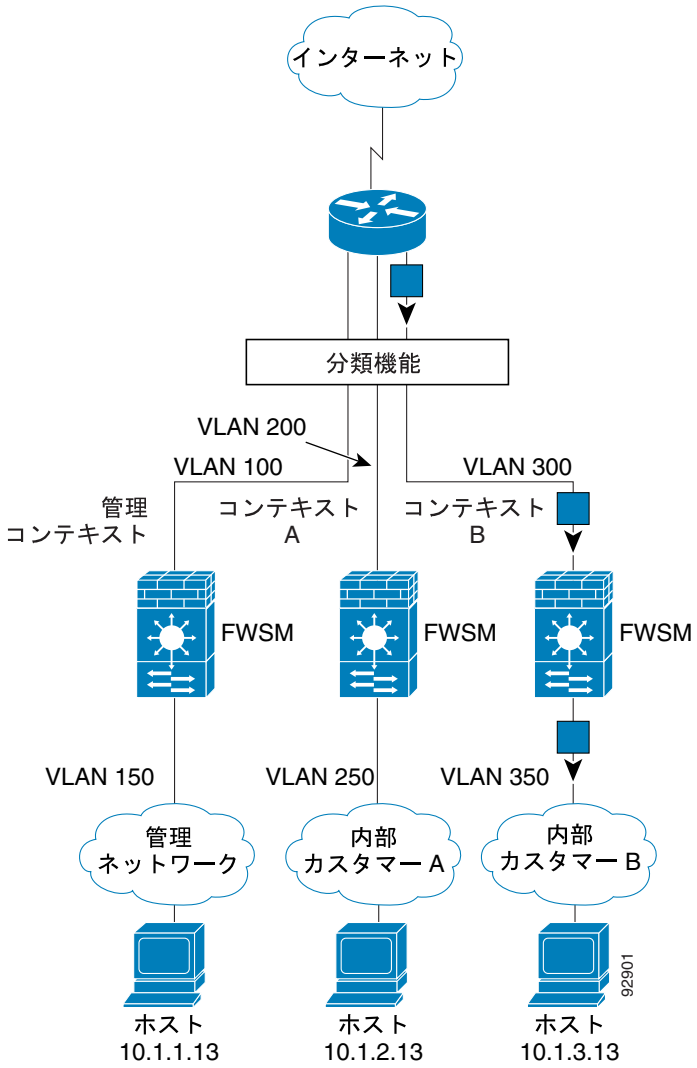
新規の着信トラフィックは、内部ネットワークからのトラフィックであってもすべて分類する必要があります。図 4-2 は、インターネットにアクセスするネットワーク内のコンテキスト B のホストを示しています。入力側インターフェイス VLAN 300 がコンテキスト B に割り当てられているため、分類機能はパケットをコンテキスト B に割り当てています。

図 4-2　内部ネットワークからの着信トラフィック



透過ファイアウォールの場合、固有のインターフェイスを使用する必要があります。分類機能では透過モードでの NAT をサポートしていないため、分類を行うには固有のインターフェイスを使用するしか方法がありません。図 4-3 は、インターネットにアクセスするネットワーク内のコンテキスト B のホストを示しています。入力側インターフェイス VLAN 300 がコンテキスト B に割り当てられているため、分類機能はパケットをコンテキスト B に割り当てています。

図 4-3　透過ファイアウォールのコンテキスト



コンテキスト間でのインターフェイスの共有

ルーテッド モードのみ

FWSM では、コンテキスト間でインターフェイスを共有できます。たとえば、インターフェイスを保全するために外部インターフェイスを共有できます。内部インターフェイスを共有して、コンテキスト間でリソースを共有することもできます。ただし、パケット分類要件により、共有インターフェイスを実行できないことがあります。

ここでは、次の内容について説明します。

- 共有インターフェイスの注意事項（p.4-7）
- セキュリティ コンテキストのカスケード（p.4-9）

共有インターフェイスの注意事項

共有インターフェイスからのトラフィックが FWSM を通過できるようにするには、トラフィックの*宛先*アドレスを変換する必要があります。分類機能は、アドレス変換コンフィギュレーションを使用してコンテキスト内のパケットを分類します。NAT を実行しない場合は、固有のインターフェイスを使用する必要があります。（インターフェイスを共有し、インターフェイスとやり取りする管理トラフィックのみを許可する場合、分類機能はインターフェイス IP アドレス コンフィギュレーション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はこのプロセスでは使用されません）。

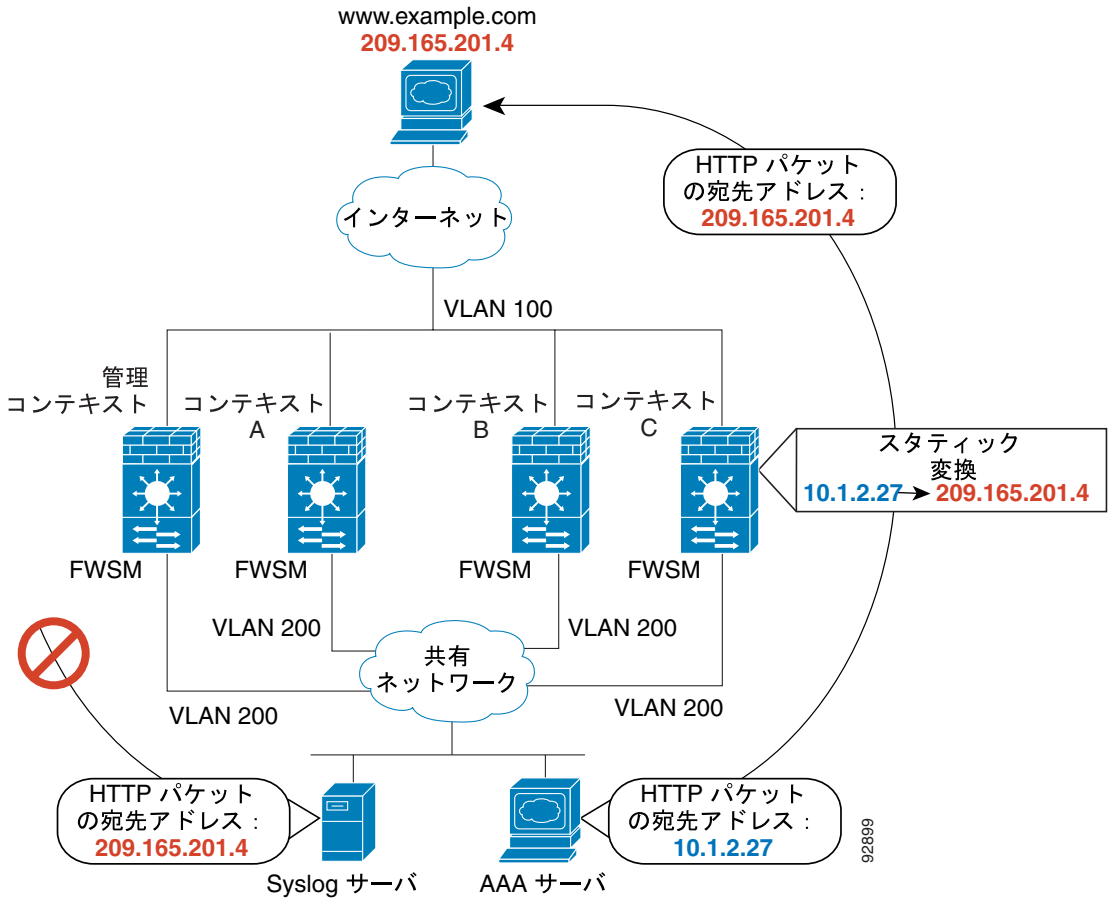
宛先アドレスに設定する NAT のタイプによって、共有インターフェイスでトラフィックを発信できるかどうか、または既存の接続への応答のみが可能かどうかが決まります。宛先アドレスにダイナミック NAT を使用する場合、これらのアドレスへの接続を開始することはできません。このため、共有インターフェイスからのトラフィックは、既存の接続への応答でなければなりません。ただし、スタティック NAT では接続を開始できるため、宛先アドレスにスタティック NAT を使用する場合、共有インターフェイス上で接続を開始できます。

外部共有インターフェイス（インターネットへの接続など）を使用している場合、内部の宛先アドレスは制限され、システム管理者に通知されます。このため、スタティック NAT であっても、これらのアドレスに対しては容易に NAT を設定できます。

ただし、宛先アドレスに制限のない環境で共有インターフェイスとインターネット間の通信を許可する場合、内部共有インターフェイスの設定によって問題が生じます。たとえば、共有インターフェイス上の内部ホストからインターネットへのトラフィックの開始を許可する場合、各インターネット アドレスに対してスタティック NAT を設定する必要があります。この要件により、必然的に内部共有インターフェイス上のユーザに提供できるインターネット アクセスの種類が制限されます。（インターネット サーバのアドレスをスタティックに変換する場合は、DNS エントリのアドレスと NAT によってそれがどのような影響を受けるかということも考慮する必要があります。たとえば、サーバが www.example.com にパケットを送信した場合、DNS サーバは変換されるアドレスを戻す必要があります。NAT コンフィギュレーションによって DNS エントリの管理が決定されます）。

図 4-4 に、内部共有インターフェイス上の 2 つのサーバを示します。一方のサーバは Web サーバの変換対象アドレスにパケットを送信し、FWSM がパケットを分類してコンテキスト C に流します。コンテキスト C でそのアドレスがスタティック変換されるためです。他方のサーバは変換されない実アドレスにパケットを送信しますが、FWSM がパケットを分類できないので、そのパケットは廃棄されます。

図 4-4　共有インターフェイス上を発信元とするトラフィック

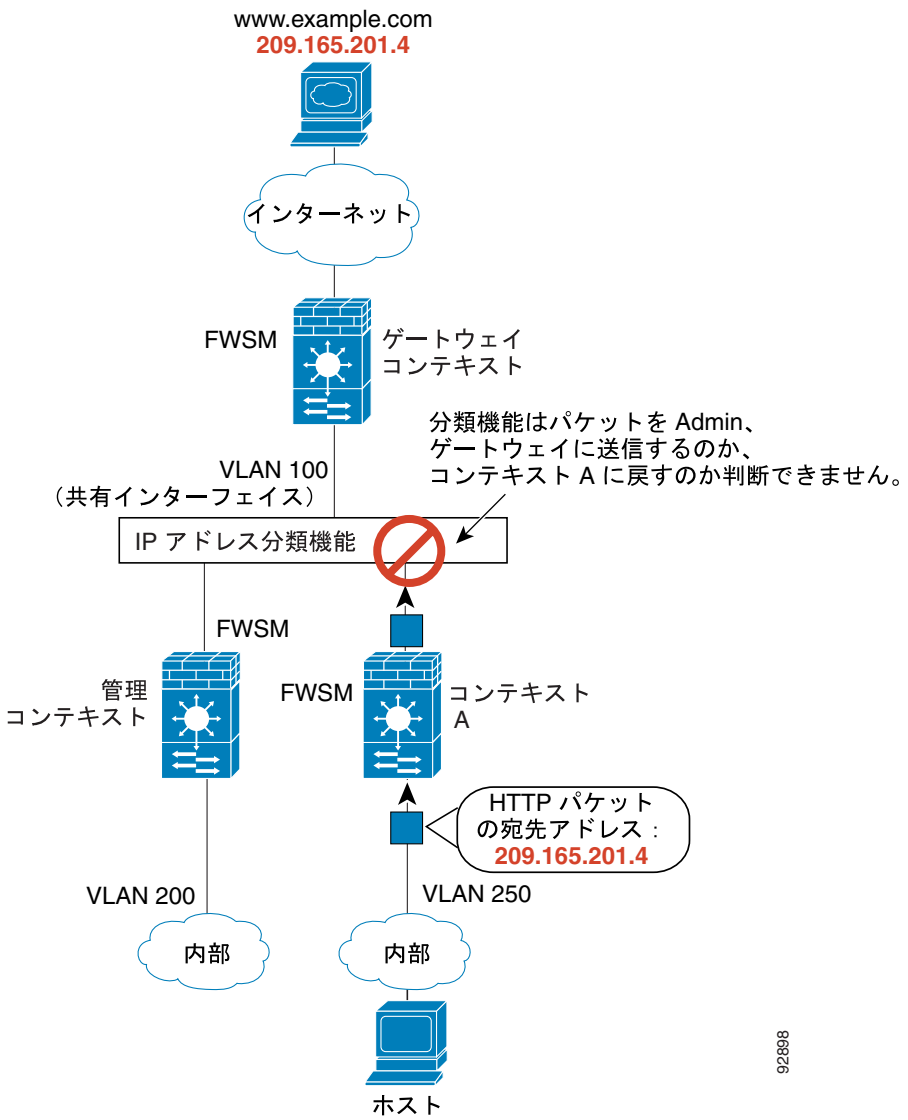


セキュリティ コンテキストのカスケード

共有インターフェイス上を発信元とするトラフィックには制約があるので、あるコンテキストを別のコンテキストの後ろに配置する場合、最後尾のコンテキストに接続されたユーザがアクセスする外部アドレスごとに、先頭のコンテキストでスタティック ステートメントを設定することが必要です。

図 4-5 は、最後尾のコンテキスト（コンテキスト A）のユーザが www.example.com にアクセスする場合を示しています。ゲートウェイ コンテキストでは www.example.com に対するスタティック変換が行われないため、ユーザは Web サーバにアクセスできず、分類機能は共有インターフェイス上のどのコンテキストにパケットを割り当てればよいのか判断できません。

図 4-5　コンテキストのカスケード



マルチコンテキスト モードの FWSM へのログイン

スイッチから FWSM へのセッションを確立するときには、システム実行スペースにアクセスします。あとで Telnet または Secure Shell（SSH; セキュア シェル）によるコンテキスト アクセスを設定する場合は、特定のコンテキストにログインできます。特定のコンテキストにログインした場合、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です。ただし、管理コンテキストまたはシステム実行スペースにログインした場合は、あらゆるコンテキストにアクセスできます。

コンテキストを管理またはシステムから変更する場合は、ユーザ名をデフォルトの「enable_15」ユーザ名に変更します。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」ユーザのための許可権限を設定する必要があります。そのコンテキストのコマンド許可コンフィギュレーションで必要な権限を付与した、別の名前でログインすることもできます。ユーザ名でログインするには、**login** コマンドを入力します。たとえば、管理コンテキストにはユーザ名「admin」でログインします。管理コンテキストにはコマンド許可コンフィギュレーションは含まれませんが、他のすべてのコンテキストにはコマンド許可が含まれます。便宜上、各コンテキスト コンフィギュレーションには最大限の権限が付与されたユーザ「admin」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 に変更すると、ユーザ名が変更されるため、**login** コマンドを入力して「admin」として再度ログインする必要があります。コンテキスト B に変更する場合は、再度 **login** コマンドを入力して「admin」としてログインする必要があります。

システム実行スペースは AAA コマンドを受け付けませんが、セッション確立の際はローカル データベースで専用のログイン パスワード、イネーブル パスワードとともにユーザ名を設定することによって、個別のログインが可能になります。

マルチコンテキスト モードのイネーブル化またはディセーブル化

FWSM は発注に基づいて、出荷段階でマルチセキュリティ コンテキスト対応としてすでに設定されていることがあります。ただし、アップグレードする場合は、この項の手順に従ってシングルモードからマルチモードに変更する必要があります。ASDM ではモードの変更はサポートされていないため、CLI を使用してモードを変更する必要があります。

ここでは、次の内容について説明します。

- シングルモード コンフィギュレーションのバックアップ（p.4-11）
- マルチコンテキスト モードのイネーブル化（p.4-11）
- シングルコンテキスト モードの復元（p.4-12）

シングルモード コンフィギュレーションのバックアップ

シングルモードからマルチモードに変更すると、FWSM が実行ファイルを 2 つのファイルに変換します。元のスタートアップ コンフィギュレーションは保存されないので、実行コンフィギュレーションと異なる場合は、先にバックアップを作成する必要があります。

マルチコンテキスト モードのイネーブル化

コンテキスト モード（シングルまたはマルチ）は、再起動後まで維持される場合であっても、コンフィギュレーション ファイルには保存されません。設定を別のデバイスにコピーする場合は、**mode** コマンドを使用して一致するように新規デバイスのモードを設定します。

シングルモードからマルチモードに変更すると、FWSM は実行コンフィギュレーションをシステム コンフィギュレーションで構成される新規のスタートアップ コンフィギュレーション ファイルと管理コンテキストで構成される admin.cfg ファイル（内部フラッシュ メモリのルート ディレクトリ）の 2 つのファイルに変換します。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 ディレクトリで）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。FWSM はシステム コンフィギュレーションに、「admin」の名前で管理コンテキストのエントリを自動的に追加します。

次のコマンドを入力して、マルチモードをイネーブルにします。

```
hostname(config)# mode multiple
```

FWSM を再起動するように求められます。

シングルコンテキスト モードの復元

マルチモードからシングルモードに変更する場合、（可能な場合）最初にスタートアップ コンフィギュレーションをすべて FWSM にコピーします。マルチモードから継承されたシステム コンフィギュレーションは、シングルモード デバイスにとって完全に機能するコンフィギュレーションではありません。たとえば、可能な場合はシングルモードの旧実行コンフィギュレーションを、スタートアップ コンフィギュレーションとして復元できます。システム コンフィギュレーションには、コンフィギュレーションの一部としてネットワーク インターフェイスが含まれていないので、スイッチ セッションから FWSM にアクセスし、コピーを実行する必要があります。

旧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、モードをシングルモードに変更するには、システム実行スペースで次の手順を実行します。

ステップ 1　システム実行スペースで次のコマンドを入力して、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。

```
hostname(config)# copy old_running.cfg startup-config
```

ステップ 2　システム実行スペースで次のコマンドを入力して、モードをシングルモードに設定します。

```
hostname(config)# mode single
```

FWSM が再起動します。

リソース管理の設定

コンテキストあたりの最大限度を設定しないかぎり、すべてのセキュリティ コンテキストはデフォルトで FWSM のリソースに無制限にアクセスできます。ただし、1 つまたは複数のコンテキストがあまり多くのリソースを使用してしまうと、他のコンテキストの接続が拒否されることがあるので、コンテキストあたりのリソース利用が制限されるように、リソース管理を設定できます。

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

ここでは、次の内容について説明します。

- クラスおよびクラス メンバーの概要（p.4-13）
- クラスの設定（p.4-16）

クラスおよびクラス メンバーの概要

FWSM 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。各コンテキストは、クラスによって設定されたリソース限度を使用します。ここでは、次の内容について説明します。

- リソース限度（p.4-13）
- デフォルト クラス（p.4-14）
- クラス メンバー（p.4-15）

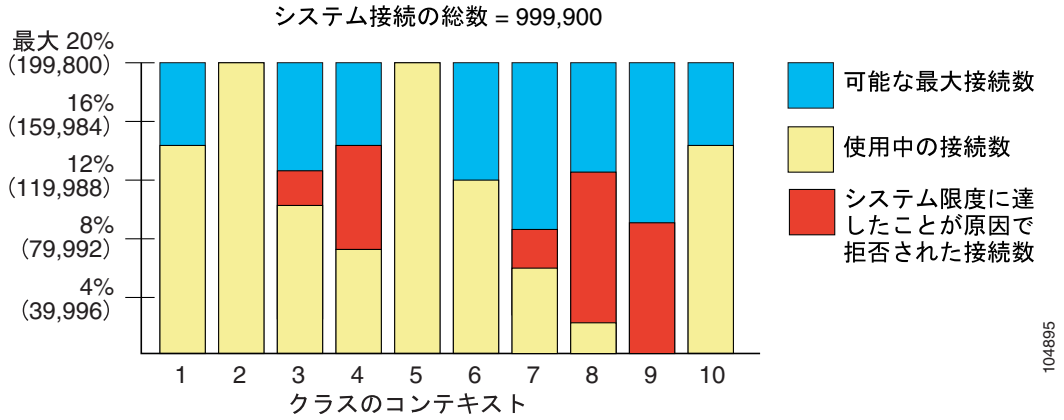
リソース限度

クラスを作成した場合、FWSM はクラスに割り当てられた各コンテキスト用に一定のリソースを確保するのではありません。FWSM はコンテキストに最大限度を設定します。リソースがオーバーサブスクライブされた場合、または一部のリソースが無制限に利用された場合、少数のコンテキストがこれらのリソースを使い果たしてしまい、他のコンテキストに対するサービスが影響を受ける可能性があります。

デバイスで利用できる全体に対する割合として、すべてのリソースにまとめて限度を設定できます。または、個々のリソースに割合または絶対値として限度を設定することもできます。

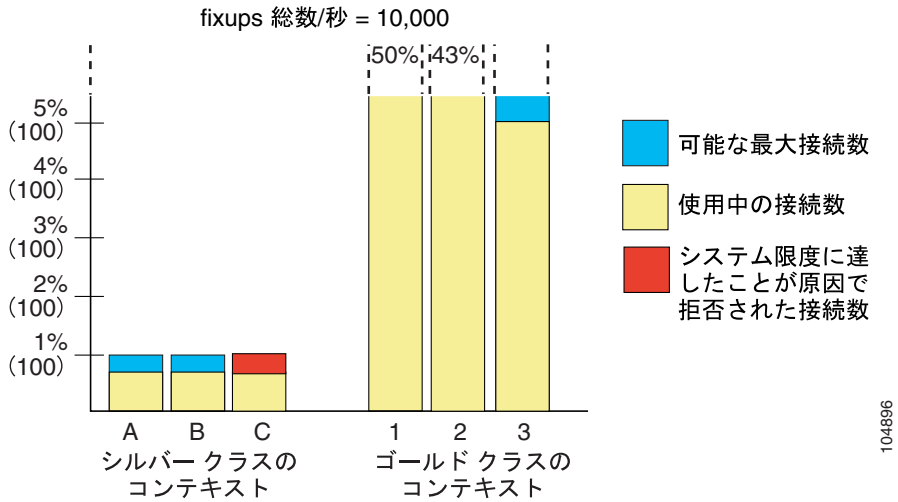
全コンテキストに 100% を超えるリソースを割り当てると、FWSM のオーバーサブスクライブが可能です。たとえば、コンテキストあたりの接続数を 20% に制限するようにブロンズ クラスを設定し、そのクラスに 10 のコンテキストを割り当てた場合、合計で 200% になります。同時にコンテキストの利用がシステム限度を超えると、各コンテキストに与えられるのは、予定の 20% より少なくなります（図 4-6 を参照）。

図 4-6　リソースのオーバーサブスクライブ



FWSM では、割合または絶対値ではなく、クラスで 1 つまたは複数のリソースに無制限アクセスを割り当てることもできます。リソースを無制限にすると、コンテキストはシステムが提供できるだけのリソースを使用できます。たとえば、コンテキスト A、B、および C をシルバー クラスに割り当て、各クラス メンバーをシステムインスペクション回数 / 秒の 1% に制限すると、合計で 3% になりますが、現在、3 つのコンテキストで合計 2% しか使用していないとします。ゴールド クラスは無制限にインスペクションを利用できます。この場合、ゴールド クラスのコンテキストは、「未割り当て」インスペクションの 97% より多くを使用できます。コンテキスト A、B、および C が合計限度である 3% に到達しなくても、コンテキスト A、B、および C が現在使用していない 1% を合わせて使用できるからです（図 4-7 を参照）。無制限アクセスを設定するということは、システムのオーバーサブスクライブの程度をあまり制御できないという点を除き、FWSM をオーバーサブスクライブにするのと同様です。

図 4-7　無制限のリソース



デフォルト クラス

別のクラスに割り当てないかぎり、すべてのコンテキストはデフォルト クラスに属します。デフォルト クラスにコンテキストを割り当てる必要はありません。

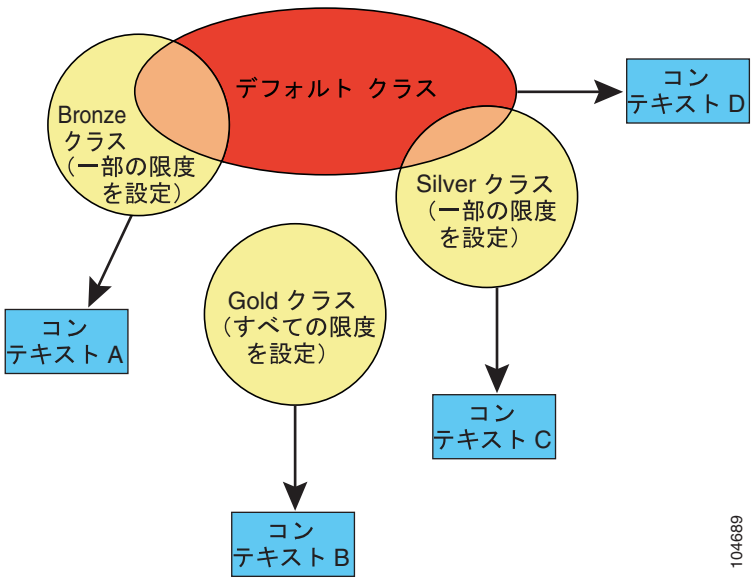
コンテキストがデフォルト クラス以外のクラスに属している場合は必ず、これらのクラスの設定値によってデフォルト クラスの設定値が上書きされます。ただし、他のクラスに未定義の設定値がある場合、そのクラス メンバーであるコンテキストはデフォルト クラスの限度を使用します。たとえば、すべての同時接続に対して 2% の限度を設定してクラスを作成し、その他の限度については設定しなかった場合、他のすべての限度はデフォルト クラスの値を引き継ぎます。逆に、すべてのリソースに 2% の限度を設定してクラスを作成した場合、そのクラスではデフォルト クラスの設定値は使用されません。

デフォルトでは、デフォルト クラスはすべてのコンテキストに対して、リソースの無制限アクセスを認めます。ただし、次の限度については、デフォルトでコンテキストあたりの許容最大値に設定されます。

- Telnet セッション — 5 セッション
- SSH セッション — 5 セッション
- IPSec セッション — 5 セッション
- MAC アドレス — 65,535 エントリ

図 4-8 に、デフォルト クラスとその他のクラスの関係を示します。コンテキスト A および C はいくつか限度が設定されたクラスに属しています。その他の限度は、デフォルト クラスから引き継ぎます。コンテキスト B は、割り当てられたクラスであるゴールド クラスですべての限度が設定されているので、デフォルトの限度は引き継ぎません。コンテキスト D はクラスに割り当てられていないので、デフォルトでデフォルト クラスのメンバーです。

図 4-8　リソース クラス



クラス メンバー

クラスの設定値を使用するには、コンテキストの定義時に、クラスにコンテキストを割り当てます。別のクラスに割り当てないかぎり、すべてのコンテキストはデフォルト クラスに属します。デフォルトにコンテキストを割り当てる必要はありません。コンテキストを割り当てることのできるリソース クラスは 1 つだけです。このルールの例外は、メンバー クラスで未定義の限度はデフォルト クラスから継承されるということです。したがって、コンテキストは事実上、デフォルトおよび別のクラスのメンバーにできます。

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ための手順は、次のとおりです。特定のリソース限度の値を変更する場合は、新しい値を使用してコマンドを再入力します。

ステップ 1　システム実行スペースに次のコマンドを入力して、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。

```
hostname(config)# class name
```

name は最大 20 文字の文字列です。デフォルト クラスの限度を設定する場合は、名前として **default** を入力します。

ステップ 2　次のオプションを参照して、リソース限度を設定します。

- すべてのリソース限度（表 4-1 を参照）を設定する場合は、次のコマンドを入力します。

  ```
  hostname(config-resmgmt)# limit-resource all {number% | 0}
  ```

  number は 1 以上の整数です。（パーセント記号 [%] を付けずに）**0** を指定すると、リソースがシステム限度に設定されます。デバイスをオーバーサブスクライブにする場合は、100% を超えて割り当てることができます。
- 特定のリソース限度を設定する場合は、次のコマンドを入力します。

  ```
  hostname(config-resmgmt)# limit-resource [rate] resource_name number[%]
  ```

  この特定のリソースについては、**all** で設定された限度が上書きされます。**rate** 引数を入力して、特定のリソースにレート / 秒を設定します。レート / 秒を設定できるリソースについては、表 4-1 を参照してください。

  表 4-1 に、リソース タイプおよび限度を示します。**show resource types** コマンドも参照してください。

表 4-1　リソース名および限度

リソース名	コンテキストあたりの最小値および最大値	システム全体での総数	説明
mac-addresses	適用外	同時に 65,535	透過ファイアウォール モードの場合、MAC アドレス テーブルで使用できる MAC アドレス数
conns	適用外	同時に 999,900 102,400/ 秒（レート）	2 つのホスト間の TCP または UDP 接続数（あるホストと他の複数のホスト間を含む） **（注）** 同時接続に関して、FWSM は接続を受け付ける 2 つのネットワーク プロセッサに、限度の半分ずつを割り当てます。通常、接続数は NP 間で均等に分けられます。ただし、状況によっては、接続数が均等に分配されず、一方の NP で最大接続限度に達する前に、他方で限度に達してしまうことがあります。この場合、使用できる最大接続数は、設定した限度未満になります。NP への分配は、アルゴリズムに基づいてスイッチが制御します。このアルゴリズムは、スイッチ上で調整することも、不均衡の原因となった接続限度を引き上げて調整することもできます。

表 4-1　リソース名および限度（続き）

リソース名	コンテキストあたりの最小値および最大値	システム全体での総数	説明
fixups	適用外	10,000/ 秒（レート）	アプリケーション検査
hosts	適用外	同時に 262,144	FWSM を介して接続できるホスト数
ipsec	最小 1 最大 5（同時）	同時に 10	IPSec セッション数
asdm	最小 1 最大 5（同時）	同時に 80	ASDM 管理セッション数 **（注）** ASDM セッションでは、2 つの HTTPS 接続を使用します。1 つは常に使用されるモニタ用、もう 1 つは変更時のみに使用される設定変更用です。たとえば、システム制限の ASDM セッション数が 80 の場合、HTTPS セッション数は 160 に制限されます。
ssh	最小 1 最大 5（同時）	同時に 100	SSH セッション数
syslogs	適用外	30,000/ 秒（レート）	システム ログ メッセージ **（注）** FWSM は、FWSM の端末またはバッファへのメッセージ送信に関して、30,000 メッセージ / 秒をサポートできます。Syslog サーバにメッセージを送信する場合、FWSM は 25,000/ 秒をサポートします。
telnet	最小 1 最大 5（同時）	同時に 100	Telnet セッション
xlates	適用外	同時に 266,144	アドレス変換

たとえば、conns のデフォルト クラス限度を無制限ではなく 10% に設定する場合は、次のコマンドを入力します。

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
```

その他のリソースはすべて無制限のままです。

fixups を 10% に設定する以外、すべてのリソースを 5% に設定して、gold というクラスを追加する場合は、次のコマンドを入力します。

```
hostname(config)# class gold
hostname(config-class)# limit-resource all 5%
hostname(config-class)# limit-resource fixups 10%
```

syslogs を 500/ 秒に設定する以外、すべてのリソースを 3% に設定して、silver というクラスを追加する場合は、次のコマンドを入力します。

```
hostname(config)# class silver
hostname(config-class)# limit-resource all 3%
hostname(config-class)# limit-resource rate syslogs 500
```

メモリ パーティションの設定

マルチコンテキスト モードでは、FWSM はルール コンフィギュレーションに割り当てられたメモリをパーティションに分割し、各コンテキストをパーティションに割り当てます。デフォルトでは、コンテキストは、ACE、AAA ルールなど最大 12,130 のルールを提供する 12 のパーティションのうちの 1 つに属します。FWSM は各コンテキストを、スタートアップ時にロードされる順序でパーティションに割り当てます。たとえば、12 のコンテキストを設定した場合、各コンテキストはそれぞれ個別のパーティションに割り当てられ、12,130 のルールを使用できます。さらに 1 つのコンテキストを追加すると、コンテキスト番号 1 および新しいコンテキスト番号 13 の両方がパーティション 1 に割り当てられるので、2 つのコンテキストが 12,130 のルールを共有します。他の 11 のコンテキストは単独で 12,130 のルールを使用できます。コンテキストを削除してもパーティションのメンバーシップには影響しません。したがって、再起動してコンテキストを均等に割り当てるまでは、コンテキストの割り当てが不均一になります。

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

ルールの制限の詳細については、「ルールの制限」（p.A-6）を参照してください。

コンテキストをパーティションに手動で割り当てることもできます。コンテキストをパーティションに割り当てる場合は、「セキュリティ コンテキストの設定」（p.4-20）を参照してください。コンテキストの数と一致するように、パーティションの数を減らすこともできます。

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

メモリ パーティションの数を変更する手順は、次のとおりです。

ステップ 1　システム実行スペースで次のコマンドを入力して、パーティションの数を設定します。

```
hostname(config)# resource acl-partition number_of_partitions
```

number_of_partitions は 1 ～ 12 です。

(注) コンテキストをパーティションに割り当てる場合、パーティション番号は 0 から始まります。したがって、パーティションが 12 個ある場合は、パーティション番号は 0 ～ 11 になります。コンテキストをパーティションに割り当てる方法については「セキュリティ コンテキストの設定」（p.4-20）を参照してください。

次のプロンプトが表示されます。

```
This configuration command leads to repartitioning of ACL memory. It will not take
effect unless you save the configuration to startup configuration and reboot. Would
you like to save the configuration and reboot now? [n]
```

ステップ 2　**Y** を入力して FWSM をリロードします。

今すぐに **FWSM** をリロードしない場合は、設定を保存してあとでリロードします。

フェールオーバーを使用している場合、メモリ パーティションは両方の装置で一致しなければならないため、他のフェールオーバー装置もリロードする必要があります。両方の装置が同時にダウンするため、トラフィック ロスが生じる可能性があります。

ステップ 3　フェールオーバーを使用している場合は、次のコマンドを入力して他の装置をリロードします。

```
hostname(config)# reload
```

次の例は、コンテキストからメモリ パーティションへの現在のマッピングを確認する方法を示しています。

```
hostname(config)# show resource acl-partition
Total number of configured partitions = 2
Partition #0
        Mode                        :exclusive
        List of Contexts          :bandn, borders
        Number of contexts     :2(RefCount:2)
        Number of rules           :0(Max:53087)
Partition #1
        Mode                        :non-exclusive
        List of Contexts          :admin, momandpopA, momandpopB, momandpopC
                                        momandpopD
        Number of contexts     :5(RefCount:5)
        Number of rules           :6(Max:53087)
```

排他的パーティションおよび包括的パーティションの詳細については、「セキュリティ コンテキストの設定」（p.4-20）を参照してください。

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 コンテキストの定義では、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、および他のコンテキスト パラメータを指定します。

（注） コンテキストをアクティブ / アクティブ フェールオーバーのフェールオーバー グループに割り当てるには、「アクティブ / アクティブ フェールオーバーの使用」（p.13-26）を参照してください。

管理コンテキストがない場合（設定を消去した場合など）は、まず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。

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

このコンテキスト名はまだ設定には存在しませんが、その後 **context** *name* コマンドを入力して指定した名前を照合し、管理コンテキストの設定を続行することができます。

システム コンフィギュレーションでコンテキストを設定するための手順は、次のとおりです。

ステップ 1　コンテキストを設定するには、システム実行スペースで次のコマンドを入力します。

```
hostname(config)# context name
```

name は最大 32 文字の文字列です。この名前は大文字と小文字が区別されるので、たとえば「customerA」と「CutomerA」という名前でコンテキストを 2 つ設定できます。文字、数字、ハイフンを使用できますが、名前の始めと終わりにハイフンを使用することはできません。

「System」または「Null」（大文字または小文字）は予約名であるため、使用できません。

ステップ 2　（任意）次のコマンドを入力して、このコンテキストの説明を追加します。

```
hostname(config-ctx)# description text
```

ステップ 3　次のコマンドを入力して、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。

```
hostname(config-ctx)# allocate-interface vlannumber[-vlannumber] [map_name[-map_name]
[invisible | visible]]
```

このコマンドを繰り返し入力すると、さまざまな範囲を指定できます。このコマンドの **no** 形式で割り当てを削除すると、このインターフェイスを含むすべてのコンテキスト コマンドが実行コンフィギュレーションから削除されます。

通常は 2 ～ 1000 および 1025 ～ 4094 の VLAN 番号または VLAN 範囲を入力します（サポートされる VLAN については、スイッチのマニュアルを参照）。**show vlan** コマンドを使用して、FWSM に割り当てられた VLAN のリストを表示します。FWSM にまだ割り当てられていない VLAN を割り当てることはできますが、トラフィックを渡す場合は、スイッチから割り当てを行う必要があります。インターフェイスを割り当てると、FWSM はシステム コンフィギュレーションで各 VLAN に自動的に **interface** コマンドを追加します。

必要であれば、ルーテッド モードで複数のコンテキストに同じ VLAN を割り当ててもかまいません。共有 VLAN の制限事項の詳細については、「コンテキスト間でのインターフェイスの共有」（p.4-7）を参照してください。

map_name はインターフェイスの英数字のエイリアスで、コンテキスト内で VLAN ID の代わりに使用できます。マップ名を指定しない場合、コンテキスト内で VLAN ID が使用されます。セキュリティ上の理由から、コンテキストの管理者にコンテキストが使用しているインターフェイスを知らせないでおいた方がよい場合があります。

マップ名は英字から始め、英字または数字で終わらなければなりません。中間の文字として使用できるのは英字、数字、または下線だけです。使用できる名前の例を示します。

```
int0

inta

int_0
```

VLAN ID 範囲を指定する場合は、対応するマップ名の範囲を指定できます。範囲に関する注意事項は、次のとおりです。

- マップ名は英字部分とその後ろの数字部分で構成しなければなりません。マップ名の英字部分は、範囲の先頭と末尾で一致していなければなりません。範囲の入力例を示します。

  ```
  int0-int10
  ```

- マップ名の数字部分には、**vlan***x*-**vlan***y* ステートメントと同じ数だけ含まれていなければなりません。次の例では、どちらの範囲にも 100 個のインターフェイスが含まれています。

  ```
  vlan100-vlan199 int1-int100
  ```

  たとえば、**vlan100-vlan199 int1-int15** または **vlan100-vlan199 happy1-sad5** を入力した場合、コマンドは失敗します。

マップ名を設定した場合、**visible** を指定して、**show interface** コマンドのマップ名だけでなく VLAN ID も表示します。デフォルトの **invisible** キーワードでは、マップ名のみが表示されます。

VLAN 100、200、および 300 ～ 305 をコンテキストに割り当てる例を示します。マップ名は int1 ～ int8 です。

```
hostname(config-ctx)# allocate-interface vlan100 int1
hostname(config-ctx)# allocate-interface vlan200 int2
hostname(config-ctx)# allocate-interface vlan300-vlan305 int3-int8
```

ステップ 4　次のコマンドを入力して、システムがどこからコンテキスト コンフィギュレーションをダウンロードするのかを URL で指定します。

```
hostname(config-ctx)# config-url url
```

コンテキストの URL を追加すると、設定がある場合、システムはそのコンテキストをただちにロードして、動作するようにします。

（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。FWSM は、コンテキスト コンフィギュレーションをロードする前に、コンテキストに VLAN インターフェイスを割り当てる必要があります。コンテキスト コンフィギュレーションにインターフェイスを参照するコマンド（**interface**、**nat**、**global** など）が含まれていることがあるからです。**config-url** コマンドを先に入力すると、FWSM 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。コンテキストにインターフェイスを参照するコマンドが含まれていた場合、それらのコマンドは失敗します。

URL の構文は次のとおりです。

- ***disk:/***[*path/*]*filename*

  この URL は内部フラッシュ メモリを示します。ファイル名にファイル拡張子は不要ですが、「.cfg」の使用を推奨します。コンフィギュレーション ファイルがない場合は、次のメッセージが表示されます。

  ```
  WARNING: Could not fetch the URL disk:/url
  INFO: Creating context with default config
  ```

  その後、コンテキストに切り替えて、CLI でコンテキストを設定し、**write memory** コマンドを入力してファイルをフラッシュ メモリに書き込むことができます。

  (注) 管理コンテキストのファイルは、内部フラッシュ メモリに保管する必要があります。

- ***ftp://***[*user*[***:****password*]***@***]*server*[*:port*]*/*[*path/*]*filename*[***;type****=xx*]

  type には、次のいずれかのキーワードを指定できます。

  — ***ap*** — ASCII パッシブ モード

  — ***an*** — ASCII 標準モード

  — ***ip*** —（デフォルト）バイナリ パッシブ モード

  — ***in*** — バイナリ標準モード

  サーバは管理コンテキストからアクセスできなければなりません。ファイル名にファイル拡張子は不要ですが、「.cfg」の使用を推奨します。コンフィギュレーション ファイルがない場合は、次のメッセージが表示されます。

  ```
  WARNING: Could not fetch the URL ftp://url
  INFO: Creating context with default config
  ```

  その後、コンテキストに切り替えて、CLI でコンテキストを設定し、**write memory** コマンドを入力してファイルを FTP サーバに書き込むことができます。

- ***http***[*s*]***://***[*user*[***:****password*]***@***]*server*[*:port*]*/*[*path/*]*filename*

  サーバは管理コンテキストからアクセスできなければなりません。ファイル名にファイル拡張子は不要ですが、「.cfg」の使用を推奨します。コンフィギュレーション ファイルがない場合は、次のメッセージが表示されます。

  ```
  WARNING: Could not fetch the URL http://url
  INFO: Creating context with default config
  ```

  コンテキストに切り替えて、CLI でコンテキストを設定する場合、**write memory** コマンドを使用して変更を HTTP または HTTPS サーバに保存することはできません。ただし、**copy tftp** コマンドを使用して実行コンフィギュレーションを TFTP サーバにコピーすることはできます。

- ***tftp://***[*user*[***:****password*]***@***]*server*[*:port*]*/*[*path/*]*filename*[***;int****=interface_name*]

  サーバは管理コンテキストからアクセスできなければなりません。ルートをサーバ アドレスに優先する場合は、インターフェイス名を指定します。ファイル名にファイル拡張子は不要ですが、「.cfg」の使用を推奨します。コンフィギュレーション ファイルがない場合は、次のメッセージが表示されます。

  ```
  WARNING: Could not fetch the URL tftp://url
  INFO: Creating context with default config
  ```

  その後、コンテキストに切り替えて、CLI でコンテキストを設定し、**write memory** コマンドを入力してファイルを TFTP サーバに書き込むことができます。

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 コンテキストの URL の変更」（p.4-26）を参照してください。

コマンドの入力例を示します。

```
hostname(config-ctx)# config-url ftp://joe:passw0rd1@10.1.1.1/configlets/test.cfg
```

ステップ 5　（任意）次のコマンドを入力して、リソース クラスにコンテキストを割り当てます。

```
hostname(config-ctx)# member class_name
```

クラスを指定しなかった場合、コンテキストはデフォルト クラスに属します。コンテキストを割り当てることのできるリソース クラスは 1 つだけです。

次のコマンドを入力して、gold クラスにコンテキストを割り当てます。

```
hostname(config-ctx)# member gold
```

ステップ 6　（任意）次のコマンドを入力して、コンテキストを特定のメモリ パーティションにマップします。

```
hostname(config-ctx)# allocate-acl-partition partition_number
```

partition_number は「0」から「パーティション数 - 1」の整数です。デフォルトは 12 パーティションであるため、範囲は 0 ～ 11 になります。メモリ パーティションの数の設定については「メモリ パーティションの設定」（p.4-18）を参照してください。

コンテキストをパーティションに割り当てると、そのパーティションは*排他的*になります。排他的なパーティションには、明確に割り当てられたコンテキストのみが含まれます。コンテキストを明確に割り当てられていないパーティションは包括的であり、コンテキストがラウンドロビン形式で割り当てられます。

（注）　コンテキストをすべてのパーティションに割り当てた場合、すべてのパーティションが排他的になります。その後、パーティションに割り当てられていないコンテキストを追加した場合、そのコンテキストはデフォルトでパーティション 0 に割り当てられます。

たとえば、コンテキストを最初のパーティションに割り当てるには、次のコマンドを入力します。

```
hostname(config-ctx)# allocate-acl-partition 0
```

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

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface vlan10
hostname(config-ctx)# allocate-interface vlan11
hostname(config-ctx)# config-url disk:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface vlan100 int1
hostname(config-ctx)# allocate-interface vlan102 int2
hostname(config-ctx)# allocate-interface vlan110-vlan115 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold
hostname(config-ctx)# allocate-acl-partition 0


hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface vlan200 int1
hostname(config-ctx)# allocate-interface vlan212 int2
hostname(config-ctx)# allocate-interface vlan230-vlan235 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver
```

コンテキストとシステム実行スペース間の切り替え

システム実行スペース（または Telnet か SSH を使用した管理コンテキスト）にログインすると、コンテキストを切り替えて、各コンテキストで設定作業やモニタ作業を実行できます。コンフィギュレーション モードで編集する、または **copy** コマンドや **write** コマンドの影響を受ける実行コンフィギュレーションは、どこで作業するかによって決まります。システム実行スペースで作業する場合、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だけで構成されます。コンテキストで作業する場合、実行コンフィギュレーションに含まれるのは、そのコンテキスト コンフィギュレーションだけです。たとえば、**show running-config** コマンドですべての実行コンフィギュレーション（システムおよび全コンテキスト）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。ただし、**write memory all** コマンドを使用すると、システム実行スペースからすべてのコンテキスト実行コンフィギュレーションを保存できます。

コンテキスト間での切り替え時のコマンド許可の詳細については、「マルチコンテキスト モードの FWSM へのログイン」（p.4-10）を参照してください。

システム実行スペースとコンテキスト間で切り替えるか、またはコンテキスト間で切り替える場合は、次のコマンドを参照してください。

- コンテキストに切り替える場合は、次のコマンドを入力します。

  hostname# **changeto context** *name*

  プロンプトが次のように変わります。

  hostname/*name*#

- システム実行スペースに切り替える場合は、次のコマンドを入力します。

  hostname/admin# **changeto system**

  プロンプトが次のように変わります。

  hostname#

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 コンテキストの管理方法について説明します。内容は次のとおりです。

- セキュリティ コンテキストの削除（p.4-25）
- 管理コンテキストの変更（p.4-25）
- セキュリティ コンテキストの URL の変更（p.4-26）
- セキュリティ コンテキストのリロード（p.4-27）
- セキュリティ コンテキストのモニタリング（p.4-28）

セキュリティ コンテキストの削除

コンテキストを削除する唯一の方法は、システム コンフィギュレーションを編集することです。**clear context** コマンドを使用してすべてのコンテキストを削除しないかぎり、現在の管理コンテキストを削除することはできません。

（注） フェールオーバーを使用する場合、アクティブ ユニットまたはグループ上でコンテキストを削除してから、スタンバイ ユニットまたはグループ上でコンテキストが削除されるまでに遅延が生じます。アクティブ ユニットとスタンバイ ユニット間でインターフェイス数が一致していないことを伝えるエラー メッセージが表示される場合がありますが、このエラーは一時的なものなので、無視してかまいません。

コンテキストを削除するには、次のコマンドを使用します。

- 個々のコンテキストを削除する場合は、システム実行スペースで次のコマンドを入力します。

  hostname(config)# **no context** *name*

- （管理コンテキストを含めて）すべてのコンテキストを削除する場合は、システム実行スペースで次のコマンドを入力します。

  hostname(config)# **clear context**

管理コンテキストの変更

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かぎり、すべてのコンテキストを管理コンテキストに設定できます。システム実行スペースで次のコマンドを入力して、管理コンテキストを設定します。

hostname(config)# **admin-context** *context_name*

管理コンテキストに接続されている、Telnet、SSH、HTTPS などの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） 管理コンテキストに属するインターフェイス名を識別するシステム　コマンドは少数です。このため、管理コンテキストを変更し、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場合、そのインターフェイスを参照するすべてのシステム コマンドを更新する必要があります。

セキュリティ コンテキストの URL の変更

新しい URL から設定をリロードしないかぎり、セキュリティ コンテキストの URL を変更することはできません。

FWSM は、新しい設定を現在の実行コンフィギュレーションと結合します。同一 URL を再入力した場合も、保存された設定と実行コンフィギュレーションが結合されます。結合によって、新しい設定のコマンドが実行コンフィギュレーションに追加されます。設定が同じ場合、変更はありません。コマンドが矛盾する場合、またはコマンドがコンテキストの稼働に影響を与える場合、結合の影響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あれば、予想外の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ブランクの場合（サーバが利用できなかった、設定が一度もダウンロードされていないなど）、新しい設定が使用されます。設定の結合が望ましくない場合は、実行コンフィギュレーションを消去できます。この場合、コンテキストを介した通信が中断され、新しい URL から設定がリロードされます。

コンテキストの URL を変更する手順は、次のとおりです。

ステップ 1　設定を結合しない場合、次のコマンドを入力してコンテキストに切り替え、そのコンテキスト コンフィギュレーションを消去します。結合を実行する場合は、ステップ 2 に進みます。

```
hostname# changeto context name
hostname/name# configure terminal
hostname/name(config)# clear configure all
```

ステップ 2　必要に応じて次のコマンドを入力して、システム実行スペースに切り替えます。

```
hostname/name(config)# changeto system
```

ステップ 3　次のコマンドを入力して、変更するコンテキストに対応するコンテキスト コンフィギュレーション モードを開始します。

```
hostname(config)# context name
```

ステップ 4　次のコマンドを入力して、新しい URL を指定します。

```
hostname(config)# config-url new_url
```

システムがコンテキストをただちにロードして、動作するようにします。

セキュリティ コンテキストのリロード

コンテキストは、2 通り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消去し、スタートアップ コンフィギュレーションをインポートします。

  この処理によって、接続、NAT テーブルなど、コンテキストに対応付けられた属性の大部分が消去されます。
- システム コンフィギュレーションからコンテキストを削除します。

  この処理によって、メモリ割り当てなど、その他の属性が消去されます。これはトラブルシューティングに役立つ場合があります。ただし、システムにもう一度コンテキストを追加するには、URL とインターフェイスを再指定しなければなりません。

ここでは、次の内容について説明します。

- 設定の消去によるリロード（p.4-27）
- コンテキストの削除および再追加によるリロード（p.4-28）

設定の消去によるリロード

コンテキスト コンフィギュレーションを消去することによってコンテキストをリロードし、URL から設定をリロードする手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、リロードするコンテキストに切り替えます。

```
hostname# changeto context name
```

ステップ 2　次のコマンドを入力して、コンフィギュレーション モードにアクセスします。

```
hostname/name# configure terminal
```

ステップ 3　次のコマンドを入力して、実行コンフィギュレーションを消去します。

```
hostname/name(config)# clear configure all
```

このコマンドはすべての接続をクリアします。

ステップ 4　次のコマンドを入力して、設定をリロードします。

```
hostname/name(config)# copy startup-config running-config
```

FWSM が、システム コンフィギュレーションで指定された URL から設定をコピーします。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てからもう一度追加することによって、コンテキストをリロードする場合は、次の手順を実行します。

1. 「セキュリティ コンテキストの削除」（p.4-25）
2. 「セキュリティ コンテキストの設定」（p.4-20）

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してモニタする方法について説明します。内容は次のとおりです。

- コンテキスト情報の表示（p.4-28）
- リソース割り当ての表示（p.4-30）
- リソース使用状況の表示（p.4-32）
- コンテキストでの SYN 攻撃のモニタリング（p.4-34）

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、割り当てられたインターフェイス、およびコンフィギュレーション ファイルの URL を示したコンテキストの一覧を表示できます。

システム実行スペースから次のコマンドを入力して、すべてのコンテキストを表示します。

```
hostname# show context [name | detail| count]
```

detail オプションを指定すると、詳細情報が表示されます。次の出力例を参照してください。

特定のコンテキストについて情報を表示する場合は、*name* を指定します。

count オプションを指定すると、コンテキストの総数が表示されます。

次に、**show context** コマンドの出力例を示します。次に、3 つのコンテキストの出力例を示します。

```
hostname# show context

Context Name      Class       Interfaces        Mode          URL
*admin            default     Vlan100,101       Routed        disk:/admin.cfg
contexta          Gold        Vlan200,201       Transparent   disk:/contexta.cfg
contextb          Silver      Vlan300,301       Routed        disk:/contextb.cfg
Total active Security Contexts: 3
```

表 4-2 で、各フィールドについて説明します。

表 4-2　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を表示。アスタリスク（*）の付いたコンテキスト名は、管理コンテキストです。
Class	コンテキストが属しているリソース クラス
Interfaces	コンテキストに割り当てられているインターフェイス
Mode	各コンテキストのファイアウォール モード（ルーテッド モードまたは透過モード）
URL	FWSM 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

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

```
hostname# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk:/admin.cfg
  Real Interfaces: Vlan100
  Mapped Interfaces: Vlan100
  Class: default, Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: disk:/ctx.cfg
  Real Interfaces: Vlan10,20,30
  Mapped Interfaces: int1, int2, int3
  Class: default, Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Vlan100,10,20,30
  Class: default, Flags: 0x00000019, ID: 257

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

detail の出力については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』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。

```
hostname# 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すべてのクラス メンバーについて、各リソースの割り当てを表示できます。

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。

```
hostname# show resource allocation [detail]
```

このコマンドで表示されるのは、リソース割り当てであり、実際に使用されているリソースではありません。実際のリソース使用状況の詳細については、「リソース使用状況の表示」（p.4-32）を参照してください。

detail 引数を指定すると、詳細情報が表示されます。次の出力例を参照してください。

次に、各リソースの総割り当てを絶対値および使用可能なシステム リソースの割合で表した出力例を示します。

```
hostname# show resource allocation
Resource                     Total       % of Avail
 Conns [rate]                35000           35.00%
 Fixups [rate]               35000           35.00%
 Syslogs [rate]              10500           35.00%
 Conns                      305000           30.50%
 Hosts                       78842           30.07%
 IPsec                           7           35.00%
 SSH                            35           35.00%
 Telnet                         35           35.00%
 Xlates                      91749           34.99%
 All                     unlimited
```

表 4-3 で、各フィールドについて説明します。

表 4-3　show resource allocation のフィールド

フィールド	説明
Resource	制限できるリソースの名前
Total	すべてのコンテキスト間で割り当てられているリソースの総量。量とは、同時インスタンスの絶対数またはインスタンス数 / 秒です。クラス定義で割合を指定した場合、FWSM がこの出力のために割合を絶対数に変換します。
% of Avail	総システム リソースのうち、すべてのコンテキスト間で割り当てられている割合。

次に、**detail** オプションを指定した場合の出力例を示します。

```
hostname# 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     20.00%
                 silver             1      CA      17000      17000     10.00%
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     30.00%

Fixups [rate]    default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     10.00%
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     10.00%

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     20.00%
                 silver             1      CA       3000       3000     10.00%
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     30.00%

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      9.99%
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      9.99%

IPSec            default          all       C          5
                 gold               1       D          5          5     50.00%
                 silver             1      CA          1          1     10.00%
                 bronze             0      CA  unlimited
                 All Contexts:      3                            11    110.00%

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%

Xlates           default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      23040      23040     10.00%
                 bronze             0      CA      11520
                 All Contexts:      3                         23040     10.00%

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 4-4 で、各フィールドについて説明します。

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

フィールド	説明
Resource	制限できるリソースの名前
Class	デフォルト クラスを含めた各クラスの名前 All Contexts フィールドに、全クラスでの合計値が示されます。
Mmbrs	各クラスに割り当てられたコンテキスト数
Origin	次に示す、リソース限度の設定元 • A — 個々のリソースではなく、**all** オプションで設定された限度 • C — メンバー クラスから導出された限度 • D — メンバー クラスでは定義されていない、デフォルト クラスから導出された限度。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、この値は「D」ではなく「C」になります。 FWSM は、「A」と、「C」または「D」を結合できます。
Limit	絶対値で表したコンテキストあたりのリソース限度。クラス定義で割合を指定した場合、FWSM がこの出力のために割合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間で割り当てられているリソースの総量。量とは、同時インスタンスの絶対数またはインスタンス数 / 秒です。リソースが無制限の場合、この表示はブランクになります。
Total %	総システム リソースのうち、クラス内のすべてのコンテキスト間で割り当てられている割合。リソースが無制限の場合、この表示はブランクになります。

リソース使用状況の表示

システム実行スペースから、各コンテキストのリソース使用状況およびシステムのリソース使用状況を表示できます。

システム実行スペースから次のコマンドを入力して、各コンテキストのリソース使用状況を表示します。

```
hostname# show resource usage [context context_name | top n | all | summary | system]
[resource {resource_name | all}] [counter counter_name [count_threshold]]
```

デフォルトでは、**all** のコンテキストのリソース使用状況が表示されます（各コンテキストは別個に表示されます）。

top *n* キーワードを入力すると、指定したリソースの利用上位 *n* 番までのユーザのコンテキストが表示されます。このオプションでは、**resource all** ではなく、特定のリソース タイプを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集計されて表示されます。

system オプションではすべてのコンテキストの使用状況が集計されて表示されますが、限度は集計されたコンテキスト限度ではなくリソースのシステム限度が表示されます。

resource *resource_name* については、表 4-1 で使用可能なリソース名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。すべてのタイプに対して、**all**（デフォルト）を指定します。

counter *counter_name* は、次のキーワードの 1 つです。

- **current** — アクティブな同時インスタンスの数または現在のリソース レートが表示されます。
- **denied** — リソース割り当てを超えたために拒否されたインスタンスの数が表示されます。
- **peak** — **clear resource usage** コマンドによって、またはデバイスの再起動によって、統計情報が前回消去されて以後、最大の同時インスタンス数または最大リソース レートが表示されます。
- **all** —（デフォルト）すべての統計情報が表示されます。

count_threshold で設定した値を上回ると、リソースが表示されます。デフォルトは 1 です。リソースの使用状況が設定した値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** を指定すると、現在の使用数に *count_threshold* が適用されます。

（注） すべてのリソースを表示する場合は、*count_threshold* を **0** に設定します。

次に、管理コンテキストのリソース使用状況を表す **show resource usage context** コマンドの出力例を示します。

```
hostname# 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、すべてのコンテキストおよびすべてのリソースのリソース使用状況を表す **show resource usage summary** コマンドの出力例を示します。この例では、6 つのコンテキストの制限を示します。

```
hostname# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      12000(U)       0 Summary
Conns                     584          763     100000(S)       0 Summary
Xlates                   8526         8966      93400          0 Summary
Hosts                     254          254     262144          0 Summary
Conns [rate]              270          535      42200       1704 Summary
Fixups [rate]             270          535     100000(S)       0 Summary
U = Some contexts are unlimited and are not included in the total.
S = All contexts are unlimited; system limit is shown.
```

次に、**show resource usage system** コマンドの出力例を示します。すべてのコンテキストのリソース使用状況が表示されますが、限度は集計されたコンテキスト限度ではなくシステム限度が表示されます。

```
hostname# show resource usage system

Resource              Current         Peak      Limit    Denied  Context
Telnet                      3            5        100         0  System
SSH                         5            7        100         0  System
Conns                      40           55        N/A         0  System
Hosts                      44           56        N/A         0  System
```

コンテキストでの SYN 攻撃のモニタリング

FWSM 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阻止します。SYN フラッディング攻撃では、通常、スプーフィングされた IP アドレスから一連の SYN パケットが送信されます。継続的に送信される SYN パケットにより、サーバの SYN キューが常に満杯状態になり、接続要求を処理できなくなります。接続が、初期接続スレッシュホールドに達すると、FWSM はサーバのプロキシとして動作し、クライアントの SYN 要求に対して SYN-ACK 応答を生成します。FWSM は、クライアントから ACK の返信を受信すると、そのクライアントを認証し、サーバへの接続を許可します。

個々のコンテキストへの攻撃率をモニタするには、**show perfmon** コマンドを使用します。個々のコンテキスト用に TCP 代行受信が使用したリソース量をモニタするには、**show resource usage detail** コマンドを使用します。TCP 代行受信がシステム全体で使用したリソース量をモニタするには、**show resource usage summary detail** コマンドを使用します。

次に、管理コンテキストの TCP 代行受信レートを表す **show perfmon** コマンドの出力例を示します。

```
hostname/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、各コンテキストの TCP 代行受信で使用されるリソース量を表す **show resource usage detail** コマンドの出力例を示します（イタリック体の表示が TCP 代行受信に関する情報です）。

```
hostname(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-intercept-rate     328787       803610  unlimited             0 admin
np-statics                  3            3  unlimited             0 admin
statics                     1            1  unlimited             0 admin
ace-rules                   1            1        N/A             0 admin
console-access-rul          2            2        N/A             0 admin
fixup-rules                14           15        N/A             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        N/A             0 c1
console-access-rul          2            2        N/A             0 c1
fixup-rules                14           15        N/A             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
```

次に、システム全体で TCP 代行受信が使用したリソースを表示する例を示します（イタリック体の表示が TCP 代行受信に関する情報です）。

```
hostname(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       8192(S)          0 Summary
block:2048                 32           35       1000(S)          0 Summary
tcp-intercept-rate     341306       811579  unlimited             0 Summary
globals                     1            1       1051(S)          0 Summary
np-statics                  6            6       4096(S)          0 Summary
statics                     2            2       2048(S)          0 Summary
nats                        1            1       2048(S)          0 Summary
ace-rules                   3            3     116448(S)          0 Summary
console-access-rul          4            4       4356(S)          0 Summary
fixup-rules                43           44       8032(S)          0 Summary
S = System:Total exceeds the system limit; the system limit is shown
```

ファイアウォール モードの設定

この章では、ファイアウォール モードの設定方法、および各ファイアウォール モードでファイアウォールがどのように機能するかについて説明します。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。

FWSM（またはマルチモードでの各コンテキスト）は、2 種類のファイアウォール モードのいずれかで動作可能です。

- ルーテッド モード
- 透過モード

ルーテッド モードの場合、FWSM はネットワーク上のルータ ホップとみなされます。接続されたネットワーク間で NAT を実行できます。また、OSPF またはパッシブ RIP（シングルコンテキスト モード限定）を使用できます。ルーテッド モードは、異なるサブネット上にある複数のインターフェイスをサポートします。一定の制限のもとに、コンテキスト間でインターフェイスを共有できます。

透過モードの場合、FWSM は「ワイヤの凹凸」、すなわち「ステルス ファイアウォール」のように動作し、ルータ ホップにはなりません。FWSM は内部および外部インターフェイス上の同一ネットワークに接続します。マルチコンテキスト モードを使用しない場合、またはコンテキストを最大限に使用する場合は、ブリッジ グループと呼ばれるインターフェイスの複数のペアを作成できます。各ブリッジ グループは別々のネットワークに接続します。ダイナミック ルーティング プロトコルや NAT は使用しません。ただし、ルーテッド モードと同様、透過モードでも、自動的に通過を許可される Address Resolution Protocol（ARP; アドレス解決プロトコル）パケットを除くすべてのトラフィックが FWSM を通過できるようにするためのアクセス リストが必要です。透過モードでは、ルーテッド モードでブロックされる特定のタイプのトラフィックをアクセス リストで許可できます。サポート対象外のルーティング プロトコルなどが該当します。透過モードの場合、任意で EtherType アクセス リストを使用して、IP 以外のトラフィックを通過させることができます。

（注） ブリッジ グループはそれぞれ管理 IP アドレスが必要です。FWSM 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。管理用 IP アドレスは、接続先ネットワークと同じサブネット上になければなりません。

この章で説明する内容は、次のとおりです。

- ルーテッド モードの概要（p.5-2）
- 透過モードの概要（p.5-9）
- 透過ファイアウォール モードまたはルーテッド ファイアウォール モードの設定（p.5-17）

ルーテッド モードの概要

- IP ルーティング サポート（p.5-2）
- NAT（p.5-2）
- ルーテッド ファイアウォール モードで FWSM を通過するデータ（p.5-3）

IP ルーティング サポート

FWSM は、接続されたネットワーク間でルータとして動作します。各インターフェイスには、異なるサブネット上の IP アドレスが必要です。シングルコンテキスト モードの場合、ルーテッド ファイアウォールは OSPF および RIP（パッシブ モード）をサポートします。マルチコンテキスト モードがサポートするのは、スタティック ルートだけです。広範なルーティング ニーズに対応するには、FWSM に依存するのではなく、アップストリームおよびダウンストリーム 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。

NAT

Network Address Translation（NAT; ネットワーク アドレス変換）は、パケットの実アドレスを宛先ネットワーク上でルーティング可能なマップ アドレスに置き換えます。デフォルトでは NAT は必要ありません。セキュリティの高いインターフェイス上のホストがセキュリティの低いインターフェイス（外部）と通信するときに NAT の使用を要求する NAT ポリシーを適用する場合、NAT 制御をイネーブルにできます（**nat-control** コマンドを参照）。

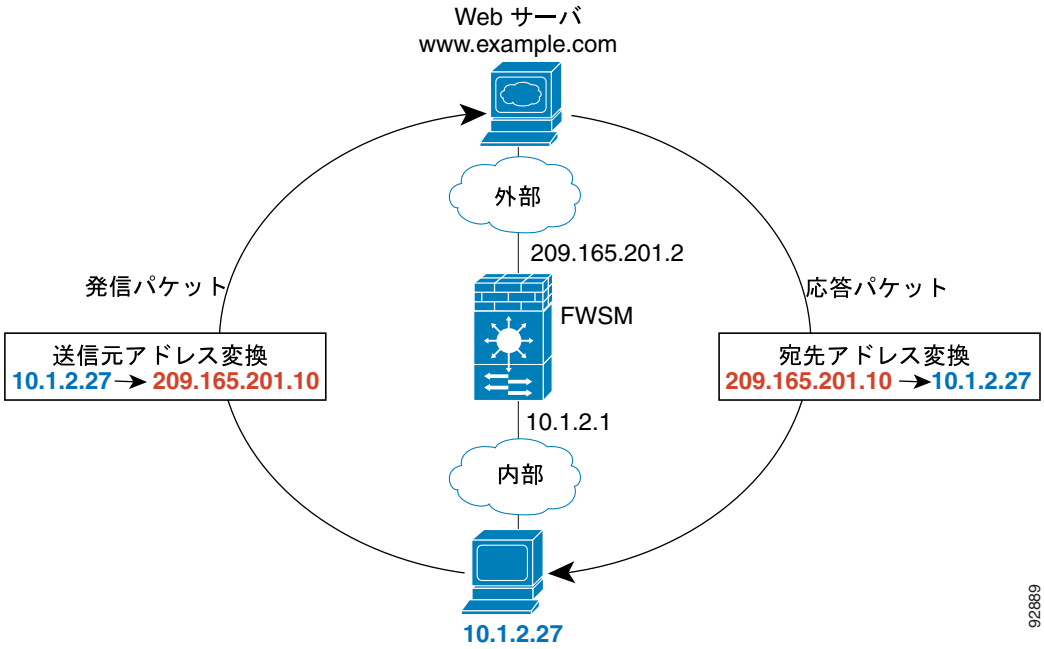
（注）Version 3.1 以前のソフトウェア リリースでは、NAT 制御はデフォルト動作となっていました。FWSM を旧バージョンからアップグレードした場合は、コンフィギュレーションに **nat-control** コマンドが自動的に追加され、予期された動作が保持されます。

NAT の利点の一部は、次のとおりです。

- 内部ネットワーク上でプライベート 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上でルーティングできません。
- NAT は他のネットワークに対してローカル アドレスを隠すので、攻撃側はホストの実アドレスを突き止めることができません。
- NAT は IP アドレスのオーバーラップをサポートすることによって、IP ルーティングに伴う問題を解決します。

図 5-1 に、内部にプライベート ネットワークのある、NAT の一般的な使用例を示します。内部ユーザがインターネット上の Web サーバにパケットを送信すると、そのパケットのローカルな送信元アドレスがルーティング可能なグローバル アドレスに変更されます。応答時、Web サーバはグローバル アドレスに応答を送り、FWSM がパケットを受信します。FWSM はさらに、グローバル アドレスをローカル アドレスに変換してからユーザに送ります。

図 5-1　NAT の例



ルーテッド ファイアウォール モードで FWSM を通過するデータ

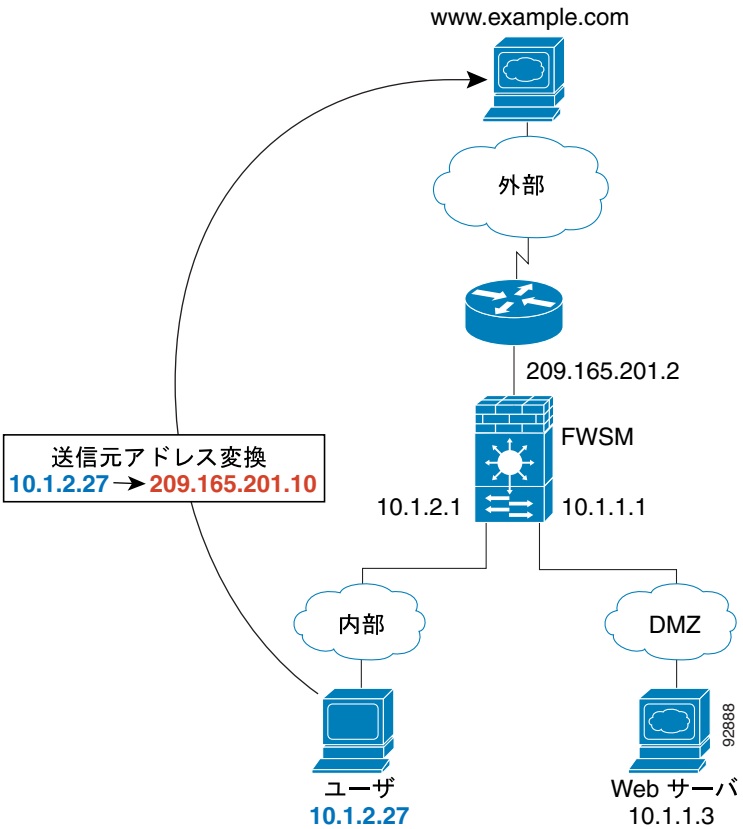
ここでは、ルーテッド ファイアウォール モードにおいて、データが FWSM をどのように通過するかについて説明します。内容は次のとおりです。

- 内部ユーザによる Web サーバ アクセス（p.5-4）
- 外部ユーザによる DMZ 上の Web サーバ アクセス（p.5-5）
- 内部ユーザによる DMZ 上の Web サーバ アクセス（p.5-6）
- 外部ユーザによる内部ホストへのアクセス試行（p.5-7）
- DMZ ユーザによる内部ホストへのアクセス試行（p.5-8）

内部ユーザによる Web サーバ アクセス

図 5-2 に、内部ユーザが外部の Web サーバにアクセスする例を示します。

図 5-2　内部から外部



データが FWSM を通過する順序は、次のとおりです（図 5-2 を参照）。

1. 内部ネットワーク上のユーザが www.example.com に Web ページを要求します。
2. FWSM がパケットを受信します。新しいセッションなので、FWSM はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に基づいて、そのパケットが許可されるかどうかを検証します。

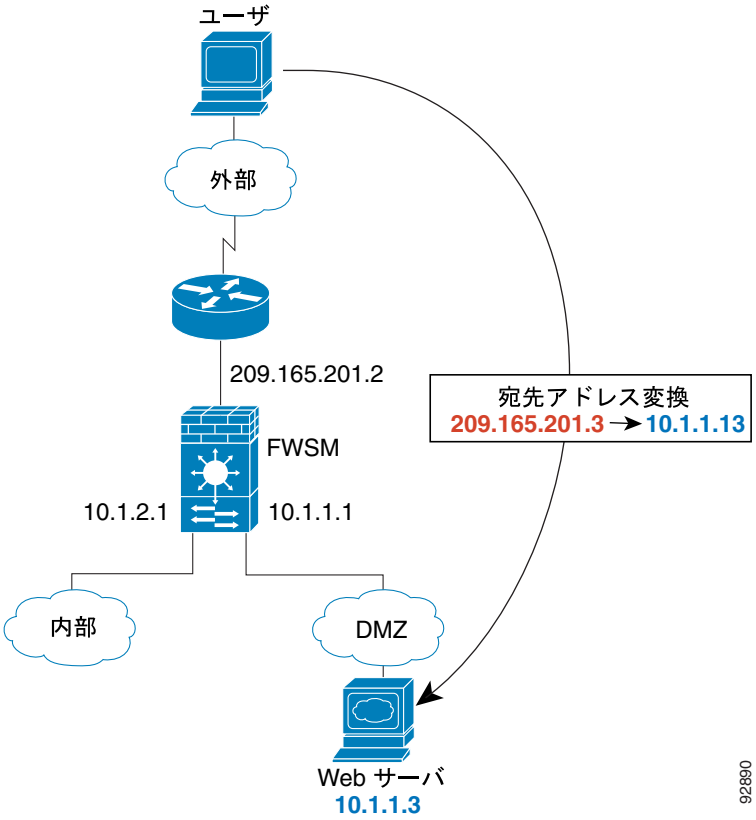
   マルチコンテキスト モードの場合、FWSM はまず固有のインターフェイスまたはコンテキストに対応付けられた固有の宛先アドレスに従ってパケットを分類します。宛先アドレスは、コンテキストのアドレス変換を照合することで対応付けられます。この場合、インターフェイスは固有です。www.example.com の IP アドレスはコンテキストでアドレス変換が行われません。
3. FWSM は、ローカル送信元アドレス（10.1.2.27）をグローバル アドレス 209.165.201.10 に変換します。このグローバル アドレスは外部インターフェイスのサブネット上にあります。

   グローバル アドレスは任意のサブネット上に設定できますが、外部インターフェイスのサブネット上に設定すると、ルーティングが簡素化されます。
4. FWSM はさらに、セッションが確立されたことを記録して、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 FWSM を通過します。すでにセッションが確立されているので、パケットは新しい接続に伴うさまざまな検査をバイパスします。FWSM は NAT を実行し、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 に変換します。
6. FWSM が内部ユーザにパケットを転送します。

外部ユーザによる DMZ 上の Web サーバ アクセス

図 5-3 に、外部ユーザが DMZ 上の Web サーバにアクセスする例を示します。

図 5-3　外部から DMZ



データが FWSM を通過する順序は、次のとおりです（図 5-3 を参照）。

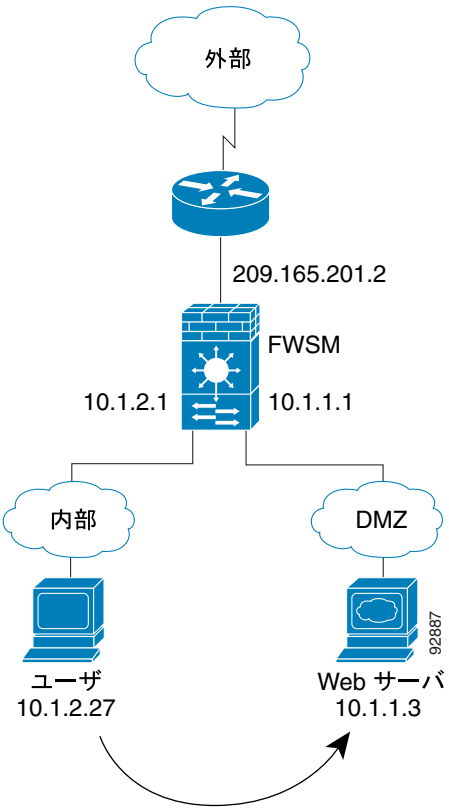
1. 外部ネットワーク上のユーザがグローバル宛先アドレス 209.165.201.3 を使用して、DMZ 上の Web サーバに Web ページを要求します。これは、外部インターフェイスのサブネット上のアドレスです。
2. FWSM がパケットを受信します。新しいセッションなので、FWSM はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に基づいて、そのパケットが許可されるかどうかを検証します。

   マルチコンテキスト モードの場合、FWSM はまず固有のインターフェイスまたはコンテキストに対応付けられた固有の宛先アドレスに従ってパケットを分類します。宛先アドレスは、コンテキストのアドレス変換を照合することで対応付けられます。この場合、分類機能はサーバ アドレス変換によって、DMZ 上の Web サーバのアドレスが特定のコンテキストに属することを「認識」します。
3. FWSM は宛先アドレスをローカル アドレス 10.1.1.3 に変換します。
4. FWSM はさらに、高速パスにセッション エントリを追加し、DMZ インターフェイスからパケットを転送します。
5. DMZ 上の Web サーバが要求に応答すると、パケットは FWSM を通過します。すでにセッションが確立されているので、パケットは新しい接続に伴うさまざまな検査をバイパスします。FWSM は NAT を実行し、ローカル送信元アドレスを 209.165.201.3 に変換します。
6. FWSM が外部ユーザにパケットを転送します。

内部ユーザによる DMZ 上の Web サーバ アクセス

図 5-4 に、内部ユーザが DMZ 上の Web サーバにアクセスする例を示します。

図 5-4　内部から DMZ



データが FWSM を通過する順序は、次のとおりです（図 5-4 を参照）。

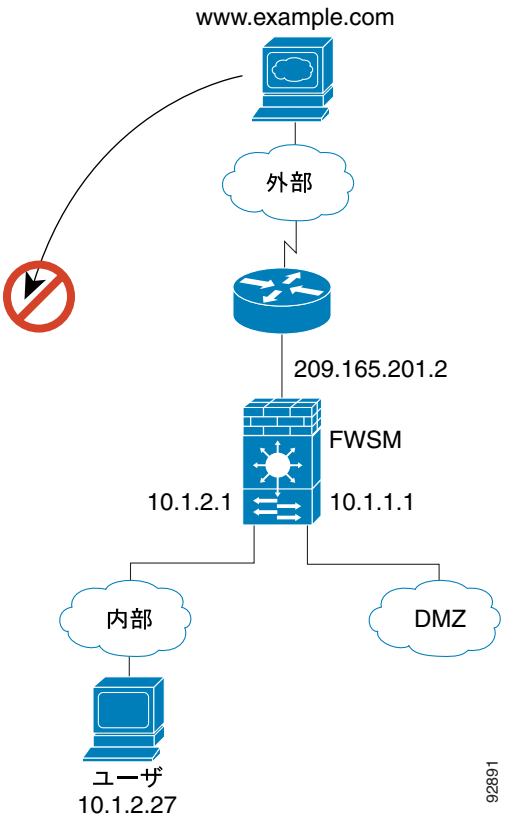
1. 内部ネットワーク上のユーザが宛先アドレス 10.1.1.3 を使用して、DMZ の Web サーバに Web ページを要求します。
2. FWSM がパケットを受信します。新しいセッションなので、FWSM はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に基づいて、そのパケットが許可されるかどうかを検証します。

   マルチコンテキスト モードの場合、FWSM はまず固有のインターフェイスまたはコンテキストに対応付けられた固有の宛先アドレスに従ってパケットを分類します。宛先アドレスは、コンテキストのアドレス変換を照合することで対応付けられます。この場合、インターフェイスは固有です。Web サーバの IP アドレスはアドレス変換が行われません。
3. FWSM はさらに、セッションが確立されたことを記録して、DMZ のインターフェイスからパケットを転送します。
4. DMZ の 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。したがって、パケットは新しい接続に伴うさまざまな検査をバイパスできます。
5. FWSM が内部ユーザにパケットを転送します。

外部ユーザによる内部ホストへのアクセス試行

図 5-5 に、外部ユーザから内部ネットワークにアクセスを試みる例を示します。

図 5-5　外部から内部



データが FWSM を通過する順序は、次のとおりです（図 5-5 を参照）。

1. 外部ネットワーク上のユーザが内部ホストにアクセスしようとしています（ホストにルーティング可能な IP アドレスが与えられているものとします）。

   内部ネットワークでプライベート アドレスを使用している場合、NAT を実行しないかぎり、外部ユーザが内部ネットワークにアクセスすることはできません。外部ユーザは既存の NAT セッションを使用することによって、内部ユーザへのアクセスを試みる可能性があります。

2. FWSM がパケットを受信します。新しいセッションなので、FWSM はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）に基づいて、そのパケットが許可されるかどうかを検証します。

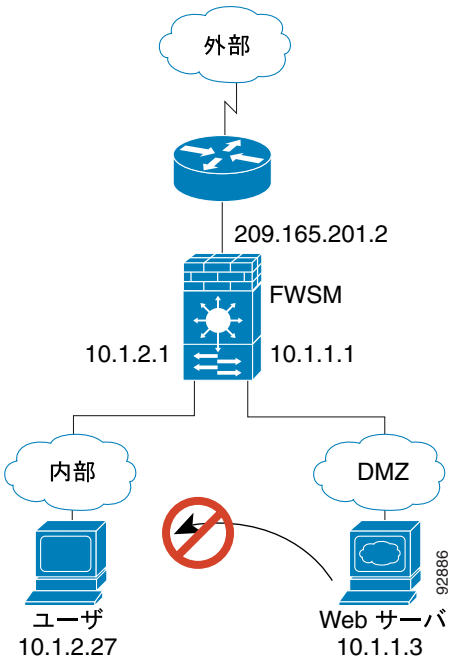
3. パケットが拒否され、FWSM がパケットを廃棄して、接続試行を記録します。

   外部ユーザが内部ネットワークの攻撃を試みている場合、FWSM はさまざまなテクノロジーを駆使し、確立済みの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 ユーザによる内部ホストへのアクセス試行

図 5-6 に、DMZ 上のユーザから内部ネットワークにアクセスを試みる例を示します。

図 5-6　DMZ から内部



データが FWSM を通過する順序は、次のとおりです（図 5-6 を参照）。

1. DMZ　ネットワーク上のユーザが内部ホストにアクセスしようとしています。DMZ　で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ため、プライベート アドレッシング スキームはルーティングを阻止しません。
2. FWSM がパケットを受信します。新しいセッションなので、FWSM はセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）に基づいて、そのパケットが許可されるかどうかを検証します。
3. パケットが拒否され、FWSM がパケットを廃棄して、接続試行を記録します。

透過モードの概要

ここでは、透過ファイアウォール モードについて説明します。内容は次のとおりです。

- 透過ファイアウォールの機能（p.5-9）
- ネットワークでの透過ファイアウォールの使用例（p.5-10）
- 透過ファイアウォールの注意事項（p.5-11）
- 透過モードでサポートされていない機能（p.5-12）
- 透過ファイアウォールを通過するデータ（p.5-13）

透過ファイアウォールの機能

従来のファイアウォールはルーティングされるホップであり、ファイアウォールが保護しているサブネットの 1 つに接続するホストに対して、デフォルト ゲートウェイとして動作します。一方、透過ファイアウォールは、「ワイヤの凹凸」すなわち「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、接続先装置へのルータ ホップとはみなされません。FWSM は内部および外部インターフェイス上の同一ネットワークに接続します。

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、ブリッジ グループと呼ばれる最大 8 つのペアのインターフェイスを設定できます。各ブリッジ グループは別々のネットワークに接続します。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 FWSM 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 FWSM 内の他のブリッジ グループにルーティングされる前に、FWSM から出る必要があります。ブリッジング機能はブリッジ グループごとに別々ですが、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、すべてのブリッジ グループはシステム ログ サーバまたは AAA サーバのコンフィギュレーションを共有します。セキュリティ ポリシーを完全に分離するには、各コンテキストで単一ブリッジ グループのセキュリティ コンテキストを使用します。

透過ファイアウォールはルーティング対象のホップではないので、既存のネットワークに容易に導入できます。IP 再アドレッシングは不要です。複雑なルーティング パターンのトラブルシューティングや NAT 設定が不要なので、メンテナンスが容易です。

透過モードはブリッジとして動作しますが、IP トラフィックなどのレイヤ 3 トラフィックは、拡張アクセス リストで明示的に許可されていないかぎり、FWSM を通過できません。アクセス リストなしに透過ファイアウォールを通過できるトラフィックは、ARP トラフィックだけです。ARP トラフィックは、ARP インスペクションで制御できます。

ルーテッド モードでは、アクセス リストで許可されていても、一部のトラフィック タイプは FWSM を通過できません。ただし、透過ファイアウォールの場合は、拡張アクセス リスト（IP トラフィックの場合）または EtherType アクセス リスト（IP 以外のトラフィックの場合）のどちらかを使用することによって、あらゆるトラフィックを通過させることができます。

（注） 透過モードの場合、CDP パケット、または 0x600 以上の有効な EtherType を持たないパケットはすべて FWSM を通過できません。たとえば、IS-IS パケットは通過できません。BPDU に対しては例外が設定されています。

たとえば、透過ファイアウォールをまたいでルーティング プロトコルの隣接関係を確立できます。拡張アクセス リストに基づいて、OSPF、RIP、EIGRP、または BGP トラフィックを通過させることができます。同様に、HSRP または VRRP などのプロトコルも FWSM を通過できます。特定のトラフィックを許可する処理については、表 10-2（p.10-8）を参照してください。

EtherType アクセス リストを使用することによって、IP 以外のトラフィック（AppleTalk、IPX、BPDU、MPLS など）を通過させるように設定できます。

透過ファイアウォールで直接サポートされていない機能については、アップストリーム ルータおよびダウンストリーム 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できます。たとえば、拡張アクセス リストを使用して、DHCP トラフィック（サポート対象外の 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 トラフィックの通過を許可できます。

FWSM が透過モードで稼働している場合、パケットの発信インターフェイスはルート検索ではなく、MAC アドレス検索を実行することによって判別されます。ルート ステートメントも設定できますが、適用されるのは FWSM を起点とするトラフィックだけです。たとえば、Syslog サーバがリモート ネットワークに配置されている場合、FWSM がそのサブネットにアクセスできるように、スタティック ルートを使用する必要があります。

ネットワークでの透過ファイアウォールの使用例

図 5-7 に、外部デバイスが内部デバイスと同一サブネット上にある、標準的な透過ファイアウォール ネットワークを示します。内部ルータと内部ホストは、見かけ上、外部ルータに直接接続されています。

図 5-7　透過ファイアウォール ネットワーク

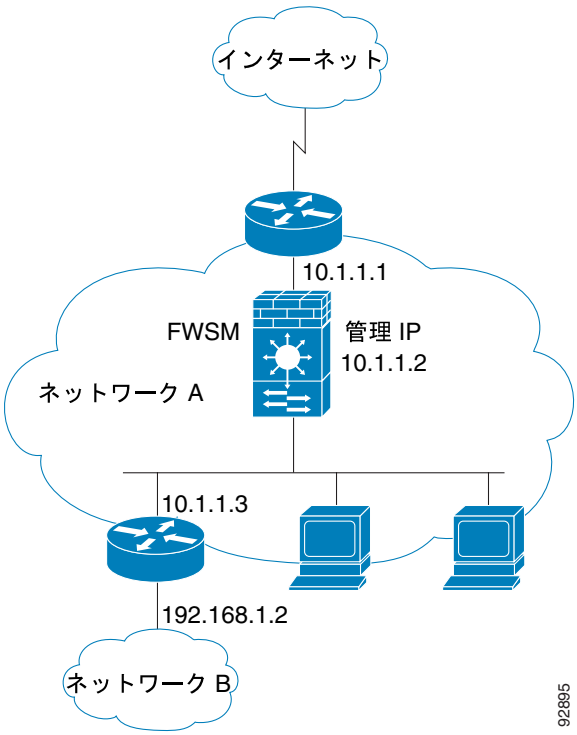
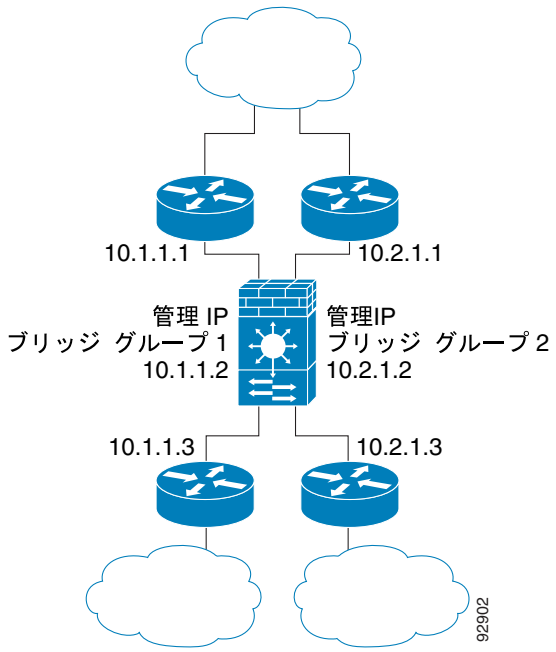


図 5-8 に、2 つのブリッジ グループを持つ、FWSM に接続されている 2 つのネットワークを示します。

図 5-8　2 つのブリッジ グループを持つ透過ファイアウォール ネットワーク



透過ファイアウォールの注意事項

透過ファイアウォール ネットワークを計画するときの注意事項は、次のとおりです。

- 各ブリッジ グループに管理 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、透過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。FWSM はシステム メッセージ、AAA 通信など、FWSM 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。

  管理用 IP アドレスは、接続先ネットワークと同じサブネット上になければなりません。管理 IP サブネットの詳細については、「IP アドレスのブリッジ グループへの割り当て」（p.6-7）を参照してください。
- 各ブリッジ グループは、内部インターフェイスと外部インターフェイスだけを使用します。
- 直接接続された各ネットワークは、同一サブネット上になければなりません。
- ブリッジ グループの管理用 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。デバイスには、FWSM の反対側にあるルータをデフォルト 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、透過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のみ適用されます。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。

- マルチコンテキスト モードの場合、コンテキストごとに異なるインターフェイスを使用する必要があります。複数のコンテキスト間で同じ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 モードの場合、各コンテキストは一般に異なるサブネットを使用します。オーバーラップするサブネットを使用することはできますが、ルーティングの見地から重複サブネットを可能にするようにルータと NAT を設定したネットワーク トポロジーが必要です。
- 拡張アクセス リストを使用して、IP トラフィックなどのレイヤ 3 トラフィックが FWSM を通過できるようにしなければなりません。

  任意で EtherType アクセス リストを使用することによって、IP 以外のトラフィックを通過させることもできます。

透過モードでサポートされていない機能

透過モードでは、次の機能はサポートされていません。

- NAT

  NAT はアップストリーム ルータで実行します。
- ダイナミック ルーティング プロトコル

  ただし、FWSM を発信元とするトラフィックのスタティック ルートを追加できます。拡張アクセス リストを使用して、ダイナミック ルーティング プロトコルが FWSM を通過できるようにすることもできます。
- ブリッジ グループ IP アドレスの IPv6。ただし、EtherType アクセス リストを使用して IPv6 EtherType を通過させることはできます。
- DHCP リレー

  透過ファイアウォールは DHCP サーバとして機能することはできますが、DHCP リレー コマンドはサポートしません。拡張アクセス リストを使用して DHCP トラフィックを通過させることができるため、DHCP リレーは必要ありません。
- マルチキャスト

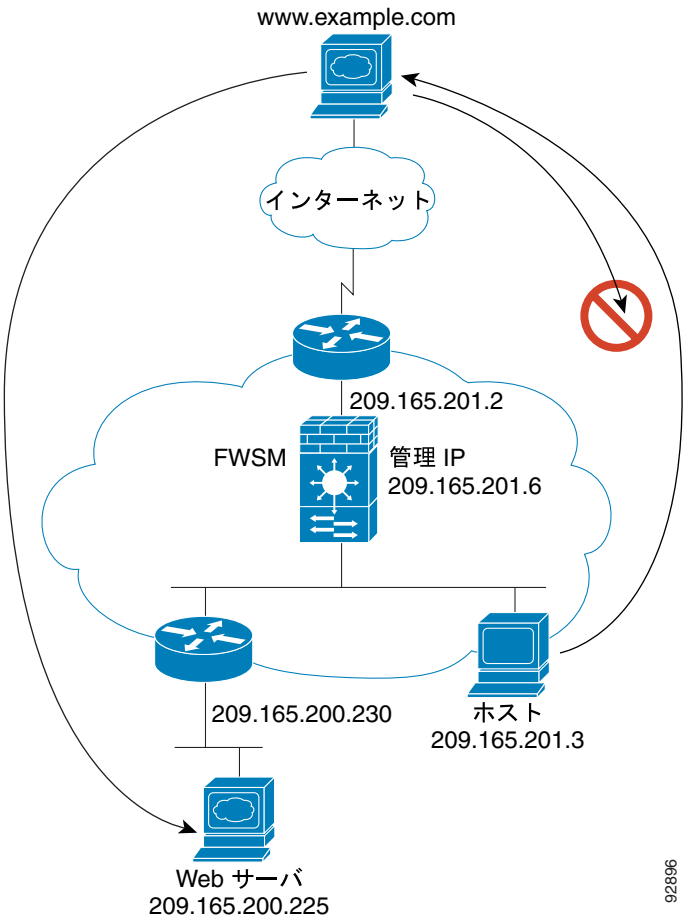
  ただし、拡張アクセス リストで許可することで、マルチキャスト トラフィックが FWSM を通過できるようにすることはできます。
- 管理用リモート アクセス VPN

  管理のためにサイト間 VPN を使用できます。

透過ファイアウォールを通過するデータ

図5-9 に、内部ネットワークにパブリック Web サーバが配置されている状況で、透過ファイアウォールを使用する一般的な宅装例を示します。FWSM には、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にするアクセス リストが 1 つ設定されています。さらに、もう 1 つのアクセス リストで、外部ユーザが内部ネットワーク上の Web サーバに限ってアクセスできるようにしています。

図 5-9　一般的な透過ファイアウォールのデータ パス



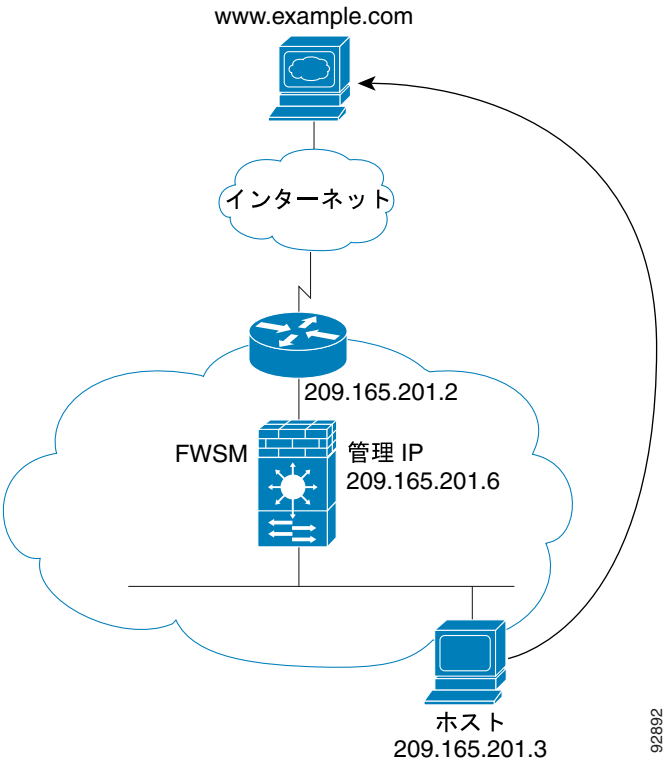
ここでは、データが FWSM をどのように通過するかについて説明します。内容は次のとおりです。

- 内部ユーザによる Web サーバ アクセス（p.5-14）
- 外部ユーザによる内部ネットワーク上の Web サーバ アクセス（p.5-15）
- 外部ユーザによる内部ホストへのアクセス試行（p.5-16）

内部ユーザによる Web サーバ アクセス

図 5-10 に、内部ユーザが外部の Web サーバにアクセスする例を示します。

図 5-10　内部から外部



データが FWSM を通過する順序は、次のとおりです（図 5-10 を参照）。

1. 内部ネットワーク上のユーザが www.example.com に Web ページを要求します。
2. FWSM はパケットを受信し、必要に応じて送信元 MAC アドレスを MAC アドレス テーブルに追加します。新しいセッションなので、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に基づいて、そのパケットが許可されるかどうかを検証します。

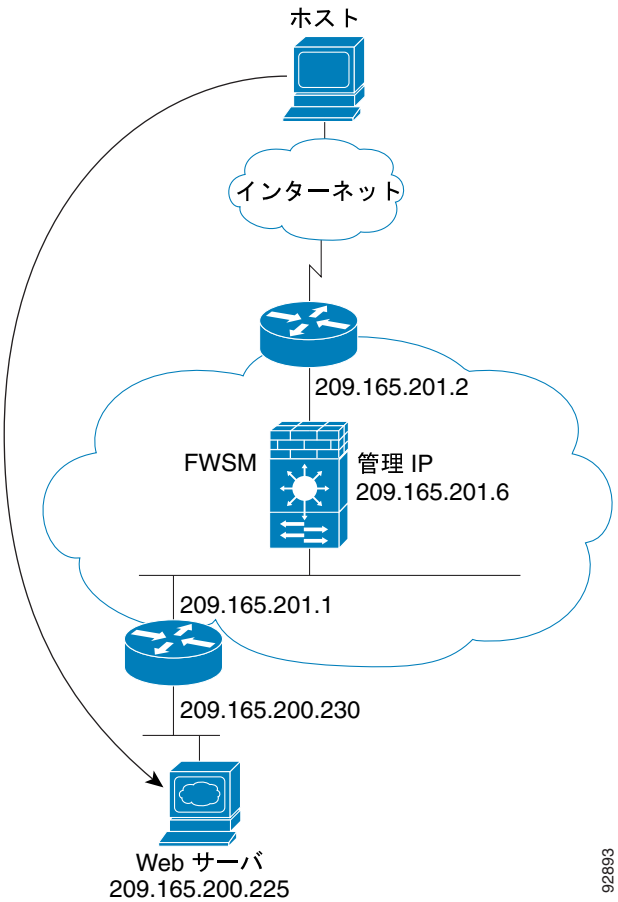
   マルチコンテキスト モードの場合、FWSM はまず固有のインターフェイスに応じてパケットを分類します。
3. FWSM がセッションの確立を記録します。
4. 宛先 MAC アドレスが MAC アドレス テーブルに含まれている場合、FWSM は外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータのアドレス 209.186.201.2 です。

   宛先 MAC アドレスが FWSM のテーブルに含まれていない場合、FWSM は ARP 要求を送信し、ping を実行することによって、MAC アドレスを突き止めようとします。最初のパケットは廃棄されます。
5. Web サーバが要求に応答すると、FWSM は必要に応じて Web サーバ MAC アドレスを MAC アドレス テーブルに追加します。すでにセッションが確立されているので、パケットは新しい接続に伴うさまざまな検査をバイパスします。
6. FWSM が内部ユーザにパケットを転送します。

外部ユーザによる内部ネットワーク上の Web サーバ アクセス

図 5-11 に、外部ユーザが内部の Web サーバにアクセスする例を示します。

図 5-11　外部から内部



データが FWSM を通過する順序は、次のとおりです（図 5-11 を参照）。

1. 外部ネットワーク上のユーザが内部の Web サーバに Web ページを要求します。
2. FWSM はパケットを受信し、必要に応じて送信元 MAC アドレスを MAC アドレス テーブルに追加します。新しいセッションなので、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に基づいて、そのパケットが許可されるかどうかを検証します。

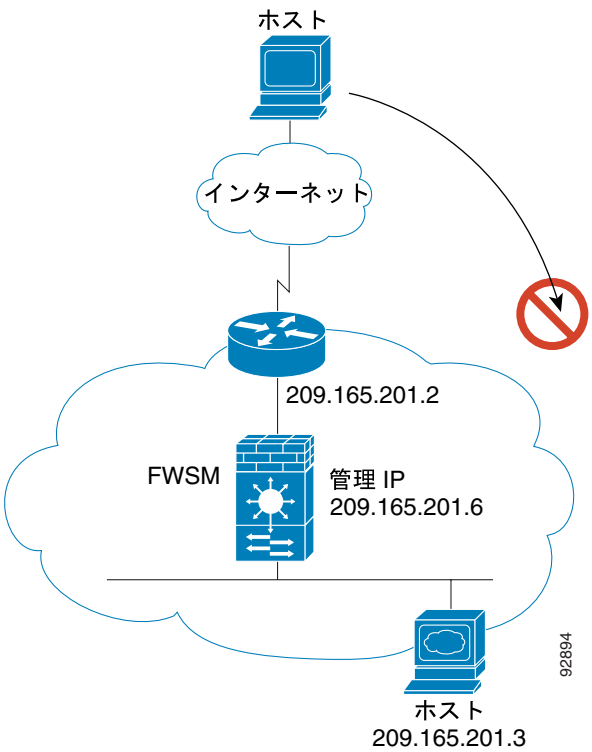
   マルチコンテキスト モードの場合、FWSM はまず固有のインターフェイスに応じてパケットを分類します。
3. FWSM がセッションの確立を記録します。
4. 宛先 MAC アドレスが MAC アドレス テーブルに含まれている場合、FWSM は内部インターフェイスからパケットを転送します。宛先 MAC アドレスは、ダウンストリーム ルータのアドレス 209.186.201.1 です。

   宛先 MAC アドレスが FWSM のテーブルに含まれていない場合、FWSM は ARP 要求を送信し、ping を実行することによって、MAC アドレスを突き止めようとします。最初のパケットは廃棄されます。
5. Web サーバが要求に応答すると、FWSM は必要に応じて Web サーバ MAC アドレスを MAC アドレス テーブルに追加します。すでにセッションが確立されているので、パケットは新しい接続に伴うさまざまな検査をバイパスします。
6. FWSM が外部ユーザにパケットを転送します。

外部ユーザによる内部ホストへのアクセス試行

図 5-12 に、外部ユーザから内部ネットワーク上のホストにアクセスを試みる例を示します。

図 5-12　外部から内部



データが FWSM を通過する順序は、次のとおりです（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アクセスしようとしています。
2. FWSM はパケットを受信し、必要に応じて送信元 MAC アドレスを MAC アドレス テーブルに追加します。新しいセッションなので、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に基づいて、そのパケットが許可されるかどうかを検証します。

   マルチコンテキスト モードの場合、FWSM はまず固有のインターフェイスに応じてパケットを分類します。
3. パケットが拒否され、FWSM がパケットを廃棄します。
4. 外部ユーザが内部ネットワークの攻撃を試みている場合、FWSM はさまざまなテクノロジーを駆使し、確立済みの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。

透過ファイアウォール モードまたはルーテッド ファイアウォール モードの設定

ルーテッド ファイアウォール モード（デフォルト）または透過ファイアウォール モードで動作するように、各コンテキストを設定できます。

モードを変更すると、FWSM によってコンフィギュレーションが消去されます。両方のモードでサポートされるコマンドは少ないからです。入力済みのコンフィギュレーションがすでにある場合は、必ず、モードを変更する前にコンフィギュレーションのバックアップを行ってください。新しいコンフィギュレーションを作成するときに、このバックアップを参照できます。

firewall transparent コマンドでモードを変更するテキスト コンフィギュレーションを FWSM にダウンロードする場合は、必ず、コンフィギュレーションの先頭にこのコマンドを指定してください。FWSM はコマンドを読み取るとただちにモードを変更し、そのあとでダウンロードされたコンフィギュレーションの残りを読み取ります。コンフィギュレーションの後ろの方にこのコマンドが指定されていると、FWSM はコンフィギュレーションのそこまでの行をすべて消去します。

- モードを透過的に設定するには、各コンテキストに次のコマンドを入力します。

  ```
  hostname(config)# firewall transparent
  ```

- モードをルーテッドに設定するには、各コンテキストに次のコマンドを入力します。

  ```
  hostname(config)# no firewall transparent
  ```

インターフェイス パラメータの設定

この章では、各インターフェイスに名前、セキュリティ レベル、IP アドレスを設定する方法について説明します。さらに透過ファイアウォールでは、各インターフェイスのペアにブリッジ グループの設定が必要です。

この章で説明する内容は、次のとおりです。

- セキュリティ レベルの概要（p.6-2）
- ルーテッド ファイアウォール モードのインターフェイスの設定（p.6-3）
- 透過ファイアウォール モードのインターフェイスの設定（p.6-5）
- 同じセキュリティ レベルのインターフェイス間の通信の許可（p.6-8）
- インターフェイスのオン / オフ（p.6-8）

セキュリティ レベルの概要

各インターフェイスに 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、最もセキュアにする必要があるネットワークには、レベル 100 を割り当てる必要があります。一方、インターネットに接続する外部ネットワークのレベルは 0 でかまいません。DMZ などその他のネットワークは範囲内の任意のレベルにできます。同じセキュリティ レベルに複数のインターフェイスを割り当てることもできます。詳細については、「同じセキュリティ レベルのインターフェイス間の通信の許可」（p.6-8）を参照してください。

このレベルでは、次の動作を制御します。

- インスペクション エンジン — 一部のインスペクション エンジンはセキュリティ レベルに依存します。同一セキュリティ レベルのインターフェイスの場合、インスペクション エンジンはどちらの方向のトラフィックにも適用されます。
  - NetBIOS インスペクション エンジン — 発信接続だけに適用されます。
  - OraServ インスペクション エンジン — ホスト ペア間に OraServ ポート用の制御接続がある場合、着信データ接続だけが FWSM の通過を許可されます。
- フィルタリング — HTTP（S）および FTP フィルタリングは発信接続にのみ適用されます。同一セキュリティ レベルのインターフェイスの場合、どちらの方向のトラフィックもフィルタリングできます。
- NAT 制御 — NAT 制御をイネーブルにする場合、セキュリティの高いインターフェイス（内部）上のホストがセキュリティの低いインターフェイス（外部）上のホストにアクセスするときに NAT 制御を設定する必要があります。

  NAT 制御を行わない場合、または同一セキュリティ レベルのインターフェイスの場合、すべてのインターフェイス間で NAT を使用することも、NAT を使用しないことも選択できます。外部インターフェイスに NAT を設定する場合は、特別なキーワードが必要となります。
- **established** コマンド — このコマンドを使用すると、セキュリティ レベルが上位のホストから下位のホストへの接続がすでに確立されている場合に、下位のホストから上位のホストへの戻り接続が可能になります。

  同一セキュリティ レベルのインターフェイスの場合、どちらの方向にも **established** コマンドを設定できます。

ルーテッド ファイアウォール モードのインターフェイスの設定

トラフィックに FWSM の通過を許可するには、事前にインターフェイス名と IP アドレスを設定しておく必要があります。また、セキュリティ レベルをデフォルトの 0 から変更する必要があります。インターフェイスに「内部」という名前を付けて、セキュリティ レベルを明示的に設定しない場合、セキュリティ レベルは 100 に設定されます。

(注) フェールオーバーを使用する場合、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用に確保するインターフェイスには、ここで紹介する手順で名前を設定しないでください。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 13 章「フェールオーバーの設定」を参照してください。

マルチコンテキスト モードに関する注意事項は、次のとおりです。

- 各コンテキスト内でコンテキスト インターフェイスを設定します。
- 設定できるのは、システム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- フェールオーバー インターフェイスはシステム コンフィギュレーションでのみ設定可能です。この手順ではフェールオーバー インターフェイスは設定しないでください。詳細については、第 13 章「フェールオーバーの設定」を参照してください。
- インターフェイスのセキュリティ レベルを変更し、既存の接続がタイムアウトする前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、接続を消去します。

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 FWSM に割り当てられた VLAN だけです。**show vlan** コマンドを使用して、FWSM に割り当てられたすべての VLAN を表示します。

インターフェイスを設定するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、設定するインターフェイスを指定します。

```
hostname(config)# interface {vlan number | mapped_name}
```

マルチコンテキスト モードの場合、マップ名が **allocate-interface** コマンドを使用して割り当てられていれば、そのマップ名を入力します。

コマンドの入力例を示します。

```
hostname(config)# interface vlan 101
```

ステップ 2　次のコマンドを入力して、インターフェイスに名前を付けます。

```
hostname(config-if)# nameif name
```

name は最大 48 文字の文字列です。大文字と小文字は区別されません。名前を変更する場合は、新しい値を使用してコマンドを再入力します。**no** 形式での入力は行わないでください。この名前を参照するすべてのコマンドが削除されます。

（注） インターフェイスの名前を設定すると、セキュリティ レベルは自動的に 0 に変更されます。ただし、名前が「内部」の場合、セキュリティ レベルは 100 になります。

ステップ 3　次のコマンドを入力して、セキュリティ レベルを設定します。

```
hostname(config-if)# security-level number
```

number は、0（最小）～ 100（最大）の整数です。

ステップ 4　次のコマンドを入力して、IP アドレスを設定します。

```
hostname(config-if)# ip address ip_address [mask] [standby ip_address]
```

フェールオーバーには、**standby** キーワードとアドレスを使用します。詳細については、第 13 章「フェールオーバーの設定」を参照してください。

（注） IPv6 アドレスの設定については、「インターフェイス上での IPv6 の設定」（p.9-3）を参照してください。

次に、VLAN 101 のパラメータの設定例を示します。

```
hostname(config)# interface vlan 101
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(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。

```
hostname/contextA(config)# interface int1
hostname/contextA(config-if)# nameif outside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

透過ファイアウォール モードのインターフェイスの設定

トラフィックに FWSM の通過を許可するには、事前にインターフェイス名、セキュリティ レベル、およびブリッジ グループ アソシエーションを設定しておく必要があります。最後に、各ブリッジ グループに管理 IP アドレスを割り当てます。ここでは、次の内容について説明します。

- 透過ファイアウォール インターフェイスのパラメータの設定（p.6-5）
- IP アドレスのブリッジ グループへの割り当て（p.6-7）

透過ファイアウォール インターフェイスのパラメータの設定

透過ファイアウォールは内部および外部インターフェイス上の同一ネットワークに接続します。インターフェイスの各ペアはブリッジ グループに属します。このブリッジ グループには管理 IP アドレスを割り当てる必要があります（「IP アドレスのブリッジ グループへの割り当て」[p.6-7] を参照）。2 つのインターフェイスそれぞれに、8 つまでブリッジ グループを設定できます。各ブリッジ グループは別々のネットワークに接続します。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 FWSM 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 FWSM 内の他のブリッジ グループにルーティングされる前に、FWSM から出る必要があります。

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、複数のブリッジ グループを使用できます。ブリッジング機能はブリッジ グループごとに別々ですが、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、すべてのブリッジ グループはシステム ログ サーバまたは AAA サーバのコンフィギュレーションを共有します。セキュリティ ポリシーを完全に分離するには、各コンテキストで単一ブリッジ グループのセキュリティ コンテキストを使用します。

（注） フェールオーバーを使用する場合、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用に確保するインターフェイスには、ここで紹介する手順で名前を設定しないでください。

マルチコンテキスト モードでのインターフェイスの設定に関する注意事項は、次のとおりです。

- 各コンテキスト内でコンテキスト インターフェイスを設定します。
- 設定できるのは、システム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- フェールオーバー インターフェイスはシステム コンフィギュレーションでのみ設定可能です。この手順ではフェールオーバー インターフェイスは設定しないでください。
- インターフェイスのセキュリティ レベルを変更し、既存の接続がタイムアウトする前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、接続を消去します。

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 FWSM に割り当てられた VLAN だけです。**show vlan** コマンドを使用して、FWSM に割り当てられたすべての VLAN を表示します。

インターフェイスをブリッジ グループに割り当てるには、名前とセキュリティ レベルを設定して、次の手順を実行します。

ステップ 1　次のコマンドを入力して、インターフェイスを識別します。

```
hostname(config)# interface {vlan number | mapped_name}
```

マルチコンテキスト モードの場合、マップ名が **allocate-interface** コマンドを使用して割り当てられていれば、そのマップ名を入力します。

ステップ 2　次のコマンドを入力して、インターフェイスをブリッジ グループに割り当てます。

```
hostname(config-if)# bridge-group number
```

number は 1 ～ 100 の整数です。1 つのブリッジ グループには 2 つのインターフェイスしか割り当てることができません。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　次のコマンドを入力して、インターフェイスに名前を付けます。

```
hostname(config-if)# nameif name
```

name は最大 48 文字の文字列です。大文字と小文字は区別されません。名前を変更する場合は、新しい値を使用してコマンドを再入力します。**no** 形式での入力は行わないでください。この名前を参照するすべてのコマンドが削除されます。インターフェイスに「内部」という名前を付けて、セキュリティ レベルを明示的に設定しない場合、セキュリティ レベルは 100 に設定されます。

ステップ 4　次のコマンドを入力して、セキュリティ レベルを設定します。

```
hostname(config-if)# security-level number
```

number は、0（最小）～ 100（最大）の整数です。デフォルトでは、インターフェイスに名前を付けると、セキュリティ レベルは 0 になります。

IP アドレスのブリッジ グループへの割り当て

透過ファイアウォールは、IP ルーティングに参加しません。FWSM に必要な IP 設定は、各ブリッジ グループに管理 IP アドレスを設定することだけです。このアドレスが必要なのは、FWSM がシステム メッセージ、AAA サーバとの通信など、FWSM が発信元となるトラフィックの送信元アドレスとしてこのアドレスを使用するからです。リモート管理アクセスにこのアドレスを使用することもできます。

管理 IP アドレスを設定するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、ブリッジ グループを識別します。

```
hostname(config)# interface bvi bridge_group_number
```

ステップ 2　次のコマンドを入力して、IP アドレスを指定します。

```
hostname(config-if)# ip address ip_address [mask] [standby ip_address]
```

透過ファイアウォールにホスト アドレス（/32 または 255.255.255.255）を割り当てないでください。また、/30 サブネットなど（255.255.255.252）、ホスト アドレスが 3 つ未満（アップストリーム ルータ、ダウンストリーム ルータ、透過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。FWSM は、サブネットの最初と最後のアドレスへの（またはアドレスからの）すべての ARP パケットを廃棄します。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、FWSM 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 要求を廃棄します。

フェールオーバーには、**standby** キーワードとアドレスを使用します。詳細については、第 13 章「フェールオーバーの設定」を参照してください。

次に、VLAN 300 および 301 をブリッジ グループ 1 に割り当てて、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。

```
hostname(config)# interface vlan 300
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# bridge-group 1
hostname(config-if)# interface vlan 301
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# bridge-group 1
hostname(config-if)# interface bvi 1
hostname(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

同じセキュリティ レベルのインターフェイス間の通信の許可

デフォルトでは、同一セキュリティ レベルのインターフェイスは相互に通信できません。同一セキュリティ レベルのインターフェイス間での通信を許可すると、101 を超える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レベルを使用し、同一セキュリティ レベルにインターフェイスを割り当てない場合、1 つのレベル（0 ～ 100）に 1 つのインターフェイスのみ設定できます。

（注） NAT 制御をイネーブルにする場合、同一セキュリティ レベルのインターフェイス間では NAT を設定する必要がありません。NAT および同一セキュリティ レベルのインターフェイスの詳細については、「NAT および同一セキュリティ レベルのインターフェイス」（p.12-13）を参照してください。

セキュリティ レベルが同じインターフェイス間で通信できるようにした場合でも、通常どおり、さまざまなセキュリティ レベルでインターフェイスを設定できます。

同じセキュリティ レベルのインターフェイスが相互に通信できるようにするには、次のコマンドを入力します。

```
hostname(config)# same-security-traffic permit inter-interface
```

この設定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。

インターフェイスのオン / オフ

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。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、影響を受けるのは、そのコンテキストのインターフェイスだけです。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 VLAN インターフェイスに影響します。

インターフェイスをディセーブルにする、または再度イネーブルにする手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、インターフェイス コンフィギュレーション モードを開始します。

```
hostname(config)# interface {vlan number | mapped_name}
```

マルチコンテキスト モードの場合、マップ名が **allocate-interface** コマンドを使用して割り当てられていれば、そのマップ名を入力します。

ステップ 2　次のコマンドを入力して、インターフェイスをディセーブルにします。

```
hostname(config)# shutdown
```

ステップ 3　次のコマンドを入力して、インターフェイスを再度イネーブルにします。

```
hostname(config)# no shutdown
```

基本設定

ここでは、設定を機能させるために FWSM で通常必要な基本設定について説明します。この章で説明する内容は、次のとおりです。

- パスワードの変更（p.7-2）
- ホスト名の設定（p.7-5）
- ドメイン名の設定（p.7-5）
- プロンプトの設定（p.7-6）
- ログイン バナーの設定（p.7-7）
- 透過ファイアウォール モードと NAT を設定しない場合の接続制限の設定（p.7-8）

パスワードの変更

ここでは、ログイン パスワードとイネーブル パスワードの変更方法について説明します。内容は次のとおりです。

- ログイン パスワードの変更（p.7-2）
- イネーブル パスワードの変更（p.7-2）
- メンテナンス ソフトウェア パスワードの変更（p.7-3）

（注） マルチコンテキスト　モードでは、各コンテキストとシステム実行スペースに、それぞれ専用のログイン ポリシーおよびパスワードがあります。

ログイン パスワードの変更

ログイン パスワードは、スイッチからのセッションおよび Telnet 接続と SSH 接続に使用します。デフォルトのログイン パスワードは、「cisco」です。パスワードを変更するには、次のコマンドを入力します。

```
hostname(config)# {passwd | password} password
```

passwd または **password** を入力できます。*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以外、任意の文字を使用できます。

パスワードは暗号化されて設定に保存されるので、入力後に元のパスワードを表示することはできません。パスワードをデフォルトの設定に戻す場合は、**no password** コマンドを使用します。

イネーブル パスワードの変更

イネーブル パスワードを使用すると、イネーブル EXEC モードを開始できます。デフォルトのイネーブル パスワードは、ブランクです。イネーブル パスワードを変更するには、次のコマンドを入力します。

```
hostname(config)# enable password password
```

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以外、任意の文字を使用できます。

このコマンドによって、最上位の権限レベルに対応するパスワードが変更されます。ローカルなコマンド許可を設定する場合は、0 ～ 15 の各権限レベルにイネーブル パスワードを設定できます。

パスワードは暗号化されて設定に保存されるので、入力後に元のパスワードを表示することはできません。パスワードを指定しないで **enable password** コマンドを入力すると、パスワードがデフォルトのブランクに設定されます。

メンテナンス ソフトウェア パスワードの変更

メンテナンス ソフトウェアは、トラブルシューティングに役立ちます。メンテナンス ソフトウェアから、たとえば、アプリケーション パーティションに新しいソフトウェアをインストールしたり、パスワードをリセットしたり、クラッシュ ダンプ情報を表示したりできます。メンテナンス ソフトウェアにアクセスする唯一の方法は、FWSM とのセッションを開始することです。

メンテナンス ソフトウェアには、アクセス権限の異なる 2 つのユーザ レベルがあります。

- root — ネットワーク パーティション パラメータの設定、アプリケーション パーティション上のソフトウェア イメージのアップグレード、ゲスト アカウント パスワードの変更、およびゲスト アカウントのイネーブル化またはディセーブル化を実行できます。

  デフォルトのパスワードは、「cisco」です。
- guest — ネットワーク パーティション パラメータを設定し、クラッシュ ダンプ情報を表示できます。

  デフォルトのパスワードは、「cisco」です。

両方のユーザのメンテナンス パーティション パスワードを変更する手順は、次のとおりです。

ステップ 1　スイッチのプロンプトに次のコマンドを入力して、メンテナンス パーティションで FWSM を再起動します。

```
Router# hw-module module mod_num reset cf:1
```

ステップ 2　次のコマンドを入力して、FWSM とのセッションを確立します。

```
Router# session slot mod_num processor 1
```

ステップ 3　次のコマンドを入力して、root としてログインします。

```
Login: root
```

ステップ 4　プロンプトにパスワードを入力します。

```
Password:
```

デフォルトのパスワードは、「cisco」です。

ステップ 5　次のコマンドを入力して、root パスワードを変更します。

```
root@localhost# passwd
```

ステップ 6　プロンプトに新しいパスワードを入力します。

```
Changing password for user root
New password:
```

ステップ 7　新しいパスワードを再入力します。

```
Retype new password:
passwd: all authentication tokens updated successfully
```

ステップ 8　次のコマンドを入力して、guest パスワードを変更します。

```
root@localhost# passwd-guest
```

ステップ 9　プロンプトに新しいパスワードを入力します。

```
Changing password for user guest
New password:
```

ステップ 10　新しいパスワードを再入力します。

```
Retype new password:
passwd: all authentication tokens updated successfully
```

次に、root アカウントのパスワードを設定する例を示します。

```
root@localhost# passwd
Changing password for user root
New password: *sh1p
Retype new password: *sh1p
passwd: all authentication tokens updated successfully
```

次に、guest アカウントのパスワードを設定する例を示します。

```
root@localhost# passwd-guest
Changing password for user guest
New password: f1rc8t
Retype new password: f1rc8t
passwd: all authentication tokens updated successfully
```

ホスト名の設定

FWSM にホスト名を設定すると、その名前がコマンドライン プロンプトに表示されます。複数のデバイスとセッションを確立する場合は、ホスト名によって、コマンドの入力先を識別しやすくなります。

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 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。

FWSM 用のホスト名なのか、コンテキスト用のホスト名なのかを指定するには、次のコマンドを入力します。

```
hostname(config)# hostname name
```

名前に使用できる文字数は最大 63 文字です。ホスト名は始めと終わりは英字または数字でなければなりません。中間の文字として使用できるのは英字、数字、またはハイフンだけです。

この名前はコマンドライン プロンプトに表示されます。次に例を示します。

```
hostname(config)# hostname farscape
farscape(config)#
```

ドメイン名の設定

FWSM には非修飾名の接尾辞としてドメイン名が付けられます。たとえば、ドメイン名を「example.com」に設定し、syslog サーバに非修飾名「jupiter」を指定する場合、FWSM には「jupiter.example.com」という名前が与えられます。

デフォルトのドメイン名は default.domain.invalid です。

マルチコンテキスト モードの場合、各コンテキストにドメイン名を設定できます。また、システム実行スペースでもドメイン名を設定できます。

FWSM のドメイン名を指定するには、次のコマンドを入力します。

```
hostname(config)# domain-name name
```

たとえば、ドメインを example.com として設定する場合、次のコマンドを入力します。

```
hostname(config)# domain-name example.com
```

プロンプトの設定

ホスト名、コンテキスト名、ドメイン名、スロット、フェールオーバー ステータス、フェールオーバー プライオリティなどの CLI プロンプトに表示される情報を設定できます。マルチコンテキスト モードでは、システム実行スペースまたは管理（admin）コンテキストへのログイン時に拡張プロンプトを表示できます。管理（admin）以外のコンテキストでは、ホスト名とコンテキスト名を示すデフォルト プロンプトのみが表示されます。

プロンプトに含める情報を設定するには、次のコマンドを入力します。

```
hostname(config)# prompt [hostname] [context] [domain] [slot] [state] [priority]
```

キーワードを入力する順序によって、プロンプト内の要素の順序が決まります。各要素はスラッシュ（/）で区切られます。各キーワードについては、次の説明を参照してください。

- **hostname** ― ホスト名を表示します。
- **domain** ― ドメイン名を表示します。
- **context** ― （マルチモード限定）現在のコンテキストを表示します。
- **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）で表示します。プライオリティは **failover lan unit** コマンドを使用して設定します。
- **slot** ― スイッチ内のスロットの位置を表示します。
- **state** ― 装置のトラフィック転送ステートを表示します。**state** キーワードには、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、装置はトラフィックをアクティブに転送しています。
  - stby ― フェールオーバーはイネーブルで、装置はトラフィックを転送しておらず、ステートはスタンバイ、失敗、またはその他の非アクティブ ステートです。
  - actNoFailover ― フェールオーバーはイネーブルではなく、装置はトラフィックをアクティブに転送しています。
  - stbyNoFailover ― フェールオーバーはイネーブルではなく、装置はトラフィックを転送していません。これは、スタンバイ ユニットのインターフェイス障害数がスレッシュホールドを超過した場合に発生することがあります。

たとえば、可能なすべての要素をプロンプトに表示するには、次のコマンドを入力します。

```
hostname(config)# prompt hostname context priority slot state
```

プロンプトが次の文字列に変わります。

```
hostname/admin/pri/6/act(config)#
```

ログイン バナーの設定

FWSM に接続するとき、Telnet を使用して FWSM にログインするとき、またはユーザ EXEC モードを開始するときに表示されるメッセージを設定できます。

ログイン バナーを設定するには、システム実行スペースで、またはコンテキスト内で、次のコマンドを入力します。

```
hostname(config)# banner {motd | login | exec} text
```

motd キーワードでは、初回接続時にバナーが表示されます。

The **login** キーワードでは、Telnet を使用して FWSM にログインするときにバナーが表示されます。

exec キーワードでは、ユーザ EXEC モードにアクセスするときにバナーが表示されます。

ユーザが FWSM に接続すると、最初に MoTD（Message-of-The-Day）バナーが表示され、続いてログイン バナーとプロンプトが表示されます。このバナーは Telnet 接続以外では表示されません。さらに、ユーザが FWSM に正しくログインすると（Telnet 接続の場合）、exec バナーが表示されます。

CLI を使用してバナーのテキストにスペースを含めることができますが、タブを入力することはできません。**$(hostname)** および **$(domain)** という文字列を指定することによって、FWSM のホスト名またはドメイン名を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と、コンテキスト コンフィギュレーションで **$(system)** という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。

複数行にする場合は、各行の前に banner コマンドを指定します。

たとえば、MoTD バナーを追加する場合は、次のように入力します。

```
hostname(config)# banner motd Welcome to $(hostname)
hostname(config)# banner motd Contact me at admin@example.com for any
hostname(config)# banner motd issues
```

透過ファイアウォール モードと NAT を設定しない場合の接続制限の設定

NAT を設定すると、トラフィックの接続限度を設定できます。透過ファイアウォール モード（NAT をサポートしません）または NAT を設定しないルーテッド モード コンフィギュレーションの場合、スタティック アイデンティティ NAT を設定して接続制限を設定できます。スタティック アイデンティティ NAT を使用すると、限度を設定し、なおかつ変換を実行しないアドレスを指定できます（ルーテッド モードの場合、NAT 除外など NAT をバイパスする任意の方法を使用して、制限を設定できます。詳細については、「NAT のバイパス」[p.12-32] を参照してください。透過モードの場合、FWSM がサポートするのは次の方式だけです）。

Modular Policy Framework を使用して接続制限（初期接続制限は設定できません）を設定することもできます。詳細については、「接続制限とタイムアウトの設定」（p.19-2）を参照してください。初期接続制限は NAT を使用する場合のみ設定できます。両方の方法を使用する同一トラフィックに対してこれらを設定した場合、FWSM は低い制限値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルになっている場合、FWSM は TCP シーケンスのランダム化をディセーブルにします。

初期接続数を制限することで、DoS 攻撃からシステムを保護できます。FWSM は初期接続制限を使用して、TCP 代行受信機能をトリガーします。初期接続とは、送信元と宛先間で所定のハンドシェイクが完了していない接続要求です。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阻止します。SYN フラッディング攻撃では、通常、スプーフィングされた IP アドレスから一連の SYN パケットが送信されます。継続的に送信される SYN パケットにより、サーバの SYN キューが常に満杯状態になり、接続要求を処理できなくなります。接続が、初期接続スレッシュホールドに達すると、FWSM はサーバのプロキシとして動作し、クライアントの SYN 要求に対して SYN-ACK 応答を生成します。FWSM は、クライアントから ACK の返信を受信すると、そのクライアントを認証し、サーバへの接続を許可します。

接続制限を設定するには、次のコマンドを入力します。

```
hostname(config)# static (real_interface,mapped_interface) real_ip real_ip [netmask
mask] [dns] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns] [norandomseq]
```

両方の *real_ip* 引数に、同じ IP アドレスを指定します。

norandomseq キーワードは TCP Initial Sequence Number（ISN）ランダム化をディセーブルにします。TCP シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化し、その結果、データのスクランブルが発生する場合だけです。TCP 接続ごとに、ISN を 2 つずつ使用します。1 つはクライアントが作成し、もう 1 つはサーバが作成します。FWSM はホスト / サーバによって生成された ISN をランダム化します。攻撃側が次の ISN を予測してセッションをハイジャックする可能性を排除するために、ISN の少なくとも一方はランダムに生成する必要があります。

tcp *tcp_max_conns* および **udp** *udp_max_conns* キーワードはサブネット全体における同時 TCP/UDP 接続の最大数（65,536 まで）を設定します。デフォルトはどちらのプロトコルでも 0 で、これは最大接続数を意味します。

emb_limit 引数は、ホストあたりの最大初期接続数（65,536 まで）を設定します。初期接続とは、送信元と宛先間で所定のハンドシェイクが完了していない接続要求です。この制限によって、TCP 代行受信機能を使用できます。デフォルトは 0 で、これは初期接続の最大数を意味します。*emb_limit* を入力する前に、**tcp** *tcp_max_conns* を入力する必要があります。*tcp_max_conns* にはデフォルト値を使用し、*emb_limit* は変更する場合は、*tcp_max_conns* に **0** を入力します。

たとえば、ホスト 10.1.1.1 にオプションを設定する場合は、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) 10.1.1.1 10.1.1.1 netmask 255.255.255.255
tcp 1000 200 udp 1000 norandomseq
```

IP ルーティングおよび DHCP サービスの設定

この章では、FWSM で IP ルーティングと DHCP を設定する方法について説明します。内容は次のとおりです。

- スタティック ルートおよびデフォルト ルートの設定（p.8-2）
- OSPF の設定（p.8-5）
- RIP の設定（p.8-18）
- マルチキャスト ルーティングの設定（p.8-20）
- 非対称ルーティング サポートの設定（p.8-28）
- DHCP の設定（p.8-30）

スタティック ルートおよびデフォルト ルートの設定

ここでは、FWSM 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を説明します。

マルチコンテキスト モードはダイナミック ルーティングをサポートしないので、ネットワークと FWSM の間にルータが配置されている場合など、FWSM が直接接続されていないネットワークには、スタティック ルートを使用する必要があります。

シングルコンテキスト モードでスタティック ルートを使用する状況は、次のとおりです。

- ネットワークで RIP または OSPF 以外の Router Discovery Protocol を使用する場合
- ネットワークが小規模で、スタティック ルートの管理が容易な場合
- ルーティング プロトコルに伴うトラフィックまたは CPU のオーバーヘッドが望ましくない場合

最も単純なオプションは、デフォルト ルートを設定してすべてのトラフィックをアップストリーム ルータへ送り、トラフィックのルーティングをルータに任せてしまうことです。ただし、デフォルト ゲートウェイが宛先ネットワークに到達できない場合もあるので、より具体的なスタティック ルートを設定することも必要です。たとえば、デフォルト ゲートウェイが外部の場合、FWSM に直接接続されていない内部ネットワークには、デフォルト ルートからトラフィックを転送できません。

透過ファイアウォール モードでは、FWSM を発信元とする、直接接続されていないネットワークを宛先とするトラフィックには、どのインターフェイスからトラフィックを送信するのかを FWSM が認識できるように、デフォルト ルートまたはスタティック ルートのどちらかを設定する必要があります。FWSM が発信元になるトラフィックには、システム ログ サーバ、Websense/N2H2 サーバ、AAA サーバなどへの通信が含まれます。単一のデフォルト ルートから到達できないサーバがある場合は、スタティック ルートを設定しなければなりません。

(注) 管理トラフィックの戻りパスを指定するために必要な、透過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のみ適用されます。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。

FWSM は、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 つまでサポートするので、負荷分散が可能です。

ここでは、次の内容について説明します。

- スタティック ルートの設定（p.8-3）
- デフォルト ルートの設定（p.8-4）

IPv6 スタティック / デフォルト ルートの設定の詳細については、「IPv6 デフォルト / スタティック ルートの設定」（p.9-6）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 ルートを追加するには、次のコマンドを入力します。

```
hostname(config)# route if_name dest_ip mask gateway_ip [distance]
```

dest_ip と *mask* は宛先ネットワークの IP アドレスで、*gateway_ip* はネクストホップ ルータのアドレスです。

distance はルートの管理ディスタンスです。値を指定しなかった場合、デフォルトの 1 が使用されます。管理ディスタンスは、異なるルーティング プロトコル間のルートを比較するためのパラメータです。スタティック ルートのデフォルト管理ディスタンスは 1 で、ダイナミック ルーティング プロトコルによって検出されたルートに優先します。ただし、直接接続されたルートには優先しません。OSPF によって検出されたルートのデフォルト管理ディスタンスは 110 です。スタティック ルートのデフォルト管理ディスタンスがダイナミック ルートと同じ場合、スタティック ルートが優先します。接続されたルートは常に、スタティック ルートまたは動的に検出されたルートに優先します。

指定したゲートウェイが使用不能になった場合でも、スタティック ルートはルーティング テーブルに残ります。指定したゲートウェイが使用不能になった場合、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、関連するインターフェイスがダウンすると、スタティック ルートはルーティング テーブルから削除されます。インターフェイスが元に戻ると、スタティック ルートは復旧します。

(注) 管理ディスタンスの値を FWSM 上で実行されているルーティング プロトコルの管理ディスタンスよりも大きくしてスタティック ルートを作成すると、このルーティング プロトコルによって検出された指定の宛先へのルートは、スタティック ルートに優先します。スタティック ルートは、動的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のみ使用されます。

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。

```
hostname(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
```

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。ECMP は複数のインターフェイス間で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。

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。FWSM は、指定したゲートウェイ間にトラフィックを分配します。

```
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.2
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.3
```

デフォルト ルートの設定

デフォルト ルートでは、FWSM が、学習したルートまたはスタティック ルートのないすべての IP パケットを送信するゲートウェイ IP アドレスを識別します。デフォルト ルートは、宛先 IP アドレスが 0.0.0.0/0 のスタティック ルートです。特定の宛先が識別されたルートは、デフォルト ルートに優先されます。

デバイスごとに、コストの等しいデフォルト ルート エントリを 3 つまで定義できます。コストの等しいデフォルト ルート エントリを複数定義すると、デフォルト ルートに送信されたトラフィックは、指定したゲートウェイ間に分配されます。複数のデフォルト ルートを定義する場合、各エントリに対して同じインターフェイスを指定する必要があります。

コストの等しいデフォルト ルート エントリを 3 つより多く定義しようとすると、または定義済みのデフォルト ルートとは異なる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、「ERROR: Cannot add route entry, possible conflict with existing routes.」というメッセージが表示されます。

デフォルト ルートを定義するには、次のコマンドを入力します。

```
hostname(config)# route if_name 0.0.0.0 0.0.0.0 gateway_ip [distance]
```

ヒント　宛先ネットワーク アドレスおよびマスクに、0.0.0.0 0.0.0.0 ではなく 0 0 を入力できます。例を示します。

```
hostname(config)# route outside 0 0 192.168.1 1
```

次に、コストの等しい 3 つのデフォルト ルートが設定された FWSM の例を示します。FWSM が受信したトラフィックで、スタティック ルートまたは学習したルートのないものは、IP アドレス 192.168.2.1、192.168.2.2、192.168.2.3 のゲートウェイ間に分配されます。

```
hostname(config)# route outside 0 0 192.168.2.1
hostname(config)# route outside 0 0 192.168.2.2
hostname(config)# route outside 0 0 192.168.2.3
```

OSPF の設定

ここでは、OSPF の設定方法について説明します。内容は次のとおりです。

- OSPF の概要（p.8-5）
- OSPF のイネーブル化（p.8-6）
- OSPF プロセス間でのルートの再分配（p.8-7）
- OSPF インターフェイス パラメータの設定（p.8-9）
- OSPF エリア パラメータの設定（p.8-11）
- OSPF NSSA の設定（p.8-12）
- OSPF エリア間のルート集約の設定（p.8-13）
- OSPF へのルート再分配時のルート集約の設定（p.8-14）
- デフォルト ルートの生成（p.8-14）
- ルート計算タイマーの設定（p.8-15）
- ネイバのアップまたはダウンのロギング（p.8-16）
- OSPF アップデート パケット ペーシングの表示（p.8-16）
- OSPF のモニタリング（p.8-17）
- OSPF プロセスの再起動（p.8-17）

OSPF の概要

OSPF では、リンク ステート アルゴリズムを使用し、既知のすべての宛先に到達する最短経路を作成して算出します。OSPF エリア内の各ルータには同じリンク ステート データベースが与えられます。このデータベースは、ルータが使用できるインターフェイスと到達できるネイバを個々に指定したリストです。

OSPF over RIP の利点は、次のとおりです。

- OSPF リンク ステート データベースのアップデートは、RIP のアップデートほど頻繁には送信されません。また、リンク ステート データベースの場合、古い情報は期限切れになるので、アップデートが緩慢ではなく瞬間的に行われます。
- ルーティングはコストに基づいて決定されます。コストとは、パケットを特定のインターフェイスに送信するために必要なオーバーヘッドを指します。FWSM は、宛先へのホップ数ではなくリンクの帯域幅に基づいてコストを計算します。優先経路を指定する目的で、コストを設定できます。

最短経路を優先させるアルゴリズムの短所は、多くの CPU サイクルとメモリが必要になることです。

FWSM は、OSPF プロトコルのプロセスを 2 つ同時に、異なるインターフェイス セット上で実行できます。複数のインターフェイスで同じ IP アドレスを使用する場合に、2 つのプロセスを実行しなければならない場合があります（NAT はこのようなインターフェイスの共存を認めますが、OSPF はアドレスのオーバーラップを認めません）。または、一方のプロセスを内部で、他方を外部で実行し、2 つのプロセス間でルートのサブセットを再分配したいという場合もあります。プライベート アドレスをパブリック アドレスから隔離しなければならないこともあります。

2 つの OSPF プロセス間での再分配がサポートされます。FWSM では、OSPF がイネーブルのインターフェイス上で設定したスタティック ルートと接続ルートを、OSPF プロセスに再分配することもできます。OSPF がイネーブルの場合、FWSM で RIP をイネーブルにすることはできません。RIP と OSPF 間の再分配はサポートされません。

FWSM は次の OSPF 機能をサポートします。

- エリア内ルート、エリア間ルート、および外部（タイプ I、タイプ II）ルートのサポート
- 仮想リンクのサポート
- OSPF LSA フラッディング
- OSPF パケットの認証（パスワードおよび MD5 認証の両方）
- FWSM を指定ルータまたは指定バックアップ ルータとして設定。FWSM を Area Boundary Router（ABR; エリア境界ルータ）として設定することもできますが、FWSM を ASBR として設定する機能はデフォルト情報のみ（デフォルト ルートの導入など）に限定されています。
- スタブ エリアおよび Not-So-Stubby-Area のサポート
- ABR タイプ 3 LSA フィルタリング
- スタティック アドレス変換およびグローバル アドレス変換のアドバタイズ

OSPF のイネーブル化

OSPF をイネーブルにするには、OSPF ルーティング プロセスを作成し、ルーティング プロセスに対応する IP アドレス範囲を指定し、さらに IP アドレス範囲に対応するエリア ID を割り当てる必要があります。

（注） RIP がイネーブルの場合、OSPF をイネーブルにすることはできません。

OSPF を設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、OSPF ルーティング プロセスを作成します。

```
hostname(config)# router ospf process_id
```

このコマンドによって、この OSPF プロセスに対応するルータ コンフィギュレーション モードが開始されます。

process_id は、このルーティング プロセスを識別するための内部 ID です。任意の正の整数を指定できます。内部で使用するだけなので、この ID を他のデバイスの ID と一致させる必要はありません。最大 2 つのプロセスを使用できます。

ステップ 2　次のコマンドを入力して、OSPF を実行する IP アドレスを定義し、さらにそのインターフェイスのエリア ID を定義します。

```
hostname(config-router)# network ip_address mask area area_id
```

次に、OSPF をイネーブルに設定する例を示します。

```
hostname(config)# router ospf 2
hostname(config-router)# network 10.0.0.0 255.0.0.0 area 0
```

OSPF プロセス間でのルートの再分配

FWSM は、OSPF ルーティング プロセス間におけるルートの再分配を制御できます。FWSM は、**redistribute** コマンドの設定値に従って、またはルート マップを使用することによって、ルートを照合して変更します。ルート マップのその他の用途については、「デフォルト ルートの生成」（p.8-14）も参照してください。

（注） FWSM は、ルーティング プロトコル間ではルートを再分配できません。ただし、FWSM はスタティック ルートと接続ルートを再分配できます。

ここでは、次の内容について説明します。

- ルート マップの追加（p.8-7）
- OSPF プロセスへのスタティック ルート、接続ルート、または OSPF ルートの再分配（p.8-8）

ルート マップの追加

ルート マップを定義する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、ルート マップ エントリを作成します。

```
hostname(config)# route-map name {permit | deny} [sequence_number]
```

ルート マップ エントリは順番に読み取られます。*sequence_number* オプションを使用すると、順番を指定できます。順番を指定しなかった場合、FWSM はエントリが追加された順番に従います。

ステップ 2　1 つまたは複数の **match** コマンドを入力します。

- 宛先ネットワークが標準アクセス リストと一致するルートを照合する場合は、次のコマンドを入力します。

  ```
  hostname(config-route-map)# match ip address acl_id [acl_id] [...]
  ```

  複数のアクセス リストを指定した場合、いずれかのアクセス リストが一致するルートを検出します。
- メトリックが指定されたルートを照合する場合は、次のコマンドを入力します。

  ```
  hostname(config-route-map)# match metric metric_value
  ```

  metric_value には 0 ～ 4,294,967,295 を指定できます。
- ネクスト ホップ ルータ アドレスが標準アクセス リストと一致するルートを照合する場合は、次のコマンドを入力します。

  ```
  hostname(config-route-map)# match ip next-hop acl_id [acl_id] [...]
  ```

  複数のアクセス リストを指定した場合、いずれかのアクセス リストが一致するルートを検出します。
- ネクスト ホップ インターフェイスが指定されているルートを照合する場合は、次のコマンドを入力します。

  ```
  hostname(config-route-map)# match interface if_name
  ```

  複数のインターフェイスを指定した場合、いずれかのインターフェイスが一致するルートを検出します。

- 標準アクセス リストと一致するルータによってアドバタイズされたルートを照合する場合は、次のコマンドを入力します。

  ```
  hostname(config-route-map)# match ip route-source acl_id [acl_id] [...]
  ```

  複数のアクセス リストを指定した場合、いずれかのアクセス リストが一致するルートを検出します。
- ルート タイプを照合する場合は、次のコマンドを入力します。

  ```
  hostname(config-route-map)# match route-type {internal | external [type-1 |
  type-2]}
  ```

ステップ 3　1 つまたは複数の **set** コマンドを入力します。

ルートが **match** コマンドと一致すると、次の **set** コマンドによって、再分配の前にルートに対して実行するアクションが決まります。

- メトリックを設定する場合は、次のコマンドを入力します。

  ```
  hostname(config-route-map)# set metric metric_value
  ```

  metric_value には 0 ～ 294,967,295 の任意の値を指定できます。
- メトリック タイプを設定する場合は、次のコマンドを入力します。

  ```
  hostname(config-route-map)# set metric-type {type-1 | type-2}
  ```

次に、ホップ カウントが 1 のルートを再分配する例を示します。FWSM は、メトリックが 5、メトリック タイプが Type 1、タグが 1 の外部 LSA として、これらのルートを再分配します。

```
hostname(config)# route-map 1-to-2 permit
hostname(config-route-map)# match metric 1
hostname(config-route-map)# set metric 5
hostname(config-route-map)# set metric-type type-1
```

OSPF プロセスへのスタティック ルート、接続ルート、または OSPF ルートの再分配

ある OSPF プロセスから別の OSPF プロセスにスタティック ルート、接続ルート、または OSPF ルートを再分配する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、再分配先の OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　次のコマンドを入力して、再分配するルートを指定します。

```
hostname(config-router)# redistribute {ospf process_id
[match {internal | external 1 | external 2}] | static | connect} [metric metric-value]
[metric-type {type-1 | type-2}] [tag tag_value] [subnets] [route-map map_name]
```

ospf *process_id*、**static**、および **connect** キーワードでは、どこからルートを再分配するかを指定します。

このコマンドのオプションを使用して、ルート プロパティを照合したり設定したりできます。またはルート マップを使用することもできます。**tag** オプションおよび **subnets** オプションに相当するオプションは、**route-map** コマンドにはありません。ルート マップと **redistribute** コマンドのオプションを両方とも使用する場合は、両方を一致させる必要があります。

メトリックが 1 のルートと照合することによって、OSPF プロセス 1 から OSPF プロセス 2 にルートを再分配する例を示します。FWSM はメトリックが 5、メトリック タイプが Type 1、タグが 1 の外部 LSA として、これらのルートを再分配します。

```
hostname(config)# route-map 1-to-2 permit
hostname(config-route-map)# match metric 1
hostname(config-route-map)# set metric 5
hostname(config-route-map)# set metric-type type-1
hostname(config-route-map)# set tag 1
hostname(config-route-map)# router ospf 2
hostname(config-router)# redistribute ospf 1 route-map 1-to-2
```

次に、指定した OSPF プロセスのルートが OSPF プロセス 109 に再分配される例を示します。OSPF メトリックは 100 に再マッピングされます。

```
hostname(config)# router ospf 109
hostname(config-router)# redistribute ospf 108 metric 100 subnets
```

次に、リンク ステート コストが 5、メトリック タイプが外部に設定されたルートの再分配の例を示します。この場合、内部メトリックよりプライオリティが下がります。

```
hostname(config)# router ospf 1
hostname(config-router)# redistribute ospf 2 metric 5 metric-type external
```

OSPF インターフェイス パラメータの設定

必要に応じて、インターフェイス固有の OSPF パラメータを一部変更できます。これらのパラメータは、特に変更する必要はありませんが、次のインターフェイス パラメータについては、接続先ネットワーク上のすべてのルータで一致している必要があります。**ospf hello-interval**、**ospf dead-interval**、および **ospf authentication-key** です。これらのパラメータを設定する場合には、ネットワーク上のすべてのルータのコンフィギュレーションに矛盾しない値が設定されていることを確認してください。

OSPF インターフェイス パラメータを設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、インターフェイス コンフィギュレーション モードを開始します。

```
hostname(config)# interface if_name
```

ステップ 2　次のコマンドを任意で入力します。

- インターフェイスの認証タイプを指定する場合は、次のコマンドを入力します。

  ```
  hostname(config-interface)# ospf authentication [message-digest | null]
  ```

- OSPF 簡易パスワード認証を使用するネットワーク 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る場合は、次のコマンドを入力します。

  ```
  hostname(config-interface)# ospf authentication-key key
  ```

key には、長さ 8 バイトまでの連続する任意の文字列を指定できます。

このコマンドによって作成されたパスワードは、FWSM のソフトウェアがルーティング プロトコル パケットを発信するときに、OSPF ヘッダーに直接挿入するキーとして使用されます。インターフェイス単位で、ネットワークごとに異なるパスワードの割り当てが可能です。OSPF 情報を交換できるように、同一ネットワーク上のすべての近接ルータに、同じパスワードを与える必要があります。

- OSPF インターフェイス上でのパケット送信コストを明示的に指定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf cost cost
```

cost は 1 ～ 65,535 の整数です。

- hello パケットの最後の受信から、デバイスで近接する OSPF ルータのダウンを宣言するまでの待機時間（秒）を設定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf dead-interval seconds
```

この値は、ネットワーク上のすべてのノードで一致させる必要があります。

- FWSM が OSPF インターフェイス上で送信する hello パケットの時間間隔を指定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf hello-interval seconds
```

この値は、ネットワーク上のすべてのノードで一致させる必要があります。

- OSPF MD5 認証をイネーブルにするには、次のコマンドを入力します。

```
hostname(config-interface)# ospf message-digest-key key_id md5 key
```

次の値を設定します。

－ *key_id* ― 1 ～ 255 の範囲の ID

－ *key* ― 最大 16 バイトの英数字パスワード

通常、1 つのインターフェイスに 1 つのキーを使用して、パケットの送信時に認証情報を生成し、着信パケットを認証します。近接するルータの同じキー ID には同じキー値を与える必要があります。

1 つのインターフェイスに複数のキーを使用しないことを推奨します。新しいキーを追加するたびに古いキーを削除し、ローカル システムが、古いキーを知っている好ましくないシステムといつまでも通信しないようにしてください。古いキーを削除することによって、ロールオーバー時のオーバーヘッドも軽減されます。

