



# **Cisco セキュリティ アプライアンス コマンド ライン コンフィギュレーション ガイド**

Cisco ASA 5500 シリーズおよび Cisco PIX 500 シリーズ用

Software Version 7.1(1)



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

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

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) パブリック ドメイン パージョンとして、UCB が開発したプログラムを最適化したものです。All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知らされていても、それらに対する責任を一切負いません。

CCSP、Cisco Square Bridge のロゴ、Follow Me Browsing、および StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn および iQuick Study は、Cisco Systems, Inc. のサービスマークです。Access Registrar、Aironet、ASIST、BPX、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Cisco Unity、Empowering the Internet Generation、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、FormShare、GigaDrive、GigaStack、HomeLink、Internet Quotient、IOS、IP/TV、iQ Expertise、iQ のロゴ、iQ Net Readiness Scorecard、LightStream、Linksys、MeetingPlace、MGX、Networkers のロゴ、Networking Academy、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、ProConnect、RateMUX、ScriptShare、SlideCast、SMARTnet、StrataView Plus、SwitchProbe、TeleRouter、The Fastest Way to Increase Your Internet Quotient、TransPath、および VCO は、米国および一部の国における Cisco Systems, Inc. とその関連会社の登録商標です。

このマニュアルおよび Web サイトで言及されているその他の商標はすべて、それぞれの所有者のものです。「パートナー」という語の使用は、シスコと他社の提携関係を意味するものではありません。(0501R)

Cisco セキュリティ アプライアンス コマンド ライン コンフィギュレーション ガイド  
Copyright © 2006 Cisco Systems, Inc.  
All rights reserved.



|                                 |        |
|---------------------------------|--------|
| <b>このマニュアルについて</b>              | xxix   |
| <b>マニュアルの目的</b>                 | xxx    |
| 対象読者                            | xxx    |
| 関連マニュアル                         | xxx    |
| マニュアルの構成                        | xxxi   |
| 表記法                             | xxxi   |
| <b>技術情報の入手方法</b>                | xxxiv  |
| Cisco.com                       | xxxiv  |
| マニュアルの発注方法（英語版）                 | xxxiv  |
| シスコシステムズマニュアルセンター               | xxxiv  |
| <b>テクニカル サポート</b>               | xxxv   |
| Cisco Technical Support Web サイト | xxxv   |
| Japan TAC Web サイト               | xxxv   |
| サービス リクエストの発行                   | xxxvi  |
| サービス リクエストのシビラティの定義             | xxxvi  |
| その他の資料および情報の入手                  | xxxvii |

---

PART 1

---

**準備と一般情報**

---

CHAPTER 1

|                                                                                  |     |
|----------------------------------------------------------------------------------|-----|
| <b>セキュリティ アプライアンスの概要</b>                                                         | 1-1 |
| <b>ファイアウォール機能の概要</b>                                                             | 1-2 |
| <b>セキュリティ ポリシーの概要</b>                                                            | 1-2 |
| アクセスリストによるトラフィックの許可または拒否                                                         | 1-2 |
| NAT の適用                                                                          | 1-3 |
| スルー トラフィックに対する AAA の使用                                                           | 1-3 |
| HTTP、HTTPS、または FTP フィルタリングの適用                                                    | 1-3 |
| アプリケーション検査の適用                                                                    | 1-3 |
| Advanced Inspection and Prevention Security Services Module (AIP SSM) へのトラフィック送信 | 1-3 |
| QoS ポリシーの適用                                                                      | 1-3 |
| 接続の制限と TCP 正規化の適用                                                                | 1-4 |
| <b>ファイアウォール モードの概要</b>                                                           | 1-4 |

|                     |     |
|---------------------|-----|
| ステートフル インспекションの概要 | 1-4 |
| VPN 機能の概要           | 1-6 |
| 侵入防御サービス機能の概要       | 1-6 |
| セキュリティ コンテキストの概要    | 1-7 |

## CHAPTER 2

|                                        |     |
|----------------------------------------|-----|
| <b>はじめに</b>                            | 2-1 |
| コマンドライン インターフェイスへのアクセス                 | 2-2 |
| 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 | 2-3 |
| コンフィギュレーションの処理                         | 2-4 |
| コンフィギュレーション変更の保存                       | 2-4 |
| 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  | 2-4 |
| コンフィギュレーションの表示                         | 2-5 |
| コンフィギュレーション設定のクリアと削除                   | 2-5 |
| テキスト コンフィギュレーション ファイルのオフラインでの作成        | 2-6 |

## CHAPTER 3

|                                     |      |
|-------------------------------------|------|
| <b>マルチコンテキスト モードのイネーブル化</b>         | 3-1  |
| セキュリティ コンテキストの概要                    | 3-2  |
| セキュリティ コンテキストの一般的な使用方法              | 3-2  |
| サポートされていない機能                        | 3-2  |
| コンテキスト コンフィギュレーション ファイル             | 3-3  |
| セキュリティ アプライアンスによるパケットの分類方法          | 3-3  |
| コンテキスト間でのインターフェイス共有                 | 3-7  |
| インターフェイス共有のためのガイドライン                | 3-7  |
| セキュリティ コンテキストのカスケード接続               | 3-8  |
| マルチコンテキスト モードでのセキュリティ アプライアンスへのログイン | 3-9  |
| マルチコンテキスト モードのイネーブル化とディセーブル化        | 3-10 |
| 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          | 3-10 |
| マルチコンテキスト モードのイネーブル化                | 3-10 |
| シングルコンテキスト モードの復元                   | 3-11 |

## CHAPTER 4

|                                   |     |
|-----------------------------------|-----|
| <b>イーサネットとサブインターフェイスの設定</b>       | 4-1 |
| RJ-45 インターフェイスの設定とイネーブル化          | 4-2 |
| 4GE SSM でのファイバ インターフェイスの設定とイネーブル化 | 4-4 |
| サブインターフェイスの設定とイネーブル化              | 4-5 |

## CHAPTER 5

|                            |     |
|----------------------------|-----|
| <b>セキュリティ コンテキストの追加と管理</b> | 5-1 |
| セキュリティ コンテキストの設定           | 5-2 |

|                         |      |
|-------------------------|------|
| セキュリティ コンテキストの削除        | 5-6  |
| 管理コンテキストの変更             | 5-7  |
| コンテキストとシステム実行スペース間の切り替え | 5-7  |
| セキュリティ コンテキスト URL の変更   | 5-8  |
| セキュリティ コンテキストのリロード      | 5-9  |
| コンフィギュレーションのクリアによるリロード  | 5-9  |
| コンテキストの削除および再追加によるリロード  | 5-9  |
| セキュリティ コンテキストの監視        | 5-10 |
| コンテキスト情報の表示             | 5-10 |
| リソースの使用状況の表示            | 5-11 |

## CHAPTER 6

|                                |     |
|--------------------------------|-----|
| <b>インターフェイス パラメータの設定</b>       | 6-1 |
| セキュリティ レベルの概要                  | 6-2 |
| インターフェイスの設定                    | 6-3 |
| 同一セキュリティ レベルにあるインターフェイス間の通信の許可 | 6-7 |

## CHAPTER 7

|                          |     |
|--------------------------|-----|
| <b>基本設定</b>              | 7-1 |
| イネーブル パスワードの変更           | 7-1 |
| ホスト名の設定                  | 7-2 |
| ドメイン名の設定                 | 7-2 |
| 日付と時刻の設定                 | 7-3 |
| 時間帯と夏時間の日付範囲の設定          | 7-3 |
| NTP サーバを使用する日付と時刻の設定     | 7-4 |
| 手動での日付と時刻の設定             | 7-5 |
| 透過ファイアウォールの管理 IP アドレスの設定 | 7-6 |

## CHAPTER 8

|                                                       |      |
|-------------------------------------------------------|------|
| <b>IP ルーティングと DHCP サービスの設定</b>                        | 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 プロセス間のルート再配布                                     | 8-7  |
| ルートマップの追加                                             | 8-7  |
| スタティック ルート、接続されているルート、または OSPF ルートを OSPF プロセスに再配布する方法 | 8-8  |
| OSPF インターフェイスのパラメータの設定                                | 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 にルートを再配布する場合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 |
| ネイバーがアップ状態またはダウン状態になった時点でのロギング     | 8-16 |
| OSPF アップデート パケットのペーシングの表示          | 8-16 |
| OSPF のモニタリング                       | 8-17 |
| OSPF プロセスの再始動                      | 8-18 |
| RIP の設定                            | 8-18 |
| RIP の概要                            | 8-18 |
| RIP のイネーブル化                        | 8-19 |
| 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              | 8-21 |
| IGMP 機能の設定                         | 8-21 |
| インターフェイスにおける IGMP のディセーブル化         | 8-22 |
| グループ メンバーシップの設定                    | 8-22 |
| グループのスタティック加入の設定                   | 8-22 |
| マルチキャスト グループへのアクセスの制御              | 8-23 |
| インターフェイスにおける IGMP 状態の数の制限          | 8-23 |
| クエリー間隔およびクエリー タイムアウトの修正            | 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              | 8-25 |
| PIM 機能の設定                          | 8-25 |
| インターフェイスにおける PIM のディセーブル化          | 8-26 |
| スタティック ランデブー ポイント アドレスの設定          | 8-26 |
| 代表ルータの優先順位の設定                      | 8-27 |
| PIM 登録メッセージのフィルタリング                | 8-27 |
| PIM メッセージ間隔の設定                     | 8-27 |
| マルチキャスト ルーティングの参考資料                | 8-27 |
| DHCP の設定                           | 8-28 |
| DHCP サーバの設定                        | 8-28 |
| DHCP サーバのイネーブル化                    | 8-28 |
| DHCP オプションの設定                      | 8-30 |
| DHCP サーバを利用する Cisco IP Phone の使用方法 | 8-31 |

DHCP リレー サービスの設定 8-32

DHCP クライアントの設定 8-33

## CHAPTER 9

### IPv6 の設定 9-1

IPv6 対応のコマンド 9-2

インターフェイスでの IPv6 の設定 9-3

IPv6 デフォルト ルートおよびスタティック ルートの設定 9-5

IPv6 アクセスリストの設定 9-6

IPv6 コンフィギュレーションの確認 9-7

show ipv6 interface コマンド 9-7

show ipv6 route コマンド 9-8

インターフェイスでのデュアル IP スタックの設定 9-8

IPv6 コンフィギュレーションの例 9-9

## CHAPTER 10

### AAA サーバとローカル データベースの設定 10-1

AAA の概要 10-2

認証の概要 10-2

認可の概要 10-2

アカウンティングの概要 10-3

AAA サーバおよびローカル データベースのサポート 10-4

サポートの要約 10-4

RADIUS サーバのサポート 10-5

認証方法 10-5

アトリビュートのサポート 10-5

RADIUS 機能 10-5

TACACS+ サーバのサポート 10-6

SDI サーバのサポート 10-7

SDI バージョンのサポート 10-7

2 ステップ認証プロセス 10-8

SDI プライマリ サーバおよびレプリカ サーバ 10-8

NT サーバのサポート 10-8

Kerberos サーバのサポート 10-8

LDAP サーバのサポート 10-9

LDAP による認証 10-9

LDAP での認可 10-10

LDAP アトリビュート マッピング 10-11

HTTP Form での WebVPN に対する SSO サポート 10-12

ローカル データベースのサポート 10-13

ユーザ プロファイル 10-13

|                           |       |
|---------------------------|-------|
| ローカル データベースの機能            | 10-13 |
| フォールバック サポート              | 10-14 |
| ローカル データベースの設定            | 10-15 |
| AAA サーバ グループおよびサーバの識別     | 10-17 |
| 証明書とユーザ ログイン クレデンシャルの使用方法 | 10-20 |
| ユーザ ログイン クレデンシャルの使用方法     | 10-20 |
| 証明書の使用方法                  | 10-20 |

## CHAPTER 11

|                                                            |       |
|------------------------------------------------------------|-------|
| <b>フェールオーバーの設定</b>                                         | 11-1  |
| フェールオーバーの概要                                                | 11-2  |
| フェールオーバーのシステム要件                                            | 11-2  |
| ハードウェア要件                                                   | 11-2  |
| ソフトウェア要件                                                   | 11-3  |
| ライセンス要件                                                    | 11-3  |
| フェールオーバー リンクとステートフル フェールオーバー リンク                           | 11-3  |
| フェールオーバー リンク                                               | 11-4  |
| ステートフル フェールオーバー リンク                                        | 11-6  |
| Active/Active フェールオーバーと Active/Standby フェールオーバー            | 11-7  |
| Active/Standby フェールオーバー                                    | 11-7  |
| Active/Active フェールオーバー                                     | 11-11 |
| 使用するフェールオーバーのタイプの決定                                        | 11-15 |
| 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                                 | 11-16 |
| 標準フェールオーバー                                                 | 11-16 |
| ステートフル フェールオーバー                                            | 11-16 |
| フェールオーバー ヘルスのモニタリング                                        | 11-17 |
| 装置ヘルスのモニタリング                                               | 11-17 |
| インターフェイスのモニタリング                                            | 11-17 |
| フェールオーバーの設定                                                | 11-19 |
| Active/Standby フェールオーバーの設定                                 | 11-19 |
| 前提条件                                                       | 11-19 |
| ケーブルベースの Active/Standby フェールオーバーの設定 (PIX セキュリティ アプライアンスのみ) | 11-19 |
| LAN ベースの Active/Standby フェールオーバーの設定                        | 11-21 |
| オプションの Active/Standby フェールオーバー設定値の設定                       | 11-25 |
| Active/Active フェールオーバーの設定                                  | 11-27 |
| 前提条件                                                       | 11-27 |
| ケーブルベースの Active/Active フェールオーバーの設定 (PIX セキュリティ アプライアンスのみ)  | 11-28 |
| LAN ベースの Active/Active フェールオーバーの設定                         | 11-30 |



|                                      |       |
|--------------------------------------|-------|
| オプションの Active/ Active フェールオーバー設定値の設定 | 11-34 |
| フェールオーバー通信の認証 / 暗号化の設定               | 11-38 |
| フェールオーバー コンフィギュレーションの確認              | 11-39 |
| show failover コマンドの使用方法              | 11-40 |
| 監視対象インターフェイスの表示                      | 11-47 |
| 実行コンフィギュレーション内のフェールオーバー コマンドの表示      | 11-48 |
| フェールオーバー機能のテスト                       | 11-48 |
| フェールオーバーの制御およびモニタリング                 | 11-49 |
| 強制フェールオーバー                           | 11-49 |
| フェールオーバーのディセーブル化                     | 11-49 |
| 故障した装置またはフェールオーバー グループの復元            | 11-50 |
| フェールオーバーのモニタリング                      | 11-50 |
| フェールオーバー システム メッセージ                  | 11-50 |
| デバッグ メッセージ                           | 11-50 |
| SNMP                                 | 11-51 |
| フェールオーバー コンフィギュレーションの例               | 11-51 |
| ケーブルベースの Active/Standby フェールオーバーの例   | 11-51 |
| LAN ベースの Active/Standby フェールオーバーの例   | 11-53 |
| LAN ベースの Active/ Active フェールオーバーの例   | 11-55 |

## PART 2

## ファイアウォールの設定

## CHAPTER 12

|                                              |       |
|----------------------------------------------|-------|
| ファイアウォール モードの概要                              | 12-1  |
| ルーテッド モードの概要                                 | 12-2  |
| IP ルーティングのサポート                               | 12-2  |
| ネットワーク アドレス変換                                | 12-2  |
| ルーテッド ファイアウォール モードでデータがセキュリティ アプライアンスを通過する方法 | 12-3  |
| 内部ユーザが Web サーバにアクセスする                        | 12-4  |
| 外部ユーザが DMZ 上の Web サーバにアクセスする                 | 12-5  |
| 内部ユーザが DMZ 上の Web サーバにアクセスする                 | 12-6  |
| 外部ユーザが内部ホストにアクセスしようとする                       | 12-7  |
| DMZ ユーザが内部ホストにアクセスしようとする                     | 12-8  |
| 透過モードの概要                                     | 12-9  |
| 透過ファイアウォールの機能                                | 12-9  |
| ネットワークでの透過ファイアウォールの使用                        | 12-10 |
| 透過ファイアウォール ガイドライン                            | 12-10 |
| 透過モードでサポートされない機能                             | 12-11 |

|                                 |       |
|---------------------------------|-------|
| 透過ファイアウォールを通過するデータの動き           | 12-12 |
| 内部ユーザが Web サーバにアクセスする           | 12-13 |
| 外部ユーザが内部ネットワーク上の Web サーバにアクセスする | 12-14 |
| 外部ユーザが内部ホストにアクセスしようとする          | 12-15 |

## CHAPTER 13

**アクセスリストによるトラフィックの指定** 13-1

|                                 |       |
|---------------------------------|-------|
| アクセスリストの概要                      | 13-2  |
| アクセスリストのタイプ                     | 13-2  |
| ACE の順序                         | 13-3  |
| アクセス コントロールによる暗黙的な拒否            | 13-3  |
| NAT 使用時にアクセスリストで使用する IP アドレス    | 13-3  |
| 拡張アクセスリストの追加                    | 13-6  |
| 拡張アクセスリストの概要                    | 13-6  |
| 透過ファイアウォールを通過する特殊な IP トラフィックの許可 | 13-6  |
| 拡張 ACE の追加                      | 13-7  |
| EtherType アクセスリストの追加            | 13-9  |
| 標準アクセスリストの追加                    | 13-11 |
| Webtype アクセスリストの追加              | 13-11 |
| オブジェクト グループ化機能によるアクセスリストの簡略化    | 13-12 |
| オブジェクト グループ化機能の動作               | 13-12 |
| オブジェクト グループの追加                  | 13-13 |
| プロトコル オブジェクト グループの追加            | 13-13 |
| ネットワーク オブジェクト グループの追加           | 13-14 |
| サービス オブジェクト グループの追加             | 13-15 |
| ICMP タイプ オブジェクト グループの追加         | 13-16 |
| オブジェクト グループのネスト                 | 13-17 |
| アクセスリストでのオブジェクト グループの使用         | 13-18 |
| オブジェクト グループの表示                  | 13-19 |
| オブジェクト グループの削除                  | 13-19 |
| アクセスリストへのコメントの追加                | 13-20 |
| 拡張アクセスリストのアクティブ化のスケジュール設定       | 13-21 |
| 時間範囲の追加                         | 13-21 |
| ACE への時間範囲の適用                   | 13-22 |
| アクセスリスト アクティビティのロギング            | 13-23 |
| アクセスリスト ロギングの概要                 | 13-23 |
| アクセス コントロール エントリのロギングの設定        | 13-24 |
| 拒否フローの管理                        | 13-25 |

## CHAPTER 14

|                               |       |
|-------------------------------|-------|
| <b>NAT の適用</b>                | 14-1  |
| NAT の概要                       | 14-2  |
| NAT の概要                       | 14-2  |
| NAT 制御                        | 14-3  |
| NAT のタイプ                      | 14-5  |
| ダイナミック NAT                    | 14-5  |
| PAT                           | 14-7  |
| スタティック NAT                    | 14-8  |
| スタティック PAT                    | 14-8  |
| NAT 制御がイネーブルな状態での NAT のバイパス   | 14-9  |
| ポリシー NAT                      | 14-10 |
| NAT および同じセキュリティ レベルのインターフェイス  | 14-13 |
| 実際のアドレスとの照合に使用される NAT コマンドの順序 | 14-13 |
| マッピング アドレスに関するガイドライン          | 14-14 |
| DNS および NAT                   | 14-14 |
| NAT 制御の設定                     | 14-16 |
| ダイナミック NAT および PAT の使用        | 14-17 |
| ダイナミック NAT および PAT の実装        | 14-17 |
| ダイナミック NAT または PAT の設定        | 14-23 |
| スタティック NAT の使用                | 14-26 |
| スタティック PAT の使用                | 14-28 |
| NAT のバイパス                     | 14-31 |
| アイデンティティ NAT の設定              | 14-31 |
| スタティック アイデンティティ NAT の設定       | 14-32 |
| NAT 免除の設定                     | 14-33 |
| NAT の例                        | 14-35 |
| アドレスが重複するネットワーク               | 14-35 |
| ポートのリダイレクト                    | 14-37 |

## CHAPTER 15

|                            |      |
|----------------------------|------|
| <b>ネットワーク アクセスの許可または拒否</b> | 15-1 |
| 着信アクセスリストおよび発信アクセスリストの概要   | 15-2 |
| インターフェイスへのアクセスリストの適用       | 15-5 |

## CHAPTER 16

|                              |      |
|------------------------------|------|
| <b>ネットワーク アクセスへの AAA の適用</b> | 16-1 |
| AAA パフォーマンス                  | 16-1 |
| ネットワーク アクセス認証の設定             | 16-2 |
| 認証の概要                        | 16-2 |
| ネットワーク アクセス認証のイネーブル化         | 16-3 |
| Web クライアントのセキュアな認証のイネーブル化    | 16-4 |

|                                        |       |
|----------------------------------------|-------|
| ネットワーク アクセス認可の設定                       | 16-7  |
| TACACS+ 認可の設定                          | 16-7  |
| RADIUS 認可の設定                           | 16-8  |
| ダウンロード可能な ACL を送信するための RADIUS サーバの設定   | 16-9  |
| ユーザごとの ACL 名をダウンロードするための RADIUS サーバの設定 | 16-13 |
| ネットワーク アクセスのアカウンティングの設定                | 16-14 |
| MAC アドレスによるトラフィックの認証と認可の免除             | 16-16 |

## CHAPTER 17

|                                 |             |
|---------------------------------|-------------|
| <b>フィルタリング サービスの適用</b>          | <b>17-1</b> |
| フィルタリングの概要                      | 17-1        |
| ActiveX オブジェクトのフィルタリング          | 17-2        |
| ActiveX フィルタリングの概要              | 17-2        |
| ActiveX フィルタリングのイネーブル化          | 17-2        |
| Java アプレットのフィルタリング              | 17-4        |
| 外部サーバによる URL および FTP 要求のフィルタリング | 17-5        |
| URL フィルタリングの概要                  | 17-5        |
| フィルタリング サーバの指定                  | 17-5        |
| コンテンツ サーバ応答のバッファリング             | 17-6        |
| サーバ アドレスのキャッシング                 | 17-7        |
| HTTP URL のフィルタリング               | 17-8        |
| HTTP フィルタリングの設定                 | 17-8        |
| 長い HTTP URL のフィルタリングのイネーブル化     | 17-8        |
| 長い HTTP URL の切り捨て               | 17-8        |
| トラフィックに対するフィルタリングの免除            | 17-9        |
| HTTPS URL のフィルタリング              | 17-9        |
| FTP 要求のフィルタリング                  | 17-10       |
| フィルタリング統計情報とフィルタリング設定の表示        | 17-11       |
| フィルタリング サーバ統計情報の表示              | 17-11       |
| バッファ コンフィギュレーションと統計情報の表示        | 17-11       |
| キャッシュ統計情報の表示                    | 17-12       |
| フィルタリング性能統計情報の表示                | 17-12       |
| フィルタリング コンフィギュレーションの表示          | 17-12       |

## CHAPTER 18

|                             |             |
|-----------------------------|-------------|
| <b>モジュラ ポリシー フレームワークの使用</b> | <b>18-1</b> |
| 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 グローバル ポリシー            | 18-2        |
| クラスマップによるトラフィックの特定          | 18-3        |

|                                     |       |
|-------------------------------------|-------|
| ポリシーマップによるアクションの定義                  | 18-6  |
| ポリシーマップの概要                          | 18-6  |
| デフォルト ポリシーマップ                       | 18-7  |
| ポリシーマップの追加                          | 18-8  |
| サービス ポリシーによるインターフェイスへのポリシーの適用       | 18-10 |
| モジュラ ポリシー フレームワークの例                 | 18-11 |
| HTTP トラフィックへの検査と QoS ポリシングの適用       | 18-11 |
| HTTP トラフィックへの検査のグローバルな適用            | 18-11 |
| 特定のサーバへの HTTP トラフィックに対する検査と接続制限値の適用 | 18-12 |
| NAT による HTTP トラフィックへの検査の適用          | 18-13 |

## CHAPTER 19

|                                |       |
|--------------------------------|-------|
| <b>AIP SSM および CSC SSM の管理</b> | 19-1  |
| AIP SSM の管理                    | 19-2  |
| AIP SSM について                   | 19-2  |
| AIP SSM の準備                    | 19-2  |
| AIP SSM へのトラフィックの誘導            | 19-3  |
| AIP SSM へのセッションの接続とセットアップの実行   | 19-5  |
| CSC SSM の管理                    | 19-7  |
| CSC SSM について                   | 19-7  |
| CSC SSM の準備                    | 19-9  |
| スキャンするトラフィックの指定                | 19-11 |
| CSC SSM を通過する接続の制限             | 19-13 |
| CSC SSM へのトラフィックの誘導            | 19-14 |
| SSM ステータスのチェック                 | 19-17 |
| SSM へのイメージの転送                  | 19-18 |

## CHAPTER 20

|                         |      |
|-------------------------|------|
| <b>ネットワーク攻撃の防止</b>      | 20-1 |
| TCP の正規化の設定             | 20-2 |
| 接続の制限値とタイムアウトの設定        | 20-5 |
| IP スプーフィングの防止           | 20-7 |
| フラグメント サイズの設定           | 20-7 |
| 不要な接続のブロック              | 20-8 |
| 基本 IPS をサポートする IP 監査の設定 | 20-9 |

## CHAPTER 21

|                    |      |
|--------------------|------|
| <b>QoS ポリシーの適用</b> | 21-1 |
| 概要                 | 21-2 |
| QoS の概念            | 21-3 |
| QoS の実装            | 21-4 |

|                                    |       |
|------------------------------------|-------|
| QoS の対象にするトラフィックの特定                | 21-6  |
| QoS ポリシーマップの定義                     | 21-8  |
| レート制限の適用                           | 21-9  |
| サービス ポリシーのアクティブ化                   | 21-10 |
| 低遅延キューイングの適用                       | 21-11 |
| プライオリティ キューイングの設定                  | 21-11 |
| プライオリティキューのサイズの変更                  | 21-12 |
| キュー遅延の低減                           | 21-12 |
| QoS の設定                            | 21-13 |
| QoS コンフィギュレーションの表示                 | 21-17 |
| QoS サービス ポリシー コンフィギュレーションの表示       | 21-17 |
| QoS ポリシーマップ コンフィギュレーションの表示         | 21-18 |
| インターフェイスのプライオリティキュー コンフィギュレーションの表示 | 21-18 |
| QoS 統計情報の表示                        | 21-19 |
| QoS ポリシング統計情報の表示                   | 21-19 |
| QoS プライオリティ統計情報の表示                 | 21-19 |
| QoS プライオリティキュー統計情報の表示              | 21-20 |

## CHAPTER 22

|                             |             |
|-----------------------------|-------------|
| <b>アプリケーション層プロトコル検査の設定</b>  | <b>22-1</b> |
| 検査エンジンの概要                   | 22-2        |
| アプリケーション プロトコル検査を使用するタイミング  | 22-2        |
| 検査に関する制限事項                  | 22-2        |
| デフォルトの検査ポリシー                | 22-3        |
| アプリケーション検査の設定               | 22-5        |
| CTIQBE 検査                   | 22-9        |
| CTIQBE 検査の概要                | 22-9        |
| 制限事項                        | 22-9        |
| CTIQBE 検査の確認と監視             | 22-10       |
| DNS 検査                      | 22-12       |
| DNS アプリケーション検査の動作           | 22-12       |
| DNS リライトの動作                 | 22-13       |
| DNS リライトの設定                 | 22-14       |
| DNS リライト用の static コマンドの使用   | 22-14       |
| DNS リライト用の alias コマンドの使用    | 22-14       |
| 2 つの NAT ゾーンを持つ DNS リライトの設定 | 22-15       |
| 3 つの NAT ゾーンを持つ DNS リライト    | 22-16       |
| 3 つの NAT ゾーンを持つ DNS リライトの設定 | 22-18       |
| DNS 検査の確認と監視                | 22-19       |

|                             |       |
|-----------------------------|-------|
| FTP 検査                      | 22-20 |
| FTP 検査の概要                   | 22-20 |
| strict オプションの使用             | 22-20 |
| 検査制御を追加するための FTP マップの設定     | 22-21 |
| FTP 検査の確認と監視                | 22-23 |
| GTP 検査                      | 22-24 |
| GTP 検査の概要                   | 22-24 |
| 検査制御を追加するための GTP マップの設定     | 22-25 |
| GTP 検査の確認と監視                | 22-29 |
| H.323 検査                    | 22-31 |
| H.323 検査の概要                 | 22-31 |
| H.323 の動作                   | 22-31 |
| 制限事項                        | 22-32 |
| H.323 および H.225 のタイムアウト値の設定 | 22-33 |
| H.323 検査の確認と監視              | 22-33 |
| H.225 セッションの監視              | 22-33 |
| H.245 セッションの監視              | 22-34 |
| H.323 RAS セッションの監視          | 22-34 |
| HTTP 検査                     | 22-35 |
| HTTP 検査の概要                  | 22-35 |
| 検査制御を追加するための HTTP マップの設定    | 22-35 |
| ICMP 検査                     | 22-39 |
| ICMP エラー検査                  | 22-39 |
| ILS 検査                      | 22-40 |
| MGCP 検査                     | 22-41 |
| MGCP 検査の概要                  | 22-41 |
| 検査制御を追加するための MGCP マップの設定    | 22-43 |
| MGCP タイムアウト値の設定             | 22-44 |
| MGCP 検査の確認と監視               | 22-44 |
| NetBIOS 検査                  | 22-45 |
| PPTP 検査                     | 22-46 |
| RSH 検査                      | 22-46 |
| RTSP 検査                     | 22-47 |
| RTSP 検査の概要                  | 22-47 |
| RealPlayer の使用              | 22-48 |
| 制限事項                        | 22-48 |
| SIP 検査                      | 22-49 |
| SIP 検査の概要                   | 22-49 |

|                      |       |
|----------------------|-------|
| SIP インスタント メッセージ     | 22-49 |
| SIP タイムアウト値の設定       | 22-50 |
| SIP 検査の確認と監視         | 22-51 |
| Skippy (SCCP) 検査     | 22-52 |
| SCCP 検査の概要           | 22-52 |
| Cisco IP Phone のサポート | 22-52 |
| 制限事項                 | 22-53 |
| SCCP 検査の確認と監視        | 22-53 |
| SMTP および拡張 SMTP 検査   | 22-54 |
| SNMP 検査              | 22-55 |
| SQL*Net 検査           | 22-56 |
| Sun RPC 検査           | 22-57 |
| Sun RPC 検査の概要        | 22-57 |
| Sun RPC サービスの管理      | 22-57 |
| Sun RPC 検査の確認と監視     | 22-58 |
| TFTP 検査              | 22-60 |
| XDMCP 検査             | 22-60 |