- ネットワーク用の OSPF 指定ルータを決定するときに役立つプライオリティを設定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf priority number_value
```

number_value は 0 ～ 255 です。

- OSPF インターフェイスに属している隣接ノードへの LSA 再送信間隔（秒）を指定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf retransmit-interval seconds
```

seconds は、接続ネットワーク上の 2 つのルータ間で予期される往復遅延より大きくする必要があります。値の範囲は 1 ～ 65,535 秒です。デフォルトは 5 秒です。

- OSPF インターフェイス上でリンク ステート アップデート パケットを送信するときに必要な推定秒数を設定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf transmit-delay seconds
```

seconds は 1 ～ 65,535 秒です。デフォルトは 1 秒です。

次に、OSPF インターフェイスを設定する例を示します。

```
hostname(config)# router ospf 2
hostname(config-router)# network 2.0.0.0 255.0.0.0 area 0
hostname(config-router)# interface inside
hostname(config-interface)# ospf cost 20
hostname(config-interface)# ospf retransmit-interval 15
hostname(config-interface)# ospf transmit-delay 10
hostname(config-interface)# ospf priority 20
hostname(config-interface)# ospf hello-interval 10
hostname(config-interface)# ospf dead-interval 40
hostname(config-interface)# ospf authentication-key cisco
hostname(config-interface)# ospf message-digest-key 1 md5 cisco
hostname(config-interface)# ospf authentication message-digest
```

次に、**show ospf** コマンドの出力例を示します。

```
hostname(config)# show ospf

Routing Process "ospf 2" with ID 20.1.89.2 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
```

OSPF エリア パラメータの設定

複数のエリア パラメータを設定できます。これらのエリア パラメータ（次の作業手順を参照）には、認証の設定、スタブ エリアの定義、およびデフォルトの集約ルートへの特定コストの割り当てが含まれます。認証により、エリアへの不正アクセスに対して、パスワード ベースの保護が提供されます。

スタブ エリアは、外部ルートの情報が送信されないエリアです。その代わりに、スタブ エリアには、Autonomous System（AS; 自律システム）外部の宛先について、ABR が生成したデフォルトの外部ルートが設定されます。OSPF のスタブ エリア サポートを有効に利用するには、スタブ エリアでデフォルトのルーティングを使用する必要があります。スタブ エリアに送信される LSA 数を減らすには、ABR に **area stub** コマンドの **no-summary** キーワードを設定して、ABR からスタブ エリアへの集約リンク アドバタイズ（LSA タイプ 3）の送信を阻止できます。

ネットワークのエリア パラメータを指定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　次のコマンドを任意で入力します。

- OSPF エリアの認証をイネーブルにするには、次のコマンドを入力します。

  ```
  hostname(config-router)# area area-id authentication
  ```

- OSPF エリアの MD5 認証をイネーブルにするには、次のコマンドを入力します。

  ```
  hostname(config-router)# area area-id authentication message-digest
  ```

- エリアをスタブ エリアとして定義するには、次のコマンドを入力します。

  ```
  hostname(config-router)# area area-id stub [no-summary]
  ```

- スタブ エリアで使用するデフォルトの集約ルートに、特定のコストを割り当てるには、次のコマンドを入力します。

  ```
  hostname(config-router)# area area-id default-cost cost
  ```

  cost は 1 ～ 65,535 の整数です。デフォルトは 1 です。

次に、OSPF エリア パラメータを設定する例を示します。

```
hostname(config)# router ospf 2
hostname(config-router)# area 0 authentication
hostname(config-router)# area 0 authentication message-digest
hostname(config-router)# area 17 stub
hostname(config-router)# area 17 default-cost 20
```

OSPF NSSA の設定

OSPF NSSA は OSPF スタブ エリアと似ています。NSSA では、コアからエリアへのタイプ 5 外部 LSA のフラッディングは実行されませんが、限定された方法で、AS の外部ルートをエリア内にインポートできます。

NSSA では、再分配により、NSSA エリア内にタイプ 7 AS 外部ルートをインポートします。これらのタイプ 7 LSA は、NSSA の ABR によってタイプ 5 LSA に変換され、ルーティング ドメイン全体へフラッディングされます。変換時には、集約およびフィルタリングがサポートされます。

OSPF を使用している中央サイトから別のルーティング プロトコルを使用しているリモート サイトに接続する必要がある ISP またはネットワーク管理者は、NSSA を使用して管理を簡素化できます。

スタブ エリアにはリモート サイトのルートが再分配されないので、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 ルータ間の接続に OSPF スタブ エリアを利用できず、2 つのルーティング プロトコルを維持する必要がありました。一般的には RIP などの簡易プロトコルを使用し、再分配を行っていました。NSSA の実装により、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で、リモート接続にも OSPF を適用できます。

OSPF NSSA の設定に必要なネットワークのエリア パラメータを指定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　次のコマンドを任意で入力します。

- NSSA エリアを定義するには、次のコマンドを入力します。

  ```
  hostname(config-router)# area area-id nssa [no-redistribution]
  [default-information-originate]
  ```

- アドレス グループを集約するには、次のコマンドを入力します。

  ```
  hostname(config-router)# summary address ip_address mask [not-advertise] [tag tag]
  ```

  このコマンドは、ルーティング テーブルの容量縮小に有効です。OSPF にこのコマンドを使用すると、OSPF ASBR によって、アドレスに含まれるすべての再分配ルートを集約したものとして、外部ルートが 1 つアドバタイズされます。

  OSPF は **summary-address 0.0.0.0 0.0.0.0** をサポートしません。

  次の例では、集約アドレス 10.1.0.0 にアドレス 10.1.1.0、10.1.2.0、10.1.3.0 などが含まれています。外部 Link State Advertisement（LSA; 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。

  ```
  hostname(config-router)# summary-address 10.1.1.0 255.255.0.0
  ```

  この機能を使用する前に、次の注意事項を考慮してください。

  — 外部の宛先に到達するためのタイプ 7 デフォルト ルートを設定できます。この設定により、ルータは NSSA または NSSA の ABR が使用するタイプ 7 デフォルト ルートを生成します。

  — 同じエリア内のすべてのルータは、そのエリアが NSSA であることを認識している必要があります。認識していないと、ルータ間の通信ができません。

OSPF エリア間のルート集約の設定

ルート集約は、アドバタイズされたアドレスの統合を意味します。この機能により、ABR から他のエリアに、1 つの集約ルートだけをアドバタイズできます。OSPF では、ABR が 1 つのエリアのネットワークを別のエリアにアドバタイズします。1 つのエリア内のネットワーク番号が連続して割り当てられている場合、そのエリア内のすべてのネットワークが指定範囲内に収まる 1 つの集約ルートを生成し、そのルートだけがアドバタイズされるように、ABR を設定できます。

ルート集約のアドレス範囲を定義する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　次のコマンドを入力して、アドレス範囲を設定します。

```
hostname(config-router)# area area-id range ip-address mask [advertise |
not-advertise]
```

次に、OSPF エリア間のルート集約を設定する例を示します。

```
hostname(config)# router ospf 1
hostname(config-router)# area 17 range 12.1.0.0 255.255.0.0
```

OSPF へのルート再分配時のルート集約の設定

他のプロトコルからのルートが OSPF に再分配される場合、各ルートは外部 LSA により個別にアドバタイズされます。ただし、ネットワーク アドレスとマスクの範囲を指定することにより、範囲内のすべての再分配ルートを含む単一ルートがアドバタイズされるように、FWSM を設定できます。この設定により、OSPF リンク ステート データベースのサイズを縮小できます。

指定したネットワーク アドレスとマスクの範囲内のすべての再分配ルートを 1 つの集約ルートとしてアドバタイズする手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　次のコマンドを入力して、集約アドレスを設定します。

```
hostname(config-router)# summary-address ip_address mask [not-advertise] [tag tag]
```

OSPF は **summary-address 0.0.0.0 0.0.0.0** をサポートしません。

次に、ルート集約を設定する例を示します。集約アドレス 10.1.0.0 にアドレス 10.1.1.0、10.1.2.0、10.1.3.0 などが含まれています。外部 LSA では、アドレス 10.1.0.0 だけがアドバタイズされます。

```
hostname(config)# router ospf 1
hostname(config-router)# summary-address 10.1.0.0 255.255.0.0
```

デフォルト ルートの生成

ASBR に、OSPF ルーティング ドメインへのデフォルト ルートを強制的に生成させることができます。OSPF ルーティング ドメインへのルート再分配を明確に設定すると、ルータは自動的に ASBR になります。ただし、ASBR のデフォルトでは、OSPF ルーティング ドメインへのデフォルト ルートは生成されません。

デフォルト ルートを生成する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　次のコマンドを入力して、ASBR にデフォルト ルートを強制的に生成させます。

```
hostname(config-router)# default-information originate [always] [metric metric-value]
[metric-type {1 | 2}] [route-map map-name]
```

次に、デフォルト ルートを生成する例を示します。

```
hostname(config)# router ospf 2
hostname(config-router)# default-information originate always
```

ルート計算タイマーの設定

OSPF がトポロジー変更を受信してから、SPF の計算を開始するまでの遅延時間を設定できます。また、2 つの連続する SPF 計算の間隔となるホールドタイムを設定できます。

ルート計算タイマーを設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　次のコマンドを入力して、ルート計算時間を設定します。

```
hostname(config-router)# timers spf spf-delay spf-holdtime
```

spf-delay には、OSPF がトポロジー変更を受信してから、SPF 計算を開始するまでの遅延時間（秒）を指定します。0 ～ 65,535 の整数を指定できます。デフォルトは 5 秒です。0 の値は遅延がないことを意味するので、SPF 計算がただちに開始されます。

spf-holdtime で、連続する 2 回の SPF 計算の最小間隔（秒）を指定します。0 ～ 65,535 の整数を指定できます。デフォルトは 10 秒です。0 を指定すると遅延は発生しません。1 つの SPF 計算の終了後、ただちに次の SPF 計算が開始されます。

次に、ルート計算タイマーを設定する例を示します。

```
hostname(config)# router ospf 1
hostname(config-router)# timers spf 10 120
```

ネイバのアップまたはダウンのロギング

デフォルトでは、OSPF ネイバがアップまたはダウンになると、システム メッセージが送信されます。

debug ip ospf adjacency コマンドを実行しないで、OSPF ネイバのアップまたはダウンを調べる場合には、ロギングを設定します。**log-adj-changes** ルータ コンフィギュレーション コマンドを使用すると、少ない出力で、高いレベルのピア関係情報が得られます。各ステート変更のメッセージを表示する場合には、**log-adj-changes detail** を設定します。

ネイバのアップまたはダウンをロギングする手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

ステップ 2　次のコマンドを入力して、ネイバのアップ / ダウンに関するロギングを設定します。

```
hostname(config-router)# log-adj-changes [detail]
```

（注）　送信するネイバのアップ / ダウン メッセージに対して、ロギングをイネーブルにする必要があります。

次に、ネイバのアップ / ダウン メッセージをロギングする例を示します。

```
hostname(config)# router ospf 1
hostname(config-router)# log-adj-changes detail
```

OSPF アップデート パケット ペーシングの表示

OSPF アップデート パケットは、自動的にペーシングされるので、最低 33 ミリ秒の間隔をあけて送信されます。ペーシングが実行されないと、リンクが遅い状況で一部のアップデート パケットが失われたり、ネイバが適切な速度でアップデートを受信できなかったり、ルータのバッファ スペースが不足したりする可能性があります。たとえば、次のいずれかのトポロジーの場合、ペーシングを行わないと、パケットが廃棄されることがあります。

- ポイントツーポイント リンクを使用して高速ルータを低速ルータに接続する場合
- フラッディング中に、複数のネイバが 1 つのルータに同時にアップデートを送信する場合

再送信の場合にも、効率を向上させて再送信時の損失を最小限に抑えるために、ペーシングが使用されます。インターフェイスからの送出を待機している LSA を表示することもできます。ペーシングには、OSPF のアップデート パケットと再送信パケットをより効率的に送信できるという利点があります。

この機能は自動的にサポートされるので、設定を行う必要はありません。

指定したインターフェイス上でフラッディングされる待機中 LSA のリストを表示し、OSPF パケット ペーシングを確認するには、次のコマンドを入力します。

```
hostname# show ospf flood-list if_name
```

OSPF のモニタリング

IP ルーティング テーブル、キャッシュ、および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。提供された情報を使用して、リソース利用状況を判別したり、ネットワークの問題を解決したりできます。また、ノードへの到達可能性情報を表示したり、デバイスのパケットがネットワーク上で使用しているルーティング パスを検出したりすることもできます。

各種のルーティング統計情報を表示するには、必要に応じて、次のいずれかの作業を行います。

- OSPF ルーティング プロセスに関する一般情報を表示するには、次のコマンドを入力します。

  hostname# **show ospf** [*process-id [area-id]*]

- ABR および ASBR への内部 OSPF ルーティング テーブルのエントリを表示するには、次のコマンドを入力します。

  hostname# **show ospf border-routers**

- 特定のルータについて、OSPF データベース関連の情報リストを表示するには、次のコマンドを入力します。

  hostname# **show ospf** [*process-id* [*area-id*]] **database**

- (OSPF パケット ペーシングを確認するために)指定したインターフェイス上でフラッディングを待機中の LSA のリストを表示するには、次のコマンドを入力します。

  hostname# **show ospf flood-list** *if-name*

- OSPF 関連のインターフェイス情報を表示するには、次のコマンドを入力します。

  hostname# **show ospf interface** [*if_name*]

- OSPF ネイバ情報をインターフェイス単位で表示するには、次のコマンドを入力します。

  hostname# **show ospf neighbor** [*if-name*] [*neighbor-id*] [**detail**]

- ルータが要求したすべての LSA のリストを表示するには、次のコマンドを入力します。

  hostname# **show ospf request-list** *neighbor if_name*

- 再送信待ちになっているすべての LSA のリストを表示するには、次のコマンドを入力します。

  hostname# **show ospf retransmission-list** *neighbor if_name*

- OSPF プロセスに基づいて設定したすべての集約アドレス再分配情報のリストを表示するには、次のコマンドを入力します。

  hostname# **show ospf** [*process-id*] **summary-address**

- OSPF 関連の仮想リンク情報を表示するには、次のコマンドを入力します。

  hostname# **show ospf** [*process-id*] **virtual-links**

OSPF プロセスの再起動

OSPF プロセスを再起動し、再分配またはカウンタを消去するには、次のコマンドを入力します。

hostname(config)# **clear ospf** *pid* {**process** | **redistribution** | **counters** [**neighbor** [*neighbor-interface*] [*neighbor-id*]]}

RIP の設定

ここでは、RIP の設定方法について説明します。内容は次のとおりです。

- RIP の概要（p.8-18）
- RIP のイネーブル化（p.8-18）

RIP の概要

RIP をサポートするデバイスは、定期的におよびネットワーク トポロジー変更時に、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 RIP パケットには、装置が到達できるネットワークに関する情報とともに、パケットが宛先アドレスに到達するまでの間に通過するルータまたはゲートウェイの数が含まれます。RIP の方が OSPF より多くのトラフィックを生成しますが、初期設定は容易です。

RIP は、初期設定が容易であり、トポロジーの変更時にコンフィギュレーションを更新する必要がないので、スタティック ルートより有利です。RIP の短所は、スタティック ルーティングよりネットワークおよび処理のオーバーヘッドが増えることです。

FWSM では、限定バージョンの RIP を使用します。FWSM が到達できるネットワークを示す RIP アップデートは送信されません。ただし、次の方法の一方または両方を使用できます。

- パッシブ RIP — FWSM は、RIP アップデートを待ち受けますが、インターフェイスからはネットワークに関するアップデートを送出しません。

  パッシブ RIP を使用すると、FWSM は直接接続されていないネットワークについて学習できます。
- デフォルト ルート アップデート — FWSM を介して到達可能なあらゆるネットワークを示した通常の RIP アップデートを送信する代わりに、FWSM は FWSM をデフォルト ゲートウェイとして認識する参加デバイスまでのデフォルト ルートを送信します。

  デフォルト ルート オプションは、パッシブ RIP と組み合わせて使用することも、単独で使用することもできます。FWSM 上でスタティック ルートを使用し、なおかつダウンストリーム ルータ上でスタティック ルートを設定しない場合は、デフォルト ルート オプションを単独で使用します。通常、外部インターフェイスではデフォルト ルート オプションをイネーブルにしません。FWSM がアップストリーム ルータのデフォルト ゲートウェイになることはあまりないからです。

RIP のイネーブル化

インターフェイス上で RIP をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# rip if_name {default | passive} [version {1 | 2
[authentication {text | md5} key key_id]}]
```

rip コマンドをそれぞれの方法について 1 回ずつ入力することで、インターフェイス上の RIP のパッシブ モードおよびデフォルト モードの両方をイネーブル化できます。コマンドの入力例を示します。

```
hostname(config)# rip inside default version 2 authentication md5 scorpius 1
hostname(config)# rip inside passive version 2 authentication md5 scorpius 1
```

すべてのインターフェイスでパッシブ RIP をイネーブルにし、デフォルト ルートに関しては内部インターフェイスに限定してイネーブルにするという場合は、次のコマンドを入力します。

```
hostname(config)# rip inside default version 2 authentication md5 scorpius 1
hostname(config)# rip inside passive version 2 authentication md5 scorpius 1
hostname(config)# rip outside passive version 2 authentication md5 scorpius 1
```

(注) コンフィギュレーションをテストする前に、FWSM に接続されたすべてのルータ上で、ARP キャッシュをフラッシュしてください。Cisco ルータの場合、**clear arp** コマンドを使用して ARP キャッシュをフラッシュします。

OSPF がイネーブルの場合、RIP をイネーブルにすることはできません。

マルチキャスト ルーティングの設定

ここでは、マルチキャスト ルーティングの設定方法について説明します。内容は次のとおりです。

- マルチキャスト ルーティングの概要（p.8-20）
- マルチキャスト ルーティングのイネーブル化（p.8-20）
- IGMP 機能の設定（p.8-21）
- スタブ マルチキャスト ルーティングの設定（p.8-24）
- スタティック マルチキャスト ルートの設定（p.8-24）
- PIM 機能の設定（p.8-25）
- マルチキャスト ルーティングの詳細について（p.8-27）

マルチキャスト ルーティングの概要

FWSM 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ます。ただし、1 つの FWSM で両方を同時に設定することはできません。

スタブ マルチキャスト ルーティングでは動的なホスト登録が行われるため、マルチキャスト ルーティングが効率化されます。スタブ マルチキャスト ルーティング用に設定された場合、FWSM は IGMP プロキシ エージェントとして機能します。FWSM 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、マルチキャスト データの配信を設定するアップストリームのマルチキャスト ルータに転送します。FWSM をスタブ マルチキャスト ルーティング用に設定した場合、PIM 用には設定できません。

FWSM は PIM-SM および双方向 PIM の両方をサポートします。PIM-SM は、ユニキャスト ルーティング情報ベースまたは別個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。マルチキャスト グループごとに、単一の Rendezvous Point（RP; ランデブー ポイント）をルートとする単方向の共有ツリーを作成します。また、任意でマルチキャストの送信元ごとに最短パス ツリーを作成します。

双方向 PIM は PIM-SM のバリアントで、マルチキャストの送信元とレシーバーを接続する双方向の共有ツリーを作成します。双方向ツリーは、マルチキャスト トポロジーの各リンクで実行される DF 選定プロセスを使用して作成します。マルチキャスト データは DF を使用して送信元から RP へ、そして共有ツリーからレシーバーへ転送されます。送信元固有のステートは必要ありません。DF 選定は RP 検出時に行われ、RP へのデフォルト ルートを指定します。

（注） FWSM が PIM RP の場合、FWSM の変換されていない外部アドレスを RP アドレスとして使用します。

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化すると、FWSM でマルチキャスト パケットを転送できます。マルチキャスト ルーティングをイネーブル化すると、すべてのインターフェイスで PIM と IGMP が自動的にイネーブルになります。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。

```
hostname(config)# multicast-routing
```

マルチキャスト ルーティング テーブルのエントリ数は、システムの RAM の容量に制限されます。表 8-1 に、FWSM の RAM 容量に基づく、特定のマルチキャスト テーブルの最大エントリ数を示します。最大エントリ数に達すると、新規エントリはすべて廃棄されます。

表 8-1　マルチキャスト テーブルのエントリ制限

テーブル	16 MB	128 MB	128+ MB
MFIB	1000	3000	5000
IGMP グループ	1000	3000	5000
PIM ルート	3000	7000	12000

IGMP 機能の設定

IP ホストは IGMP を使用して、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 ルータにレポートします。IGMP は、グループ アドレス（クラス D IP アドレス）をグループ ID として使用します。ホスト グループ アドレスには 224.0.0.0 ～ 239.255.255.255 の範囲を指定できます。アドレス 224.0.0.0 は、どのグループにも割り当てられません。アドレス 224.0.0.1 は、サブネット上のすべてのシステムに割り当てられます。アドレス 224.0.0.2 は、サブネット上のすべてのルータに割り当てられます。

FWSM でマルチキャスト ルーティングをイネーブルにすると、すべてのインターフェイスで IGMP Version 2 が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、**no igmp** コマンドのみがインターフェイス コンフィギュレーションに表示されます。**multicast-routing** コマンドがデバイス コンフィギュレーションに表示されると、すべてのインターフェイスで自動的に IGMP が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。内容は次のとおりです。

- インターフェイス上での IGMP のディセーブル化（p.8-21）
- グループ メンバーシップの設定（p.8-22）
- 静的に加入するグループの設定（p.8-22）
- マルチキャスト グループへのアクセスの制御（p.8-22）
- インターフェイス上の IGMP ステート数の制限（p.8-23）
- クエリー間隔とクエリー タイムアウトの変更（p.8-23）
- クエリー応答時間の変更（p.8-24）
- IGMP バージョンの変更（p.8-24）

インターフェイス上での IGMP のディセーブル化

特定のインターフェイスで IGMP をディセーブルにできます。これは、特定のインターフェイスにマルチキャスト ホストがないことがわかっていて、FWSM からそのインターフェイスにホスト クエリー メッセージを送信しないようにする場合に役立ちます。

インターフェイス上で 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。

```
hostname(config-if)# no igmp
```

インターフェイス上で IGMP を再びイネーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# igmp
```

（注）　**no igmp** コマンドのみがインターフェイス コンフィギュレーションに表示されます。

グループ メンバーシップの設定

FWSM をマルチキャスト グループのメンバーにするように設定できます。FWSM をマルチキャスト グループに参加するように設定すると、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 テーブル情報を保持して、そのグループのパスをアクティブにし続けます。

FWSM をマルチキャスト グループに参加させるには、次のコマンドを入力します。

```
hostname(config-if)# igmp join-group group-address
```

静的に加入するグループの設定

グループ メンバーがグループのメンバーシップをレポートできなかったり、ネットワーク セグメントにグループのメンバーが存在しない場合でも、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 セグメントに送信しなければならないことがあります。このような場合、次のいずれかの方法で、そのグループのマルチキャスト トラフィックをセグメントに送信できます。

- **igmp join-group** コマンドを使用（「グループ メンバーシップの設定」[p.8-22] を参照）。FWSM はマルチキャスト パケットを受信して転送することができます。
- **igmp static-group** コマンドを使用。FWSM はマルチキャスト パケットを受信せずに、指定されたインターフェイスに転送します。

静的に加入するマルチキャスト グループをインターフェイス上で設定するには、次のコマンドを入力します。

```
hostname(config-if)# igmp static-group group-address
```

マルチキャスト グループへのアクセスの制御

FWSM インターフェイスのホストが参加できるマルチキャスト グループを制御するには、次の手順を実行します。

ステップ 1　マルチキャスト トラフィックのアクセス リストを作成します。1 つのアクセス リストに複数のエントリを作成できます。拡張アクセス リストまたは標準アクセス リストを使用できます。

- 標準アクセス リストを作成するには、次のコマンドを入力します。

  ```
  hostname(config)# access-list name standard [permit | deny] ip_addr mask
  ```

  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。
- 拡張アクセス リストを作成するには、次のコマンドを入力します。

  ```
  hostname(config)# access-list name extended [permit | deny] protocol src_ip_addr
  src_mask dst_ip_addr dst_mask
  ```

  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　次のコマンドを入力して、アクセス リストをインターフェイスに適用します。

```
hostname(config-if)# igmp access-group acl
```

acl 引数は、標準または拡張 IP アクセス リストの名前です。

インターフェイス上の IGMP ステート数の制限

IGMP メンバーシップ レポートから生成される IGMP ステート数を、インターフェイス単位で制限できます。設定した制限を超えるメンバーシップ レポートは IGMP キャッシュに保存されず、超過したメンバーシップ レポートのトラフィックは転送されません。

インターフェイスの IGMP ステート数を制限にするには、次のコマンドを入力します。

```
hostname(config-if)# igmp limit number
```

有効値の範囲は 0 ～ 500 で、500 がデフォルト値です。値を 0 に設定すると、学習したグループは追加されませんが、（**igmp join-group** 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追加できます。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。

クエリー間隔とクエリー タイムアウトの変更

FWSM 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たネットワーク上でメンバーを持つマルチキャスト グループを検出します。メンバーが IGMP レポート メッセージに応答した場合、そのメンバーは特定グループのマルチキャスト パケットを受信したいことを示します。クエリー メッセージは、アドレスが 224.0.0.1 で Time To Live（TTL）の値が 1 の全システムのマルチキャスト グループ宛てに送信されます。

FWSM に保存されているメンバーシップ情報をリフレッシュするために、これらのメッセージは定期的に送信されます。FWSM はインターフェイスに接続されているマルチキャスト グループのローカル メンバーがいなくなったことを検出すると、そのグループのマルチキャスト パケットを接続されているネットワークに転送することをやめて、Prune メッセージをそのパケットの送信元に送り返します。

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。デフォルトでは、メッセージは 125 秒ごとに送信されます。この間隔を変更するには、次のコマンドを入力します。

```
hostname(config-if)# igmp query-interval seconds
```

FWSM が指定したタイムアウト値（デフォルトは 255 秒）の間インターフェイスでクエリー メッセージを受信しない場合、FWSM 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。このタイムアウト値を変更するには、次のコマンドを入力します。

```
hostname(config-if)# igmp query-timeout seconds
```

（注）　**igmp query-timeout** および **igmp query-interval** コマンドでは IGMP Version 2 が必要です。

クエリー応答時間の変更

デフォルトでは、IGMP クエリーでアドバタイズされる最大クエリー応答時間は 10 秒です。FWSM がこの時間内にホスト クエリーへの応答を受信しない場合、そのグループを削除します。

最大クエリー応答時間を変更するには、次のコマンドを入力します。

```
hostname(config-if)# igmp query-max-response-time seconds
```

IGMP バージョンの変更

デフォルトでは、FWSM は IGMP Version 2 を実行します。このプロトコルにより、**igmp query-timeout** や **igmp query-interval** コマンドなど複数の追加機能がイネーブルになります。

サブネット上のすべてのマルチキャスト ルータで、同じバージョンの IGMP がサポートされている必要があります。FWSM は Version 1 のルータを自動的には検出せず、Version 1 に切り替えます。ただし、サブネット上に IGMP Version 1 と Version 2 ホストを混在させることができます。すなわち、IGMP Version 1 ホストが存在する場合、IGMP Version 2 を実行する FWSM は正しく機能します。

インターフェイスで実行する 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。

```
hostname(config-if)# igmp version {1 | 2}
```

スタブ マルチキャスト ルーティングの設定

スタブ エリアへのゲートウェイとして機能する FWSM は、PIM に参加する必要はありません。代わりに、IGMP プロキシ エージェントとして動作し、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上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ように設定できます。FWSM を IGMP プロキシ エージェントとして設定するには、ホスト ジョインを転送して、スタブ エリア インターフェイスからアップストリーム インターフェイスにメッセージを残します。

ホスト ジョインを転送してメッセージを残すには、スタブ エリアに接続されたインターフェイスから次のコマンドを入力します。

```
hostname(config-if)# igmp forward interface if_name
```

(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。

スタティック マルチキャスト ルートの設定

PIM を使用する場合、FWSM は同一インターフェイス上でのパケット受信を予期します（このインターフェイスからユニキャスト パケットを送信元に返します）。マルチキャスト ルーティングをサポートしないルートをバイパスする場合など、ユニキャスト パケットとマルチキャスト パケットに別々のパスを使用させたいことがあります。

スタティック マルチキャスト ルートはアドバタイズまたは再分配されません。

PIM 用のスタティック マルチキャスト ルートを設定するには、次のコマンドを入力します。

```
hostname(config)# mroute src_ip src_mask input_if_name [distance]
```

スタブ エリア用のスタティック マルチキャスト ルートを設定するには、次のコマンドを入力します。

```
hostname(config)# mroute src_ip src_mask input_if_name [dense output_if_name]
[distance]
```

(注) ***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 ルーティングに対してのみサポートされます。

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管理します。FWSM でマルチキャスト ルーティングをイネーブルにすると、すべてのインターフェイスで PIM と IGMP が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でのみ動作するためです。

ここでは、任意の PIM 設定を行う方法について説明します。内容は次のとおりです。

- インターフェイス上での PIM のディセーブル化（p.8-25）
- スタティック RP アドレスの設定（p.8-26）
- 指定ルータのプライオリティの設定（p.8-26）
- PIM Register メッセージのフィルタリング（p.8-26）
- PIM メッセージ間隔の設定（p.8-27）

インターフェイス上での PIM のディセーブル化

特定のインターフェイスで PIM をディセーブルにできます。インターフェイス上で PIM をディセーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# no pim
```

インターフェイス上で PIM を再びイネーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# pim
```

(注) **no pim** コマンドのみがインターフェイス コンフィギュレーションに表示されます。

スタティック RP アドレスの設定

一般的な PIM sparse（疎）モードまたは bidir ドメイン内のすべてのルータは、PIM RP アドレスを知っ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静的に設定されます。

（注） FWSM は Auto-RP や PIM BSR をサポートしないため、ユーザは **pim rp-address** コマンドを使用して RP アドレスを指定する必要があります。

FWSM を複数グループの RP として設定できます。アクセス リストで指定されているグループ範囲によって、PIM RP グループ マッピングが決定されます。アクセス リストが指定されていない場合、そのグループの RP がマルチキャスト グループ範囲全体（224.0.0.0/4）に適用されます。

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。

```
hostname(config)# pim rp-address ip_address [acl] [bidir]
```

ip_address 引数は、PIM RP となるルータのユニキャスト IP アドレスです。*acl* 引数は、RP を使用するマルチキャスト グループを指定するアクセス リストの名前または番号です。***bidir*** キーワードを除外すると、グループは PIM sparse（疎）モードで動作します。

（注） 実際の bidir 設定に関係なく、FWSM は常に bidir 機能を PIM の hello メッセージで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 レジスタ、ジョイン、Prune メッセージの RP への送信を担当します。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、DR のプライオリティに基づいて DR を選択する選定プロセスが行われます。複数のデバイスが同じ DR プライオリティの場合、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、FWSM は DR プライオリティ 1 を持ちます。次のコマンドを入力して、この値を変更できます。

```
hostname(config-if)# pim dr-priority num
```

num 引数には 1 ～ 4,294,967,294 の任意の値を指定できます。

PIM Register メッセージのフィルタリング

PIM Register メッセージをフィルタリングするように FWSM を設定できます。PIM Register 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。

```
hostname(config)# pim accept-register {list acl | route-map map-name}
```

PIM メッセージ間隔の設定

ルータ クエリー メッセージを使用して PIM DR を選定します。PIM DR はルータ クエリー メッセージの送信を担当します。デフォルトでは、ルータ クエリー メッセージは 30 秒ごとに送信されます。次のコマンドを入力して、この値を変更できます。

```
hostname(config-if)# pim hello-interval seconds
```

seconds 引数の有効値の範囲は 1 ～ 3600 秒です。

FWSM は 60 秒ごとに PIM ジョイン /Prune メッセージを送信します。この値を変更するには、次のコマンドを入力します。

```
hostname(config-if)# pim join-prune-interval seconds
```

seconds 引数の有効値の範囲は 10 ～ 600 秒です。

マルチキャスト ルーティングの詳細について

次の Internet Engineering Task Force（IETF）による RFC には、SMR 機能を実装するための、IGMP 規格およびマルチキャスト ルーティング規格に関する技術的な詳細が示されています。

- RFC 2236 IGMPv2
- RFC 2362 PIM-SM
- RFC 2588 IP マルチキャストとファイアウォール
- RFC 2113 IP ルータ アラート オプション
- IETF draft-ietf-idmr-igmp-proxy-01.txt

非対称ルーティング サポートの設定

セッションの戻りトラフィックが、発信元と異なるインターフェイスを経由してルーティングされることもあります。フェールオーバー コンフィギュレーションでは、ある装置から発信された接続の戻りトラフィックが、ピア装置を経由して返送されることがあります。これは一般に、1 つの FWSM 上の 2 つのインターフェイス、またはフェールオーバー ペアの 2 つの FWSM が別々のサービス プロバイダーに接続され、発信接続で NAT アドレスを使用しない場合に起こります。FWSM では、戻りトラフィックは接続情報がないためデフォルトでは廃棄されます。

廃棄が発生する可能性のあるインターフェイス上で **asr-group** コマンドを使用して、戻りトラフィックの廃棄を阻止できます。**asr-group** コマンドで設定したインターフェイスがセッション情報のないパケットを受信すると、同一グループ内の他のインターフェイスのセッション情報を確認します。

(注) フェールオーバー コンフィギュレーションでは、スタンバイ ユニットまたはフェールオーバー グループからアクティブ ユニットまたはフェールオーバー グループに転送されるセッション情報について、ステートフル フェールオーバーをイネーブルにする必要があります。

一致が見つからない場合、パケットは廃棄されます。一致が見つかった場合、次のいずれかの処理が行われます。

- 着信トラフィックがフェールオーバー コンフィギュレーションのピア装置で発信された場合、レイヤ 2 ヘッダの一部または全部が書き換えられ、パケットは他の装置にリダイレクトされます。このリダイレクションは、セッションがアクティブなかぎり継続します。
- 着信トラフィックが同一装置上の異なるインターフェイスで発信された場合、レイヤ 2 ヘッダの一部または全部が書き換えられ、パケットは再度ストリームに入れられます。

(注) **asr-group** コマンドを使用して非対象ルーティング サポートを設定する方が、***nailed*** オプションを指定して **static** コマンドを使用するよりもセキュアです。

ここでは、次の内容について説明します。

- インターフェイスの ASR グループへの追加（p.8-28）
- 非対称ルーティング サポートの例（p.8-29）

インターフェイスの ASR グループへの追加

次のコマンドを入力して、インターフェイスを非対象ルーティング グループに追加します。フェールオーバー コンフィギュレーションの装置間で非対象ルーティング サポートを適切に機能させるためには、ステートフル フェールオーバーをイネーブルにする必要があります。

```
hostname/ctx1(config)# interface if
hostname/ctx1(config-if)# asr-group num
```

num の有効値の範囲は 1 ～ 32 です。ASR グループに参加するインターフェイスごとに、コマンドを入力する必要があります。**show interface detail** コマンドを使用して、伝送された ASR パケット数、受信された ASR パケット数、またはインターフェイスによって廃棄された ASR パケット数を表示できます。

最大 32 個の ASR グループを作成し、各グループに最大 8 個のインターフェイスを割り当てることができます。

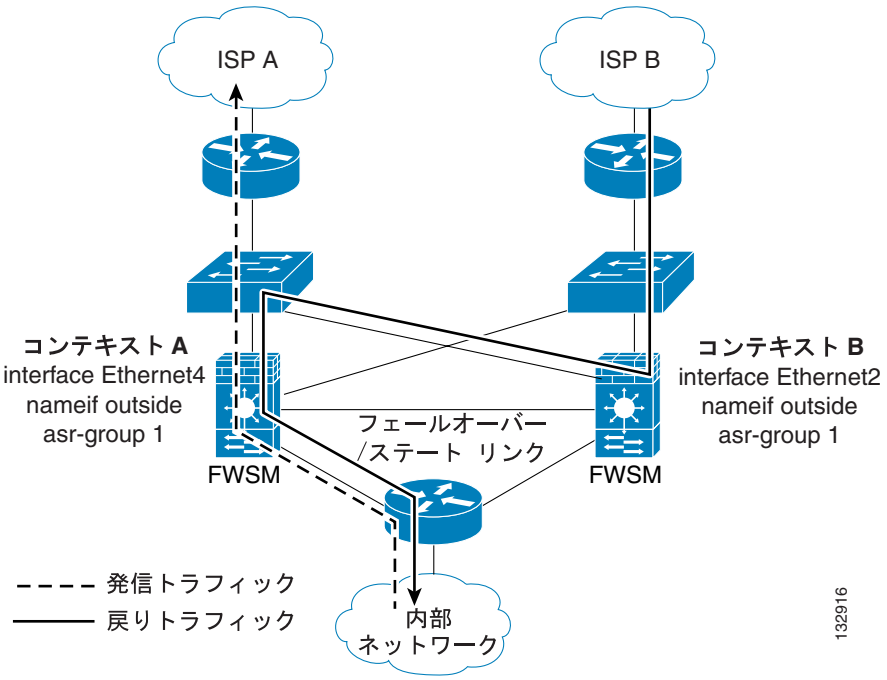
(注)

フェールオーバー コンフィギュレーションのスタンバイ ユニットからアクティブ ユニットへのパケットのリダイレクションを可能にするために、アップストリーム ルータおよびダウンストリーム ルータは、VLAN ごとに 1 つの MAC アドレスを使用し、異なる VLAN には異なる MAC アドレスを使用する必要があります。

非対称ルーティング サポートの例

図 8-1 に、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の非対称ルーティング サポートに **asr-group** コマンドを使用する例を示します。

図 8-1　アクティブ / アクティブ フェールオーバーでの ASR の例



一方の装置でコンテキスト A がアクティブで、もう一方の装置でコンテキスト B がアクティブです。各コンテキストには「outside」という名前のインターフェイスがあり、両方とも **asr-group** 1 の一部として設定されています。発信トラフィックは、コンテキスト A がアクティブな装置を経由してルーティングされます。ただし、戻りトラフィックはコンテキスト B がアクティブな装置を経由してルーティングされています。通常、装置上に戻りトラフィックのセッション情報はないため、戻りトラフィックは廃棄されます。ただし、インターフェイスは **asr-group** 番号を使用して設定されているため、装置は同じ **asr-group** が割り当てられた他のインターフェイスのセッション情報を検索します。そして、装置上でスタンバイ ステートのコンテキスト A の外部インターフェイスでセッション情報を見つけて、戻りトラフィックをコンテキスト A がアクティブな装置に転送します。

トラフィックは、コンテキスト A がスタンバイ ステートの装置上でコンテキスト A の外部インターフェイスを経由して転送され、コンテキスト A がアクティブ ステートの装置上でコンテキスト A の外部インターフェイスを経由して返送されます。転送は、セッションが終了するまで継続します。

DHCP の設定

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。FWSM は DHCP サーバまたは DHCP リレー サービスを、FWSM インターフェイスに接続された DHCP クライアントに提供します。DHCP サーバはネットワーク コンフィギュレーション パラメータを直接 DHCP クライアントに提供します。DHCP リレーでは、あるインターフェイスで受信した DHCP 要求を、別のインターフェイスの背後に配置された外部 DHCP サーバに転送します。

ここでは、次の内容について説明します。

- DHCP サーバの設定（p.8-30）
- DHCP リレー サービスの設定（p.8-34）

DHCP サーバの設定

ここでは、FWSM の DHCP サーバを設定する方法を説明します。内容は次のとおりです。

- DHCP サーバのイネーブル化（p.8-30）
- DHCP オプションの設定（p.8-32）
- DHCP サーバで Cisco IP Phone を使用する方法（p.8-33）

DHCP サーバのイネーブル化

FWSM は DHCP サーバとして動作可能です。DHCP は、ホスト IP アドレス、デフォルト ゲートウェイ、DNS サーバなどのネットワーク設定値をホストに供給するプロトコルです。

（注） FWSM の DHCP サーバは BOOTP 要求をサポートしません。

マルチコンテキスト モードの場合、複数のコンテキストが使用するインターフェイス上で DHCP サーバまたは DHCP リレーをイネーブルにすることはできません。

FWSM の各インターフェイス上で DHCP サーバを設定できます。各インターフェイスは、アドレスを抽出する固有のアドレス プールを持つことができます。ただし、DNS サーバ、ドメイン名、オプション、ping タイムアウト、WINS サーバなどのその他の 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 サーバで使用されます。

DHCP クライアントまたは DHCP リレー サービスを、サーバがイネーブル化されたインターフェイス上で設定することはできません。また、DHCP クライアントは、サーバがイネーブル化されたインターフェイスに直接接続する必要があります。

特定の FWSM インターフェイス上で DHCP サーバをイネーブルにする手順は、次のとおりです。

ステップ 1　DHCP アドレス プールを作成します。次のコマンドを入力して、アドレス プールを定義します。

```
hostname(config)# dhcpd address ip_address-ip_address interface_name
```

FWSM は、このプールからアドレスを 1 つクライアントに割り当て、一定時間だけ使用できるようにします。これらのアドレスは、直接接続されたネットワークで使用する、変換されないローカル アドレスです。

アドレス プールは、FWSM インターフェイスと同じサブネットになければなりません。

ステップ 2　（任意）次のコマンドを入力して、クライアントに使用させる DNS サーバ（複数可）の IP アドレス（複数可）を指定します。

```
hostname(config)# dhcpd dns dns1 [dns2]
```

DNS サーバを 2 つまで指定できます。

ステップ 3　（任意）次のコマンドを入力して、クライアントに使用させる WINS サーバ（複数可）の IP アドレス（複数可）を指定します。

```
hostname(config)# dhcpd wins wins1 [wins2]
```

WINS サーバを 2 つまで指定できます。

ステップ 4　（任意）次のコマンドを入力して、クライアントに付与するリース期間を変更します。

```
hostname(config)# dhcpd lease lease_length
```

このリースとは、リース期限が切れるまでに、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）です。0 ～ 1,048,575 の値を入力します。デフォルトは 3600 秒です。

ステップ 5　（任意）次のコマンドを入力して、クライアントが使用するドメイン名を設定します。

```
hostname(config)# dhcpd domain domain_name
```

ステップ 6　（任意）次のコマンドを入力して、DHCP の ping タイムアウト値を設定します。

```
hostname(config)# dhcpd ping_timeout milliseconds
```

アドレスの競合を防ぐために、FWSM はアドレスを DHCP クライアントに割り当てる前に、アドレスに 2 つの ICMP ping パケットを送信します。このコマンドは、これらのパケットのタイムアウト値を指定します。

ステップ 7　（透過ファイアウォール モード）デフォルト ゲートウェイを定義します。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するには、次のコマンドを入力します。

```
hostname(config)# dhcpd option 3 ip gateway_ip
```

DHCP オプション 3 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 クライアントは管理インターフェイスの IP アドレスを使用します。管理インターフェイスは、トラフィックをルーティングしません。

ステップ 8　次のコマンドを入力して、FWSM 内の DHCP デーモンが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待ち受けるようにします。

```
hostname(config)# dhcpd enable interface_name
```

たとえば、内部インターフェイスに接続されたホストに 10.0.1.101 ～ 10.0.1.110 の範囲を割り当てる場合、次のコマンドを入力します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 209.165.201.2 209.165.202.129
hostname(config)# dhcpd wins 209.165.201.5
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

DHCP オプションの設定

RFC 2132 に示されている DHCP オプションの情報を送信するように FWSM を設定できます。DHCP オプションは次の 3 つのいずれかのカテゴリに属します。

- IP アドレスを返すオプション
- テキスト文字列を返すオプション
- 16 進数値を返すオプション

FWSM は、DHCP オプションの 3 つのカテゴリすべてをサポートします。DHCP オプションを設定するには、次のいずれかを実行します。

- 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、次のコマンドを入力します。

  ```
  hostname(config)# dhcpd option code ip addr_1 [addr_2]
  ```

- テキスト文字列を返す DHCP オプションを設定するには、次のコマンドを入力します。

  ```
  hostname(config)# dhcpd option code ascii text
  ```

- 16 進数値を返す DHCP オプションを設定するには、次のコマンドを入力します。

  ```
  hostname(config)# dhcpd option code hex value
  ```

(注) FWSM は、ユーザが指定したオプション タイプと値が RFC 2132 で定義されたオプション コードの予測タイプと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** を入力した場合、オプション 46 は RFC 2132 で 1 桁の 16 進数値として定義されているにもかかわらず、FWSM はこのコンフィギュレーションを受け付けます。オプション コードとオプション コードに対応付けられたタイプおよび予測値の詳細については、RFC 2132 を参照してください。

表 8-2 に、**dhcpd option** コマンドでサポートされない DHCP オプションを示します。

表 8-2　サポート対象外の 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

表 8-2　サポート対象外の DHCP オプション（続き）

オプション コード	説明
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

特定オプション（DHCP オプション 3、66、150）を使用して Cisco IP Phone を設定します。これらのオプションの設定については、「DHCP サーバで Cisco IP Phone を使用する方法」（p.8-33）を参照してください。

DHCP サーバで Cisco IP Phone を使用する方法

小規模な支社で構成される企業が Cisco IP Telephony Voice over IP（VoIP）ソリューションを実装する場合、通常、セントラル オフィスに Cisco CallManager を配置して、小規模な支社の Cisco IP Phone を制御します。この方式によって、コール処理を一元化し、必要な装置数を減らし、支社で Cisco CallManager やその他のサーバを管理する余分な負担を排除できます。

Cisco IP Phone は、TFTP サーバからコンフィギュレーションをダウンロードします。Cisco IP Phone が起動したときに、IP アドレスと TFTP サーバの IP アドレスの両方があらかじめ設定されていなかった場合、Cisco IP Phone はオプション 150 または 66 を指定した要求を DHCP サーバへ送り、この情報を取得します。

- DHCP オプション 150 を指定すると、TFTP サーバ リストの IP アドレスが得られます。
- DHCP オプション 66 を指定すると、単一 TFTP サーバの IP アドレスまたはホスト名が得られます。

Cisco IP Phone は、要求に DHCP オプション 3 を含めることもあります。この場合、デフォルト ルートが設定されます。

Cisco IP Phone は、1 つの要求にオプション 150 と 66 の両方を含めることがあります。この場合、FWSM DHCP サーバは、FWSM 上で値が設定されていれば、両方のオプションに対応する値を応答として提供します。

RFC 2132 で指定されている大部分のオプションに対応する情報を送信するように、FWSM を設定できます。次に、オプション番号の構文とともに、よく使用されるオプション 66、150、および 3 の構文を示します。

- 次のコマンドを入力して、RFC 2132 の指定に従って、オプション番号が含まれている DHCP 要求に対応する情報を提供します。

  ```
  hostname(config)# dhcpd option number value
  ```

- 次のコマンドを入力して、オプション 66 に対応する TFTP サーバの IP アドレスまたは名前を提供します。

  ```
  hostname(config)# dhcpd option 66 ascii server_name
  ```

- 次のコマンドを入力して、オプション 150 に対応する 1 つまたは 2 つの TFTP サーバの IP アドレスまたは名前を提供します。

  ```
  hostname(config)# dhcpd option 150 ip server_ip1 [server_ip2]
  ```

  server_ip1 はプライマリ TFTP サーバの IP アドレスまたは名前です。*server_ip2* は、セカンダリ TFTP サーバの IP アドレスまたは名前です。オプション 150 を使用して、最大 2 つの TFTP サーバを指定できます。
- デフォルト ルートを設定するには、次のコマンドを入力します。

  ```
  hostname(config)# dhcpd option 3 ip router_ip1
  ```

DHCP リレー サービスの設定

DHCP リレー エージェントを利用すると、FWSM はクライアントから異なるインターフェイスに接続されたルータへ DHCP 要求を転送できます。

DHCP リレー エージェントの利用には、次の制約があります。

- DHCP サーバ機能がイネーブルのときに、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。
- DHCP リレー サービスは、透過ファイアウォール 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。透過モードで DHCP 要求および応答が FWSM を通過できるようにするには、内部インターフェイスから外部インターフェイスへの DCHP 要求を許可するアクセス リストと、別方向のサーバからの応答を許可するアクセス リストの 2 つのアクセス リストを設定する必要があります。
- FWSM にクライアントを直接接続する必要があります。クライアントから別のリレー エージェントまたはルータを介して要求を送ることはできません。
- マルチコンテキスト モードの場合、複数のコンテキストが使用するインターフェイス上で DHCP リレーをイネーブルにすることはできません。

DHCP リレーをイネーブル化する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、DHCP クライアントと異なるインターフェイス上の DHCP サーバの IP アドレスを設定します。

```
hostname(config)# dhcprelay server ip_address if_name
```

このコマンドは 4 回まで使用でき、最大 4 サーバを指定できます。

ステップ 2　次のコマンドを入力して、クライアントに接続されたインターフェイス上で DHCP リレーをイネーブルにします。

```
hostname(config)# dhcprelay enable interface
```

ステップ 3　（任意）次のコマンドを入力して、リレー アドレス ネゴシエーションが可能な秒数を設定します。

```
hostname(config)# dhcprelay timeout seconds
```

ステップ 4　（任意）次のコマンドを入力して、DHCP サーバから FWSM インターフェイスのアドレスに送信されるパケットに組み込む、最初のデフォルト ルータ アドレスを変更します。

```
hostname(config)# dhcprelay setroute if_name
```

この作業によって、DHCP サーバで別のルータが指定されている場合でも、クライアントは FWSM に接続できるデフォルト ルートを設定できます。

パケットにデフォルト ルータ オプションが指定されていない場合、FWSM はインターフェイス アドレスが含まれているオプションを 1 つ追加します。

次に、FWSM が、内部インターフェイスに接続されたクライアントから外部インターフェイス上の DHCP サーバへ、DHCP 要求を転送できるようにする例を示します。

```
hostname(config)# dhcprelay server 201.168.200.4
hostname(config)# dhcprelay enable inside
hostname(config)# dhcprelay setroute inside
```

DHCP クライアントの設定

FWSM インターフェイスを DHCP クライアントとして設定するための手順は、次のとおりです。

```
hostname(config-if)# ip address dhcp [retry num] [setroute]
```

任意の ***retry*** *num* 引数は、インターフェイスが DHCP サーバへの接続を試行する回数を指定します。デフォルト値は 4 で、最大値は 48 です。***setroute*** キーワードでは、DHCP サーバが戻すデフォルト ゲートウェイを使用してデフォルト ルートが設定されます。

（注）　DHCP クライアントとして設定されたインターフェイス上で、DHCP サーバまたは DHCP リレー サービスをイネーブル化することはできません。

IPv6 の設定

この章では、FWSM で IPv6 をイネーブルにして設定する方法について説明します。IPv6 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。

この章で説明する内容は、次のとおりです。

- IPv6 対応 コマンド（p.9-2）
- インターフェイス上での IPv6 の設定（p.9-3）
- インターフェイス上でのデュアル IP スタックの設定（p.9-4）
- IPv6 重複アドレス検出の設定（p.9-5）
- IPv6 デフォルト / スタティック ルートの設定（p.9-6）
- IPv6 アクセス リストの設定（p.9-7）
- IPv6 ネイバ検出の設定（p.9-8）
- スタティック IPv6 ネイバの設定（p.9-12）
- IPv6 コンフィギュレーションの確認（p.9-13）

IPv6 の設定例については、「例 4：IPv6 の設定例」（p.B-14）を参照してください。

IPv6 対応 コマンド

IPv6 アドレスを受け付けて表示できる FWSM コマンドは次のとおりです。

- capture
- configure
- copy
- http
- name
- object-group
- ping
- show conn
- show local-host
- show tcpstat
- ssh
- telnet
- tftp-server
- who
- write

（注） フェールオーバー機能は IPv6 をサポートしません。**ipv6 address** コマンドは、フェールオーバー コンフィギュレーションのためのスタンバイ アドレスの設定はサポートしません。**failover interface ip** コマンドは、フェールオーバーおよびステートフル フェールオーバー インターフェイスでの IPv6 アドレスの使用はサポートしません。

IPv6 対応コマンドに IPv6 アドレスを入力する場合、**`ping fe80::2e0:b6ff:fe01:3b7a`** など IPv6 の標準表記法で入力します。FWSM は IPv6 アドレスを正しく認識して処理します。ただし、次のような状況では、IPv6 アドレスを角カッコ（[ ]）で囲む必要があります。

- アドレスのポート番号を指定する必要がある場合。例：**`[fe80::2e0:b6ff:fe01:3b7a]:8080`**
- **write net** コマンドや **config net** コマンドのように、コマンドで区切り記号としてコロンを使用する場合。例：**`configure net [fe80::2e0:b6ff:fe01:3b7a]:/tftp/config/pixconfig`**

次のコマンドは、IPv6 で使用するために変更されました。

- debug
- fragment
- ip verify
- mtu
- icmp（**ipv6 icmp** のように入力されます）

次のインスペクション エンジンは IPv6 に対応しています。

- FTP
- HTTP
- ICMP
- SMTP
- SIP
- TCP
- UDP

インターフェイス上での IPv6 の設定

少なくとも、各インターフェイスに IPv6 リンクローカル アドレスを設定する必要があります。インターフェイスにサイトローカル アドレスとグローバル アドレスを追加することもできます。

（注） FWSM は IPv6 エニキャスト アドレスをサポートしません。

1 つのインターフェイスに IPv6 アドレスと IPv4 アドレスの両方を設定できます。

（注） 複数のコンテキスト（共有 VLAN）で使用されているインターフェイスに IPv6 を設定することはできません。

インターフェイス上で IPv6 を設定するには、次の手順を実行します。

ステップ 1　IPv6 アドレスを設定するインターフェイスでインターフェイス コンフィギュレーション モードを開始します。

```
hostname(config)# interface interface_name
```

ステップ 2　インターフェイスの IPv6 アドレスを設定します。1 つのインターフェイスに、IPv6 リンクローカル、サイトローカル、グローバル アドレスなど複数の IPv6 アドレスを割り当てることができます。ただし、リンクローカル アドレスは必ず設定しなければなりません。

インターフェイスに IPv6 アドレスを設定する方法はいくつかあります。次の中から、ニーズに合った方法を選択してください。

- 最も簡単な方法は、インターフェイス上でステートレス自動設定をイネーブルにする方法です。インターフェイス上でステートレス自動設定をイネーブルにして、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クスに基づいて IPv6 アドレスを設定します。ステートレス自動設定がイネーブルの場合、修正 EUI-64 インターフェイス ID に基づいて、インターフェイスにリンクローカル アドレスが自動生成されます。ステートレス自動設定をイネーブルにするには、次のコマンドを入力します。

  ```
  hostname(config-if)# ipv6 address autoconfig
  ```

- インターフェイスにリンクローカル アドレスのみを設定し、他の IPv6 アドレスを割り当てる予定がない場合、リンクローカル アドレスを手動で定義するか、インターフェイス MAC アドレス（修正 EUI-64 形式）に基づいて生成できます。

  リンクローカル アドレスを手動で指定するには、次のコマンドを入力します。

  ```
  hostname(config-if)# ipv6 address ipv6-address link-local
  ```

次のコマンドを入力して、インターフェイス上で IPv6 をイネーブルにし、インターフェイス MAC アドレスに基づく修正 EUI-64 インターフェイス ID を使用してリンクローカル アドレスを自動生成します。

```
hostname(config-if)# ipv6 enable
```

（注） インターフェイス上に他の **ipv6 address** コマンドを入力する場合、**ipv6 enable** コマンドを使用する必要はありません。IPv6 アドレスをインターフェイスに割り当てると同時に、IPv6 対応は自動的にイネーブルになります。

- インターフェイスにサイトローカル アドレスまたはグローバル アドレスを割り当てます。サイトローカル アドレスまたはグローバル アドレスを割り当てると、リンクローカル アドレスが自動生成されます。インターフェイスにサイトローカル アドレスまたはグローバル アドレスを追加するには、次のコマンドを入力します。アドレスの下位 64 ビットで修正 EUI-64 インターフェイス ID を使用するには、任意の ***eui-64*** キーワードを使用します。

  ```
  hostname(config-if)# ipv6 address ipv6-address [eui-64]
  ```

ステップ 3　（任意）インターフェイス上でルータ アドバタイズメント メッセージをディセーブルにします。デフォルトでは、ルータ送信要求メッセージに対してルータ アドバタイズメント メッセージが自動的に送信されます。FWSM で IPv6 プレフィクスを提供しないインターフェイス上において（外部インターフェイスなど）、ルータ アドバタイズメント 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でルータ アドバタイズメント メッセージをディセーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd suppress-ra
```

インターフェイスに適用する IPv6 アドレスの例については、「例 4：IPv6 の設定例」（p.B-14）を参照してください。

インターフェイス上でのデュアル IP スタックの設定

FWSM では、1 つのインターフェイスに IPv6 と IPv4 の両方を設定できます。特別なコマンドを入力する必要はなく、通常の場合と同様に、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 コマンドを入力するだけで済みます。IPv4 と IPv6 の両方に対して、デフォルト ルートを設定する必要があります。

IPv6 重複アドレス検出の設定

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、まず新規リンクローカル アドレスで実行します。リンクローカル アドレスが一意であることが確認されたら、インターフェイス上の他のすべての IPv6 ユニキャスト アドレスに対して重複アドレス検出を実行します。

インターフェイスが「administratively down（管理者によって明示的に閉じられている）」ステートの場合、重複アドレス検出は停止されます。インターフェイスが「administratively down」ステートの間、インターフェイスに割り当てられたユニキャスト IPv6 アドレスは保留ステートに設定されます。インターフェイスが「administratively up」ステートに戻ると、インターフェイス上のすべてのユニキャスト IPv6 アドレスに対して重複アドレス検出が再開されます。

重複アドレスが識別されると、アドレスのステートは「DUPLICATE」に設定され、そのアドレスは使用されません。重複アドレスがインターフェイスのリンクローカル アドレスである場合、インターフェイス上での IPv6 パケットの処理はディセーブルになり、エラー メッセージが発行されます。重複アドレスがインターフェイスのグローバル アドレスである場合、そのアドレスは使用されず、エラー メッセージが発行されます。アドレスのステートは「DUPLICATE」に設定されますが、重複アドレスに関連するすべてのコンフィギュレーション コマンドは設定どおりに保持されます。

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ると、新しいリンクローカル アドレスに対して重複アドレス検出が実行され、インターフェイスに関連する他のすべての IPv6 アドレスが再生成されます（重複アドレス検出は新しいリンクローカル アドレスでのみ実行されます）。

FWSM は、ネイバ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、インターフェイスで重複アドレス検出が実行される回数は 1 回です。

重複アドレス検出の試行回数を変更するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd dad attempts value
```

value 引数には 0 ～ 600 までの任意の値を指定できます。*value* 引数を 0 に設定すると、インターフェイス上の重複アドレス検出がディセーブルになります。

複数の重複アドレス検出試行を送信するようにインターフェイスを設定する場合は、**ipv6 nd ns-interval** コマンドを使用してネイバ送信要求メッセージの送信間隔を設定できます。デフォルトでは、1000 ミリ秒ごとに送信されます。

ネイバ送信要求メッセージの間隔を変更するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd ns-interval value
```

value 引数には 1000 ～ 3,600,000 ミリ秒の値を指定できます。

（注） この値を変更すると、重複アドレス検出に使用される分だけでなく、インターフェイス上で送信されるすべてのネイバ送信要求メッセージの間隔が変更されます。

IPv6 デフォルト / スタティック ルートの設定

IPv6 ユニキャスト ルーティングは常にイネーブルです。インターフェイスで IPv6 がイネーブルになっていて、アクセス リストが IPv6 トラフィックを許可すれば、FWSM はインターフェイス間でトラフィックをルーティングします。**ipv6 route** コマンドを使用して、デフォルト ルートおよびスタティック ルートを追加できます。

IPv6 デフォルト / スタティック ルートを設定するには、次の手順を実行します。

ステップ 1　デフォルト ルートを追加するには、次のコマンドを入力します。

```
hostname(config)# ipv6 route interface_name ::/0 next_hop_ipv6_addr
```

アドレス ::/0 は、「any」に相当する IPv6 の形式です。

ステップ 2　(任意)IPv6 スタティック ルートを定義します。IPv6 スタティック ルートを IPv6 ルーティング テーブルに追加するには、次のコマンドを使用します。

```
hostname(config)# ipv6 route if_name destination next_hop_ipv6_addr [admin_distance]
```

(注)　**ipv6 route** コマンドは、IPv4 スタティック ルートを定義するための **route** コマンドと同じ役割を果たします。

デフォルト ルートを設定するための **ipv6 route** コマンドの例については、「例 4：IPv6 の設定例」(p.B-14)を参照してください。

IPv6 アクセス リストの設定

IPv6 アクセス リストの設定は、IPv6 アドレスを扱う点が異なるだけで、IPv4 アクセス リストの設定とほぼ同じです。

IPv6 アクセス リストを設定するには、次の手順を実行します。

ステップ 1　アクセス エントリを作成します。アクセス リストを作成するには、**ipv6 access-list** コマンドを使用してアクセス リストのエントリを作成します。このコマンドには ICMP トラフィック専用のアクセス リスト エントリを作成するための形式と、他のすべてのタイプの IP トラフィックのアクセス リスト エントリを作成するための形式という 2 つの形式があり、どちらかを選択します。

- ICMP トラフィック専用の IPv6 アクセス リスト エントリを作成するには、次のコマンドを入力します。

  ```
  hostname(config)# ipv6 access-list id [line num] {permit | deny} icmp source
  destination [icmp_type]
  ```

- IPv6 アクセス リスト エントリを作成するには、次のコマンドを入力します。

  ```
  hostname(config)# ipv6 access-list id [line num] {permit | deny} protocol source
  [src_port] destination [dst_port]
  ```

次に、**ipv6 access-list** コマンドの引数について説明します。

- *id* — アクセス リストの名前。アクセス リストに複数のエントリを入力する場合、各コマンドに同じ *id* を使用します。
- **line** *num* — アクセス リストにエントリを追加するときに、エントリを表示するリスト内の行番号を指定できます。
- ***permit*** | ***deny*** — 指定トラフィックをブロックするか通過させるかを決定します。
- ***icmp*** — アクセス リスト エントリを ICMP トラフィックに適用することを示します。
- *protocol* — アクセス リスト エントリで制御するトラフィックを指定します。IP プロトコルの名前（***ip***、***tcp***、または ***udp***）または数字（1 ～ 254）を指定できます。***object-group*** *grp_id* を使用してプロトコル オブジェクト グループを指定することもできます。
- *source* および *destination* — トラフィックの送信元または宛先を指定します。送信元または宛先には、アドレス範囲を示す *prefix/length* 形式の IPv6 プレフィクス、任意のアドレスを指定するキーワード ***any***、または ***host*** *host_ipv6_addr* によって指定される特定ホストを指定できます。
- *src_port* および *dst_port* — 送信元ポートと宛先ポート（またはサービス）の引数。演算子（***lt*** [より小さい]、***gt*** [より大きい]、***eq*** [等しい]、***neq*** [等しくない]、***range*** [包括的範囲]）の後にスペースとポート番号（または ***range*** キーワードをスペースで区切った 2 つのポート番号）を入力します。
- *icmp_type* — アクセス ルールでフィルタリングする ICMP メッセージ タイプを指定します。値には、有効な ICMP タイプ数（0 ～ 155）、または付録 D「アドレス、プロトコル、およびポート」に示す ICMP タイプの文字名の 1 つを指定できます。***object-group*** *id* を使用して ICMP オブジェクト グループを指定することもできます。

ステップ 2　次のコマンドを入力して、アクセス リストをインターフェイスに適用します。

```
hostname(config)# access-group access_list_name {in | out} interface if_name
```

IPv6 アクセス リストの例については、「例 4：IPv6 の設定例」（p.B-14）を参照してください。

IPv6 ネイバ検出の設定

IPv6 ネイバ検出プロセスでは ICMPv6 メッセージおよび送信要求ノードのマルチキャスト アドレスを使用して、同一ネットワーク（ローカル リンク）上のネイバのリンク層アドレスの特定、ネイバの到達可能性の検証、近接ルータの追跡を行います。

ここでは、次の内容について説明します。

- ネイバ送信要求メッセージの設定（p.9-8）
- ルータ アドバタイズメント メッセージの設定（p.9-9）

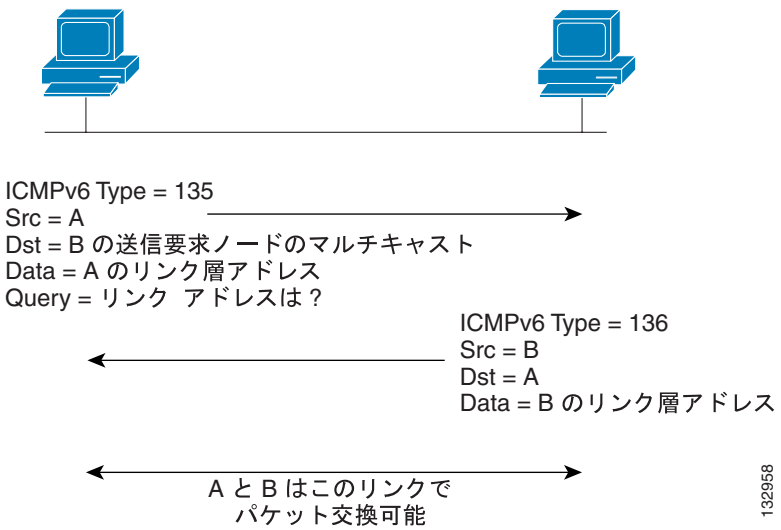
ネイバ送信要求メッセージの設定

ネイバ送信要求メッセージ（ICMPv6 Type 135）は、ノードがローカル リンク上の別のノードのリンク層アドレスの検出を試行する場合に、ローカル リンク上に送信されます。ネイバ送信要求メッセージは送信要求ノードのマルチキャスト アドレスに送信されます。ネイバ送信要求メッセージの送信元アドレスは、ネイバ送信要求メッセージを送信するノードの IPv6 アドレスです。ネイバ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。

ネイバ送信要求メッセージの受信後、宛先ノードは、ネイバ アドバタイズメント メッセージ（ICMPv6 Type 136）をローカル リンク上に送信して応答します。ネイバ アドバタイズメント メッセージの送信元アドレスは、ネイバ アドバタイズメント メッセージを送信するノードの IPv6 アドレスです。宛先アドレスは、ネイバ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 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 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。

送信元ノードと宛先ノードが通信できるのは、送信元ノードがネイバ アドバタイズメントを受信したあとです。図 9-1 に、ネイバ送信要求および応答プロセスを示します。

図 9-1　IPv6 ネイバ検出 — ネイバ送信要求メッセージ



ネイバ送信要求メッセージを使用して、ネイバのリンク層アドレスが特定されたあと、ネイバの到達可能性を検証することもできます。ノードでネイバの到達可能性を検証する場合、ネイバ送信要求メッセージの宛先アドレスは、ネイバのユニキャスト アドレスです。

ローカル リンク上のノードのリンク層アドレスに変更がある場合も、ネイバ アドバタイズメント メッセージが送信されます。この場合、ネイバ アドバタイズメントの宛先アドレスは、全ノードのマルチキャスト アドレスとなります。

ネイバ送信要求メッセージの間隔とネイバ到達可能時間を、インターフェイス単位で設定できます。詳細については、次の項を参照してください。

- ネイバ送信要求メッセージの間隔の設定（p.9-9）
- ネイバ到達可能時間の設定（p.9-9）

ネイバ送信要求メッセージの間隔の設定

インターフェイス上の IPv6 ネイバ送信要求の再送信間隔を設定するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd ns-interval value
```

value 引数の有効値は 1000 ～ 3,600,000 ミリ秒です。デフォルト値は 1000 ミリ秒です。

この設定は、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。

ネイバ到達可能時間の設定

ネイバ到達可能時間により、使用できないネイバを検出できます。短い値を設定すると、使用できないネイバをより速く検出できますが、IPv6 ネットワークの帯域幅およびすべての IPv6 ネットワーク デバイスの処理リソースの消費が大きくなります。IPv6 の標準運用では、非常に短い値を設定することは推奨しません。

到達可能性確認イベントの発生後、リモート IPv6 ノードを到達可能とみなす時間を設定するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd reachable-time value
```

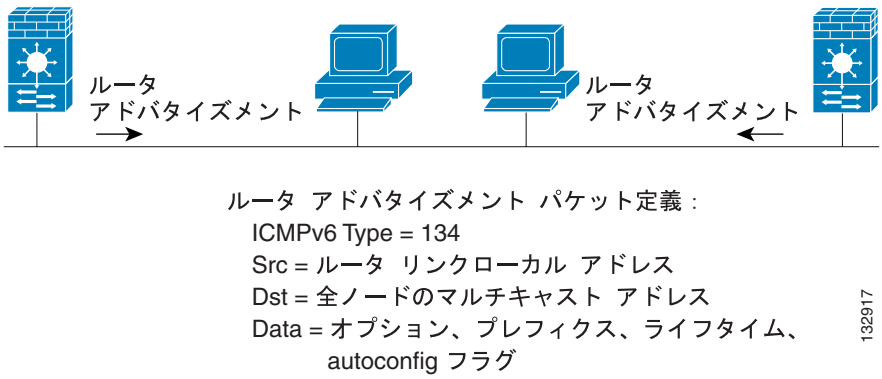
value 引数の有効値は 0 ～ 3,600,000 ミリ秒です。デフォルトは 0 です。

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。

ルータ アドバタイズメント メッセージの設定

ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、FWSM の各 IPv6 対応インターフェイスに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、全ノードのマルチキャスト アドレスに送信されます。

図 9-2　IPv6 ネイバ検出 — ルータ アドバタイズメント メッセージ



ルータ アドバタイズメント メッセージには、通常、次の情報が含まれます。

- 1 つまたは複数の IPv6 プレフィクス。ローカル リンク上のノードは、このプレフィクスを使用してノードの IPv6 アドレスを自動設定します。
- アドバタイズメントに含まれる各プレフィクスのライフタイム情報。
- 実行可能な自動設定の種類（ステートレスまたはステートフル）を示す複数のフラグ。
- デフォルトのルータ情報（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かどうか、使用する場合、ルータをデフォルト ルータとして使用する時間 [秒]）。
- ホップ制限やホストが送信するパケットに使用すべき MTU など、ホストの追加情報。
- 所定のリンク上で、ネイバ送信要求メッセージを再送信する時間間隔。
- ノードがネイバを到達可能とみなす時間。

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の応答でも使用されます（ICMPv6 Type 133）。ルータ送信要求メッセージは、システム起動時にホストによって送信されます。これにより、ホストは次に予定されているルータ アドバタイズメント メッセージを待たずに、ただちに自動設定できます。ルータ送信要求メッセージは一般にシステム起動時にホストによって送信され、ホストには設定済みのユニキャスト アドレスはないため、ルータ送信要求メッセージの送信元アドレスは一般に未指定のアドレス（0:0:0:0:0:0:0:0）になります。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 アドレスは、メッセージ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、リンクのスコープを持つ全ルータのマルチキャスト アドレスです。ルータ アドバタイズメントがルータ送信要求の応答として送信される場合、ルータ アドバタイズメント メッセージの宛先アドレスは、ルータ送信要求メッセージの送信元のユニキャスト アドレスとなります。

ルータ アドバタイズメント メッセージには次の値を設定できます。

- 定期的なルータ アドバタイズメント メッセージ間の時間間隔
- ルータのライフタイム値。この値は、IPv6 ノードが FWSM をデフォルト ルータとみなす時間を示します。
- リンクで使用する IPv6 ネットワークのプレフィクス
- インターフェイスがルータ アドバタイズメント メッセージを伝送するかどうか。

特に明記しないかぎり、ルータ アドバタイズメント メッセージの設定はインターフェイス固有であり、インターフェイス コンフィギュレーション モードで開始されます。これらの設定の変更方法については、次の項を参照してください。

- ルータ アドバタイズメント送信間隔の設定（p.9-10）
- ルータのライフタイム値の設定（p.9-11）
- IPv6 プレフィクスの設定（p.9-11）
- ルータ アドバタイズメント メッセージのディセーブル（p.9-11）

ルータ アドバタイズメント送信間隔の設定

デフォルトでは、ルータ アドバタイズメントは 200 秒ごとに送信されます。インターフェイス上のルータ アドバタイズメント送信間隔を変更するには、次のコマンドを入力します。

```
ipv6 nd ra-interval [msec] value
```

有効値の範囲は 3 ～ 1800 秒（**msec** キーワードを使用する場合は 500 ～ 1,800,000 ミリ秒）です。

FWSM が **ipv6 nd ra-lifetime** コマンドを使用してデフォルト 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内でなければなりません。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。

ルータのライフタイム値の設定

ルータのライフタイム値は、ローカル リンク上のノードが FWSM をリンクのデフォルト ルータとみなす時間を指定します。

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 ライフタイム値を設定するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd ra-lifetime seconds
```

有効値の範囲は 0 ～ 9000 秒です。デフォルトは 1800 秒です。値 0 は、FWSM を選択したインターフェイス上のデフォルト ルータとしてみなすべきではないことを示します。

IPv6 プレフィクスの設定

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た IPv6 プレフィクスを使用して、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。

どの IPv6 プレフィクスを IPv6 ルータ アドバタイズメントに含めるかを設定するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd prefix ipv6-prefix/prefix-length
```

（注） 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クスの長さが常に 64 ビットである必要があります。

ルータ アドバタイズメント メッセージのディセーブル

デフォルトでは、ルータ送信要求メッセージに対してルータ アドバタイズメント メッセージが自動的に送信されます。FWSM で IPv6 プレフィクスを提供しないインターフェイス上において（外部インターフェイスなど）、ルータ アドバタイズメント 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で IPv6 ルータ アドバタイズメントを送信しないようにするには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd suppress-ra
```

スタティック IPv6 ネイバの設定

IPv6 ネイバ キャッシュでネイバを手動で定義できます。指定した IPv6 アドレスのエントリがすでにネイバ検出キャッシュにある場合（IPv6 ネイバ検出プロセスで学習した場合）、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 ネイバ検出キャッシュ内のスタティック エントリは、ネイバ検出プロセスでは変更されません。

IPv6 ネイバ検出キャッシュ内のスタティック エントリを設定するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 neighbor ipv6_address if_name mac_address
```

ipv6_address 引数はネイバの IPv6 リンクローカルアドレス、*if_name* 引数はネイバの使用が可能なインターフェイス、*mac_address* 引数は近接インターフェイスの MAC アドレスです。

（注）**clear ipv6 neighbors** コマンドは IPv6 ネイバ検出キャッシュからスタティック エントリを削除しません。

IPv6 コンフィギュレーションの確認

ここでは、IPv6 コンフィギュレーションを確認する方法について説明します。さまざまな表示コマンドを使用して、IPv6 設定を確認できます。

このセクションでは、次の内容について説明します。

- IPv6 インターフェイス設定の表示（p.9-13）
- IPv6 ルートの表示（p.9-14）

IPv6 インターフェイス設定の表示

IPv6 インターフェイス設定を表示するには、次のコマンドを入力します。

```
hostname# show ipv6 interface [if_name]
```

「outside」などのインターフェイス名を入れると、指定したインターフェイスの設定が表示されます。名前をコマンドから除外すると、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。コマンドの出力には次の事項が表示されます。

- インターフェイスの名前とステータス
- リンクローカル アドレスとユニキャスト 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
- ネイバ検出設定

次に、**show ipv6 interface** コマンドの出力例を示します。

```
hostname# show ipv6 interface

ipv6interface is down, line protocol is down
  IPv6 is enabled, link-local address is fe80::20d:88ff:feee:6a82 [TENTATIVE]
  No global unicast address is configured
  Joined group address(es):
    ff02::1
    ff02::1:ffee:6a82
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
```

（注） **show interface** コマンドは、インターフェイスの IPv4 設定のみを表示します。インターフェイスの IPv6 コンフィギュレーションを表示するには、**show ipv6 interface** コマンドを使用します。**show ipv6 interface** コマンドは、インターフェイスの IPv4 設定は表示しません（インターフェイス上で両方が設定されている場合）。

IPv6 ルートの表示

IPv6 ルーティング テーブルのルートを表示するには、次のコマンドを入力します。

```
hostname# show ipv6 route
```

show ipv6 route コマンドの出力は、IPv4 **show route** コマンドの出力とほぼ同じです。次の情報が表示されます。

- ルートを導出したプロトコル
- リモート ネットワークの IPv6 プレフィクス
- ルートの管理ディスタンスおよびメトリック
- ネクストホップ ルータのアドレス
- ネクストホップ ルータから指定ネットワークに到達するためのインターフェイス

次に、**show ipv6 route** コマンドの出力例を示します。

```
hostname# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   ff00::/8 [0/0]
     via ::, inside
```

アクセス リストでのトラフィックの識別

この章では、アクセス リストでトラフィックを識別する方法について説明します。アクセス リストはさまざまな機能で使用します。Modular Policy Framework を使用する機能の場合、アクセス リストを使用してトラフィック クラス マップ内のトラフィックを識別できます。Modular Policy Framework の詳細については、第 18 章「モジュラ ポリシー フレームワークの使用」を参照してください。この章で説明する内容は、次のとおりです。

- アクセス リストの概要（p.10-2）
- 拡張アクセス リストの追加（p.10-7）
- EtherType アクセス リストの追加（p.10-10）
- 標準アクセス リストの追加（p.10-12）
- オブジェクトのグループ化によるアクセス リストの簡素化（p.10-13）
- アクセス リストへのコメントの追加（p.10-20）
- 拡張アクセス リストのアクティベーションのスケジューリング（p.10-21）
- アクセス リスト アクティビティのロギング（p.10-23）

IPv6 アクセス リストの詳細については、「IPv6 アクセス リストの設定」（p.9-7）を参照してください。

アクセス リストの概要

アクセス リストは 1 つまたは複数の Access Control Entry（ACE; アクセス制御エントリ）からなります。ACE は許可または拒否のルールを指定する、アクセス リストの個々のエントリであり、プロトコル、送信元 IP アドレス、宛先 IP アドレス、またはネットワークに適用されます。任意で、送信元ポートと宛先ポートにも適用されます。

このセクションでは、次の内容について説明します。

- アクセス リストのタイプ（p.10-2）
- ACE の順序（p.10-3）
- アクセス リストの暗黙拒否（p.10-3）
- NAT 使用時のアクセス リスト用 IP アドレス（p.10-3）
- アクセス リストのコミット（p.10-5）
- ACE の最大数（p.10-6）

アクセス リストのタイプ

表 10-1 に、アクセス リストのタイプと一般的な用途を示します。

表 10-1　アクセス リストのタイプと一般的な用途

アクセス リストの用途	アクセス リストのタイプ	説明
IP トラフィック（ルーテッド / 透過モード）のネットワーク アクセスの制御	拡張	FWSM は、拡張アクセス リストで明示的に許可されていないかぎり、どのようなトラフィックも通過させません。 **（注）** 管理アクセス用に FWSM インターフェイスにアクセスするために、アクセス リストでホスト IP アドレスを許可する必要はありません。第 21 章「管理アクセスの設定」に従って管理アクセスを設定するだけで済みます。
AAA ルールの対象トラフィックの特定	拡張	AAA ルールではアクセス リストを使用してトラフィックを特定します。
特定ユーザの IP トラフィックについてネットワーク アクセスの制御	拡張、ユーザ別に 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 アクセス リストをダウンロードするように RADIUS サーバを設定できます。 RADIUS サーバは FWSM ですでに設定済みのアクセス リストの名前を送信することもできます。
NAT（ポリシー NAT および NAT 除外）の対象アドレスの特定	拡張	ポリシー NAT では、拡張アクセス リストで送信元アドレスと宛先アドレスを指定することによって、アドレス変換対象のローカル アドレスを特定します。
VPN アクセスの確立	拡張	VPN コマンドで拡張アクセス リストを使用できます。
トラフィック クラス マップでの Modular Policy のトラフィックの識別	拡張 EtherType	Modular Policy Framework をサポートする機能では、アクセス リストを使用してクラス マップ内のトラフィックを識別できます。Modular Policy Framework をサポートする機能には、TCP、一般的な接続設定、インスペクションなどがあります。

表 10-1　アクセス リストのタイプと一般的な用途（続き）

アクセス リストの用途	アクセス リストのタイプ	説明
透過ファイアウォール モードにおける IP 以外のトラフィックのネットワーク アクセス制御	EtherType	EtherType に基づいてトラフィックを制御するアクセス リストを設定できます。
OSPF ルート再分配の指定	標準	標準アクセス リストには、宛先アドレスのみが含まれます。標準アクセス リストを使用して、OSPF ルートの再分配を制御できます。

ACE の順序

アクセス リストは 1 つまたは複数の ACE からなります。アクセス リストのタイプに応じて、送信元アドレス、宛先アドレス、プロトコル、ポート（TCP または UDP の場合）、ICMP タイプ（ICMP の場合）、または EtherType を指定できます。

任意のアクセス リスト名に入力した各 ACE は、ACE で行番号を指定した場合を除き、アクセス リストの末尾に追加されます（拡張アクセス リストのみ）。

ACE の順序は重要です。FWSM がパケットを転送するかまたは廃棄するかを決定する場合、FWSM は各 ACE に対して、エントリが指定された順番どおりにパケットをテストします。一致すると、それ以上、ACE は確認されません。たとえば、アクセス リストの先頭に、すべてのトラフィックを許可する ACE を設定した場合は、後ろのステートメントはいっさい確認されません。

ACE を非アクティブ状態にすることで、ACE をディセーブルにできます。

アクセス リストの暗黙拒否

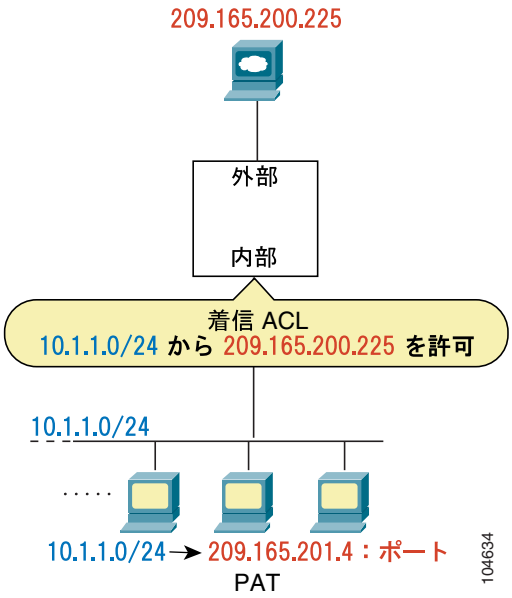
アクセス リストはリストの末尾に暗黙の拒否があるので、明示的に許可しないかぎり、トラフィックは通過できません。たとえば、特定のアドレスを除くすべてのユーザに、FWSM を通過してネットワークにアクセスすることを許可する場合、特定のアドレスを拒否したうえで、他のすべてのユーザを許可します。

NAT 使用時のアクセス リスト用 IP アドレス

NAT を使用する場合、アクセス リストに指定する IP アドレスは、アクセス リストを結合するインターフェイスによって決まります。インターフェイスに接続したネットワーク上で有効なアドレスを使用する必要があります。この注意事項は着信アクセス グループと発信アクセス グループの両方に当てはまります。使用するアドレスは方向によって左右されません。アドレスを決定付けるのはインターフェイスだけです。

たとえば、内部インターフェイスの着信方向に対してアクセス リストを適用する場合、外部アドレスへのアクセス時に、内部送信元アドレスに NAT を実行するように FWSM を設定します。内部インターフェイスにアクセス リストが適用されるので、送信元アドレスは変換されていない元のアドレスになります。外部アドレスが変換されないので、アクセス リストで使用する宛先アドレスは実アドレスです（図 10-1 を参照）。

図 10-1　アクセス リストの IP アドレス：送信元アドレスに NAT を使用

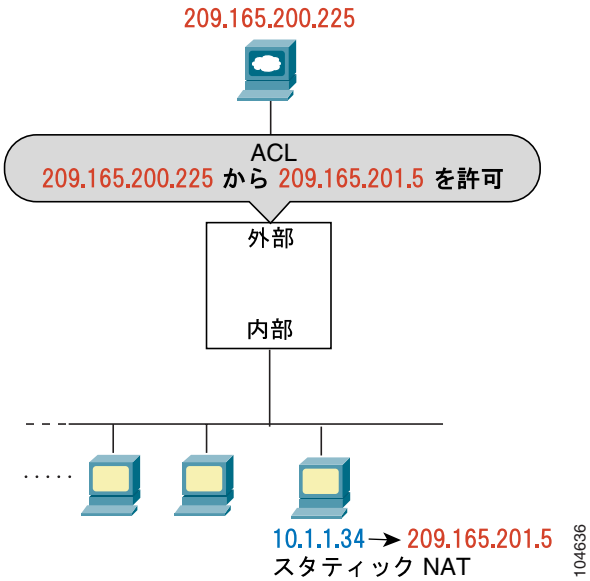


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# access-list INSIDE extended permit ip 10.1.1.0 255.255.255.0 host
209.165.200.225
hostname(config)# access-group INSIDE in interface inside
```

外部ホストから内部ホストにアクセスできるようにする場合は、外部インターフェイス上で着信アクセス リストを適用できます。アクセス リストに内部ホストの変換後のアドレスを指定する必要があります。これが外部ネットワーク上で使用できるアドレスであるためです（図 10-2 を参照）。

図 10-2　アクセス リストの IP アドレス：宛先アドレスに NAT を使用

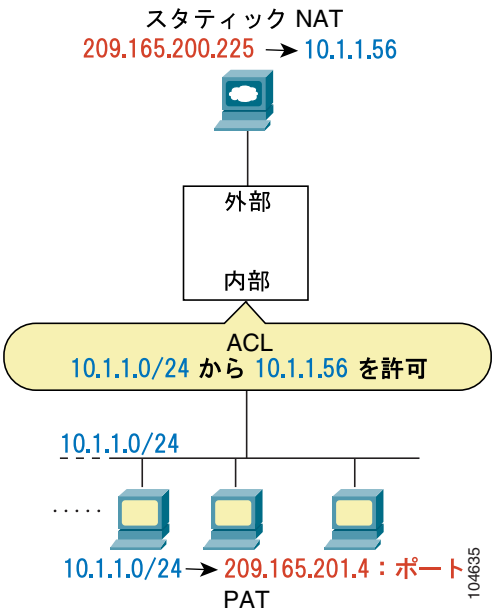


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# access-list OUTSIDE extended permit ip host 209.165.200.225 host
209.165.201.5
hostname(config)# access-group OUTSIDE in interface outside
```

両方のインターフェイスで NAT を実行する場合は、個々のインターフェイスに見せるアドレスを覚えておいてください。図 10-3 では、外部サーバがスタティック NAT を使用するので、変換されたアドレスが内部ネットワークに表示されます。

図 10-3　アクセス リストの IP アドレス：送信元および宛先アドレスに NAT を使用



この例に対応するコマンドは、次のとおりです。

```
hostname(config)# access-list INSIDE extended permit ip 10.1.1.0 255.255.255.0 host
10.1.1.56
hostname(config)# access-group INSIDE in interface inside
```

アクセス リストのコミット

アクセス リストに ACE が追加されると、FWSM はネットワーク プロセッサにアクセス リストをコミットすることによって、そのアクセス リストをアクティブにします。FWSM は、最後の **access-list** コマンドが入力されたあと、短い時間待ってからアクセス リストをコミットします。コミット開始後に ACE を入力すると、FWSM はこのコミットを打ち切り、短い待機時間のあとにアクセス リストを再コミットします。FWSM がアクセス リストをコミットすると、次のようなメッセージが表示されます。

```
Access Rules Download Complete: Memory Utilization: < 1%
```

約 60 K の ACE で構成される大きなアクセス リストの場合、大きさにより、コミットに 3 ～ 4 分かかることがあります。

メモリ限度の超過については、「ACE の最大数」（p.10-6）を参照してください。

ACE の最大数

FWSM は、シングルモードの場合、システム全体で最大 80 K、マルチモードで 142 K のルールをサポートします。ルールには ACE、ポリシー NAT に使用される ACE、フィルタ、AAA、ICMP、Telnet、SSH、HTTP、および確立されたルールが含まれます。

アクセス リストによっては、他のアクセス リストよりメモリを多く使用します。大きいポート番号範囲やオーバーラップしたネットワーク（たとえば、ある ACE で 10.0.0.0/8 を指定し、別の ACE で 10.1.1.0/24 を指定して、ACE のネットワークがオーバーラップする場合など）を使用するアクセス リストがこれに該当します。アクセス リストのタイプによって、システムがサポートできる実際の限度は 80 K 未満（シングルモード）または 142 K（マルチモード）未満になります。

ACE でオブジェクト グループを使用した場合、実際に入力する ACE の数は少なくなりますが、*拡張* ACE の数はオブジェクト グループを使用しない場合と同じになり、拡張 ACE カウントがシステム限度に近づきます。アクセス リストに指定されている拡張 ACE の数を確認するには、**show access-list** コマンドを入力します。

ACE を追加して、FWSM がアクセス リストをコミットすると、コンソールに次のようなメッセージで使用メモリが表示されます。

```
Access Rules Download Complete: Memory Utilization: < 1%
```

メモリ限度を超えると、エラー メッセージとシステム メッセージ（106024）が表示され、このコミットで追加されたすべてのアクセス リストがコンフィギュレーションから削除されます。前回のコミットで正常にコミットされた 1 組のアクセス リストだけが使用されます。たとえば、プロンプトに 1000 個の ACE をペーストし、最後の ACE でメモリ限度を超えた場合、1000 個の ACE がすべて拒否されます。

拡張アクセス リストの追加

ここでは、拡張アクセス リストの追加方法について説明します。内容は次のとおりです。

- 拡張アクセス リストの概要（p.10-7）
- 拡張 ACE の追加（p.10-8）

拡張アクセス リストの概要

拡張アクセス リストは 1 つまたは複数の ACE からなり、ACE を挿入する行番号、送信元アドレスおよび宛先アドレス、ACE タイプに応じてプロトコル、ポート（TCP/UDP の場合）、または ICMP タイプ（ICMP の場合）を指定できます。これらのすべてのパラメータを **access-list** コマンドで指定できます。または、各パラメータに対応するオブジェクト グループを使用することもできます。ここでは、コマンド内でパラメータを指定する方法について説明します。オブジェクト グループを使用する場合は、「オブジェクトのグループ化によるアクセス リストの簡素化」（p.10-13）を参照してください。

ACE の末尾に追加できるロギング オプションについては、「アクセス リスト アクティビティのロギング」（p.10-23）を参照してください。時間範囲オプションについては、「拡張アクセス リストのアクティベーションのスケジューリング」（p.10-21）を参照してください。

TCP/UDP 接続に関しては、トラフィックを戻すためにアクセス リストを使用する必要はありません。FWSM は、確立済みの双方向接続でのすべての戻りトラフィックを許可するからです。ただし、ICMP などのコネクションレス型プロトコルの場合、FWSM は単方向セッションを確立するため、アクセス リストで（アクセス リストを送信元インターフェイスと宛先インターフェイスに適用することによって）双方向で ICMP を使用できるようにするか、または ICMP インスペクション エンジンをイネーブルにする必要があります。ICMP インスペクション エンジンは、ICMP セッションを双方向接続として扱います。

インターフェイスの各方向に、各タイプ（拡張および EtherType）のアクセス リストを 1 つだけ適用できます。同じアクセス リストを複数のインターフェイスに適用することもできます。アクセス リストのインターフェイスへの適用の詳細については、第 11 章「ネットワーク アクセスの許可または拒否」を参照してください。

（注） アクセス リストの設定を変更し、既存の接続がタイムアウトする前に新しいアクセス リスト情報を使用したい場合、**clear local-host** コマンドを使用して接続を消去できます。

透過ファイアウォールを通過できる特殊な IP トラフィック

ルーテッド ファイアウォール モードでは、一部の IP トラフィック タイプはアクセス リストで許可されていてもブロックされます。サポートされないダイナミック ルーティング プロトコル、DHCP（DHCP リレーを設定している場合を除く）などです。透過ファイアウォール モードでは、すべての IP トラフィックの通過を許可します。このような特殊なトラフィック タイプはコネクションレス型であり、両方のインターフェイスにアクセス リストを適用しなければならないので、戻りトラフィックの通過が可能です。

表 10-2 に、透過ファイアウォールを通過させることができる一般的なトラフィック タイプを示します。

表 10-2　透過ファイアウォールの特殊なトラフィック

トラフィック タイプ	プロトコルまたはポート	説明
BGP	TCP ポート 179	—
DHCP	UDP ポート 67 および 68	DHCP サーバをイネーブルにした場合、FWSM は DHCP パケットを通過させません。
EIGRP	プロトコル 88	—
OSPF	プロトコル 89	—
マルチキャスト ストリーム	UDP ポートはアプリケーションに応じて変動	マルチキャスト ストリームの宛先は常にクラス D アドレス（224.0.0.0 ～ 239.x.x.x）です。
RIP（v1 または v2）	TCP ポート 520	—

拡張 ACE の追加

任意のアクセス リスト名を指定して **access-list** コマンドを入力すると、**line** の番号を指定する場合を除き、そのアクセス リストの末尾に ACE が追加されます。

次のコマンドを入力して、ACE を追加します。

```
hostname(config)# access-list access_list_name [line line_number] [extended]
{deny | permit} protocol source_address mask [operator port] dest_address mask
[operator port | icmp_type] [inactive]
```

ヒント　コンフィギュレーションを確認するときに名前をわかりやすくするために、アクセス リスト名は大文字で入力してください。インターフェイスを示すアクセス リスト名（INSIDE など）、または作成された目的を示すアクセス リスト名（NO_NAT、VPN など）を指定できます。

通常、プロトコルとして **ip** キーワードを指定しますが、他のプロトコルも受け付けることができます。プロトコル名のリストについては、「プロトコルおよびアプリケーション」（p.D-13）を参照してください。

単一アドレスを指定する場合は、IP アドレスの前に **host** キーワードを入力します。この場合、マスクは入力しません。すべてのアドレスを指定する場合は、アドレスとマスクの代わりに **any** キーワードを入力します。

送信元ポートと宛先ポートは、**tcp** または **udp** プロトコルに対してのみ指定できます。使用できるキーワードおよび well-known ポートの割り当てについては、「TCP ポートおよび UDP ポート」（p.D-14）を参照してください。DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk はいずれも、TCP 用の定義と UDP 用の定義が 1 つずつ必要です。TACACS+ は、TCP ポート 49 の定義が 1 つ必要です。

*演算子*を使用して、送信元または宛先に使用させるポート番号を一致させます。使用できる演算子は、次のとおりです。

- **lt** — less than（より小さい）
- **gt** — greater than（より大きい）
- **eq** — equal to（等しい）
- **neq** — not equal to（等しくない）

- **range** — 指定された値を含めた範囲。この演算子を使用する場合は、次の例のように、2 つのポート番号を指定します。

  ```
  range 100 200
  ```

ICMP タイプは **icmp** プロトコルに対してのみ指定できます。ICMP はコネクションレス型プロトコルなので、アクセス リストを使用して（送信元インターフェイスと宛先インターフェイスにアクセス リストを適用することによって）双方向で ICMP を使用できるようにするか、または ICMP インスペクション エンジンをイネーブルにする必要があります（「ICMP タイプ オブジェクト グループの追加」[p.10-16] を参照）。ICMP インスペクション エンジンは、ICMP セッションをステートフル接続として扱います。ping を制御するには、**echo-reply**（**0**）（FWSM からホストへ）または **echo**（**8**）（ホストから FWSM へ）を指定します。ICMP タイプのリストについては、「ICMP タイプ オブジェクト グループの追加」（p.10-16）を参照してください。

ネットワーク マスクを指定する方法は、Cisco IOS ソフトウェアの **access-list** コマンドとは異なります。FWSM ではネットワーク マスクを使用します（クラス C マスクには 255.255.255.0 など）。Cisco IOS ではマスクはワイルドカード ビットを使用します（0.0.0.255 など）。

ACE を非アクティブ状態にするには、**inactive** キーワードを使用します。再度イネーブルにするには、**inactive** キーワードを使用せずに全 ACE を入力します。この機能によってコンフィギュレーション内の非アクティブな ACE を記録し、再イネーブルを容易にすることができます。

次の例を参照してください。

次のアクセス リストは、（アクセス リストが適用されるインターフェイス上の）すべてのホストに FWSM の通過を許可します。

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

次のアクセス リストの例は、192.168.1.0/24 上のホストに対して、ネットワーク 209.165.201.0/27 へのアクセスを阻止します。それ以外のすべてのアドレスは許可されます。

```
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
```

アクセスを一部のホストだけに限定する場合は、制限付き許可 ACE を入力します。デフォルトでは、他のすべてのトラフィックは明示的に許可しないかぎり拒否されます。

```
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
```

次のアクセス リストは、（アクセス リストが適用されるインターフェイス上の）すべてのホストに対して、アドレス 209.165.201.29 の Web サイトへのアクセスを制限します。その他のすべてのトラフィックは許可されます。

```
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
```

EtherType アクセス リストの追加

透過ファイアウォール モード限定

ここでは、EtherType アクセス リストの追加方法について説明します。内容は次のとおりです。

- EtherType アクセス リストの概要（p.10-10）
- 拡張 ACE の追加（p.10-8）

EtherType アクセス リストの概要

EtherType アクセス リストは EtherType を指定する 1 つまたは複数の ACE からなります。EtherType ACE は、16 ビットの 16 進数で指定されたあらゆる EtherType を制御します。EtherType ACE は IPv4 パケットまたは ARP パケットには影響しません。EtherType アクセス リストは、イーサネット V2 フレームをサポートします。802.3 フォーマットのフレームは、タイプ フィールドではなく長さ フィールドを使用するので、アクセス リストでは処理されません。唯一の例外は、アクセス リストで処理する BPDU です。BPDU は SNAP でカプセル化され、FWSM は BPDU を処理できるように設計されています。

FWSM のポートはトランク ポート（シスコ独自）なので、FWSM はトランク ポート BPDU を受信します。トランク BPDU にはペイロード内に VLAN 情報が含まれるので、BPDU を許可した場合、FWSM は発信 VLAN を使用してペイロードを変更します。フェールオーバーを使用する場合は、ブリッジング ループを防止するために、EtherType アクセス リストで両方のインターフェイスの BPDU を許可する必要があります。

EtherType はコネクションレス型なので、双方向にトラフィックを流す場合は、両方のインターフェイスにアクセス リストを適用する必要があります。

MPLS を許可する場合、LDP および TDP TCP 接続が FWSM を介して確立されるようにする必要があります。これは、FWSM に接続された両方の MPLS ルータが、LDP または TDP セッションのルータ ID として FWSM に接続されたルータ インターフェイス上の IP アドレスを使用するように設定することによって行います（LDP および TDP によって、MPLS ルータはパケット転送用ラベル「アドレス」のネゴシエーションができます）。

Cisco IOS ルータ上で、プロトコル（LDP または TDP）に応じたコマンドを入力します。*interface* は FWSM に接続されたインターフェイスです。

```
hostname(config)# mpls ldp router-id interface force
```

または

```
hostname(config)# tag-switching tdp router-id interface force
```

インターフェイスの各方向に、各タイプ（拡張および EtherType）のアクセス リストを 1 つだけ適用できます。同じアクセス リストを複数のインターフェイスに適用することもできます。

EtherType ACE の追加

次のコマンドを入力して、EtherType ACE を追加します。

```
hostname(config)# access-list access_list_name ethertype {permit | deny} {ipx | bpdu |
mpls-unicast | mpls-multicast | any | hex_number}
```

hex_number は、0x600 以上の 16 ビット 16 進数で指定できる任意の EtherType です。EtherType のリストについては、http://www.ietf.org/rfc/rfc1700.txt にアクセスし、RFC 1700 「Assigned Numbers」を参照してください。

任意のアクセス リスト名を指定して **access-list** コマンドを入力すると、そのアクセス リストの末尾に ACE が追加されます。

ヒント　コンフィギュレーションを確認するときに名前をわかりやすくするために、*access_list_name* は大文字で入力してください。インターフェイスを示すアクセス リスト名（INSIDE など）、または目的を示すアクセス リスト名（MPLS、IPX など）を指定できます。

たとえば、次のアクセス リストの例では、内部インターフェイスを起点とする一般的な EtherType を許可します。

```
hostname(config)# access-list ETHER ethertype permit ipx
hostname(config)# access-list ETHER ethertype permit bpdu
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

次のアクセス リストでは、一部の EtherType に FWSM の通過を許可しますが、IPX は拒否します。

```
hostname(config)# access-list ETHER ethertype deny ipx
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit bpdu
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

次のアクセス リストでは、EtherType 0x1256 が指定されたトラフィックを拒否しますが、それ以外はすべて、両方のインターフェイスについて許可します。

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

標準アクセス リストの追加

標準アクセス リストは、宛先 IP アドレスを識別する一部のコマンドにのみ使用します。たとえば、標準アクセス リストを使用して、OSPF 再分配用のルート マップで使用する OSPF ルートの宛先アドレスを識別します。トラフィックを制御するインターフェイスに標準アクセス リストを適用することはできません。

次のコマンドで標準 ACE を追加します。アクセス リストの末尾に別の ACE を追加する場合は、同じアクセス リスト名を指定して **access-list** コマンドをもう 1 つ入力します。

次のコマンドを入力して、ACE を追加します。

```
hostname(config)# access-list access_list_name standard {deny | permit} {any |
ip_address mask}
```

次に、アクセス リストで 192.168.1.0/24 へのルートを識別する例を示します。

```
hostname(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

オブジェクトのグループ化によるアクセス リストの簡素化

ここでは、オブジェクトをグループ化してアクセス リストの作成 / 管理を簡素化する方法について説明します。内容は次のとおりです。

- オブジェクト グループ化の機能（p.10-13）
- オブジェクト グループの追加（p.10-13）
- オブジェクト グループのネスト（p.10-17）
- オブジェクト グループの表示（p.10-19）
- オブジェクト グループの削除（p.10-19）
- アクセス リストでオブジェクト グループを使用する方法（p.10-18）

オブジェクト グループ化の機能

類似のオブジェクトをグループとしてまとめることによって、オブジェクトごとに個別に ACE を入力しなくても、ACE でオブジェクト グループを使用できます。次のタイプのオブジェクト グループを作成できます。

- プロトコル
- ネットワーク
- サービス
- ICMP タイプ

例として、次の 3 つのオブジェクト グループを取り上げます。

- MyServices — 内部ネットワークにアクセスできるサービス要求の TCP/UDP ポート番号を指定します。
- TrustedHosts — 最大範囲のサービスおよびサーバにアクセスできるホストおよびネットワークのアドレスを指定します。
- PublicServers — 最大限のアクセス権を与えるサーバのホスト アドレスを指定します。

これらのグループを作成したあとで、ACE を 1 つだけ使用して、信頼できるホストがパブリック サーバのグループに対して、特定のサービス要求を行うことができるようにします。

オブジェクト グループを他のオブジェクト グループにネストすることもできます。

（注） 拡張アクセス リストには ACE のシステム限度が適用されます。ACE でオブジェクト グループを使用した場合、実際に入力する ACE の数は少なくなりますが、拡張 ACE の数はオブジェクト グループを使用しなかった場合と同じになります。オブジェクト グループは通常、手動で追加する場合より多くの ACE を作成します。手動で ACE を作成する場合の方がオブジェクト グループよりアドレスを集約する傾向があるからです。アクセス リストに指定されている拡張 ACE の数を確認するには、**show access-list** コマンドを入力します。

オブジェクト グループの追加

ここでは、オブジェクト グループの追加方法について説明します。内容は次のとおりです。

- プロトコル オブジェクト グループの追加（p.10-14）
- ネットワーク オブジェクト グループの追加（p.10-14）
- サービス オブジェクト グループの追加（p.10-15）
- ICMP タイプ オブジェクト グループの追加（p.10-16）

プロトコル オブジェクト グループの追加

プロトコル オブジェクト グループを追加または変更する手順は、次のとおりです。グループを追加したあと、同じグループ名で次の手順を繰り返し、他のオブジェクトを指定することによって、オブジェクトを必要なだけ追加できます。既存のオブジェクトを再入力する必要はありません。設定済みのコマンドは、コマンドの **no** 形式を指定して削除しないかぎり維持されます。

プロトコル グループを追加する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、プロトコル グループを追加します。

```
hostname(config)# object-group protocol grp_id
```

grp_id は、最大 64 文字の文字列です。

プロンプトがプロトコル コンフィギュレーション モードに変わります。

ステップ 2　（任意）次のコマンドを入力して、説明を追加します。

```
hostname(config-protocol)# description text
```

説明に使用できる文字数は最大 200 文字です。

ステップ 3　プロトコルごとに次のコマンドを入力して、グループのプロトコルを定義します。

```
hostname(config-protocol)# protocol-object protocol
```

protocol は、特定の IP プロトコルを表す識別番号（1 ～ 254）または識別キーワード（***icmp***、***tcp***、または ***udp***）です。すべての IP プロトコルを指定する場合は、キーワード ***ip*** を使用します。指定が可能なプロトコルのリストについては、「プロトコルおよびアプリケーション」（p.D-13）を参照してください。

たとえば、TCP、UDP、および ICMP に対応するプロトコル グループを作成する場合は、次のコマンドを入力します。

```
hostname(config)# object-group protocol tcp_udp_icmp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object icmp
```

ネットワーク オブジェクト グループの追加

ネットワーク オブジェクト グループを追加または変更する手順は、次のとおりです。グループを追加したあと、同じグループ名で次の手順を繰り返し、他のオブジェクトを指定することによって、オブジェクトを必要なだけ追加できます。既存のオブジェクトを再入力する必要はありません。設定済みのコマンドは、コマンドの **no** 形式を指定して削除しないかぎり維持されます。

（注）　ネットワーク オブジェクト グループは、アクセス リストのタイプに応じて IPv4 アドレスおよび IPv6 アドレスをサポートします。IPv6 アクセス リストの詳細については、「IPv6 アクセス リストの設定」（p.9-7）を参照してください。

ネットワーク グループを追加する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、ネットワーク グループを追加します。

```
hostname(config)# object-group network grp_id
```

grp_id は、最大 64 文字の文字列です。

プロンプトがネットワーク コンフィギュレーション モードに変わります。

ステップ 2　（任意）次のコマンドを入力して、説明を追加します。

```
hostname(config-network)# description text
```

説明に使用できる文字数は最大 200 文字です。

ステップ 3　ネットワークまたはアドレスごとに次のコマンドを入力して、グループのネットワークを定義します。

```
hostname(config-network)# network-object {host ip_address | ip_address mask}
```

たとえば、3 人の管理者の IP アドレスからなるネットワーク グループを作成する場合は、次のコマンドを入力します。

```
hostname(config)# object-group network admins
hostname(config-network)# description Administrator Addresses
hostname(config-network)# network-object host 10.1.1.4
hostname(config-network)# network-object host 10.1.1.78
hostname(config-network)# network-object host 10.1.1.34
```

サービス オブジェクト グループの追加

サービス オブジェクト グループを追加または変更する手順は、次のとおりです。グループを追加したあと、同じグループ名で次の手順を繰り返し、他のオブジェクトを指定することによって、オブジェクトを必要なだけ追加できます。既存のオブジェクトを再入力する必要はありません。設定済みのコマンドは、コマンドの **no** 形式を指定して削除しないかぎり維持されます。

サービス グループを追加する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、サービス グループを追加します。

```
hostname(config)# object-group service grp_id {tcp | udp | tcp-udp}
```

grp_id は、最大 64 文字の文字列です。

追加するサービス（ポート）に対応するプロトコルを指定します。**tcp**、**udp**、または **tcp-udp** キーワードのいずれかになります。DNS（ポート 53）のように、サービスが同じポート番号で TCP と UDP の両方を使用する場合は、**tcp-udp** キーワードを入力します。

プロンプトがサービス コンフィギュレーション モードに変わります。

ステップ 2　（任意）次のコマンドを入力して、説明を追加します。

```
hostname(config-service)# description text
```

説明に使用できる文字数は最大 200 文字です。

ステップ 3　ポートまたはポート範囲ごとに次のコマンドを入力して、グループのポートを定義します。

```
hostname(config-service)# port-object {eq port | range begin_port end_port}
```

使用できるキーワードおよび well-known ポートの割り当てのリストについては、「プロトコルおよびアプリケーション」（p.D-13）を参照してください。

たとえば、DNS（TCP/UDP）、LDAP（TCP）、および RADIUS（UDP）からなるサービス グループを作成する場合は、次のコマンドを入力します。

```
hostname(config)# object-group service services1 tcp-udp
hostname(config-service)# description DNS Group
hostname(config-service)# port-object eq domain

hostname(config-service)# object-group service services2 udp
hostname(config-service)# description RADIUS Group
hostname(config-service)# port-object eq radius
hostname(config-service)# port-object eq radius-acct

hostname(config-service)# object-group service services3 tcp
hostname(config-service)# description LDAP Group
hostname(config-service)# port-object eq ldap
```

ICMP タイプ オブジェクト グループの追加

ICMP タイプ オブジェクト グループを追加または変更する手順は、次のとおりです。グループを追加したあと、同じグループ名で次の手順を繰り返し、他のオブジェクトを指定することによって、オブジェクトを必要なだけ追加できます。既存のオブジェクトを再入力する必要はありません。設定済みのコマンドは、コマンドの **no** 形式を指定して削除しないかぎり維持されます。

ICMP タイプ グループを追加する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、ICMP タイプ グループを追加します。

```
hostname(config)# object-group icmp-type grp_id
```

grp_id は、最大 64 文字の文字列です。

プロンプトが ICMP タイプ コンフィギュレーション モードに変わります。

ステップ 2　（任意）次のコマンドを入力して、説明を追加します。

```
hostname(config-icmp-type)# description text
```

説明に使用できる文字数は最大 200 文字です。

ステップ 3　タイプごとに次のコマンドを入力して、グループの ICMP タイプを定義します。

```
hostname(config-icmp-type)# icmp-object icmp_type
```

ICMP タイプのリストについては、「ICMP のタイプ」（p.D-17）を参照してください。

たとえば、（ping を制御する）echo-reply および echo からなる ICMP タイプ グループを作成する場合は、次のコマンドを入力します。

```
hostname(config)# object-group icmp-type ping
hostname(config-service)# description Ping Group
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object echo-reply
```

オブジェクト グループのネスト

オブジェクト グループを同じタイプの別のオブジェクト グループにネストする場合は、「オブジェクト グループの追加」（p.10-13）に従って、ネストするグループを先に作成します。さらに、次の作業を行います。

ステップ 1　次のコマンドを入力して、別のオブジェクト グループをネストするオブジェクト グループを追加または編集します。

```
hostname(config)# object-group {{protocol | network | icmp-type} grp_id |
service grp_id {tcp | udp | tcp-udp}}
```

ステップ 2　次のコマンドを入力して、ステップ 1 で指定したオブジェクト グループの中に指定のグループを追加します。

```
hostname(config-group_type)# group-object grp_id
```

ネストするグループは、同じタイプでなければなりません。

1 つのオブジェクト グループの中で、ネストされたグループ オブジェクトと標準オブジェクトを混在させて照合できます。

各部門の権限のあるユーザからなるネットワーク オブジェクト グループを作成する例を示します。

```
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-network)# 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-network)# object-group network finance
hostname(config-network)# network-object host 10.1.4.89
hostname(config-network)# network-object host 10.1.4.100
```

さらに、3 つのグループを 1 つにネストします。

```
hostname(config)# object-group network admin
hostname(config-network)# group-object eng
hostname(config-network)# group-object hr
hostname(config-network)# group-object finance
```

次のように、ACE で管理（admin）オブジェクト グループを指定するだけで済むようになります。

```
hostname(config)# access-list ACL_IN extended permit ip object-group admin host
209.165.201.29
```

アクセス リストでオブジェクト グループを使用する方法

アクセス リストでオブジェクト グループを使用するには、標準プロトコル（*protocol*）、ネットワーク（*source_address mask* など）、サービス（*operator port*）、または ICMP タイプ（*icmp_type*）パラメータを **object-group** *grp_id* パラメータに置き換えます。

たとえば、**access-list** {**tcp** | **udp**} コマンドで使用できるすべてのパラメータにオブジェクト グループを使用する場合は、次のコマンドを入力します。

```
hostname(config)# access-list access_list_name [line line_number] [extended] {deny |
permit} {tcp | udp} object-group nw_grp_id [object-group svc_grp_id] object-group
nw_grp_id [object-group svc_grp_id]
```

すべてのパラメータにオブジェクト グループを使用する必要はありません。たとえば、送信元アドレスにオブジェクト グループを使用すれば、宛先アドレスはアドレスとマスクで特定できるといったことが可能です。

次のオブジェクト グループを使用しない標準アクセス リストは、内部ネットワーク上の複数のホストに対して、複数の Web サーバへのアクセスを制限します。その他のすべてのトラフィックは許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host
209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host
209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host
209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host
209.165.201.16 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host
209.165.201.16 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host
209.165.201.16 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host
209.165.201.78 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host
209.165.201.78 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host
209.165.201.78 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

内部ホストと Web サーバ用に 1 つずつ、2 つのネットワーク オブジェクト グループを作成すると、設定が簡素化され、ホストを追加するときの変更が容易になります。

```
hostname(config)# object-group network denied
hostname(config-network)# network-object host 10.1.1.4
hostname(config-network)# network-object host 10.1.1.78
hostname(config-network)# network-object host 10.1.1.89

hostname(config-network)# object-group network web
hostname(config-network)# network-object host 209.165.201.29
hostname(config-network)# network-object host 209.165.201.16
hostname(config-network)# network-object host 209.165.201.78

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
```

オブジェクト グループの表示

現在設定されているオブジェクト グループを表示するには、次のコマンドを入力します。

```
hostname(config)# show object-group [protocol | network | service | icmp-type |
id grp_id]
```

パラメータを指定しないでコマンドを入力すると、設定されているすべてのオブジェクト グループが表示されます。

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

```
hostname# show object-group
object-group network ftp_servers
  description: This is a group of FTP servers
  network-object host 209.165.201.3
  network-object host 209.165.201.4
object-group network TrustedHosts
  network-object host 209.165.201.1
  network-object 192.168.1.0 255.255.255.0
  group-object ftp_servers
```

オブジェクト グループの削除

オブジェクト グループを削除するには、次のいずれかのコマンドを入力します。

(注) アクセス リストで使用中のオブジェクト グループを削除したり、または空にしたりすることはできません。

- 特定のオブジェクト グループを削除する場合は、次のコマンドを入力します。

  ```
  hostname(config)# no object-group grp_id
  ```

- 指定したタイプのオブジェクト　グループをすべて削除する場合は、次のコマンドを入力します。

  ```
  hostname(config)# clear object-group [protocol | network | services | icmp-type]
  ```

  タイプを入力しなかった場合は、すべてのオブジェクト グループが削除されます。

アクセス リストへのコメントの追加

拡張アクセス リスト、EtherType アクセス リスト、標準アクセス リストをはじめ、あらゆるアクセス リストでエントリに関するコメントを追加できます。コメントによってアクセス リストがわかりやすくなります。

次のコマンドを入力して、アクセス リストにコメントを追加します。

```
hostname(config)# access-list access_list_name [line line_number] remark text
```

任意のアクセス リスト名を指定して **access-list remark** コマンドを入力すると、**line** の番号を指定する場合を除き、そのアクセス リストの末尾にコメントが追加されます。

clear configure access-list *access_list_name* コマンドを使用してアクセス リストを削除すると、コメントもすべて削除されます。

テキストは最大 100 文字の長さまで入力できます。テキストの先頭に先行スペースを入力することもできます。後続スペースは無視されます。

たとえば、各 ACE の前にコメントを追加すると、アクセス リスト内のその位置にコメントが入ります。コメント テキストの前にダッシュ（-）を入力すると、ACE との区別が容易になります。

```
hostname(config)# access-list OUT remark - this is the inside admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT remark - this is the hr admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

拡張アクセス リストのアクティベーションのスケジューリング

ACE に時間範囲を適用して、各 ACE を特定の時刻および曜日にアクティブ化するようにスケジューリングできます。このセクションでは、次の内容について説明します。

- 時間範囲の追加（p.10-21）
- 時間範囲の ACE への適用（p.10-22）

時間範囲の追加

時間範囲を追加して時間ベースのアクセス リストを実装するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、時間範囲名を指定します。

```
hostname(config)# time-range name
```

ステップ 2　時間範囲として、定期時間範囲または絶対間範囲のどちらかを指定します。

time-range コマンドごとに複数の定期エントリを入力できます。**time-range** コマンドに **absolute** 値と **periodic** 値の両方を指定した場合、**periodic** コマンドは **absolute** 開始時間の到達後にのみ評価され、**absolute** 終了時間の到達後には評価されません。

- 定期時間範囲：

  ```
  hostname(config-time-range)# periodic days-of-the-week time to [days-of-the-week]
  time
  ```

  days-of-the-week に対して次の値を指定できます。

  - **monday**、**tuesday**、**wednesday**、**thursday**、**friday**、**saturday**、および **sunday**
  - **daily**
  - **weekdays**
  - **weekend**

  time の形式は *hh*:*mm* です。たとえば、8:00 は 8:00 a.m で 20:00 は 8:00 p.m になります。
- 絶対時間範囲：

  ```
  hostname(config-time-range)# absolute start time date [end time date]
  ```

  time の形式は *hh*:*mm* です。たとえば、8:00 は 8:00 a.m で 20:00 は 8:00 p.m になります。

  date の形式は*日月年*で、**1 january 2006** のようになります。

次に、2006 年 1 月 1 日 8:00 a.m. に始まる絶対時間範囲の例を示します。終了日時を指定しないため、時間範囲は無期限に有効です。

```
hostname(config)# time-range for2006
hostname(config-time-range)# absolute start 8:00 1 january 2006
```

次に、平日の 8:00 a.m. から 6:00 p.m. の週の定期時間範囲の例を示します。

```
hostname(config)# time-range workinghours
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
```

時間範囲の ACE への適用

次のコマンドを入力して、時間範囲を ACE に適用します。

```
hostname(config)# access-list access_list_name [extended] {deny |
permit}...[time-range name]
```

access-list コマンド構文の詳細については、「拡張アクセス リストの追加」（p.10-7）を参照してください。

（注） ACE のロギングもイネーブルにする場合、**time-range** キーワードの前に **log** キーワードを使用します。**inactive** キーワードを使用して ACE をディセーブルにする場合、最後のキーワードとして **inactive** キーワードを使用します。

次に、「Sales」という名前のアクセス リストを「New_York_Minute」という名前の時間範囲に結合する例を示します。

```
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
```

アクセス リスト アクティビティのロギング

ここでは、拡張アクセス リストと Webtype アクセス リストにアクセス リスト ロギングを設定する方法について説明します。

内容は次のとおりです。

- アクセス リスト ロギングの概要（p.10-23）
- ACE ロギングの設定（p.10-24）
- 拒否フローの管理（p.10-25）

アクセス リスト ロギングの概要

デフォルトでは、拡張 ACE によってトラフィックが拒否された場合、FWSM は拒否されたパケットごとにシステム メッセージ 106023 を生成します。メッセージの形式は次のとおりです。

```
%XXX-106023: Deny protocol src [interface_name:source_address/source_port] dst
interface_name:dest_address/dest_port [type {string}, code {code}] by access_group
acl_id
```

FWSM が攻撃を受けると、拒否パケットに関するシステム メッセージの数が膨大になりかねません。代わりに、システム メッセージ 106100 を使用するロギングをイネーブルにすることを推奨します。各 ACE の統計情報が得られ、生成されるシステム メッセージ数を制限できます。または、すべてのロギングをディセーブルにすることもできます。

（注） ロギング メッセージを生成するのは、アクセス リストで指定された ACE だけです。アクセス リストの末尾の暗黙拒否はメッセージを生成しません。拒否されたすべてのトラフィックでメッセージが生成されるようにする場合は、次のように、アクセス リストの末尾に暗黙的な ACE を手動で追加します。

```
hostname(config)# access-list TEST deny ip any any log
```

拡張 **access-list** コマンドの末尾に **log** オプションを指定すると、次の動作を設定できます。

- メッセージ 106023 の代わりにメッセージ 106100 をイネーブルにする
- すべてのロギングをディセーブルにする
- メッセージ 106023 を使用するデフォルトのロギングに戻す

システム メッセージ 106100 の形式は、次のとおりです。

```
%XXX-n-106100: access-list acl_id {permitted | denied} protocol
interface_name/source_address(source_port) -> interface_name/dest_address(dest_port)
hit-cnt number ({first hit | number-second interval})
```

メッセージ 106100 のロギングがイネーブルのときに、パケットが ACE と一致すると、FWSM は一定の間隔で受信パケット数を追跡するフロー エントリを作成します。FWSM は、最初のヒットと各インターバルの最後にシステム メッセージを生成し、インターバルの間のヒット総数を示します。インターバルが終了するたびに、FWSM はヒット カウントを 0 にリセットします。インターバルの間にパケットが ACE と一致しなかった場合、FWSM はフロー エントリを削除します。

フローは送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびポートによって定義されます。同じ 2 つのホスト間でも、新しい接続では送信元ポートが異なる可能性があり、接続用に新しいフローが作成されるので、フローの増加分が同じではないことがあります。

確立済みの接続に属する許可パケットは、改めてアクセス リストと照合する必要はありません。最初のパケットだけを記録し、ヒット カウントに含めます。ICMP などのコネクションレス型プロトコルの場合は、許可された場合でも、すべてのパケットが記録されます。拒否されたパケットはすべて記録されます。

システム メッセージの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages*』を参照してください。

ACE ロギングの設定

ACE ロギングを設定する場合は、次の **log** オプションの説明を参照してください。

```
hostname(config)# access-list access_list_name [extended] {deny | permit}...[log
[[level] [interval secs] | disable | default]]
```

access-list コマンド構文の詳細については、「拡張アクセス リストの追加」（p.10-7）を参照してください。

（注） ACE の時間範囲もイネーブルにする場合、**time-range** キーワードの前に **log** キーワードを使用します。**inactive** キーワードを使用して ACE をディセーブルにする場合、最後のキーワードとして **inactive** キーワードを使用します。

引数を指定しないで **log** オプションを入力した場合は、システム ログ メッセージ 106100 がデフォルトのレベル（6）、デフォルトのインターバル（300 秒）でイネーブルになります。次のオプションを指定できます。

- *level* ― 重大度レベル 0 ～ 7。デフォルトは 6 です。
- **interval** *secs* ― 秒数で指定するシステム メッセージの時間間隔（1 ～ 600）。デフォルトは 300 です。アクティブではないフローを削除するタイムアウト値としても、この値を使用します。
- **disable** ― すべてのアクセス リスト ロギングがディセーブルになります。
- **default** ― メッセージ 106023 でのロギングがイネーブルになります。この設定は、**log** オプションを指定しないのと同じことです。

次に、アクセス リストの設定例を示します。

```
hostname(config)# access-list outside-acl permit ip host 1.1.1.1 any log 7 interval
600
hostname(config)# access-list outside-acl permit ip host 2.2.2.2 any
hostname(config)# access-list outside-acl deny ip any any log 2
hostname(config)# access-group outside-acl in interface outside
```

outside-acl の最初の ACE によってパケットが許可された場合、FWSM は次のようなシステム メッセージを生成します。

```
%PIX-7-106100: access-list outside-acl permitted tcp outside/1.1.1.1(12345) ->
inside/192.168.1.1(1357) hit-cnt 1 (first hit)
```

この接続ではさらに 20 のパケットが外部インターフェイスに届きますが、トラフィックをアクセス リストと照合する必要はなく、ヒット カウントも増えません。

10 分と指定したインターバルの間に、同じホストでさらにもう 1 つ接続が開始された場合（送信元ポートと宛先ポートは同じまま）、ヒット カウントは 1 だけ増え、10 分のインターバルの最後に次のようなメッセージが表示されます。

```
%PIX-7-106100: access-list outside-acl permitted tcp outside/1.1.1.1(12345)->
inside/192.168.1.1(1357) hit-cnt 2 (600-second interval)
```

3 番めの ACE によってパケットが拒否された場合、FWSM は次のようなシステム メッセージを生成します。

```
%PIX-2-106100: access-list outside-acl denied ip outside/3.3.3.3(12345) ->
inside/192.168.1.1(1357) hit-cnt 1 (first hit)
```

5 分のインターバル（デフォルト）の試行回数が 20 回だった場合、5 分経過後に次のようなメッセージが表示されます。

```
%PIX-2-106100: access-list outside-acl denied ip outside/3.3.3.3(12345) ->
inside/192.168.1.1(1357) hit-cnt 21 (300-second interval)
```

拒否フローの管理

メッセージ 106100 のロギングがイネーブルのときに、パケットが ACE と一致すると、FWSM は一定の間隔で受信パケット数を追跡するフロー エントリを作成します。FWSM が ACE に使用するロギング フローは、最大で 32 K です。多数のフローが同時に存在可能です。メモリおよび CPU リソースが無限に消費されないように、FWSM は同時に存在する*拒否*フロー数を制限します。この限度が設定されるのは、（許可フローではなく）攻撃を示す可能性のある拒否フローだけです。この限度に達した場合、FWSM は既存のフローがタイムアウトするまで、ロギング用の新しい拒否フローを作成しません。

たとえば、ある人が DoS 攻撃を開始した場合、FWSM は短時間に大量の拒否フローを作成する可能性があります。拒否フロー数を制限することによって、メモリおよび CPU リソースが無限に消費されることがなくなります。

拒否フローの最大数に達すると、FWSM はシステム メッセージ 106100 を発行します。

```
%XXX-1-106101: The number of ACL log deny-flows has reached limit (number).
```

拒否フローの最大数を設定し、拒否フロー アラート メッセージ（106101）のインターバルを設定する場合は、次のコマンドを入力します。

- FWSM がロギングを停止するまでに、1 つのコンテキストで許可される拒否フローの最大数を設定する場合は、次のコマンドを入力します。

  ```
  hostname(config)# access-list deny-flow-max number
  ```

  number は 1 ～ 4096 です。4096 がデフォルトです。
- 拒否フローの最大数に達したことを伝えるシステム メッセージ（106101）の発行間隔を設定するには、次のコマンドを入力します。

  ```
  hostname(config)# access-list alert-interval secs
  ```

  seconds は 1 ～ 3600 です。300 がデフォルトです。

ネットワーク アクセスの許可または拒否

ここでは、アクセス リストを使用して FWSM を通過するネットワーク アクセスを制御する方法について説明します。拡張アクセス リストまたは EtherType アクセス リストを作成する場合は、第 10 章「アクセス リストでのトラフィックの識別」を参照してください。

(注) ルーテッド ファイアウォール モードと透過ファイアウォール モードの両方とも、アクセス リストを使用してネットワーク アクセスを制御します。透過モードでは、拡張アクセス リスト（レイヤ 3 トラフィック）と EtherType アクセス リスト（レイヤ 2 トラフィック）の両方を使用できます。

管理アクセス用に FWSM インターフェイスにアクセスするために、アクセス リストでホスト IP アドレスを許可する必要はありません。第 21 章「管理アクセスの設定」に従って管理アクセスを設定するだけで済みます。

この章で説明する内容は、次のとおりです。

- 着信および発信アクセス リストの概要（p.11-2）
- アクセス リストのインターフェイスへの適用（p.11-5）

着信および発信アクセス リストの概要

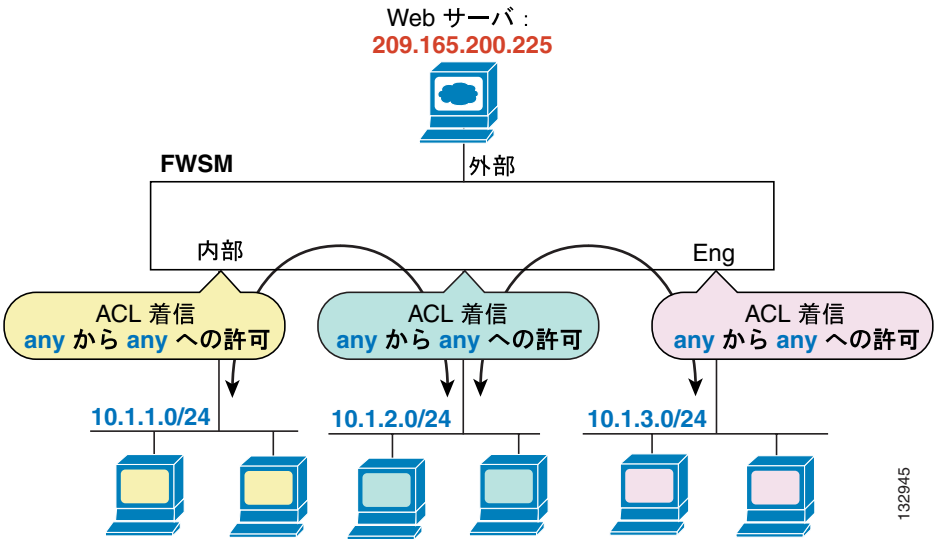
FWSM のインターフェイス上を流れるトラフィックは、2 通りの方法で制御できます。FWSM に入ってくるトラフィックは、送信元インターフェイスに着信アクセス リストを結合することによって制御できます。FWSM から出ていくトラフィックは、宛先インターフェイスに発信アクセス リストを結合することによって制御できます。トラフィックが FWSM に入ってくるようにするには、インターフェイスに着信アクセス リストを結合する必要があります。そうしないと、FWSM はそのインターフェイスに届いたあらゆるトラフィックを自動的に廃棄します。デフォルトでは、発信アクセス リストを使用して制限しないかぎり、トラフィックは FWSM のすべてのインターフェイスから出ていくことが可能です。発信アクセス リストによって、着信アクセス リストですでに設定されているものに制限を加えます。

(注)

「着信」および「発信」とは、インターフェイス上でのアクセス　リストの適用方法を意味します。FWSM のインターフェイスに入ってくるトラフィックにアクセス リストを適用するのか、それとも FWSM のインターフェイスから出ていくトラフィックにアクセス リストを適用するのかという意味です。セキュリティ レベルの低いインターフェイスから高いインターフェイスへのトラフィックの流れ（一般に、着信といいます）または高いインターフェイスから低いインターフェイスへのトラフィックの流れ（一般に、発信といいます）を表すわけではありません。

発信アクセス リストを使用して、アクセス リストの設定を簡素化する場合があります。たとえば、3 つの異なるインターフェイス上の 3 つの内部ネットワークが相互にアクセスできるようにする場合、各内部インターフェイス上ですべてのトラフィックを許可する単純な着信アクセス リストを作成します（図 11-1 を参照）。

図 11-1　着信アクセス リスト

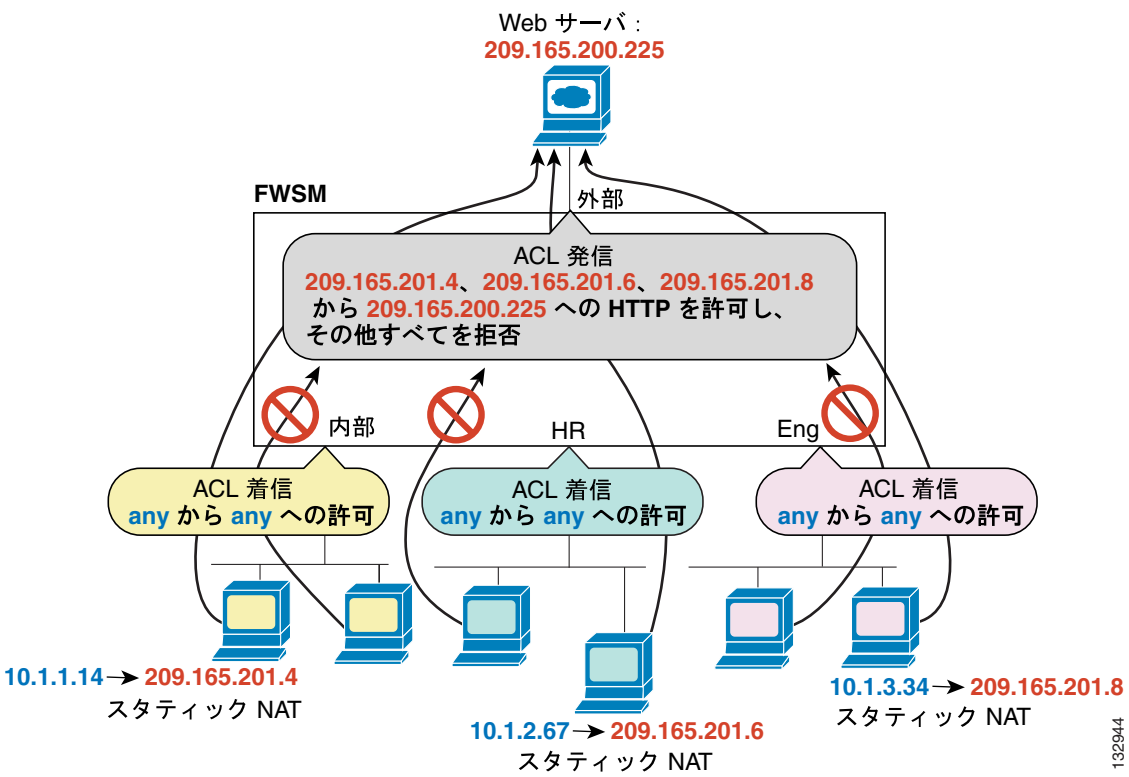


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# access-list INSIDE extended permit ip any any
hostname(config)# access-group INSIDE in interface inside

hostname(config)# access-list HR extended permit ip any any
hostname(config)# access-group HR in interface hr

hostname(config)# access-list ENG extended permit ip any any
hostname(config)# access-group ENG in interface eng
```

さらに、内部ネットワーク上の特定のホストだけが外部ネットワーク上の Web サーバにアクセスできるようにする場合、指定したホストだけを許可する、より制約の強化されたアクセス リストを作成し、外部インターフェイスの発信方向にそのアクセス リストを適用します（図 11-1 を参照）。NAT および IP アドレスについては、「NAT 使用時のアクセス リスト用 IP アドレス」（p.10-3）を参照してください。発信アクセス リストによって、その他のホストから外部ネットワークへの接続が禁止されます。

図 11-2　発信アクセス リスト



この例に対応するコマンドは、次のとおりです。

```
hostname(config)# access-list INSIDE extended permit ip any any
hostname(config)# access-group INSIDE in interface inside

hostname(config)# access-list HR extended permit ip any any
hostname(config)# access-group HR in interface hr

hostname(config)# access-list ENG extended permit ip any any
hostname(config)# access-group ENG in interface eng

hostname(config)# access-list OUTSIDE extended permit tcp host 209.165.201.4
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 209.165.201.6
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 209.165.201.8
host 209.165.200.225 eq www
hostname(config)# access-group OUTSIDE out interface outside
```

アクセス リストのインターフェイスへの適用

次のコマンドを入力して、インターフェイスの着信方向と発信方向に拡張アクセス リストを適用します。

```
hostname(config)# access-group access_list_name {in | out} interface interface_name
[per-user-override]
```

インターフェイスの両方向に、各タイプ（拡張および EtherType）のアクセス リストを 1 つ適用できます。アクセス リストの方向の詳細については、「着信および発信アクセス リストの概要」（p.11-2）を参照してください。

per-user-override キーワードではダイナミック アクセス リストを使用できます。ダイナミック アクセス リストはユーザ許可用にダウンロードされ、インターフェイスに割り当てられたアクセス リストに優先されます。たとえば、インターフェイス アクセス リストが 10.0.0.0 からのすべてのトラフィックを拒否し、ダイナミック アクセス リストが 10.0.0.0 からのすべてのトラフィックを許可する場合、そのユーザに対してはダイナミック アクセス リストがインターフェイス アクセス リストに優先されます。ユーザ単位のアクセス リストの詳細については、「RADIUS 許可の設定」（p.15-8）を参照してください。**per-user-override** キーワードは、着信アクセス リストに対してのみ使用できます。

コネクションレス型プロトコルで、双方向にトラフィックを流す場合は、送信元インターフェイスと宛先インターフェイスにアクセス リストを適用する必要があります。たとえば、透過モードの EtherType アクセス リストで BGP を許可する場合、両方のインターフェイスにアクセス リストを適用する必要があります。

IP アドレス 209.165.201.12（この IP アドレスは NAT の実行後に外部インターフェイス上で認識されます）の内部 Web サーバにアクセスできるようにするには、次のコマンドが必要です。

```
hostname(config)# access-list ACL_OUT extended permit tcp any host 209.165.201.12 eq
www
hostname(config)# access-group ACL_OUT in interface outside
```

Web サーバの NAT を設定することも必要です。

次のアクセス リストは、すべてのホストに対して、内部ネットワークと hr ネットワーク間の通信を許可しますが、外部ネットワークへのアクセスは一部のホストに限定して許可します。

```
hostname(config)# access-list ANY extended permit ip any any
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any

hostname(config)# access-group ANY in interface inside
hostname(config)# access-group ANY in interface hr
hostname(config)# access-group OUT out interface outside
```

たとえば、次のアクセス リストの例では、内部インターフェイスを起点とする一般的な EtherType を許可します。

```
hostname(config)# access-list ETHER ethertype permit ipx
hostname(config)# access-list ETHER ethertype permit bpdu
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

次のアクセス リストでは、一部の EtherType に FWSM の通過を許可しますが、それ以外はすべて拒否します。

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit bpdu
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

次のアクセス リストでは、EtherType 0x1256 が指定されたトラフィックを拒否しますが、それ以外はすべて、両方のインターフェイスについて許可します。

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

NAT の設定

この章では、Network Address Translation（NAT; ネットワーク アドレス変換）について説明します。ルーテッド ファイアウォール モードでは、FWSM は各ネットワーク間で NAT を実行します。

（注） 透過ファイアウォール モードでは、接続制限を設定する場合を除き、FWSM は NAT をサポートしません。「透過ファイアウォール モードと NAT を設定しない場合の接続制限の設定」（p.7-8）を参照してください。

この章で説明する内容は、次のとおりです。

- NAT の概要（p.12-2）
- NAT 制御の設定（p.12-16）
- ダイナミック NAT および PAT の使用方法（p.12-17）
- スタティック NAT の使用方法（p.12-27）
- スタティック PAT の使用方法（p.12-29）
- NAT のバイパス（p.12-32）
- NAT の例（p.12-36）

NAT の概要

ここでは、FWSM 上での NAT の機能について説明します。

- NAT の説明（p.12-2）
- NAT 制御（p.12-3）
- NAT のタイプ（p.12-5）
- ポリシー NAT（p.12-10）
- NAT および同一セキュリティ レベルのインターフェイス（p.12-13）
- 実アドレス照合用 NAT コマンドの順序（p.12-13）
- NAT ステートメントの最大数（p.12-13）
- マップ アドレスに関する注意事項（p.12-14）
- DNS および NAT（p.12-14）

NAT の説明

アドレス変換は、パケットの実アドレスを宛先ネットワーク上でルーティング可能なマップ アドレスに置き換えます。NAT は、実アドレスをマップ アドレスに変換する処理と、その後、変換を取り消してトラフィックを戻す処理の 2 つの手順で構成されています。

FWSM は NAT ルールと トラフィックが一致したときにアドレスを変換します。NAT ルールが一致しない場合は、パケット処理を続行します。ただし、NAT 制御をイネーブルにした場合は別です。NAT 制御では、セキュリティの高いインターフェイス（内部）からセキュリティの低いインターフェイス（外部）へのトラフィックは NAT ルールと一致する必要があり、一致しない場合、パケット処理は中止されます（セキュリティ レベルの詳細については「セキュリティ レベルの概要」[p.6-2]、NAT 制御の詳細については「NAT 制御」[p.12-3] を参照）。

（注） このマニュアルでは、通常すべてのタイプの変換を NAT と呼びます。NAT について説明する場合、*内部*および*外部*という用語も関連し、任意の 2 つのインターフェイス間のセキュリティ関係を表します。セキュリティ レベルの高い方が内部で、低い方が外部です。たとえば、インターフェイス 1 が 60 で、インターフェイス 2 が 50 という設定の場合、インターフェイス 1 が「内部」、インターフェイス 2 が「外部」となります。

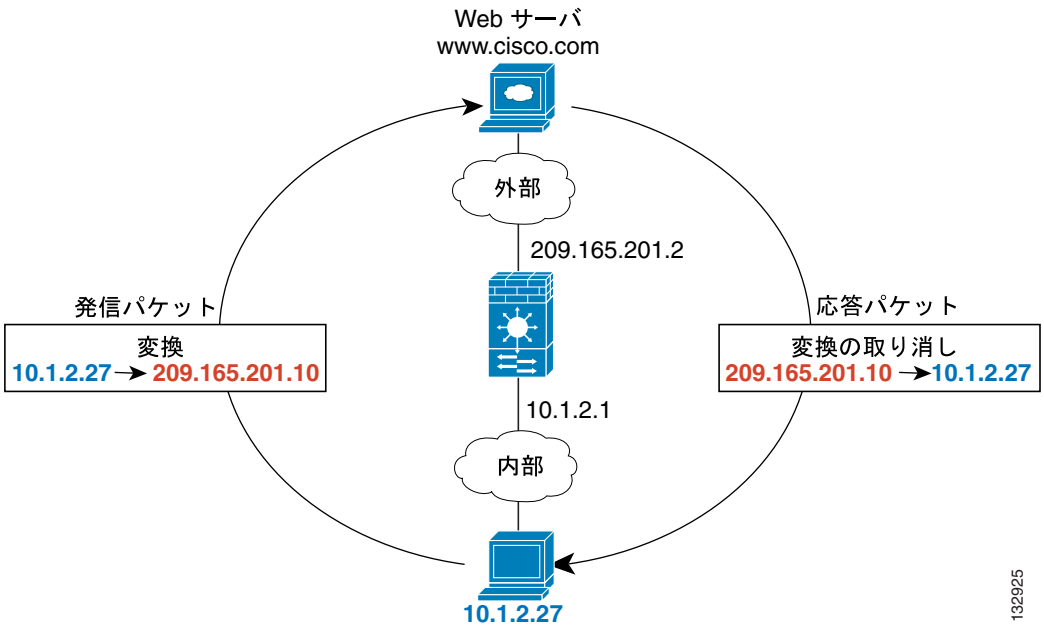
NAT の利点の一部を紹介します。

- 内部ネットワーク上でプライベート 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上でルーティングできません（詳細については、「プライベート ネットワーク」[p.D-2] を参照）。
- NAT は他のネットワークから実アドレスを隠すので、攻撃側はホストの実アドレスを突き止めることができません。
- アドレスの重複といった IP ルーティング関連の問題を解決できます。

（注） NAT でサポートされないプロトコルについては、表 20-1（p.20-5）を参照してください。

図 12-1 に、内部にプライベート ネットワークのある、NAT の一般的な使用例を示します。10.1.1.27 にある内部ホストが Web サーバにパケットを送信すると、そのパケットの送信元実アドレス 10.1.1.27 がマップ アドレス 209.165.201.10 に変更されます。応答時、Web サーバはマップ アドレス 209.165.201.10 に応答を送り、FWSM がパケットを受信します。その後、FWSM はマップ アドレス 209.165.201.10 の変換を取り消して実アドレス 10.1.1.1.27 に戻してから、ホストにパケットを送信します。

図 12-1　NAT の例



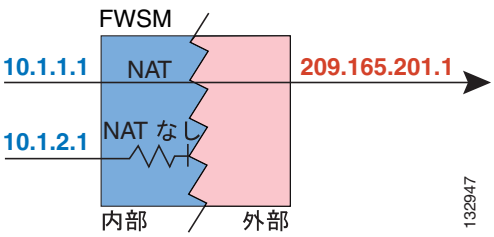
この例に対応するコマンドは、次のとおりです。

```
hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.1-209.165.201.15
```

NAT 制御

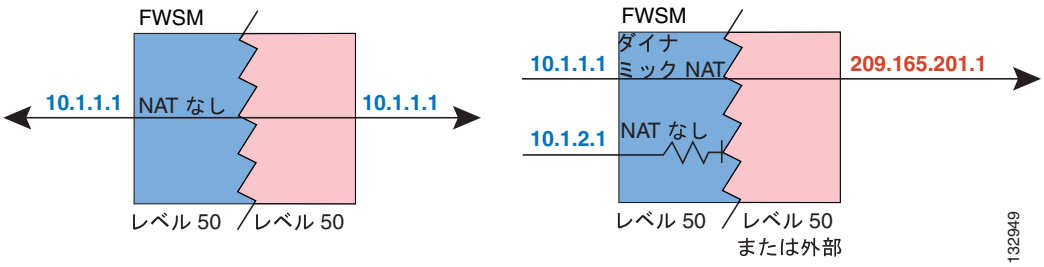
NAT 制御では、内部インターフェイスから外部インターフェイスへのパケットは NAT ルールと一致する必要があります。内部ネットワークのホストから外部ネットワークのホストにアクセスする場合は、内部ホスト アドレスを変換するように NAT を設定する必要があります（図 12-2 を参照）。

図 12-2　NAT 制御と発信トラフィック



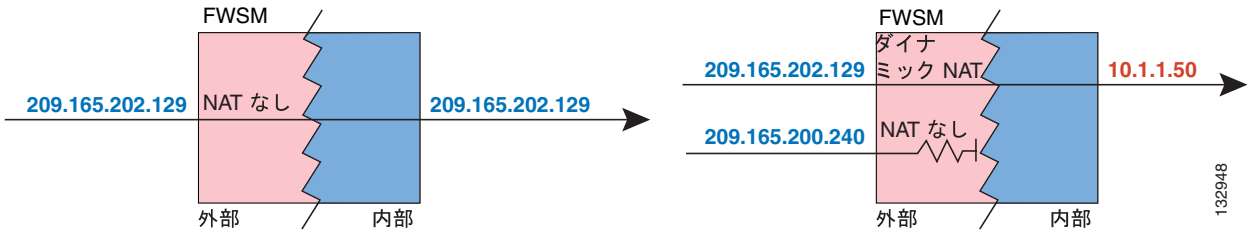
セキュリティ レベルが同一のインターフェイスは、通信に NAT を使用する必要がありません。ただし、NAT 制御をイネーブルにして同一セキュリティ インターフェイスでダイナミック NAT または PAT を設定する場合、そのインターフェイスから同一セキュリティ インターフェイスまたは外部インターフェイスへのすべてのトラフィックは、NAT ルールと一致する必要があります（図 12-3 を参照）。

図 12-3　NAT 制御と同一セキュリティ トラフィック



同様に、NAT 制御で外部ダイナミック NAT または PAT をイネーブルにする場合、内部インターフェイスにアクセスするすべての外部トラフィックは NAT ルールと一致する必要があります（図 12-4 を参照）。

図 12-4　NAT 制御と着信トラフィック



NAT 制御でスタティック NAT をイネーブルにした場合、これらの制約は発生しません。

デフォルトでは NAT 制御はディセーブルになっているため、ネットワーク上で NAT を使用するかどうかを任意に選択できます。ただし、新バージョンのソフトウェアにアップグレードした場合、NAT 制御がイネーブルになっていることがあります。

（注） NAT を設定しない場合でも、FWSM はすべてのトラフィックに対して自動的に変換セッションを作成します。この場合、実アドレスから同じ実アドレスへの変換が行われます。変換セッションについては、**show xlate** コマンドを参照してください。

NAT 制御によってセキュリティ レベルを上げたいけれども、一部のケースで内部アドレスを変換したくない場合、このようなアドレスに NAT 除外またはアイデンティティ NAT ルールを適用できます。（詳細については、「NAT のバイパス」[p.12-32] を参照）。

NAT 制御を設定するには、「NAT 制御の設定」（p.12-16）を参照してください。

（注） マルチコンテキスト モードにおいて、パケット分類機能は NAT コンフィギュレーションに依存してパケットをコンテキストに割り当てることがあります。NAT 制御がディセーブルであるために NAT を実行しない場合、分類機能により、ネットワーク コンフィギュレーションの変更が必要になることがあります。分類機能と NAT の関係の詳細については、「FWSM によるパケットの分類方法」（p.4-3）を参照してください。

NAT のタイプ

ここでは、使用可能な NAT タイプについて説明します。アドレス変換は、ダイナミック NAT、Port Address Translation（PAT; ポートアドレス変換）、スタティック NAT、スタティック PAT、またはこれらのタイプを組み合わせたものとして実行できます。NAT 制御をイネーブルにしても NAT を実行しない場合など、NAT をバイパスするルールを設定することもできます。ここでは次の内容について説明します。

- ダイナミック NAT（p.12-5）
- PAT（p.12-7）
- スタティック NAT（p.12-7）
- スタティック PAT（p.12-8）
- NAT 制御をイネーブルにした場合の NAT のバイパス（p.12-9）

ダイナミック NAT

ダイナミック NAT では、実アドレス グループを宛先ネットワーク上でルーティング可能なマップ アドレスのプールに変換します。マップ プールは、実グループより少ないアドレスで構成されます。変換対象のホストが宛先ネットワークにアクセスすると、FWSM はホストにマップ プール内の IP アドレスを割り当てます。変換は、実ホストが接続を開始するときにのみ追加されます。変換が有効なのは、接続されている間だけなので、どのユーザも変換のタイムアウト後に同じ IP アドレスを維持することはできません（『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **timeout xlate** コマンドを参照）。そのため、宛先ネットワークのユーザは、ダイナミック NAT を使用するホストに対して（接続がアクセス リストによって許可された場合でも）、接続を確実に開始することはできず、FWSM は実ホスト アドレスに直接行われる接続試行をすべて拒否します。ホストへの確実なアクセスについては、次の 「スタティック NAT」または「スタティック PAT」を参照してください。

図 12-5 は、リモート ホストによる実アドレスへの接続試行を示しています。FWSM はマップ アドレスへの戻り接続しか許可しないため、接続は拒否されます。

図 12-5　リモート ホストによる実アドレスへの接続試行

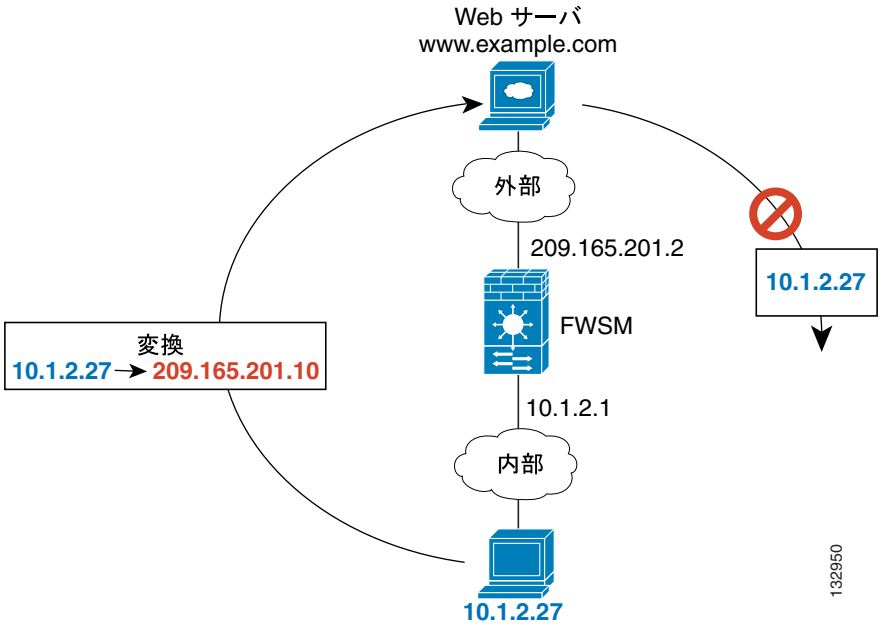
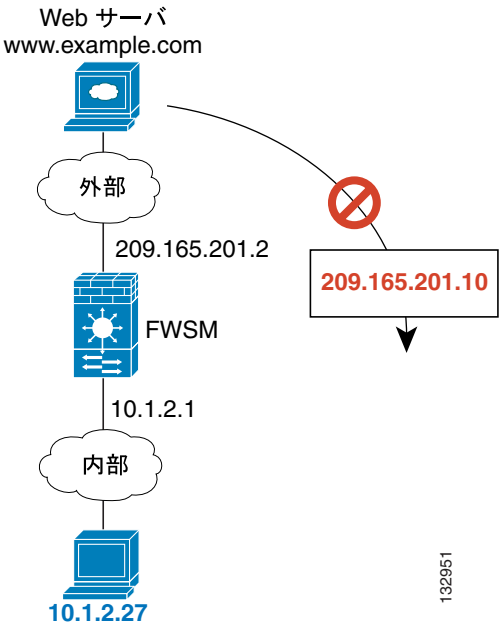


図 12-6 は、リモート ホストによるマップ アドレスへの接続試行を示しています。このアドレスは現在変換テーブルにないため、FWSM はパケットを廃棄します。

図 12-6　リモート ホストによるマップ アドレスへの接続試行



(注) 変換中であれば、リモート ホストはアクセス リストで許可されている場合は、変換対象ホストへの接続を開始できます。アドレスは予測不能なので、ホストに接続できる可能性は非常に少なくなります。万一、接続に成功した場合は、アクセス リストのセキュリティに頼ることになります。

ダイナミック NAT の短所は、次のとおりです。

- マップ プール内のアドレスが実グループより少ない場合、トラフィック量が予想を上回るとアドレスが不足する可能性があります。

  この現象が頻繁に発生する場合は、PAT を使用します。PAT は単一アドレスのポートを使用して 64,000 以上の変換を実行できます。
- ルーティング可能なアドレスをマップ プールで大量に使用する必要があります。インターネットなどの登録アドレスが宛先ネットワークに必要な場合は、使用可能なアドレスが不足することがあります。

ダイナミック NAT の利点は、一部のプロトコルで PAT を使用できないということです。たとえば、PAT は GRE バージョン 0 などオーバーロード ポートを持たない IP プロトコルでは動作しません。PAT は、データ ストリームと制御パスが異なるポートに存在する非オープン スタンダードの一部のマルチメディア アプリケーションでも動作しません。NAT および PAT のサポートの詳細については、「アプリケーション インスペクション エンジンの概要」（p.20-2）を参照してください。

PAT

PAT では、複数の実アドレスを 1 つのマップ IP アドレスに変換します。特に、FWSM は実アドレスと送信元ポート（実ソケット）を、マップ アドレスおよび 1024 より上の一意のポートに変換します（マップ ソケット）。送信元ポートは接続ごとに異なるため、接続ごとに別個の変換が必要となります。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは異なる変換が必要です。

接続が期限切れになったあと、ポート変換も 30 秒の休止状態後に期限切れになります。タイムアウトは設定できません。宛先ネットワークのユーザは、PAT を使用するホストに対して（ACL によって接続が許可されていた場合でも）、接続を確実に開始することはできません。ホストの実またはマップ ポート番号を予測できないだけでなく、FWSM は変換対象ホストが接続を開始する側でないかぎり、変換を作成しません。ホストへの確実なアクセスについては、次の「スタティック NAT」または「スタティック PAT」を参照してください。

PAT で使用するマップ アドレスは 1 つだけなので、ルーティング可能アドレスの節約になります。FWSM インターフェイスの IP アドレスを PAT アドレスとして使用することもできます。PAT は、データ ストリームが制御パスと異なる一部のマルチメディア アプリケーションでは動作しません。NAT および PAT のサポートの詳細については、「アプリケーション インスペクション エンジンの概要」（p.20-2）を参照してください。

（注） 変換中であれば、リモート ホストはアクセス リストで許可されている場合は、変換対象ホストへの接続を開始できます。ポート アドレスは（実およびマップの両方とも）予測不能なので、ホストに接続できる可能性は非常に少なくなります。万一、接続に成功した場合は、アクセス リストのセキュリティに頼ることになります。

スタティック NAT

スタティック NAT では、実アドレスからマップ アドレスへの固定変換を作成します。ダイナミック NAT および PAT の場合、各ホストは以後の各変換で異なるアドレス / ポートを使用します。スタティック NAT では、マップ アドレスは連続する各接続で同じあり、持続型の変換ルールが適用されるので、スタティック NAT の場合、（アクセス リストで許可されていれば）宛先ネットワークのホストから変換対象ホストへのトラフィックを開始できます。

ダイナミック NAT とスタティック NAT のアドレス範囲における主な相違は、スタティック NAT では、（アクセス リストで許可されていれば）リモート ホストから変換対象ホストへ接続を開始できるのに対して、ダイナミック NAT では開始できないことです。スタティック NAT ではさらに、実アドレスと同数のマップ アドレスが必要です。

スタティック PAT

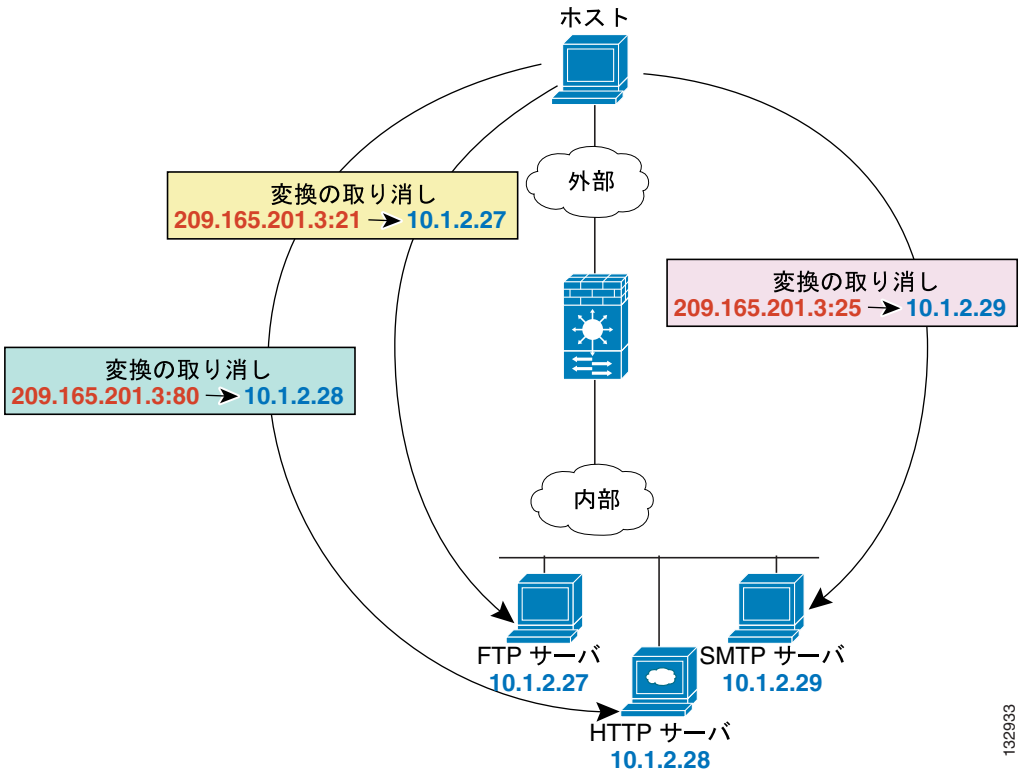
スタティック PAT は、実アドレスとマップ アドレスに対応するプロトコル（TCP または UDP）とポートを指定できることを除き、スタティック NAT と同じです。

この機能を使用すると、ステートメントごとにポートが異なるかぎり、多数のさまざまなスタティック ステートメントで同じマップ アドレスを指定できます（複数のスタティック *NAT* ステートメントに同じマップ アドレスを指定することはできません）。

セカンダリ チャネル（FTP、VoIP など）でアプリケーション検査を必要とするアプリケーションの場合、FWSM はセカンダリ ポートを自動的に変換します。

たとえば、FTP、HTTP、および SMTP にアクセスする複数のリモート ユーザに単一アドレスを提供し、実際にはそれぞれが実ネットワーク上の別々のサーバである場合、マップ IP アドレスは同じでもポートが異なる各サーバに対し、スタティック PAT ステートメントを指定できます（図 12-7 を参照）。

図 12-7　スタティック PAT



この例に対応するコマンドは、次のとおりです。

```
hostname(config)# static (inside,outside) tcp 209.165.201.3 ftp 10.1.2.27 ftp netmask
255.255.255.255
hostname(config)# static (inside,outside) tcp 209.165.201.3 http 10.1.2.28 http
netmask 255.255.255.255
hostname(config)# static (inside,outside) tcp 209.165.201.3 smtp 10.1.2.29 smtp
netmask 255.255.255.255
```

スタティック PAT を使用して、well-known ポートを非標準ポートに、またはその逆に変換することもできます。たとえば、内部 Web サーバがポート 8080 を使用する場合、外部ユーザにポート 80 へのアクセスを許可したあと、元のポート 8080 に対する変換を取り消すことができます。同様に、セキュリティを強化したい場合に、Web ユーザに非標準ポート 6785 に接続するように通知したあと、ポート 8080 に対する変換を取り消すことができます。

NAT 制御をイネーブルにした場合の NAT のバイパス

NAT 制御をイネーブルにした場合、外部ホストにアクセスするときに、内部ホストは NAT ルールと一致する必要があります。一部のホストで NAT を実行したくない場合は、これらのホストに対して NAT をバイパスできます（または、NAT 制御をディセーブルにすることもできます）。NAT をサポートしないアプリケーションを使用している場合などに、NAT をバイパスできます（NAT をサポートしないインスペクション エンジンについては、「アプリケーション インスペクション エンジンの概要」[p.20-2] を参照）。

3 とおりの方法で、NAT をバイパスするようにトラフィックを設定できます。どの方法でも、インスペクション エンジンとの互換性が確保されます。ただし、機能は少しずつ異なります。

- アイデンティティ NAT（**nat 0** コマンド）— アイデンティティ NAT を設定する場合（ダイナミック NAT と同様）、ホストの変換を特定のインターフェイスに限定しないでください。すべてのインターフェイスでの接続にアイデンティティ NAT を使用する必要があります。したがって、インターフェイス A にアクセスするときに、実アドレス上で標準変換を実行し、インターフェイス B にアクセスするときにアイデンティティ NAT を使用するといった選択はできません。これに対して、通常のダイナミック NAT を使用した場合は、アドレスを変換する特定のインターフェイスを指定できます。アイデンティティ NAT を使用する実アドレスは、アクセス リストに基づく使用可能なすべてのネットワーク上でルーティング可能でなければなりません。

  アイデンティティ NAT を使用した場合、マップ アドレスが実アドレスと同じでも、（アクセス リストで許可されている場合を含めて）外部から内部への接続を開始することはできません。外部から内部に接続するには、スタティック アイデンティティ NAT を使用するか、または NAT 除外を適用します。

- スタティク アイデンティティ NAT（**static** コマンド）— スタティック アイデンティティ NAT を使用すると、実アドレスを見せてもよいインターフェイスを指定できるので、インターフェイス A にアクセスするときにアイデンティティ NAT を使用し、インターフェイス B にアクセスするときに標準変換を使用することが可能です。スタティック アイデンティティ NAT では、ポリシー NAT も使用できます。この場合、変換する実アドレスを決定するときに、実アドレスと宛先アドレスを指定します（ポリシー NAT の詳細については、「ポリシー NAT」（p.12-10）を参照）。たとえば、内部アドレスから外部インターフェイスにアクセスし、宛先がサーバ A の場合に、内部アドレスにスタティック アイデンティティ NAT を使用し、外部サーバ B にアクセスするときには標準変換を使用するといったことが可能です。

- NAT 除外（**nat 0 access-list** コマンド）— 変換対象ホストとリモート ホストの両方で接続を開始できます。アイデンティティ NAT と同様に、ホストの変換を特定インターフェイスに制限せずに、NAT 除外をすべてのインターフェイスでの接続に使用する必要があります。ただし、NAT 除外では、変換する実アドレスを決定するときに、（ポリシー NAT と同様）実アドレスと宛先アドレスを指定できるので、きめ細い制御が可能になります。一方、ポリシー NAT と異なり、NAT 除外ではアクセス リストのポートは考慮されません。

ポリシー NAT

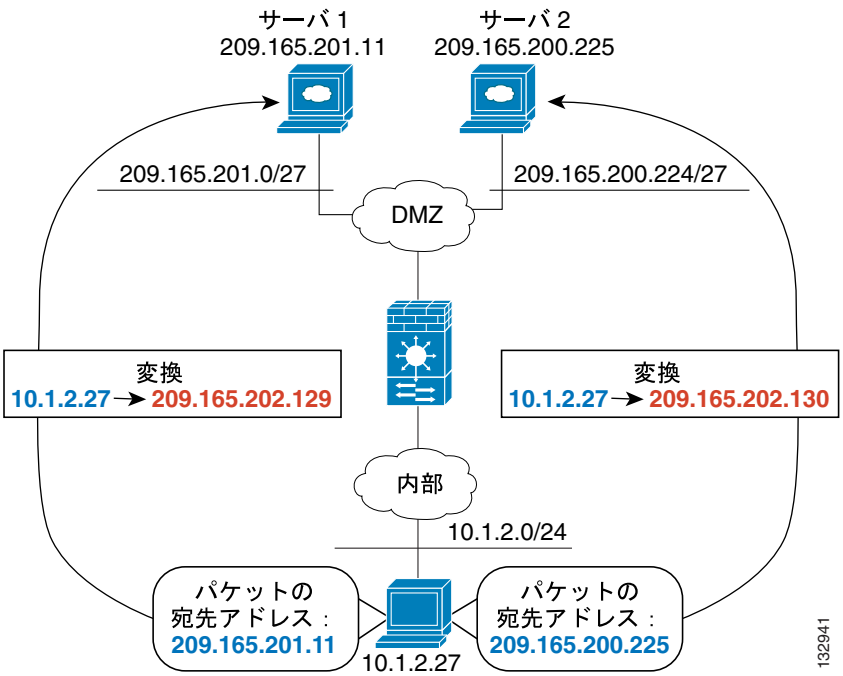
ポリシー NAT では、拡張アクセス リストで送信元アドレスと宛先アドレスを指定することによって、アドレス変換対象の実アドレスを特定します。任意で、送信元ポートと宛先ポートも指定できます。標準 NAT で考慮されるのは、実アドレスだけです。たとえば、サーバ A にアクセスするときには実アドレスをマップ アドレス A に変換しますが、アクセス サーバ B にアクセスするときには実アドレスをマップ アドレス B に変換します。

アプリケーション検査がセカンダリ チャネル（FTP、VoIP など）用に必要なアプリケーションに対してポリシー NAT でポートを指定するとき、FWSM はセカンダリ ポートを自動的に変換します。

（注） NAT 除外を除くすべてのタイプの NAT がポリシー NAT をサポートします。NAT 除外では、アクセス リストを使用して実アドレスを識別しますが、ポートが考慮されない点がポリシー NAT とは異なります。その他の相違点については、「NAT のバイパス」（p.12-32）を参照してください。ポリシー NAT をサポートしないスタティック アイデンティティ NAT を使用すると、NAT 除外と同じ結果を得ることができます。

図 12-8 に、10.1.2.0/24 のネットワークに存在し、2 種類のサーバにアクセスするホストを示します。ホストが 209.165.201.11 のサーバにアクセスすると、実アドレスが 209.165.202.129 に変換されます。ホストが 209.165.200.255 のサーバにアクセスすると、実アドレスが 209.165.202.130 に変換され、ホストがサーバと同じネットワーク上にあるように見せかけることができるため、ルーティングが可能になります。

図 12-8　異なる宛先アドレスを使用するポリシー NAT

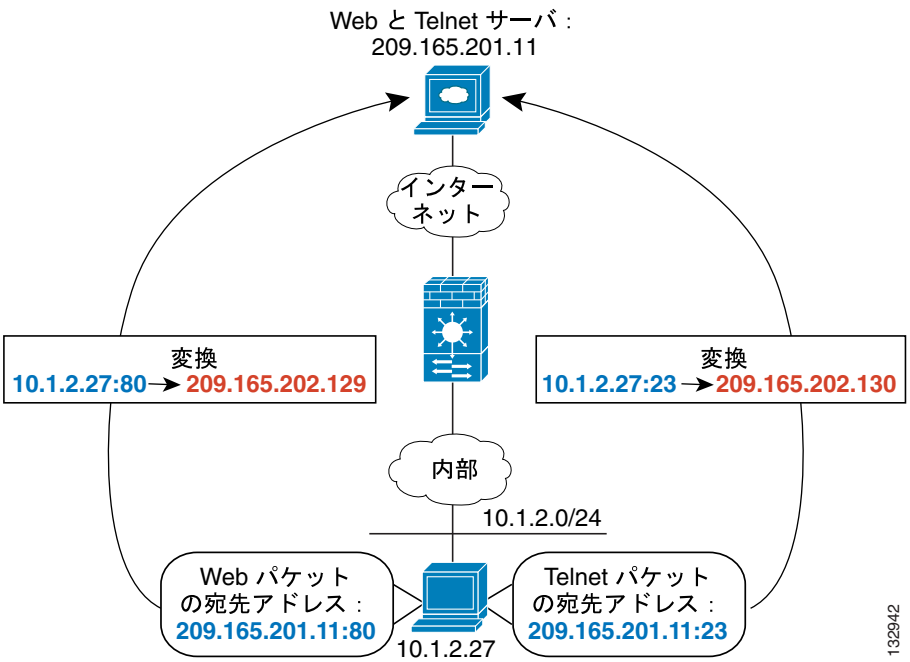


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 1 access-list NET1
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list NET2
hostname(config)# global (outside) 2 209.165.202.130
```

図 12-9 に、送信元ポートと宛先ポートの使用例を示します。10.1.2.0/24 のネットワーク上のホストは、単一ホストにアクセスして Web サービスと Telnet サービスの両方を利用します。ホストが Web サービスのためにサーバにアクセスした場合、実アドレスは 209.165.202.129 に変換されます。ホストが Telnet サービスのために同じサーバにアクセスした場合は、実アドレスは 209.165.202.130 に変換されます。

図 12-9　異なる宛先ポートを使用するポリシー NAT



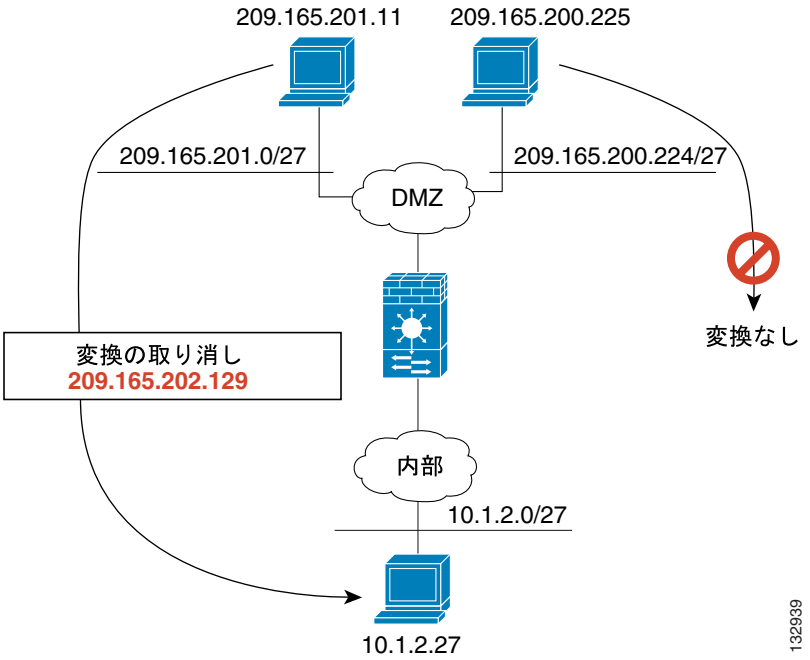
この例に対応するコマンドは、次のとおりです。

```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
hostname(config)# nat (inside) 1 access-list WEB
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list TELNET
hostname(config)# global (outside) 2 209.165.202.130
```

ポリシー スタティック NAT（および、同様にアクセス リストでトラフィックを識別する NAT 除外）の場合、変換対象ホストとリモート ホストの両方からトラフィックを発信できます。NAT アクセス リストは、変換対象ネットワークから発信されたトラフィックについては、実アドレスと*宛先*アドレスを指定しますが、リモート ネットワークから発信されたトラフィックについては、この変換を使用してホストに接続を許可されたリモート ホストの実アドレスと*送信元*アドレスを識別します。

図 12-10 は、変換対象ホストに接続するリモート ホストを示しています。変換対象ホストには、ネットワーク 209.165.201.0/27 との双方向のトラフィックだけに対し実アドレスを変換する、ポリシー スタティック NAT 変換が設定されています。ネットワーク 209.165.200.224/27 には変換が設定されていないので、変換対象ホストからこのネットワークに接続することはできません。また、このネットワーク上のホストから変換対象ホストに接続することもできません。

図 12-10　宛先アドレス変換を行うポリシー スタティック NAT



この例に対応するコマンドは、次のとおりです。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.224 209.165.201.0
255.255.255.224
hostname(config)# static (inside,outside) 209.165.202.129 access-list NET1
```

（注） ポリシー NAT は SQL*Net をサポートしませんが、標準 NAT は SQL*Net をサポートします。他のプロトコルの NAT サポートについては、「アプリケーション インスペクション エンジンの概要」（p.20-2）を参照してください。

NAT および同一セキュリティ レベルのインターフェイス

同一セキュリティ レベルのインターフェイス間では、NAT 制御がイネーブルになっている場合であっても、NAT は必要ありません。必要に応じて任意で NAT を設定することは可能です。ただし、NAT 制御がイネーブルになっている場合にダイナミック NAT を設定するときは、NAT が必要です。詳細については、「NAT 制御」（p.12-3）を参照してください。また、同一セキュリティ レベルのインターフェイス上でダイナミック NAT または PAT に対して IP アドレス グループを指定する場合、そのアドレス グループが下位または同一セキュリティ レベルのインターフェイスにアクセスするときには、アドレス グループに対して NAT を実行する必要があります（NAT 制御がイネーブルでない場合でも）。スタティック NAT として識別されたトラフィックは影響を受けません。

同一セキュリティ レベルの通信をイネーブルにする方法については、「同じセキュリティ レベルのインターフェイス間の通信の許可」（p.6-8）を参照してください。

（注） 同じセキュリティ レベルのインターフェイス上に NAT を設定した場合、FWSM は VoIP インスペクション エンジンをサポートしません。これらのインスペクション エンジンには、Skinny、SIP、および H.323 が含まれます。サポートされるインスペクション エンジンについては、「アプリケーション インスペクション エンジンの概要」（p.20-2）を参照してください。

実アドレス照合用 NAT コマンドの順序

FWSM は、次の順序で NAT コマンドに対して実アドレスを照合します。

1. NAT 除外（**nat 0 access-list**）— 最初の一致が見つかるまで順番どおり。アイデンティティ NAT はこのカテゴリではなく、標準スタティック NAT または標準 NAT のカテゴリに含まれます。予想外の結果が生じる可能性があるので、NAT 除外ステートメントには重複するアドレスを指定しないことを推奨します。
2. スタティック NAT およびスタティック PAT（標準およびポリシー）（**static**）— 最初の一致が見つかるまで順番どおり。スタティック アイデンティティ NAT はこのカテゴリに含まれません。**スタティック** ステートメント内でアドレスが重複する場合、警告が表示されますが、サポートは行われます。
3. ポリシー ダイナミック NAT（**nat access-list**）— 最初の一致が見つかるまで順番どおり。アドレスの重複は可能です。
4. 標準ダイナミック NAT（**nat**）— 最良の一致。標準アイデンティティ NAT はこのカテゴリに含まれます。NAT コマンドの順番は重要ではありません。実アドレスと最も一致した NAT ステートメントが使用されます。たとえば、インターフェイス上のすべてのアドレス（0.0.0.0）を変換する汎用ステートメントを作成できます。ネットワークのサブセット（10.1.1.1）を別のアドレスに変換する場合は、10.1.1.1 だけを変換するステートメントを作成できます。10.1.1.1 が接続を開始する場合、実アドレスと最も一致するので、10.1.1.1 用のステートメントが使用されます。重複するステートメントの使用は推奨できません。メモリの消費量が増え、FWSM のパフォーマンスが低下する可能性があるからです。

NAT ステートメントの最大数

FWSM は、次に示す数の **nat** コマンド、**global** コマンド、および **static** コマンドをサポートします。この数はすべてのコンテキスト間で分割されるか、またはシングルモードで使用されます。

- **nat** コマンド — 2 K
- **global** コマンド — 4 K
- **static** コマンド — 2 K

FWSM ではポリシー NAT 用として、シングルモードではアクセス リストに最大 3942 の ACE、マルチモードでは 7272 の ACE を指定できます。

マップ アドレスに関する注意事項

実アドレスをマップ アドレスに変換するときには、次のマップ アドレスを使用できます。

- マップ インターフェイスと同じネットワーク上のアドレス

  （FWSM から出ていくトラフィックが通過する）マップ インターフェイスと同じネットワーク上のアドレスを使用した場合、FWSM はプロキシ ARP を使用してマップ アドレスの要求に応答することによって、実アドレス宛てのトラフィックを代行受信します。このソリューションにより、FWSM は他のネットワークに対するゲートウェイにはならないので、ルーティングが簡素化されます。ただし、この方式は、変換に使用できるアドレス数に制限があります。

  PAT の場合、マップ インターフェイスの IP アドレスも使用できます。

- 固有のネットワーク上のアドレス

  マップ インターフェイス ネットワーク上で使用できる数より多くのアドレスが必要な場合、別のサブネット上のアドレスを指定できます。FWSM は、プロキシ ARP を使用してマップ アドレス要求に応答することによって、実アドレス宛てのトラフィックを代行受信します。OSPF を使用し、マップ インターフェイス上でルートをアドバタイズする場合、FWSM はマップ アドレスをアドバタイズします。マップ インターフェイスがパッシブの場合（ルートをアドバタイズしない）、またはスタティック ルーティングを使用する場合は、マップ アドレス宛てのトラフィックを FWSM に送信するアップストリーム ルータ上でスタティック ルートを追加する必要があります。

DNS および NAT

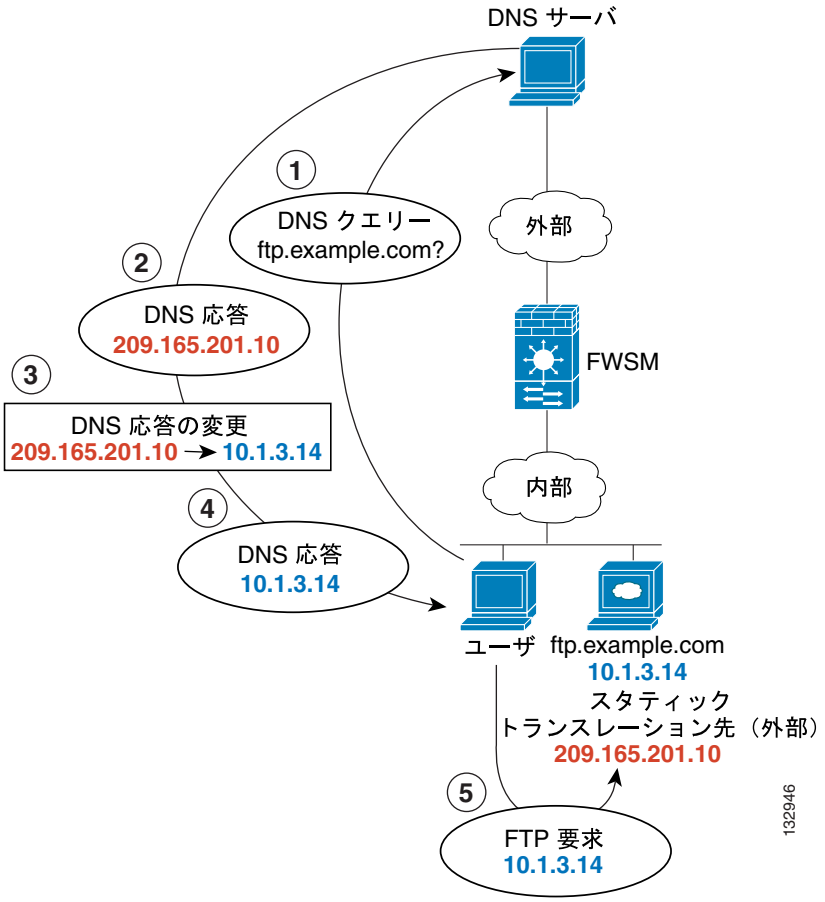
DNS 応答内のアドレスを NAT の設定と一致するアドレスに置き換えることで応答を変更するように、FWSM を設定しなければならない場合があります。DNS の変更は、各変換を設定するときに行うことができます。

たとえば、DNS サーバは外部インターフェイスからアクセスできます。サーバ ftp.example.com は内部インターフェイス上にあります。ftp.example.com の実アドレス（10.1.3.14）が外部ネットワークで表示されるマップ アドレス（209.165.201.10）にスタティックに変換されるように、FWSM を設定します（図 12-11 を参照）。この場合、このスタティック ステートメントで DNS 応答の変更をイネーブルに設定し、実アドレスを使用して ftp.example.com にアクセスする内部ユーザが、マップ アドレスではなく、DNS サーバから実アドレスを受信するようにします。

内部ホストが ftp.example.com のアドレスを求める DNS 要求を送信すると、DNS サーバはマップ アドレス（209.165.201.10）で応答します。FWSM は内部サーバのスタティック ステートメントを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答の変換をイネーブルにしなかった場合、内部ホストは ftp.example.com に直接アクセスする代わりに、209.165.201.10 にトラフィックを送信しようとします。

（注） DNS クエリー応答内の実 IP アドレスに対し、ルートを指定する必要があります。指定しないと、FWSM は NAT を実行しません。必要なルートは、スタティック ルーティング、または RIP や OSPF などのルーティング プロトコルによって突き止めることができます。

図 12-11　DNS 応答の変更

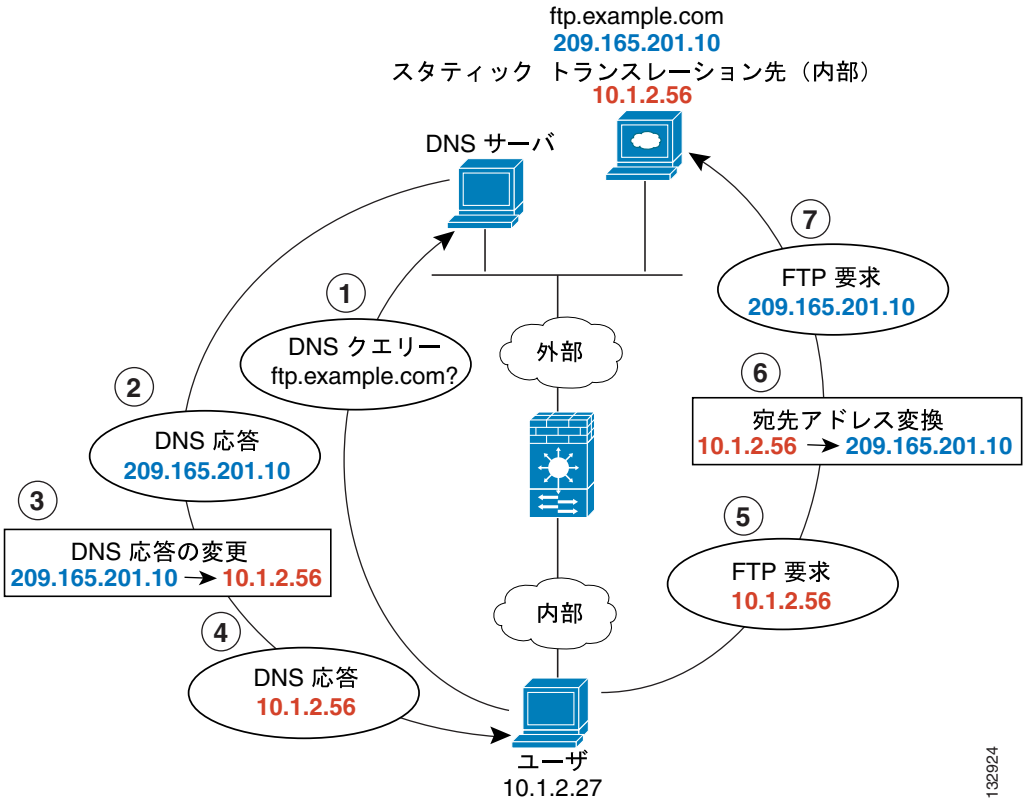


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# static (inside,outside) 209.165.201.10 10.1.3.14 netmask
255.255.255.255 dns
```

図 12-12 に、外部の Web サーバと DNS サーバを示します。FWSM には、外部サーバ用のスタティック トランスレーションが設定されています。この場合、内部ユーザが DNS サーバに ftp.example.com のアドレスを要求すると、DNS サーバは実アドレス 209.165.20.10 で応答します。内部ユーザには、ftp.example.com のマップ アドレス（10.1.2.56）を使用させるので、このスタティック トランスレーションに対して DNS 応答の変更を設定する必要があります。

図 12-12　DNS 応答の変更（外部 NAT を使用する場合）



この例に対応するコマンドは、次のとおりです。

```
hostname(config)# static (outside,inside) 10.1.2.56 209.165.201.10 netmask
255.255.255.255 dns
```

NAT 制御の設定

NAT 制御では、内部インターフェイスから外部インターフェイスへのパケットは NAT ルールと一致する必要があります。詳細については、「NAT 制御」（p.12-3）を参照してください。

NAT 制御をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# nat-control
```

NAT 制御をディセーブルにするには、このコマンドの **no** 形式を入力します。

ダイナミック NAT および PAT の使用方法

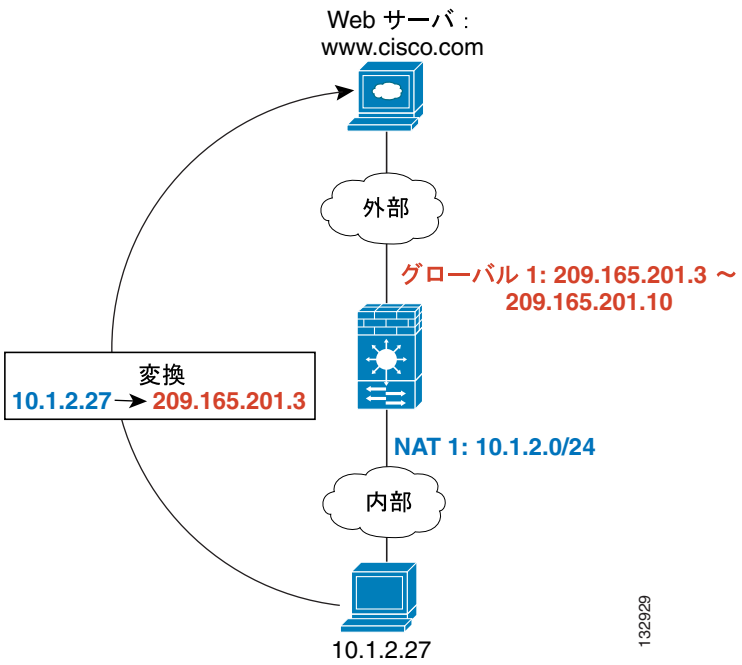
ここでは、ダイナミック NAT および PAT の設定方法について説明します。内容は次のとおりです。

- ダイナミック NAT および PAT の実装（p.12-17）
- ダイナミック NAT または PAT の設定（p.12-23）

ダイナミック NAT および PAT の実装

ダイナミック NAT および PAT の場合、最初に **nat** コマンドを設定して、変換するインターフェイス上の実アドレスを指定します。次に、別の **global** コマンドを設定して、別のインターフェイスから出るときのマップ アドレスを指定します（PAT の場合、このアドレスは 1 つです）。NAT ID、各コマンドに割り当てる番号を比較して、各 **nat** コマンドと **global** コマンドを照合します（図 12-13 を参照）。

図 12-13　NAT およびグローバル ID の照合

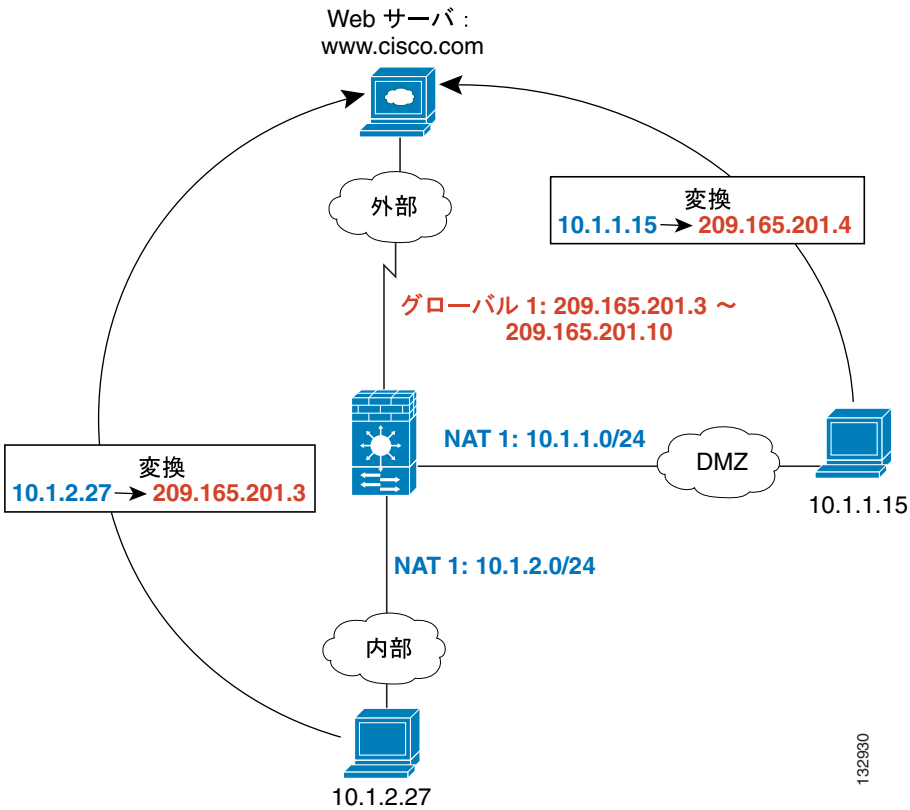


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.3-209.165.201.10
```

同じ NAT ID を使用して各インターフェイスに 1 つずつ **nat** コマンドを入力できます。その場合、トラフィックがインターフェイスから出ていくときに、すべてのインターフェイスで同じ **global** コマンドが使用されます。たとえば、内部インターフェイスと DMZ インターフェイスに NAT ID 1 を使用して、**nat** コマンドを設定します。さらに、同様に ID 1 を使用して、外部インターフェイスに **global** コマンドを設定します。内部インターフェイスと DMZ インターフェイスからのトラフィックは、外部インターフェイスを出るときに、マップ プールまたは PAT アドレスを共有します（図 12-14 を参照）。

図 12-14　複数のインターフェイスにおける NAT コマンド

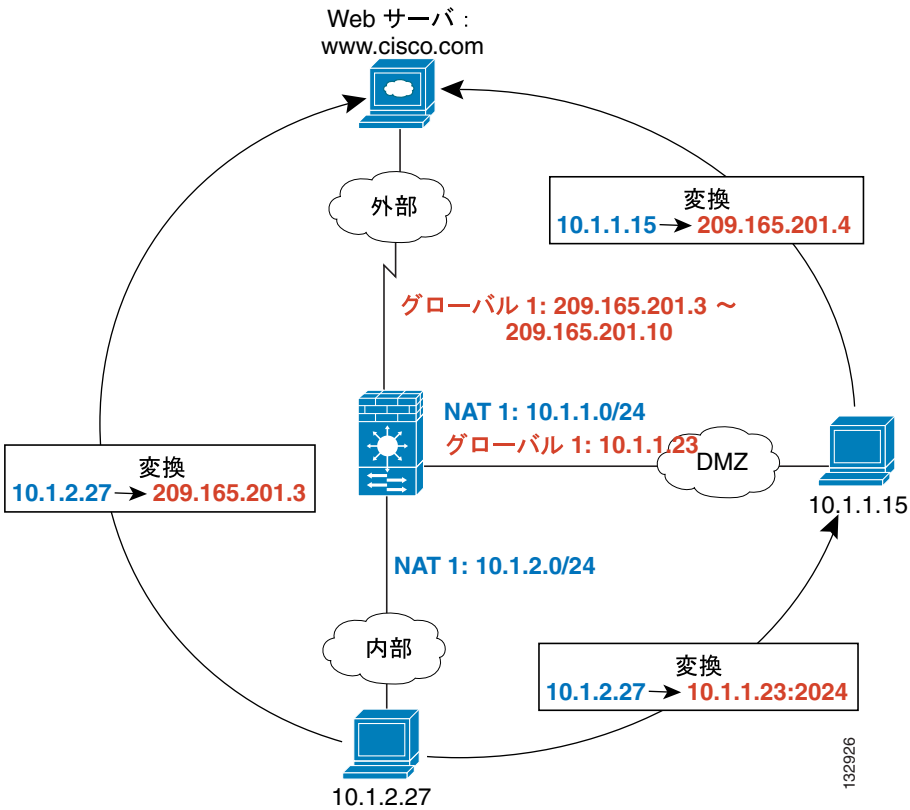


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0
hostname(config)# nat (dmz) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.3-209.165.201.10
```

同じ NAT ID を使用して、各インターフェイスに **global** コマンドを 1 つずつ入力することもできます。ID 1 を使用して、外部インターフェイスと DMZ インターフェイスに **global** コマンドを入力した場合、内部 **nat** コマンドでは、外部インターフェイスと DMZ インターフェイスの両方に送る場合に、トラフィックを変換することを指定します。同様に、DMZ インターフェイスにも ID 1 を使用して **nat** コマンドを入力した場合、DMZ トラフィックにも外部インターフェイス上の **global** コマンドが使用されます（図 12-15 を参照）。

図 12-15　複数のインターフェイスにおけるグローバルおよび NAT コマンド

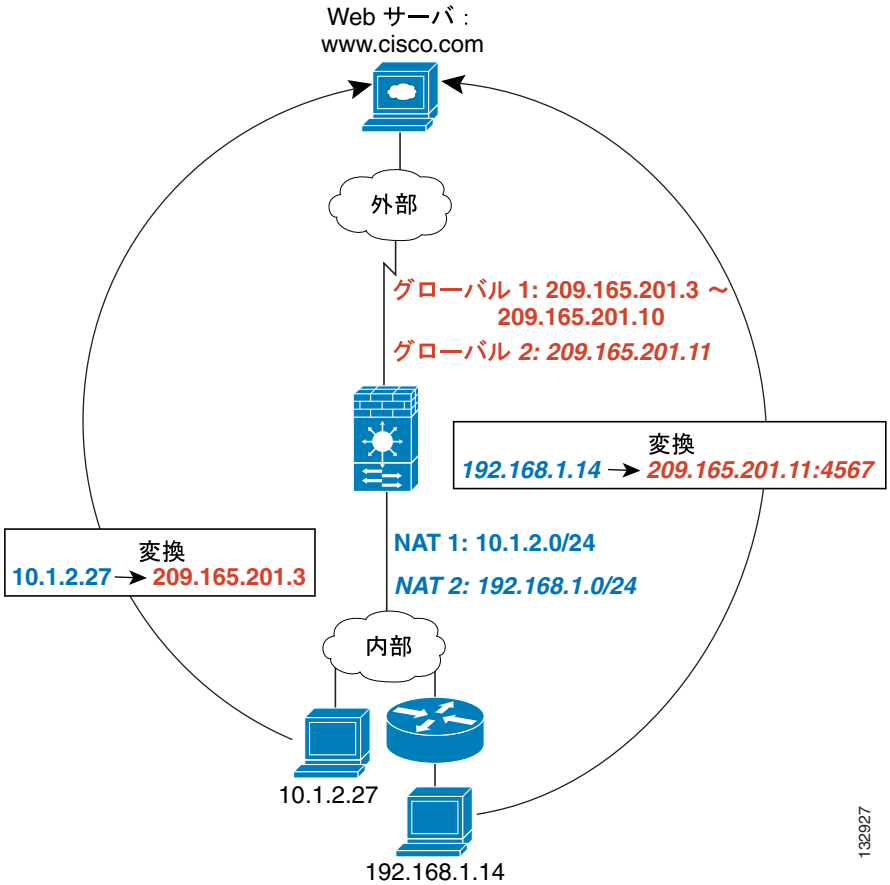


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0
hostname(config)# nat (dmz) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.3-209.165.201.10
hostname(config)# global (dmz) 1 10.1.1.23
```

複数の異なる NAT ID を使用する場合は、さまざまな実アドレス セットにそれぞれ異なるマップ アドレスが割り当てられるように指定します。たとえば、内部インターフェイス上で、2 つの **nat** コマンドを 2 つの NAT ID に指定できます。外部インターフェイスでは、この 2 つの ID に対応する **global** コマンドを 2 つ設定できます。さらに、内部ネットワーク A のトラフィックが外部インターフェイスから出るときに、IP アドレスはプール A のアドレスに変換されます。内部ネットワーク B のトラフィックはプール B のアドレスに変換されます（図 12-16 を参照）。ポリシー NAT を使用する場合、各アクセス リストで宛先アドレスとポートが一意であれば、複数の **nat** コマンドに同一の実アドレスを指定できます。

図 12-16　異なる NAT ID

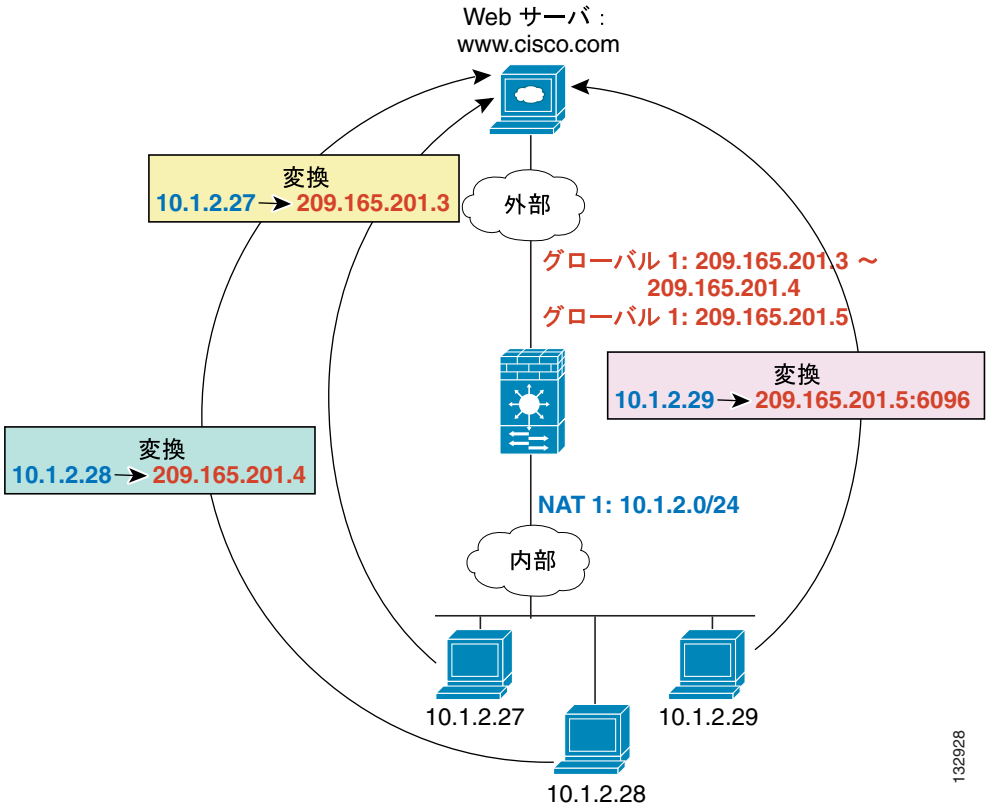


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0
hostname(config)# nat (inside) 2 192.168.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.3-209.165.201.10
hostname(config)# global (outside) 2 209.165.201.11
```

同じ NAT ID を使用して、1 つのインターフェイスに複数の **global** コマンドを入力できます。この場合、FWSM は最初に、ダイナミック NAT の **global** コマンドをコンフィギュレーションで指定された順番どおりに使用し、次に PAT の **global** コマンドを順番どおりに使用します。特定のアプリケーションにダイナミック NAT を使用する必要があり、なおかつダイナミック NAT アドレスをすべて使い果たした場合に備えてバックアップ用の PAT ステートメントも必要だという場合、ダイナミック NAT **global** コマンドと PAT **global** コマンドの両方を入力します。同様に、1 つの PAT マップ ステートメントでサポートされる約 64,000 より多くの PAT セッションが必要な場合、PAT ステートメントを 2 つ入力できます（図 12-17 を参照）。

図 12-17　NAT および PAT の併用

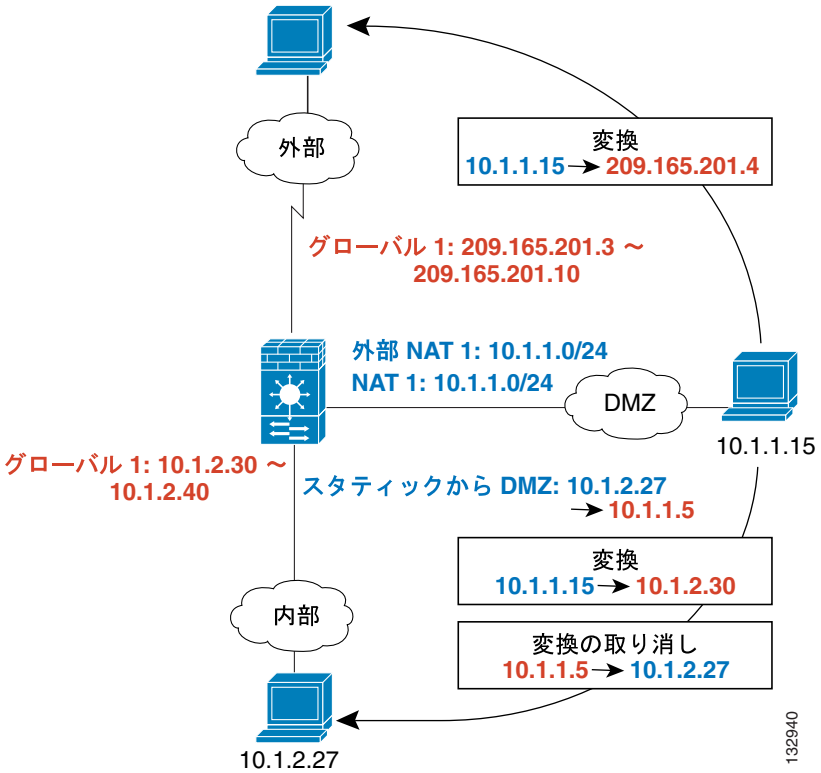


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.3-209.165.201.4
hostname(config)# global (outside) 1 209.165.201.5
```

外部 NAT の場合、外部 NAT 用の **nat** コマンドを識別する必要があります（**outside** キーワード）。内部インターフェイスにアクセスしたときにも同じトラフィックを変換する場合は（DMZ 上のトラフィックを内部インターフェイスにアクセスするときにも、外部インターフェイスにアクセスするときにも変換するような状況）、**outside** オプションを使用せずに、別個の **nat** コマンドを設定する必要があります。この場合、両方のステートメントで同じアドレスを指定し、同じ NAT ID を使用できます（図 12-18 を参照）。外部 NAT（DMZ インターフェイスから内部インターフェイス）の場合、内部ホストは **static** コマンドを使用して外部アクセスを許可するので、送信元アドレスと宛先アドレスの両方が変換されることに注意してください。

図 12-18　外部 NAT および内部 NAT の組み合わせ



この例に対応するコマンドは、次のとおりです。

```
hostname(config)# nat (dmz) 1 10.1.1.0 255.255.255.0 outside
hostname(config)# nat (dmz) 1 10.1.1.0 255.255.255.0
hostname(config)# static (inside,dmz) 10.1.2.27 10.1.1.5 netmask 255.255.255.255
hostname(config)# global (outside) 1 209.165.201.3-209.165.201.4
hostname(config)# global (inside) 1 10.1.2.30-1-10.1.2.40
```

nat コマンドで IP アドレス グループを指定する場合、そのアドレス グループが下位または同一セキュリティ レベルのインターフェイスにアクセスするときに、そのアドレス グループに対して NAT を実行する必要があります。各インターフェースで同じ NAT ID を持つ **global** コマンドを適用するか、**static** コマンドを使用します。アドレス グループが上位セキュリティ レベルのインターフェイスにアクセスする場合、NAT は必要ありません。外部から内部に NAT を実行するには、**outside** キーワードを使用して別個の **nat** コマンドを作成する必要があるためです。外部 NAT を適用する場合、アドレス グループがすべての上位セキュリティ レベルのインターフェイスにアクセスするときに、直前の NAT 要件がそのアドレス グループに対して有効になります。**static** コマンドによって識別されたトラフィックは影響を受けません。

ダイナミック NAT または PAT の設定

ここでは、ダイナミック NAT またはダイナミック PAT の設定方法について説明します。ダイナミック NAT およびダイナミック PAT の設定方法はほぼ同じですが、NAT ではマップ アドレス範囲を指定するのに対して、PAT では単一アドレスを指定します。

図 12-19 に、一般的なダイナミック NAT の使用例を示します。変換対象ホストのみが NAT セッションを作成することができ、応答トラフィックの返信が許可されます。マップ アドレスは **global** コマンドによって定義されたプールから動的に割り当てられます。

図 12-19　ダイナミック NAT

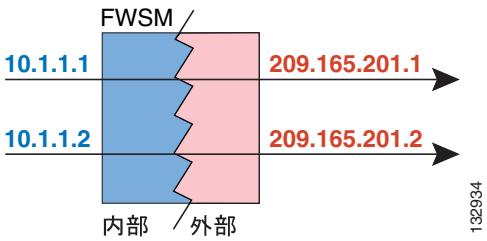
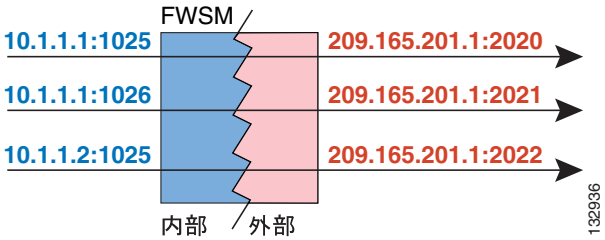


図 12-20 に、一般的なダイナミック PAT の使用例を示します。変換対象ホストのみが NAT セッションを作成することができ、応答トラフィックの返信が許可されます。**global** コマンドによって定義されたマップ アドレスは各変換で同一ですが、ポートは動的に割り当てられます。

図 12-20　ダイナミック PAT



ダイナミック NAT の詳細については、「ダイナミック NAT」（p.12-5）を参照してください。PAT の詳細については、「PAT」（p.12-7）を参照してください。

（注） NAT の設定を変更し、既存の変換がタイムアウトする前に新しい NAT 情報を使用する必要がある場合は、**clear xlate** コマンドを使用して、変換テーブルを消去します。ただし、変換テーブルを消去すると、その変換を使用するすべての接続が切断されます。

ダイナミック NAT または PAT を設定するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、変換する実アドレスを指定します。

- ポリシー NAT：

```
hostname(config)# nat (real_interface) nat_id access-list acl_name [dns] [outside]
[[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns] [norandomseq]
```

他の **nat** コマンドで重複するアドレスを指定できます。たとえば、あるコマンドで 10.1.1.0 を指定し、別のコマンドで 10.1.1.1 を指定できます。トラフィックは最初の一致が見つかるまで順番にポリシー NAT コマンドと照合されます。または標準 NAT の場合は、最良の一致を使用します。

このコマンドのオプションについて説明します。

— **access-list** *acl_name* — 拡張アクセス リストを使用して、実アドレスと宛先アドレスを指定します。**access-list** コマンドを使用してアクセス リストを作成します（「拡張アクセス リストの追加」[p.10-7] を参照）。このアクセス リストには、**permit** ACE しか含めることができません。**eq** 演算子を使用して、アクセス リストに実ポートと宛先ポートを任意に指定できます。ポリシー NAT では **inactive** または **time-range** キーワードは考慮されず、すべての ACE がポリシー NAT コンフィギュレーションに対してアクティブであるとみなされます。

— *nat_id* — 1 ～ 65,535 の整数です。NAT ID は **global** コマンドの NAT ID と一致する必要があります。NAT ID の使用方法の詳細については、「ダイナミック NAT および PAT の実装」（p.12-17）を参照してください。**0** は NAT 除外用として予約されています（NAT 除外の詳細については、「NAT 除外の設定」[p.12-34] を参照）。

— **dns** — DNS サーバにエントリが作成されているホストのアドレスを **nat** コマンドに指定し、なおかつ DNS サーバがクライアントとは異なるインターフェイス上に配置されている場合、クライアントと DNS サーバに必要なホスト アドレスはそれぞれ異なります。一方はマップ アドレスが必要で、もう一方は実アドレスが必要です。このオプションを使用すると、クライアントに対する DNS 応答のアドレスが書き換えられます。変換対象のホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上に存在していなければなりません。通常、外部インターフェイスからアクセス許可が必要なホストにはスタティック変換を使用するので、このオプションは **static** コマンドと組み合わせて使用するのが一般的です（詳細については、「DNS および NAT」[p.12-14] を参照）。

— **outside** — このインターフェイスのセキュリティ レベルが **global** ステートメントの一致によって特定されたインターフェイスより低い場合、**outside** を入力し、NAT インスタンスを外部 NAT として指定する必要があります。

— **tcp** *tcp_max_conns* — サブネット全体における同時 TCP 接続の最大数（65,536 まで）を指定します。デフォルトは 0 で、これは最大接続数を意味します。

— *emb_limit* — ホストごとの初期接続の最大数（65,536 まで）です。デフォルトは 0 で、これは最大接続数を意味します。*emb_limit* を入力する前に、**tcp** *tcp_max_conns* を入力する必要があります。*tcp_max_conns* にはデフォルト値を使用し、*emb_limit* を変更する場合は、*tcp_max_conns* に **0** を入力します。

初期接続とは、送信元と宛先間で所定のハンドシェークが完了していない接続要求のことです。初期接続数を制限すると、DoS 攻撃からシステムを保護できます。FWSM は初期接続制限を使用して、TCP 代行受信機能をトリガーします。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阻止します。SYN フラッディング攻撃では通常、スプーフィングされた IP アドレスから一連の SYN パケットが送信されます。継続的に送信される SYN パケットにより、サーバの SYN キューが常に満杯状態になり、接続要求を処理できなくなります。接続が、初期接続スレッシュホールドに達すると、FWSM はサーバのプロキシとして動作し、クライアントの SYN 要求に対して SYN-ACK 応答を生成します。FWSM は、クライアントから ACK の返信を受信すると、そのクライアントを認証し、サーバへの接続を許可します。

— **udp** *udp_max_conns* — サブネット全体における同時 UDP 接続の最大数（65,536 まで）を設定します。デフォルトは 0 で、これは最大接続数を意味します。

— **norandomseq** — TCP Initial Sequence Number（ISN）ランダム化をディセーブルにします。TCP シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化し、その結果、データのスクランブルが発生する場合だけです。各 TCP 接続には、2 つの Initial Sequence Number（ISN）があります。1 つはクライアントが作成し、もう 1 つはサーバが作成します。FWSM はホスト / サーバによって生成された ISN をランダム化します。攻撃側が次の ISN を予測してセッションを乗っ取る可能性を排除するために、ISN の少なくとも一方はランダムに作成する必要があります。

（注） Modular Policy Framework を使用して接続制限（初期接続制限は設定できません）を設定することもできます。詳細については、「接続制限とタイムアウトの設定」（p.19-2）を参照してください。NAT を使用する場合のみ、初期接続制限を設定できます。両方の方法を使用する同一トラフィックに対してこれらを設定した場合、FWSM は低い制限値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルになっている場合、FWSM は TCP シーケンスのランダム化をディセーブルにします。

- 標準 NAT

```
hostname(config)# nat (real_interface) nat_id real_ip [mask [dns] [outside]
[[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns] [norandomseq]]
```

nat_id は 1 ～ 2,147,483,647 の整数です。NAT ID は **global** コマンドの NAT ID と一致する必要があります。NAT ID の使用方法の詳細については、「ダイナミック NAT および PAT の実装」（p.12-17）を参照してください。**0** はアイデンティティ NAT 用として予約されています。アイデンティティ NAT の詳細については、「アイデンティティ NAT の設定」（p.12-32）を参照してください。

その他のオプションについては、前述のポリシー NAT コマンドを参照してください。

ステップ 2　次のコマンドを入力して、特定のインターフェイスから送信される実アドレスに割り当てるマップアドレス（複数可）を指定します。

```
hostname(config)# global (mapped_interface) nat_id {mapped_ip[-mapped_ip]}
```

この NAT ID は、**nat** コマンドの NAT ID と一致する必要があります。対応する **nat** コマンドで、このインターフェイスを出るときに変換するアドレスを指定します。

単一アドレス（PAT の場合）またはアドレス範囲（NAT の場合）を指定できます。範囲は必要に応じて、サブネット境界を超えて指定できます。次に、指定できる「スーパーネット」の例を示します。

```
192.168.1.1-192.168.2.254
```

たとえば、内部インターフェイスの 10.1.1.0/24 ネットワークを変換する場合、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.1-209.165.201.30
```

ダイナミック NAT のアドレス プールとともに、NAT プールを使い果たしたときのために PAT アドレスを指定する場合は、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.5
hostname(config)# global (outside) 1 209.165.201.10-209.165.201.20
```

ルーティングを簡素化する場合など、セキュリティ レベルの低い DMZ ネットワークのアドレスを変換し、内部ネットワーク（10.1.1.0）と同じネットワーク上にあるように見せるには、次のコマンドを入力します。

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
```

ポリシー NAT を使用して、1 つの実アドレスに 2 つの宛先アドレスを指定するには、次のコマンドを入力します（図 12-8（p.12-10）を参照）。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 1 access-list NET1 tcp 0 2000 udp 10000
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list NET2 tcp 1000 500 udp 2000
hostname(config)# global (outside) 2 209.165.202.130
```

ポリシー NAT を使用して、1 つの実アドレス / 宛先アドレス ペアに複数の異なるポートを指定するには、次のコマンドを入力します（図 12-9（p.12-11）を参照）。

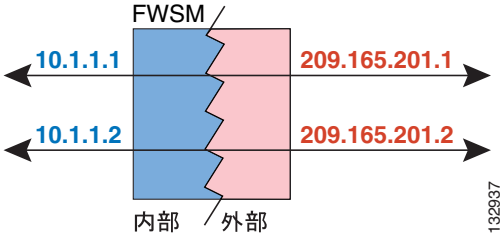
```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
hostname(config)# nat (inside) 1 access-list WEB
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list TELNET
hostname(config)# global (outside) 2 209.165.202.130
```

スタティック NAT の使用方法

ここでは、スタティック トランスレーションの設定方法について説明します。

図 12-21 に、一般的なスタティック NAT の使用例を示します。変換は常にアクティブであるため、変換対象ホストとリモート ホストの両方で接続を生成でき、マップ アドレスは **static** コマンドによって静的に割り当てられます。

図 12-21　スタティック NAT



同じ 2 つのインターフェイス間で複数の **static** コマンドに、同じ実アドレスまたはマップ アドレスを使用することはできません。同一マップ インターフェイスの **global** コマンドにも定義されたマップ アドレスを、**static** コマンドに使用しないでください。

スタティック NAT の詳細については、「スタティック NAT」（p.12-7）を参照してください。

（注） **static** コマンドを削除しても、その変換を使用する既存の接続は影響を受けません。これらの接続を削除するには、**clear local-host** コマンドを入力します。

変換テーブルから **clear xlate** コマンドでスタティック トランスレーションを消去することはできません。代わりに、**static** コマンドを削除する必要があります。**nat** および **global** コマンドで作成されたダイナミック変換のみ、**clear xlate** コマンドで削除できます。

スタティック NAT を設定するには、次のいずれかのコマンドを入力します。

- ポリシー スタティック NAT の場合、次のコマンドを入力します。

```
hostname(config)# static (real_interface,mapped_interface) mapped_ip
access-list acl_name [dns] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
[norandomseq]
```

  access-list コマンドを使用してアクセス リストを作成します（「拡張アクセス リストの追加」[p.10-7] を参照）。このアクセス リストには、**permit** ACE しか含めることができません。アクセス リストで使用した送信元サブネット マスクをマップ アドレスにも使用します。**eq** 演算子を使用して、アクセス リストに実ポートと宛先ポートを指定することもできます。ポリシー NAT では **inactive** または **time-range** キーワードは考慮されず、すべての ACE がポリシー NAT コンフィギュレーションに対してアクティブであるとみなされます。詳細については、「ポリシー NAT」（p.12-10）を参照してください。

  変換のためにネットワークを指定する場合（10.1.1.0 255.255.255.0 など）、FWSM はアドレス .0 および .255 を変換します。これらのアドレスへのアクセスを阻止する場合は、アクセスを拒否するようにアクセス リストを設定します。

  その他のオプションについては、「ダイナミック NAT または PAT の設定」（p.12-23）を参照してください。

- 標準スタティック NAT を設定する場合、次のコマンドを入力します。

  hostname(config)# **static (***real_interface***,***mapped_interface***)** *mapped_ip real_ip* [**netmask** *mask*] [**dns**] [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]

  オプションについては、「ダイナミック NAT または PAT の設定」(p.12-23)を参照してください。

次のポリシー スタティック NAT の例では、1 つの実アドレスが宛先アドレスに応じて 2 つのマップ アドレスに変換されます（図 12-8 [p.12-10] を参照）。

```
hostname(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224
255.255.255.224
hostname(config)# static (inside,outside) 209.165.202.129 access-list NET1
hostname(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

次のコマンドで、内部 IP アドレス（10.1.1.3）を外部 IP アドレス（209.165.201.12）に対応付けます。

```
hostname(config)# static (inside,outside) 209.165.201.12 10.1.1.3 netmask
255.255.255.255
```

次のコマンドで、外部アドレス（209.165.201.15）を内部アドレス（10.1.1.6）に対応付けます。

```
hostname(config)# static (outside,inside) 10.1.1.6 209.165.201.15 netmask
255.255.255.255
```

次のコマンドで、サブネット全体をスタティックに対応付けます。

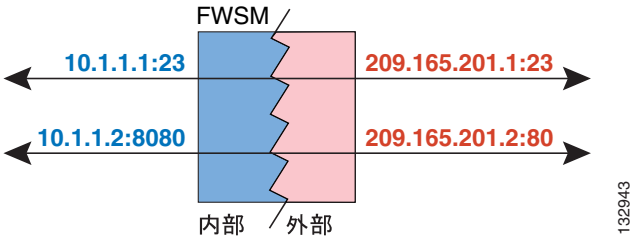
```
hostname(config)# static (inside,dmz) 10.1.1.0 10.1.2.0 netmask 255.255.255.0
```

スタティック PAT の使用方法

ここでは、スタティック ポート トランスレーションの設定方法について説明します。スタティック PAT を使用すると、実 IP アドレスをマップ IP アドレスに変換し、さらに実ポートをマップ ポートに変換できます。実ポートを同一ポートを変換する場合は、特定のトラフィック タイプのみを変換できます。または、別のポートに変換することによってさらに細かく制御することもできます。

図 12-22 に、一般的なスタティック PAT の使用例を示します。変換は常にアクティブであるため、変換対象ホストとリモート ホストの両方で接続を生成でき、マップ アドレスおよびポートは **static** コマンドによって静的に割り当てられます。

図 12-22　スタティック PAT



セカンダリ チャネル（FTP、VoIP など）でアプリケーション検査を必要とするアプリケーションの場合、FWSM はセカンダリ ポートを自動的に変換します。

同じ 2 つのインターフェイス間で複数の **static** ステートメントに、同じ実アドレスまたはマップ アドレスを使用することはできません。同一マップ インターフェイスの **global** コマンドにも定義されたマップ アドレスを、**static** コマンドに使用しないでください。

スタティック PAT の詳細については、「スタティック PAT」（p.12-8）を参照してください。

（注） **static** コマンドを削除しても、その変換を使用する既存の接続は影響を受けません。これらの接続を削除するには、**clear local-host** コマンドを入力します。

変換テーブルから **clear xlate** コマンドでスタティック トランスレーションを消去することはできません。代わりに、**static** コマンドを削除する必要があります。**nat** および **global** コマンドで作成されたダイナミック変換のみ、**clear xlate** コマンドで削除できます。

スタティック PAT を設定するには、次のいずれかのコマンドを入力します。

- ポリシー スタティック PAT の場合、次のコマンドを入力します。

```
hostname(config)# static (real_interface,mapped_interface) {tcp | udp} mapped_ip
mapped_port access-list acl_name [dns] [[tcp] tcp_max_conns [emb_limit]]
[udp udp_max_conns] [norandomseq]
```

  access-list コマンドを使用してアクセス リストを作成します（「拡張アクセス リストの追加」[p.10-7] を参照）。アクセス リストのプロトコルとこのコマンドで設定するプロトコルは一致している必要があります。たとえば、**static** コマンドで **tcp** を指定する場合は、アクセス リストで **tcp** を指定する必要があります。ポートを指定するには、**eq** 演算子を使用します。このアクセス リストには、**permit** ACE しか含めることができません。アクセス リストで使用した送信元サブネット マスクをマップ アドレスにも使用します。ポリシー NAT では **inactive** または **time-range** キーワードは考慮されず、すべての ACE がポリシー NAT コンフィギュレーションに対してアクティブであるとみなされます。

変換に対してネットワークを指定する場合（10.1.1.0 255.255.255.0 など）、FWSM はアドレス .0 および .255 を変換します。これらのアドレスへのアクセスを阻止する場合は、アクセスを拒否するようにアクセス リストを設定します。

その他のオプションについては、「ダイナミック NAT または PAT の設定」（p.12-23）を参照してください。

- 標準スタティック PAT を設定する場合は、次のコマンドを入力します。

```
hostname(config)# static (real_interface,mapped_interface) {tcp | udp} mapped_ip
mapped_port real_ip real_port [netmask mask] [dns] [[tcp] tcp_max_conns
[emb_limit]] [udp udp_max_conns] [norandomseq]
```

オプションについては、「ダイナミック NAT または PAT の設定」（p.12-23）を参照してください。

たとえば、ネットワーク 10.1.3.0 上のホストから FWSM の外部インターフェイス（10.1.2.14）に Telnet トラフィックを送信する場合、次のコマンドを入力すると、10.1.1.15 の内部ホストにトラフィックをリダイレクトできます。

```
hostname(config)# access-list TELNET permit tcp host 10.1.1.15 eq telnet 10.1.3.0
255.255.255.0 eq telnet
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet access-list TELNET
```

ネットワーク 10.1.3.0 上のホストから FWSM の外部インターフェイス（10.1.2.14）に HTTP トラフィックを送信する場合、次のように入力すると、10.1.1.15 の内部ホストにトラフィックをリダイレクトできます。

```
hostname(config)# access-list HTTP permit tcp host 10.1.1.15 eq http 10.1.3.0
255.255.255.0 eq http
hostname(config)# static (inside,outside) tcp 10.1.2.14 http access-list HTTP
```

FWSM の外部インターフェイス（10.1.2.14）から 10.1.1.15 の内部ホストに Telnet トラフィックをリダイレクトする場合、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
```

ただし、この例で前述の実 Telnet サーバに接続を開始させる場合は、追加の変換が必要です。たとえば、他のすべてのトラフィック タイプを変換する場合は、次のコマンドを入力します。元の **static** コマンドがサーバへの Telnet を変換するのに対して、**nat** コマンドおよび **global** コマンドはサーバからの発信接続に PAT を実行します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
```

さらに、すべての内部トラフィックに別個の変換を実行し、内部ホストで Telnet サーバとは異なるマップ アドレスを使用する場合でも、Telnet サーバから開始されたトラフィックに、サーバへの Telnet トラフィックを可能にする **static** ステートメントと同じマップ アドレスを使用できます。その場合、Telnet サーバ用に、より排他的な **nat** ステートメントを作成する必要があります。**nat** ステートメントは最良の一致方式で読み取られるので、排他性の強い **nat** ステートメントは一般的な

ステートメントより先に照合されます。次に、Telnet **static** ステートメント、Telnet サーバから開始されたトラフィックに対応する排他性の強い **nat** ステートメント、および他の内部ホストに対応し、別のマップ アドレスを使用するステートメントの例を示します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
hostname(config)# nat (inside) 2 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 2 10.1.2.78
```

well-known ポート（80）を別のポート（8080）に変換するには、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.45 80 10.1.1.16 8080 netmask
255.255.255.255
```

NAT のバイパス

ここでは、NAT のバイパス方法について説明します。NAT 制御をイネーブルにするときに、NAT をバイパスできます。アイデンティティ NAT、スタティック アイデンティティ NAT、または NAT 除外を使用することによって、NAT をバイパスできます。各方式の詳細については、「NAT 制御をイネーブルにした場合の NAT のバイパス」（p.12-9）を参照してください。このセクションでは、次の内容について説明します。

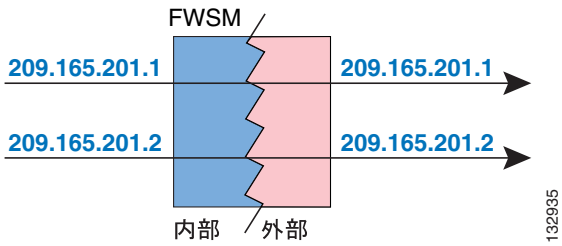
- アイデンティティ NAT の設定（p.12-32）
- スタティック アイデンティティ NAT の設定（p.12-33）
- NAT 除外の設定（p.12-34）

アイデンティティ NAT の設定

アイデンティティ NAT では、実 IP アドレスを同一 IP アドレスに変換します。「変換対象」ホストのみが NAT 変換を作成することができ、応答トラフィックの返信が許可されます。

図 12-23 に、一般的なアイデンティティ NAT の使用例を示します。

図 12-23　アイデンティティ NAT



（注） NAT の設定を変更し、既存の変換がタイムアウトする前に新しい NAT 情報を使用する必要がある場合は、**clear xlate** コマンドを使用して、変換テーブルを消去します。ただし、変換テーブルを消去すると、その変換を使用するすべての接続が切断されます。

アイデンティティ NAT を設定するには、次のコマンドを入力します。

```
hostname(config)# nat (real_interface) 0 real_ip [mask [dns] [outside]
[[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns] [norandomseq]]
```

オプションについては、「ダイナミック NAT または PAT の設定」（p.12-23）を参照してください。

たとえば、内部のネットワーク 10.1.1.0/24 にアイデンティティ NAT を使用する場合、次のコマンドを入力します。

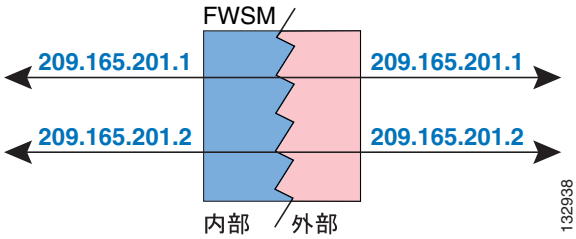
```
hostname(config)# nat (inside) 0 10.1.1.0 255.255.255.0
```

スタティック アイデンティティ NAT の設定

スタティック アイデンティティ NAT では、実 IP アドレスを同一 IP アドレスに変換します。変換は常にアクティブであるため、「変換対象」ホストとリモート ホストの両方で接続を生成できます。スタティック アイデンティティ NAT では、標準 NAT またはポリシー NAT を使用できます。ポリシー NAT の場合は、変換する実アドレスを決定するときに、実アドレスと宛先アドレスを指定します（ポリシー NAT の詳細については、「ポリシー NAT」[p.12-10] を参照）。たとえば、内部アドレスが外部インターフェイスにアクセスし、宛先がサーバ A の場合に、内部アドレスにポリシー スタティック アイデンティティ NAT を使用します。ただし、外部サーバ B にアクセスするときには標準変換を使用します。

図 12-24 に、一般的なスタティック アイデンティティ NAT の使用例を示します。

図 12-24　スタティック アイデンティティ NAT



(注) **static** コマンドを削除しても、その変換を使用する既存の接続は影響を受けません。これらの接続を削除するには、**clear local-host** コマンドを入力します。

変換テーブルから **clear xlate** コマンドでスタティック トランスレーションを消去することはできません。代わりに、**static** コマンドを削除する必要があります。**nat** および **global** コマンドで作成されたダイナミック変換のみ、**clear xlate** コマンドで削除できます。

スタティック アイデンティティ NAT を設定するには、次のいずれかのコマンドを入力します。

- ポリシー スタティック アイデンティティ NAT を設定する場合は、次のコマンドを入力します。

  ```
  hostname(config)# static (real_interface,mapped_interface) real_ip access-list
  acl_id [dns] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns] [norandomseq]
  ```

  access-list コマンドを使用してアクセス リストを作成します（「拡張アクセス リストの追加」[p.10-7] を参照）。このアクセス リストには、**permit** ACE しか含めることができません。アクセス リストの送信元アドレスが、このコマンドの *real_ip* と一致する必要があります。ポリシー NAT では **inactive** または **time-range** キーワードは考慮されず、すべての ACE がポリシー NAT コンフィギュレーションに対してアクティブであるとみなされます。詳細については、「ポリシー NAT」（p.12-10）を参照してください。

  その他のオプションについては、「ダイナミック NAT または PAT の設定」（p.12-23）を参照してください。

- 標準スタティック アイデンティティ NAT を設定する場合、次のコマンドを入力します。

  ```
  hostname(config)# static (real_interface,mapped_interface) real_ip real_ip
  [netmask mask] [dns] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
  [norandomseq]
  ```

  両方の *real_ip* 引数に、同じ IP アドレスを指定します。

  その他のオプションについては、「ダイナミック NAT または PAT の設定」（p.12-23）を参照してください。

次のコマンドでは、外部からアクセスされたときに、スタティック アイデンティティ NAT を内部 IP アドレス（10.1.1.3）に対して使用します。

```
hostname(config)# static (inside,outside) 10.1.1.3 10.1.1.3 netmask 255.255.255.255
```

次のコマンドでは、内部からアクセスされたときに、スタティック アイデンティティ NAT を外部アドレス（209.165.201.15）に対して使用します。

```
hostname(config)# static (outside,inside) 209.165.201.15 209.165.201.15 netmask
255.255.255.255
```

次のコマンドで、サブネット全体をスタティックに対応付けます。

```
hostname(config)# static (inside,dmz) 10.1.2.0 10.1.2.0 netmask 255.255.255.0
```

次のスタティック アイデンティティ ポリシー NAT の例で、ある宛先アドレスにアクセスするときにアイデンティティ NAT を使用し、別の宛先アドレスにアクセスするときには変換を使用する、単一実アドレスを示します。

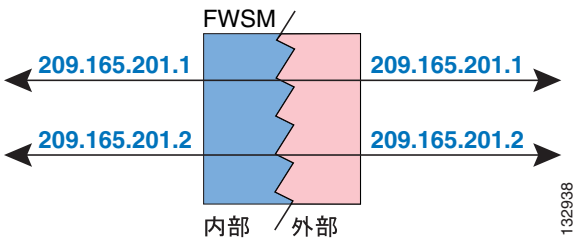
```
hostname(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224
255.255.255.224
hostname(config)# static (inside,outside) 10.1.2.27 access-list NET1
hostname(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

NAT 除外の設定

NAT 除外ではアドレスを変換処理から除外して、実ホストとリモート ホストの両方で接続を開始できるようにします。NAT 除外では、（ポリシー NAT と同様）除外する実トラフィックを決定するときに実アドレスと宛先アドレスを指定できるので、アイデンティティ NAT を使用するよりも NAT 除外を使用する方がきめ細かい制御が行えます。ただし、NAT 除外はポリシー NAT とは異なり、アクセス リストに指定されたポートを考慮しません。アクセス リストのポートを考慮するには、スタティック アイデンティティ NAT を使用します。

図 12-25 に、一般的な NAT 除外の使用例を示します。

図 12-25　NAT 除外



（注）NAT 除外の設定を削除しても、その NAT 除外を使用する既存の接続は影響を受けません。これらの接続を削除するには、**clear local-host** コマンドを入力します。

NAT 除外を設定するには、次のコマンドを入力します。

```
hostname(config)# nat (real_interface) 0 access-list acl_name [outside] [[tcp]
tcp_max_conns [emb_limit]] [udp udp_max_conns] [norandomseq]
```

access-list コマンドを使用してアクセス リストを作成します（「拡張アクセス リストの追加」[p.10-7]を参照）。このアクセス リストには、**permit** ACE と **deny** ACE の両方を含めることができます。アクセス リストで実ポートと宛先ポートを指定しないでください。NAT 除外では、ポートは考慮されません。NAT 除外では **inactive** または **time-range** キーワードも考慮されず、すべての ACE が NAT 除外コンフィギュレーションに対してアクティブであるとみなされます。

その他のオプションについては、「ダイナミック NAT または PAT の設定」（p.12-23）を参照してください。

デフォルトでは、このコマンドは内部から外部へのトラフィックを除外します。外部から内部へのトラフィックに対して NAT をバイパスする場合は、新たに **nat** コマンドを追加して **outside** を入力し、NAT インスタンスを外部 NAT として識別します。外部インターフェイスに対してダイナミック NAT を設定して、他のトラフィックを除外する場合は、外部 NAT 除外を使用できます。

任意の宛先アドレスにアクセスするときに、内部ネットワークを適用除外にする場合は、次のコマンドを入力します。

```
hostname(config)# access-list EXEMPT permit ip 10.1.2.0 255.255.255.0 any
hostname(config)# nat (inside) 0 access-list EXEMPT
```

DMZ ネットワークにダイナミック外部 NAT を使用し、他の DMZ ネットワークを除外するには、次のコマンドを入力します。

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
hostname(config)# access-list EXEMPT permit ip 10.1.3.0 255.255.255.0 any
hostname(config)# nat (dmz) 0 access-list EXEMPT
```

2 つの異なる宛先アドレスにアクセスするときに、内部ネットワークを適用除外にする場合は、次のコマンドを入力します。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 0 access-list NET1
```

NAT の例

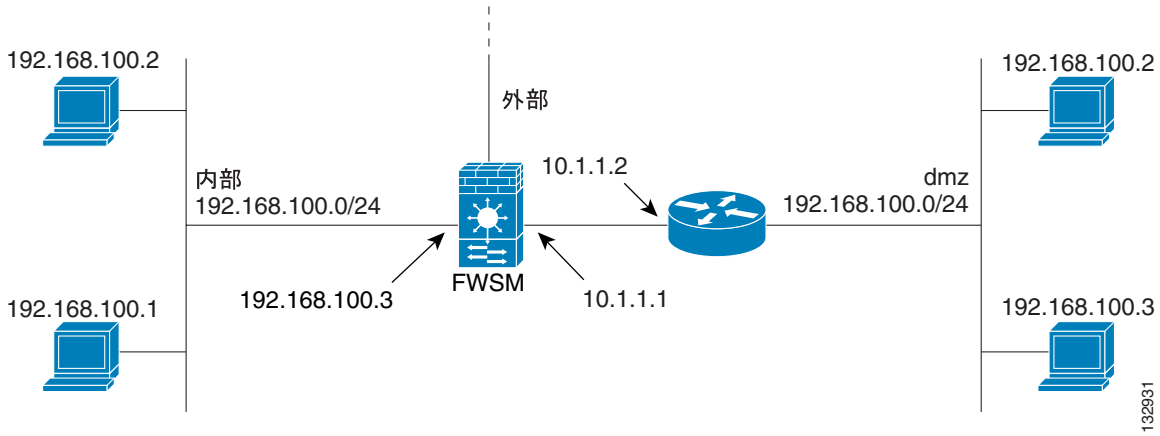
ここでは、一般的な NAT ソリューションの使用例を示します。内容は次のとおりです。

- 重複したネットワーク（p.12-36）
- ポートのリダイレクション（p.12-37）

重複したネットワーク

図 12-26 では、FWSM はアドレス範囲の重複する 2 つのプライベート ネットワークを接続します。

図 12-26　重複したネットワークで外部 NAT を使用する場合



2 つのネットワークで重複するアドレス スペース（192.168.100.0/24）が使用されていますが、各ネットワーク上のホストは（アクセス リストの許可に従って）相互に通信しなければなりません。NAT を使用しない場合、内部ネットワーク上のホストが重複した DMZ ネットワーク上のホストにアクセスしようとしても、パケットは FWSM を通過できません。パケットの宛先アドレスが内部ネットワーク上のアドレスであるとみなされるためです。さらに、内部ネットワーク上の別のホストがその宛先アドレスを使用している場合は、そのホストがパケットを受信します。

この問題を解決するには、NAT を使用して重複しないアドレスを提供します。双方向にアクセスできるようにするには、両方のネットワークにスタティック NAT を使用します。内部インターフェイスから DMZ 上のホストへのアクセスだけを許可する場合は、内部アドレスにダイナミック NAT を使用し、アクセス先の DMZ アドレスにスタティック NAT を使用します。この例は、スタティック NAT を示しています。

この 2 つのインターフェイスにスタティック NAT を設定するための手順は、次のとおりです。DMZ 上のネットワーク 10.1.1.0/24 は変換されません。

ステップ 1　内部から DMZ にアクセスするときに、内部の 192.168.100.0/24 を 10.1.2.0/24 に変換するため、次のコマンドを入力します。

```
hostname(config)# static (inside,dmz) 10.1.2.0 192.168.100.0 netmask 255.255.255.0
```

ステップ 2　DMZ から内部にアクセスするときに、DMZ のネットワーク 192.168.100.0/24 を 10.1.3.0/24 に変換するため、次のコマンドを入力します。

```
hostname(config)# static (dmz,inside) 10.1.3.0 192.168.100.0 netmask 255.255.255.0
```

ステップ 3　FWSM が DMZ ネットワークへのトラフィックを正しくルーティングできるように、次のスタティック ルートを設定します。

```
hostname(config)# route dmz 192.168.100.128 255.255.255.128 10.1.1.2 1
hostname(config)# route dmz 192.168.100.0 255.255.255.128 10.1.1.2 1
```

FWSM にはすでに、内部ネットワーク用に接続されたルートがあります。FWSM はこれらのスタティック ルートを使用して、ネットワーク 192.168.100.0/24 宛てのトラフィックを DMZ インターフェイスから 10.1.1.2 のゲートウェイ ルータに送信します（接続されたルートとまったく同じネットワークを指定してスタティック ルートを作成することはできないので、ネットワークを 2 つに分割する必要があります）。または、DMZ トラフィックにデフォルト ルートなど、より一般的なルートを使用することもできます。

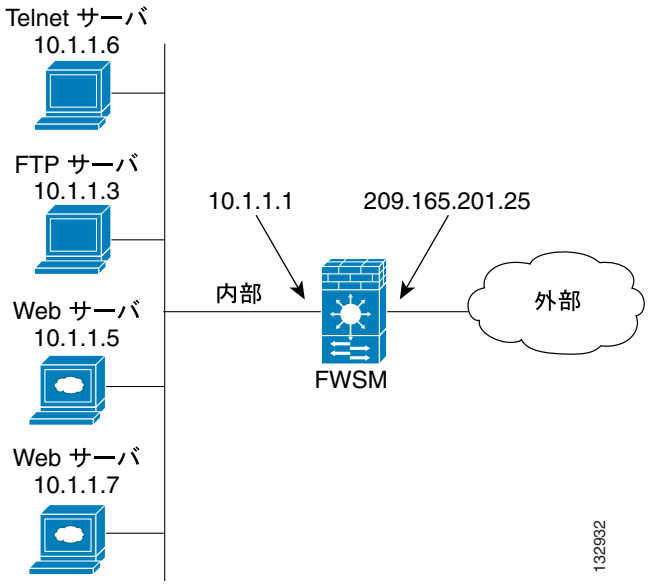
DMZ ネットワーク上のホスト 192.168.100.2 が内部ネットワーク上のホスト 192.168.100.2 への接続を開始しようとすると、次のイベントが発生します。

1. DMZ ホスト 192.168.100.2 が IP アドレス 10.1.2.2 にパケットを送信します。
2. FWSM がこのパケットを受信すると、送信元アドレスが 192.168.100.2 から 10.1.3.2 に変換されます。
3. その後、宛先アドレスが 10.1.2.2 から 192.168.100.2 に変換されたあとで、パケットが転送されます。

ポートのリダイレクション

図 12-27 に、ポートのリダイレクション機能が役立つ一般的なネットワーク例を示します。

図 12-27　スタティック PAT を使用するポートのリダイレクション



ここで説明する設定では、外部ネットワーク上のホストに対してポート リダイレクションが次のように実行されます。

- IP アドレス 209.165.201.5 に対する Telnet 要求は、10.1.1.6 にリダイレクトされます。
- IP アドレス 209.165.201.5 に対する FTP 要求は、10.1.1.3 にリダイレクトされます。
- FWSM の外部 IP アドレス 209.165.201.5 に対する HTTP 要求は、10.1.1.5 にリダイレクトされます。
- PAT アドレス 209.165.201.15 に対する HTTP ポート 8080 要求は、10.1.1.7 のポート 80 にリダイレクトされます。

この実装を行うための設定手順は、次のとおりです。

ステップ 1　内部ネットワークに PAT を設定するため、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 0.0.0.0 0.0.0.0 0 0
hostname(config)# global (outside) 1 209.165.201.15
```

ステップ 2　209.165.201.5 への Telnet 要求を 10.1.1.6 にリダイレクトするため、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 209.165.201.5 telnet 10.1.1.6 telnet
netmask 255.255.255.255
```

ステップ 3　IP アドレス 209.165.201.5 への FTP 要求を 10.1.1.3 にリダイレクトするため、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 209.165.201.5 ftp 10.1.1.3 ftp netmask
255.255.255.255
```

ステップ 4　FWSM の外部インターフェイス アドレスへの HTTP 要求を 10.1.1.5 にリダイレクトするため、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp interface www 10.1.1.5 www netmask
255.255.255.255
```

ステップ 5　PAT アドレス 209.165.201.15 へのポート 8080 の HTTP 要求を 10.1.1.7 のポート 80 にリダイレクトするため、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 209.165.201.15 8080 10.1.1.7 www netmask
255.255.255.255
```

フェールオーバーの設定

この章では、FWSM のフェールオーバー機能について説明します。2 つの FWSM を設定することで、1 つに障害が発生しても、もう 1 つに操作を引き継がせることができます。フェールオーバー機能はルーテッド ファイアウォール モードと透過ファイアウォール モードの両方で使用でき、コンテキスト モードはシングルでもマルチでもかまいません。

この章で説明する内容は、次のとおりです。

- フェールオーバーの概要（p.13-2）
- フェールオーバーの設定（p.13-21）
- フェールオーバーの制御とモニタ（p.13-42）

フェールオーバーの設定例については、「フェールオーバーの設定例」（p.B-20）を参照してください。

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 FWSM が必要です。アクティブ インターフェイスと装置がヘルス モニタされ、特定のフェールオーバー条件に合致するかどうかが判断されます。これらの条件に合致すると、フェールオーバーが発生します。

FWSM では、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設定がサポートされます。各フェールオーバー設定には、フェールオーバーを決定および実行するための独自の方法があります。

アクティブ / アクティブ フェールオーバーでは、両方の装置がネットワーク トラフィックを転送することができます。従って、負荷分散をネットワーク上で設定できます。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 モードで動作する装置でのみ使用できます。

アクティブ / スタンバイ フェールオーバーでは、1 つの装置のみがトラフィックを転送し、もう 1 つの装置はスタンバイ状態で待機します。アクティブ / スタンバイ フェールオーバーは、シングル コンテキスト モードまたはマルチコンテキスト モードのいずれでも使用できます。

いずれのフェールオーバー設定も、ステートフルまたはステートレス（標準）フェールオーバーをサポートします。

ここでは、次の内容について説明します。

- フェールオーバーのシステム要件（p.13-2）
- フェールオーバー リンクとステート リンク（p.13-3）
- シャーシ内およびシャーシ間のモジュール配置（p.13-4）
- 透過ファイアウォールの要件（p.13-8）
- アクティブ/スタンバイ フェールオーバーとアクティブ/アクティブ フェールオーバー（p.13-9）
- 標準フェールオーバーとステートフル フェールオーバー（p.13-17）
- フェールオーバーのヘルス モニタ（p.13-18）

フェールオーバーのシステム要件

ここでは、FWSM のフェールオーバー設定のソフトウェア要件とライセンス要件について説明します。内容は次のとおりです。

- ソフトウェア要件（p.13-2）
- ライセンス要件（p.13-2）

ソフトウェア要件

フェールオーバー設定をした 2 つの装置は、同じメジャー（最初の番号）ソフトウェア バージョンおよびマイナー（2 番めの番号）ソフトウェア バージョンを持つ必要があります。ただし、アップグレード プロセス中は異なるソフトウェア バージョンを使用できます。たとえば、ある装置を Version 3.1(1) から Version 3.1(2) にアップグレードして、フェールオーバーをアクティブのままにすることができます。長期的な互換性を確保するために、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推奨します。

ライセンス要件

両装置とも同じライセンスを持つ必要があります。

フェールオーバー リンクとステート リンク

ここでは、フェールオーバー設定での 2 つの装置間の専用接続である、フェールオーバー リンクとステート リンクについて説明します。内容は次のとおりです。

- フェールオーバー リンク（p.13-3）
- ステート リンク（p.13-4）

フェールオーバー リンク

フェールオーバー ペアの 2 つの装置はフェールオーバー リンク経由で常時通信を行い、それぞれの装置の動作ステータスを把握します。フェールオーバー リンク経由で通信する情報は次のとおりです。

- 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 ステータス
- MAC アドレス交換
- 設定の複製と同期化

注意　フェールオーバー　キーで通信をセキュリティ保護している場合を除き、フェールオーバーおよびステートフル フェールオーバー リンク間の情報はすべてクリア テキストで送信されます。

フェールオーバー リンクでは、標準のネットワーキング インターフェイスとしては設定しない、フェールオーバー通信専用の特別な VLAN インターフェイスを使用します。この VLAN は、フェールオーバー リンク（および任意で使用するステート リンク）だけに使用する必要があります。フェールオーバー リンク VLAN を他の VLAN と共有すると、断続的なトラフィック障害や ping エラーおよび ARP エラーが発生することがあります。シャーシ間のフェールオーバーでは、フェールオーバー リンク用としてスイッチ上の専用インターフェイスを使用します。

マルチコンテキスト モードで動作するシステムでは、システム コンテキストにフェールオーバー リンクが常時設定されます。このインターフェイス（および使用する場合はステート リンク）は、システム コンテキストで設定可能な唯一のインターフェイスです。他のすべてのインターフェイスは、セキュリティ コンテキスト内で割り当てられ、設定されます。

（注）　フェールオーバー リンク用の IP アドレスおよび MAC アドレスは、フェールオーバー実行後も変更されません。

ステート リンク

ステートフル フェールオーバーを使用するには、すべてのステート情報を渡すためのステート リンクを設定する必要があります。このリンクはフェールオーバー リンクと同じでもかまいませんが、ステート リンク用に別の VLAN および IP アドレスを割り当てることを推奨します。ステート トラフィックはサイズが大きいことがあるので、別のリンクを使用した方がパフォーマンスは向上します。

ステート リンク インターフェイスは標準ネットワーキング インターフェイスとしては設定されず、ステートフル フェールオーバー通信のためにのみ使用されます。ステート リンクとフェールオーバー リンクを共有する場合は、任意でフェールオーバー通信にも使用されます。

マルチコンテキスト モードでは、システム コンテキストにステート リンクが常時設定されます。システム コンテキストのインターフェイスは、このインターフェイスとフェールオーバー インターフェイスだけです。他のすべてのインターフェイスは、セキュリティ コンテキスト内で割り当てられ、設定されます。

(注) ステート リンク用の IP アドレスおよび MAC アドレスは、フェールオーバー実行後も変更されません。

注意 フェールオーバー キーで通信をセキュリティ保護している場合を除き、フェールオーバーおよびステートフル フェールオーバー リンク間の情報はすべてクリア テキストで送信されます。

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 FWSM 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.13-4）
- シャーシ間フェールオーバー（p.13-5）

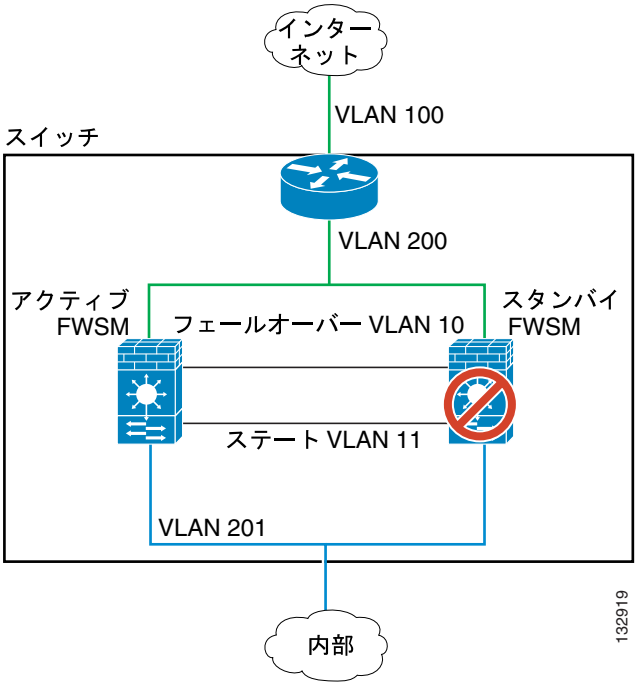
シャーシ内フェールオーバー

セカンダリ FWSM をプライマリ FWSM 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する必要があります。モジュール レベルの障害のほか、スイッチ レベルの障害を保護するには、「シャーシ間フェールオーバー」（p.13-5）を参照してください。

両方の FWSM 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 13-1 に、一般的なスイッチ間の構成を示します。

図 13-1　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 FWSM を別のスイッチに搭載することができます。FWSM は直接スイッチとフェールオーバーを調整するのではなく、スイッチと協調してフェールオーバー操作を行います。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。

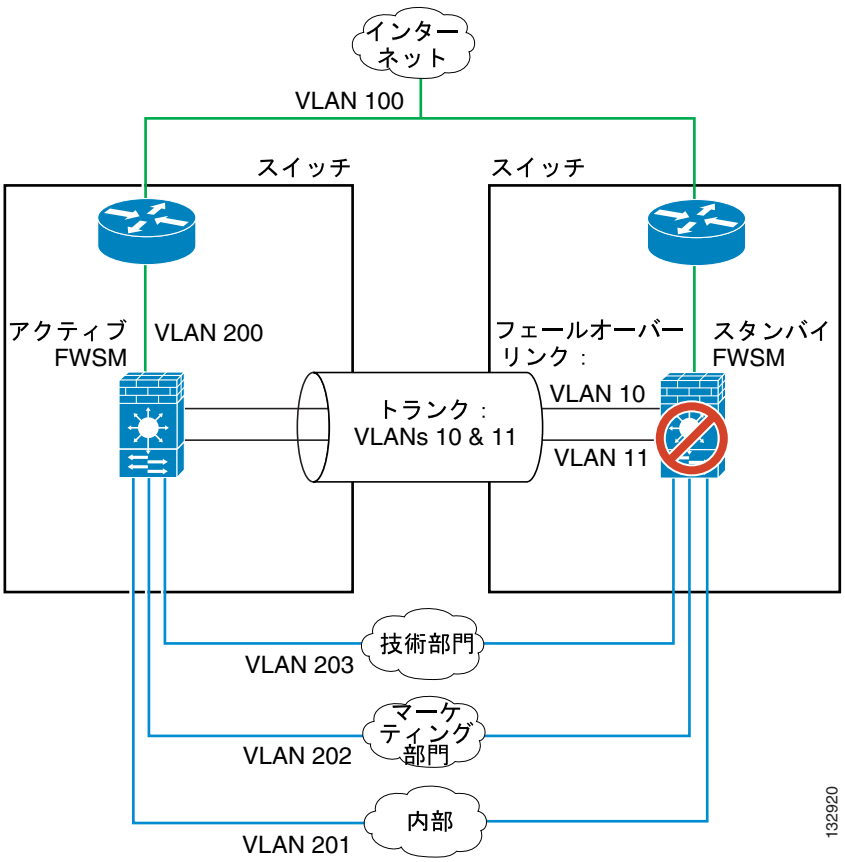
FWSM 間でフェールオーバー通信を行うには、2 台のスイッチ間に、フェールオーバーおよびステート VLAN を伝送するトランク ポートを設定することを推奨します。トランクにより、2 つの装置間のフェールオーバー通信の障害リスクは最小限に抑えられます。

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 13-2 に、スイッチと FWSM 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 FWSM VLAN（VLAN 10 と 11）を転送します。

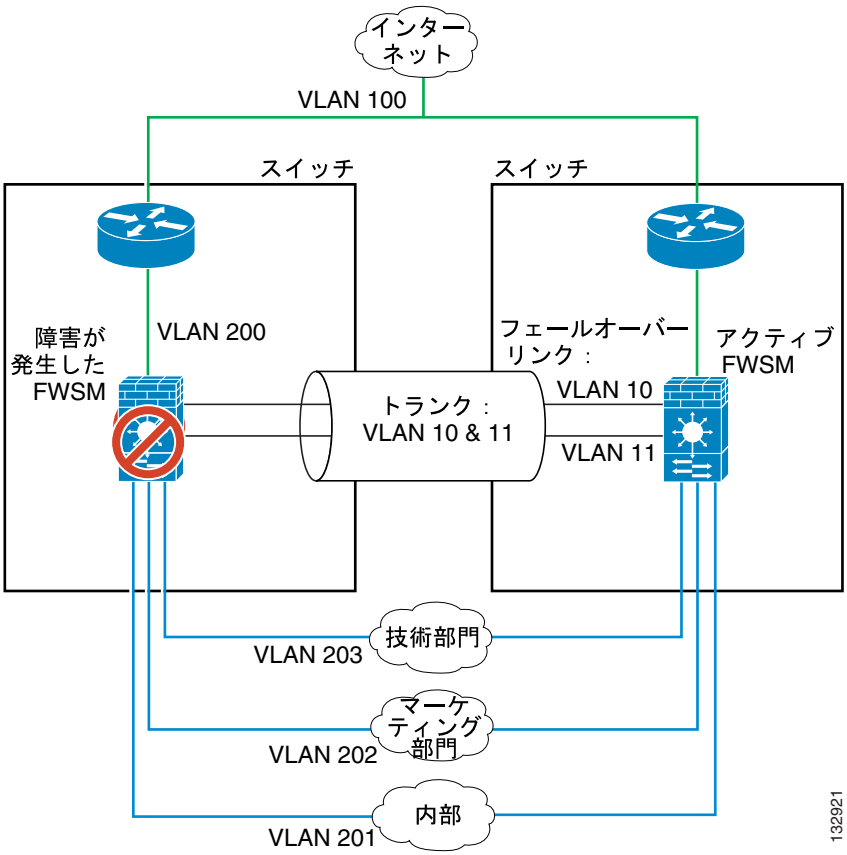
（注） FWSM のフェールオーバーはスイッチのフェールオーバーに依存しない独立した機能ですが、スイッチのフェールオーバーが発生した場合には、FWSM もそれに対応します。

図 13-2　標準操作



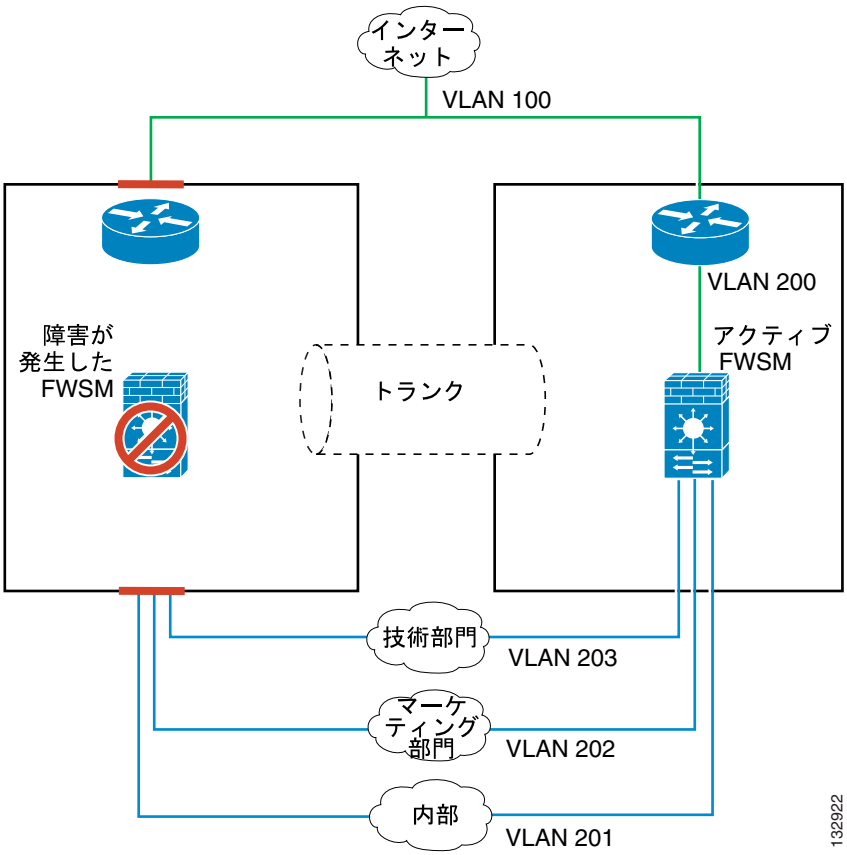
プライマリ FWSM に障害が発生すると、セカンダリ FWSM がアクティブになってファイアウォール VLAN を通過します（図 13-3）。

図 13-3　FWSM の障害



スイッチ全体に障害が発生し、FWSM にも障害が発生した場合（電源切断など）には、スイッチと FWSM 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 13-4）。

図 13-4　スイッチの障害



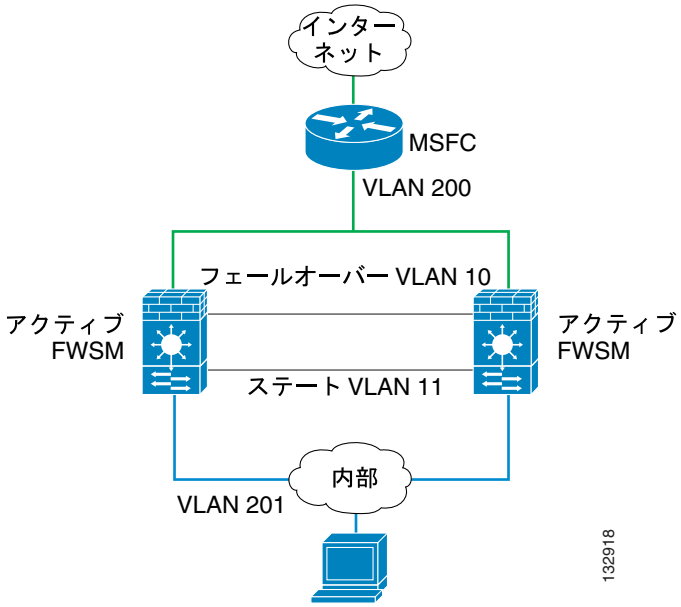
透過ファイアウォールの要件

透過モードでフェールオーバー機能を使用しているときにループを回避するには、BPDU の送信をサポートするスイッチ ソフトウェアを使用し、BPDU が許可されるように FWSM を設定する必要があります。BPDU が自動的に許可されるスイッチ ソフトウェアのバージョンについては、「スイッチ ハードウェアおよびソフトウェアの互換性」（p.A-2）を参照してください。

FWSM 経由の BPDU を許可するには、EtherType ACL を設定して、「EtherType アクセス リストの追加」（p.10-10）の説明のとおりに、両方のインターフェイスに適用します。

両モジュールが相手の存在を検出したり、フェールオーバー リンクが不正であったりするなど、両方のモジュールが同時にアクティブのときに、ループが発生することがあります。両方の FWSM 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 FWSM によって無限に複製され、ループが発生します（図 13-5 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 13-5　透過モード時の潜在的なループ



アクティブ / スタンバイ フェールオーバーとアクティブ / アクティブ フェールオーバー

ここでは、各フェールオーバーの設定について詳しく説明します。内容は次のとおりです。

- アクティブ / スタンバイ フェールオーバー（p.13-9）
- アクティブ / アクティブ フェールオーバー（p.13-13）
- 使用するフェールオーバー タイプの決定（p.13-17）

アクティブ / スタンバイ フェールオーバー

ここでは、アクティブ / スタンバイ フェールオーバーを設定する手順について説明します。内容は次のとおりです。

- アクティブ / スタンバイ フェールオーバーの概要（p.13-9）
- プライマリ / セカンダリ ステータスとアクティブ / スタンバイ ステータス（p.13-10）
- デバイスの初期化と設定の同期化（p.13-10）
- コマンドの複製（p.13-11）
- フェールオーバーのトリガー（p.13-11）
- フェールオーバーの動作（p.13-12）

アクティブ / スタンバイ フェールオーバーの概要

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 FWSM に引き継ぐことができます。アクティブ ユニットに障害が発生すると、その装置はスタンバイ ステートに移行し、逆にスタンバイ ユニットがアクティブ ステートに移行します。アクティブになった装置は障害が発生した装置の IP アドレス（透過ファイアウォールの場合は管理 IP アドレス）と MAC アドレスを推定して、トラフィックの転送を開始します。スタンバイ ステートに移行した装置は、スタンバイ IP アドレス /MAC アドレスを引き継ぎます。ネットワーク デバイスは MAC/IP アドレスのペアの変更を知らないため、ネットワーク上で ARP エントリの変更やタイムアウトは発生しません。

（注）マルチコンテキスト モードでは、FWSM は装置全体（すべてのコンテキストを含む）のフェールオーバーを行いますが、各コンテキストを個別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 ステータスとアクティブ / スタンバイ ステータス

フェールオーバーの 2 台の装置の主要な違いは、一方がアクティブで一方がスタンバイであること、すなわち、どちらの IP アドレスを使用し、どちらの装置がアクティブにトラフィックを転送するか、ということです。

ただし、プライマリ（設定に指定されている）かセカンダリかによって、両装置に多少の違いがあります。

- 両方の装置を同時に起動した場合、（動作状態が同じであれば）プライマリ ユニットが常にアクティブになります。
- プライマリ ユニットの MAC アドレスは常にアクティブ IP アドレスと組み合わされます。例外が発生するのは、セカンダリ ユニットがアクティブになり、フェールオーバー リンクでプライマリ MAC アドレスを取得できない場合です。この場合、セカンダリ モジュールの MAC アドレスが使用されます。

デバイスの初期化と設定の同期化

設定の同期化は、フェールオーバー ペアの一方または両方のデバイスが起動するときに行われます。設定は常に、アクティブ ユニットからスタンバイ ユニットに同期されます。スタンバイ ユニットの初期起動が完了すると、実行コンフィギュレーションが消去され（アクティブ ユニット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 ユニットはスタンバイ ユニットに設定全体を送信します。

アクティブ ユニットは次のように決定されます。

- 装置の起動時にすでにアクティブに実行しているピアが検出された場合、この装置がスタンバイ ユニットになります。
- 装置の起動時にピアが検出されなかった場合、この装置がアクティブ ユニットになります。
- 両方の装置を同時に起動する場合、プライマリ ユニットがアクティブ ユニットになり、セカンダリ ユニットがスタンバイ ユニットになります。

（注）セカンダリ ユニットの起動時にプライマリ ユニットが検出されなかった場合、セカンダリ ユニットがアクティブ ユニットになります。セカンダリ ユニットは、アクティブ IP アドレスに独自の MAC アドレスを使用します。ただし、プライマリ ユニットが使用可能になると、セカンダリ ユニットは MAC アドレスをプライマリ ユニットの MAC アドレスに変更します。これにより、ネットワーク トラフィックが一時停止することがあります。

設定の同期化が開始されると、アクティブ ユニットの FWSM コンソールで「Beginning configuration replication: Sending to mate」というメッセージが表示され、同期化が終了すると「End Configuration Replication to mate」というメッセージが表示されます。設定の同期化の間、アクティブ ユニットに入力されたコマンドがスタンバイ ユニットに正しく複製されず、スタンバイ ユニットに入力されたコマンドがアクティブ ユニットから複製された設定によって上書きされることがあります。設定の複製プロセス中に、フェールオーバー ペアの各装置にコマンドを入力することは避けてください。設定の大きさによっては、複製に数秒から数分かかることがあります。

アクティブ ユニットに **write standby** コマンドを入力すると、スタンバイ ユニットの実行コンフィギュレーションが消去され（アクティブ ユニット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 ユニットはスタンバイ ユニットに設定全体を送信します。

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。1 つのコンテキスト内で **write standby** コマンドを入力すると、そのコンテキストの設定だけが複製されます。

スタンバイ ユニットでは、複製された設定は実行メモリにのみ保存されます。同期後の設定をフラッシュ メモリに保存する手順は、次のとおりです。

- シングルコンテキスト モードで、アクティブ ユニットに **write memory** コマンドを入力します。コマンドがスタンバイ ユニットに複製され、設定がフラッシュ メモリに書き込まれます。
- マルチコンテキスト モードで、システム実行スペースからアクティブ ユニットに **write memory all** コマンドを入力します。このコマンドにより、システム コンフィギュレーションとすべてのコンテキスト コンフィギュレーションが保存されます。コマンドがスタンバイ ユニットに複製され、設定がフラッシュ メモリに書き込まれます。外部サーバ上にスタートアップ コンフィギュレーションのあるコンテキストには、ネットワーク経由でどちらの装置からでもアクセスできるので、各装置に個別に保存する必要はありません。または、アクティブ ユニットから外部サーバにディスク上のコンテキストをコピーし、さらにスタンバイ ユニット上のディスクにコピーすることもできます。これらは装置をリロードしたときに使用可能になります。

コマンドの複製

アクティブ ユニット上に入力されたコマンドは、フェールオーバー リンクを経由してスタンバイ ユニットに送信されます。コマンドの複製は、常にアクティブ ユニットからスタンバイ ユニットへと行われます。複製されたコマンドは、スタンバイ ユニットの実行コンフィギュレーションに保存されます。実行コンフィギュレーションをアクティブ ユニットのスタートアップ コンフィギュレーションに保存すると、実行コンフィギュレーションがスタンバイ ユニットのスタートアップ コンフィギュレーションに保存されます。ただし、コマンドを複製するために、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。

（注）　**mode** コマンドはセカンダリ ユニットには複製されません。

スタンバイ ユニット上での変更は、アクティブ ユニットには複製されません。スタンバイ ユニット上でコマンドを入力すると、FWSM に、「`**** WARNING **** Configuration Replication is NOT performed from Standby module to Active module. Configurations are no longer synchronized.`」（警告：スタンバイ ユニットからアクティブ ユニットへの設定の複製は実行できません。設定は同期化されません）というメッセージが表示されます。このメッセージは、設定に影響しないコマンドを多数入力した場合にも表示されます。

フェールオーバーのトリガー

装置の障害は、次のいずれかの状況で発生します。

- 装置にハードウェア障害または電源障害が発生した場合
- 装置にソフトウェア障害が発生した場合
- モニタ対象のインターフェイスの多くで障害が発生した場合
- アクティブ ユニット上に **no failover active** コマンドが入力された場合、またはスタンバイ ユニット上に **failover active** コマンドが入力された場合

フェールオーバーの動作

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単位で発生します。マルチコンテキスト モードで実行されているシステムであっても、アクティブ / スタンバイ フェールオーバーでは、個別のコンテキストまたはコンテキスト グループのフェールオーバーを行うことはできません。

表 13-1 に、各障害イベントのフェールオーバーの動作を示します。各障害イベントについて、フェールオーバー ポリシー（フェールオーバーあり / フェールオーバーなし）、アクティブ ユニットにより実行される動作、スタンバイ ユニットにより実行される動作、フェールオーバー状態および動作に関するコメントを示します。

表 13-1　フェールオーバーの動作

障害イベント	ポリシー	アクティブ ユニットの動作	スタンバイ ユニットの動作	説明
アクティブ ユニットの障害（電源またはハードウェア）	フェールオーバー	適用外	アクティブになる アクティブ ユニットを障害装置としてマークする	モニタ対象インターフェイスまたはフェールオーバー リンク上で、hello メッセージが受信されません。
以前のアクティブ ユニットの回復	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 ユニットの障害（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 ユニットを障害装置としてマークする	適用外	スタンバイ ユニットが障害装置してマークされた場合、インターフェイスの障害数がスレッシュホールドを超過しても、アクティブ ユニットはフェールオーバーを試行しません。
運用中のフェールオーバー リンクの障害	フェールオーバーなし	フェールオーバー インターフェイスを障害としてマークする	フェールオーバー インターフェイスを障害としてマークする	フェールオーバー リンクがダウンしていると、スタンバイ ユニットへのフェールオーバーを実行できないので、フェールオーバー リンクをできるだけ早く回復させる必要があります。
起動時のフェールオーバー リンクの障害	フェールオーバーなし	フェールオーバー インターフェイスを障害としてマークする	アクティブになる	起動時にフェールオーバー リンクがダウンした場合、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	ステート情報が更新されず、フェールオーバーが発生するとセッションは終了します。
アクティブ ユニットのインターフェイス障害がスレッシュホールドを超過	フェールオーバー	アクティブ ユニットを障害装置としてマークする	アクティブになる	なし
スタンバイ ユニットのインターフェイス障害がスレッシュホールドを超過	フェールオーバーなし	動作なし	スタンバイ ユニットを障害装置としてマークする	スタンバイ ユニットが障害装置としてマークされた場合、インターフェイスの障害数がスレッシュホールドを超過しても、アクティブ ユニットはフェールオーバーを試行しません。

アクティブ / アクティブ フェールオーバー

ここでは、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。内容は次のとおりです。

- アクティブ / アクティブ フェールオーバーの概要（p.13-13）
- プライマリ / セカンダリ ステータスとアクティブ / スタンバイ ステータス（p.13-13）
- デバイスの初期化と設定の同期化（p.13-14）
- コマンドの複製（p.13-14）
- フェールオーバーのトリガー（p.13-15）
- フェールオーバーの動作（p.13-16）

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 フェールオーバーは、FWSM のマルチコンテキスト モードでのみ使用できます。アクティブ / アクティブ フェールオーバーの設定では、両方の FWSM がネットワーク トラフィックを転送できます。

アクティブ / アクティブ フェールオーバーでは、FWSM のセキュリティ コンテキストを *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です。FWSM に最大 2 つのフェールオーバー グループを作成できます。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、デフォルトでは、割り当てられていないセキュリティ コンテキストもすべてフェールオーバー グループ 1 のメンバーです。

フェールオーバー グループは、アクティブ / アクティブ フェールオーバーでのフェールオーバーの基本単位となります。インターフェイス障害モニタリング、フェールオーバー、アクティブ / スタンバイ ステータスはすべて、装置ではなくフェールオーバー グループの属性です。プライマリ ユニットの MAC アドレスは、アクティブ コンテキストのすべてのインターフェイスで使用されます。

アクティブ フェールオーバー グループに障害が発生すると、スタンバイ ステートに移行し、関連するスタンバイ フェールオーバー グループがアクティブになります。アクティブになったフェールオーバー グループのインターフェイスは、障害が発生したフェールオーバー グループのインターフェイスの MAC アドレスと IP アドレスを推定します。スタンバイ ステートに移行したフェールオーバー グループのインターフェイスは、スタンバイ フェールオーバー グループの MAC アドレスと IP アドレスを引き継ぎます。

（注） 装置上のフェールオーバー　グループの障害は、その装置に障害が発生していることを意味するものではありません。装置には、トラフィックを転送する別のフェールオーバー グループが存在する可能性があります。

フェールオーバー グループを作成する場合、アクティブ ステートのフェールオーバー グループ 1 を持つ装置上に作成する必要があります。

プライマリ / セカンダリ ステータスとアクティブ / スタンバイ ステータス

アクティブ / スタンバイ フェールオーバーと同様、アクティブ / アクティブ フェールオーバー ペアの 1 つの装置がプライマリ ユニットに指定され、もう 1 つの装置がセカンダリ ユニットに指定されます。アクティブ / スタンバイ フェールオーバーとは異なり、両方の装置を同時に起動したときにアクティブになる装置は決まっていません。代わりに、プライマリ / セカンダリの指定で、ペアに実行コンフィギュレーションを提供する装置、および両方の装置を同時に起動したときにフェールオーバー グループがアクティブ ステートとして表示される装置が決まります。

設定内の各フェールオーバー グループには、プライマリ ユニットまたはセカンダリ ユニットのプリファレンスが指定されます。このプリファレンスにより、両方の装置を同時に起動したときに、フェールオーバー グループのコンテキストがアクティブ ステートになるフェールオーバー ペアの装置が決まります。ペアの 1 つの装置上で両方のフェールオーバー グループをアクティブ ステートにして、もう 1 つの装置にスタンバイ ステートのフェールオーバー グループを含めることもできます。ただし、一般的な設定では、各フェールオーバー グループに別々のロール プリファレンスに割り当てて、それぞれを別の装置上でアクティブにし、デバイス間のトラフィックを分散させています。

（注） FWSM では負荷分散サービスは提供されていません。負荷分散は、FWSM にトラフィックを転送するルータで処理する必要があります。

デバイスの初期化と設定の同期化

設定の同期化は、フェールオーバー ペアの一方または両方の装置が起動するときに行われます。

ピア装置が使用できない間、装置を起動すると、フェールオーバー グループおよび装置のプライマリ / セカンダリ指定に関係なく、両方のフェールオーバー グループがその装置上でアクティブになります。設定の同期化は行われません。ピア装置が使用できない理由として、ピア装置の電源が切られている、ピア装置が障害ステートにある、装置間のフェールオーバー リンクが確立されていない、などがあります。

ピア装置がアクティブの間、（両方のフェールオーバー グループをアクティブにして）装置を起動すると、起動している装置はアクティブ ユニットに接続して実行コンフィギュレーションを取得します。デフォルトでは、各フェールオーバー グループおよび装置のプライマリ / セカンダリ指定に関係なく、フェールオーバー グループはアクティブ ユニット上でアクティブのままです（**preempt** コマンドで設定されていないかぎり）。次のいずれかが発生するまで、フェールオーバー グループは最初の装置上でアクティブのままになります。

- フェールオーバー状態により、フェールオーバー　グループがピア装置上でアクティブになった。
- **no failover active** コマンドを使用して、フェールオーバー グループをピア装置上で強制的に手動でアクティブにした。
- フェールオーバー グループの優先装置が使用可能になったときに、**preempt** コマンドにより、その装置上でフェールオーバー グループを強制的にアクティブにした。

両方の装置を同時に起動すると、プライマリ ユニットがアクティブ ユニットになります。セカンダリ ユニットは、プライマリ ユニットから実行コンフィギュレーションを取得します。設定が同期されると、各フェールオーバー グループはその優先装置上でアクティブになります。

コマンドの複製

両方の装置が実行されたあと、一方の装置からもう一方の装置に、次のようにコマンドが複製されます。

- セキュリティ コンテキスト内で入力されたコマンドは、セキュリティ コンテキストがアクティブ ステートに表示される装置からピア装置に複製されます。

（注） 所属するフェールオーバー グループが装置上でアクティブ ステートであれば、コンテキストはその装置上でアクティブ ステートとみなされます。

- システム実行スペースで入力されたコマンドは、フェールオーバー グループ 1 がアクティブ ステートの装置からフェールオーバー グループ 1 がスタンバイ ステートの装置に複製されます。
- 管理コンテキストで入力されたコマンドは、フェールオーバー グループ 1 がアクティブ ステートの装置からフェールオーバー グループ 1 がスタンバイ ステートの装置に複製されます。

コマンドを適切な装置に入力せず、コマンドの複製が失敗した場合、設定は同期されません。次回、設定の同期化を行なったときに、それらの変更内容が失われる可能性があります。

（注） **mode** コマンドは複製されません。

write standby コマンドを使用して、同期されなかった設定を再度同期化することができます。アクティブ / アクティブ フェールオーバーの場合、**write standby** コマンドは次のように動作します。

- **write standby** コマンドをシステム実行スペースに入力すると、FWSM のシステム コンフィギュレーションおよびすべてのセキュリティ コンテキストの設定がピア装置に書き込まれます。これには、スタンバイ ステートのセキュリティ コンテキストの設定情報も含まれます。コマンドは、フェールオーバー グループ 1 がアクティブ ステートになっている装置のシステム実行スペースに入力する必要があります。
- **write standby** コマンドをセキュリティ コンテキストに入力すると、そのセキュリティ コンテキストの設定だけがピア装置に書き込まれます。コマンドは、セキュリティ コンテキストがアクティブ ステートに表示される装置上のセキュリティ コンテキストに入力する必要があります。

ピア装置への複製の場合、複製されたコマンドはフラッシュ メモリには保存されず、実行コンフィギュレーションに追加されます。複製されたコマンドを両方の装置のフラッシュ メモリに保存するには、変更を加えた装置上で **write memory** コマンドまたは **copy running-config startup-config** コマンドを使用します。コマンドがピア装置に複製され、設定がそのピア装置上のフラッシュ メモリに保存されます。

フェールオーバーのトリガー

アクティブ / アクティブ フェールオーバーでは、次のいずれかのイベントが発生した場合、装置レベルでフェールオーバーをトリガーできます。

- 装置にハードウェア障害が発生した場合
- 装置に電源障害が発生した場合
- 装置にソフトウェア障害が発生した場合
- システム実行スペースに **no failover active** コマンドまたは **failover active** コマンドが入力された場合

次のいずれかのイベントが発生した場合、フェールオーバー グループ レベルでフェールオーバーがトリガーされます。

- フェールオーバー グループに属するコンテキストの、非常に多くのモニタ対象インターフェイスで障害が発生した場合
- **no failover active group** *group_id* コマンドが入力された場合

フェールオーバー グループに障害が発生する前に、障害が発生する必要のあるフェールオーバー グループ内のインターフェイスの数または割合を指定して、各フェールオーバー グループのフェールオーバー スレッシュホールドを設定します。フェールオーバー グループにはマルチコンテキストを含めることが可能で、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可能であるため、シングルコンテキストのすべてのインターフェイスに障害が発生しても、関連するフェールオーバー グループには障害を発生させません。

インターフェイスおよび装置のモニタリングの詳細については、「フェールオーバーのヘルス モニタ」（p.13-18）を参照してください。

フェールオーバーの動作

アクティブ / アクティブ フェールオーバーの設定では、フェールオーバーはシステム単位ではなくフェールオーバー グループ単位で発生します。たとえば、両方のフェールオーバー グループをプライマリ ユニット上でアクティブに指定すると、フェールオーバー グループ 1 に障害が発生した場合、フェールオーバー グループ 2 はプライマリ ユニット上でアクティブのままになります。他方、フェールオーバー グループ 1 はセカンダリ ユニット上でアクティブになります。

（注） アクティブ / アクティブ フェールオーバーを設定する場合、両方の装置の合計トラフィックが各装置の容量内に収まるようにしてください。

表 13-2 に、各障害イベントのフェールオーバーの動作を示します。各障害イベントについて、ポリシー（フェールオーバーが発生するかどうか）、アクティブ フェールオーバー グループの動作、スタンバイ フェールオーバー グループの動作を示します。

表 13-2　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動作

障害イベント	ポリシー	アクティブ グループの動作	スタンバイ グループの動作	説明
装置に電源障害またはソフトウェア障害が発生	フェールオーバー	スタンバイ ユニットを障害装置としてマークする	アクティブになる アクティブ ユニットを障害装置としてマークする	フェールオーバー ペア内の装置に障害が発生すると、その装置上のすべてのアクティブ フェールオーバー グループが障害フェールオーバー グループとしてマークされ、ピア装置上でアクティブになります。
アクティブ フェールオーバー グループのインターフェイス障害がスレッシュホールドを超過	フェールオーバー	アクティブ グループを障害グループとしてマークする	アクティブになる	なし
スタンバイ フェールオーバー グループのインターフェイス障害がスレッシュホールドを超過	フェールオーバーなし	動作なし	スタンバイ グループを障害グループとしてマークする	スタンバイ フェールオーバー グループが障害フェールオーバー グループとしてマークされた場合、インターフェイスの障害数がスレッシュホールドを超過しても、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試行しません。
以前のアクティブ フェールオーバー グループの回復	フェールオーバーなし	動作なし	動作なし	**preempt** コマンドで設定された場合を除き、フェールオーバー グループは現在の装置上でアクティブのままになります。
起動時のフェールオーバー リンクの障害	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	起動時にフェールオーバー リンクがダウンした場合、両方の装置上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。

表 13-2　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動作（続き）

障害イベント	ポリシー	アクティブ グループの動作	スタンバイ グループの動作	説明
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	ステート情報が更新されず、フェールオーバーが発生するとセッションは終了します。
運用中のフェールオーバーリンクの障害	フェールオーバーなし	適用外	適用外	各装置はフェールオーバー インターフェイスを障害としてマークします。フェールオーバー リンクがダウンしていると、スタンバイ ユニットへのフェールオーバーを実行できないので、フェールオーバーリンクはできるだけ早く回復させる必要があります。

使用するフェールオーバー タイプの決定

選択するフェールオーバー タイプは、FWSM の設定および FWSM の使用方法によって異なります。

FWSM をシングルモードで実行している場合、アクティブ / スタンバイ フェールオーバーのみ使用可能です。アクティブ / アクティブ フェールオーバーは、FWSM をマルチコンテキスト モードで実行している場合のみ使用できます。FWSM をマルチコンテキスト モードで実行している場合、アクティブ / アクティブ フェールオーバーまたはアクティブ / スタンバイ フェールオーバーのいずれの設定も可能です。

アップストリーム ルータを使用して負荷分散を行っている場合は、アクティブ / アクティブ フェールオーバーを使用します。負荷分散を行わない場合は、アクティブ / アクティブ フェールオーバーまたはアクティブ / スタンバイ フェールオーバーのいずれかを使用します。

表 13-3 で、各フェールオーバー タイプの設定でサポートされる一部の機能を比較します。

表 13-3　フェールオーバーの設定でサポートされる機能

機能	アクティブ/アクティブ	アクティブ/スタンバイ
シングルコンテキスト モード	不可	可
マルチコンテキスト モード	可	可
負荷分散ネットワーク コンフィギュレーション	可	不可
装置のフェールオーバー	可	可
コンテキスト グループのフェールオーバー	可	不可
個別コンテキストのフェールオーバー	不可	不可

標準フェールオーバーとステートフル フェールオーバー

FWSM は、標準フェールオーバーとステートフル フェールオーバーの 2 つのタイプのフェールオーバーをサポートします。ここは、次の内容について説明します。

- 標準フェールオーバー（p.13-18）
- ステートフル フェールオーバー（p.13-18）

標準フェールオーバー

フェールオーバーが発生すると、アクティブな接続はすべて切断されます。新しいアクティブ ユニットが接続を引き継ぐときに、接続を再確立する必要があります。

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 ユニットは各接続ステート情報をスタンバイ ユニットに渡し続けます。フェールオーバー発生後は、新しいアクティブ ユニットで同じ接続情報を使用できます。同じ通信セッションを保持するために、サポート対象のエンド ユーザ アプリケーションを再接続する必要はありません。

スタンバイ ユニットに渡されるステート情報には、次のデータが含まれます。

- NAT 変換テーブル
- TCP 接続ステート
- UDP 接続ステート
- ARP テーブル
- レイヤ 2 ブリッジ テーブル（透過ファイアウォール モードで実行している場合）
- HTTP 接続ステート（HTTP の複製がイネーブルになっている場合）
- ISAKMP および IPSec SA テーブル
- GTP PDP 接続データベース

ステートフル フェールオーバーがイネーブルの場合、次の情報はスタンバイ ユニットには渡されません。

- HTTP 接続テーブル（HTTP の複製がイネーブルの場合を除く）
- ユーザ認証（uauth）テーブル
- ルーティング テーブル

（注） Cisco IP SoftPhone セッション中にフェールオーバーが発生した場合、通話セッション ステート情報はスタンバイ ユニットに複製されるため、通話はアクティブのままになります。通話が中断されると、IP SoftPhone クライアントは CallManager との接続を失います。これは、スタンバイ ユニットに CTIQBE ハングアップ メッセージに関するセッション情報がないためです。IP SoftPhone クライアントは一定時間内に CallManager から応答を受信しない場合、CallManager を到達不能とみなして自らを登録解除します。

フェールオーバーのヘルス モニタ

FWSM は、各装置について、全体の動作状態とインターフェイスの動作状態をモニタします。FWSM が各装置の状態を判別するために実行するテストの詳細については、次の項目を参照してください。

- 装置のヘルス モニタ（p.13-19）
- インターフェイスのモニタ（p.13-19）

装置のヘルス モニタ

FWSM は、フェールオーバー リンクをモニタすることによって、他方の装置の状態を判別します。一方の装置がフェールオーバー リンク上で hello メッセージを受信しない場合、その装置はフェールオーバー インターフェイスを含めたすべてのインターフェイスに ARP 要求を送信します。FWSM はユーザによって設定可能な回数だけ、再試行します。FWSM の動作は、他方の装置からの応答状態によって異なります。具体的には、次のように動作します。

- FWSM がいずれかのインターフェイスから応答を受信した場合、フェールオーバーは実行されません。
- FWSM がどのインターフェイスからも応答を受信しない場合、スタンバイ ユニットがアクティブ モードに切り替わり、他方の装置は障害装置としてマークされます。
- FWSM がフェールオーバー リンク上でのみ応答を受信しない場合には、フェールオーバーは実行されません。フェールオーバー リンクは障害としてマークされます。フェールオーバー リンクがダウンしていると、スタンバイ ユニットへのフェールオーバーを実行できないので、フェールオーバー リンクはできるだけ早く回復させる必要があります。

（注） 障害がないと判断された装置が、障害状態から回復しない場合は、**failover reset** コマンドを入力してステートをリセットできます。ただし、フェールオーバーの条件が存続している場合には、装置は再び障害状態になります。

インターフェイスのモニタ

コンテキスト全体で最大 250 のインターフェイスをモニタできます。1 つのコンテキストが共有インターフェイスをモニタするように設定できます（インターフェイスが共有されているため、全コンテキストがモニタされるため）。

装置がモニタ対象のインターフェイス上で hello メッセージを受信しない場合、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 ステータスのテストです。リンク アップ / ダウン テストでインターフェイスの正常な動作が確認されると、FWSM はネットワークのテストを実行します。ネットワークのテストは、ネットワーク トラフィックを生成して、障害のある装置（両方の場合もあり）を判別することが目的です。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 カウントをクリアします。テストが完了すると、各装置はトラフィックを受信しているかどうかを確認します。受信していれば、インターフェイスは正常であるとみなされます。一方の装置がテスト用トラフィックを受信し、他方の装置が受信していない場合、トラフィックを受信していない装置に障害があると判断されます。どちらの装置もトラフィックを受信していない場合には、次のテストが実行されます。
2. ネットワーク動作のテスト — ネットワークの受信動作のテストです。装置は、最大 5 秒間、すべての受信パケットをカウントします。この間にパケットを受信すれば、インターフェイスは正常であるとみなされ、テストは終了します。トラフィックを受信しなかった場合、ARP テストが実行されます。
3. ARP テスト — 装置の ARP キャッシュから、最新の 2 つのエントリが読み取られます。1 つのエントリごとに、装置はこれらの宛先に ARP 要求を送信し、ネットワーク トラフィックを流すことを試みます。各要求の送信後、装置は最大 5 秒間、すべての受信トラフィックをカウントします。トラフィックを受信すれば、インターフェイスは正常であるとみなされます。トラフィックを受信しなかった場合、次の宛先に ARP 要求が送信されます。最後のエントリまで、まったくトラフィックを受信しなかった場合には、ping テストが実行されます。
4. ブロードキャスト ping テスト — このテストでは、ブロードキャスト ping 要求が送信されます。その後、装置は、最大 5 秒間すべての受信パケットをカウントします。この間にパケットを受信すれば、インターフェイスは正常であるとみなされ、テストは終了します。

特定のインターフェイスがすべてのネットワークのテストに失敗し、他方の装置では同じインターフェイスが正常にトラフィックを伝送している場合、テストに失敗したインターフェイスに障害があるとみなされます。障害のあるインターフェイス数がスレッシュホールドの値に達した場合、フェールオーバーが実行されます。他方の装置のインターフェイスもすべてのネットワーク テストに失敗した場合、これらのインターフェイスはいずれも「不明（Unknown）」ステートとなり、フェールオーバー用の障害インターフェイスとしてはカウントされません。

インターフェイスは、トラフィックを受信すれば、再び正常な状態に戻ります。障害インターフェイス数がスレッシュホールド未満になると、障害状態の FWSM はスタンバイ モードに戻ります。

（注）障害がないと判断された装置が、障害状態から回復しない場合には、**failover reset** コマンドを入力してステートをリセットできます。ただし、フェールオーバーの条件が存続している場合には、装置は再び障害状態になります。

フェールオーバーの設定

ここでは、フェールオーバーを設定する手順について説明します。内容は次のとおりです。

- アクティブ / スタンバイ フェールオーバーの使用（p.13-21）
- アクティブ / アクティブ フェールオーバーの使用（p.13-26）
- フェールオーバー通信の認証 / 暗号化の設定（p.13-31）
- フェールオーバーの設定の確認（p.13-32）

アクティブ / スタンバイ フェールオーバーの使用

ここでは、アクティブ / スタンバイ フェールオーバーの設定手順を説明します。内容は次のとおりです。

- 前提条件（p.13-21）
- アクティブ / スタンバイ フェールオーバーの設定（p.13-21）
- 任意のアクティブ / スタンバイ フェールオーバーの設定（p.13-25）

一般的なフェールオーバーの設定例については、「フェールオーバーの設定例」（p.B-20）を参照してください。

前提条件

作業を開始する前に、次のことを確認します。

- 両装置とも正規のライセンスを持っていること。
- プライマリ ユニットがシングルコンテキスト モードの場合、セカンダリ ユニットもシングルコンテキスト モードで、さらにプライマリ ユニットと同じファイアウォール モードでなければなりません。
- プライマリ ユニットがマルチコンテキスト モードの場合、セカンダリ ユニットもマルチコンテキスト モードでなければなりません。セカンダリ ユニット上でセキュリティ コンテキストのファイアウォール モードを設定する必要はありません。フェールオーバー リンクおよびステート リンクはシステム コンテキスト内に常時設定されているためです。セカンダリ ユニットは、プライマリ ユニットからセキュリティ コンテキスト コンフィギュレーションを取得します。

（注）　**mode** コマンドはセカンダリ ユニットには複製されません。

アクティブ / スタンバイ フェールオーバーの設定

ここでは、アクティブ / スタンバイ フェールオーバーの設定方法について説明します。プライマリ ユニットから実行コンフィギュレーションを取得する前にフェールオーバー リンクを認識するように、セカンダリ ユニットを設定する必要があります。

このセクションでは、次の内容について説明します。

- プライマリ ユニットの設定（p.13-22）
- セカンダリ ユニットの設定（p.13-24）

プライマリ ユニットの設定

次の手順に従って、アクティブ / スタンバイ フェールオーバー設定内のプライマリ ユニットを設定します。これらの手順は、プライマリ ユニットでフェールオーバーをイネーブルにするための最小限の設定です。マルチコンテキスト モードでは、特に明記されていないかぎり、すべての手順をシステム実行スペースで行います。

アクティブ / スタンバイ フェールオーバー ペアのプライマリ ユニットを設定するには、次の手順に従います。

ステップ 1　各インターフェイス（ルーテッド モード）および各管理アドレス（透過モード）のアクティブ IP アドレスとスタンバイ IP アドレスをまだ設定していない場合は、設定します。スタンバイ IP アドレスは、現在スタンバイ ユニットである FWSM で使用されます。この IP アドレスは、アクティブ IP アドレスと同じサブネットに属している必要があります。

（注）　フェールオーバー リンクまたはステート リンク（ステートフル フェールオーバーを使用する予定の場合）の IP アドレスは設定しないでください。

```
hostname(config-if)# ip address active_addr netmask standby standby_addr
```

（注）　マルチコンテキスト モードでは、各コンテキスト内でインターフェイス アドレスを設定する必要があります。**changeto context** コマンドを使用して、コンテキスト間の切り替えを行います。コマンド プロンプトが `hostname/context(config-if)#` に変わります。*context* は現在のコンテキストの名前です。

ステップ 2　装置をプライマリ ユニットとして指定します。

```
hostname(config)# failover lan unit primary
```

ステップ 3　フェールオーバー インターフェイスを定義します。

a. フェールオーバー インターフェイスとして使用するインターフェイスを指定します。

```
hostname(config)# failover lan interface if_name vlan vlan
```

if_name 引数は、名前を *vlan* 引数で指定されたインターフェイスに割り当てます。

b. 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。

```
hostname(config)# failover interface ip if_name ip_addr mask standby ip_addr
```

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に属している必要があります。スタンバイ アドレスのサブネット マスクを特定する必要はありません。

フェールオーバー リンクの IP アドレスおよび MAC アドレスは、フェールオーバー実行後も変更されません。プライマリ ユニットは常にフェールオーバー リンクのアクティブ IP アドレスを使用し、セカンダリ ユニットは常にスタンバイ IP アドレスを使用します。

ステップ 4　（任意）ステートフル フェールオーバーをイネーブルにするには、ステート リンクを設定します。ステート リンクは未使用のインターフェイス上で設定する必要があります。

a. 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。

```
hostname(config)# failover link if_name [vlan vlan]
```

（注） ステート リンクがフェールオーバー リンクを使用する場合、*if_name* 引数を指定するだけで済みます。

if_name 引数は、論理名を *vlan* 引数で指定されたインターフェイスに割り当てます。このインターフェイスはほかの目的には使用しないでください（フェールオーバー リンクを除く［任意］）。

b. アクティブ IP アドレスとスタンバイ IP アドレスをステート リンクに割り当てます。

（注） ステート リンクがフェールオーバー リンクを使用する場合、この手順は省略します。すでにフェールオーバー リンクのアクティブ IP アドレスとスタンバイ IP アドレスを指定しているためです。

```
hostname(config)# failover interface ip if_name ip_addr mask standby ip_addr
```

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に属している必要があります。スタンバイ アドレスのサブネット マスクを特定する必要はありません。

ステート リンクの IP アドレスおよび MAC アドレスは、フェールオーバー実行後も変更されません。プライマリ ユニットは常にアクティブ IP アドレスを使用し、スタンバイ ユニットは常にスタンバイ IP アドレスを使用します。

ステップ 5　次のコマンドを入力して、トンネル インターフェイスのモニタをイネーブルにします。

```
hostname(config)# monitor-interface interface_name
```

FWSM 上（すべてのコンテキスト全体）でモニタできるインターフェイスの最大数は、250 です。

（注） マルチコンテキスト モードでは、各コンテキスト内でインターフェイス モニタリングを設定する必要があります。**changeto context** コマンドを使用して、コンテキスト間の切り替えを行います。コマンド プロンプトが `hostname/context(config)#` に変わります。*context* は現在のコンテキストの名前です。

ステップ 6　フェールオーバーをイネーブルにします。

```
hostname(config)# failover
```

ステップ 7　設定を保存します。

```
hostname(config)# write memory
```

（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に **write memory all** コマンドを入力してすべてのコンテキストのコンフィギュレーションを保存します。