## CHAPTER 23

**ARP 検査およびブリッジング パラメータの設定** 23-1

|                        |      |
|------------------------|------|
| ARP 検査の設定              | 23-2 |
| ARP 検査の概要              | 23-2 |
| スタティック ARP エントリの追加     | 23-3 |
| ARP 検査のイネーブル化          | 23-3 |
| MAC アドレス テーブルのカスタマイズ   | 23-4 |
| MAC アドレス テーブルの概要       | 23-4 |
| スタティック MAC アドレスの追加     | 23-4 |
| MAC アドレス タイムアウトの設定     | 23-5 |
| MAC アドレス ラーニングのディセーブル化 | 23-5 |
| MAC アドレス テーブルの表示       | 23-5 |

## PART 3

**VPN の設定**

## CHAPTER 24

|                             |      |
|-----------------------------|------|
| <b>IPSec と ISAKMP の設定</b>   | 24-1 |
| トンネリングの概要                   | 24-1 |
| IPSec の概要                   | 24-2 |
| ISAKMP の設定                  | 24-3 |
| ISAKMP の概要                  | 24-3 |
| ISAKMP ポリシーの設定              | 24-6 |
| 外部インターフェイスでの ISAKMP のイネーブル化 | 24-7 |



|                                        |       |
|----------------------------------------|-------|
| Aggressive モードでの ISAKMP のディセーブル化       | 24-7  |
| ISAKMP ピアの識別方式の決定                      | 24-8  |
| IPSec over NAT-T のイネーブル化               | 24-8  |
| NAT-T の使用                              | 24-9  |
| IPSec over TCP のイネーブル化                 | 24-9  |
| リブートの前にアクティブ セッションの終了を待機               | 24-10 |
| 接続解除の前にピアに警告する                         | 24-11 |
| 証明書グループ照合の設定                           | 24-12 |
| 証明書グループ照合の規則とポリシーの作成                   | 24-12 |
| tunnel-group-map default-group コマンドの使用 | 24-13 |
| IPSec の設定                              | 24-14 |
| IPSec トンネルの理解                          | 24-14 |
| トランスフォーム セットの概要                        | 24-14 |
| 暗号マップの定義                               | 24-15 |
| インターフェイスへの暗号マップの適用                     | 24-21 |
| インターフェイス アクセスリストの使用                    | 24-22 |
| IPSec SA のライフタイムの変更                    | 24-24 |
| 基本的な IPSec コンフィギュレーションの作成              | 24-24 |
| ダイナミック暗号マップの使用                         | 24-26 |
| サイトツーサイト冗長性の定義                         | 24-29 |
| IPSec コンフィギュレーションの表示                   | 24-29 |
| セキュリティ アソシエーションのクリア                    | 24-30 |
| 暗号マップ コンフィギュレーションのクリア                  | 24-30 |

## CHAPTER 25

|                                                 |       |
|-------------------------------------------------|-------|
| <b>IPSec VPN の一般パラメータの設定</b>                    | 25-1  |
| 単一のルーテッド モードでの VPN の設定                          | 25-1  |
| ACL をバイパスするための IPSec の設定                        | 25-2  |
| インターフェイス内トラフィックの許可                              | 25-3  |
| インターフェイス内トラフィックにおける NAT の注意事項                   | 25-4  |
| アクティブな IPSec VPN セッションの最大数の設定                   | 25-4  |
| 許可されるクライアント リビジョン レベル確認のためのクライアント アップ<br>デートの使用 | 25-5  |
| ロードバランシングの概要                                    | 25-8  |
| ロードバランシングの実装                                    | 25-9  |
| 前提条件                                            | 25-9  |
| 適格なプラットフォーム                                     | 25-9  |
| 適格なクライアント                                       | 25-9  |
| VPN ロードバランシング クラスタ コンフィギュレーション                  | 25-10 |
| 一部の一般的な混在クラスタのシナリオ                              | 25-10 |

|                                       |       |
|---------------------------------------|-------|
| シナリオ 1: WebVPN 接続のない混在クラスタ            | 25-11 |
| シナリオ 2: WebVPN 接続を処理する混在クラスタ          | 25-11 |
| <b>ロードバランシングの設定</b>                   | 25-12 |
| ロードバランシング用のパブリックおよびプライベート インターフェイスの設定 | 25-12 |
| ロードバランシング クラスタ アトリビュートの設定             | 25-13 |
| VPN セッション制限の設定                        | 25-15 |

## CHAPTER 26

|                                            |       |
|--------------------------------------------|-------|
| <b>トンネルグループ、グループポリシー、およびユーザの設定</b>         | 26-1  |
| トンネルグループ、グループポリシー、およびユーザの概要                | 26-2  |
| トンネルグループ                                   | 26-3  |
| トンネルグループの一般接続パラメータ                         | 26-3  |
| トンネルグループの IPSec 接続パラメータ                    | 26-4  |
| トンネルグループの WebVPN 接続パラメータ                   | 26-5  |
| トンネルグループの設定                                | 26-6  |
| デフォルトの IPSec リモートアクセス トンネルグループのコンフィギュレーション | 26-6  |
| トンネルグループの IPSec 一般パラメータの設定                 | 26-6  |
| IPSec リモートアクセス トンネルグループの設定                 | 26-7  |
| IPSec リモートアクセス トンネルグループの名前とタイプの指定          | 26-7  |
| IPSec リモートアクセス トンネルグループの一般アトリビュートの設定       | 26-7  |
| IPSec リモートアクセス トンネルグループの IPSec アトリビュートの設定  | 26-10 |
| LAN-to-LAN トンネルグループの設定                     | 26-12 |
| デフォルトの LAN-to-LAN トンネルグループのコンフィギュレーション     | 26-12 |
| LAN-to-LAN トンネルグループの名前とタイプの指定              | 26-12 |
| LAN-to-LAN トンネルグループの一般アトリビュートの設定           | 26-13 |
| LAN-to-LAN IPSec アトリビュートの設定                | 26-14 |
| WebVPN トンネルグループの設定                         | 26-15 |
| WebVPN トンネルグループの名前とタイプの指定                  | 26-15 |
| WebVPN トンネルグループの一般アトリビュートの設定               | 26-16 |
| WebVPN トンネルグループの WebVPN アトリビュートの設定         | 26-18 |
| WebVPN ユーザ用のログイン ウィンドウのカスタマイズ              | 26-22 |
| グループポリシー                                   | 26-24 |
| デフォルトのグループポリシー                             | 26-24 |
| グループポリシーの設定                                | 26-26 |
| 外部グループポリシーの設定                              | 26-26 |
| 内部グループポリシーの設定                              | 26-27 |

|                              |       |
|------------------------------|-------|
| グループポリシー アトリビュートの設定          | 26-27 |
| WINS サーバおよび DNS サーバの設定       | 26-27 |
| VPN 固有アトリビュートの設定             | 26-28 |
| セキュリティ アトリビュートの設定            | 26-31 |
| バナー メッセージの設定                 | 26-33 |
| IPSec-UDP アトリビュートの設定         | 26-34 |
| スプリット トンネリング アトリビュートの設定      | 26-35 |
| トンネリング用ドメイン アトリビュートの設定       | 26-36 |
| VPN ハードウェア クライアント用アトリビュートの設定 | 26-38 |
| バックアップ サーバ アトリビュートの設定        | 26-41 |
| ファイアウォール ポリシーの設定             | 26-42 |
| クライアント アクセス規則の設定             | 26-45 |
| グループポリシーの WebVPN アトリビュートの設定  | 26-47 |
| ユーザ アトリビュートの設定               | 26-60 |
| ユーザ名のコンフィギュレーションの表示          | 26-60 |
| 特定ユーザのアトリビュートの設定             | 26-61 |
| ユーザのパスワードと特権レベルの設定           | 26-61 |
| ユーザ アトリビュートの設定               | 26-62 |
| VPN ユーザ アトリビュートの設定           | 26-62 |
| 特定ユーザの WebVPN の設定            | 26-66 |

## CHAPTER 27

|                         |      |
|-------------------------|------|
| <b>VPN の IP アドレスの設定</b> | 27-1 |
| IP アドレスの割り当て方式の設定       | 27-2 |
| ローカル IP アドレス プールの設定     | 27-2 |
| AAA アドレッシングの設定          | 27-3 |
| DHCP アドレッシングの設定         | 27-4 |

## CHAPTER 28

|                                            |      |
|--------------------------------------------|------|
| <b>リモートアクセス IPSec VPN の設定</b>              | 28-1 |
| コンフィギュレーションのまとめ                            | 28-2 |
| インターフェイスの設定                                | 28-3 |
| ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化 | 28-4 |
| アドレス プールの設定                                | 28-5 |
| ユーザの追加                                     | 28-6 |
| トランスフォーム セットの作成                            | 28-6 |
| トンネルグループの定義                                | 28-7 |
| ダイナミック暗号マップの作成                             | 28-8 |
| ダイナミック暗号マップを使用するための暗号マップ エントリの作成           | 28-9 |

## CHAPTER 29

**LAN-to-LAN IPSec VPN の設定** 29-1

**コンフィギュレーションのまとめ** 29-1

**インターフェイスの設定** 29-2

**ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化** 29-3

**トランスフォーム セットの作成** 29-5

**ACL の設定** 29-6

**トンネルグループの定義** 29-7

**暗号マップの作成とインターフェイスへの適用** 29-8

**暗号マップのインターフェイスへの適用** 29-9

## CHAPTER 30

**WebVPN の設定** 30-1

**WebVPN の準備** 30-2

**WebVPN セキュリティ対策の順守** 30-2

**WebVPN でサポートされていない機能の概要** 30-3

**中央サイトにアクセスするための SSL の使用** 30-3

**WebVPN セッションでの HTTPS の使用** 30-3

**同一インターフェイス上での WebVPN と ASDM の設定** 30-4

**WebVPN HTTP/HTTPS プロキシの設定** 30-4

**SSL/TLS 暗号化プロトコルの設定** 30-4

**デジタル証明書による認証** 30-5

**Web VPN 用にブラウザのクッキーをイネーブルにする** 30-5

**パスワードの管理** 30-5

**WebVPN でのシングル サインオンの使用** 30-6

**HTTP Basic 認証または NTLM 認証による SSO の設定** 30-6

**SiteMinder による SSO 認証の設定** 30-7

**HTTP Form プロトコルを使用した SSO の設定** 30-10

**デジタル証明書による認証** 30-16

**WebVPN ポリシーの作成と適用** 30-17

**グローバル コンフィギュレーション モードでのポート転送、URL、およびアクセスリストの作成** 30-17

**グループポリシー モードまたはユーザ モードでのグループポリシーとユーザへのリストの割り当て** 30-17

**グループポリシーとユーザ用の機能のイネーブル化** 30-17

**グループポリシーへのユーザの割り当て** 30-17

**セキュリティ アプライアンス認証サーバを使用する** 30-17

**RADIUS サーバを使用する** 30-18

**WebVPN トンネルグループ アトリビュートの定義** 30-19

**WebVPN グループポリシーとユーザ アトリビュートの設定** 30-20

|                                               |       |
|-----------------------------------------------|-------|
| Application Access の設定                        | 30-21 |
| ポート転送アプレットの自動ダウンロード                           | 30-21 |
| hosts ファイル エラーを回避するための Application Access の終了 | 30-21 |
| Application Access 使用時の hosts ファイル エラーの回復     | 30-21 |
| hosts ファイルの概要                                 | 30-22 |
| 不正な Application Access の終了                    | 30-22 |
| hosts ファイルの再設定                                | 30-22 |
| ファイル アクセスの設定                                  | 30-25 |
| Citrix MetaFrame サービスへのアクセスの設定                | 30-28 |
| PDA での WebVPN の使用                             | 30-29 |
| WebVPN を介した電子メールの使用                           | 30-30 |
| 電子メール プロキシの設定                                 | 30-30 |
| 電子メールプロキシの証明書認証                               | 30-31 |
| MAPI の設定                                      | 30-31 |
| Web 電子メール MS Outlook Web Access の設定           | 30-31 |
| WebVPN のパフォーマンスの最適化                           | 30-32 |
| キャッシングの設定                                     | 30-32 |
| コンテンツの変換の設定                                   | 30-32 |
| コンテンツのリライトのディセーブル化                            | 30-33 |
| プロキシのバイパスの使用                                  | 30-33 |
| アプリケーション プロファイル カスタマイゼーション フレームワークの設定         | 30-34 |
| APCF シンタックス                                   | 30-34 |
| APCF の例                                       | 30-36 |
| WebVPN エンド ユーザ設定の概要                           | 30-36 |
| エンド ユーザ インターフェイスの定義                           | 30-36 |
| WebVPN ホームページの表示                              | 30-37 |
| WebVPN Application Access パネルの表示              | 30-38 |
| フローティング ツールバーの表示                              | 30-38 |
| WebVPN ページのカスタマイズ                             | 30-39 |
| Cascading Style Sheet パラメータの使用                | 30-39 |
| WebVPN Login ページのカスタマイズ                       | 30-40 |
| WebVPN Logout ページのカスタマイズ                      | 30-42 |
| WebVPN ホームページのカスタマイズ                          | 30-43 |
| Application Access ウィンドウのカスタマイズ               | 30-45 |
| プロンプト ダイアログのカスタマイズ                            | 30-46 |
| トンネルグループ、グループ、およびユーザへのカスタマイゼーションの適用           | 30-47 |
| ユーザ名とパスワードの要求                                 | 30-48 |

|                               |       |
|-------------------------------|-------|
| セキュリティのヒントの通知                 | 30-49 |
| WebVPN 機能を使用するためのリモート システムの設定 | 30-49 |
| WebVPN データのキャプチャ              | 30-55 |
| キャプチャ ファイルの作成                 | 30-55 |
| キャプチャ データを表示するためのブラウザの使用      | 30-56 |

## CHAPTER 31

|                          |       |
|--------------------------|-------|
| <b>SSL VPN クライアントの設定</b> | 31-1  |
| SVC のインストール              | 31-2  |
| プラットフォームの要件              | 31-2  |
| SVC ソフトウェアのインストール        | 31-2  |
| SVC のイネーブル化              | 31-4  |
| 相手先固定 SVC のインストールのイネーブル化 | 31-6  |
| キーの再生成のイネーブル化            | 31-6  |
| デッド ピア検知のイネーブル化と調整       | 31-7  |
| キーペアライブのイネーブル化           | 31-8  |
| SVC 圧縮の使用                | 31-9  |
| SVC セッションの表示             | 31-10 |
| SVC セッションのログオフ           | 31-11 |
| SVC のアップデート              | 31-12 |

## CHAPTER 32

|                       |       |
|-----------------------|-------|
| <b>証明書の設定</b>         | 32-1  |
| 公開キー暗号化               | 32-2  |
| 公開キー暗号化について           | 32-2  |
| 証明書のスケーラビリティ          | 32-2  |
| キー ペアについて             | 32-3  |
| トラストポイントについて          | 32-3  |
| CRL について              | 32-4  |
| サポート対象の CA サーバ        | 32-4  |
| <b>証明書の設定</b>         | 32-5  |
| 証明書の準備                | 32-5  |
| キー ペアの設定              | 32-5  |
| キー ペアの生成              | 32-6  |
| キー ペアの削除              | 32-7  |
| トラストポイントの設定           | 32-7  |
| 証明書の取得                | 32-9  |
| SCEP を使用した証明書の取得      | 32-9  |
| 手動での証明書の取得            | 32-11 |
| トラストポイントの CRL の設定     | 32-13 |
| トラストポイントのエクスポートとインポート | 32-15 |

|                             |       |
|-----------------------------|-------|
| トラストポイント コンフィギュレーションのエクスポート | 32-15 |
| トラストポイント コンフィギュレーションのインポート  | 32-16 |
| CA 証明書マップ規則の設定              | 32-16 |

## PART 4

## システム管理

## CHAPTER 33

|                            |       |
|----------------------------|-------|
| <b>システム アクセスの管理</b>        | 33-1  |
| Telnet アクセスの許可             | 33-2  |
| SSH アクセスの許可                | 33-3  |
| SSH アクセスの設定                | 33-3  |
| SSH クライアントの使用              | 33-4  |
| ログイン パスワードの変更              | 33-4  |
| ASDM の HTTPS アクセスの許可       | 33-5  |
| システム管理者の AAA               | 33-6  |
| CLI アクセスの認証の設定             | 33-6  |
| 特権 EXEC モードにアクセスするための認証の設定 | 33-7  |
| enable コマンドの認証の設定          | 33-7  |
| login コマンドによるユーザの認証        | 33-8  |
| コマンド認可の設定                  | 33-8  |
| コマンド認可の概要                  | 33-9  |
| ローカル コマンド認可の設定             | 33-9  |
| TACACS+ コマンド認可の設定          | 33-12 |
| コマンド アカウンティングの設定           | 33-16 |
| 現在のログイン ユーザの表示             | 33-17 |
| ロックアウトからの回復                | 33-17 |
| ログイン バナーの設定                | 33-19 |

## CHAPTER 34

## ソフトウェア、ライセンス、およびコンフィギュレーションの管理 34-1

|                                                  |      |
|--------------------------------------------------|------|
| ライセンスの管理                                         | 34-2 |
| アクティベーション キーの取得                                  | 34-2 |
| 新しいアクティベーション キーの入力                               | 34-2 |
| フラッシュ メモリ内のファイルの表示                               | 34-3 |
| フラッシュ メモリへのソフトウェアまたはコンフィギュレーションのダウンロード           | 34-4 |
| 特定の場所へのファイルのダウンロード                               | 34-4 |
| スタートアップ コンフィギュレーションまたは実行コンフィギュレーションへのファイルのダウンロード | 34-5 |
| ブートするアプリケーション イメージと ASDM イメージの設定                 | 34-6 |
| スタートアップ コンフィギュレーションとしてブートするファイルの設定               | 34-7 |

|                                                         |       |
|---------------------------------------------------------|-------|
| フェールオーバー ペアのゼロ ダウンタイム アップグレードの実行                        | 34-8  |
| Active/Standby フェールオーバー コンフィギュレーションのアップグレード             | 34-8  |
| Active/Active フェールオーバー コンフィギュレーションのアップグレード              | 34-9  |
| コンフィギュレーション ファイルのバックアップ                                 | 34-11 |
| 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のシステム<br>コンフィギュレーションのバックアップ | 34-11 |
| コンテキスト コンフィギュレーションのフラッシュ メモリへのバック<br>アップ                | 34-11 |
| コンテキスト内でのコンテキスト コンフィギュレーションのバックアッ<br>プ                  | 34-12 |
| 端末の表示からのコンフィギュレーションのコピー                                 | 34-12 |
| Auto Update サポートの設定                                     | 34-13 |
| Auto Update Server との通信の設定                              | 34-13 |
| Auto Update ステータスの表示                                    | 34-14 |

## CHAPTER 35

|                              |             |
|------------------------------|-------------|
| <b>セキュリティ アプライアンスのモニタリング</b> | <b>35-1</b> |
| システム ログ メッセージの使用             | 35-1        |
| SNMP の使用方法                   | 35-1        |
| SNMP の概要                     | 35-1        |
| SNMP のイネーブル化                 | 35-3        |

## CHAPTER 36

|                                               |             |
|-----------------------------------------------|-------------|
| <b>セキュリティ アプライアンスのトラブルシューティング</b>             | <b>36-1</b> |
| コンフィギュレーションのテスト                               | 36-2        |
| ICMP デバッグ メッセージとシステム メッセージのイネーブル化             | 36-2        |
| セキュリティ アプライアンス インターフェイスの ping                 | 36-3        |
| セキュリティ アプライアンスによる ping                        | 36-5        |
| テスト コンフィギュレーションのディセーブル化                       | 36-6        |
| セキュリティ アプライアンスのリロード                           | 36-7        |
| パスワード回復の実行                                    | 36-8        |
| ASA 5500 シリーズ適応型セキュリティ アプライアンスのパスワード回復の<br>実行 | 36-8        |
| PIX 500 シリーズ セキュリティ アプライアンスのパスワード回復           | 36-9        |
| パスワード回復のディセーブル化                               | 36-11       |
| その他のトラブルシューティング ツール                           | 36-12       |
| デバッグ メッセージの表示                                 | 36-12       |
| パケットの取得                                       | 36-12       |
| クラッシュ ダンプの表示                                  | 36-12       |
| 一般的な問題                                        | 36-13       |



## PART 5

## 参考資料

## APPENDIX A

## 機能のライセンスと仕様 A-1

|                            |     |
|----------------------------|-----|
| サポートされているプラットフォーム          | A-1 |
| プラットフォームの機能のライセンス          | A-2 |
| セキュリティ サービス モジュール サポート     | A-6 |
| VPN 仕様                     | A-7 |
| Cisco VPN クライアント サポート      | A-7 |
| Cisco Secure Desktop のサポート | A-7 |
| サイトツーサイト VPN 互換性           | A-7 |
| 暗号化標準                      | A-8 |

## APPENDIX B

## 設定例 B-1

|                                       |      |
|---------------------------------------|------|
| 例 1：外部アクセスのあるマルチモード ファイアウォール          | B-2  |
| 例 1：システム コンフィギュレーション                  | B-3  |
| 例 1：管理コンテキスト コンフィギュレーション              | B-4  |
| 例 1：顧客 A コンテキスト コンフィギュレーション           | B-4  |
| 例 1：顧客 B コンテキスト コンフィギュレーション           | B-5  |
| 例 1：顧客 C コンテキスト コンフィギュレーション           | B-5  |
| 例 2：同じセキュリティ レベルを使用したシングルモード ファイアウォール | B-6  |
| 例 3：マルチコンテキストの共有リソース                  | B-8  |
| 例 3：システム コンフィギュレーション                  | B-9  |
| 例 3：管理コンテキスト コンフィギュレーション              | B-10 |
| 例 3：部門 1 コンテキスト コンフィギュレーション           | B-11 |
| 例 3：部門 2 コンテキスト コンフィギュレーション           | B-12 |
| 例 4：外部アクセスのあるマルチモード、透過ファイアウォール        | B-13 |
| 例 4：システム コンフィギュレーション                  | B-14 |
| 例 4：管理コンテキスト コンフィギュレーション              | B-15 |
| 例 4：顧客 A コンテキスト コンフィギュレーション           | B-15 |
| 例 4：顧客 B コンテキスト コンフィギュレーション           | B-15 |
| 例 4：顧客 C コンテキスト コンフィギュレーション           | B-16 |
| 例 5：WebVPN コンフィギュレーション                | B-17 |

## APPENDIX C

## コマンドライン インターフェイスの使用 C-1

|                                |     |
|--------------------------------|-----|
| ファイアウォール モードとセキュリティ コンテキスト モード | C-2 |
| コマンドのモードとプロンプト                 | C-3 |
| シンタックスの書式                      | C-4 |
| コマンドの省略形                       | C-4 |

|                             |     |
|-----------------------------|-----|
| コマンドラインの編集                  | C-4 |
| コマンドの完成                     | C-5 |
| コマンドのヘルプ                    | C-5 |
| show コマンド出力のフィルタリング         | C-6 |
| コマンド出力のページング                | C-7 |
| コメントの追加                     | C-7 |
| テキスト コンフィギュレーション ファイル       | C-8 |
| テキスト ファイルでコマンドと行が対応する仕組み    | C-8 |
| コマンド固有のコンフィギュレーション モード コマンド | C-8 |
| 自動テキスト入力                    | C-8 |
| 行の順序                        | C-9 |
| 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-9 |
| パスワード                       | C-9 |
| マルチセキュリティ コンテキスト ファイル       | C-9 |

## APPENDIX D

|                          |      |
|--------------------------|------|
| <b>アドレス、プロトコル、およびポート</b> | D-1  |
| IPv4 アドレスとサブネット 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 アドレス形式              | 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 プレフィックス        | D-12 |
| プロトコルとアプリケーション           | D-13 |
| TCP ポートと UDP ポート         | D-14 |
| ローカル ポートとプロトコル           | D-17 |
| ICMP タイプ                 | D-18 |

## APPENDIX E

|                                |     |
|--------------------------------|-----|
| <b>認可および認証用の外部サーバの設定</b>       | E-1 |
| LDAP、RADIUS、またはローカルの認証および認可の選択 | E-2 |
| 権限およびアトリビュートのポリシー実施の概要         | E-3 |
| 外部 LDAP サーバの設定                 | E-4 |

|                                                            |      |
|------------------------------------------------------------|------|
| LDAP ディレクトリ構造の確認と設定の手順                                     | E-4  |
| セキュリティ アプライアンスで使用する LDAP スキーマの構成                           | E-5  |
| 階層の検索                                                      | E-5  |
| セキュリティ アプライアンスと LDAP サーバのバインディング                           | E-6  |
| セキュリティ アプライアンスの LDAP スキーマの定義                               | E-6  |
| Cisco -AV-Pair アトリビュートのシンタックス                              | E-14 |
| セキュリティ アプライアンスの認可スキーマの例                                    | E-16 |
| LDAP サーバへのスキーマのロード                                         | E-18 |
| ユーザ権限の定義                                                   | E-18 |
| ユーザ ファイルの例                                                 | E-19 |
| Active Directory の設定の確認                                    | E-19 |
| 例 1: Microsoft Active Directory を使用した LDAP 認可の設定 (ASA/PIX) | E-19 |
| 例 2: Microsoft Active Directory を使用した LDAP 認可の設定           | E-21 |
| 例 3: Microsoft Active Directory を使用した LDAP 認証および LDAP 認可   | E-24 |
| 外部 RADIUS サーバの設定                                           | E-26 |
| RADIUS 設定の手順の確認                                            | E-26 |
| セキュリティ アプライアンスの RADIUS 認可アトリビュート                           | E-26 |

GLOSSARY

**用語集**

INDEX

**索引**





# このマニュアルについて

---

ここでは、『Cisco セキュリティ アプライアンス コマンド ライン コンフィギュレーション ガイド』の概要を示します。次の項について説明します。

- [マニュアルの目的 \(P.xxx\)](#)
- [技術情報の入手方法 \(P.xxxiv\)](#)
- [テクニカル サポート \(P.xxxv\)](#)
- [その他の資料および情報の入手 \(P.xxxvii\)](#)

## マニュアルの目的

このマニュアルは、コマンドライン インターフェイスを使用してセキュリティ アプライアンスを設定する際に役立ちます。このマニュアルは、すべての機能を網羅しているわけではなく、ごく一般的なコンフィギュレーションの事例を紹介しています。

セキュリティ アプライアンスの設定と監視は、ASDM (Web ベースの GUI アプリケーション) を使用して行うこともできます。ASDM では、コンフィギュレーション ウィザードを使用して、いくつかの一般的なコンフィギュレーションを設定できます。また、あまり一般的ではない事例には、オンラインのヘルプが用意されています。詳細については、

<http://www.cisco.com/univercd/cc/td/doc/product/netsec/secmgmt/asdm/index.htm> を参照してください。

このマニュアルは、Cisco PIX 500 シリーズのセキュリティ アプライアンス (PIX 515E、PIX 525、および PIX 535) と、Cisco ASA 5500 シリーズのセキュリティ アプライアンス (ASA 5510、ASA 5520、および ASA 5540) に利用できます。このマニュアル全体で、「セキュリティ アプライアンス」という用語は、特に指定がない限り、サポートされているすべてのモデルを意味します。PIX 501、PIX 506E、および PIX 520 セキュリティ アプライアンスは、Software Version 7.0 ではサポートされていません。

## 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を対象としています。

- ネットワーク セキュリティの管理
- ファイアウォールとセキュリティ アプライアンスのインストールおよび設定
- VPN の設定
- 侵入検知ソフトウェアの設定

## 関連マニュアル

詳細については、次のマニュアルを参照してください。

- *Cisco PIX Security Appliance Release Notes*
- *Cisco ASDM Release Notes*
- *Cisco PIX 515E Quick Start Guide*
- *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*
- *Migrating to ASA for VPN 3000 Series Concentrator Administrators*
- *Cisco Security Appliance Command Reference*
- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco Security Appliance Logging Configuration and System Log Messages*
- *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*

## マニュアルの構成

このマニュアルは、表 1 に示す章と付録で構成されています。

**表 1      マニュアルの構成**

| 章 / 付録                          | 内容                                                                                                                     |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>Part 1：準備と一般情報</b>           |                                                                                                                        |
| 第 1 章「セキュリティ アプライアンスの概要」        | セキュリティ アプライアンスの概要を示します。                                                                                                |
| 第 2 章「はじめに」                     | コマンドライン インターフェイスへのアクセス方法、ファイアウォール モードの設定方法、およびコンフィギュレーションの処理方法について説明します。                                               |
| 第 3 章「マルチコンテキスト モードのイネーブル化」     | セキュリティ コンテキストの使用方法和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。                                                                  |
| 第 4 章「イーサネットとサブインターフェイスの設定」     | 物理インターフェイスのイーサネットの設定方法、およびサブインターフェイスの追加方法について説明します。                                                                    |
| 第 5 章「セキュリティ コンテキストの追加と管理」      | セキュリティ アプライアンスにマルチセキュリティ コンテキストを設定する方法について説明します。                                                                       |
| 第 6 章「インターフェイス パラメータの設定」        | 各インターフェイスおよびサブインターフェイスの名前、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。                                                            |
| 第 7 章「基本設定」                     | 機能を果たすコンフィギュレーションに通常必要とされる基本設定を行う方法について説明します。                                                                          |
| 第 8 章「IP ルーティングと 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。                                                                                      |
| 第 9 章「IPv6 の設定」                 | IPv6 をイネーブルにする方法および設定する方法について説明します。                                                                                    |
| 第 10 章「AAA サーバとローカル データベースの設定」  | AAA サーバとローカル データベースの設定方法について説明します。                                                                                     |
| 第 11 章「フェールオーバーの設定」             | セキュリティ アプライアンスのフェールオーバー機能について説明します。この機能を使用すると、2つのセキュリティ アプライアンスを設定して、一方の装置が故障した場合に、もう一方の装置が動作を引き継ぐようにできます。             |
| <b>Part 2：ファイアウォールの設定</b>       |                                                                                                                        |
| 第 12 章「ファイアウォール モードの概要」         | セキュリティ アプライアンスの 2つのオペレーション モード（ルーテッド モードと透過モード）、および各モードでのデータの処理方法の違いについて詳細に説明します。                                      |
| 第 13 章「アクセスリストによるトラフィックの指定」     | アクセスリストを使用してトラフィックを指定する方法について説明します。                                                                                    |
| 第 14 章「NAT の適用」                 | アドレス変換の実行方法について説明します。                                                                                                  |
| 第 15 章「ネットワーク アクセスの許可または拒否」     | セキュリティ アプライアンスを経由するネットワーク アクセスを、アクセスリストを使用して制御する方法について説明します。                                                           |
| 第 16 章「ネットワーク アクセスへの AAA の適用」   | ネットワーク アクセスに対して AAA をイネーブルにする方法について説明します。                                                                              |
| 第 17 章「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 リスクを低減したり不適切な使用を防止したりする方法について説明します。                                                        |
| 第 18 章「モジュラ ポリシー フレームワークの使用」    | モジュラ ポリシー フレームワークを使用して、TCP、一般的な接続設定、検査、および QoS に関するセキュリティ ポリシーを作成する方法について説明します。                                        |
| 第 19 章「AIP SSM および CSC SSM の管理」 | セキュリティ アプライアンスを設定してトラフィックを AIP SSM または CSC SSM に送信する方法、SSM のステータスを確認する方法、およびインテリジェント SSM のソフトウェア イメージを更新する方法について説明します。 |