セカンダリ ユニットの設定

セカンダリ ユニットに必要なのは、フェールオーバー インターフェイスの設定だけです。プライマリ ユニットと初回の通信を開始するには、セカンダリ ユニットにこれらのコマンドが必要です。プライマリ ユニットからセカンダリ ユニットに設定が送信されたあと、2 つの設定で唯一異なるのが、各装置をプライマリまたはセカンダリとして識別する **failover lan unit** コマンドです。

マルチコンテキスト モードでは、特に明記されていないかぎり、すべての手順をシステム実行スペースで行います。

セカンダリ ユニットを設定するには、次の手順を実行します。

ステップ 1　フェールオーバー インターフェイスを定義します。プライマリ ユニットに使用した設定と同じ設定を使用します。

a. フェールオーバー インターフェイスとして使用するインターフェイスを指定します。

```
hostname(config)# failover lan interface if_name vlan vlan
```

if_name 引数は、名前を *vlan* 引数で指定されたインターフェイスに割り当てます。

b. 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。

```
hostname(config)# failover interface ip if_name ip_addr mask standby ip_addr
```

（注） このコマンドは、フェールオーバー インターフェイスの設定時にプライマリ ユニットに入力したとおりに入力します。

ステップ 2　（任意）この装置をセカンダリ ユニットとして指定します。

```
hostname(config)# failover lan unit secondary
```

（注） すでに設定してある場合を除き、デフォルトでは装置はセカンダリ ユニットとして指定されるため、この手順は任意となります。

ステップ 3　フェールオーバーをイネーブルにします。

```
hostname(config)# failover
```

フェールオーバーをイネーブルにすると、アクティブ ユニットからスタンバイ ユニットに、実行メモリ内の設定が送信されます。設定を同期化すると、アクティブ ユニットのコンソールに「Beginning Configuration replication: Sending to mate」および「End Configuration Replication to mate」というメッセージが表示されます。

ステップ 4　実行コンフィギュレーションで複製が完了したら、設定をフラッシュ メモリに保存します。

```
hostname(config)# write memory
```

任意のアクティブ / スタンバイ フェールオーバーの設定

フェールオーバーの初期設定時またはフェールオーバーの設定後に、次の任意のアクティブ / スタンバイ フェールオーバー設定を指定することができます。特に指定のないかぎり、コマンドはアクティブ ユニットに入力します。

ここでは、次の内容について説明します。

- ステートフル フェールオーバーでの HTTP 複製のイネーブル化（p.13-25）
- インターフェイスおよび装置のポーリング間隔の設定（p.13-25）
- フェールオーバー条件の設定（p.13-25）

ステートフル フェールオーバーでの HTTP 複製のイネーブル化

ステート情報の複製に HTTP 接続を含めるには、HTTP の複製をイネーブルにする必要があります。HTTP 接続は一般に存続時間が短く、HTTP クライアントは失敗した接続を再試行することが多いため、HTTP 接続は複製されたステート情報には自動的には含められません。

ステートフル フェールオーバーがイネーブルである場合、次のコマンドをグローバル コンフィギュレーション モードで入力して、HTTP ステートの複製をイネーブルにします。

```
hostname(config)# failover replication http
```

インターフェイスおよび装置のポーリング間隔の設定

FWSM は、フェールオーバーについて、装置とインターフェイスの両方をヘルス モニタします。装置とインターフェイスをヘルス モニタする際、hello メッセージの間隔を設定できます。ポーリング間隔を短くすると、インターフェイスまたは装置の障害をより速く検出できますが、システム リソースの消費量が大きくなります。

インターフェイスのポーリング間隔を変更するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

```
hostname(config)# failover polltime interface seconds
```

装置のポーリング間隔を変更するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

```
hostname(config)# failover polltime seconds
```

フェールオーバー条件の設定

デフォルトでは、モニタ対象インターフェイスの障害が 50% になるとフェールオーバーが実行されます。フェールオーバーを実行するために必要な、モニタ対象の障害インターフェイスの数または割合を指定できます。

デフォルトのフェールオーバー条件を変更するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

```
hostname(config)# failover interface-policy num[%]
```

インターフェイスの数を指定する場合、*num* 引数に 1 ～ 250 を指定できます。インターフェイスの割合を指定する場合、*num* 引数に 1 ～ 100 を指定できます。

アクティブ / アクティブ フェールオーバーの使用

ここでは、アクティブ / アクティブ フェールオーバーの設定方法について説明します。

内容は次のとおりです。

- 前提条件（p.13-26）
- アクティブ / アクティブ フェールオーバーの設定（p.13-26）
- アクティブ / アクティブ フェールオーバーの任意の設定（p.13-30）

一般的なフェールオーバーの設定例については、「フェールオーバーの設定例」（p.B-20）を参照してください。

前提条件

作業を開始する前に、次のことを確認します。

- 両装置とも正規のライセンスを持っていること。
- 両装置ともマルチコンテキスト モードであること。セカンダリ ユニット上でセキュリティ コンテキストのファイアウォール モードを設定する必要はありません。フェールオーバー リンクおよびステート リンクはシステム コンテキスト内に常時設定されているためです。セカンダリ ユニットは、プライマリ ユニットからセキュリティ コンテキスト コンフィギュレーションを取得します。

（注）　**mode** コマンドはセカンダリ ユニットには複製されません。

アクティブ / アクティブ フェールオーバーの設定

ここでは、アクティブ / アクティブ フェールオーバーの設定方法について説明します。プライマリ ユニットから実行コンフィギュレーションを取得する前にフェールオーバー リンクを認識するように、セカンダリ ユニットを設定する必要があります。

ここでは、次の内容について説明します。

- プライマリ ユニットの設定（p.13-27）
- セカンダリ ユニットの設定（p.13-28）

プライマリ ユニットの設定

アクティブ / アクティブ フェールオーバーの設定内のプライマリ ユニットを設定するには、次の手順に従います。

ステップ 1　システム実行スペースで基本フェールオーバー パラメータを設定します。

a. 装置をプライマリ ユニットとして指定します。

```
hostname(config)# failover lan unit primary
```

b. フェールオーバー リンクを指定します。

```
hostname(config)# failover lan interface if_name vlan vlan
```

if_name 引数は、*vlan* 引数で指定されたインターフェイスに論理名を割り当てます。このインターフェイスはその他目的では使用しないでください（ステート リンクを除く［任意］）。

c. フェールオーバー リンクのアクティブ IP アドレスとスタンバイ IP アドレスを指定します。

```
hostname(config)# failover interface ip if_name ip_addr mask standby ip_addr
```

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に属している必要があります。スタンバイ IP アドレスのサブネット マスクを特定する必要はありません。フェールオーバー リンクの IP アドレスは、フェールオーバー実行後も変更されません。プライマリ ユニットは常にアクティブ IP アドレスを使用し、スタンバイ ユニットは常にスタンバイ IP アドレスを使用します。

ステップ 2　（任意）ステートフル フェールオーバーをイネーブルにするには、ステート リンクを設定します。ステート リンクは未使用のインターフェイス上で設定する必要があります。

a. 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。

```
hostname(config)# failover link if_name [vlan vlan]
```

if_name 引数は、*vlan* 引数で指定されたインターフェイスに論理名を割り当てます。このインターフェイスはその他の目的では使用しないでください（フェールオーバー リンクを除く［任意］）。

（注） ステート リンクがフェールオーバー リンクを使用する場合、*if_name* 引数を指定するだけで済みます。

b. アクティブ IP アドレスとスタンバイ IP アドレスをステート リンクに割り当てます。

（注） ステート リンクがフェールオーバー リンクを使用する場合、この手順は省略します。すでにフェールオーバー リンクのアクティブ IP アドレスとスタンバイ IP アドレスを指定しているためです。

```
hostname(config)# failover interface ip if_name ip_addr mask standby ip_addr
```

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に属している必要があります。スタンバイ アドレスのサブネット マスクを特定する必要はありません。

ステート リンクの IP アドレスは、フェールオーバー実行後も変更されません。プライマリ ユニットは常にアクティブ IP アドレスを使用し、スタンバイ ユニットは常にスタンバイ IP アドレスを使用します。

ステップ 3　フェールオーバー グループを設定します。最大 2 つのフェールオーバー グループを作成できます。指定されたフェールオーバー グループが存在しない場合、**failover group** コマンドはこのグループを作成し、フェールオーバー グループ コンフィギュレーション モードを開始します。

各フェールオーバー グループについて、**primary** または **secondary** コマンドを使用して、そのフェールオーバー グループでのプライマリ / セカンダリのプリファレンスを指定する必要があります。両方のフェールオーバー グループに同じプリファレンスを割り当ててもかまいません。負荷分散設定の場合は、各フェールオーバー グループに異なるプリファレンスを割り当てる必要があります。

次に、フェールオーバー グループ 1 にプライマリ プリファレンスを割り当て、フェールオーバー グループ 2 にセカンダリ プリファレンスを割り当てる例を示します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# exit
```

ステップ 4　コンテキスト コンフィギュレーション モードで **join-failover-group** コマンドを使用して、各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。

割り当てられていないコンテキストは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。

次のコマンドを入力して、各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。

```
hostname(config)# context context_name
hostname(config-context)# join-failover-group {1 | 2}
```

ステップ 5　フェールオーバーをイネーブルにします。

```
hostname(config)# failover
```

ステップ 6　インターフェイス上のモニタリングをイネーブルにするには、コンテキストに切り替えて、次のコマンドを入力します。

```
hostname(config)# changeto context context_name
hostname(config)# monitor-interface interface_name
```

FWSM 上（すべてのコンテキスト全体）でモニタできるインターフェイスの最大数は、250 です。

セカンダリ ユニットの設定

フェールオーバー リンクを認識するには、セカンダリ ユニットを設定する必要があります。これにより、セカンダリ ユニットはプライマリ ユニットと通信し、プライマリ ユニットから実行コンフィギュレーションを取得することができます。

アクティブ / アクティブ フェールオーバー コンフィギュレーションのセカンダリ ユニットを設定するには、次の手順に従います。

ステップ 1　フェールオーバー インターフェイスを定義します。プライマリ ユニットに使用した設定と同じ設定を使用します。

a. フェールオーバー インターフェイスとして使用するインターフェイスを指定します。

```
hostname(config)# failover lan interface if_name vlan vlan
```

if_name 引数は、*vlan* 引数で指定されたインターフェイスに論理名を割り当てます。

b. 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。

```
hostname(config)# failover interface ip if_name ip_addr mask standby ip_addr
```

（注） このコマンドは、フェールオーバー インターフェイスの設定時にプライマリ ユニットに入力したとおりに入力します。

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に属している必要があります。スタンバイ アドレスのサブネット マスクを特定する必要はありません。

ステップ 2　（任意）この装置をセカンダリ ユニットとして指定します。

```
hostname(config)# failover lan unit secondary
```

（注） すでに設定してある場合を除き、デフォルトでは装置はセカンダリ ユニットとして指定されるため、この手順は任意となります。

ステップ 3　フェールオーバーをイネーブルにします。

```
hostname(config)# failover
```

フェールオーバーをイネーブルにすると、アクティブ ユニットからスタンバイ ユニットに、実行メモリ内の設定が送信されます。設定を同期化すると、アクティブ ユニットのコンソールに「Beginning Configuration replication: Sending to mate」および「End Configuration Replication to mate」というメッセージが表示されます。

ステップ 4　実行コンフィギュレーションで複製が完了したら、次のコマンドを入力して、設定をフラッシュ メモリに保存します。

```
hostname(config)# write memory
```

ステップ 5　必要に応じて、プライマリ ユニット上でアクティブな任意のフェールオーバー グループを、強制的にセカンダリ ユニット上でアクティブ ステートにすることができます。フェールオーバー グループをセカンダリ ユニット上で強制的にアクティブにするには、プライマリ ユニットのシステム実行スペースで次のコマンドを入力します。

```
hostname# no failover active group group_id
```

group_id 引数には、セカンダリ ユニット上でアクティブにするグループを指定します。

アクティブ / アクティブ フェールオーバーの任意の設定

フェールオーバーの初期設定時またはフェールオーバーの設定後に、次の任意のアクティブ / アクティブ フェールオーバー設定を指定することができます。特に指定のないかぎり、コマンドは、アクティブ ステートのフェールオーバー グループ 1 を持つ装置に入力する必要があります。

ここでは、次の内容について説明します。

- フェールオーバー グループ プリエンプションの設定（p.13-30）
- ステートフル フェールオーバーでの HTTP 複製のイネーブル化（p.13-30）
- インターフェイスおよび装置のポーリング間隔の設定（p.13-31）
- フェールオーバー条件の設定（p.13-31）

フェールオーバー グループ プリエンプションの設定

フェールオーバー グループにプライマリまたはセカンダリの優先度を割り当てることで、両方の装置を同時に起動したときに、フェールオーバー グループがアクティブになる装置を指定します。ただし、一方の装置を他方より先に起動すると、その装置上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。もう一方の装置がオンラインになると、この装置を優先するフェールオーバー グループはすべて、手動で強制しないか、フェールオーバーが発生するか、**preempt** コマンドでフェールオーバー グループが設定されない限り、この装置上ではアクティブにはなりません。**preempt** コマンドにより、指定した装置が使用可能になると、フェールオーバー グループはこの装置上で自動的にアクティブになります。

次のコマンドを入力して、指定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ます。

```
hostname(config)# failover group {1 | 2}
hostname(config-fover-group)# preempt [delay]
```

任意で *delay* 値を入力することができます。この値は、フェールオーバー グループが指定した装置上で自動的にアクティブになるまで、現在の装置上でアクティブのままでいる秒数を指定します。

ステートフル フェールオーバーでの HTTP 複製のイネーブル化

ステート情報に HTTP 接続を含めるには、HTTP の複製をイネーブルにする必要があります。HTTP 接続は一般に存続時間が短く、HTTP クライアントは失敗した接続を再試行することが多いため、HTTP 接続は複製されたステート情報には自動的には含められません。**replication http** コマンドを使用して、ステートフル フェールオーバーがイネーブルの場合に、フェールオーバー グループに HTTP ステート情報を複製させることができます。

フェールオーバー グループによる HTTP ステートの複製をイネーブルにするには、次のコマンドを入力します。このコマンドは、コマンドが設定されたフェールオーバー グループにのみ影響します。両方のフェールオーバー グループによる HTTP ステートの複製をイネーブルにするには、各グループにこのコマンドを入力します。このコマンドは、システム実行スペースに入力する必要があります。

```
hostname(config)# failover group {1 | 2}
hostname(config-fover-group)# replication http
```

インターフェイスおよび装置のポーリング間隔の設定

フェールオーバー グループのインターフェイスをヘルス モニタする際、hello メッセージの間隔を設定できます。インターフェイスのポーリング間隔を短くすると、フェールオーバーを速く実行できますが、システム リソースの消費量が大きくなります。

デフォルトのインターフェイス ポーリング間隔を変更するには、次のコマンドを入力します。

```
hostname(config)# failover group {1 | 2}
hostname(config-fover-group)# polltime interface seconds
```

装置のポーリング間隔は、ピア装置の動作状態を判断するために、フェールオーバー リンクで 送信する hello メッセージの間隔を指定します。装置のポーリング間隔を短くすると、装置の障害をより速く検出できますが、システム リソースの消費量が大きくなります。装置のポーリング間隔を変更するには、グローバル コンフィギュレーション モードでシステム実行スペースに次のコマンドを入力します。

```
hostname(config)# failover polltime seconds
```

フェールオーバー条件の設定

デフォルトでは、モニタ対象インターフェイスの障害が 50% になるとフェールオーバーが実行されます。フェールオーバーを実行するために必要な、モニタ対象の障害インターフェイスの数または割合を指定できます。フェールオーバー条件は、フェールオーバー グループ単位で指定します。

指定したフェールオーバー グループのデフォルトのフェールオーバー条件を変更するには、次のコマンドを入力します。

```
hostname(config)# failover group {1 | 2}
hostname(config-fover-group)# interface-policy num[%]
```

インターフェイスの数を指定する場合、*num* 引数に 1 ～ 250 を指定できます。インターフェイスの割合を指定する場合、*num* 引数に 1 ～ 100 を指定できます。

フェールオーバー通信の認証 / 暗号化の設定

共有秘密鍵または 16 進数鍵を指定することで、フェールオーバー ピア間の通信の暗号化および認証を実行できます。

注意　フェールオーバー キーで通信をセキュリティ保護している場合を除き、フェールオーバーおよびステートフル フェールオーバー リンク間の情報はすべてクリア テキストで送信されます。FWSM を使用して VPN トンネルを終端する場合、この情報には任意のユーザ名、パスワードおよびトンネルの確立に使用した事前共有鍵が含まれます。この機密データをクリア テキストで伝送すると、重大なセキュリティ リスクが生じる可能性があります。FWSM を使用して VPN トンネルを終端している場合、フェールオーバー通信をフェールオーバー キーでセキュリティ保護することを推奨します。

アクティブ / スタンバイ フェールオーバー ペアのアクティブ ユニット上、またはアクティブ / アクティブ フェールオーバー ペア内のアクティブ ステートのフェールオーバー グループ 1 を持つ装置上で、次のコマンドを入力します。

```
hostname(config)# failover key {secret | hex key}
```

secret 引数は、暗号化鍵の生成に使用する共有秘密鍵を指定します。値には、数字、文字、句読点の任意の組み合わせの 1 ～ 63 文字を指定できます。***hex key*** 引数は、16 進数の暗号化鍵を指定します。このキーには 32 ビットの 16 進文字（0 ～ 9、a ～ f）を指定する必要があります。

（注） フェールオーバー キーが既存のフェールオーバーの設定のために、ピア装置にクリア テキストで複製されないようにするには、アクティブ ユニット（または、アクティブ ステートのフェールオーバー グループ 1 を持つ装置のシステム実行スペースで）でフェールオーバーをディセーブルにして、両方の装置にフェールオーバー キーを入力してから、フェールオーバーを再びイネーブルにします。フェールオーバーが再びイネーブルになると、フェールオーバー通信はフェールオーバー キーで暗号化されます。

新しいフェールオーバーの設定では、**failover key** コマンドが初期フェールオーバー ペアの設定の一部でなければなりません。

フェールオーバーの設定の確認

ここでは、フェールオーバーの設定を確認する手順について説明します。内容は次のとおりです。

- フェールオーバー ステータスの表示（p.13-32）
- モニタ対象インターフェイスの表示（p.13-40）
- フェールオーバーの設定の表示（p.13-41）
- フェールオーバー機能のテスト（p.13-41）

フェールオーバー ステータスの表示

ここでは、フェールオーバー ステータスを確認する方法について説明します。各装置で **show failover** コマンドを入力してフェールオーバー ステータスを確認できます。表示される情報は、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 フェールオーバーのどちらを使用しているかによって異なります。

ここでは、次の内容について説明します。

- アクティブ / スタンバイのフェールオーバー ステータスの表示（p.13-33）
- アクティブ / アクティブのフェールオーバー ステータスの表示（p.13-37）

アクティブ / スタンバイのフェールオーバー ステータスの表示

次に、アクティブ / スタンバイ フェールオーバーの **show failover** コマンドの出力例を示します。表 13-4 で、表示される情報について説明します。

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan 100(up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
failover replication http
Last Failover at: 22:44:03 UTC Dec 8 2004
        This host: Primary - Active
                Active time: 13434 (sec)
                Interface inside (10.130.9.3): Normal
                Interface outside (10.132.9.3): Normal
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                Interface inside (10.130.9.4): Normal
                Interface outside (10.132.9.4): Normal

Stateful Failover Logical Update Statistics
        Link : fover Vlan100 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         1950       0          1733       0
        sys cmd         1733       0          1733       0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        6          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         106        0          0          0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       2       1733
        Xmit Q:         0       2       15225
```

マルチコンテキスト モードでは、セキュリティ コンテキストで **show failover** コマンドを使用すると、そのコンテキストのフェールオーバー情報が表示されます。この情報は、シングルコンテキスト モードでこのコマンドを使用した場合に表示される情報とほぼ同じです。装置のアクティブ / スタンバイ ステータスではなく、コンテキストのアクティブ / スタンバイ ステータスが表示されます。表 13-4 で、表示される情報について説明します。

```
Failover On
Last Failover at: 04:03:11 UTC Jan 4 2003
        This context: Negotiation
                Active time: 1222 (sec)
                Interface outside (192.168.5.121): Normal
                Interface inside (192.168.0.1): Normal
        Peer context: Not Detected
                Active time: 0 (sec)
                Interface outside (192.168.5.131): Normal
                Interface inside (192.168.0.11): Normal

Stateful Failover Logical Update Statistics
        Status: Configured.
        Stateful Obj    xmit       xerr       rcv        rerr
        RPC services    0          0          0          0
        TCP conn        99          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         22          0          0          0
        Xlate_Timeout   0          0          0          0
        GTP PDP         0          0          0          0
        GTP PDPMCB      0          0          0          0
```

表 13-4　show failover コマンドの出力の説明

フィールド	説明
Failover	• オン • オフ
Failover Unit	プライマリまたはセカンダリ
Failover LAN Interface	フェールオーバー リンク名を表示します。
Unit Poll frequency	ピア装置に hello メッセージを送信する間隔（秒）、およびピアの障害を宣言するまでにピア装置がフェールオーバー リンク上で hello メッセージを受信する時間（秒）を指定します。
Interface Poll frequency	*n* 秒 **failover polltime interface** コマンドで設定した秒数が表示されます。デフォルトは 15 秒です。
Interface Policy	フェールオーバーをトリガーするために必要な、障害インターフェイスの数または比率を表示します。
Monitored Interfaces	モニタ可能な最大インターフェイス数のうち、モニタ対象のインターフェイス数を表示します。
failover replication http	ステータス フェールオーバーに対して HTTP ステートの複製がイネーブルかどうかを示します。
Last Failover at	最終フェールオーバー日時を次の形式で示します。 *hh*:*mm*:*ss* **UTC** *DayName Month Day yyyy* UTC（協定世界時）は GMT（グリニッジ標準時）に相当します。

表 13-4　show failover コマンドの出力の説明（続き）

フィールド	説明
This host Other host	各ホストについて、次の情報が表示されます。
Primary または Secondary	• アクティブ • スタンバイ
Acitive time	*n*（秒） 装置がアクティブな時間。累積時間なので、スタンバイ ユニットが以前にアクティブだった場合、その時間が表示されます。
Interface *name* (*n.n.n.n*):	各インターフェイスについて、装置上で現在使用されている IP アドレスと、次のいずれかの状態が表示されます。 • Failed — インターフェイスに障害が発生しています。 • No Link — インターフェイス ライン プロトコルがダウンしています。 • Normal — インターフェイスは正常に動作しています。 • Link Down — インターフェイスは管理者によって明示的に閉じられています。 • Unknown — FWSM はこのインターフェイスのステータスを判別できません。 • Waiting — 他の装置上のネットワーク インターフェイスのモニタリングは、まだ開始されていません。
Stateful Failover Logical Update Statistics	ステートフル フェールオーバー機能の関連フィールドが表示されます。Link フィールドにインターフェイス名が示されている場合、ステートフル フェールオーバーの統計情報が表示されます。
Link	• *interface_name* — ステートフル フェールオーバー リンクに使用されているインターフェイス • Unconfigured — ステートフル フェールオーバーが使用されていません。 • up — インターフェイスは開かれて機能しています。 • down — インターフェイスは管理者によって明示的に閉じられているか、物理的にダウンしています。 • failed — インターフェイスに障害が発生しているため、ステートフル データは転送されません。
Stateful Obj	各フィールド タイプに、次の統計情報が表示されます。これらは 2 つの装置間で送信されたステート情報パケット数のカウンタです。必ずしも装置を通過するアクティブな接続が表示されるわけではありません。 • xmit — 他方の装置への送信パケット数 • xerr — 他方の装置へのパケット送信中に発生したエラー数 • rcv — 受信パケット数 • rerr — 他方の装置からのパケット受信中に発生したエラー数
General	すべてのステートフル オブジェクトの合計
sys cmd	論理更新システム コマンド：LOGIN、Stay Alive など
up time	アクティブ ユニットからスタンバイ ユニットに渡される動作時間
RPC services	リモート プロシージャ コールの接続情報

表 13-4　show failover コマンドの出力の説明（続き）

フィールド	説明
TCP conn	TCP 接続情報
UDP conn	動的な UDP 接続情報
ARP tbl	動的な ARP テーブル情報
L2BRIDGE tbl	レイヤ 2 ブリッジ テーブル情報（透過ファイアウォール モード限定）
Xlate_Timeout	接続変換のタイムアウト情報を示します
VPN IKE upd	IKE 接続情報
VPN IPSEC upd	IPSec 接続情報
VPN CTCP upd	cTCP トンネル接続情報
VPN SDI upd	SDI AAA 接続情報
VPN DHCP upd	トンネル経由の DHCP 接続情報
GTP PDP	GTP PDP 更新情報。この情報は、GTP 検査がイネーブルの場合にのみ表示されます。
GTP PDPMCB	GTP PDPMCB 更新情報。この情報は、GTP 検査がイネーブルの場合にのみ表示されます。
Logical Update Queue Information	各フィールド タイプに、次の統計情報が表示されます。 • Cur ― 現在のパケット数 • Max ― 最大パケット数 • Total ― 合計パケット数
Recv Q	受信キューのステータス
Xmit Q	送信キューのステータス

アクティブ / アクティブのフェールオーバー ステータスの表示

次に、アクティブ / アクティブ フェールオーバーの **show failover** コマンドの出力例を示します。表 13-5 で、表示される情報について説明します。

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan 100 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004

  This host:    Primary
  Group 1       State:          Active
                Active time:    2896 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                admin Interface outside (10.132.8.5): Normal
                admin Interface third (10.132.9.5): Normal
                admin Interface inside (10.130.8.5): Normal
                admin Interface fourth (10.130.9.5): Normal
                ctx1 Interface outside (10.1.1.1): Normal
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    190 (sec)
  Group 2       State:          Active
                Active time:    3322 (sec)

                admin Interface outside (10.132.8.6): Normal
                admin Interface third (10.132.9.6): Normal
                admin Interface inside (10.130.8.6): Normal
                admin Interface fourth (10.130.9.6): Normal
                ctx1 Interface outside (10.1.1.2): Normal
                ctx1 Interface inside (10.2.2.2): Normal
                ctx2 Interface outside (10.3.3.1): Normal
                ctx2 Interface inside (10.4.4.1): Normal

Stateful Failover Logical Update Statistics
        Link : fover Vlan100 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         1973       0          1895       0
        sys cmd         380        0          380        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1435       0          1450       0
        UDP conn        0          0          0          0
        ARP tbl         124        0          65         0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1895
        Xmit Q:         0       0       1940
```

次に、アクティブ / アクティブ フェールオーバーの **show failover group** コマンドの出力例を示します。表示される情報は、**show failover** コマンドの情報とほぼ同じですが、指定したグループに限定されます。表 13-5 で、表示される情報について説明します。

```
hostname# show failover group 1

  Last Failover at: 04:09:59 UTC Jan 4 2005

  This host:    Secondary
                State:          Active
                Active time:    186 (sec)

                admin Interface outside (192.168.5.121): Normal
                admin Interface inside (192.168.0.1): Normal


  Other host:   Primary
                State:          Standby
                Active time:    0 (sec)

                admin Interface outside (192.168.5.131): Normal
                admin Interface inside (192.168.0.11): Normal

  Stateful Failover Logical Update Statistics
        Status: Configured.
        RPC services    0          0          0          0
        TCP conn        33         0          0          0
        UDP conn        0          0          0          0
        ARP tbl         12         0          0          0
        Xlate_Timeout   0          0          0          0
        GTP PDP         0          0          0          0
        GTP PDPMCB      0          0          0          0
```

表 13-5　show failover コマンドの出力の説明

フィールド	説明
Failover	• オン • オフ
Failover Unit	プライマリまたはセカンダリ
Failover LAN Interface	フェールオーバー リンク名を表示します。
Unit Poll frequency	ピア装置に hello メッセージを送信する間隔（秒）、およびピアの障害を宣言するまでにピア装置がフェールオーバー リンク上で hello メッセージを受信する時間（秒）を指定します。
Interface Poll frequency	*n* 秒 **failover polltime interface** コマンドで設定した秒数が表示されます。デフォルトは 15 秒です。
Interface Policy	フェールオーバーをトリガーするために必要な、障害インターフェイスの数または比率を表示します。
Monitored Interfaces	モニタ可能な最大インターフェイス数のうち、モニタ対象のインターフェイス数を表示します。
Group 1 Last Failover at : Group 2 Last Failover at :	各グループの最終フェールオーバー日時を次の形式で示します。 *hh*:*mm*:*ss* **UTC** *DayName Month Day yyyy* UTC（協定世界時）は GMT（グリニッジ標準時）に相当します。

表 13-5　show failover コマンドの出力の説明（続き）

フィールド	説明
This host : Other host :	各ホストについて、次の情報が表示されます。
Role	プライマリまたはセカンダリ
System State	• アクティブまたはスタンバイ準備完了 • アクティブ時間（秒）
Group 1 State Group 2 State	• アクティブまたはスタンバイ準備完了 • アクティブ時間（秒）
context Interface *name* (*n.n.n.n*)	各インターフェイスについて、装置上で現在使用されている IP アドレスと、次のいずれかの状態が表示されます。 • Failed — インターフェイスに障害が発生しています。 • No Link — インターフェイス ライン プロトコルがダウンしています。 • Normal — インターフェイスは正常に動作しています。 • Link Down — インターフェイスは管理者によって明示的に閉じられています。 • Unknown — FWSM はこのインターフェイスのステータスを判別できません。 • Waiting — 他の装置上のネットワーク インターフェイスのモニタリングは、まだ開始されていません。
Stateful Failover Logical Update Statistics	ステートフル フェールオーバー機能の関連フィールドが表示されます。Link フィールドにインターフェイス名が示されている場合、ステートフル フェールオーバーの統計情報が表示されます。
Link	• *interface_name* — ステートフル フェールオーバー リンクに使用されているインターフェイス。 • Unconfigured — ステートフル フェールオーバーが使用されていません。 • up — インターフェイスは開かれて機能しています。 • down — インターフェイスは管理者によって明示的に閉じられているか、物理的にダウンしています。 • failed — インターフェイスに障害が発生しているため、ステートフル データは転送されません。
Stateful Obj	各フィールド タイプに、次の統計情報が表示されます。これらは 2 つの装置間で送信されたステート情報パケット数のカウンタです。必ずしも装置を通過するアクティブな接続が表示されるわけではありません。 • xmit — 他方の装置への送信パケット数 • xerr — 他方の装置へのパケット送信中に発生したエラー数 • rcv — 受信パケット数 • rerr — 他方の装置からのパケット受信中に発生したエラー数
General	すべてのステートフル オブジェクトの合計
sys cmd	論理更新システム コマンド：LOGIN、Stay Alive など
up time	アクティブ ユニットからスタンバイ ユニットに渡される動作時間
RPC services	リモート プロシージャ コールの接続情報

表 13-5　show failover コマンドの出力の説明（続き）

フィールド	説明
TCP conn	TCP 接続情報
UDP conn	動的な UDP 接続情報
ARP tbl	動的な ARP テーブル情報
L2BRIDGE tbl	レイヤ 2 ブリッジ テーブル情報（透過ファイアウォール モード限定）
Xlate_Timeout	接続変換のタイムアウト情報を示します。
VPN IKE upd	IKE 接続情報
VPN IPSEC upd	IPSec 接続情報
VPN CTCP upd	cTCP トンネル接続情報
VPN SDI upd	SDI AAA 接続情報
VPN DHCP upd	トンネル経由の DHCP 接続情報
GTP PDP	GTP PDP 更新情報。この情報は、GTP 検査がイネーブルの場合にのみ表示されます。
GTP PDPMCB	GTP PDPMCB 更新情報。この情報は、GTP 検査がイネーブルの場合にのみ表示されます。
Logical Update Queue Information	各フィールド タイプに、次の統計情報が表示されます。 • Cur ― 現在のパケット数 • Max ― 最大パケット数 • Total ― 合計パケット数
Recv Q	受信キューのステータス
Xmit Q	送信キューのステータス

モニタ対象インターフェイスの表示

モニタ対象インターフェイス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。シングル コンテキスト モードでは、このコマンドをグローバル コンフィギュレーション モードで入力します。マルチコンテキスト モードでは、このコマンドをコンテキスト内で入力します。

```
primary/context(config)# show monitor-interface
```

次に例を示します。

```
hostname/context(config)# show monitor-interface
        This host: Primary - Active
                Interface outside (192.168.1.2): Normal
                Interface inside (10.1.1.91): Normal
        Other host: Secondary - Standby
                Interface outside (192.168.1.3): Normal
                Interface inside (10.1.1.100): Normal
```

フェールオーバーの設定の表示

実行コンフィギュレーションのフェールオーバー コマンドを表示するには、次のコマンドを入力します。

```
hostname(config)# show running-config failover
```

すべてのフェールオーバー コマンドが表示されます。マルチコンテキスト モードで実行する装置では、このコマンドをシステム実行スペースで入力します。**show running-config all failover** コマンドを入力すると、実行コンフィギュレーションのフェールオーバー コマンドが表示され、デフォルト値を変更していないコマンドが含められます。

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手順は、次のとおりです。

ステップ 1　異なるインターフェイスのホスト間で FTP（他の方法でも可）を使用してファイルを送信し、アクティブ ユニットまたはフェールオーバー グループが正常にトラフィックを転送しているかどうかをテストします。

ステップ 2　次のコマンドを入力して、スタンバイ ユニットへの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 フェールオーバーの場合、アクティブ ユニットに次のコマンドを入力します。

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

- アクティブ / アクティブ フェールオーバーの場合、ホストに接続しているインターフェイスを含むフェールオーバー グループがアクティブになっている装置に次のコマンドを入力します。

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

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

ステップ 4　テストに失敗した場合は、**show failover** コマンドを入力して、フェールオーバーのステータスを確認します。

ステップ 5　終了後、次のコマンドを入力して、装置またはフェールオーバー グループをアクティブ ステータスに戻すことができます。

- アクティブ / スタンバイ フェールオーバーの場合、アクティブ ユニットに次のコマンドを入力します。

  ```
  hostname(config)# failover active
  ```

- アクティブ / アクティブ フェールオーバーの場合、ホストに接続しているインターフェイスを含むフェールオーバー グループがアクティブな装置に次のコマンドを入力します

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

フェールオーバーの制御とモニタ

ここでは、フェールオーバーを制御およびモニタする方法について説明します。内容は次のとおりです。

- フェールオーバーの強制実行（p.13-42）
- フェールオーバーのディセーブル化（p.13-42）
- 設定の同期化のディセーブル化（p.13-43）
- 障害が発生した装置またはフェールオーバー グループの復元（p.13-43）
- フェールオーバー動作のモニタ（p.13-43）

フェールオーバーの強制実行

スタンバイ ユニットまたはスタンバイ フェールオーバー グループを強制的にアクティブにするには、次のいずれかのコマンドを入力します。

- アクティブ / スタンバイ フェールオーバーの場合：

  次のコマンドをスタンバイ ユニットに入力します。

  ```
  hostname# failover active
  ```

  または、次のコマンドをアクティブ ユニットに入力します。

  ```
  hostname# no failover active
  ```

- アクティブ / アクティブ フェールオーバーの場合：

  次のコマンドを、スタンバイ ステートのフェールオーバー グループを持つ装置のシステム実行スペースに入力します。

  ```
  hostname# failover active group group_id
  ```

  または、次のコマンドを、アクティブ ステートのフェールオーバー グループを持つ装置のシステム実行スペースに入力します。

  ```
  hostname# no failover active group group_id
  ```

  次のコマンドをシステム実行スペースに入力すると、すべてのフェールオーバー グループがアクティブになります。

  ```
  hostname# failover active
  ```

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、次のコマンドを入力します。

```
hostname(config)# no failover
```

アクティブ / スタンバイ ペアのフェールオーバーをディセーブルにすると、各装置のアクティブ ステートとスタンバイ ステートが、再起動するまで保持されます。たとえば、スタンバイ ユニットはスタンバイ モードのままなので、両方の装置によるトラフィック転送は開始されません。（フェールオーバーをディセーブルにした状態で）スタンバイ ユニットを強制的にアクティブにする場合は、「フェールオーバーの強制実行」（p.13-42）を参照してください。

アクティブ / アクティブ ペアのフェールオーバーをディセーブルにすると、どの装置を優先するように設定されたかに関係なく、現在アクティブなすべての装置上で、フェールオーバー グループはアクティブ ステートのままになります。no failover コマンドは、システム実行スペースに入力する必要があります。

設定の同期化のディセーブル化

FWSM を複雑な設定にアップグレードすると、管理アプリケーションの接続が失われることがあります。このような場合には、スタンバイ FWSM に、不完全なコンフィギュレーション ファイルが適用されます。設定の自動同期化をディセーブルに設定しておけば、スタンバイ FWSM に不完全な設定が適用されるのを防止できます。ソフトウェア イメージをアップグレードする場合、またはアクティブ FWSM の設定を変更する場合には、スタンバイ FWSM に完全なコンフィギュレーション ファイルが同期化されるように、設定の同期化をディセーブルにする必要があります。設定が完了したことを確認したあと、設定の同期化を再びイネーブルに設定します。

設定の同期化をディセーブルにするには、次のコマンドを入力します。

```
hostname(config)# failover suspend-config-sync
```

設定の同期化を再びイネーブルにするには、このコマンドの **no** 形式を使用します。

障害が発生した装置またはフェールオーバー グループの復元

障害が発生した装置を障害前のステートに復元するには、次のコマンドを入力します。

```
hostname(config)# failover reset
```

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 グループを障害前のステートに復元するには、次のコマンドを入力します。

```
hostname(config)# failover reset group group_id
```

障害が発生した装置またはグループを障害前のステートに復元しても、自動的にアクティブにはなりません。復元された装置またはグループは、フェールオーバー（強制実行または自然実行）によってアクティブにされるまで、スタンバイ ステートのままになります。**preempt** コマンドで設定されたフェールオーバー グループは例外です。前にアクティブであった場合、フェールオーバー グループが **preempt** コマンドで設定されていて、優先装置上で障害が発生したのであれば、このフェールオーバー グループはアクティブになります。

フェールオーバー動作のモニタ

フェールオーバーが実行されると、両方の FWSM からシステム メッセージが送信されます。ここでは、次の内容について説明します。

- フェールオーバー システム メッセージ（p.13-43）
- デバッグ メッセージ（p.13-44）
- SNMP（p.13-44）

フェールオーバー システム メッセージ

FWSM は、クリティカル状態を示すプライオリティ レベル 2 で、フェールオーバー関連のシステム メッセージを多数生成します。これらのメッセージを表示するには、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages*』を参照し、ロギングをイネーブルにして、システム メッセージの説明を参照してください。

(注) スイッチオーバーの過程では、フェールオーバーが論理的にシャット ダウンされて、インターフェイスが開かれ、システム ログ メッセージ 411001 および 411002 が生成されます。これが標準動作です。

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、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

(注) デバッグの出力は CPU 処理でハイ プライオリティが割り当てられているため、システム パフォーマンスに大きな影響を及ぼす可能性があります。このため、**debug fover** コマンドは、特定の問題のトラブルシューティングまたは Cisco TAC によるトラブルシューティング セッションを行う場合にのみ使用してください。

SNMP

フェールオーバーに関する SNMP の Syslog トラップを受信するには、SNMP エージェントから SNMP 管理ステーションに SNMP トラップを送信するように設定し、Syslog ホストを定義し、Cisco syslog MIB を SNMP 管理ステーションにコンパイルします。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **snmp-server** コマンドと **logging** コマンドを参照してください。

AAA サーバとローカル データベースの設定

この章では、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）（［トリプル A］と発音）のサポートと、AAA サーバおよびローカル データベースを設定する方法について説明します。

この章で説明する内容は、次のとおりです。

- AAA の概要（p.14-2）
- AAA サーバおよびローカル データベースのサポート（p.14-4）
- ローカル データベースの設定（p.14-11）
- AAA サーバ グループおよびサーバの識別（p.14-13）

AAA の概要

AAA により、FWSM はユーザの識別（認証）、ユーザが実行できる作業（許可）、ユーザが実行した作業（アカウンティング）を判別できます。

AAA は、アクセス リストだけを使用する場合よりも、ユーザ アクセスに関する保護および制御をさらに強化します。たとえば、すべての外部ユーザに対して、内部インターフェイス上のサーバへの Telnet アクセスを許可するアクセス リストを作成できますが、サーバへのアクセスを一部のユーザだけに限定する場合で、対象ユーザの IP アドレスが必ずしも明らかでないときには、AAA をイネーブルにして、認証または許可されたユーザだけに FWSM を通過させることができます（Telnet サーバは認証を実行しますが、FWSM は不正ユーザによるサーバへのアクセス試行を防止します）。

認証は単独で使用することも、許可およびアカウンティングと併用することもできます。許可を適用するには、最初にユーザを認証する必要があります。アカウンティングは単独で使用することも、認証および許可と併用することもできます。

複数のセキュリティ コンテキストを使用する場合、コンテキスト単位で別々に AAA を設定できますが、コンテキストの間で共有することはできません。そのため、アクセス制御、リソースとコマンドの許可、アカウンティングをコンテキスト間で別々に実行することができます。

次の内容について説明します。

- 認証の概要（p.14-2）
- 許可の概要（p.14-3）
- アカウンティングの概要（p.14-3）

認証の概要

認証では、有効な証明書（一般にはユーザ名とパスワード）を要求することによって、アクセスを制御します。FWSM では、次の項目の認証を設定できます。

- 次のセッションを含む、FWSM へのすべての管理接続：
  - 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

許可の概要

許可では、ユーザを認証したあと、*各ユーザ*のアクセスを制御できます。FWSM では、次の項目の許可を設定できます。

- 管理コマンド
- ネットワーク アクセス
- 管理接続用の VPN アクセス

認証された各ユーザが使用できるサービスとコマンドを許可によって制御することができます。許可をイネーブルにせずに認証だけを使用する場合、認証されたすべてのユーザに対し、サービスへのアクセスが一様に提供されます。

許可する内容を制御する必要がある場合は、広範囲の許可ルールを定義して、詳細な許可を設定できます。たとえば、内部ユーザを認証して外部ネットワークの任意サーバにアクセスできるようにしたあと、外部サーバへのアクセスを制限して、特定のユーザだけが許可を使用してアクセスできるように設定することができます。

FWSM は、ユーザごとに最初の 16 の許可要求をキャッシュします。したがって、ユーザが現在の許可セッション中に同じサービスにアクセスする場合は、FWSM から認証サーバに要求が再送信されることはありません。

アカウンティングの概要

アカウンティングでは、FWSM を通過するトラフィックを追跡し、ユーザ アクティビティを記録できます。トラフィックの認証をイネーブルにした場合は、ユーザごとにトラフィックをアカウントできます。トラフィックを認証しない場合は、IP アドレスごとにトラフィックをアカウントできます。アカウンティング情報には、セッションの開始時および終了時、ユーザ名、セッション中に FWSM を通過したバイト数、使用されたサービス、および各セッションの長さが含まれます。

AAA サーバおよびローカル データベースのサポート

FWSM は、さまざまな AAA サーバ タイプのほか、FWSM に保管されるローカル データベースをサポートします。ここでは、各 AAA サーバ タイプおよびローカル データベースのサポートについて説明します。

ここでは、次の内容について説明します。

- サポートの概要（p.14-4）
- RADIUS サーバのサポート（p.14-5）
- TACACS+ サーバのサポート（p.14-6）
- SDI サーバのサポート（p.14-7）
- NT サーバのサポート（p.14-8）
- Kerberos サーバのサポート（p.14-8）
- LDAP サーバのサポート（p.14-8）
- ローカル データベースのサポート（p.14-9）

サポートの概要

表 14-1 に、ローカル データベースを含めた、各 AAA サーバ タイプ別の AAA サービス タイプを説明します。特定の AAA サーバ タイプのサポートの詳細については、表の下の説明を参照してください。

表 14-1　AAA サポートのまとめ

	データベース タイプ						
AAA サービス	**ローカル**	**RADIUS**	**TACACS+**	**SDI**	**NT**	**Kerberos**	**LDAP**
認証 . .							
VPN ユーザ[1]	あり	あり	あり	あり	あり	あり	なし
ファイアウォール セッション	あり	あり	あり	なし	なし	なし	なし
管理者	あり	あり	あり	なし	なし	なし	なし
許可 . .							
VPN ユーザ[1]	あり	あり	なし	なし	なし	なし	あり
ファイアウォール セッション	なし	あり[2]	あり	なし	なし	なし	なし
管理者	あり[3]	なし	あり	なし	なし	なし	なし
アカウンティング . .							
VPN 接続[1]	なし	あり	あり	なし	なし	なし	なし
ファイアウォール セッション	なし	あり	あり	なし	なし	なし	なし
管理者	なし	なし	あり	なし	なし	なし	なし

1. VPN は管理接続の場合のみ、利用できます。
2. ファイアウォール セッションの場合、RADIUS 許可は、ユーザ指定のアクセス リストでのみサポートされます。アクセス リストは、Remote Authentication Dial-In User Service（RADIUS）認証応答で受信または指定されます。
3. ローカル コマンドによる許可はイネーブル レベルでのみ、サポートされます。

RADIUS サーバのサポート

FWSM は RADIUS サーバをサポートします。

ここでは、次の内容について説明します。

- 認証方法（p.14-5）
- 属性のサポート（p.14-5）
- RADIUS の機能（p.14-5）

認証方法

FWSM は、RADIUS を使用した次の認証方法をサポートします。

- PAP
- CHAP
- MS-CHAPv1
- MS-CHAPv2（パスワードの有効期限を含む）（IPSec ユーザ専用）

属性のサポート

FWSM は、次の RADIUS 属性をサポートします。

- RFC 2138 で定義された認証属性
- RFC 2139 で定義されたアカウンティング属性
- RFC 2868 で定義されたトンネル プロトコル サポートの RADIUS 属性
- Cisco IOS VSA（RADIUS ベンダー ID 9 で識別）
- Cisco VPN 関連 VSA（RADIUS ベンダー ID 3076 で識別）
- RFC 2548 で定義された Microsoft VSA

RADIUS の機能

FWSM は、表 14-2 に示す RADIUS サーバの機能を使用できます。

表 14-2　RADIUS の機能

機能	説明
CLI アクセスのユーザ認証	ユーザが Telnet、SSH、HTTP、またはシリアル コンソール接続を使用して FWSM へのアクセスを試み、トラフィックが認証ステートメントと一致すると、FWSM はユーザ名とパスワードを照合し、RADIUS サーバへ証明書を送信し、サーバからの応答に基づいてユーザの CLI アクセスを認可または拒否します。
enable コマンドのユーザ認証	ユーザが **enable** コマンドへのアクセスを試みると、FWSM はユーザのパスワードを照合して、ユーザ名とイネーブル パスワードを RADIUS サーバへ送信し、サーバからの応答に基づいてユーザ アクセスを認可または拒否して、モードをイネーブルにします。
ネットワーク アクセスのユーザ認証	ユーザが FWSM 経由でネットワークへのアクセスを試み、トラフィックが認証ステートメントと一致すると、FWSM は RADIUS サーバにユーザ証明書（通常ユーザ名とパスワード）を送信し、サーバからの応答に基づいてユーザのネットワーク アクセスを認可または拒否します。

表 14-2　RADIUS の機能（続き）

機能	説明
ユーザ単位のダイナミック ACL を使用したネットワーク アクセスのユーザ認証	ダイナミック アクセス リストを実行するには、RADIUS サーバがこの認証をサポートするように設定しておく必要があります。ユーザが認証されると、RADIUS サーバから FWSM にダウンロード可能なアクセス リストが送信されます。特定サービスへのアクセスは、このアクセス リストによって許可または拒否されます。認証セッションがタイムアウトになると、この アクセス リストは FWSM から削除されます。
ダウンロードしたユーザ単位の アクセス リスト名を使用したネットワーク アクセスのユーザ認証	ダウンロードしたアクセス リスト名を実行するには、RADIUS サーバがこの認証をサポートするように設定しておく必要があります。ユーザが認証されると、RADIUS サーバから、アクセス リストの名前が送信されます。指定された名前を含んだアクセス リストが FWSM に存在する場合、特定サービスへのアクセスは、このアクセス リストに基づいて許可または拒否されます。複数のユーザに同じ アクセス リスト を指定できます。
VPN 認証	ユーザが VPN を使用して管理接続の確立を試み、適用可能なトンネル グループ レコードが RADIUS 認証サーバ グループを指定する場合、FWSM は RADIUS サーバにユーザ名とパスワードを送信してから、サーバからの応答に基づいてユーザのアクセスを認可または拒否します。
VPN 許可	VPN アクセスのユーザ認証が成功し、適用可能なトンネル グループ レコードが RADIUS 許可サーバ グループを指定すると、FWSM は RADIUS 許可サーバに要求を送り、受信された許可を VPN セッションに適用します。
VPN アカウンティング	VPN アクセスのユーザ認証が成功し、適用可能なトンネル グループ レコードが RADIUS アカウンティング サーバ グループを指定すると、FWSM は VPN セッションに関する RADIUS サーバ グループ アカウンティング データを送信します。
ユーザまたは IP アドレスごとのネットワーク アクセスのアカウンティング	FWSM を通過する任意のトラフィックについて、FWSM から RADIUS サーバにアカウンティング情報を送信できます。

TACACS+ サーバのサポート

FWSM は、表 14-3 に示す Terminal Access Controller Access Control System Plus（TACACS+）サーバの機能を使用できます。FWSM は、ASCII、PAP、CHAP、MS-CHAPv1 を使用して TACACS+ 認証をサポートします。

表 14-3　TACACS+ 機能

機能	説明
CLI アクセスのユーザ認証	ユーザが Telnet、SSH、HTTP、またはシリアル コンソール接続を使用して FWSM へのアクセスを試み、トラフィックが認証ステートメントと一致すると、FWSM はユーザ名とパスワードを照合し、TACACS+ サーバへ証明書を送信し、サーバからの応答に基づいてユーザの CLI アクセスを認可または拒否します。
enable コマンドのユーザ認証	ユーザが **enable** コマンドへのアクセスを試みると、FWSM はユーザのパスワードを照合して、ユーザ名とイネーブル パスワードを TACACS+ サーバへ送信し、サーバからの応答に基づいてユーザ アクセスを認可または拒否して、モードをイネーブルにします。
CLI アクセスのアカウンティング	管理セッションに関するアカウンティング情報を TACACS+ サーバに送信するよう FWSM を設定できます。

表 14-3　TACACS+ 機能（続き）

機能	説明
ネットワーク アクセスのユーザ認証	ユーザが FWSM 経由でネットワークへのアクセスを試み、トラフィックが認証ステートメントと一致すると、FWSM は TACACS+ サーバにユーザ証明書（通常ユーザ名とパスワード）を送信し、サーバからの応答に基づいてユーザのネットワーク アクセスを認可または拒否します。
ネットワーク アクセスのユーザ許可	ユーザが認証後に FWSM 上の許可ステートメントと一致した場合、FWSM は TACACS+ サーバを使用してユーザのアクセス権限を照合します。
VPN 認証	ユーザが VPN を使用して管理接続の確立を試み、適用可能なトンネル グループ レコードが TACACS+ 認証サーバ グループを指定する場合、FWSM は TACACS+ サーバにユーザ名とパスワードを送信してから、サーバからの応答に基づいてユーザのアクセスを認可または拒否します。
VPN アカウンティング	VPN アクセスのユーザ認証が成功し、適用可能なトンネル グループ レコードが TACACS+ アカウンティング サーバ グループを指定すると、FWSM は VPN セッションに関する TACACS+ サーバ グループ アカウンティング データを送信します。
管理コマンドのユーザ許可	TACACS+ サーバ上で、CLI アクセスの認証後にユーザが使用できるコマンドを設定します。ユーザが CLI から入力したコマンドはすべて、TACACS+ サーバによって検証されます。
ユーザまたは IP アドレスごとのネットワーク アクセスのアカウンティング	FWSM を通過する任意のトラフィックについて、FWSM から TACACS+ サーバにアカウンティング情報を送信できます。

SDI サーバのサポート

FWSM では、RSA SecureID サーバを VPN 認証に使用できます。このサーバは、SDI サーバとして知られています。ユーザが VPN アクセスの確立を試み、適用可能なトンネル グループ レコードが SDI 認証サーバ グループを指定する場合、FWSM は SDI サーバにユーザ名と One Time Password（OTP; ワンタイム パスワード）を送信し、サーバからの応答に基づいてユーザのアクセスを認可または拒否します。

ここでは、次の内容について説明します。

- SDI バージョンのサポート（p.14-7）
- 2 段階の認証プロセス（p.14-8）
- SDI プライマリ サーバとレプリカ サーバ（p.14-8）

SDI バージョンのサポート

FWSM は、次の SDI バージョンをサポートします。

- **バージョン 5.0 以前のバージョン** — バージョン 5.0 以前の SDI バージョンでは、単一ノード シークレット ファイル（SECURID）を共有する SDI マスター サーバおよび SDI スレーブ サーバの概念を使用します。
- **バージョン 5.0** — SDI バージョン 5.0 では、SDI プライマリ サーバおよび SDI レプリカ サーバの概念を使用します。各プライマリ サーバとそのレプリカ サーバは、単一ノード シークレット ファイルを共有します。ノード シークレット ファイルには、.sdi を付加した ACE/Server IP アドレスの 16 進数の値に基づく名前が付けられています。

  FWSM 上で設定されたバージョン 5.0 の SDI サーバは、プライマリ サーバにも、レプリカ サーバのいずれにもすることができます。SDI エージェントがユーザを認証する方法については、次の 「SDI プライマリ サーバとレプリカ サーバ」（p.14-8）を参照してください。

2 段階の認証プロセス

SDI バージョン 5.0 は、2 段階のプロセスを使用して、侵入者が RSA SecurID 認証要求からの情報を得て別のサーバへの認証に使用するのを防ぎます。ユーザ認証要求を送信する前に、SDI エージェントはまず、SecurID サーバへのロック要求を送信します。サーバは、ユーザ名をロックし、別の（レプリカ）サーバがそのユーザ名を受け入れないようにします。そのため、同じユーザが同じ認証サーバを同時に使用して、2 台の FWSM に認証することができなくなります。ユーザ名を正常にロックできた場合、FWSM コンセントレータはパスコードを送信します。

SDI プライマリ サーバとレプリカ サーバ

最初のユーザが設定済みのサーバに認証すると、FWSM はサーバ リストを取得します。このときのサーバは、プライマリ サーバでもレプリカ サーバでも構いません。次に、FWSM は、リストにある各サーバに優先順位を割り当て、その優先順位からランダムにサーバを選択します。優先順位が一番高いサーバが、選択される可能性が高くなります。

NT サーバのサポート

FWSM は、NTLM バージョン 1 をサポートする Microsoft Windows サーバ オペレーティング システムで、VPN ベースの管理接続の認証をサポートします。Microsoft Windows サーバはまとめて NT サーバと呼びます。ユーザが VPN アクセスの確立を試み、適用可能なトンネル グループ レコードが NT 認証サーバ グループを指定する場合、FWSM は、Microsoft Windows ドメイン サーバでユーザ認証に NTLM バージョン 1 を使用します。FWSM は、ドメイン サーバからの応答に基づいてユーザのアクセスを認可または拒否します。

（注） NT サーバのユーザのパスワードは最長 14 文字です。15 文字めからは切り捨てられます。これは、NTLM バージョン 1 の制限事項です。

Kerberos サーバのサポート

FWSM は、VPN ベースの管理接続に Kerberos サーバを使用できます。ユーザが VPN アクセスの確立を試み、トラフィックが認証ステートメントと一致すると、FWSM は Kerberos サーバを使用してユーザ認証を照合し、サーバからの応答に基づいてユーザのネットワーク アクセスを認可または拒否します。

FWSM がサポートする暗号化タイプは、3DES、DES、RC4 です。

（注） FWSM は、トンネル ネゴシエーション時には、ユーザのパスワード変更をサポートしません。偶発的に起こるこの状況を回避するには、FWSM に接続するユーザに対して、Kerberos/Active Directory サーバ上でのパスワード有効期間を無効にしてください。

LDAP サーバのサポート

FWSM は、VPN ベースの管理接続に LDAP サーバを使用できます。VPN アクセスのユーザ認証が成功し、適用可能なトンネル グループ レコードが LDAP 許可サーバ グループを指定すると、FWSM は LDAP サーバに照会し、許可が受信された VPN セッションに適用されます。

ローカル データベースのサポート

FWSM は、ユーザ プロファイルが登録されたローカル データベースを維持します。

ここでは、次の内容について説明します。

- ユーザ プロファイル（p.14-9）
- ローカル データベースの機能（p.14-9）
- フォールバックのサポート（p.14-10）

ユーザ プロファイル

ユーザ プロファイルには、少なくともユーザ名が含まれます。パスワードの設定は任意ですが、通常は、各ユーザ名に割り当てられます。

username attributes コマンドを使用すると、username モードを開始できます。このモードでは、別の情報を特定のユーザ プロファイルに追加できます。追加可能な情報には、VPN 関連属性（VPN セッション タイムアウト値など）が含まれます。

ローカル データベースの機能

FWSM は、表 14-4 に示す ローカル データベースの機能を使用できます。

表 14-4　ローカル データベースの機能

機能	説明
CLI アクセスのユーザ認証	ユーザが Telnet、SSH、HTTP、またはシリアル コンソール接続を使用して FWSM へのアクセスを試み、トラフィックが認証ステートメントと一致すると、FWSM はユーザ名とパスワードを照合し、ローカル データベースに対して証明書を検証し、その結果に基づいてユーザの CLI アクセスを認可または拒否します。
enable コマンドまたは **login** コマンドのユーザ認証	ユーザが **enable** コマンドへのアクセスを試みると、FWSM はユーザのパスワードを照合して、ローカル データベースに対してユーザ名とパスワードを照合し、その結果に基づいてユーザ アクセスを認可または拒否して、モードをイネーブルにします。
管理コマンドのユーザ許可	**enable** コマンドで認証された（または **login** コマンドでログインした）ユーザは、FWSM により、ローカル データベースに定義されているイネーブル レベルに設定されます。各コマンドは、FWSM 上で 0 ～ 15 のイネーブル レベルに設定できます。
ネットワーク アクセスのユーザ認証	ユーザが FWSM 経由でネットワークへのアクセスを試み、トラフィックが認証ステートメントと一致すると、FWSM はユーザ名とパスワードを照合し、ローカル データベースに対して証明書を検証し、その結果に基づいてユーザの ネットワーク アクセスを認可または拒否します。
VPN 認証	ユーザが VPN を使用して管理接続の確立を試み、トラフィックが認証ステートメントと一致すると、FWSM はローカル ユーザ データベースに対して受信したユーザ名とパスワードを検証し、その結果に基づいて VPN アクセスを認可または拒否します。
VPN 許可	VPN アクセスのユーザ認証が成功すると、FWSM は、ユーザ名と適用可能なグループ ポリシーに対応付けられたローカル データベースからの属性を、VPN セッションに適用します。

フォールバックのサポート

ネットワーク アクセス認証のフォールバックは別として、ローカル データベースは 表 14-4 に記載された機能のフォールバック方式として動作します。フォールバックにより、FWSM からの意図しないロックアウトを回避することができます。

フォールバック サポートを必要とするユーザの場合、ローカル データベースのユーザ名とパスワードを AAA サーバのユーザ名とパスワードと一致させることを推奨します。これにより、透過的なフォールバック サポートが提供されます。ユーザは、AAA サーバまたはローカル データベースによってこのサービスが提供されているかどうかを判断できないため、ローカル データベースのものと異なる AAA サーバのユーザ名とパスワードを使用すると、ユーザは自分のユーザ名とパスワードが正しいのかどうか確信が持てなくなります。

ローカル データベースでは、次のフォールバック機能をサポートします。

- **コンソールおよびイネーブル パスワードの認証** — **aaa authentication console** コマンドを使用する場合、AAA サーバ グループ タグのあとに **LOCAL** キーワードを追加できます。すべてのグループのサーバが利用できない場合、FWSM 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。これにもイネーブル パスワードの認証を含めることができます。
- **コンソールの許可** — **aaa authorization command** コマンドを使用する場合、AAA サーバ グループ タグのあとに **LOCAL** キーワードを追加できます。すべてのグループの TACACS+ サーバが利用できない場合、ローカル データベースを使用して、イネーブル レベルに基づいてコマンドを許可します。
- **VPN 認証および許可** — VPN サービスを正常にサポートするはずの AAA サーバを利用できない場合、VPN 認証および許可がサポートされ、FWSM へのリモート アクセスからイネーブルになります。トンネル グループの一般属性モードで利用可能な **authentication-server-group** コマンドを使用する場合、トンネル グループの属性を設定するときに **LOCAL** キーワードを指定します。管理者の 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に設定されたトンネル グループを指定する場合、AAA サーバ グループを利用できなくても、ローカル データベースに必要な属性が設定されていれば、VPN トンネルを確立できます。

ローカル データベースの設定

ここでは、ローカル データベース内のユーザを管理する手順について説明します。ローカル データベースは、CLI アクセスの認証、イネーブル モードの認証、コマンドの許可、ネットワーク アクセスの認証、VPN の認証および許可に使用できます。ネットワーク アクセスの許可にローカル データベースを使用することはできません。ローカル データベースでは、アカウンティングはサポートされません。

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ユーザ名を設定し、**login** コマンドによって個別ログインを提供できますが、システム実行スペースには **aaa** コマンドを設定することはできません。

注意　CLI へのアクセスが許可され、イネーブル モードの使用が許可されないユーザをローカル データベースに追加する場合は、コマンド許可をイネーブルにします（「ローカル コマンド許可の設定」[p.21-16] を参照）。コマンド許可を使用しない場合、イネーブル レベルが 2 以上（2 はデフォルト値）のユーザは、個人のパスワードを使用して CLI のイネーブル モード（およびすべてのコマンド）にアクセスできます。別の方法としては、RADIUS または TACACS+ 認証を使用してユーザが **login** コマンドを使用できないように設定するか、またはすべてのローカル ユーザをレベル 1 に設定してから、システム イネーブル パスワードを使用してイネーブル モードにアクセスできるユーザを制御します。

ローカル データベースにユーザ アカウントを定義する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、ユーザ アカウントを作成します。

```
hostname/contexta(config)# username username {nopassword | password password}
[encrypted] [privilege level]
```

オプションは次のとおりです。

- *username* — 4 ～ 64 文字の長さの文字列を指定します。
- **password** *password* — 3 ～ 16 文字の長さの文字列を指定します。
- **encrypted** — 指定のパスワードが暗号化されていることを示します。
- **privilege** *level* — 新しいユーザ アカウントに割り当てるイネーブル レベル（0 ～ 15）を指定します。デフォルトは 2 です。イネーブル レベルはコマンド許可と併用します。
- **nopassword** — パスワードを使用しないユーザ アカウントを作成します。

ステップ 2　VPN 属性を持ったローカル ユーザ アカウントを定義する手順は、次のとおりです。

a.　次のコマンドを入力します。

```
hostname/contexta(config)# username username attributes
```

username attributes コマンドを入力すると、username モードが開始されます。このモードで利用できるコマンドは、次のとおりです。

- **group-lock**
- **password-storage**
- **vpn-access-hours**
- **vpn-filter**

- **vpn-framed-ip-address**
- **vpn-group-policy**
- **vpn-idle-timeout**
- **vpn-session-timeout**
- **vpn-simultaneous-logins**
- **vpn-tunnel-protocol**

このコマンドを必要に応じて使用して、ユーザ プロファイルを設定してください。このコマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

b. ユーザ プロファイルの設定を終了する場合、**exit** を入力してコンフィギュレーション モードに戻ります。

次に、admin ユーザのアカウントにイネーブル レベル 15 を割り当てる例を示します。

```
hostname/contexta(config)# username admin password passw0rd privilege 15
```

次に、パスワードを許可しないユーザ アカウントを作成する例を示します。

```
hostname/contexta(config)# username bcham34 nopassword
```

次のコマンドはパスワードのあるユーザ アカウントを作成し、username モードを開始し、2 ～ 3 の VPN 属性を指定します。

```
hostname/contexta(config)# username rwilliams password gOgeOus
hostname/contexta(config)# username rwilliams attributes
hostname/contexta(config-username)# vpn-tunnel-protocol IPSec
hostname/contexta(config-username)# vpn-simultaneous-logins 6
hostname/contexta(config-username)# exit
```

AAA サーバ グループおよびサーバの識別

認証、許可、またはアカウンティングに外部の AAA サーバを使用する場合は、まず、AAA プロトコルごとに 1 つまたは複数の AAA サーバ グループを作成し、各グループに 1 つまたは複数のサーバを追加します。AAA サーバ グループは名前ごとに識別します。各サーバ グループは、Kerberos、LDAP、NT、RADIUS、SDI、または TACACS+ のそれぞれのサーバ タイプで固有です。

FWSM は、グループ内の最初のサーバと通信します。最初のサーバが使用できない場合、FWSM はグループ内の次のサーバ（設定されている場合）と通信します。グループ内のすべてのサーバが使用できない場合、フォールバック方式としてローカル データベースが設定されていれば、FWSM はローカル データベースと通信します（管理認証および許可のみ）。フォールバック方式が設定されていない場合、FWSM は AAA サーバとの通信を継続的に試みます。

サーバ グループを作成し AAA サーバを追加する手順は、次のとおりです。

ステップ 1　作成する必要のある各 AAA サーバ グループには、次の手順を実行します。

a. サーバ グループ名およびプロトコルを識別します。そのためには、次のコマンドを入力します。

```
hostname/contexta(config)# aaa-server server_group protocol {kerberos | ldap | nt |
radius | sdi | tacacs+}
```

たとえば、RADIUS を使用してネットワーク アクセスを認証したり、TACACS+ を使用して CLI アクセスを認証したりするには、2 つ以上のサーバ グループ（1 つは RADIUS サーバ用、1 つは TACACS+ サーバ用）を作成する必要があります。

最大 15 個のシングル モード サーバ グループまたは 4 個のマルチ モード サーバ グループを作成できます。各サーバ グループには、シングル モードで最大 16 個のサーバ、またはマルチ モードで最大 4 個のサーバを含めることが可能です。

aaa-server protocol コマンドを入力すると、グループ モードが開始されます。

b. 次のサーバに移行する前に、グループ内の 1 つの AAA サーバに送信する要求の最大数を指定するには、次のコマンドを入力します。

```
hostname/contexta(config-aaa-server-group)# max-failed-attempts number
```

number の範囲は、1 ～ 5 です。デフォルトは 3 です。

ローカル データベースを使用するフォールバック方式（管理アクセスのみに使用。フォールバック機能の設定方法については 「システム管理者用の AAA」[p.21-13] および 「TACACS+ コマンド許可の設定」[p.21-20] を参照）を設定した場合は、グループ内のすべてのサーバが応答に失敗すると、そのグループは応答不可とみなされ、フォールバック方式が試行されます。サーバ グループが応答不可としてマークされる時間は 10 分間（デフォルト）です。その間、追加の AAA 要求はサーバ グループには送信されず、ただちにフォールバック方式が採用されます。応答不可の時間をデフォルト以外に変更する場合は、次の **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、FWSM はグループ内のサーバへの通信を継続的に試みます。

c. グループ内の失敗したサーバを再開する方法（再開ポリシー）を指定するには、**reactivation-mode** コマンドを使用します。このコマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

d. アカウンティング メッセージを単一 サーバに送信するか（シングル モード）、グループ内のすべてのサーバに送信するか（Simultaneous モード）を指定する場合、**accounting-mode** コマンドを使用します。このコマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

e. AAA サーバ グループの設定を終了する場合、**exit** を入力します。

ステップ 2　使用するネットワークの各 AAA サーバの場合、手順は次のとおりです。

a. AAA サーバが所属する AAA サーバ グループを含め、サーバを識別します。そのためには、次のコマンドを入力します。

```
hostname/contexta(config)# aaa-server server_group (interface_name) host server_ip
```

aaa-server host コマンドを入力すると、host モードを開始します。

b. host モード コマンドを必要に応じて使用し、AAA サーバを設定ください。

host モードのコマンドは、AAA サーバ タイプすべてに適用されるわけではありません。表 14-5 に、使用できるコマンド、適用されるサーバ タイプ、新しい AAA サーバ定義にコマンドのデフォルト値があるかどうか示します。指定したサーバ タイプにコマンドを適用でき、デフォルト値がない（[—] で表示）場合、次のコマンドを使用して値を指定します。このコマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

表 14-5　host モード コマンド、サーバ タイプ、デフォルト値

コマンド	適用可能な AAA サーバ タイプ	デフォルト値
accounting-port	RADIUS	1646
authentication-port	RADIUS	1645
kerberos-realm	Kerberos	—
key	RADIUS	—
	TACACS+	—
ldap-base-dn	LDAP	—
ldap-login-dn	LDAP	—
ldap-login-password	LDAP	—
ldap-naming-attribute	LDAP	—
ldap-scope	LDAP	—
nt-auth-domain-controller	NT	—
radius-common-pw	RADIUS	—
retry-interval	Kerberos	10 秒
	RADIUS	10 秒
sdi-pre-5-slave	SDI	—
sdi-version	SDI	sdi-5
server-port	Kerberos	88
	LDAP	389
	NT	139
	SDI	5500
	TACACS+	49
timeout	すべて	10 秒

c. AAA サーバ ホストの設定を終了するには、**exit** を入力します。

たとえば、プライマリ サーバとバックアップ サーバを 1 つずつ指定した 1 つの TACACS+ グループ、単一サーバを指定した 1 つの RADIUS グループ、1 つの NT ドメイン サーバを追加するには、次のコマンドを入力します。

```
hostname/contexta(config)# aaa-server AuthInbound protocol tacacs+
hostname/contexta(config-aaa-server-group)# max-failed-attempts 2
hostname/contexta(config-aaa-server-group)# reactivation-mode depletion deadtime 20
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server AuthInbound (inside) host 10.1.1.1
hostname/contexta(config-aaa-server-host)# key TACPlusUauthKey
hostname/contexta(config-aaa-server-host)# exit
hostname/contexta(config)# aaa-server AuthInbound (inside) host 10.1.1.2
hostname/contexta(config-aaa-server-host)# key TACPlusUauthKey2
hostname/contexta(config-aaa-server-host)# exit
hostname/contexta(config)# aaa-server AuthOutbound protocol radius
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
hostname/contexta(config-aaa-server-host)# key RadUauthKey
hostname/contexta(config-aaa-server-host)# exit
hostname/contexta(config)# aaa-server NTAuth protocol nt
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server NTAuth (inside) host 10.1.1.4
hostname/contexta(config-aaa-server-host)# nt-auth-domain-controller primary1
hostname/contexta(config-aaa-server-host)# exit
```

ネットワーク アクセスへの AAA の適用

この章では、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）（［トリプル A］と発音）をネットワーク アクセスに対してイネーブルにする方法を説明します。

管理アクセスの AAA の詳細については、「システム管理者用の AAA」（p.21-13）を参照してください。

この章で説明する内容は、次のとおりです。

- AAA パフォーマンス（p.15-1）
- ネットワーク アクセスの認証の設定（p.15-2）
- ネットワーク アクセスの許可の設定（p.15-7）
- ネットワーク アクセスのアカウンティングの設定（p.15-12）
- MAC アドレスを使用した認証および許可からのトラフィックの除外（p.15-13）

AAA パフォーマンス

FWSM では、「カットスルー プロキシ」を採用することによって、従来のプロキシ サーバに比べてパフォーマンスが著しく改善されています。従来のプロキシ サーバは、Open Systems Interconnection（OSI; 開放型システム間相互接続）モデルのアプリケーション レイヤですべてのパケットを分析するので、パフォーマンスが損なわれます。FWSM のカットスルー プロキシは、最初にアプリケーション レイヤでユーザを照合したあと、標準の Remote Authentication Dial-In User Service（RADIUS）、Terminal Access Controller Access Control System Plus（TACACS+）、またはローカル データベースを使用して認証を行います。FWSM でユーザが認証されてからセッション フローに移行するので、すべてのトラフィックが送信元と宛先の間で直接かつ迅速に伝送され、セッション ステート情報も保持されます。

ネットワーク アクセスの認証の設定

ここでは、次の内容について説明します。

- 認証の概要（p.15-2）
- ネットワーク アクセス認証のイネーブル化（p.15-3）
- Web クライアントのセキュア認証のイネーブル化（p.15-4）
- プロトコル単位の認証チャレンジのディセーブル化（p.15-6）

認証の概要

FWSM では、AAA サーバを使用したネットワーク アクセス認証を設定できます。

特定の IP アドレスのユーザに必要な認証は、認証セッションがタイムアウトになるまでは、すべてのルールとタイプに対して 1 回だけです（タイムアウトの値については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **timeout uauth** コマンドを参照してください）。たとえば、FWSM に Telnet と FTP の認証を設定した場合、ユーザは最初に Telnet の認証に成功すれば、そのセッションの継続中は FTP の認証を受ける必要はありません。

任意のプロトコルまたはサービスについてネットワーク アクセスの認証を必要とするよう FWSM を設定できますが、HTTP、Telnet、または FTP に限り、認証を直接設定できます。FWSM が認証を必要とする他のトラフィックを許可する前に、ユーザはまず、これらのサービスのいずれかで認証される必要があります。

FWSM を経由する HTTP、Telnet、または FTP を許可せずに、他のタイプのトラフィックを認証する場合には、仮想 Telnet を設定できます。この場合、ユーザが FWSM 上に設定された指定の IP アドレスに Telnet 接続すると、FWSM に Telnet プロンプトが表示されます。**virtual telnet** コマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

Telnet、HTTP、FTP の場合、FWSM によって認証プロンプトが生成されます。宛先サーバに独自の認証が設定されている場合には、ユーザは別途ユーザ名とパスワードを入力することになります。

（注） **aaa authentication secure-http-client** コマンドを使用せずに HTTP 認証を行うと、ユーザ名とパスワードはクリア テキストで宛先 Web サーバに送信され、AAA サーバには送信されません。たとえば、外部の Web サーバにアクセスする内部ユーザを認証する場合、外部の者は誰でも有効なユーザ名とパスワードを学習できます。HTTP 認証をイネーブルにするときは、**aaa authentication secure-http-client** コマンドを使用することを推奨します。

FTP の場合、FWSM のユーザ名のあとにアットマーク（@）を入力し、続けて FTP ユーザ名を入力できます（name1@name2）。パスワードの場合も、FWSM のパスワードのあとにアットマーク（@）を入力し、さらに FTP パスワードを入力します（password1@password2）。次に、例を示します。

```
name> terryc@jchrichton
password> letmein@he110
```

この機能は、ファイアウォールをカスケード接続して設定し、複数のログインが必要となる場合に便利です。複数の名前とパスワードを、複数のアットマーク（@）で区切ることができます。

ネットワーク アクセス認証のイネーブル化

ネットワーク アクセス認証をイネーブルにする手順は、次のとおりです。

ステップ 1　**aaa-server** コマンドを使用して、AAA サーバを識別します。すでに AAA サーバを識別している場合、次の手順を行います。

AAA サーバの識別の詳細については、「AAA サーバ グループおよびサーバの識別」（p.14-13）を参照してください。

ステップ 2　**access-list** コマンドを使用して、認証したいトラフィックの送信元アドレスおよび宛先アドレスを識別するアクセス リストを作成します。手順については、「拡張アクセス リストの追加」（p.10-7）を参照してください。

permit Access Control Entry（ACE; アクセス制御エントリ）は一致するトラフィックを認証し、**deny** エントリは一致するトラフィックの認証を拒否します。アクセス リストには HTTP、Telnet、または FTP のいずれかの宛先ポートを必ず指定してください。ユーザは、FWSM 経由の他のサービスの許可を得る前に、これらのサービスのいずれかで認証される必要があるからです。

ステップ 3　認証を設定するには、次のコマンドを入力します。

```
hostname/contexta(config)# aaa authentication match acl_name interface_name
server_group
```

acl_name は ステップ 2 で作成したアクセス リストの名前です。*interface_name* は **nameif** コマンドで指定されたインターフェイスの名前です。*server_group* は ステップ 1 で作成した AAA サーバ グループです。

（注）　**aaa authentication include** コマンド（コマンド内でトラフィックを識別する）を使用することもできます。ただし、同じ設定で両方の方法を使用することはできません。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

ステップ 4　（任意）ネットワーク アクセス認証にローカル データベースを使用していて、FWSM がいずれのユーザ アカウントに対しても、連続して失敗できるログイン試行回数を制限する場合、**aaa local authentication attempts max-fail** コマンドを使用します。次に、例を示します。

```
hostname/contexta(config)# aaa local authentication attempts max-fail 7
```

ヒント　特定のユーザまたはすべてのユーザのロックアウト ステータスをクリアするには、**clear aaa local user lockout** コマンドを使用します。

次に、すべての内部 HTTP トラフィックおよび SMTP トラフィックを認証する例を示します。

```
hostname/contexta(config)# aaa-server AuthOutbound protocol tacacs+
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server AuthOutbound (inside) host 10.1.1.1
hostname/contexta(config-aaa-server-host)# key TACPlusUauthKey
hostname/contexta(config-aaa-server-host)# exit
hostname/contexta(config)# access-list MAIL_AUTH extended permit tcp any any eq smtp
hostname/contexta(config)# access-list MAIL_AUTH extended permit tcp any any eq www
hostname/contexta(config)# aaa authentication match MAIL_AUTH inside AuthOutbound
```

次に、外部インターフェイスから特定サーバ（209.165.201.5）への Telnet トラフィックを認証する例を示します。

```
hostname/contexta(config)# aaa-server AuthInbound protocol tacacs+
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server AuthInbound (inside) host 10.1.1.1
hostname/contexta(config-aaa-server-host)# key TACPlusUauthKey
hostname/contexta(config-aaa-server-host)# exit
hostname/contexta(config)# access-list TELNET_AUTH extended permit tcp any host
209.165.201.5 eq telnet
hostname/contexta(config)# aaa authentication match TELNET_AUTH outside AuthInbound
```

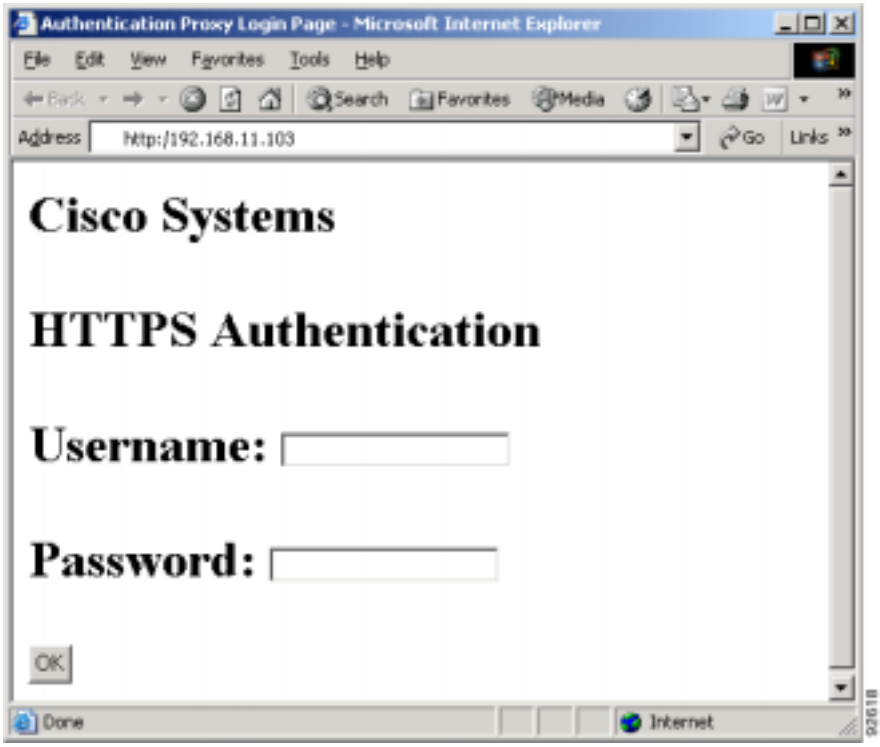
Web クライアントのセキュア認証のイネーブル化

FWSM は、安全に HTTP 認証を行う方法を提供します。HTTP 認証を保護しないと、FWSM に提供されたユーザ名とパスワードは宛先 Web サーバに転送されます。

aaa authentication secure-http-client コマンドを使用すると、Web クライアントおよび HTTPS 認証を設定した FWSM の間でユーザ名とパスワードを交換できます。HTTPS により伝送が暗号化され、ユーザ名とパスワードが HTTP によって外部 Web サーバに転送されるのを回避します。

この機能をイネーブルにした場合、認証を必要とする Web ページにユーザがアクセスすると、図 15-1 に示す Authentication Proxy Login ページが FWSM によって表示されます。

図 15-1　Authentication Proxy Login ページ



(注) この画面に表示されている Cisco Systems のテキスト フィールドは、**auth-prompt** コマンドを使用して変更できます。このコマンドの詳細な構文については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。**auth-prompt** コマンドを使用してテキストを指定しない場合、このフィールドは空白になります。

有効なユーザ名とパスワードを入力すると、「Authentication Successful」（認証成功）のページが表示され、自動的に終了します。ユーザ名とパスワードが無効の場合には、「Authentication Failed」（認証失敗）のページが表示されます。

セキュア Web クライアントの認証には次の制限があります。

- 最大 16 の同時 HTTPS 認証セッションがサポートされます。最大 16 の HTTPS 認証プロセスが実行されている場合、認証を必要とする新しい接続は失敗します。
- **uauth timeout 0** が設定されている（**uauth timeout** が 0 に設定されている）場合、HTTPS 認証は機能しないことがあります。HTTPS 認証後、ブラウザが Web ページをロードするために複数の TCP 接続を開始した場合、最初の接続は許可されますが、以降の接続に対しては認証が発生します。その結果、正しいユーザ名とパスワードを入力しても、認証ページが継続的に表示されることになります。この問題を回避するには、**timeout uauth 0:0:1** コマンドを使用して、**uauth timeout** を 1 秒に設定してください。ただし、ウィンドウが 1 秒間オープンしているため、同じ送信元 IP アドレスからアクセスする未認証のユーザが、ファイアウォールを通過する可能性があります。

- HTTPS 認証は SSL ポート 443 で実行されるので、ポート 443 で HTTP クライアントから HTTP サーバへのトラフィックをブロックするように **access-list** コマンド ステートメントを設定しないでください。また、ポート 80 に Web トラフィック用のスタティック PAT を設定する場合には、SSL ポートにもスタティック PAT を設定する必要があります。次の例では、1 行めで Web トラフィックに対してスタティック PAT を設定しているため、2 行めを追加して、HTTPS 認証設定をサポートする必要があります。

```
static (inside,outside) tcp 10.132.16.200 www 10.130.16.10 www
static (inside,outside) tcp 10.132.16.200 443 10.130.16.10 443
```

- **aaa authentication secure-http-client** が設定されていない場合、HTTP ユーザには、ブラウザが生成するポップアップ ウィンドウが表示されます。**aaa authentication secure-http-client** が設定されている場合、ブラウザのフォームがロードされると、ユーザ名とパスワードが収集されます。また、ユーザの入力したパスワードが誤っている場合では、ユーザは再入力を求められます。Web サーバと認証サーバがそれぞれ別のホスト上にある場合、正常な認証処理を実行するには **virtual** コマンドを使用します。

Web クライアントのセキュアな認証をイネーブルにする手順は、次のとおりです。

ステップ 1　HTTP 認証をイネーブルにします。認証のイネーブル化の詳細については、「ネットワーク アクセス認証のイネーブル化」（p.15-3）を参照してください。

ステップ 2　Web クライアントのセキュアな認証をイネーブルにするには、次のコマンドを入力します。

```
aaa authentication secure-http-client
```

（注）　**aaa authentication secure-http-client** コマンドの使用は、HTTP 認証のイネーブル化に依存しません。あとで HTTP 認証をイネーブルにしたときに、セキュア Web クライアント認証によってユーザ名とパスワードが保護されているようにするには、HTTP 認証をイネーブルにする前にこのコマンドを入力します。

プロトコル単位の認証チャレンジのディセーブル化

FWSM がユーザに対し、ユーザ名とパスワードの照合を行うかどうかを設定できます。デフォルトでは、AAA ルールが新しいセッションでトラフィックの認証を強化し、トラフィックのプロトコルが FTP、Telnet、HTTP、または HTTPS である場合、FWSM はユーザに指示を出します。1 つまたは複数のプロトコルの認証照合をディセーブルにする場合は、**aaa authentication** コマンドを使用できます。

```
hostname/contexta(config)# aaa authentication protocol challenge disable
```

たとえば、FTP を使用して新しい接続のためのユーザ名とパスワードの照合をディセーブルにするには、次のコマンドを入力します。

```
hostname/contexta(config)# aaa authentication ftp challenge disable
```

特定のプロトコルの認証照合をディセーブルにした場合、そのプロトコルを使用するトラフィックは、以前に認証されたセッションに属している場合にのみ、許可されます。この認証は、認証照合がイネーブルであるプロトコルを使用したトラフィックによって実行されます。たとえば、FTP の認証照合をディセーブルにすると、トラフィックが許可ルールに指定されている場合、FWSM は FTP を使用する新しいセッションを拒否します。ユーザが、認証照合がイネーブルであるプロトコル（HTTP など）を使用してセッションを確立する場合、FTP トラフィックは許可されます。

ネットワーク アクセスの許可の設定

特定の接続についてユーザが認証されると、FWSM はユーザからのトラフィックをさらに制御する許可を使用できます。

次の内容について説明します。

- TACACS+ 許可の設定（p.15-7）
- RADIUS 許可の設定（p.15-8）

TACACS+ 許可の設定

TACACS+ を使用したネットワーク アクセス許可を実行するよう FWSM を設定することができます。許可ルールと一致する必要のあるアクセス リストを指定することで、許可するトラフィックを識別します。または、許可ルール内で直接、トラフィックを識別します。

ヒント　許可するトラフィックを、アクセス リストを使用して識別すると、入力しなければならない許可コマンドの数を大幅に減らすことができます。これにより、許可ルールに指定できる送信元と宛先のサブネットおよびサービスは 1 つだけですが、アクセス リストには複数のエントリを指定できます。

認証および許可ステートメントは独立していますが、認証されないトラフィックが許可ステートメントと一致しても拒否されます。許可されるには、ユーザはまず、FWSM で認証される必要があります。特定の IP アドレスのユーザに必要な認証は、認証セッションがタイムアウトになるまでは、すべてのルールとタイプに対して 1 回だけなので、トラフィックが許可ステートメントと一致すれば許可できます。

ユーザの認証後、FWSM はトラフィックが許可ルールに一致しているかどうかを検証します。トラフィックが許可ステートメントに一致すると、FWSM から TACACS+ サーバにユーザ名が送信されます。TACACS+ サーバは、ユーザのプロファイルに基づいて、そのトラフィックの許可または拒否の応答を FWSM に戻します。FWSM は応答における許可ルールを強化します。

ユーザのネットワーク アクセス許可の設定の詳細については、TACACS+ サーバのマニュアルを参照してください。

TACACS+ 許可を設定する手順は、次のとおりです。

ステップ 1　認証をイネーブルにします。詳細については、「ネットワーク アクセス認証のイネーブル化」（p.15-3）を参照してください。すでに認証をイネーブルにしている場合は、次の手順を行います。

ステップ 2　**access-list** コマンドを使用して、許可するトラフィックの送信元アドレスおよび宛先アドレスを識別するアクセス リストを作成します。手順については、「拡張アクセス リストの追加」（p.10-7）を参照してください。

permit ACE は一致するトラフィックを許可し、**deny** エントリは一致するトラフィックの許可を拒否します。許可の一致に使用するアクセス リストには、認証の一致に使用するアクセス リストのルールと同じか、またはそのサブセットを含んでいる必要があります。

（注） 認証を設定して、認証されるトラフィックをすべて許可する場合、**aaa authentication match** コマンドを使用して作成した同じアクセス リストを使用できます。

ステップ 3　許可をイネーブルにするには、次のコマンドを入力します。

```
hostname/contexta(config)# aaa authorization match acl_name interface_name
server_group
```

acl_name は ステップ 2 で作成したアクセス リストの名前です。*interface_name* は **nameif** コマンドで指定されたインターフェイスの名前、またはデフォルトのインターフェイスの名前です。*server_group* は 認証をイネーブルにしたときに作成した AAA サーバ グループです。

（注） **aaa authorization include** コマンド（コマンド内でトラフィックを識別する）を使用することもできますが、同じ設定で両方の方法を使用することはできません。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

次に、内部 Telnet トラフィックを認証し、許可する例を示します。209.165.201.5 以外のサーバへの Telnet トラフィックは認証されるだけですが、209.165.201.5 へのトラフィックには許可が必要です。

```
hostname/contexta(config)# access-list TELNET_AUTH extended permit tcp any any eq
telnet
hostname/contexta(config)# access-list SERVER_AUTH extended permit tcp any host
209.165.201.5 eq telnet
hostname/contexta(config)# aaa-server AuthOutbound protocol tacacs+
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server AuthOutbound (inside) host 10.1.1.1
hostname/contexta(config-aaa-server-host)# key TACPlusUauthKey
hostname/contexta(config-aaa-server-host)# exit
hostname/contexta(config)# aaa authentication match TELNET_AUTH inside AuthOutbound
hostname/contexta(config)# aaa authorization match SERVER_AUTH inside AuthOutbound
```

RADIUS 許可の設定

認証が成功すると、RADIUS プロトコルは、RADIUS サーバによって送信されたアクセス許可パケットにユーザ許可を戻します。認証の設定の詳細については、「ネットワーク アクセスの認証の設定」（p.15-2）を参照してください。

ネットワークにアクセスするユーザを認証するよう FWSM を設定した場合、RADIUS 許可を暗黙でイネーブルにできますが、ここでは FWSM 上で RADIUS 許可を設定する詳細については説明しません。FWSM が RADIUS サーバから受信したアクセス リスト情報を処理する方法について説明します。

RADIUS サーバを設定し、認証時に FWSM にアクセス リストまたはアクセス リスト名をダウンロードできます。ユーザに実行できるのは、ユーザ指定のアクセス リストで許可された内容だけです。

（注）**access-group** コマンドを使用してアクセス リストをインターフェイスに適用した場合、**per-user-override** キーワードは、ユーザ指定のアクセス リストによる許可に与える以下の影響について注意してください。

- **per-user-override** キーワードを使用しない場合、ユーザ セッションのトラフィックは、インターフェイス アクセス リストとユーザ指定のアクセス リスト両方によって許可される必要があります。
- **per-user-override** キーワードを使用する場合、ユーザ指定のアクセス リストが許可の内容を判別します。

詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **access-group** コマンド エントリを参照してください。

ここでは、次の内容について説明します。

- RADIUS サーバからユーザごとの ACL をダウンロードする設定（p.15-9）
- RADIUS サーバからユーザごとの ACL 名をダウンロードする設定（p.15-11）

RADIUS サーバからユーザごとの ACL をダウンロードする設定

ここでは、Cisco Secure ACS RADIUS サーバまたはサードパーティ製の RADIUS サーバの設定手順について説明します。内容は次のとおりです。

- Cisco Secure ACS RADIUS サーバでのダウンロード可能なアクセス リストの設定（p.15-9）
- RADIUS サーバでのダウンロード可能なアクセス リストの設定（p.15-10）

Cisco Secure ACS RADIUS サーバでのダウンロード可能なアクセス リストの設定

Cisco Secure ACS に共有プロファイル コンポーネントとしてダウンロード可能なアクセス リストを設定し、グループまたは個人ユーザにアクセス リストを割り当てることができます。

アクセス リストの定義には、拡張 **access-list** コマンドと同様の 1 つまたは複数の FWSM コマンドを設定します。ただし、次のプレフィクスは不要です。

```
access-list acl_name extended
```

次に、Cisco Secure ACS バージョン 3.3 でダウンロード可能なアクセス リストの例を示します。

```
+-------------------------------------------+
| Shared profile Components                 |
|                                           |
|      Downloadable IP ACLs Content         |
|                                           |
| Name:    acs_ten_acl                      |
|                                           |
|      ACL Definitions                      |
|                                           |
| permit tcp any host 10.0.0.254            |
| permit udp any host 10.0.0.254            |
| permit icmp any host 10.0.0.254           |
| permit tcp any host 10.0.0.253            |
| permit udp any host 10.0.0.253            |
| permit icmp any host 10.0.0.253           |
| permit tcp any host 10.0.0.252            |
| permit udp any host 10.0.0.252            |
| permit icmp any host 10.0.0.252           |
| permit ip any any                         |
+-------------------------------------------+
```

ダウンロード可能なアクセス リストの作成、およびユーザへの対応付けに関する詳細については、Cisco Secure ACS のバージョンに対応するユーザ マニュアルを参照してください。

FWSM にダウンロードしたアクセス リストは、次の名前になります。

```
#ACSACL#-ip-acl_name-number
```

acl_name 引数は Cisco Secure ACS で定義された名前です（前の例では、acs_ten_acl）。*number* は Cisco Secure ACS によって生成された固有のバージョン ID です。

FWSM にダウンロードしたアクセス リストには、次の行が含まれます。

```
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.254
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.254
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.254
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.253
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.253
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.253
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.252
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.252
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.252
access-list #ACSACL#-ip-xxx-acs_ten_acl-3b5385f7 permit ip any any
```

RADIUS サーバでのダウンロード可能なアクセス リストの設定

Cisco IOS RADIUS VSA をサポートする RADIUS サーバを、Cisco IOS RADIUS cisco-av-pair VSA（VSA 番号 1）の FWSM にユーザ固有のアクセス リストを送信するよう設定します。Cisco IOS RADIUS VSA は、RADIUS ベンダー ID 9 で識別されます。

cisco-av-pair VSA では、**access-list extended** コマンドと同様の 1 つまたは複数の ACE を設定してください。ただし、次のコマンド プレフィクスは、

access-list *acl_name* **extended**

次のテキストに置換されます。

ip:inacl#*nnn***=**

nnn 引数は、FWSM に設定するコマンド ステートメントの順序を表す 0 ～ 999,999,999 の範囲の数値です。このパラメータを省略すると、シーケンス値は 0 になり、cisco-av-pair RADIUS VSA 内の ACE の順序が使用されます。

次に、RADIUS サーバで cisco-av-pair VSA 用に設定する必要があるアクセス リスト定義の例を示します。

```
ip:inacl#1=permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
ip:inacl#99=deny tcp any any
ip:inacl#2=permit udp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
ip:inacl#100=deny udp any any
ip:inacl#3=permit icmp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
```

cisco-av-pair アトリビュートで送信されるアクセス リストのユーザ別の設定については、RADIUS サーバのマニュアルを参照してください。

FWSM にダウンロードしたアクセス リスト名は、次の形式になります。

```
AAA-user-username
```

username 引数 は、認証されるユーザの名前です。

FWSM にダウンロードしたアクセス リストには、次の行が含まれます。順序が、RADIUS サーバ上の番号に基づいていることに注意してください。

```
access-list  AAA-user-bcham34-79AD4A08 permit tcp 10.1.0.0 255.0.0.0 10.0.0.0
255.0.0.0
access-list  AAA-user-bcham34-79AD4A08 permit udp 10.1.0.0 255.0.0.0 10.0.0.0
255.0.0.0
access-list  AAA-user-bcham34-79AD4A08 permit icmp 10.1.0.0 255.0.0.0 10.0.0.0
255.0.0.0
access-list  AAA-user-bcham34-79AD4A08 deny tcp any any
access-list  AAA-user-bcham34-79AD4A08 deny udp any any
```

ダウンロードしたアクセス リストでは、access-list と名前の間に 2 つのスペースが挿入されます。これらのスペースにより、ダウンロードしたアクセス リストとローカル アクセス リストを区別できます。この例での 79AD4A08 は、RADIUS サーバ上でアクセス リスト定義が変更されたときを判別するため、FWSM によって生成されたハッシュ値です。

RADIUS サーバからユーザごとの ACL 名をダウンロードする設定

ユーザ認証時に、FWSM ですでに作成されているアクセス リストの名前をダウンロードするには、IETF RADIUS filter-id アトリビュート（アトリビュート 11）を次のように設定します。

filter-id=*acl_name*

（注） Cisco Secure ACS では、filter-id アトリビュートの値は HTML インターフェイスのボックスで指定され、**filter-id=** は省略され *acl_name* のみ入力します。

filter-id アトリビュート値のユーザ別の設定については、RADIUS サーバのマニュアルを参照してください。

FWSM でのアクセス リストの作成手順については、「拡張アクセス リストの追加」（p.10-7）を参照してください。

ネットワーク アクセスのアカウンティングの設定

FWSM では、FWSM を通過する任意の TCP/UDP トラフィックについて、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できます。トラフィックが認証されている場合は、AAA サーバでユーザ名ごとにアカウンティング情報を保持できます。トラフィックが認証されていない場合、AAA サーバで IP アドレスごとにアカウンティング情報を保持できます。アカウンティング情報には、セッションの開始時および終了時、ユーザ名、セッション中に FWSM を通過したバイト数、使用されたサービス、および各セッションの長さが含まれます。

アカウンティングを設定する手順は、次のとおりです。

ステップ 1　FWSM にユーザごとにアカウンティング データを提供させる場合、認証をイネーブルにする必要があります。詳細については、「ネットワーク アクセス認証のイネーブル化」（p.15-3）を参照してください。FWSM に IP アドレスごとにアカウンティング データを提供させる場合、認証をイネーブルにする必要はなく、次の手順を続行します。

ステップ 2　**access-list** コマンドを使用して、アカウント対象のトラフィックの送信元アドレスおよび宛先アドレスを識別するアクセス リストを作成します。手順については、「拡張アクセス リストの追加」（p.10-7）を参照してください。

permit ACE は一致するトラフィックを許可し、**deny** エントリは一致するトラフィックの許可を拒否します。

（注）　認証を設定して、認証されるすべてのトラフィックのデータをアカウントする場合、**aaa authentication match** コマンドを使用して作成した同じアクセス リストを使用できます。

ステップ 3　アカウン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。

```
hostname/contexta(config)# aaa accounting match acl_name interface_name server_group
```

（注）　**aaa accounting include** コマンド（コマンド内でトラフィックを識別する）を使用することもできますが、同じ設定で両方の方法を使用することはできません。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

次に、内部 Telnet トラフィックの AAA を設定する例を示します。209.165.201.5 以外のサーバへの Telnet トラフィックは認証されるだけですが、209.165.201.5 へのトラフィックには許可およびアカウンティングが必要です。

```
hostname/contexta(config)# aaa-server AuthOutbound protocol tacacs+
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server AuthOutbound (inside) host 10.1.1.1
hostname/contexta(config-aaa-server-host)# key TACPlusUauthKey
hostname/contexta(config-aaa-server-host)# exit
hostname/contexta(config)# access-list TELNET_AUTH extended permit tcp any any eq
telnet
hostname/contexta(config)# access-list SERVER_AUTH extended permit tcp any host
209.165.201.5 eq telnet
hostname/contexta(config)# aaa authentication match TELNET_AUTH inside AuthOutbound
hostname/contexta(config)# aaa authorization match SERVER_AUTH inside AuthOutbound
hostname/contexta(config)# aaa accounting match SERVER_AUTH inside AuthOutbound
```

MAC アドレスを使用した認証および許可からのトラフィックの除外

FWSM は、特定の MAC アドレスのトラフィックを認証および許可の対象から除外できます。

たとえば、FWSM は特定のネットワークから発信される TCP トラフィックを認証しますが、特定のサーバから未認証の TCP 接続を許可したい場合、**mac-list** コマンドを使用してサーバの MAC アドレスからのトラフィックを許可するルールを作成してから、**aaa mac-exempt** コマンドを使用して MAC リストによって指定されたサーバのトラフィックを認証および許可の対象から除外します。

逆に、認証したにもかかわらず特定のコンピュータからのトラフィックは許可したくない場合、そのコンピュータの **mac-list** コマンドの MAC アドレスを使用できます。この事例の **aaa mac-exempt** コマンドを使用すると、このコンピュータからのトラフィックは許可ルールによって許可されても、アクセスを拒否されます。

MAC アドレスを使用して、認証および許可からトラフィックを除外する手順は、次のとおりです。

ステップ 1　MAC リストを設定するには、次のコマンドを入力します。

```
hostname/contexta(config)# mac-list id {deny | permit} mac macmask
```

id は MAC リストに付けたアルファベットの文字列です。*mac* は許可または拒否するトラフィックのコンピュータの MAC アドレスです。*macmask* は MAC アドレス マスクです。**mac-list** コマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

ステップ 2　特定の MAC リストで指定された MAC アドレスのトラフィックを除外するには、次のコマンドを入力します。

```
hostname/contexta(config)# aaa mac-exempt match id
```

id は MAC アドレスを含んだ MAC リストを識別する文字列です。このトラフィックは、認証および許可の対象から除外する必要があります。

次のコマンドは、それぞれ 1 個の MAC アドレスで構成された 2 つの MAC リストを作成します。MAC リストの 1 つは MAC アドレスのトラフィックを許可し、もう 1 つは拒否します。最後の 2 つのコマンドを使用すると、FWSM が 2 つのリスト内の MAC アドレスから発信されるトラフィックを認証および許可から除外するように設定します。

```
hostname/contexta(config)# mac-list adc permit 00a0.cp5d.0282 ffff.ffff.ffff
hostname/contexta(config)# mac-list ac deny 0061.54ff.b440 ffff.ffff.ffff
hostname/contexta(config)# aaa mac-exempt match adc
hostname/contexta(config)# aaa mac-exempt match ac
```

フィルタリング サービスの適用

この章では、Web トラフィックをフィルタリングして、セキュリティ リスクを低減し、不適切な使用を回避する方法について説明します。この章で説明する内容は、次のとおりです。

- フィルタリングの概要（p.16-1）
- ActiveX オブジェクトのフィルタリング（p.16-2）
- Java アプレットのフィルタリング（p.16-4）
- 外部サーバによる URL および FTP 要求のフィルタリング（p.16-5）
- フィルタリングの統計情報とフィルタリング設定の表示（p.16-11）

フィルタリングの概要

ここでは、フィルタリングが FWSM を通過するトラフィックをより制御できる方法について説明します。フィルタリングは次の 2 つの方法に使用できます。

- ActiveX オブジェクトまたは Java アプレットのフィルタリング
- 外部フィルタリング サーバを使用した URL のフィルタリング

アクセスを一緒にブロックしないで、特定の不適切なオブジェクト（ActiveX オブジェクトまたは Java アプレットなど）を HTTP トラフィックから削除できます。これは、所定の状況でセキュリティ リスクが発生させることがあります。

URL フィルタリングを使用して、特定のトラフィックを N2H2 Sentian または Websense フィルタリング サーバなどの外部フィルタリング サーバへ転送できます。フィルタリング サーバは、セキュリティ ポリシーで指定された特定のサイトへのトラフィック、またはサイト タイプへのトラフィックをブロックできます。

URL フィルタリングは CPU 中心なので、外部フィルタリング サーバを使用すると、他のトラフィックのスループットは影響を受けません。ただし、ネットワーク速度と URL フィルタリング サーバのキャパシティに応じて、外部フィルタリング サーバを使用してトラフィックをフィルタリングするときに、初期接続に必要な時間は著しく遅くなります。

ActiveX オブジェクトのフィルタリング

ここでは、フィルタリングを適用して、ファイアウォールを通過する HTTP トラフィックから ActiveX オブジェクトを削除する手順について説明します。次の内容について説明します。

- ActiveX フィルタリングの概要（p.16-2）
- ActiveX フィルタリングのイネーブル化（p.16-2）

ActiveX フィルタリングの概要

ActiveX オブジェクトには保護されたネットワーク上のホストやサーバを攻撃する目的のコードが含まれているので、セキュリティ リスクを発生させることがあります。ActiveX フィルタリングを使用して ActiveX オブジェクトをディセーブルにできます。

ActiveX コントロール（従来の OLE コントロールまたは OCX コントロール）は、Web ページまたはその他のアプリケーションに挿入できるコンポーネントです。これらのコントロールには、カスタム フォーム、カレンダー、または情報の収集と表示に使用するサード パーティ製の広範ななフォームが含まれています。ActiveX は、技術的に、ネットワーク クライアントに対して多くの問題を発生させる可能性があります。たとえば、ワークステーションの障害の原因となる、ネットワーク セキュリティ問題を引き起こす、サーバへの攻撃に利用されるなどの恐れがあります。

filter activex コマンドは、HTML <object> コマンドを HTML Web ページ内でコメントアウトすることでブロックします。HTML ファイルの ActiveX のフィルタリングは、<APPLET> タグ、</APPLET> タグ、<OBJECT CLASSID> タグ、</OBJECT> タグを選別し、コメントで置き換えることによって実行されます。ネストされたタグのフィルタリングは、最上位タグをコメントに変換することによってサポートされます。

注意　このコマンドは、オブジェクト タグに組み込まれた Java アプレット、イメージ ファイル、またはマルチメディア オブジェクトもブロックします。

<object> または </object> HTML タグがネットワーク パケットに分割されている場合、またはタグ内のコードが Maximum Transmission Unit（MTU; 最大伝送ユニット）のバイト数より長い場合、FWSM はそのタグをブロックできません。

ActiveX ブロックは、ユーザが ***alias*** コマンドによって参照される IP アドレスにアクセスしている場合は実行されません。

ActiveX フィルタリングのイネーブル化

ここでは、FWSM を通過する HTTP トラフィック内の ActiveX オブジェクトを削除する方法について説明します。ActiveX オブジェクトを削除するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

```
hostname(config)# filter activex {port[-port] | except} local_ip local_mask foreign_ip
foreign_mask
```

このコマンドを使用するには、フィルタリングを適用する TCP ポートに *port* を置き換えます。一般的には、これはポート 80 ですが、他の値は受け入れられます。**http** または **url** の文字列はポート 80 に使用できます。開始ポート番号と終了ポート番号の間にハイフンを使用することでポート範囲を指定できます。

以前のフィルタリング条件の例外を作成するには、キーワード **except** を指定します。

ローカル IP アドレスとマスクは、フィルタリングされるトラフィックの送信元である 1 つまたは複数の内部ホストを識別します。外部アドレスとマスクは、フィルタリングされるトラフィックの外部宛先を指定します。

すべてのホストを指定するには、いずれかのアドレスを **0.0.0.0**（または短縮形 **0**）に設定します。すべてのホストを指定するには、いずれかのマスクとして **0.0.0.0**（または短縮形 **0**）を使用します。

次に、すべての発信接続で ActiveX オブジェクトをブロックする例を示します。

```
hostname(config)# filter activex 80 0 0 0 0
```

このコマンドは、ActiveX オブジェクト ブロックが、あらゆるローカル ホストからあらゆる外部ホストへのポート 80 の Web トラフィックに対して、適用されることを指定しています。

この設定を削除するには、次の例のように、このコマンドの **no** 形式を使用します。

```
hostname(config)# no filter activex 80 0 0 0 0
```

Java アプレットのフィルタリング

ここでは、フィルタリングを適用して、ファイアウォールを通過する HTTP トラフィックから Java アプレットを削除する手順について説明します。Java アプレットには保護されたネットワーク上のホストやサーバを攻撃する目的のコードが含まれているので、セキュリティ リスクを発生させることがあります。**filter java** コマンドを使用して、Java アプレットを削除できます。

filter java コマンドは、発信接続から FWSM へ戻る Java アプレットをフィルタリングします。それでもユーザは HTML ページを受信できますが、Java アプレットの Web ページの発信元がコメントアウトされるため、アプレットは実行できなくなります。

(注) <object> タグに組み込まれた Java アプレットを削除するには、**filter activex** コマンドを使用します。

FWSM を通過する HTTP トラフィック内の Java アプレットを削除するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

```
hostname(config)# filter java {port[-port] | except} local_ip local_mask foreign_ip
foreign_mask
```

このコマンドを使用するには、フィルタリングを適用する TCP ポートに *port* を置き換えます。一般的には、これはポート 80 ですが、他の値は受け入れられます。**http** または **url** の文字列はポート 80 に使用できます。開始ポート番号と終了ポート番号の間にハイフンを使用することでポート範囲を指定できます。

以前のフィルタリング条件の例外を作成するには、キーワード **except** を指定します。

ローカル IP アドレスとマスクは、フィルタリングされるトラフィックの送信元である 1 つまたは複数の内部ホストを識別します。外部アドレスとマスクは、フィルタリングされるトラフィックの外部宛先を指定します。

すべてのホストを指定するには、いずれかのアドレスを **0.0.0.0**（または短縮形 **0**）に設定します。すべてのホストを指定するには、いずれかのマスクとして **0.0.0.0**（または短縮形 **0**）を使用します。

すべてのホストを指定するには、アドレスを **0.0.0.0**（または短縮形 **0**）に設定します。すべてのホストを指定するには、マスクとして **0.0.0.0**（または短縮形 **0**）を使用します。

次に、すべての発信接続で Java アプレットをブロックする例を示します。

```
hostname(config)# filter java 80 0 0 0 0
```

このコマンドは、Java アプレット ブロックが、あらゆるローカル ホストからあらゆる外部ホストへのポート 80 の Web トラフィックに対して、適用されることを指定しています。

次に、保護されたネットワーク上のホストに Java アプレットがダウンロードされないようにする例を示します。

```
hostname(config)# filter java http 192.168.3.3 255.255.255.255 0 0
```

このコマンドは、ホスト 192.168.3.3 による Java アプレットのダウンロードをブロックします。

この設定を削除するには、次の例のように、このコマンドの **no** 形式を使用します。

```
hostname(config)# no filter java http 192.168.3.3 255.255.255.255 0 0
```

外部サーバによる URL および FTP 要求のフィルタリング

ここでは、外部サーバによる URL および FTP 要求をフィルタリングする手順について説明します。次の内容について説明します。

- URL フィルタリングの概要（p.16-5）
- フィルタリング サーバの指定（p.16-5）
- コンテンツ サーバの応答のバッファリング（p.16-6）
- サーバ アドレスのキャッシング（p.16-7）
- HTTP URL のフィルタリング（p.16-8）
- HTTPS URL のフィルタリング（p.16-9）
- FTP 要求のフィルタリング（p.16-10）

URL フィルタリングの概要

安全性の高いネットワークから安全性の低いネットワークへの接続要求にフィルタリングを適用できます。アクセス リストを使用して、特定のコンテンツ サーバへの発信アクセスを阻止できますが、インターネットの規模およびダイナミック特性を考慮すると、この方法での使用の管理は困難です。次のいずれかのインターネット フィルタリング製品で稼働する別途サーバを使用することで、設定を簡素化し、FWSM のパフォーマンスを向上できます。

- HTTP、HTTPS、FTP のフィルタリング用 Websense Enterprise
- HTTP のフィルタリング専用の N2H2 による Sentian（一部の Sentian バージョンは HTTPS をサポートしていますが、FWSM がサポートしているのは Sentian の HTTP フィルタリングだけです）。

外部サーバを使用するときは FWSM のパフォーマンスはほとんど影響を受けませんが、フィルタリング サーバが FWSM から離れた場所にある場合には、Web サイトまたは FTP サーバへのアクセス時間が大幅に長くなることがあります。

フィルタリングがイネーブルで、接続要求を FWSM 経由で転送すると、その要求はコンテンツ サーバとフィルタリング サーバに同時に送信されます。フィルタリング サーバによって接続が許可されると、FWSM はコンテンツ サーバからの応答を、発信元のクライアントに転送します。フィルタリング サーバが接続を拒否した場合、FWSM は応答を廃棄し、接続が成功しなかったことを示すメッセージまたはリターン コードを送信します。

認証が FWSM 上でイネーブルの場合、FWSM はまたユーザ名をフィルタリング サーバに送信します。フィルタリング サーバで、ユーザ名のフィルタリング設定を使用するか、使用に関する拡張レポート機能を提供できます。

フィルタリング サーバの指定

各コンテキストに最大 4 つのフィルタリング サーバを指定できます。FWSM は、サーバから応答が得られるまで、各サーバを順番に使用します。コンフィギュレーションに指定できるサーバは、1 つのタイプ（Websense または N2H2）だけです。

（注） **filter** コマンドで HTTP または HTTPS のフィルタリングを設定するには、事前にフィルタリング サーバを追加する必要があります。コンフィギュレーションからフィルタリング サーバを削除すると、すべての **filter** コマンドも一緒に削除されます。

url-server コマンドを使用してフィルタリング サーバのアドレスを指定します。

Websense の場合は次のとおりです。

```
hostname(config)# url-server (if_name) host local_ip [timeout seconds] [protocol TCP
connections number| UDP version 1|4]
```

N2H2 の場合は次のとおりです。

```
hostname(config)# url-server (if_name) vendor n2h2 host local_ip[:port number]
[timeout seconds] [protocol TCP connections number | UDP]
```

if_name には、フィルタリング サーバに接続される FWSM インターフェイスの名前を指定します。*local_ip* には、フィルタリング サーバの IP アドレスを指定します。*seconds* には、FWSM がフィルタリング サーバへの接続を試行する秒数を指定します。

(注) デフォルト ポートは 4005 です。これは、TCP または UDP 経由で FWSM と通信するのに N2H2 サーバが使用するデフォルト ポートです。デフォルト ポートの変更の詳細については、『*Filtering by N2H2 Administrator's Guide*』を参照してください。

たとえば、1 つの Websense フィルタリング サーバを指定するには、次のコマンドを入力します。

```
hostname(config)# url-server (perimeter) host 10.0.1.1 protocol TCP version 4
```

このコマンドは、Websense フィルタリング サーバに FWSM の境界インターフェイス上の IP アドレス 10.0.1.1 を指定します。バージョン 4 ではキャッシングがサポートされているので、この例では Websense はイネーブルであるバージョン 4 を推奨します。

冗長 N2H2 Sentian サーバを指定するには、次のコマンドを入力します。

```
hostname(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
hostname(config)# url-server (perimeter) vendor n2h2 host 10.0.1.2
```

このコマンドは、FWSM の境界インターフェイス上で 2 つの Sentian フィルタリング サーバを指定します。

コンテンツ サーバの応答のバッファリング

ユーザが コンテンツ サーバへの接続要求を発行すると、FWSM はその要求を コンテンツ サーバとフィルタリング サーバに同時に送信します。フィルタリング サーバがコンテンツ サーバより先に応答しなかった場合、サーバからの応答は廃棄されます。これにより、Web クライアントは要求を再発行する必要があるので、Web クライアントからの Web サーバの応答が遅れます。

HTTP 応答バッファをイネーブルにすることにより、Web コンテンツ サーバからの応答はバッファリングされ、フィルタリング サーバによって接続が許可された場合に、要求クライアントに転送されます。これにより、他の遅延の発生を回避します。

HTTP または FTP 要求への応答のバッファリングを設定する手順は、次のとおりです。

ステップ 1　フィルタリング サーバからの応答が保留中である HTTP または FTP 要求に対する応答のバッファリ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。

```
hostname(config)# url-block block block-buffer-limit
```

block-buffer-limit に、バッファリングするブロックの最大数を指定します。

（注）　1159 バイトより長い URL のバッファリングは、Websense フィルタリング サーバでのみサポートされています。

ステップ 2　保留中の URL のバッファリング（および Websense による長い URL のバッファリング）に使用できる最大メモリを設定するには、次のコマンドを入力します。

```
hostname(config)# url-block url-mempool memory-pool-size
```

memory-pool-size に、最大メモリ割り当ての 2 KB ～ 10 MB に相当する 2 ～ 10240 の値を指定します。

サーバ アドレスのキャッシング

ユーザがサイトにアクセスしたあと、宛先アドレスでホスティングされている全サイトが常時許可されるカテゴリに含まれていれば、フィルタリング サーバは一定時間、FWSM にサーバ アドレスのキャッシュを許可できます。これにより、ユーザが同じサーバに再アクセスしたり、別のユーザが同じサーバにアクセスした場合、FWSM からフィルタリング サーバに再度、問い合わせる必要がありません。

（注）　キャッシュされている IP アドレスへの要求は、フィルタリング サーバに転送されないのでロギングされません。その結果、これらの動作は記録されません。***url-cache*** コマンドを使用する前に、Websense 実行ログを蓄積できます。

スループットを高める必要がある場合は、次のように **url-cache** コマンドを使用します。

```
hostname(config)# url-cache {dst | src_dst} size
```

size に、1 ～ 128 KB 範囲のキャッシュ サイズの値を指定します。

URL 宛先アドレスに基づいて、エントリをキャッシュするには、***dst*** キーワードを使用します。すべてのユーザが Websense サーバ上で同一の URL フィルタリング ポリシーを共有している場合に、このモードを選択します。

URL 要求を開始した発信元アドレスと URL 宛先アドレスの両方に基づいて、エントリをキャッシュするには、***src_dst*** キーワードを使用します。ユーザが Websense サーバ上で同一の URL フィルタリング ポリシーを共有していない場合に、このモードを選択します。

HTTP URL のフィルタリング

ここでは、外部フィルタリング サーバを使用して HTTP フィルタリングを設定する手順について説明します。次の内容について説明します。

- HTTP フィルタリングの設定（p.16-8）
- 長い HTTP URL のフィルタリングのイネーブル化（p.16-8）
- 長い HTTP URL の短縮（p.16-9）
- フィルタリングから除外するトラフィックを指定（p.16-9）

HTTP フィルタリングの設定

HTTP フィルタリングをイネーブルにする前に、URL フィルタリング サーバを指定およびイネーブルにする必要があります。

フィルタリング サーバが HTTP 接続要求を許可すると、FWSM は Web サーバからの応答を発信元のクライアントに到達させます。フィルタリング サーバによって応答が拒否された場合、FWSM はアクセスが拒否されたことを示すブロック ページにユーザをリダイレクトします。

HTTP フィルタリ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。

```
hostname(config)# filter url [http | port[-port] | except} local_ip local_mask
foreign_ip foreign_mask] [allow] [proxy-block]
```

HTTP（80）のデフォルト ポートとは異なるポートが使用されている場合、*port* に、1 つまたは複数のポート番号を指定します。*local_ip* と *local_mask* には、要求を行うユーザまたはサブネットワークの IP アドレスとサブネット マスクを指定します。*foreign_ip* と *foreign_mask* には、要求に応答するサーバまたはサブネットワークの IP アドレスとサブネット マスクを指定します。

以前のフィルタリング条件の例外を作成するには、キーワード **except** を指定します。

allow オプションは、プライマリ フィルタリング サーバが利用できないときに、FWSM がフィルタリングせずに HTTP トラフィックを転送するようにします。プロキシ サーバへの要求をすべて廃棄するには、***proxy-block*** コマンドを使用します。

長い HTTP URL のフィルタリングのイネーブル化

デフォルトでは、FWSM は、1159 文字を超える長さの HTTP URL を長い URL であるとみなします。Websense サーバの場合、最大長を増加できます。

（Websense のみ）次のコマンドを入力して、1 つの URL の最大サイズを設定します。

```
hostname(config)# url-block url-size long_url_size
```

long_url_size に、最大 URL サイズの 2 ～ 4 KB に相当する 2 ～ 4 の値を指定します。デフォルト値は 2 です。

（Websense のみ）次のコマンドを入力して、URL バッファ メモリ プールの最大サイズを設定することもできます。

```
hostname(config)# url-block url-mempool memory_pool_size
```

memory_pool_size に、URL バッファ メモリ プール サイズの 2 ～ 10,240 KB に相当する 2 ～ 10240 の値を指定します。

長い HTTP URL の短縮

最大許可サイズを超える URL は、デフォルトでは廃棄されます。これを回避するには、次のコマンドを入力して、長い URL を短縮するように FWSM を設定できます。

```
hostname(config)# filter url [longurl-truncate | longurl-deny | cgi-truncate]
```

URL が最大許可長を超えている場合、**longurl-truncate** オプションを指定すると、フィルタリング サーバで評価するために、FWSM は URL のホスト名または IP アドレスの部分だけを送信します。URL が最大許可長を超えている場合、**longurl-deny** オプションを指定すると、発信 URL トラフィックは拒否されます。

cgi-truncate オプションを指定すると、CGI URL を、CGI スクリプトの場所およびスクリプト名（パラメータは含まない）だけになるように短縮します。長い HTTP 要求の多くは、CGI 要求です。パラメータ リストが非常に長い場合、パラメータ リストを含む完全な CGI 要求を待機および送信すると、メモリ リソースが浪費され、ファイアウォールのパフォーマンスに影響します。

フィルタリングから除外するトラフィックを指定

フィルタリングから除外する特定のトラフィックを指定するには、次のコマンドを入力します。

```
hostname(config)# filter url except source_ip source_mask dest_ip dest_mask
```

たとえば、次のコマンドを使用すると、10.0.2.54 からの要求を除く、すべての HTTP 要求をフィルタリング サーバに転送します。

```
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

HTTPS URL のフィルタリング

HTTPS フィルタリングをイネーブルにする前に、URL フィルタリング サーバを指定およびイネーブルにする必要があります。

（注） HTTPS URL のフィルタリングは、Websense フィルタリング サーバでのみサポートされています。

HTTPS コンテンツは暗号化されているため、FWSM からフィルタリング サーバに送信される URL 検索には、ディレクトリおよびファイル名の情報は含まれません。フィルタリング サーバが HTTPS 接続要求を許可すると、FWSM は SSL 接続ネゴシエーションを完了させ、Web サーバからの応答を発信元のクライアントに到達させます。フィルタリング サーバが要求を拒否すると、FWSM は SSL 接続ネゴシエーションの完了を阻止します。ブラウザには、「The Page or the content cannot be displayed.（ページまたはコンテンツを表示できません）」などのエラー メッセージが表示されます。

（注） FWSM は HTTPS 用に認証プロンプトを提供しないので、HTTPS サーバにアクセスする前に、HTTP または FTP を使用して FWSM でまずユーザを認証する必要があります。

HTTPS フィルタリ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。

```
hostname(config)# filter https port localIP local_mask foreign_IP foreign_mask [allow]
```

HTTPS（443）のデフォルト ポートとは異なるポートが使用されている場合、*port* に、ポート番号を指定します。

（注） HTTPS と HTTP トラフィックの両方に同じ GET 要求がある場合、HTTPS プロトコル インスペクタも指定したポート番号上の HTTP トラフィックをフィルタリングします。

local_ip と *local_mask* には、要求を行うユーザまたはサブネットワークの IP アドレスとサブネット マスクを指定します。*foreign_ip* と *foreign_mask* には、要求に応答するサーバまたはサブネットワークの IP アドレスとサブネット マスクを指定します。

allow オプションは、プライマリ フィルタリング サーバが利用できないときに、FWSM がフィルタリングせずに HTTPS トラフィックを転送するようにします。

FTP 要求のフィルタリング

FTP フィルタリングをイネーブルにする前に、URL フィルタリング サーバを指定およびイネーブルにする必要があります。

（注） FTP URL のフィルタリングは、Websense フィルタリング サーバでのみサポートされています。

フィルタリング サーバが FTP 接続要求を許可すると、FWSM は成功を示す FTP リターン コードを発信元のクライアントに到達させます。たとえば、「250: CWD command successful.」は成功したリターン コードです。フィルタリング サーバが要求を拒否した場合、接続が拒否されたことを示すため FTP リターン コードを変更します。たとえば、FWSM は、コード 250 を「550 Requested file is prohibited by URL filtering policy.」に変更します。

FTP フィルタリ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。

```
hostname(config)# filter ftp {port[-port] | except} localIP local_mask foreign_IP
foreign_mask [allow] [interact-block]
```

FTP（21）のデフォルト ポートとは異なるポートが使用されている場合、*port* に、ポート番号を指定します。*local_ip* と *local_mask* には、要求を行うユーザまたはサブネットワークの IP アドレスとサブネット マスクを指定します。*foreign_ip* と *foreign_mask* には、要求に応答するサーバまたはサブネットワークの IP アドレスとサブネット マスクを指定します。

以前のフィルタリング条件の例外を作成するには、キーワード **except** を指定します。

allow オプションは、プライマリ フィルタリング サーバが利用できないときに、FWSM がフィルタリングせずに FTP トラフィックを転送するようにします。

interact-block オプションを指定すると、完全なディレクトリ パスが提供されないインタラクティブ FTP セッションが阻止されます。インタラクティブ FTP クライアントにより、完全なパスを入力しなくてもディレクトリを変更できます。たとえば、**cd /public/files** ではなく、**cd ./files** を入力します。

フィルタリングの統計情報とフィルタリング設定の表示

ここでは、フィルタリングの統計情報をモニタする手順について説明します。次の内容について説明します。

- フィルタリング サーバの統計情報の表示（p.16-11）
- バッファ設定とバッファ統計情報の表示（p.16-11）
- キャッシングの統計情報の表示（p.16-12）
- フィルタリング パフォーマンスの統計情報の表示（p.16-12）
- フィルタリング設定の表示（p.16-12）

フィルタリング サーバの統計情報の表示

フィルタリング サーバに関する情報を表示するには、次のコマンドを入力します。

```
hostname# show running-config url-server
```

次に、**show url-server** コマンドの出力例を示します。

```
hostname# show running-config url-server
url-server (outside) vendor n2h2 host 128.107.254.202 port 4005 timeout 5 protocol TCP
```

フィルタリング サーバの情報または統計情報を表示するには、次のコマンドを入力します。

次に、フィルタリングの統計情報を表示する **show url-server** コマンドの出力例を示します。

```
hostname# show url-server
URL Server Statistics:
----------------------
Vendor                           websense
URLs total/allowed/denied        50/35/15
HTTPSs total/allowed/denied      1/1/0
FTPs total/allowed/denied        3/1/2

URL Server Status:
------------------
10.130.28.18            UP

URL Packets Sent and Received Stats:
------------------------------------
Message                 Sent    Received
STATUS_REQUEST          65155   34773
LOOKUP_REQUEST          0       0
LOG_REQUEST             0       NA
------------------------------------
```

バッファ設定とバッファ統計情報の表示

show running-config url-block コマンドは、url-block バッファで保持されるパケット数と、バッファ制限を超えた場合または再送信が発生した場合に廃棄される数（存在する場合）を示します。

次に、**show running-config url-block** コマンドの出力例を示します。

```
hostname# show running-config url-block
    url-block url-mempool 128
    url-block url-size 4
    url-block block 128
```

この出力では、URL ブロック バッファの設定が表示されています。

次に、**show url-block** コマンドの出力例を示します。

```
hostname# show url-block

URL Pending Packet Buffer Stats with max block  128
----------------------------------------------------
Cumulative number of packets held:              896
Maximum number of packets held (per URL):       3
Current number of packets held (global):        38
Packets dropped due to
       exceeding url-block buffer limit:        7546
       HTTP server retransmission:              10
Number of packets released back to client:      0
```

この出力では、URL ブロックの統計情報が表示されています。

キャッシングの統計情報の表示

次に、**show url-cache** コマンドの出力例を示します。

```
hostname# show url-cache
URL Filter Cache Stats
----------------------
    Size :     128KB
 Entries :      1724
  In Use :       456
 Lookups :        45
    Hits :         8
```

この出力では、キャッシュがどのように使用されているかが表示されています。

フィルタリング パフォーマンスの統計情報の表示

次に、**show perfmon** コマンドの出力例を示します。

```
hostname# show perfmon
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          2/s
TCP Conns            0/s          2/s
UDP Conns            0/s          0/s
URL Access           0/s          2/s
URL Server Req       0/s          3/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          3/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
```

この出力では、URL フィルタリング パフォーマンスの統計情報、および他のパフォーマンスの統計情報が表示されています。フィルタリング統計情報は、URL Access および URL Server Req の行に表示されています。

フィルタリング設定の表示

次に、**show running-config filter** コマンドの出力例を示します。

```
hostname# show running-config filter
filter url http 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

ARP 検査およびブリッジング パラメータの設定

透過ファイアウォール モード限定

この章では、Address Resolution Protocol（ARP; アドレス解決プロトコル）検査をイネーブルにし、FWSM 用にブリッジング動作をカスタマイズする方法について説明します。マルチコンテキスト モードでは、この章のコマンドはセキュリティ コンテキストに入力できますが、システムには入力できません。

この章で説明する内容は、次のとおりです。

- ARP 検査の設定（p.17-2）
- MAC アドレス テーブルのカスタマイズ（p.17-4）

ARP 検査の設定

ここでは、ARP 検査および ARP 検査をイネーブルにする方法について説明します。

- ARP 検査の概要（p.17-2）
- スタティック ARP エントリの追加（p.17-2）
- ARP 検査のイネーブル化（p.17-3）

ARP 検査の概要

デフォルトでは、すべての ARP パケットが FWSM を通過できます。ARP 検査をイネーブルにすると、ARP パケットのフローを制御できます。ARP 検査はすべてのブリッジ グループに適用されます。

ARP 検査をイネーブルにすると、FWSM 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 エントリと照合して、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 エントリと一致した場合、パケットを通過させます。
- MAC アドレス、IP アドレス、または送信元インターフェイスが一致しない場合、FWSM はそのパケットを廃棄します。
- ARP パケットのエントリがスタティック ARP テーブルのエントリと 1 つも一致しなかった場合に、FWSM がそのパケットをすべてのインターフェイスに転送するように（フラッディング）設定するか、またはパケットを廃棄するように設定できます。

ARP 検査によって、不正なユーザが他のホストまたはルータになりすます（ARP スプーフィング）ことを防止できます。ARP スプーフィングは「Man-In-The-Middle（MITM; 仲介者）」攻撃を引き起こします。たとえば、ホストからゲートウェイ ルータに ARP 要求を送ると、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。ところが、攻撃側は、ルータの MAC アドレスの代わりに攻撃側の MAC アドレスを使用して別の ARP 応答をホストに送ります。これにより、攻撃側は、ルータに転送される前にあらゆるホスト トラフィックを代行受信できるようになります。

ARP 検査により、スタティック ARP テーブルに正しい MAC アドレスとそれに対応する IP アドレスが指定されているかぎり、攻撃側が自分の MAC アドレスを使用して ARP 応答を送信できないことが保証されます。

スタティック ARP エントリの追加

ARP 検査では、ARP パケットと、ARP テーブルに登録されたスタティック ARP エントリを照合します。スタティック ARP エントリを追加するには、次のコマンドを入力します。

```
hostname(config)# arp interface_name ip_address mac_address
```

interface_name は、ARP パケットの送信元インターフェイスです。*ip_address* は送信元アドレスで、*mac_address* は関連 MAC アドレスです。

たとえば、MAC アドレス 0009.7cbe.2100 を持つルータの外部インターフェイス 10.1.1.1 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。

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

（注）透過ファイアウォールは、管理トラフィックなどの FWSM の間のトラフィックに関して、ARP テーブルのダイナミック ARP エントリを使用します。

ARP 検査のイネーブル化

ARP 検査をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# arp-inspection interface_name enable [flood | no-flood]
```

interface_name は、ARP 検査をイネーブルにするインターフェイスです。**flood** キーワード を使用すると、一致しなかった ARP パケットはすべてのインターフェイスに転送されます。**no-flood** を使用すると、一致しなかったパケットは廃棄されます。

（注）デフォルト設定は、一致しなかったパケットをフラッディングします。FWSM 経由でスタティックエントリにのみ ARP を制限するには、このコマンドを **no-flood** に設定します。

たとえば、外部インターフェイス上で ARP 検査をイネーブルにして、一致しなかったすべての ARP パケットを廃棄する場合は、次のコマンドを入力します。

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

すべてのインターフェイス上で ARP 検査の現在の設定を表示するには、**show arp-inspection** コマンドを入力します。

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 テーブルについて説明します。内容は次のとおりです。

- MAC アドレス テーブルの概要（p.17-4）
- スタティック MAC アドレスの追加（p.17-4）
- MAC アドレス タイムアウトの設定（p.17-5）
- MAC アドレス学習のディセーブル化（p.17-5）
- MAC アドレス テーブルの表示（p.17-5）

MAC アドレス テーブルの概要

FWSM は、通常のブリッジまたはスイッチと同様に、MAC アドレスを学習して MAC アドレス テーブルを作成します。装置が FWSM を介してパケットを送信すると、FWSM が MAC アドレスをアドレス テーブルに追加します。このテーブルで MAC アドレスと送信元インターフェイスが対応付けられ、グループがブリッジングされるので、FWSM は適切なインターフェイスから装置宛てのパケットを送信できます。トラフィックが複数のブリッジ グループを経由して送信される場合、MAC アドレスはテーブルに、複数のエントリを持つことができます。FWSM が MAC アドレスにパケットを配信する出力インターフェイスを決定する必要があるとき、FWSM はパケットの入力インターフェイスを含んだブリッジ グループのエントリを使用します。

FWSM 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含まれていなくても、通常のブリッジのように、ブリッジ グループのすべてのインターフェイスに元のパケットを FWSM がフラッディングすることはありません。その代わり、直接接続された装置またはリモート装置用に次のパケットを生成します。

- 直接接続装置用のパケット — FWSM は宛先 IP アドレスへの ARP 要求を生成し、FWSM に ARP 応答を受信するインターフェイスがわかるようにします。
- リモート装置用のパケット — FWSM は宛先 IP アドレスへの ping を生成し、FWSM に ping 応答を受信するインターフェイスがわかるようにします。

元のパケットは廃棄されます。

スタティック MAC アドレスの追加

MAC アドレスは通常、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届いたときに、MAC アドレス テーブルに動的に追加されます。MAC アドレス テーブルには、必要に応じてスタティック MAC アドレスを追加できます。スタティック エントリを追加する利点の 1 つとして、MAC スプーフィングに対する防御が挙げられます。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 エントリと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する場合、FWSM はそのトラフィックを廃棄し、システム メッセージを生成します。

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。

```
hostname(config)# mac-address-table static interface_name mac_address
```

interface_name は送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 エントリのタイムアウト値は、デフォルトで 5 分です。このタイムアウト値は変更可能です。タイムアウト値を変更するには、次のコマンドを入力します。

```
hostname(config)# mac-address-table aging-time timeout_value
```

timeout_value（分単位）は、5 ～ 720 分（12 時間）です。5 分がデフォルトです。

MAC アドレス学習のディセーブル化

デフォルトでは、各インターフェイスが着信トラフィックの MAC アドレスを自動的に学習し、FWSM が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 アドレス学習をディセーブルにできます。ただし、MAC アドレスを統計的にテーブルに追加しない場合、トラフィックは FWSM を通過できません。

MAC アドレス学習をディセーブルにするには、次のコマンドを入力します。

```
hostname(config)# mac-learn interface_name disable
```

MAC アドレス学習を再びイネーブルにするには、このコマンドの **no** 形式を使用します。**clear configure mac-learn** コマンドは、すべてのインターフェイス上で MAC アドレス学習を再びイネーブルにします。

MAC アドレス テーブルの表示

MAC アドレス テーブル全体（スタティックおよびダイナミック エントリを含めて）、特定のインターフェイスの MAC アドレス テーブル、または特定のブリッジ グループの 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。

```
hostname# show mac-address-table [interface_name | bridge_group]
```

次に、テーブル全体を表示する **show mac-address-table** コマンドの出力例を示します。

```
hostname# show mac-address-table
interface          mac address       type      Age min)   Group
-----------------------------------------------------------------
outside            0009.7cbe.2100    static      -        Eng
inside             0010.7cbe.6101    static      -        Eng
inside             0009.7cbe.5101    dynamic     10       Eng
```

次に、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。

```
hostname# show mac-address-table inside
interface          mac address       type      Age min)   Group
-----------------------------------------------------------------
inside             0010.7cbe.6101    static      -        Eng
inside             0009.7cbe.5101    dynamic     10       Eng
```

モジュラ ポリシー フレームワークの使用

この章では、モジュラ ポリシー フレームワークを使用して、TCP 用のセキュリティ ポリシー、一般的な接続設定、検査を作成する方法について説明します。

この章で説明する内容は、次のとおりです。

- モジュラ ポリシー フレームワークの概要（p.18-2）
- クラス マップを使用したトラフィックの識別（p.18-3）
- ポリシー マップを使用した動作の定義（p.18-5）
- サービス ポリシーを使用したインターフェイスへのポリシーの適用（p.18-8）
- モジュラ ポリシー フレームワークの例（p.18-9）

モジュラ ポリシー フレームワークの概要

モジュラ ポリシー フレームワークは、Cisco IOS ソフトウェア QoS CLI と同様に、FWSM の機能を設定する一貫したフレキシブルな方法を提供します。たとえば、モジュラ ポリシー フレームワークを使用してタイムアウトを設定すると、すべての TCP アプリケーションにではなく、特定の TCP アプリケーションに固有に適用できます。

モジュラ ポリシー フレームワークは、次の機能とともにサポートされます。

- TCP 接続制限およびタイムアウト
- アプリケーション検査

モジュラ ポリシー フレームワークの設定には、3 つのタスクが含まれます。

1. アクションを適用するトラフィックを識別します。「クラス マップを使用したトラフィックの識別」（p.18-3）を参照してください。
2. トラフィックにアクションを適用します。「ポリシー マップを使用した動作の定義」（p.18-5）を参照してください。
3. インターフェイス上でアクションを実行します。「サービス ポリシーを使用したインターフェイスへのポリシーの適用」（p.18-8）を参照してください。

デフォルトのグローバル ポリシー

デフォルトの設定では、すべてのデフォルトのアプリケーション検査トラフィックと一致し、全インターフェイス上のトラフィックに検査を適用するポリシー（グローバル ポリシー）が含まれます。適用できるのは 1 つのグローバル ポリシーだけなので、グローバル ポリシーを変更する場合は、デフォルト ポリシーを編集するか、またはデフォルト ポリシーをディセーブルにして新しいポリシーを適用する必要があります。

デフォルトのポリシー設定には、次のコマンドが含まれます。

```
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect smtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
service-policy global_policy global
```

クラス マップを使用したトラフィックの識別

クラス マップは、アクションを適用するトラフィックを識別します。クラス マップの最大数はシングル モードまたはマルチ モードの各コンテキストで 255 です。設定には、FWSM がデフォルト グローバル ポリシーで使用するデフォルトのクラス マップが含まれます。これは **inspection_default** といい、デフォルトのインスペクション トラフィックに一致します。

```
class-map inspection_default
 match default-inspection-traffic
```

クラス マップを定義する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、クラス マップを作成します。

```
hostname(config)# class-map class_map_name
```

class_map_name は、最大 40 文字の文字列です。

ステップ 2　（任意）次のコマンドを入力して、クラス マップに説明を追加します。

```
hostname(config-cmap)# description string
```

ステップ 3　次の特性のいずれかと一致させて、クラスに含まれるトラフィックを定義します。別途指定のない限り、**match** コマンド 1 つだけをクラス マップに含めることができます。

- 任意のトラフィック — クラスをすべてのトラフィックに一致させます。

  ```
  hostname(config-cmap)# match any
  ```

- アクセス リスト — クラスを拡張アクセス リストで指定されたトラフィックに一致させます。FWSM が透過ファイアウォール モードで稼働している場合、EtherType アクセス リストを使用できます。

  ```
  hostname(config-cmap)# match access-list acl_ID
  ```

  アクセス リストの作成の詳細については、「拡張アクセス リストの追加」（p.10-7）または「EtherType アクセス リストの追加」（p.10-10）を参照してください。

  Network Address Translation（NAT; ネットワーク アドレス変換）を使用したアクセス リストの作成の詳細については、「NAT 使用時のアクセス リスト用 IP アドレス」（p.10-3）を参照してください。

- TCP または UDP 宛先ポート — クラスを単一ポートまたは連続したポート範囲と一致させることができます。

  ```
  hostname(config-cmap)# match port {tcp | udp} {eq port_num | range port_num
  port_num}
  ```

ヒント　連続しない複数のポートを使用するアプリケーションの場合、**match access-list** コマンドを使用して、各ポートと一致するよう Access Control Entry（ACE; アクセス制御エントリ）を定義します。

ポートのリストについては、「TCP ポートおよび UDP ポート」（p.D-14）を参照してください。

たとえば、次のコマンドを入力して、ポート 80（HTTP）上の TCP パケットを一致させます。

```
hostname(config-cmap)# match tcp eq 80
```

- 検査用のデフォルトのトラフィック — デフォルトで FWSM が検査するトラフィックにクラスを一致させます。

```
hostname(config-cmap)# match default-inspection-traffic
```

match default-inspection-traffic コマンドは、デフォルトで検査されるプロトコルやポートを指定します。デフォルトのインスペクション トラフィックについては、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』のコマンドを参照してください。FWSM には、デフォルト インスペクション トラフィックと一致し、すべてのインターフェイス上のトラフィックに検査を適用するデフォルト グローバル ポリシーが含まれます。

match default-inspection-traffic コマンドと一緒に **match access-list** コマンドを指定すると、一致したトラフィックを絞り込むことができます。クラスは、**match default-inspection-traffic** コマンドにすでに含まれている **match access-list** コマンド内で指定されたプロトコルまたはポート情報を除外します。

- IP ヘッダーの DSCP 値 — クラスを最大 8 つの DSCP 値に一致させることができます。

```
hostname(config-cmap)# match dscp value1 [value2] [...] [value8]
```

次に、入力例を示します。

```
hostname(config-cmap)# match dscp af43 cs1 ef
```

- 優先 — クラスを最大で 4 つの優先値に一致できます。値は IP ヘッダーの TOS バイトで示されます。

```
hostname(config-cmap)# match precedence value1 [value2] [value3] [value4]
```

value1 ～ *value4* は、優先順位に相当する 0 ～ 7 です。

- RTP トラフィック — クラスを RTP トラフィックに一致させることができます。

```
hostname(config-cmap)# match rtp starting_port range
```

starting_port は 2000 ～ 65,534 の間の偶数の UDP 宛先ポートを指定します。*range* は、上述の *starting_port* と一致した追加の UDP ポートの番号を指定します。範囲は 0 ～ 16,383 です。

次に、**class-map** コマンドの例を示します。

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255
hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp
hostname(config-cmap)# exit
hostname(config)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp
hostname(config-cmap)# exit
hostname(config)# class-map all_http
hostname(config-cmap)# description "This class-map matches all HTTP traffic"
hostname(config-cmap)# match port tcp eq http
hostname(config-cmap)# exit
hostname(config)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server
10.1.1.1"
hostname(config-cmap)# match access-list host_foo
hostname(config-cmap)# exit
```

ポリシー マップを使用した動作の定義

ここでは、ポリシー マップを作成してアクションとクラス マップを対応付ける手順について説明します。次の内容について説明します。

- ポリシー マップの概要（p.18-5）
- デフォルトのポリシー マップ（p.18-6）
- ポリシー マップの追加（p.18-6）

ポリシー マップの概要

ポリシー マップで複数のクラス マップを指定できます。1 つまたは複数の機能タイプの複数のアクションを各クラス マップに割り当てることができます。機能タイプには次が含まれます。

- TCP 接続制限およびタイムアウト
- アプリケーション検査

1 つのパケットは、各機能タイプのポリシー マップのクラス マップ 1 つと一致させることができます。パケットが各機能タイプのクラス マップと一致すると、FWSM はパケットをその機能タイプの以降のクラス マップに一致させようとはしません。ただし、パケットが別の機能タイプの以降のクラス マップと一致すると、FWSM は以降のクラス マップのアクションを適用します。

たとえば、パケットが接続制限のクラス マップと一致し、アプリケーション検査のクラス マップとも一致した場合、両方のクラス マップのアクションが適用されます。パケットがアプリケーション検査のクラス マップと一致し、アプリケーション検査の別のクラス マップとも一致した場合、2 番めのクラス マップのアクションは適用されません。

動作はトラフィックに双方向に適用されます。トラフィックが双方向のクラス マップと一致すると、ポリシー マップの適用先であるインターフェイスに発着するすべてのトラフィックが影響を受けます。

（注） グローバル　ポリシーを使用すると、すべての機能は単一方向になります。単一インターフェイスに適用されると通常は双方向である機能が、グローバルに適用された場合は、各インターフェイスの入力方向のみに適用されます。ポリシーはすべてのインターフェイスに適用されるので、ポリシーは双方向に適用されます。したがって、この場合の双方向性は冗長になります。

ポリシー マップの異なるアクション タイプが実行される順番は、ポリシー マップで動作が表示される順番とは関係ありません。実行される動作は、次の順番で行われます。

- TCP 接続制限およびタイムアウト
- アプリケーション検査

ポリシー マップはインターフェイスごとに 1 つしか割り当てることができませんが、同じポリシー マップを複数のインターフェイスに適用することができます。

デフォルトのポリシー マップ

設定には、FWSM がデフォルト グローバル ポリシーで使用するデフォルトのポリシー マップが含まれます。これは **global_policy** といい、デフォルトのインスペクション トラフィック上の検査で実行されます。適用できるのは 1 つのグローバル ポリシーだけなので、グローバル ポリシーを変更する場合は、デフォルト ポリシーを編集するか、またはデフォルト ポリシーをディセーブルにして新しいポリシーを適用する必要があります。

デフォルトのポリシー マップ設定には、次のコマンドが含まれます。

```
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect smtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
```

ポリシー マップの追加

ポリシー マップを作成する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、ポリシー マップを追加します。

```
hostname(config)# policy-map policy_map_name
```

ステップ 2　（任意）ポリシー マップの説明を指定します。

```
hostname(config-pmap)# description text
```

ステップ 3　次のコマンドを使用して、すでに設定済みのクラス マップを指定します。

```
hostname(config-pmap)# class class_map_name
```

クラス マップを追加するには、「クラス マップを使用したトラフィックの識別」（p.18-3）を参照してください。

ステップ 4　クラス マップに 1 つまたは複数のアクションを指定します。

- 接続制限。「接続制限とタイムアウトの設定」（p.19-2）を参照してください。
- アプリケーション検査。第 20 章「アプリケーション レイヤ プロトコル検査の適用」を参照してください。

（注） **match default_inspection_traffic** コマンドがクラス マップにない場合、**inspect** コマンドを 1 つだけ、クラスの下に設定できます。

ステップ 5　このポリシー マップに指定する各クラス マップについて、ステップ 4 を繰り返します。

次に、接続ポリシー用の **policy-map** コマンドの例を示します。このコマンドは、Web サーバ 10.1.1.1 への接続を許可する数を制限します。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning
connection to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

次に、複数の一致がポリシー マップ内で動作する例を示します。

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

次に、トラフィックが最初に利用可能なクラス マップと一致し、同一の機能ドメイン内でアクションを指定する以降のクラス マップとは一致しない例を示します。

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

Telnet 接続が開始されると、トラフィックは **class telnet_traffic** と一致します。同様に、FTP 接続が開始されると、トラフィックは **class ftp_traffic** と一致します。Telnet および FTP 以外の TCP 接続の場合、トラフィックは **class tcp_traffic** と一致します。Telnet または FTP 接続が **class tcp_traffic** と一致できても、この接続は他のクラスと以前に一致しているので FWSM ではこの一致は行われません。

サービス ポリシーを使用したインターフェイスへのポリシーの適用

ポリシー マップを実行するには、ポリシー マップを 1 つまたは複数のインターフェイスに適用するか、またはすべてのインターフェイスにグローバルに適用するサービス ポリシーを作成します。インターフェイス サービス ポリシーは、グローバル サービス ポリシーより優先されます。

- ポリシー マップとインターフェイスを対応付けてサービス ポリシーを作成するには、次のコマンドを入力します。

  ```
  hostname(config)# service-policy policy_map_name interface interface_name
  ```

- 特定のポリシーを持たないインターフェイスすべてに適用するサービス　ポリシーを作成するには、次のコマンドを入力します。

  ```
  hostname(config)# service-policy policy_map_name global
  ```

  デフォルトの設定では、すべてのデフォルトのアプリケーション検査トラフィックと一致し、検査をトラフィックにグローバルに適用するグローバル ポリシーが含まれます。適用できるのは 1 つのグローバル ポリシーだけなので、グローバル ポリシーを変更する場合は、デフォルト ポリシーを編集するか、またはデフォルト ポリシーをディセーブルにして新しいポリシーを適用する必要があります。

  デフォルトのサービス ポリシーには、次のコマンドが含まれます。

  ```
  service-policy global_policy global
  ```

たとえば、次のコマンドを使用すると、inbound_policy ポリシー マップを外部インターフェイス上でイネーブルにします。

```
hostname(config)# service-policy inbound_policy interface outside
```

次のコマンドを使用すると、デフォルトのグローバル ポリシーをディセーブルにし、その他すべての FWSM インターフェイス上で new_global_policy という新しいポリシーをイネーブルにします。

```
hostname(config)# no service-policy global_policy global
hostname(config)# service-policy new_global_policy global
```

モジュラ ポリシー フレームワークの例

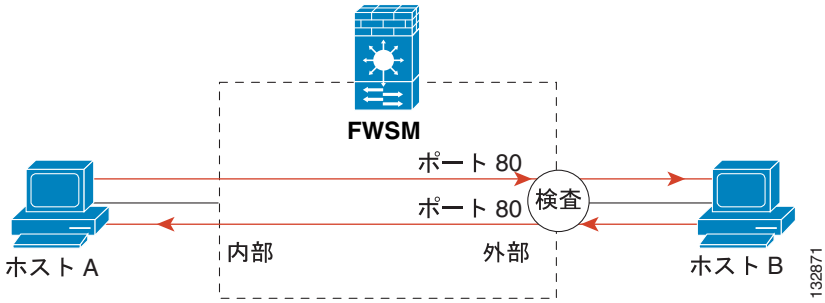
ここでは、モジュラ ポリシー フレームワークの例について説明します。内容は次のとおりです。

- HTTP トラフィックへの検査の適用（p.18-9）
- HTTP トラフィックへの検査のグローバルな適用（p.18-10）
- 特定のサーバに対する HTTP トラフィックの検査および接続制限の適用（p.18-11）
- NAT を使用した HTTP トラフィックへの検査の適用（p.18-12）

HTTP トラフィックへの検査の適用

この例では（図 18-1 を参照）、外部インターフェイス経由で FWSM に発着する HTTP 接続（ポート 80 上の TCP トラフィック）は HTTP 検査用に分類されます。

図 18-1　HTTP 検査



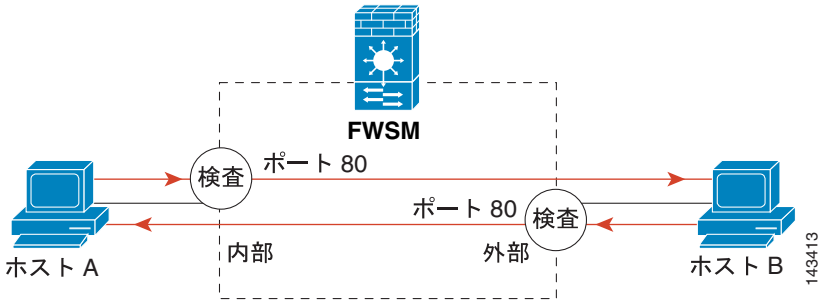
この例に対応するコマンドは、次のとおりです。

```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config)# service-policy http_traffic_policy interface outside
```

HTTP トラフィックへの検査のグローバルな適用

この例では（図 18-2 を参照）、任意のインターフェイス経由で FWSM に入る HTTP 接続（ポート 80 上の TCP トラフィック）は HTTP 検査用に分類されます。ポリシーはグローバル ポリシーなので、トラフィックがインターフェイスに入ったときのみ検査が実行されます。

図 18-2　グローバル HTTP 検査



この例に対応するコマンドは、次のとおりです。

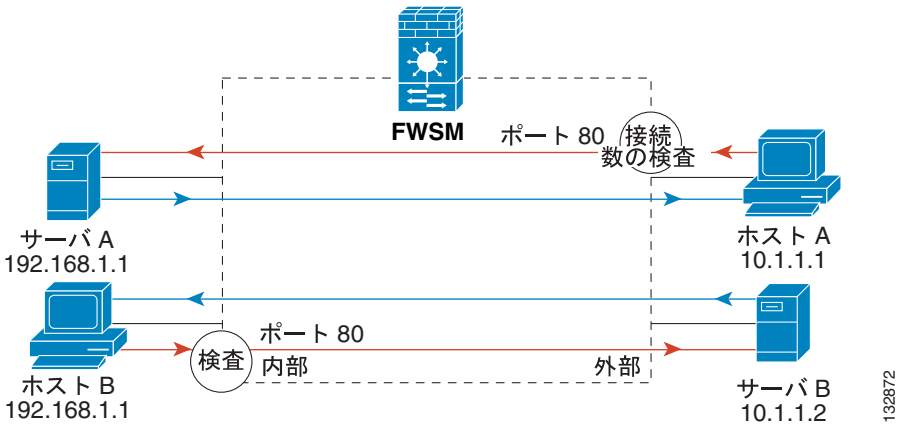
```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config)# service-policy http_traffic_policy global
```

特定のサーバに対する HTTP トラフィックの検査および接続制限の適用

この例では（図 18-3 を参照）、外部インターフェイス経由で FWSM に入り、宛先がサーバ A の HTTP 接続（ポート 80 上の TCP トラフィック）は HTTP 検査用に分類され、最大接続が制限されます。サーバ A からホスト A に開始された接続は、クラス マップのアクセス リストと一致しないので、影響を受けません。

内部インターフェイス経由で FWSM に入り、宛先がサーバ B である HTTP 接続は、HTTP 検査用に分類されます。サーバ B からホスト B に開始された接続は、クラス マップのアクセス リストと一致しないので、影響を受けません。

図 18-3　特定のサーバの HTTP 検査および接続制限



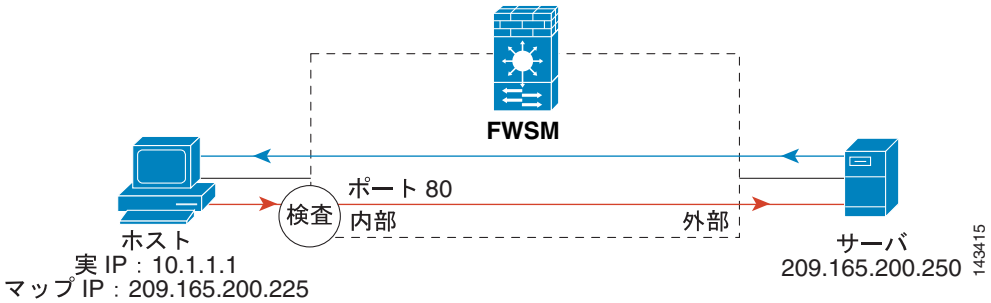
この例に対応するコマンドは、次のとおりです。

```
hostname(config)# access-list serverA extended permit tcp any host 192.168.1.1 eq 80
hostname(config)# access-list ServerB extended permit tcp any host 10.1.1.2 eq 80

hostname(config)# class-map http_serverA
hostname(config-cmap)# match access-list serverA
hostname(config)# class-map http_serverB
hostname(config-cmap)# match access-list serverB

hostname(config)# policy-map policy_serverA
hostname(config-pmap)# class http_serverA
hostname(config-pmap-c)# inspect http http_map_serverA
hostname(config-pmap-c)# set connection conn-max 100
hostname(config)# policy-map policy_serverB
hostname(config-pmap)# class http_serverB
hostname(config-pmap-c)# inspect http http_map_serverB

hostname(config)# service-policy policy_serverB interface inside
hostname(config)# service-policy policy_serverA interface outside
```

NAT を使用した HTTP トラフィックへの検査の適用

この例では、内部ネットワーク上のホストには、実 IP アドレス 10.1.1.1 と、外部ネットワークで使用されるマップされた IP アドレス 209.165.200.225 があります。ポリシーは内部インターフェイスに適用されているので、実アドレスが使用されている場合、実 IP アドレスをクラス マップのアクセス リストで使用する必要があります。ポリシーを外部インターフェイスに適用する場合、マップされたアドレスを使用してください。

図 18-4　NAT を使用した HTTP 検査



この例に対応するコマンドは、次のとおりです。

```
hostname(config)# static (inside,outside) 209.165.200.225 10.1.1.1
hostname(config)# access-list http_client extended permit tcp host 10.1.1.1 any eq 80

hostname(config)# class-map http_client
hostname(config-cmap)# match access-list http_client

hostname(config)# policy-map http_client
hostname(config-pmap)# class http_client
hostname(config-pmap-c)# inspect http

hostname(config)# service-policy http_client interface inside
```

ネットワーク攻撃の回避

この章では、ネットワーク攻撃を回避する手順について説明します。内容は次のとおりです。

- 接続制限とタイムアウトの設定（p.19-2）
- IP スプーフィングの回避（p.19-4）
- フラグメント サイズの設定（p.19-4）
- 不正な接続のブロック（p.19-5）

接続制限とタイムアウトの設定

ここでは、TCP および UDP 接続の最大数を設定し、接続タイムアウトを設定し、TCP シーケンスのランダム化をディセーブルにする手順について説明します。

TCP シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化し、データをスクランブル化している場合だけにしてください。TCP 接続ごとに、Initial Sequence Number（ISN）を 2 つずつ使用します。1 つはクライアントが作成し、もう 1 つはサーバが作成します。FWSM は、ホスト / サーバによって生成された ISN をランダム化します。攻撃側が次の ISN を予測してセッションを乗っ取る可能性を排除するために、ISN の少なくとも一方はランダムに作成する必要があります。

（注） Network Address Translation（NAT; ネットワーク アドレス変換）設定で最大接続数と、TCP シーケンスのランダム化も設定できます。両方の方法を使用して、同じトラフィックに設定値を設定する場合、FWSM は低い方の制限を使用します。いずれかの方法を使用して TCP シーケンスのランダム化がディセーブルである場合、FWSM は TCP シーケンスのランダム化をディセーブルにします。

NAT も初期接続制限を設定します。これにより、Denial of Service（DoS; サービスの拒絶）攻撃を回避するための TCP 代行受信が開始されます。接続制限、TCP のランダム化、初期制限を設定するには、「透過ファイアウォール モードと NAT を設定しない場合の接続制限の設定」（p.7-8）および 第 12 章「NAT の設定」を参照してください。

接続制限を設定する手順は、次のとおりです。

ステップ 1　トラフィックを識別するには、**class-map** コマンドを使用してクラス マップ コマンドを追加します。詳細については、「クラス マップを使用したトラフィックの識別」（p.18-3）を参照してください。

ステップ 2　クラス マップ トラフィックで行うアクションを設定するポリシー マップを追加または編集するには、次のコマンドを入力します。

```
hostname(config)# policy-map name
```

ステップ 3　アクションを割り当てるステップ 1 のクラス マップを特定するには、次のコマンドを入力します。

```
hostname(config-pmap)# class class_map_name
```

ステップ 4　最大接続数（TCP と UDP 両方）を設定するか、または TCP シーケンスのランダム化をイネーブルあるいはディセーブルにするには、次のコマンドを入力します。

```
hostname(config-pmap-c)# set connection {[conn-max number] [random-sequence-number
{enable | disable}]}
```

number は 0 ～ 65,535 です。デフォルトは 0 で、これは接続に制限がないことを意味します。

1 行すべてにこのコマンドを（任意の順序で）入力することも、各属性を別のコマンドとして入力することもできます。実行コンフィギュレーションでは、このコマンドは 1 行に統合されています。

ステップ 5　接続のタイムアウト、初期接続（ハーフオープン）、ハーフクローズ接続を設定するには、次のコマンドを入力します。

```
hostname(config-pmap-c)# set connection timeout {[embryonic seconds]
[half-closed minutes] [tcp minutes]}
```

embryonic *seconds* は、1 ～ 255（秒）です。デフォルトは 20 秒です。この値を 0 に設定できます。これは接続が決してタイムアウトしないことを意味します。**set connection** コマンドを使用しても初期接続の最大数は設定できませんが、タイムアウトは設定できます。

half-closed *minutes* は 1 ～ 255（分）です。デフォルトは 10 分です。この値を 0 に設定できます。これは接続が決してタイムアウトしないことを意味します。

tcp *minutes* は 5 ～ 65535（分）です。デフォルトは 60 分です。この値を 0 に設定できます。これは接続が決してタイムアウトしないことを意味します。

1 行すべてにこのコマンドを（任意の順序で）入力することも、各属性を別のコマンドとして入力することもできます。実行コンフィギュレーションでは、このコマンドは 1 行に統合されています。

ステップ 6　1 つまたは複数のインターフェイス上でポリシー マップを実行するには、次のコマンドを入力します。

```
hostname(config)# service-policy policymap_name {global | interface interface_name}
```

global はポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。許可されるのはグローバル ポリシー 1 つのみです。サービス ポリシーをインターフェイスに適用すると、そのインターフェイス上のグローバル ポリシーが上書きされます。各インターフェイスに対し、ポリシー マップ 1 つを適用できます。

IP スプーフィングの回避

Unicast Reverse Path Forwarding（uRPF）をインターフェイス上でイネーブルにすることができます。uRPF は、すべてのパケットの送信元 IP アドレスが、ルーティング テーブル内の正しい送信元インターフェイスと一致するかどうかを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用して正しい送信元を不明にすること）を防ぎます。

通常、パケットの送信先を決定する場合、FWSM は宛先アドレスのみを認識します。uRPF は送信元アドレスも認識するよう FWSM に指示します。そのため、この機能は Reverse Path Forwarding と呼ばれます。FWSM 経由で許可したい任意のトラフィックについては、FWSM ルーティング テーブルに送信元アドレスまで戻るルートを含める必要があります。詳細については、RFC 2267 を参照してください。

外部トラフィックについては、たとえば、FWSM は uRPF 保護要件を満たすため、デフォルトのルートを使用できます。トラフィックが外部インターフェイスから入り、ルーティング テーブルがその送信元アドレスを知らない場合、FWSM はデフォルトのルートを使用して、外部インターフェイスを送信元インターフェイスとして正しく指定します。

トラフィックが、ルーティング テーブルにとって既知であるが、内部インターフェイスに対応付けられているアドレスから外部インターフェイスに入る場合、FWSM はパケットを廃棄します。同様に、トラフィックが未知の送信元アドレスから内部インターフェイスに入る場合、一致するルート（デフォルトのルート）が外部インターフェイスを示すので、FWSM はパケットを廃棄します。

ユニキャスト RPF は次のように実行されます。

- Internet Control Message Protocol（ICMP）パケットにはセッションがないので、各パケットが検証されます。
- UDP および TCP にはセッションがあるので、初期パケットはリバース ルート検索を必要とします。セッション中に着信する以降のパケットは、セッションの一部として維持された既存のステートを使用して検証されます。非初期パケットは、初期パケットが使用する同一のインターフェイス上に着信するように検証されます。

uRPF をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# ip verify reverse-path interface interface_name
```

フラグメント サイズの設定

デフォルトでは、FWSM は、IP パケットにつき最大 24 のフラグメント、およびリアセンブリを待つ最大 200 のフラグメントを許可します。定期的にパケットをフラグメント化するアプリケーション（NFS over UDP など）がある場合、ネットワーク上でフラグメント化を行う必要があるかもしれません。ただし、トラフィックをフラグメント化するアプリケーションがない場合、FWSM 経由でフラグメントを許可しないことを推奨します。フラグメント化されたパケットは、DoS 攻撃としてしばしば使用されます。フラグメントを許可しないようにするには、次のコマンドを入力します。

```
hostname(config)# fragment chain 1 [interface_name]
```

特定のインターフェイスでフラグメント化を回避したい場合、インターフェイス名を入力します。デフォルトでは、このコマンドはすべてのインターフェイスに適用されます。

不正な接続のブロック

ホストがネットワークを攻撃しようとしていることが分かっている（たとえば、システム ログ メッセージが攻撃を表示する）場合、IP アドレスおよび他の識別パラメータに基づいて接続をブロック（または排除）できます。排除を解除するまで新しい接続は実行されません。

（注） トラフィックをモニタする IPS がある場合、IPS は自動的に接続を排除します。

接続を手動で排除する手順は、次のとおりです。

ステップ 1　必要に応じて、次のコマンドを入力して接続の詳細を表示します。

```
hostname# show conn
```

FWSM に、次のような各接続の詳細を表示します。

```
TCP out 64.101.68.161:4300 in 10.86.194.60:23 idle 0:00:00 bytes 1297 flags UIO
```

ステップ 2　送信元 IP アドレスから接続を排除するには、次のコマンドを入力します。

```
hostname(config)# shun src_ip [dst_ip src_port dest_port [protocol]] [vlan vlan_id]
```

送信元 IP アドレスのみを入力すると、以降の接続はすべて排除されます。既存の接続はアクティブのままです。

既存の接続を廃棄するには、送信元 IP アドレスからの以降の接続をブロックするのと同様に、宛先 IP アドレス、送信元ポートおよび宛先ポート、プロトコルを入力します。デフォルトでは、IP のプロトコルは 0 です。

マルチコンテキスト モードの場合、このコマンドを admin コンテキストに入力できます。他のコンテキストに割り当てられた VLAN（仮想 LAN）ID を指定することで、別のコンテキストで接続を回避できます。

ステップ 3　排除を解除するには、次のコマンドを入力します。

```
hostname(config)# no shun src_ip [vlan vlan_id]
```

アプリケーション レイヤ プロトコル検査の適用

この章では、アプリケーション検査の使用方法および設定手順について説明します。この章で説明する内容は、次のとおりです。

- アプリケーション インスペクション エンジンの概要（p.20-2）
  - インスペクション エンジンの機能（p.20-3）
  - NAT、PAT、アプリケーション検査（p.20-4）
  - サポート対象プロトコル（p.20-4）
  - アプリケーション エンジンのデフォルト（p.20-5）
- アプリケーション検査コンフィギュレーションの概要（p.20-7）
- デフォルトのアプリケーション検査（p.20-8）
- CTIQBE 検査（p.20-9）
- DNS 検査（p.20-13）
- FTP 検査（p.20-22）
- GTP 検査（p.20-28）
- H.323 検査（p.20-34）
- HTTP 検査（p.20-42）
- ICMP 検査（p.20-45）
- ILS 検査（p.20-45）
- MGCP 検査（p.20-46）
- NetBIOS 検査（p.20-52）
- PPTP 検査（p.20-52）
- RSH 検査（p.20-52）
- RTSP 検査（p.20-53）
- SIP 検査（p.20-57）
- Skinny（SCCP）検査（p.20-63）
- SMTP および拡張 SMTP 検査（p.20-67）
- SNMP 検査（p.20-70）
- SQL*Net 検査（p.20-72）
- Sun RPC 検査（p.20-73）
- TFTP 検査（p.20-77）
- XDMCP 検査（p.20-77）

アプリケーション インスペクション エンジンの概要

ここでは、アプリケーション インスペクション エンジンの機能について説明します。FWSM がステートフル アプリケーション検査用に使用するアダプティブ セキュリティ アルゴリズム（ASA）により、アプリケーションとサービスの安全な使用が保証されます。一部のアプリケーションでは FWSM による特別な処理を必要とし、特定のアプリケーション インスペクション エンジンはこの目的のために提供されています。特別なアプリケーション インスペクション エンジンを必要とするアプリケーションには、ユーザ データ パケットに IP アドレス情報を組み込んでいるものや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開始するものがあります。

アプリケーション インスペクション エンジンは Network Address Translation（NAT; ネットワーク アドレス変換）と連携して、組み込まれたアドレス情報の場所を特定します。この連携により、NAT は組み込まれたアドレスを変換し、変換によって影響を受けたチェックサムまたは他のフィールドを更新できます。

各アプリケーション インスペクション エンジンはセッションをモニタして、セカンダリ チャネルのポート番号を決定します。ほとんどのプロトコルは、パフォーマンスを向上するため、セカンダリの TCP ポートまたは UDP ポートをオープンします。well-known ポートでの初期セッションは、ダイナミックに割り当てられるポート番号のネゴシエーションに使用されます。アプリケーション インスペクション エンジンはこのセッションをモニタし、ダイナミック ポートの割り当てを確認し、特定のセッションの間、これらのポート上でのデータ交換を許可します。

次の内容について説明します。

- インスペクション エンジンの機能（p.20-3）
- サポート対象プロトコル（p.20-4）

インスペクション エンジンの機能

図 20-1 に示すように、FWSM は基本的な動作で、次のデータベースを使用します。

- アクセス リスト — 特定のネットワーク、ホスト、サービス（TCP/UDP ポート番号）に基づいた接続の認証および許可に使用されます。
- 検査 — スタティックで定義済みのアプリケーションレベルの検査機能がセットで含まれます。
- 接続（XLATE テーブルおよび CONN テーブル）— 確立された各接続のステートや情報を保持します。この情報は、確立されたセッション内におけるトラフィック転送を効率的に行うために、ASA とカットスルー プロキシによって使用されます。

図 20-1　ASA の基本的な動作

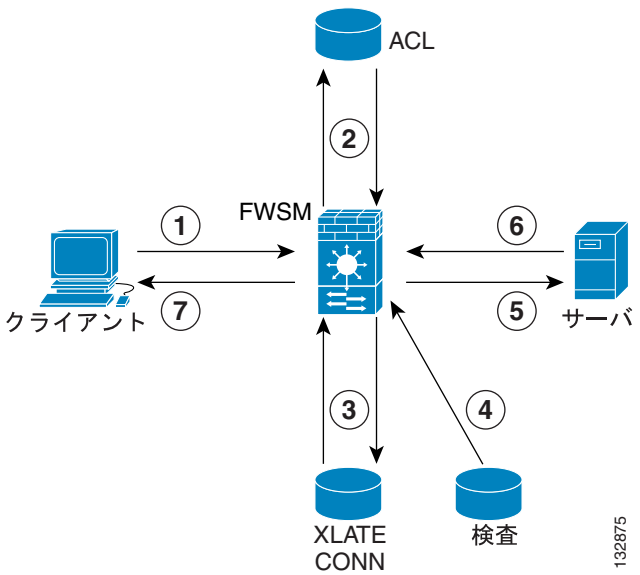


図 20-1 に、動作を実行順に説明します。

1. TCP SYN パケットが、新しい接続を確立するために FWSM に到着します。
2. FWSM は、アクセス リスト データベースを確認して、その接続を許可するかどうかを判別します。
3. FWSM は、接続データベース（XLATE テーブルおよび CONN テーブル）内に新しいエントリを作成します。
4. FWSM は、検査データベースを検証して、接続に対してアプリケーション レベルの検査が必要かどうかを判別します。
5. パケットに対してアプリケーション　インスペクション　エンジンの必要な処理が完了したら、FWSM は宛先システムにパケットを転送します。
6. 宛先システムは、初期要求に応答します。
7. FWSM は、応答パケットを受信し、接続データベースで接続を検索したあと、確立されたセッションに属しているパケットを転送します。

FWSM のデフォルトの設定には、アプリケーション検査エントリのセットが含まれています。このエントリは、サポートされているプロトコルを特定の TCP ポート番号または UDP ポート番号に対応付け、必要とされる特別な処理を指定します。

NAT、PAT、アプリケーション検査

NAT および Port Address Translation（PAT; ポートアドレス変換）を使用すると、次の方法でアプリケーション検査に影響を及ぼします。

- 一部のアプリケーション インスペクション エンジンは、変更できない固定ポートが割り当てられているので、NAT または PAT をサポートしません。アプリケーション エンジンがサポートする NAT および PAT の要約については、表 20-1 を参照してください。
- 検査されているトラフィックに PAT を設定すると、FWSM は、実ポート番号ではなく、変換されたポート番号でアプリケーション検査を実行します。

  変換されたポート番号を持つトラフィックに検査を適用するサービス ポリシーは、変換されたポート番号を使用して、トラフィックを識別するクラスマップを使用する必要があります。たとえば、PAT を実行してポート 2727 とポート 2427 をポート 1400 に変換する場合、well-known ポート 2427 とポート 2727 ではなく、ポート 1400 に送信されたトラフィックと一致するよう MGCP（メディア ゲートウェイ制御プロトコル）を設定する必要があります。

サポート対象プロトコル

FWSM は、次のインスペクション エンジンをサポートしています。

- CTIQBE — 「CTIQBE 検査」（p.20-9）を参照してください。
- Domain Name System（DNS; ドメイン ネーム システム）— 「DNS 検査」（p.20-13）を参照してください。
- FTP（ファイル転送プロトコル）— 「FTP 検査」（p.20-22）を参照してください。
- GTP — 「GTP 検査」（p.20-28）を参照してください。
- H.323 — 「H.323 検査」（p.20-34）を参照してください。
- HTTP — 「HTTP 検査」（p.20-42）を参照してください。
- Internet Control Message Protocol（ICMP）—『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect icmp** および **inspect icmp error** コマンド ページを参照してください。
- ILS —『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect ils** コマンド ページを参照してください。
- MGCP — 「MGCP 検査」（p.20-46）を参照してください。
- NetBIOS —『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect netbios** コマンド ページを参照してください。
- PPTP —『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect pptp** コマンド ページを参照してください。
- RSH —『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect rsh** コマンド ページを参照してください。
- RTSP — 「RTSP 検査」（p.20-53）を参照してください。
- SIP — 「SIP 検査」（p.20-57）を参照してください。
- Skinny — 「Skinny（SCCP）検査」（p.20-63）を参照してください。
- SMTP/ESMTP — 「SMTP および拡張 SMTP 検査」（p.20-67）を参照してください。
- SNMP — 「SNMP 検査」（p.20-70）を参照してください。
- SQL*Net —『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect sqlnet** コマンド ページを参照してください。
- SunRPC — 「Sun RPC 検査」（p.20-73）を参照してください。
- TFTP —『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect tftp** コマンド ページを参照してください。
- XDMCP —『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect xdmcp** コマンド ページを参照してください。

アプリケーション エンジンのデフォルト

表 20-1 に、FWSM でサポートされる各プロトコルに提供されたアプリケーション検査のタイプを要約します。

表 20-1　アプリケーション インスペクション エンジンおよびデフォルト

アプリケーション	デフォルトでのイネーブル化	PAT の有無	NAT（1 対 1）の有無	ポート設定の有無	デフォルトポート	標準	説明
CTIQBE	なし	あり	あり	あり	TCP/2748	—	—
DNS[1]	あり	あり	あり	なし	UDP/53	RFC 1123	NAT のみ転送します。PTR レコードの変更はありません。 デフォルトの最大パケット長は 512 バイトです。
FTP	あり	あり	あり	あり	TCP/21	RFC 959	デフォルトの FTP 検査は、RFC 規格への準拠を強制しません。強制するには、***strict*** キーワードを指定して **inspect ftp** コマンドを設定します。
GTP	なし	あり	あり	あり	UDP/3386 UDP/2123	—	特別なライセンスが必要です。
H.323	あり	あり	あり	あり	TCP/1720 UDP/1718 UDP（RAS）1718 ～ 1719	ITU-T H.323、H.245、H225.0、Q.931、Q.932	デフォルトでは、RAS 検査と H.225 検査の両方がイネーブルです。
HTTP	なし	あり	あり	あり	TCP/80	RFC 2616	ActiveX および Java のストリッピング時の MTU 制限に注意してください[2]。
ICMP	なし	あり	あり	なし	—	—	—
ICMP ERROR	なし	あり	あり	なし	—	—	—
ILS（LDAP）	なし	あり	あり	あり	—	—	—
MGCP	なし	あり	あり	あり	2427、2727	RFC2705bis-05	—
NetBIOS Datagram Service / UDP	あり	あり	あり	なし	UDP/138	—	—
NetBIOS Name Service / UDP	あり	なし	なし	なし	UDP/137	—	WINS はサポートしません。
NetBIOS over IP[3]	あり	なし	なし	なし	—	—	—
PPTP	なし	あり	あり	あり	1723	RFC2637	—
RSH	あり	あり	あり	あり	TCP/514	Berkeley UNIX	—
RTSP	なし	なし	なし	あり	TCP/554	RFC 2326、RFC 2327、RFC 1889	HTTP クローキングは処理されません。
SIP	あり	あり	あり	あり	TCP/5060 UDP/5060	RFC 2543	—

表 20-1　アプリケーション インスペクション エンジンおよびデフォルト（続き）

アプリケーション	デフォルトでのイネーブル化	PAT の有無	NAT（1 対 1）の有無	ポート設定の有無	デフォルトポート	標準	説明
Skinny（SCCP）	あり	あり	あり	あり	TCP/2000	—	所定の状況では、TFTP でアップロードした Cisco IP Phone コンフィギュレーションは処理されません。
SNMP	あり	なし	なし	あり	UDP/161、162	RFC 1155、1157、1212、1213、1215	v.2 RFC 1902 ～ 1908、v.3 RFC 2570 ～ 2580
SMTP/ESMTP	あり	あり	あり	あり	TCP/25	RFC 821、1123	デフォルトでは、ESMTP 検査ではなく、SMTP 検査がイネーブルです。
SQL*Net	あり	あり	あり	あり	TCP/1521（v.1）	—	V.1 および v.2
Sun RPC	あり	なし	あり	なし	UDP/111 TCP/111	—	ペイロードは NAT 処理しません。
TFTP	あり	あり	あり	あり	TCP/69 UDP/69	RFC 1530	—
XDCMP	あり	なし	なし	なし	UDP/177	—	—

1. WINS による名前解決用の NAT はサポートされません。
2. MTU が小さすぎて Java タグまたは ActiveX タグを 1 つのパケットに納められない場合は、ストリッピングは行われません。
3. NetBIOS は、NetBIOS ネーム サービス UDP ポート 137 および NetBIOS データグラム サービス UDP ポート 138 に対してパケットの NAT 処理を実行することでサポートされます。

アプリケーション検査コンフィギュレーションの概要

アプリケーション インスペクション エンジンを設定するには、MPF コマンドを使用します。アプリケーション検査を設定する前に、第 18 章「モジュラ ポリシー フレームワークの使用」をお読みください。この章では、MPF の概念と、アプリケーション検査を設定するのに使用しなければならない共通コマンドについて説明しています。

アプリケーション インスペクション エンジンのイネーブル化と適用には、必ず以下が含まれます。

- FWSM がインスペクション エンジンに送信するトラフィックを識別するクラス マップ
- クラス マップ（および関連トラフィック）をインスペクション エンジンにリンクするポリシー マップ
- ポリシー マップを 1 つまたはすべてのインターフェイスに適用するサービス ポリシー

第 18 章「モジュラ ポリシー フレームワークの使用」では、MPF を構成する、すなわちアプリケーション検査を設定する前述の 3 つの要素に関する詳細な概要を示します。この章で述べたインスペクション エンジンについては、詳細な設定手順および設定例を示します。この章で言及しないインスペクション エンジンについては、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の利用可能な **inspect** コマンド エントリを参照してください。

ただし、アプリケーション検査マップは例外です。これらのマップはアプリケーション検査コンフィギュレーションに固有のものです。アプリケーション検査マップにより、特定のインスペクション エンジン用に名前の付いたインスペクション パラメータのセットを作成します。検査マップをサポートするアプリケーション インスペクション エンジンにポリシー マップを設定する場合、名前で検査マップを指定できます。

次のプロトコルに対して、インスペクション エンジンはアプリケーション マップをサポートします。

- FTP — 詳細については、「request-command deny コマンド」（p.20-23）を参照してください。
- GTP — 詳細については、「GTP マップおよびコマンド」（p.20-29）を参照してください。
- HTTP — 詳細については、「拡張 HTTP 検査コマンド」（p.20-43）を参照してください。
- MGCP — 詳細については、「MGCP コール エージェントおよびゲートウェイの設定」（p.20-48）を参照してください。
- SIP — 詳細については、「IP アドレス プライバシー」（p.20-58）を参照してください。
- SNMP — 詳細については、「SNMP 検査の概要」（p.20-70）を参照してください。

デフォルトのアプリケーション検査

アプリケーション検査はデフォルトでは、すべてのプロトコルではないものの多くのプロトコルに対して、イネーブルです。表 20-1 には、アプリケーション インスペクション エンジンがデフォルトでイネーブルである場合の情報が示されています。ただし、デフォルトのポリシー コンフィギュレーションを検証して、デフォルトでイネーブルであるインスペクション エンジンを判別できます。内容は次のとおりです。

```
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect smtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
service-policy global_policy global
```

CTIQBE 検査

ここでは、CTIQBE アプリケーション検査をイネーブルにして、デフォルトのポート設定を変更する手順について説明します。次の内容について説明します。

- CTIQBE 検査の概要（p.20-9）
- 制限事項および制約事項（p.20-9）
- CTIQBE 検査のイネーブル化および設定（p.20-10）
- CTIQBE 検査の確認およびモニタ（p.20-11）

CTIQBE 検査の概要

inspect ctiqbe コマンドを使用すると、Computer Telephony Interface Quick Buffer Encoding（CTIQBE）プロトコル検査をイネーブルにします。これは、NAT、PAT、双方向 NAT をサポートします。これにより、Cisco IP SoftPhone および他の Cisco Telephony Application Programming Interface（TAPI）/Java Telephony Application Programming Interface（JTAPI）アプリケーションは、FWSM 上でコールセットアップのため、Cisco CallManager と連動できます。

TAPI および JTAPI は、多くの Cisco VoIP アプリケーションで使用されます。CTIQBE は、Cisco TAPI Service Provider（TSP; TAPI サービス プロバイダー）が Cisco CallManager と通信するために使用します。

制限事項および制約事項

次に、CTIQBE アプリケーション検査の使用時に適用される制限を要約します。

- CTIQBE アプリケーション検査では、**alias** コマンドを使用したコンフィギュレーションをサポートしていません。
- CTIQBE コールのステートフル フェールオーバーはサポートされて*いません*。
- **debug ctiqbe** コマンドを入力すると、メッセージの伝送が遅れる場合があり、リアルタイム環境のパフォーマンスに影響することがあります。このデバッグまたはログをイネーブルにし、FWSM を経由して Cisco IP SoftPhone でコール セットアップを完了できない場合は、Cisco IP SoftPhone が稼働するシステムで Cisco TSP 設定のタイムアウト値を増やします。

次に、CTIQBE アプリケーション検査を特定の事例で使用する場合に、特別に注意が必要な事項を要約します。

- 2 台の Cisco IP SoftPhone が異なる Cisco CallManager に登録されていて、各 CallManager が FWSM の異なるインターフェイスに接続されている場合、これら 2 台の電話間のコールは失敗します。
- Cisco IP SoftPhone と比較して Cisco CallManager の方がセキュリティの高いインターフェイス上に配置されており、NAT または外部 NAT が Cisco CallManager IP アドレスに必要な場合、マッピングはスタティックである必要があります。Cisco IP SoftPhone では Cisco CallManager IP アドレスを PC 上の Cisco TSP コンフィギュレーションで明示的に指定する必要があるからです。
- PAT または外部 PAT を使用しているときに Cisco CallManager IP アドレスを変換する場合、Cisco IP SoftPhone の登録を成功させるため、TCP ポート 2748 を PAT（インターフェイス）アドレスの**同一ポート**に対してスタティックにマッピングする必要があります。CTIQBE リスニング ポート（TCP 2748）は固定されていて、Cisco CallManager、Cisco IP SoftPhone、または Cisco TSP において、ユーザによる設定はできません。

CTIQBE 検査のイネーブル化および設定

CTIQBE 検査をイネーブルにする、または CTIQBE トラフィックの受信に使用するデフォルト ポートを変更する手順は、次のとおりです。

ステップ 1　CTIQBE トラフィックを識別するには、クラス マップを作成するか、または既存のクラス マップを変更します。**class-map** コマンドを次のように使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

class_map_name は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI はクラス マップ 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　CTIQBE トラフィックを識別するには、次のように **match port** コマンドを使用します。

```
hostname(config-cmap)# match port tcp eq 2748
```

ステップ 3　CTIQBE インスペクション エンジンを FTP トラフィックに適用するために使用するポリシー マップを作成するか、または既存のポリシー マップを変更します。そのためには、**policy-map** コマンドを次のように使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

policy_map_name は、ポリシー マップの名前です。CLI はポリシー マップ コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 4　ステップ 1 で作成したクラス マップを指定します。このクラス マップは CTIQBE トラフィックを識別します。**class** コマンドを次のように使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name は、ステップ 1 で作成したクラス マップの名前です。CLI はポリシー マップ クラス コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 5　CTIQBE アプリケーション検査をイネーブルにします。

```
hostname(config-pmap-c)# inspect ctiqbe
```

ステップ 6　ポリシー マップをグローバルに、または特定のインターフェイスに適用するには、**service-policy** コマンドを次のように使用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface
interface_ID]
hostname(config)#
```

policy_map_name は、ステップ 3 で設定したポリシー マップです。ポリシー マップをすべてのインターフェイス上のトラフィックに適用する場合、**global** オプションを使用します。ポリシー マップを特定のインターフェイス上のトラフィックに適用する場合、***interface*** *interface_ID* オプションを使用します。*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

FWSM は、指定のとおりに CTIQBE トラフィックの検査を開始します。

例 20-1　CTIQBE 検査のイネーブル化および設定

次に、デフォルト ポート（2748）の CTIQBE トラフィックと一致し、CTIQBE トラフィックと一致するクラスを使用して、ポリシーで CTIQBE 検査をイネーブルにするクラス マップを作成する例を示します。それからサービス ポリシーを外部インターフェイスに適用します。

```
hostname(config)# class-map ctiqbe_port
hostname(config-cmap)# match port tcp eq 2748
hostname(config-cmap)# policy-map sample_policy
hostname(config-pmap)# class ctiqbe_port
hostname(config-pmap-c)# inspect ctiqbe
hostname(config-pmap-c)# service-policy sample_policy interface outside
hostname(config)#
```

CTIQBE 検査の確認およびモニタ

show ctiqbe コマンドは、FWSM を超えて確立された CTIQBE セッションに関する情報を表示します。このコマンドは、CTIQBE インスペクション エンジンによって割り当てられたメディア接続に関する情報を示します。

次に、以下の条件における **show ctiqbe** コマンドの出力例を示します。FWSM を越えてセットアップされているアクティブ CTIQBE セッションは 1 つだけです。そのセッションは、ローカル アドレス 10.0.0.99 の内部 CTI デバイス（たとえば、Cisco IP SoftPhone）と 172.29.1.77 の外部 Cisco Call Manager の間で確立されています。ここで、TCP ポート 2748 は Cisco CallManager です。このセッションのハートビート間隔は 120 秒です。

```
hostname# # show ctiqbe

Total: 1
        LOCAL           FOREIGN         STATE   HEARTBEAT
-----------------------------------------------------------------
1       10.0.0.99/1117  172.29.1.77/2748        1       120
        ---------------------------------------------
        RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 - 1029)
        ---------------------------------------------
        MEDIA: Device ID 27     Call ID 0
               Foreign 172.29.1.99      (1028 - 1029)
               Local   172.29.1.88      (26822 - 26823)
        ---------------------------------------------
```

CTI デバイスは、CallManager に登録済みです。デバイスの内部アドレスと RTP リスニング ポートは、172.29.1.99 UDP ポート 1028 に PAT 変換されます。その RTCP リスニング ポートは、UDP 1029 に PAT 変換されます。

`RTP/RTCP:PAT xlates:` で始まる行は、内部 CTI デバイスが外部 CallManager に登録され、CTI デバイスのアドレスとポートがその外側インターフェイスに PAT 変換されている場合にのみ、表示されます。この行は、CallManager が内側インターフェイス上に位置する場合、または内部 CTI デバイスのアドレスとポートが、CallManager が使用しているのと同じ外側インターフェイスに NAT 処理されている場合は、表示されません。

この出力は、コールがこの CTI デバイスと 172.29.1.88 にある別の電話の間に確立されていることを示します。他の電話の RTP および RTCP リスニング ポートは、UDP 26822 および 26823 です。FWSM は 2 番めの電話と CallManager に関連する CTIQBE セッション レコードを維持できないので、他の電話は CallManager と同じインターフェイス上にあります。CTI デバイス側のアクティブ コール レグは、Device ID 27 および Call ID 0 で確認できます。

次に、これらの CTIBQE 接続に対する **show xlate debug** コマンドの出力例を示します。

```
hostname# show xlate debug
3 in use, 3 most used
Flags:  D - DNS, d - dump, I - identity, i - inside, n - no random,
        r - portmap, s - static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
```

show conn state ctiqbe　コマンドは、CTIQBE 接続のステータスを表示します。出力には、CTIQBE インスペクション エンジンによって割り当てられたメディア接続が「C」フラグで示されます。次に、**show conn state ctiqbe** コマンドの出力例を示します。

```
hostname# show conn state ctiqbe
1 in use, 10 most used
hostname# show conn state ctiqbe detail
1 in use, 10 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, 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 - Skinny media,
       M - SMTP data, m - SIP media, O - outbound data, P - inside back connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
```

DNS 検査

ここでは、DNS アプリケーション検査を管理する手順について説明します。次の内容について説明します。

- DNS アプリケーション検査の動作（p.20-13）
- DNS Rewrite の動作（p.20-14）
- DNS Rewrite の設定（p.20-15）
- DNS 検査の設定（p.20-20）
- DNS 検査の確認およびモニタ（p.20-21）

DNS アプリケーション検査の動作

FWSM によって DNS 応答が転送されると、FWSM は DNS クエリーに対応付けられた DNS セッションをただちに終了します。FWSM はまた、DNS 応答の ID が DNS クエリーの ID と一致していることを確認するために、メッセージ交換をモニタします。

デフォルトで DNS 検査はイネーブルの場合、FWSM は、次の作業を追加します。

- **alias**、**static**、**nat** コマンドを使用して設定を作成し、これに基づいて DNS レコードを変換します（DNS Rewrite）。変換は DNS 応答の A レコードにのみ適用されます。したがって、DNS Rewrite は PTR レコードを要求するリバース検索に影響を及ぼしません。

（注） 複数の PAT 規則が各 A レコードに適用され、使用する PAT 規則があいまいになるので、DNS Rewrite は PAT には適用されません。

- DNS メッセージの最大長を適用します（デフォルトは 512 バイトで、最大長は 65,535 バイト）。パケット長が設定済みの最大長以下であるか確認するため、FWSM は必要に応じてリアセンブリします。パケット長が最大長を超えた場合、FWSM はパケットを廃棄します。

（注） **maximum-length** オプションを指定しないで **inspect dns** コマンドを入力すると、DNS パケット サイズは検証されません。

- ドメイン名の長さを 255 バイトに、ラベルの長さを 63 バイトにします。
- 圧縮ポインタが DNS メッセージ内で発生すると、ポインタによって参照されるドメイン名の正当性を確認します。
- 圧縮ポインタのループが存在するかどうか検証します。

複数の DNS セッションが同じ 2 つのホストの間にあり、セッションが同じ 5 つのタプル（送信元 / 宛先 IP アドレス、送信元 / 宛先ポート、プロトコル）を取得していれば、単一の接続がこの複数の DNS セッション用に作成されます。DNS 識別は、*app_id* によって追跡され、各 app_id のアイドル タイマーは独立して動作します。

app_id は独立してタイムアウトになるので、正規の DNS 応答は制限された時間内で FWSM を通過するだけで、リソース構築はされません。ただし、**show conn** コマンドを入力すると、新しい DNS セッションによってリセットされる DNS 接続のアイドル タイマーが表示されます。これは共有の DNS 接続の特性と設計によるものです。

DNS Rewrite の動作

DNS 検査がイネーブルの場合、DNS Rewrite は任意のインターフェイスから発信される DNS メッセージの NAT を完全にサポートします。

内部ネットワーク上のクライアントが外部インターフェイス上の DNS サーバからの内部アドレスの DNS 解決を要求した場合、DNS A レコードは正しく変換されます。DNS インスペクション エンジンがディセーブルの場合、A レコードは変換されません。

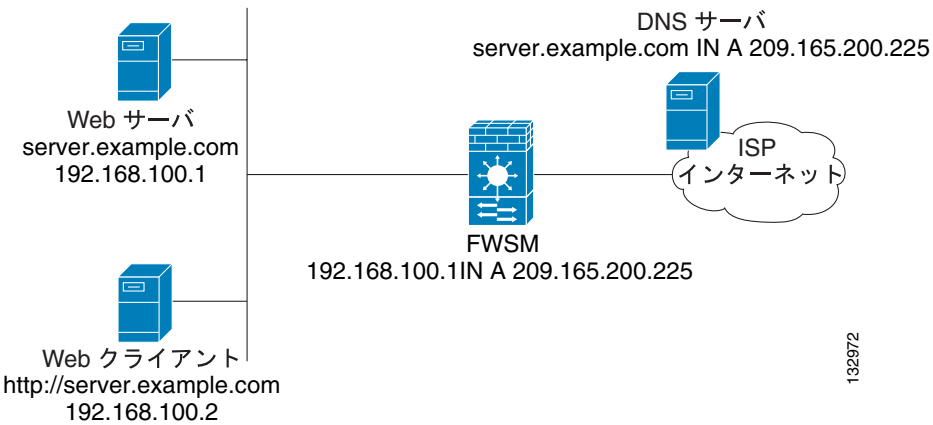
DNS 検査がイネーブルであれば、**alias**、**static** または **nat** コマンドを使用して、DNS Rewrite を設定できます。必要な設定の詳細については、「DNS Rewrite の設定」（p.20-15）を参照してください。

DNS Rewrite は次の 2 つの機能を実行します。

- DNS クライアントがプライベート インターフェイス上にある場合、DNS 応答のパブリック アドレス（ルーティング可能な、または「マッピングされた」アドレス）を、プライベート アドレス（「実」アドレス）に変換します。
- DNS クライアントがパブリック インターフェイス上にある場合、プライベート アドレスをパブリック アドレスに変換します。

図 20-2 では、DNS サーバは外部（ISP）ネットワーク上に存在します。FWSM では、**static** コマンドは、Web サーバ（192.168.100.1）の実アドレスを ISP 割り当てアドレス（209.165.200.5）へマッピングします。内部インターフェイス上の Web クライアントが、URL http://server.example.com の Web サーバにアクセスしようとすると、Web クライアントが稼働するホストは Web サーバの IP アドレスを解決するため、DNS サーバに DNS 要求を送信します。FWSM は、IP ヘッダー内のルーティング不可能な送信元アドレスを変換して、その外部インターフェイス上の ISP ネットワークに要求を転送します。DNS 応答が返送されると、FWSM は宛先アドレスだけでなく、Web サーバの組み込み IP アドレスにもアドレス変換を適用します。この組み込み IP アドレスは、DNS 応答の A レコードに含まれています。結果として、内部ネットワーク上の Web クライアントは、内部ネットワーク上の Web サーバとの接続に必要な正しいアドレスを取得します。この例の NAT および DNS コンフィギュレーションの詳細については、例 20-2 を参照してください。これと同様の事例に関する設定手順については、「2 つの NAT ゾーンを使用した DNS Rewrite の設定」（p.20-16）を参照してください。

図 20-2　2 つの NAT ゾーンを使用した DNS Rewrite



DNS 要求を行うクライアントが DMZ ネットワーク上にあり、DNS サーバが内部インターフェイス上にある場合にも、DNS Rewrite は機能します。この事例に関する図および設定手順については、「3 つの NAT ゾーンを使用した DNS Rewrite」（p.20-17）を参照してください。

DNS Rewrite の設定

alias、**static**、または **nat** コマンドを使用して、DNS Rewrite を設定できます。**alias** および **static** コマンドは同じ意味で使用されます。ただし、**static** コマンドはより正確ではっきりしているので、新しい配置に使用することを推奨します。また、DNS Rewrite は **static** コマンド使用時のオプションです。

ここでは、**alias** および **static** コマンドを使用して DNS Rewrite を設定する手順について説明します。単純な事例や複雑な事例で、**static** コマンドを使用する設定手順を提供します。**nat** コマンドの使用は、DNS Rewrite がスタティック マッピングではなくダイナミック変換に基づいている点を除いて、**static** コマンドの使用と同様です。

次の内容について説明します。

- DNS Rewrite の alias コマンドの使用（p.20-15）
- DNS Rewrite の static コマンドの使用（p.20-15）
- 2 つの NAT ゾーンを使用した DNS Rewrite の設定（p.20-16）
- 3 つの NAT ゾーンを使用した DNS Rewrite（p.20-17）
- 3 つの NAT ゾーンを使用した DNS Rewrite の設定（p.20-19）

alias、**nat**、**static** コマンドの詳細な構文およびその他の機能については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の対応する コマンド ページを参照してください。

DNS Rewrite の alias コマンドの使用

alias コマンドを使用すると、FWSM は、*任意のインターフェイス*に存在する IP ネットワーク上のアドレスを、異なるインターフェイスを介して接続された別の IP ネットワークのアドレスに変換できます。このコマンドの構文は、次のとおりです。

```
hostname(config)# alias (inside) mapped-address real-address
```

次に、内部インターフェイス*以外の*任意のインターフェイス上の実アドレス（192.168.100.10）を、内部インターフェイス上でマッピングされたアドレス（209.165.200.225）に変換する例を示します。192.168.100.10 の場所は厳密に定義されていないことに注意してください。

```
hostname(config)# alias (inside) 209.165.200.225 192.168.100.10
```

（注） DNS Rewrite を設定するのに **alias** コマンドを使用する場合、マッピングされたアドレスに対してプロキシ ARP が実行されます。これを回避するには、**alias** コマンドを入力したあとに、**sysopt noproxyarp internal_interface** コマンドを入力することで、プロキシ ARP をディセーブルにします。

DNS Rewrite の static コマンドの使用

static コマンドを使用すると、*特定のインターフェイス*に存在する IP ネットワーク上のアドレスを、異なるインターフェイス上の別の IP ネットワークのアドレスに変換できます。このコマンドの構文は、次のとおりです。

```
hostname(config)# static (inside,outside) mapped-address real-address dns
```

次に、内部インターフェイス上のアドレス 192.168.100.10 を外部インターフェイス上の 209.165.200.5 に変換する例を示します。

```
hostname(config)# static (inside,outside) 209.165.200.225 192.168.100.10 dns
```

（注）　**nat** コマンドの使用は、DNS Rewrite がスタティック マッピングではなくダイナミック変換に基づいている点を除いて、**static** コマンドの使用と同様です。

2 つの NAT ゾーンを使用した DNS Rewrite の設定

図 20-2 で示す事例のような DNS Rewrite の事例を実装する手順は、次のとおりです。

ステップ 1　次のように、Web サーバ用にスタティックな変換を作成します。

```
hostname(config)# static (inside,outside) mapped-address real-address netmask
255.255.255.255 dns
```

引数は次のとおりです。

- *inside* — FWSM の内部インターフェイスの名前
- *outside* — FWSM の外部インターフェイスの名前
- *mapped-address* — Web サーバの変換された IP アドレス
- *real-address* — Web サーバの IP 実アドレス

ステップ 2　HTTP 要求に対し、Web サーバが待ち受けるポートへのトラフィックを許可するアクセス リストを作成します。

```
hostname(config)# access-list acl-name permit tcp any host mapped-address eq port
```

引数は次のとおりです。

acl-name — アクセス リストに付けた名前

mapped-address — Web サーバの変換された IP アドレス

port — HTTP 要求に対し、Web サーバが待ち受ける TCP ポート

ステップ 3　ステップ　2　で作成したアクセス　リストを外部インターフェイスに適用します。そのためには、**access-group** コマンドを次のように使用します。

```
hostname(config)# access-group acl-name in interface outside
```

ステップ 4　DNS 検査がディセーブルである、または DNS 最大パケット長を変更する場合、DNS 検査を設定します。DNS アプリケーション検査はデフォルトではイネーブルで、DNS 最大パケット長は 512 バイトです。設定手順については、「DNS 検査の設定」（p.20-20）を参照してください。

ステップ 5　パブリック DNS サーバ上では、次のような Web サーバの A レコードを追加します。

```
domain-qualified-hostname. IN A mapped-address
```

domain-qualified-hostname は、server.example.com のようなドメイン サフィックスのあるホスト名です。ホスト名のあとのピリオドは重要です。*mapped-address* は、Web サーバの変換された IP アドレスです。

次に、図 20-2 で示す事例の FWSM を設定する例を示します。DNS 検査はすでにイネーブルであるとみなされます。

例 20-2　2 つの NAT ゾーンを使用した DNS Rewrite

```
hostname(config)# static (inside,outside) 209.165.200.225 192.168.100.1 netmask
255.255.255.255 dns
hostname(config)# access-list 101 permit tcp any host 209.165.200.225 eq www
hostname(config)# access-group 101 in interface outside
```

この設定は DNS サーバ上の次の A レコードを必要とします。

```
server.example.com. IN A 209.165.200.225
```

3 つの NAT ゾーンを使用した DNS Rewrite

図 20-3 に、より複雑な事例を示します。DNS 検査により、NAT は、最低限設定された DNS サーバを使用して透過的に動作できます。これと同様の事例に関する設定手順については、「3 つの NAT ゾーンを使用した DNS Rewrite の設定」（p.20-19）を参照してください。

図 20-3　3 つの NAT ゾーンを使用した DNS Rewrite

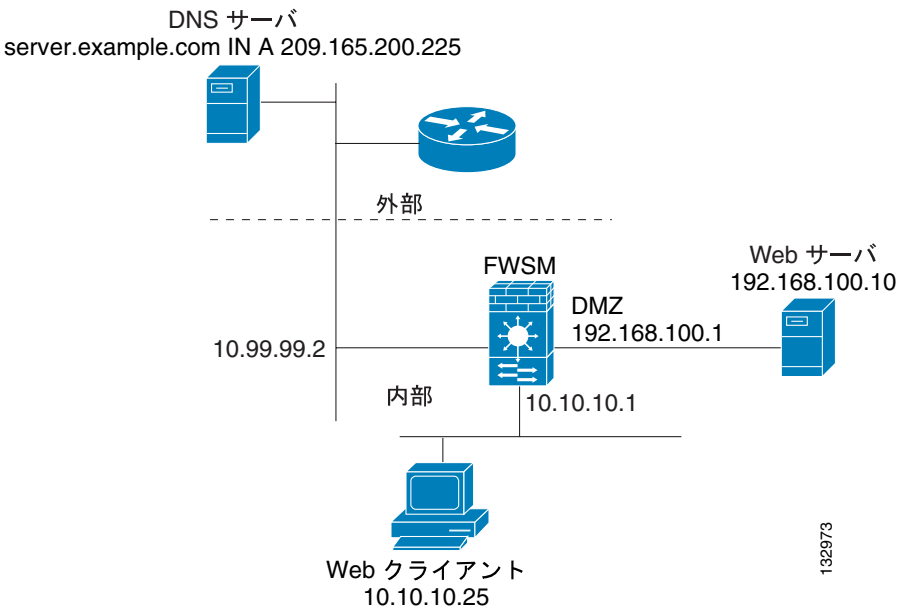


図 20-3 では、Web サーバ（server.example.com）には FWSM の DMZ インターフェイス上に実アドレス 192.168.100.10 があります。IP アドレス 10.10.10.25 を持つ Web クライアントは内部インターフェイス上にあり、パブリック DNS サーバは外部インターフェイス上にあります。サイト NAT ポリシーは次のとおりです。

- 外部 DNS サーバは、server.example.com 用に信頼性のあるアドレス レコードを保有します。
- 外部ネットワーク上のホストは、外部 DNS サーバ経由でドメイン名 server.example.com を持つ Web サーバ、または IP アドレス 209.165.200.225 を持つ Web サーバに接続できます。
- 内部ネットワーク上のクライアントは、外部 DNS サーバ経由でドメイン名 server.example.com を持つ Web サーバ、または IP アドレス 192.168.100.10 を持つ Web サーバにアクセスできます。

任意のインターフェイス上のホストまたはクライアントが DMZ Web サーバにアクセスする場合、サーバは server.example.com の A レコードに関して公開 DNS サーバに照会します。DNS サーバは、server.example.com がアドレス 209.165.200.225 にバインドすることを示す A レコードを戻します。

*外部*ネットワーク上の Web クライアントが http://server.example.com にアクセスしようとすると、次のイベントが発生します。

1. Web クライアントを実行するホストは、DNS サーバに server.example.com の IP アドレスの要求を送信します。
2. DNS サーバは、IP アドレス 209.165.200.225 で応答します。
3. Web クライアントはその HTTP 要求を 209.165.200.225 に送信します。
4. 外部ホストからのパケットは、外部インターフェイスで FWSM に到達します。
5. スタティック規則はアドレス 209.165.200.225 を 192.168.100.10 に変換し、FWSM は DMZ 上の Web サーバにパケットを転送します。

*内部*ネットワーク上の Web クライアントが http://server.example.com にアクセスしようとすると、次のイベントが発生します。

1. Web クライアントを実行するホストは、DNS サーバに server.example.com の IP アドレスの要求を送信します。
2. DNS サーバは、IP アドレス 209.165.200.225 で応答します。
3. FWSM は DNS 応答を受信し、DNS アプリケーション インスペクション エンジンに応答を送信します。
4. DNS アプリケーション インスペクション エンジンは以下を行います。
   a. 組み込み A レコード アドレス（[outside]:209.165.200.5）の変換を元に戻す NAT 規則を検索します。次に、スタティック コンフィギュレーションの例を示します。

      ```
      static (dmz,outside) 209.165.200.225 192.168.100.10 dns
      ```

   b. **dns** オプションが含まれているので、スタティック規則を使用して A レコードを次のように書き換えます。

      ```
      [outside]:209.165.200.225 --> [dmz]:192.168.100.10
      ```

      （注） **dns** オプションは、**static** コマンドに含まれていないので、DNS Rewrite は実行されず、他のパケット処理が継続されます。

   c. 内部 Web クライアントと通信する場合、Web サーバ アドレス（[dmz]:192.168.100.10）を変換する NAT を検索します。

      NAT 規則は適用されないので、アプリケーション検査が完了します。

      NAT 規則（nat または static）を適用する場合、**dns** オプションを指定する必要があります。**dns** オプションを指定しない場合、ステップ b の A レコードの書き換えは無効になり、他のパケット処理が継続されます。
5. FWSM は、HTTP 要求を DMZ インターフェイス上の server.example.com に送信します。

3 つの NAT ゾーンを使用した DNS Rewrite の設定

図 20-3 の事例の NAT ポリシーをイネーブルにする手順は、次のとおりです。

ステップ 1　次のように、DMZ ネットワーク上の Web サーバにスタティックな変換を作成します。

```
hostname(config)# static (dmz,outside) mapped-address real-address dns
```

引数は次のとおりです。

- *dmz* — FWSM の DMZ インターフェイスの名前
- *outside* — FWSM の外部インターフェイスの名前
- *mapped-address* — Web サーバの変換された IP アドレス
- *real-address* — Web サーバの IP 実アドレス

ステップ 2　HTTP 要求に対し、Web サーバが待ち受けるポートへのトラフィックを許可するアクセス リストを作成します。

```
hostname(config)# access-list acl-name permit tcp any host mapped-address eq port
```

引数は次のとおりです。

acl-name — アクセス リストに付けた名前

mapped-address — Web サーバの変換された IP アドレス

port — HTTP 要求に対し、Web サーバが待ち受ける TCP ポート

ステップ 3　ステップ　2　で作成したアクセス　リストを外部インターフェイスに適用します。そのためには、**access-group** コマンドを次のように使用します。

```
hostname(config)# access-group acl-name in interface outside
```

ステップ 4　DNS 検査がディセーブルである、または DNS 最大パケット長を変更する場合、DNS 検査を設定します。DNS アプリケーション検査はデフォルトではイネーブルで、DNS 最大パケット長は 512 バイトです。設定手順については、「DNS 検査の設定」（p.20-20）を参照してください。

ステップ 5　パブリック DNS サーバ上では、次のような Web サーバの A レコードを追加します。

```
domain-qualified-hostname. IN A mapped-address
```

domain-qualified-hostname は、server.example.com のようなドメイン サフィックスのあるホスト名です。ホスト名のあとのピリオドは重要です。*mapped-address* は、Web サーバの変換された IP アドレスです。

次に、図 20-3 で示す事例の FWSM を設定する例を示します。DNS 検査はすでにイネーブルであるとみなされます。

例 20-3　3 つの NAT ゾーンを使用した DNS Rewrite

```
hostname(config)# static (dmz,outside) 209.165.200.225 192.168.100.10 dns
hostname(config)# access-list 101 permit tcp any host 209.165.200.225 eq www
hostname(config)# access-group 101 in interface outside
```

この設定は DNS サーバ上の次の A レコードを必要とします。

```
server.example.com. IN A 209.165.200.225
```

DNS 検査の設定

DNS 検査はデフォルトではイネーブルです。

DNS 検査をイネーブルにする（検査が以前にディセーブルであった場合に）、または DNS トラフィックの受信に使用するデフォルト ポートを変更するには、次の手順を実行します。

ステップ 1　DNS トラフィックを識別するには、クラス マップを作成するか、または既存のクラス マップを変更します。**class-map** コマンドを次のように使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

class_map_name は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI はクラス マップ 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　**match port** コマンドを使用して、DNS トラフィックを識別します。DNS のデフォルト ポートは UDP ポート 53 です。

```
hostname(config-cmap)# match port udp eq 53
```

ステップ 3　DNS インスペクション エンジンを FTP トラフィックに適用するために使用するポリシー マップを作成するか、または 既存のポリシー マップを変更します。そのためには、**policy-map** コマンドを次のように使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

policy_map_name は、ポリシー マップの名前です。CLI はポリシー マップ コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 4　DNS アプリケーション検査をイネーブルにします。そのためには、**inspect dns** コマンドを次のように使用します。

```
hostname(config-pmap-c)# inspect dns [maximum-length max-pkt-length]
```

DNS パケットの最大長をデフォルト（512）から変更するには、***maximum-length*** 引数を使用して、*max-pkt-length* に新しい数値を指定します。長いパケットは廃棄されます。DNS パケット長の検証をディセーブルにするには、**maximum-length** キーワードを指定しないで **inspect dns** コマンドを入力します。

ステップ 5　ポリシー マップをグローバルに、または特定のインターフェイスに適用するには、**service-policy** コマンドを次のように使用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface
interface_ID]
hostname(config)#
```

policy_map_name は、ステップ 3 で設定したポリシー マップです。ポリシー マップをすべてのインターフェイス上のトラフィックに適用する場合、**global** オプションを使用します。ポリシー マップを特定のインターフェイス上のトラフィックに適用する場合、***interface*** *interface_ID* オプションを使用します。*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

FWSM は、指定のとおりに DNS トラフィックの検査を開始します。

例 20-4　DNS 検査のイネーブル化および設定

次に、デフォルト ポート（53）上の DNS トラフィックと一致するクラス マップを作成し、sample_policy ポリシー マップで DNS 検査をイネーブルにし、DNS 検査を外部インターフェイスに適用する例を示します。

```
hostname(config)# class-map dns_port
hostname(config-cmap)# match port udp eq 53
hostname(config-cmap)# policy-map sample_policy
hostname(config-pmap)# class dns_port
hostname(config-pmap-c)# inspect dns maximum-length 1500
hostname(config-pmap-c)# service-policy sample_policy interface outside
```

DNS 検査の確認およびモニタ

現在の DNS 接続に関する情報を表示するには、次のコマンドを入力します。

```
hostname# show conn
```

DNS サーバを使用した接続については、接続の送信元ポートは、show conn コマンド出力で DNS サーバの IP アドレスに置き換えられる場合があります。

複数の DNS セッションが同じ 2 つのホストの間にあり、セッションが同じ 5 つのタプル（送信元 / 宛先 IP アドレス、送信元 / 宛先ポート、プロトコル）を取得していれば、単一の接続がこの DNS セッション用に作成されます。DNS 識別は、app_id によって追跡され、各 app_id のアイドル タイマーは独立して動作します。

app_id は独立してタイムアウトになるので、正規の DNS 応答は制限された時間内で FWSM を通過するだけで、リソース構築はされません。ただし、**show conn** コマンドを入力すると、新しい DNS セッションによってリセットされる DNS 接続のアイドル タイマーが表示されます。これは共有 DNS 接続の特性と設計によるものです。

DNS アプリケーション検査の統計情報を表示するには、**show service-policy** コマンドを入力します。次に、**show service-policy** コマンドの出力例を示します。

```
hostname# show service-policy
Interface outside:
  Service-policy: sample_policy
    Class-map: dns_port
      Inspect: dns maximum-length 1500, packet 0, drop 0, reset-drop 0
```

FTP 検査

ここでは、FTP インスペクション エンジンの機能と、その設定を変更する手順について説明します。次の内容について説明します。

- FTP 検査の概要（p.20-22）
- strict オプションの使用（p.20-22）
- request-command deny コマンド（p.20-23）
- FTP 検査の設定（p.20-24）
- FTP 検査の確認およびモニタ（p.20-27）

FTP 検査の概要

FTP アプリケーション検査は FTP セッションを検査し、4 つのタスクを実行します。

- 動的なセカンダリ データ接続の準備
- ***ftp*** コマンドの応答シーケンスの追跡
- 監査証跡の生成
- 組み込み IP アドレスの NAT 処理

FTP アプリケーション検査によって、FTP データ転送用にセカンダリ チャネルが用意されます。チャネルのポートは、PORT コマンドまたは PASV コマンドを使用してネゴシエートされます。チャネルは、ファイルのアップロード、ファイルのダウンロード、またはディレクトリ リスト イベントの応答として割り当てられます。

（注） **no inspect ftp** コマンドを使用して FTP インスペクション エンジンをディセーブルにした場合、発信ユーザが接続を開始できるのはパッシブ モードだけで、すべての着信 FTP はディセーブルになります。

strict オプションの使用

inspect ftp コマンドで **strict** オプションを使用すると、Web ブラウザが FTP 要求に組み込まれたコマンドを送信することを防止でき、保護ネットワークのセキュリティを向上させます。

ヒント FWSM を通過することを許可されていない FTP コマンドを指定するには、FTP マップを作成し、FTP マップ コンフィギュレーション モードで **request-command deny** コマンドを入力します。

インターフェイスで **strict** オプションがイネーブルになったあと、FTP 検査は次の処理を実行します。

- FWSM が新しいコマンドを許可する前に、FTP コマンドに対して確認応答が返される必要があります。
- FWSM は、組み込みコマンドを送信する接続を廃棄します。
- 227 コマンドと PORT コマンドは、エラー文字列に表示されないように検証されます。

注意　*strict* オプションを使用すると、FTP RFC に厳密に準拠しない FTP クライアントの障害が発生する場合があります。

strict オプションがイネーブルである場合、次の異常動作について、各 ***ftp*** コマンドと応答シーケンスが追跡されます。

- 不完全なコマンド — PORT および PASV 応答コマンド内のカンマ数が 5 つかどうかが確認されます。5 つ以外の場合、PORT コマンドは不完全であるとみなされ、TCP 接続は終了します。
- 不正コマンド — RFC に規定されているように、***ftp*** コマンドが <CR><LF> 文字で終了しているかどうかが確認されます。異なっている場合、接続は終了します。
- RETR コマンドおよび STOR コマンドのサイズ — 固定数になっているかどうかが確認されます。サイズが大きい場合、エラー メッセージが記録され、接続は終了します。
- コマンド スプーフィング — PORT コマンドは常にクライアントから送信される必要があります。PORT コマンドがサーバから送信されている場合、TCP 接続は拒否されます。
- 応答スプーフィング — PASV 応答コマンド（227）は常にサーバから送信される必要があります。PASV 応答コマンドがクライアントから送信されている場合、TCP 接続は拒否されます。これにより、ユーザが「227 xxxxx a1, a2, a3, a4, p1, p2」を実行した場合のセキュリティ ホールが防止されます。
- TCP ストリーム編集 — TCP ストリーム編集が検出されると、FWSM は接続を終了します。
- 無効なポートのネゴシエーション — ネゴシエートされたダイナミック ポートの値が 1024 未満かどうかが確認されます。1 ～ 1024 のポート番号は well-known 接続用に予約されているので、ネゴシエートされたポートがこの範囲内の場合には、TCP 接続は解放されます。
- コマンドのパイプライン化 — PORT コマンドおよび PASV 応答コマンド内のポート番号よりあとの文字数が、定数の 8 であるかどうかが相互確認されます。8 を超えている場合、TCP 接続は終了します。
- FWSM は、SYST コマンドに対する FTP サーバの応答を一連の X に置き換え、サーバが FTP クライアントに対し、そのシステム タイプを開示するのを回避します。このデフォルト動作を上書きするには、FTP マップ コンフィギュレーション モードで **no mask-syst-reply** コマンドを使用します。

request-command deny コマンド

request-command deny コマンドを使用すると、FWSM がどの FTP コマンドに対し、FTP トラフィックが FWSM を通過する許可を与えるか制御できます。このコマンドは FTP マップ コンフィギュレーション モードで利用可能です。そのため、このコマンドを利用するには、「FTP 検査の設定」（p.20-24）に従って FTP マップを作成し、FTP 検査をイネーブルにするときにそのマップを使用する必要があります。

表 20-2 に、**request-command deny** コマンドを使用することで、許可できなくする FTP コマンドを示します。

表 20-2　FTP マップの request-command deny オプション

request-command deny オプション	目的
appe	ファイルに追加するコマンドを許可しません。
cdup	現在のワーキング ディレクトリのペアレント ディレクトリに変わるコマンドを許可しません。
dele	サーバのファイルを削除するコマンドを許可しません。

表 20-2　FTP マップの request-command deny オプション（続き）

request-command deny オプション	目的
get	サーバからファイルを検索するクライアント コマンドを許可しません。
help	ヘルプ情報を提供するコマンドを許可しません。
mkd	サーバ上にディレクトリを作成するコマンドを許可しません。
put	サーバにファイルを送信するクライアント コマンドを許可しません。
rmd	サーバ上のディレクトリを削除するコマンドを許可しません。
rnfr	ファイル名から rename を指定するコマンドを許可しません。
rnto	ファイル名へ rename を指定するコマンドを許可しません。
site	サーバ システムに固有なコマンドを許可しません。通常はリモート管理用に使用されます。
stou	一意なファイル名を使用してファイルを保存するコマンドを許可しません。

FTP 検査の設定

FTP アプリケーション検査はデフォルトではイネーブルなので、次の方法で手順を実行する必要があるのはデフォルトの FTP 設定を変更する場合だけです。

- **strict** オプションをイネーブルにします。
- FWSM を通過することを許可されていない特定の FTP コマンドを識別します。
- デフォルトのポート番号を変更します。

FTP 検査を設定する手順は、次のとおりです。

ステップ 1　FWSM の後ろで FTP サーバが待ち受けるポートを決定します。デフォルトの FTP ポートは TCP ポート 21 です。ただし、thwart 攻撃に対する簡単な手段として、代替ポートがしばしば使用されます。すべての FTP トラフィックを検査することを確認するには、TCP ポート 21 以外のポートの使用に関して、FTP サーバを検証してください。

ステップ 2　FTP トラフィックを識別するには、クラス マップを作成するか、または既存のクラス マップを変更します。**class-map** コマンドを次のように使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

class_map_name は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI はクラス マップ コンフィギュレーション モードを開始します。

ステップ 3　ステップ 1 で決定した FTP ポートに送信されたトラフィックを識別します。そのためには、**match port** または **match access-list** コマンドを使用します。

連続しない複数のポートを特定する必要がある場合、**access-list extended** コマンドを使用してアクセス リストを作成し、各ポートと一致する Access Control Entry（ACE; アクセス制御エントリ）を追加してから、**match access-list** コマンドを使用します。次のコマンドは、アクセス リストを使用して、アクセス リストを持った複数の TCP ポートを特定します。

```
hostname(config)# access-list acl-name any any tcp eq port_number_1
hostname(config)# access-list acl-name any any tcp eq port_number_2
hostname(config)# class-map class_map_name
hostname(config-cmap)# match access-list acl-name
```

単一ポートを特定する必要がある場合、次のように **match port** コマンドを使用します。

```
hostname(config-cmap)# match port tcp port_number
```

port_number は、FWSM の後ろの FTP サーバが待ち受ける TCP ポートのみです。

単一プロトコルの連続したポート範囲を特定する必要がある場合、次のように **range** キーワードを指定して **match port** コマンドを使用します。

```
hostname(config-cmap)# match port tcp range begin_port_number end_port_number
```

begin_port_number は、FTP ポート範囲の最小ポートで、*end_port_number* は最大ポートです。

ステップ 4　（任意）FTP 検査を実行する場合は、次の手順を実行します。

- FTP クライアントに対して、FTP サーバのシステム タイプの開示を許可します。
- 許可された FTP コマンドを制限します。

FTP マップを作成して、設定します。そのためには、次の手順を実行します。

a. FTP 検査の追加パラメータを含んだ FTP マップを作成します。**ftp-map** コマンドを次のように使用します。

```
hostname(config-cmap)# ftp-map map_name
hostname(config-ftp-map)#
```

map_name は、FTP マップの名前です。CLI は、FTP マップ コンフィギュレーション コマンドを開始します。

b. （任意）SYST メッセージに応答して、FTP サーバにシステム タイプを FTP クライアントに開示させる場合、次のように **mask-syst-reply** コマンドの **no** 形式を使用します。

```
hostname(config-ftp-map)# no mask-syst-reply
hostname(config-ftp-map)#
```

（注）　デフォルトでは、FTP 検査がイネーブルである場合、SYST メッセージへの応答はマスクされます。SYST 応答マスキングをディセーブルにした場合、**mask-syst-response** コマンドを使用して、マスキングを再度イネーブルにできます。

c. （任意）特定の FTP コマンドを許可しない場合、**request-command deny** コマンドを使用して、許可しない各 FTP コマンドを次のように指定します。

```
hostname(config-ftp-map)# request-command deny ftp_command [ftp_command...]
hostname(config-ftp-map)#
```

ftp_command は、制限する 1 つまたは複数の FTP コマンドです。制限可能な FTP コマンドのリストについては、表 20-2 を参照してください。

ステップ 5　FTP インスペクション エンジンを FTP トラフィックに適用するために使用するポリシー マップを作成するか、または既存のポリシー マップを変更します。そのためには、**policy-map** コマンドを次のように使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

policy_map_name は、ポリシー マップの名前です。CLI はポリシー マップ コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 6　ステップ 2 で作成したクラス マップを指定します。このクラス マップは FTP トラフィックを識別します。**class** コマンドを次のように使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name は、ステップ 2 で作成したクラス マップの名前です。CLI はポリシー マップ クラス コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 7　必要なオプションを指定して、FTP　アプリケーション検査をイネーブルにします。そのためには、次の手順のいずれかを実行します。

- 完全な FTP 検査をイネーブルにする場合、次のように ***strict*** キーワードを指定して、**inspect ftp** コマンドを使用します。

  ```
  hostname(config-pmap-c)# inspect ftp strict
  ```

- ステップ 4 で設定したオプションの FTP マップを使用して完全な FTP 検査をイネーブルにする場合、次のように ***strict*** キーワードと FTP マップ名を指定して、**inspect ftp** コマンドを使用します。

  ```
  hostname(config-pmap-c)# inspect ftp strict ftp_map_name
  ```

- デフォルトの FTP 検査に戻す場合、次のように キーワードを指定しないで、**inspect ftp** コマンドを使用します。

  ```
  hostname(config-pmap-c)# inspect ftp
  ```

ステップ 8　ポリシー マップをグローバルに、または特定のインターフェイスに適用するには、**service-policy** コマンドを次のように使用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface
interface_ID]
hostname(config)#
```

policy_map_name は、ステップ 5 で設定したポリシー マップです。ポリシー マップをすべてのインターフェイス上のトラフィックに適用する場合、**global** オプションを使用します。ポリシー マップを特定のインターフェイス上のトラフィックに適用する場合、***interface*** *interface_ID* オプションを使用します。*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

FWSM は、指定のとおりに FTP トラフィックの検査を開始します。

次に、FTP トラフィックを識別し、FTP マップを定義し、ポリシーを定義し、そのポリシーを外部インターフェイスに適用する例を示します。

例 20-5　完全な FTP 検査のイネーブル化および設定

```
hostname(config)# class-map ftp_port
hostname(config-cmap)# match port tcp eq 21
hostname(config-cmap)# ftp-map sample_map
hostname(config-ftp-map)# request-command deny put stou appe
hostname(config-ftp-map)# policy-map sample_policy
hostname(config-pmap)# class ftp_port
hostname(config-pmap-c)# inspect ftp strict sample_map
hostname(config-pmap-c)# service-policy sample_policy interface outside
```

FTP 検査の確認およびモニタ

FTP アプリケーション検査では、次のログ メッセージが生成されます。

- 取り込まれた、またはアップロードされた各ファイルについて、監査記録 302002 が生成されます。
- FTP コマンドが RETR または STOR であるかを判断するため検証され、retrieve コマンドおよび store コマンドが記録されます。
- ユーザ名は、IP アドレスを提供するテーブルを検索することで取得されます。
- ユーザ名、送信元 IP アドレス、宛先 IP アドレス、NAT アドレス、ファイル操作が記録されます。
- メモリ不足によってセカンダリ ダイナミック チャネルの準備に失敗した場合、監査記録 201005 が生成されます。

NAT と連携することにより、FTP アプリケーション検査では、アプリケーション ペイロード内の IP アドレスが変換されます。詳細については RFC 959 に規定されています。

GTP 検査

ここでは、GTP インスペクション エンジンの機能と、その設定を変更する手順について説明します。次の内容について説明します。

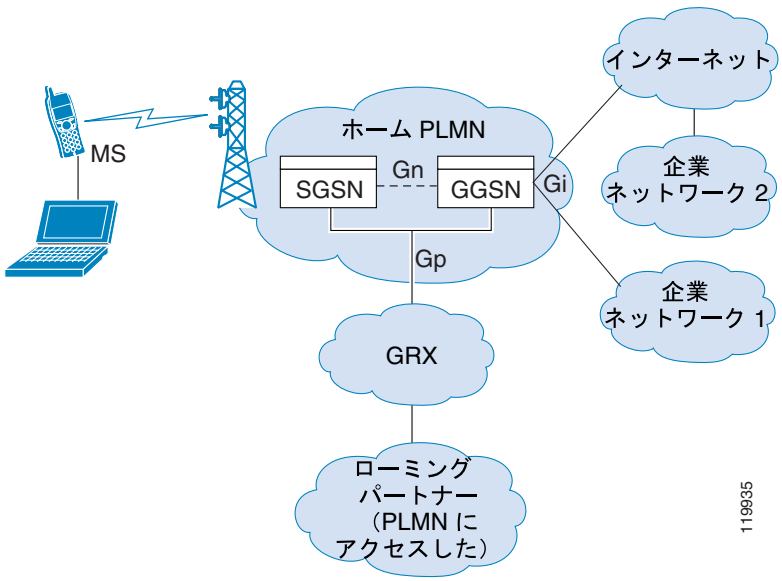
- GTP 検査の概要（p.20-28）
- GTP マップおよびコマンド（p.20-29）
- GTP 検査のイネーブル化および設定（p.20-30）
- GTP 検査の確認およびモニタ（p.20-32）

（注） GTP 検査には、特別なライセンスが必要です。必要なライセンスなしで FWSM で GTP 関連コマンドを入力すると、FWSM はエラー メッセージを表示します。

GTP 検査の概要

General Packet Radio Service（GPRS）は、GSM ネットワークと企業ネットワーク、またはインターネットの間で、携帯電話加入者に連続した接続を提供します。Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）は、GPRS ワイヤレス データ ネットワークと他のネットワークの間のインターフェイスです。Serving GPRS Support Node（SGSN）は、モビリティ管理、データ セッション管理、データ圧縮を行います（図 20-4 を参照）。

図 20-4　GPRS トンネリング プロトコル



Universal Telecommunications System（UMTS）は、固定回線電話、携帯電話、インターネット、コンピュータ技術を融合したものです。Universal Terrestrial Radio Access Network（UTRAN）は、このシステムでワイヤレス ネットワークを実装するのに使用するネットワーキング プロトコルです。GTP により、GGSN、SGSN、UTRAN の間の UMTS/GPRS バックボーンを介して、マルチプロトコル パケットをトンネリングできます。

GTP には、固有のセキュリティまたはユーザ データの暗号化は含まれませんが、FWSM で GTP を使用するとリスクからネットワークを保護できます。

SGSN は GTP を使用して、論理的に GGSN に接続されています。GTP により、マルチプロトコル パケットを GSN の間の GPRS バックボーンを介してトンネリングできます。GTP は、トンネルを作成、変更、削除することで、SGSN にモバイル ステーションの GPRS ネットワーク アクセスを許可するトンネル制御および管理プロトコルを提供します。GTP は、ユーザ データ パケットの伝送サービスを提供するため、トンネリング メカニズムを使用します。

(注) フェールオーバーのある GTP を使用して GTP 接続が確立され、データがトンネル上で転送される前にアクティブ ユニットが失敗した場合、GTP データ接続（[j] フラグ セット付き）はスタンバイ ユニットに複製されません。これが発生するのは、アクティブ ユニットがスタンバイ ユニットへの初期接続を複製しないからです。

GTP マップおよびコマンド

GTP トラフィック上に追加の検査パラメータを実行できます。**gtp-map** コマンドは、検査パラメータを指定します。**inspect gtp** コマンドを使用して GTP 検査をイネーブルにする場合、GTP マップを指定するオプションがあります。

inspect gtp コマンドを使用してマップを指定しない場合、FWSM はデフォルトの GTP マップを使用します。このマップは、次のデフォルト値で設定済みのものです。

- **request-queue** 200
- **timeout gsn** 0:30:00
- **timeout pdp-context** 0:30:00
- **timeout request** 0:01:00
- **timeout signaling** 0:30:00
- **timeout tunnel** 0:01:00
- **tunnel-limit** 500

表 20-3 に、GTP 検査パラメータの設定に使用するコマンドを要約します。次のコマンドは、GTP マップ コンフィギュレーション モードで利用できます。各コマンドの詳細な構文については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の対応するコマンド ページを参照してください。

表 20-3　GTP マップ コンフィギュレーション コマンド

コマンド	説明
description	GTP コンフィギュレーション マップの説明を指定します。
drop	廃棄するメッセージ ID、APN、または GTP バージョンを指定します。
mcc	3 桁の Mobile Country Code（000 ～ 999）を指定します。1 桁または 2 桁のエントリの場合は前に 0 が付きます。
message-length	最小および最大メッセージ長を指定します。
permit errors	エラーのあるパケットまたは異なる GTP バージョンのパケットを許可します。
request-queue	キューで許可される要求の最大数を指定します。
timeout（gtp-map）	GSN、PDP コンテキスト、要求、シグナリング接続、トンネルのアイドル タイムアウトを指定します。
tunnel-limit	許可されるトンネルの最大数を指定します。

GTP 検査のイネーブル化および設定

GTP アプリケーション検査はデフォルトではディセーブルなので、GTP 検査をイネーブルにするには、ここで説明する手順を実行する必要があります。

(注) GTP 検査には、特別なライセンスが必要です。必要なライセンスなしで FWSM で GTP 関連コマンドを入力すると、FWSM はエラー メッセージを表示します。

GTP 設定をイネーブルにする、または変更する手順は、次のとおりです。

ステップ 1　GTP トラフィックに必要なポートを特定する ACE を持つアクセス リストを定義します。標準ポートは、UDP ポート 2123 および 3386 です。アクセス リストを作成するには、次のように各 ACE に 1 回だけ **access-list extended** コマンドを使用します。

```
hostname(config)# access-list acl-name permit {udp | tcp} any any eq port
```

acl-name はアクセス リストに割り当てられた名前で、*port* は ACE が識別する GTP ポートです。

ステップ 2　GTP トラフィックを識別するには、クラス マップを作成するか、または 既存のクラス マップを変更します。**class-map** コマンドを次のように使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

class_map_name は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI はクラス マップ コンフィギュレーション モードを開始します。

ステップ 3　**match access-list** コマンドを使用して、ステップ 1 で作成したアクセス リストで GTP トラフィックを識別します。

```
hostname(config-cmap)# match access-list acl-name
```

ステップ 4　（任意）GTP トラフィック上で追加パラメータを実行する場合、GTP マップを作成および設定します。GTP マップを指定しない場合の GTP マップと実行されるデフォルト値の詳細については、「GTP マップおよびコマンド」（p.20-29）を参照してください。GTP マップを作成および設定する手順は、次のとおりです。

a. GTP 検査の追加パラメータを含んだ GTP マップを作成します。**gtp-map** コマンドを次のように使用します。

```
hostname(config-cmap)# gtp-map map_name
hostname(config-gtp-map)#
```

map_name は、GTP マップの名前です。CLI は、GTP マップ コンフィギュレーション モードを開始します。

b. GTP 検査のパラメータ設定します。そのためには、実行する GTP マップ コンフィギュレーション モード コマンドを使用します。コマンド リストについては、表 20-3 を参照してください。

ステップ 5　GTP インスペクション エンジンを GTP トラフィックに適用するために使用するポリシー マップを作成するか、または既存のポリシー マップを変更します。そのためには、**policy-map** コマンドを次のように使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

policy_map_name は、ポリシー マップの名前です。CLI はポリシー マップ コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 6　ステップ 2 で作成したクラス マップを指定します。このクラス マップは GTP トラフィックを識別します。**class** コマンドを次のように使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name は、ステップ 2 で作成したクラス マップの名前です。CLI はポリシー マップ クラス コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 7　GTP アプリケーション検査をイネーブルにします。そのためには、**inspect gtp** コマンドを次のように使用します。

```
hostname(config-pmap-c)# inspect gtp [map_name]
hostname(config-pmap-c)#
```

map_name は、ステップ 4（任意）で作成した GTP マップです。

ステップ 8　ポリシー マップをグローバルに、または特定のインターフェイスに適用するには、**service-policy** コマンドを次のように使用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface
interface_ID]
hostname(config)#
```

policy_map_name は、ステップ 5 で設定したポリシー マップです。ポリシー マップをすべてのインターフェイス上のトラフィックに適用する場合、**global** オプションを使用します。ポリシー マップを特定のインターフェイス上のトラフィックに適用する場合、***interface*** *interface_ID* オプションを使用します。*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

FWSM は、指定のとおりに GTP トラフィックの検査を開始します。

次に、アクセス リストを使用して、GTP トラフィックを識別し、GTP マップを定義し、ポリシーを定義し、そのポリシーを外部インターフェイスに適用する例を示します。

例 20-6　GTP 検査のイネーブル化および設定

```
hostname(config)# access-list gtp_acl permit udp any any eq 3386
hostname(config)# access-list gtp_acl permit udp any any eq 2123
hostname(config)# class-map gtp-traffic
hostname(config-cmap)# match access-list gtp_acl
hostname(config-cmap)# gtp-map sample_map
hostname(config-gtp-map)# request-queue 300
hostname(config-gtp-map)# permit mcc 111 mnc 222
hostname(config-gtp-map)# message-length min 20 max 300
hostname(config-gtp-map)# drop message 20
hostname(config-gtp-map)# tunnel-limit 10000
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class gtp-traffic
hostname(config-pmap-c)# inspect gtp sample_map
hostname(config)# service-policy sample_policy outside
```

GTP 検査の確認およびモニタ

GTP 設定を表示するには、イネーブル EXEC モードで **show service-policy inspect gtp** コマンドを入力します。このコマンドの詳細な構文については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』のコマンド ページを参照してください。

GTP 検査の統計情報を表示するには、**show service-policy inspect gtp statistics** コマンドを使用します。次に、**show service-policy inspect gtp statistics** コマンドの出力例を示します。

```
hostname# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support                0     msg_too_short              0
  unknown_msg                        0     unexpected_sig_msg         0
  unexpected_data_msg                0     ie_duplicated              0
  mandatory_ie_missing               0     mandatory_ie_incorrect     0
  optional_ie_incorrect              0     ie_unknown                 0
  ie_out_of_order                    0     ie_unexpected              0
  total_forwarded                    0     total_dropped              0
  signalling_msg_dropped             0     data_msg_dropped           0
  signalling_msg_forwarded           0     data_msg_forwarded         0
  total created_pdp                  0     total deleted_pdp          0
  total created_pdpmcb               0     total deleted_pdpmcb       0
  pdp_non_existent                   0
```

表示をフィルタリングするには、縦棒（|）を使用します。詳細なフィルタ オプションを表示するには、**?|** と入力します。

PDP コンテキスト関連情報を表示するには、**show service-policy inspect gtp pdp-context** コマンドを使用します。次に、**show service-policy inspect gtp pdp-context** コマンドの出力例を示します。

```
hostname# show service-policy inspect gtp pdp-context detail
1 in use, 1 most used, timeout 0:00:00

Version TID                  MS Addr        SGSN Addr    Idle      APN
v1      1234567890123425         10.0.1.1        10.0.0.2 0:00:13  gprs.example.com

    user_name (IMSI): 214365870921435    MS address:         1.1.1.1
    primary pdp: Y                       nsapi: 2
    sgsn_addr_signal:        10.0.0.2    sgsn_addr_data:          10.0.0.2
    ggsn_addr_signal:        10.1.1.1    ggsn_addr_data:          10.1.1.1
    sgsn control teid:     0x000001d1    sgsn data teid:        0x000001d3
    ggsn control teid:     0x6306ffa0    ggsn data teid:        0x6305f9fc
    seq_tpdu_up:                    0    seq_tpdu_down:                  0
    signal_sequence:                0
    upstream_signal_flow:          0     upstream_data_flow:          0
    downstream_signal_flow:        0     downstream_data_flow:        0
    RAupdate_flow:                 0
```

PDP コンテキストはトンネル ID によって識別されます。トンネル ID は IMSI 値と NSAPI 値を組み合わせたものです。GTP トンネルは、異なる GSN ノードで対応付けられた 2 つの PDP コンテキストによって定義され、トンネル ID で識別されます。GTP トンネルは、外部パケット データ ネットワークと MS ユーザの間でパケットを転送するのに必要です。

次に、縦棒（|）を使用して表示をフィルタリングする例を示します。

```
hostname# show service-policy gtp statistics | grep gsn
```

H.323 検査

ここでは、H.323 アプリケーション検査をイネーブルにして、デフォルトのポート設定を変更する手順について説明します。次の内容について説明します。

- H.323 検査の概要（p.20-34）
- H.323 の動作（p.20-34）
- 制限事項および制約事項（p.20-35）
- H.225 設定を必要とするトポロジー（p.20-36）
- H.225 マップ コマンド（p.20-37）
- H.323 検査のイネーブル化および設定（p.20-37）
- H.323 および H.225 タイムアウト値の設定（p.20-40）
- H.323 検査の確認およびモニタ（p.20-40）

H.323 検査の概要

H.323 検査は、H.323 準拠アプリケーション（Cisco CallManager および VocalTec Gatekeeper など）をサポートします。H.323 は、International Telecommunication Union（ITU; 国際電気通信連合）により、LAN 上でのマルチメディア会議用として定義されているプロトコル スイートです。FWSM では、H.323 v3 機能の Multiple Calls on One Call Signaling Channel（1 つのコール シグナリング チャネルでの複数コール）を含め、H.323 Version 4 がサポートされます。

H.323 検査がイネーブルの場合、FWSM では、H.323 Version 3 で導入された機能である同一コール シグナリング チャネルでの複数コールをサポートします。この機能によってセットアップ時間が短縮され、FWSM でのポート使用が減少します。

H.323 検査には、2 つの主要機能があります。

- H.225 および H.245 メッセージ内に組み込まれた必要な IPv4 アドレスに対し、NAT を実行します。H.323 メッセージは PER 符号化フォーマットで符号化されているので、FWSM は ASN.1 デコーダを使用して H.323 メッセージをデコードします。
- ネゴシエートされた H.245 および RTP/RTCP 接続が、動的に割り当てられます。

H.323 の動作

H.323 のプロトコルは、合計で、最大 2 つの TCP 接続と 4 ～ 6 つの UDP 接続を使用できます。FastConnect は 1 つの TCP 接続だけを使用します。RAS は登録、アドミッション、ステータスに 1 つの UDP 接続を使用します。

H.323 クライアントでは、最初に TCP ポート 1720 を使用して H.323 サーバへの TCP 接続を確立し、Q.931 コールのセットアップを要求できます。コール セットアップ プロセスの一環として、H.323 端末は、H.245 TCP 接続に使用するポート番号をクライアントに提供します。H.323 ゲートキーパを使用している環境では、最初のパケットは UDP によって送信されます。

H.323 検査は、Q.931 TCP 接続をモニタして、H.245 のポート番号を判別します。H.323 端末が FastConnect を使用していない場合、FWSM は、H.225 メッセージの検査に基づいて H.245 接続を動的に割り当てます。

各 H.245 メッセージ内で、H.323 エンドポイントは、以降の UDP データ ストリームに使用するポート番号を交換します。H.323 検査は、H.245 メッセージを検査してこれらのポートを識別し、メディア交換用の接続を動的に作成します。Real-Time Transport Protocol（RTP）はネゴシエートされたポート番号を使用しますが、RTP Control Protocol（RTCP）は次の上位ポート番号を使用します。

H.323 制御チャネルは、H.225、H.245、および H.323 RAS を処理します。H.323 検査は、次のポートを使用します。

- UDP ポート 1718 ― ゲートキーパ検出
- UDP ポート 1719 ― RAS
- TCP ポート 1720 ― 制御ポート

H.225 コール シグナリングについて、well-known H.323 ポート 1720 のトラフィックを許可しておく必要があります。ただし、H.245 シグナリング ポートは、H.225 シグナリング内のエンドポイントの間でネゴシエートされます。H.323 ゲートキーパが使用されている場合、FWSM は、AdmissionConfirm（ACF）メッセージの検査に基づいて H.225 接続を開始します。

FWSM は、H.225 メッセージを検査したあと、H.245 チャネルを開き、H.245 チャネル上で送信されたトラフィックを同様に検査します。すなわち、FWSM を通過した H.245 メッセージはすべて H.245 アプリケーション検査を通過し、組み込み IP アドレスが NAT 処理され、H.245 メッセージでネゴシエートされたメディア チャネルが開始されることを意味します。

H.323 ITU 標準規格では、信頼性のある接続上に送信する前に、H.225 および H.245 の前に TPKT ヘッダーによりメッセージの長さを定義することが規定されています。TPKT ヘッダーは H.225 および H.245 メッセージと同じ TCP パケットで送信されるとは限らないので、メッセージを適切に処理およびデコードするには、FWSM で TPKT 長を保持しておく必要があります。FWSM は各接続に対して、1 つのレコードを維持します。このレコードには次に送信されるメッセージの TPKT 長が含まれます。

FWSM でメッセージ内の IP アドレスを NAT 処理する必要がある場合、チェックサム、User-User Information Element（UUIE; ユーザ対ユーザ情報要素）の長さ、TPKT（H.225 メッセージの TCP パケットに含まれている場合）を変更する必要があります。TPKT が別の TCP パケットで送信される場合には、FWSM は TPKT のプロキシ ACK を実行し、H.245 メッセージに新しい長さの TPKT を付加します。

（注） FWSM による TPKT のプロキシ ACK では、TCP オプションはサポートされません。

H.323 検査を通過するパケットを使用する各 UDP 接続は、H.323 接続としてマークされ、***timeout*** コマンドによって設定した H.323 タイムアウトが適用されます。

制限事項および制約事項

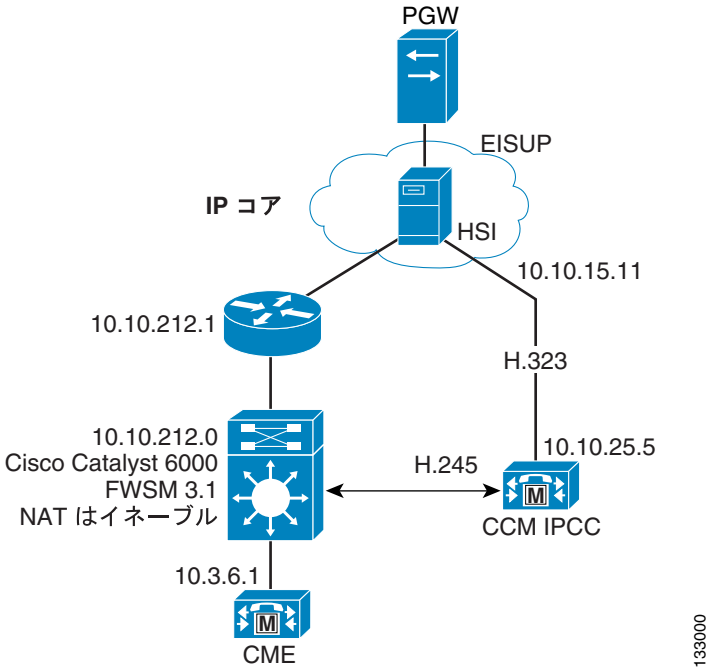
H.323 アプリケーション検査の一部の既知の問題と制限事項は、次のとおりです。

- スタティック PAT は、H.323 メッセージ内のオプション フィールドに組み込まれた IP アドレスを正しく変換しない場合があります。この種類の問題が発生したら、H.323 ではスタティック PAT を使用しないでください。
- NetMeeting クライアントが H.323 ゲートキーパに登録し、H.323 ゲートキーパに登録された H.323 ゲートウェイを呼び出そうとする場合、接続は確立されますが、音声はどの方向でも聞こえません。この問題は、FWSM とは無関係です。
- ネットワーク スタティック アドレスがサードパーティのネットマスクおよびアドレスと同じであるときに、ネットワーク スタティック アドレスを設定する場合、発信 H.323 接続は切断されます。

H.225 設定を必要とするトポロジー

FWSM を介して接続している H.323 エンドポイントの間でコール制御が発生したトポロジーでは、一部の追加 H.225 設定が必要です（図 20-5 を参照）。

図 20-5　H.225 設定を必要とするトポロジー



このトポロジーでは、FWSM の片側の Cisco CallManager と HSI の間で、もう片方の側の HSI と Cisco CallManager エンドポイントの間で、コール シグナリングが発生します。それから、Cisco CallManager と Cisco CallManager エンドポイントの間でコール制御が発生します。HSI と 1 つのエンドポイントが FWSM によって保護されたネットワーク上にあり、もう 1 つのエンドポイントが別のネットワーク上にある場合、H.225 設定を追加しないとコール制御は実施されません。

FWSM は、このトポロジーの Cisco CallManager の存在を認識していません。ファイアウォール経由で発生するパケット フローのみでは、FWSM はコールを成功させる適切なピンホールをオープンできません。したがって、この事例ではいくつかの追加 H.225 設定が必要となります。

必要な設定を提供するには、HSI と HSI グループ内の関連エンドポイントを特定します。設定が完了すると、FWSM は HSI を H.225 接続の通信ホストの 1 つとみなし、HSI グループ内のエンドポイントの間で H.245 ホールをオープンします。実際の H.245 接続は、これらのピンホールの 1 つと一致し、正しく実行されます。

H.225 マップ コマンド

H.225 マップにより、HSI が H.225 コール シグナリングに関与している場合に、FWSM は H.245 接続のため、動的なポート固有のピンホールをオープンします。H.225 マップは、HSI および関連するエンドポイントに関する情報を提供します。この情報は、FWSM によって保護されたネットワーク セキュリティを損なうことなく、この接続を確立するのに必要です。

h225-map コマンドは、H.225 マップを作成します。1 つの H225 マップには、最大 5 つの HSI グループを含めることができます。表 20-4 に、H.225 マップ コンフィギュレーション モードで利用可能なコマンドを示します。

表 20-4　H.225 コンフィギュレーション コマンド

コマンド	コンフィギュレーション モード	説明
hsi-group	H.225 マップ コンフィギュレーション モード	HSI グループを定義し、HSI グループ コンフィギュレーション モードを開始します。各 HSI グループには最大で 10 個のエンドポイントを含めることができます。
hsi	HSI グループ コンフィギュレーション モード	HSI を特定します。
endpoint	HSI グループ コンフィギュレーション モード	HSI グループ内の 1 つまたは複数のエンドポイントを特定します。

H.323 検査のイネーブル化および設定

H.323 検査はデフォルトではイネーブルです。

H.225 マップのオプション使用を含めた、H.323 検査をイネーブルにする手順は、次のとおりです。

ステップ 1　H.323 トラフィックに必要なポートを特定する ACE を持つアクセス リストを定義します。標準ポートは、UDP ポート 1718 と 1719、TCP ポート 1720 です。アクセス リストを作成するには、次のように各 ACE に 1 回だけ **access-list extended** コマンドを使用します。

```
hostname(config)# access-list acl-name permit {udp | tcp} any any eq port
```

acl-name はアクセス リストに割り当てられた名前で、*port* は ACE が識別する H.323 ポートです。

ステップ 2　H.323 トラフィックを識別するには、クラス マップを作成するか、または既存のクラス マップを変更します。**class-map** コマンドを次のように使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

class_map_name は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI はクラス マップ コンフィギュレーション モードを開始します。

ステップ 3　**match access-list** コマンドを使用して、ステップ 1 で作成したアクセス リストで H.323 トラフィックを識別します。

```
hostname(config-cmap)# match access-list acl-name
```

ステップ 4　（任意）ネットワーク トポロジーで必要な場合、H.225 マップを設定します。ネットワークが H.225 マップを必要とするかどうかについては、「H.225 設定を必要とするトポロジー」（p.20-36）を参照してください。H.225 マップを作成および設定する手順は、次のとおりです。

a. H.225 マップを作成します。

```
hostname(config)# h225-map map_name
hostname(config-h225-map)#
```

システムは H.225 マップ コンフィギュレーション モードを開始し、CLI プロンプトがそれに応じて変わります。

b. HSI グループを識別します。そのためには、**hsi-group** コマンドを次のように使用します。

```
hostname(config-h225-map)# hsi-group group_ID
hostname(config-h225-map-hsi-grp)#
```

group_ID は、0 ～ 2147483647 の番号で、HSI グループを識別します。

（注） H.225 マップ単位で許可された HSI グループの最大数は 5 です。

システムは HSI グループ コンフィギュレーション モードを開始し、CLI プロンプトがそれに応じて変わります。

c. グループの HIS を定義します。

```
hostname(config-h225-map-hsi-grp)# hsi ip_address
```

ip_address は、HIS のアドレスです。

d. 最大 10 個のエンドポイントを定義します。そのためには、エンドポイントごとに **endpoint** コマンドを 1 回、次のように使用します。

```
hostname(config-h225-map-hsi-grp)# endpoint ip_address interface
```

interface は、エンドポイントに接続された FWSM 上のインターフェイスです。*ip_address* はそのエンドポイントのアドレスです。

e. 追加の HSI グループを作成する場合、ステップ b ～ d を繰り返します。

ステップ 5　H.323 インスペクション エンジンを H.323 トラフィックに適用するために使用するポリシー マップを作成するか、または既存のポリシー マップを変更します。そのためには、**policy-map** コマンドを次のように使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

policy_map_name は、ポリシー マップの名前です。CLI はポリシー マップ コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 6　ステップ 2 で作成したクラス マップを指定します。このクラス マップは H.323 トラフィックを識別します。**class** コマンドを次のように使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name は、ステップ 2 で作成したクラス マップの名前です。CLI はポリシー マップ クラス コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 7　H.323 アプリケーション検査をイネーブルにします。そのためには、**inspect h323** コマンドを次のように使用します。

```
hostname(config-pmap-c)# inspect h323 [h225 map_name]
hostname(config-pmap-c)#
```

map_name は、ステップ 4（任意）で作成した H.225 マップです。

ステップ 8　ポリシー マップをグローバルに、または特定のインターフェイスに適用するには、**service-policy** コマンドを次のように使用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface
interface_ID]
hostname(config)#
```

policy_map_name は、ステップ 5 で設定したポリシー マップです。ポリシー マップをすべてのインターフェイス上のトラフィックに適用する場合、**global** オプションを使用します。ポリシー マップを特定のインターフェイス上のトラフィックに適用する場合、***interface*** *interface_ID* オプションを使用します。*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

FWSM は、指定のとおりに H.323 トラフィックの検査を開始します。

例 20-7　H.225 マップを使用しない場合の H.323 検査の設定

次の例では、H.323 インスペクション エンジンをイネーブルにし、デフォルト ポート（1720）の H.323 トラフィックと一致するクラス マップを作成します。それからサービス ポリシーを外部インターフェイスに適用します。

```
hostname(config)# access-list h323_acl permit udp any any eq 1718
hostname(config)# access-list h323_acl permit udp any any eq 1719
hostname(config)# access-list h323_acl permit tcp any any eq 1720
hostname(config)# class-map h323-traffic
hostname(config-cmap)# match access-list h323_acl
hostname(config-cmap)# policy-map sample_policy
hostname(config-pmap)# class h323_port
hostname(config-pmap-c)# inspect h323 ras
hostname(config-pmap-c)# inspect h323 h225
hostname(config-pmap-c)# service-policy sample_policy interface outside
hostname(config)#
```

例 20-8 には、H.323 設定全体の一部として、2 つの HSI グループを持った H.225 マップが含まれます。

例 20-8　H.225 マップを使用した場合の H.323 検査の設定

```
hostname(config)# access-list h323_acl permit udp any any eq 1718
hostname(config)# access-list h323_acl permit udp any any eq 1719
hostname(config)# access-list h323_acl permit tcp any any eq 1720
hostname(config)# class-map h323-traffic
hostname(config-cmap)# match access-list h323_acl
hostname(config-cmap)# h225-map sample_map
hostname(config-h225-map)# hsi-group 1
hostname(config-h225-map-hsi-grp)# hsi 10.10.15.11
hostname(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
hostname(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
hostname(config-h225-map-hsi-grp)# policy-map sample_policy
hostname(config-pmap)# class h323_port
hostname(config-pmap-c)# inspect h323 ras
hostname(config-pmap-c)# inspect h323 h225 sample_map
hostname(config-pmap-c)# service-policy sample_policy interface outside
hostname(config)#
```

H.323 および H.225 タイムアウト値の設定

H.225 シグナリング接続が終了するまでのアイドル時間を設定するには、**timeout h225** コマンドを使用します。H.225 タイムアウトのデフォルト値は 1 時間です。

H.323 制御接続が終了するまでのアイドル時間を設定するには、**timeout h323** コマンドを使用します。デフォルトは 5 分です。

H.323 検査の確認およびモニタ

ここでは、H.323 セッションに関する情報を表示する手順について説明します。次の内容について説明します。

- H.225 セッションのモニタ（p.20-40）
- H.245 セッションのモニタ（p.20-41）
- H.323 RAS セッションのモニタ（p.20-41）

H.225 セッションのモニタ

show h225 コマンドは、FWSM を超えて確立された H.225 セッションに関する情報を表示します。**debug h323 h225 event**、**debug h323 h245 event**、**show local-host** コマンドとともに、このコマンドは、H.323 インスペクション エンジンの問題のトラブルシューティングに使用されます。

show h225、**show h245**、または **show h323-ras** コマンドを入力する前に、**pager** コマンドの設定を推奨します。多くのセッション レコードが存在し、**pager** コマンドが設定されていない場合、**show** コマンドの出力が最後まで到達するには、しばらく時間がかかることがあります。非常に膨大な接続数がある場合、デフォルトのタイムアウト値または設定された値に基づいて、セッションがタイムアウトするか検証します。セッションがタイムアウトしない場合、調査を必要とする問題があります。

次に、**show h225** コマンドの出力例を示します。

```
hostname# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
    1. CRV 9861
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
    Local:   10.130.56.4/1050   Foreign: 172.30.254.205/1720
```

この出力では、現在 FWSM を通過しているアクティブ H.323 コールが 1 つ、ローカル エンドポイント 10.130.56.3 と外部のホスト 172.30.254.203 の間にあることを示します。また、これらの特定のエンドポイントの間に、同時コールが 1 つあり、そのコールの Call Reference Value（CRV）が 9861 であることを示します。

ローカル エンドポイント 10.130.56.4 と外部ホスト 172.30.254.205 に対して、同時コールは 0 です。つまり H.225 セッションがまだ存在しているものの、このエンドポイントの間にはアクティブ コールがないことを意味します。この状況は、**show h225** コマンドを実行したときに、コールはすでに終了しているが、H.225 セッションがまだ削除されていない場合に発生する可能性があります。または、2 つのエンドポイントが、「maintainConnection」を TRUE に設定しているため、TCP 接続をまだ開いたままにしていることを意味する可能性もあります。したがって、「maintainConnection」を再度 FALSE に設定するまで、または設定内の H.225 タイムアウト値に基づいてセッションがタイムアウトするまで、セッションは開いたままになります。

H.245 セッションのモニタ

show h245 コマンドは、スロースタートを使用しているエンドポイントが FWSM を超えて確立された H.245 セッションに関する情報を表示します。スロースタートは、コールの 2 つのエンドポイントが H.245 用の別の TCP コントロール チャネルを開いた場合です。ファスト スタートは、H.245 メッセージが H.225 コントロール チャネル上の H.225 メッセージの一部として交換された場合です。**debug h323 h245 event**、**debug h323 h225 event**、**show local-host** コマンドとともに、このコマンドは、H.323 インスペクション エンジンの問題のトラブルシューティングに使用されます。

次に、**show h245** コマンドの出力例を示します。

```
hostname# show h245
Total: 1
        LOCAL            TPKT    FOREIGN          TPKT
1       10.130.56.3/1041        0       172.30.254.203/1245    0
        MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
                       Local   10.130.56.3 RTP 49608 RTCP 49609
        MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
                       Local   10.130.56.3 RTP 49606 RTCP 49607
```

FWSM を越えたアクティブな H.245 コントロール セッションが、現在 1 つあります。ローカル エンドポイントは、10.130.56.3 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します。TKTP ヘッダーは、各 H.225/H.245 メッセージの前に置かれる 4 バイトのヘッダーです。このヘッダーで、この 4 バイトのヘッダーを含むメッセージの長さが分かります。外部のホストのエンドポイントは、172.30.254.203 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します。

これらのエンドポイント間でネゴシエートされたメディアには、258 という LCN（論理チャネル番号）があり、外部に 172.30.254.203/49608 という RTP IP アドレス / ポート ペアと 172.30.254.203/49609 という RTCP IP アドレス / ポート ペアを持ち、ローカルに 10.130.56.3/49608 という RTP IP アドレス / ポート ペアと 49609 という RTCP ポートを持っています。

259 という 2 番めの LCN には、外部に 172.30.254.203/49606 という RTP IP アドレス / ポート ペアと 172.30.254.203/49607 という RTCP IP アドレス / ポート ペアがあり、ローカルに 10.130.56.3/49606 という RTP IP アドレス / ポート ペアと 49607 という RTCP ポートを持っています。

H.323 RAS セッションのモニタ

show h323-ras コマンドは、FWSM を越えてゲートキーパとその H.323 エンドポイントの間に確立された H.323 RAS セッションの情報を表示します。**debug h323 ras event** および **show local-host** コマンドとともに、このコマンドは、H.323 RAS インスペクション エンジンの問題のトラブルシューティングに使用されます。

show h323-ras コマンドは、H.323 RAS インスペクション エンジンの問題をトラブルシューティングするための接続情報を表示します。次に、**show h323-ras** コマンドの出力例を示します。

```
hostname# show h323-ras
Total: 1
        GK                      Caller
        172.30.254.214 10.130.56.14
```

この出力は、ゲートキーパ 172.30.254.214 とそのクライアント 10.130.56.14 の間にアクティブな登録が 1 つあることを示します。

HTTP 検査

ここでは、HTTP インスペクション エンジンの機能と、その設定を変更する手順について説明します。次の内容について説明します。

- HTTP 検査の概要（p.20-42）
- 拡張 HTTP 検査コマンド（p.20-43）
- 拡張 HTTP 検査のイネーブル化および設定（p.20-43）

HTTP 検査の概要

Use the **inspect http** コマンドを使用して、HTTP 固有の攻撃や HTTP に対応付けられた他の脅威からネットワークを保護します。HTTP 検査では、次の機能を実行します。

- 拡張 HTTP 検査
- N2H2 または Websense を介した URL スクリーニング
- Java および ActiveX のフィルタリング

あとの 2 つの機能は、**filter** コマンドとともに設定します。フィルタリングの詳細については、第 20 章「アプリケーション レイヤ プロトコル検査の適用」を参照してください。

（注） また、**no inspect http** コマンドは、**filter url** コマンドをディセーブルにします。

拡張 HTTP 検査機能は、アプリケーション ファイアウォールとして知られており、攻撃側がネットワーク セキュリティ ポリシーを回避するため HTTP メッセージを使用するのを防ぎます。この機能は次の HTTP メッセージすべてを確認します。

- RFC 2616 への適合
- RFC 定義方法のみを使用
- 表 20-5 のコマンドで定義された追加基準への準拠

inspect http コマンドで HTTP マップを指定する場合、拡張 HTTP 検査をイネーブルにします。拡張 HTTP インスペクション エンジンのパラメータは、HTTP マップによって定義されます。このマップは、**http-map** コマンドを使用して作成し、HTTP マップ コンフィギュレーション モードで利用可能なコマンドを使用して設定されます。

（注） HTTP マップのある HTTP 検査をイネーブルにすると、アクションのある完全な HTTP 検査はリセットされ、デフォルトではログはイネーブルになります。検査失敗に応じて実行されるアクションを変更できますが、HTTP マップがイネーブルであるかぎり、完全な検査をディセーブルにできません。

拡張 HTTP 検査コマンド

表 20-5 に、拡張 HTTP 検査パラメータの設定に使用するコマンドを要約します。次のコマンドは、HTTP マップ コンフィギュレーション モードで利用できます。各コマンドは、コマンドによって実行されたパラメータに対して、メッセージが違反した場合に取るアクションを指定します。このアクションには、メッセージの許可、リセット メッセージの送信、メッセージの廃棄が含まれます。このアクションのほかに、イベントを記録するかどうか指定できます。

各コマンドの詳細な構文については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の対応するコマンド ページを参照してください。

表 20-5　HTTP マップ コンフィギュレーション コマンド

コマンド	説明
content-length	HTTP コンテンツの長さに基づいて、検査をイネーブルにします。
content-type-verification	HTTP コンテンツのタイプに基づいて、検査をイネーブルにします。
max-header-length	HTTP ヘッダーの長さに基づいて、検査をイネーブルにします。
max-uri-length	URI の長さに基づいて、検査をイネーブルにします。
port-misuse	アプリケーション ファイアウォール検査をイネーブルにします。
request-method	HTTP 要求方法に基づいて、検査をイネーブルにします。
strict-http	完全な HTTP 検査をイネーブルにします。
transfer-encoding	転送符号化タイプに基づいて、検査をイネーブルにします。

拡張 HTTP 検査のイネーブル化および設定

拡張 HTTP 検査をイネーブルにして設定する手順は、次のとおりです。

ステップ 1　FWSM の後ろの HTTP サーバが HTTP トラフィックを待ち受けるポートを決定します。デフォルトの ポートは TCP ポート 80 です。ただし、thwart 攻撃に対する簡単な手段として、代替ポートがしばしば使用されます。すべての HTTP トラフィックを検査対象とするには、TCP ポート 80 以外のポートの使用に関して、HTTP サーバを検証してください。

ステップ 2　HTTP トラフィックを識別するには、クラス マップを作成するか、または既存のクラス マップを変更します。**class-map** コマンドを次のように使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

class_map_name は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI はクラス マップ コンフィギュレーション モードを開始します。

ステップ 3　ステップ 1 で決定した HTTP ポートに送信されたトラフィックを識別します。そのためには、**match port** または **match access-list** コマンドを使用します。

連続しない複数のポートを特定する必要がある場合、**access-list extended** コマンドを使用してアクセス リストを作成し、各ポートと一致する ACE を追加してから、**match access-list** コマンドを使用します。次のコマンドは、アクセス リストを使用して、アクセス リストを持った複数の TCP ポートを特定します。

```
hostname(config)# access-list acl-name any any tcp eq port_number_1
hostname(config)# access-list acl-name any any tcp eq port_number_2
hostname(config)# class-map class_map_name
hostname(config-cmap)# match access-list acl-name
```

単一ポートを特定する必要がある場合、次のように **match port** コマンドを使用します。

```
hostname(config-cmap)# match port tcp port_number
```

port_number は、FWSM の後ろの HTTP サーバが待ち受ける TCP ポートのみです。

単一プロトコルの連続したポート範囲を特定する必要がある場合、次のように **range** キーワードを指定して **match port** コマンドを使用します。

```
hostname(config-cmap)# match port tcp range begin_port_number end_port_number
```

begin_port_number は、HTTP ポート範囲の最小ポートで、*end_port_number* は最大ポートです。

ステップ 4　（任意）拡張 HTTP 検査をイネーブルにする場合、次の手順を実行します。

a. HTTP 検査の追加パラメータを含む HTTP マップを作成します。**http-map** コマンドを次のように使用します。

```
hostname(config-cmap)# http-map map_name
hostname(config-http-map)#
```

map_name は、HTTP マップの名前です。CLI は、HTTP マップ コンフィギュレーション モードを開始します。

b. 拡張 HTTP 検査パラメータを設定します。そのためには、使用する拡張 HTTP コマンドを決定します。コマンド リストについては、表 20-5 を参照してください。

ステップ 5　HTTP インスペクション エンジンを HTTP トラフィックに適用するために使用するポリシー マップを作成するか、または既存のポリシー マップを変更します。そのためには、**policy-map** コマンドを次のように使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

policy_map_name は、ポリシー マップの名前です。CLI はポリシー マップ コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 6　ステップ 2 で作成したクラス マップを指定します。このクラス マップは HTTP トラフィックを識別します。**class** コマンドを次のように使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name は、ステップ 2 で作成したクラス マップの名前です。CLI はポリシー マップ クラス コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 7　HTTP アプリケーション検査をイネーブルにします。そのためには、**inspect http** コマンドを次のように使用します。

```
hostname(config-pmap-c)# inspect http [map_name]
hostname(config-pmap-c)#
```

map_name は、ステップ 4（任意）で作成した HTTP マップです。

ステップ 8　ポリシー マップをグローバルに、または特定のインターフェイスに適用するには、**service-policy** コマンドを次のように使用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface
interface_ID]
hostname(config)#
```

policy_map_name は、ステップ 5 で設定したポリシー マップです。ポリシー マップをすべてのインターフェイス上のトラフィックに適用する場合、**global** オプションを使用します。ポリシー マップを特定のインターフェイス上のトラフィックに適用する場合、***interface*** *interface_ID* オプションを使用します。*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

FWSM は、指定のとおりに HTTP トラフィックの検査を開始します。

例 20-9　拡張 HTTP 検査のイネーブル化および設定

次に、アクセス リストを使用して、HTTP トラフィックを識別し、HTTP マップを定義し、ポリシーを定義し、そのポリシーを外部インターフェイスに適用する例を示します。

```
hostname(config)# class-map http_port
hostname(config-cmap)# match port tcp eq 80
hostname(config-cmap)# http-map sample_map
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# content-type-verification match-req-rsp action reset log
hostname(config-http-map)# max-header-length request 100 action reset log
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)# policy-map sample_policy
hostname(config-pmap)# class http_port
hostname(config-pmap-c)# inspect http sample_map
hostname(config-pmap-c)# service-policy sample_policy interface outside
hostname(config)#
```

ICMP 検査

ICMP 検査は、デフォルトではディセーブルです。

ICMP 検査の詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect icmp** および **inspect icmp error** コマンド ページを参照してください。

ILS 検査

ILS 検査は、デフォルトではディセーブルです。

ILS 検査の詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect ils** コマンド ページを参照してください。

MGCP 検査

ここでは、MGCP アプリケーション検査をイネーブルにして設定し、デフォルトのポート設定を変更する手順について説明します。次の内容について説明します。

- MGCP 検査の概要（p.20-46）
- MGCP コール エージェントおよびゲートウェイの設定（p.20-48）
- MGCP 検査の設定およびイネーブル化（p.20-48）
- MGCP タイムアウト値の設定（p.20-51）
- MGCP 検査の確認およびモニタ（p.20-51）

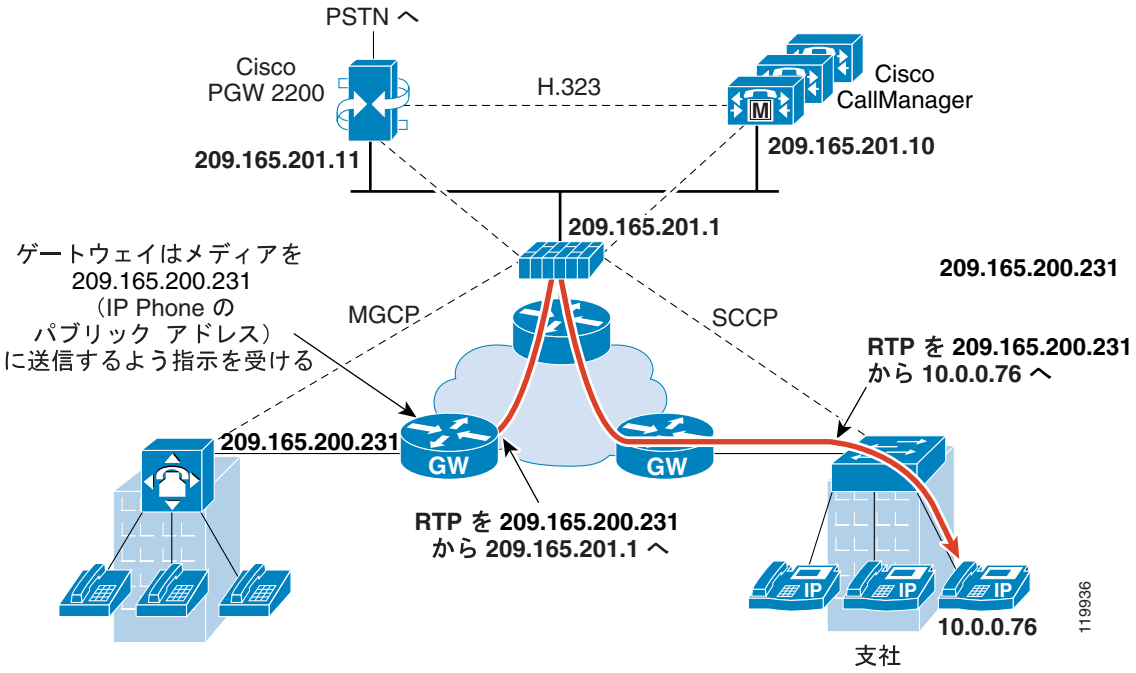
MGCP 検査の概要

MGCP は、メディア ゲートウェイ コントローラまたはコール エージェントと呼ばれる外部コール制御エレメントからメディア ゲートウェイを制御するために使用するマスター/ スレーブ プロトコルです。メディア ゲートウェイは、一般的に、電話回線上で伝送されるオーディオ信号と、インターネットまたは他のパケット ネットワーク上で伝送されるデータ パケット間の変換を行うネットワーク エレメントです。MGCP とともに NAT や PAT を使用すると、制限された外部（グローバル）アドレスを持った内部ネットワーク上で、多数のデバイスをサポートします。次に、メディア ゲートウェイの例を示します。

- トランキング ゲートウェイ。電話網と Voice over IP（VoIP）ネットワーク間のインターフェイスです。このゲートウェイは一般的に多数のデジタル回線を管理します。
- レジデンシャル ゲートウェイ。VoIP ネットワークに従来のアナログ（RJ11）インターフェイスを提供します。レジデンシャル ゲートウェイの例としては、ケーブル モデム / ケーブル セットトップ ボックス、xDSL デバイス、ブロードバンド ワイヤレス デバイスなどがあります。
- ビジネス ゲートウェイ。VoIP ネットワークに従来のデジタル PBX（構内交換機）インターフェイスまたは統合ソフト PBX インターフェイスを提供します。

MGCP メッセージは、UDP 上で転送されます。応答は、コマンドの送信元（IP アドレスおよび UDP ポート番号）に返送されますが、コマンドの宛先と同じアドレスから応答が戻されるとは限りません。たとえば、複数のコール エージェントがフェールオーバー設定に使用され、コマンドを受信したコール エージェントからバックアップ コール エージェントに制御が渡されたあとで、応答が戻される場合です。図 20-6 に、MGCP とともに NAT を使用する例を示します。

図 20-6　MGCP と NAT の使用



MGCP エンドポイントは、データ用の物理的または仮想の送信元 / 宛先です。メディア ゲートウェイには、コール エージェントが、他のマルチメディア エンドポイントとのメディア セッションを確立し制御するための接続を実行、変更、削除できるエンドポイントが含まれます。また、コール エージェントはエンドポイントに対し、所定のイベントを検出し、信号を生成するよう指示できます。エンドポイントは、サービス ステートの変更を自動的にコール エージェントに通知します。

MGCP トランザクションは、コマンドと必須応答で構成されています。次に、コマンドのタイプを示します。

- CreateConnection
- ModifyConnection
- DeleteConnection
- NotificationRequest
- Notify
- AuditEndpoint
- AuditConnection
- RestartInProgress

最初の 4 つのコマンドはコール エージェントによってゲートウェイに送信されます。Notify コマンドはゲートウェイによってコール エージェントに送信されます。ゲートウェイは、DeleteConnection コマンドも送信します。MGCP　ゲートウェイをコール　エージェントに登録することは、RestartInProgress コマンドを使用してできます。AuditEndpoint コマンドおよび AuditConnection コマンドは、コール エージェントによってゲートウェイに送信されます。

すべてのコマンドは Command ヘッダーで構成され、セッションの説明があとに続く場合があります。すべての応答は Response ヘッダーで構成され、セッションの説明があとに続く場合があります。

MGCP を使用するには、通常、次の 2 つのポートに送信されるトラフィックの検査を設定する必要があります。

- ゲートウェイがコール　エージェントからコマンドを受信するポート。ゲートウェイは通常、UDP ポート 2427 を待ち受けます。
- コール エージェントがゲートウェイからコマンドを受信するポート。コール エージェントは通常、UDP ポート 2727 を待ち受けます。

（注） MGCP 検査は、MGCP シグナリングおよび RTP データの異なる IP アドレスの使用をサポートしません。共通の推奨する操作は、レジリエント IP アドレス（ループバックまたは仮想 IP アドレスなど）から RTP データを送信することです。ただし、FWSM は RTP データに対し、MGCP シグナリングと同じアドレスから着信するよう要求します。

MGCP コール エージェントおよびゲートウェイの設定

1 つまたは複数のゲートウェイを管理できるコール エージェントのグループを指定するには、**call-agent** コマンドを使用します。コール エージェント情報は、（ゲートウェイからのコマンド送信先と異なる）グループ内のコール エージェントで接続を開始する場合に使用されます。したがって、どのコール エージェントからでも応答を送信できます。同じ *group_id* を持つコール エージェントは、同じグループに属します。コール エージェントは複数のグループに所属できます。*group_id* オプションは 0 ～ 4,294,967,295 の数字です。*ip_address* オプションはコール エージェントの IP アドレスを指定します。

コール エージェント グループを指定するには、MGCP マップ コンフィギュレーション モードで **call-agent** コマンドを入力します。これは、グローバル コンフィギュレーション モードで **mgcp-map** コマンドを入力することで利用できます。

特定のゲートウェイを管理するコール エージェント グループを指定するには、**gateway** コマンドを入力します。ゲートウェイの IP アドレスは、*ip_address* オプションで指定します。*group_id* オプションに、0 ～ 4,294,967,295 の数値を指定します。この値は、ゲートウェイを管理しているコール エージェントの *group_id* と一致している必要があります。ゲートウェイは、1 つのグループにのみ、所属できます。

（注） MGCP コール エージェントは、MGCP エンドポイントがあるかどうかを判別するため、AUEP メッセージを送信します。これにより FWSM 経由のフローが確立され、MGCP エンドポイントはコール エージェントに登録できます。

MGCP 検査の設定およびイネーブル化

MGCP アプリケーション検査をイネーブルにして設定する手順は、次のとおりです。

ステップ 1　MGCP トラフィックの受信に必要な次の 2 つのポートを特定する ACE を持つアクセス リストを定義します。標準ポートは、UDP ポート 2427 および 2727 です。アクセス リストを作成するには、次のように **access-list extended** コマンドを使用します。

```
hostname(config)# access-list acl-name permit udp any any eq port-1
hostname(config)# access-list acl-name permit udp any any eq port-2
```

acl-name はアクセス リストに割り当てられた名前です。*port-1* は最初の MGCP ポートで、*port-2* は 2 番めの MGCP ポートです。

ステップ 2　MGCP トラフィックを識別するには、クラス マップを作成するか、または既存のクラス マップを変更します。**class-map** コマンドを次のように使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

class_map_name は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI はクラス マップ コンフィギュレーション モードを開始します。

ステップ 3　**match access-list** コマンドを使用して、ステップ 1 で作成したアクセス リストで MGCP トラフィックを識別します。

```
hostname(config-cmap)# match access-list acl-name
```

ステップ 4　（任意）FWSM がピンホールをオープンする必要がある複数のコール エージェントおよびゲートウェイがネットワークにある場合、MGCP マップを作成します。そのためには、次の手順を実行します。

a. **mgcp-map** コマンドを使用して、MGCP マップを作成します。**mgcp-map** コマンドは、GCP 検査のパラメータを作成します。次のように、**mgcp-map** コマンドを使用します。

```
hostname(config-cmap)# mgcp-map map_name
hostname(config-mgcp-map)#
```

map_name は、MGCP マップの名前です。システムは MGCP マップ コンフィギュレーション モードを開始し、CLI プロンプトがそれに応じて変わります。

b. コール エージェントを設定します。そのためには、コール エージェントごとに **call-agent** コマンドを 1 回、次のように使用します。

```
hostname(config-mgcp-map)# call-agent ip_address group_id
```

c. ゲートウェイを設定します。そのためには、ゲートウェイごとに **gateway** コマンドを 1 回、次のように使用します。

```
hostname(config-mgcp-map)# gateway ip_address group_id
```

d. （任意）MGCP コマンド キューで許可されたコマンドの最大数を変更する場合、次のように **command-queue** コマンドを使用します。

```
hostname(config-mgcp-map)# command-queue command_limit
```

ステップ 5　MGCP インスペクション エンジンを MGCP トラフィックに適用するために使用するポリシー マップを作成するか、または既存のポリシー マップを変更します。そのためには、**policy-map** コマンドを次のように使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

policy_map_name は、ポリシー マップの名前です。CLI はポリシー マップ コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 6　ステップ 2 で作成したクラス マップを指定します。このクラス マップは MGCP トラフィックを識別します。**class** コマンドを次のように使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name は、ステップ 2 で作成したクラス マップの名前です。CLI はポリシー マップ クラス コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 7　MGCP アプリケーション検査をイネーブルにします。そのためには、**inspect mgcp** コマンドを次のように使用します。

```
hostname(config-pmap-c)# inspect mgcp [map_name]
hostname(config-pmap-c)#
```

map_name は、ステップ 4（任意）で作成した MGCP マップです。

ステップ 8　ポリシー マップをグローバルに、または特定のインターフェイスに適用するには、**service-policy** コマンドを次のように使用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface
interface_ID]
hostname(config)#
```

policy_map_name は、ステップ 5 で設定したポリシー マップです。ポリシー マップをすべてのインターフェイス上のトラフィックに適用する場合、**global** オプションを使用します。ポリシー マップを特定のインターフェイス上のトラフィックに適用する場合、***interface*** *interface_ID* オプションを使用します。*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

FWSM は、指定のとおりに MGCP トラフィックの検査を開始します。

例 20-10 に、MGCP トラフィックを識別し、MGCP マップを定義し、ポリシーを定義し、そのポリシーを外部インターフェイスに適用する例を示します。これは、デフォルト ポート（2427 および 2727）上の MGCP トラフィックと一致するクラス マップを作成します。この設定により、コール エージェント 10.10.11.5 および 10.10.11.6 がゲートウェイ 10.10.10.115 を制御し、コール エージェント 10.10.11.7 および 10.10.11.8 がゲートウェイ 10.10.10.116 および 10.10.10.117 の両方を制御できます。MGCP コマンド キューの最大数は 150 です。サービス ポリシーが外部インターフェイスに適用されます。

例 20-10　MGCP 検査のイネーブル化および設定

```
hostname(config)# access-list mgcp_acl permit udp any any eq 2427
hostname(config)# access-list mgcp_acl permit udp any any eq 2727
hostname(config)# class-map mgcp-traffic
hostname(config-cmap)# match access-list mgcp_acl
hostname(config-cmap)# mgcp-map sample_map
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
hostname(config-mgcp-map)# command-queue 150
hostname(config-mgcp-map)# policy-map sample_policy
hostname(config-pmap)# class mgcp_port
hostname(config-pmap-c)# inspect mgcp sample_map
hostname(config-pmap-c)# service-policy sample_policy interface outside
```

MGCP タイムアウト値の設定

timeout mgcp コマンドは、MGCP メディア接続が終了したあとの、非アクティビティ間隔を設定します。デフォルトは 5 分です。

timeout mgcp-pat コマンドは、PAT xlate のタイムアウトを設定します。MGCP にはキープアライブ メカニズムがないので、シスコ製ではない MGCP ゲートウェイ（コール エージェント）を使用する場合、30 秒のデフォルト タイムアウト間隔が終了すると PAT xlate は切断されます。

MGCP 検査の確認およびモニタ

show mgcp commands コマンドは、コマンド キュー内の MGCP コマンドの個数を表示します。**show mgcp sessions** コマンドは、既存の MGCP セッションの個数を表示します。**detail** オプションを指定すると、各コマンド（またはセッション）に関する追加情報が含まれます。次に、**show mgcp commands** コマンドの出力例を示します。

```
hostname# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
```

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

```
hostname# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
        Gateway IP      host-pc-2
        Transaction ID  2052
        Endpoint name   aaln/1
        Call ID         9876543210abcdef
        Connection ID
        Media IP        192.168.5.7
        Media port      6058
```

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

```
hostname# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
```

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

```
hostname# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
        Gateway IP      host-pc-2
        Call ID         9876543210abcdef
        Connection ID   6789af54c9
        Endpoint name   aaln/1
        Media lcl port  6166
        Media rmt IP    192.168.5.7
        Media rmt port  6058
```

NetBIOS 検査

NetBIOS 検査はデフォルトではイネーブルです。

NetBIOS 検査の詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect netbios** コマンド ページを参照してください。

PPTP 検査

PPTP 検査はデフォルトではディセーブルです。

PPTP 検査の詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect pptp** コマンド ページを参照してください。

RSH 検査

RSH 検査はデフォルトではイネーブルです。

RSH 検査の詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect rsh** コマンド ページを参照してください。

RTSP 検査

ここでは、RTSP アプリケーション検査をイネーブルにして、デフォルトのポート設定を変更する手順について説明します。次の内容について説明します。

- RTSP 検査の概要（p.20-53）
- RealPlayer の使用（p.20-54）
- 制限事項および制約事項（p.20-54）
- RTSP 検査のイネーブル化および設定（p.20-54）

RTSP 検査の概要

inspect rtsp コマンドを使用すると、RTSP アプリケーション検査を制御します。このコマンドは、ポリシー マップ クラス コンフィギュレーション モードで利用できます。このコマンドは、デフォルトではディセーブルです。**inspect rtsp** コマンドは、FWSM に RTSP パケットを通過させます。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、Cisco IP/TV 接続によって使用されます。

（注） Cisco IP/TV の場合、RTSP TCP ポート 554 および TCP 8554 を使用します。

RTSP アプリケーションは、well-known ポート 554 の TCP（まれに UDP）を制御チャネルとして使用します。FWSM は、RFC 2326 に基づき、TCP だけをサポートしています。TCP 制御チャネルは、クライアント上に設定されたトランスポート モードに応じて、オーディオ / ビデオ トラフィックの伝送に使用するデータ チャネルをネゴシエートするために使用されます。

サポートされる RDT トランスポートは、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、x-pn-tng/udp です。

FWSM は、SETUP 応答メッセージをステータス コード 200 によって解析します。FWSM よりも外部にあるサーバからの応答メッセージを着信させるには、サーバからの着信接続用にダイナミック チャネルをオープンする必要があります。応答メッセージを発信する場合は、FWSM でダイナミック チャネルをオープンする必要はありません。

RFC 2326 は、SETUP 応答にクライアント ポートとサーバ ポートを含めることを規定していないので、FWSM でステートを保持し、SETUP メッセージ内のクライアント ポートを記憶します。QuickTime では、SETUP メッセージにクライアント ポートが設定され、サーバはサーバ ポートでのみ応答します。

RTSP 検査は PAT またはデュアル NAT をサポートしません。FWSM では、RTSP メッセージが HTTP メッセージ内に隠されている場合、HTTP クローキングを認識できません。

RealPlayer の使用

RealPlayer を使用する場合は、トランスポート モードを正しく設定することが重要です。FWSM では、サーバからクライアントに、またはクライアントからサーバに、**access-list** コマンドを追加します。RealPlayer では、**Options** >**Preferences** >**Transport** >**RTSP Settings** の順にクリックして、トランスポート モードを変更します。

RealPlayer で TCP モードを使用する場合は、**Use TCP to Connect to Server** および **Attempt to use TCP for all content** のチェックボックスを選択します。FWSM でインスペクション エンジンを設定する必要はありません。

RealPlayer で UDP モードを使用する場合は、**Use TCP to Connect to Server** および **Attempt to use UDP for static content** のチェックボックスを選択します。マルチキャスト経由でライブ コンテンツは利用できません。FWSM で、**inspect rtsp** *port* コマンドを追加します。

制限事項および制約事項

RTSP 検査には、次の制限が適用されます。

- FWSM は、UDP 上のマルチキャスト RTSP または RTSP メッセージをサポートしません。
- PAT はサポートされません。
- FWSM では、RTSP メッセージが HTTP メッセージ内に隠されている場合に HTTP クローキングを認識する機能はありません。
- FWSM では、RTSP メッセージ上で NAT を実行できません。組み込み IP アドレスが、HTTP または RTSP メッセージの一部である Session Description Protocol（SDP）ファイル内に含まれているからです。パケットは分割されることがあります。FWSM は、分割されたパケットに対しては NAT を実行できません。
- Cisco IP/TV を使用する場合、FWSM がメッセージの SDP 部分で実行する NAT 数は、Content Manager 内のプログラム リスト数に比例します（各プログラム リストには最低 6 つの IP アドレスが組み込まれています）。
- Apple QuickTime 4 または RealPlayer については、NAT を設定できます。Cisco IP/TV は、Viewer および Content Manager が外部ネットワーク上にあり、サーバが内部ネットワーク上にある場合に限り、NAT をサポートします。

RTSP 検査のイネーブル化および設定

RTSP アプリケーション検査をイネーブルにして設定する手順は、次のとおりです。

ステップ 1　FWSM の後ろで RTSP SETUP メッセージを受信するポートを決定します。デフォルト ポートは、TCP ポート 554 および 8554 です。

ステップ 2　RTSP SETUP メッセージを識別するアクセス リストを作成します。**access-list extended** コマンドを使用して、次のように各ポートと一致する ACE を追加します。

```
hostname(config)# access-list acl-name any any tcp eq port_number
```

ヒント　1 つのポート上にのみ、または連続したポート範囲に RTSP SETUP メッセージを許可する場合、アクセス リストの作成を省略できます。ステップ 4 では、**match access-list** コマンドではなく、**match port** コマンドを使用します。

ステップ 3　RTSP トラフィックを識別するには、クラス マップを作成するか、または既存のクラス マップを変更します。**class-map** コマンドを次のように使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

class_map_name は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI はクラス マップ 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　ステップ 1 で決定した RTSP ポートに送信されたトラフィックを識別します。そのためには、**match access-list** コマンドを次のように使用します。

```
hostname(config-cmap)# match access-list acl-name
```

ステップ 5　RTSP インスペクション エンジンを RTSP トラフィックに適用するために使用するポリシー マップを作成するか、または既存のポリシー マップを変更します。そのためには、**policy-map** コマンドを次のように使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

policy_map_name は、ポリシー マップの名前です。CLI はポリシー マップ コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 6　ステップ 3 で作成したクラス マップを指定します。このクラス マップは RTSP トラフィックを識別します。**class** コマンドを次のように使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name は、ステップ 2 で作成したクラス マップの名前です。CLI はポリシー マップ クラス コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 7　RTSP アプリケーション検査をイネーブルにします。そのためには、**inspect rtsp** コマンドを次のように使用します。

```
hostname(config-pmap-c)# inspect rtsp
hostname(config-pmap-c)#
```

ステップ 8　ポリシー マップをグローバルに、または特定のインターフェイスに適用するには、**service-policy** コマンドを次のように使用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface
interface_ID]
hostname(config)#
```

policy_map_name は、ステップ 5 で設定したポリシー マップです。ポリシー マップをすべてのインターフェイス上のトラフィックに適用する場合、**global** オプションを使用します。ポリシー マップを特定のインターフェイス上のトラフィックに適用する場合、***interface*** *interface_ID* オプションを使用します。*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

FWSM は、指定のとおりに RTSP トラフィックの検査を開始します。

例 20-11 に、デフォルト ポート（554 および 8554）上で RTSP インスペクション エンジンの RTSP トラフィックをイネーブルにする手順を示します。サービス ポリシーを外部インターフェイスに適用します。

例 20-11　RTSP 検査のイネーブル化および設定

```
hostname(config)# access-list rtsp_acl permit tcp any any eq 554
hostname(config)# access-list rtsp_acl permit tcp any any eq 8554
hostname(config)# class-map rtsp-traffic
hostname(config-cmap)# match access-list rtsp_acl
hostname(config-cmap)# policy-map sample_policy
hostname(config-pmap)# class rtsp_port
hostname(config-pmap-c)# inspect rtsp 554
hostname(config-pmap-c)# inspect rtsp 8554
hostname(config-pmap-c)# service-policy sample_policy interface outside
```

SIP 検査

ここでは、SIP アプリケーション検査をイネーブルにして、デフォルトのポート設定を変更する手順について説明します。次の内容について説明します。

- SIP 検査の概要（p.20-57）
- SIP インスタント メッセージング（p.20-57）
- IP アドレス プライバシー（p.20-58）
- SIP 検査のイネーブル化および設定（p.20-59）
- SIP タイムアウト値の設定（p.20-61）
- SIP 検査の確認およびモニタ（p.20-61）

SIP 検査の概要

Session Initiation Protocol（SIP）は、Internet Engineering Task Force（IETF）に定義されているように、コール処理セッションをイネーブルにします。特に、二者間オーディオ会議または「コール」に使用されます。SIP は、SDP と連携してコール シグナリングを処理します。SDP は、メディア ストリームのポートを指定します。SIP を使用すると、FWSM は、任意の SIP VoIP ゲートウェイと VoIP プロキシ サーバをサポートできます。SIP と SDP の定義は、次の RFC で定義されています。

- SIP：Session Initiation Protocol、RFC 2543
- SDP：Session Description Protocol、RFC 2327

FWSM 経由の SIP コールをサポートするには、メディア接続アドレス、メディア ポート、メディアの初期接続のシグナリング メッセージを検査する必要があります。SIP シグナリングが well-known 宛先ポート（UDP/TCP 50/60）に送信される間に、メディア ストリームはダイナミックに割り当てられたポートを使用します。また、SIP は、IP パケットのユーザ データ部分に IP アドレスを組み込みます。SIP 検査は、これらの組み込まれた IP アドレスに対して NAT を適用します。

SIP とともに PAT を使用する場合に、次の制限事項および制約事項が適用されます。

- リモート エンドポイントが、FWSM によって保護されたネットワーク上の SIP プロキシに登録しようとする場合、次の特殊な状態では登録できません。
  - PAT がリモート エンドポイントに設定されています。
  - SIP 登録サーバが、外部ネットワーク上にあります。
  - エンドポイントによってプロキシ サーバに送信された REGISTER メッセージ内の接続フィールドで、ポートが失われます。
- SIP デバイスが、SDP 部分に owner/creator フィールド（o=）の IP アドレスがあるパケットを送信する場合、o= フィールドの IP アドレスは正しく変換されないことがあります。この owner/creator フィールドの IP アドレスは、接続フィールド（c=）の IP アドレスとは異なります。これは、SIP プロトコルの制限事項によるもので、o= フィールドにポート値を提供しません。

SIP インスタント メッセージング

インスタント メッセージングは、ユーザの間でほぼリアルタイムでメッセージを転送することです。SIP は、Windows Messenger RTC Client バージョン 4.7.0105 のみを使用して、Windows XP 上でチャット機能をサポートします。MESSAGE/INFO 方法および 202 Accept 応答は、次の RFC で定義された IM をサポートするのに使用されます。

- Session Initiation Protocol（SIP）-Specific Event Notification、RFC 3265
- Session Initiation Protocol（SIP）Extension for Instant Messaging、RFC 3428

MESSAGE/INFO 要求は、登録 / 加入後いつでも行うことができます。たとえば、2 人のユーザが常時オンライン上にいても、数時間チャットできません。したがって、SIP インスペクション エンジンは、設定された SIP タイムアウト値に従って、タイムアウトするピンホールを開きます。この値は、Subscription 時間よりも 5 分以上長く設定する必要があります。Subscription 時間は、Contact Expires 値で定義され、一般的に 30 分です。

MESSAGE/INFO 要求は一般的に、ポート 5060 以外のダイナミックに割り当てられたポートを使用して送信されるので、SIP インスペクション エンジンを通過する必要があります。

(注) 現在、チャット機能のみサポートされます。ホワイトボード、ファイル転送、アプリケーション共有 はサポートされていません。RTC Client 5.0 はサポートされません。

SIP 検査は、SIP のテキスト ベースのメッセージで NAT を実行し、メッセージの SDP 部分のコンテンツの長さを再計算し、さらにパケット長とチェックサムを再計算します。また、SIP メッセージの SDP 部分に指定されたポートのメディア接続をダイナミックにオープンします。エンドポイントは、そのアドレス / ポート上で待ち受けるからです。

SIP 検査には、SIP ペイロードからの CALL_ID/FROM/TO インデックスを持ったデータベースがあります。このインデックスは、コール、送信元、宛先を識別します。このデータベースには、SDP メディア情報フィールドのメディア アドレスとメディア ポート、およびメディアのタイプが保管されます。1 つのセッションに複数のメディア アドレスとポートが存在することもあります。FWSM は、これらのメディア アドレス / ポートを使用して 2 つのエンドポイント間で RTP/RTCP 接続をオープンします。

初回のコール セットアップ（INVITE）メッセージには、well-known ポート 5060 を使用する必要があります。ただし、以降のメッセージには、このポート番号を含める必要はありません。SIP インスペクション エンジンは、シグナリング接続ピンホールをオープンし、これらの接続を SIP 接続としてマークします。これは、メッセージに SIP を適用し、NAT を実行するためです。

コールがセットアップされると、SIP セッションは、接続先エンドポイントからの応答メッセージにより、接続先エンドポイントが待ち受ける RTP ポートを示すメディア アドレスとメディア ポートを受信するまで、「一時的な」ステートになります。1 分以内に応答メッセージを受信しなかった場合、そのシグナリング接続は切断されます。

最終ハンドシェイクが完了すると、コール ステートがアクティブになり、BYE メッセージを受信するまで、シグナリング接続が持続されます。

内部エンドポイントから外部エンドポイントにコールを開始する場合には、内部エンドポイントからの INVITE メッセージに指定される内部エンドポイントのメディア アドレスおよびメディア ポートに RTP/RTCP UDP パケットが転送されるように、外部インターフェイスに対してメディア ホールがオープンされます。内部インターフェイスへの非送信要求 RTP/RTCP UDP パケットは、FWSM の設定で具体的に許可されている場合を除き、FWSM を通過しません。

IP アドレス プライバシー

IP アドレス プライバシーをイネーブルにすると、IP Phone コールまたはインスタント メッセージング セッションに参加している 2 つの SIP エンドポイントが、同じ内部ファイアウォール インターフェイスを使用して、外部ファイアウォール インターフェイス上の SIP プロキシ サーバに接続する場合、すべての SIP シグナリング メッセージは SIP プロキシ サーバを通過します。