## ■ マニュアルの目的

表1 マニュアルの構成 (続き)

| 章 / 付録                                 | 内容                                                                                                                                                                   |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 第 20 章「ネットワーク攻撃の防止」                    | ネットワーク攻撃を代行受信して対応するように保護機能を設定する方法について説明します。                                                                                                                          |
| 第 21 章「QoS ポリシーの適用」                    | フレーム リレー、Asynchronous Transfer Mode (ATM; 非同期転送モード)、イーサネットと 802.1 ネットワーク、SONET、IP ルーティング型ネットワークなど、多様なテクノロジーを通じて、特定のネットワーク トラフィックに、より良いサービスを提供するネットワークの設定方法について説明します。 |
| 第 22 章「アプリケーション層プロトコル検査の設定」            | アプリケーション検査の使用方法和設定方法について説明します。                                                                                                                                       |
| 第 23 章「ARP 検査およびブリッジングパラメータの設定」        | ARP 検査をイネーブルにする方法と、ブリッジング オペレーションをカスタマイズする方法について説明します。                                                                                                               |
| <b>Part 3：VPN の設定</b>                  |                                                                                                                                                                      |
| 第 24 章「IPSec と ISAKMP の設定」             | ISAKMP と IPSec を設定して、VPN の「トンネル」、つまり、リモート ユーザとプライベートな企業ネットワークとの間のセキュアな接続を構築および管理する方法について説明します。                                                                       |
| 第 25 章「IPSec VPN の一般パラメータの設定」          | さまざまな VPN 設定手順について説明します。                                                                                                                                             |
| 第 26 章「トンネルグループ、グループポリシー、およびユーザの設定」    | VPN のトンネルグループ、グループポリシー、およびユーザの設定方法について説明します。                                                                                                                         |
| 第 27 章「VPN の IP アドレスの設定」               | プライベート ネットワークのアドレッシング方式で IP アドレスを設定する方法について説明します。この方式では、クライアントがトンネルのエンドポイントとして機能します。                                                                                 |
| 第 28 章「リモートアクセス IPSec VPN の設定」         | リモートアクセス VPN 接続の設定方法について説明します。                                                                                                                                       |
| 第 29 章「LAN-to-LAN IPSec VPN の設定」       | LAN-to-LAN VPN 接続の構築方法について説明します。                                                                                                                                     |
| 第 30 章「WebVPN の設定」                     | ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモート アクセス VPN トンネルを確立する方法について説明します。                                                                                                    |
| 第 31 章「SSL VPN クライアントの設定」              | SSL VPN クライアントをインストールし、設定する方法について説明します。                                                                                                                              |
| 第 32 章「証明書の設定」                         | デジタル証明書を設定する方法について説明します。デジタル証明書には、ユーザまたはデバイスを識別する情報が含まれています。このような情報には、名前、シリアル番号、社名、部署、IP アドレスなどがあります。デジタル証明書には、ユーザまたは装置の公開キーのコピーが含まれています。                            |
| <b>Part 4：システム管理</b>                   |                                                                                                                                                                      |
| 第 33 章「システム アクセスの管理」                   | Telnet、SSH、および HTTPS を介してシステム管理のためにセキュリティ アプライアンスにアクセスする方法について説明します。                                                                                                 |
| 第 34 章「ソフトウェア、ライセンス、およびコンフィギュレーションの管理」 | ライセンス キーを入力し、ソフトウェアと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。                                                                                                            |
| 第 35 章「セキュリティ アプライアンスのモニタリング」          | セキュリティ アプライアンスの監視方法について説明します。                                                                                                                                        |
| 第 36 章「セキュリティ アプライアンスのトラブルシューティング」     | セキュリティ アプライアンスのトラブルシューティングの方法について説明します。                                                                                                                              |



表 1 マニュアルの構成（続き）

| 章 / 付録                     | 内容                                           |
|----------------------------|----------------------------------------------|
| Part 5: 参考資料               |                                              |
| 付録 A 「機能のライセンスと仕様」         | 機能のライセンスと仕様について説明します。                        |
| 付録 B 「設定例」                 | セキュリティ アプライアンスを実装するいくつかの一般的な方法について説明します。     |
| 付録 C 「コマンドライン インターフェイスの使用」 | CLI を使用してセキュリティ アプライアンスを設定する方法について説明します。     |
| 付録 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、およびアプリケーションのクイック リファレンスを提供します。 |
| 付録 E 「認可および認証用の外部サーバの設定」   | LDAP および RADIUS 認可サーバの設定について説明します。           |

## 表記法

コマンドの説明では、次の表記法を使用しています。

- 選択する必要があるものは、波カッコ（{ }）で囲んで示しています。
- オプションの要素は、角カッコ（[ ]）で囲んで示しています。
- どちらか選択する必要がある要素は、縦棒（|）で区切って示しています。
- 記載されているとおりに入力するコマンドおよびキーワードは、**太字**で示しています。
- ユーザが値を指定する引数は、*イタリック体*で示しています。

例では、次の表記法を使用しています。

- 画面に表示される情報およびコマンドラインは、`screen` フォントで示しています。
- ユーザが入力する情報は、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。



**(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。

## 技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、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

次の URL から、シスコ製品の最新資料を入手することができます。

<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>

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

<http://www.cisco.com/jp>

### マニュアルの発注方法（英語版）

英文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\\_inpc/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpc/pdi.htm)

シスコ製品の英文マニュアルは、次の方法で発注できます。

- Cisco.com 登録ユーザ（Cisco Direct Customers）の場合、Ordering ツールからシスコ製品の英文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/index.shtml>

- 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。

### シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

<http://www2.hipri.com/cisco/>

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

<http://www2.hipri.com/cisco/>

なお、技術内容に関するお問い合わせは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合わせください。

## テクニカル サポート

シスコと正式なサービス契約を交わしているすべてのお客様、パートナー、および代理店は、Cisco Technical Support で 24 時間テクニカル サポートを利用することができます。Cisco.com の Cisco Technical Support Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、Cisco Technical Assistance Center (TAC) のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店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、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間 365 日、いつでも利用可能です。URL は次のとおりです。

<http://www.cisco.com/techsupport>

Cisco Technical Support Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID または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://tools.cisco.com/RPF/register/register.do>



(注)

Web または電話でサービス リクエストを発行する前に、Cisco Product Identification (CPI) ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

### 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>

## サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、Cisco TAC のエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

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

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合わせください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、Cisco TAC のエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

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

## サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1 (S1)：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2 (S2)：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3 (S3)：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4 (S4)：シスコ製品の機能、インストレーション、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な場合。業務の運用には、ほとんど影響がありません。

## その他の資料および情報の入手

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できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

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

- 『Cisco Product Catalog』には、シスコシステムズが提供するネットワーキング製品のほか、発注方法やカスタマー サポート サービスについての情報が記載されています。『Cisco Product Catalog』には、次の URL からアクセスしてください。

<http://cisco.com/univercd/cc/td/doc/pcat/>

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。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技術者向けの雑誌で、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ために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンラインサービスへのリンクの内容が含まれます。『Packet』には、次の URL からアクセスしてください。

<http://www.cisco.com/packet>

日本語版『Packet』は、米国版『Packet』と日本版のオリジナル記事で構成されています。日本語版『Packet』には、次の URL からアクセスしてください。

<http://www.cisco.com/japanese/warp/public/3/jp/news/packet/>

- 『iQ Magazine』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、事例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『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>

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。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>





## PART 1

### 準備と一般情報









# セキュリティ アプライアンスの概要

セキュリティ アプライアンスは、高度なステートフル ファイアウォールと VPN コンセントレータの機能を 1 つの装置に組み合わせたもので、一部のモデルでは、AIP SSM と呼ばれる総合的な侵入防御モジュールが組み込まれています。セキュリティ アプライアンスの多数の高度な機能には、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）ファイアウォール動作またはルーテッド（レイヤ 3）ファイアウォール動作、高度な検査エンジン、IPSec および WebVPN のサポート、その他の機能があります。サポートされているプラットフォームおよび機能については、[付録 A「機能のライセンスと仕様」](#)を参照してください。新機能のリストについては、『Cisco ASA 5500 Series Release Notes』または『Cisco PIX Security Appliance Release Notes』を参照してください。



(注)

Cisco PIX 501 セキュリティ アプライアンスおよび PIX 506E セキュリティ アプライアンスは、ソフトウェア バージョン 7.0 ではサポートされていません。

次の事項について説明します。

- [ファイアウォール機能の概要 \(P.1-2\)](#)
- [VPN 機能の概要 \(P.1-6\)](#)
- [侵入防御サービス機能の概要 \(P.1-6\)](#)
- [セキュリティ コンテキストの概要 \(P.1-7\)](#)

## ファイアウォール機能の概要

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

ファイアウォールに接続されているネットワークに言及する場合、*外部ネットワーク*はファイアウォールの手前にあるネットワーク、*内部ネットワーク*はファイアウォールの背後にある保護されているネットワーク、そして *DMZ* はファイアウォールの背後にあるが、外部ユーザに制限付のアクセスが許されているネットワークです。セキュリティ アプライアンスを使用すると、数多くのインターフェイスに対してさまざまなセキュリティ ポリシーが設定できます。このインターフェイスには、多数の内部インターフェイス、多数の DMZ、および必要に応じて多数の外部インターフェイスが含まれるため、ここでは、このインターフェイスの区分は一般的な意味で使用するだけです。

ここでは、次の項目について説明します。

- [セキュリティ ポリシーの概要 \(P.1-2\)](#)
- [ファイアウォール モードの概要 \(P.1-4\)](#)
- [ステートフル インスペクションの概要 \(P.1-4\)](#)

## セキュリティ ポリシーの概要

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

- [アクセスリストによるトラフィックの許可または拒否 \(P.1-2\)](#)
- [NAT の適用 \(P.1-3\)](#)
- [スルー トラフィックに対する AAA の使用 \(P.1-3\)](#)
- [HTTP、HTTPS、または FTP フィルタリングの適用 \(P.1-3\)](#)
- [アプリケーション検査の適用 \(P.1-3\)](#)
- [Advanced Inspection and Prevention Security Services Module \(AIP SSM\) へのトラフィック送信 \(P.1-3\)](#)
- [QoS ポリシーの適用 \(P.1-3\)](#)
- [接続の制限と TCP 正規化の適用 \(P.1-4\)](#)

## アクセスリストによるトラフィックの許可または拒否

アクセスリストは、内部から外部へのトラフィックを制限するため、および外部から内部へのトラフィックを許可するために使用することができます。透過ファイアウォール モードでは、非 IP トラフィックを許可するための EtherType アクセスリストも適用できます。

## NAT の適用

NAT の利点のいくつかを次に示します。

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

## スルー トラフィックに対する AAA の使用

HTTP など特定のタイプのトラフィックに対して、認証と認可のいずれかまたは両方を要求することができます。セキュリティ アプライアンスは、RADIUS サーバまたは TACACS+ サーバにアカウント情報を送信することもあります。

## HTTP、HTTPS、または FTP フィルタリングの適用

アクセスリストを使用して、特定の Web サイトまたは FTP サーバへの発信アクセスを禁止できますが、このような方法で Web サイトの使用方法を設定し管理することは、インターネットの規模とダイナミックな特性から、実用的とはいえません。セキュリティ アプライアンスを、次のインターネット フィルタリング製品のいずれかを実行している別のサーバと連携させて使用することを推奨します。

- Websense Enterprise
- N2H2 の Sentian

## アプリケーション検査の適用

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

## Advanced Inspection and Prevention Security Services Module (AIP SSM) へのトラフィック送信

使用しているモデルが侵入防御用の AIP SSM をサポートしている場合、トラフィックを AIP SSM に送信して検査することができます。

## QoS ポリシーの適用

音声やストリーミング ビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。QoS は、この種のトラフィックに優先順位を設定するネットワーク機能です。QoS は、1 つのネットワークの性能を参照して、さまざまな技術を経由するネットワーク トラフィックの選択された一部に優れたサービスを提供します。これは、基盤技術の帯域制限のもとで全体として最善のサービスを提供するためです。

## 接続の制限と TCP 正規化の適用

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

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

## ファイアウォール モードの概要

セキュリティ アプライアンスは、次の 2 つのファイアウォール モードで動作します。

- ルーテッド
- 透過

ルーテッド モードでは、セキュリティ アプライアンスは、ネットワークのルータ ホップと見なされます。

透過モードでは、セキュリティ アプライアンスは「bump-in-the-wire (BITW)」または「ステルス ファイアウォール」のように動作し、ルータ ホップとは見なされません。セキュリティ アプライアンスでは、内部インターフェイスと外部インターフェイスに同じネットワークが接続されます。

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

## ステートフル インспекションの概要

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

しかし、セキュリティ アプライアンスのようなステートフル ファイアウォールは、パケットの次のようなステートについて検討します。

- 新規の接続かどうか。

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

セッション管理パスで行われるタスクは次のとおりです。

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

**(注)**

セッション管理パスおよびファーストパスが「アクセラレーション セキュリティ パス」を構成します。

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

- 確立済みの接続かどうか。

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

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

UDP プロトコルまたは他のコネクションレス型プロトコルに対して、セキュリティ アプライアンスはコネクション ステート情報を作成して、ファースト パスも使用できるようにします。

レイヤ7 検査を必要とするプロトコルに合致するデータ パケットもファースト パスを通過できます。

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

## VPN 機能の概要

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

セキュリティ アプライアンスが実行する機能は次のとおりです。

- トンネルの確立
- トンネル パラメータのネゴシエーション
- ユーザの認証
- ユーザ アドレスの割り当て
- データの暗号化と復号化
- セキュリティ キーの管理
- トンネルを通したデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信データと発信データの転送の管理

セキュリティ アプライアンスは、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

## 侵入防御サービス機能の概要

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは、多数の埋め込みシグニチャ ライブラリに基づいて異常や悪用を探索することでネットワーク トラフィックの監視およびリアルタイム分析を行う侵入防御サービス モジュール AIP SSM をサポートします。システムで不正なアクティビティが検出されると、侵入防御サービス機能は、該当する接続を終了して攻撃元のホストを永続的にブロックし、この事象をログに記録し、さらにアラートを Device Manager に送信します。その他の正規の接続は、中断することなく独立した動作を継続します。詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*』を参照してください。

## セキュリティ コンテキストの概要

1 台のセキュリティ アプライアンスを、セキュリティ コンテキストと呼ばれる複数の仮想装置に分割することができます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立した装置です。マルチコンテキストは、複数のスタンドアロン装置を使用することに似ています。マルチコンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、IPS、管理など、多くの機能がサポートされます。VPN、ダイナミック ルーティング プロトコルなど、いくつかの機能はサポートされません。

マルチコンテキスト モードの場合、セキュリティ アプライアンスには、セキュリティ ポリシー、インターフェイス、およびスタンドアロン装置で設定できるほとんどのオプションを識別するコンテキストごとのコンフィギュレーションが含まれます。システム管理者は、システム コンフィギュレーションに設定することでコンテキストを追加および管理します。このコンフィギュレーションは、シングルモードのコンフィギュレーション同様、スタートアップ コンフィギュレーションです。システム コンフィギュレーションは、セキュリティ アプライアンスの基本設定を識別します。システム コンフィギュレーションには、自分自身のネットワーク インターフェイスまたはネットワーク設定は含まれません。システムがネットワーク リソースにアクセスする必要があるとき（サーバからコンテキストをダウンロードするときなど）は、管理コンテキストとして指定されたコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。



(注)

管理者は、自分のコンテキストすべてをルーテッド モードまたは透過モードで実行することができますが、一部のコンテキストを一方のモードで実行し、他のコンテキストをもう一方のモードで実行することはできません。

マルチコンテキスト モードでは、スタティック ルーティングのみサポートします。







# はじめに

---

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、ファイアウォール モードの設定方法、およびコンフィギュレーションの処理方法について説明します。次の事項について説明します。

- [コマンドライン インターフェイスへのアクセス \(P.2-2\)](#)
- [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 \(P.2-3\)](#)
- [コンフィギュレーションの処理 \(P.2-4\)](#)

## コマンドライン インターフェイスへのアクセス

初期コンフィギュレーションでは、コンソール ポートから直接コマンドライン インターフェイスにアクセスします。その後は、第33章「システム アクセスの管理」の方法によって Telnet または SSH を使用してリモートアクセスを設定することができます。システムがすでにマルチコンテキスト モードで動作している場合は、コンソール ポートにアクセスするとシステムの実行スペースに入ります。マルチコンテキスト モードの詳細については、第3章「マルチコンテキスト モードのイネーブル化」を参照してください。



(注)

コマンドライン インターフェイスの代わりに、ASDM を使用してセキュリティ アプライアンスを設定する場合、デフォルトの管理アドレス 192.168.1.1 に接続することができます（セキュリティ アプライアンスが工場出荷時のデフォルト コンフィギュレーションの状態にある場合）。ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、ASDM に接続するインターフェイスは Management 0/0 です。PIX 500 シリーズ適応型セキュリティ アプライアンスでは、ASDM に接続するインターフェイスは Ethernet 1 です。工場出荷時のデフォルト コンフィギュレーションになっていない場合は、この項の手順でコマンドライン インターフェイスにアクセスします。そこで、**setup** コマンドを入力すると、ASDM にアクセスするための最小限のパラメータが設定できます。

コマンドライン インターフェイスにアクセスするには、次の手順を実行します。

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

コンソール ケーブルの詳細については、セキュリティ アプライアンスに添付されているハードウェア ガイドを参照してください。

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

```
hostname>
```

このプロンプトは、EXEC モードで作業していることを示します。

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

```
hostname> enable
```

次のプロンプトが表示されます。

```
Password:
```

- ステップ 4** プロンプトに対して、イネーブル パスワードを入力します。

デフォルトではパスワードは空白に設定されているため、**Enter** キーを押して先に進みます。イネーブル パスワードの変更については、P.7-1 の「イネーブル パスワードの変更」を参照してください。

プロンプトが次のように変化します。

```
hostname#
```

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

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

```
hostname# configure terminal
```

プロンプトが次のように変化します。

```
hostname(config)#
```

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

## 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

セキュリティ アプライアンスは、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設定できます。

マルチコンテキスト モードでは、すべてのコンテキストで 1 つのファイアウォール モードしか使用できません。モードの設定は、システム実行スペースで行う必要があります。

モードを変更すると、セキュリティ アプライアンスはコンフィギュレーションをクリアします。これは、多くのコマンドが両方のモードでサポートされていないためです。すでに実装済みのコンフィギュレーションがある場合は、モードを変更する前に必ずコンフィギュレーションのバックアップを作成してください。新しくコンフィギュレーションを作成するときにこのバックアップを参照する場合があります。

**firewall transparent** コマンドでモードを変更するセキュリティ アプライアンスにテキスト コンフィギュレーションをダウンロードする場合は、必ずこのコマンドをコンフィギュレーションの最上部に置いてください。このようにすると、セキュリティ アプライアンスは、このコマンドを読み取り次第すぐにモードを変更し、その後は、ダウンロードしたコンフィギュレーションの読み取りを続けます。このコマンドがコンフィギュレーションの後ろの方にあると、セキュリティ アプライアンスはそれ以前に記述されているコンフィギュレーションの行をすべてクリアします。

- 透過モードに設定するには、システム実行スペースで次のコマンドを入力します。

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

このコマンドは、情報提供のためだけに各コンテキスト コンフィギュレーションにも表示されるため、このコマンドをコンテキストに入力することはできません。

- ルーテッド モードに設定するには、システム実行スペースで次のコマンドを入力します。

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

## コンフィギュレーションの処理

この項では、コンフィギュレーションを処理する方法について説明します。セキュリティ アプライアンスは、スタートアップ コンフィギュレーションと呼ばれるコンフィギュレーションをテキスト ファイルからロードします。このファイルは、デフォルトでは隠しファイルとして内部フラッシュ メモリに常駐しています。しかし、ユーザはスタートアップ コンフィギュレーションに異なるパス を指定することができます（詳細については、[第 34 章「ソフトウェア、ライセンス、およびコン フィギュレーションの管理」](#)を参照してください）。

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

この項で説明する内容は、特に指定がない限り、シングルモードとマルチモードの両セキュリティ コンテキストに適用されます。コンテキストの詳細については、[第 3 章「マルチコンテキスト モー ドのイネーブル化」](#)を参照してください。

ここでは、次の項目について説明します。

- [コンフィギュレーション変更の保存 \(P.2-4\)](#)
- [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 \(P.2-4\)](#)
- [コンフィギュレーションの表示 \(P.2-5\)](#)
- [コンフィギュレーション設定のクリアと削除 \(P.2-5\)](#)
- [テキスト コンフィギュレーション ファイルのオフラインでの作成 \(P.2-6\)](#)

## コンフィギュレーション変更の保存

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

```
hostname# write memory
```

マルチコンテキスト モードの場合は、各コンテキスト内でこのコマンドを入力する必要があります。コンテキストのスタートアップ コンフィギュレーションは、外部サーバに置くことができま す。この場合、そのコンフィギュレーションは、コンテキスト URL (HTTP URL および HTTPS URL を除く) に指定されているサーバにセキュリティ アプライアンスによって戻され、保存されるた め、サーバにコンフィギュレーションを保存する必要はありません。



(注)

`copy running-config startup-config` コマンドは、`write memory` コマンドに相当します。

## 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

次のいずれかのオプションを使用して、新規スタートアップ 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。

- 実行コンフィギュレーションでスタートアップ コンフィギュレーションをマージするには、次 のコマンドを入力します。

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

- スタートアップ コンフィギュレーションをロードして実行コンフィギュレーションを廃棄するには、次のコマンドを入力してセキュリティ アプライアンスを再起動します。

```
hostname# reload
```

あるいは、次のコマンドを使用し、リブートを要求せずにスタートアップ コンフィギュレーションをロードして実行コンフィギュレーションを廃棄することができます。

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

## コンフィギュレーションの表示

実行コンフィギュレーションとスタートアップ コンフィギュレーションを表示するには、次のコマンドを使用します。

- 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
```

- 特定の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
```

## コンフィギュレーション設定のクリアと削除

設定を消去するには、次のいずれかのコマンドを入力します。

- 指定したコマンドのコンフィギュレーションすべてをクリアするには、次のコマンドを入力します。

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

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

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

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

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

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

- ある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* で特定されるコンフィギュレーションを削除します。

たとえば、特定の **nat** コマンドを削除するには、次のように、それを一意に識別するのに十分な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消去するには、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消去するには、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を削除し、実行中のコンフィギュレーションを停止することにもなります。

## テキスト コンフィギュレーション ファイルのオフラインでの作成

このマニュアルは、セキュリティ アプライアンスを設定するための CLI の使用方法について説明しています。コマンドを保存すると、変更内容はテキスト ファイルに書き込まれます。一方、CLI を使用する代わりに、テキスト ファイルを PC で直接編集して、コンフィギュレーション モードのコマンドライン プロンプトから、コンフィギュレーションを全部または1行ずつペーストすることができます。あるいは、テキスト ファイルをセキュリティ アプライアンスの内部フラッシュ メモリにダウンロードすることもできます。コンフィギュレーション ファイルをセキュリティ アプライアンスにダウンロードする方法の詳細については、[第 34 章「ソフトウェア、ライセンス、およびコンフィギュレーションの管理」](#)を参照してください。

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

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

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

```
context a
```

テキスト コンフィギュレーション ファイルのフォーマットの詳細については、[付録 C「コマンドライン インターフェイスの使用」](#)を参照してください。



# マルチコンテキスト モードのイネーブル化

---

この章では、セキュリティ コンテキストの使用方法と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。次の事項について説明します。

- [セキュリティ コンテキストの概要 \(P.3-2\)](#)
- [マルチコンテキスト モードのイネーブル化とディセーブル化 \(P.3-10\)](#)

## セキュリティ コンテキストの概要

1 台のセキュリティ アプライアンスを、セキュリティ コンテキストと呼ばれる複数の仮想装置に分割することができます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立した装置です。マルチコンテキストは、複数のスタンドアロン装置を使用することに似ています。マルチコンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、IPS、管理など、多くの機能がサポートされます。VPN、ダイナミック ルーティング プロトコルなど、いくつかの機能はサポートされません。

マルチコンテキスト モードの場合、セキュリティ アプライアンスには、セキュリティ ポリシー、インターフェイス、およびスタンドアロン装置で設定できるほとんどのオプションを識別するコンテキストごとのコンフィギュレーションが含まれます。システム管理者は、システム コンフィギュレーションに設定することでコンテキストを追加および管理します。このコンフィギュレーションは、シングルモードのコンフィギュレーション同様、スタートアップ コンフィギュレーションです。システム コンフィギュレーションは、セキュリティ アプライアンスの基本設定を識別します。システム コンフィギュレーションには、自分自身のネットワーク インターフェイスまたはネットワーク設定は含まれません。システムがネットワーク リソースにアクセスする必要があるとき（サーバからコンテキストをダウンロードするときなど）は、管理コンテキストとして指定されたコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。

この項では、セキュリティ コンテキストの概要について説明します。次の項目を取り上げます。

- [セキュリティ コンテキストの一般的な使用方法 \(P.3-2\)](#)
- [サポートされていない機能 \(P.3-2\)](#)
- [コンテキスト コンフィギュレーション ファイル \(P.3-3\)](#)
- [セキュリティ アプライアンスによるパケットの分類方法 \(P.3-3\)](#)
- [コンテキスト間でのインターフェイス共有 \(P.3-7\)](#)
- [マルチコンテキスト モードでのセキュリティ アプライアンスへのログイン \(P.3-9\)](#)

## セキュリティ コンテキストの一般的な使用方法

マルチセキュリティ コンテキストを使用する状況には次のようなものがあります。

- サービス プロバイダーとして、多数の顧客にセキュリティ サービスを販売する。セキュリティ アプライアンス上でマルチセキュリティ コンテキストをイネーブルにすることによって、費用対効果の高い、省スペース ソリューションを実装できます。このソリューションでは、顧客のトラフィックすべての分離とセキュリティが確保され、設定も容易です。
- 大企業または広大な大学の構内で、各部門の完全な独立を維持する必要がある。
- 企業で、部門ごとに個別のセキュリティ ポリシーの提供が求められている。
- 複数のセキュリティ アプライアンスが必要なネットワークを使用している。

## サポートされていない機能

マルチコンテキスト モードでサポートされていない機能は、次のとおりです。

- ダイナミック ルーティング プロトコル

セキュリティ コンテキストは、スタティック ルートのみサポートします。マルチコンテキスト モードでは、OSPF または RIP をイネーブルにできません。



- VPN
- 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

各コンテキストには、独自のコンフィギュレーション ファイルがあり、セキュリティ ポリシーおよびインターフェイスを識別し、サポートされている機能に対しては、スタンドアロン装置で設定できるオプションすべてを識別します。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または外部フラッシュ メモリ カードに保存することも、TFTP サーバ、FTP サーバ、または HTTP (S) サーバからダウンロードすることもできます。

個々のセキュリティ コンテキストに加えて、セキュリティ アプライアンスには、コンテキストのリストなどセキュリティ アプライアンスの基本設定を識別するシステム コンフィギュレーション ファイルも含まれています。シングルモード コンフィギュレーション同様、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駐しています。

システム コンフィギュレーションには、自分自身のネットワーク インターフェイスまたはネットワーク設定は含まれません。システムがネットワーク リソースにアクセスする必要があるとき（サーバからコンテキストをダウンロードするときなど）は、管理コンテキストとして指定されたコンテキストのいずれかを使用します。システム コンフィギュレーションに含まれているものに、フェールオーバー トラフィック専用の特殊なフェールオーバー インターフェイスがあります。システムがすでにマルチコンテキスト モードになっている場合、またはシングルモードから変換された場合、管理コンテキストが `admin.cfg` と呼ばれるファイルとして内部フラッシュ メモリに自動的に作成されます。このコンテキストは「admin」と名付けられます。`admin.cfg` を管理コンテキストとして使用しない場合は、管理コンテキストを変更できます。

## セキュリティ アプライアンスによるパケットの分類方法

セキュリティ アプライアンスに入ってくるパケットはいずれも分類する必要があります。その結果、セキュリティ アプライアンスは、どのコンテキストにパケットを送信するかを決定できます。分類子は、次のルールに従ってパケットをコンテキストに割り当てます。

1. 入力インターフェイスに関連付けられているコンテキストが1つだけの場合、セキュリティ アプライアンスはパケットをそのコンテキストに分類します。

透過ファイアウォール モードでは、各コンテキストに固有のインターフェイスが必要なため、この方法は、常にパケット分類の目的で使用されます。

2. マルチコンテキスト モードが入力インターフェイスに関連付けられている場合は、セキュリティ アプライアンスは、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してパケットをコンテキストに分類します。

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

分類子は、管理トラフィックなど、1つのインターフェイス宛てのトラフィックに対するインターフェイス IP アドレスを検査します。

- b. スタティック NAT 文 (`static` コマンド) のグローバル アドレス

分類子は、グローバル インターフェイスとパケットの入力インターフェイスが一致する場合に限り、`static` コマンドを検査します。

- c. グローバル NAT プール アドレス (`global` コマンド)

分類子は、入力インターフェイスに対してグローバル プールで識別された IP アドレスを検査します。



(注)