SIP over TCP または UDP アプリケーション検査がイネーブルならば、IP アドレス プライバシーをイネーブルにできます。この機能は、デフォルトではディセーブルです。IP アドレス プライバシーがイネーブルの場合、FWSM は、着信 SIP トラフィックの TCP または UDP ペイロードに組み込まれた内部および外部ホスト IP アドレスを変換せず、IP アドレスの変換規則は無視されます。

SIP マップ コンフィギュレーション モードで **ip-address-privacy** コマンドを使用すると、この機能がイネーブルであるかどうか制御できます。

SIP 検査のイネーブル化および設定

SIP 検査はデフォルトではイネーブルです。

SIP 検査をイネーブルにするには、IP アドレス プライバシー機能をイネーブルにすることに関係なく、次の手順を実行します。

ステップ 1　FWSM の後ろの SIP サーバが SIP トラフィックを待ち受けるポートを決定します。デフォルト ポートは、TCP および UDP ポート 5060 です。

ステップ 2　SIP トラフィックを識別するには、クラス マップを作成するか、または既存のクラス マップを変更します。**class-map** コマンドを次のように使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

class_map_name は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI はクラス マップ コンフィギュレーション モードを開始します。

ステップ 3　ステップ 1 で決定した SIP ポートに送信されたトラフィックを識別します。そのためには、**match port** または **match access-list** コマンドを使用します。

UDP および TCP ポートを識別する、または連続しない 2 つ以上のポートを特定する必要がある場合、**access-list extended** コマンドを使用してアクセス リストを作成し、各ポートと一致する ACE を追加してから、**match access-list** コマンドを使用します。次のコマンドは、アクセス リストを使用して、アクセス リストを持った UDP および TCP ポートを識別します。

```
hostname(config)# access-list acl-name any any tcp eq port_number
hostname(config)# access-list acl-name any any udp eq port_number
hostname(config)# class-map class_map_name
hostname(config-cmap)# match access-list acl-name
```

単一プロトコルを使用して単一ポートを特定する必要がある場合、次のように **match port** コマンドを使用します。

```
hostname(config-cmap)# match port {tcp | udp} port_number
```

port_number は、FWSM の後ろの SIP サーバが待ち受けるポートのみです。

単一プロトコルの連続したポート範囲を特定する必要がある場合、次のように **range** キーワードを指定して **match port** コマンドを使用します。

```
hostname(config-cmap)# match port tcp range begin_port_number end_port_number
```

begin_port_number は SIP ポート範囲の最小ポートで、*end_port_number* は最大ポートです。

ステップ 4　（任意）IP アドレス プライバシーをイネーブルにする場合、次の手順を実行します。

a. SIP 検査のパラメータを含む SIP マップを作成します。**sip-map** コマンドを次のように使用します。

```
hostname(config-cmap)# sip-map map_name
hostname(config-sip-map)#
```

map_name は、SIP マップの名前です。CLI は、SIP マップ コンフィギュレーション コマンドを開始します。

b. 次のコマンドを入力して、SIP マップの設定を定義します。

```
hostname(config-sip-map)# ip-address-privacy
```

ステップ 5　SIP インスペクション エンジンを SIP トラフィックに適用するために使用するポリシー マップを作成するか、または既存のポリシー マップを変更します。そのためには、**policy-map** コマンドを次のように使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

policy_map_name は、ポリシー マップの名前です。CLI はポリシー マップ コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 6　ステップ 2 で作成したクラス マップを指定します。このクラス マップは SIP トラフィックを識別します。**class** コマンドを次のように使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name は、ステップ 2 で作成したクラス マップの名前です。CLI はポリシー マップ クラス コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 7　SIP アプリケーション検査をイネーブルにします。そのためには、**inspect sip** コマンドを次のように使用します。

```
hostname(config-pmap-c)# inspect sip [map_name]
hostname(config-pmap-c)#
```

map_name は、ステップ 4 （任意）で作成した SIP マップです。

ステップ 8　ポリシー マップをグローバルに、または特定のインターフェイスに適用するには、**service-policy** コマンドを次のように使用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface
interface_ID]
hostname(config)#
```

policy_map_name は、ステップ 5 で設定したポリシー マップです。ポリシー マップをすべてのインターフェイス上のトラフィックに適用する場合、**global** オプションを使用します。ポリシー マップを特定のインターフェイス上のトラフィックに適用する場合、***interface*** *interface_ID* オプションを使用します。*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

FWSM は、指定のとおりに SIP トラフィックの検査を開始します。

例 20-12 に示すように、SIP インスペクション エンジンをイネーブルにし、デフォルト ポート（5060）の SIP トラフィックと一致するクラス マップを作成します。それからサービス ポリシーを外部インターフェイスに適用します。

例 20-12　SIP アプリケーション検査のイネーブル化

```
hostname(config)# class-map sip_port
hostname(config-cmap)# match port tcp eq 5060
hostname(config-cmap)# sip-map sample_map
hostname(config-snmp-map)# ip-address-privacy
hostname(config-snmp-map)# policy-map sample_policy
hostname(config-pmap)# class sip_port
hostname(config-pmap-c)# inspect sip sample_map
hostname(config-pmap-c)# service-policy sample_policy interface outside
```

SIP タイムアウト値の設定

メディア接続は、接続が休止してから 2 分以内に切断されます。ただし、このタイムアウトの値は変更できるので、より短い（または長い）時間を設定できます。SIP 制御接続のタイムアウト値を設定するには、次のコマンドを使用します。

```
hostname(config)# timeout sip hh:mm:ss
```

このコマンドを使用して、SIP 制御接続を終了するまでののアイドル タイムアウトを設定します。

SIP メディア接続のタイムアウト値を設定するには、次のコマンドを使用します。

```
hostname(config)# timeout sip_media hh:mm:ss
```

このコマンドを使用して、SIP メディア接続を終了するまでのアイドル タイムアウトを設定します。

SIP 検査の確認およびモニタ

show sip コマンドは、SIP インスペクション エンジンの問題のトラブルシューティングに役立ち、**inspect protocol sip udp 5060** コマンドで説明します。**show timeout sip** コマンドは、指定されたプロトコルのタイムアウト値を表示します。

show sip コマンドは、FWSM を超えて確立された SIP セッションに関する情報を表示します。**debug sip** および **show local-host** コマンドとともに、このコマンドは、SIP インスペクション エンジンの問題のトラブルシューティングに使用されます。

（注） **show sip** コマンドを入力する前に、**pager** コマンドを設定することを推奨します。多くの SIP セッション レコードが存在し、**pager** コマンドが設定されていない場合、**show sip** コマンドの出力が最後まで到達するには、しばらく時間がかかります。

次に、**show sip** コマンドの出力例を示します。

```
hostname# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
    state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
    state Active, idle 0:00:06
```

この例では、FWSM 上に 2 つのアクティブ SIP セッションがあります（Total フィールドを参照）。各 call-id　はコールを示します。

最初のセッションは、call-id c3943000-960ca-2e43-228f@10.130.56.44 で、Call Init 状態にあります。これは、このセッションはまだコール セットアップ中であることを示しています。コール セットアップは、コールへの最後の応答が受信されるまでは完了しません。たとえば、発信者はすでに INVITE を送信して、100 Response を受信した可能性がありますが、200 OK はまだ受信していません。したがって、コール セットアップはまだ完了していません。1xx で始まっていない応答メッセージは最後の応答と考えられます。このセッションは、1 秒間アイドル状態でした。

2 番めのセッションは、Active ステートです。ここでは、コール セットアップは完了して、エンドポイントはメディアを交換しています。このセッションは、6 秒間アイドル状態でした。

Skinny（SCCP）検査

ここでは、SCCP アプリケーション検査をイネーブルにして、デフォルトのポート設定を変更する手順について説明します。次の内容について説明します。

- SCCP 検査の概要（p.20-63）
- Cisco IP Phone のサポート（p.20-63）
- 制限事項および制約事項（p.20-64）
- SCCP 検査の設定およびイネーブル化（p.20-64）
- SCCP 検査の確認およびモニタ（p.20-66）

SCCP 検査の概要

Skinny（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境と併用できます。Cisco CallManager を使用することにより、SCCP クライアントと H.323 準拠端末を相互運用できます。FWSM におけるアプリケーション レイヤ機能では、SCCP Version 3.3 を認識します。SCCP プロトコルには、2.4、3.0.4、3.1.1、3.2、3.3.2 の 5 つのバージョンがあります。FWSM は、Version 3.3.2 までのすべてのバージョンをサポートします。

FWSM は、SCCP の PAT と NAT をサポートします。PAT は、使用する IP Phone のグローバル IP アドレスより IP Phone の数が多い場合に必要です。SCCP シグナリング パケットの NAT および PAT をサポートすることで、Skinny アプリケーション検査では、SCCP シグナリング パケットとメディア パケットのすべてが FWSM を通過することを保証します。

Cisco CallManager と Cisco IP Phone の間の通常のトラフィックは SCCP を使用し、特別な設定をすることなく SCCP 検査によって処理されます。FWSM は、DHCP オプション 150 および 66 もサポートしているので、Cisco IP Phone および他の DHCP クライアントに TFTP サーバの場所を送信できます。Cisco IP Phone は、要求に DHCP オプション 3 を含めることもあります。これは、デフォルト ルートを設定します。詳細については、「DHCP サーバで Cisco IP Phone を使用する方法」（p.8-33）を参照してください。

Cisco IP Phone のサポート

Cisco IP Phone と比較して Cisco CallManager の方がセキュリティの高いインターフェイス上に配置されているトポロジーでは、NAT が Cisco CallManager IP アドレスに必要な場合、マッピングは**スタティック**である必要があります。Cisco IP Phone では Cisco CallManager IP アドレスをその設定で明示的に指定する必要があるからです。スタティック アイデンティティ エントリにより、セキュリティの高いインターフェイス上の Cisco CallManager は Cisco IP Phone からの登録を受け入れることができます。Cisco IP Phone では、TFTP サーバにアクセスして、Cisco CallManager サーバに接続するのに必要な設定情報をダウンロードする必要があります。

TFTP サーバと比較して Cisco IP Phone の方がセキュリティの低いインターフェイス上にある場合は、アクセス リストを使用して UDP ポート 69 上の保護された TFTP サーバに接続する必要があります。TFTP サーバに対してはスタティック アイデンティティ エントリが必要ですが、アイデンティティ スタティック エントリにする必要はありません。NAT を使用する場合、スタティック アイデンティティ エントリは同じ IP アドレスにマッピングされます。PAT を使用する場合は、同じ IP アドレスとポートにマッピングされます。

TFTP サーバと Cisco CallManager と比較して Cisco IP Phone の方がセキュリティの高いインターフェイス上にある場合、Cisco IP Phone で接続を開始するためにアクセス リストもスタティック アイデンティティ エントリも必要ありません。

制限事項および制約事項

SCCP に対する現在のバージョンの PAT および NAT サポートに適用される制限は、次のとおりです。

- PAT は、**alias** コマンドを使用する設定とは連動しません。
- 外部 NAT または PAT も*サポートされません*。

内部 Cisco CallManager のアドレスが別のアドレスまたはポートに対して NAT または PAT 用に設定されている場合、外部 Cisco IP Phone の登録は失敗します。これは、FWSM が TFTP で転送されたファイル内容の NAT または PAT をサポートしていないからです。FWSM は TFTP メッセージの NAT をサポートし、TFTP ファイル用にピンホールを開きますが、FWSM は 電話の登録中に TFTP によって転送された Cisco IP Phone のコンフィギュレーション ファイルに埋め込まれた Cisco CallManager の IP アドレスおよびポートを変換できません。

（注） FWSM では、コール セットアップ中であるコール以外の SCCP コールのステートフル フェールオーバーはサポートされていません。

SCCP 検査の設定およびイネーブル化

SCCP 検査はデフォルトではイネーブルです。

SCCP 検査をイネーブルにする、または SCCP トラフィックの受信に使用するデフォルト ポートを変更する手順は、次のとおりです。

ステップ 1　グローバル コンフィギュレーション モードで次のコマンドを入力して、トラフィック クラスの名前を指定します。

```
hostname(config)# class-map class_map_name
```

class_map_name に、次のようなトラフィック クラスの名前を指定します。

```
hostname(config)# class-map sccp_port
```

class-map コマンドを入力すると、CLI はクラス マップ コンフィギュレーション モードを開始し、プロンプトが変わります。次に例を示します。

```
hostname(config-cmap)#
```

ステップ 2　クラス マップ コンフィギュレーション モードで、**match** コマンドを定義します。次に例を示します。

```
hostname(config-cmap)# match port tcp eq 2000
hostname(config-cmap)# exit
hostname(config)#
```

連続したポート範囲を割り当てるには、**range** キーワードを入力します。次に例を示します。

```
hostname(config-cmap)# match port tcp range 2000-2010
```

連続しない複数のポートを SCCP 検査に割り当てるには、**access-list extended** コマンドを入力して、各ポートと一致するよう ACE を定義します。それから **match** コマンドを入力して、アクセス リストと SCCP トラフィック クラスを対応付けます。

ステップ 3　次のコマンドを入力して、ポリシー マップの名前を指定します。

```
hostname(config)# policy-map policy_map_name
```

policy_map_name にポリシー マップの名前を指定します。次に例を示します。

```
hostname(config)# policy-map sample_policy
```

CLI はポリシー マップ コンフィギュレーション モードを開始し、それに応じてプロンプトが次のように変わります。

```
hostname(config-pmap)#
```

ステップ 4　次のコマンドを入力して、ステップ 1 で定義されたトラフィック クラスをポリシー マップに含めるよう指定します。

```
hostname(config-pmap)# class class_map_name
```

たとえば、次のコマンドを使用すると、sccp_port トラフィック クラスを現在のポリシー マップに割り当てます。

```
hostname(config-pmap)# class sccp_port
```

CLI はポリシー マップ クラス コンフィギュレーション モードを開始し、それに応じてプロンプトが次のように変わります。

```
hostname(config-pmap-c)#
```

ステップ 5　（任意）SCCP トラフィックを受信するため FWSM が使用するデフォルト ポートを変更するには、次のコマンドを入力します。

```
hostname(config-pmap-c)# inspect skinny
```

ステップ 6　次のコマンドを入力して、ポリシー マップ コンフィギュレーション モードに戻ります。

```
hostname(config-pmap-c)# exit
hostname(config-pmap)#
```

ステップ 7　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 モードに戻ります。

```
hostname(config-pmap)# exit
hostname(config)#
```

ステップ 8　次のコマンドを入力して、ポリシー マップをグローバルに、または特定のインターフェイスに適用します。

```
hostname(config)# service-policy policy_map_name [global | interface interface_ID
```

policy_map_name に ステップ 3 で設定したポリシー マップを指定し、**global** オプションを使用してすべてのインターフェイスを識別する、あるいは **nameif** コマンドで割り当てられた名前を使用して特定のインターフェイスを識別します。

たとえば、次のコマンドは sample_policy を外部インターフェイスに適用します。

```
hostname(config)# service-policy sample_policy interface outside
```

次のコマンドは sample_policy をすべての FWSM インターフェイスに適用します。

```
hostname(config)# service-policy sample_policy global
```

例 20-13 に示すように、SCCP インスペクション エンジンをイネーブルにし、デフォルト ポート（2000）の SCCP トラフィックと一致するクラス マップを作成します。それからサービス ポリシーを外部インターフェイスに適用します。

例 20-13　SCCP アプリケーション検査のイネーブル化

```
hostname(config)# class-map sccp_port
hostname(config-cmap)# match port tcp eq 2000
hostname(config-cmap)# exit
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class sccp_port
hostname(config-pmap-c)# inspect skinny
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

SCCP 検査の確認およびモニタ

show skinny コマンドは、SCCP（Skinny）インスペクション エンジンの問題のトラブルシューティングに役立ちます。次に、以下の条件における **show skinny** コマンドの出力例を示します。FWSM を越えてセットアップされているアクティブな Skinny セッションが 2 つあります。最初のセッションは、ローカル アドレス 10.0.0.11 にある内部 Cisco IP Phone と 172.18.1.33 にある外部 Cisco CallManager の間に確立されたオーディオ接続です。TCP ポート 2000 は CallManager です。2 番めのセッションは、ローカル アドレス 10.0.0.22 にある別の内部 Cisco IP Phone と同じ Cisco CallManager の間に確立されたビデオ接続です。

```
hostname# show skinny
        LOCAL                   FOREIGN                 STATE
----------------------------------------------------------------
1       10.0.0.11/52238         172.18.1.33/2000                1
  AUDIO 10.0.0.11/22948         172.18.1.22/20798
2       10.0.0.22/52232         172.18.1.33/2000                1
  VIDEO 10.0.0.22/20798         172.18.1.11/22948
```

この出力は、両方の内部 Cisco IP Phone の間でコールが確立されていることを示します。最初と 2 番めの電話の RTP リスニング ポートは、それぞれ UDP 22948 と 20798 です。

次に、これらの Skinny 接続に対する **show xlate debug** コマンドの出力例を示します。

```
hostname# show xlate debug
2 in use, 2 most used
Flags:  D - DNS, d - dump, I - identity, i - inside, n - no random,
        r - portmap, s - static
NAT from inside:10.0.0.11 to outside:172.18.1.11 flags si idle 0:00:16 timeout 0:05:00
NAT from inside:10.0.0.22 to outside:172.18.1.22 flags si idle 0:00:14 timeout 0:05:00
```

SMTP および拡張 SMTP 検査

ここでは、SMTP および ESMTP アプリケーション検査をイネーブルにして、デフォルトのポート設定を変更する手順について説明します。次の内容について説明します。

- SMTP および拡張 SMTP 検査の概要（p.20-67）
- SMTP および拡張 SMTP アプリケーション検査の設定およびイネーブル化（p.20-68）

SMTP および拡張 SMTP 検査の概要

FWSM は、SMTP および ESMTP のアプリケーション検査をサポートします。これらのプロトコルのアプリケーション検査は、FWSM を通過できる SMTP または ESMTP コマンドのタイプを制限したり、モニタ機能を追加することで、攻撃から保護します。

ESMTP は SMTP プロトコルの機能を強化したもので、SMTP と同様の機能を持ちます。便宜上、ここでは SMTP という用語を使用して、SMTP と ESMTP 両方を表します。ESMTP のアプリケーション検査プロセスには、SMTP セッションのサポートが含まれます。ESMTP セッションで使用するコマンドの多くは、SMTP セッションで使用するコマンドと同じですが、ESMTP セッションはかなり高速で、信頼性とセキュリティに関連したオプション（配信ステータス通知など）をより多く提供します。

inspect smtp コマンドは、7 つの RFC 821 コマンド（DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET）をサポートします。**inspect esmtp** コマンドは、この 7 つのコマンドをサポートし、拡張 SMTP コマンド（AUTH、HELP、EHLO、ETRN、SAML、SEND、SOML、VRFY）もサポートします。

他の SMTP または ESMTP コマンド、および ESMTP のプライベートな拡張はサポートされません。サポートされないコマンドは X に変換され、FWSM で保護された SMTP サーバによって拒否されます。この場合、「500 Command unknown: 'XXX'」というメッセージが表示されます。不完全なコマンドは廃棄されます。

SMTP アプリケーション検査は、**inspect smtp** コマンドでイネーブルになって、高速パス処理で実行されます。したがって、この検査は FWSM 上の 3 つのネットワーク プロセッサのいずれかで実行されます。ESMTP アプリケーション検査は、**inspect esmtp** コマンドでイネーブルになって、制御プレーン パス処理で実行されます。したがって、この検査は FWSM 上の 1 つの汎用プロセッサで実行されます。

（注） ポリシー マップに **inspect smtp** コマンドと **inspect esmtp** コマンドの両方が含まれる場合、ポリシー マップに記載された最初のコマンドのみが一致するトラフィックに適用されます。

検査では、「2」、「0」、「0」の文字を除き、サーバの SMTP バナーの文字をアスタリスクに変更します。Carriage Return（CR; 復帰）および Linefeed（LF; 改行）の文字は無視されます。

SMTP 検査がイネーブルで、次の規則が順守されていない場合、インタラクティブ SMTP に使用する Telnet セッションが中断することがあります。SMTP コマンドの長さは 4 文字以上で、CR および LF で終了する必要があります。また、次の応答を発行する前に、応答を待つ必要があります。

SMTP サーバは、応答コードの番号と任意の読み取り可能な文字列によって、クライアントの要求に応答します。SMTP アプリケーション検査は、ユーザが使用できるコマンドおよびサーバが戻すメッセージを制御して、削減します。SMTP 検査は、次の 3 つの主要なタスクを実行します。

- SMTP 要求を、7 つの基本的な SMTP コマンドと 8 つの拡張コマンドに制限します。
- SMTP コマンド応答シーケンスをモニタします。
- 監査追跡の生成 — メール アドレス内の無効文字が置換された場合、監査記録 108002 が生成されます。詳細については、RFC 821 を参照してください。

SMTP 検査は、コマンドと応答のシーケンスをモニタして、次の異常を検出します。

- 不完全なコマンド
- コマンドの不正な終了（<CR><LR> で終了していない）
- MAIL コマンドおよび RCPT コマンドには、メールの送信者および受信者が指定されています。不正な文字が含まれていないかどうか、メール アドレスがスキャンされます。パイプライン文字（|）は削除されます（空白スペースに変更されます）。「<」および「>」は、メール アドレスを定義している場合にのみ認められます（「>」の前に必ず「<」があることが前提です）。
- SMTP サーバによる予期しない移行
- 未知のコマンドがあると、FWSM はパケット内のすべての文字を X に変更します。この場合、サーバからクライアントにエラー コードが戻されます。パケット内が変更されるので、TCP チェックサムが再計算または調整されます。
- TCP ストリームの編集
- コマンドのパイプライン化

SMTP および拡張 SMTP アプリケーション検査の設定およびイネーブル化

SMTP 検査はデフォルトではイネーブルです。

SMTP または拡張 SMTP 検査をイネーブルにする手順は、次のとおりです。

ステップ 1　FWSM の後ろの SMTP サーバが SMTP トラフィックを待ち受けるポートを決定します。デフォルト ポートは TCP ポート 25 ですが、他のポートを待ち受けるよう SMTP サーバを設定できます。

ステップ 2　SMTP トラフィックを識別するには、クラス マップを作成するか、または既存のクラス マップを変更します。**class-map** コマンドを次のように使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

class_map_name は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI はクラス マップ コンフィギュレーション モードを開始します。

ステップ 3　**match** コマンドを使用して、ステップ 1 で決定した SMTP ポートに送信されたトラフィックを識別します。

ポート マッパ プロセスが単一ポートを待ち受ける場合、**match port** コマンドを使用して、ポートに送信されたトラフィックを次のように識別できます。

```
hostname(config-cmap)# match port tcp eq port_number
```

port_number は、ポート マッパ プロセスが待ち受けるポートです。連続したポート範囲を割り当てる必要がある場合、**range** キーワードを使用します。次に例を示します。

```
hostname(config-cmap)# match port tcp range begin_port_number end_port_number
```

ヒント　連続しない複数のポートを識別する必要がある場合、**access-list extended** コマンドを入力して、各ポートと一致するよう ACE を定義します。それから、**match port** コマンドではなく、**match access-list** コマンドを使用して、アクセス リストと SMTP トラフィック クラスを対応付けます。

ステップ 4　SMTP インスペクション エンジンを SMTP トラフィックに適用するのに使用するポリシー マップを作成します。そのためには、**policy-map** コマンドを次のように使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

policy_map_name は、ポリシー マップの名前です。CLI はポリシー マップ コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 5　ステップ 2 で作成したクラス マップを指定します。このクラス マップは SMTP トラフィックを識別します。**class** コマンドを次のように使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name は、ステップ 2 で作成したクラス マップの名前です。CLI はポリシー マップ クラス コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 6　次のうち、いずれかの作業を実行します。

a.　拡張 SMTP アプリケーション検査をイネーブルにするには、次のコマンドを入力します。

```
hostname(config-pmap-c)# inspect esmtp
```

b.　SMTP アプリケーション検査をイネーブルにするには、次のコマンドを入力します。

```
hostname(config-pmap-c)# inspect smtp
```

（注）　**inspect smtp** コマンドと **inspect esmtp** コマンドの違いについては、「SMTP および拡張 SMTP 検査の概要」（p.20-67）を参照してください。

ステップ 7　ポリシー マップをグローバルに、または特定のインターフェイスに適用するには、**service-policy** コマンドを次のように使用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface
interface_ID]
hostname(config)#
```

policy_map_name は、ステップ 4 で設定したポリシー マップです。ポリシー マップをすべてのインターフェイス上のトラフィックに適用する場合、**global** オプションを使用します。ポリシー マップを特定のインターフェイス上のトラフィックに適用する場合、***interface*** *interface_ID* オプションを使用します。*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

FWSM は、指定のとおりに SMTP トラフィックの検査を開始します。

例 20-14　ESMTP 検査の設定およびイネーブル化

```
hostname(config)# class-map smtp_port
hostname(config-cmap)# match port tcp eq 25
hostname(config-cmap)# policy-map sample_policy
hostname(config-pmap)# class smtp_port
hostname(config-pmap-c)# inspect esmtp
hostname(config-pmap-c)# service-policy sample_policy interface outside
hostname(config)#
```

SNMP 検査

ここでは、SNMP アプリケーション検査をイネーブルにして、デフォルトのポート設定を変更する手順について説明します。次の内容について説明します。

- SNMP 検査の概要（p.20-70）
- SNMP アプリケーション検査のイネーブル化および設定（p.20-70）

SNMP 検査の概要

SNMP アプリケーション検査は、SNMP の特定のバージョンへの SNMP トラフィックを制限します。SNMP の初期のバージョンはセキュリティが低く、したがって、セキュリティ ポリシーによって所定の SNMP バージョンを拒否する必要があります。FWSM は、SNMP バージョン 1、2、2c、または 3 を拒否できます。SNMP マップ コンフィギュレーション モードで **deny version** コマンドを使用することにより、許可するバージョンを制御します。

SNMP アプリケーション検査のイネーブル化および設定

SNMP 検査のデフォルト設定を変更する手順は、次のとおりです。

ステップ 1　FWSM の後ろの ネットワーク デバイスが SNMP トラフィックを待ち受けるポートを決定します。デフォルト ポートは、TCP ポート 161 および 162 です。

ステップ 2　SNMP トラフィックを識別するには、クラス マップを作成するか、または既存のクラス マップを変更します。**class-map** コマンドを次のように使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

class_map_name は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI はクラス マップ コンフィギュレーション モードを開始します。

ステップ 3　**match** コマンドを使用して、ステップ 1 で決定した SNMP ポートに送信されたトラフィックを識別します。

連続したポート範囲を割り当てる必要がある場合、**range** キーワードを使用します。次に例を示します。

```
hostname(config-cmap)# match port tcp range begin_port_number end_port_number
```

begin_port_number は、SNMP ポート範囲の最小ポートで、*end_port_number* は最大ポートです。

ヒント　連続しない複数のポートを識別する必要がある場合、**access-list extended** コマンドを入力して、各ポートと一致するよう ACE を定義します。それから、**match port** コマンドではなく、**match access-list** コマンドを使用して、アクセス リストと SNMP トラフィック クラスを対応付けます。

ステップ 4　SNMP 検査のパラメータを含む SNMP マップを作成します。**snmp-map** コマンドを次のように使用します。

```
hostname(config-cmap)# snmp-map map_name
hostname(config-snmp-map)#
```

map_name は、SNMP マップの名前です。CLI は、SNMP マップ コンフィギュレーション コマンドを開始します。

ステップ 5　SNMP マップによって許可された SNMP のバージョンを指定します。そのためには、**deny version** コマンドを使用して、許可しないバージョンを次のように否定します。

```
hostname(config-snmp-map)# deny version version
hostname(config-snmp-map)#
```

version は、制限する SNMP バージョンです。*version* の有効な値は 1、2、2c、3 です。**deny version** コマンドを必要な回数入力できます。

ステップ 6　SNMP インスペクション エンジンを SNMP トラフィックに適用するために使用するポリシー マップを作成するか、または既存のポリシー マップを変更します。そのためには、**policy-map** コマンドを次のように使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

policy_map_name は、ポリシー マップの名前です。CLI はポリシー マップ コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 7　ステップ 2 で作成したクラス マップを指定します。このクラス マップは SNMP トラフィックを識別します。**class** コマンドを次のように使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name は、ステップ 2 で作成したクラス マップの名前です。CLI はポリシー マップ クラス コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 8　SNMP アプリケーション検査をイネーブルにします。そのためには、**inspect snmp** コマンドを次のように使用します。

```
hostname(config-pmap-c)# inspect snmp snmp_map_name
hostname(config-pmap-c)#
```

snmp_map_name は、ステップ 4 で作成した SNMP マップです。

ステップ 9　ポリシー マップをグローバルに、または特定のインターフェイスに適用するには、**service-policy** コマンドを次のように使用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface
interface_ID]
hostname(config)#
```

policy_map_name は、ステップ 6 で設定したポリシー マップです。ポリシー マップをすべてのインターフェイス上のトラフィックに適用する場合、**global** オプションを使用します。ポリシー マップを特定のインターフェイス上のトラフィックに適用する場合、***interface*** *interface_ID* オプションを使用します。*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

FWSM は、指定のとおりに SNMP トラフィックの検査を開始します。

例 20-15 は、外部インターフェイスから TCP ポート 161 および 162 に送信されたトラフィック上で SNMP アプリケーション検査をイネーブルにします。

例 20-15　SNMP アプリケーション検査の設定

```
hostname(config)# class-map snmp_port
hostname(config-cmap)# match port tcp range 161 162
hostname(config-cmap)# snmp-map sample_map
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# deny version 2
hostname(config-snmp-map)# policy-map sample_policy
hostname(config-pmap)# class snmp_port
hostname(config-pmap-c)# inspect snmp sample_map
hostname(config-pmap-c)# service-policy sample_policy interface outside
hostname(config)#
```

SQL*Net 検査

SQL*Net 検査はデフォルトではイネーブルです。

SQL*Net 検査の詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect sqlnet** コマンド ページを参照してください。

Sun RPC 検査

ここでは、Sun RPC アプリケーション検査をイネーブルにして、デフォルトのポート設定を変更し、Sun RPC サービス テーブルを管理する手順について説明します。次の内容について説明します。

- Sun RPC 検査の概要（p.20-73）
- Sun RPC 検査のイネーブル化および設定（p.20-73）
- Sun RPC サービスの管理（p.20-75）
- Sun RPC 検査の確認およびモニタ（p.20-76）

Sun RPC 検査の概要

Sun RPC アプリケーション検査をイネーブルにする、または FWSM が待ち受けるポートを変更するには、ポリシー マップ クラス コンフィギュレーション モードで **inspect sunrpc** コマンドを使用します。このモードは、ポリシー マップ コンフィギュレーション モード内で **class** コマンドを使用すると利用できます。コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect sunrpc コマンドは、Sun RPC プロトコルのアプリケーション検査をイネーブルまたはディセーブルにします。Sun RPC は NFS および Network Information Service（NIS; ネットワーク情報サービス）によって使用されます。Sun RPC サービスは、任意のポート上で実行できます。クライアントからサーバ上の Sun RPC サーバにアクセスする場合には、サービスを実行しているポートを学習する必要があります。そのためには、well-known ポート 111 上のポート マッパ プロセス（通常は rpcbind）にクエリーを送信します。

クライアントからサービスの Sun RPC プログラム番号を送信すると、ポート マッパ プロセスはサービスのポート番号を戻します。クライアントは Sun RPC クエリーをサーバに送信し、ポート マッパ プロセスによって特定されたポートを指定します。サーバから応答が送信されると、FWSM はこのパケットを代行受信し、そのポート上で、TCP/UDP の両方の初期接続をオープンします。

（注） Sun RPC ペイロード情報の NAT または PAT はサポートされません。

Sun RPC 検査のイネーブル化および設定

Sun RPC 検査はデフォルトではイネーブルです。

（注） UDP 上で Sun RPC 検査をイネーブルにしたり設定したりするには、別のトラフィック クラスまたは新しいポリシー マップを定義する必要はありません。単に **inspect sunrpc** コマンドをポリシー マップに追加します。このポリシー マップのトラフィック クラスはデフォルトのトラフィック クラスによって定義されます。この設定の例を 例 20-17（p.20-75）に示します。

Sun RPC 検査をイネーブルにする、または TCP を使用して Sun RPC トラフィックの受信に使用するデフォルト ポートを変更する手順は、次のとおりです。

ステップ 1　ポート マッパ プロセスが待ち受けるポートを決定します。これはほとんどの場合、ポート 111 で、オペレーティング システムと実装状態に応じて異なります。

ステップ 2　Sun RP トラフィックを識別するには、クラス マップを作成するか、または既存のクラス マップを変更します。**class-map** コマンドを次のように使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

class_map_name は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI はクラス マップ コンフィギュレーション モードを開始します。

ステップ 3　**match** コマンドを使用して、ステップ 1 で決定したポートに送信されたトラフィックを識別します。

ポート マッパ プロセスが単一ポートを待ち受ける場合、**match port** コマンドを使用して、ポートに送信されたトラフィックを次のように識別できます。

```
hostname(config-cmap)# match port tcp eq port_number
```

port_number は、ポート マッパ プロセスが待ち受けるポートです。連続したポート範囲を割り当てる必要がある場合、**range** キーワードを使用します。次に例を示します。

```
hostname(config-cmap)# match port tcp range begin_port_number end_port_number
```

ヒント　連続しない複数のポートを識別する必要がある場合、**access-list extended** コマンドを入力して、各ポートと一致するよう ACE を定義します。それから、**match port** コマンドではなく、**match access-list** コマンドを使用して、アクセス リストと Sun RPC トラフィック クラスを対応付けます。

ステップ 4　Sun RPC インスペクション エンジンを Sun RPC トラフィックに適用するために使用するポリシー マップを作成するか、または既存のポリシー マップを変更します。そのためには、**policy-map** コマンドを次のように使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

policy_map_name は、ポリシー マップの名前です。CLI はポリシー マップ コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 5　ステップ 2 で作成したクラス マップを指定します。このクラス マップは Sun RPC トラフィックを識別します。**class** コマンドを次のように使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name は、ステップ 2 で作成したクラス マップの名前です。CLI はポリシー マップ クラス コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 6　Sun RPC アプリケーション検査をイネーブルにします。そのためには、次のコマンドを入力します。

```
hostname(config-pmap-c)# inspect sunrpc
hostname(config-pmap-c)#
```

ステップ 7　ポリシー マップをグローバルに、または特定のインターフェイスに適用するには、**service-policy** コマンドを次のように使用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface
interface_ID]
hostname(config)#
```

policy_map_name は、ステップ 4 で設定したポリシー マップです。ポリシー マップをすべてのインターフェイス上のトラフィックに適用する場合、**global** オプションを使用します。ポリシー マップを特定のインターフェイス上のトラフィックに適用する場合、***interface*** *interface_ID* オプションを使用します。*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

FWSM は、指定のとおりに Sun RPC トラフィックの検査を開始します。

例 20-16　TCP ベースの Sun RPC 検査のイネーブル化および設定

次に、外部インターフェイスから TCP ポート 111 に送信されたトラフィック上で Sun RPC アプリケーション検査をイネーブルにする例を示します。

```
hostname(config)# class-map sunrpc_port
hostname(config-cmap)# match port tcp eq 111
hostname(config-cmap)# policy-map sample_policy
hostname(config-pmap)# class sunrpc_port
hostname(config-pmap-c)# inspect sunrpc
hostname(config-pmap-c)# service-policy sample_policy interface outside
hostname(config)#
```

例 20-17 に、Sun RPC over UDP をイネーブルにする例を示します。これを行うには、アクションをデフォルト トラフィック クラスに適用するポリシー マップに、**inspect sunrpc** コマンドを追加します。

例 20-17　UDP ベースの Sun RPC 検査のイネーブル化および設定

```
hostname(config)# policy-map asa_global_fw_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect sunrpc
hostname(config-pmap-c)#
```

Sun RPC サービスの管理

FWSM は、確立された Sun RPC セッションを制御するための Sun RPC サービス テーブルを保持します。Sun RPC サービス テーブルにエントリを作成するには、グローバル コンフィギュレーション モードで **sunrpc-server** コマンドを使用します。

sunrpc-server コマンドを使用して、FWSM が Sun RPC アプリケーション検査によってオープンしたピンホールを閉じるまでのタイムアウトを指定します。たとえば、IP アドレス 192.168.100.2 を持つ Sun RPC サーバに 30 分のタイムアウトを作成するには、次のコマンドを入力します。

```
hostname(config)# sunrpc-server inside 192.168.100.2 255.255.255.255 service 100003
protocol tcp 111 timeout 00:30:00
```

このコマンドは、Sun RPC アプリケーション検査によってオープンしたピンホールが 30 分後に閉じるよう指定します。この例では、Sun RPC サーバは TCP ポート 111 を使用する内部インターフェイス上にあります。UDP、異なるポート番号、またはポート範囲も指定できます。ポート範囲を指定するには、開始ポート番号と終了ポート番号の間にハイフンを使用して区切ります（例、111-113）。

サービス タイプは、特定のサービス タイプとサービスに使用するポート番号の間にマッピングを指定します。サービス タイプ（この例では 100003）を決定するには、Sun RPC サーバ マシン上の UNIX または Linux コマンドラインで **sunrpcinfo** コマンドを使用します。

Sun RPC コンフィギュレーションを消去するには、次のコマンドを入力します。

```
hostname(config)# clear configure sunrpc-server
```

これは、**sunrpc-server** コマンドを使用して、実行されたコンフィギュレーションを削除します。**sunrpc-server** コマンドを使用すると、指定されたタイムアウトでピンホールを作成できます。

アクティブ Sun RPC サービスを消去するには、次のコマンドを入力します。

```
hostname(config)# clear sunrpc-server active
```

Sun RPC アプリケーション検査はポート マッパ サービスへのサービス要求に基づいてトラフィックをイネーブルにしたので、これはオープンしたピンホールを消去します。

Sun RPC 検査の確認およびモニタ

ここでの出力例は、内部インターフェイス上で IP アドレス 192.168.100.2 を持つ Sun RPC サーバ、および外部インターフェイス上で IP アドレス 209.168.200.5 を持つ Sun RPC クライアントが対象です。

現在の Sun RPC 接続に関する情報を表示するには、**show conn** コマンドを入力します。次に、**show conn** コマンドの出力例を示します。

```
hostname# show conn
15 in use, 21 most used
UDP out 209.165.200.5:800 in 192.168.100.2:2049 idle 0:00:04 flags -
UDP out 209.165.200.5:714 in 192.168.100.2:111 idle 0:00:04 flags -
UDP out 209.165.200.5:712 in 192.168.100.2:647 idle 0:00:05 flags -
UDP out 192.168.100.2:0 in 209.165.200.5:714 idle 0:00:05 flags i
hostname(config)#
```

Sun RPC サービス テーブル コンフィギュレーションに関する情報を表示するには、**show running-config sunrpc-server** コマンドを入力します。次に、**show running-config sunrpc-server** コマンドの出力例を示します。

```
hostname(config)# show running-config sunrpc-server
sunrpc-server inside 192.168.100.2 255.255.255.255 service 100003 protocol UDP port
111 timeout 0:30:00
sunrpc-server inside 192.168.100.2 255.255.255.255 service 100005 protocol UDP port
111 timeout 0:30:00
```

この出力では、30 分のタイムアウト間隔が、内部インターフェイス上で IP アドレス 192.168.100.2 を持つ Sun RPC サーバの UDP ポート 111 に設定されたことを示します。

Sun RPC サービスのオープンしたピンホールを表示するには、**show sunrpc-server active** コマンドを入力します。次に、**show sunrpc-server active** コマンドの出力例を示します。

```
hostname# show sunrpc-server active
LOCAL FOREIGN SERVICE TIMEOUT
-----------------------------------------------
1 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
2 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
3 209.165.200.5/0 192.168.100.2/647 100005 0:30:00
4 209.165.200.5/0 192.168.100.2/650 100005 0:30:00
```

LOCAL カラムのエントリは内部インターフェイス上のクライアントまたはサーバの IP アドレスを示します。FOREIGN カラムの値は外部インターフェイス上のクライアントまたはサーバの IP アドレスを示します。

Sun RPC サーバ上で実行する Sun RPC サービスに関する情報を表示するには、Linux または UNIX サーバのコマンドラインから **rpcinfo -p** コマンドを入力します。次に、**rpcinfo -p** コマンドの出力例を示します。

```
sunrpcserver:~ # rpcinfo -p
program vers proto port
100000 2 tcp 111 portmapper
100000 2 udp 111 portmapper
100024 1 udp 632 status
100024 1 tcp 635 status
100003 2 udp 2049 nfs
100003 3 udp 2049 nfs
100003 2 tcp 2049 nfs
100003 3 tcp 2049 nfs
100021 1 udp 32771 nlockmgr
100021 3 udp 32771 nlockmgr
100021 4 udp 32771 nlockmgr
100021 1 tcp 32852 nlockmgr
100021 3 tcp 32852 nlockmgr
100021 4 tcp 32852 nlockmgr
100005 1 udp 647 mountd
100005 1 tcp 650 mountd
100005 2 udp 647 mountd
100005 2 tcp 650 mountd
100005 3 udp 647 mountd
100005 3 tcp 650 mountd
```

この出力では、ポート 647 は UDP 上で動作する mountd デーモンに相当します。mountd プロセスでは、一般的にポート 32780 がよく使用されますが、この例では TCP ポート 650 を使用します。

TFTP 検査

TFTP 検査はデフォルトではイネーブルです。

TFTP 検査の詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **inspect tftp** コマンド ページを参照してください。

XDMCP 検査

XDMCP 検査はデフォルトではイネーブルです。ただし、XDMCP インスペクション エンジンは **established** コマンドの設定が正しくないと動作しません。

XDMCP 検査の詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **established** および **inspect pptp** コマンド ページを参照してください。

管理アクセスの設定

この章では、システム管理のために Telnet、SSH、HTTPS、および VPN 経由で FWSM にアクセスする方法を説明します。ユーザ認証および許可の方法についても説明します。

この章で説明する内容は次のとおりです。

- Telnet アクセスの許可（p.21-2）
- SSH アクセスの許可（p.21-3）
- ASDM 用の HTTPS アクセスの許可（p.21-5）
- VPN 管理接続の許可（p.21-6）
- FWSM との ICMP 送受信の許可（p.21-12）
- システム管理者用の AAA（p.21-13）

（注） 管理アクセスのために FWSM インターフェイスにアクセスするには、ホスト IP アドレスを許可するためのアクセス リストは不要です。この章の説明にしたがって、管理アクセスを設定してください。

Telnet アクセスの許可

FWSM では、管理を目的とした FWSM への Telnet 接続を設定できます。IPSec トンネル内部で Telnet を使用する場合を除き、セキュリティが最低のインターフェイスでは Telnet を使用できません。

FWSM では、各コンテキストについて最大 5 つの同時 Telnet 接続を実行でき、全コンテキスト間で最大 100 の接続が可能です。コンテキストごとに許可する Telnet セッション数を管理するには、リソース クラスを使用します（「クラスの設定」[p.4-16] を参照）。

FWSM に Telnet アクセスを設定する手順は、次のとおりです。

ステップ 1　各アドレスまたはサブネットについて次のコマンドを入力して、FWSM で接続を許可する IP アドレスを指定します。

```
hostname(config)# telnet source_IP_address mask source_interface
```

インターフェイスが 1 つだけの場合、インターフェイスのセキュリティ レベルが 100 であれば、そのインターフェイスへのアクセスに Telnet を設定することができます。

ステップ 2　（任意）FWSM によってセッションが切断されるまでの、Telnet セッションのアイドル時間の長さを設定するには、次のコマンドを入力します。

```
hostname(config)# telnet timeout minutes
```

タイムアウトの設定範囲は、1 ～ 1440 分です。デフォルトは 5 分です。ほとんどの場合、デフォルトのタイムアウト値は短すぎるので、すべての事前テストおよびトラブルシューティングが完了するまでは、タイムアウト値を増やしてください。

次に、アドレス 192.168.1.2 の内部インターフェイス上のホストに FWSM へのアクセスを許可する例を示します。

```
hostname(config)# telnet 192.168.1.2 255.255.255.255 inside
hostname(config)# telnet timeout 30
```

次に、192.168.3.0 ネットワーク上のすべてのユーザに、内部インターフェイス上の FWSM へのアクセスを許可する例を示します。

```
hostname(config)# telnet 192.168.3.0 255.255.255.0 inside
```

SSH アクセスの許可

FWSM では、管理を目的とした FWSM への SSH（セキュア シェル）接続を設定できます。FWSM では、コンテキストごとに最大 5 つの同時 SSH 接続を実行でき、全コンテキスト間で最大 100 の接続が可能です。各コンテキストに許可する SSH セッション数を管理するには、リソース クラスを使用します（「クラスの設定」[p.4-16] を参照）。

SSH は、TCP/IP などのトランスポート レイヤの上位で動作し、強力な認証および暗号化機能を提供するアプリケーションです。FWSM は SSH Version 1 および 2 で提供される SSH リモート シェル機能をサポートし、DES および 3DES 暗号をサポートします。

（注） SSL および SSH 上での XML 管理はサポートされません。

ここでは、次の内容について説明します。

- SSH アクセスの設定（p.21-3）
- SSH クライアントの使用（p.21-4）

SSH アクセスの設定

FWSM に SSH アクセスを設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、SSH に必要な RSA キー ペアを生成します。

```
hostname(config)# crypto key generate rsa modulus modulus_size
```

モジュール（ビット単位）は 512、768、1024、または 2048 です。指定するキー モジュールのサイズが大きいほど、RSA 生成に時間がかかります。推奨する値は 1024 です。

ステップ 2　次のコマンドを入力して、RSA キーを固定フラッシュ メモリに保存します。

```
hostname(config)# write memory
```

ステップ 3　各アドレスまたはサブネットについて次のコマンドを入力して、FWSM で接続を許可する IP アドレスを指定します。

```
hostname(config)# ssh source_IP_address mask source_interface
```

FWSM は、セキュリティ レベルが最低のものを含め、すべてのインターフェイスからの SSH 接続を受け入れます。

ステップ 4　（任意）FWSM によってセッションが切断されるまでの、SSH セッションのアイドル時間の長さを設定するには、次のコマンドを入力します。

```
hostname(config)# ssh timeout minutes
```

タイムアウトの設定範囲は、1 ～ 60 分です。デフォルトは 5 分です。ほとんどの場合、デフォルトのタイムアウト値は短すぎるので、すべての事前テストおよびトラブルシューティングが完了するまでは、タイムアウト値を増やしてください。

ステップ 5　（任意）次のコマンドを入力して、FWSM で許可する SSH のバージョンを制限します。デフォルトでは、FWSM は両方のバージョンを許可します。

```
hostname(config)# ssh version {1 | 2}
```

次に、RSA キーを生成し、アドレス 192.168.1.2 の内部インターフェイス上のホストに FWSM へのアクセスを許可する例を示します。

```
hostname(config)# crypto key generate rsa modulus 1024
hostname(config)# write mem
hostname(config)# ssh 192.168.1.2 255.255.255.255 inside
hostname(config)# ssh 192.168.1.2 255.255.255.255 inside
hostname(config)# ssh timeout 30
```

次に、192.168.3.0 ネットワーク上のすべてのユーザに、内部インターフェイス上の FWSM へのアクセスを許可する例を示します。

```
hostname(config)# ssh 192.168.3.0 255.255.255.0 inside
```

SSH クライアントの使用

SSH を使用して FWSM のコンソールにアクセスするには、SSH クライアントからユーザ名 **pix** を入力し、**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（「ログイン パスワードの変更」[p.7-2] を参照）。デフォルトのパスワードは「cisco」です。

SSH セッションが開始すると、FWSM のコンソールにドット（.）が表示され、続いて次のような SSH ユーザ認証プロンプトが表示されます。

```
hostname(config)# .
```

ドット表示は、SSH の機能には影響を与えません。コンソールのドット表示は、ユーザ認証を実行する前に、サーバ キーを生成しているか、または SSH キー交換中にプライベート キーを使用してメッセージを復号化していることを示しています。これらの処理には 2 分以上かかることがあります。ドットは、FWSM が稼働していて、処理実行中であることを示す進行状況インジケータです。

ASDM 用の HTTPS アクセスの許可

ASDM を使用するには、HTTPS サーバをイネーブルにして、FWSM への HTTPS 接続を許可する必要があります。**setup** コマンドを使用すると、これらの設定は完了します。ここでは、ASDM アクセスを手動で設定する場合の手順について説明します。

FWSM では、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 80 の ASDM インスタンスの使用が可能です。コンテキストごとに許可する ASDM セッション数を管理するには、リソース クラスを使用します（「クラスの設定」[p.4-16] を参照）。

ASDM アクセスを設定する手順は、次のとおりです。

ステップ 1　各アドレスまたはサブネットについて次のコマンドを入力して、FWSM で HTTPS 接続を許可する IP アドレスを指定します。

```
hostname(config)# http source_IP_address mask source_interface
```

ステップ 2　次のコマンドを入力して、HTTPS サーバをイネーブルにします。

```
hostname(config)# http server enable
```

次に、HTTPS サーバをイネーブルに設定し、アドレス 192.168.1.2 の内部インターフェイス上のホストに ASDM へのアクセスを許可する例を示します。

```
hostname(config)# http server enable
hostname(config)# http 192.168.1.2 255.255.255.255 inside
```

次に、192.168.3.0 ネットワーク上の全ユーザに、内部インターフェイス上の ASDM へのアクセスを許可する例を示します。

```
hostname(config)# http 192.168.3.0 255.255.255.0 inside
```

VPN 管理接続の許可

FWSM は、IPSec を使用した管理アクセスをサポートしています。IPSec Virtual Private Network（VPN; 仮想私設網）では、インターネットなどの安全性の低いネットワーク上で、IP パケットを確実かつ安全に転送できます。2 つの VPN ピア間の通信はすべて、セキュア トンネルを通じて転送されます。つまり、パケットは暗号化され、各ピアに認証されます。

FWSM は、サイトツーサイト トンネルを使用して、Cisco PIX セキュリティ アプライアンスまたは Cisco IOS ルータなどの他の VPN コンセントレータに接続できます。このトンネルを通じて通信できるピア ネットワークを指定します。FWSM の場合、トンネルの FWSM 側で使用できるアドレスは、対象インターフェイスのアドレスだけです。

ルーテッド モードの場合、FWSM は、VPN クライアントからの接続も受け入れます。VPN クライアントとは、Cisco VPN クライアント、または Cisco PIX セキュリティ アプライアンスなどの VPN コンセントレータを稼働するホスト、あるいは Easy VPN クライアントを稼働する Cisco IOS ルータを指します。この場合、サイトツーサイト トンネルとは異なり、クライアントの IP アドレスを事前に取得することはできないため、クライアント認証に依存することになります。透過ファイアウォール モードでは、リモート クライアントはサポートされていません。透過モードでは、サイトツーサイトのトンネルがサポートされます。

FWSM は、最大 5 つの同時 IPSec 接続をサポートし、全コンテキスト間で最大 10 の同時接続が可能です。コンテキストごとに許可する IPSec セッション数を管理するには、リソース クラスを使用します（「クラスの設定」[p.4-16] を参照）。

ここでは、次の内容について説明します。

- 全トンネルの基本的な設定（p.21-6）
- VPN クライアント アクセスの設定（p.21-8）
- サイトツーサイト トンネルの設定（p.21-10）

全トンネルの基本的な設定

VPN クライアント アクセスとサイトツーサイト トンネルの両方で次の手順を実行します。また、IKE ポリシー（IKE は ISAKMP の一部）および IPSec トランスフォームの設定も必要です。

すべてのトンネルに基本設定を設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、IKE 暗号化アルゴリズムを設定します。

```
hostname(config)# isakmp policy priority encryption {des | 3des}
```

3des キーワードのほうが、**des** キーワードよりも安全です。

複数の IKE ポリシーを設定できます。FWSM は、ピアのポリシーと一致するまで、*priority* の順序で各ポリシーを検証します。*priority* の値は 1 ～ 65,534 です。プライオリティは 1 が最高で、65,534 が最低です。次の **isakmp** コマンドにも、同じプライオリティ値を使用してください。

ステップ 2　次のコマンドを入力して、キー交換に使用する Diffie-Hellman グループを設定します。

```
hostname(config)# isakmp policy priority group {1 | 2}
```

グループ 1 は 768 ビット、グループ 2 は 1024 ビット（より安全性が高い）です。

ステップ 3　次のコマンドを入力して、認証アルゴリズムを設定します。

```
hostname(config)# isakmp policy priority hash {md5 | sha}
```

sha キーワードのほうが、**md5** キーワードよりも安全です。

ステップ 4　次のコマンドを入力して、IKE 認証方式を共有鍵として設定します。

```
hostname(config)# isakmp policy priority authentication pre-share
```

rsa-sig オプションを指定すると、共有鍵の代わりに証明書を使用できます。この方法の詳細については『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

ステップ 5　次のコマンドを入力して、トンネル インターフェイス上で IKE をイネーブルにします。

```
hostname(config)# isakmp enable interface_name
```

ステップ 6　次のコマンドを入力して、トランスフォーム セットの IPSec トンネルに使用する認証方式および暗号化方式を設定します。

```
hostname(config)# crypto ipsec transform-set transform_name
[esp-md5-hmac | esp-sha-hmac] {esp-aes-256 | esp-aes-192 | esp-aes |
esp-des | esp-3des}
```

認証のみ、または暗号化のみを指定することもできますが、これらの方法は安全ではありません。

このトランスフォーム セットは、VPN クライアント グループまたはサイトツーサイト トンネルの設定時に参照します。

トンネルでは最大 6 つのトランスフォーム セットを参照できます。トランスフォームが一致するまで、各セットが検証されます。

このトランスフォームの認証および暗号化アルゴリズムは通常、IKE ポリシー（**isakmp policy** コマンド）と一致します。サイトツーサイト トンネルの場合には、このトランスフォームがピアのトランスフォームと一致する必要があります。

認証オプションは、（安全性の高いほうから順に）次のとおりです。

- **esp-sha-hmac**
- **esp-md5-hmac**

暗号化オプションは、（安全性の高いほうから順に）次のとおりです。

- **esp-aes-256**
- **esp-aes-192**
- **esp-aes**
- **esp-3des**
- **esp-des**

（注）　**esp-null**（暗号化なし）を使用するのは、テストを行う場合だけです。

次に、複数の IKE ポリシーおよび IPSec トランスフォーム セットを設定する例を示します。

```
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)# isakmp policy 1 group 2
hostname(config)# isakmp policy 1 hash sha
hostname(config)# isakmp enable outside
hostname(config)# crypto ipsec transform-set vpn_client esp-3des esp-sha-hmac
hostname(config)# crypto ipsec transform-set site_to_site esp-3des ah-sha-hmac
```

VPN クライアント アクセスの設定

ルーテッド モードの場合、Cisco VPN クライアントの Version 3.0 がインストールされているホストであれば、インターネットなどの公衆ネットワークを通じて、管理目的で FWSM に接続できます。Cisco VPN クライアント Version 4.0 では、リモート アクセス VPN トンネルのエンド ポイントとして設定されたファイアウォール インターフェイスへの Telnet または SSH は許可されていません。

透過ファイアウォール モードでは、リモート クライアントはサポートされていません。透過モードでは、サイトツーサイトのトンネルがサポートされています。

VPN の基本設定（「全トンネルの基本的な設定」を参照）を完了したあと、リモート クライアントから FWSM への管理アクセスを許可する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、クライアント トンネルに許可するトランスフォーム セット（「全トンネルの基本的な設定」[p.21-6] で定義したセット）を指定します。

```
hostname(config)# crypto dynamic-map dynamic_map_name priority set transform-set
transform_set1 [transform_set2] [...]
```

複数のトランスフォーム セットを使用する場合は、プライオリティの順序（最高のプライオリティが最初）で指定します。

ダイナミック クリプト マップでは、未知の IP アドレスから FWSM に接続できます。

dynamic-map の名前は、ステップ 2 で使用します。

priority には、複数のコマンドを評価する優先順位を指定します。1 つのコマンドに 1 つのトランスフォーム セットを指定し、別のコマンドに別のセットを指定した場合、プライオリティの値に基づいて最初に評価されるコマンドが決まります。

ステップ 2　次のコマンドを入力して、スタティック トンネルに（ステップ 1 で指定した）ダイナミック クリプト マップを割り当てます。

```
hostname(config)# crypto map crypto_map_name priority ipsec-isakmp dynamic
dynamic_map_name
```

ステップ 3　次のコマンドを入力して、クライアント トンネルを終端するインターフェイスを指定します。

```
hostname(config)# crypto map crypto_map_name interface interface_name
```

1 つのインターフェイスに割り当てることのできる **crypto map** 名は 1 つだけです。したがって、サイトツーサイト トンネルと VPN クライアントの両方を同じインターフェイス上で終端する場合は、同じ **crypto map** 名を共有する必要があります。

ステップ 4　次のコマンドを入力して、VPN クライアントが FWSM 上で使用するアドレス範囲を指定します。

```
hostname(config)# ip local pool pool_name first_ip_address-last_ip_address [mask mask]
```

クライアントからのトンネル経由の全パケットが、送信元アドレスとして、これらのアドレスの 1 つを使用します。

ステップ 5　次のコマンドを入力して、FWSM 宛てのトラフィックを指定します。ステップ 7 の **tunnel group** コマンドで指定したトラフィックだけをトンネル化できます。

```
hostname(config)# access-list acl_name [extended] permit {protocol} host
fwsm_interface_address pool_addresses mask
```

このアクセス リストでは、ローカル プール（ステップ 4 を参照）から FWSM のインターフェイスに送信するトラフィックを特定しています。アクセス リストの詳細については、「拡張アクセス リストの追加」（p.10-7）を参照してください。

ステップ 6　次のコマンドを入力して、VPN グループに VPN アドレス プールを割り当てます。

```
hostname(config)# vpngroup group_name address-pool pool_name
```

このグループは、クライアントの接続に必要な VPN 特性です。クライアントは、FWSM への接続時に、この VPN グループ名と、ステップ 8 で指定する VPN グループ パスワードを入力する必要があります。

ステップ 7　次のコマンドを入力して、FWSM 宛てのトラフィックだけをトンネル化します。

```
hostname(config)# vpngroup group_name split-tunnel acl_name
```

このコマンドは必須です。

ステップ 8　次のコマンドを入力して、VPN グループのパスワードを設定します。

```
hostname(config)# vpngroup group_name password password
```

ステップ 9　「Telnet アクセスの許可」（p.21-2）および「SSH アクセスの許可」（p.21-3）を参照して、Telnet アクセスまたは SSH アクセスを許可します。

telnet コマンドおよび **ssh** コマンドに、VPN プール アドレスを指定してください。

次に、VPN クライアントに、外部インターフェイス（209.165.200.225）上での Telnet の使用を許可する例を示します。ユーザ認証はローカル データベースです。この場合、指定の VPN グループ名とパスワード、およびユーザ名「admin」とパスワード「passw0rd」を持つユーザが、FWSM に接続できます。

```
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)# isakmp policy 1 group 2
hostname(config)# isakmp policy 1 hash sha
hostname(config)# isakmp enable outside
hostname(config)# username admin password passw0rd
hostname(config)# crypto ipsec transform-set vpn esp-3des esp-sha-hmac
hostname(config)# crypto dynamic-map vpn_client 1 set transform-set vpn
hostname(config)# crypto map telnet_tunnel 1 ipsec-isakmp dynamic vpn_client
hostname(config)# crypto map telnet_tunnel interface outside
hostname(config)# crypto map telnet_tunnel client authentication LOCAL
hostname(config)# ip local pool client_pool 10.1.1.1-10.1.1.2
hostname(config)# access-list VPN_SPLIT extended permit ip host 209.165.200.225 host
10.1.1.1
hostname(config)# access-list VPN_SPLIT extended permit ip host 209.165.200.225 host
10.1.1.2
hostname(config)# vpngroup admin address-pool client_pool
hostname(config)# vpngroup admin split-tunnel VPN_SPLIT
hostname(config)# vpngroup admin password $ecure23
hostname(config)# telnet 10.1.1.1 255.255.255.255 outside
hostname(config)# telnet 10.1.1.2 255.255.255.255 outside
hostname(config)# telnet timeout 30
```

サイトツーサイト トンネルの設定

VPN の基本設定（「全トンネルの基本的な設定」を参照）を完了したあと、サイトツーサイト トンネルを設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、両方のピアで使用する共有鍵を設定します。

```
hostname(config)# isakmp key keystring address peer-address
```

ステップ 2　次のコマンドを入力して、トンネルを通過させるトラフィックを特定します。

```
hostname(config)# access-list acl_name [extended] {deny | permit} {protocol} host
fwsm_interface_address dest_address mask
```

宛先アドレスには、FWSM へのアクセスを許可したアドレスを指定します。

アクセス リストの詳細については、「拡張アクセス リストの追加」（p.10-7）を参照してください。

ステップ 3　次のコマンドを入力して、IPSec トンネルを作成します。

```
hostname(config)# crypto map crypto_map_name priority ipsec-isakmp
```

トンネルのアトリビュートはすべて、同じ **crypto map** 名で識別します。

priority には、複数のコマンドを評価する優先順位を指定します。1 つのコマンドでこの **crypto map** 名と **ipsec-isakmp** を指定し、別のコマンドで **ipsec-isakmp dynamic**（VPN クライアント接続用）を指定した場合、プライオリティの値に基づいて最初に評価されるコマンドが決まります。

ステップ 4　次のコマンドを入力して、トンネルに（ステップ 2 で指定した）アクセス リストを割り当てます。

```
hostname(config)# crypto map crypto_map_name priority match address acl_name
```

ステップ 5　次のコマンドを入力して、トンネルを終端するリモート ピアを指定します。

```
hostname(config)# crypto map crypto_map_name priority set peer ip_address
```

ステップ 6　次のコマンドを入力して、トンネルに使用するトランスフォーム セット（「全トンネルの基本的な設定」[p.21-6] で定義したもの）を指定します。

```
hostname(config)# crypto map crypto_map_name priority set transform-set transform_set1
[transform_set2] [...]
```

複数のトランスフォーム セットを使用する場合は、プライオリティの順序（最高のプライオリティが最初）で指定します。最大 6 つのトランスフォーム セットを指定できます。

ステップ 7　次のコマンドを入力して、トンネルを終端するインターフェイスを指定します。

```
hostname(config)# crypto map crypto_map_name interface interface_name
```

1 つのインターフェイスに割り当てることができる **crypto map** 名は 1 つだけです。したがって、サイトツーサイト トンネルと VPN クライアントの両方を同じインターフェイス上で終端する場合には、同じ **crypto map** 名を共有する必要があります。

このコマンドは、必ず他のすべての **crypto map** コマンドを入力したあとで、最後に指定してください。いずれかの **crypto map** コマンドの設定を変更する場合は、このコマンドの **no** 形式を入力して一度削除してから、再度入力してください。

ステップ 8　「Telnet アクセスの許可」（p.21-2）および「SSH アクセスの許可」（p.21-3）を参照して、Telnet アクセスまたは SSH アクセスを許可します。

次に、ピア ルータ（209.165.202.129）に接続しているホストに、外部インターフェイス（209.165.200.225）上での Telnet の使用を許可する例を示します。

```
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)# isakmp policy 1 group 2
hostname(config)# isakmp policy 1 hash sha
hostname(config)# isakmp enable outside
hostname(config)# crypto ipsec transform-set vpn esp-3des esp-sha-hmac
hostname(config)# isakmp key 7mfi02lirotn address 209.165.200.223
hostname(config)# access-list TUNNEL extended permit ip host 209.165.200.225
209.165.201.0 255.255.255.224
hostname(config)# crypto map telnet_tunnel 2 ipsec-isakmp
hostname(config)# crypto map telnet_tunnel 1 match address TUNNEL
hostname(config)# crypto map telnet_tunnel 1 set peer 209.165.202.129
hostname(config)# crypto map telnet_tunnel 1 set transform-set vpn
hostname(config)# crypto map telnet_tunnel interface outside
hostname(config)# telnet 209.165.201.0 255.255.255.224 outside
hostname(config)# telnet timeout 30
```

FWSM との ICMP 送受信の許可

デフォルトの場合、FWSM のインターフェイス（または FWSM を経由。FWSM を*経由*する ICMP の許可については、第 11 章「ネットワーク アクセスの許可または拒否」を参照）上では、ICMP（ping を含む）は許可されていません。ICMP はネットワーク接続をテストする重要なツールですが、同時に FWSM またはネットワークを攻撃する手段にもなります。ICMP は初期テストの実行時に限って許可し、通常の運用中は許可しないことを推奨します。

システム全体で許可される ICMP ルールの最大数については、「ルールの制限」（p.A-6）を参照してください。

ICMP を使用して、FWSM のインターフェイスに到達するアドレスを許可または拒否するには（ホストから FWSM へ、または FWSM からホストへ送信し、ICMP 応答の返信を許可する）、次のコマンドを入力します。

```
hostname(config)# icmp {permit | deny} {host ip_address | ip_address mask | any}
[icmp_type] interface_name
```

icmp_type を指定しないと、すべてのタイプが対象になります。番号または名前で指定できます。ping を制御するには、**echo-reply**（**0**）（FWSM からホストへ）または **echo**（**8**）（ホストから FWSM へ）を指定します。ICMP タイプのリストについては、「ICMP のタイプ」（p.D-17）を参照してください。

アクセス リストと同様に、FWSM はパケットを、各 **icmp** ステートメントに対して順番に照合します。特定のステートメントを最初に設定し、一般的なステートメントをあとに設定してください。最後に暗黙の拒否を設定します。たとえば、最初にすべてのアドレスを許可し、次に特定のアドレスを拒否した場合、そのアドレスは最初のステートメントにすでに一致しているので、許可されることになります。

（注） FWSM からホストへの ping を許可（すなわち、インターフェイスへのエコー応答を許可）し、ホストから FWSM への ping を許可したくない場合には、上記のコマンドを入力する代わりに、ICMP インスペクション エンジンをイネーブルにする方法もあります。第 20 章「アプリケーション レイヤ プロトコル検査の適用」を参照してください。

次に、10.1.1.15 を除くすべてのホストに対して、内部インターフェイスへの ICMP の使用を許可する例を示します。

```
hostname(config)# icmp deny host 10.1.1.15 inside
hostname(config)# icmp permit any inside
```

次に、10.1.1.15 のホストに、内部インターフェイスへの ping だけを許可する例を示します。

```
hostname(config)# icmp permit host 10.1.1.15 inside
```

システム管理者用の AAA

ここでは、システム管理者が認証、コマンド許可、コマンド アカウンティングをイネーブルにする方法について説明します。システム管理者用の AAA を設定する前に、第 14 章「AAA サーバとローカル データベースの設定」にしたがってローカル データベースまたは AAA サーバを設定してください。

ここでは、次の内容について説明します。

- CLI アクセスの認証の設定（p.21-13）
- イネーブル EXEC モード アクセス認証の設定（p.21-14）
- コマンド許可の設定（p.21-15）
- コマンド アカウンティングの設定（p.21-23）
- 現在のログイン ユーザの表示（p.21-24）
- ロックアウトからの回復（p.21-25）

CLI アクセスの認証の設定

CLI 認証をイネーブルにすると、FWSM により、ログイン用のユーザ名とパスワードの入力が要求されます。これらの情報を入力すると、ユーザ EXEC モードにアクセスできます。

イネーブル EXEC モードを開始するには、**enable** コマンドまたは **login** コマンド（ローカル データベースだけを使用する場合）を入力します。

イネーブル認証を設定した場合（「enable コマンドの認証の設定」[p.21-14] を参照）、FWSM により、個人のユーザ名とパスワードの入力が要求されます。イネーブル認証を設定していない場合は、**enable** コマンドの入力時に（**enable password** コマンドで設定した）システム イネーブル パスワードを入力します。ただし、イネーブル認証を使用しない場合は、**enable** コマンドを入力しても、特定ユーザとしてログインできません。個人ユーザ名を保持するには、イネーブル認証を使用してください。

ローカル データベースを使用する認証では、**login** コマンドを使用できます。この場合、ユーザ名が保持されますが、認証を有効にするための設定は不要です。

（注） FWSM で Telnet、SSH、または HTTP ユーザを認証する前に、**telnet** コマンド、**ssh** コマンド、および **http** コマンドを使用して FWSM へのアクセスを設定しておく必要があります。これらのコマンドを使用して、FWSM と通信するための IP アドレスを指定します。

CLI にアクセスするユーザを認証するには、次のコマンドを入力します。

```
hostname(config)# aaa authentication {telnet | ssh | http | serial} console {LOCAL |
server_group [LOCAL]}
```

http キーワードを指定すると、HTTPS を使用して FWSM にアクセスする ASDM クライアントが認証されます。RADIUS または TACACS+ サーバを使用するには、HTTP 認証を設定します。デフォルトでは、このコマンドを設定しなくても、ASDM は認証にローカル データベースを使用します。

認証に TACACS+ または RADIUS サーバ グループを使用する場合、AAA サーバが使用できないときには、フォールバック方式としてローカル データベースを使用するように FWSM を設定できます。**LOCAL**（**LOCAL** はすべて大文字）のあとに、サーバ グループ名を指定してください。FWSM のプロンプトでは使用中の方法を判別できないので、ローカル データベースには 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。

LOCAL だけを入力して、ローカル データベースをメインの認証方法（フォールバックなし）として設定することもできます。

イネーブル EXEC モード アクセス認証の設定

enable コマンドの入力時に、AAA サーバまたはローカル データベースを使用してユーザ認証を行うように FWSM を設定できます。または、**login** コマンドの入力時にローカル データベースを使用してユーザを自動的に認証します。この場合、イネーブル EXEC モードへのアクセスは、ローカル データベース内のユーザ レベルに応じて許可されます。

ここでは、次の内容について説明します。

- enable コマンドの認証の設定（p.21-14）
- login コマンドを使用したユーザ認証（p.21-14）

enable コマンドの認証の設定

enable コマンドの入力時に、ユーザ認証を行うように FWSM を設定できます。**enable** コマンドの認証を行わない場合、**enable** コマンドを入力すると、FWSM により（**enable password** コマンドで設定した）システム イネーブル パスワードの入力を要求されます。この場合、特定ユーザとしてのログインではなくなります。**enable** コマンドに認証を適用すると、ユーザ名は保持されます。この機能は、コマンド許可を実行する場合に役立ちます。各ユーザが入力できるコマンドを制御するには、ユーザ名が重要になるからです。

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。

```
hostname(config)# aaa authentication enable console {LOCAL | server_group [LOCAL]}
```

ユーザは、ユーザ名とパスワードの入力を要求されます。

認証に TACACS+ または RADIUS サーバ グループを使用する場合、AAA サーバが使用できないときには、フォールバック方式としてローカル データベースを使用するように FWSM を設定できます。**LOCAL**（**LOCAL** はすべて大文字）のあとに、サーバ グループ名を指定してください。FWSM のプロンプトでは使用中の方法を判別できないので、ローカル データベースには 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。

LOCAL だけを入力して、ローカル データベースをメインの認証方法（フォールバックなし）として設定することもできます。

login コマンドを使用したユーザ認証

ユーザ EXEC モードで **login** コマンドを使用すると、ローカル データベース内の任意のユーザ名でログインできます。イネーブル認証と異なり、この方法は、マルチコンテキスト モードのシステム実行スペースで使用できます。

この方法では、ユーザは独自のユーザ名とパスワードを使用してイネーブル EXEC モードにアクセスできるので、すべてのユーザにシステム イネーブル パスワードを提供する必要がありません。ログイン時にユーザにイネーブル EXEC モード（およびすべてのコマンド）へのアクセスを許可するには、ユーザのイネーブル レベルを 2（デフォルト値）～ 15 に設定します。ローカル コマンド許可を設定すると、ユーザが入力できるコマンドは、そのユーザのイネーブル レベル以下のコマンドだけに限定されます。詳細については、「ローカル コマンド許可の設定」（p.21-16）を参照してください。

注意　CLI へのアクセスを許可し、イネーブル EXEC モードの使用を許可したくないユーザをローカル データベースに追加する場合には、コマンド許可を設定する必要があります。コマンド許可を使用しない場合、イネーブル レベルが 2 以上（2 はデフォルト値）のユーザは、個人のパスワードを使用して CLI のイネーブル EXEC モード（およびすべてのコマンド）にアクセスできます。別の方法として、RADIUS または TACACS+ 認証を使用できます。または、すべてのローカル ユーザをレベル 1 に設定して、システム イネーブル パスワードを使用してイネーブル EXEC モードにアクセスできるユーザを制御することもできます。

ローカル データベースの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。

```
hostname> login
```

FWSM により、個人のユーザ名とパスワードの入力が要求されます。パスワードを入力すると、ユーザはローカル データベースに指定されているイネーブル レベルになります。

コマンド許可の設定

デフォルトでは、ログイン時にアクセスできるのは最小限のコマンドだけを使用できるユーザ EXEC モードです。**enable** コマンド（またはローカル データベースを使用する場合は **login** コマンド）を入力すると、イネーブル EXEC モードにアクセスでき、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を使用できます。コマンドへのアクセスを制御する場合には、FWSM にコマンド許可を設定し、各ユーザに許可するコマンドを制限します。

ここでは、次の内容について説明します。

- コマンド許可の概要（p.21-15）
- ローカル コマンド許可の設定（p.21-16）
- TACACS+ コマンド許可の設定（p.21-20）

コマンド許可の概要

2 つのコマンド許可方法のいずれかを使用することができます。

- ローカル データベース — FWSM でコマンド イネーブル レベルを設定します。**enable** コマンドで認証された（または **login** コマンドでログインした）ローカル ユーザは、FWSM により、ローカル データベースに定義されているイネーブル レベルに設定されます。ユーザは、自身のイネーブル レベル以下のコマンドにアクセスできます。

  ローカル コマンド許可は、ローカル データベースにユーザを設定しない場合、および CLI 認証またはイネーブル認証を設定しない場合にも使用できます。この場合、**enable** コマンドの入力時にシステム イネーブル パスワードを使用すると、FWSM によってデフォルトのユーザ名が「enable_15」に設定され、レベルは 15 となります。各レベルで、イネーブル パスワードを作成できます。**enable** *n*（2 ～ 15）と入力すると、FWSM によってレベルが *n* に設定されます。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した場合に限り、使用されます（「ローカル コマンド許可の設定」を参照）。**enable** コマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

- TACACS+ サーバ — TACACS+ サーバ上で、CLI アクセスの認証後にユーザまたはグループに許可するコマンドを設定します。ユーザが CLI から入力したコマンドはすべて、TACACS+ サーバによって検証されます。

セキュリティ コンテキストとコマンド許可

複数のセキュリティ コンテキストでコマンド許可を実装する際、次の点を考慮する必要があります。

- AAA 設定はコンテキスト間で共有するのではなく、コンテキストごとの個別設定となります。

  コマンド許可の設定時に、各セキュリティ コンテキストを個別に設定する必要があります。これにより、セキュリティ コンテキストごとに異なるコマンド許可を実行できるようになります。

  セキュリティ コンテキストの切り替えの際、ログイン時に指定されたユーザ名に許可されるコマンドが、新しいコンテキスト セッションへのログイン時には異なる場合があり、新しいコンテキストではそのコマンド許可がまったく設定されていない場合があることを管理者は理解していてください。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ことを理解していないと、混乱を招くもととなります。この動作は、次の点によってより複雑になります。

- **changeto** コマンドで開始される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ていたユーザ名とは関係なく、管理者 ID として常にデフォルト ユーザ名「enable_15」を使用します。enable_15 ユーザに対して共通の許可が設定されていない場合や、この enable_15 ユーザの許可と前のコンテキスト セッションのユーザでの許可とが異なる場合、混乱を生じることがあります。

  この動作は、コマンド アカウンティングにも影響を及ぼします。コマンド アカウンティングは、特定の管理者が発行した各コマンドを正確に対応付けられる場合のみ有効に使用できます。**changeto** コマンドの使用を許可された管理者は他のコンテキストでユーザ名 enable_15 を使用することができるため、コマンド アカウンティング記録を見ても、誰がユーザ名 enable_15 でログインしたのかを容易に特定できないことがあります。コンテキストごとに異なるアカウンティング サーバを使用している場合、ユーザ名 enable_15 の使用者を追跡するには、複数のサーバのデータを照らし合わせる必要があります。

  コマンド許可の設定時には、次の点を考慮してください。

  - **changeto** コマンドの効果的な使用を許可された管理者は、他の各コンテキストでもユーザ enable_15 に許可されたコマンドをすべて使用することができます。
  - コンテキストごとに異なるコマンドを許可する場合、**changeto** コマンドの使用を許可された管理者が使用できないコマンドは、ユーザ名 enable_15 も各コンテキストでこれらのコマンドを使用できないようにします。

  セキュリティ コンテキストを切り替えるとき、管理者はイネーブル EXEC モードを終了して **enable** コマンドを再度入力することにより、必要なユーザ名を使用できるようになります。

(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ていないため、システム実行スペースではコマンド許可は利用できません。

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すると、各ユーザにイネーブル レベルが設定されます。ユーザは、各自のイネーブル レベル以下である任意のコマンドを入力できます。FWSM では、各コマンドに 16 のイネーブル レベル（0 ～ 15）のいずれかを指定できます。デフォルトでは、各コマンドはイネーブル レベル 0 または 15 のどちらかに割り当てられます。

ここでは、次の内容について説明します。

- ローカル コマンド許可の前提条件（p.21-17）
- デフォルトのコマンド イネーブル レベル（p.21-17）
- コマンド イネーブル レベルの指定および許可のイネーブル化（p.21-17）
- コマンド イネーブル レベルの表示（p.21-19）

ローカル コマンド許可の前提条件

コマンド許可の設定の一部として、次の作業を完了してください。

- **enable** 認証を設定します（「イネーブル EXEC モード アクセス認証の設定」（p.21-14）を参照）。

  login コマンド（認証した **enable** コマンドと同等）を使用する場合には、設定は不要です。ただし、イネーブル認証に比べて安全性が低いので、この方法は推奨しません。

  CLI 認証の設定もできますが、必須ではありません。
- ローカル データベース内の各ユーザに、0 ～ 15 のイネーブル レベルを設定します。

デフォルトのコマンド イネーブル レベル

デフォルトでは、次のコマンドにイネーブル レベル 0 が割り当てられます。他のコマンドはすべて、イネーブル レベル 15 になります。

- **show checksum**
- **show curpriv**
- **enable**（イネーブル モード）
- **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 コマンドのいずれかを 15 より低いレベルに変更する場合は、必ず、**configure** コマンドを同じレベルに変更してください。変更しない場合、ユーザはコンフィギュレーション モードを開始できません。

すべてのイネーブル レベルを表示する手順は、「コマンド イネーブル レベルの表示」（p.21-19）を参照してください。

コマンド イネーブル レベルの指定および許可のイネーブル化

コマンドに新しいイネーブル レベルを指定し、許可をイネーブルにする手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、コマンドにイネーブル レベルを指定します。

```
hostname(config)# privilege [show | clear | cmd] level level [mode {enable | cmd}]
command command
```

レベルを変更するコマンドごとに、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の詳細は、次のとおりです。

- **show** | **clear** | **cmd** — コマンドの show、clear、または configure 形式のレベルだけを指定できる任意のキーワードです。コマンドの configure 形式は通常、コマンドの原型（**show** または **clear** のプレフィクスが付いていない状態）または **no** 形式のいずれかで、設定の変更を伴います。これらのキーワードをいずれも使用しない場合、コマンドのすべての形式が対象になります。
- **level** *level* — 0 ～ 15 のレベルを指定します。

- **mode**{**enable** | **configure**} ― コマンドをユーザ EXEC/ イネーブル EXEC モードとコンフィギュレーション モードの両方で入力できるが、モードによってコマンドの動作が異なる場合は、モードごとにイネーブル レベルを個別に設定できます。
  - **enable** ― ユーザ EXEC モードとイネーブル EXEC モードの両方が対象です。
  - **configure** ― **configure terminal** コマンドを使用してアクセスするコンフィギュレーション モードが対象です。
- **command** *command* ― 設定するコマンドを指定します。メイン コマンドのイネーブル レベルだけを設定できます。たとえば、すべての **aaa** コマンドが対象となるレベルは設定できますが、**aaa authentication** コマンドおよび **aaa authorization** コマンドのレベルを個別に設定することはできません。

  また、メイン コマンドとは別にサブコマンドのイネーブル レベルを設定することもできません。たとえば、**context** コマンドのレベルは設定できますが、**context** コマンドの設定を継承する **allocate-interface** コマンドのレベルは設定できません。

ステップ 2　次のコマンドを入力して、ローカル コマンド許可をイネーブルにします。

```
hostname(config)# aaa authorization command LOCAL
```

コマンドのイネーブル レベルを設定しても、このコマンドを使用してコマンド許可をイネーブルにしないと、コマンド許可は実行されません。

次に、**filter** コマンドの形式を示します。

- **filter**（**configure** オプションの対象）
- **show running-config filter**
- **clear configure filter**

各形式に個別のイネーブル レベルを設定するか、オプションを指定しないで全形式に同じイネーブル レベルを設定します。次に、各形式を個別に設定する例を示します。

```
hostname(config)# privilege show level 5 command filter
hostname(config)# privilege clear level 10 command filter
hostname(config)# privilege cmd level 10 command filter
```

次に、すべての filter コマンドに同じレベルを設定する例を示します。

```
hostname(config)# privilege level 5 command filter
```

show privilege コマンドを入力すると、各形式の設定が個別に表示されます。

次に、**mode** キーワードを使用する例を示します。**enable** コマンドはユーザ EXEC モードで入力する必要がありますが、**enable password** コマンドはコンフィギュレーション モードで入力するので、最上位のイネーブル レベルが必要になります。

```
hostname(config)# privilege cmd level 0 mode enable command enable
hostname(config)# privilege cmd level 15 mode cmd command enable
hostname(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。

```
hostname(config)# privilege show level 5 mode cmd command configure
hostname(config)# privilege clear level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode enable command configure
```

（注）　最後の行は、**configure terminal** コマンドのレベル設定です。

コマンド イネーブル レベルの表示

コマンドのイネーブル レベルを表示するには、次のコマンドを使用します。

- すべてのコマンドのレベルを表示するには、次のコマンドを入力します。

  hostname(config)# **show running-config all privilege all**

- 特定レベルのコマンドを表示するには、次のコマンドを入力します。

  hostname(config)# **show running-config privilege level** *level*

  level は、0 ～ 15 の整数です。

- 特定コマンドのレベルを表示するには、次のコマンドを入力します。

  hostname(config)# **show running-config privilege command** *command*

次に、**show running-config all privilege all** コマンドの出力例を示します。各 CLI コマンドの現在のイネーブル レベル設定状況が表示されます。

```
hostname(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
....
```

次に、イネーブル レベル 10 が設定されているコマンドを表示する例を示します。

```
hostname(config)# show running-config privilege level 10
privilege show level 10 command aaa
```

次に、**access-list** コマンドのレベル設定を表示する例を示します。

```
hostname(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+ コマンド許可の設定

TACACS+ コマンド許可をイネーブルにすると、ユーザが CLI にコマンドを入力した時点で FWSM から TACACS+ サーバにコマンドとユーザ名が送信され、そのコマンドが許可されているかどうかが判別されます。

TACACS+ サーバによるコマンド許可を設定する場合は、設定が正しいことを確認するまで設定を保存しないでください。設定ミスによってロックアウトされた場合、通常は FWSM を再起動することによってアクセスを回復できます。再起動しても、ロックアウトされる場合には、「ロックアウトからの回復」（p.21-25）を参照してください。

TACACS+ システムが確実に安定し、信頼性があることを確認してください。必要レベルの信頼性を確保するには通常、完全冗長設定の TACACS+ サーバと、FWSM への完全冗長接続が必要になります。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続したサーバと、インターフェイス 2 に接続した別のサーバを設定します。TACACS+ サーバが使用できない場合に備えて、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、ローカル ユーザおよびコマンド イネーブル レベルを設定する必要があります（「コマンド許可の設定」[p.21-15] を参照）。

ここでは、次の内容について説明します。

- TACACS+ コマンド許可の前提条件（p.21-20）
- TACACS+ サーバ上でのコマンドの設定（p.21-20）
- TACACS+ コマンド許可のイネーブル化（p.21-23）

TACACS+ コマンド許可の前提条件

コマンド許可の設定の一部として、次の作業を完了してください。

- CLI 認証を設定します（「ローカル コマンド許可の設定」[p.21-16] を参照）。
- **enable** 認証を設定します（「イネーブル EXEC モード アクセス認証の設定」[p.21-14] を参照）。

TACACS+ サーバ上でのコマンドの設定

グループまたは個人ユーザの共有プロファイル コンポーネントとして、Cisco Secure Access Control Server（ACS）上でコマンドを設定できます。サードパーティ製の 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サーバのマニュアルを参照してください。

Cisco Secure ACS V.3.1 でコマンドを設定する場合は、次の注意事項を参照してください。これらの事項のほとんどは、サードパーティ製のサーバにも適用されます。

- FWSM は、許可するコマンドを「shell」コマンドとして送信するので、TACACS+ サーバ上でコマンドを設定する場合には shell コマンドとして設定してください。

（注） CiscoSecure ACS には、「pix-shell」と呼ばれるコマンド タイプが含まれていることがあります。FWSM でのコマンド許可には、このタイプを使用しないでください。

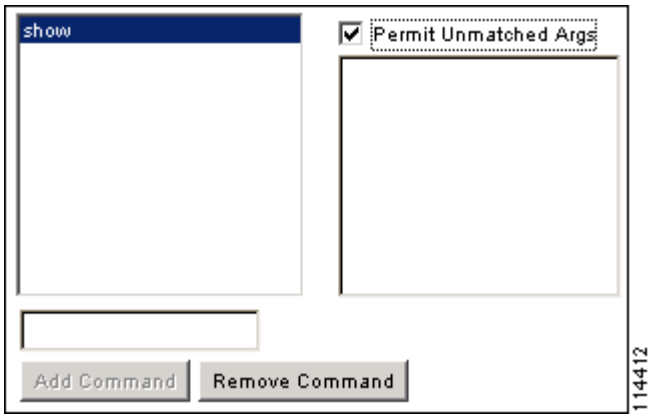
- コマンドの最初の語が、メイン コマンドであると判断されます。その他の文字はすべて引数としてみなされるので、**permit** または **deny** のプレフィクスが必要です。

  たとえば、**show running-configuration aaa-server** コマンドを許可するには、コマンド ボックスに **show running-configuration** を追加し、引数ボックスに **permit** ***aaa-server*** を入力します。

- **Permit Unmatched Args** チェックボックスを選択すると、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。

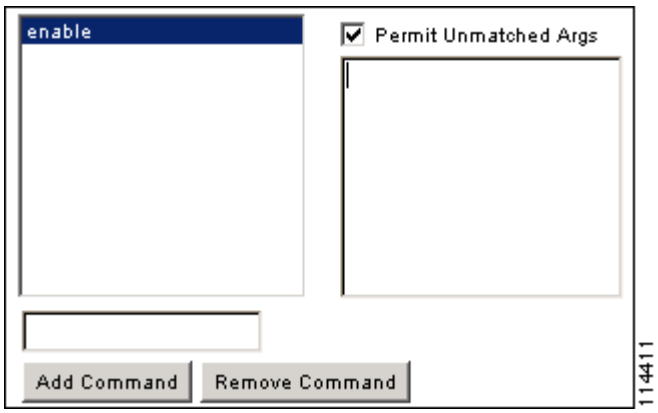
  たとえば、**show** コマンドだけを設定すると、すべての **show** コマンドが許可されます。コマンドのすべての変形（短縮形および CLI の使用方法を示す **?** など）を考慮する必要がないので、この方法を使用することを推奨します（図 21-1 を参照）。

図 21-1　すべての関連コマンドの許可



- **enable** または **help** のように単一語のコマンドの場合には、コマンドの引数がなくても、「Permit Unmatched Args」を選択する*必要があります*（図 21-2 を参照）。

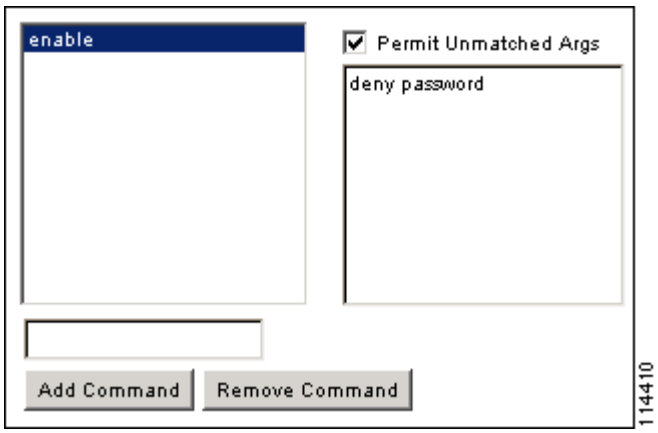
図 21-2　単一ワードのコマンドの許可



- 一部の引数を許可しない場合には、**deny** のプレフィクスを付けて引数を入力します。

  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 ボックスに **enable** を入力し、引数ボックスに **deny password** を入力します。**enable** だけが許可されるように、必ず、「Permit Unmatched Args」チェックボックスを選択してください（図 21-3 を参照）。

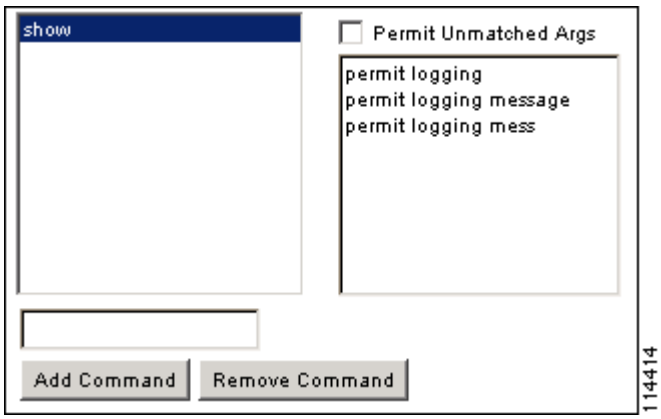
図 21-3　引数の拒否



- コマンドラインにコマンドの短縮形を入力すると、FWSM はプレフィクスとメイン コマンドをフル テキストに拡張しますが、追加の引数は入力されたとおりに TACACS+ サーバに送信されます。

  たとえば、**sh log** と入力すると、FWSM から TACACS+ サーバにコマンドの完全形である **show logging** が送信されます。ただし、**sh log mess** と入力した場合には、FWSM から TACACS+ サーバに **show logging mess** が送信され、完全形の **show logging message** は送信されません。短縮形を識別できるように、同じ引数について複数のスペルを設定できます（図 21-4 を参照）。

図 21-4　短縮形の指定



- 次の基本コマンドは、すべてのユーザに対して許可することを推奨します。
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**
  - **logout**
  - **pager**
  - **show pager**

- **clear pager**
- **quit**
- **show version**

TACACS+ コマンド許可のイネーブル化

TACACS+ コマンド許可をイネーブルにするには、設定者が TACACS+ サーバ上に定義されているユーザとして FWSM にログインし、FWSM の設定を行うために必要なコマンド許可を得ている必要があります。たとえば、すべてのコマンドが許可されている admin ユーザとしてログインします。そうでない場合、意図せずにロックアウトされることがあります。

TACACS+ サーバを使用してコマンド許可を実行するには、次のコマンドを入力します。

```
hostname(config)# aaa authorization command tacacs+_server_group [LOCAL]
```

TACACS+ サーバが使用できない場合、フォールバック方式としてローカル データベースを使用するように FWSM 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、**LOCAL**（**LOCAL** はすべて大文字）のあとに、サーバ グループ名を指定します。FWSM のプロンプトでは使用中の方法を判別できないので、ローカル データベースには 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。ユーザがローカル データベースに設定され（「コマンド許可の設定」[p.21-15] を参照）、コマンド イネーブル レベルが設定されていることを確認してください（「ローカル コマンド許可の設定」[p.21-16] を参照）。

コマンド アカウンティングの設定

管理セッション中にシステム管理者が発行したコマンドのアカウンティング　レコードが TACACS+ サーバに送信されるように FWSM を設定することができます。最低のイネーブル レベルを指定することにより、FWSM の対象となるコマンドを制限できます。最低のイネーブル レベル未満のコマンドは FWSM の対象となりません。

コマンド アカウンティングをイネーブルにするには、次のように **aaa accounting command** コマンドを使用します。

```
hostname(config)# aaa accounting command [privilege level] server-tag
```

level は最低のイネーブル レベル、*server-tag* は FWSM がコマンド アカウンティング メッセージを送信する先の TACACS+ サーバ グループの名前です。TACACS+ サーバ グループ設定をあらかじめ行っておく必要があります。AAA サーバ グループの詳細については、「AAA サーバ グループおよびサーバの識別」（p.14-13）を参照してください。

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。

```
hostname# show curpriv
```

次に、**show curpriv** コマンドの出力例を示します。各フィールドの説明は、以下を参照してください。

```
hostname# show curpriv
Username : admin
Current privilege level : 15
Current Mode/s : P_PRIV
```

表 21-1 に、**show curpriv** コマンドの出力の説明を示します。

表 21-1　show curpriv の出力の説明

フィールド	説明
Username	ユーザ名です。デフォルト ユーザとしてログインしている場合、名前は enable_1（ユーザ EXEC）または enable_15（イネーブル EXEC）になります。
Current privilege level	0 ～ 15 のレベルです。ローカル コマンド許可を設定し、コマンドに中間のイネーブル レベルを割り当てた場合をのぞき、使用できるレベルはレベル 0 およびレベル 15 だけです。
Current Mode/s	アクセス モードが表示されます。 • P_UNPR ― ユーザ EXEC モード（レベル 0 および 1） • P_PRIV ― イネーブル 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

ロックアウトからの回復

一部の状況では、コマンド許可または CLI 認証をイネーブルにすると、FWSM の CLI からロックアウトされることがあります。通常は、FWSM を再起動することによって回復できます。ただし、設定がすでに保存されている場合には、再びロックアウトされる可能性があります。表 21-2 に、一般的なロックアウトの条件および回復方法を示します。

表 21-2　CLI 認証およびコマンド許可のロックアウト

機能	ロックアウトの条件	説明	対処方法：シングル モード	対処方法：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されていない。	ローカル データベースにユーザが設定されていない場合、ログインできず、ユーザを追加できません。	ログインし、パスワードと **aaa** コマンドを再設定します。	スイッチから FWSM にセッションを開始します。システム実行スペースからコンテキストに移動し、ユーザを追加します。
TACACS+ コマンド許可 TACACS+ CLI 認証 RADIUS CLI 認証	サーバがダウンしたか、または到達不能で、かつフォールバック方式が設定されていない。	サーバが到達不能な場合、ログインまたはコマンド入力ができません。	**1.** ログインし、パスワードと aaa コマンドを再設定します。 **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、フォールバック方式としてローカル データベースを設定します。	**1.** FWSM 上のネットワーク設定が不正であるためにサーバに到達できない場合には、スイッチから FWSM にセッションを開始します。システム実行スペースからコンテキストに移動し、ネットワークを再設定します。 **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、フォールバック方式としてローカル データベースを設定します。
TACACS+ コマンド許可	十分なレベルを持たないユーザとして、または存在しないユーザとしてログインした場合	コマンド許可をイネーブルにすると、ユーザはそれ以上、コマンドを入力できません。	TACACS+ サーバのユーザアカウントを修正します。 TACACS+ サーバにアクセスできず、FWSM をただち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、パスワードおよび **aaa** コマンドを再設定します。	スイッチから FWSM にセッションを開始します。システム実行スペースからコンテキストに移動し、設定の変更を完了します。TACACS+ の設定を修正するまで、コマンド許可をディセーブルにしておくこともできます。
ローカル コマンド許可	十分なレベルを持たないユーザとしてログインした場合	コマンド許可をイネーブルにすると、ユーザはそれ以上、コマンドを入力できません。	ログインし、パスワードと **aaa** コマンドを再設定します。	スイッチから FWSM にセッションを開始します。システム実行スペースからコンテキストに移動し、ユーザ レベルを変更します。

ソフトウェア、ライセンス、および設定の管理

この章では、FTP、TFTP、HTTP、または HTTPS サーバから FWSM に新しいソフトウェアをインストールする方法について説明します。アプリケーション ソフトウェア、メンテナンス ソフトウェア、および ASDM 管理ソフトウェアはアップグレード可能です。自動アップデート サポートをイネーブルにすることもできます。この章で説明する内容は次のとおりです。

- ライセンスの管理（p.22-2）
- アプリケーションまたは ASDM ソフトウェアのインストール（p.22-4）
- フェールオーバー ペアのアップグレード（p.22-11）
- メンテナンス ソフトウェアのインストール（p.22-14）
- コンフィギュレーション ファイルのダウンロードおよびバックアップ（p.22-17）
- 自動アップデート サポートの設定（p.22-21）

ライセンスの管理

ソフトウェアをインストールすると、オリジナル イメージから既存のアクティベーション キーが取り出され、FWSM ファイル システムのファイルに保存されます。ここでは、次の内容について説明します。

- アクティベーション キーの取得（p.22-2）
- 新しいアクティベーション キーの入力（p.22-3）

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、製品許可キーが必要です。これは、シスコの代理店から購入できます。製品許可キーの取得後、アクティベーション キーを取得するための登録を Web 上で行います。手順は次のとおりです。

ステップ 1　次のコマンドを入力して、FWSM のシリアル番号を取得します。

```
hostname> show version | include Number
```

コマンドの一部としてパイプ記号（|）を入力します。

ステップ 2　Web ブラウザを次のいずれかの Web サイトに接続します（URL は大文字と小文字が区別されます）。

Cisco.com に登録されている場合、次の Web サイトを使用してください。

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

Cisco.com に登録されていない場合、次の Web サイトを使用してください。

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

ステップ 3　プロンプトが表示されたら、次の情報を入力します。

- 製品許可キー
- FWSM 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、入力した電子メール アドレスに送信されます。

新しいアクティベーション キーの入力

アクティベーション キーを入力するには、次のコマンドを入力します。

```
hostname(config)# activation-key key
```

key は 4 つの要素からなる 16 進数の文字列です。各要素の間にスペースを 1 つずつ入れます。有効な形式のキーは、次のとおりです。

0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e

先行する 0x は、省略してもかまいません。値はすべて 16 進数とみなされます。

すでにマルチコンテキスト モードになっている場合は、システム実行スペースでこのコマンドを入力します。

(注) アクティベーション キーはコンフィギュレーション ファイルに保管されません。キーは、装置のシリアル番号と対応付けられています。

実行中のイメージに変更を反映するには、新しいアクティベーション キーの入力後に FWSM を再起動する必要があります。

次に、FWSM でアクティベーション キーを変更する例を示します。

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

アプリケーションまたは ASDM ソフトウェアのインストール

ここでは、次の内容について説明します。

- インストレーションの概要（p.22-4）
- FWSM CLI からのアプリケーション ソフトウェアのインストール（p.22-4）
- メンテナンス パーティションからのアプリケーション ソフトウェアのインストール（p.22-6）
- FWSM CLI からの ASDM のインストール（p.22-10）

インストレーションの概要

アプリケーション ソフトウェアは、次のいずれかの方法でアップグレードできます。

- FWSMCLI から現在のアプリケーション パーティションへのインストール

  この方法の利点は、メンテナンス パーティションを起動する必要がないことです。通常どおりにログインし、新しいソフトウェアをコピーできます。

  TFTP、FTP、HTTP、または HTTPS サーバからのダウンロードがサポートされます。

  ソフトウェアを、他方のアプリケーション パーティションにコピーすることはできません。ただし、旧バージョンのソフトウェアをバックアップとして現在のパーティションに保存する場合には、他のパーティションにコピーするほうが便利なことがあります。

  その場合には、ネットワーク アクセスにより運用設定を行う必要があります。マルチコンテキスト モードでは、admin コンテキスト経由でネットワークに接続する必要があります。

- メンテナンス パーティションから任意のアプリケーション パーティションへのインストール

  この方法の利点は、両方のアプリケーション パーティションにソフトウェアをコピーできることです。運用設定を行う必要はありません。メンテナンス パーティションのルーティング パラメータの一部を設定するだけで、VLAN 1 上のサーバに到達できます。

  欠点としては、メンテナンス パーティションを起動しなければならない点があります。アプリケーション パーティションを運用している場合には、不便なことがあります。

  この方法でサポートされるのは、FTP サーバからのダウンロードだけです。

ASDM をアップグレードする場合、FWSMCLI から現在のアプリケーション パーティションへのインストールのみが可能です。

アプリケーション パーティションおよびメンテナンス パーティションの詳細については、「Firewall Services Module ブート パーティションの管理」（p.2-14）を参照してください。

FWSM CLI からのアプリケーション ソフトウェアのインストール

通常の運用中に FWSM にログインし、TFTP、FTP、HTTP、または HTTPS サーバからアプリケーション ソフトウェアを現在のアプリケーション パーティションにコピーすることができます。

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で作業する必要があります。

FTP、TFTP、または HTTP(S) サーバから現在のアプリケーション パーティションにソフトウェアをアップグレードする手順は、次のとおりです。

ステップ 1　選択した FTP、TFTP、または HTTP(S) サーバへのアクセスを確認するため、次のコマンドを入力します。

```
hostname# ping ip_address
```

ステップ 2 アプリケーション ソフトウェアをコピーするには、次のコマンドを使用して、適切なダウンロード サーバを指定します。

- TFTP サーバからコピーするには、次のコマンドを入力します。

  ```
  hostname# copy tftp://server[/path]/filename flash:
  ```

  flash キーワードは、FWSM のアプリケーション パーティションを示します。**flash** パーティションにコピーできるのは、イメージと ASDM ソフトウェアのみです。コンフィギュレーション ファイルは **disk** パーティションにコピーされます。

- FTP サーバからコピーするには、次のコマンドを入力します。

  ```
  hostname# copy ftp://[user[:password]@]server[/path]/filename flash:
  ```

- HTTP または HTTPS サーバからコピーするには、次のコマンドを入力します。

  ```
  hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename flash:
  ```

- セキュア コピーを使用するには、SSH をイネーブルにしてから、次のコマンドを入力します。

  ```
  hostname# ssh scopy enable
  ```

  次に、Linux クライアントから次のコマンドを入力します。

  ```
  scp -v -pw password filename username@fwsm_address
  ```

  -v は詳細の意味です。**-pw** を指定しない場合、パスワードの入力を求められます。

次に、FTP サーバからアプリケーション ソフトウェアをコピーする例を示します。

```
hostname# copy ftp://10.94.146.80/tftpboot/bnair/cdisk flash:

copying ftp://10.94.146.80/tftpboot/bnair/cdisk to flash:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 6128128 bytes.
Erasing current image.This may take some time..
Writing 6127616 bytes of image.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image installed.
```

ステップ 3　新しいソフトウェアを実行するには、システムをリロードする必要があります。フェールオーバーのペアがない場合、次のコマンドを入力します。

```
hostname# reload
Proceed with reload? [confirm]
```

「Proceed with reload?」のプロンプトで、**Enter** を押してコマンドを確定します。

```
Rebooting...
```

フェールオーバーのペアがある場合は、「フェールオーバー ペアのアップグレード」（p.22-11）を参照してください。

メンテナンス パーティションからのアプリケーション ソフトウェアのインストール

メンテナンス パーティションにログインすると、アプリケーション ソフトウェアをいずれかのアプリケーション パーティション（cf:4 または cf:5）にインストールできます。

（注） FWSM のメンテナンス パーティションで使用できるのは、スイッチ上の VLAN 1 だけです。FWSM は、VLAN 1 での 802.1Q タギングをサポートしていません。

FWSM では、メンテナンス ソフトウェア Release 2.1(2) 以降を使用することが必要です。アップグレードの詳細については、「メンテナンス ソフトウェアのインストール」（p.22-14）を参照してください。

（注） アクティブ / スタンバイのフェールオーバー ペアを使用している場合、まずスタンバイ ユニットでこの手順を実行し、スタンバイ ユニットのリロード後に、アクティブ ユニットのシステム実行スペースで **no failover active** コマンドを使用してアクティブ ユニットをスタンバイ ユニットに切り替えてから、アクティブ ユニットをアップグレードします。

アクティブ / アクティブのフェールオーバーの場合、プライマリ ユニットのシステム実行スペースで **failover active** コマンドを入力して、プライマリ ユニットで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。その後、セカンダリ ユニットでもこの手順を実行します。セカンダリ ユニットのアップグレード手順が完了したら、プライマリ ユニットのシステム実行スペースで **no failover active** コマンドを使用して、セカンダリ ユニットで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。その後、アクティブ ユニットをアップグレードします。

FWSM では、2.3 から 3.1 へのフェールオーバー ペアのアップグレードを行うには、システムを停止させる必要があります。停止させずにアップグレードが行えるのは、リリース 3.1 以降のみです。2.x からのアップグレードの詳細については、『*Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module to Release 3.1*』を参照してください。

メンテナンス パーティションにログインし、FTP サーバからアプリケーション ソフトウェアをインストールする手順は、次のとおりです。

ステップ 1　アプリケーション パーティションには、それぞれ独自のスタートアップ コンフィギュレーションがあるため、必要に応じて、バックアップ アプリケーション パーティションにコピーするために、現在の設定を利用できるようにする必要があります。利用可能な TFTP、FTP、または HTTP(S) サーバにコピーするか、**show running-config** コマンドを入力して、端末から設定をカット＆ペーストします。

ステップ 2　必要に応じて、次のコマンドを入力して、FWSM のセッションを終了します。

```
hostname# exit

Logoff

[Connection to 127.0.0.31 closed by foreign host]
Router#
```

コンフィギュレーション モードで作業している場合、**exit** コマンドを複数回入力しなければならないことがあります。

ステップ 3　現在のブート パーティションを表示するには、OS に応じたコマンドを入力します。新しいデフォルト ブート パーティションを設定する際、現在のブート パーティションをメモしておいてください。

- Cisco IOS ソフトウェア

  ```
  Router# show boot device [mod_num]
  ```

  次に例を示します。

  ```
  Router# show boot device
  [mod:1 ]:
  [mod:2 ]:
  [mod:3 ]:
  [mod:4 ]: cf:4
  [mod:5 ]: cf:4
  [mod:6 ]:
  [mod:7 ]: cf:4
  [mod:8 ]:
  [mod:9 ]:
  ```

- Catalyst OS ソフトウェア

  ```
  Console> (enable) show boot device mod_num
  ```

  次に例を示します。

  ```
  Console> (enable) show boot device 4
  Device BOOT variable = cf:4
  ```

ステップ 4　OS に応じて、次のコマンドを入力して、デフォルト ブート パーティションをバックアップに変更します。

- Cisco IOS ソフトウェア

  ```
  Router(config)# boot device module mod_num cf:{4 | 5}
  ```

- Catalyst OS ソフトウェア

  ```
  Console> (enable) set boot device cf:{4 | 5} mod_num
  ```

ステップ 5 OS に応じて、スイッチのプロンプトで次のコマンドを入力して、FWSM のメンテナンス パーティションを起動します。

- Cisco IOS ソフトウェアの場合、次のコマンドを入力します。

  ```
  Router# hw-module module mod_num reset cf:1
  ```

- Catalyst OS ソフトウェアの場合、次のコマンドを入力します。

  ```
  Console> (enable) reset mod_num cf:1
  ```

ステップ 6 OS に応じて、次のコマンドを入力して、FWSM へのセッションを開始します。

- Cisco IOS ソフトウェア

  ```
  Router# session slot number processor 1
  ```

- Catalyst OS ソフトウェア

  ```
  Console> (enable) session module_number
  ```

ステップ 7 次のコマンドを入力して、FWSM のメンテナンス パーティションにルートとしてログインします。

```
Login: root
Password:
```

デフォルトのパスワードは、**cisco** です。

ステップ 8 ネットワーク パラメータを設定する手順は、次のとおりです。

a. 次のコマンドを入力して、メンテナンス パーティションに IP アドレスを割り当てます。

```
root@localhost# ip address ip _address netmask
```

これは、メンテナンス パーティションで使用できる唯一の VLAN である VLAN 1 のアドレスです。

b. 次のコマンドを入力して、メンテナンス パーティションにデフォルト ゲートウェイを割り当てます。

```
root@localhost# ip gateway ip_address
```

c. （任意）FTP サーバに ping を実行して接続していることを確認する場合は、次のコマンドを入力します。

```
root@localhost# ping ftp_address
```

ステップ 9 次のコマンドを入力して、FTP サーバからアプリケーション ソフトウェアをダウンロードします。

```
root@localhost# upgrade ftp://[user[:password]@]server[/path]/filename cf:{4 | 5}
```

cf:4 および **cf:5** は、FWSM 上のアプリケーション パーティションです。新しいソフトウェアをバックアップ パーティションにインストールします。

画面に表示されるプロンプトに従って、アップグレードします。

ステップ 10 次のコマンドを入力して、メンテナンス パーティションからログアウトします。

```
root@localhost# logout
```

ステップ 11 OS に応じたコマンドを入力して、バックアップ アプリケーション パーティション（ステップ 4 でデフォルトとして設定した）で FWSM を再起動します。

- Cisco IOS ソフトウェアの場合、次のコマンドを入力します。

  `Router# hw-module module mod_num reset`

- Catalyst OS ソフトウェアの場合、次のコマンドを入力します。

  `Console> (enable) reset mod_num`

ステップ 12 OS に応じて、次のコマンドを入力して、FWSM へのセッションを開始します。

- Cisco IOS ソフトウェア

  `Router# session slot number processor 1`

- Catalyst OS ソフトウェア

  `Console> (enable) session module_number`

デフォルトでは、FWSM にログインするためのパスワードは **cisco** です（**password** コマンドで変更可能）。このパーティションにスタートアップ コンフィギュレーションがない場合、デフォルト パスワードが使用されます。

ステップ 13 次のコマンドを入力して、イネーブル EXEC モードを開始します。

```
hostname> enable
```

デフォルト パスワードは空白です（**enable password** コマンドで変更可能）。このパーティションにスタートアップ コンフィギュレーションが存在しない場合、デフォルト パスワードが使用されます。

ステップ 14 アプリケーション パーティションには、それぞれ独自のスタートアップ コンフィギュレーションがあるため、場合によっては、現在の設定をアプリケーション パーティションにコピーする必要あります。このパーティションで古い設定が動作している場合、実行コンフィギュレーションへのコピーを行う前に古い設定を消去することが必要な場合があります。実行コンフィギュレーションを消去するには、**clear configure all** コマンドを入力します。設定を実行コンフィギュレーションにコピーするには、次のいずれかの方法を使用します。

- コマンド ラインに設定をペーストします。
- TFTP サーバからコピーするには、次のコマンドを入力します。

  `hostname# copy tftp://server[/path]/filename running-config`

- FTP サーバからコピーするには、次のコマンドを入力します。

  `hostname# copy ftp://[user[:password]@]server[/path]/filename running-config`

- HTTP または HTTPS サーバからコピーするには、次のコマンドを入力します。

  `hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename running-config`

- ローカル フラッシュ メモリからコピーするには、次のコマンドを入力します。

  `hostname# copy disk:[path/]filename running-config`

ステップ 15 次のコマンドを使用して、実行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。

```
hostname# write memory
```

ステップ 16 デフォルトのコンテキスト モードはシングル モードなので、マルチ コンテキスト モードで作業している場合は、次のコマンドを使用して、新しいアプリケーション パーティションでモードをマルチに設定します。

```
hostname# configuration terminal
hostname(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
```

確定すると、FWSM のリロードが開始されます。

FWSM CLI からの ASDM のインストール

通常の運用中に FWSM にログインし、TFTP、FTP、HTTP、または HTTPS サーバから ASDM ソフトウェアを現在のアプリケーション パーティションにコピーすることができます。

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で作業する必要があります。

接続状態を確認するには、**ping** コマンドを使用します。

ASDM ソフトウェアをコピーするには、次のコマンドを使用して、適切なダウンロード サーバを指定します。

- TFTP サーバからコピーするには、次のコマンドを入力します。

  ```
  hostname# copy tftp://server[/path]/filename flash:asdm
  ```

  flash キーワードは、FWSM のアプリケーション パーティションを示します。**flash** パーティションにコピーできるのは、イメージと ASDM ソフトウェアのみです。コンフィギュレーション ファイルは **disk** パーティションにコピーされます。
- FTP サーバからコピーするには、次のコマンドを入力します。

  ```
  hostname# copy ftp://[user[:password]@]server[/path]/filename flash:asdm
  ```

- HTTP または HTTPS サーバからコピーするには、次のコマンドを入力します。

  ```
  hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename flash:asdm
  ```

- セキュア コピーを使用するには、SSH をイネーブルにしてから、次のコマンドを入力します。

  ```
  hostname# ssh scopy enable
  ```

  そして、Linux クライアントから次のコマンドを入力します。

  ```
  scp -v -pw password filename username@fwsm_address
  ```

  -v は詳細の意味です。**-pw** を指定しない場合、パスワードの入力を求められます。

次に、TFTP サーバから ASDM をコピーする例を示します。

```
hostname# copy tftp://209.165.200.226/cisco/asdm.bin flash:asdm
```

次に、HTTPS サーバから ASDM をコピーする例を示します。

```
hostname# copy http://admin:letmein@209.165.200.228/adsm/asdm.bin flash:asdm
```

フェールオーバー ペアのアップグレード

フェールオーバー設定の 2 台のユニットには、同じメジャー（最初の番号）、マイナー（2 番めの番号）、メンテナンス（3 番めの番号）バージョンのソフトウエアがインストールされている必要があります。ただし、アップグレード作業中はユニットのバージョン パリティを維持する必要はなく、各ユニットで異なるバージョンのソフトウェアが動作していても、フェールオーバーはサポートされます。長期的な互換性と安定性を確保するには、できるだけ両モジュールとも同じバージョンにアップグレードすることを推奨します。

表 22-1 に、フェールオーバー ペアで無停止アップグレードを実行するためにサポートされているシナリオを示します。

表 22-1　無停止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	マイナー リリース内の任意のメンテナンスから任意のメンテナンス 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 リリースをインストールしなくても、3.1(1) から 3.1(3) に直接アップグレードできます。
マイナー リリース	あるマイナー リリースからその次のマイナー リリースにアップグレードできます。連続していないマイナー リリースにアップグレードすることはできません。 たとえば、3.1 から 3.2 へのアップグレードが可能です。無停止アップグレードでは、3.1 から 3.3 に直接アップグレードすることはサポートされていません。まず 3.2 にアップグレードする必要があります。
メジャー リリース	前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、4.1 のリリースの前の最後のマイナー バージョンが 3.9 だとすると、3.9 から 4.1 へのアップグレードが可能です。 **（注）** FWSM では、2.3 から 3.1 へのアップグレードを行うには、システムを停止させる必要があります。停止させずにアップグレードが行えるのは、リリース 3.1 以降のみです。2.x からのアップグレードの詳細については、『*Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module to Release 3.1*』を参照してください。

ここでは、次の内容について説明します。

- 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.22-12）
- 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.22-13）

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 フェールオーバー設定の 2 台のユニットをアップグレードする手順は、次のとおりです。

(注) FWSM では、2.3 から 3.1 へのアップグレードを行うには、システムを停止させる必要があります。停止させずにアップグレードが行えるのは、リリース 3.1 以降のみです。2.x からのアップグレードの詳細については、『*Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module to Release 3.1*』を参照してください。

ステップ 1　新しいソフトウェアを 2 台のユニットにダウンロードします。「FWSM CLI からのアプリケーション ソフトウェアのインストール」（p.22-4）を参照してください。

ステップ 2　アクティブ ユニットで次のコマンドを入力して、スタンバイ ユニットをリロードし、新しいイメージをブートします。

```
active# failover reload-standby
```

ステップ 3　スタンバイ ユニットのリロードが完了し、Standby Ready ステートになったら、アクティブ ユニットで次のコマンドを入力して、アクティブ ユニットをスタンバイ モードに切り替えます。

(注) スタンバイ ユニットが Standby Ready ステートになっているかどうかを確認するには、**show failover** コマンドを使用します。

```
active# no failover active
```

ステップ 4　次のコマンドを入力して、前のアクティブ ユニット（現在は新しいスタンバイ ユニット）をリロードします。

```
newstandby# reload
```

ステップ 5　（任意）新しいスタンバイ ユニットのリロードが完了し、Standby Ready ステートになったら、次のコマンドを入力して、元のアクティブ ユニットをアクティブ状態に戻します。

```
newstandby# failover active
```

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 フェールオーバー設定の 2 台のユニットをアップグレードする手順は、次のとおりです。

（注） FWSM では、2.3 から 3.1 へのアップグレードを行うには、システムを停止させる必要があります。停止させずにアップグレードが行えるのは、リリース 3.1 以降のみです。2.x からのアップグレードの詳細については、『*Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module to Release 3.1*』を参照してください。

ステップ 1　新しいソフトウェアを 2 台のユニットにダウンロードします。「FWSM CLI からのアプリケーション ソフトウェアのインストール」（p.22-4）を参照してください。

ステップ 2　プライマリ ユニットのシステム実行スペースで次のコマンドを入力して、プライマリ ユニットで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。

```
primary# failover active
```

ステップ 3　プライマリ ユニットのシステム実行スペースで次のコマンドを入力して、セカンダリ ユニットをリロードと新しいイメージのブーとを行います。

```
primary# failover reload-standby
```

ステップ 4　セカンダリ ユニットのリロードが完了し、ユニットの両方のフェールオーバー グループが Standby Ready ステートになったら、プライマリ ユニットのシステム実行スペースで次のコマンドを入力して、セカンダリ ユニットで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。

```
primary# no failover active
```

（注） セカンダリ ユニットで両方のフェールオーバー グループが Standby Ready ステートになっているかどうかを確認するには、**show failover** コマンドを使用します。

ステップ 5　プライマリ ユニットの両方のフェールオーバー グループが Standby Ready ステートになっていることを確認してから、次のコマンドを使用してプライマリ ユニットをリロードします。

```
primary# reload
```

preempt コマンドで設定した場合、フェールオーバー グループは、先行遅延時間の経過後、指定ユニット上で自動的にアクティブになります。**preempt** コマンドで設定されていない場合、フェールオーバー グループは、**failover active group** コマンドを使用して指定ユニット上でアクティブ状態に戻すことができます。

メンテナンス ソフトウェアのインストール

FWSMRelease 3.1 へのアップグレードを行うには、事前にメンテナンス ソフトウェア Release 2.1(2) 以降をインストールしておく必要があります。ここでは、次の内容について説明します。

- メンテナンス ソフトウェア リリースの確認（p.22-14）
- メンテナンス ソフトウェアのアップグレード（p.22-15）

メンテナンス ソフトウェア リリースの確認

メンテナンス ソフトウェア リリースを確認するには、メンテナンス パーティションを起動し、次の手順でリリースを表示します。

ステップ 1　必要に応じて、次のコマンドを入力して、FWSM のセッションを終了します。

```
hostname# exit

Logoff

[Connection to 127.0.0.31 closed by foreign host]
Router#
```

コンフィギュレーション モードで作業している場合、**exit** コマンドを複数回入力しなければならないことがあります。

ステップ 2　OS に応じて、スイッチのプロンプトで次のコマンドを入力して、FWSM のメンテナンス パーティションを起動します。

- Cisco IOS ソフトウェアの場合、次のコマンドを入力します。

  `Router# hw-module module mod_num reset cf:1`

- Catalyst OS ソフトウェアの場合、次のコマンドを入力します。

  `Console> (enable) reset mod_num cf:1`

ステップ 3　OS に応じて、次のコマンドを入力して、FWSM へのセッションを開始します。

- Cisco IOS ソフトウェア

  `Router# session slot number processor 1`

- Catalyst OS ソフトウェア

  `Console> (enable) session module_number`

ステップ 4　次のコマンドを入力して、FWSM のメンテナンス パーティションにルートとしてログインします。

```
Login: root

Password:
```

デフォルトのパスワードは、**cisco** です。

FWSM では、最初のログイン時にバージョンが表示されます。

```
Maintenance image version: 2.1(2)
```

ステップ 5　次のコマンドを入力して、ログイン後にメンテナンス バージョンを表示します。

```
root@localhost# show version

Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 : integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-FWM-1
Number of Pentium-class Processors :       2
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.9
Total available memory: 1004 MB
Size of compact flash: 123 MB
Daughter Card Info: Number of DC Processors: 3
Size of DC Processor Memory (per proc): 32 MB
```

メンテナンス ソフトウェアのアップグレード

メンテナンス ソフトウェアをアップグレードする必要がある場合、次の手順を実行します。

ステップ 1　次の URL で Cisco.com からメンテナンス ソフトウェアをダウンロードします。

http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-serv-maint

FWSM 管理コンテキストからアクセス可能な TFTP、HTTP、または HTTPS サーバにソフトウェアをプットします。

ステップ 2　必要に応じて、次の手順で、メンテナンス　パーティションからログアウトし、アプリケーション パーティションをリロードします。

a. 次のコマンドを入力して、メンテナンス パーティションからログアウトします。

```
root@localhost# logout
```

b. 必要に応じて、OS に応じたコマンドを入力して、アプリケーション パーティションで FWSM を再起動します。

— Cisco IOS ソフトウェアの場合、次のコマンドを入力します。

```
Router# hw-module module mod_num reset
```

— Catalyst OS ソフトウェアの場合、次のコマンドを入力します。

```
Console> (enable) reset mod_num
```

c. OS に応じて、次のコマンドを入力して、FWSM へのセッションを開始します。

— Cisco IOS ソフトウェア

```
Router# session slot number processor 1
```

— Catalyst OS ソフトウェア

```
Console> (enable) session module_number
```

ステップ 3　メンテナンス パーティション ソフトウェアをアップグレードするには、次のいずれかのコマンドを使用して、適切なダウンロード サーバを指定します。

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で作業する必要があります。

- TFTP サーバからメンテナンス ソフトウェアをダウンロードするには、次のコマンドを入力します。

  ```
  hostname# upgrade-mp tftp[://server[:port][/path]/filename]
  ```

  サーバ情報を確定するよう促されます。コマンドにサーバ情報を指定しなかった場合は、このプロンプトが出力された時点で入力することができます。
- HTTP または HTTPS サーバからメンテナンス ソフトウェアをダウンロードするには、次のコマンドを入力します。

  ```
  hostname# upgrade-mp http[s]://[user[:password]@]server[:port][/path]/filename
  ```

メンテナンス パーティションのルート アカウントおよびゲスト アカウントのパスワードは、アップグレード後も保持されます。

ステップ 4　次のコマンドを入力して、FWSM のリロードと新しいメンテナンス ソフトウェアのロードを行います。

```
hostname# reload
```

または、メンテナンス パーティションの起動の準備として FWSM からログアウトすることもできます。メンテナンス パーティションから、両方のアプリケーション パーティションにアプリケーション ソフトウェアをインストールできます。FWSM セッションを終了するには、次のコマンドを入力します。

```
hostname# exit

Logoff

[Connection to 127.0.0.31 closed by foreign host]
Router#
```

コンフィギュレーション モードで作業している場合、**exit** コマンドを複数回入力しなければならないことがあります。

FWSM をメンテナンス パーティションにリロードする方法については、「メンテナンス パーティションからのアプリケーション ソフトウェアのインストール」（p.22-6）を参照してください。

次に、TFTP サーバ情報のプロンプトの例を示します。

```
hostname# upgrade-mp tftp
Address or name of remote host [127.0.0.1]? 10.1.1.5
Source file name [cdisk]? mp.2-1-0-3.bin.gz
copying tftp://10.1.1.5/mp.2-1-0-3.bin.gz to flash
[yes|no|again]? yes
!!!!!!!!!!!!!!!!!!!!!!!
Received 1695744 bytes.
Maintenance partition upgraded.
```

コンフィギュレーション ファイルのダウンロードおよびバックアップ

ここでは、コンフィギュレーション ファイルのダウンロードおよびバックアップの手順について説明します。内容は次のとおりです。

- フラッシュ メモリ内のファイルの確認（p.22-17）
- スタートアップまたは実行コンフィギュレーションへのテキスト　コンフィギュレーションのダウンロード（p.22-17）
- ディスクへのコンテキスト コンフィギュレーションのダウンロード（p.22-18）
- 設定のバックアップ（p.22-19）

フラッシュ メモリ内のファイルの確認

フラッシュ メモリ内のファイルを表示し、ファイルに関する情報を確認することができます。

- 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。

  ```
  hostname# dir disk:
  ```

  次に例を示します。

  ```
  hostname# dir

  Directory of disk:/

  9       -rw-  1411        08:53:42 Oct 06 2005  old_running.cfg
  10      -rw-  959         09:21:50 Oct 06 2005  admin.cfg
  11      -rw-  1929        08:23:44 May 07 2005  admin_backup.cfg
  ```

- 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（ディスク :/）です。

  次に例を示します。

  ```
  hostname# show file info admin.cfg

  disk:/admin.cfg:
    type is ascii text
    file size is 959 bytes
  ```

スタートアップまたは実行コンフィギュレーションへのテキスト コンフィギュレーションのダウンロード

次のタイプのサーバからシングル 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に、テキスト ファイルをダウンロードすることができます。

- TFTP
- FTP
- HTTP
- HTTPS

マルチモード コンテキストについては、「ディスクへのコンテキスト コンフィギュレーションのダウンロード」（p.22-18）を参照してください。

(注) 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場合、2 つの設定を結合します。結合によって、新しいコンフィギュレーションのコマンドが実行コンフィギュレーションに追加されます。設定が同じ場合、変更はありません。コマンドが矛盾する場合、またはコマンドがコンテキストの稼働に影響を与える場合、結合の作用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あれば、予想外の結果が生じることもあります。

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を、サーバから FWSM にコピーするには、次のコマンドを使用して、適切なダウンロード サーバを指定します。

- TFTP サーバからコピーするには、次のコマンドを入力します。

  hostname# **copy tftp://***server*[**/***path*]**/***filename* {**startup-config** | **running-config**}

- FTP サーバからコピーするには、次のコマンドを入力します。

  hostname# **copy ftp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***filename*[**;type=***xx*] {**startup-config** | **running-config**}

  type には、次のいずれかのキーワードを指定できます。

  — **ap** — ASCII パッシブ モード

  — **an** — ASCII 標準モード

  — **ip** — （デフォルト）バイナリ パッシブ モード

  — **in** — バイナリ標準モード

  コンフィギュレーション ファイルには、ASCII またはバイナリを使用できます。

- HTTP または HTTPS サーバからコピーするには、次のコマンドを入力します。

  hostname# **copy http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][**/***path*]**/***filename* {**startup-config** | **running-config**}

次に、TFTP サーバから設定をコピーする例を示します。

```
hostname# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

次に、FTP サーバから設定をコピーする例を示します。

```
hostname# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg;type=an
startup-config
```

次に、HTTP サーバから設定をコピーする例を示します。

```
hostname# copy http://209.165.200.228/configs/startup.cfg startup-config
```

ディスクへのコンテキスト コンフィギュレーションのダウンロード

コンテキスト コンフィギュレーションをディスクにコピーするには、次のコマンドを使用して、システム実行スペースの適切なダウンロード サーバを指定します。

- TFTP サーバからコピーするには、次のコマンドを入力します。

  hostname# **copy tftp://***server*[**/***path*]**/***filename* **disk:**[*path***/**]*filename*

- FTP サーバからコピーするには、次のコマンドを入力します。

  hostname# **copy ftp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***filename* **disk:**[*path***/**]*filename*

- HTTP または HTTPS サーバからコピーするには、次のコマンドを入力します。

  hostname# **copy http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][**/***path*]**/***filename*
  disk:[*path***/**]*filename*

設定のバックアップ

設定をバックアップするには、次のコマンドのいずれかを入力します。

- 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.22-19）
- 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のバックアップ（p.22-19）
- コンテキスト内のコンテキスト コンフィギュレーションのバックアップ（p.22-20）
- 端末ディスプレイからの設定のコピー（p.22-20）

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、外部サーバまたはローカル フラッシュ メモリに、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コピーすることができます。

- TFTP サーバにコピーするには、次のコマンドを入力します。

  hostname# **copy** {**startup-config** | **running-config**} **tftp:**//*server*[**/***path*]**/***filename*

- FTP サーバにコピーするには、次のコマンドを入力します。

  hostname# **copy** {**startup-config** | **running-config**}
  ftp://[*user*[**:***password*]**@**]*server*[**/***path*]**/***filename*

- ローカル フラッシュ メモリにコピーするには、次のコマンドを入力します。

  hostname# **copy** {**startup-config** | **running-config**} **disk:**[*path***/**]*filename*

  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、**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のバックアップ

マルチ コンテキスト モードで、ローカル 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をコピーするには、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します。

- TFTP サーバにコピーするには、次のコマンドを入力します。

  hostname# **copy disk:**[*path***/**]*filename* **tftp:**//*server*[**/***path*]**/***filename*

- FTP サーバにコピーするには、次のコマンドを入力します。

  hostname# **copy disk:**[*path***/**]*filename* **ftp:**//[*user*[**:***password*]**@**]*server*[**/***path*]**/***filename*

- ローカル フラッシュ メモリにコピーするには、次のコマンドを入力します。

  hostname# **copy disk:**[*path***/**]*filename* **disk:**[*path***/**]newfilename

  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、**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、コンテキスト内で、次のバックアップを実行できます。

- 実行コンフィギュレーションを（admin コンテキストに接続している）スタートアップ コンフィギュレーション サーバにコピーするには、次のコマンドを入力します。

  ```
  hostname/contexta# copy running-config startup-config
  ```

- 実行コンフィギュレーションを、コンテキスト ネットワークに接続している TFTP サーバにコピーするには、次のコマンドを入力します。

  ```
  hostname/contexta# copy running-config tftp:/server[/path]/filename
  ```

端末ディスプレイからの設定のコピー

設定を端末に出力するには、次のコマンドを入力します。

```
hostname# show running-config
```

コマンドの出力をコピーして、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。

自動アップデート サポートの設定

自動アップデートとは、自動アップデート サーバで設定とソフトウェア イメージを多数の FWSM にダウンロードし、中央の離れた場所から FWSM の基本的監視を行えるようにするためのプロトコル仕様です。FWSM は、ソフトウェア イメージやコンフィギュレーション ファイルのアップデートがないかどうか確認するため、定期的に自動アップデート サーバへのポーリングを行います。

（注） 自動アップデートは、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。

ここでは、次の内容について説明します。

- 自動アップデート サーバとの通信の設定（p.22-21）
- 自動アップデート ステータスの表示（p.22-22）

自動アップデート サーバとの通信の設定

自動アップデートを設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、AUS の URL を指定します。

```
hostname(config)# auto-update server url [source interface] [verify-certificate]
```

url の構文は次のとおりです。

```
http[s]://[user:password@]server_ip[:port]/pathname
```

設定できるサーバは 1 台のみです。***https*** を指定した場合、SSL が使用されます。URL の *user* および *password* 引数は、サーバへのログイン時の基本認証に使用されます。設定の表示に、**write terminal**、**show configuration**、または **show tech-support** コマンドを使用した場合、user と password は「********」と表示されます。

デフォルト ポートは、HTTP の場合は 80、HTTPS の場合は 443 です。

source *interface* 引数には、AUS への要求送信時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のと同じインターフェイスを指定した場合、自動アップデート要求は、管理アクセスで使用されるのと同じ IPSec VPN トンネルを使用して送信されます。

verify-certificate キーワードを指定すると、AUS によって返された証明書を確認します。

ステップ 2　（任意）次のコマンドを入力して、AUS との通信時の送信先となる装置 ID を特定します。

```
hostname(config)# auto-update device-id {hardware-serial | hostname | ipaddress
[if-name] | mac-address [if-name] | string text}
```

使用する ID を指定するには、次のいずれかのパラメータを使用します。

- **hardware-serial** ― FWSM のシリアル番号を使用します。
- **hostname** ― FWSM のホスト名を使用します。
- **ipaddress** ― 指定したインターフェイスの IP アドレスを使用します。インターフェイス名を指定しなかった場合、AUS 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。
- **mad-address** ― 指定したインターフェイスの MAC アドレスを使用します。インターフェイス名を指定しなかった場合、AUS 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** ― 指定したテキスト識別子を使用します。テキスト識別子には、スペース、「‘」、「“」、「>」、「&」、「?」の文字は使用できません。

ステップ 3　（任意）次のコマンドを入力して、設定またはイメージのアップデートがあるかどうかを確認するための AUS へのポーリングの間隔を指定します。

```
hostname(config)# auto-update poll-period poll-period [retry-count [retry-period]]
```

poll-period 引数には、アップデートの確認を行う間隔（分単位）を指定します。デフォルトは 720 分（12 時間）です。

retry-count 引数には、最初の接続に失敗した場合の、サーバへの再接続の試行回数を指定します。デフォルトは 0 回です。

poll-period 引数には、次の再試行までの待ち時間（分単位）を指定します。デフォルトは 5 です。

ステップ 4　（任意）自動アップデート サーバへのアクセスが一定時間ない場合、次のコマンドを入力して、トラフィックを中断します。

```
hostname(config)# auto-update timeout period
```

period には、タイムアウト時間を分単位で指定します。指定可能な範囲は 1 ～ 35,791 です。デフォルトはタイムアウトなし（0）です。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

このコマンドを使用して、FWSM のイメージとコンフィギュレーションが最新であることを保証します。この状態は、システム ログ メッセージ 201008 としてレポートされます。

次の例では、外部インターフェイスから IP アドレス 209.165.200.224、ポート番号 1742 の AUS にポーリングし、証明書の確認を行うよう FWSM を設定します。

また、装置 ID として FWSM のホスト名を使用し、ポーリング間隔をデフォルトの 720 分から 600 分に減らすよう設定します。ポーリングに失敗した場合、AUS への再接続を 10 回行い、次の再接続の試行まで 3 分待つようにします。

```
hostname(config)# auto-update server
https://jcrichton:farscape@209.165.200.224:1742/management source outside
verify-certificate
hostname(config)# auto-update device-id hostname
hostname(config)# auto-update poll-period 600 10 3
```

自動アップデート ステータスの表示

自動アップデート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。

```
hostname(config)# show auto-update
```

次に、**show auto-update** コマンドの出力例を示します。

```
hostname(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
```

FWSM のモニタリング

この章では、FWSM のためのロギングと SNMP（簡易ネットワーク管理プロトコル）の設定方法について説明します。システム ログ メッセージの内容とシステム ログ メッセージのフォーマットについても説明します。

この章は、モニタリングとロギングのコマンドやオプションについて包括的な説明をするものではありません。詳しい説明とその他のコマンドについては、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

この章で説明する内容は次のとおりです。

- SNMP の設定（p.23-2）
- ログの設定および管理（p.23-6）

SNMP の設定

ここでは、SNMP の使用方法について説明します。内容は次のとおりです。

- SNMP の概要（p.23-2）
- SNMP のイネーブル化（p.23-4）

SNMP の概要

FWSM は、SNMP v1 および v2c を使用したネットワーク モニタをサポートしています。FWSM では、トラップおよび SNMP リード アクセスはサポートされますが、SNMP ライト アクセスはサポートされません。

FWSM から Network Management Station（NMS; ネットワーク管理ステーション）にトラップ（イベント通知）が送信されるように設定したり、NMS を使用して FWSM 上の MIB（管理情報ベース）を参照できます。MIB は定義の集合で、FWSM は各定義の値のデータベースを保持します。MIB を参照するには、NMS から SNMP get 要求を発行します。SNMP トラップを受信して、MIB を参照するには、CiscoWorks for Windows またはその他の SNMP v1、MIB-II 準拠ブラウザを使用します。

表 23-1 に、サポート対象の MIB、FWSM のトラップ、およびマルチモードの各コンテキストのトラップを示します。Cisco MIB は、次の Web サイトからダウンロードできます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

ダウンロードした MIB を、NMS 用にコンパイルします。

表 23-1　SNMP の MIB およびトラップのサポート

サポート対象の MIB またはトラップ	説明
SNMP コア トラップ	FWSM は、次のコア SNMP トラップを送信します。 • 認証 — NMS が正しいコミュニティ ストリングを認証しなかったために SNMP 要求に失敗した場合 • リンクアップ — インターフェイスが「up」ステートに移行した場合 • リンクダウン — **nameif** コマンドを削除したりして、インターフェイスがダウンした場合 • コールドスタート — FWSM をリロードして実行した場合
MIB-II	FWSM は、次のグループおよびテーブルの参照をサポートしています。 • システム
IF-MIB	セキュリティ アプライアンスは、次のテーブルの参照をサポートしています。 • ifTable • ifXTable
RFC1213-MIB	セキュリティ アプライアンスは、次のテーブルの参照をサポートしています。 • ip.ipAddrTable
SNMPv2-MIB	セキュリティ アプライアンスは、次の参照をサポートしています。 • snmp

表 23-1　SNMP の MIB およびトラップのサポート（続き）

サポート対象の MIB またはトラップ	説明
ENTITY-MIB	FWSM は、次のグループおよびテーブルの参照をサポートしています。 • entPhysicalTable • entLogicalTable FWSM は、次のトラップの参照をサポートしています。 • config-change • fru-insert • fru-remove
CISCO-IPSEC-FLOW-MONITOR-MIB	FWSM は、MIB の参照をサポートしています。 FWSM は、次のトラップの参照をサポートしています。 • start • stop
CISCO-REMOTE-ACCESS-MONITOR-MIB	FWSM は、MIB の参照をサポートしています。 FWSM は、次のトラップの参照をサポートしています。 • session-threshold-exceeded
CISCO-CRYPTO-ACCELERATOR-MIB	FWSM は、MIB の参照をサポートしています。
ALTIGA-GLOBAL-REG	FWSM は、MIB の参照をサポートしています。
Cisco Firewall MIB	FWSM は、次のグループの参照をサポートしています。 • cfwSystem この情報は、単一コンテキストではなく装置全体のフェールオーバーステータスに関する cfwSystem.cfwStatus です。
Cisco メモリ プール MIB	FWSM は、次のテーブルの参照をサポートしています。 • ciscoMemoryPoolTable　―　このテーブルに保存されるメモリ使用状況は、FWSM の汎用プロセッサだけに適用され、ネットワーク プロセッサには適用されません。
Cisco プロセス MIB	FWSM は、次のテーブルの参照をサポートしています。 • cpmCPUTotalTable
Cisco Syslog MIB	FWSM は、次のトラップをサポートしています。 • clogMessageGenerated この MIB は参照できません。

SNMP のイネーブル化

FWSM 上で実行される SNMP エージェントは、2 つの機能を実行します。

- NMS からの SNMP 要求への応答
- NMS へのトラップ（イベント通知）の送信

SNMP エージェントをイネーブルにし、FWSM に接続できる NMS を指定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、FWSM で SNMP サーバがイネーブルになっていることを確認します。

```
hostname(config)# snmp-server enable
```

デフォルトでは、SNMP サーバはイネーブルです。

ステップ 2　次のコマンドを入力して、FWSM に接続できる NMS の IP アドレスを指定します。

```
hostname(config)# snmp-server host interface_name ip_address [trap | poll]
[community text] [version {1 | 2c}] [udp-port port]
```

NMS をトラップ受信またはブラウジング（ポーリング）だけに制限する場合には、**trap** または **poll** を指定します。デフォルトでは、NMS は両方の機能を実行します。

SNMP トラップは、デフォルトでは UDP ポート 162 上で送信されます。**udp-port** キーワードを使用すると、ポート番号を変更できます。

ステップ 3　次のコマンドを入力して、コミュニティ ストリングを指定します。

```
hostname(config)# snmp-server community key
```

SNMP コミュニティ ストリングは、FWSM と NMS 間の共有シークレットです。キーには、最大 32 文字の値を大文字と小文字を区別して指定します。スペースは入力できません。

ステップ 4　（任意）SNMP サーバの場所またはコンタクト情報を設定する場合には、次のコマンドを入力します。

```
hostname(config)# snmp-server {contact | location} text
```

ステップ 5　次のコマンドを入力して、FWSM から NMS へのトラップ送信をイネーブルにします。

```
hostname(config)# snmp-server enable traps [all | syslog | snmp [trap] [...] |
entity [trap] [...] | ipsec [trap] [...] | remote-access [trap]]
```

個々のトラップまたはトラップのセットをイネーブルにするには、各機能タイプに対してこのコマンドを入力します。または、すべてのトラップをイネーブルにするには、**all** キーワードを入力します。

デフォルト設定では、すべての **snmp** トラップはイネーブルになっています（**snmp-server enable traps snmp authentication linkup linkdown coldstart**）。**snmp** キーワードを指定して、このコマンドの **no** 形式を使用すると、これらのトラップをディセーブルにすることができます。ただし、**clear configure snmp-server** コマンドを使用すると、SNMP トラップのデフォルトのイネーブル化がリストアされます。

このコマンドを入力してトラップ タイプを指定しない場合、デフォルトは **syslog** となります（デフォルトの **snmp** トラップは、**syslog** トラップと一緒にイネーブルのままです）。

snmp のトラップには、次のものがあります。

- **authentication**
- **linkup**
- **linkdown**
- **coldstart**

entity のトラップには、次のものがあります。

- **config-change**
- **fru-insert**
- **fru-remove**

ipsec のトラップには、次のものがあります。

- **start**
- **stop**

remote-access のトラップには、次のものがあります。

- **session-threshold-exceeded**

ステップ 6　次のコマンドを入力して、システム メッセージが NMS にトラップとして送信されるように設定します。

```
hostname(config)# logging history level
```

上記の **snmp-server enable traps** コマンドを使用して、**syslog** トラップをイネーブルにしておく必要があります。

ステップ 7　次のコマンドを入力して、NMS に送信されるシステム メッセージが生成されるように、ロギングをイネーブルにします。

```
hostname(config)# logging enable
```

次に、FWSM が内部インターフェイス上でホスト 192.168.3.2 から要求を受信するよう設定する例を示します。

```
hostname(config)# snmp-server host 192.168.3.2
hostname(config)# snmp-server location building 42
hostname(config)# snmp-server contact Pat lee
hostname(config)# snmp-server community ohwhatakeyisthee
```

ログの設定および管理

ここでは、ロギングの機能と設定について説明します。システム ログ メッセージのフォーマット、オプション、変数についても説明します。

- ロギングの概要（p.23-6）
- マルチコンテキスト モードでのロギング（p.23-7）
- ロギングのイネーブル化およびディセーブル化（p.23-7）
- ログの出力先の設定（p.23-9）
- 出力先に送信するシステム ログ メッセージのフィルタリング（p.23-19）
- ログ設定のカスタマイズ（p.23-22）
- システム ログ メッセージの内容（p.23-27）

ロギングの概要

FWSM のシステム ログでは、FWSM のモニタリングやトラブルシューティングのためのロギング情報が得られます。ロギングの設定は非常に柔軟性が高く、FWSM でのシステム ログ メッセージの処理方法に関して、さまざまな面からカスタマイズが可能です。

ロギング機能を使用すると、次のことができます。

- 記録するシステム ログ メッセージの指定
- システム ログ メッセージの重大度のディセーブル化または変更
- システム ログ メッセージの 1 つまたは複数の送信先の指定。これには、内部バッファ、1 台または複数台の Syslog サーバ、ASDM、SNMP 管理ステーション、指定した電子メール アドレス、Telnet および SSH セッションなどが含まれます。
- 重大度やメッセージ クラスなどによる、グループ内でのシステム ログ メッセージの設定と管理
- バッファが一杯になってラップアラウンドした場合の、内部バッファの内容に対する処理方法の指定。バッファの内容を FTP サーバに送信したり、内容を内部フラッシュ メモリに保存したりするよう FWSM を設定できます。
- ログ ファイルを FTP サーバに送信
- ログ ファイルを内部フラッシュ メモリに保存
- システム ログ メッセージのリモート モニタリング。Adaptive Security Device Manager（ASDM）、Telnet、SSH セッションを使用するか、または内部ログ バッファの内容を Web ブラウザにダウンロードすることによって行います。

システム ログ メッセージ全体、またはシステム ログ メッセージのサブセットを、任意の出力先またはすべての出力先に送信することができます。システム ログ メッセージの重大度、システム ログ メッセージのクラスにより、またはカスタム ログ メッセージ リストを作成することにより、どこにどのシステム ログ メッセージを送信するかをフィルタリングできます。

マルチコンテキスト モードでのロギング

各セキュリティ コンテキストに独自の設定があるように、各セキュリティ コンテキストには独自のロギング設定とシステム メッセージ ログがあります。セキュリティ コンテキスト用のメッセージ ログには、そのコンテキストのためにイネーブル化された機能に関するメッセージが含まれます。たとえば、コンテキスト ログには、そのコンテキストのセキュリティ ポリシー、ルーティング、設定変更に関するメッセージが含まれます。シングル コンテキスト モードで動作するセキュリティ アプライアンスと同様に、セキュリティ コンテキストのロギングはデフォルトではイネーブルになっていません。セキュリティ コンテキストのためにログを保持するには、セキュリティ コンテキストにアクセスしてロギングを設定する必要があります。同様に、セキュリティ コンテキストのログ メッセージを表示するには、セキュリティ コンテキストにアクセスする必要があります。

システムまたは admin コンテキストにログインして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ものだけです。

システム実行スペースで生成されるシステム メッセージ（フェールオーバー メッセージを含む）が、admin コンテキストで生成されたメッセージと一緒に、admin コンテキストに表示されます。admin コンテキストでロギングを設定してイネーブルにした場合、システム実行スペースで発生するメッセージは、自動的に admin コンテキスト メッセージに追加されます。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。

各メッセージにセキュリティ コンテキストのロギング装置 ID を記述するようにロギングを設定できます。このように設定した場合、各メッセージに、メッセージが作成されたコンテキストの名前が記述されます。admin コンテキストのロギング装置 ID をイネーブルにすると、システム実行スペースで生成されたメッセージには「system」という装置 ID が使用され、admin コンテキストで生成されたメッセージには装置 ID としてコンテキスト名が使用されます。ロギング装置 ID のイネーブル化の詳細については、「システム ログ メッセージへの装置 ID の記載」（p.23-23）を参照してください。

セキュリティ コンテキストの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』の「Enabling Multiple Context Mode」の章を参照してください。

ロギングのイネーブル化およびディセーブル化

ここでは、FWSM のロギングをイネーブル化 / ディセーブル化する方法について説明します。内容は次のとおりです。

- 設定された全出力先へのロギングのイネーブル化（p.23-7）
- 設定された全出力先へのロギングのディセーブル化（p.23-8）
- ログ設定の表示（p.23-8）

設定された全出力先へのロギングのイネーブル化

次の手順でロギングはイネーブルにできますが、ロギングされたメッセージを表示したり保存したりできるように、少なくとも 1 つの出力先を指定する必要もあります。出力先を指定していない場合、FWSM はイベント発生時に生成されるシステム ログ メッセージを保存しません。

ログ出力先の設定の詳細については、「ログの出力先の設定」（p.23-9）を参照してください。

ロギングをイネーブルにする手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、コンフィギュレーション モードにアクセスします。

```
hostname># config t
```

ステップ 2　次のコマンドを入力して、ロギングを開始します。

```
hostname(config)# logging enable
```

ステップ 3　次のコマンドを入力して、イネーブルになっているロギングのタイプを表示します。

```
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

設定された全出力先へのロギングのディセーブル化

設定された全出力先へのロギ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。

```
hostname(config)# no logging enable
```

ログ設定の表示

実行中のログ設定を表示するには、次のコマンドを入力します。