分類子は、分類の目的では NAT 免除コンフィギュレーションは使用しません。これは、NAT 免除がグローバル インターフェイスを識別しないためです。

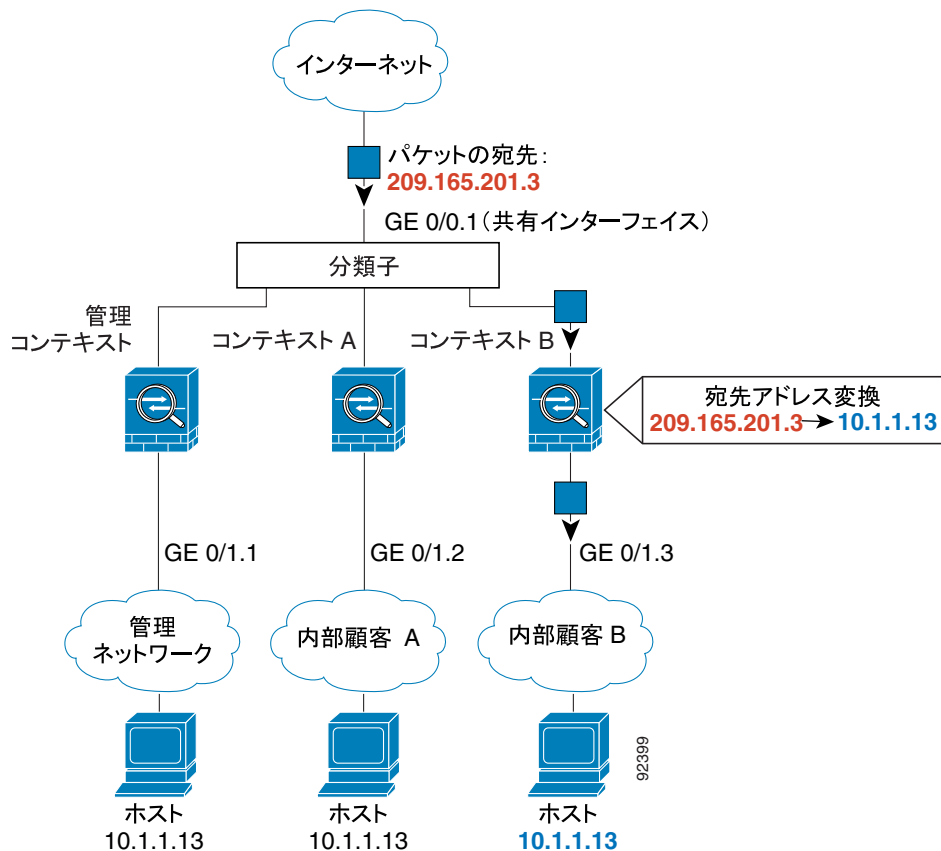
パケットは、上記の方法のいずれか 1 つに基づいてコンテキストに分類される必要があります。たとえば、あるサブネットへのネクストホップとして外部ルータをポイントするスタティック ルートがコンテキストに含まれていて、同じサブネットに対する **static** コマンドが別のコンテキストに含まれている場合、分類子は、そのサブネットを宛先とするパケットを **static** コマンドを使用して分類し、スタティック ルートを無視します。

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、分類子は入力インターフェイスに基づいてパケットとコンテキストを関連付けます。しかし、コンテキスト全体で 1 つのインターフェイスを共有する場合は、分類子は宛先アドレスを使用します。

宛先アドレスの分類では、(トラフィックを通すために) NAT が必要です。したがって、NAT を使用しない場合は、各コンテキストで固有のインターフェイスを使用してください。あるいは、コンテキストに実際のアドレスを指定する **global** コマンドを入力インターフェイスに追加します。この場合、照合を行う **nat** コマンドを分類目的で使用する必要はありません。

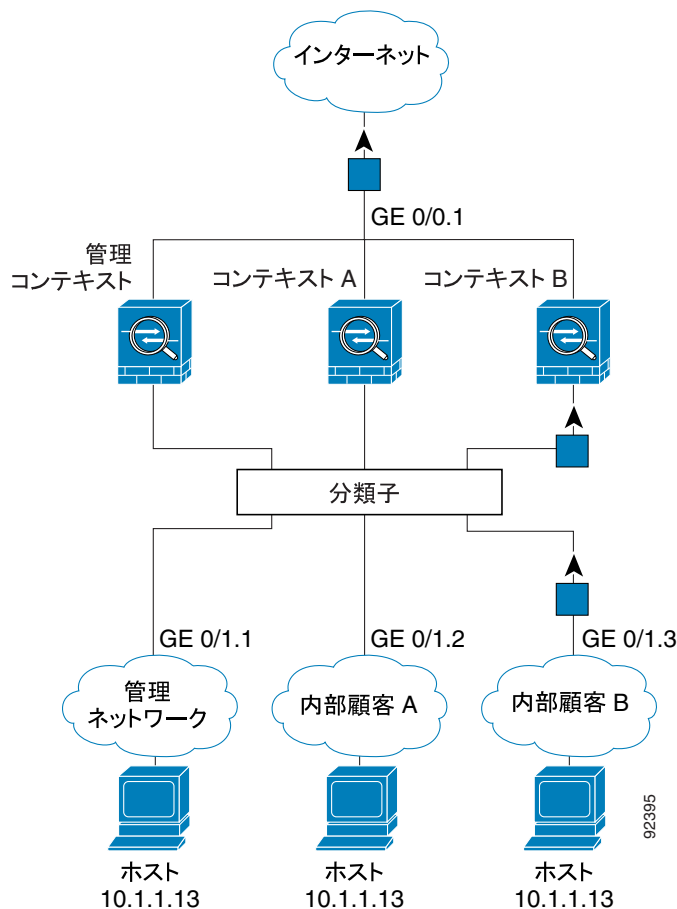
図 3-1 に、外部インターフェイスを共有する一方で、固有の内部インターフェイスを持ち、IP アドレスの重複が許容されているマルチコンテキストを示します。コンテキスト B には宛先アドレスに一致するアドレス変換が含まれるため、分類子はパケットをコンテキスト B に割り当てます。

図 3-1 共有インターフェイスを持つパケット分類



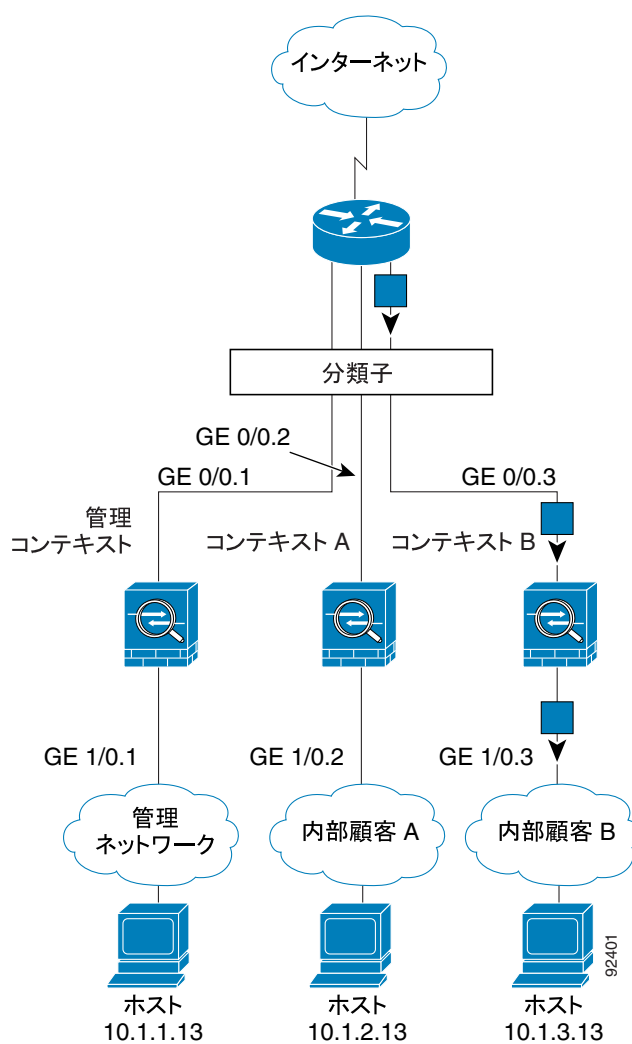
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。図 3-2 に、内部ネットワークのコンテキスト B 上のホストがインターネットにアクセスしている場合を示します。分類子は、パケットをコンテキスト B に割り当てます。これは、入力インターフェイスがギガビット イーサネット 0/1.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 3-2 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では、固有のインターフェイスを使用する必要があります。分類子にとって、透過モードで NAT のサポートがない場合、固有のインターフェイスが唯一の分類の手段になります。図 3-3 に、内部ネットワークのコンテキスト B 上のホストがインターネットにアクセスしている場合を示します。分類子は、パケットをコンテキスト B に割り当てます。これは、入力インターフェイスがギガビット イーサネット 1/0.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 3-3 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共有

### ルーテッド モードのみ

セキュリティ アプライアンスでは、コンテキスト間でインターフェイスを共有することができます。たとえば、インターフェイスを節約するために外部インターフェイスを共有する場合があります。また、コンテキスト間でリソースを共有するために内部インターフェイスを共有することもできます。

ここでは、次の項目について説明します。

- [インターフェイス共有のためのガイドライン \(P.3-7\)](#)
- [セキュリティ コンテキストのカスケード接続 \(P.3-8\)](#)

## インターフェイス共有のためのガイドライン

共有インターフェイスからのトラフィックにセキュリティ アプライアンスを通過するのを許可する場合、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。これは、分類子がアドレス変換コンフィギュレーションに基づいてコンテキスト内のパケットを分類するためです。NAT を実行しない場合でも、共有インターフェイスに **global** コマンドを指定すると、パケットを確実にコンテキストに分類できます。これは、**global** コマンドで実宛先アドレスが指定されるので、照合を行う **nat** コマンドが不要になるためです（インターフェイスを共有し、管理トラフィックに対してのみそのインターフェイスとの行き来を許可する場合、分類子はそのインターフェイスの 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には加わりません）。

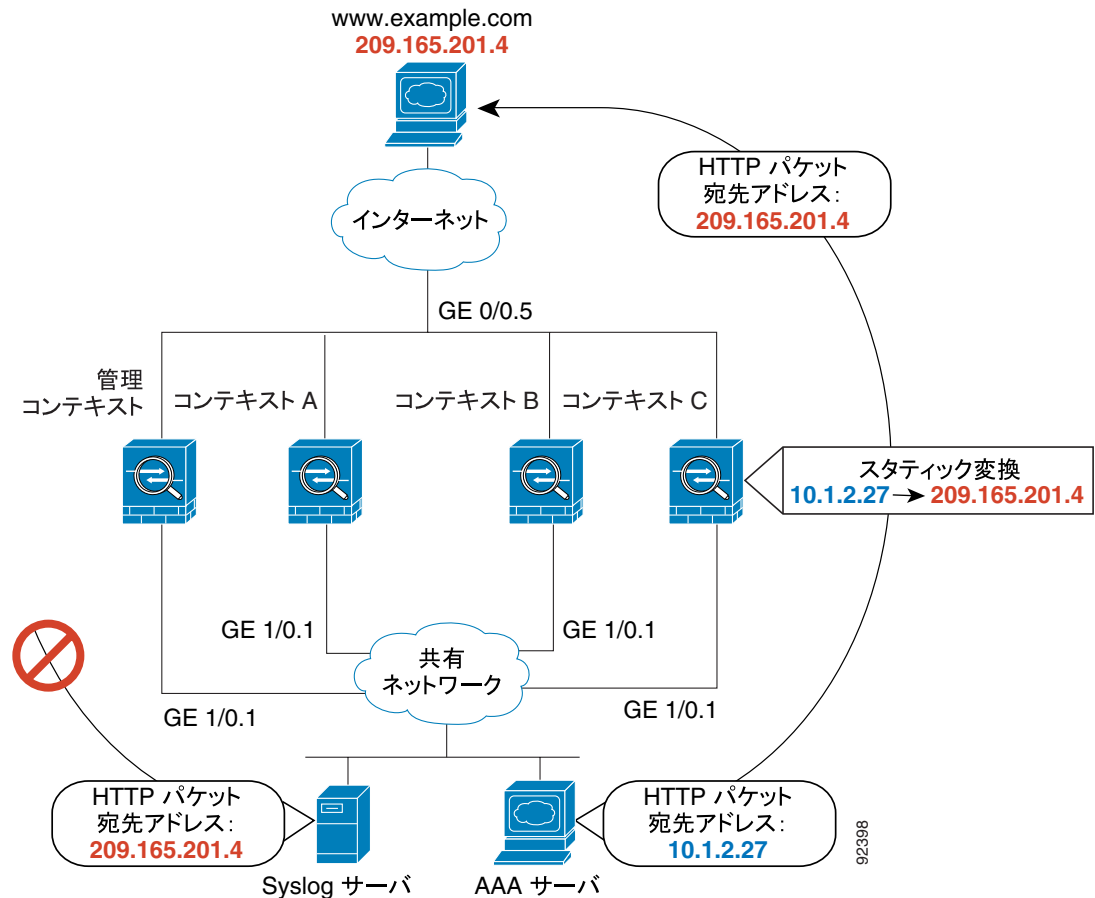
宛先アドレスに設定された NAT のタイプによって、トラフィックが共有インターフェイスから発信できるか、または既存の接続に対する応答のみ可能なかが決定されます。宛先アドレスにダイナミック NAT を使用する場合は、これらのアドレスへの接続は開始できません。したがって、共有インターフェイスからのトラフィックは、既存の接続への応答内に存在しなければなりません。しかし、スタティック NAT を使用すると接続を開始できるため、宛先アドレスにスタティック NAT を使用すると、共有インターフェイスへの接続を開始できます。

外部インターフェイスを共有する場合（インターネットと接続する場合など）は、内部の宛先アドレスが限定され、またシステム管理者がこれを把握しているため、このアドレスへの NAT 設定は、スタティック NAT を設定する場合でも容易に実行できます。

しかし、共有インターフェイスと宛先アドレスが無限にあるインターネットの間の通信を許可する場合は、内部の共有インターフェイスの設定で問題が発生します。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を許可する場合、各インターネット アドレスにスタティック NAT 文を設定する必要があります。この必要条件のため、共有する内部インターフェイス上のユーザに提供可能なインターネット アクセスの種類は必然的に制限されます（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予定の場合は、DNS エントリ アドレスとそれに対する NAT の影響についても検討が必要です。たとえば、あるサーバが [www.example.com](#) にパケットを送信する場合、DNS サーバは変換したアドレスを返す必要があります。NAT コンフィギュレーションによって DNS エントリ管理が決まります）。

**図 3-4** では、内部共有インターフェイス上に 2 台のサーバがあります。1 つのサーバが Web サーバの変換アドレスにパケットを送信すると、セキュリティ アプライアンスがこのパケットを分類して、このアドレスのスタティック変換が含まれているコンテキスト C にパケットを転送します。もう 1 つのサーバが未変換の実アドレスにパケットを送信すると、そのパケットは、セキュリティ アプライアンスが分類できないために、ドロップされます。

図 3-4 共有インターフェイス上でのトラフィックの発信

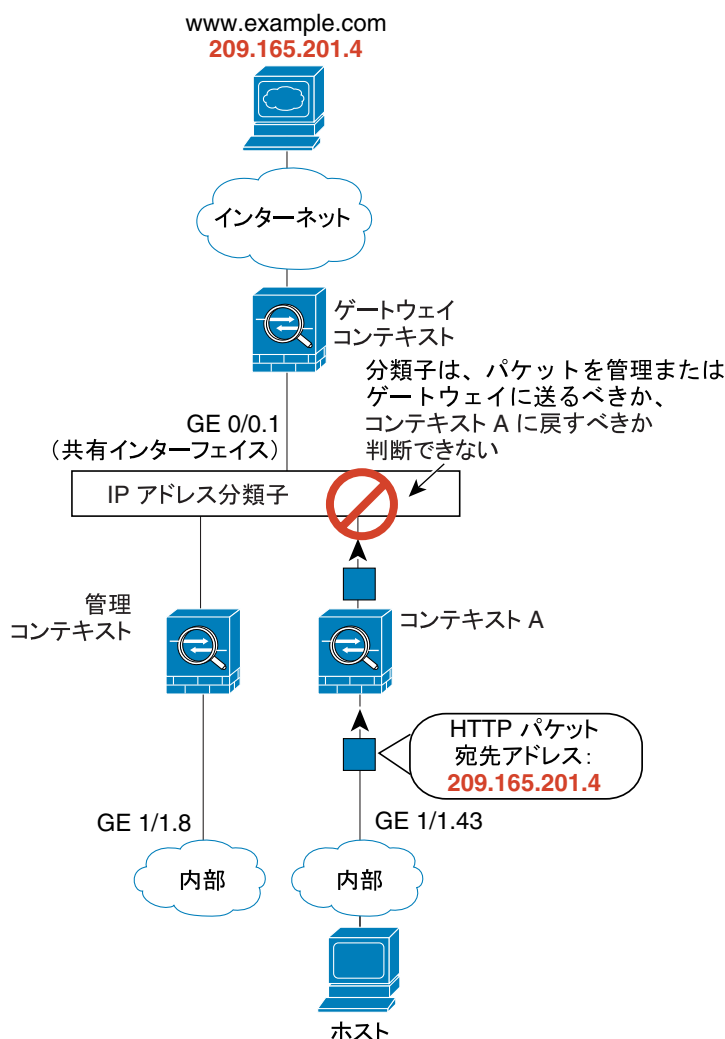


## セキュリティ コンテキストのカスケード接続

共有インターフェイス上でのトラフィック発信に制約があるため、あるコンテキストを別のコンテキストの背後に設定するシナリオでは、最下位のコンテキストのユーザがアクセスを希望する外部アドレスすべてに対して、最上位のコンテキストにスタティック文を設定する必要があります。

図 3-5 では、最下位のコンテキスト（コンテキスト A）のユーザが www.example.com にアクセスしようとしています。ゲートウェイのコンテキストには www.example.com のスタティック変換がないために、このユーザはこの Web サーバにアクセスできません。これは、共有インターフェイス上のどのコンテキストを使用してパケットを割り当てるかを分類子が把握していないためです。

図 3-5 コンテキストのカスケード接続



92396

## マルチコンテキスト モードでのセキュリティ アプライアンスへのログイン

セキュリティ アプライアンスのコンソールにアクセスする場合は、システム実行スペースにアクセスします。その後、Telnet または SSH にコンテキストへのアクセスを設定すると、特定のコンテキストにログインできるようになります。特定のコンテキストにログインすると、アクセスできるのはそのコンテキストのコンフィギュレーションだけになります。しかし、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すると、すべてのコンテキストにアクセスできます。

管理コンテキストからコンテキストに変更しても、管理コンテキストに設定されているユーザ名とコマンド認可の設定を引き続き使用します。

システム実行スペースでは AAA コマンドはサポートされていませんが、個別のログインのために、固有のイネーブル パスワードおよびユーザ名をローカル データベースに設定することができます。

## マルチコンテキスト モードのイネーブル化とディセーブル化

シスコへの発注方法によっては、セキュリティ アプライアンスがすでにマルチセキュリティ コンテキスト用に設定されている場合があります。ただし、アップグレードする場合は、この項で説明する手順に従ってシングルモードからマルチモードに変換することが必要になる場合があります。ASDM はモードの変更をサポートしていないため、CLI を使用してモードを変更する必要があります。

ここでは、次の項目について説明します。

- シングルモード コンフィギュレーションのバックアップ (P.3-10)
- マルチコンテキスト モードのイネーブル化 (P.3-10)
- シングルコンテキスト モードの復元 (P.3-11)

### 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

シングルモードからマルチモードに変換すると、セキュリティ アプライアンスは実行コンフィギュレーションを2つのファイルに変換します。元のスタートアップ コンフィギュレーションは保存されないため、実行コンフィギュレーションと異なる場合は、手順を進める前にバックアップを取る必要があります。

### マルチコンテキスト モードのイネーブル化

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

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

マルチモードをイネーブルにするには、次のコマンドを入力します。

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

セキュリティ アプライアンスをリブートするよう求められます。



## シングルコンテキスト モードの復元

マルチモードからシングルモードに変換する場合、最初にスタートアップ コンフィギュレーション全体をセキュリティ アプライアンスにコピーします（可能な場合）。これは、シングルモードの装置にとって、マルチモードから継承されるシステム コンフィギュレーションは完全に機能を果たすコンフィギュレーションではないためです。システム コンフィギュレーションは、自身のコンフィギュレーションの一部としてネットワーク インターフェイスを持たないため、コンソールからセキュリティ アプライアンスにアクセスしてコピーをとる必要があります。

以前の実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてモードをシングルモードに変更するには、システム実行スペースで次の手順を実行します。

- 
- ステップ 1** 元の実行コンフィギュレーションのバックアップ バージョンを現在のスタートアップ コンフィギュレーションにコピーするには、システムの実行スペースで次のコマンドを入力します。

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

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

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

セキュリティ アプライアンスがリブートします。

---





# イーサネットとサブインターフェイスの設定

この章では、物理イーサネット インターフェイスを設定し、イネーブルにする方法、およびサブインターフェイスを追加する方法について説明します。ASA 5000 シリーズ適応型セキュリティ アプライアンスに 4GE SSM を使用している場合は、インターフェイスのメディア タイプを設定する方法について、この章を参照してください。

シングルコンテキスト モードの場合は、この章で説明する手順をすべて実行してから、[第 6 章「インターフェイス パラメータの設定」](#)で説明するインターフェイス設定に進んでください。マルチコンテキスト モードの場合は、システム実行スペースでこの章の手順をすべて実行してから、[第 5 章「セキュリティ コンテキストの追加と管理」](#)の説明に従ってインターフェイスとサブインターフェイスをコンテキストに割り当て、最後に、[第 6 章「インターフェイス パラメータの設定」](#)の説明に従って各コンテキスト内にインターフェイス パラメータを設定してください。

次の事項について説明します。

- [RJ-45 インターフェイスの設定とイネーブル化 \(P.4-2\)](#)
- [4GE SSM でのファイバ インターフェイスの設定とイネーブル化 \(P.4-4\)](#)
- [サブインターフェイスの設定とイネーブル化 \(P.4-5\)](#)

## RJ-45 インターフェイスの設定とイネーブル化

この項では、物理インターフェイスのイーサネット設定値を設定する方法、およびインターフェイスをイネーブルにする方法について説明します。デフォルトでは、物理インターフェイスはすべてシャットダウンされています。インターフェイスまたはサブインターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチコンテキスト モードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、この手順に従って、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。

デフォルトでは、銅線（RJ-45）インターフェイスの速度と二重通信は、自動ネゴシエーションに設定されます。

ASA 5000 シリーズ適応型セキュリティ アプライアンス用の 4GE SSM には、銅線 RJ-45 とファイバ SFP の 2 種類のコネクタ タイプがあります。RJ-45 がデフォルトです。ファイバ SFP コネクタを使用するように 4GE SSM を設定する場合は、[P.4-4 の「4GE SSM でのファイバ インターフェイスの設定とイネーブル化」](#)を参照してください。

ASA 5500 シリーズ適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、自動ネゴシエーション フェーズでストレート ケーブルが検出されると、内部クロスオーバーを実行して、クロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、速度または二重通信のいずれかを自動ネゴシエーションに設定する必要があります。速度と二重通信の両方に固定値を明示的に設定して、両方の設定に関する自動ネゴシエーションをディセーブルにすると、Auto-MDI/MDIX もディセーブルになります。

インターフェイスをイネーブルにするには、または特定の速度と二重通信を設定するには、次の手順を実行します。

---

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

```
hostname(config)# interface physical_interface
```

*physical\_interface* ID には、タイプ、スロット、およびポート番号を *type[slot]/port* という形式で指定します。

物理インターフェイスには、次のタイプがあります。

- **ethernet**
- **gigabitethernet**

PIX 500 シリーズ セキュリティ アプライアンスでは、タイプの後ろにポート番号を入力します（**ethernet0** など）。

ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、タイプの後ろにスロット / ポートを入力します（**gigabitethernet0/1** など）。シャーシに組み込まれているインターフェイスはスロット 0 に割り当てられていますが、4GE SSM 上のインターフェイスはスロット 1 に割り当てられています。

ASA 5500 シリーズ適応型セキュリティ アプライアンスには、次のタイプもあります。

- **management**

管理インターフェイスは、管理トラフィックのみを対象に設計されているファースト イーサネット インターフェイスであり、**management0/0** と指定されます。ただし、必要であれば、トラフィックを通すために使用することもできます（**management-only** コマンドを参照）。透過ファイアウォール モードでは、トラフィックの通過を許可する 2 つのインターフェイスの他に、管理インターフェイスを使用できます。サブインターフェイスを管理インターフェイスに追加して、マルチコンテキスト モードのセキュリティ コンテキストごとに管理を提供することもできます。

**ステップ 2** （オプション）速度を設定するには、次のコマンドを使用します。

```
hostname(config-if)# speed {auto | 10 | 100 | 1000 | nonegotiate}
```

**auto** 設定がデフォルトです。**speed nonegotiate** コマンドは、リンク ネゴシエーションをディセーブルにします。

**ステップ 3** （オプション）二重通信を設定するには、次のコマンドを使用します。

```
hostname(config-if)# duplex {auto | full | half}
```

**auto** 設定がデフォルトです。

**ステップ 4** インターフェイス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)# no shutdown
```

インターフェイスをディセーブルにするには、**shutdown** コマンドを入力します。物理インターフェイスに対して **shutdown** コマンドを入力すると、すべてのサブインターフェイスもシャットダウンします。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでシャットダウンします。

---

## 4GE SSM でのファイバ インターフェイスの設定とイネーブル化

この項では、物理インターフェイスのイーサネット設定値を設定する方法、およびインターフェイスをイネーブルにする方法について説明します。デフォルトでは、物理インターフェイスはすべてシャットダウンされています。インターフェイスまたはサブインターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチコンテキスト モードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、この手順に従って、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。

デフォルトでは、4GE SSM で使用されるコネクタは RJ-45 コネクタです。ファイバ SFP コネクタを使用するには、メディア タイプを SFP に設定する必要があります。ファイバ インターフェイスでは、速度は固定であり、二重通信はサポートされていませんが、インターフェイスをリンク パラメータ ネゴシエーションあり（デフォルト）またはネゴシエーションなしに設定することができます。

インターフェイスのイネーブル化、メディア タイプの設定、またはネゴシエーションの設定を行うには、次の手順を実行します。

---

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

```
hostname(config)# interface gigabitethernet 1/port
```

4GE SSM インターフェイスは、このシンタクスのインターフェイス ID に示されているように、スロット 1 に割り当てられています（シャーシに組み込まれているインターフェイスはスロット 0 に割り当てられています）。

### ステップ 2 メディア タイプを SFP に設定するには、次のコマンドを入力します。

```
hostname(config-if)# media-type sfp
```

デフォルトの RJ-45 に戻すには、**media-type rj45** コマンドを入力します。

### ステップ 3 （オプション）リンク ネゴシエーションをディセーブルにするには、次のコマンドを使用します。

```
hostname(config-if)# speed nonegotiate
```

ファイバ ギガビット イーサネット インターフェイスの場合、デフォルトは **no speed nonegotiate** です。このコマンドは速度を 1000 Mbps に設定し、フロー制御パラメータとリモート障害情報のリンク ネゴシエーションをイネーブルにします。**speed nonegotiate** コマンドは、リンク ネゴシエーションをディセーブルにします。

### ステップ 4 インターフェイス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)# no shutdown
```

インターフェイスをディセーブルにするには、**shutdown** コマンドを入力します。物理インターフェイスに対して **shutdown** コマンドを入力すると、すべてのサブインターフェイスもシャットダウンします。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでシャットダウンします。

---

## サブインターフェイスの設定とイネーブル化

この項では、サブインターフェイスを設定し、イネーブルにする方法について説明します。イネーブルになっているサブインターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります（詳細については、[P.4-2 の「RJ-45 インターフェイスの設定とイネーブル化」](#)または [P.4-4 の「4GE SSMでのファイバインターフェイスの設定とイネーブル化」](#)を参照してください）。マルチコンテキスト モードの場合、サブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。しかし、トラフィックがコンテキスト インターフェイスを通過するためには、この手順に従って、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。

サブインターフェイスを使用すると、1つの物理インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN では、指定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたはセキュリティ アプライアンスを追加しなくても、ネットワークで使用可能なインターフェイスの数を増やすことができます。この機能は、マルチコンテキスト モードで特に有効なため、各コンテキストにそれぞれ固有のインターフェイスを割り当てることができます。

プラットフォームに許容されるサブインターフェイスの数を決定するには、[付録 A「機能のライセンスと仕様」](#)を参照してください。



(注)

サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。サブインターフェイスでトラフィックを通過させるためには物理インターフェイスをイネーブルにする必要があるため、**nameif** コマンドを除外して、物理インターフェイスがトラフィックを通過させないようにしてください。物理インターフェイスでタグのないパケットを通過できるようにする場合は、通常どおりに **nameif** コマンドを設定します。インターフェイス設定の詳細については、[P.6-1 の「インターフェイス パラメータの設定」](#)を参照してください。

サブインターフェイスを追加して、そのサブインターフェイスに VLAN を割り当てるには、次の手順を実行します。

**ステップ 1** サブインターフェイスを新たに指定するには、次のコマンドを入力します。

```
hostname(config)# interface physical_interface.subinterface
```

物理インターフェイス ID については、[P.4-2 の「RJ-45 インターフェイスの設定とイネーブル化」](#)の説明を参照してください。

**subinterface** ID は、1 ～ 4294967293 の整数です。

たとえば、次のコマンドを入力します。

```
hostname(config)# interface gigabitethernet0/1.100
```

**ステップ2** サブインターフェイスに VLAN を指定するには、次のコマンドを入力します。

```
hostname(config-subif)# vlan vlan_id
```

`vlan_id` は、1 ～ 4094 の整数です。一部の VLAN ID は接続スイッチ用に予約されている場合があります。詳細については、スイッチのマニュアルを確認してください。

VLAN は1つだけサブインターフェイスに割り当てることができ、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。各サブインターフェイスは、VLAN ID がなければトラフィックを通過させることはできません。VLAN ID を変更するには、**no** オプションを使用して以前の VLAN ID を削除する必要はありません。異なる VLAN ID を使用して **vlan** コマンドを入力すると、セキュリティアプライアンスで以前の ID が変更されます。