```
hostname(config)# show logging
```

show logging コマンドの出力内容は、次のようになります。

```
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
```

ステータス行エントリの定義は、次のとおりです。

ロギング ステータス行	説明
System Log logging	システム ロギング全体のステータス
Facility	Syslog サーバに送信されたシステム ログ メッセージに使用されたロギング ファシリティ
Timestamp logging	システム ログ メッセージにタイムスタンプが記録されるかどうかを示します。
Standby logging	イネーブルにすると、フェールオーバーの発生時にフェールオーバー スタンバイ FWSM のシステム ログ メッセージの同期を維持します。
Deny Conn when Queue Full	イネーブルにすると、ログ キューがいっぱいになったときにすべてのトラフィックを拒否します。
Monitor logging	コンソールのロギングが Telnet または SSH セッションを通して表示可能かどうかを示します。
Buffer logging	内部ログ バッファがログ出力先としてイネーブルになっているかどうかを示します。
Trap logging	1 台または複数台の Syslog サーバへのログの送信がイネーブルになっているかどうかを示します。
History logging	SNMP 管理ステーションへのログの送信がイネーブルになっているかどうかを示します。
Device ID	システム ログ メッセージに装置 ID が記述されるかどうかを示します。
Mail logging	1 つまたは複数の電子メール アドレスへのログの送信がイネーブルになっているかどうかを示します。
ASDM logging	ASDM へのログの送信がイネーブルになっているかどうかを示します。

ログの出力先の設定

ここでは、FWSM で生成されたログ メッセージの保存先と送信先を指定する方法について説明します。内容は次のとおりです。

- ログの出力先の概要（p.23-9）
- 出力先としての Syslog サーバの指定（p.23-10）
- 出力先としての電子メール アドレスの指定（p.23-12）
- 出力先としての ASDM の指定（p.23-13）
- Telnet セッションを使用したログの表示（p.23-15）
- 出力先としてのログ バッファの指定（p.23-16）

ログの出力先の概要

FWSM で生成されたログを表示するには、ログの出力先を指定する必要があります。ログの出力先を指定せずにロギングをイネーブルにした場合、FWSM でメッセージは生成されますが、参照が可能な場所への保存は行われません。

FWSM では、ログの送信先として次の場所を設定できます。

- 1 台または複数の Syslog サーバ

- 1 つまたは複数の電子メール アドレス
- ASDM
- Telnet セッション
- 内部ログ バッファ

出力先としての Syslog サーバの指定

ここでは、FWSM のログの出力先として Syslog サーバを設定する方法について説明します。

FWSM のログを Syslog サーバに送信するよう設定すると、ログをアーカイブしてサーバの空きディスク スペース以外の制約を受けないようにし、保存後にログ データを操作できるようになります。たとえば、特定のタイプのシステム ログ メッセージがロギングされたときに実行されるアクションを指定したり、ログからデータを抽出して、レポートのためにレコードを別のファイルに保存したり、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することができます。

Syslog サーバでは、syslogd というプログラム（サーバ）を実行する必要があります。UNIX では、OS（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、別のベンダーから syslogd サーバを入手してください。

FWSM では、UDP または TCP を使用してデータを Syslog サーバに送信するよう設定することができますが、両方を同時に使用することはできません。TCP を指定した場合、FWSM は Syslog サーバに障害が発生したために中断されたログ送信を検知します。UDP を指定した場合、FWSM は Syslog サーバが動作可能かどうかに関係なく、ログの送信を続行します。

ログ メッセージにタイムスタンプが必要であれば、ロギング タイムスタンプをイネーブルにすることができます。Syslog サーバへのログ送信に UDP を選択した場合、Syslog サーバの EMBLEM フォーマットのロギングをイネーブルにすることができます。

FWSM でシステム ログ メッセージを Syslog サーバに送信するよう設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、ログを受信する Syslog サーバを指定します。

```
hostname(config)# logging host if_name ip_address {[tcp/port] | udp/port]} [format
emblem]
```

ここで

format emblem — Syslog サーバの EMBLEM フォーマットのロギングをイネーブルにします（UDP のみ）。

interface_name — Syslog サーバが常駐するインターフェイスを指定します。

port — Syslog サーバがシステム ログ メッセージを待ち受けるポートを指定します。有効なポートの値は、どちらのプロトコルも 1025 ～ 65,535 です。以前にコマンドを入力したときに使用した *port* と *protocol* の値を表示するには、**show running-config logging** コマンドを使用して一覧からコマンドを探します。TCP プロトコルは 6、UDP プロトコルは 17 としてリストに表示されます。

ip_address — Syslog サーバの IP アドレスを指定します。

tcp — FWSM が Syslog サーバへのシステム ログ メッセージの送信に TCP を使用するよう指定します。

udp — FWSM が Syslog サーバへのシステム ログ メッセージの送信に UDP を使用するよう指定します。

次に例を示します。

```
hostname(config)# logging host dmz1 192.168.1.5
```

出力先として複数の Syslog サーバを指定するには、指定する Syslog サーバごとに個別にコマンドを入力します。

ステップ 2　次のコマンドを入力して、Syslog サーバに送信するシステム ログ メッセージを指定します。

```
hostname(config)# logging trap {severity_level (1-7) | message_list}
```

ここで

severity_level — Syslog サーバに送信するメッセージの重大度を指定します。たとえば、レベルの設定を 3 にすると、FWSM はレベルが 3、2、1、および 0 のシステム ログ メッセージを送信します。数字（2 など）か名前（critical など）のどちらかを指定できます。

メッセージの重大度の詳細については、「重大度」（p.23-28）を参照してください。

message_list — Syslog サーバに送信するシステム ログ メッセージを識別するカスタム メッセージ リストを指定します。カスタム メッセージ リストの作成方法の詳細については、「カスタム メッセージ リストによるシステム ログ メッセージのフィルタリング」（p.23-21）を参照してください。

次に、FWSM が重大度 3（errors）以上のシステム ログ メッセージをすべて Syslog サーバに送信するよう指定する例を示します。FWSM は、重大度が 3、2、1 のメッセージを送信します。

```
hostname(config)# logging trap errors
```

ステップ 3　サーバに送信するシステム ログ メッセージに装置 ID を記述する場合は、次のコマンドを入力します。

```
hostname(config)# logging device-id {hostname | ipaddress if_name | string text}
```

Syslog サーバに送信されるシステム ログ メッセージに、指定した装置 ID（指定したインターフェイスのホスト名と IP アドレス、または文字列）が記述されます。

ステップ 4　必要に応じて、ロギング ファシリティをデフォルトの 20 以外の値に設定します（大部分の UNIX システムではシステム ログ メッセージがファシリティ 20 で届くことを想定しています）。

ロギング ファシリティの設定を変更するには、次のコマンドを入力します。

```
hostname(config)# logging facility number
```

次に例を示します。

```
hostname(config)# logging facility 16
```

ステップ 5　次のコマンドを入力して、設定の変更を確認します。

```
hostname(config)# show logging
```

次に、**show logging** コマンドの出力例を示します。

```
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
```

出力先としての電子メール アドレスの指定

FWSM のシステム ログ メッセージの一部またはすべてを、電子メール アドレスに送信するよう設定することができます。電子メールで送信した場合、システム ログ メッセージは電子メール メッセージの件名の行に表示されます。このため、このオプションは、critical、alert、emergency など重大度の高いシステム ログ メッセージを管理者に通知する場合に設定することを推奨します。

出力先として電子メール アドレスを指定する手順は、次のとおりです。

ステップ 1　1 つまたは複数の電子メール アドレスに送信するシステム ログ メッセージを指定します。システム ログ メッセージの重大度またはシステム ログ メッセージ リスト変数を使用して、送信するシステム ログ メッセージを指定します。

送信するシステム ログ メッセージを指定するには、次のコマンドを入力します。

```
hostname(config)# logging mail {message_list | severity_level}
```

次に、以前に **logging list** コマンドで設定した「high-priority」という名前の *message_list* を使用する例を示します。

```
hostname(config)# logging mail high-priority
```

ステップ 2　次のコマンドを入力して、システム ログ メッセージを電子メール アドレスに送信する際に使用する送信元の電子メール アドレスを指定します。

```
hostname(config)# logging from-address email_address
```

次に例を示します。

```
hostname(config)# logging from-address xxx-001@example.com
```

ステップ 3　システム ログ メッセージを電子メール アドレスに送信する際に使用する受信者の電子メール アドレスを指定します。受信者のアドレスを 5 つまで設定できます。各受信者を個別に入力する必要があります。

受信者のアドレスを指定するには、次のコマンドを入力します。

```
hostname(config)# logging recipient-address e-mail_address [severity_level]
```

次に例を示します。

```
hostname(config)# logging recipient-address admin@example.com
```

(注)　重大度を指定しなかった場合、デフォルトの重大度が使用されます（エラー状態：重大度 3）。

ステップ 4　次のコマンドを入力して、システム ログ メッセージを電子メール アドレスに送信する際に使用する SMTP サーバを指定します。

```
hostname(config)# smtp-server hostname
```

次に例を示します。

```
hostname(config)# smtp-server smtp-host-1
```

出力先としての ASDM の指定

FWSM では、システム ログ メッセージを ASDM に送信するよう設定することができます。

FWSM は、ASDM への送信を待つシステム ログ 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 のログ バッファは、内部ログ バッファとは異なります。内部ログ バッファの詳細については、「ログ バッファの概要」（p.23-16）を参照してください。

ASDM のログ バッファがいっぱいになると、FWSM は新しいシステム ログ メッセージのためにバッファを確保するため、最も古いシステム ログ メッセージを削除します。ASDM のログ バッファに保存されるシステム ログ メッセージの数を制御するには、バッファのサイズを変更します。

出力先として ASDM を指定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、ASDM に送信するシステム ログ メッセージを指定します。

```
hostname(config)# logging asdm {message_list | severity_level}
```

コマンド オプションは次のとおりです。

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルの設定を 3 にすると、FWSM はレベルが 3、2、1、および 0 のシステム ログ メッセージを生成します。次のように、数字または名前を指定できます。 • **0** または **emergencies** — システム使用不能 • **1** または **alerts** — 早急に処置が必要 • **2** または **critical** — クリティカル状態 • **3** または **errors** — エラー • **4** または **warnings** — 警告 • **5** または **notifications** — 正常だが注意が必要な状態 • **6** または **informational** — 情報 • **7** または **debugging** — デバッグ メッセージ、log FTP コマンド、および WWW URL
message_list	ASDM のログ バッファに送信するシステム ログ メッセージを識別するリストを指定します。リストの作成方法の詳細については、「カスタム メッセージ リストによるシステム ログ メッセージのフィルタリング」（p.23-21）を参照してください。

次に、ロギングをイネーブルにして、ASDM のログ バッファに重大度 0、1、2 のシステム ログ メッセージを送信する例を示します。

```
hostname(config)# logging asdm 2
```

ステップ 2　次のようにグローバル コンフィギュレーション モードで **logging asdm-buffer-size** コマンドを使用して、ASDM のログ バッファに保存可能なシステム ログ メッセージの数を指定します。

```
hostname(config)# logging asdm-buffer-size num_of_msgs
```

num_of_msgs に、FWSM が ASDM のログ バッファに保存するシステム ログ メッセージの数を指定します。

次に、ASDM のログ バッファ サイズを 200 システム ログ メッセージに設定する例を示します。

```
hostname(config)# logging asdm-buffer-size 200
```

ASDM ログ バッファの現在の内容を消去するには、次のコマンドを入力します。

```
hostname(config)# clear logging asdm
```

Telnet セッションを使用したログの表示

Telnet セッションで Syslog メッセージを表示する手順は、次のとおりです。

ステップ 1　インターフェイス内部のホストから FWSM へのアクセスを許可するための FWSM の設定をまだ行っていない場合、次の手順で設定します。

a. 次のコマンドを入力して、IP アドレスとインターフェイス名を指定します。

```
hostname(config)# telnet ip_address [subnet_mask] [if_name]
```

たとえば、ホストの IP アドレスが 192.168.1.2 の場合、コマンドは次のようになります。

```
hostname(config)# telnet 192.168.1.2 255.255.255.255
```

b. 応答がない場合に FWSM がセッションを切断するまでの Telnet セッションの待ち時間を、デフォルトの 5 分より大きな値に設定します。15 分以上に設定するのが望ましいです。設定方法は次のとおりです。

```
hostname(config)# telnet timeout 15
```

ステップ 2　ホストで Telnet を起動し、FWSM の内部インターフェイスを指定します。

Telnet の接続時に、FWSM で次のようなプロンプトが表示されます。

```
FWSM passwd
```

ステップ 3　Telnet のパスワードを入力します。デフォルトのパスワードは、**cisco** です。

ステップ 4　次のコマンドを入力して、コンフィギュレーション モードを開始します。

```
hostname(config)# enable
(Enter your password at the prompt)

hostname(config)# configure terminal
```

ステップ 5　次のコマンドを入力して、メッセージ ロギングを開始します。

```
hostname(config)# logging monitor level (1-7)
```

ステップ 6　次のコマンドを入力して、この Telnet セッションにログを送信します。

```
hostname(config)# terminal monitor
```

このコマンドにより、現在の Telnet セッションでのみロギングがイネーブルになります。**logging monitor** コマンドはすべての Telnet セッションのロギングに関する設定を行いますが、**terminal monitor**（および **terminal no monitor**）コマンドは個々の Telnet セッションのロギングを制御します。

ステップ 7　ホストに ping を実行するか、または Web ブラウザを起動することにより、イベントをトリガーします。

Telnet セッション ウィンドウに Syslog メッセージが表示されます。

ステップ 8　完了したら、次のコマンドでこの機能をディセーブルにします。

```
hostname(config)# terminal no monitor
hostname(config)# no logging monitor
```

出力先としてのログ バッファの指定

ここでは、FWSM でシステム ログ メッセージを内部ログ バッファに保存するよう設定する方法について説明します。内容は次のとおりです。

- 出力先としてのログ バッファのイネーブル化（p.23-16）
- ログ バッファがいっぱいになった場合の動作の指定（p.23-17）
- 内部フラッシュ メモリへのログ バッファの内容の保存（p.23-18）
- ログ バッファの内容の消去（p.23-18）

ログ バッファの概要

出力先として設定すると、ログ バッファはシステム ログ メッセージの一時保存場所として機能します。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場合、新しいメッセージが生成されると古いメッセージは上書きされます。ログ メッセージを保存するには、バッファがいっぱいになるたびにバッファの内容を FTP サーバや内部フラッシュ メモリに保存するよう FWSM を設定して、古いメッセージが上書きされないようにすることができます。

ログ バッファのサイズは、バッファが一杯になる前にバッファに保存できるメッセージの数によって決まります。デフォルトのログ バッファ サイズは 4 KB です。

ログ バッファを出力先としてイネーブルにする場合、保存するメッセージも指定できます。指定しなければ、メッセージの生成時にすべてのメッセージがログ バッファに保存されます。FWSM で保存するメッセージの選択を行うとき、重大度や、カスタム メッセージ リストで指定する基準に基づいて設定することができます。保存するメッセージの制限の詳細については、「出力先に送信するシステム ログ メッセージのフィルタリング」（p.23-19）を参照してください。

出力先としてのログ バッファのイネーブル化

ログの出力先としてログ バッファをイネーブルにし、オプションのログ バッファ設定値を設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、FWSM でのシステム ログ メッセージのログ バッファへの保存をイネーブルにし、ログ バッファに保存するメッセージを指定します。

```
hostname(config)# logging buffered {level | message_list}
```

level は保存するメッセージの重大度、*message_list* はログ バッファに保存するメッセージを選択するために使用するカスタム リストの名前です。

level オプションには、数値（3 など）または名前（error など）で重大度を指定します。どちらを指定しても、その重大度以上のメッセージが選択されます。つまり、重大度 3 を選択した場合、重大度が 3、2、1 のメッセージがログ バッファに保存されます。

たとえば、重大度が 1 と 2 のメッセージをログ バッファに保存するよう指定するには、次のいずれかのコマンドを入力します。

```
hostname(config)# logging buffered critical
```

または

```
hostname(config)# logging buffered level 2
```

message_list オプションには、ログ バッファに保存するメッセージの選択基準を記述したメッセージ リストの名前を指定します。

```
hostname(config)# logging buffered notif-list
```

logging list コマンドを使用してカスタム メッセージ リストを作成することができます。カスタム メッセージ リストの作成方法の詳細については、「カスタム メッセージ リストによるシステム ログ メッセージのフィルタリング」（p.23-21）を参照してください。

ステップ 2　（任意）次のコマンドを入力して、ログ バッファのサイズを変更します。

```
hostname(config)# logging buffer-size bytes
```

bytes オプションにはログ バッファに使用するメモリの容量（バイト単位）を設定します。たとえば、8192 と指定すると、FWSM はログ バッファに 8 KB のメモリを使用します。

次に、FWSM でログ バッファに 16 KB のメモリを使用するよう指定する例を示します。

```
hostname(config)# logging buffer-size 16384
```

ログ バッファがいっぱいになった場合の動作の指定

この設定を行わない場合、FWSM はメッセージを連続的にログ バッファに記録し、バッファがいっぱいになると古いメッセージは上書きされます。ログの履歴が必要な場合、バッファがいっぱいになるたびにバッファの内容を別の出力先に送信するよう FWSM を設定できます。バッファの内容は、内部フラッシュ メモリまたは FTP サーバに保存できます。

バッファの内容を別の場所に保存するとき、FWSM は次のようなデフォルトのタイムスタンプ フォーマットを使用した名前でログ 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、*HHMMSS* は時刻（時、分、秒）です。

FWSM は、ログ バッファの内容を内部フラッシュ メモリまたは FTP サーバに書き込んでいる間も、ログ バッファへの新しいメッセージの保存を続行します。

バッファがいっぱいになるたびにログ バッファのメッセージを内部フラッシュ メモリに保存するよう指定するには、次のコマンドを入力します。

```
hostname(config)# logging flash-bufferwrap
```

バッファがいっぱいになるたびにログ バッファのメッセージを FTP サーバに保存するよう指定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、バッファがいっぱいになるたびにログ バッファの内容を FTP サーバに送信する FWSM の機能をイネーブルにします。

```
hostname(config)# logging ftp-bufferwrap
```

ステップ 2　次のコマンドを入力して、FTP サーバの詳細を指定します。

```
hostname(config)# logging ftp-server {server_address | server_hostname} path username
password
```

ここで

server_address ― 外部 FTP サーバの IP アドレスを指定します。

server_hostname ― 外部 FTP サーバのホスト名を指定します。

path ― ログ バッファ データを保存する FTP サーバのディレクトリ パスを指定します。このパスは FTP の root ディレクトリへの相対パスです。例：`/security_appliances/syslogs/appliance107`

username ― FTP サーバにログインできるユーザ名を指定します。

password ― 指定したユーザ名のパスワードを指定します。

次に、サーバ名に「logserver-352」、パスに「/syslogs」、ユーザ名に「logsupervisor」、パスワードに「1luvMy10gs」を指定するコマンドの例を示します。

```
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
```

内部フラッシュ メモリへのログ バッファの内容の保存

バッファの内容は、いつでも内部フラッシュ メモリに保存できます。ログ バッファの現在の内容を内部フラッシュ メモリに保存するには、次のコマンドを入力します。

```
hostname(config)# logging savelog [savefile]
```

次に、ログ バッファの現在の内容を「latest-logfile.txt」という名前で内部フラッシュ メモリに保存する例を示します。

```
hostname(config)# logging savelog latest-logfile.txt
```

ログ バッファの内容の消去

ログ バッファの内容を消去するには、次のコマンドを入力します。

```
hostname(config)# clear logging buffer
```

出力先に送信するシステム ログ メッセージのフィルタリング

ここでは、特定の出力先へ送信するシステム ログ メッセージを指定する方法について説明します。内容は次のとおりです。

- メッセージのフィルタリングの概要（p.23-19）
- クラスによるシステム ログ メッセージのフィルタリング（p.23-19）
- カスタム メッセージ リストによるシステム ログ メッセージのフィルタリング（p.23-21）

メッセージのフィルタリングの概要

特定の出力先に特定のシステム ログ メッセージだけが送信されるように、生成されたシステム ログ メッセージをフィルタリングすることができます。たとえば、ある出力先にすべてのシステム ログ メッセージを送信し、別の出力先にはシステム ログ メッセージのサブセットを送信するように FWSM を設定できます。

特に、システム ログ メッセージが 1 つの出力先に送信されるように、FWSM で次の項目を設定します。

- システム ログ メッセージの ID 番号
- システム ログ メッセージの重大度
- システム ログ メッセージのクラス（FWSM の機能領域に相当）
- 作成するシステム ログ メッセージ リスト

たとえば、重大度が 1、2、3 のシステム ログ メッセージをすべて内部ログ バッファに送信したり、クラスが「ha」のシステム ログ メッセージをすべて特定の Syslog サーバに送信したり、「high-priority」という名前のメッセージ リストを作成して、問題をシステム管理者に通知するために電子メール アドレスに送信したりするように FWSM を設定することができます。

クラスによるシステム ログ メッセージのフィルタリング

システム ログ メッセージのクラスを使用して、FWSM の機能に相当するタイプごとに、システム ログ メッセージを分類することができます。たとえば、「vpnc」クラスは VPN クライアントを示します。

ロギング クラスでは、1 つのコマンドでシステム ログ メッセージのカテゴリ全体の出力先を指定できます。

システム メッセージ クラスは、2 通りの方法で使用できます。

- **logging class** コマンドを発行して、システム ログ メッセージのカテゴリ全体の出力先を指定します。
- システム ログ メッセージのカスタム リストの作成時に *message_class* 変数を使用して、システム ログ メッセージのクラス全体をカスタム リストに含めます。

特定のクラス内のシステム ログ メッセージはすべて、システム ログ メッセージ ID 番号の先頭 3 桁が同じになります。たとえば、611 で始まるシステム ログ メッセージ ID はすべて、vpnc（VPN クライアント）クラスに関連しています。VPN クライアント機能に関連するシステム ログ メッセージは、611,101 ～ 611,323 です。

指定の出力先へのクラス内の全メッセージの送信

設定した出力先にシステム ログ メッセージ クラス全体を送信するよう FWSM を設定するには、次のコマンドを入力します。

```
hostname(config)# logging class message_class {buffered | console | history | mail |
monitor | trap} [severity_level]
```

ここで

message_class — 指定の出力先に送信するシステム ログ メッセージのクラスを指定します。システム ログ メッセージ クラスの一覧については、表 23-2 を参照してください。

buffered | console | history | mail | monitor | trap — このクラスのシステム ログ メッセージを送信する出力先を指定します。コマンド ライン エントリごとに出力先を 1 つ指定してください。クラスを複数の出力先に送信するよう指定する場合は、出力先ごとに個別にコマンドを入力します。

severity_level — 重大度を指定することにより、出力先に送信するシステム ログ メッセージをさらに制限します。メッセージの重大度の詳細については、重大度（p.23-28）を参照してください。

次に、クラス「ha」（ハイ アベイラビリティ：フェールオーバーともいう）に関する重大度が 1（警告）のシステム ログ メッセージをすべて内部ロギング バッファに送信するよう指定する例を示します。

```
hostname(config)# logging ha buffered alerts
hostname(config)#
```

表 23-2 に、システム ログ メッセージのクラスと、各クラスに関連するシステム ログ メッセージ ID の範囲を示します。

表 23-2　システム ログ メッセージのクラスおよび関連するメッセージ ID 番号

クラス	定義	システム ログ メッセージの ID 番号
ha	フェールオーバー（ハイ アベイラビリティ）	101、102、103、104、210、311、709
rip	RIP ルーティング	107、312
auth	ユーザ認証	109、113
bridge	透過ファイアウォール	110、220
config	コマンド インターフェイス	111、112、208、308
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711
session	ユーザ セッション	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
ip	IP スタック	209、215、313、317、408
snmp	SNMP	212
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPSec	316、320、402、404、501、602、702、713、714、715
ospf	OSPF ルーティング	318、409、503、613
np	ネットワーク プロセッサ	319
rm	リソース マネージャ	321
ids	Intrusion Detection System（IDS; 侵入検知システム）	400、401、415
vpnc	VPN クライアント	611

表 23-2　システム ログ メッセージのクラスおよび関連するメッセージ ID 番号（続き）

クラス	定義	システム ログ メッセージの ID 番号
ca	PKI 認定機関	717
電子メール	電子メール プロキシ	719
vpnlb	VPN 負荷分散	718
vpnfo	VPN フェールオーバー	720

カスタム メッセージ リストによるシステム ログ メッセージのフィルタリング

カスタム メッセージ リストを作成すると、出力先に送信するシステム ログ メッセージの管理を柔軟に行えます。カスタム システム ログ メッセージ リストでは、基準の一部または全部を使用して、システム ログ メッセージのグループを指定します。基準となるのは、重大度、メッセージ ID、システム メッセージ ID の範囲、メッセージ クラスです。

たとえば、メッセージ リストを使用して次のことができます。

- 重大度が 1 および 2 のシステム ログ メッセージを選択して 1 つまたは複数の電子メール アドレスに送信
- メッセージ クラス（「ha」など）に関連するシステム ログ メッセージを選択して内部バッファに保存

メッセージ リストには、メッセージ選択の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。メッセージ選択基準が重複するメッセージ リストを作成することも可能です。メッセージ リストの 2 つの基準によって同一のメッセージが選択される場合でも、メッセージのロギングは 1 回しか行われません。

（注） システム ログ メッセージ リストの名前として重大度の名前を使用しないでください。使用が禁止された *message_list* の名前には、「emergencies」、「alert」、「critical」、「error」、「warning」、「notification」、「informational」、および「debugging」があります。また、ファイル名の最初に、これらの用語の最初の 3 文字を使用しないでください。たとえば、「err」という文字で始まるファイル名を使用しないでください。

ログ バッファに保存するメッセージを選択するために FWSM が使用するカスタム リストを作成する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、メッセージ選択基準を含むメッセージ リストを作成します。

```
hostname(config)# logging list {message_list | [severity_level | message_class |
message_ID | range_of_IDs]}
```

ここで

message_list ― メッセージ選択基準を含むリストの名前を指定します。

severity_level ― 指定した重大度のメッセージをすべてログ バッファに保存するよう指定します。

message_class ― 指定したメッセージ クラスに関連するメッセージをすべてログ バッファに保存するよう指定します。

message_ID ― 個々のシステム ログ メッセージ ID 番号を指定します。

range_of_IDs — メッセージ ID 番号の範囲（例：103401-103599）を指定します。

次に、重大度が 3 以上のメッセージをログ バッファに保存するよう指定する、「notif-list」という名前のメッセージ リストを作成する例を示します。

```
hostname(config)# logging list notif-list level 3
```

ステップ 2　（任意）リストにさらにメッセージ選択基準を追加する場合は、前の手順と同じコマンドを入力して、既存のメッセージ リストの名前と追加する基準を指定します。リストに追加する基準ごとに、個別にコマンドを入力します。

次に、メッセージ リストに基準を追加する例を示します。追加する基準は、メッセージ ID 番号の範囲、およびメッセージ クラス「ha」（ハイ アベイラビリティ：フェールオーバー）です。メッセージ クラスの詳細については、「クラスによるシステム ログ メッセージのフィルタリング」（p.23-19）を参照してください。

```
hostname(config)# logging list notif-list 104024-105999
hostname(config)# logging list my-list level critical
hostname(config)# logging list notif-list class ha
(config)# logging list my-list level warning class vpn
```

上記の例では、指定した基準に一致するシステム ログ メッセージがログ バッファに送信されます。リストに含めるためのシステム ログ メッセージの基準は、次のとおりです。

- 範囲が 100100 ～ 100110 のシステム ログ メッセージ ID
- 重大度が critical レベル以上のすべてのシステム ログ メッセージ（emergency、alert、または critical）
- 重大度が warning レベル以上のすべての VPN クラスのシステム ログ メッセージ（emergency、alert、critical、error、または warning）

これらの条件のいずれかを満たしたシステム ログ メッセージがロギングされます。1 つのシステム ログが複数の条件を満たしている場合でも、メッセージのロギングは 1 回しか行われません。

ログ設定のカスタマイズ

ここでは、ロギング設定を微調整するためのオプションについて説明します。内容は次のとおりです。

- ロギング キューの設定（p.23-22）
- システム ログ メッセージへの日付および時刻の記載（p.23-23）
- システム ログ メッセージへの装置 ID の記載（p.23-23）
- EMBLEM フォーマットのシステム ログ メッセージの生成（p.23-24）
- システム ログ メッセージのディセーブル化（p.23-24）
- システム ログ メッセージの重大度の変更（p.23-25）
- ログに使用する内部フラッシュ メモリの容量の変更（p.23-26）

ロギング キューの設定

セキュリティ アプライアンスには、指定の出力先への送信を待つ間、システム ログ メッセージをバッファリングしておくためのメモリの固定ブロックがあります。必要なブロック数は、システム ログ メッセージ キューの長さと、指定された Syslog サーバの数によって決まります。

指定された出力先に送信する前に FWSM がキューに保持できるシステム ログ メッセージの数を指定するには、次のコマンドを入力します。

```
hostname(config)# logging queue message_count
```

message_count 変数には、処理待ちのシステム ログ メッセージをシステム ログ メッセージ キューに保持する数を指定します。デフォルトは 512 システム ログ メッセージです。0（ゼロ）を設定すると、システム ログ メッセージの数は無制限になります。つまり、キュー サイズの制約が、利用可能なブロック メモリのみとなります。

キューおよびキュー統計情報を表示するには、次のコマンドを入力します。

```
hostname(config)# show logging queue
```

システム ログ メッセージへの日付および時刻の記載

システム ログ メッセージの生成日時をシステム ログ メッセージに記載するように指定するには、次のコマンドを入力します。

```
hostname(config)# logging timestamp
```

システム ログ メッセージへの装置 ID の記載

非 EMBLEM フォーマットのシステム ログ メッセージに装置 ID を記載するように FWSM を設定するには、次のコマンドを入力します。

```
hostname(config)# logging device-id {context-name | hostname | ipaddress interface_name
| string text}
```

ここで

context-name — 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 モードで動作している FWSM にのみ適用されます）。

hostname — FWSM のホスト名を装置 ID として使用するよう指定します。

ipaddress *interface_name* — *interface_name* に指定したインターフェイスの IP アドレスを装置 ID として使用するよう指定します。

ipaddress オプションを使用すると、システム ログ メッセージの送信元のインターフェイスに関係なく、その装置 ID が指定された FWSM のインターフェイス IP アドレスになります。このキーワードが、装置から送信されるすべてのシステム ログ メッセージのための統一された装置 ID になります。

string *text* — *text* オプションに入力された文字を装置 ID として使用するよう指定します。文字列は 16 文字まで入力可能です。*text* には、スペースと以下の文字は使用できません。

- &（アンパサンド）
- '（一重引用符）
- "（二重引用符）
- <（より小さい）
- >（より大きい）
- ?（クエスチョン マーク）

（注）イネーブルにすると、装置 ID は EMBLEM フォーマットのシステム ログ メッセージや SNMP トラップに表示されません。

次に、FWSM のロギング装置 ID をイネーブルにする例を示します。

```
hostname(config)# logging device-id hostname
```

次に、FWSM のセキュリティ コンテキストのロギング装置 ID をイネーブルにする例を示します。

```
hostname(config)# logging device-id context-name
```

マルチコンテキスト モードで admin コンテキストのロギング装置 ID をイネーブルにすると、システム実行スペースで生成されたメッセージには「**system**」という装置 ID が使用され、admin コンテキストで生成されたメッセージには装置 ID として admin コンテキスト名が使用されます。

EMBLEM フォーマットのシステム ログ メッセージの生成

Syslog サーバ以外の出力先に送信するシステム ログ メッセージに EMBLEM フォーマットを使用するには、次のコマンドを入力します。

```
hostname(config)# logging emblem
```

UDP 経由で Syslog サーバに送信されるシステム ログ メッセージに EMBLEM フォーマットを使用するには、Syslog サーバを出力先として設定するときに **format emblem** オプションを指定します。次のコマンドを入力します。

```
hostname(config)# logging host interface_name ip_address {tcp[/port] | udp[/port]}
[format emblem]
```

ここで

interface_name および *IP_address* にはシステム ログ メッセージを受信する Syslog サーバを指定します。**tcp**[/*port*] および **udp**[/*port*] は使用するプロトコルとポートを示します。**format emblem** は、Syslog サーバに送信するメッセージに対して EMBLEM フォーマットをイネーブルにします。

セキュリティ アプライアンスでは、システム ログ メッセージの送信に UDP および TCP プロトコルを使用できますが、EMBLEM フォーマットをイネーブルにできるのは、UDP 経由で送信されるメッセージのみです。デフォルトのプロトコルおよびポートは、UDP/514 です。

次に例を示します。

```
hostname(config)# logging host interface_1 122.243.006.123 udp format emblem
```

システム ログ メッセージのディセーブル化

FWSM で特定のシステム ログ メッセージが生成されないようにするには、次のコマンドを入力します。

```
hostname(config)# no logging message message_number
hostname(config)#
```

次に例を示します。

```
hostname(config)# no logging message 113019
hostname(config)#
```

ディセーブルにしたシステム ログ メッセージを再度イネーブルにするには、次のコマンドを入力します。

```
hostname(config)# logging message message_number
```

次に例を示します。

```
hostname(config)# logging message 113019
hostname(config)#
```

ディセーブルにしたシステム ログ メッセージのリストを表示するには、次のコマンドを入力します。

```
hostname(config)# show logging message
```

ディセーブルにしたすべてのシステム ログ メッセージのロギングを再度イネーブルにするには、次のコマンドを入力します。

```
hostname(config)# clear config logging disabled
```

システム ログ メッセージの重大度の変更

システム ログ メッセージのロギング レベルを指定するには、次のコマンドを入力します。

```
hostname(config)# logging message message_ID level severity_level
```

次に、システム ログ メッセージ ID 113019 の重大度を 4（warnings）から 5（notifications）に変更する例を示します。

```
hostname(config)# logging message 113019 level 5
hostname(config)#
```

システム ログ メッセージのロギング レベルをデフォルトのレベルに戻すには、次のコマンドを入力します。

```
hostname(config)# logging message message_ID level severity_level
```

次に、システム ログ メッセージ ID 113019 の重大度をデフォルトの 4（warnings）に戻す例を示します。

```
hostname(config)# no logging message 113019 level 5
hostname(config)#
```

重大度が変更されたシステム ログ メッセージのリストを表示するには、次のコマンドを入力します。

```
hostname(config)# show logging message
```

変更したすべてのシステム ログ メッセージの重大度をデフォルトに戻すには、次のコマンドを入力します。

```
hostname(config)# clear config logging level
hostname(config)#
```

次の例の一連のコマンドは、**logging message** コマンドにより、システム ログ メッセージのイネーブル化と、システム ログ メッセージの重大度の両方を制御する方法を示しています。

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

ログに使用する内部フラッシュ メモリの容量の変更

ログ バッファの現在の内容を内部フラッシュ メモリに保存するよう FWSM を設定するには、次の 2 つの方法があります。

- バッファがいっぱいになるたびにログ バッファの内容が内部フラッシュ メモリに保存されるようロギングを設定する。
- コマンドを入力して、ログ バッファの現在の内容をただちに内部フラッシュ メモリに保存するよう FWSM に指示する。

デフォルトでは、FWSM はログ データ用に最大 1 MB の内部フラッシュ メモリを使用できます。FWSM でのログ データの保存のために解放する必要がある内部フラッシュ メモリのデフォルトの最低容量は、3 MB です。

内部フラッシュ メモリへのログ ファイルの保存により、内部フラッシュ メモリの空き容量が、設定された最低限度を下回ると、新しいログ ファイルを保存しても最低限のメモリの空き容量が確保されるよう、FWSM は古いログ ファイルを削除します。削除するファイルがない場合、または古いファイルをすべて削除しても空き容量が最低限度以上にならない場合は、FWSM は新しいログ ファイルを保存できません。

ログに利用できる内部フラッシュ メモリの容量の設定を変更する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、ログ ファイルの保存に利用できる内部フラッシュ メモリの最大容量を指定します。

```
hostname(config)# logging flash-maximum-allocation kbytes
```

kbytes は、ログ ファイルの保存に使用可能な内部フラッシュ メモリの最大容量（KB 単位）です。

次に、ログ ファイルのために使用できる内部フラッシュ メモリの最大容量を約 1.2 MB に設定する例を示します。

```
hostname(config)# logging flash-maximum-allocation 1200
```

ステップ 2　次のコマンドを入力して、FWSM でのログ ファイルの保存のために解放する必要がある内部フラッシュ メモリの最低容量を指定します。

```
hostname(config)# logging flash-minimum-free kbytes
```

kbytes には、FWSM で新しいログ ファイルを保存するために空いている必要のある内部フラッシュ メモリの最低容量（KB 単位）を指定します。

次に、FWSM で新しいログ ファイルを保存するために内部フラッシュ メモリに 4000 KB の最低空き容量が必要であるという指定を行う例を示します。

```
hostname(config)# logging flash-minimum-free 4000
```

システム ログ メッセージの内容

ここでは、FWSM で生成されるシステム ログ メッセージの内容について説明します。内容は次のとおりです。

- システム ログ メッセージのフォーマット（p.23-27）
- 重大度（p.23-28）
- システム ログ メッセージで使用される変数（p.23-28）
- logging コマンドのリスト（p.23-31）

システム ログ メッセージのフォーマット

システム ログ メッセージは、パーセント記号（%）で始まり、構成内容は次のとおりです。

```
%FWSM Level Message_number: Message_text
```

フィールドの内容は次のとおりです。

FWSM	セキュリティ アプライアンスで生成されるメッセージのシステム ログ メッセージ ファシリティ コードを示します。この値は常に FWSM です。
Level	1 ～ 7。レベルは、システム ログ メッセージで記述される状態の重大度に対応します。値が小さいほど、重大な状況です。詳細については、表 23-3 を参照してください。
Message_number	システム ログ メッセージを示す 6 桁の一意の数値
Message_text	状態を説明する文字列。システム ログ メッセージのこの部分には、IP アドレス、ポート番号、ユーザ名が含まれることがあります。表 23-4 に、変数フィールドとその情報のタイプを示します。

重大度

表 23-3 に、システム ログ メッセージの重大度を示します。

表 23-3　システム ログ メッセージの重大度

レベル番号	レベル キーワード	説明
0	**emergencies**	システム使用不能
1	**alert**	早急に処置が必要
2	**critical**	クリティカル状態
3	**error**	エラー状態
4	**warning**	警告状態
5	**notification**	正常だが注意が必要な状態
6	**informational**	情報メッセージ
7	**debugging**	デバッグ中のみ表示

(注) FWSM は、重大度 0（emergencies）のシステム ログ メッセージは生成しません。このレベルは、UNIX システム ログ機能との互換性のために **logging** コマンドで提供されますが、セキュリティ アプライアンスでは使用されません。

システム ログ メッセージで使用される変数

システム ログ メッセージでは、よく変数が使用されます。表 23-4 に、システム ログ メッセージの説明のためにこのガイドで使用する変数を示します。1 つのシステム ログ メッセージでしか使用しない変数は、このリストに示していません。

表 23-4　システム ログ メッセージの変数フィールド

変数	情報のタイプ
acl_ID	ACL の名前
bytes	バイト数
code	システム ログ メッセージから返される、エラー原因またはエラー発生源（システム ログ メッセージによって異なる）を示す 10 進数
command	コマンド名
command_modifier	*command_modifier* は、次のいずれかの文字列です。 • cmd（この文字列の場合、コマンドに修飾子はありません） • clear • no • show
connections	接続数

表 23-4　システム ログ メッセージの変数フィールド（続き）

変数	情報のタイプ
connection_type	接続タイプ： • SIGNALLING UDP • SIGNALLING TCP • SUBSCRIBE UDP • SUBSCRIBE TCP • UDP 経由 • ルート • RTP • RTCP
dec	10 進数
dest_address	パケットの宛先アドレス
dest_port	宛先ポート番号
device	メモリ ストレージ装置。フロッピー ディスク、内部フラッシュ メモリ、TFTP、フェールオーバー スタンバイ ユニット、コンソール端末など
econns	初期接続の数
elimit	**static** または **nat** コマンドで指定された初期接続の数
filename	タイプ セキュリティ アプライアンス イメージ、ASDM ファイル、コンフィギュレーションのファイル名
ftp-server	外部 FTP サーバの名前または IP アドレス
gateway_address	ネットワーク ゲートウェイの IP アドレス
global_address	グローバル IP アドレス、セキュリティ レベルの低いインターフェイスのアドレス
global_port	グローバル ポート番号
hex	16 進数
inside_address	内部（ローカル）IP アドレス、セキュリティ レベルの高いインターフェイスのアドレス
inside_port	内部ポート番号
interface_name	インターフェイスの名前
IP_address	*n.n.n.n* 形式の IP アドレス。*n* は 1 ～ 255 の整数
MAC_address	MAC アドレス
mapped_address	変換された IP アドレス
mapped_port	変換されたポート番号
message_class	FWSM の機能領域に対応付けられたシステム ログ メッセージのカテゴリ
message_list	システム ログ メッセージの ID 番号、クラス、重大度などを記述した、ユーザが作成するファイルの名前
message_number	システム ログ メッセージの ID
nconns	スタティックまたは xlate テーブルに許可された接続の数
netmask	サブネット マスク
number	数値。形式はシステム ログ メッセージによって異なります。
octal	8 進数
outside_address	外部 IP アドレス。外部ルータを越えたネットワークの、通常はセキュリティ レベルの低いインターフェイス上に存在する Syslog サーバのアドレス

表 23-4　システム ログ メッセージの変数フィールド（続き）

変数	情報のタイプ
outside_port	外部ポート番号
port	TCP または UDP のポート番号
privilege_level	ユーザの権限レベル
protocol	パケットのプロトコル。ICMP、TCP、UDP など
real_address	Network Address Translation（NAT; ネットワーク アドレス変換）前の実際の IP アドレス
real_port	NAT の前の実際のポート番号
reason	システム ログ メッセージの理由を説明する文字列
service	パケットによって指定されるサービス。SNMP、Telnet など
severity_level	システム ログ メッセージの重大度
source_address	パケットの送信元アドレス
source_port	送信元ポート番号
string	文字列（ユーザ名など）
tcp_flags	TCP ヘッダーのフラグ • ACK • FIN • PSH • RST • SYN • URG
time	*hh*:*mm*:*ss* の形式の期間
url	URL
user	ユーザ名

logging コマンドのリスト

ここでは、システム ロギングの設定とモニタリングのために FWSM で利用できる logging コマンドのリストを紹介し、各コマンドを簡単に説明します。各コマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

表 23-5 に、FWSM でシステム ロギングの設定とモニタリングのために利用できるコマンドの一覧を示します。

表 23-5　logging コマンドのリスト

コマンド	説明
clear configure logging	ロギング コンフィギュレーションの設定をデフォルト値に戻します。
clear logging asdm	ASDM ログ バッファからすべてのシステム ログ メッセージを削除します。
clear logging buffer	システム ログ バッファからすべてのシステム ログ メッセージを削除します。
clear running-config logging rate-limit	ロギング レート リミットをデフォルトに戻します。
logging asdm	システム ログ メッセージの一部またはすべてを ASDM に送信するよう FWSM を設定します。
logging asdm-buffer-size	ASDM に送信されるのを待っているメッセージを格納しておくためのバッファのサイズを設定します。
logging buffered	システム ログ メッセージの一部またはすべてをシステム ログ バッファに保存するよう FWSM を設定します。
logging buffer-size	システム メッセージを格納しておくためのバッファのサイズを設定します。
logging class	指定したメッセージ クラスのすべてのメッセージが指定の出力先に送信されるよう指定します。
logging console	FWSM のコンソール セッション中にシステム ログ メッセージが表示されるようにします。
logging debug trace	デバッギング メッセージがシステム ログに保存されるようにします。
logging device-id	非 EMBLEM フォーマットのシステム ログ メッセージに装置 ID を記載するように FWSM を設定します。
logging emblem	Syslog サーバ以外の出力先に送信するシステム ログ メッセージに EMBLEM フォーマットを使用するよう FWSM を設定します。
logging enable	設定された全出力先へのロギングをイネーブルにします。
logging facility	システム メッセージ サーバに送信されるメッセージに使用するロギング ファシリティを指定します。
logging flash-bufferwrap	バッファがいっぱいになるたびにログ バッファの内容が内部フラッシュ メモリに書き込まれるよう FWSM を設定します。
logging flash-maximum-allocation	FWSM がログ データを格納するために使用する内部フラッシュ メモリの最大容量を指定します。
logging flash-minimum-free	FWSM が新しいログ ファイルを保存するために空いている必要のある内部フラッシュ メモリの最低容量を指定します。
logging from-adress	FWSM によって電子メール送信されるシステム ログ メッセージの送信元電子メール アドレスを指定します。
logging ftp-bufferwrap	バッファがいっぱいになるたびにログ バッファの内容が FTP サーバに書き込まれるよう FWSM をイネーブルにします。
logging ftp-server	**logging ftp-bufferwrap** がイネーブルの場合に、FWSM からログ バッファ データを送信される FTP サーバの詳細を指定します。

表 23-5　logging コマンドのリスト（続き）

コマンド	説明
logging history	SNMP ロギングをイネーブルにし、SNMP サーバに送信されるメッセージを指定します。
logging host	ログの出力先として Syslog サーバを定義します。
logging list	特定の出力先に送信するメッセージをフィルタリングするためのメッセージ選択基準のリストを作成または編集します。
logging mail	FWSM から電子メールによってシステム ログ メッセージを送信するようにし、電子メールで送信するメッセージを指定します。
logging message	システム ログ メッセージの重大度の取り消しまたは変更を行います。
logging monitor	SSH および Telnet セッションでシステム ログ メッセージを表示するよう FWSM を設定します。
logging permit-hostdown	動作していない TCP ベースの Syslog サーバに対して、FWSM が新しいネットワーク アクセス セッションを許可するか拒否するかを指定します。
logging queue	設定した出力先に送信するために FWSM がシステム ログ キューに保持できるシステム ログ メッセージの数を指定します。
loggign rate limit	システム メッセージを生成するレートを制限します。
logging recipient-adress	FWSM によって電子メールで送信されるシステム ログ メッセージの受信者の電子メール アドレスを指定します。
logging savelog	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 standby	フェールオーバー スタンバイ FWSM でこの FWSM のシステム ログ メッセージをログ出力先に送信するよう設定します。
logging timestamp	システム ログ メッセージにメッセージの生成日時を記載するよう指定します。
logging trap	FWSM から Syslog サーバに送信するシステム ログ メッセージを指定します。
remote access threshold	FWSM からのトラップの送信先となる、アクティブなリモート アクセス セッションの数を指定します。
show logging	現在のロギング設定と現在のシステム ログ内部バッファの内容を表示します。
show running-config logging	現在使用されているすべてのロギング コンフィギュレーションの設定を表示します。
show running config logging rate-limit	システム メッセージを生成するレートの制限を表示します。

FWSM のトラブルシューティング

この章では、FWSM のトラブルシューティングの手順について説明します。内容は次のとおりです。

- 設定のテスト（p.24-2）
- FWSM のリロード（p.24-7）
- パスワード復旧の実行（p.24-8）
- その他のトラブルシューティング ツール（p.24-10）
- 一般的な問題（p.24-11）

設定のテスト

ここでは、シングルモードの FWSM、または各セキュリティ コンテキストについて、接続テストを行う手順について説明します。FWSM のインターフェイスに ping を実行する方法、および 1 つのインターフェイス上のホストから他のインターフェイス上のホストに ping を実行する方法を示しています。

トラブルシューティングでは、ping およびデバッグに関するメッセージだけをイネーブルにすることを推奨します。FWSM のテストが終了したら、「テスト設定のディセーブル化」（p.24-6）の手順に従ってください。

ここでは、次の内容について説明します。

- ICMP デバッグ メッセージおよびシステム メッセージのイネーブル化（p.24-2）
- FWSM のインターフェイスへの ping の実行（p.24-3）
- FWSM 経由の ping の実行（p.24-5）
- テスト設定のディセーブル化（p.24-6）

ICMP デバッグ メッセージおよびシステム メッセージのイネーブル化

デバッグ メッセージおよびシステム メッセージは、ping が失敗した原因を判別する場合に役立ちます。FWSM には、FWSM のインターフェイスへの ping に関する ICMP デバッグ メッセージだけが表示されます。FWSM 経由で他のホストに宛てた ping のメッセージは表示されません。デバッグ メッセージおよびシステム メッセージをイネーブルにする手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、FWSM のインターフェイスへの ping に関する ICMP パケット情報が表示されるように設定します。

```
hostname(config)# debug icmp trace
```

ステップ 2　次のコマンドを入力して、Telnet または SSH セッションにシステム メッセージが送信されるように設定します。

```
hostname(config)# logging monitor debug
```

または、**logging buffer debug** コマンドを使用してメッセージをバッファに送信し、あとで **show logging** コマンドを使用して表示することもできます。

ステップ 3　次のコマンドを入力して、使用する Telnet または SSH セッションにシステム メッセージが送信されるように設定します。

```
hostname(config)# terminal monitor
```

ステップ 4　次のコマンドを入力して、システム メッセージをイネーブルにします。

```
hostname(config)# logging enable
```

次に、外部ホスト（209.165.201.2）から FWSM の外部インターフェイス（209.165.201.1）への ping に成功した例を示します。

```
hostname(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

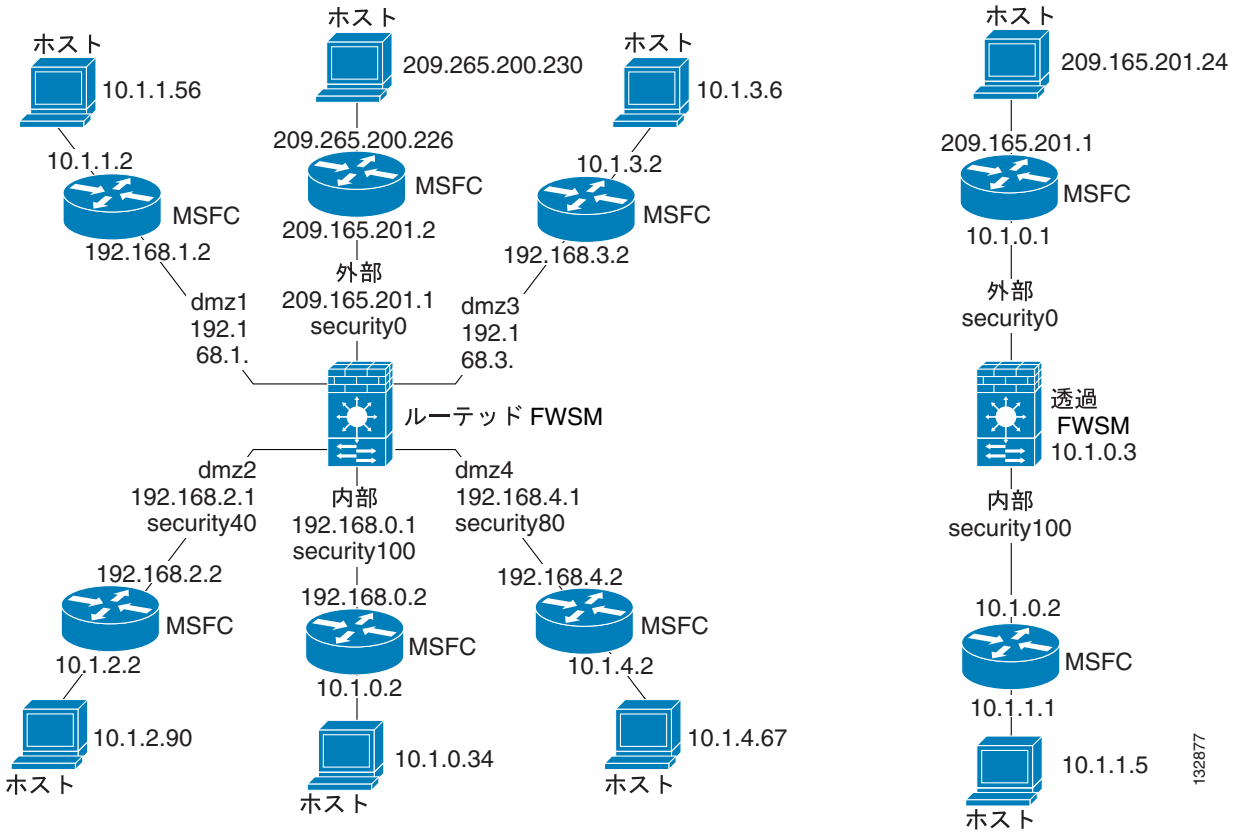
この例には、ICMP パケット長（32 バイト）、ICMP パケット ID（1）、および ICMP シーケンス番号が示されています（ICMP シーケンス番号は 0 から開始され、要求が送信されるごとに増分されます）。

FWSM のインターフェイスへの ping の実行

FWSM のインターフェイスが動作していて実行中であり、FWSM と接続先ルータのルーティングが正しく実行されているかどうかをテストするには、FWSM のインターフェイスに ping を実行します。FWSM のインターフェイスに ping を実行する手順は、次のとおりです。

ステップ 1　シングルモード FWSM、またはインターフェイス名、セキュリティ レベル、および IP アドレスを明記したセキュリティ コンテキストの接続図を作成します。この接続図には、直接接続されたルータ、および FWSM に対して ping を実行するルータの反対側のホストも明記する必要があります。この情報は、ここで説明する手順、および「FWSM 経由の ping の実行」（p.24-5）の手順で使用します。次に例を示します。

図 24-1　インターフェイス、ルータ、およびホストを明記したネットワーク接続図

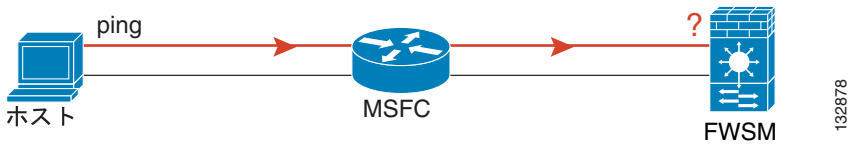


ステップ 2　*直接接続されたルータから* FWSM の各インターフェイスに ping を実行します。透過モードの場合は、管理 IP アドレスに ping を送信します。

このテストによって、FWSM のインターフェイスがアクティブで、VLAN が正しく設定されているかどうかを確認します。

ping に失敗した場合、FWSM のインターフェイスがアクティブでないか、インターフェイスの設定が不正であるか、または FWSM とルータ間のスイッチがダウンしている可能性があります（図 24-2 を参照）。失敗した場合、パケットが到達しないので、FWSM 上にデバッグ メッセージまたはシステム メッセージは表示されません。

図 24-2　FWSM インターフェイスへの ping の失敗

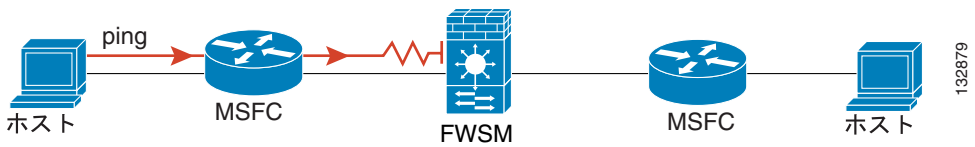


ping が FWSM に到達し、FWSM から応答が返されると、次のようなデバッグ メッセージが表示されます。

```
ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
```

ping 応答がルータに返らない場合、スイッチ ループが発生しているか、または IP アドレスが重複している可能性があります（図 24-3 を参照）。

図 24-3　IP アドレスの重複による ping の失敗



ステップ 3　リモート ホストから FWSM の各インターフェイスに ping を実行します。透過モードの場合は、管理 IP アドレスに ping を送信します。

このテストでは、直接接続されたルータがホストと FWSM 間のパケットをルーティングできること、および FWSM からホストに返されるパケットが正しくルーティングされていることを確認します。

ping に失敗した場合、FWSM に、中継ルータを経由したホストまでのルートが正しく設定されていない可能性があります（図 24-4 を参照）。この場合、ping に成功したことを示すデバッグ メッセージが表示されますが、システム メッセージ 110001 によりルーティング障害が発生していることが示されます。

図 24-4　FWSM のルート未設定による ping の失敗

FWSM 経由の ping の実行

FWSM のインターフェイスへの ping に成功したら、FWSM 経由でトラフィックを正しく転送できるかどうかを確認する必要があります。ルーテッド モードでは、このテストによって、NAT が設定されている場合に正しく実行されるかどうかを確認できます。NAT を使用しない透過モードの場合には、このテストによって FWSM が正しく動作していることを確認します。透過モードで ping に失敗した場合は、Cisco TAC に連絡してください。

異なるインターフェイス上のホスト間で ping を実行する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、任意の送信元ホストからの ICMP を許可するアクセス リストを追加します。

```
hostname(config)# access-list ICMPACL extended permit icmp any any
```

デフォルトでは、ホストがセキュリティの低いインターフェイスにアクセスする場合、すべてのトラフィックが許可されます。ただし、セキュリティの高いインターフェイスにアクセスするには、前述のアクセス リストが必要です。

ステップ 2　次のコマンドを入力して、各送信元インターフェイスにアクセス リストを割り当てます。

```
hostname(config)# access-group ICMPACL in interface interface_name
```

各送信元インターフェイスについて、このコマンドを繰り返します。

ステップ 3　次のコマンドを入力して、ICMP 応答が送信元ホストに戻されるように、ICMP インスペクション エンジンをイネーブルにします。

```
hostname(config)# class-map ICMP-CLASS
hostname(config-cmap)# match access-list ICMPACL
hostname(config-cmap)# policy-map ICMP-POLICY
hostname(config-pmap)# class ICMP-CLASS
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# service-map ICMP-POLICY global
```

または、ICMPACL アクセス リストを宛先インターフェイスに適用して、FWSM 経由で ICMP トラフィックを返すことを許可することもできます。

ステップ 4　送信元インターフェイス上のホストまたはルータから、他のインターフェイス上の他のホストまたはルータに ping を実行します。

確認するインターフェイスの各ペアについて、この手順を繰り返します。

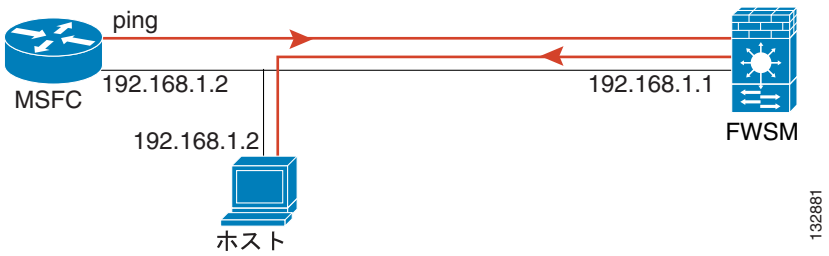
ping に成功すると、ルーテッド モードのアドレス変換を確認するシステム メッセージ（305009 または 305011）、および ICMP 接続が確立されたことを示すメッセージ（302020）が表示されます。**show xlate** コマンドまたは **show conns** コマンドを入力して、この情報を表示することもできます。

透過モードで ping に失敗した場合は、Cisco TAC に連絡してください。

ルーテッド モードで ping に失敗した場合、NAT が正しく設定されていない可能性があります（図 24-5 を参照）。この状況は、NAT 制御をイネーブルにしている場合によく発生します。この場合、NAT 変換に失敗したことを示すシステム メッセージ（305005 または 305006）が表示されます。外部ホストから内部ホストに ping を実行した場合、スタティック変換が設定されていないと（NAT 制御に必要）、メッセージ 106010：deny inbound icmp が表示されます。

（注）　FWSM には、FWSM のインターフェイスへの ping に関する ICMP デバッグ メッセージだけが表示されます。FWSM 経由で他のホストに宛てた ping のメッセージは表示されません。

図 24-5　FWSM のアドレス変換の問題による ping の失敗



テスト設定のディセーブル化

テストが完了したら、FWSM 宛て、または FWSM 経由の ICMP を許可し、デバッグ メッセージを出力するテスト用の設定をディセーブルにします。設定をそのまま有効にしておくと、重大なセキュリティ リスクが生じることがあります。また、デバッグ メッセージを生成すると、FWSM のパフォーマンスが遅くなります。

テスト設定をディセーブルにする手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、ICMP デバッグ メッセージをディセーブルにします。

```
hostname(config)# no debug icmp trace
```

ステップ 2　必要に応じて、次のコマンドを入力して、ロギングをディセーブルにします。

```
hostname(config)# no logging on
```

ステップ 3　次のコマンドを入力して、ICMPACL アクセス リストを削除し、関連する **access-group** コマンドを削除します。

```
hostname(config)# no access-list ICMPACL
```

ステップ 4　（任意）ICMP インスペクション エンジンをディセーブルにする場合には、次のコマンドを入力します。

```
hostname(config)# no service-map ICMP-POLICY
```

FWSM のリロード

マルチモードでは、システム実行スペースからのみリロードできます。次のコマンドを入力して、FWSM をリロードします。

```
hostname# reload
```

パスワード復旧の実行

ここでは、パスワードを忘れた場合、または AAA 設定が原因でロックアウトされた場合の回復手順について説明します。

- アプリケーション パーティションのパスワードおよび AAA 設定の消去（p.24-8）
- メンテナンス パーティション パスワードのリセット（p.24-9）

アプリケーション パーティションのパスワードおよび AAA 設定の消去

パスワードを忘れた場合、または AAA（認証、許可、アカウンティング）設定によってロックアウトされた場合には、パスワードおよび AAA コンフィギュレーションの一部をデフォルト値にリセットできます。この手順を実行するには、メンテナンス パーティションにログインする必要があります。

ステップ 1　スイッチのプロンプトで次のコマンドを入力して、現在のアプリケーション ブート パーティションを確認します。

```
Router# show boot device [mod_num]
```

モジュールのブート パーティションが、cf:4 または cf:5 として出力されます。このあとの手順で、パスワードを消去するブート パーティションを指定します。

ステップ 2　次のコマンドを入力して、FWSM をメンテナンス パーティションで起動します。

```
Router# hw-module module mod_num reset cf:1
```

ステップ 3　次のコマンドを入力して、FWSM とのセッションを開始します。

```
Router# session slot mod_num processor 1
```

ステップ 4　次のコマンドを入力して、メンテナンス パーティションに root としてログインします。

```
Login: root
```

ステップ 5　プロンプトにパスワードを入力します。

```
Password: password
```

デフォルトのパスワードは「cisco」です。

ステップ 6　次のコマンドを入力して、ログイン パスワード、イネーブル パスワード、**aaa authentication console** コマンド、および **aaa authorization command** コマンドを消去します。

```
root@localhost# clear passwd cf:{4 | 5}
```

パスワードを消去するブート パーティションを指定します。FWSM はデフォルトで、**cf:4** から起動します。ブート パーティションの表示方法の詳細については、ステップ 1 を参照してください。

ステップ 7　次のように、画面のプロンプトに従って入力します。

```
Do you wish to erase the passwords? [yn] y
The following lines will be removed from the configuration:
        enable password 8Ry2YjIyt7RRXU24 encrypted
        passwd 2KFQnbNIdI.2KYOU encrypted
Do you want to remove the commands listed above from the configuration?
[yn] y
Passwords and aaa commands have been erased.
```

メンテナンス パーティション パスワードのリセット

メンテナンス パーティションのパスワードを忘れた場合は、デフォルト値にリセットできます。この場合、アプリケーション パーティションにログインしている必要があります。マルチモードでは、システム実行スペースからのみ、パスワードをリセットできます。

メンテナンス パスワードをリセットするには、次のコマンドを入力します。

```
hostname# clear mp-passwd
```

その他のトラブルシューティング ツール

FWSM には、Cisco TAC から支援を受けるときに役立つ、他のトラブルシューティング ツールが提供されています。

- デバッグ メッセージの表示（p.24-10）
- パケットのキャプチャ（p.24-10）
- クラッシュ ダンプの表示（p.24-10）

デバッグ メッセージの表示

デバッグ出力には、CPU 処理の中で高いプライオリティが割り当てられるため、システム性能が低下することがあります。このため、**debug** コマンドは、特別な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 セッション中以外は使用しないでください。また、**debug** コマンドの実行は、使用中のユーザが少なく、ネットワーク トラフィックが少ないときに行うようにしてください。こうすることにより、デバッグ コマンドの処理のオーバーヘッドによって被る影響が少なくなります。デバッグ メッセージをイネーブルにするときは、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **debug** コマンドの説明を参照してください。

パケットのキャプチャ

接続に関する問題のトラブルシューティングを行ったり、不審な動作をモニタしたりする場合には、パケットのキャプチャが役立つことがあります。FWSM では、管理トラフィックおよびインスペクション エンジンを含め、汎用プロセッサを通過するトラフィックのパケット情報を追跡できます。（多くの転送トラフィックのように）ネットワーク プロセッサを通過するトラフィックを、FWSM でキャプチャすることはできません。パケット キャプチャ機能を使用する場合には、テクニカルサポートに連絡することを推奨します。『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **capture** コマンドの説明を参照してください。

クラッシュ ダンプの表示

FWSM がクラッシュした場合には、クラッシュ ダンプ情報を表示できます。クラッシュ ダンプを解釈する際には、Cisco TAC に連絡することを推奨します。『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **show crashdump** コマンドの説明を参照してください。

一般的な問題

ここでは、FWSM の一般的な問題と、解決方法について説明します。

現象　スイッチの CLI から FWSM をリセットすると、システムが常にメンテナンス パーティションで起動される。

考えられる原因　デフォルトのブート パーティションが cf:1 に設定されています。

推奨処置　「デフォルト ブート パーティションの設定」（p.2-14）の説明に従って、デフォルトのブート パーティションを変更します。

現象　アプリケーション パーティションと同じパスワードでメンテナンス パーティションにログインできない。

考えられる原因　アプリケーション パーティションとメンテナンス パーティションのパスワード データベースが異なっています。

推奨処置　パーティションに対応するパスワードを使用します。詳細については、「パスワードの変更」（p.7-2）を参照してください。

現象　トラフィックが FWSM を通過しない。

考えられる原因　VLAN がスイッチに設定されていないか、FWSM に割り当てられていません。

推奨処置　VLAN を設定し、「Firewall Services Module への VLAN 割り当て」（p.2-4）の説明に従って、FWSM に VLAN を割り当てます。

現象　コンテキスト内で VLAN インターフェイスを設定できない。

考えられる原因　その VLAN はコンテキストに割り当てられていません。

推奨処置　「セキュリティ コンテキストの設定」（p.4-20）の説明に従って、コンテキストに VLAN を割り当てます。

現象　MSFC に複数の Switched Virtual Interface（SVI）を追加できない。

考えられる原因　複数の SVI がイネーブルに設定されていません。

推奨処置　「MSFC への SVI の追加」（p.2-7）の説明に従って、複数の SVI をイネーブルにします。

現象　FWSM のインターフェイスに Telnet または SSH（セキュア シェル）で接続できない。

考えられる原因　FWSM への Telnet 接続または SSH 接続がイネーブルに設定されていません。

推奨処置　「Telnet アクセスの許可」（p.21-2）または「SSH アクセスの許可」（p.21-3）の説明に従って、FWSM への Telnet 接続または SSH 接続をイネーブルにします。

現象　FWSM のインターフェイスに ping を実行できない。

考えられる原因　FWSM への ICMP がイネーブルに設定されていません。

推奨処置　「FWSM との ICMP 送受信の許可」（p.21-12）の説明に従って、FWSM への ICMP をイネーブルにします。

現象　アクセス リストで許可されているのに、FWSM から ping を実行できない。

考えられる原因　ICMP インスペクション エンジンがイネーブルに設定されていないか、送信元インターフェイスおよび宛先インターフェイスの両方にアクセス リストが適用されていません。

推奨処置　ICMP はコネクションレス型プロトコルなので、FWSM は戻りトラフィックを自動的には許可しません。応答トラフィックを許可するには、送信元インターフェイスだけでなく宛先インターフェイスにもアクセス リストを適用するか、または ICMP インスペクション エンジンをイネーブルにして、ICMP 接続をステートフル接続として処理します。

現象　セキュリティの高いインターフェイスからセキュリティの低いインターフェイスへのトラフィックが、FWSM を通過しない。

考えられる原因　セキュリティの高いインターフェイスに、トラフィックを許可するアクセス リストが適用されていません。PIX セキュリティ アプライアンスと異なり、FWSM では、インターフェイス間のトラフィックは自動的には許可されません。

推奨処置　送信元インターフェイスに、トラフィックを許可するアクセス リストを適用します。「拡張アクセス リストの追加」（p.10-7）を参照してください。

現象　同じセキュリティ レベルの 2 つのインターフェイス間でトラフィックを転送できない。

考えられる原因　同じセキュリティ レベルのインターフェイス間のトラフィックを許可する機能が、イネーブルに設定されていません。

推奨処置　「同じセキュリティ レベルのインターフェイス間の通信の許可」（p.6-8）の説明に従って、この機能をイネーブルにします。

現象　FWSM のフェールオーバーが実行されても、セカンダリ ユニットがトラフィックを転送しない。

考えられる原因　両方の装置に共通の VLAN が割り当てられていません。

推奨処置　スイッチ コンフィギュレーションで、両方の装置に共通の VLAN が割り当てられているかどうかを確認します。

仕様

この付録では、FWSM の仕様について説明します。次の内容について説明します。

- スイッチ ハードウェアおよびソフトウェアの互換性（p.A-2）
- ライセンス対象機能（p.A-2）
- 物理仕様（p.A-3）
- 機能の制限（p.A-3）
- 管理対象のシステム リソース（p.A-4）
- 固定システム リソース（p.A-5）
- ルールの制限（p.A-6）

スイッチ ハードウェアおよびソフトウェアの互換性

FWSM をサポートするスイッチ モデルには、次のプラットフォームがあります。

- 次の必須コンポーネントを装備した Catalyst 6500 シリーズ スイッチ
  - Cisco IOS ソフトウェア（スーパーバイザ IOS）*または* Catalyst Operating System（OS; オペレーティング システム）を搭載したスーパーバイザ エンジン。サポート対象のスーパーバイザ エンジンおよびソフトウェア リリースについては、表 A-1 を参照してください。
  - Cisco IOS ソフトウェアを搭載した MSFC 2。サポート対象の Cisco IOS リリースについては、表 A-1 を参照してください。
- 次の必須コンポーネントを装備した Cisco 7600 シリーズ ルータ
  - Cisco IOS ソフトウェアを搭載したスーパーバイザ エンジン。サポート対象のスーパーバイザ エンジンおよびソフトウェア リリースについては、表 A-1 を参照してください。
  - Cisco IOS ソフトウェアを搭載した MSFC 2。サポート対象の Cisco IOS リリースについては、表 A-1 を参照してください。

（注） WAN ポートはスタティック VLAN（仮想 LAN）を使用しないので、スイッチの WAN ポートに FWSM を直接接続することはできません。ただし、WAN ポートから MSFC に接続し、MSFC から FWSM に接続することは可能です。

表 A-1 に、スーパーバイザ エンジンのバージョンとソフトウェアを示します。

表 A-1　FWSM 3.1 のサポート

	スーパーバイザ エンジン[1]
Cisco IOS	
12.2(18)SXF 以上	720、32
12.2(18)SXF2 以上	2、720、32
Catalyst OS[2]	
8.5(3) 以上	2、720、32

1. FWSM は、スーパーバイザ 1 および 1A をサポートしません。
2. スーパーバイザ上で Catalyst OS を使用する場合、MSFC 上でサポート対象の任意の Cisco IOS リリースを使用できます（スーパーバイザ上で Cisco IOS ソフトウェアを使用する場合は、MSFC 上でも同じリリースを使用します）。

ライセンス対象機能

FWSM は次のライセンス対象機能をサポートします。

- マルチセキュリティ コンテキスト。FWSM では、ライセンスなしでも、2 つの仮想コンテキストと 1 つの管理コンテキストの計 3 つのセキュリティ コンテキストをサポートしています。4 つ以上のコンテキストが必要な場合、次のいずれかのライセンスを取得してください。
  - 20
  - 50
  - 100
  - 250
- GTP/GPRS サポート

物理仕様

表 A-2 に、FWSM の物理仕様を示します。

表 A-2　物理仕様

仕様	説明
帯域幅	SFM（搭載されている場合）への 6 Gbps パスを備えた CEF256 ライン カード、または 32 Gbps 共有バス
メモリ	• 1 GB RAM • 128 MB フラッシュ メモリ
各スイッチのモジュール数	各スイッチに 4 台までのモジュールを搭載可能。 フェールオーバーを使用して 2 台をスタンバイ モードにした場合でも、各スイッチに搭載できるモジュールは 4 台までです。

機能の制限

表 A-3 に、FWSM の機能の制限を示します。

表 A-3　機能の制限

	コンテキスト モード	
仕様	シングル	マルチ
AAA サーバ（RADIUS および TACACS+）	16	各コンテキストに 4
モニタできるフェールオーバー インターフェイス	250	すべてのコンテキスト全体で 250
フィルタリング サーバ（Websense Enterprise および N2H2 の Sentian）	16	各コンテキストに 4
ジャンボ イーサネット パケット	8500 バイト	8500 バイト
セキュリティ コンテキスト	適用外	250 セキュリティ コンテキスト（ソフトウェア ライセンスによる）
Syslog サーバ	16	各コンテキストに 4
VLAN インターフェイス		
ルーテッド モード	256	各コンテキストに 100 FWSM の VLAN インターフェイス数は、すべてのコンテキスト全体で 1000 までに限定されています。外部インターフェイスは複数のコンテキストで共有でき、状況によっては内部インターフェイスも共有できます。
透過モード	8 ペア	各コンテキストに 8 ペア

管理対象のシステム リソース

表 A-4 に、FWSM の管理対象のシステム リソースを示します。リソース マネージャを使用して、これらのリソースをコンテキスト単位で管理できます。「リソース管理の設定」（p.4-13）を参照してください。

表 A-4　管理対象のシステム リソース

仕様	コンテキスト モード	
	シングル	マルチ
MAC アドレス（透過ファイアウォール モードのみ）	64 K	すべてのコンテキスト全体で 64 K
FWSM で接続が許可されるホスト、同時	256 K	すべてのコンテキスト全体で 256 K
インスペクション エンジンの接続、レート	10,000/ 秒	すべてのコンテキスト全体で 10,000/ 秒
IPSec 管理接続、同時	5	各コンテキストに 5 すべてのコンテキスト全体で最大 10
ASDM 管理セッション、同時[1]	5	各コンテキストで最大 5 すべてのコンテキスト全体で最大 80
NAT 変換、同時	256 K	すべてのコンテキスト全体で 256 K
SSH 管理接続、同時	5	各コンテキストに 5 すべてのコンテキスト全体で最大 100
システム メッセージ、レート	FWSM の端末またはバッファへの送信メッセージは、30,000/ 秒 Syslog サーバへの送信メッセージは、25,000/秒	FWSM の端末またはバッファへの送信メッセージは、すべてのコンテキスト全体で 30,000/ 秒 Syslog サーバへの送信メッセージは、すべてのコンテキスト全体で 25,000/ 秒
1 台のホストと複数の他のホスト間の接続を含む、任意の 2 つのホスト間の TCP/UDP[2] [3] 接続、同時接続およびレート	999,900[4] 100,000/ 秒	すべてのコンテキスト全体で 999,900[4] すべてのコンテキスト全体で 100,000/秒
Telnet 管理接続、同時	5	各コンテキストに 5 すべてのコンテキスト全体で最大 100 の接続

1. ASDM セッションでは、2 つの HTTPS 接続を使用します。1 つは常に使用されるモニタ用、もう 1 つは変更時のみに使用される設定変更用です。たとえば、システム制限の ASDM セッション数が 80 の場合、HTTPS 接続数は 160 に制限されます。
2. 初期接続は、接続の総数に含まれます。初期接続の制限を設定した場合、制限を超える初期接続はカウントされません。
3. FWSM では、削除のマークが付いた接続を削除するために、最大 500 ミリ秒 かかることがあります。この間、接続上のトラフィックは廃棄されるため、接続が削除されるまで、同じ送信元ポートおよび宛先ポートを使用して同じ宛先への新しい接続を開始することはできません。大部分の TCP アプリケーションでは、バックツーバック接続で同じポートを再利用しませんが、RSH は同じポートを再利用することがあります。RSH など、バックツーバック接続で同じポートを再利用するアプリケーションを使用する場合、FWSM によりパケットが廃棄されることがあります。
4. PAT（ポート アドレス変換）では各接続に個別の変換が必要なので、PAT を使用する接続の有効な制限値は、接続制限ではなく変換の制限（256 K）になります。接続制限を適用するには、同じ変換セッションで複数の接続が可能な NAT を使用する必要があります。

固定システム リソース

表 A-5 に、FWSM の固定システム リソースを示します。

表 A-5　固定システム リソース

仕様	コンテキスト モード	
	シングル	マルチ
AAA 接続、レート	80/ 秒	すべてのコンテキスト全体で 80/ 秒
ACL ロギングのフロー、同時	32 K	すべてのコンテキスト全体で 32 K
エイリアス ステートメント	1 K	すべてのコンテキスト全体で 1 K
ARP テーブル エントリ、同時	64 K	すべてのコンテキスト全体で 64 K
DNS 検査、レート	5000/ 秒	すべてのコンテキスト全体で 5000/ 秒
グローバル ステートメント	4 K	すべてのコンテキスト全体で 4 K
インスペクション ステートメント	32	各コンテキストに 32
NAT ステートメント	2 K	すべてのコンテキスト全体で 2 K
パケット再組み立て、同時	30,000	すべてのコンテキスト全体で 30,000 フラグメント
ルート テーブル エントリ、同時	32 K	すべてのコンテキスト全体で 32 K
shun ステートメント	5 K	すべてのコンテキスト全体で 5 K
SIP 接続、同時	5 K	すべてのコンテキスト全体で 5 K
スタティック NAT ステートメント	2 K	すべてのコンテキスト全体で 2 K
TFTP セッション、同時[1]	999,100	すべてのコンテキスト全体で 999,100
ユーザ認証セッション、同時	50 K	すべてのコンテキスト全体で 50 K
ユーザ許可セッション、同時	150 K 各ユーザで最大 15 セッション	すべてのコンテキスト全体で 150 K 各ユーザで最大 15 セッション

1. FWSM Version 1.1 では、TFTP セッションの数は 1024 セッションに制限されていました。

ルールの制限

FWSM がシステム全体でサポートできるルール数は、シングルモードで約 80 K、マルチモードで約 142 K です。

デフォルトが 12 メモリ パーティションのマルチコンテキスト モードでは、各コンテキストで最大 12,130 のルールをサポートできますが、実際に 1 つのコンテキストでサポートできるルール数は、設定するコンテキスト数とパーティション数に応じて、これより増減ことがあります。コンテキスト間のメモリ配分の詳細については、「メモリ パーティションの設定」(p.4-18)を参照してください。

表 A-6 に、タイプ別のルールの最大数を示します。

表 A-6　ルールの制限

仕様	コンテキスト モード	
	シングル	12 プールのマルチ（パーティションごとの最大数）
AAA ルール	6451	992[1]
ACE	72,806	11,200
ネットワーク アクセス許可用にダウンロードされる ACE	5000	5000
established ルール	460	70
フィルタ ルール	2764	425
ICMP、Telnet、SSH、および HTTP ルール	1843	283
ポリシー NAT ACE	1843	283
inspect ルール	5529	850

1. たとえば、96 のコンテキストを 12 プールに均等に割り当てた場合、各プールに 8 つのコンテキストがあるので、各コンテキストが均等に使用できるフィルタ ルール数は 75 になります。

設定例

この付録では、FWSM の一般的な導入例を、図を示しながら説明します。内容は次のとおりです。

- ルーテッド モードの設定例（p.B-1）
- 透過モードでの設定例（p.B-15）
- フェールオーバーの設定例（p.B-20）

ルーテッド モードの設定例

ここでは、次の内容について説明します。

- 例 1：外部からアクセスのあるマルチモード ファイアウォール（p.B-1）
- 例 2：同じセキュリティ レベルを使用するシングル モード ファイアウォールの例（p.B-6）
- 例 3：マルチコンテキストの共有リソースの例（p.B-8）
- 例 4：IPv6 の設定例（p.B-14）

例 1：外部からアクセスのあるマルチモード ファイアウォール

次の構成では、それぞれ内部インターフェイスと外部インターフェイスを持つ 3 つのセキュリティ コンテキストと、admin コンテキストを作成します。カスタマー C（customerC）コンテキストには、サービス プロバイダー側に HTTP フィルタリング用の Websense サーバが設置された DMZ インターフェイスが含まれています（図 B-1 を参照）。

内部ホストはダイナミック NAT または PAT を使用して外部インターフェイスを通してインターネットにアクセスできますが、外部ホストから内部へのアクセスはできません。

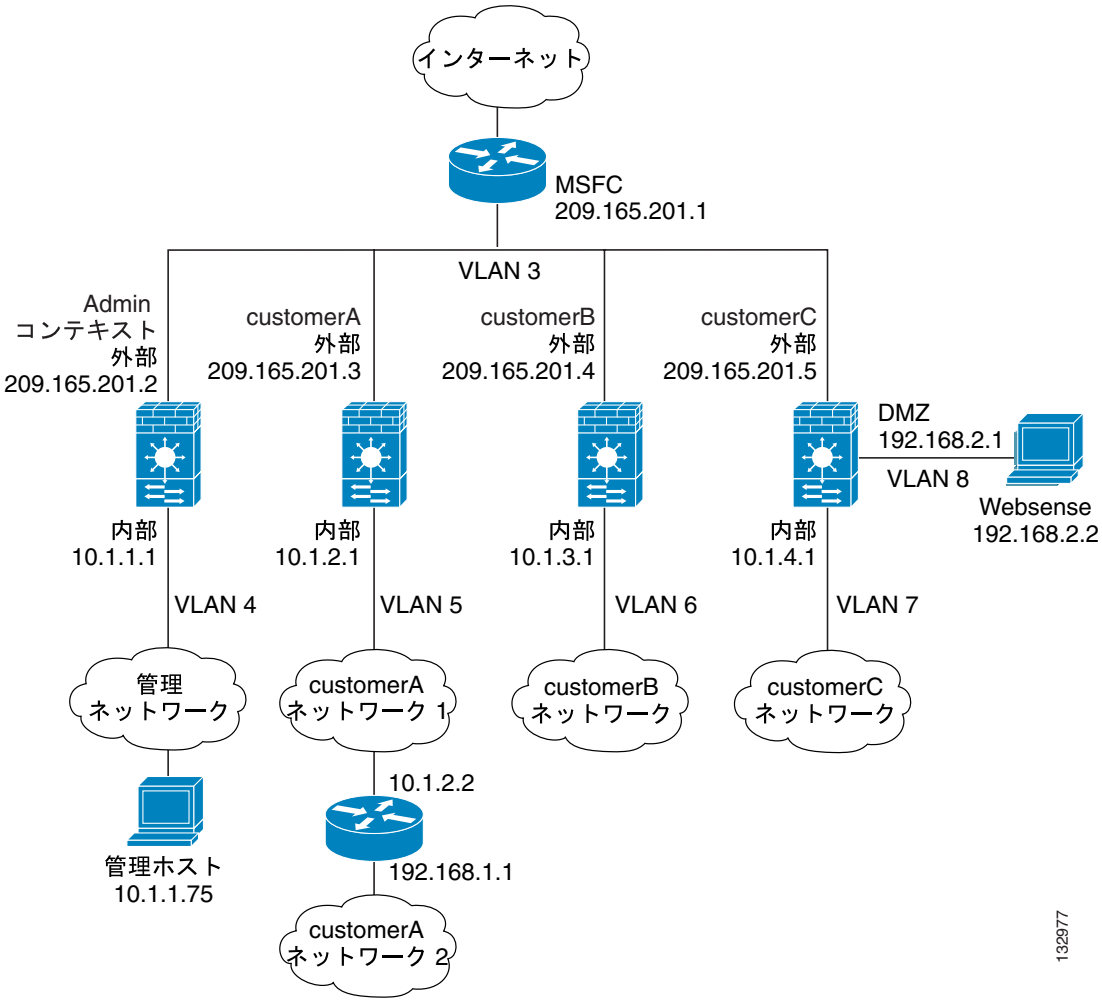
カスタマー A（customerA）コンテキストには、内部ルータの後ろに 2 つめのネットワークがあります。

admin コンテキストでは、1 つのホストから FWSM への SSH セッションを許可しています。

各カスタマー コンテキストは、リソースが制限されたクラス（ゴールド、シルバー、またはブロンズ）に属しています。

インターフェイスを固有にする場合、コンテキスト間で同じ内部 IP アドレスを共有できますが、個別の IP アドレスを設定するほうが管理は簡単です。

図 B-1　例 1



この構成の詳細については、次の項目を参照してください。

- システム コンフィギュレーション（例 1）（p.B-3）
- admin コンテキスト コンフィギュレーション（例 1）（p.B-4）
- カスタマー A のコンテキスト コンフィギュレーション（例 1）（p.B-4）
- カスタマー B のコンテキスト コンフィギュレーション（例 1）（p.B-5）
- カスタマー C のコンテキスト コンフィギュレーション（例 1）（p.B-5）
- スイッチの設定（例 1）（p.B-6）

システム コンフィギュレーション（例 1）

まず、**mode multiple** コマンドを使用して、マルチコンテキスト モードをイネーブルにします。次に、複数のコンテキストを使用できるように、アクティベーション キーを入力します。モードおよびアクティベーション キーは、再起動後も保持されますが、コンフィギュレーション ファイルには保存されません。**write terminal**、**show startup-config**、または **show running-config** コマンドを使用して FWSM 上で設定を表示すると、FWSM のリリースの次にモードが表示されます（ブランクはシングルモード、<system> はマルチモードのシステム コンフィギュレーション、<context> はマルチモードのコンテキストを意味します）。

```
hostname Farscape
password passw0rd
enable password chr1cht0n
admin-context admin
interface vlan 3
interface vlan 4
interface vlan 5
interface vlan 6
interface vlan 7
interface vlan 8
context admin
    allocate-interface vlan3
    allocate-interface vlan4
    config-url disk://admin.cfg
    member default
context customerA
    description This is the context for customer A
    allocate-interface vlan3
    allocate-interface vlan5
    config-url disk://contexta.cfg
    member gold
context customerB
    description This is the context for customer B
    allocate-interface vlan3
    allocate-interface vlan6
    config-url disk://contextb.cfg
    member silver
context customerC
    description This is the context for customer C
    allocate-interface vlan3
    allocate-interface vlan7-vlan8
    config-url disk://contextc.cfg
    member bronze
class gold
    limit-resource all 7%
    limit-resource rate conns 2000
    limit-resource conns 20000
class silver
    limit-resource all 5%
    limit-resource rate conns 1000
    limit-resource conns 10000
class bronze
    limit-resource all 3%
    limit-resource rate conns 500
    limit-resource conns 5000
```

admin コンテキスト コンフィギュレーション（例 1）

10.1.1.75 のホストは、SSH を使用してコンテキストにアクセスできます。それには、**crypto key generate** コマンドを使用してキーを生成する必要があります。証明書は、フラッシュ メモリに保存されます。

```
interface vlan 3
    nameif outside
    security-level 0
    ip address 209.165.201.2 255.255.255.224
interface vlan 4
    nameif inside
    security-level 100
    ip address 10.1.1.1 255.255.255.0
passwd secret1969
enable password h1and10
route outside 0 0 209.165.201.1 1
ssh 10.1.1.75 255.255.255.255 inside
nat (inside) 1 10.1.1.0 255.255.255.0
! This context uses dynamic NAT for inside users that access the outside
global (outside) 1 209.165.201.10-209.165.201.29
! The host at 10.1.1.75 has access to the Websense server in Customer C, and
! it needs a static translation for use in Customer C's access list
static (inside,outside) 209.165.201.30 10.1.1.75 netmask 255.255.255.255
access-list INTERNET remark -Allows inside hosts to access the outside for any IP
traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
```

カスタマー A のコンテキスト コンフィギュレーション（例 1）

```
interface vlan 3
    nameif outside
    security-level 0
    ip address 209.165.201.3 255.255.255.224
interface vlan 5
    nameif inside
    security-level 100
    ip address 10.1.2.1 255.255.255.0
passwd hell0!
enable password enter55
route outside 0 0 209.165.201.1 1
! The Customer A context has a second network behind an inside router that requires a
! static route. All other traffic is handled by the default route pointing to the
router.
route inside 192.168.1.0 255.255.255.0 10.1.2.2 1
nat (inside) 1 10.1.2.0 255.255.255.0
! This context uses dynamic PAT for inside users that access that outside. The outside
! interface address is used for the PAT address
global (outside) 1 interface
access-list INTERNET remark -Allows inside hosts to access the outside for any IP
traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
```

カスタマー B のコンテキスト コンフィギュレーション（例 1）

```
interface vlan 3
    nameif outside
    security-level 0
    ip address 209.165.201.4 255.255.255.224
interface vlan 6
    nameif inside
    security-level 100
    ip address 10.1.3.1 255.255.255.0
passwd tenac10us
enable password defen$e
route outside 0 0 209.165.201.1 1
nat (inside) 1 10.1.3.0 255.255.255.0
! This context uses dynamic PAT for inside users that access the outside
global (outside) 1 209.165.201.9 netmask 255.255.255.255
access-list INTERNET remark Inside users only access HTTP and HTTPS servers on the
outside
access-list INTERNET extended permit tcp any any eq http
access-list INTERNET extended permit tcp any any eq https
access-group INTERNET in interface inside
```

カスタマー C のコンテキスト コンフィギュレーション（例 1）

```
interface vlan 3
    nameif outside
    security-level 0
    ip address 209.165.201.5 255.255.255.224
interface vlan 7
    nameif inside
    security-level 100
    ip address 10.1.4.1 255.255.255.0
interface vlan 8
    nameif dmz
    security-level 50
    ip address 192.168.2.1 255.255.255.0
passwd fl0wer
enable password treeh0u$e
route outside 0 0 209.165.201.1 1
url-server (dmz) vendor websense host 192.168.2.2 url-block block 50
url-cache dst 128
filter url http 10.1.4.0 255.255.255.0 0 0
! When inside users access an HTTP server, FWSM consults with a
! Websense server to determine if the traffic is allowed
nat (inside) 1 10.1.4.0 255.255.255.0
! This context uses dynamic NAT for inside users that access the outside
global (outside) 1 209.165.201.9 netmask 255.255.255.255
! A host on the admin context requires access to the Websense server for management
using
! pcAnywhere, so the Websense server uses a static translation for its private address
static (dmz,outside) 209.165.201.6 192.168.2.2 netmask 255.255.255.255
access-list INTERNET remark -Allows all inside hosts to access the outside for any IP
access-list INTERNET remark -traffic, but denies them access to the dmz.
access-list INTERNET extended deny ip any 192.168.2.0 255.255.255.0
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list MANAGE remark -Allows the management host to use pcAnywhere on the
access-list MANAGE remark -Websense server
access-list MANAGE extended permit tcp host 209.165.201.30 host 209.165.201.6 eq
pcanywhere-data
access-list MANAGE extended permit udp host 209.165.201.30 host 209.165.201.6 eq
pcanywhere-status
access-group MANAGE in interface outside
access-list WEBSENSE remark -The Websense server needs to access the Websense updater
access-list WEBSENSE remark -server on the outside
access-list WEBSENSE extended permit tcp host 192.168.2.2 any eq http
access-group WEBSENSE in interface dmz
```

スイッチの設定（例 1）

次に、FWSM に関連する Cisco IOS スイッチの設定を示します。

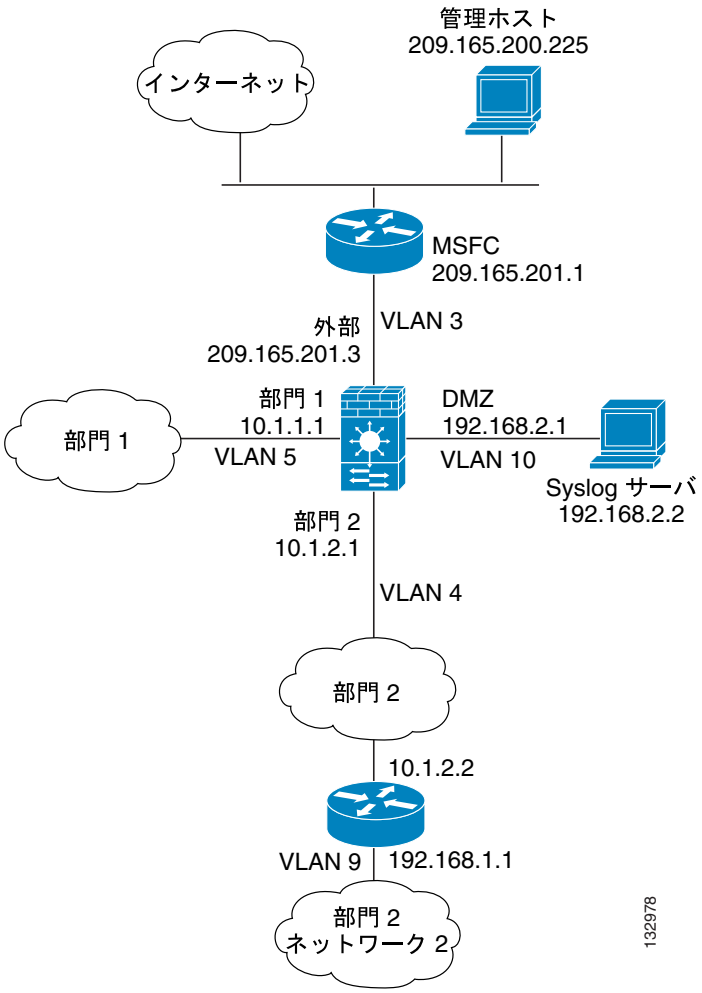
```
...
firewall module 8 vlan-group 1
firewall vlan-group 1 3-8
interface vlan 3
    ip address 209.165.201.1 255.255.255.224
    no shutdown
...
```

例 2：同じセキュリティ レベルを使用するシングル モード ファイアウォールの例

次の構成では、3 つの内部インターフェイスを作成します。インターフェイスのうちの 2 つは同じセキュリティ レベルの部門に接続します。DMZ インターフェイスは Syslog サーバのホスティングを行います。外部の管理ホストは、Syslog サーバと FWSM にアクセスする必要があります。FWSM との接続のため、ホストは VPN 接続を使用します。FWSM は、ルートの学習のために、内部インターフェイスの RIP を使用します。FWSM は RIP で学習したルートをアドバタイズしないので、アップストリーム ルータは FWSM トラフィックにスタティック ルートを使用する必要があります（図 B-2 を参照）。

各部門のネットワークはインターネットへのアクセスを許可され、PAT を使用します。

図 B-2　例 2



この構成の詳細については、次の項目を参照してください。

- FWSM の設定（例 2）（p.B-7）
- スイッチの設定（例 2）（p.B-8）

FWSM の設定（例 2）

```
interface vlan 3
    nameif outside
    security-level 0
    ip address 209.165.201.3 255.255.255.224
interface vlan 4
    nameif dept2
    security-level 100
    ip address 10.1.2.1 255.255.255.0
interface vlan 5
    nameif dept1
    security-level 100
    ip address 10.1.1.1 255.255.255.0
interface vlan 10
    nameif dmz
    security-level 50
    ip address 192.168.2.1 255.255.255.0
passwd g00fba11
enable password gen1u$
hostname Buster
same-security-traffic permit inter-interface
route outside 0 0 209.165.201.1 1
nat (dept1) 1 10.1.1.0 255.255.255.0
nat (dept2) 1 10.1.2.0 255.255.255.0
! The dept1 and dept2 networks use PAT when accessing the outside
global (outside) 1 209.165.201.9 netmask 255.255.255.255
! Because we perform dynamic NAT on these addresses for outside access, we need to
perform
! NAT on them for all other interface access. This identity static statement just
! translates the local address to the same address.
static (dept1,dept2) 10.1.1.0 10.1.1.0 netmask 255.255.255.0
static (dept2,dept1) 10.1.2.0 10.1.2.0 netmask 255.255.255.0
! The syslog server uses a static translation so the outside management host can
access
! the server
static (dmz,outside) 209.165.201.5 192.168.2.2 netmask 255.255.255.255
access-list DEPTS remark -Allows all dept1 and dept2 hosts to access the
access-list DEPTS remark -outside for any IP traffic
access-list DEPTS extended permit ip any any
access-group DEPTS in interface dept1
access-group DEPTS in interface dept2
access-list MANAGE remark Allows the management host to access the syslog server
access-list MANAGE extended permit tcp host 209.165.200.225 host 209.165.201.5 eq
telnet
access-group MANAGE in interface outside
! Advertises the FWSM IP address as the default gateway for the downstream
! router. FWSM does not advertise a default route to the router.
rip dept2 default version 2 authentication md5 scorpius 1
! Listens for RIP updates from the downstream router. FWSM does not
! listen for RIP updates from the router because a default route to the router is all
that
! is required.
rip dept2 passive version 2 authentication md5 scorpius 1
! The client uses a pre-shared key to connect to the FWSM over IPSec. The
! key is the password in the username command following.
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 group 2
isakmp policy 1 hash sha
isakmp enable outside
```

```
crypto ipsec transform-set vpn_client esp-3des esp-sha-hmac
username admin password passw0rd
crypto ipsec transform-set vpn esp-3des esp-sha-hmac
crypto dynamic-map vpn_client 1 set transform-set vpn
crypto map telnet_tunnel 1 ipsec-isakmp dynamic vpn_client
crypto map telnet_tunnel interface outside
ip local pool client_pool 10.1.1.2
access-list VPN_SPLIT extended permit ip host 209.165.201.3 host 10.1.1.2
telnet 10.1.1.2 255.255.255.255 outside
telnet timeout 30
logging trap 5
! System messages are sent to the syslog server on the DMZ network
logging host dmz 192.168.2.2
logging enable
```

スイッチの設定（例 2）

次に、FWSM に関連するスイッチの設定を示します。

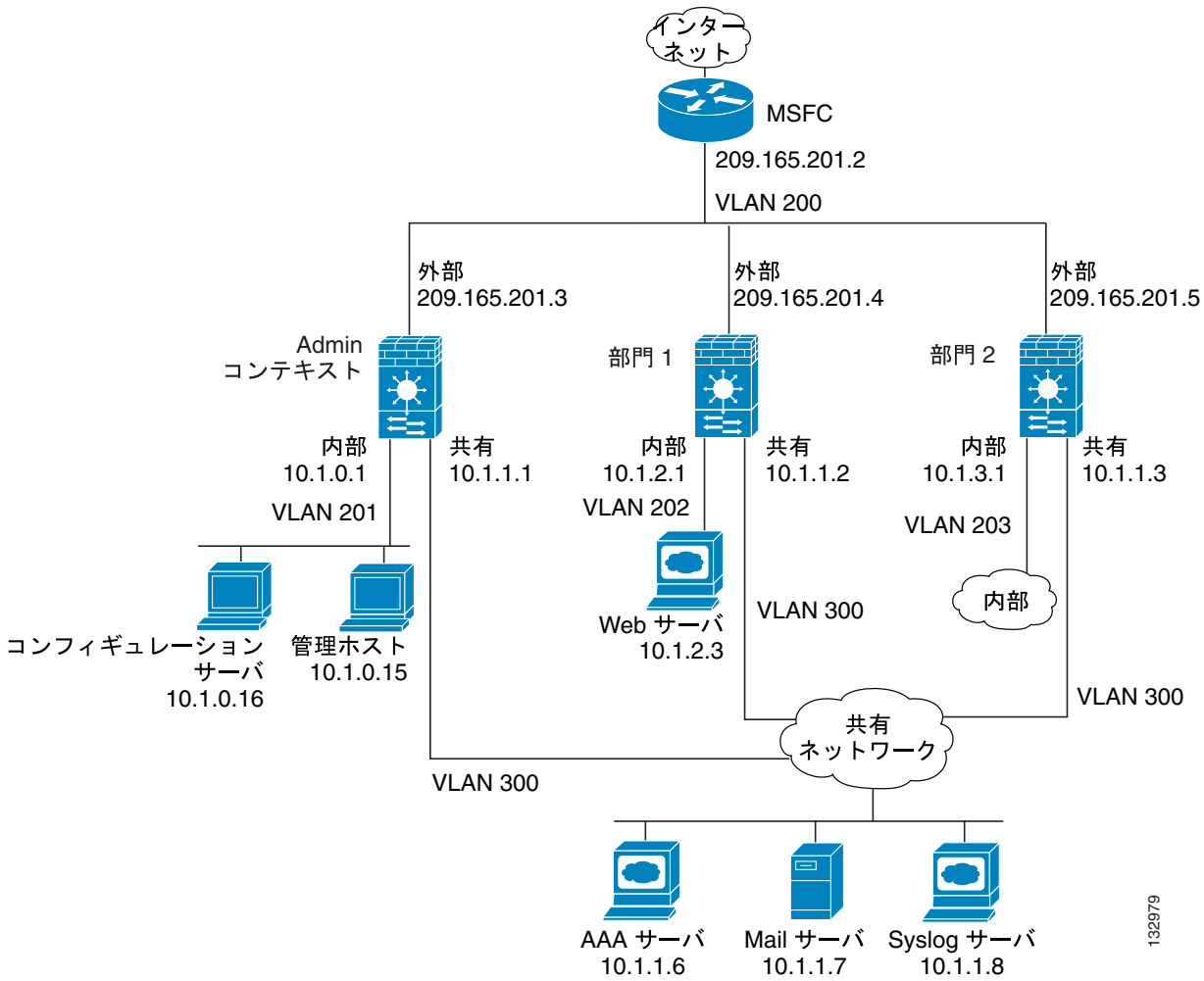
```
interface vlan 3
    ip address 209.165.201.1 255.255.255.224
    no shutdown
...
```

例 3：マルチコンテキストの共有リソースの例

次の構成には、1 つの企業内の複数部門用のマルチコンテキストが含まれます。各部門が独自のセキュリティ ポリシーを使用できるように、各部門に独自のセキュリティ コンテキストを設定します。ただし、Syslog サーバ、メール サーバ、および AAA（認証、許可、アカウンティング）サーバは、すべての部門で共有します。これらのサーバは、共有インターフェイス上に置かれます（図 B-3 を参照）。

部門 1 には、AAA サーバによって認証された外部ユーザがアクセスできる Web サーバがあります。

図 B-3　例 3



この構成の詳細については、次の項目を参照してください。

- システム コンフィギュレーション（例 3）（p.B-10）
- admin コンテキスト コンフィギュレーション（例 3）（p.B-11）
- 部門 1 のコンテキスト コンフィギュレーション（例 3）（p.B-12）
- 部門 2 のコンテキスト コンフィギュレーション（例 3）（p.B-13）
- スイッチの設定（例 3）（p.B-13）

システム コンフィギュレーション（例 3）

まず、**mode multiple** コマンドを使用して、マルチコンテキスト モードをイネーブルにします。次に、複数のコンテキストを使用できるように、**activation-key** コマンドを使用してアクティベーション キーを入力します。モードおよびアクティベーション キーは、再起動後も保持されますが、コンフィギュレーション ファイルには保存されません。**write terminal**、**show startup-config**、または **show running-config** コマンドを使用して FWSM 上で設定を表示すると、FWSM のリリースの次にモードが表示されます（ブランクはシングルモード、<system> はマルチモードのシステム コンフィギュレーション、<context> はマルチモードのコンテキストを意味します）。

```
hostname Ubik
password pkd55
enable password deckard69
interface vlan 200
interface vlan 201
interface vlan 202
interface vlan 203
interface vlan 300
admin-context admin
context admin
    allocate-interface vlan200
    allocate-interface vlan201
    allocate-interface vlan300
    config-url disk0://admin.cfg
context department1
    allocate-interface vlan200
    allocate-interface vlan202
    allocate-interface vlan300
    config-url ftp://admin:passw0rd@10.1.0.16/dept1.cfg
context department2
    allocate-interface vlan200
    allocate-interface vlan203
    allocate-interface vlan300
    config-url ftp://admin:passw0rd@10.1.0.16/dept2.cfg
```

admin コンテキスト コンフィギュレーション（例 3）

```
interface vlan 200
    nameif outside
    security-level 0
    ip address 209.165.201.3 255.255.255.224
interface vlan 201
    nameif inside
    security-level 100
    ip address 10.1.0.1 255.255.255.0
interface vlan 300
    nameif shared
    security-level 50
    ip address 10.1.1.1 255.255.255.0
passwd v00d00
enable password d011
route outside 0 0 209.165.201.2 1
nat (inside) 1 10.1.0.0 255.255.255.0
! This context uses PAT for inside users that access the outside
global (outside) 1 209.165.201.6 netmask 255.255.255.255
! This context uses PAT for inside users that access the shared network
global (shared) 1 10.1.1.30
! Because this host can access the web server in the Department 1 context, it requires
a
! static translation
static (inside,outside) 209.165.201.7 10.1.0.15 netmask 255.255.255.255
! Because this host has management access to the servers on the Shared interface, it
! requires a static translation to be used in an access list
static (inside,shared) 10.1.1.78 10.1.0.15 netmask 255.255.255.255
access-list INTERNET remark -Allows all inside hosts to access the outside
access-list INTERNET remark -and shared network for any IP traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list SHARED remark -Allows only mail traffic from inside to exit shared
interface
access-list SHARED remark -but allows the admin host to access any server.
access-list SHARED extended permit ip host 10.1.1.78 any
access-list SHARED extended permit tcp host 10.1.1.30 host 10.1.1.7 eq smtp
! Note that the translated addresses are used.
access-group SHARED out interface shared
! Allows 10.1.0.15 to access the admin context using Telnet. From the admin context,
you
! can access all other contexts.
telnet 10.1.0.15 255.255.255.255 inside
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (shared) host 10.1.1.6
    key TheUauthKey
    server-port 16
! The host at 10.1.0.15 must authenticate with the AAA server to log in
aaa authentication telnet console AAA-SERVER
logging trap 6
! System messages are sent to the syslog server on the Shared network
logging host shared 10.1.1.8
logging on
```

部門 1 のコンテキスト コンフィギュレーション（例 3）

```
interface vlan 200
    nameif outside
    security-level 0
    ip address 209.165.201.4 255.255.255.224
interface vlan 202
    nameif inside
    security-level 100
    ip address 10.1.2.1 255.255.255.0
interface vlan 300
    nameif shared
    security-level 50
    ip address 10.1.1.2 255.255.255.0
passwd cugel
enable password rhialto
nat (inside) 1 10.1.2.0 255.255.255.0
! The inside network uses PAT when accessing the outside
global (outside) 1 209.165.201.8 netmask 255.255.255.255
! The inside network uses dynamic NAT when accessing the shared network
global (shared) 1 10.1.1.31-10.1.1.37
! The web server can be accessed from outside and requires a static translation
static (inside,outside) 209.165.201.9 10.1.2.3 netmask 255.255.255.255
access-list INTERNET remark -Allows all inside hosts to access the outside
access-list INTERNET remark -and shared network for any IP traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list WEBSERVER remark -Allows the management host (its translated address) on
the access-list WEBSERVER remark -admin context to access the web server for
management
access-list WEBSERVER remark -it can use any IP protocol
access-list WEBSERVER extended permit ip host 209.165.201.7 host 209.165.201.9
access-list WEBSERVER remark -Allows any outside address to access the web server
access-list WEBSERVER extended permit tcp any eq http host 209.165.201.9 eq http
access-group WEBSERVER in interface outside
access-list MAIL remark -Allows only mail traffic from inside to exit out the shared
int
! Note that the translated addresses are used.
access-list MAIL extended permit tcp host 10.1.1.31 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.32 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.33 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.34 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.35 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.36 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.37 eq smtp host 10.1.1.7 eq smtp
access-group MAIL out interface shared
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (shared) host 10.1.1.6
    key TheUauthKey
    server-port 16
! All traffic matching the WEBSERVER access list must authenticate with the AAA server
aaa authentication match WEBSERVER outside AAA-SERVER
logging trap 4
! System messages are sent to the syslog server on the Shared network
logging host shared 10.1.1.8
logging on
```

部門 2 のコンテキスト コンフィギュレーション（例 3）

```
interface vlan 200
    nameif outside
    security-level 0
    ip address 209.165.201.5 255.255.255.224
interface vlan 203
    nameif inside
    security-level 100
    ip address 10.1.3.1 255.255.255.0
interface vlan 300
    nameif shared
    security-level 50
    ip address 10.1.1.3 255.255.255.0
passwd maz1r1an
enable password ly0ne$$e
route outside 0 0 209.165.201.2 1
nat (inside) 1 10.1.3.0 255.255.255.0
! The inside network uses PAT when accessing the outside
global (outside) 1 209.165.201.10 netmask 255.255.255.255
! The inside network uses PAT when accessing the shared network
global (shared) 1 10.1.1.38
access-list INTERNET remark -Allows all inside hosts to access the outside
access-list INTERNET remark -and shared network for any IP traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list MAIL remark -Allows only mail traffic from inside to exit out the shared
int
access-list MAIL extended permit tcp host 10.1.1.38 host 10.1.1.7 eq smtp
! Note that the translated PAT address is used.
access-group MAIL out interface shared
logging trap 3
! System messages are sent to the syslog server on the Shared network
logging host shared 10.1.1.8
logging on
```

スイッチの設定（例 3）

次に、FWSM に関連する Cisco IOS スイッチの設定を示します。

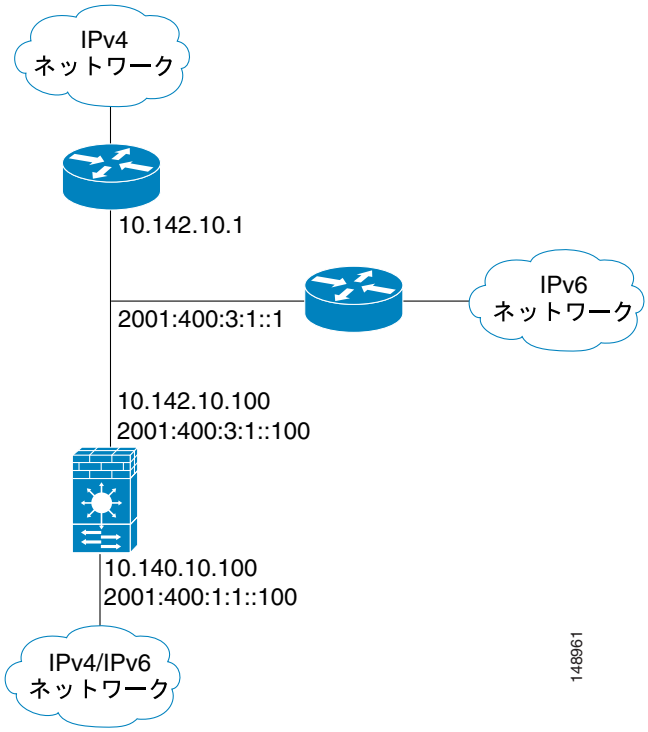
```
...
firewall module 6 vlan-group 1
firewall vlan-group 1 200-203,300
interface vlan 200
    ip address 209.165.201.2 255.255.255.224
    no shutdown
...
```

例 4：IPv6 の設定例

次の構成（図 B-4 を参照）は、FWSM 上で設定された IPv6 のいくつかの機能を示しています。

- 各インターフェイスは、IPv6 アドレスと IPv4 アドレスの両方で設定されます。
- IPv6 のデフォルト ルートは **ipv6 route** コマンドで設定されます。
- IPv6 のアクセス リストは外部インターフェイスに適用されます。

図 B-4　例 4：IPv4 と IPv6 のデュアル スタック構成




```
password pkd
enable password happy
hostname ubik
interface vlan 100
    nameif outside
    security-level 0
    ip address 10.142.10.100 255.255.255.0
    ipv6 address 2001:400:3:1::100/64
    ipv6 nd suppress-ra
interface vlan 101
    nameif inside
    security-level 100
    ip address 10.140.10.100 255.255.255.0
    ipv6 address 2001:400:1:1::100/64
route outside 0.0.0.0 0.0.0.0 10.142.10.1 1
access-list INTERNET remark -Allows all inside IPv4 hosts to access the outside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
ipv6 route outside ::/0 2001:400:3:1::1
ipv6 access-list IPV6INTERNET permit ip any any
access-group IPV6INTERNET in interface inside
ipv6 access-list OUTACL permit icmp6 2001:400:2:1::/64 2001:400:1:1::/64
ipv6 access-list OUTACL permit tcp 2001:400:2:1::/64 2001:400:1:1::/64 eq telnet
ipv6 access-list OUTACL permit tcp 2001:400:2:1::/64 2001:400:1:1::/64 eq ftp
ipv6 access-list OUTACL permit tcp 2001:400:2:1::/64 2001:400:1:1::/64 eq www
access-group OUTACL in interface outside
```

透過モードでの設定例

ここでは、次の内容について説明します。

- 例 5：外部からのアクセスのあるマルチモードの透過ファイアウォールの例（p.B-15）

例 5：外部からのアクセスのあるマルチモードの透過ファイアウォールの例

次の構成では、3 つのセキュリティ コンテキストと admin コンテキストを作成します。各コンテキストで、内部ルータと外部ルータ間で転送される OSPF トラフィックを許可します（図 B-5 を参照）。

また、透過ファイアウォールは DHCP リレー機能をサポートしていないため、DHCP パケットは透過ファイアウォールを通過します。

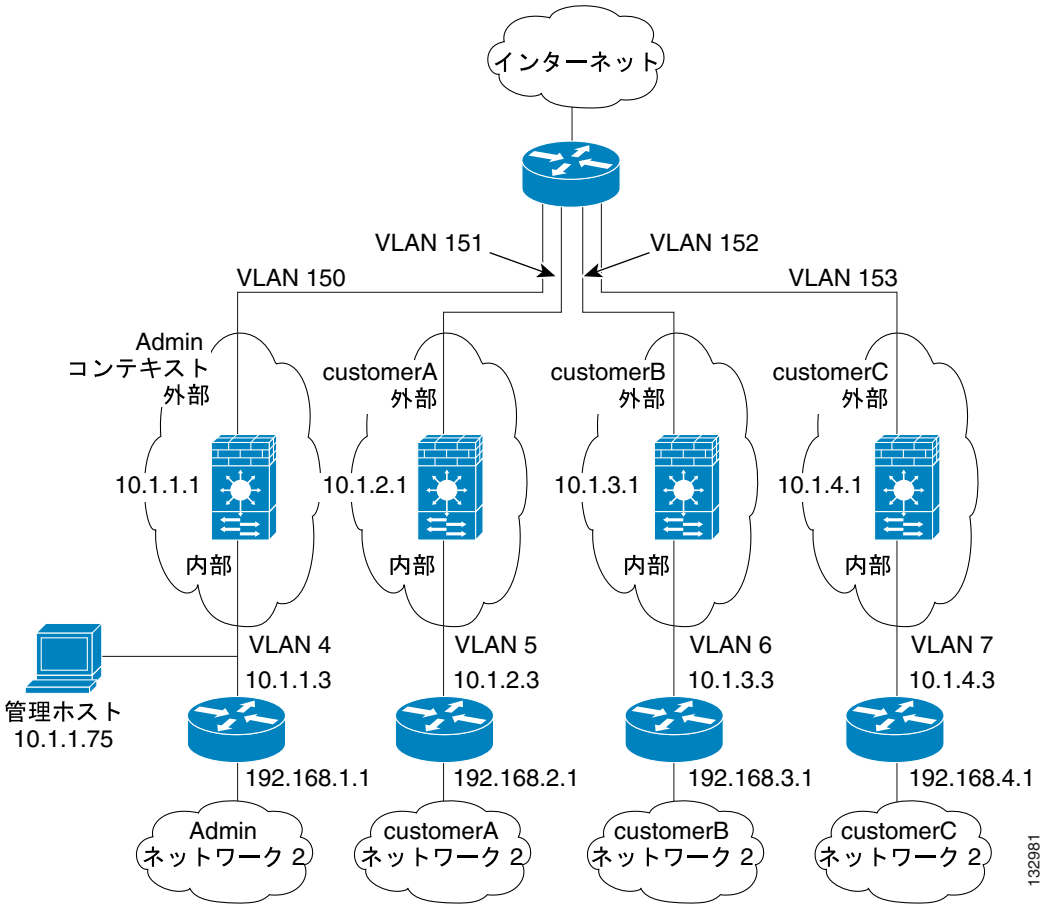
内部ホストからは外部のインターネットにアクセスできますが、外部ホストは内部にアクセスできません。

admin コンテキストでは、1 つのホストから FWSM への SSH セッションを許可しています。アップストリームおよびダウンストリーム ルータの IP スプーフィングを防止するため、ARP 検査も使用します。

各カスタマー コンテキストは、リソースが制限されたクラス（ゴールド、シルバー、またはブロンズ）に属しています。

コンテキスト間で同じ内部 IP アドレスを共有できますが、個別の IP アドレスを設定するほうが管理は簡単です。

図 B-5　例 5



この構成の詳細については、次の項目を参照してください。

- システム コンフィギュレーション（例 5）（p.B-17）
- admin コンテキスト コンフィギュレーション（例 5）（p.B-18）
- カスタマー A のコンテキスト コンフィギュレーション（例 5）（p.B-18）
- カスタマー B のコンテキスト コンフィギュレーション（例 5）（p.B-19）
- カスタマー C のコンテキスト コンフィギュレーション（例 5）（p.B-19）

システム コンフィギュレーション（例 5）

まず、**mode multiple** コマンドを使用して、マルチコンテキスト モードをイネーブルにします。モードは、再起動後も保持されますが、コンフィギュレーション ファイルには保存されません。**write terminal**、**show startup-config**、または **show running-config** コマンドを使用して FWSM 上で設定を表示すると、FWSM のリリースの次にモードが表示されます（ブランクはシングルモード、<system> はマルチモードのシステム コンフィギュレーション、<context> はマルチモードのコンテキストを意味します）。

```
hostname Farscape
password passw0rd
enable password chr1cht0n
interface vlan 4
interface vlan 5
interface vlan 6
interface vlan 7
interface vlan 150
interface vlan 151
interface vlan 152
interface vlan 153
admin-context admin
context admin
    allocate-interface vlan150
    allocate-interface vlan4
    config-url disk://admin.cfg
    member default
context customerA
    description This is the context for customer A
    allocate-interface vlan151
    allocate-interface vlan5
    config-url disk://contexta.cfg
    member gold
context customerB
    description This is the context for customer B
    allocate-interface vlan152
    allocate-interface vlan6
    config-url disk://contextb.cfg
    member silver
context customerC
    description This is the context for customer C
    allocate-interface vlan153
    allocate-interface vlan7
    config-url disk://contextc.cfg
    member bronze
class gold
    limit-resource all 7%
    limit-resource rate conns 2000
    limit-resource conns 20000
class silver
    limit-resource all 5%
    limit-resource rate conns 1000
    limit-resource conns 10000
class bronze
    limit-resource all 3%
    limit-resource rate conns 500
    limit-resource conns 5000
```

admin コンテキスト コンフィギュレーション（例 5）

10.1.1.75 のホストは、SSH を使用してコンテキストにアクセスできます。それには、**crypto key generate** コマンドを使用してキー のペアを生成する必要があります。

```
firewall transparent
passwd secret1969
enable password h1and10
interface vlan 150
    nameif outside
    security-level 0
    bridge-group 1
interface vlan 4
    nameif inside
    security-level 100
    bridge-group 1
interface bvi 1
    ip address 10.1.1.1 255.255.255.0
route outside 0 0 10.1.1.2 1
ssh 10.1.1.75 255.255.255.255 inside
arp outside 10.1.1.2 0009.7cbe.2100
arp inside 10.1.1.3 0009.7cbe.1000
arp-inspection inside enable flood
arp-inspection outside enable flood
access-list INTERNET remark -Allows all inside hosts to access the outside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list RETURN remark -Allows OSPF back
access-list RETURN extended permit 89 any any
access-list RETURN remark -Allows DHCP back
access-list RETURN extended permit udp any any eq 68
access-group RETURN in interface outside
```

カスタマー A のコンテキスト コンフィギュレーション（例 5）

```
firewall transparent
passwd hell0!
enable password enter55
interface vlan 151
    nameif outside
    security-level 0
    bridge-group 45
interface vlan 5
    nameif inside
    security-level 100
    bridge-group 45
interface bvi 45
    ip address 10.1.2.1 255.255.255.0
route outside 0 0 10.1.2.2 1
access-list INTERNET remark -Allows all inside hosts to access the outside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list RETURN remark -Allows OSPF back
access-list RETURN extended permit 89 any any
access-list RETURN remark -Allows DHCP back
access-list RETURN extended permit udp any any eq 68
access-group RETURN in interface outside
```

カスタマー B のコンテキスト コンフィギュレーション（例 5）

```
firewall transparent
passwd tenac10us
enable password defen$e
interface vlan 152
    nameif outside
    security-level 0
    bridge-group 1
interface vlan 6
    nameif inside
    security-level 100
    bridge-group 1
interface bvi 1
    ip address 10.1.3.1 255.255.255.0
route outside 0 0 10.1.3.2 1
access-list INTERNET remark -Allows all inside hosts to access the outside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list RETURN remark -Allows OSPF back
access-list RETURN extended permit 89 any any
access-list RETURN remark -Allows DHCP back
access-list RETURN extended permit udp any any eq 68
access-group RETURN in interface outside
```

カスタマー C のコンテキスト コンフィギュレーション（例 5）

```
firewall transparent
passwd fl0wer
enable password treeh0u$e
interface vlan 153
    nameif outside
    security-level 0
    bridge-group 100
interface vlan 7
    nameif inside
    security-level 100
    bridge-group 100
interface bvi 100
    ip address 10.1.4.1 255.255.255.0
route outside 0 0 10.1.4.2 1
access-list INTERNET remark -Allows all inside hosts to access the outside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list RETURN remark -Allows OSPF back
access-list RETURN extended permit 89 any any
access-list RETURN remark -Allows DHCP back
access-list RETURN extended permit udp any any eq 68
access-group RETURN in interface outside
```

フェールオーバーの設定例

ここでは、次の内容について説明します。

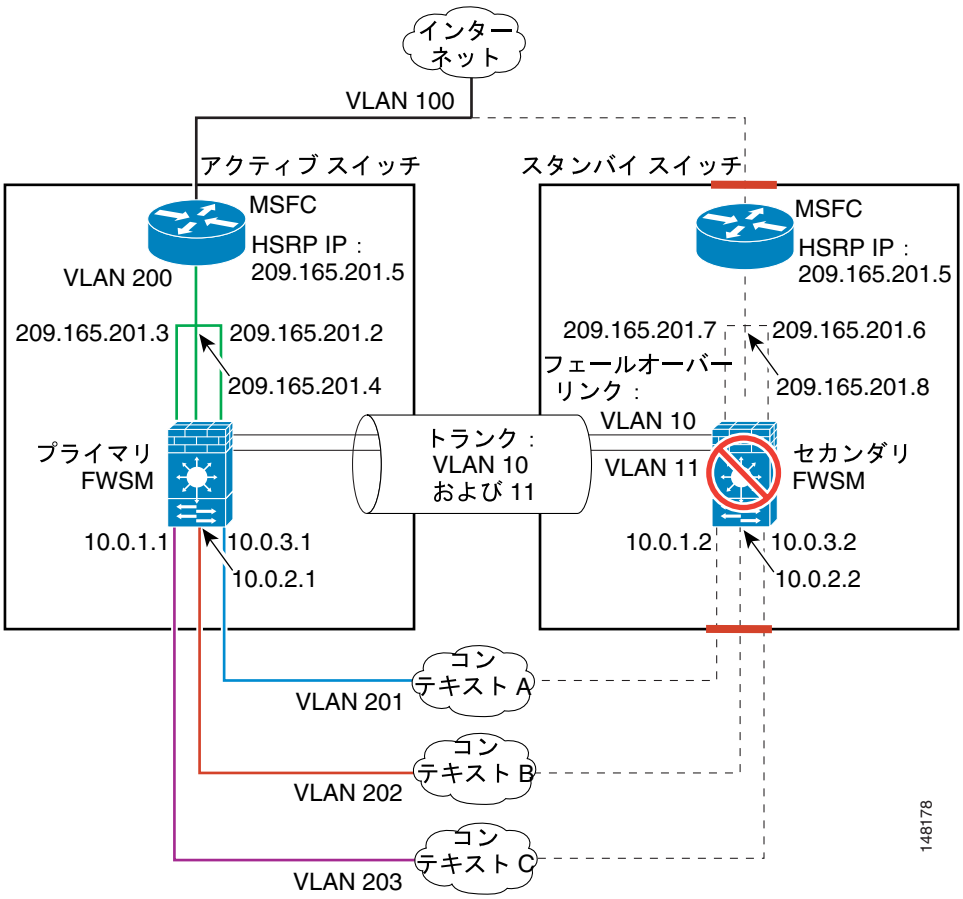
- 例 6：ルーテッド モードのフェールオーバー（p.B-20）
- 例 7：透過モードのフェールオーバー（p.B-24）
- 例 8：非対称ルーティング サポートを使用したアクティブ / アクティブのフェールオーバー（p.B-28）

例 6：ルーテッド モードのフェールオーバー

次の構成では、1 台のスイッチにルーテッド モードの各コンテキストを持つマルチコンテキスト モードの FWSM、および 2 台めのスイッチでバックアップとして動作する別の FWSM を示しています（図 B-6 を参照）。各コンテキスト（A、B、および C）は内部インターフェイスをモニタします。admin コンテキストであるコンテキスト A は、外部インターフェイスもモニタします。外部インターフェイスはすべてのコンテキストの共有インターフェイスなので、1 つのコンテキストでモニタするだけで、すべてのコンテキストをモニタできます。

セカンダリ FWSM もマルチコンテキスト モードで、ソフトウェア リリースも同じです。

図 B-6　　例 6



この構成の詳細については、次の項目を参照してください。

- プライマリ FWSM の設定（例 6）（p.B-21）
- セカンダリ FWSM のシステム コンフィギュレーション（例 6）（p.B-23）
- スイッチの設定（例 6）（p.B-23）

プライマリ FWSM の設定（例 6）

以下の項目はすべて、プライマリ FWSM の設定です。

- システム コンフィギュレーション（プライマリ ユニット — 例 6）（p.B-21）
- コンテキスト A コンフィギュレーション（プライマリ ユニット — 例 6）（p.B-22）
- コンテキスト B コンフィギュレーション（プライマリ ユニット — 例 6）（p.B-22）
- コンテキスト C コンフィギュレーション（プライマリ ユニット — 例 6）（p.B-23）

システム コンフィギュレーション（プライマリ ユニット — 例 6）

まず、**mode multiple** コマンドを使用して、マルチコンテキスト モードをイネーブルにします。次に、複数のコンテキストを使用できるように、**activation-key** コマンドを使用してアクティベーション キーを入力します。モードおよびアクティベーション キーは、再起動後も保持されますが、コンフィギュレーション ファイルには保存されません。**write terminal**、**show startup**、または **show running** コマンドを使用して FWSM 上で設定を表示すると、FWSM のリリースの次にモードが表示されます（ブランクはシングルモード、<system> はマルチモードのシステム コンフィギュレーション、<context> はマルチモードのコンテキストを意味します）。

```
hostname primary
enable password farscape
password crichton
!The vlan 10 and 11 interfaces are created when you enter the failover lan interface
and failover link commands.
interface vlan 10
    description LAN Failover interface
interface vlan 11
    description STATE Failover interface
interface vlan 200
interface vlan 201
interface vlan 202
interface vlan 203
failover lan interface faillink vlan 10
failover link statelink vlan 11
failover lan unit primary
failover interface ip faillink 192.168.253.1 255.255.255.252 standby 192.168.253.2
failover interface ip statelink 192.168.253.5 255.255.255.252 standby 192.168.253.6
failover interface-policy 50%
failover replication http
failover
admin-context contexta
context contexta
    allocate-interface vlan200
    allocate-interface vlan201
    config-url disk://contexta.cfg
context contextb
    allocate-interface vlan200
    allocate-interface vlan202
    config-url ftp://admin:passw0rd@10.0.3.16/contextb.cfg
context contextc
    allocate-interface vlan200
    allocate-interface vlan203
    config-url ftp://admin:passw0rd@10.0.3.16/contextc.cfg
```

コンテキスト A コンフィギュレーション（プライマリ ユニット — 例 6）

```
interface vlan 200
    nameif outside
    security-level 0
    ip address 209.165.201.2 255.255.255.224 standby 209.165.201.6
interface vlan 201
    nameif inside
    security-level 100
    ip address 10.0.3.1 255.255.255.0 standby 10.0.3.2
passwd secret1969
enable password h1and10
monitor-interface inside
monitor-interface outside
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
global (outside) 1 209.165.201.10 netmask 255.255.255.224
! This context uses dynamic PAT for inside users that access the outside
route outside 0 0 209.165.201.5 1
telnet 10.0.3.75 255.255.255.255 inside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
! Allows all inside hosts to access the outside for any IP traffic
```

コンテキスト B コンフィギュレーション（プライマリ ユニット — 例 6）

```
interface vlan 200
    nameif outside
    security-level 0
    ip address 209.165.201.4 255.255.255.224 standby 209.165.201.8
interface vlan 202
    nameif inside
    security-level 100
    ip address 10.0.2.1 255.255.255.0 standby 10.0.2.2
passwd secret1978
enable password 7samura1
monitor-interface inside
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
global (outside) 1 209.165.201.11 netmask 255.255.255.224
! This context uses dynamic PAT for inside users that access the outside
route outside 0 0 209.165.201.5 1
telnet 10.0.2.14 255.255.255.255 inside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
! Allows all inside hosts to access the outside for any IP traffic
```

コンテキスト C コンフィギュレーション（プライマリ ユニット — 例 6）

```
interface vlan 200
    nameif outside
    security-level 0
    ip address 209.165.201.3 255.255.255.224 standby 209.165.201.7
interface vlan 203
    nameif inside
    security-level 100
    ip address 10.0.1.1 255.255.255.0 standby 10.0.1.2
passwd secret0997
enable password strayd0g
monitor-interface inside
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
global (outside) 1 209.165.201.12 netmask 255.255.255.224
! This context uses dynamic PAT for inside users that access the outside
route outside 0 0 209.165.201.5 1
telnet 10.0.1.65 255.255.255.255 inside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
! Allows all inside hosts to access the outside for any IP traffic
```

セカンダリ FWSM のシステム コンフィギュレーション（例 6）

次の最小限のシステム コンフィギュレーションを行うだけで、コンテキストを設定する必要はありません。

まず、**mode multiple** コマンドを使用して、マルチコンテキスト モードをイネーブルにします。次に、複数のコンテキストを使用できるように、**activation-key** コマンドを使用してアクティベーション キーを入力します。モードおよびアクティベーション キーは、再起動後も保持されますが、コンフィギュレーション ファイルには保存されません。**write terminal**、**show startup**、または **show running** コマンドを使用して FWSM 上で設定を表示すると、FWSM のリリース ラインの次にモードが表示されます（ブランクはシングルモード、<system> はマルチモードのシステム コンフィギュレーション、<context> はマルチモードのコンテキストを意味します）。

```
failover lan interface faillink vlan 10
failover interface ip faillink 192.168.253.1 255.255.255.252 standby 192.168.253.2
failover lan unit secondary
failover
```

スイッチの設定（例 6）

次に、FWSM に関連する両方のスイッチ上の Cisco IOS スイッチの設定を示します。スイッチの冗長設定の詳細については、スイッチのマニュアルを参照してください。

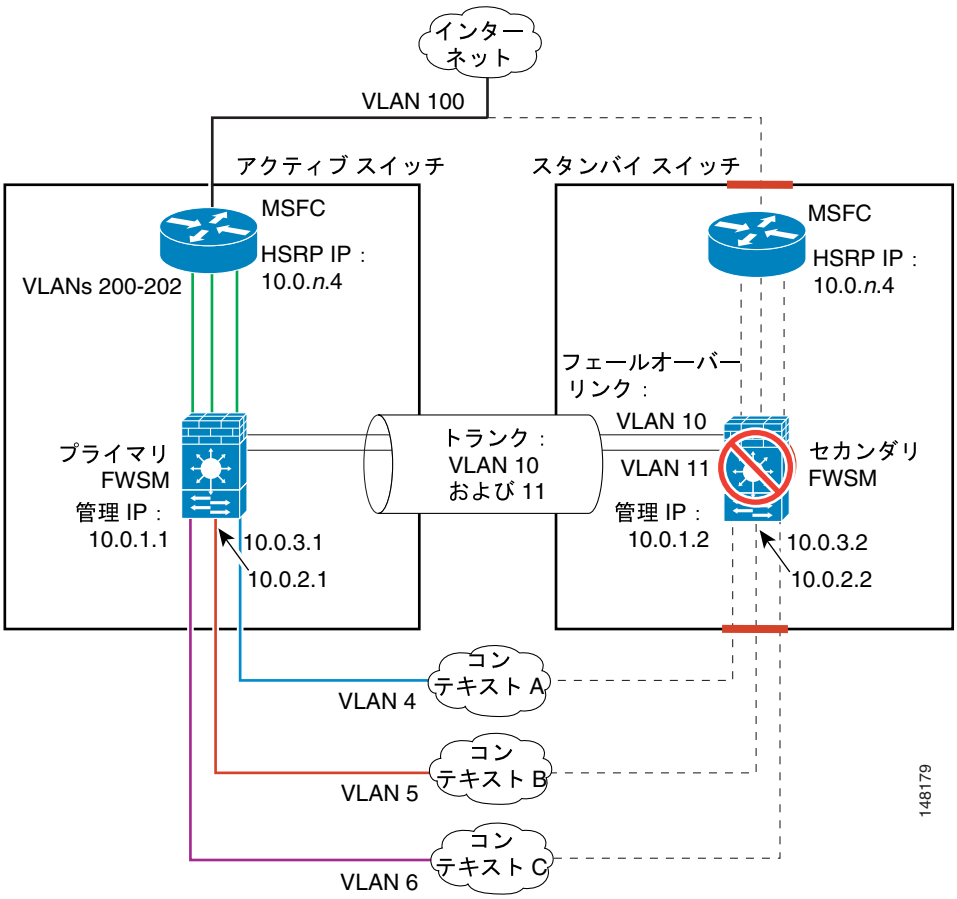
```
...
firewall module 1 vlan-group 1
firewall vlan-group 1 10,11,200-203
interface vlan 200
    ip address 209.165.201.1 255.255.255.224
    standby 200 ip 209.165.201.5
    standby 200 priority 110
    standby 200 preempt
    standby 200 timers 5 15
    standby 200 authentication Secret
    no shutdown
interface range gigabitethernet 2/1-3
    channel-group 2 mode on
    switchport trunk encapsulation dot1q
    no shutdown
...
```

例 7：透過モードのフェールオーバー

次の構成では、1 台のスイッチに透過モードのコンテキストを持つマルチコンテキスト モードの FWSM、および 2 台めのスイッチでバックアップとして動作する別の FWSM を示しています（図 B-6 を参照）。各コンテキスト（A、B、および C）は、内部インターフェイスと外部インターフェイスをモニタします。

セカンダリ FWSM もマルチコンテキスト モードで、ソフトウェア リリースも同じです。

図 B-7　例 7



この構成の詳細については、次の項目を参照してください。

- プライマリ FWSM の設定（例 7）（p.B-24）
- セカンダリ FWSM のシステム コンフィギュレーション（例 7）（p.B-27）
- スイッチの設定（例 7）（p.B-28）

プライマリ FWSM の設定（例 7）

以下の項目はすべて、プライマリ FWSM の設定です。

- システム コンフィギュレーション（プライマリ ユニット — 例 7）（p.B-25）
- コンテキスト A コンフィギュレーション（プライマリ ユニット — 例 7）（p.B-26）
- コンテキスト B コンフィギュレーション（プライマリ ユニット — 例 7）（p.B-26）
- コンテキスト C コンフィギュレーション（プライマリ ユニット — 例 7）（p.B-27）

システム コンフィギュレーション（プライマリ ユニット — 例 7）

まず、**mode multiple** コマンドを使用して、マルチコンテキスト モードをイネーブルにします。次に、複数のコンテキストを使用できるように、**activation-key** コマンドを使用してアクティベーション キーを入力します。モードおよびアクティベーション キーは、再起動後も保持されますが、コンフィギュレーション ファイルには保存されません。**write terminal**、**show startup**、または **show running** コマンドを使用して FWSM 上で設定を表示すると、FWSM のリリースの次にモードが表示されます（ブランクはシングルモード、<system> はマルチモードのシステム コンフィギュレーション、<context> はマルチモードのコンテキストを意味します）。

```
hostname primary
enable password farscape
password crichton
interface vlan 4
interface vlan 5
interface vlan 6
!The vlan 10 and 11 interfaces are created when you enter the failover lan interface
and failover link commands.
interface vlan 10
    description LAN Failover interface
interface vlan 11
    description STATE Failover interface
interface vlan 200
interface vlan 201
interface vlan 202
failover lan interface faillink vlan 10
failover link statelink vlan 11
failover lan unit primary
failover interface ip faillink 192.168.253.1 255.255.255.252 standby 192.168.253.2
failover interface ip statelink 192.168.253.5 255.255.255.252 standby 192.168.253.6
failover interface-policy 1
failover replication http
failover
admin-context contexta
context contexta
    allocate-interface vlan200
    allocate-interface vlan4
    config-url disk:/contexta.cfg
context contextb
    allocate-interface vlan201
    allocate-interface vlan5
    config-url ftp://admin:passw0rd@10.0.3.16/contextb.cfg
context contextc
    allocate-interface vlan202
    allocate-interface vlan6
    config-url ftp://admin:passw0rd@10.0.3.16/contextc.cfg
```

コンテキスト A コンフィギュレーション（プライマリ ユニット — 例 7）

```
firewall transparent
passwd secret1969
enable password h1and10
interface vlan 200
    nameif outside
    security-level 0
    bridge-group 56
interface vlan 4
    nameif inside
    security-level 100
    bridge-group 56
interface bvi 56
    ip address 10.0.3.1 255.255.255.0 standby 10.0.3.2
monitor-interface inside
monitor-interface outside
route outside 0 0 10.0.3.4 1
telnet 10.0.3.75 255.255.255.255 inside
access-list INTERNET remark -Allows all inside hosts to access the outside for
access-list INTERNET remark -any IP traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list BPDU ethertype permit bpdu
access-group BPDU in interface inside
access-group BPDU in interface outside
```

コンテキスト B コンフィギュレーション（プライマリ ユニット — 例 7）

```
firewall transparent
passwd secret1978
enable password 7samura1
interface vlan 201
    nameif outside
    security-level 0
    bridge-group 2
interface vlan 5
    nameif inside
    security-level 100
    bridge-group 2
interface bvi 2
ip address inside 10.0.2.1 255.255.255.0 standby 10.0.2.2
monitor-interface inside
monitor-interface outside
route outside 0 0 10.0.2.4 1
telnet 10.0.2.14 255.255.255.255 inside
access-list INTERNET remark -Allows all inside hosts to access the outside for
access-list INTERNET remark -any IP traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list BPDU ethertype permit bpdu
access-group BPDU in interface inside
access-group BPDU in interface outside
```

コンテキスト C コンフィギュレーション（プライマリ ユニット — 例 7）

```
firewall transparent
passwd secret0997
enable password strayd0g
interface vlan 202
    nameif outside
    security-level 0
    bridge-group 1
interface vlan 6
    nameif inside
    security-level 100
    bridge-group 1
interface bvi 1
    ip address inside 10.0.1.1 255.255.255.0 standby 10.0.1.2
monitor-interface inside
monitor-interface outside
route outside 0 0 10.0.1.4 1
telnet 10.0.1.65 255.255.255.255 inside
access-list INTERNET remark -Allows all inside hosts to access the outside for
access-list INTERNET remark -any IP traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list BPDU ethertype permit bpdu
access-group BPDU in interface inside
access-group BPDU in interface outside
```

セカンダリ FWSM のシステム コンフィギュレーション（例 7）

次の最小限のシステム コンフィギュレーションを行うだけで、コンテキストを設定する必要はありません。

```
    failover lan interface faillink vlan 10
failover interface ip faillink 192.168.253.1 255.255.255.252 standby 192.168.253.2
failover lan unit secondary
failover
```

スイッチの設定（例 7）

次に、FWSM に関連する両方のスイッチ上の Cisco IOS スイッチの設定を示します。スイッチの冗長設定の詳細については、スイッチのマニュアルを参照してください。

```
...
firewall multiple-vlan-interfaces
firewall module 1 vlan-group 1
firewall vlan-group 1 4-6,10,11,200-202
interface vlan 200
    ip address 10.0.1.3 255.255.255.0
    standby 200 ip 10.0.1.4
    standby 200 priority 110
    standby 200 preempt
    standby 200 timers 5 15
    standby 200 authentication Secret
    no shutdown
interface vlan 201
    ip address 10.0.2.3 255.255.255.0
    standby 200 ip 10.0.2.4
    standby 200 priority 110
    standby 200 preempt
    standby 200 timers 5 15
    standby 200 authentication Secret
    no shutdown
interface vlan 202
    ip address 10.0.3.3 255.255.255.0
    standby 200 ip 10.0.3.4
    standby 200 priority 110
    standby 200 preempt
    standby 200 timers 5 15
    standby 200 authentication Secret
    no shutdown
interface range gigabitethernet 2/1-3
    channel-group 2 mode on
    switchport trunk encapsulation dot1q
    no shutdown
...
```

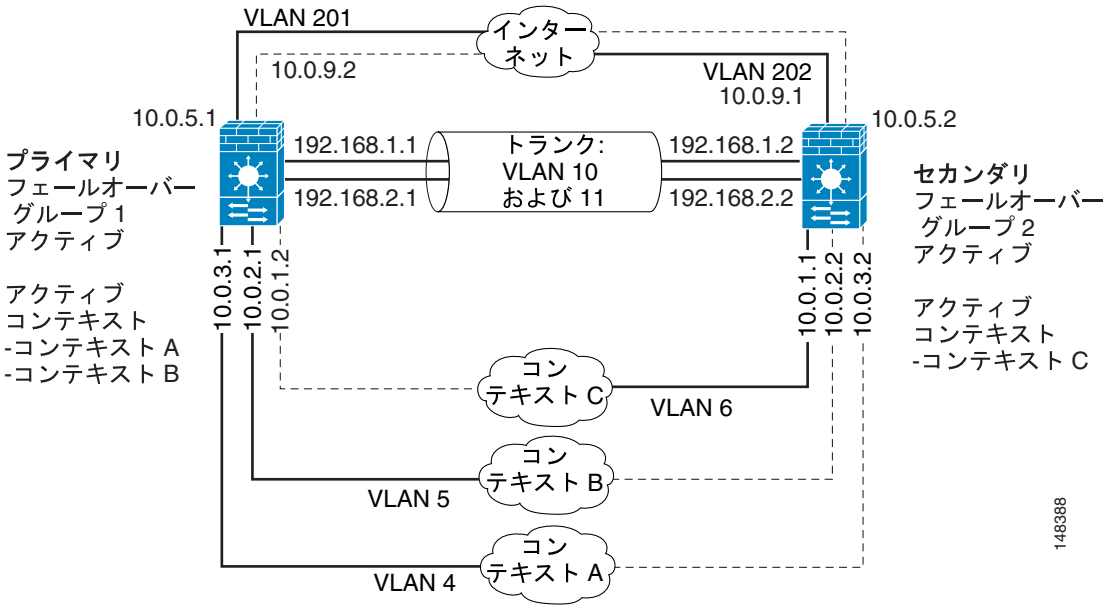
例 8：非対称ルーティング サポートを使用したアクティブ / アクティブのフェールオーバー

次に、アクティブ / アクティブのフェールオーバーを設定する例を示します。この例では、コンテキスト A（admin コンテキスト）、コンテキスト B、コンテキスト C という 3 つのコンテキストが使用されます。

- フェールオーバー グループは、**preempt** コマンドで設定されます。
- admin コンテキストが使用するインターフェイスは 1 つのみです。

図 B-8 に、この例のネットワーク図を示します。

図 B-8　アクティブ / アクティブのフェオーバー構成



前提条件

両方のユニットがマルチコンテキスト モードでなければなりません。**mode multiple** コマンドを使用して、プライマリとセカンダリの FWSM をマルチコンテキスト モードに切り替えます。**mode multiple** コマンドは、プライマリ ユニットとセカンダリ ユニットの両方で入力してモードを変更する必要があります。アクティブ / スタンバイ フェイールオーバー構成の場合でも、**mode multiple** コマンドはセカンダリ ユニットにコピーされません。

両方の FWSM には、同じ数のセキュリティ コンテキストのライセンスが必要です。

プライマリ FWSM の設定（例 8）

以下の項目はすべて、プライマリ FWSM の設定です。

- システム コンテキスト コンフィギュレーション（プライマリ FWSM — 例 8）（p.B-30）
- コンテキスト A コンフィギュレーション（プライマリ FWSM — 例 8）（p.B-31）
- コンテキスト B コンフィギュレーション（プライマリ FWSM — 例 8）（p.B-31）
- コンテキスト C コンフィギュレーション（プライマリ FWSM — 例 8）（p.B-32）

システム コンテキスト コンフィギュレーション（プライマリ FWSM — 例 8）

システム コンテキストで、フェールオーバー グループと、フェールオーバーおよびステートフル フェールオーバー VLAN が設定されます。

```
hostname cisco-primary
enable password farscape
password crichton
interface vlan 4
interface vlan 5
interface vlan 6
!The vlan 10 and 11 interfaces are created when you enter the failover lan interface
and failover link commands.
interface vlan 10
    description LAN Failover interface
interface vlan 11
    description STATE Failover interface
interface vlan 201
interface vlan 202
failover
failover lan unit primary
failover lan interface faillink vlan 10
failover key MySecretKey
failover link statelink vlan 11
failover interface ip faillink 192.168.1.1 255.255.255.0 standby 192.168.1.2
failover interface ip statelink 192.168.2.1 255.255.255.0 standby 192.168.2.2
failover group 1
    preempt
    replication http
    interface-policy 50%
failover group 2
    secondary
    preempt
    replication http
    interface-policy 50%
admin-context contexta
context contexta
    description administrative context
    allocate-interface vlan4
    config-url disk:/contexta.cfg
    join-failover-group 1
context contextb
    allocate-interface vlan201
    allocate-interface vlan5
    config-url ftp://admin:passw0rd@10.0.3.16/contextb.cfg
    join-failover-group 1
context contextc
    allocate-interface vlan202
    allocate-interface vlan6
    config-url ftp://admin:passw0rd@10.0.3.16/contextc.cfg
    join-failover-group 2
```

コンテキスト A コンフィギュレーション（プライマリ FWSM — 例 8）

コンテキスト A は admin コンテキストです。この例では、admin コンテキストで 1 つのインターフェイスのみが使用されます。管理アクセス用の内部インターフェイスです。コンテキストで 1 つのインターフェイスしか使用できないため、Telnet を使用してインターネットで FWSM にアクセスすることはできません。コンテキスト内のセキュリティ レベルが最低のインターフェイスには Telnet アクセスは許可されません。また、コンテキスト A には 1 つのインターフェイスしかないため、デフォルトでは最低レベルのインターフェイスとなります。このインターフェイス経由で FWSM を管理するには、SSH 接続を定義する必要があります。

```
interface vlan 4
    nameif mgmt
    security-level 5
    ip address 10.0.3.1 255.255.255.0 standby 10.0.3.2
passwd secret1969
enable password h1and10
monitor-interface inside
crypto key generate rsa modulus 1024
ssh 10.0.3.0 255.255.255.0 inside
ssh version 2
```

コンテキスト B コンフィギュレーション（プライマリ FWSM — 例 8）

```
interface vlan 201
    nameif outside
    security-level 0
    ip address 10.0.5.1 255.255.255.0 standby 10.0.5.2
    asr-group 1
interface vlan 5
    nameif inside
    security-level 100
    ip address 10.0.2.1 255.255.255.0 standby 10.0.2.2
passwd secret1978
enable password 7samura1
monitor-interface inside
monitor-interface outside
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
global (outside) 1 10.0.5.1 netmask 255.255.255.0
! This context uses dynamic PAT for inside users that access the outside
route outside 0 0 10.0.5.5 1
telnet 10.0.2.14 255.255.255.255 inside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
! Allows all inside hosts to access the outside for any IP traffic
```

コンテキスト C コンフィギュレーション（プライマリ FWSM ― 例 8）

```
interface vlan 202
    nameif outside
    security-level 0
    ip address 10.0.9.1 255.255.255.224 standby 10.0.9.2
    asr-group 1
interface vlan 6
    nameif inside
    security-level 100
    ip address 10.0.1.1 255.255.255.0 standby 10.0.1.2
passwd secret0997
enable password strayd0g
monitor-interface inside
monitor-interface outside
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
global (outside) 1 10.0.9.1 netmask 255.255.255.0
! This context uses dynamic PAT for inside users that access the outside
route outside 0 0 10.0.9.5 1
telnet 10.0.1.65 255.255.255.255 inside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
! Allows all inside hosts to access the outside for any IP traffic
```

セカンダリ FWSM の設定（例 8）

フェールオーバー リンクの認識するには、セカンダリ FWSM を設定します。セカンダリ FWSM は、起動時または **failover** が最初にイネーブルになったときに、プライマリ FWSM からコンテキスト コンフィギュレーションを取得します。フェールオーバー グループの設定内の **preempt** コマンドを使用すると、設定が同期化されて先行遅延時間が経過したときに、フェールオーバー グループが指定ユニット上でアクティブになります。

プライマリ FWSM から設定を受信するには、セカンダリ FWSM で **failover key** コマンドを設定する必要があります。

```
failover
failover lan unit secondary
failover lan interface faillink vlan 10
failover key MySecretKey
failover interface ip faillink 192.168.253.1 255.255.255.252 standby 192.168.253.2
```

failover コマンドでフェールオーバーをイネーブルにすると、セカンダリ FWSM がプライマリ FWSM から設定を取得します。

スイッチの設定（例 8）

次に、FWSM に関連する両方のスイッチ上の Cisco IOS スイッチの設定を示します。スイッチの冗長設定の詳細については、スイッチのマニュアルを参照してください。

```
...
firewall multiple-vlan-interfaces
firewall module 1 vlan-group 1
firewall vlan-group 1 4-6,10,11,201,202
interface vlan 201
    ip address 10.0.5.3 255.255.255.0
    standby 200 ip 10.0.5.4
    standby 200 priority 110
    standby 200 preempt
    standby 200 timers 5 15
    standby 200 authentication Secret
    no shutdown
interface vlan 202
    ip address 10.0.9.3 255.255.255.0
    standby 200 ip 10.0.9.4
    standby 200 priority 110
    standby 200 preempt
    standby 200 timers 5 15
    standby 200 authentication Secret
    no shutdown
interface range gigabitethernet 2/1-3
    channel-group 2 mode on
    switchport trunk encapsulation dot1q
    no shutdown
...
```

■ フェールオーバーの設定例

CLI の使用

この付録では、FWSM 上での CLI の使用法について説明します。内容は次のとおりです。

- ファイアウォール モードおよびセキュリティ コンテキスト モード（p.C-1）
- コマンド モードおよびプロンプト（p.C-2）
- 構文の形式（p.C-3）
- コマンドの短縮形（p.C-3）
- コマンドラインの編集（p.C-3）
- コマンドの補完（p.C-4）
- コマンド ヘルプ（p.C-4）
- show コマンド出力のフィルタリング（p.C-5）
- コマンド出力のページング（p.C-6）
- コメントの追加（p.C-6）
- テキスト コンフィギュレーション ファイル（p.C-7）

（注）この CLI の構文およびその他の規則は Cisco IOS CLI と同様ですが、FWSM の Operating System（OS; オペレーティング システム）は、Cisco IOS ソフトウェアのバージョンではありません。Cisco IOS CLI のコマンドを FWSM でそのまま使用できたり、または FWSM OS の CLI 機能が Cisco IOS CLI と同様の機能を持つとは限りません。

ファイアウォール モードおよびセキュリティ コンテキスト モード

FWSM は、次のモードを組み合わせて動作します。

- 透過ファイアウォール 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 モードにより、FWSM がレイヤ 2 ファイアウォールとして動作するかレイヤ 3 ファイアウォールとして動作するかが決まります。

- 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 モードにより、FWSM がシングル デバイスとして動作するか、仮想デバイスのようなマルチ セキュリティ コンテキストとして動作するかが決まります。

コマンドによっては、特定のモードでしか使用できないものもあります。

コマンド モードおよびプロンプト

FWSM CLI には、コマンド モードがあります。コマンドによっては、特定のモードでしか使用できないものもあります。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別なモードに切り替える必要があります。また、誤ってコンフィギュレーションの変更が入力されないようにするには、コンフィギュレーション モードに切り替える必要があります。下位のコマンドは、上位のモードで入力できます。たとえば、イネーブル EXEC コマンドはグローバル コンフィギュレーション モードで入力できます。

システム コンフィギュレーションまたはシングルコンテキスト モードの場合、プロンプトはホスト名から開始されます。

```
hostname
```

コンテキスト内では、プロンプトのホスト名のあとにコンテキスト名が表示されます。

```
hostname/context
```

プロンプトの表示は、アクセス モードによって異なります。

- ユーザ ECEC モード

  ユーザ EXEC モードでは、最小限の FWSM 設定が表示されます。最初に FWSM にアクセスしたときのユーザ EXEC モードのプロンプトは、次のようになります。

  ```
  hostname>

  hostname/context>
  ```

- イネーブル ECEC モード

  イネーブル EXEC モードでは、ユーザのイネーブル レベルまでの現在の設定がすべて表示されます。ユーザ EXEC モードのコマンドは、イネーブル EXEC モードで機能します。イネーブル 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（パスワードが必要）。プロンプトに、番号記号（#）が追加されます。

  ```
  hostname#

  hostname/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、FWSM の設定を変更することができます。このモードでは、すべてのユーザ EXEC コマンド、イネーブル EXEC コマンド、およびグローバル コンフィギュレーション コマンドを使用できます。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、イネーブル 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わります。

  ```
  hostname(config)#

  hostname/context(config)#
  ```

- コマンド固有コンフィギュレーション モード

  一部のコマンドは、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コンフィギュレーション モードに入ります。このモードでは、すべてのユーザ EXEC コマンド、イネーブル EXEC コマンド、グローバル コンフィギュレーション コマンド、およびコマンド固有コンフィギュレーション コマンドを使用できます。たとえば、**interface** コマンドを入力するとインターフェイス コンフィギュレーション モードが開始します。プロンプトが次のように変わります。

  ```
  hostname(config-if)#

  hostname/context(config-if)#
  ```

構文の形式

コマンド構文の記述には、次の表記法を使用しています。

表 C-1　構文の表記法

表記	説明
太字	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
イタリック	イタリックの文字は、ユーザが値を指定する引数です。
[x]	角カッコで囲まれているものは、省略可能な要素（キーワードまたは引数）です。
|	縦棒で区切られている場合、複数の任意または必須のキーワードまたは引数から、1 つを選択します。
[x | y]	角カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、任意の選択肢です。
{x | y}	波カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、必須の選択肢です。
[x {y | z}]	角カッコまたは波カッコが重複している場合、任意または必須の要素内の、任意または必須の選択肢を示します。角カッコ内の波カッコおよび縦棒は、任意の要素内の必須の選択肢です。

コマンドの短縮形

コマンドは、そのコマンドが固有であることを示す最小限の文字数に短縮できます。たとえば、完全形の **write terminal** コマンドを入力する代わりに **wr t** と入力してコンフィギュレーションを表示したり、**en** と入力してイネーブル モードを開始したり、**conf** t と入力してコンフィギュレーション モードを開始できます。また、**0** は、**0.0.0.0** を意味します。

コマンドラインの編集

FWSM のコマンドラインの編集規則は、Cisco IOS ソフトウェアと同じです。**show history** コマンドを使用すると、入力済みの全コマンドが表示されます。また、上矢印キーまたは **^p** コマンドを使用して、前に入力したコマンドを 1 つずつ表示できます。入力したコマンドを確認したあと、下矢印キーまたは **^n** コマンドを使用して、表示された内容の中で次に進むことができます。再使用したいコマンドに到達したら、構文を編集するか、**Enter** キーを押して実行します。**^w** を押すとカーソルの左側の文字が削除され、**^u** を押すと行全体が消去されます。

FWSM では、1 つのコマンドに入力できるのは 512 文字までです。これを超えて入力された文字は無視されます。

コマンドの補完

文字列の一部の入力後にコマンドまたはキーワードを補完するには、**Tab** キーを押します。FWSM では、文字列の一部が 1 つのコマンドまたはキーワードにのみ一致する場合だけ、コマンドまたはキーワードが補完されます。たとえば、**s** と入力して **Tab** キーを押した場合、FWSM ではコマンドは補完されません。該当するコマンドが複数あるためです。しかし、**dis** と入力して **Tab** キーを押した場合、**disable** コマンドが完成します。

コマンド ヘルプ

コマンド ラインでヘルプ情報を利用するには、次のコマンドを入力します。

- **help** *command_name*

  該当するコマンドのヘルプを表示します。
- **help ?**

  ヘルプが利用できるコマンドを表示します。
- *command_name* **?**

  利用可能な引数のリストを表示します。
- *string***?**（スペースなし）

  指定した文字列で始まるコマンドの候補を一覧表示します。
- **?** および **+?**

  利用可能なすべてのコマンドを一覧表示します。**?** と入力した場合、FWSM では現在のモードで利用可能なコマンドのみが表示されます。下位のモード用のものも含めて利用可能なすべてのコマンドを表示するには、**+?** と入力します。

（注） コマンド文字列にクエスチョン マーク（?）を含めるには、CLI のヘルプが呼び出されないように、**Ctrl-V** を押してからクエスチョン マークを入力する必要があります。

show コマンド出力のフィルタリング

show コマンドにフィルタ オプションおよびフィルタリング表現を指定するには、縦棒（|）を使用します。フィルタリングを実行すると、Cisco IOS ソフトウェアと同様に、各出力行が正規表現に対して照合されます。各種のフィルタ オプションを選択することによって、表現と一致するすべての出力を表示または除外できます。また、表現に一致する行で開始され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 オプションを指定する構文は、次のとおりです。

```
hostname# show command | {include | exclude | begin | grep [-v]} regexp
```

このコマンド文字列では、最初の縦棒（|）が、このコマンドに必須の演算子です。この演算子により、**show** コマンドの出力にフィルタが適用されます。構文内の他の縦棒（|）は代替オプションを示すもので、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含まれます。**-v** を指定しないで **grep** オプションを使用する場合も、結果は同じです。**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** を指定して **grep** オプションを使用する場合も、結果は同じです。**begin** オプションを指定すると、正規表現に一致する行で開始されるすべての出力行が表示されます。

regexp に、Cisco IOS の任意の正規表現を指定します。正規表現は引用符または二重引用符で囲まないので、末尾にスペースが含まれていないかどうか注意してください。末尾のスペースは正規表現の一部とみなされます。

正規表現を作成する場合には、照合する任意の文字または数字を使用できます。また、正規表現で使用すると、特別な意味を持つキーボード文字があります。表 C-2 に、特別な意味の文字を示します。

表 C-2　正規表現での特殊文字の使用

文字タイプ	文字	特別な意味
ピリオド	.	空白スペースを含め、任意の 1 文字と一致します。
アスタリスク	*	パターンの 0 個以上のシーケンスと一致します。
プラス符号	+	パターンの 1 個以上のシーケンスと一致します。
クエスチョン マーク	?[1]	パターンの 0 または 1 文字と一致します。
キャレット	^	入力文字列の先頭と一致します。
ドル記号	$	入力文字列の末尾と一致します。
アンダースコア	_	カンマ（,）、左波カッコ、右波カッコ、左丸カッコ、右丸カッコ、入力文字列の先頭、入力文字列の末尾、またはスペースと一致します。
角カッコ	[]	1 文字のパターンの範囲を指定します。
ハイフン	-	範囲の終点を区切ります。

1. クエスチョン マークがヘルプ コマンドとして解釈されないようにするため、クエスチョン マークを入力する前に **Ctrl-V** を押します。

これらの特殊文字を 1 文字のパターンとして使用するには、各文字の前にバックスラッシュ（\）を付けて特別な意味を消去します。

コマンド出力のページング

help または **?**、**show**、**show xlate**、または出力行が長い他のコマンドでは、1 画面の情報だけを表示して停止するか、全情報を一度に表示するかを指定できます。**pager** コマンドを使用すると、何行表示したあとで More プロンプトを表示するかを設定できます。

ページングをイネーブルにすると、次のプロンプトが表示されます。

```
<--- More --->
```

More プロンプトの使用方法は、UNIX の **more** コマンドと同様です。

- 次の画面を表示するには、スペースバーを押します。
- 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

コメントを作成するには、行の先頭にコロン（:）を付けます。ただし、コメントが表示されるのはコマンド ヒストリ バッファ内だけで、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、コメントを表示するには、**show history** コマンドを使用するか、または矢印キーを押して前のコマンドを検索します。コメントはコンフィギュレーションには含まれないので、**write terminal** コマンドを使用しても表示されません。

テキスト コンフィギュレーション ファイル

ここでは、FWSM 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 ファイルの作成方法について説明します。内容は次のとおりです。

- テキスト ファイル内の行とコマンドの対応（p.C-7）
- コマンド固有コンフィギュレーション モードのコマンド（p.C-7）
- 自動テキスト エントリ（p.C-7）
- 行の順序（p.C-8）
- 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.C-8）
- パスワード（p.C-8）
- 複数のセキュリティ コンテキスト ファイル（p.C-8）

テキスト ファイル内の行とコマンドの対応

テキスト コンフィギュレーション ファイルに含まれる行は、このマニュアルに説明されているコマンドに対応しています。

たとえば、コマンドの先頭に CLI プロンプトが記述されます。次に、[hostname (config)#] プロンプトの例を示します。

```
hostname(config)# context a
```

テキスト コンフィギュレーション ファイルでは、コマンド入力のプロンプトはないので、プロンプトは省略されます。

```
context a
```

コマンド固有コンフィギュレーション モードのコマンド

コマンドラインで入力する場合には、コマンド固有コンフィギュレーション モードのコマンドはメイン コマンドの下にインデントされて表示されます。テキスト ファイルの行では、メイン コマンドのすぐあとにコマンドがあれば、インデントする必要はありません。たとえば、次のインデントなしの前半の 2 行は、インデントされている後半の 2 行と同じ意味です。

```
interface gigabitethernet0
nameif inside
interface gigabitethernet1
    nameif outside
```

自動テキスト エントリ

FWSM にコンフィギュレーションをダウンロードすると、FWSM により一部の行が自動的に挿入されます。たとえば、デフォルト設定行または設定変更日時などが、FWSM によって挿入されます。これらの自動エントリの情報は、テキスト ファイルの作成時に入力する必要はありません。

行の順序

ほとんどの場合、ファイルには、任意の順序でコマンドを設定できます。ただし、Access Control Entry（ACE; アクセス制御エントリ）などの行は表示された順序で処理され、この順序が、アクセス リストの動作に影響します。ほかにも、順序が影響するコマンドがあります。たとえば、最初にインターフェイスの **nameif** コマンドを入力する必要があります。後続の多数のコマンドでそのインターフェイスの名前を使用するからです。また、コマンド固有コンフィギュレーション モードのコマンドは、メイン コマンドのすぐあとに指定する必要があります。

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

一部のコマンドは、コンフィギュレーションの行に挿入されません。たとえば、**show running-config** などの実行時コマンドは、テキスト ファイルに対応する行が含まれません。

パスワード

ログイン、イネーブル、およびユーザの各パスワードは、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、[cisco] パスワードは、jMorNbK0514fadBh のように暗号化されます。コンフィギュレーションのパスワードは別の FWSM に暗号化された状態でコピーできますが、パスワードの暗号をユーザが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 FWSM にコピーしても、FWSM によってパスワードが自動的に暗号化されることはありません。FWSM 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** コマンドを入力して、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する場合だけです。

複数のセキュリティ コンテキスト ファイル

セキュリティ コンテキストが複数ある場合、コンフィギュレーション全体が複数のパーツに分割されます。

- セキュリティ コンテキストのコンフィギュレーション
- コンテキストのリストなど、FWSM の基本設定を含むシステム 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のネットワーク インターフェイスを提供する admin コンテキスト

  システム コンフィギュレーション自体には、インターフェイスまたはネットワーク設定は含まれません。（サーバからコンテキストをダウンロードするなど）ネットワーク リソースにアクセスする必要がある場合、システムは、admin コンテキストとして設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 モードの設定と同様です。システム コンフィギュレーションは、コンテキストのコンフィギュレーションとは異なります。システム コンフィギュレーションにはシステム専用コマンド（全コンテキストのリストなど）だけが含まれ、（多数のインターフェイス パラメータなどの）一般的なコマンドは含まれません。

アドレス、プロトコル、およびポート

この付録は、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 リファレンスです。ここで説明する内容は次のとおりです。

- IPv4 アドレスおよびサブネット マスク（p.D-2）
- IPv6 アドレス（p.D-6）
- プロトコルおよびアプリケーション（p.D-13）
- TCP ポートおよび UDP ポート（p.D-14）
- ローカル ポートおよびプロトコル（p.D-16）
- ICMP のタイプ（p.D-17）

IPv4 アドレスおよびサブネット マスク

ここでは、FWSM で IPv4 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 進数で表記される 32 ビットの数値です。バイナリから 10 進数に変換された 4 つの 8 ビット フィールド（オクテット）が、ドットで区切られて表記されます。IP アドレスの最初のパートはホストが存在するネットワークを識別し、2 つめのパートは特定ネットワーク上の特定ホストを識別します。ネットワーク番号フィールドは、ネットワーク プレフィクスと呼ばれます。特定ネットワーク上のホストはすべて同じネットワーク プレフィクスを共有しますが、ホスト番号は固有でなければなりません。クラスフル IP では、アドレスのクラスによって、ネットワーク プレフィクスとホスト番号を区切る位置が異なります。

次の内容について説明します。

- クラス（p.D-2）
- プライベート ネットワーク（p.D-2）
- サブネット マスク（p.D-3）

クラス

IP ホスト アドレスは 3 つの異なるアドレス クラスに分けられています。クラス A、クラス B、およびクラス C です。各クラスは、32 ビット アドレス内のネットワーク プレフィクスとホスト番号の区切り箇所がそれぞれ異なります。クラス D アドレスは、マルチキャスト IP 専用です。

- クラス 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 プレフィクスとして使用します。
- クラス 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 プレフィクスとして使用します。
- クラス 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 プレフィクスとして使用します。

クラス A アドレスには 16,777,214 のホスト アドレス、クラス B には 65,534 のホスト アドレスが存在するので、サブネット マスクを使用して、これらの巨大なネットワークを、より小さなサブネットに分割できます。

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で、これらをインターネット上にルーティングする必要がない場合には、Internet Assigned Numbers Authority（IANA）が推奨しているプライベート IP アドレスを使用できます（RFC 1918 を参照）。プライベート ネットワークに使用できるアドレス範囲は、次のとおりです。これらのアドレスはアドバタイズすべきではありません。

- 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、単一のクラス A、クラス B、またはクラス 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 マスクでは、ホスト番号のビットをネットワーク プレフィクスに追加して、拡張ネットワーク プレフィクスを作成できます。たとえば、クラス C のネットワーク プレフィクスには、常に IP アドレスの最初の 3 オクテットが使用されます。クラス C 拡張ネットワーク プレフィクスの場合には、さらに 4 つめのオクテットの一部が使用されます。

サブネット マスクは、ドット付き 10 進数ではなくバイナリ表記を使用するほうが簡単に理解できます。サブネット マスク内のビットは、インターネット アドレスと 1 対 1 で対応しています。

- IP アドレス内の対応ビットが拡張ネットワーク プレフィクスの一部である場合には、ビットは 1 に設定されます。
- 対応ビットがホスト番号の一部である場合には、ビットは 0 に設定されます。

例 1：クラス B アドレス 129.10.0.0 について、3 つめのオクテット全部をホスト番号ではなく拡張ネットワーク プレフィクスに使用したい場合、サブネット マスク 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、クラス B アドレスは、最後のオクテットだけをホスト番号に使用するクラス C アドレスと同等になります。

例 2：3 つめのオクテットの一部だけを拡張ネットワーク プレフィクスに使用したい場合には、サブネット マスクを 11111111.11111111.11111000.00000000 などのように指定します。この場合、3 つめ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*）マスクで記述できます。例 1 の場合、ドット付き 10 進数マスクにすると、各バイナリ オクテットを 10 進数に変換した 255.255.255.0 になります。/ *ビット* マスクの場合、1 の数を指定するため、/24 になります。例 2 の場合、ドット付き 10 進数は 255.255.248.0、/ ビットは /21 です。

また、3 つめ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することによって、複数のクラス C ネットワークを、より大規模なネットワークに統合することもできます（たとえば、192.168.0.0/20）。

次の内容について説明します。

- サブネット マスクの判別（p.D-3）
- サブネット マスクで使用するアドレスの判別（p.D-4）

サブネット マスクの判別

使用したいホスト数に適したサブネット マスクを判別するには、表 D-1 を参照してください。

表 D-1　ホスト、ビット、およびドット付き 10 進数マスク

ホスト数[1]	/ 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 クラス A ネットワーク
65,536	/16	255.255.0.0 クラス 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

表 D-1　ホスト、ビット、およびドット付き 10 進数マスク（続き）

ホスト数[1]	/ ビット マスク	ドット付き 10 進数マスク
512	/23	255.255.254.0
256	/24	255.255.255.0 クラス 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
未使用	/31	255.255.255.254
1	/32	255.255.255.255 単一ホスト アドレス

1. 単一ホストである /32 を除き、サブネットの最初と最後の番号は予約済みです。

サブネット マスクで使用するアドレスの判別

ここでは、クラス C およびクラス B 規模のネットワークにサブネット マスクを適用する場合、使用できるネットワーク アドレスを判別する方法を示します。次の内容について説明します。

- クラス C 規模のネットワーク アドレス（p.D-4）
- クラス B 規模のネットワーク アドレス（p.D-5）

クラス C 規模のネットワーク アドレス

2 ～ 254 のホスト数のネットワークでは、4 つめのオクテットが 0 から始まり、ホスト アドレス数の倍数になります。次に、192.168.0.x の 8 ホストのサブネット（/29）の例を示します。

マスク /29（255.255.255.248）のサブネット	アドレス範囲[1]
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

1. サブネットの最初と最後のアドレスは予約済みです。最初のサブネットの例では、192.168.0.0 または 192.168.0.7 は使用できません。

クラス B 規模のネットワーク アドレス

ホスト数が 254 ～ 65,534 のネットワークにサブネット マスクを適用する場合、使用するネットワーク アドレスを判別するには、使用できる各拡張ネットワーク プレフィクスについて、3 つめのオクテットの値を決定する必要があります。たとえば、10.1.*x*.0 のようなアドレスのサブネットを作成する場合、最初の 2 つのオクテットは拡張ネットワーク プレフィクスに使用されるので固定され、4 つめのオクテットの全ビットがホスト番号に使用されます。

3 つめのオクテットの値を決定する手順は、次のとおりです。

ステップ 1　65,536（3 つめと 4 つめのオクテットで使用できるアドレスの総数）を使用したいホスト アドレス数で割って、ネットワークに作成できるサブネット数を計算します。

たとえば、65,536 を 4096 で割った値は 16 です。

したがって、クラス B ネットワークに、それぞれ 4096 のアドレスを持つ 16 のサブネットを作成できます。

ステップ 2　256（3 つめのオクテットの値の数）をサブネット数で割って、3 つめのオクテット値の倍数を算出します。

この例では、256/16 = 16 です。

3 つめのオクテットは、0 から開始され、16 の倍数になります。

次に、ネットワーク 10.1 の 16 のサブネットを示します。

マスク /20（255.255.240.0）のサブネット	アドレス範囲[1]
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

1. サブネットの最初と最後のアドレスは予約済みです。最初のサブネットの例では、10.1.0.0 または 10.1.15.255 は使用できません。

IPv6 アドレス

IPv6 は IPv4 の次世代のインターネット プロトコルです。アドレス スペースが拡張され、ヘッダー フォーマットが簡素化され、拡張やオプション、フロー ラベリング機能、認証やプライバシー機能のサポートが向上しています。IPv6 は RFC 2460 で規定されています。IPv6 のアドレス指定アーキテクチャは RFC 3513 で規定されています。

ここでは、IPv6 アドレス フォーマットとアーキテクチャについて説明します。内容は次のとおりです。

- IPv6 アドレス フォーマット（p.D-6）
- IPv6 アドレス タイプ（p.D-7）
- IPv6 アドレス プレフィクス（p.D-12）

（注） ここでは、IPv6 のアドレス フォーマット、タイプ、プレフィクスについて説明します。FWSM で IPv6 を使用するよう設定する方法については、第 9 章「IPv6 の設定」を参照してください。

IPv6 アドレス フォーマット

IPv6 アドレスは、コロン（:）で区切った 8 個の 16 ビット 16 進数フィールドで表現されます。x:x:x:x:x:x:x:x というフォーマットになります。IPv6 アドレスの例を 2 つ挙げます。

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A

（注） IPv6 アドレスの 16 進数の文字では、大文字と小文字は区別されません。

アドレスの個々のフィールドで、先行 0 は記述する必要がありません。しかし、各フィールドに 1 桁以上の値を入力する必要があります。そのため、アドレスの例 2001:0DB8:0000:0000:0008:0800:200C:417A の場合、左から 3 番めから 6 番めのフィールドの先行 0 を省略して、2001:0DB8:0:0:8:800:200C:417A とすることができます。すべてが 0 のフィールド（左から 3 番めと 4 番め）は、1 個の 0 として表現できます。左から 5 番めのフィールドは 3 個の先行 0 を省略して 8 だけを残し、左から 6 番めのフィールドは 1 個の先行 0 を省略して 800 だけを残しています。

いくつかの連続する 16 進数の 0 のフィールドを持つことは、IPv6 のアドレスに一般的に見られることです。2 個のコロン（::）を使用して、IPv6 アドレスの最初、中間、最後の連続する 0 のフィールドを圧縮することができます（コロンは連続する 16 進数の 0 のフィールドを示します）。表 D-2 に、各種 IPv6 アドレスのアドレス圧縮の例を示します。

表 D-2　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）連続した 0 のフィールドを示すために IPv6 アドレスで 2 つのコロン（::）を使用できるのは 1 回のみです。

IPv4 と IPv6 が混在する環境では、別の IPv6 フォーマットも使用されます。そのフォーマットは x:x:x:x:x:x:y.y.y.y です。ここで、x は IPv6 の上位 6 個の部分を示す 16 進数の値で、y は 32 ビットの IPv4 アドレス部分を示す 10 進数の値（IPv6 アドレスの残りの 2 つの 16 ビット部分を利用）です。たとえば、192.168.1.1 という IPv4 アドレスは、IPv6 アドレスで 0:0:0:0:0:0:FFFF:192.168.1.1 または ::FFFF:192.168.1.1 と表現できます。

IPv6 アドレス タイプ

IPv6 アドレスの主要タイプは、次の 3 つです。

- **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るパケットは、このアドレスで識別されるインターフェイスに伝送されます。1 つのインターフェイスには、複数のユニキャスト アドレスを割り当てることができます。
- **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るパケットは、このアドレスで識別されるすべてのアドレスに伝送されます。
- **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 アドレスと異なり、エニーキャスト アドレスに送信されるパケットは、ルーティング プロトコルの距離測定に従って、「直近の」インターフェイスにのみ伝送されます。

（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 アドレスがブロードキャスト機能を提供します。

次の内容について説明します。

- ユニキャスト アドレス（p.D-7）
- マルチキャスト アドレス（p.D-10）
- エニーキャスト アドレス（p.D-11）
- 必須アドレス（p.D-11）

ユニキャスト アドレス

ここでは、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示します。

次の内容について説明します。

- グローバル アドレス（p.D-8）
- サイトローカル アドレス（p.D-8）
- リンクローカル アドレス（p.D-8）
- IPv4 互換 IPv6 アドレス（p.D-8）
- 未指定アドレス（p.D-9）
- ループバック アドレス（p.D-9）
- インターフェイス識別子（p.D-9）

グローバル アドレス

IPv6 グローバル ユニキャスト アドレスの一般フォーマットは、グローバル ルーティング プレフィクス、サブネット ID、インターフェイス ID を順に並べた形になります。グローバル ルーティング プレフィクスには、IPv6 アドレス タイプで予約されているものを除いて、任意のプレフィクスを使用できます（IPv6 アドレス タイプのプレフィクスの詳細については、「IPv6 アドレス プレフィクス」[p.D-12] を参照）。

グローバル ユニキャスト アドレス（バイナリ 000 で始まるものを除く）は、Modified EUI-64 フォーマットの 64 ビット インターフェイス ID を持ちます。インターフェイス識別子の Modified EUI-64 フォーマットの詳細については、「インターフェイス識別子」（p.D-9）を参照してください。

バイナリ 000 で始まるグローバル ユニキャスト アドレスは、アドレスのインターフェイス ID 部分のサイズや構成について、制約はありません。このタイプのアドレスの一例は、IPv4 アドレスが組み込まれた IPv6 アドレスです（「IPv4 互換 IPv6 アドレス」[p.D-8] を参照）。

サイトローカル アドレス

サイトローカル アドレスは、サイト内のアドレス指定に使用されます。グローバルに一意なプレフィクスを使用しなくても、サイト全体のアドレス指定が行えます。サイトローカル アドレスは、プレフィクス FEC0::/10 のあとに、54 ビットのサブネット ID、Modified EUI-64 フォーマットの 64 ビットのインターフェイス ID が続きます。

サイトローカル ルータは、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サイト外部に転送しません。そのため、サイトローカル アドレスはプライベート アドレスと考えられます。

リンクローカル アドレス

インターフェイスには、少なくとも 1 つのリンクローカル アドレスが必要です。各インターフェイスに複数の 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、リンクローカル プレフィクス FE80::/10 と Modified EUI-64 フォーマットのインターフェイス識別子によって任意のインターフェイス上で自動的に設定される 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、Neighbor Discovery Protocol およびステートレス自動コンフィギュレーション 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、通信用のサイトローカル アドレスまたはグローバルに一意なアドレスがなくても、通信が可能です。

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転送しません。そのため、リンクローカル アドレスはプライベート アドレスと考えられます。

IPv4 互換 IPv6 アドレス

IPv4 アドレスの組み込みが可能な IPv6 アドレスは、2 種類あります。

1 つめのタイプは、「IPv4 互換 IPv6 アドレス」です。IPv6 移行メカニズムでは、ホストとルータで IPv4 ルーティング インフラストラクチャ上を IPv6 パケットをダイナミックにトンネリングさせる技法が取られています。この技法を使用した IPv6 ノードには、下位 32 ビットにグローバル IPv4 アドレスを組み込んだ特別な 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、フォーマットは ::y.y.y.y です。y.y.y.y が IPv4 ユニキャスト アドレスです。

（注）「IPv4 互換 IPv6 アドレス」で使用される IPv4 アドレスは、グローバルに一意な IPv4 ユニキャスト アドレスでなければなりません。

2 つめのタイプの IPv6 アドレスは、Ipv4 アドレスが組み込まれており、「IPv4 マップ 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 アドレスとして表現するために使用します。このタイプのアドレス フォーマットは、::FFFF:y.y.y.y です。y.y.y.y が 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ます。たとえば、IPv6 ネットワークで新しく初期化したノードは、IPv6 アドレスを受信するまで、パケットの送信元アドレスとして未指定アドレスを使用することができます。

（注）IPv6 未指定アドレスは、インターフェイスには割り当てることができません。未指定 IPv6 アドレスは、IPv6 パケットまたは IPv6 ルーティング ヘッダーの宛先アドレスとして使用しないでください。

ループバック アドレス

ノードで IPv6 パケットを自分宛に送信するため、ループバック アドレス 0:0:0:0:0:0:0:1 を使用することができます。IPv6 のループバック アドレスの機能は、IPv4 のループバック アドレス（127.0.0.1）と同じです。

（注）IPv6 ループバック アドレスは、物理インターフェイスには割り当てることができません。送信元アドレスまたは宛先アドレスとして IPv6 ループバック アドレスを持つパケットは、パケットを作成したノードの外部に転送されないようにする必要があります。IPv6 ルータは、送信元アドレスまたは宛先アドレスに IPv6 ループバック アドレスを持つ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 アドレスのインターフェイス識別子は、リンク上でのインターフェイスの識別に使用されます。これは、サブネット プレフィクス内で一意でなければなりません。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のリンク層アドレスに基づいて作成されます。インターフェイスが異なるサブネットに属していれば、同じインターフェイス識別子をシングル ノードの複数のインターフェイスで使用することができます。

ユニキャスト アドレス（バイナリ 000 で始まるものを除く）の場合、インターフェイス識別子は 64 ビットの Modified EUI-64 フォーマットで構成する必要があります。Modified EUI-64 フォーマットは、アドレスのユニバーサル / ローカル ビットを反転し、MAC アドレスの上位 3 バイトと下位 3 バイトの間に 16 進数の FFFE を挿入することにより、48 ビット MAC アドレスから生成されます。

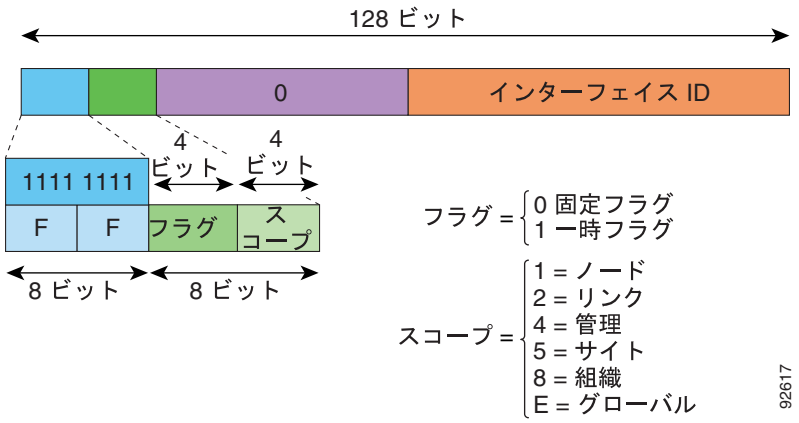
たとえば、MAC アドレスが 00E0.b601.3B7A のインターフェイスの場合、64 ビットのインターフェイス ID は 02E0:B6FF:FE01:3B7A となります。

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るパケットは、このマルチキャスト アドレスで示されるすべてのアドレスに伝送されます。1 つのインターフェイスは、任意の数のマルチキャスト グループに属することができます。

IPv6 マルチキャスト アドレスのプレフィクスは FF00::/8（1111 1111）です。プレフィクスに続くオクテットは、マルチキャスト アドレスのタイプとスコープを定義するためのものです。永久に割り当てられる（「既知」）マルチキャスト アドレスにはフラグ パラメータ 0 が割り当てられ、一時（「一時的」）マルチキャスト アドレスにはフラグ パラメータ 1 が割り当てられます。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 アドレスは、それぞれ 1、2、5、8、E のスコープ パラメータを持ちます。たとえば、プレフィクスが FF02::/16 のマルチキャスト アドレスは、リンク スコープを持つ永久マルチキャスト アドレスです。図 D-1 に、IPv6 マルチキャスト アドレスのフォーマットを示します。

図 D-1　IPv6 マルチキャスト アドレス フォーマット



IPv6 ノード（ホストとルータ）は、次のマルチキャスト グループに加入する必要があります。

- 全ノードのマルチキャスト 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）
- ノード上の各 IPv6 ユニキャスト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 FF02:0:0:0:0:1:FFXX:XXXX/104。XX:XXXX はユニキャストまたはエニーキャスト アドレスの下位 24 ビット

（注） 送信要求ノード アドレスは、ネイバの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 グループに加入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 パケットの送信元アドレスとして使用することはできません。

（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、異なるノードに属する）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るパケットは、そのアドレスを持つ直近のインターフェイスにルーティングされます。直近インターフェイスは、有効なルーティング プロトコルに基づいて判断されます。

エニーキャスト アドレスはユニキャスト アドレス スペース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 アドレスで、その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インターフェイスを設定する必要があります。

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することはできません。
- 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 ルータへの割り当てだけが可能です。

（注）FWSM では、エニーキャスト アドレス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、次のアドレスを設定する必要があります（自動または手動で）。

- 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
- 全ノードのマルチキャスト アドレス
- 各ユニキャスト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、次のアドレスを設定する必要があります（自動または手動で）。

- 必須ホスト アドレス
- 全インターフェイスのルータとして動作するよう設定したサブネットルータのエニーキャスト アドレス
- 全ルータのマルチキャスト アドレス

IPv6 アドレス プレフィクス

アドレス スペース全体の連続するビット ブロックを示すため、ipv6-prefix/prefix-length というフォーマットの IPv6 アドレス プレフィックスを使用することができます。IPv6 のプレフィックスは、RFC 2373 に規定された形式でなければなりません。RFC 2373 では、アドレスは 16 ビットの値をコロンで区切った 16 進数で指定されています。プレフィクス長は、プレフィクスを構成するアドレスの上位の連続ビット（アドレスのネットワーク部分）の桁数を示す 10 進数の値です。たとえば、2001:0DB8:8086:6502::/32 は IPv6 プレフィクスとして有効です。

IPv6 プレフィクスは IPv6 アドレスのタイプを識別するためのものです。表 D-3 に、IPv6 の各アドレス タイプのプレフィクスを示します。

表 D-3　IPv6 アドレス タイプのプレフィクス

アドレス タイプ	バイナリ プレフィクス	IPv6 の表記
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）	その他のアドレス	
エニーキャスト	ユニキャスト アドレス スペースから取得	

プロトコルおよびアプリケーション

表 D-4 に、プロトコルの文字名およびポート番号を示します。どちらも、FWSM のコマンドに入力できます。

表 D-4　プロトコルの文字名

文字名	番号	説明
ah	51	IPv6 の認証ヘッダー、RFC 1826
eigrp	88	Enhanced Interior Gateway Routing Protocol
esp	50	IPv6 の Encapsulated Security Payload（カプセル化セキュリティ ペイロード）、RFC 1827
gre	47	Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）
icmp	1	Internet Control Message Protocol、RFC 792
icmp6	58	IPv6 の Internet Control Message Protocol、RFC 2463
igmp	2	Internet Group Management Protocol、RFC 1112
igrp	9	Interior Gateway Routing Protocol
ip	0	Internet Protocol
ipinip	4	IP-in-IP カプセル化
ipsec	50	IP セキュリティ。ipsec プロトコルの文字の入力は、esp プロトコルの文字の入力と同じです。
nos	94	Network Operating System（Novell NetWare）
ospf	89	Open Shortest Path First（OSPF）ルーティング プロトコル、RFC 1247
pcp	108	Payload Compression Protocol
pim	103	Protocol Independent Multicast
pptp	47	Point-to-Point Tunneling Protocol（ポイントツーポイント トンネリング プロトコル）。pptp プロトコルの文字の入力は、gre プロトコルの文字の入力と同じです。
snp	109	Sitara Networks Protocol
tcp	6	TCP、RFC 793
udp	17	UDP、RFC 768

プロトコル番号は、IANA の Web サイトからオンラインで表示できます。

http://www.iana.org/assignments/protocol-numbers

TCP ポートおよび UDP ポート

表 D-5 に、文字名およびポート番号を示します。どちらも、FWSM のコマンドに入力できます。次の事項に注意してください。

- FWSM は、SQL*Net 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 のポート割り当てと一致していません。
- FWSM は、ポート 1645 および 1646 で RADIUS を待ち受けます。RADIUS サーバが標準ポート 1812 および 1813 を使用している場合、**authentication-port** および **accounting-port** コマンドを使用して、これらのポートを待ち受けるよう FWSM を設定することができます。
- ポートに DNS アクセスを割り当てる場合には、**dns** ではなく、**domain** 文字名を使用してください。**dns** を使用した場合、FWSM では **dnsix** 文字名が使用されたとみなされます。

ポート番号は、IANA の Web サイトからオンラインで表示できます。

http://www.iana.org/assignments/port-numbers

表 D-5　ポートの文字名

文字名	TCP/UDP	番号	説明
aol	TCP	5190	America Online
bgp	TCP	179	Border Gateway Protocol（BGP）、RFC 1163
biff	UDP	512	新着メールをユーザに通知するメール システムで使用
bootpc	UDP	68	ブートストラップ プロトコル クライアント
bootps	UDP	67	ブートストラップ プロトコル サーバ
chargen	TCP	19	キャラクタ ジェネレータ
citrix-ica	TCP	1494	Citrix Independent Computing Architecture（ICA）プロトコル
cmd	TCP	514	**exec** と同様だが、**cmd** は自動認証をサポート
ctiqbe	TCP	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	TCP	13	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	エコー
exec	TCP	512	リモート プロセスの実行
finger	TCP	79	フィンガ
ftp	TCP	21	FTP（ファイル転送プロトコル）（制御ポート）
ftp-data	TCP	20	FTP（データ ポート）
gopher	TCP	70	Gopher
https	TCP	443	HTTP over SSL
h323	TCP	1720	H.323 コール シグナリング
hostname	TCP	101	NIC ホスト ネーム サーバ
ident	TCP	113	Ident 認証サービス
imap4	TCP	143	Internet Message Access Protocol（IMAP）Version 4
irc	TCP	194	Internet Relay Chat Protocol
isakmp	UDP	500	Internet Security Association and Key Management Protocol（ISAKMP）

表 D-5　ポートの文字名（続き）

文字名	TCP/UDP	番号	説明
kerberos	TCP、UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn Shell
ldap	TCP	389	Lightweight Directory Access Protocol
ldaps	TCP	636	Lightweight Directory Access Protocol（SSL）
lpd	TCP	515	Line Printer Deamon ― プリンタ スプーラ
login	TCP	513	リモート ログイン
lotusnotes	TCP	1352	IBM Lotus Notes
mobile-ip	UDP	434	Mobile IP エージェント
nameserver	UDP	42	ホスト ネーム サーバ
netbios-ns	UDP	137	NetBIOS ネーム サービス
netbios-dgm	UDP	138	NetBIOS データグラム サービス
netbios-ssn	TCP	139	NetBIOS セッション サービス
nntp	TCP	119	Network News Transfer Protocol（NNTP）
ntp	UDP	123	Network Time Protocol（NTP）
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、リバース パス フラッディング、dense（密）モード
pop2	TCP	109	POP Version 2
pop3	TCP	110	POP Version 3
pptp	TCP	1723	Point-to-Point Tunneling Protocol（PPTP）
radius	UDP	1645	Remote Authentication Dial-In User Service（RADIUS）
radius-acct	UDP	1646	RADIUS（アカウンティング）
rip	UDP	520	Routing Information Protocol（RIP）
secureid-udp	UDP	5510	SecureID over UDP
smtp	TCP	25	Simple Mail Transport Protocol（SMTP）
snmp	UDP	161	SNMP（簡易ネットワーク管理プロトコル）
snmptrap	UDP	162	SNMP ― トラップ
sqlnet	TCP	1521	Structured Query Language（SQL）ネットワーク
ssh	TCP	22	Secure Shell
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（TACACS+）
talk	TCP、UDP	517	Talk
telnet	TCP	23	RFC 854 Telnet
tftp	UDP	69	TFTP（簡易ファイル転送プロトコル）
time	UDP	37	Time
uucp	TCP	540	UNIX-to-UNIX Copy Program（UUCP）
who	UDP	513	Who

表 D-5　ポートの文字名（続き）

文字名	TCP/UDP	番号	説明
whois	TCP	43	Who Is
www	TCP	80	WWW
xdmcp	UDP	177	X Display Manager Control Protocol

ローカル ポートおよびプロトコル

表 D-6 に、FWSM 宛に送信されたトラフィックを処理するために FWSM がオープンするプロトコル、TCP ポート、UDP ポートの一覧を示します。表 D-6 に示した機能とサービスをイネーブルにしないと、FWSM はローカル プロトコル、TCP ポート、UDP ポートをオープンしません。FWSM でデフォルトのリスニング プロトコルまたはポートをオープンするには、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場合、デフォルトポート以外のポートを設定できます。

表 D-6　機能とサービスによりオープンされるプロトコルおよびポート

機能またはサービス	プロトコル	ポート番号	説明
DHCP	UDP	67、68	—
フェールオーバー制御	108	適用外	—
HTTP	TCP	80	—
HTTPS	TCP	443	—
ICMP	1	適用外	—
IGMP	2	適用外	プロトコルは宛先 IP アドレス 224.0.0.1 でのみオープン
ISAKMP/IKE	UDP	500	設定可能
IPSec（ESP）	50	適用外	—
NTP	UDP	123	—
OSPF	89	適用外	プロトコルは宛先 IP アドレス 224.0.0.5 および 224.0.0.6 でのみオープン
PIM	103	適用外	プロトコルは宛先 IP アドレス 224.0.0.13 でのみオープン
RIP	UDP	520	—
RIPv2	UDP	520	プロトコルは宛先 IP アドレス 224.0.0.9 でのみオープン
SNMP	UDP	161	設定可能
SSH	TCP	22	—
ステートフル アップデート	105	適用外	—
Telnet	TCP	23	—

ICMP のタイプ

表 D-7 に、FWSM のコマンドに入力できる ICMP のタイプ番号および名前を示します。

表 D-7　ICMP のタイプ

ICMP 番号	ICMP 名
0	echo-reply（エコー応答）
3	unreachable（到達不能）
4	source-quench
5	redirect（リダイレクト）
6	alternate-address（代替アドレス）
8	echo（エコー）
9	router-advertisement（ルータ アドバタイズ）
10	router-solicitation（ルータ送信要求）
11	time-exceeded（時間超過）
12	parameter-problem（パラメータの問題）
13	timestamp-request（タイムスタンプ要求）
14	timestamp-reply（タイムスタンプ応答）
15	information-request（情報要求）
16	information-reply（情報応答）
17	mask-request（マスク要求）
18	mask-reply（マスク応答）
31	conversion-error（変換エラー）
32	mobile-redirect（モバイル リダイレクト）

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | あ | い | お | か | き | く | こ | さ | し | す | せ | た | て | と | に | ね | の | は | ひ | ふ | へ | ほ | ま | め | も | ゆ | り | る | れ |

数値

3DES DES を参照してください。

A

A レコード アドレス 「A」はアドレスの意味で、DNS の名前 / アドレス マップ レコードを指します。

AAA Authentication, Authorization, Accounting（認証、許可、アカウンティング）。TACACS+ および RADIUS も参照してください。

ABR Area Border Router（エリア境界ルータ）。OSPF では、マルチエリアのインターフェイスを持つルータ。

ACE Access Cntrol Entry（アクセス制御エントリ）。設定に入力された情報で、インターフェイスで許可または拒否するトラフィックのタイプを指定するものです。デフォルトでは、明示的に許可されていないトラフィックは拒否されます。

ACL Access Control List（アクセス制御リスト）。ACE の集まり。ACL を使用すると、インターフェイス上で許可するトラフィックのタイプを指定できます。デフォルトでは、明示的に許可されていないトラフィックは拒否されます。通常、ACL は着信トラフィックの送信元のインターフェイスに適用されます。ルール、発信 ACL の項も参照してください。

ActiveX モバイル（ポータブル）プログラムを作成するために使用される、オブジェクト指向プログラミング テクノロジーとツールのセット。ActiveX プログラムは Java アプレットに類似したものです。

Address Resolution Protocol ARP を参照してください。

AES Advanced Encryption Standard（高度暗号規格）。情報を暗号化および復号化できる対称ブロック サイファ。AES アルゴリズムでは、128、192、256 ビットの暗号キーを使用して、128 ビットのブロック単位でデータの暗号化と復号化を行うことができます。DES の項も参照してください。

AH Authentication Header（認証ヘッダー）。データの整合性、認証、および再送検出を保証するための IP プロトコル（タイプ 51）。AH は、保護対象のデータに組み込まれます（完全 IP データグラムなど）。AH は、単独で使用することも、ESP と一緒に使用することもできます。これは古い IPSec プロトコルで、大部分のネットワークにおいて ESP ほどの重要性はありません。AH は認証サービスには対応していますが、暗号化サービスには対応していません。これは ESP（認証と暗号化の両方に対応）をサポートしていない IPSec ピアとの互換性を保証するために用意されています。暗号化および VPN の項も参照してください。RFC 2402 を参照してください。

ARP Address Resolution Protocol（アドレス解決プロトコル）。ハードウェア アドレス（MAC アドレス）を IP アドレスにマッピングする下位レベルの TCP/IP プロトコル。ハードウェア アドレスは、00:00:a6:00:01:ba のようになります。最初の 3 つの文字グループ（00:00:a6）は製造メーカーを示し、残りの文字（00:01:ba）はシステム カードを示します。ARP は RFC 826 で定義されています。

ASA Adaptive Security Algorithm（アダプティブ セキュリティ アルゴリズム）。検査を実行するために FWSM で使用されます。ASA では、内部システムとアプリケーションの明示的な設定がなくても、一方向（内部から外部へ）の接続が可能です。インスペクション エンジンの項も参照してください。

ASA Adaptive Security Appliance（アダプティブ セキュリティ アプライアンス）。

ASDM Adaptive Security Device Manager（アダプティブ セキュリティ デバイス マネージャ）。シングル FWSM の管理と設定を行うためのアプリケーション。

B

BGP Border Gateway Protocol。BGP は、TCP/IP ネットワークのドメイン間ルーティングを行います。BGP は Exterior Gateway Protocol（EGP; 外部ゲートウェイ プロトコル）で、複数の Autonomous System（AS; 自律システム）やドメイン間のルーティングを行い、他の BGP システムとルーティング情報やアクセス情報を交換します。FWSM は BGP をサポートしていません。EGP の項も参照してください。

BLT ストリーム Bandwidth Limited Traffic（帯域幅制限トラフィック）ストリーム。帯域幅が制限されたパケットのストリームまたはフロー。

BOOTP Bootstrap Protocol（ブートストラップ プロトコル）。ディスクレス ワークステーションをネットワーク上でブートできます。RFC 951 および RFC 1542 に規定されています。

BPDU Bridge Protocol Data Unit（ブリッジ プロトコル データ ユニット）。ネットワークのブリッジ間で情報を交換するため、設定可能な間隔で送出されるスパニングツリー プロトコルの hello パケット。プロトコル データ ユニットはパケットに相当する OSI の用語です。

C

CA Certificate Authority、Certification Authority（認承局）。証明書の発行と取り消しを行うサードパーティの機関。CA の公開鍵を持つ装置は、CA が発行した証明書を持つ装置の認証を行うことができます。CA という用語は、CA サービスを提供するソフトウェアを指す用語としても使用されます。証明書、CRL、公開鍵、RA の項も参照してください。

CBC Cipher Block Chaining（暗号ブロック連鎖）。アルゴリズムの暗号化強度を高める暗号技法。CBC には、暗号化を開始するための Initialization Vector（初期化ベクトル）が必要です。IV は IPSec のパケットで明示的に与えられます。

CHAP Challenge Handshake Authentication Protocol。

CLI Command-Line Interface（コマンドライン インターフェイス）。FWSM にコンフィギュレーションおよびモニタリング コマンドを入力するためのプライマリ インターフェイス。

CPU Central Processing Unit（中央演算処理装置）。メイン プロセッサ。

CRC Cyclical Redundancy Check（巡回冗長検査）。エラーチェック技法。この技法では、フレーム受信側が、フレームの容量に生成多項式の除算を適用して剰余を計算し、それを送信側ノードがフレームに保存した値と比較します。

CRL

Certificate Revocation List（証明書失効リスト）。所定の CA によってリスト化された、最新だが取り消された証明書をすべて記載したデジタル署名付きメッセージ。これは、店が不正なクレジット カードを拒否するために使用する、盗まれたクレジット カード番号のリストと同様のものです。証明書が取り消されると、その情報が CRL に追加されます。証明書を使用した認証を実装する場合、CRL を使用するかどうかを選択できます。CRL を使用すると、期限切れになる前に容易に証明書の取り消しが行えますが、CRL は一般的に CA や RA でのみ管理されています。CRL を使用していて、認証が要求されたときに CA や RA との接続ができない場合、認証要求は失敗します。CA、証明書、公開鍵、RA の項も参照してください。

CRV

Call Reference Value（呼参照値）。2 つのエンティティ間で発信されるコール レッグを区別するために H.225.0 で使用されます。

CTIQBE

Computer Telephony Interface Quick Buffer Encoding。IP テレフォニーにおいて、Cisco CallManager と CTI TAPI および JTAPI アプリケーションの間で使用されるプロトコル。CTIQBE は TAPI/JTAPI プロトコル検査モジュールで使用され、NAT、PAT、および双方向 NAT をサポートしています。これにより、Cisco IP SoftPhone や Cisco TAPI/JTAPI アプリケーションが、FWSM を越えて Cisco CallManager とコール セットアップや音声トラフィックの通信を行うことができます。

D

DES

Data Encryption Standard（データ暗号化規格）。DES は 1977 年に米国商務省標準局によって発表された、IBM の Lucifer アルゴリズムに基づく秘密鍵暗号化方式です。Cisco では、標準暗号 DES（40 ビットおよび 56 ビットのキー長）、IPSec 暗号（56 ビットのキー）、3DES（トリプル DES：56 ビットのキーにより 3 回暗号化を行う）を使用しています。3DES は DES よりも安全性が高いですが、暗号化と復号化に多くの処理が必要となります。AES、ESP の項も参照してください。

DHCP

Dynamic Host Configuration Protocol。ホストで IP アドレスが不要になったときにそのアドレスが再利用でき、モバイル コンピュータ（ラップトップなど）が接続する LAN で有効な IP アドレスを受け取れるよう、ホストにダイナミックに IP アドレスを割り当てるメカニズムを提供します。

Diffie-Hellman

セキュアでない通信チャネルで 2 者が秘密情報を共有するための公開鍵暗号化プロトコル。Diffie-Hellman は、IKE 内でセッション キーを確立するために使用されます。Diffie-Hellman は Oakley キー交換のコンポーネントです。

Diffie-Hellman グループ 1、グループ 2、グループ 5、グループ 7

Diffie-Hellman とは、フェーズ 1 とフェーズ 2 の SA を確立するために、大きな素数に基づく非対称暗号化を使用した公開鍵暗号化のタイプです。グループ 1 はグループ 2 より小さな素数を使用しますが、IPSec ピアでグループ 1 しかサポートされていないこともあります。Diffie-Hellman グループ 5 では 1536 ビットの素数を使用するため、安全度が最も高く、AES での使用に最適です。グループ 7 は 163 ビットの楕円曲線フィールドを持ち、Movian VPN クライアントでの使用に適していますが、グループ 7（ECC）をサポートしているピアであれば一緒に使用することができます。VPN および暗号化の項も参照してください。

DMZ

インターフェイスを参照してください。

DN

Distinguished Name（認定者名）。OSI Direcroty（X.500）のグローバルな正規のエントリ名です。

DNS

Domain Nama System（ドメイン ネーム システム）、Domain Name Service（ドメイン ネーム サービス）。ドメイン名を IP アドレスに変換するインターネット サービス。

DoS

Denial of Service。ネットワーク サービスを利用不能にすることを目的としたネットワーク攻撃。

DSL

Digital Subscriber Line（デジタル加入者線）。従来の銅線で距離の制限された高帯域を提供する公共ネットワーク テクノロジー。DSL はモデム ペアを介して利用可能で、1 台のモデムはセントラル オフィスに、もう 1 台のモデムは顧客サイトに設置されます。大部分の DSL テクノロジーではツイストペアの帯域幅全体を使用しないので、音声チャネルのための余裕があります。

DSP Digital Signal Processor（デジタル シグナル プロセッサ）。DSP は、音声信号をフレームに分割し、音声パケットに格納します。

DSS Digital Signature Standard（デジタル シグニチャ規格）。公開鍵暗号化に基づいて米国国立標準技術研究所によって規定されたデジタル署名アルゴリズム。DSS は、ユーザ データグラムの暗号化を行いません。DSS は標準暗号化や Redcreek IPSec カードのコンポーネントですが、Cisco IOS ソフトウェアで実装されている IPSec のコンポーネントではありません。

E

ECHO ping、ICMP の項を参照してください。インスペクション エンジンの項も参照してください。

EGP Exterior Gateway Protocol（外部ゲートウェイ プロトコル）。BGP で代用されています。FWSM は EGP をサポートしていません。BGP の項も参照してください。

EIGRP Enhanced Interior Gateway Routing Protocol。FWSM は EIGRP をサポートしていません。

EMBLEM Enterprise Management BaseLine Embedded Manageability。Cisco IOS のシステム ログ フォーマットとの互換性を考慮して設計された Syslog フォーマットです。CiscoWorks 管理アプリケーションとの互換性が高められています。

ESMTP Extended SMTP（拡張 SMTP）。配信通知、セッション配信などの付加機能を持つ拡張版の SMTP。ESMTP については、RFC 1869「SMTP Service Extensions」に規定されています。

ESP Encapsulating Security Payload。IPSec プロトコルである ESP は、セキュアでないネットワーク上で、セキュアなトンネルを確立するための認証および暗号化サービスを提供します。詳細については、RFC 2406 および 1827 を参照してください。

F

FQDN/IP Fully Qualified Domain Name（完全修飾ドメイン名）/IP アドレス。セキュリティ ゲートウェイであるピアを識別するための IPSec のパラメータ。

FragGuard IP フラグメント保護の機能を持ち、すべての ICMP エラー メッセージの完全再組み立てと、FWSM でルーティングされる残りの IP フラグメントの仮想再組み立てを行います。

FTP File Transfer Protocol（ファイル転送プロトコル）。TCP/IP プロトコル スタックの一部で、ホスト間でのファイルの転送に使用されます。

G

GGSN Geteway GPRS Support Node（ゲートウェイ GPRS サポート ノード）。携帯電話ユーザが公共データ ネットワークや指定のプライベート IP ネットワークにアクセスできるようにする無線ゲートウェイ。

GMT Greenwich Mean Time（グリニッジ標準時）。世界標準時は、1967 年に Coordinated Universal Time（UTC; 協定世界時）に変わりました。

GPRS General Packet Radio Service。欧州通信規格協会によって定義および標準化されたサービス。GPRS は GSM ネットワークを IP パケットベースで拡張したもので、モバイル無線データ通信を可能にします。

GRE RFC 1701 および 1702 で規定された Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）。GRE は、IP トンネル内の各種プロトコル パケットをカプセル化し、IP ネットワーク上のリモート ポイントでルータへの仮想のポイントツーポイント リンクを作成する、トンネリング プロトコルです。シングル プロトコル バックボーン環境でマルチプロトコル サブネットワークを接続することにより、GRE を使用した IP トンネリングは、シングル プロトコル バックボーン環境でのネットワーク拡張を可能にします。

GSM Global System for Mobile Communication。モバイル無線音声通信用に開発されたデジタル モバイル無線通信の規格。

GTP GPRS Tunneling Protocol（GPRS トンネリング プロトコル）。GTP は、GPRS ネットワークの SGSN と GGSN の間で、ユーザ パケットとシグナリング情報のフローを処理します。GTP は GPRS ネットワークの Gn および Gp インターフェイスで定義されます。

H

H.225 テレビ会議などの用途で TCP シグナリングのために使用するプロトコル。H.323 およびインスペクション エンジンの項も参照してください。

H.225.0 H.225.0 セッションの確立とパケット化を管理する ITU 規格。H.225.0 では、実際に数種類のプロトコルを規定しています。規定されているのは、RAS、Q.931 の使用、RTP の使用などです。

H.245 H.245 のエンドポイント制御を管理する ITU 規格。

H.320 ISDN、フラクショナル T-1、交換型 56 K 回線などの回線交換型メディア上でのテレビ会議に関する一連の ITU-T 標準仕様。ITU-T 標準 H.320 の拡張を使用することで、LAN やパケット交換ネットワークを使用したテレビ会議、およびインターネットを使用したテレビ会議も可能になります。

H.323 標準の通信プロトコルを使用して、異種の通信デバイスが相互に通信できます。H.323 では、CODEC の共通セット、コール セットアップとネゴシエーション手順、および基本的なデータ転送方式を定義しています。

H.323 RAS Registration, Admission, Status（RAS）シグナリング プロトコル。デバイスでの VoIP ゲートウェイとゲートキーパ間の登録、アドミッション、帯域幅変更、状態の検出と接続解除の手順の実行を可能にします。

H.450.2 H.323 へのコール転送サービスの補足。

H.450.3 H.323 へのコール迂回サービスの補足。

HMAC SHA-1 や MD5 などの暗号化ハッシュを使用したメッセージ認証のためのメカニズム。

HTTP HyperText Transfer Protocol。ファイル転送のためにブラウザや Web サーバで使用されるプロトコル。ユーザが Web ページを参照するとき、ブラウザは HTTP を使用して Web ページで使用するファイルを要求したり受信したりすることができます。HTTP 送信は暗号化されません。

HTTPS HTTP over SSL。SSL を暗号化したバージョンの HTTP。

I

IANA Internet Assigned Number Authority。インターネットで使用するポート番号とプロトコル番号を割り当てます。

ICMP Internet Control Message Protocol。エラーを報告し、IP パケット処理に関するその他の情報を提供するネットワーク レイヤ インターネット プロトコル。

IETF Internet Engineering Task Force。インターネットのプロトコルを定義する RFC ドキュメントを作成する技術標準化団体。

IGMP
Internet Group Management Protocol。IGMP は、隣接するマルチキャスト ルータに IP マルチキャストメンバーシップを報告するために IPv4 システムで使用されるプロトコルです。

IKE
Internet Key Exchange（インターネット キー交換）。IKE は共有セキュリティ ポリシーを確立し、キーを必要とするサービス（IPSec など）のためにキーを認証します。IPSec トラフィックを通過させるには、FWSM でピアの ID を確認する必要があります。この確認は、両方のホストに事前共有鍵を手動で入力するか、または CA サービスにより行われます。IKE は、ISAKMP フレームワーク内で SKEME と呼ばれるプロトコル スイートと Oakley を部分的に使用するハイブリッド プロトコルです。このプロトコルは、以前は ISAKMP/Oakley と呼ばれていました。RFC 2409 で定義されています。

IKE 拡張認証
IKE Extended Authenticate（Xauth）は、IETF draft-ietf-ipsec-isakmp-xauth-04.txt（「extended authentication」ドラフト）に従って実装されます。このプロトコルは、TACACS+ または RADIUS を使用する IKE 内でユーザの認証を行う機能を提供します。

IKE モード コンフィギュレーション
IKE モード コンフィギュレーションは、IETF draft-ietf-ipsec-isakmp-mode-cfg-04.txt に従って実装されます。IKE モード コンフィギュレーションを使用すると、セキュリティ ゲートウェイで IKE ネゴシエーションの一部として VPN クライアントに IP アドレス（および他のネットワーク レベル コンフィギュレーション）をダウンロードすることができます。

ILS
Internet Locator Service。ILS は LDAP をベースにしており、ILSv2 に準拠しています。ILS は、Microsoft の NetMeeting、SiteServer、および Active Directory 製品で使用するために、Microsoft 社が開発したものです。

IMAP
Internet Message Access Protocol。共有が可能なメール サーバに保存された、電子メールや掲示板メッセージにアクセスする方式。IMAP では、クライアントの電子メール アプリケーション からリモートのメッセージの格納場所へのアクセスを、メッセージの転送を行わずにローカルでアクセスしているかのように行うことができます。

IMSI
International Mobile Subscriber Identity。GTP トンネル ID の 2 つのコンポーネントのうちの 1 つで、もう一方は NSAPI です。NSAPI の項も参照してください。

inside
FWSM で保護された内部の「信頼できる」ネットワークに接続する最初のインターフェイス。通常はポート 1 です。インターフェイス、インターフェイス名の項目も参照してください。

intf*n*
名前と構成のカスタマイズが可能なユーザ設計のサブセット ネットワークに接続するインターフェイス。通常はポート 2 から始まります。

IP
Internet Protocol。IP プロトコルは、最も広く使用されている公開プロトコルです。相互接続されたネットワークのどこからでも通信に利用でき、LAN 通信にも WAN 通信にも同様に適しています。

IPS
Intrusion Prevention System（侵入防御システム）。広範囲のネットワーク攻撃の軽減に役立つ、インラインのディープ パケット検査を行うソリューション。

IPSec
IP セキュリティ。参加するピア間でのデータの機密保持、データの整合性、データの認証を実現する公開規格のフレームワーク。IPSec では、IP レイヤでこれらのセキュリティ サービスが利用できます。IPSec は IKE を使用して、ローカル ポリシーに基いてプロトコルとアルゴリズムのネゴシエーションを処理し、IPSec で使用される暗号化および認証キーを生成します。IPSec は、ホストのペア間、セキュリティ ゲートウェイのペア間、またはセキュリティ ゲートウェイとホスト間の 1 つ以上のデータ フローを保護します。

IPSec トランスフォーム セット
トランスフォーム セットには、IPSec ポリシーに一致するトラフィックで使用する IPSec プロトコル、暗号化アルゴリズム、およびハッシュ アルゴリズムを指定します。トランスフォームには、1 つのセキュリティ プロトコル（AH または ESP）とそれに対応するアルゴリズムが記述されます。大部分のトランスフォーム セットで使用される IPSec プロトコルは、認証用の DES アルゴリズムと HMAC-SHA を持つ ESP です。

IPSec フェーズ 1
IPSec ネゴシエーションの第 1 フェーズで、キー交換と IPSec の ISAKMP 部分が該当します。

IPSec フェーズ 2
IPSec ネゴシエーションの第 2 フェーズ。フェーズ 2 では、ペイロードに使用する暗号化ルール、暗号化に使用する送信元と宛先、アクセス リストに基づいて処理対象とするトラフィックの定義、および IPSec ピアが決まります。IPSec は、フェーズ 2 でインターフェイスに適用されます。

IP アドレス
IP プロトコル アドレス。FWSM のインターフェイス IP アドレス。IPv4 アドレスは、32 ビット長です。このアドレス スペースは、ネットワーク番号、オプションのサブネットワーク番号、およびホスト番号の指定に使用されます。32 ビットは 4 つのオクテット（8 個のバイナリ ビット）にグループ分けされ、ピリオド（ドット）で分割された 4 つの 10 進数で表現されます。4 つのオクテットのそれぞれの意味は、ネットワークでの使用方法によって決まります。

IP プール
名前、開始 IP アドレスおよび終了 IP アドレスで示した範囲で指定される、ローカル IP アドレスの範囲。IP プールは、内部インターフェイスのクライアントにローカル IP アドレスを割り当てるために、DHCP および VPN で使用されます。

ISAKMP
Internet Security Association and Key Management Protocol。ペイロード フォーマット、キー交換プロトコルを実装するメカニズム、およびセキュリティ アソシエーションのネゴシエーションを定義するプロトコル フレームワーク。IKE を参照してください。

ISP
Internet Service Provider（インターネット サービス プロバイダー）。電話音声回線を使用したモデム ダイヤルイン、DSL などのサービスを通してインターネットへの接続を提供する組織。

J

JTAPI
Java Telephony Application Programming Interface。テレフォニー機能をサポートする Java ベースの API。TAPI の項も参照してください。

K

Kerberos
秘密鍵暗号化を使用する、クライアント / サーバ アプリケーション用の強力なネットワーク認証プロトコル。Kerberos は、LDAP サーバへのセキュリティ アプライアンス認証に利用可能な SASL メカニズムの 1 つです。

L

LAN
Local Area Network（ローカルエリア ネットワーク）。1 つの建物やキャンパスなど、1 つの場所に存在するネットワーク。インターネット、イントラネット、およびネットワークの項も参照してください。

LCN
Logical Channel Number（論理チャネル番号）。

LDAP
Lightweight Directory Access Protocol。LDAP を使用すると、管理およびブラウザ アプリケーションで X.500 ディレクトリへのアクセスが行えます。

LDP
Label Distribution Protocol。

LLA
Link-Local Address（リンクローカル アドレス）。

M

MCR
マルチキャストを参照してください。

MC ルータ
マルチキャスト（MC）ルータは、マルチキャスト データ送信を、インターネットワークの各 LAN 上のホストにルーティングします。これらのホストは、特定のマルチメディアまたはその他のブロードキャストを受信するよう登録されています。マルチキャストの項も参照してください。

MD5 Message Digest 5。128 ビットのハッシュを生成する単一方向のハッシュ アルゴリズム。MD5 も SHA-1 も MD4 から派生したもので、MD4 ハッシュ アルゴリズムのセキュリティを強化するよう設計されています。SHA-1 は MD4 や MD5 よりも安全性が高くなっています。シスコでは、IPSec フレームワーク内で認証のためにハッシュを使用します。SNMP v.2 のメッセージ認証でも使用します。MD5 は通信の整合性を確認し、発信元を認証し、適時性を確認します。MD5 は SHA-1 よりもダイジェストが小さく、若干処理速度が速いと考えられます。

MDI Media Dependent Interface（メディア依存型インターフェイス）。

MDIX Media Dependent Interface crossover（メディア依存型インターフェイス クロスオーバー）。

MGCP Media Gateway Control Protocol。MGCP は、外部コール制御エレメント（メディア ゲートウェイ コントローラまたはコール エージェント）による VoIP コールの制御を行うプロトコルです。MGCP は IPDC プロトコル と SGCP プロトコルを統合したものです。

Mode Config IKE モード コンフィギュレーションを参照してください。

MS Mobile Station（モバイル ステーション）。ネットワーク サービスにアクセスするために使用する、モバイル ハンドセットまたはコンピュータなどの任意のモバイル デバイスの総称です。GPRS ネットワークは、MS の 3 つのクラスをサポートします。これらのクラスでは、GPRS および GSM モバイル無線ネットワーク内でサポートされる操作のタイプが記述されています。たとえば、クラス A の MS は GPRS と GSM サービスの同時操作をサポートしています。

MS-CHAP Microsoft の CHAP。

MSFC Multilayer Switch Feature Card（マルチレイヤ スイッチ フィーチャ カード）。MSFC は、Catalyst 6500 スイッチまたは Cisco 7600 ルータに搭載されるルータ カードです。

MTU Maximum Transmission Unit（最大伝送ユニット）。最適な応答時間でネットワーク上で効率的に転送できる 1 パケットの最大バイト数です。イーサネットのデフォルト MTU は 1500 バイトですが、各ネットワークで値は異なります。シリアル接続では最小のバイト数になります。MTU は RFC 1191 で定義されています。

N

N2H2 FWSM と連動してユーザの Web アクセスを制御するサードパーティ製のポリシー指向フィルタリング アプリケーション。N2H2 は、宛先ホスト名、宛先 IP アドレス、およびユーザ名とパスワードに基づいて、HTTP 要求をフィルタリングできます。N2H2 社は、2003 年 10 月に Secure Computing 社に買収されました。

NAT Network Address Translation（ネットワーク アドレス変換）。グローバルに一意な IP アドレスを使用する必要性を減らすメカニズムです。NAT を使用すると、グローバルに一意でないアドレスを持つ組織が、使用しているアドレスをグローバルにルーティング可能なアドレス スペースに変換することにより、インターネットに接続できるようになります。

NEM Network Extension Mode（ネットワーク拡張モード）。これを使用すると、VPN ハードウェア クライアントは、VPN トンネル経由でリモート プライベート ネットワークに 1 つのルーティング可能なネットワークを提供できるようになります。

NetBIOS Network Basic Input/Output System。Windows のホスト名登録、セッション管理、およびデータ転送をサポートする Microsoft のプロトコル。FWSM は、NBNS UDP ポート 137 および NBDS UDP ポート 138 のパケットの NAT 処理を実行することにより、NetBIOS をサポートします。

NMS Network Management System（ネットワーク管理システム）。ネットワークの少なくとも一部分の管理に責任を負うシステム。通常、NMS には、エンジニアリング ワークステーションなどの比較的、高性能高機能のコンピュータが使用されます。NMS は、エージェントとの通信により、ネットワーク統計情報やリソース情報を把握します。

NP Network Processor（ネットワーク プロセッサ）。

NSAPI Network Service Access Point Identifier（ネットワーク サービス アクセス ポイント識別子）。GTP トンネル ID の 2 つのコンポーネントのうちの 1 つです。もう一方は IMSI です。IMSI の項も参照してください。

NSSA Not-So-Stubby-Area。RFC 1587 で定義された OSPF 機能。NSSA は、Cisco IOS ソフトウェア Release 11.2 で最初に導入されました。既存のスタブ エリア機能を汎用的に拡張するもので、限定的な方法でスタブ エリアに外部のルータを導入することができます。

NTLM NT Lan Manager。Microsoft Windows のチャレンジ レスポンス認証方式。

NTP Network Time Protocol。

O

Oakley 認証済みキー関連情報を取得する方法を定義したキー交換プロトコル。Oakley の基本的なメカニズムは、Diffie-Hellman キー交換アルゴリズムです。Oakley は RFC 2412 で定義されています。

OSPF Open Shortest Path First。OSPF は IP ネットワーク用のルーティング プロトコルです。OSPF は、ネットワーク帯域幅を有効に使用し、トポロジー変更後の収束が速いため、大規模ネットワークで広く採用されています。FWSM は OSPF をサポートしています。

OU Organizational Unit（組織ユニット）。X.500 ディレクトリの属性です。

outside FWSM の外部にある「信頼できない」ネットワーク（インターネット）に接続する最初のインターフェイス。通常はポート 0 です。インターフェイス、インターフェイス名、発信の項も参照してください。

P

PAC PPTP Access Concentrator。1 つ以上の PSTN または ISDN 回線に接続され、PPP 操作と PPTP プロトコル処理のできるデバイス。PAC で 1 つ以上の PNS にトラフィックを渡すために必要なのは、TCP/IP の実装のみです。非 IP プロトコルのトンネリングを行うこともできます。

PAT ダイナミック PAT、インターフェイス PAT、およびスタティック PAT の項も参照してください。

Perfmon 接続 / 秒、xlates/ 秒など各種機能の統計情報を収集し、レポートする FWSM 機能。

PFS Perfect Forward Secrecy。PFS は IPSec フェーズ 1 とフェーズ 2 の SA に異なるセキュリティ キーを使用することにより、セキュリティを向上させます。PFS を使用しない場合、両方のフェーズで SA を確立するため同じセキュリティ キーが使用されます。PFS は、所定の IPSec SA キーが他のシークレット（他のキーなど）から派生していないことを保証します。つまり、キーが解読されそうになった場合、PFS は攻撃者が他のキーを導出できないようにします。PFS がイネーブルになっていない場合、IKE SA 秘密鍵が解読されれば、IPSec 保護データがすべてコピーされ、IKE SA シークレットの知識を使用して、この IKE SA によって設定された IPSec SA を脆弱化することができると推測されます。PFS を使用すると、IKE が突破されても、攻撃者にすぐに IPSec にアクセスされることはありません。攻撃者は、IPSec SA を個別に突破する必要があるためです。

PIM Protocol Independent Multicast。PIM は、特定のマルチキャスト送信をホスト グループに配信するための最良のパスを特定する、スケーラブルな方法を提供します。各ホストは、伝送を受信するため、IGMP を使用して登録されています。PIM-SM の項も参照してください。

PIM-SM Protocol Independent Multicast-Sparse Mode。PIM-SM は シスコ製ルータのデフォルトで、マルチキャスト送信の送信元がブロードキャストを開始すると、登録されたすべてのホストにパケットが到達するまで、1 つの MC ルータから次のルータへと、トラフィックが順次転送されていきます。PIM の項も参照してください。

ping 2 台めのホストがアクセス可能かどうかを判断するため、ホストによって送信される ICMP 要求。

PIX
Private Internet eXchange。Cisco PIX 500 シリーズの FWSM は、小規模事業所用のコンパクトなプラグアンドプレイのデスクトップ モジュールから、要求の厳しい企業やサービス プロバイダー環境用のキャリアクラスのギガビット モジュールまで、幅広いモデルがあります。Cisco PIX FWSM は、急速に変化するネットワーク環境に対応した強力で多層的な防御を構築するための、堅牢なエンタープライズ クラスの統合ネットワーク セキュリティ サービスを提供します。

PKCS12
秘密鍵、証明書、その他のデータなど、PIK 関連のデータを転送するための規格。この規格をサポートするデバイスを使用することにより、管理者は個人 ID 情報を一括して管理できます。

PNS
PPTP Network Server。PNS は、汎用コンピューティング / サーバ プラットフォーム上で動作することを想定されています。PNS は PPTP のサーバ側を処理します。PPTP は完全に TCP/IP に依存し、インターフェイス ハードウェアからは独立しているため、PNS では LAN および WAN デバイスなどの IP インターフェイス ハードウェアを任意に組み合わせて使用できます。

POP
Post Office Protocol。クライアントの電子メール アプリケーションがメール サーバからメールを取り出すために使用するプロトコル。

PPP
Point-to-Point Protocol（ポイントツーポイント プロトコル）。アナログ電話回線とモデムを使用するダイアルアップ ISP アクセスのために開発されました。

PPTP
Point-to-Point Tunneling Protocol（ポイントツーポイント トンネリング プロトコル）。PPTP は、Windows ネットワークにセキュアなリモート アクセスを提供するために Microsoft によって導入されました。ただし、攻撃に対して脆弱なため、一般に PPTP が使用されるのは、強力なセキュリティ対策が利用できない場合や不要な場合だけです。PPTP のポートは pptp、1723/tcp、1723/udp、および pptp です。PPTP の詳細については、RFC 2637 を参照してください。PAC、PPTP GRE、PPTP GRE トンネル、PNS、PPTP セッション、および PPTP TCP の項も参照してください。

PPTP GRE
PPP トラフィックをカプセル化するための GRE のバージョン 1。

PPTP GRE トンネル
PNS-PAC ペアで定義されたトンネル。トンネル プロトコルは、GRE の修正バージョンで定義されています。トンネルは、PAC と PNS の間で PPP データグラムを送信します。1 つのトンネルで多数のセッションが多重処理されます。TCP 上で動作する制御接続は、セッションとトンネルの確立、解放、および維持を制御します。

PPTP TCP
PPTP コール制御および管理情報がやりとりされる標準の TCP セッション。制御セッションは、PPTP トンネルでトンネリングされるセッションと論理的には対応付けられますが、実際には独立しています。

PPTP セッション
PPTP はコネクション型です。PNS および PAC は、PAC に接続された各ユーザの状態を維持します。セッションは、ダイヤル ユーザと PNS の間でエンドツーエンドの PPP 接続が試みられた時点で作成されます。セッションに対応するデータグラムは、PAC と PNS の間でトンネルを介して送信されます。

Q

QoS
Quality of Service（サービス品質）。送信品質とサービスの可用性を反映させた、送信システムのパフォーマンスの指標。

R

RA
Registration Authority（登録局）。CA の公認の代理人。RA は証明書の登録と、CRL の発行ができます。CA、証明書、公開鍵の項も参照してください。

RADIUS
Remote Authentication Dial-In User Service。RADIUS は、不正アクセスに対してネットワークのセキュリティ対策を施した分散クライアント / サーバ システムです。RFC 2058 および RFC 2059 では、RADIUS プロトコルの標準を定義しています。AAA および TACACS+ の項も参照してください。

RFC
Request for Comments。RFC ドキュメントでは、インターネット上の通信のためのプロトコルと標準が定義されています。RFC は IETF によって作成され、公開されます。

RIP

Routing Information Protocol。UNIX BSD システムで提供される Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）。インターネットで最も一般的な IGP。RIP では、ルーティング メトリックとしてホップ カウントを使用します。

RLLA

Reserved Link Local Address。マルチキャスト アドレスの範囲は 224.0.0.0 ～ 239.255.255.255 ですが、利用できるのは 224.0.1.0 ～ 239.255.255.255 です。マルチキャスト アドレス範囲の最初の部分の 224.0.0.0 ～ 224.0.0.255 は、予約されており、RLLA と呼ばれます。このアドレスは利用できません。RLLA の範囲を除外するには、224.0.1.0 ～ 239.255.255.255 を指定します。224.0.0.0 ～ 239.255.255.255 を指定して、224.0.0.0 ～ 224.0.0.255 を除外すると、224.0.1.0 ～ 239.255.255.255 を指定したのと同じになります。

RP

Rendezvous Point（ランデブー ポイント）。RP は、PIM マルチキャスト環境において、マルチキャスト データの送信元と受信者が出会う場として機能します。

RPC

Remote Procedure Call。RPC は、クライアントによって指定され、サーバで実行されてから結果がネットワーク経由でクライアントに帰されるプロシージャ コールです。

RSA

キー長が可変の公開鍵暗号化アルゴリズム（開発者の Rivest、Shamir、Adelman にちなんで命名）。RSA の大きな弱点は、DES などの一般的な秘密鍵アルゴリズムに比べて、処理速度が非常に遅いことです。シスコの IKE 実装では、秘密鍵の取得に Diffie-Hellman 交換を使用しています。この交換は RSA（事前共有鍵）によって認証が可能です。Diffie-Hellman 交換では、DES キーがネットワークを越えることはありません（暗号化された形式であっても）。RSA 暗号化および署名方式ではネットワークを越えます。RSA はパブリック ドメインではなく、RSA Data Security からライセンスを取得する必要があります。

RSH

Remote Shell（リモート シェル）。ユーザがリモートのシステムにログインしなくてもリモート システムでコマンドを実行できるようにするプロトコル。たとえば、RSH を使用すると、各通信サーバに接続することなく多数のアクセス サーバのステータスをリモートで確認し、コマンドを実行して通信サーバとの接続を終了することができます。

RTCP

RTP Control Protocol。IPv6 RTP 接続の QoS をモニタし、続行中のセッションに関する情報を伝達するためのプロトコル。RTP の項も参照してください。

RTP

Real-Tme Transport Protocol。通常、IP ネットワークで使用されます。RTP は、音声、ビデオ、シミュレーション データなどのリアルタイム データをマルチキャストまたはユニキャスト ネットワーク サービス上で送信するアプリケーションのためのエンドツーエンドのネットワーク伝送機能を提供するために設計されています。RTP は、ペイロード タイプの識別、シーケンス番号付与、タイムスタンプ付与、リアルタイム アプリケーションへの配信モニタリングなどのサービスを提供します。

RTSP

Real Time Streaming Protocol。音声、ビデオなどのリアルタイム データの制御配信を可能にします。RTSP は、RTP や HTTP などの確立されたプロトコルと連動するよう設計されています。

S

SA

Security Association（セキュリティ アソシエーション）。データ フローに適用されたセキュリティ ポリシーおよびキー関連情報のインスタンス。SA は、IPSec の 2 つのフェーズで IPSec ピアによってペアで確立されます。SA は、セキュアなトンネルを作成するために使用される暗号化アルゴリズムとその他のセキュリティ パラメータを指定します。フェーズ 1 の SA（IKE SA）は、フェーズ 2 の SA のネゴシエーションのためのセキュアなトンネルを確立します。フェーズ 2 の SA（IPSec SA）は、ユーザ データの送信に使用されるセキュアなトンネルを確立します。IKE と IPSec の両方で SA が使用されますが、SA は互いに独立しています。IPSec SA は単一方向で、それぞれのセキュリティ プロトコル内で一意です。SA のセットは保護データ パイプに必要で、各プロトコルの各方向に 1 つ必要です。たとえば、ピア間で ESP をサポートするパイプがある場合、各方向に 1 つの ESP SA が必要です。SA は、宛先（IPSec エンドポイント）アドレス、セキュリティ プロトコル（AH または ESP）、およびセキュリティ パラメータ インデックスによって一意に識別されます。IKE は IPSec の代わりに SA のネゴシエーションと確立を行います。IPSec SA を手動で確立することもできます。IKE SA は IKE でのみ使用され、IPSec SA とは異なり双方向です。

SASL Simple Authentication and Security Layer。コネクション型のプロトコルに認証サポートを追加するためのインターネット標準方式。SASL は、セキュリティ アプライアンスと LDAP サーバとの間で、ユーザ認証を安全に行うために使用できます。

SCCP Skinny Client Control Protocol。Cisco Call Manager と Cisco VoIP フォンの間で使用される Cisco 独自のプロトコル。

SCEP Simple Certificate Enrollment Protocol。CA に証明書を要求し、受け取る（「登録」ともいう）ための手段。

SDP Session Definition Protocol。マルチメディア サービスを定義するための IETF プロトコル。SDP メッセージは、SGCP および MGCP メッセージの一部とすることができます。

SGCP Simple Gateway Control Protocol。外部コール制御エレメント（コール エージェント）により VoIP ゲートウェイを制御します。

SGSN Serving GPRS Support Node。SGSN は、モビリティ管理、セッション管理、およびパケット リレー機能を保証します。

SHA-1 Secure Hash Algorithm 1。SHA-1 [NIS94c] は 1994 年に公開された SHA の改訂版です。SHA は MD4 に基づいてモデル化されており、160 ビットのダイジェストを生成します。SHA は 160 ビットのダイジェストを生成するため、128 ビットのハッシュ（MD5 など）よりも Brute-Force アタックに対して抵抗力がありますが、処理に時間がかかります。SHA-1 は米国国立標準技術研究所と米国国家安全保障局が共同開発しました。このアルゴリズムは、他のハッシュ アルゴリズムと同様、送信中にメッセージの内容が改ざんされていないことを保証するために下位層のプロトコルで使用される CRC のように機能するハッシュ値（メッセージ ダイジェスト）を生成するために使用されます。一般的に、SHA-1 は MD5 よりもセキュアだと考えられています。

SIP Session Initiation Protocol。特に二者間の音声会議（「コール」）のコール処理セッションを可能にします。SIP は、コール シグナリングのために SDP と連動します。SDP はメディア ストリームのためのポートを指定します。SIP を使用すると、FWSM は 任意の SIP VoIP ゲートウェイと VoIP プロキシ サーバをサポートすることができます。

SKEME 認証済みキー関連情報を導出する方法を定義したキー交換プロトコル。キー リフレッシュが迅速です。

SMR Stub Multicast Routing。SMR では、FWSM が「スタブ ルータ」として機能します。スタブ ルータとは、IGMP プロキシ エージェントとして機能するデバイスです。IGMP は、マルチキャスト ルータのある特定 LAN 上のマルチキャスト グループに特定ホストをダイナミックに登録するために使用されます。マルチキャスト ルータはマルチキャスト データ送信を、特定のマルチメディアやブロードキャストを受信するよう登録されたホストにルーティングします。スタブ ルータは、ホストと MC ルータの間で IGMP メッセージを転送します。

SMTP Simple Mail Transfer Protocol。SMTP は電子メール サービスをサポートするインターネット プロトコルです。

SNMP Simple Network Management Protocol（簡易ネットワーク管理プロトコル）。MIB（管理情報ベース）と呼ばれるデータ構造を使用してネットワーク デバイスを管理する標準方式。

SQL*Net Structured Query Language Protocol。クライアントとサーバ プロセスの間の通信に使用される Oracle のプロトコル。

SSH Secure Shell（セキュア シェル）。TCP/IP などのトランスポート レイヤの上位で動作し、強力な認証および暗号化機能を持つアプリケーション。

SSL Secure Sockets Layer。アプリケーション層と TCP/IP の間に常駐して、データ トラフィックの透過的な暗号化を提供するプロトコル。

SVC SSL VPN Client（SVC）は、ネットワーク管理者がリモート コンピュータに IPSec VPN クライアントのインストールと設定を行わなくても、リモート ユーザが IPSec VPN クライアントの機能を利用できるようにする VPN トンネリング テクノロジーです。SVC では、すでにリモート コンピュータ上に存在する SSL 暗号化と、セキュリティ アプライアンスの WebVPN ログインおよび認証を使用します。

SVI Switched Virtual Interface（スイッチ仮想インターフェイス）。SVI は MSFC に割り当てられた VLAN です。

T

TACACS+ Terminal Access Controller Access Control System Plus。コマンド許可を含む AAA サービスをサポートするクライアント / サーバ プロトコル。AAA、RADIUS の項も参照してください。

TAPI Telephony Application Programming Interface。テレフォニー機能をサポートする Microsoft Windows のプログラミング インターフェイス。

TCP Transmission Control Protocol。信頼性の高い全二重データ送信を可能にするコネクション型トランスポート層プロトコル。

TCP 代行受信 TCP 代行受信機能を使用すると、オプションの初期接続の上限に達した場合、初期接続のカウントがこのスレッシュホールドを下回るまで、当該サーバへのすべての SYN は代行受信されます。各 SYN に対して、サーバに代わって FWSM が空の SYN/ACK セグメントで応答します。FWSM は妥当なステート情報を保持し、パケットを廃棄し、クライアントの確認応答を待ちます。ACK を受信すると、クライアント SYN セグメントのコピーがサーバに送信され、FWSM とサーバの間で TCP スリーウェイ ハンドシェイクが実行されます。このスリーウェイ ハンドシェイクが完了すると、接続が通常どおり再開される場合もあります。クライアントが接続フェーズの間に応答しない場合、FWSM は指数のバックオフを使用して必要なセグメントを再送します。

TDP Tag Distribution Protocol。TDP は、タグ スイッチング ネットワーク内の複数のネットワーク レイヤ プロトコルのタグ バインディング情報を配信、要求、および解放するため、タグ スイッチング デバイスで使用されます。TDP はルーティング プロトコルを変更しません。その代わり、ルーティング プロトコルから学習した情報を使用してタグ バインディングを作成します。TDP は、TDP セッションの開始、モニタ、および終了や、このセッション中に発生したエラーを通知するためにも使用されます。TDP は、順次配信が保障されたコネクション型のトランスポート層プロトコル（TCP など）上で動作します。TDP を使用する場合でも、他のプロトコルのピギーバック情報などのタグ バインディング情報を配信する他のメカニズムも使用できます。

Telnet インターネットなどの TCP/IP ネットワーク用の端末エミュレーション プロトコル。Telnet は Web サーバをリモート制御する一般的な方法ですが、セキュリティ面の脆弱性のため、SSH が使用されるようになってきています。

TFTP Trivial File Transfer Protocol（簡易ファイル転送プロトコル）。TFTP はファイルの転送に使用されるシンプルなプロトコルです。UDP 上で動作し、RFC 1350 で詳しく説明されています。

TLS Transport Layer Security。SSL に代わる将来の IETF プロトコル。

TSP TAPI Service Provider（TAPI サービス プロバイダー）。TAPI の項も参照してください。

U

UDP User Datagram Protocol。IP プロトコル スタックのコネクションレス型トランスポート層プロトコル。UDP は、確認応答や配信保証を行なわずに、データグラムを交換するシンプルなプロトコルであるため、エラー処理や再送を行うには別のプロトコルが必要となります。UDP は RFC 768 で定義されています。

UMTS Universal Mobile Telecommunication System。固定、無線、および衛星ネットワークを介してモバイル ユーザに商業サービスや娯楽サービスなどのブロードバンド情報を配信することにより、オール IP ネットワークを目指す、GPRS を拡張したネットワーク。

URL Uniform Resource Locator。ブラウザを使用してハイパーテキスト ドキュメントやその他のサービスにアクセスするための標準的なアドレス指定方式。http://www.cisco.com のように指定します。

UTC Coordinated Universal Time（協定世界時）。経度 0 のタイム ゾーン。以前は GMT（グリニッジ標準時）と呼ばれていました。世界標準時は、1967 年に GMT から UTC に変わりました。UTC は天文時よりも原子時に基づいています。

UTRAN Universal Terrestrial Radio Access Network。UMTS に無線ネットワークを導入するために使用するネットワーキング プロトコル。GTP では、GGSN、SGSN、および UTRAN の間で UMTS/GPRS バックボーンを経由してマルチプロトコル パケットをトンネリングすることができます。

UUIE User-User Information Element。メッセージに関係しているユーザを特定する H.225 パケットのエレメント。

V

VLAN Virtual LAN。実際には異なる多数の LAN セグメント上に存在していながら、同じ物理ネットワーク ケーブルに接続されているかのように通信できるよう（管理ソフトウェアを使用して）設定された、1 つ以上の LAN 上にあるデバイスのグループ。VLAN は物理接続ではなく論理接続に基づいているため、非常に柔軟性に優れています。

VoIP Voice over IP。VoIP は、電話やファックスなどの通常の音声トラフィックを、IP ベースのネットワーク上で伝送します。DSP は、音声信号をフレームにセグメント化し、2 つずつグループ化し、音声パケットに格納します。この音声パケットは、ITU-T 仕様 H.323 に準拠する IP を使用して送信されます。

VPN Virtual Private Network（仮想私設網）。ユーザの厳格な認証と全データ トラフィックの暗号化によりプライベート性が確保された公共ネットワーク上の 2 つのピア間でのネットワーク接続。PC などのクライアントや、FWSM などのヘッドエンドの間で VPN を確立することができます。

VSA Vendor-Specific Attribute（ベンダー固有属性）。RADIUS RFC ではなくベンダーによって定義された RADIUS パケットの属性。RADIUS プロトコルでは、VSA の識別のため IANA によって割り当てられたベンダー番号を使用します。これにより、異なるベンダーが同じ番号の VSA を持てるようになります。ベンダー番号と VSA 番号の組み合わせにより、VSA が一意になります。たとえば、cisco-av-pair VSA はベンダー番号 9 に対応付けられた VSA のセットのアトリビュート 1 になります。各ベンダーは最大 256 の VSA を定義することができます。RADIUS パケットには、ベンダー固有の名前が付けられた VSA アトリビュート 26 が含まれます。VSA はサブ属性と呼ばれることもあります。

W

WAN Wide-Area Network。広い地域にいるユーザにサービスを提供するデータ通信ネットワークであり、一般に、コモン キャリアが提供する伝送デバイスを使用します。

Websense 社員によるインターネット アクセスを管理するコンテンツ フィルタリング ソリューション。Websense は、ポリシー エンジンと URL データベースを使用して、Web サイトへのユーザ アクセスを制御します。

WEP Wired Equivalent Privacy。無線 LAN 用のセキュリティ プロトコル。IEEE 802.11b 規格で定義されています。

WINS Windows Internet Naming Service。特定のネットワーク デバイスに対応する IP アドレスを特定する Windows システムで、「名前解決」とも呼ばれます。WINS は、現在利用可能なネットワーク デバイスの NetBIOS 名と各デバイスに割り当てられた IP アドレスが自動的に更新される分散データベースを使用します。WINS は、ルーテッド ネットワーク環境でダイナミックな NetBIOS 名を IP アドレス マッピングに登録 / 照会するための分散データベースを提供します。複雑なネットワークでの名前解決に関して発生する問題を解決する目的で設計されているため、このようなルーテッド ネットワークでの NetBIOS の名前解決には最適です。

X

X.509
デジタル証明書の定義のために広く用いられている規格。X.509 は実際は ITU 勧告であるため、公式には規格としての使用が定義または承認されていない状態です。

xauth
IKE 拡張認証を参照してください。

xlate
xlate（トランスレーション エントリともいう）は、1 つの IP アドレスを別の IP アドレスにマッピングしたり、1 つの IP アドレス / ポートのペアを別のペアにマッピングしたりすることを意味します。

あ

アクセス モード
FWSM CLI では、いくつかのコマンド モードを使用します。利用できるコマンドはモードによって異なります。ユーザ EXEC モード、イネーブル EXEC モード、グローバル コンフィギュレーション モード、コマンド固有コンフィギュレーション モードの項も参照してください。

アドレス変換
あるネットワークのアドレスやポートを別のネットワークのアドレスやポートに変換すること。IP アドレス、インターフェイス PAT、NAT、PAT、スタティック PAT、xlate の項も参照してください。

暗号
ネットワーク上のセキュアな通信のために使用される、暗号化、認証、整合性、キー、その他のサービス。VPN および IPSec の項も参照してください。

暗号化
データに特定のアルゴリズムまたは暗号を適用して、情報の表示を許可されていないユーザが理解できないデータにすること。復号化の項も参照してください。

暗号マップ
FWSM で VPN の設定に使用される一意の名前とシーケンス番号を持つデータ構造。暗号マップは、セキュリティ処理の必要なデータ フローを選択し、これらのフローとトラフィックの宛先となる暗号ピアのためのポリシーを定義します。暗号マップはインターフェイスに適用されます。暗号マップの内容は、IKE と IPSec を使用した VPN 用のセキュリティ ポリシーを指定するために必要な ACL、暗号化基準、ピア、その他のパラメータです。VPN の項も参照してください。

暗黙の規則
デフォルトのルールに基づいて、またはユーザ定義のルールの結果として、FWSM によって自動的に作成されるアクセス規則。

い

イネーブル EXEC モード
イネーブル EXEC モードでは、現在の設定を変更することができます。ユーザ EXEC モードのコマンドは、イネーブル EXEC モードで機能します。コマンド固有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、ユーザ EXEC モードの項も参照してください。

インスペクション エンジン
FWSM は、トラフィック内で組み込まれたアドレッシング情報の場所を特定するため、特定のアプリケーション レベルのプロトコルを検査します。これにより、NAT は組み込まれたアドレスを変換し、変換によって影響を受けたチェックサムやフィールドを更新することができます。多くのプロトコルではセカンダリ TCP または UDP ポートをオープンするため、各アプリケーション インスペクション エンジンは、セッションをモニタして、セカンダリ チャネルのポート番号を特定します。well-known ポートでの初期セッションは、ダイナミックに割り当てられるポート番号のネゴシエーションに使用されます。アプリケーション インスペクション エンジンはこれらのセッションをモニタし、ダイナミックなポート割り当てを特定し、特定のセッションの間、このポートでのデータ交換を許可します。FWSM が検査可能なプロトコルには、CTIQBE、FTP、H.323、HTTP、MGCP、SMTP、SNMP などがあります。

インターネット
IP を使用するグローバル ネットワーク。LAN とは異なります。イントラネットの項も参照してください。

インターフェイス
特定のネットワークと FWSM との間の物理的接続。

インターフェイス IP アドレス
FWSM ネットワーク インターフェイスの IP アドレス。インターフェイス IP アドレスは一意でなければなりません。複数のインターフェイスに同じ IP アドレス（同じ IP ネットワーク上の IP アドレス）を割り当ててはいけません。

インターフェイス PAT
PAT IP アドレスが外部インターフェイスの IP アドレスでもある状態で使用される PAT。ダイナミック PAT、スタティック PAT の項を参照してください。

インターフェイス名
FWSM ネットワーク インターフェイスに割り当てられた、人が読解可能な名前。内部インターフェイスのデフォルト名は「inside」で、外部インターフェイスのデフォルト名は「outside」です。境界インターフェイスのデフォルト名は「intf*n*」です。最初の境界インターフェイスは「intf2」、2 番めの境界インターフェイスは「intf3」というようになります。intf 文字列の番号は、FWSM のインターフェイス カードの位置に対応します。デフォルト名をそのまま使用することもできますが、経験のあるユーザの場合、わかりやすい名前に変更することもできます。inside、intfn、outside の項も参照してください。

イントラネット
イントラネットワーク。IP を使用する LAN。ネットワークおよびインターネットの項も参照してください。

お

オブジェクト グルーピング
プロトコル、サービス、ホスト、ネットワークなどのネットワーク オブジェクトのグループにアクセス制御ステートメントを適用できるようにして、アクセス制御を簡略化します。

か

仮想ファイアウォール
セキュリティ コンテキストを参照してください。

カットスルー プロキシ
ユーザ認証後の FWSM でのトラフィック フローを高速化します。カットスルー プロキシは、最初はアプリケーション レイヤでユーザとやりとりします。セキュリティ アプライアンスでユーザの認証が完了すると、セッション フローに移行するので、すべてのトラフィックが送信元と送信先の間で直接かつ迅速に伝送され、セッション ステート情報も保持されます。

き

キー
暗号化、復号化、または認証に使用されるデータ オブジェクト。

キャッシュ
以前に実行されたタスクから再利用可能な情報を蓄積した一時的なリポジトリ。タスクの実行に要する時間を短縮できます。

く

クッキー
クッキーはブラウザによって保存されるオブジェクトです。クッキーは、ユーザ プリファレンスなどの情報を固定ストレージに保存します。

クライアント / サーバ コンピューティング
トランザクションの責任が、クライアント（フロント エンド）とサーバ（バック エンド）に分散される分散コンピューティング（処理）ネットワーク システム。分散コンピューティングとも呼ばれます。RPC の項も参照してください。

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、FWSM のコンフィギュレーションを変更することができます。このモードでは、すべてのユーザ EXEC コマンド、イネーブル EXEC コマンド、およびグローバル コンフィギュレーション コマンドを使用できます。ユーザ EXEC モード、イネーブル EXEC モード、コマンド固有コンフィギュレーション モードの項も参照してください。

こ

公開鍵

公開鍵は、公開鍵インフラストラクチャに属するデバイスによって生成されるキーのペアの一方です。公開鍵で暗号化されたデータは、対応する秘密鍵を使用しなければ復号化することはできません。デジタル署名の作成に秘密鍵が使用されている場合、受信者は送信者の公開鍵を使用して、送信者によってメッセージが署名されていることを確認することができます。このキー ペアの特性により、インターネットなどのセキュアでないメディアにおいて、スケーラブルでセキュアな認証方式が可能になります。

コマンド固有コンフィギュレーション モード

一部のコマンドは、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コンフィギュレーション モードを開始します。このモードでは、すべてのユーザ EXEC コマンド、イネーブル EXEC コマンド、グローバル コンフィギュレーション コマンド、およびコマンド固有コンフィギュレーション コマンドを使用できます。グローバル コンフィギュレーション モード、イネーブル EXEC モード、ユーザ EXEC モードの項も参照してください。

コンフィギュレーション、コンフィグ、コンフィグ ファイル

ASDM または CLI によって管理される設定、プリファレンス、プロパティに相当する FWSM のファイル。

さ

サイトツーサイト VPN

サイトツーサイト VPN は、リモート ネットワークを 1 つの VPN に接続する 2 つの IPSec ピア間で確立されます。このタイプの VPN では、IPSec ピアはユーザ トラフィックの宛先にも送信元にもなりません。その代わり、各 IPSec ピアは、各 IPSec ピアに接続された LAN 上のホストに暗号化および認証サービスを提供します。各 LAN 上のホストは、IPSec ピアのペアによって確立されたセキュアなトンネルを介してデータの送受信を行います。

サブネットマスク

マスクの項を参照してください。

し

事前共有鍵

事前共有鍵は、IPSec ピアの数が限られていてスタティックであるネットワークに適した IKE 認証の方法を提供します。この方法は、キーを IPSec ピアの各ペアに対して設定する必要があるため、スケーラビリティは高くありません。新しい IPSec ピアがネットワークに追加された場合、そのピアと通信する各 IPSec ピアに対して事前共有鍵を設定する必要があります。スケーラビリティの高い IKE 認証の方法は、証明書と CA を使用する方法です。

実行コンフィギュレーション

FWSM の RAM で現在実行されている設定。FWSM の動作特性を決定する設定。

証明書

ユーザまたは装置の ID と、証明書を発行した CA の公開鍵を持つ署名済み暗号オブジェクト。証明書には期限があり、妥当でないと判断された場合、CRL に登録されます。証明書は IKE ネゴシエーションのための否認防止も行うため、特定のピアとの間で IKE ネゴシエーションが完了していることを第三者に証明することができます。

シリアル送信

データ キャラクタのビットを 1 つのチャネルで順次伝信するデータ伝信方式。

す

スタティック PAT

Static Port Address Translation（スタティック ポート アドレス変換）。スタティック PAT は、ローカル ポートをグローバル ポートにマッピングするスタティック アドレスです。ダイナミック PAT、NAT の項も参照してください。

スタンバイ ユニット

セカンダリ ユニットを参照してください。

ステートフル インスペクション

ネットワーク プロトコルでは、2 台のホストのネットワーク接続の両端で、ステート情報と呼ばれるデータが保持されます。ステート情報は、保証されたパケット配信、データのシーケンス処理、フロー制御、トランザクションまたはセッション ID などのプロトコル機能を実装するために必要となります。プロトコル ステート情報の一部は、プロトコルの使用中に、パケットに組み込まれて送信されます。たとえば、Web サーバに接続されたブラウザは、HTTP とサポートする TCP/IP プロトコルを使用します。各プロトコル層は、送受信するパケット内のステート情報を保持します。FWSM やその他のファイアウォールの一部は、パケット内のステート情報を検査して、使用しているプロトコルに対して最新で有効であるかどうかを確認します。これはステートフル インスペクションと呼ばれ、ある種のコンピュータ セキュリティの脅威に対して強力な防護壁を作成することを目的としています。

スプーフィング

フィルタやアクセス リストなどのネットワーク セキュリティ メカニズムを破壊することを目的とした攻撃のタイプ。スプーフィング攻撃では、実際とは異なるアドレスから送信されているかのようなパケットが送信されます。

スプリット トンネリング

リモート VPN クライアントがプライベート ネットワークへの暗号化アクセスと、インターネットへの非暗号化アクセスのクリアを同時に実行できるようにします。スプリット トンネリングをイネーブルにしない場合、VPN クアイアントと FWSM の間のトラフィックはすべて IPSec トンネル経由で送信されます。VPN クライアントから発信されるトラフィックは、トンネルを経由して外部インターフェイスに送信され、リモート サイトからインターネットへのクライアント アクセスは拒否されます。

せ

セカンダリ ユニット

2 台がフェールオーバー モードで動作している場合のバックアップの FWSM。

セキュリティ コンテキスト

1 つの FWSM をセキュリティ コンテキストと呼ばれる複数の仮想ファイアウォールに分割できます。各コンテキストはそれぞれが独立したファイアウォールであり、独自のセキュリティ ポリシー、インターフェイス、および管理者が与えられます。マルチコンテキストは、スタンドアロンのファイアウォールを複数使用することと同様です。

セキュリティ サービス）

暗号を参照してください。

た

ダイナミック NAT

NAT およびアドレス変換を参照してください。

ダイナミック PAT

Dynamic Port Address Translation（ダイナミック ポート アドレス変換）。ダイナミック PAT では、複数の発信セッションを 1 つの IP アドレスから発信されたように見せます。PAT をイネーブルにすると、FWSM は各発信変換スロット（xlate）に対して PAT IP アドレスから一意のポート番号を選択します。この機能は、ISP が発信接続のために一意の IP アドレスを十分に割り当てることができない場合に便利です。グローバル プール アドレスは、必ず PAT アドレスが使用される前に確保されます。NAT、スタティック PAT、および xlate の項も参照してください。

ターボ ACL

ACL をコンパイルして、ルックアップ テーブルのセットにすることにより、ACL のルックアップを高速化します。既存の ACL のエントリ数に関係なく、少数かつ一定数のルックアップからなる複数のテーブルに対して、パケット ヘッダーを使用してアクセスします。

て

データの機密保持
攻撃者が読めないようにデータを操作する方法。通常これは、通信にかかわる当事者だけが利用できるデータ暗号化やキーによって実現されます。

データの整合性
秘密鍵や公開鍵アルゴリズムに基づいた暗号化を使用して、保護データの一部を受信するユーザが送信中にデータが改ざんされていないことを確認するためのメカニズム。

データ発信者認証
保護データがその送信者からのみ発信されていることを受信者が確認するためのセキュリティ サービス。このサービスには、データ整合性サービスと、秘密鍵が送信者と受信者の間だけで共有されるキー配布メカニズムが必要となります。

デジタル証明書
証明書を参照してください。

と

透過ファイアウォール モード
FWSM がルータ ホップにならないモード。透過ファイアウォール モードを使用すると、ネットワーク構成を簡略化したり、FWSM を攻撃者から見えなくしたりすることができます。また、透過ファイアウォール モードの使用により、ルーテッド ファイアウォール モードではブロックされるトラフィックを通過させることもできます。ルーテッド ファイアウォール モードの項も参照してください。

登録局
RA を参照してください。

トラフィック ポリシング
トラフィック ポリシング機能は、トラフィックが設定した最大レート（bps）を超えないことを保証します。したがって、1 つのトラフィック フローでリソース全体が占有されないことを保障します。

トランスフォーム セット
IPSec トランスフォーム セットを参照してください。

トランスポート モード
パケットのデータ部分（ペイロード）だけを暗号化し、ヘッダー部分は暗号化しない IPSec 暗号化モード。トランスポート モードはトンネル モードよりも安全性が低くなります。

トンネル
あるプロトコルを別のプロトコル内にカプセル化してデータを転送する方式。トンネリングは、非互換性、実装の簡略化、セキュリティなどの理由で使用されます。たとえば、トンネルを使用すると、リモート VPN クライアントはプライベート ネットワークに暗号化アクセスを実行できます。

トンネル モード
各パケットのヘッダーとデータ部分（ペイロード）の両方を暗号化する IPSec 暗号化モード。トンネル モードはトランスポート モードよりも安全性が高くなります。

に

認証
ユーザの身元とデータの整合性を検証するための暗号化プロトコルおよびサービス。IPSec フレームワークの機能の 1 つ。認証により、データストリームの整合性が確立され、送信の途中で改ざんされていないことが保証されます。データストリームの発信元の確認も行います。AAA、暗号化、および VPN の項も参照してください。

ね

ネットマスク
マスクを参照してください。

ネットワーク
FWSM 設定においては、ネットワークは、IP アドレス スペースの一部を共有するコンピューティング デバイスのグループを指し、1 台のホストを指すわけではありません。ネットワークは複数のノードまたはホストで構成されます。ホスト、インターネット、イントラネット、IP、LAN、およびノードの項も参照してください。

の

ノード　通常はホストとは呼ばれない、ルータやプリンタなどの装置。ホスト、ネットワークの項も参照してください。

は

ハッシュ、ハッシュ アルゴリズム　ハッシュ アルゴリズムは、任意の長さのメッセージで動作する単一方向の機能であり、データの整合性を保証するために暗号化サービスで使用される固定長のメッセージ ダイジェストを作成します。MD5 は、SHA-1 よりダイジェストが小さく、若干処理が早いと考えられます。シスコでは、IPSec フレームワークの実装において、SHA-1 と MD5 の両方のハッシュを使用しています。暗号化、HMAC、および VPN の項も参照してください。

発信　送信元インターフェイスよりもセキュリティの低いインターフェイスを宛先とするトラフィック。

発信 ACL　発信トラフィックに適用される ACL。

ひ

非対称暗号化　公開鍵システムとも呼ばれます。非対称暗号化を使用すると、誰でも別のユーザの公開鍵にアクセスできます。公開鍵へのアクセスが完了すると、公開鍵を使用して、相手に対して暗号化されたメッセージを送信できるようになります。暗号化、公開鍵の項も参照してください。

秘密鍵　秘密鍵は、送信者と受信者の間だけで共有されるキーです。キー、公開鍵の項を参照してください。

ふ

プール　IP プールを参照してください。

フィックスアップ　インスペクション エンジンを参照してください。

フェーズ 1　IPSec フェーズ 1 を参照してください。

フェーズ 2　IPSec フェーズ 2 を参照してください。

フェールオーバー、フェールオーバー モード　フェールオーバーでは、2 台の FWSM を設定し、1 台に障害が発生した場合にもう 1 台が処理を代行するようにできます。FWSM では、アクティブ / アクティブ フェールオーバー、アクティブ / スタンバイ フェールオーバーの 2 種類のフェールオーバー構成をサポートしています。それぞれのフェールオーバー構成には、フェールオーバーの判断と実行のための独自の方法があります。アクティブ / アクティブ フェールオーバーでは、2 台のユニットがネットワーク トラフィックを通過させることができます。これにより、ネットワークの負荷分散が可能になります。アクティブ / アクティブ フェールオーバーが利用できるのは、マルチコンテキスト モードで動作するユニットのみです。アクティブ / スタンバイ フェールオーバーでは、1 台のユニットのみでトラフィックの通過が可能で、もう 1 台のユニットはスタンバイ ステートで待ちます。アクティブ / スタンバイ フェールオーバーは、シングルまたはマルチコンテキスト モードで動作するユニットで利用できます。

不揮発性ストレージ、メモリ　RAM とは異なり、電源が入っていなくても内容が保持されるストレージまたはメモリ。不揮発性ストレージ デバイスのデータは、パワーオフ / パワーオン（電源再投入）やリブートを行っても失われません。

復号化　暗号化されたデータに特定アルゴリズムまたは暗号を適用して、情報の表示を許可されたユーザが理解できるデータにすること。暗号化の項も参照してください。

プライマリ、プライマリ ユニット　プライマリとセカンダリの 2 台で運用している FWSM は、通常はフェールオーバー モードで動作しています。

フラッシュ、フラッシュ メモリ
FWSM の停止時にコンフィギュレーション ファイルを格納しておくための不揮発性ストレージ装置。

プロキシ ARP
グローバル プール内の IP アドレスに対する ARP 要求に、FWSM が応答できるようにします。ARP の項も参照してください。

プロトコル、プロトコル文字列
ネットワークノード間の通信のためのパケット交換を定義した規格。プロトコルはレイヤ構造で連動します。プロトコルは、セキュリティ ポリシーの定義の一部として、文字列またはポート番号によって FWSM コンフィギュレーション内で指定されます。FWSM プロトコルの文字列としては、ahp、eigrp、esp、gre、icmp、igmp、igrp、ip、ipinip、ipsec、nos、ospf、pcp、snp、tcp、udp などが有効です。

へ

ヘッドエンド
公衆ネットワーク経由で VPN クライアント接続に対して、プライベート ネットワークへの入り口となるファイアウォール、コンセントレータ、その他のホスト。ISP および VPN の項も参照してください。

変換
xlate を参照してください。

ほ

ポート
パケットの送信元または宛先となる上位レベルのサービスを識別する TCP および UDP プロトコルのパケット ヘッダ内のフィールド。

ホスト
TCP/IP ネットワーク上の、IP アドレスを持つ装置の名前。ネットワークおよびノードの項も参照してください。

ホスト / ネットワーク
アドレス変換（xlate）や ACE などの FWSM コンフィギュレーションでシングル ホストやネットワーク サブネットを特定するために他の情報と一緒に使用する IP アドレスおよびネットマスク。

ポリシー NAT
ポリシー NAT では、アクセス リストで送信元と宛先のアドレス（またはポート）を指定することによって、アドレス変換対象のローカル トラフィックを識別します。

ま

マスク
インターネット アドレスをネットワーク、サブネット、およびホストの部分に分割する方法を示す 32 ビットのマスク。マスクには、ネットワークとサブネットの部分に使用されるビット位置の 1 部分と、ホストの部分に使用される 0 の部分があります。マスクでは、少なくとも標準のネットワーク部分を規定する必要があり、サブネット フィールドはネットワーク部分と連続している必要があります。

マルチキャスト
マルチキャストとは、送信元が複数の宛先（マルチキャスト グループ）に同時にパケットを送信するネットワーク アドレス指定方式を指します。PIM および SMR の項も参照してください。

め

メッセージ ダイジェスト
メッセージ ダイジェストは MD5 や SHA-1 などのハッシュ アルゴリズムによって作成され、メッセージの整合性を保証するために使用されます。

も

モード
アクセス モードを参照してください。

モジュラ ポリシー フレームワーク
Cisco IOS ソフトウェア Modular QoS CLI と同様の方法で FWSM 機能を設定する手段です。

ゆ

ユーザ EXEC モード
ユーザ EXEC モードでは、FWSM の設定を表示できます。最初に FWSM にアクセスしたときに、ユーザ EXEC モード プロンプトが表示されます。コマンド固有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、およびイネーブル EXEC モードの項も参照してください。

ユニキャスト RPF
Unicast Reverse Path Forwarding。ユニキャスト RPF は、パケットがルーティング テーブルに従った正しい送信元インターフェイスと一致する送信元 IP アドレスを持つように保証することによって、スプーフィングに対してガードします。

り

リプレイ検出
受信者が、リプレイ攻撃を防止するため、古いパケットや複製されたパケットを受信拒否できるセキュリティ サービス。リプレイ攻撃は、古いパケットや複製したパケットを受信者に送信する攻撃者と、偽のトラフィックを正しいものと思い込む受信者がいる状況で発生します。リプレイ検出は、シーケンス番号と認証を組み合わせて行われます。これは IPSec の標準機能です。

リフレッシュ
FWSM から実行コンフィギュレーションをリフレッシュし、画面を更新します。アイコンとボタンで、同じ機能を実行できます。

る

ルーテッド ファイアウォール モード
ルーテッド ファイアウォール モードの場合、FWSM はネットワーク上のルータ ホップとしてカウントされます。接続されたネットワーク間で NAT を実行します。OSPF または RIP を使用できます。透過ファイアウォール モードの項も参照してください。

ルート、ルーティング
ネットワーク上のパス。

ルール
特定の状況に対するセキュリティ ポリシーを定義するために FWSM 設定に追加される条件のステートメント。ACE、ACL、NAT の項も参照してください。

れ

レイヤ
ネットワーキング モデルは、異なるプロトコルが対応付けられたレイヤを実装します。最も一般的なネットワーキング モデルは OSI モデルです。このモデルは、物理層、データ リンク層、ネットワーク層、トランスポート層、セッション層、プレゼンテーション層、アプリケーション層という順序で、7 つの層により構成されています。

?
コマンド文字列 C-4
ヘルプ C-4

Symbols

/ ビット サブネット マスク D-3

A

AAA
Web クライアント 15-4
アカウンティング 15-12
概要 14-2
許可
コマンド 21-15
ダウンロード可能なアクセス リスト 15-8
ネットワーク アクセス 15-7
サーバ
タイプ 14-4
追加 14-13
サポートの概要 14-4
設定の消去 24-8
認証
CLI アクセス 21-13
イネーブル EXEC モード 21-14
ネットワーク アクセス 15-2
パフォーマンス 15-1
ルールの最大数 A-6
ローカル データベースのサポート 14-9
ACE
拡張 10-6
最大数 10-6
順序 10-3
ロギング 10-23
ARP 検査
イネーブル 17-3
概要 17-2
スタティック エントリ 17-2
設定 17-2
ARP スプーフィング 17-2
ARP テーブル、スタティック エントリ 17-2
ASDM
アクセスの許可 21-5
インストレーション 22-10
最大接続数 A-4
ASR 8-28
AUS 22-21

B

BGP 10-8
BPDU
アクセス リスト、EtherType 10-11
スイッチ上での転送 2-13

C

Catalyst 6500
スイッチを参照
Catalyst OS のバージョン A-2
CEF A-3
Cisco 7600
スイッチを参照
Cisco IOS のバージョン A-2
Cisco IP Phone
DHCP との組み合わせ 8-33
アプリケーション検査 20-63
Cisco VPN クライアント 21-8
CLI
構文の形式 C-3
コマンド出力のページング C-6
コマンドの短縮形 C-3
コマンドラインの編集 C-3

コメントの追加　C-6
認証アクセス　21-13
表示　C-6
ページング　C-6
ヘルプ　C-4
CTIQBE 検査
イネーブル　20-10
概要　20-9
制限事項および制約事項　20-9
モニタ　20-11

D

DHCP
Cisco IP Phone　8-33
サーバ　8-33
設定　8-30
透過ファイアウォール　10-8
リレー　8-34
DMZ、定義　1-1
DNS および NAT　12-14
DNS 検査
書き換え　20-14
管理　20-13
設定　20-20
DoS 攻撃、防止　7-8, 12-24
DSCP ビット　1-8

E

EIGRP　10-8
EMBLEM フォーマット、ログでの使用　23-24
ESMTP 検査
概要　20-67
設定　20-68
established コマンド
セキュリティ レベル要件　6-2
ルールの最大数　A-6
EtherChannel、バックプレーン
概要　2-12
負荷分散　2-12
EtherType アクセス リスト
概要　10-10
追加　10-11
EtherType 割り当て番号　10-11

F

FTP 検査
概要　20-22
設定　20-24
FTP フィルタリング　16-10
FWSM
接続　3-2
リセット　2-15

G

GTP 検査
概要　20-28
設定　20-30

H

H.225、設定　20-36
H.245
トラブルシューティング　20-41
モニタ　20-41
H.323 検査
概要　20-34
制限　20-35
設定　20-37
トラブルシューティング　20-40
HSRP　5-9
HTTP
フィルタリング　16-5
HTTP 検査
概要　20-42
設定　20-43
HTTP の複製
アクティブ / アクティブ フェールオーバーでの設定　13-30
アクティブ / スタンバイ フェールオーバーでの設定　13-25
HTTP(S)
最大接続数　A-4
認証　21-13
ルールの最大数　A-6

I

ICMP
- 管理アクセス 21-12
- 接続テスト 24-2
- タイプ番号 D-17
- ルールの最大数 A-6

IGMP 8-21
IKE 21-6
ILS アプリケーション検査 20-45
IM 20-57
IOS のバージョン A-2
IP アドレス
- VPN クライアント 21-9
- インターフェイス 6-4
- クラス D-2
- コンテキスト間で共有 4-4
- サブネット マスク D-5
- 透過モード 6-5
- プライベート D-2
- ルーテッド モード 6-3

IP スプーフィング、回避 19-4
IPSec
- 管理アクセス 21-6
- 基本設定 21-6
- クライアント 21-8
- トランスフォーム 21-7

IPv6
- アクセス リスト 9-7
- コンフィギュレーションの確認 9-13
- スタティック ネイバ 9-12
- 対応コマンド 9-2
- 重複アドレス検出 9-5
- デフォルトおよびスタティック ルート 9-6
- デュアル IP スタック、設定 9-4
- ネイバ検出 9-8
- ルータ アドバタイズメント メッセージ 9-9
- ルートの表示 9-14

IPX 2-7
ISAKMP 21-6
ISN、ランダム化
- NAT 12-25
- 透過ファイアウォール 7-8
- モジュラ ポリシー フレームワーク 19-2

J

Java アプレットのフィルタリング 16-2

K

Kerberos
- サポート 14-8
- 設定 14-13

L

LDAP
- アプリケーション検査 20-45
- サポート 14-8
- 設定 14-13

M

MAC アドレス テーブル
- MAC 学習、ディセーブル化 17-5
- アドレスの追加 17-4
- エントリのタイムアウト 17-5
- 概要 5-13, 17-4
- スタティック エントリ 17-4
- 表示 17-5
- リソース管理 4-16

MAC 学習、ディセーブル化 17-5
Man-In-The-Middle 攻撃 17-2
MGCP 検査
- 概要 20-46
- 設定 20-48

MIB 23-2
More プロンプト C-6
MPLS
- LDP 10-10
- router-id 10-10
- TDP 10-10

MSFC
- SVI 2-7
- 概要 1-4
- 定義 A-2

Multilayer Switch Feature Card
- MSFC を参照

N

N2H2 フィルタリング サーバ
Web サイトの URL 16-5
サポート 16-5
NAT
DNS 12-14
NAT ID 12-17
NAT 除外
概要 12-9
設定 12-34
NAT のバイパス
概要 12-9
設定 12-32
PAT
概要 12-7
実装 12-17
設定 12-23
アイデンティティ NAT
概要 12-9
設定 12-32
アドレスの重複 12-36
概要 12-2
サポートされない RPC 20-73
スタティック NAT
概要 12-7
設定 12-27
スタティック PAT
概要 12-8
設定 12-29
スタティック アイデンティティ、設定 12-33
ステートメントの順序 12-13
セキュリティ レベル要件 6-2
ダイナミック NAT
概要 12-5
実装 12-17
設定 12-23
タイプ 12-5
同一セキュリティ レベル 12-13
透過ファイアウォール 5-12
ポート リダイレクション 12-37
ポリシー NAT
概要 12-10
ルールの最大数 A-6
例 12-36
Network Address Translation
NAT を参照
NP 1-7
NT サーバ
サポート 14-8
設定 14-13
NTLM サポート 14-8

O

OSPF
authentication-key 8-9
cost 8-10
dead-interval 8-10
hello-interval 8-10
Link State Advertisement 8-13
MD5 認証 8-10
NSSA 8-12
アップデート パケット ペーシングの表示 8-16
イネーブル 8-6
インターフェイス パラメータ 8-9
エリア MD5 認証 8-12
エリア パラメータ 8-11
エリア認証 8-12
概要 8-5
集約ルート コスト 8-12
スタブ エリア 8-12
デフォルト ルート 8-14
ネイバ ステートのロギング 8-16
パケットのペーシング 8-16
プロセス 8-5
モニタ 8-17
ルート マップ 8-7
ルート計算タイマー 8-15
ルート集約 8-13
ルートの再分配 8-7

P

PAT（Port Address Translation）
制限 20-54
PIM の機能、設定 8-25
ping
ICMP を参照
Port Address Translation（ポート アドレス変換）
NAT も参照

スタティック　12-29
PORT コマンド、FTP　20-23

Q

QoS の互換性　1-8

R

RADIUS
サーバの設定　14-13
サポート　14-5
ダウンロード可能なアクセス リスト　15-9
ネットワーク アクセス許可　15-8
ネットワーク アクセス認証　15-3
RAS H.323 トラブルシューティング　20-41
RealPlayer　20-53
RIP
イネーブル化　8-18
概要　8-18
デフォルト ルート アップデート　8-18
パッシブ　8-18
RSA キー、生成　21-3
RSH 接続　A-4
RTSP 検査
概要　20-53
設定　20-54

S

SCCP（Skinny）検査
Cisco IP Phone、サポート　20-63
設定　20-63
SDI
サポート　14-7
設定　14-13
security-level
設定　6-4
show コマンド、出力のフィルタリング　C-5
SIP 検査
インスタント メッセージング　20-57
概要　20-58
設定　20-59
タイムアウト値、設定　20-61
トラブルシューティング　20-61
SMTP 検査
概要　20-67
設定　20-68
SNMP
MIB　23-2
概要　23-2
管理ステーション　23-6
トラップ　23-2
source quench、ICMP メッセージ　D-17
SPAN セッション　2-2
SSH
RSA キー　21-3
同時接続　21-3
認証　21-13
ユーザ認証　21-4
ルールの最大数　A-6
ログイン　21-4
Sun RPC 検査
概要　20-73
設定　20-73
SVI
概要　2-7
設定　2-9
複数　2-7
Switched Virtual Interfaces
SVI を参照
SYN クッキー　4-34
SYN 攻撃、モニタ　4-34
Syslog サーバ
EMBLEM フォーマット
イネーブル　23-10
設定　23-24
出力先　23-10
複数の出力先　23-11
装置 ID、メッセージへの記載　23-11
ファシリティ、指定　23-9

T

TACACS+
コマンド許可　21-20
サーバの設定　14-13
サポート　14-6
ネットワーク アクセス許可　15-7
TCP
コンテキストあたりの接続制限　4-16

シーケンスのランダム化　19-2
接続制限　19-2
接続、削除　A-4
バックツーバック接続　A-4
ポートと文字名　D-13
TCP 代行受信
透過モードの設定　7-8, 12-24
モニタ　4-34
Telnet
同時接続　21-2
認証　21-13
ルールの最大数　A-6

U

UDP
コンテキストあたりの接続制限　4-16
接続ステート情報　1-7
接続制限　19-2
ポートと文字名　D-13
Unicast Reverse Path Forwarding　19-4
URL
コンテキスト コンフィギュレーション、設定　4-21
コンテキスト コンフィギュレーション、変更　4-26
フィルタリング　16-5

V

VLAN
FWSM への割り当て　2-4
インターフェイス　2-4
共有　4-7
コンテキストへの割り当て　4-20
最大数　A-3
マップされたインターフェイス名　4-21
VoIP
トラブルシューティング　20-40
プロキシ サーバ　20-57
VPN
管理アクセス　21-6
基本設定　21-6
クライアント トンネル　21-8
サイトツーサイト トンネル　21-10
トランスフォーム　21-7
VRRP　5-9

W

WAN ポート　A-2
Web クライアント、セキュア認証　15-4

あ

アカウンティング　15-12
アクセス リスト
ACE の順序　10-3
ACE ロギング、設定　10-24
EtherType、概要　10-10
EtherType、追加　10-11
NAT アドレス　10-3
NAT 使用時の IP アドレスに関する注意事項　10-3
暗黙の拒否　10-3
インターフェイス、適用　11-5
オブジェクトのグループ化　10-13
概要　10-2
拡張　10-6
拡張、概要　10-7
拡張、追加　10-7
拒否フロー、管理　10-25
コミット　10-5
コメント　10-20
最大数のルール　10-6
ダウンロード可能　15-9
着信　11-2
発信　11-2
標準アクセス リスト、追加　10-12
メモリ パーティション　4-18
メモリ限度　10-6
ロギング　10-23
アクティブ / アクティブ フェールオーバー
アクティブ ステート　13-13
概要　13-13
コマンドの複製　13-14
スタンバイ ステート　13-13
ステータス　13-37
セカンダリ ステータス　13-13
設定
HTTP の複製　13-30
インターフェイスのポーリング間隔　13-31

装置のポーリング間隔　13-31
フェールオーバー　13-26
フェールオーバー グループ プリエンプション　13-30
設定の同期化　13-14, 13-15
設定の保存　13-15
デバイスの初期化　13-14
動作　13-16
トリガー　13-15
フェールオーバー グループ　13-13
フェールオーバーの条件　13-31
プライマリ ステータス　13-13
アクティブ / スタンバイ フェールオーバー
アクティブ ステート　13-10
概要　13-9
コマンドの複製　13-11
スタンバイ ステート　13-10
ステータス　13-33
セカンダリ ステータス　13-10
設定
HTTP の複製　13-25
インターフェイスのポーリング間隔　13-25
装置のポーリング間隔　13-25
フェールオーバー　13-21
設定の同期化　13-10, 13-11
設定の保存　13-11
デバイスの初期化　13-10
動作　13-12
トリガー　13-11
フェールオーバーの条件　13-25
プライマリ ステータス　13-10
アダプティブ セキュリティ アルゴリズム　1-7
アプリケーション パーティションのパスワード、消去　24-8
アプリケーション検査
概要　20-2
サポート対象プロトコル　20-4
セキュリティ レベル要件　6-2
設定　20-1
適用　20-7
マップ、使用　20-7

い

イネーブル EXEC モード
アクセス方法　3-3
認証　21-14
プロンプト　C-2
インスタント メッセージング　20-57
インストール
現在のパーティションへのソフトウェアのインストール　22-4, 22-10
任意パーティションへのソフトウェアのインストール　22-6
モジュールの確認　2-3
インターフェイス
オフ　6-8
オン　6-8
共有　4-7
グローバル アドレス　12-25
最大数　A-3
名前の設定　6-3, 6-6
ヘルス モニタ　13-19
ポーリング間隔の設定　13-25, 13-31
モニタ対象インターフェイスのステータスの表示　13-40
インターフェイスの名前の設定　6-3, 6-6

え

エコー応答、ICMP メッセージ　D-17

お

オーバーサブスクライブ、リソース　4-13
オープン ポート　D-16
オブジェクト グループ
拡張　10-6
削除　10-19
ネスト　10-17

か

外部ネットワーク　1-1
仮想ファイアウォール
セキュリティ コンテキストを参照
カットスルー プロキシ　15-1
画面表示のページング　C-6
管理 IP アドレス、透過ファイアウォール　6-5
管理コンテキスト
概要　1-8, 4-2
変更　4-25

関連資料　xxvii

き

基本設定　7-1
キュー、ロギング
　サイズの変更　23-23
　統計情報の表示　23-23
共有 VLAN　4-7
共有インターフェイス　4-7
許可
　概要　14-3
　コマンド　21-15
　ダウンロード可能なアクセス リスト　15-8
　ネットワーク アクセス　15-7
拒否フロー、ロギング　10-25

く

クイック スタート　xxxiv
クエスチョン マーク
　コマンド文字列　C-4
　ヘルプ　C-4
クラス
　リソース管理を参照
クラス A、B、C アドレス　D-2
クラス、メッセージ
　タイプ　23-20
　メッセージ クラス変数　23-20
　メッセージのフィルタリング　23-20
クラッシュ ダンプ　24-10
グローバル アドレス
　指定　12-25
　注意事項　12-14

け

検査
　アプリケーション検査を参照

こ

高速パス　1-7
構文の形式　C-3
コマンド プロンプト
　概要　C-2
　設定　7-6
コマンド許可
　概要　21-13
　設定　21-15
　複数のコンテキスト　21-16
コマンドの短縮形　C-3
コマンドラインの編集　C-3
コメント
　アクセス リスト　10-20
　設定　C-6
コンソール ポート、外部　3-2
コンテキスト
　セキュリティ コンテキストを参照
コンテキスト間の切り替え　4-24
コンパクト フラッシュ　2-14
コンフィギュレーション モード
　アクセス方法　3-3
　プロンプト　C-2
コンフィギュレーション モードのプロンプト　C-2

さ

最小限の設定　xxxiv
サイトツーサイト トンネル　21-10
サブネット マスク
　/ ビット　D-3
　アドレス範囲　D-5
　概要　D-3
　ドット付き 10 進数　D-3
　ホスト数　D-3

し

時間超過、ICMP メッセージ　D-17
時間範囲、アクセス リスト　10-21
システム コンフィギュレーション
　概要　4-2
　ネットワークの設定値　4-3
システム メッセージ
　クラス
　　出力先　23-19
　　リスト　23-20
　グループ内での管理
　　メッセージ クラス　23-20

メッセージ リストの作成　23-19
グループ内での設定
重大度　23-6
メッセージ リスト　23-21
重大度　23-28
メッセージの重大度の変更　23-6
リスト　23-28
出力先　23-6
Syslog メッセージ サーバ　23-6
Telnet または SSH セッション　23-6
内部バッファ　23-6
電子メール アドレス　23-12
使用される変数　23-27, 23-28
装置 ID、記載　23-23
タイムスタンプ、記載　23-23
フェールオーバー　13-43
フォーマット　23-27
メッセージ クラスによるフィルタリング　23-19
メッセージ リスト、作成　23-19
リストの作成　23-19
ロギングのディセーブル化　23-6
システム メッセージの変数、リスト　23-28
システム要件　A-2
実行コンフィギュレーション
ダウンロード　22-17
バックアップ　22-19
表示　3-6
保存　3-4
リセット　3-6
自動アップデート
ステータス　22-22
設定　22-21
重大度、システム メッセージ
定義　23-28
フィルタリング　23-6
変更　23-6
リスト　23-28
出力先　23-6
SNMP 管理ステーション　23-6
Syslog サーバ　23-6, 23-10
Telnet または SSH セッション　23-6
指定　23-12
電子メール アドレス　23-6, 23-12
内部バッファ　23-6
ログの表示　23-9
仕様　A-1
情報
応答、ICMP メッセージ　D-17
要求、ICMP メッセージ　D-17
初期接続制限　19-2
シングルモード
イネーブル化　4-11
コンフィギュレーションのバックアップ　4-11
設定　4-11
復元　4-12

す

スイッチ
BPDU の転送　2-13
FWSM とのセッション　3-2
最大モジュール数　A-3
システム要件　A-2
設定　2-1
フェールオーバーと透過ファイアウォールの両立　2-13
フェールオーバーの設定　2-13
フェールオーバー用のトランク　2-13
モジュールの搭載確認　2-3
モジュールのリセット　2-15
モジュールへの VLAN 割り当て　2-4
スイッチ ファブリック モジュール　A-3
スイッチからのセッション　3-2
スーパーバイザ IOS　A-2
スーパーバイザ エンジンのバージョン　A-2
スタートアップ コンフィギュレーション
実行コンフィギュレーションへのコピー　3-6
ダウンロード　22-17
バックアップ　22-19
表示　3-6
保存　3-4
マルチコンテキスト モード　4-3
スタティック ARP エントリ　17-2
スタティック MAC アドレス エントリ　17-4
スタティック NAT
NAT を参照
スタティック PAT
NAT を参照
スタブ マルチキャスト ルーティング　8-24
ステート リンク
ステートフル フェールオーバーを参照
ステートフル インスペクション　1-7

ステートフル フェールオーバー
概要 13-18
ステート リンク 13-4
渡されるステート情報 13-18
ステルス ファイアウォール
透過ファイアウォールを参照

せ

制御プレーン パス 1-7
セキュリティ コンテキスト
MSFC の互換性 1-5
VLAN 割り当て 4-20
概要 4-2
カスケード 4-9
管理 4-25
管理コンテキスト
概要 1-8, 4-2
変更 4-25
切り替え 4-24
コマンド許可 21-16
削除 4-25
サポートされていない機能 4-2
設定
URL、設定 4-21
URL、変更 4-26
ファイル 4-3
追加 4-20
ネスト 4-9
プロンプト C-2
分類機能 4-3
マップされたインターフェイス名 4-21
マルチモード、イネーブル化 4-11
モニタ 4-28
リソース クラスへの割り当て 4-23
リソース管理 4-13, 4-32
リロード 4-27
ログイン 4-10
セキュリティ レベル
概要 6-2
セッション管理パス 1-7
接続
削除 A-4
ブロック 19-5
接続制限
TCP および UDP 19-2
コンテキストあたり 4-16
設定 23-21
コメント C-6
コンテキスト ファイル 4-3
コンテキストの URL 4-21
最小限 xxxiv
スイッチ 2-1
テキスト ファイル 3-7
表示 3-6
保存 3-4
リセット 3-6
ログ設定の消去 23-25
設定の消去、ロギング 23-25
設定のテスト 24-2

そ

装置 ID、メッセージへの記載 23-23
装置のヘルス モニタ 13-19
装置のポーリング間隔、設定 13-25, 13-31
ソフトウェアのインストール
現在のパーティション 22-4
任意のパーティション 22-6
メンテナンス 22-14

た

帯域幅
最大数 A-3
制限 4-13
代替アドレス、ICMP メッセージ D-17
ダイナミック NAT
NAT を参照
タイムスタンプ
応答、ICMP メッセージ D-17
要求、ICMP メッセージ D-17
タイムスタンプ、システム メッセージへの記載 23-23
ダウンロード可能なアクセス リスト 15-9

ち

着信アクセス リスト 11-2

て

データ フロー
　透過ファイアウォール　5-13
　ルーテッド ファイアウォール　5-3
デバッグ メッセージ　24-10
　フェールオーバー　13-44
デフォルト クラス　4-14
デュアル IP スタック　9-4

と

同一セキュリティ レベルの通信
　NAT　12-13
　設定　6-8
透過ファイアウォール
　ARP 検査
　　イネーブル化　17-3
　　概要　17-2
　　スタティック エントリ　17-2
　DHCP パケット、許可　10-8
　HSRP　5-9
　MAC アドレス タイムアウト　17-5
　MAC 学習、ディセーブル化　17-5
　NAT　5-12
　VRRP　5-9
　インターフェイス、設定　6-5
　概要　5-9
　管理 IP アドレス　6-5
　固有のインターフェイス　4-5
　サポートされていない機能　5-12
　スタティック MAC アドレス エントリ　17-4
　設定　5-17
　注意事項　5-11
　データ フロー　5-13
　パケットの処理　10-7
　フェールオーバーの設定　13-8
　マルチキャスト トラフィック　5-10
到達不能、ICMP メッセージ　D-17
ドット付き 10 進数サブネット マスク　D-3
ドメイン名、設定　7-5
トラップ、SNMP　23-2
トラフィック フロー
　透過ファイアウォール　5-13
　ルーテッド ファイアウォール　5-3
トラブルシューティング
　H.323　20-40
　H.323 RAS　20-41
　SIP　20-61
　一般的な問題　24-11
　クラッシュ ダンプ　24-10
　設定　24-2
　デバッグ メッセージ　24-10
　パケットのキャプチャ　24-10
　パスワード復旧　24-8
トンネル
　VPN クライアント アクセス、設定　21-8
　基本設定　21-6
　サイトツーサイト、設定　21-10

な

内部、定義　1-1

に

認証
　CLI アクセス　21-13
　FTP　15-2
　HTTP　15-2
　Telnet　15-2
　Web クライアント　15-4
　イネーブル EXEC モード　21-14
　概要　14-2
　ネットワーク アクセス　15-2

ね

ネットワーキング プロセッサ　1-7
ネットワーク、重複　12-36

は

パーティション
　アプリケーション　2-14
　クラッシュ ダンプ　2-14
　ネットワーク コンフィギュレーション　2-14
　ブート　2-14
　フラッシュ メモリ　2-14
　メンテナンス　2-14

ハーフクローズ接続の制限　19-3
排除　19-5
パケット
　キャプチャ　24-10
　フロー
　　透過ファイアウォール　5-13
　　ルーテッド ファイアウォール　5-3
　分類機能　4-3
パケットのキャプチャ　24-10
パスワード
　トラブルシューティング　24-8
　復旧　24-8
　変更　7-2
　リセット
　　アプリケーション　24-8
　　メンテナンス　24-9
発信アクセス リスト　11-2
バッファラップ
　FTP サーバに送信　23-16, 23-18
　フラッシュに保存　23-6
　内部フラッシュに保存　23-17
パラメータの問題、ICMP メッセージ　D-17

ひ

非対称ルーティング サポート　8-28
ビット サブネット マスク　D-3

ふ

ファイアウォール モード
　概要　5-1
　設定　5-1
ファイアウォールのバイパス　2-7
ファシリティ、設定　23-11
フィルタリング
　ActiveX　16-2
　FTP　16-10
　HTTP　16-8
　HTTPS　16-9
　Java アプレット　16-4
　show コマンドの出力　C-5
　URL　16-5
　概要　16-1
　サポート対象のサーバ　16-5
　除外　16-9
　セキュリティ レベル要件　6-2
　長い HTTP URL
　　サイズの設定　16-8
　　短縮　16-9
　ルールの最大数　A-6
ブート
　FWSM から　24-7
　スイッチから　2-15
ブート パーティション　2-14
プール、アドレス
　DHCP　8-30
　VPN　21-9
　グローバル NAT　12-25
フェールオーバー
　SNMP トラップ　13-44
　アクティブ / アクティブ
　　アクティブ / アクティブ フェールオーバーを参照
　アクティブ / スタンバイ
　　アクティブ / スタンバイ フェールオーバーを参照
　インターフェイスのヘルス モニタ　13-19
　概要　13-2
　強制実行　13-42
　システム メッセージ　13-43
　障害装置の復元　13-43
　スイッチの設定　2-13
　ステートフル
　　ステートフル フェールオーバーを参照
　設定
　　アクティブ / アクティブ　13-26
　　アクティブ / スタンバイ　13-21
　設定の表示　13-41
　装置のヘルス モニタ　13-19
　ディセーブル化　13-42
　テスト　13-41
　デバッグ メッセージ　13-44
　透過ファイアウォールの設定　13-8
　トランク　2-13
　モジュール配置
　　シャーシ内　13-4, 13-5
　要件
　　ソフトウェア　13-2
　　ライセンス　13-2
　リンク
　　概要　13-3
　　セキュリティ保護　13-31

フェールオーバー グループ
preempt コマンド 13-30
コンテキストの割り当て先 13-28
作成 13-28
障害前のステートへの復元 13-43
定義 13-13
負荷分散、バックプレーン EtherChannel 2-12
複数の SVI 2-7
プライベート ネットワーク D-2
フラグメント サイズ、設定 19-4
フラッシュ メモリ
概要 2-14
サイズ A-3
パーティション 2-14
ブリッジ グループ
IP アドレス、割り当て 6-7
概要 1-6
ブリッジ テーブル
MAC アドレス テーブルを参照
プロキシ サーバ、SIP 20-57
プロトコルの番号と文字名 D-13
プロンプト
more C-6
コマンド C-2
設定 7-6

へ

ヘルプ、コマンドライン C-4
変換エラー、ICMP メッセージ D-17

ほ

ポート
装置でのオープン D-16
リダイレクション、NAT 12-37
ホスト名、設定 7-5
ホスト、サブネット マスク D-3
ポリシー NAT
概要 12-10
スタティック PAT、設定 12-29
スタティック、設定 12-27
ダイナミック、設定 12-24
ルールの最大数 A-6

ま

マスク
応答、ICMP メッセージ D-17
要求、ICMP メッセージ D-17
マップされたインターフェイス名 4-21
マルチキャスト トラフィック 5-10
マルチキャスト ルーティング 8-20
マルチコンテキスト モード
セキュリティ コンテキストを参照

め

メッセージ クラス
メッセージ クラスについて 23-19
リスト 23-20
メッセージ リスト
作成 23-21
フィルタリング 23-21
メッセージの重大度、リスト 23-28
メッセージのディセーブル化、特定のメッセージ ID 23-24
メッセージのフォーマット 23-27
メモリ
RAM A-3
アクセス リスト 10-6
パーティション 4-18
フラッシュ A-3
ルール 10-6
メンテナンス パーティション
アプリケーション ソフトウェアのインストール 22-6
ソフトウェアのインストール 22-14
パスワード
設定 7-3
リセット 24-9
メンテナンス ソフトウェアのインストール 22-6

も

モード
コンテキスト 4-11
ファイアウォール 5-1
モニタ
OSPF 8-17

SNMP 23-2
リソース管理 4-30
モバイル リダイレクト、ICMP メッセージ D-17

ゆ

ユーザ モード
アクセス方法 3-2
プロンプト C-2

よ

要件 A-2

ら

ライセンス 22-2

り

リセット
FWSM CLI から 24-7
スイッチから 2-15
リソース管理 4-32
オーバーサブスクライブ 4-13
概要 4-13
クラス 4-16
コンテキストの割り当て 4-23
設定 4-13
デフォルト クラス 4-14
無制限 4-14
モニタ 4-30
リソース タイプ 4-16
リダイレクト、ICMP メッセージ D-17
リブート
FWSM CLI から 24-7
スイッチから 2-15
リモート管理
ASDM 21-5
SSH 21-3
Telnet 21-2
VPN 21-6
リロード
FWSM CLI から 24-7
コンテキスト 4-27
スイッチから 2-15

る

ルータ
アドバタイズ、ICMP メッセージ D-17
送信要求、ICMP メッセージ D-17
ルーティング
OSPF 8-18
RIP 8-19
その他のプロトコル 10-7
ルーテッド ファイアウォール
インターフェイス、設定 6-3
設定 5-17
データ フロー 5-3
ルート
OSPF のモニタリング 8-17
集約 8-14
設定 8-2
デフォルトの生成 8-14
ネイバのロギング 8-16
ループ、回避 2-13
ルール
コンテキスト用のプール A-6
最大数 10-6

れ

レイヤ 2 転送テーブル
MAC アドレス テーブルを参照
レイヤ 2 ファイアウォール
透過ファイアウォールを参照

ろ

ローカル ユーザ データベース
サポート 14-9
設定 14-11
ユーザの追加 14-11
ログイン 21-14
ロギング
EMBLEM フォーマット 23-24
Syslog サーバ、指定 23-10
アクセス リスト 10-23

キュー
キュー統計情報の表示 23-23
サイズの変更 23-23
設定 23-22
クラス
タイプ 23-20
メッセージのフィルタリング 23-19
重大度、変更 23-25
出力先
ASDM 23-13
Syslog サーバ 23-11
出力先として設定 23-10
Telnet または SSH セッション 23-6
内部バッファ 23-6
ファシリティ 23-11
電子メール アドレス 23-12, 23-13
装置 ID、システム メッセージへの記載 23-23
タイムスタンプ、記載 23-23
ファシリティ、設定 23-11
フィルタリング
重大度 23-6
メッセージ クラス 23-20
メッセージ リスト 23-21
ロギング キュー、設定 23-23
電子メール
宛先アドレス 23-13
出力先として設定 23-12
送信元アドレス 23-12
ロギング キュー、設定 23-23
ログ バッファラップ
FTP サーバに送信 23-18
内部フラッシュに保存 23-17
ログイン
FTP 15-2
SSH 3-2
Telnet 3-2
セッション 3-2
ローカル ユーザ 21-14
ログイン バナー 7-7
ログの出力先
ASDM 23-13
Syslog サーバ 23-6
Telnet または SSH セッション 23-6
内部バッファ 23-6
内部バッファロギング
出力先
内部バッファ 23-6
電子メール アドレス 23-12
ログの表示 23-9
ロックアウトの回復 21-25