**ステップ3** サブインターフェイス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-subif)# no shutdown
```

インターフェイスをディセーブルにするには、**shutdown** コマンドを入力します。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでシャットダウンします。

---





# セキュリティ コンテキストの追加と管理

この章では、セキュリティ アプライアンスにマルチセキュリティ コンテキストを設定する方法について説明します。次の項で構成されています。

- [セキュリティ コンテキストの設定 \(P.5-2\)](#)
- [セキュリティ コンテキストの削除 \(P.5-6\)](#)
- [管理コンテキストの変更 \(P.5-7\)](#)
- [コンテキストとシステム実行スペース間の切り替え \(P.5-7\)](#)
- [セキュリティ コンテキスト URL の変更 \(P.5-8\)](#)
- [セキュリティ コンテキストのリロード \(P.5-9\)](#)
- [セキュリティ コンテキストの監視 \(P.5-10\)](#)

コンテキストの機能およびマルチコンテキスト モードのイネーブル化については、[第 3 章「マルチコンテキスト モードのイネーブル化」](#)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内のセキュリティ コンテキストの定義によって、コンテキストの名前、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が識別されます。



(注)

管理コンテキストがない場合（コンフィギュレーションをクリアした場合など）は、最初に次のコマンドを入力して管理コンテキスト名を指定する必要があります。

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

このコンテキスト名はコンフィギュレーションにまだ存在しませんが、この後に **context name** コマンドを入力すると、指定した名前との照合が行われて、管理コンテキスト コンフィギュレーションを続行できます。

システム コンフィギュレーションにコンテキストを追加する場合、または既存のコンテキストを変更する場合は、次の手順を実行します。

**ステップ 1** コンテキストを追加または修正するには、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。この名前では、大文字と小文字が区別されるため、たとえば、「customerA」と「CustomerA」の2種類のコンテキストが使用できます。英字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンを使用することはできません。

「System」および「Null」（大文字および小文字）は予約されている名前であるため、使用できません。

**ステップ 2** （オプション）このコンテキストに説明を追加するには、次のコマンドを使用します。

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

**ステップ 3** コンテキストで使用するインターフェイスを指定するには、1 つの物理インターフェイス、あるいは1 つまたは複数のサブインターフェイスに該当するコマンドを入力します。

- 物理インターフェイスを割り当てるには、次のコマンドを入力します。

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

- 1 つまたは複数のサブインターフェイスを割り当てるには、次のコマンドを入力します。

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

これらのコマンドを複数回入力して複数の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が含まれているコンテキスト コマンドは、すべて実行コンフィギュレーションから削除されます。

透過ファイアウォール モードでは、2つのインターフェイスのみがトラフィックを通過させることができます。ただし、ASA 適応型セキュリティ アプライアンスでは、専用の管理インターフェイス Management 0/0（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第3のインターフェイスとして使用できます。

**(注)**

透過モードの管理インターフェイスによって、MAC アドレス テーブルにないパケットがインターフェイスからフラッドされることはありません。

必要に応じて、同じインターフェイスをルーテッド モードの複数のコンテキストに割り当てることができます。透過モードでは、インターフェイスの共有は許されません。

`map_name` は、インターフェイスの英数字のエイリアスで、インターフェイス ID の代わりにコンテキスト内で使用できます。マッピング名を指定しない場合は、コンテキスト内でインターフェイス ID が使用されます。セキュリティ保護上の目的から、コンテキストでどのインターフェイスが使用されているかをコンテキスト管理者に知られないようにすることができます。

マッピング名は英字で始まり英字または数字で終わる必要があります。中の文字として使用できるのは、英字、数字、下線だけです。たとえば、次のような名前が使用できます。

`int0`

`inta`

`int_0`

サブインターフェイスでは、マッピング名の範囲が指定できます。

サブインターフェイスの範囲を指定すると、マッピング名を照合する範囲が指定できます。範囲指定については次のガイドラインに従ってください。

- マッピング名は、英字の部分とそれに続く数字の部分で構成する必要があります。マッピング名の英字部分は、範囲の両端で一致していなければなりません。たとえば、次の範囲を入力します。

`int0-int10`

たとえば、`gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5` と入力すると、コマンドは失敗します。

- マッピング名の数字の部分には、サブインターフェイスの範囲と同じ数字が含まれていなければなりません。たとえば、次の両方の範囲には、100 のインターフェイスが含まれています。

`gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100`

たとえば、`gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15` と入力すると、コマンドは失敗します。

`visible` を設定して、マッピング名を設定した場合でも、`show interface` コマンドによって、物理インターフェイスのプロパティが表示されるようになります。デフォルトの `invisible` は、マッピング名だけが表示されるように指定するキーワードです。

次の例では、gigabitethernet0/1.100、gigabitethernet0/1.200、および gigabitethernet0/2.300 ～ gigabitethernet0/2.305 がコンテキストに割り当てられることを示します。int1 ～ int8 がマッピング名です。

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

**ステップ 4** システムがコンテキスト コンフィギュレーションをダウンロードする URL を識別するには、次のコマンドを入力します。

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

コンテキストの URL を追加すると、システムは、動作中になるように、ただちにそのコンテキストをロードします（そのコンフィギュレーションが使用可能である場合）。



(注)

**allocate-interface** コマンドは、**config-url** コマンドを入力する前に入力してください。セキュリティ アプライアンスは、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インターフェイスをコンテキストに割り当てる必要があります。これは、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 (**interface**、**nat**、**global...**) を参照するコマンドが含まれている場合があるためです。**config-url** コマンドを先に入力すると、セキュリティ アプライアンスは、コンテキスト コンフィギュレーションをただちにロードします。この場合、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ると、そのコマンドは失敗します。

次の URL シンタックスを参照してください。

- **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」を使用することをお勧めします。コンフィギュレーション ファイルが使用不可の場合、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
```

この場合、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 ファイルは、内部フラッシュ メモリに保存する必要があります。

- **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 通常モード
- **ip** : (デフォルト) バイナリ パッシブ モード
- **in** : バイナリ通常モード

サーバは、管理コンテキストからアクセス可能である必要があります。ファイル名にファイル拡張子は不要ですが、「.cfg」を使用することをお勧めします。コンフィギュレーション ファイルが使用不可の場合、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
```

この場合、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可能である必要があります。ファイル名にファイル拡張子は不要ですが、「.cfg」を使用することをお勧めします。コンフィギュレーション ファイルが使用不可の場合、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した場合、**write memory** コマンドを使用して変更内容を HTTP サーバまたは HTTPS サーバに保存し直すことはできません。しかし、**copy tftp** コマンドを使用すると、実行コンフィギュレーションを TFTP サーバにコピーできます。

- **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可能である必要があります。サーバ アドレスへのルートを上書きする場合は、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」を使用することをお勧めします。コンフィギュレーション ファイルが使用不可の場合、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
```

この場合、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 を指定した **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、[P.5-8 の「セキュリティ コンテキスト URL の変更」](#)を参照してください。

たとえば、次のコマンドを入力します。

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

- ステップ 5** コンテキスト情報の表示については、『Cisco Security Appliance Command Reference』の **show context** コマンドの説明を参照してください。

次の例では、管理コンテキストを「administrator」と設定し、内部フラッシュ メモリに「administrator」という名前のコンテキストを作成してから、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 gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

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

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

## セキュリティ コンテキストの削除

システム コンフィギュレーションを編集することで、削除できるのは1つのコンテキストだけです。現在の管理コンテキストは、**clear context** コマンドを実行してすべてのコンテキストを削除しない限り、削除できません。



(注)

フェールオーバーを使用すると、アクティブ装置でコンテキストを削除した時刻と、スタンバイ装置でコンテキストが削除された時刻との間で遅延が生じます。アクティブ装置とスタンバイ装置の間でインターフェイス数が一致していないことを示すエラー メッセージが表示される場合があります。このエラーは一時的に表示されるもので、無視できます。

コンテキストの削除には、次のコマンドを使用します。

- 1つのコンテキストを削除するには、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)# no context name
```

すべてのコンテキスト コマンドを削除することもできます。

- すべてのコンテキスト（管理コンテキストを含む）を削除するには、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)# 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限り、任意のコンテキストを管理コンテキストに設定することができます。管理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)# admin-context context_name
```

Telnet、SSH、HTTPS など、管理コンテキストに接続しているリモート管理セッションはすべて終了します。新しい管理コンテキストに再接続する必要があります。



(注)

**ntp server** を含むいくつかのシステム コマンドは、管理コンテキストに所属するインターフェイス名を識別します。管理コンテキストを変更した場合に、そのインターフェイス名が新しい管理コンテキストに存在しないときは、そのインターフェイスを参照するシステム コマンドはすべて、アップデートしてください。

## 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にログインした場合（または Telnet や SSH を使用して管理コンテキストにログインした場合）は、コンテキスト間の切り替えが可能であり、各コンテキスト内でコンフィギュレーション タスクやモニタリング タスクを実行できます。実行コンフィギュレーションが、コンフィギュレーション モードで編集するか、**copy** コマンドまたは **write** コマンドに使用されるかは、ログインした場所で決まります。システム実行スペースにログインした場合、実行コンフィギュレーションはシステム コンフィギュレーションのみで構成され、コンテキストにログインした場合は、実行コンフィギュレーションはそのコンテキストのみで構成されます。たとえば、**show running-config** コマンドを入力しても、すべての実行コンフィギュレーション（システム コンテキストとすべてのコンテキスト）を表示することはできません。現在のコンフィギュレーションだけが表示されます。

システム実行スペースとコンテキスト間の切り替え、またはコンテキスト間の切り替えを行うには、次のコマンドを使用します。

- あるコンテキストに切り替えるには、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化します。

```
hostname/name#
```

- システム実行スペースに切り替えるには、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化します。

```
hostname#
```

## セキュリティ コンテキスト URL の変更

セキュリティ コンテキスト URL は、新しい URL からコンフィギュレーションをリロードしないと変更できません。

セキュリティ アプライアンスは、新しいコンフィギュレーションを現在の実行コンフィギュレーションとマージします。同じ URL を再入力しても、保存済みのコンフィギュレーションが実行コンフィギュレーションとマージされます。マージは、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドを追加します。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生すること、予期できない結果が生じることもあります。実行コンフィギュレーションが空白の場合（サーバが利用できず、コンフィギュレーションがまったくダウンロードされなかった場合など）は、新しいコンフィギュレーションが使用されます。コンフィギュレーションをマージしない場合、実行コンフィギュレーションをクリアすることができます。これを行うとコンテキストを通る通信がすべて中断されるので、後で新しい URL からコンフィギュレーションをリロードします。

コンテキストの URL を変更するには、次の手順を実行します。

- ステップ 1** コンフィギュレーションをマージしない場合、コンテキストに切り替えてそのコンフィギュレーションをクリアするには、次のコマンドを入力します。マージを実行する場合は、ステップ 2 にスキップします。

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

- ステップ 2** 必要な場合は、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** 切り替えた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 モードに入るには、次のコマンドを入力します。

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

- ステップ 4** 新しい URL を入力するには、次のコマンドを入力します。

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

システムは、動作中になるように、ただちにコンテキストをロードします。



## セキュリティ コンテキストのリロード

セキュリティ コンテキストは、次の2つの方法でリロードできます。

- 実行コンフィギュレーションをクリアしてからスタートアップ コンフィギュレーションをインポートする。  
このアクションでは、セキュリティ コンテキストに関連付けられている接続や NAT テーブルなどのアトリビュートの大部分がクリアされます。
- セキュリティ コンテキストをシステム コンフィギュレーションから削除する。  
このアクションでは、トラブルシューティングに役立つ可能性のあるメモリ割り当てなど補足的なアトリビュートがクリアされます。しかし、コンテキストをシステムに戻して追加するには、URL とインターフェイスを再指定する必要があります。

ここでは、次の項目について説明します。

- [コンフィギュレーションのクリアによるリロード \(P.5-9\)](#)
- [コンテキストの削除および再追加によるリロード \(P.5-9\)](#)

## コンフィギュレーションのクリアによるリロード

コンテキスト コンフィギュレーションをクリアし、URL からコンフィギュレーションをリロードすることによってコンテキストをリロードするには、次の手順を実行します。

---

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

```
hostname# changeto context name
```

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

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

**ステップ 3** 実行コンフィギュレーションをクリアするには、次のコマンドを入力します。

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

このコマンドを実行するとすべての接続がクリアされます。

**ステップ 4** コンフィギュレーションをリロードするには、次のコマンドを入力します。

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

セキュリティ アプライアンスは、システム コンフィギュレーションに指定された URL からコンフィギュレーションをコピーします。コンテキスト内で URL を変更することはできません。

---

## コンテキストの削除および再追加によるリロード

コンテキストを削除し、その後再追加することによってコンテキストをリロードするには、次の各項で説明してある手順を実行してください。

1. [セキュリティ コンテキストの削除 \(P.5-6\)](#)
2. [セキュリティ コンテキストの設定 \(P.5-2\)](#)

# セキュリティ コンテキストの監視

この項では、コンテキスト情報の表示および監視の方法について説明します。次の項目を取り上げます。

- [コンテキスト情報の表示 \(P.5-10\)](#)
- [リソースの使用状況の表示 \(P.5-11\)](#)

## コンテキスト情報の表示

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

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

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

**detail** オプションを指定すると、追加情報が表示されます。詳細については、次の出力例を参照してください。

特定のコンテキストの情報を表示する場合は、*name* にコンテキスト名を指定します。

**count** オプションを指定すると、コンテキストの合計数が表示されます。

次に、**show context** コマンドの出力例を示します。この出力例では、3 つのコンテキストが表示されています。

```
hostname# show context

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

[表 5-1](#) に、各フィールドの説明を示します。

**表 5-1 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します。アスタリスク (*) が付いたコンテキスト名は管理コンテキストです。 |
| Interfaces   | コンテキストに割り当てられるインターフェイス。                              |
| URL          | セキュリティ アプライアンスがコンテキスト コンフィギュレーションをロードする URL。         |

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

```
hostname# show context detail

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

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

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

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

**detail** の出力の詳細については、『Cisco Security Appliance 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
```

## リソースの使用状況の表示

システム実行スペースで、コンテキストごとのリソースの使用状況やシステム リソースの使用状況を表示できます。表示されるリソースには、同時接続、Telnet セッション、SSH セッション、ホスト、NAT 変換、およびシングルモードの IPSec セッションが含まれます。

システム実行スペースでコンテキストごとのリソースの使用状況を表示するには、次のコマンドを入力します。

```
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** (すべての) コンテキストの使用状況が表示されます。各コンテキストは個別にリスト表示されます。

指定したリソースの上位 *n* 人のユーザとなっているコンテキストを表示するには、**top n** キーワードを入力します。このオプションには、リソース タイプを1つ指定する必要がありますが、**resource all** は指定しないでください。

**summary** オプションでは、すべてのコンテキストの使用状況を組み合わせて表示されます。

**system** オプションでは、すべてのコンテキストの使用状況を組み合わせて表示されますが、組み合わせたコンテキストの制限ではなく、リソースに対するシステムの制限が表示されます。

**resource** の名前に指定する値には、次のものがあります。リスト全体を表示する **show resource type** コマンドも参照してください。すべてのタイプを表示するには **all**（デフォルト）を指定します。

- **conns**：任意の2つのホスト間の TCP 接続または UDP 接続。これには、1台のホストと他の複数台のホストとの接続も含まれます。
- **hosts**：セキュリティ アプライアンスを通して接続可能なホスト。
- **ipsec**：（シングルモードのみ）IPSec セッション。
- **ssh**：SSH セッション。
- **telnet**：Telnet セッション。
- **xlates**：NAT 変換。

**counter counter\_name** には、次のいずれかのキーワードを指定します。

- **current**：アクティブな同時インスタンスまたはリソースの現在のレートを示します。
- **peak**：同時インスタンスのピーク値、またはリソースのレートのピーク値を表示します。**clear resource usage** コマンドまたはリブートによって、最後に統計情報がクリアされて以来の値。
- **all**：（デフォルト）すべての統計情報を表示します。

**count\_threshold** は、表示するリソースの下限を設定します。デフォルトは1です。リソースの使用状況が設定した数字より少ないと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、**count\_threshold** が現在の使用状況に適用されます。



(注)

すべてのリソースを表示するには、**count\_threshold** を **0** に設定します。

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

```
hostname# show resource usage context admin
```

| Resource | Current | Peak | Limit | Context |
|----------|---------|------|-------|---------|
| Telnet   | 1       | 1    | 5     | admin   |
| Conns    | 44      | 55   | N/A   | admin   |
| Hosts    | 45      | 56   | N/A   | admin   |

**show resource usage summary** コマンドの出力例を次に示します。このコマンドは、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示します。この出力例では、6 コンテキストという限界を示しています。

```
hostname# show resource usage summary
```

| Resource | Current | Peak | Limit | Context |
|----------|---------|------|-------|---------|
| Telnet   | 3       | 5    | 30    | Summary |
| SSH      | 5       | 7    | 30    | Summary |
| Conns    | 40      | 55   | N/A   | Summary |
| Hosts    | 44      | 56   | N/A   | Summary |

次に、**show resource usage summary** コマンドの出力例を示します。この出力例では、25 コンテキストという限界を示しています。Telnet 接続および SSH 接続のコンテキストの限界がコンテキストごとに5であるため、合計の限界は125です。システムの限界が単に100であるため、システムの限界が表示されています。

```
hostname# show resource usage summary
```

| Resource | Current | Peak | Limit  | Context |
|----------|---------|------|--------|---------|
| Telnet   | 1       | 1    | 100[S] | Summary |
| SSH      | 2       | 2    | 100[S] | Summary |
| Conns    | 56      | 90   | N/A    | Summary |
| Hosts    | 89      | 102  | N/A    | Summary |

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

次に、**show resource usage system** コマンドの出力例を示します。このコマンドは、すべてのコンテキストのリソースの使用状況を表示しますが、ここでは、組み合わせたコンテキストの限界ではなく、システムの限界を表示しています。

```
hostname# show resource usage system
```

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





# 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およびサブインターフェイスの名前、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。シングルコンテキスト モードの場合は、この章の手順は、[第 4 章「イーサネットとサブインターフェイスの設定」](#)で開始したインターフェイスの設定の続きとして実行します。マルチコンテキスト モードの場合は、[第 4 章「イーサネットとサブインターフェイスの設定」](#)の手順はシステム実行スペースで実行しますが、この章の手順は各セキュリティ コンテキスト内で実行します。

次の事項について説明します。

- [セキュリティ レベルの概要 \(P.6-2\)](#)
- [インターフェイスの設定 \(P.6-3\)](#)
- [同一セキュリティ レベルにあるインターフェイス間の通信の許可 \(P.6-7\)](#)

## セキュリティ レベルの概要

各インターフェイスには、0（最下位）～ 100（最上位）のセキュリティ レベルを設定する必要があります。たとえば、内部ホスト ネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル 0 が割り当てられる場合があります。DMZ などその他のネットワークはその中間に設定できます。複数のインターフェイスを同じセキュリティ レベルに割り当てることができます。詳細については、[P.6-7](#) の「[同一セキュリティ レベルにあるインターフェイス間の通信の許可](#)」を参照してください。

各レベルは、次の動作を制御します。

- ネットワーク アクセス：デフォルトでは、高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイス（発信）へのアクセスは、暗黙的に許可されます。高位のセキュリティ インターフェイス上のホストは、それより低いセキュリティ インターフェイス上のホストすべてにアクセスできます。アクセスは、インターフェイスにアクセスリストを適用すると制限できます。

同じレベルのセキュリティ インターフェイスの場合、同じセキュリティ レベルまたはそれより低いレベルの他のインターフェイスにアクセスするインターフェイスへのアクセスは、暗黙的に許可されます。

- 検査エンジン：一部のアプリケーション検査エンジンはセキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイスの場合、検査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 検査エンジン：発信接続のみに適用されます。
  - SQL\*Net 検査エンジン：SQL\*Net（旧称 OraServ）ポートとの制御接続が一对のホスト間に存在する場合、着信データ接続のみセキュリティ アプライアンスを通過することが許可されます。

- フィルタリング：HTTP（S）フィルタリングおよびFTP フィルタリングは、発信接続（高位レベルから低位レベルへの接続）に対してのみ適用されます。

同じセキュリティ レベルのインターフェイスの場合、どちらの方向のトラフィックにもフィルタリングが適用できます。

- NAT 制御：NAT 制御をイネーブルにする場合、低位のセキュリティ インターフェイス（外部）上のホストにアクセスする高位のセキュリティ インターフェイス（内部）上のホストに NAT を設定する必要があります。

NAT 制御がない場合、または同じレベルのセキュリティ インターフェイスの場合は、任意のインターフェイス間で NAT を使用するよう選択することも、NAT を使用しないよう選択することもできます。外部インターフェイスに対して NAT を設定すると、特殊なキーワードが必要になる場合があることに留意してください。

- **established** コマンド：このコマンドを使用すると、高位レベルのホストから低位レベルのホストに接続がすでに確立されている場合に、低位のセキュリティのホストから高位のセキュリティのホストへのリターン接続が許可されます。

同じセキュリティ レベルのインターフェイスでは、両方向に対して **established** コマンドが設定できます。



## インターフェイスの設定

デフォルトでは、物理インターフェイスはすべてシャットダウンされています。イネーブルになっているサブインターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチコンテキスト モードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでダウンします。

コンフィギュレーションを完了してトラフィックがセキュリティ アプライアンスを通過できるようにするには、事前にインターフェイス名と、ルーテッド モードの場合は IP アドレスを設定する必要があります。また、セキュリティ レベルをデフォルトの 0 から変更する必要もあります。インターフェイス名を「inside」にし、セキュリティ レベルを明示的に設定しない場合は、セキュリティ アプライアンスによってセキュリティ レベルが 100 に設定されます。

**(注)**

フェールオーバーを使用している場合は、フェールオーバー通信およびステートフル フェールオーバー通信に予約されているインターフェイスには、この方法で名前を付けないでください。フェールオーバー リンクおよびステート リンクの設定については、[第 11 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 モードでは、次のガイドラインに従ってください。

- 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。
- システム コンフィギュレーションの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 インターフェイスのみが設定できます。
- システム コンフィギュレーションでは、イーサネット設定および VLAN のみが設定できます。フェールオーバー インターフェイスは例外で、この方法でフェールオーバー 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、フェールオーバーの章を参照してください。

**(注)**

インターフェイスのセキュリティ レベルを変更したときに、既存の接続がタイムアウトするまで待機せずに新しいセキュリティ 情報を使用する必要がある場合は、**clear local-host** コマンドを使用して接続をクリアできます。

インターフェイスまたはサブインターフェイスを設定するには、次の手順を実行します。

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

```
hostname(config)# interface {physical_interface[.subinterface] | mapped_name}
```

*physical\_interface* ID には、タイプ、スロット、およびポート番号を *type[slot]/port* という形式で指定します。

物理インターフェイスには、次のタイプがあります。

- ethernet
- gigabitethernet

PIX 500 シリーズ セキュリティ アプライアンスでは、タイプの後ろにポート番号を入力します (ethernet0 など)。

ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、タイプの後ろにスロット / ポートを入力します (gigabitethernet0/1 など)。シャーシに組み込まれているインターフェイスはスロット 0 に割り当てられていますが、4GE SSM 上のインターフェイスはスロット 1 に割り当てられています。

ASA 5500 シリーズ適応型セキュリティ アプライアンスには、次のタイプもあります。

- **management**

管理インターフェイスは、管理トラフィックのみを対象に設計されているファースト イーサネット インターフェイスであり、**management0/0** と指定されます。ただし、必要であれば、トラフィックを通すために使用することもできます (**management-only** コマンドを参照)。透過ファイアウォール モードでは、トラフィックの通過を許可する 2 つのインターフェイスの他に、管理インターフェイスを使用できます。サブインターフェイスを管理インターフェイスに追加して、マルチコンテキスト モードのセキュリティ コンテキストごとに管理を提供することもできます。

subinterface ID は、物理インターフェイス ID の後ろに、ピリオド (.) で区切って付加します。

マルチコンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を入力します。

たとえば、次のコマンドを入力します。

```
hostname(config)# interface gigabitethernet0/1.1
```

## ステップ 2 インターフェイスに名前を付けるには、次のコマンドを入力します。

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

*name* は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。新しい値を指定してこのコマンドを再入力すると名前を変更することができます。**no** 形式は入力しないでください。このコマンドを入力すると、この名前を参照しているコマンドがすべて削除されます。

## ステップ 3 セキュリティ レベルを設定するには、次のコマンドを入力します。

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

ここで、*number* には、0 (最下位) ~ 100 (最上位) の整数を指定します。

## ステップ 4 (ルーテッド モードのみ) IP アドレスを設定するには、次のコマンドのいずれかを入力します。



(注)

IPv6 アドレスの設定については、[P.9-3 の「インターフェイスでの IPv6 の設定」](#)を参照してください。

透過ファイアウォール モードの管理 IP アドレスを設定するには、[P.7-6 の「透過ファイアウォールの管理 IP アドレスの設定」](#)を参照してください。透過モードでは、インターフェイスごとに IP アドレスを設定するのではなく、セキュリティ アプライアンス全体またはコンテキスト全体に IP アドレスを設定します。

- IP アドレスを手動で設定するには、次のコマンドを入力します。

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

**standby** キーワードおよびアドレスはフェールオーバーで使用します。詳細については、[第11章「フェールオーバーの設定」](#)を参照してください。

- DHCP サーバから IP アドレスを取得するには、次のコマンドを入力します。

```
hostname(config-if)# ip address dhcp [setroute]
```

このコマンドを再入力すると、DHCP リースがリセットされて新しいリースが要求されます。

このコマンドは、**ip address** コマンドと同時に設定できません。

**setroute** オプションをイネーブルにする場合は、**static** コマンドを使用してデフォルト ルートを設定しないでください。

**ip address dhcp** コマンドを入力する前に **no shutdown** コマンドを使用してインターフェイスをイネーブルにしていない場合は、一部の DHCP 要求が送信されない場合があります。

#### ステップ5 インターフェイスを管理専用モードに設定するには、次のコマンドを入力します。

```
hostname(config-if)# management-only
```

ASA 5000 シリーズ適応型セキュリティ アプライアンスには、Management 0/0 と呼ばれる専用の管理インターフェイスが含まれており、このインターフェイスによってセキュリティ アプライアンスへのトラフィックをサポートします。ただし、**management-only** コマンドを使用することで、任意のインターフェイスを管理専用インターフェイスとして設定できます。また、Management 0/0 の管理専用モードをディセーブルにして、他のインターフェイスと同様にトラフィックを通過させることもできます。



(注)

透過ファイアウォール モードでは、2 つのインターフェイスのみがトラフィックを通過させることができます。ただし、ASA 5000 シリーズ適応型セキュリティ アプライアンスでは、専用の管理インターフェイス（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第3のインターフェイスとして使用できます。モードはこの場合設定不能であり、常に管理専用にする必要があります。

#### ステップ6 インターフェイスをイネーブルにするには、次のコマンドを入力します（インターフェイスがまだイネーブルになっていない場合）。

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

インターフェイスをディセーブルにするには、**shutdown** コマンドを入力します。物理インターフェイスに対して **shutdown** コマンドを入力すると、すべてのサブインターフェイスもシャットダウンします。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスを共有しているすべてのコンテキストでシャットダウンします。これは、コンテキスト コンフィギュレーションでこのインターフェイスがイネーブルであると表示される場合も例外ではありません。

次の例では、シングルモードで物理インターフェイスのパラメータを設定します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

次の例では、シングルモードでサブインターフェイスのパラメータを設定します。

```
hostname(config)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

次の例では、システム コンフィギュレーションに対してマルチコンテキスト モードでインターフェイス パラメータを設定し、gigabitethernet 0/1.1 サブインターフェイスを contextA に割り当てます。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# no shutdown
hostname(config-subif)# context contextA
hostname(config-ctx)# ...
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
```

次の例では、コンテキスト コンフィギュレーションに対してマルチコンテキスト モードでパラメータを設定します。

```
hostname/contextA(config)# interface gigabitethernet0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
hostname/contextA(config-if)# no shutdown
```

## 同一セキュリティ レベルにあるインターフェイス間の通信の許可

デフォルトでは、セキュリティ レベルが同じインターフェイス同士では通信できません。同じセキュリティ レベルのインターフェイス間で通信を許可する利点としては、次のものがあります。

- 101 より多くの通信インターフェイスが設定できます。  
各インターフェイスで異なるセキュリティ レベルを使用したときに、同一のセキュリティ レベルにインターフェイスを割り当てないと、各レベル（0 ～ 100）に 1 つのインターフェイスしか設定できません。
- アクセスリストがなくても同じセキュリティ レベルのインターフェイスすべての間で自由にトラフィックが流れるようにできます。



(注)

NAT 制御をイネーブルにすると、同じセキュリティ レベルのインターフェイス間で NAT を設定する必要がなくなります。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、[P.14-13](#) の「[NAT および同じセキュリティ レベルのインターフェイス](#)」を参照してください。

同じセキュリティ レベルを持つインターフェイス間の通信をイネーブルにした場合でも、異なるセキュリティ レベルのインターフェイスも通常どおりに設定できます。

相互通信を可能にするために同じセキュリティ レベルのインターフェイスをイネーブルにするには、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。

## ■ 同一セキュリティ レベルにあるインターフェイス間の通信の許可



# 基本設定

この章では、セキュリティ アプライアンス上で機能を果たすコンフィギュレーションに通常必要とされる基本設定を行う方法について説明します。次の事項について説明します。

- [イネーブル パスワードの変更 \(P.7-1\)](#)
- [ホスト名の設定 \(P.7-2\)](#)
- [ドメイン名の設定 \(P.7-2\)](#)
- [日付と時刻の設定 \(P.7-3\)](#)
- [透過ファイアウォールの管理 IP アドレスの設定 \(P.7-6\)](#)

## 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、特権 EXEC モードに入ることができます。デフォルトでは、イネーブル パスワードは空白に設定されています。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、最大 16 文字の英数字および特殊文字からなるパスワードで、大文字と小文字は区別されます。パスワードには疑問符 (?) とスペースを除く任意の文字を使用できます。

このコマンドは最高の特権レベルにパスワードを変更します。ローカル コマンド認可を設定すると、0 ～ 15 の各特権レベルにイネーブル パスワードを設定できます。

パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。パスワードを指定せずに **enable password** コマンドを入力すると、パスワードはデフォルトの空白に設定されます。

## ホスト名の設定

セキュリティ アプライアンスのホスト名を設定すると、そのホスト名がコマンドラインのプロンプトに表示されます。このホスト名によって、複数の装置とのセッションを確立する場合に、コマンドを入力する場所が常に把握できます。デフォルトのホスト名は、プラットフォームの種類によって決まります。

マルチコンテキスト モードでは、システム実行スペースで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。コンテキスト内にオプションで設定したホスト名はコマンドラインに表示されませんが、**banner** コマンドの **\$(hostname)** トークンで使用できます。

セキュリティ アプライアンスまたはコンテキストのホスト名を指定するには、次のコマンドを入力します。

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

名前には、63 文字以下の文字を使用できます。ホスト名は英字または数字で始まり英字または数字で終わる必要があります。中の文字として使用できるのは、英字、数字、ハイフンだけです。

この名前がコマンドライン プロンプトに表示されます。次の例を参考にしてください。

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

## ドメイン名の設定

セキュリティ アプライアンスは、ドメイン名を未修飾名に拡張子として追加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバに未修飾名「jupiter」を指定すると、セキュリティ アプライアンスは、この名前を「jupiter.example.com」に限定します。

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 モードでは、システム実行スペース内と同様、各コンテキストにドメイン名を設定することができます。

セキュリティ アプライアンス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、ドメインに example.com という名前を指定するには、次のコマンドを入力します。

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



## 日付と時刻の設定

この項では、日付と時刻の設定方法として、手動で行う方法と NTP サーバを使用するダイナミックな方法について説明します。手動で設定した時刻はすべて、NTP サーバから取得された時刻によって上書きされます。この項では、時間帯および夏時間の日付範囲の設定方法についても説明します。



(注)

マルチコンテキスト モードでは、時刻はシステム コンフィギュレーションのみに設定してください。

ここでは、次の項目について説明します。

- [時間帯と夏時間の日付範囲の設定 \(P.7-3\)](#)
- [NTP サーバを使用する日付と時刻の設定 \(P.7-4\)](#)
- [手動での日付と時刻の設定 \(P.7-5\)](#)

## 時間帯と夏時間の日付範囲の設定

デフォルトでは、時間帯は UTC（世界標準時）であり、夏時間の日付範囲は 4 月の第一日曜日の午前 2 時～10 月の最終日曜日の午前 2 時です。時間帯および夏時間の日付範囲を変更するには、次の手順を実行します。

**ステップ 1** 時間帯を設定するには、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)# clock timezone zone [-]hours [minutes]
```

ここで、*zone* 値は、時間帯を文字列で指定します。たとえば、**PST** は太平洋標準時（Pacific Standard Time）を表します。

*[-]hours* 値は、UTC との時差を時間で設定します。たとえば、PST は **-8** 時間です。

*minutes* 値は、UTC との時差を分で設定します。

**ステップ 2** 夏時間の日付範囲をデフォルトから変更するには、次のいずれかのコマンドを入力します。

定期的な日付範囲のデフォルト値は、4 月の第一日曜日の午前 2 時～10 月の最終日曜日の午前 2 時です。

- 夏時間の開始日と終了日を特定の年の特定の日付に設定するには、次のコマンドを入力します。

```
hostname(config)# clock summer-time zone date {day month | month day} year hh:mm  
{day month | month day} year hh:mm [offset]
```

このコマンドを使用する場合は、日付を毎年再設定する必要があります。

*zone* 値は、時間帯を文字列で指定します。たとえば、**PDT** は太平洋夏時間（Pacific Daylight Time）を表します。

*day* 値は、月の日付として 1～31 を設定します。使用している標準日付形式に合わせて月日を **April 1** または **1 April** のように入力することができます。

*month* 値は、月を文字列で設定します。使用する標準日付形式に合わせて月日を **April 1** または **1 April** のように入力することができます。

*year* 値は、4 桁で年を設定します（2004 など）。西暦年の範囲は 1993 ～ 2035 です。

*hh:mm* 値は、24 時間形式で、時間と分を設定します。

*offset* 値は、夏時間用に時間を変更する分数を設定します。デフォルトでは、60 分です。

- 夏時間の開始日と終了日を、ある月の日付および時刻という形式で指定し、ある年の特定の日付としては指定しない場合は、次のコマンドを入力します。

```
hostname(config)# clock summer-time zone recurring [week weekday month hh:mm week  
weekday month hh:mm] [offset]
```

このコマンドによって定期的な日付範囲が設定されるため、毎年変更する必要はありません。

*zone* 値は、時間帯を文字列で指定します。たとえば、**PDT** は太平洋夏時間（Pacific Daylight Time）を表します。

*week* 値は、月の特定の週を 1 から 4 までの整数で指定するか、**first** または **last** という単語で指定します。たとえば、日付が半端な第 5 週にあたる場合は、**last** と指定します。

*weekday* 値は、**Monday**、**Tuesday**、**Wednesday** などのように曜日を指定します。

*month* 値は、月を文字列で設定します。

*hh:mm* 値は、24 時間形式で、時間と分を設定します。

*offset* 値は、夏時間用に時間を変更する分数を設定します。デフォルトでは、60 分です。

## NTP サーバを使用する日付と時刻の設定

NTP サーバから日付と時刻を取得するには、次の手順を実行します。

### ステップ 1 NTP サーバを使用して認証を設定するには、次の手順を実行します。

- 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)# ntp authenticate
```

- 認証キー ID が信頼できるキーであると指定するには、次のコマンドを入力します。この信頼できるキーは、NTP サーバに関する認証に必要です。

```
hostname(config)# ntp trusted-key key_id
```

ここで、*key\_id* は、1 ～ 4294967295 の数字です。複数のサーバで使用する場合は複数の信頼できるキーを入力することができます。

- NTP サーバで認証を行うためのキーを設定するには、次のコマンドを入力します。

```
hostname(config)# ntp authentication-key key_id md5 key
```

ここで、*key\_id* には、**ntp trusted-key** コマンドを実行して手順 1b で設定した ID を指定し、*key* には最大 32 文字の文字列を指定します。

### ステップ 2 NTP サーバを識別するには、次のコマンドを入力します。

```
hostname(config)# ntp server ip_address [key key_id] [source interface_name] [prefer]
```

ここで、*key\_id* には、**ステップ 1b** の **ntp trusted-key** コマンドを使用して設定した ID を指定します。

*source interface\_name* には、ルーティング テーブル内のデフォルトのインターフェイスを使用しない場合に、NTP パケットを転送する発信インターフェイスを指定します。システムにはマルチコンテキスト モードのインターフェイスが含まれていないため、管理コンテキストに定義されているインターフェイス名を指定します。

**prefer** キーワードは、精度が類似する複数のサーバがある場合に、この NTP サーバを優先サーバに設定します。NTP は、アルゴリズムを使用して最も精度の高いサーバを判別し、そのサーバに同期します。複数のサーバの精度が類似している場合は、**prefer** キーワードを使用して使用するサーバを指定します。ただし、優先サーバよりはるかに精度の高いサーバがある場合は、セキュリティ アプライアンスはその精度の高いサーバを使用します。たとえば、セキュリティ アプライアンスは、優先サーバの stratum 3 の代わりに、サーバ stratum 2 を使用します。

サーバは複数指定することができ、セキュリティ アプライアンスがその中から最も精度の高いサーバを使用します。

## 手動での日付と時刻の設定

手動で日付と時刻を設定するには、次のコマンドを入力します。

```
hostname# clock set hh:mm:ss {month day | day month} year
```

ここで、*hh:mm:ss* には、24 時間形式で、時間、分、秒を設定します。たとえば、午後 8 時 54 分は **20:54:00** と設定します。

*day* 値は、月の日付として 1 ～ 31 を設定します。使用している標準日付形式に合わせて月日を **april 1** または **1 april** のように入力することができます。

*month* 値は、月を設定します。使用する標準日付形式に合わせて、月日を **april 1** または **1 april** のように入力することができます。

*year* 値は、4 桁で年を設定します（**2004** など）。西暦年の範囲は 1993 ～ 2035 です。

デフォルトの時間帯は UTC です。**clock set** コマンドを使用した後に、**clock timezone** コマンドを使用して時間帯を変更すると、設定した時刻は新しい時間帯に自動的に合せられます。

このコマンドは時刻をハードウェア チップに設定し、コンフィギュレーション ファイルには時刻を保存しません。この時刻はリブートしても保持されます。他の **clock** コマンドとは異なり、このコマンドは特権 EXEC コマンドです。クロックを再設定するには、**clock set** コマンドに新しい時刻を設定する必要があります。

## 透過ファイアウォールの管理 IP アドレスの設定

### 透過ファイアウォール モードのみ

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。セキュリティ アプライアンスで必要とされる唯一の IP コンフィギュレーションは、管理 IP アドレスの設定です。このアドレスは、システム メッセージまたは AAA サーバとの通信など、セキュリティ アプライアンス上で発信されるトラフィックの送信元アドレスとしてセキュリティ アプライアンスが使用するために必要です。このアドレスは、リモート管理アクセスにも使用できます。

マルチコンテキスト モードでは、管理 IP アドレスを各コンテキスト内に設定します。

管理 IP 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)# ip address ip_address [mask] [standby ip_address]
```

このアドレスは、アップストリーム ルータおよびダウンストリーム ルータと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。このアドレスは IPv4 でなければなりません。これは、透過ファイアウォールが IPv6 をサポートしていないためです。

フェールオーバーには、**standby** キーワードおよびアドレスを使用します。詳細については、[第 11 章「フェールオーバーの設定」](#)を参照してください。



# IP ルーティングと DHCP サービスの設定

---

この章では、セキュリティ アプライアンスの 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。次の事項について説明します。

- [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 \(P.8-20\)](#)
- [DHCP の設定 \(P.8-28\)](#)

## スタティック ルートおよびデフォルト ルートの設定

この項では、セキュリティ アプライアンスにスタティック ルートを設定する方法について説明します。

マルチコンテキスト モードではダイナミック ルーティングがサポートされていないため、ネットワークとセキュリティ アプライアンスとの間にルータが入っている場合など、セキュリティ アプライアンスに直接接続されていないネットワークでは、すべてスタティック ルートを使用する必要があります。

次の場合は、シングルコンテキスト モードでスタティック ルートを使用します。

- ネットワークで RIP または OSPF とは異なるルータ検出プロトコルを使用している。
- ネットワークが小規模でスタティック ルートを容易に管理できる。
- ルーティング プロトコルが関係するトラフィックまたは CPU のオーバーヘッドをなくす必要がある。

最も単純なオプションは、すべてのトラフィックをアップストリーム ルータに送信するようにデフォルト ルートを設定して、トラフィックのルーティングをルータに委せることです。しかし、デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティック ルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部の場合、デフォルト ルートは、セキュリティ アプライアンスに直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。

透過ファイアウォール モードでは、セキュリティ アプライアンスから直接接続されていないネットワークに宛てたトラフィック用にデフォルト ルートまたはスタティック ルートを設定して、セキュリティ アプライアンスがトラフィックの送信先インターフェイスを認識できるようにする必要があります。セキュリティ アプライアンスから発信されるトラフィックには、syslog サーバ、Websense サーバまたは N2H2 サーバ、あるいは AAA サーバとの通信もあります。1 つのデフォルト ルートで到達できないサーバがある場合、スタティック ルートを設定する必要があります。

セキュリティ アプライアンスでは、ロードバランシングのために、1 つのインターフェイスあたり最大 3 つの等コスト ルートをサポートします。

ここでは、次の項目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 ルートおよびデフォルト ルートの設定の詳細については、[P.9-5 の「IPv6 デフォルト ルートおよびスタティック ルートの設定」](#)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* および *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 ルータです。スタティック ルートに指定するアドレスは、セキュリティ アプライアンスに到達して NAT を実行する前のパケットにあるアドレスです。

*distance* は、ルートの管理ディスタンスです。値を指定しない場合、デフォルトは 1 です。管理ディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。スタティック ルートのデフォルトの管理ディスタンスは 1 で、ダイナミック ルーティング プロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPF で検出されるデフォルトの管理ディスタンスは 110 です。スタティック ルートとダイナミック ルートの管理ディスタンスが同じ場合、スタティック ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

スタティック ルートは、指定されたゲートウェイが利用できなくなってもルーティング テーブルに保持されています。指定されたゲートウェイが利用できなくなった場合は、スタティック ルートをルーティング テーブルから手動で削除する必要があります。しかし、スタティック ルートは、指定されたインターフェイスがダウンした場合はルーティング テーブルから削除されます。これらのルートは、インターフェイスが復旧すると再適用されます。



(注)

セキュリティ アプライアンスで動作中のルーティング プロトコルの管理ディスタンスよりも長い管理ディスタンスを指定してスタティック ルートを作成すると、ルーティング プロトコルで検出される指定の宛先へのルートがスタティック ルートより優先されます。スタティック ルートは、ダイナミックに検出されたルートがルーティング テーブルから削除された場合に限り使用されます。

次の例では、宛先が 10.1.1.0/24 のトラフィックがすべて、内部インターフェイスに接続されているルータ (10.1.2.45) に送信されるようにスタティック ルートを作成します。

```
hostname(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
```

インターフェイスあたり最大 3 つの等コスト ルートが同じ宛先に定義できます。複数のインターフェイス間を通る Equal Cost Multi-Path routing (ECMP; 等コスト マルチパス ルーティング) はサポートされていません。ECMP では、トラフィックはルート間で必ずしも均等に分割されません。トラフィックは、送信元と宛先の IP アドレスをハッシュするアルゴリズムに従って指定のゲートウェイ間に分散されます。

次に、外部インターフェイス上の 3 種類のゲートウェイにトラフィックを転送する等コストのスタティック ルートを設定する例を示します。セキュリティ アプライアンスは、指定された複数のゲートウェイ間にトラフィックを分散します。

```
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 ルートは、既知のルートもスタティック ルートも指定されていない IP パケットすべてを、セキュリティ アプライアンスが送信するゲートウェイの IP アドレスを特定するルートです。デフォルト ルートは、宛先の IP アドレスとして 0.0.0.0/0 が指定された単なるスタティック ルートです。特定の宛先が特定されたルートはデフォルト ルートより優先されます。

デバイスあたり最大3つの等コスト デフォルト ルート エントリを定義することができます。複数の等コスト デフォルト ルート エントリを定義すると、デフォルト ルートに送信されるトラフィックは、指定されたゲートウェイの間に分散されます。複数のデフォルト ルートを定義する場合は、各エントリに同じインターフェイスを指定する必要があります。

4 つ以上の等コスト デフォルト ルートを定義しようとした場合、またはすでに定義されているデフォルト ルートとは別のインターフェイスでデフォルト ルートを定義しようとした場合は、「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。

トンネルトラフィックには、標準のデフォルト ルートの他に別のデフォルト ルートを1つ定義することができます。**tunneled** オプションを使用してデフォルト ルートを作成すると、セキュリティ アプライアンスに着信し、既知のルートでもスタティック ルートでもルーティングできない暗号化されたトラフィックはすべて、このルートに送信されます。これ以外の暗号化されていないトラフィックには、標準のデフォルト ルート エントリが使用されます。**tunneled** オプションでは、複数のデフォルト ルートを定義することはできません。トンネルトラフィックでは ECMP がサポートされていないためです。

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 | tunneled]
```



### ヒント

宛先ネットワーク アドレスおよびマスクとして、0.0.0.0 0.0.0.0 の代わりに 0 0 と入力することができます。たとえば、次のように入力します。hostname(config)# **route** outside 0 0 192.168.1 1

次の例は、セキュリティ アプライアンスに3つの等コスト デフォルト ルートとトンネルトラフィック用のデフォルト ルート1つを設定しています。セキュリティ アプライアンスで受信した非暗号化トラフィックは、スタティック ルートも既知のルートも指定されていない場合、IP アドレスが 192.168.2.1、192.168.2.2、192.168.2.3 のゲートウェイの間に分散されます。セキュリティ アプライアンスで受信した暗号化されたトラフィックは、スタティック ルートも既知のルートも指定されていない場合、IP アドレス 192.168.2.4 のゲートウェイに転送されます。

```
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
hostname(config)# route outside 0 0 192.168.2.4 tunneled
```



## OSPF の設定

この項では、OSPF の設定方法について説明します。ここでは、次の項目について説明します。

- [OSPF の概要 \(P.8-5\)](#)
- [OSPF のイネーブル化 \(P.8-6\)](#)
- [OSPF プロセス間のルート再配布 \(P.8-7\)](#)
- [OSPF インターフェイスのパラメータの設定 \(P.8-9\)](#)
- [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 にルートを再配布する場合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 \(P.8-15\)](#)
- [ネイバーがアップ状態またはダウン状態になった時点でのロギング \(P.8-16\)](#)
- [OSPF アップデート パケットのペーシングの表示 \(P.8-16\)](#)
- [OSPF のモニタリング \(P.8-17\)](#)
- [OSPF プロセスの再始動 \(P.8-18\)](#)

## OSPF の概要

OSPF は、リンクステート アルゴリズムを使用して、すべての既知の宛先までの最短パスをビルドおよび計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

RIP に比べると OSPF は次の点で有利です。

- OSPF のリンクステート データベースのアップデート送信は RIP ほど頻繁ではなく、また、古くなった情報のタイムアウトで徐々にアップデートされるのとは異なり、リンクステート データベースは瞬時にアップデートされます。
- ルーティング決定はコストに基づいて行われます。これは、特定のインターフェイスを介してパケットを送信するためにオーバーヘッドが必要であることを示しています。セキュリティ アプライアンスは、インターフェイスのコストをリンク帯域幅に基づいて計算し、宛先までのホップ数は使用しません。コストは優先パスを指定するために設定される場合があります。

最短パス優先アルゴリズムの欠点は、CPU サイクルとメモリが大量に必要になることです。

セキュリティ アプライアンスは、OSPF プロトコルのプロセス 2 つを異なるインターフェイス セット上で同時に実行することができます。同じ IP アドレスを使用する複数のインターフェイス (NAT ではこのようなインターフェイスは共存可能ですが、OSPF ではアドレスの重複は許しません) があるときに、2 つのプロセスを実行する場合があります。あるいは、一方のプロセスを内部で実行しながら別のプロセスを外部で実行し、ルートのサブセットをこの 2 つのプロセス間で再配布する場合があります。同様に、プライベート アドレスをパブリック アドレスから分離する必要がある場合もあります。

2 つの OSPF プロセス間の再配布はサポートされています。セキュリティ アプライアンスの OSPF 対応インターフェイスに設定されているスタティック ルートおよび接続されているルートも OSPF プロセスに再配布できます。OSPF がイネーブルになっている場合は、セキュリティ アプライアンスで RIP をイネーブルにすることはできません。RIP と OSPF の間での再配布はサポートされていません。

セキュリティ アプライアンスでは、次の OSPF の機能がサポートされています。

- エリア内ルート、エリア間ルート、および外部ルート（タイプ I とタイプ II）のサポート
- 仮想リンクのサポート
- OSPF の LSA フラッディング
- OSPF パケットの認証（パスワード認証と MD5 認証の両方）
- セキュリティ アプライアンスの代表ルータまたは代表バックアップ ルータとしての設定のサポート。セキュリティ アプライアンスは、ABR としてもセットアップできます。しかし、セキュリティ アプライアンスを ASBR として設定するための機能は、デフォルト情報に限定されています（デフォルト ルートの挿入など）。
- スタブ エリアと not so stubby エリア（NSSA）のサポート
- エリア境界ルータのタイプ 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メント

## 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、このルーティング プロセスに関連付ける IP アドレスの範囲を指定し、さらにその IP アドレスの範囲にエリア ID を割り当てる必要があります。



(注)

RIP がイネーブルになっている場合は、OSPF をイネーブルにすることはできません。

OSPF をイネーブルにするには、次の手順を実行します。

**ステップ 1** OSPF ルーティング プロセスを作成するには、次のコマンドを入力します。

```
hostname(config)# router ospf process_id
```

このコマンドは、この OSPF プロセスのルータ コンフィギュレーション モードを入力します。

*process\_id* は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

**ステップ 2** OSPF が動作する IP アドレスを定義し、そのインターフェイスのエリア ID を定義するには、次のコマンドを入力します。

```
hostname(config-router)# network ip_address mask area area_id
```

OSPF をイネーブルにする方法を次に示します。

```
hostname(config)# router ospf 2
hostname(config-router)# network 10.0.0.0 255.0.0.0 area 0
```

## OSPF プロセス間のルート再配布

セキュリティ アプライアンスは、OSPF ルーティング プロセス間のルート再配布を制御できます。セキュリティ アプライアンスは、**redistribute** コマンドまたはルートマップの設定に基づいてルートの照合および変更を行います。ルートマップのこれ以外の使用方法については、[P.8-14](#) の「[デフォルト ルートの生成](#)」も参照してください。

**(注)**

セキュリティ アプライアンスは、ルーティング プロトコル間ではルートを再配布できません。しかし、セキュリティ アプライアンスは、スタティック ルートおよび接続されているルートは再配布できます。

ここでは、次の項目について説明します。

- ルートマップの追加 ([P.8-7](#))
- スタティック ルート、接続されているルート、または OSPF ルートを OSPF プロセスに再配布する方法 ([P.8-8](#))

### ルートマップの追加

ルートマップを定義するには、次の手順を実行します。

**ステップ 1** ルートマップの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)# route-map name {permit | deny} [sequence_number]
```

ルートマップのエントリは順番に読み取られます。順序は *sequence\_number* オプションを使用して識別します。このオプションを使用しないと、セキュリティ アプライアンスはユーザがエントリを追加したときの順序を使用します。

**ステップ 2** 次に挙げる **match** コマンドのうち、1つ以上を入力します。

- 標準の ACL に一致する宛先ネットワークを持つ任意のルートを照合するには、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 ACL を指定する場合、ルートは任意の ACL を照合できます。

- 指定したメトリックを持つ任意のルートを照合するには、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 ~ 4294967295 が指定できます。

- 標準の ACL に一致するネクストホップ ルータ アドレスを持つ任意のルートを照合するには、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 ACL を指定する場合、ルートは任意の ACL を照合できます。

- 指定したネクストホップ インターフェイスを持つ任意のルートを照合するには、次のコマンドを入力します。

```
hostname(config-route-map)# match interface if_name
```

2 つ以上のインターフェイスを指定する場合、ルートはいずれかのインターフェイスと一致します。

- 標準の ACL と一致するルータによってアドバタイズされている任意のルートを照合するには、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 ACL を指定する場合、ルートは任意の ACL を照合できます。

- ルート タイプを照合するには、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 つ以上の set コマンドを入力します。

ルートが **match** コマンドで一致する場合は、次の **set** コマンドによって、ルートを再配布する前にルートで実行するアクションが決まります。

- メトリックを設定するには、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 ～ 294967295 の値が指定できます。

- メトリック タイプを設定するには、次のコマンドを入力します。

```
hostname(config-route-map)# set metric-type {type-1 | type-2}
```

次の例は、ホップ カウント 1 でルートを再配布する方法を示します。セキュリティ アプライアンスは、これらのルートをメトリック 5、メトリック タイプ 1、およびタグ 1 で外部 LSA として再配布します。

```
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
```

## スタティック ルート、接続されているルート、または OSPF ルートを OSPF プロセスに再配布する方法

スタティック ルート、接続されているルート、または OSPF ルートのあるプロセスから別の OSPF プロセスに再配布するには、次の手順を実行します。

- ステップ 1** まだ移行していない場合、次のコマンドを入力して、再配布する OSPF プロセスのルータ コンフィギュレーション モードに移行します。

```
hostname(config)# router ospf process_id
```

- ステップ 2** 再配布するルートを指定するには、次のコマンドを入力します。

```
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* キーワード、**static** キーワード、および **connect** キーワードは、ルートの再配布元を指定します。

このコマンドにルート プロパティを照合および設定するためのオプションを使用するか、ルートマップを使用します。**tag** オプションおよび **subnets** オプションは、**route-map** コマンドで使用する場合と同じではありません。**redistribute** コマンドでルートマップとオプションの両方を使用した場合、これらは一致している必要があります。

次に、ルートをメトリック 1 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 にルートを再配布する例を示します。セキュリティ アプライアンスは、これらのルートを、メトリック 5、メトリック タイプ 1、およびタグ 1 で外部 LSA として再配布します。

```
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、指定された OSPF プロセスのルートを OSPF プロセス 109 に再配布する例を示します。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 に指定され、メトリック タイプが外部に設定されているルートの再配布の例を示します。外部というのは、内部メトリックより優先順位が低いことを示します。

```
hostname(config)# router ospf 1
hostname(config-router)# redistribute ospf 2 metric 5 metric-type external
```

## OSPF インターフェイスのパラメータの設定

インターフェイス固有の OSPF パラメータは、必要に応じて変更することができます。これらのパラメータは必ずしも変更する必要はありませんが、**ospf hello-interval**、**ospf dead-interval**、および **ospf authentication-key** というインターフェイス パラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータのいずれかを設定する場合は、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適合する値にするようにしてください。

OSPF インターフェイス パラメータを設定するには、次の手順を実行します。

**ステップ 1** インターフェイス コンフィギュレーション モードに入るには、次のコマンドを入力します。

```
hostname(config)# interface interface_name
```

**ステップ 2** 次のいずれかのコマンドを入力します。

- インターフェイスの認証タイプを指定するには、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中のネットワーク セグメントに存在する隣接 OSPF ルータで使用されるパスワードを割り当てるには、次のコマンドを入力します。

```
hostname(config-interface)# ospf authentication-key key
```

*key* には、最大 8 バイトの連続する文字列が指定できます。

このコマンドで作成するパスワードはキーとして使用され、このキーはセキュリティ アプライアンスのソフトウェアによるルーティング プロトコル パケットの発信時に OSPF ヘッダーに直接挿入されます。各ネットワークにはインターフェイスごとに個別のパスワードを割り当てることができます。OSPF 情報が交換できるためには、同じネットワーク上の隣接ルータはすべて、同じパスワードを持つ必要があります。

- パケット送信のコストを OSPF インターフェイスに明示的に指定するには、次のコマンドを入力します。

```
hostname(config-interface)# ospf cost cost
```

*cost* は、1 ～ 65535 の整数です。

- hello パケットが受信されなかったために、隣接 OSPF ルータがダウンしているとデバイスが宣言する場合に必要な待機時間を秒数で設定するには、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同じにする必要があります。

- セキュリティ アプライアンスが OSPF インターフェイスから hello パケットを送信する時間間隔を指定するには、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同じにする必要があります。

- 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* : 範囲 1 ～ 255 の識別子
- *key* : 最大 16 バイトの英数字によるパスワード

通常は、インターフェイスあたり 1 つのキーを使用して、パケット送信時に認証情報を生成するとともに着信パケットを認証します。隣接ルータの同一キー識別子は、キー値を同一にする必要があります。

1 インターフェイスで 2 つ以上のキーを保持しないことをお勧めします。新しいキーを追加したらその都度古いキーを削除して、ローカル システムが古いキー情報を持つ悪意のあるシステムと通信を続けることのないようにしてください。古いキーを削除すると、ロールオーバー中のオーバーヘッドを減らすことにもなります。

- ネットワークの OSPF 代表ルータを決定するための優先順位を設定するには、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する隣接ルータに LSA を再送信する間隔を秒数で指定するには、次のコマンドを入力します。

```
hostname(config-interface)# ospf retransmit-interval seconds
```

*seconds* は、接続されているネットワーク上の任意の 2 ルータ間で予想されるラウンドトリップ遅延より長い秒数でなければなりません。範囲は 1 ～ 65535 秒です。デフォルトは、5 秒です。

- OSPF インターフェイスでリンクステート アップデート パケットを送信するのに必要な予想時間を秒数で設定するには、次のコマンドを入力します。

```
hostname(config-interface)# ospf transmit-delay seconds
```

*seconds* は、1 ～ 65535 秒です。デフォルトは 1 秒です。

次の例は、OSPF インターフェイスの設定方法を示しています。

```
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 パラメータを設定することができます。これらのエリア パラメータ（後述のタスク テーブルに表示）には、認証の設定、スタブ エリアの定義、デフォルト サマリー ルートへの特定のコストの割り当てがあります。認証では、エリアへの不正アクセスに対してパスワードベースで保護します。

スタブ エリアは、外部ルートが送信されないエリアです。その代わりに、ABR で生成されるデフォルトの外部ルートがあり、このルートは自律システムの外部の宛先としてスタブ エリアに送信されます。OSPF スタブ エリアのサポートを活用するには、デフォルトのルーティングをスタブ エリアで使用する必要があります。スタブ エリアに送信される LSA の数をさらに減らすには、ABR で実行する **area stub** コマンドに **no-summary** キーワードを設定して、スタブ エリアにサマリー リンク アドバタイズメント（LSA タイプ 3）が送信されないようにします。

ネットワークにエリア パラメータを指定するには、次の手順を実行します。

- ステップ 1** まだ移行していない場合、次のコマンドを入力して、設定する OSPF プロセスのルータ コンフィギュレーション モードに移行します。

```
hostname(config)# router ospf process_id
```

- ステップ 2** 次のいずれかのコマンドを入力します。

- 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 エリアに定義するには、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 サマリー 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 ～ 65535 の整数です。デフォルトは 1 です。

次の例は、OSPF エリア パラメータの設定方法を示しています。

```
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

Not-So-Stubby Area (NSSA) の OSPF への実装は、OSPF のスタブ エリアに似ています。NSSA は、タイプ 5 の外部 LSA をコアからエリアにフラッドिंगすることはありませんが、自律システムの外部ルートのある限られた方法でエリア内にインポートできます。

NSSA は、再配布によって、タイプ 7 の自律システムの外部ルートを NSSA エリア内部にインポートします。これらのタイプ 7 の LSA は、NSSA の ABR によってタイプ 5 の LSA に変換され、ルーティング ドメイン全体にフラッドिंगされます。変換中は集約とフィルタリングがサポートされます。

OSPF を使用する中央サイトから異なるルーティング プロトコルを使用するリモート サイトに接続しなければならない ISP またはネットワーク管理者は、NSSA を使用することによって管理を簡略化できます。

NSSA が実装される前は、企業サイトの境界ルータとリモート ルータ間の接続では、OSPF スタブ エリアとしては実行されませんでした。これは、リモート サイト向けのルートは、スタブ エリアに再配布することができず、2 種類のルーティング プロトコルを維持する必要があったためです。RIP のようなシンプルなプロトコルを実行して再配布を処理する方法が一般的でした。NSSA が実装されたことで、企業ルータとリモート ルータ間のエリアを NSSA として定義することにより、NSSA で OSPF を拡張してリモート接続をカバーすることができます。



OSPF NSSA を設定するために必要なエリア パラメータをネットワークに指定するには、次の手順を実行します。

- ステップ 1** まだ移行していない場合、次のコマンドを入力して、設定する OSPF プロセスのルータ コンフィギュレーション モードに移行します。

```
hostname(config)# router ospf process_id
```

- ステップ 2** 次のいずれかのコマンドを入力します。

- 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]
```

- アドレスの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 テーブルのサイズを減らすのに役立ちます。OSPF でこのコマンドを使用すると、このアドレスでカバーされる再配布ルートすべての集約として、1 つの外部ルートが OSPF ASBR からアドバタイズされます。

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、サマリー アドレスの 10.1.0.0 に、10.1.1.0、10.1.2.0、10.1.3.0 などのアドレスが含まれます。外部のリンク状態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、次のガイドラインを参考にしてください。

- 外部の宛先に到達するために、タイプ 7 のデフォルト ルートを設定できる。設定すると、NSSA または NSSA エリア境界ルータまでのタイプ 7 のデフォルトがルータによって生成されます。
- 同じエリア内にあるルータはすべて、このエリアが NSSA であることに同意しなければなりません。そうでないと、ルータは通信できなくなります。

## OSPF エリア間のルート集約の設定

ルート集約は、アドバタイズされるアドレスを統合することです。この機能を実行すると、1 つのサマリー ルートがエリア境界ルータを通して他のエリアにアドバタイズされます。OSPF のエリア境界ルータは、ネットワークをある 1 つのエリアから別のエリアへとアドバタイズしていきます。あるエリアにおいて連続する複数のネットワーク番号が割り当てられている場合、指定された範囲に含まれるエリア内の個別のネットワークをすべてカバーするサマリー ルートをアドバタイズするようにエリア境界ルータを設定することができます。

ルート集約のアドレス範囲を定義するには、次の手順を実行します。

- ステップ 1** まだ移行していない場合、次のコマンドを入力して、設定する OSPF プロセスのルータ コンフィギュレーション モードに移行します。

```
hostname(config)# router ospf process_id
```

**ステップ2** アドレス範囲を設定するには、次のコマンドを入力します。

```
hostname(config-router)# area area-id range ip-address mask [advertise |  
not-advertise]
```

次の例は、OSPF エリア間のルート集約の設定方法を示しています。

```
hostname(config)# router ospf 1  
hostname(config-router)# area 17 range 12.1.0.0 255.255.0.0
```

## OSPF にルート を再配布する場合のルート集約の設定

他のプロトコルからのルートを OSPF に再配布する場合、各ルートは外部 LSA で個別にアドバタイズされます。その一方で、指定したネットワークアドレスとマスクでカバーされる再配布ルートすべてに対して 1 つのルートをアドバタイズするようにセキュリティ アプライアンスを設定することができます。このコンフィギュレーションによって OSPF リンクステート データベースのサイズが小さくなります。

ネットワーク アドレスとマスクでカバーされる再配布ルートすべてに対して 1 つのサマリー ルートをアドバタイズするようにソフトウェアを設定するには、次の手順を実行します。

**ステップ1** まだ移行していない場合、次のコマンドを入力して、設定する OSPF プロセスのルータ コンフィギュレーション モードに移行します。

```
hostname(config)# router ospf process_id
```

**ステップ2** サマリー 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-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。

次の例は、ルート集約の設定方法を示しています。サマリー アドレスの 10.1.0.0 には、10.1.1.0、10.1.2.0、10.1.3.0 などのアドレスが含まれます。外部のリンク状態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 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

自律システムの境界ルータによって、デフォルト ルートが OSPF ルーティング ドメインに必ず生成されるようにすることができます。ルートを OSPF ルーティング ドメインに再配布するように特に設定すると、ルータは自動的に自律システム境界ルータになります。しかし、自律システム境界ルータは、デフォルトでは OSPF ルーティング ドメインにデフォルト ルートを生成しません。

デフォルト ルートを生成するには、次の手順を実行します。

- ステップ 1** まだ移行していない場合、次のコマンドを入力して、設定する OSPF プロセスのルータ コンフィギュレーション モードに移行します。

```
hostname(config)# router ospf process_id
```

- ステップ 2** 自律システム境界ルータでデフォルト ルートが必ず生成されるようにするには、次のコマンドを入力します。

```
hostname(config-router)# default-information originate [always] [metric metric-value]  
[metric-type {1 | 2}] [route-map map-name]
```

次の例は、デフォルト ルートの生成方法を示しています。

```
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 によるトポロジ変更受信と最短パス優先（SPF）計算開始との間の遅延時間が設定できます。最初に SPF を計算してから次に計算するまでの保持時間も設定できます。

ルート計算タイマーを設定するには、次の手順を実行します。

- ステップ 1** まだ移行していない場合、次のコマンドを入力して、設定する OSPF プロセスのルータ コンフィギュレーション モードに移行します。

```
hostname(config)# router ospf process_id
```

- ステップ 2** ルート計算時刻を設定するには、次のコマンドを入力します。

```
hostname(config-router)# timers spf spf-delay spf-holdtime
```

**spf-delay** は、OSPF によるトポロジ変更受信と SPF 計算開始との間の遅延時間（秒）です。0 ～ 65535 の整数を使用できます。デフォルトの時間は 5 秒です。値の 0 は遅延がないことを意味します。つまり、SPF 計算はただちに開始されます。

**spf-holdtime** は、2 つの連続する SPF 計算の間の最短時間（秒）です。0 ～ 65535 の整数を使用できます。デフォルトの時間は 10 秒です。値の 0 は遅延がないことを意味します。つまり、2 回の SPF 計算がすぐに続けて行われます。

次の例は、ルート計算タイマーの設定方法を示しています。

```
hostname(config)# router ospf 1  
hostname(config-router)# timers spf 10 120
```

## ネイバーがアップ状態またはダウン状態になった時点でのロギング

デフォルトでは、システムは OSPF ネイバーがアップ状態またはダウン状態になったときにシステムメッセージを送信します。

アップ状態またはダウン状態になった OSPF ネイバーについて、**debug ospf adjacency** コマンドを実行せずに確認する必要がある場合に、このコマンドを設定します。**log-adj-changes router** 設定コマンドでは、少ない出力によってピアの関係が高いレベルで表示されます。それぞれの状態変化メッセージを確認する場合は、**log-adj-changes detail** を設定します。

アップ状態またはダウン状態になったネイバーをログに記録するには、次の手順を実行します。

- ステップ 1** まだ移行していない場合、次のコマンドを入力して、設定する OSPF プロセスのルータ コンフィギュレーション モードに移行します。

```
hostname(config)# router ospf process_id
```

- ステップ 2** アップ状態またはダウン状態になったネイバーに対するロギングを設定するには、次のコマンドを入力します。

```
hostname(config-router)# log-adj-changes [detail]
```



(注)

ネイバーのアップまたはダウンのメッセージが送信されるには、ロギングがイネーブルになっている必要があります。

次の例は、ネイバーのアップまたはダウンのメッセージをログに記録する方法を示しています。

```
hostname(config)# router ospf 1  
hostname(config-router)# log-adj-changes detail
```

## OSPF アップデート パケットのペーシングの表示

OSPF アップデート パケットは、自動的にペーシングされるため、各パケットの送信間隔が 33 ミリ秒未満になることはありません。ペーシングを行わないと、リンクが低速の状態アップデート パケットの一部が失われたり、ネイバーがアップデートを十分すばやく受信できなくなったり、あるいは、ルータがバッファ スペースを使い切ってしまったことがあります。たとえば、ペーシングを行わないと、次のいずれかのトポロジが存在した場合にパケットがドロップされる可能性があります。

- 高速ルータがポイントツーポイント リンクを介して低速のルータと接続している。
- フラッドイング中に、複数のネイバーから 1 つのルータに同時にアップデートが送信される。

ペーシングは、再送信間でも、送信効率を高めて再送信パケットの損失を最小にするために利用されます。インターフェイスへの送信を待機している LSA を表示することもできます。ペーシングの利点は、OSPF アップデートおよび再送信パケットの送信の効率をよくすることです。

この機能を設定するタスクはありません。自動的に行われます。

指定したインターフェイスを通したフラッディングを待機している LSA のリストを表示して OSPF パケットのペーシングを観察するには、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 テーブルの内容、キャッシュの内容、およびデータベースの内容など、特定の統計情報を表示することができます。提供される情報は、リソースの使用状況を判定してネットワークの問題を解決するために使用することができます。また、ノードの到達可能性情報を表示して、デバイス パケットがネットワークを通過するときにとるルーティングパスを見つけることもできます。

さまざまな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タスクを実行します。

- 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 までの内部 OSPF ルーティング テーブル 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
```

- 特定のルータの OSPF データベースに関連する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 [area-id]] database
```

- インターフェイスへのフラッディングを待機している LSA のリストを表示するには（OSPF パケット ペーシングの観察のため）、次のコマンドを入力します。

```
hostname# show ospf flood-list if-name
```

- OSPF に関連する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 ネイバー情報をインターフェイスごとに表示するには、次のコマンドを入力します。

```
hostname# show ospf neighbor [interface-name] [neighbor-id] [detail]
```

- ルータで要求される LSA すべて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
```

- 再送信を待機している LSA すべて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 プロセスで設定されているサマリー アドレスの再配布情報すべて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 に関連する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 プロセスの再始動

OSPF プロセスを再始動して、再配布またはカウンタをクリアするには、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

この項では、RIP の設定方法について説明します。ここでは、次の項目について説明します。

- [RIP の概要 \(P.8-18\)](#)
- [RIP のイネーブル化 \(P.8-19\)](#)

### RIP の概要

RIP をサポートしているデバイスは、ネットワークのトポロジが変更されると、ルーティングアップデート メッセージを所定の間隔で送信します。これらの RIP パケットには、デバイスが到達可能なネットワークに関する情報、さらに宛先アドレスに到達するためにパケットが通過しなければならないルータやゲートウェイの数が含まれています。RIP では、生成されるトラフィックは OSPF より多くなりますが、初期設定は OSPF より容易です。

RIP は、初期コンフィギュレーションが簡単で、トポロジが変更されても設定をアップデートする必要がないため、スタティック ルーティングより有利です。RIP の欠点は、ネットワーク数や処理オーバーヘッドがスタティック ルーティングより大きいことです。

セキュリティ アプライアンスは、一部のバージョンの RIP のみ使用します。このバージョンの RIP は、セキュリティ アプライアンスが到達可能なネットワークを識別する RIP アップデートを送信しません。ただし、次のいずれかまたは両方の方法をイネーブルにすることができます。

- パッシブ RIP：セキュリティ アプライアンスは RIP アップデートを受信しますが、ネットワークに関するいかなるアップデートもインターフェイスから送信しません。  
パッシブ RIP では、セキュリティ アプライアンスは、直接接続されていないネットワークについて知ることができます。
- デフォルト ルート アップデート：セキュリティ アプライアンスを通じて到達可能なすべてのネットワークが記述された通常の RIP アップデートを送信するのではなく、セキュリティ アプライアンスは、セキュリティ アプライアンスをデフォルトのゲートウェイとして識別する、参加デバイスへのデフォルト 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 とともに使用することも、単独で使用することもできます。セキュリティ アプライアンスでスタティック ルートを使用するがダウンストリーム ルータにはスタティック 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。一般に、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。これは、通常、セキュリティ アプライアンスはアップストリーム ルータに対するデフォルト ゲートウェイではないためです。

## RIP のイネーブル化

インターフェイスで 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 interface_name {default | passive} [version {1 | 2}
[authentication {text | md5} key key_id]]
```

**rip** コマンドを 2 回入力することで、1 つのインターフェイスでパッシブとデフォルトの両モードの RIP をイネーブルにすることができます。このとき、それぞれのモードを 1 回ずつ入力します。たとえば、次のコマンドを入力します。

```
hostname(config)# rip inside default version 2 authentication md5 scorpious 1
hostname(config)# rip inside passive version 2 authentication md5 scorpious 1
```

すべてのインターフェイスでパッシブ RIP をイネーブルにするが、内部インターフェイスではデフォルト ルートをイネーブルにするだけの場合は、次のコマンドを入力します。

```
hostname(config)# rip inside default version 2 authentication md5 scorpious 1
hostname(config)# rip inside passive version 2 authentication md5 scorpious 1
hostname(config)# rip outside passive version 2 authentication md5 scorpious 1
```



(注)

コンフィギュレーションをテストする前に、セキュリティ アプライアンスに接続されているルータすべての ARP キャッシュを消去してください。シスコ ルータに **clear arp** コマンドを発行して ARP キャッシュを消去します。

OSPF がイネーブルになっている場合は、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

この項では、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。ここでは、次の項目について説明します。

- [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 \(P.8-21\)](#)
- [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 \(P.8-25\)](#)
- [PIM 機能の設定 \(P.8-25\)](#)
- [マルチキャスト ルーティングの参考資料 \(P.8-27\)](#)

### マルチキャスト ルーティングの概要

セキュリティ アプライアンスは、スタブ マルチキャスト ルーティングと PIM マルチキャスト ルーティングの両方をサポートしています。しかし、1 つのセキュリティ アプライアンスに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 ルーティングは、ダイナミック ホスト登録の機能を提供して、マルチキャスト ルーティングを容易にします。スタブ マルチキャスト ルーティングを設定すると、セキュリティ アプライアンスは IGMP のプロキシ エージェントとして動作します。セキュリティ アプライアンスは、マルチキャスト ルーティングに全面的に参加するのではなく、IGMP メッセージをアップストリームのマルチキャスト ルータに転送し、そのルータがマルチキャスト データの送信をセットアップします。スタブ マルチキャスト ルーティングを設定する場合は、セキュリティ アプライアンスを PIM として設定することはできません。

セキュリティ アプライアンスは、PIM-SM および双方向 PIM の両方をサポートしています。PIM-SM は、基盤となるユニキャスト ルーティング情報ベースまたは別のマルチキャスト 対応ルーティング情報ベースを使用するマルチキャスト ルーティング プロトコルです。このプロトコルは、マルチキャスト グループあたり 1 つのランデブー ポイントをルートにした単方向の共有ツリーを構築し、オプションでマルチキャストの発信元ごとに最短パス ツリーを作成します。

双方向 PIM は PIM-SM の変形で、マルチキャストの発信元と受信者を接続する双方向の共有ツリーを構築します。双方向ツリーは、マルチキャスト トポロジの各リンクで動作する DF 選定プロセスを使用して構築されます。DF に支援されたマルチキャスト データは発信元からランデブー ポイントに転送されます。この結果、マルチキャスト データは発信元固有の状態を必要せず、共有ツリーをたどって受信者に送信されます。DF 選定はランデブー ポイントの検出中に行われ、これによってデフォルト ルートがランデブー ポイントに提供されます。



(注)

セキュリティ アプライアンスが PIM RP の場合は、セキュリティ アプライアンス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てください。



## マルチキャスト ルーティングのイネーブル化

マルチキャスト ルーティングをイネーブルにすると、セキュリティ アプライアンスからマルチキャスト パケットが転送されます。マルチキャスト ルーティングをイネーブルにすると、すべてのインターフェイスで PIM および 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 の量によって制限されます。表 8-1 は、セキュリティ アプライアンスの RAM の量に基づいて、固有のマルチキャスト テーブルの最大エントリ数を示しています。この上限に達すると、新しいエントリは廃棄されます。

表 8-1 マルチキャスト テーブルのエントリ数の上限

| テーブル      | 16 MB | 128 MB | 128 + MB |
|-----------|-------|--------|----------|
| MFIB      | 1000  | 3000   | 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、自身のグループ メンバーシップを直接接続されているマルチキャスト ルータに報告するために IGMP を使用します。IGMP は、グループ アドレス（Class D IP アドレス）をグループ 識別子として使用します。ホスト グループ アドレスは、224.0.0.0 ～ 239.255.255.255 の範囲で使用できます。アドレス 224.0.0.0 がグループに割り当てられることはありません。アドレス 224.0.0.1 は、サブネットのシステムすべてに割り当てられます。アドレス 224.0.0.2 は、サブネットのルータすべてに割り当てられます。

セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにすると、IGMP バージョン 2 がすべてのインターフェイスで自動的にイネーブルになります。



(注)

**show run** コマンドを使用すると、インターフェイス コンフィギュレーションには **no igmp** コマンドだけが表示されます。デバイス コンフィギュレーションに **multicast-routing** コマンドがあると、IGMP がすべてのインターフェイスで自動的にイネーブルになります。

この項では、インターフェイスごとにオプションの IGMP 設定を行う方法について説明します。ここでは、次の項目について説明します。

- インターフェイスにおける IGMP のディセーブル化 (P.8-22)
- グループ メンバーシップの設定 (P.8-22)
- グループのスタティック加入の設定 (P.8-22)
- マルチキャスト グループへのアクセスの制御 (P.8-23)
- インターフェイスにおける IGMP 状態の数の制限 (P.8-23)
- クエリー間隔およびクエリー タイムアウトの修正 (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)

## インターフェイスにおける IGMP のディセーブル化

IGMP は、特定のインターフェイスでディセーブルにできます。この機能は、マルチキャスト ホストが存在しないことが分かっている特定のインターフェイスにセキュリティ アプライアンスからホスト クエリー メッセージを送信しないようにする場合に便利です。

インターフェイスで IGMP をディセーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# no igmp
```

インターフェイスで IGMP 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-if)# igmp
```



(注)

インターフェイス コンフィギュレーションには、**no igmp** コマンドだけが表示されます。

## グループ メンバーシップの設定

セキュリティ アプライアンスをマルチキャスト グループのメンバーとして設定できます。マルチキャスト グループに加入するようにセキュリティ アプライアンスを設定すると、アップストリーム ルータはそのグループのマルチキャスト ルーティング テーブル情報を維持して、このグループをアクティブにするパスを保持します。

セキュリティ アプライアンスがマルチキャスト グループに加入するように設定するには、次のコマンドを入力します。

```
hostname(config-if)# igmp join-group group-address
```

## グループのスタティック加入の設定

ときには、グループ メンバーがグループにおける自分のメンバーシップを報告できなかったり、あるいは、ネットワーク セグメントにメンバーが存在しなかったりすることもあります。それでも、そのグループのマルチキャスト トラフィックをそのネットワーク セグメントに送信することが必要になる場合があります。このようなグループのマルチキャスト トラフィックは、次のいずれかの方法でそのセグメントに送信することができます。

- **igmp join-group** コマンドを使用する (P.8-22 の「グループ メンバーシップの設定」を参照)。これによって、セキュリティ アプライアンスはマルチキャスト パケットを受け入れ、転送します。
- **igmp static-group** コマンドを使用する。セキュリティ アプライアンスは、マルチキャスト パケットを受け入れないものの、指定したインターフェイスに転送します。

インターフェイス上のマルチキャスト グループにスタティックに加入する設定を行うには、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

セキュリティ アプライアンス インターフェイスのホストが加入可能なマルチキャスト グループを制御するには、次の手順を実行します。

**ステップ 1** 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することができます。拡張アクセスリストまたは標準アクセスリストが使用できます。

- 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** インターフェイスにアクセスリストを適用するには、次のコマンドを入力します。

```
hostname(config-if)# igmp access-group acl
```

*acl* 引数は、標準 IP アクセスリストまたは拡張 IP アクセスリストの名前です。

## インターフェイスにおける IGMP 状態の数の制限

IGMP メンバーシップ報告の結果の IGMP 状態の数は、インターフェイスごとに制限することができます。設定された上限を超過したメンバーシップ報告は IGMP キャッシュに入力されず、超過した分のメンバーシップ報告のトラフィックは転送されません。

インターフェイスでの IGMP 状態の数を制限するには、次のコマンドを入力します。

```
hostname(config-if)# igmp limit number
```

有効な値の範囲は 0 ～ 500 です。デフォルト値は 500 です。この値を 0 に設定すると、既知のグループは追加されなくなりますが、手動で定義したメンバーシップ (**igmp join-group** コマンドおよび **igmp static-group** コマンドを使用) は引き続き許可されます。このコマンドの **no** 形式を使用するとデフォルト値が復元されます。

## クエリー間隔およびクエリー タイムアウトの修正

セキュリティ アプライアンスは、クエリー メッセージを送信して、インターフェイスに接続されているネットワークにメンバーを持つマルチキャスト グループを検出します。メンバーは、IGMP 報告メッセージで応答して、特定のグループに対するマルチキャスト パケットの受信を希望していることを示します。クエリー メッセージは、アドレスが 224.0.0.1 で存続可能時間値が 1 の全システム マルチキャスト グループ宛に送信されます。

これらのメッセージが定期的に送信されることにより、セキュリティ アプライアンスに保存されているメンバーシップ情報はリフレッシュされます。セキュリティ アプライアンスで、ローカル メンバーがいなくなったマルチキャスト グループがまだインターフェイスに接続されていることが分かったら、そのグループへのマルチキャスト パケットを接続されているネットワークに転送するのを停止し、そのパケットの送信元にプルーニングメッセージを戻します。

デフォルトでは、サブネット上の PIM 代表ルータがクエリー メッセージの送信を担当します。このメッセージは、デフォルトでは 125 秒間に 1 回送信されます。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
```

セキュリティ アプライアンスは、インターフェイスでクエリー メッセージが指定されているタイムアウト値（デフォルトでは 255 秒）の間に検出できなかった場合は、代表ルータとなってクエリー 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** コマンドおよび **igmp query-interval** コマンドを実行するには、IGMP バージョン 2 が必要です。

## 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。セキュリティ アプライアンスがこの時間内にホスト クエリーの応答を受信しなかった場合、グループを削除します。

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、セキュリティ アプライアンスは IGMP バージョン 2 を実行します。このバージョンでは、**igmp query-timeout** コマンドや **igmp query-interval** コマンドなどのいくつかの追加機能が使用できます。

サブネットのマルチキャスト ルータはすべて、同じ IGMP バージョンをサポートしている必要があります。セキュリティ アプライアンスは、バージョン 1 のルータを自動的に検出し、バージョン 1 に切り替えることはありません。しかし、サブネットに IGMP のバージョン 1 のホストとバージョン 2 のホストが混在しても問題はありません。IGMP バージョン 2 を実行しているセキュリティ アプライアンスは、IGMP バージョン 1 のホストが存在しても正常に動作します。

インターフェイスで動作中の IGMP のバージョンを制御するには、次のコマンドを入力します。

```
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動作しているセキュリティ アプライアンスは、PIM に参加する必要はありません。その代わりに、そのセキュリティ アプライアンスを IGMP プロキシ エージェントとして設定すると、あるインターフェイスに接続されているホストから、別のインターフェイスのアップストリーム マルチキャスト ルータに IGMP メッセージを転送することができます。セキュリティ アプライアンスを IGMP プロキシ エージェントとして設定するには、ホスト加入 (join) メッセージおよびホスト脱退 (leave) メッセージをスタブ エリアからアップストリーム インターフェイスに転送します。

ホスト加入メッセージおよびホスト脱退メッセージを転送するには、スタブエリアに接続されているインターフェイスから次のコマンドを入力します。

```
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、セキュリティ アプライアンスは、ユニキャスト パケットを発信元に返送するのと同じインターフェイスでパケットを受信することを想定しています。マルチキャスト ルーティングをサポートしていないルートをバイパスする場合などは、ユニキャスト パケットで 1 つのパスを使用し、マルチキャスト パケットで別の 1 つのパスを使用することもあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

PIM 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 ルーティングで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維持します。セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにすると、PIM および IGMP がすべてのインターフェイスで自動的にイネーブルになります。



(注)

PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

この項では、オプションの PIM 設定を行う方法について説明します。ここでは、次の項目について説明します。

- インターフェイスにおける PIM のディセーブル化 (P.8-26)
- スタティック ランデブー ポイント アドレスの設定 (P.8-26)
- 代表ルータの優先順位の設定 (P.8-27)
- PIM 登録メッセージのフィルタリング (P.8-27)
- PIM メッセージ間隔の設定 (P.8-27)

## インターフェイスにおける PIM のディセーブル化

PIM は、特定のインターフェイスでディセーブルにできます。インターフェイスで 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
```

インターフェイスで PIM 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-if)# pim
```



(注)

インターフェイス コンフィギュレーションには、**no pim** コマンドだけが表示されます。

## スタティック ランデブー ポイント アドレスの設定

共通の PIM 希薄モードまたは双方向ドメイン内のルータはすべて、PIM RP アドレスを認識している必要があります。このアドレスは、**pim rp-address** コマンドを使用してスタティックに設定されます。



(注)

セキュリティ アプライアンスは、Auto-RP または PIM BSR をサポートしていません。RP アドレスを指定するには、**pim rp-address** コマンドを使用する必要があります。

セキュリティ アプライアンスを複数のグループの RP として機能するように設定することができます。アクセスリストに指定されているグループ範囲によって、PIM RP のグループ マッピングが決まります。アクセスリストが指定されていない場合は、マルチキャスト グループ全体の範囲 (224.0.0.0/4) にグループの RP が適用されます。

PIM RP 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 とともに使用する必要があるマルチキャスト グループを定義している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 希薄モードで動作するようになります。



(注)

セキュリティ アプライアンスは、実際の双方向構成にかかわらず、PIM の hello メッセージを使用して双方向の機能を常時アドバタイズします。

## 代表ルータの優先順位の設定

Designated Router (DR; 代表ルータ) は、PIM 登録メッセージ、PIM 加入メッセージ、およびプルニングメッセージの RP への送信を担当します。ネットワーク セグメントに 2 つ以上のマルチキャスト ルータがある場合、DR の優先順位に基づいて DR を選定するプロセスがあります。複数のデバイスの DR 優先順位が等しい場合、最上位の IP アドレスを持つデバイスが DR になります。

デフォルトでは、セキュリティ アプライアンスには優先順位 1 の DR があります。この値は、次のコマンドを入力すると変更できます。

```
hostname(config-if)# pim dr-priority num
```

*num* は 1 ～ 4294967294 の任意の数字にできます。

## PIM 登録メッセージのフィルタリング

PIM 登録メッセージをフィルタリングするようにセキュリティ アプライアンスを設定することができます。PIM 登録メッセージをフィルタリングするには、次のコマンドを入力します。

```
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 メッセージは PIM DR を選定するために使用されます。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 秒間隔で送信されます。この値は、次のコマンドを入力すると変更できます。

```
hostname(config-if)# pim hello-interval seconds
```

*seconds* 引数の有効な値は、1 ～ 3600 秒です。

60 秒ごとに、セキュリティ アプライアンスは PIM 加入メッセージおよびプルニング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* 引数の有効な値は、10 ～ 600 秒です。

## マルチキャスト ルーティングの参考資料

SMR 機能の実装に使用される IGMP およびマルチキャスト ルーティングの規格の技術詳細については、IETF 発行の次の RFC を参照してください。

- RFC 2236 IGMPv2
- RFC 2362 PIM-SM
- RFC 2588 IP Multicast and Firewalls
- RFC 2113 IP Router Alert Option
- IETF draft-ietf-idmr-igmp-proxy-01.txt

## 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。セキュリティ アプライアンスは、DHCP サーバまたは DHCP リレー サービスをセキュリティ アプライアンスのインターフェイスに接続されている DHCP クライアントに提供することができます。DHCP サーバは、ネットワーク コンフィギュレーション パラメータを DHCP クライアントに直接提供します。DHCP リレーでは、1つの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向こう側に位置する外部 DHCP サーバに渡します。

ここでは、次の項目について説明します。

- [DHCP サーバの設定 \(P.8-28\)](#)
- [DHCP リレー サービスの設定 \(P.8-32\)](#)

## DHCP サーバの設定

この項では、セキュリティ アプライアンスによって提供される DHCP サーバの設定方法について説明します。ここでは、次の項目について説明します。

- [DHCP サーバのイネーブル化 \(P.8-28\)](#)
- [DHCP オプションの設定 \(P.8-30\)](#)
- [DHCP サーバを利用する Cisco IP Phone の使用方法 \(P.8-31\)](#)

## DHCP サーバのイネーブル化

セキュリティ アプライアンスは DHCP サーバとして動作することができます。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をホストに供給するプロトコルです。



(注)

セキュリティ アプライアンス DHCP サーバは、BOOTP 要求をサポートしていません。

マルチコンテキスト モードでは、DHCP サーバまたは DHCP リレーは、複数のコンテキストで使われるインターフェイス上ではイネーブルにすることはできません。

DHCP サーバは、セキュリティ アプライアンスの各インターフェイスに設定することができます。各インターフェイスには、それ自体のアドレス プールがあり、利用できます。しかし、DNS サーバ、ドメイン名、オプション、ping のタイムアウト、WINS サーバなど他の DHCP 設定はグローバルに設定され、すべてのインターフェイス上の DHCP サーバによって使用されます。

DHCP クライアントまたは DHCP リレー サービスは、DHCP サーバがイネーブルになっているインターフェイス上では設定することはできません。これに加えて、DHCP クライアントは、DHCP サーバがイネーブルになっているインターフェイスに直接接続されている必要があります。

指定されたセキュリティ アプライアンスのインターフェイスで DHCP サーバをイネーブルにするには、次の手順を実行します。

**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
```



セキュリティ アプライアンスは、1 つのクライアントに対して一定時間だけ使用可能なアドレスを 1 つこのプールから割り当てます。これらのアドレスは、直接接続されているネットワークのための、変換されていないローカルアドレスです。

アドレス プールは、セキュリティ アプライアンス インターフェイスと同じサブネット内にある必要があります。

- ステップ 2** (オプション) クライアントが使用する DNS サーバの IP 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)# dhcpd dns dns1 [dns2]
```

DNS サーバは最大 2 つまで指定できます。

- ステップ 3** (オプション) クライアントが使用する WINS サーバの IP 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)# dhcpd wins wins1 [wins2]
```

WINS サーバは最大 2 つまで指定できます。

- ステップ 4** (オプション) クライアントに許可するリース期間を変更するには、次のコマンドを入力します。

```
hostname(config)# dhcpd lease lease_length
```

リース期間は、その期間が終了するまでクライアントがその割り当て IP アドレスを使用できる時間 (秒) のことです。0 ~ 1,048,575 の間の値を入力します。デフォルト値は 3600 秒です。

- ステップ 5** (オプション) クライアントが使用するドメイン名を設定するには、次のコマンドを入力します。

```
hostname(config)# dhcpd domain domain_name
```

- ステップ 6** (オプション) DHCP に ping のタイムアウト値を設定するには、次のコマンドを入力します。

```
hostname(config)# dhcpd ping_timeout milliseconds
```

アドレスの衝突を避けるために、セキュリティ アプライアンスは、1 つのアドレスに ICMP ping パケットを 2 回送信してから、そのアドレスを DHCP クライアントに割り当てます。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) デフォルトの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の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 のオプション 3 を使用せずにデフォルトのゲートウェイを定義する場合、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** セキュリティ アプライアンス内の DHCP デーモンをイネーブルにし、イネーブルになったインターフェイス上で DHCP クライアント要求を受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)# dhcpd enable interface_name
```

たとえば、内部インターフェイスに接続されているホストに範囲 10.0.1.101 ~ 10.0.1.110 を割り当てるには、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

セキュリティ アプライアンスは、RFC 2132 に記載されている DHCP オプションの情報を送信するように設定することができます。DHCP オプションには次の 3 種類があります。

- 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

セキュリティ アプライアンスは DHCP オプションの 3 カテゴリをすべてサポートしています。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)

セキュリティ アプライアンスは、指定されたオプションのタイプおよび値が RFC 2132 に定義されているオプション コードに対して期待されているタイプおよび値と一致するかどうかは確認しません。たとえば、`dhcpd option 46 ascii hello` と入力することは可能であり、セキュリティ アプライアンスはこのコンフィギュレーションを受け入れますが、RFC 2132 では、オプション 46 には 1 桁の 16 進数値が期待値として定義されています。オプション コードとその関連タイプおよび期待値の詳細については、RFC 2132 を参照してください。

表 8-2 に、`dhcpd option` コマンドでサポートされていない DHCP オプションを示します。

表 8-2 サポートされていない DHCP オプション

| オプション コード | 説明                        |
|-----------|---------------------------|
| 0         | DHCPOPT_PAD               |
| 1         | HCPOPT_SUBNET_MASK        |
| 12        | DHCPOPT_HOST_NAME         |
| 50        | DHCPOPT_REQUESTED_ADDRESS |
| 51        | DHCPOPT_LEASE_TIME        |
| 52        | DHCPOPT_OPTION_OVERLOAD   |
| 53        | DHCPOPT_MESSAGE_TYPE      |
| 54        | DHCPOPT_SERVER_IDENTIFIER |
| 58        | DHCPOPT_RENEWAL_TIME      |
| 59        | DHCPOPT_REBINDING_TIME    |
| 61        | DHCPOPT_CLIENT_IDENTIFIER |
| 67        | DHCPOPT_BOOT_FILE_NAME    |
| 82        | DHCPOPT_RELAY_INFORMATION |
| 255       | DHCPOPT_END               |

特定のオプション、つまり DHCP オプション 3、66、および 150 は、Cisco IP Phone を設定するために使用します。これらのオプション設定の詳細については、P.8-31 の「[DHCP サーバを利用する Cisco IP Phone の使用方法](#)」を参照してください。

## DHCP サーバを利用する Cisco IP Phone の使用方法

Cisco IP テレフォニー VoIP ソリューションを実装する小規模な支社を持つ企業では、一般に本社で Cisco CallManager を実装し、支社の Cisco IP Phone を制御します。この実装により中央集中型のコール プロセッシングが可能となり、必要な機器を少なく抑え、支店側で Cisco CallManager およびその他のサーバを管理する必要がなくなります。

Cisco IP Phone では、コンフィギュレーションを TFTP サーバからダウンロードします。Cisco IP Phone の起動時に、IP アドレスと TFTP サーバの IP アドレスの両方が事前に設定されていない場合、Cisco IP Phone ではオプション 150 または 66 を伴う要求を DHCP サーバに送信して、この情報を取得します。

- DHCP オプション 150 では、TFTP サーバのリストの IP アドレスが提供されます。
- DHCP オプション 66 では、1 つの TFTP サーバの IP アドレスまたはホスト名が与えられます。

Cisco IP Phone では、デフォルト ルートを設定する DHCP オプション 3 を要求に含めることもできます。

Cisco IP Phone では、1 つの要求にオプション 150 とオプション 66 の両方が含まれることがあります。この場合、両者がセキュリティ アプライアンスで設定されていると、セキュリティ アプライアンスの DHCP サーバは、その応答で両方のオプションに対する値を提供します。

RFC 2132 に記載されているオプションの大部分の情報を送信するようにセキュリティ アプライアンスを設定することができます。次に、任意のオプション番号のシンタックスと、一般的に使用されているオプション 66、150、および 3 のシンタックスを示します。

- RFC-2132 に指定されているオプション番号を含む DHCP 要求の情報を提供するには、次のコマンドを入力します。

```
hostname(config)# dhcpd option number value
```

- オプション 66 の IP アドレスまたは TFTP サーバ名を提供するには、次のコマンドを入力します。

```
hostname(config)# dhcpd option 66 ascii server_name
```

- オプション 150 の IP アドレスあるいは 1 つまたは 2 つの TFTP サーバ名を提供するには、次のコマンドを入力します。

```
hostname(config)# dhcpd option 150 ip server_ip1 [server_ip2]
```

*server\_ip1* には、プライマリ TFTP サーバの IP アドレスまたは名前を、*server\_ip2* には、セカンダリ TFTP サーバの IP アドレスまたは名前を指定します。オプション 150 を使用すると、最大 2 つの TFTP サーバが指定できます。

- デフォルト ルートの設定を提供するには、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 エージェントを使用すると、セキュリティ アプライアンスを介して DHCP 要求をクライアントから別のインターフェイスに接続されているルータに転送することができます。

DHCP リレー エージェントを使用する場合、次の制限が適用されます。

- DHCP サーバもイネーブルになっている場合、リレー エージェントをイネーブルにできない。
- クライアントは直接セキュリティ アプライアンスに接続する必要があり、他のリレー エージェントやルータを介して要求を送信できない。
- マルチコンテキスト モードでは、複数のコンテキストによって使用されるインターフェイス上で DHCP リレーをイネーブルにできない。



(注)

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。透過ファイアウォール モードの場合、セキュリティ アプライアンスは ARP トラフィックのみ通過を許可します。他のトラフィックはすべて ACL が必要です。透過モードで DHCP 要求と応答がセキュリティ アプライアンスを通過できるようにするには、2 つの ACL を設定する必要があります。その 1 つは内部インターフェイスから外部への DHCP 要求を許可するもので、もう 1 つは逆方向に向かうサーバからの応答を許可するためのものです。

DHCP リレーをイネーブルにするには、次の手順を実行します。

- ステップ 1** DHCP クライアントとは異なるインターフェイス上の DHCP サーバの IP アドレスを設定するには、次のコマンドを入力します。

```
hostname(config)# dhcprelay server ip_address if_name
```

このコマンドを使用して 4 つまでのサーバを 4 回まで設定できます。

- ステップ 2** クライアントが接続されているインターフェイス上で DHCP リレー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)# dhcprelay enable interface
```

- ステップ 3** (オプション) リレー アドレス ネゴシエーションに許可する時間を秒数で設定するには、次のコマンドを入力します。

```
hostname(config)# dhcprelay timeout seconds
```

- ステップ 4** (オプション) DHCP サーバから送信されたパケットの最初のデフォルト ルータ アドレスを、セキュリティ アプライアンス インターフェイスのアドレスに変更するには、次のコマンドを入力します。

```
hostname(config)# dhcprelay setroute interface_name
```

このアクションを行うと、クライアントは、自分のデフォルト ルートを設定して、DHCP サーバで異なるルータが指定されている場合でも、セキュリティ アプライアンスをポイントすることができます。

パケット内にデフォルトのルータ オプションがなければ、セキュリティ アプライアンスは、そのインターフェイスのアドレスを含んでいるデフォルト ルータを追加します。

次の例では、セキュリティ アプライアンスは、内部インターフェイスに接続されているクライアントからの DHCP 要求を、外部インターフェイス上の DHCP サーバに転送することができるようになります。

```
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

セキュリティ アプライアンスのインターフェイスを DHCP クライアントとして設定するには、次の手順を実行します。

```
hostname(config-if)# ip address dhcp [retry num] [setroute]
```

オプションの **retry num** 引数は、そのインターフェイスが DHCP サーバにアクセス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** キーワードを使用すると、セキュリティ アプライアンスは、DHCP サーバが返すデフォルト ゲートウェイを使用してデフォルト ルートを設定します。



(注)

DHCP クライアントとして設定されているインターフェイス上では、DHCP サーバまたは DHCP リレー サービスをイネーブルにすることはできません。





# IPv6 の設定

---

この章では、セキュリティ アプライアンスで IPv6 をイネーブルにする方法および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。

次の事項について説明します。

- [IPv6 対応のコマンド \(P.9-2\)](#)
- [インターフェイスでの IPv6 の設定 \(P.9-3\)](#)
- [IPv6 デフォルト ルートおよびスタティック ルートの設定 \(P.9-5\)](#)
- [IPv6 アクセスリストの設定 \(P.9-6\)](#)
- [IPv6 コンフィギュレーションの確認 \(P.9-7\)](#)
- [インターフェイスでのデュアル IP スタックの設定 \(P.9-8\)](#)
- [IPv6 コンフィギュレーションの例 \(P.9-9\)](#)

## IPv6 対応のコマンド

次に示すセキュリティ アプライアンスのコマンドは、IPv6 アドレスの受け入れと表示が可能です。

- capture
- configure
- copy
- http
- name
- object-group
- ping
- show conn
- show local-host
- show tcpstat
- ssh
- telnet
- tftp-server
- who
- write



(注)

フェールオーバーでは、IPv6 はサポートされません。 **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スタンバイ アドレスの設定をサポートしません。 **failover interface ip** コマンドは、フェールオーバー インターフェイスおよびステートフル フェールオーバー インターフェイス上の IPv6 アドレスの使用をサポートしません。

IPv6 アドレスをサポートするコマンドに IPv6 アドレスを入力するときは、単純に、標準 IPv6 表記で IPv6 アドレスを入力します (**ping fe80::2e0:b6ff:fe01:3b7a** など)。セキュリティ アプライアンスは、IPv6 アドレスを正しく認識し、処理します。ただし、次の場合は、IPv6 アドレスを角カッコ ([ ]) で囲む必要があります。

- アドレスとポート番号を指定する必要がある場合 (**[fe80::2e0:b6ff:fe01:3b7a]:8080** など)
- **write net** コマンド、**config net** コマンドなど、コマンドの区切り記号としてコロンを使用する場合 (**configure net [fe80::2e0:b6ff:fe01:3b7a]:/tftp/config/pixconfig** など)

次のコマンドは、IPv6 で動作するように変更されました。

- debug
- fragment
- ip verify
- mtu
- icmp (**ipv6 icmp** と入力されます)

次の検査エンジンは、IPv6 をサポートします。

- FTP
- HTTP
- ICMP
- SMTP
- TCP
- UDP



## インターフェイスでの 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。さらに、サイトローカル アドレスおよびグローバル アドレスをインターフェイスに追加できます。

**(注)**

セキュリティ アプライアンスは、IPv6 エニーキャスト アドレスはサポートしません。

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。

インターフェイスに 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に対応するインターフェイス コンフィギュレーション モードに入ります。

```
hostname(config)# interface if
```

- 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複数の IPv6 アドレス (IPv6 リンクローカル アドレス、サイトローカル アドレス、グローバル アドレスなど) を割り当てることができます。ただし、少なくとも、リンクローカル アドレスを設定する必要があります。

インターフェイスの IPv6 アドレスを設定するには、いくつかの方法があります。次の方法から、要件に合った方法を選びます。

- 最も単純な方法は、インターフェイスでステートレスな自動設定をイネーブルにする方法です。インターフェイスでステートレスな自動設定をイネーブルにすると、ルータ アドバタイズメント メッセージで受信したプレフィックスに基づいて IPv6 アドレスが設定されます。ステートレスな自動設定がイネーブルになっている場合、インターフェイスのリンクローカル アドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。ステートレスな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
```

- インターフェイスのリンクローカル アドレスだけを設定する必要があり、その他の IPv6 アドレスをインターフェイスに割り当てない場合は、手動でリンクローカル アドレスを定義するか、インターフェイス MAC アドレス (Modified EUI-64 形式) に基づいて生成するかを選択できます。

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
```

インターフェイスで IPv6 をイネーブルにして、インターフェイス MAC アドレスに基づく Modified EUI-64 インターフェイス ID を使用してリンクローカル アドレスを生成するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 enable
```

**(注)**

インターフェイスで、その他の **ipv6 address** コマンドを入力した場合は、**ipv6 enable** コマンドを使用する必要はありません。IPv6 サポートは、インターフェイスに IPv6 アドレスが割り当てられるとすぐに、自動的にイネーブルになります。

- サイトローカル アドレスまたはグローバル アドレスをインターフェイスに割り当てます。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 アドレスが自動的に作成されます。グローバル アドレスまたはサイトローカル アドレスをインターフェイスに追加するには、次のコマンドを入力します。アドレスの下位 64 ビットに Modified EUI-64 インターフェイス ID を使用する場合は、オプションの **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** (オプション) インターフェイスでルータ アドバタイズメント メッセージを抑止します。デフォルトでは、ルータ アドバタイズメント メッセージは、ルータ送信要求メッセージへの応答として自動的に送信されます。セキュリティ アプライアンスで IPv6 プレフィックスを提供する必要があるインターフェイス (外部インターフェイスなど) では、これらのメッセージをディセーブルにできます。

インターフェイスでルータ アドバタイズメント メッセージを抑止するには、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される IPv6 アドレスの例については、[P.9-9 の「IPv6 コンフィギュレーションの例」](#)を参照してください。

## IPv6 デフォルト ルートおよびスタティック 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。インターフェイスが IPv6 対応で、IPv6 ACL でトラフィックが許可されている場合、セキュリティ アプライアンスはそのインターフェイス間の IPv6 トラフィックをルーティングします。デフォルト ルートとスタティック ルートは、**ipv6 route** コマンドで追加できます。

IPv6 デフォルト ルートおよびスタティック 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、次のコマンドを使用します。

```
hostname(config)# ipv6 route interface_name ::/0 next_hop_ipv6_addr
```

アドレス ::/0 は、IPv6 で「any」と同じです。

**ステップ 2** (オプション) IPv6 スタティック ルートを定義します。次のコマンドを使用して、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 ルートの定義に使用する **route** コマンドと同じように機能します。

デフォルト ルートの設定に使用する **ipv6 route** コマンドの例については、[P.9-9 の「IPv6 コンフィギュレーションの例」](#)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、IPv4 アクセスの設定に似ていますが、IPv6 アドレスを使用するという違いがあります。

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2つの主な形式があり、いずれかを選択できます。1つは、特に ICMP トラフィック用のアクセスリスト エントリを作成する形式で、もう1つは、その他のすべての種類の IP トラフィック用のアクセスリスト エントリを作成する形式です。

- 特に ICMP トラフィック用の 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]
```

**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。1 つのアクセスリストに複数のエントリを入力する場合は、各コマンドで同じ **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、そのエントリを入力するリスト内の行番号を指定できます。
- permit|deny** : 指定したトラフィックの通過をブロックするか、許可するかを決定します。
- 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かどうかを示します。
- 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**) または番号 (1 ~ 254) を使用できます。**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 プレフィックス、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** で指定された特定のホストを使用できます。
- src\_port** および **dst\_port** : 送信元および宛先ポート (またはサービス) 引数。演算子 (より小さいを表す **lt**、より大きいを表す **gt**、等しいを表す **eq**、等しくないを表す **neq**、両端を含む範囲を表す **range**) の後ろにスペースとポート番号を続けます (**range** キーワードの場合は、2つのポート番号をスペースで区切ります)。
- icmp\_type** : アクセス規則によってフィルタリングされる ICMP メッセージ タイプを指定します。値は、有効な ICMP タイプ番号 (0 ~ 155) または付録 D「アドレス、プロトコル、およびポート」で示す ICMP タイプ リテラルのいずれかにできます。**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** アクセスリストをインターフェイスに適用するには、次のコマンドを入力します。

```
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、P.9-9 の「IPv6 コンフィギュレーションの例」を参照してください。

## IPv6 コンフィギュレーションの確認

この項では、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 show コマンドを使用して、IPv6 設定を確認できます。

ここでは、次の項目について説明します。

- [show ipv6 interface コマンド \(P.9-7\)](#)
- [show ipv6 route コマンド \(P.9-8\)](#)

### show ipv6 interface コマンド

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含めると、指定したインターフェイスの設定が表示されます。コマンドに名前を含めないと、IPv6 がイネーブルになっているすべてのインターフェイスの設定が表示されます。コマンドの出力では、次の項目が表示されます。

- インターフェイスの名前とステータス
- リンクローカルおよびグローバルなユニキャスト アドレス
- インターフェイスが属するマルチキャスト グループ
- ICMP リダイレクトおよびエラー メッセージの設定
- 近隣探索の設定

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** コマンドを使用する必要があります。**show ipv6 interface** コマンドでは、インターフェイスの IPv4 設定は表示されません（そのインターフェイスで両方が設定されている場合）。

## show ipv6 route コマンド

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 の **show route** コマンドに似ています。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 プレフィックス
- ルートの管理ディスタンスとメトリック
- ネクストホップ ルータのアドレス
- ネクストホップ ルータから指定の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
```

## インターフェイスでのデュアル IP スタックの設定

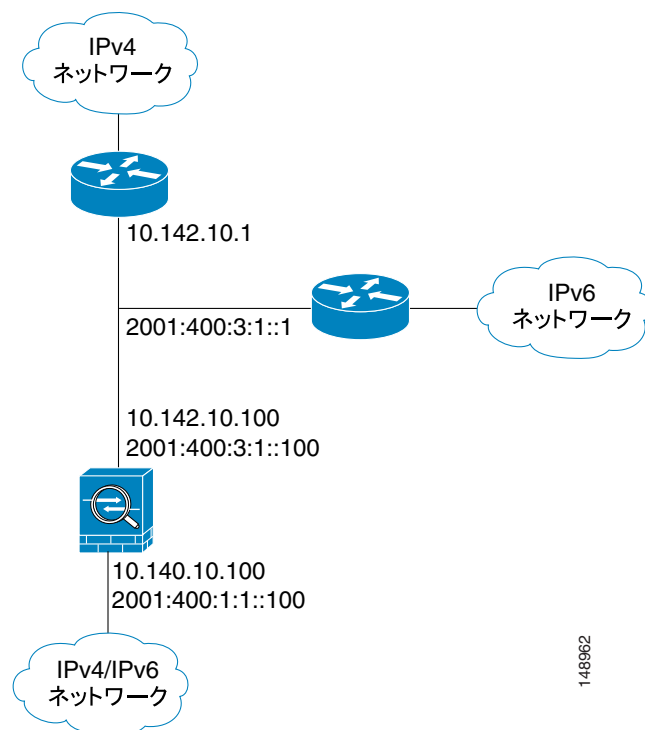
セキュリティ アプライアンスは、1つのインターフェイス上で IPv6 と IPv4 の両方のコンフィギュレーションをサポートします。そのために特別なコマンドを入力する必要はありません。単純に、IPv4 コンフィギュレーション コマンドと IPv6 コンフィギュレーション コマンドを通常と同じように入力します。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

## IPv6 コンフィギュレーションの例

例 9-1 で、IPv6 コンフィギュレーションの機能をいくつか示します。

- 各インターフェイスに IPv6 と IPv4 の両方のアドレスが設定されています。
- **ipv6 route** コマンドで IPv6 デフォルト ルートが設定されています。
- IPv6 アクセスリストが外部インターフェイスに適用されています。

図 9-1 IPv6 デュアル スタック コンフィギュレーション



例 9-1 IPv6 コンフィギュレーションの例

```
interface Ethernet0
  speed auto
  duplex auto
  nameif outside
  security-level 0
  ip address 16.142.10.100 255.255.255.0
  ipv6 address 2001:400:3:1::100/64
  ipv6 nd suppress-ra
  ospf mtu-ignore auto
!
interface Ethernet1
  speed auto
  duplex auto
  nameif inside
  security-level 100
  ip address 16.140.10.100 255.255.255.0
  ipv6 address 2001:400:1:1::100/64
  ospf mtu-ignore auto
!
```

```

enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname coyupix
boot system flash:/cdisk.7.0.0.16
ftp mode passive
names
access-list allow extended permit icmp any any
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
ipv6 route outside ::/0 2001:400:3:1::1
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
no failover
monitor-interface outside
monitor-interface inside
asdm image
no asdm history enable
arp timeout 14400
access-group allow in interface outside
access-group outacl in interface outside
route outside 0.0.0.0 0.0.0.0 16.142.10.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:02:00 rpc 0:10:00 h323
0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 outside
fragment chain 24 outside
fragment size 200 inside
fragment chain 24 inside
sysopt nodnsalias inbound
sysopt nodnsalias outbound
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map global_policy
  class inspection_default
    inspect dns
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect smtp
    inspect sqlnet
    inspect sip
    inspect skinny
    inspect rpc
    inspect xdmcp
    inspect netbios
    inspect mgcp
    inspect tftp
    inspect snmp
  !
terminal width 80
service-policy global_policy global
Cryptochecksum:00000000000000000000000000000000
: end

```





# AAA サーバとローカル データベース の設定

---

この章では、AAA（「トリプル エー」と発音）のサポート、および AAA サーバとローカル データベースの設定方法について説明します。

ここでは、次の項目を取り上げます。

- [AAA の概要 \(P.10-2\)](#)
- [AAA サーバおよびローカル データベースのサポート \(P.10-4\)](#)
- [ローカル データベースの設定 \(P.10-15\)](#)
- [AAA サーバ グループおよびサーバの識別 \(P.10-17\)](#)

## AAA の概要

AAA によって、セキュリティ アプライアンスが、ユーザが誰か（認証）、ユーザが何を実行できるか（認可）、およびユーザが何を実行したか（アカウンティング）を判別することが可能になります。

AAA には、ユーザ アクセスに対して、ACL のみを使用する場合よりもレベルの高い保護および制御機能が用意されています。たとえば、すべての外部ユーザが DMZ ネットワークのサーバ上の Telnet にアクセスできるようにする ACL を作成できます。一部のユーザのみがサーバにアクセスできるようにするが、そのユーザの IP アドレスを常に認識しているとは限らない場合、AAA を使用すると、認証済みまたは認可済みのユーザのみがセキュリティ アプライアンスを介してアクセスすることが許可されるようにできます（Telnet サーバもまた、認証を実行します。セキュリティ アプライアンスは、認可されないユーザがサーバにアクセスできないようにします）。

認証のみで使用することも、認可およびアカウンティングとともに使用することもできます。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングのみで使用することも、認証および認可とともに使用することもできます。

ここでは、次の項目について説明します。

- [認証の概要 \(P.10-2\)](#)
- [認可の概要 \(P.10-2\)](#)
- [アカウンティングの概要 \(P.10-3\)](#)

## 認証の概要

認証では、有効なユーザ クレデンシャルを要求してアクセスを制御します。このクレデンシャルは通常、ユーザ名とパスワードです。次の項目を認証するように、セキュリティ アプライアンスを設定できます。

- セキュリティ アプライアンスへのすべての管理接続（この接続には、次のセッションが含まれます）
  - Telnet
  - SSH
  - シリアル コンソール
  - ASDM（HTTPS を使用）
  - VPN 管理アクセス
- **enable** コマンド
- ネットワーク アクセス
- VPN アクセス

## 認可の概要

認可では、ユーザ認証後、ユーザごとにアクセスを制御します。次の項目を認可するように、セキュリティ アプライアンスを設定できます。

- 管理コマンド
- ネットワーク アクセス
- VPN アクセス

認可では、各認証済みユーザが使用可能なサービスおよびコマンドを制御します。認可をイネーブルにしていない場合は、認証のみで、すべての認証済みユーザがサービスに同じようにアクセスできます。

認可で提供される制御が必要な場合、広範な認証規則を設定して、詳細な認可が設定できます。たとえば、外部ネットワーク上のサーバにアクセスする内部ユーザを認証して、特定のユーザがアクセスできる外部サーバを認可によって制限します。

セキュリティ アプライアンスはユーザあたり最初の 16 個の認証要求をキャッシュするため、ユーザが現在の認証セッション中に同じサービスにアクセスした場合、セキュリティ アプライアンスは認可サーバに要求を再送信しません。

## アカウントिंगの概要

アカウントINGは、セキュリティ アプライアンスを通過するトラフィックを追跡して、ユーザ アクティビティを記録できるようにします。トラフィックの認証をイネーブルにすると、ユーザごとにトラフィックをアカウントING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INGできます。アカウントING情報には、セッションの開始時刻と終了時刻、ユーザ名、そのセッションでセキュリティ アプライアンスを経由したバイト数、使用されたサービス、セッションの継続時間が含まれます。

## AAA サーバおよびローカル データベースのサポート

セキュリティ アプライアンスは、さまざまな AAA サーバ タイプおよびセキュリティ アプライアンスに保存されているローカル データベースをサポートします。ここでは、各 AAA サーバ タイプとローカル データベースに関するサポートについて説明します。

ここでは、次の項目について説明します。

- サポートの要約 (P.10-4)
- RADIUS サーバのサポート (P.10-5)
- TACACS+ サーバのサポート (P.10-6)
- SDI サーバのサポート (P.10-7)
- NT サーバのサポート (P.10-8)
- Kerberos サーバのサポート (P.10-8)
- LDAP サーバのサポート (P.10-9)
- ローカル データベースのサポート (P.10-13)

### サポートの要約

表 10-1 に、各 AAA サービスのサポート状況の要約を AAA サーバ タイプ（ローカル データベースを含む）別に示します。特定の AAA サーバ タイプのサポートの詳細については、表に続く項目を参照してください。

**表 10-1 AAA サポートの要約**

| AAA サービス        | データベース タイプ      |                 |         |     |    |          |      |                 |
|-----------------|-----------------|-----------------|---------|-----|----|----------|------|-----------------|
|                 | ローカル            | RADIUS          | TACACS+ | SDI | NT | Kerberos | LDAP | HTTP Form       |
| <b>認証</b>       |                 |                 |         |     |    |          |      |                 |
| VPN ユーザ         | あり              | あり              | あり      | あり  | あり | あり       | あり   | あり <sup>1</sup> |
| 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   | なし              |
| 管理者             | あり              | あり              | あり      | なし  | なし | なし       | なし   | なし              |
| <b>認可</b>       |                 |                 |         |     |    |          |      |                 |
| VPN ユーザ         | あり              | あり              | なし      | なし  | なし | なし       | あり   | なし              |
| ファイアウォールセッション   | なし              | あり <sup>2</sup> | あり      | なし  | なし | なし       | なし   | なし              |
| 管理者             | あり <sup>3</sup> | なし              | あり      | なし  | なし | なし       | なし   | なし              |
| <b>アカウントिंग</b> |                 |                 |         |     |    |          |      |                 |
| VPN 接続          | なし              | あり              | あり      | なし  | 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   | なし              |
| 管理者             | なし              | なし              | あり      | なし  | なし | なし       | なし   | なし              |

1. HTTP Form プロトコルは、WebVPN ユーザに対してのみシングルサインオン認証をサポートします。

2. ファイアウォールセッションの場合、RADIUS 認可はユーザ固有の ACL でのみサポートされます。この ACL は RADIUS 認証応答で受信または指定されます。

3. ローカル コマンド認可は、特権レベルに限りサポートされます。

## RADIUS サーバのサポート

セキュリティ アプライアンスは RADIUS サーバをサポートします。

ここでは、次の項目について説明します。

- [認証方法 \(P.10-5\)](#)
- [アトリビュートのサポート \(P.10-5\)](#)
- [RADIUS 機能 \(P.10-5\)](#)

### 認証方法

セキュリティ アプライアンスは、RADIUS で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 エージングを含む) (IPSec ユーザ専用)

### アトリビュートのサポート

セキュリティ アプライアンスは、次の RADIUS アトリビュートのセットをサポートします。

- RFC 2138 に定義されている認証アトリビュート
- RFC 2139 に定義されているアカウントリング アトリビュート
- RFC 2868 に定義されているトンネル プロトコル サポート用の RADIUS アトリビュート
- RADIUS ベンダー ID 9 によって識別される Cisco IOS VSA
- RADIUS ベンダー ID 3076 によって識別される Cisco VPN 関連 VSA
- RFC 2548 に定義されている Microsoft VSA

### RADIUS 機能

セキュリティ アプライアンスは、[表 10-2](#) に説明されている機能に関して、RADIUS サーバを使用できます。

表 10-2 RADIUS 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 コンソール接続でセキュリティ アプライアンスにアクセスしようとしたとき、トラフィックが認証文と一致する場合、セキュリティ アプライアンスはユーザのユーザ名とパスワードを要求し、これらのクレデンシャルを RADIUS サーバに送信して、サーバからの応答に基づいてユーザの CLI アクセスを許可または拒否します。 |
| enable コマンドのユーザ認証 | ユーザが <b>enable</b> コマンドにアクセスしようとする、セキュリティ アプライアンスはユーザのパスワードを要求し、RADIUS サーバにユーザ名とイネーブル パスワードを送信して、サーバからの応答に基づいてイネーブル モードへのユーザのアクセスを許可または拒否します。                                            |
| ネットワーク アクセスのユーザ認証 | ユーザがセキュリティ アプライアンスを使用してネットワークにアクセスしようとしたとき、トラフィックが認証文と一致する場合、セキュリティ アプライアンスは RADIUS サーバにユーザ クレデンシャル (通常は、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 アクセスを許可または拒否します。                       |

表 10-2 RADIUS 機能（続き）

| 機能                                          | 説明                                                                                                                                                                                                         |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ネットワーク アクセスのユーザ認証（ユーザごとにダイナミック ACL を使用）     | ダイナミック ACL を実装するには、これをサポートするように RADIUS サーバを設定する必要があります。ユーザを認証する場合、RADIUS サーバによってダウンロード可能な ACL がセキュリティ アプライアンスに送信されます。所定のサービスへのアクセスが ACL によって許可または拒否されます。認証セッションの有効期限が切れると、セキュリティ アプライアンスによって ACL が削除されます。  |
| ネットワーク アクセスのユーザ認証（ユーザごとにダウンロードされた ACL 名を使用） | ダウンロードされた ACL 名を実装するには、その ACL 名をサポートするように RADIUS サーバを設定する必要があります。ユーザを認証する場合、RADIUS サーバによって ACL の名前が送信されます。指定された名前の ACL がセキュリティ アプライアンスに存在する場合、所定のサービスへのアクセスが ACL によって許可または拒否されます。複数のユーザに同じ名前の ACL を指定できます。 |
| VPN 認証                                      | ユーザが VPN アクセスを確立しようとしたとき、適用可能なトンネルグループ レコードに RADIUS 認証サーバ グループが指定されている場合、セキュリティ アプライアンスは RADIUS サーバにユーザ名とパスワードを送信し、その後サーバからの応答に基づいてユーザのアクセスを許可または拒否します。                                                    |
| VPN 認可                                      | 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 レコードによって RADIUS 認可サーバ グループが指定されている場合、セキュリティ アプライアンスは RADIUS 認可サーバに要求を送信して、受信した認可を 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 レコードによって RADIUS アカウンティングサーバ グループが指定されている場合、セキュリティ アプライアンスは RADIUS サーバに、VPN セッションについてのグループ 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       | セキュリティ アプライアンスを通過するトラフィックすべてについて、アカウンティング情報を RADIUS サーバに送信するように、セキュリティ アプライアンスを設定できます。                                                                                                                     |

## TACACS+ サーバのサポート

セキュリティ アプライアンスは、表 10-3 に説明されている機能に関して、TACACS+ サーバを使用できます。セキュリティ アプライアンスは、ASCII、PAP、CHAP、および MS-CHAPv1 で TACACS+ 認証をサポートします。

表 10-3 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 コンソール接続でセキュリティ アプライアンスにアクセスしようとしたとき、トラフィックが認証文と一致する場合、セキュリティ アプライアンスはユーザのユーザ名とパスワードを要求し、これらのクレデンシャルを TACACS+ サーバに送信して、サーバからの応答に基づいてユーザの CLI アクセスを許可または拒否します。 |
| enable コマンドのユーザ認証 | ユーザが <b>enable</b> コマンドにアクセスしようとする、セキュリティ アプライアンスはユーザのパスワードを要求し、TACACS+ サーバにユーザ名とイネーブル パスワードを送信して、サーバからの応答に基づいてイネーブル モードへのユーザのアクセスを許可または拒否します。                                            |
| 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に、セキュリティ アプライアンスを設定できます。                                                                                                                         |

表 10-3 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                     | ユーザがセキュリティ アプライアンスを使用してネットワークにアクセスしようとしたとき、トラフィックが認証文と一致する場合、セキュリティ アプライアンスは TACACS+ サーバにユーザ クレデンシャル (通常は、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 アクセスを許可または拒否します。 |
| ネットワーク アクセスのユーザ認可                     | 認証後に、ユーザがセキュリティ アプライアンス上の認可文と一致すると、セキュリティ アプライアンスは、TACACS+ サーバにユーザのアクセス特権について問い合わせます。                                                                               |
| VPN 認証                                | ユーザが VPN アクセスを確立しようとしたとき、適用可能なトンネルグループ レコードによって TACACS+ 認証サーバ グループが指定されている場合、セキュリティ アプライアンスは TACACS+ サーバにユーザ名とパスワードを送信し、その後サーバからの応答に基づいてユーザのアクセスを許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 レコードに TACACS+ アカウンティングサーバ グループが指定されている場合、セキュリティ アプライアンスは TACACS+ サーバに、VPN セッションについてのグループ 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認可                          | TACACS+ サーバで、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 で入力するコマンドはそれぞれ、TACACS+ サーバによってチェックされます。                                                                      |
| 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 | セキュリティ アプライアンスを通過するトラフィックすべてについて、アカウンティング情報を TACACS+ サーバに送信するように、セキュリティ アプライアンスを設定できます。                                                                             |

## SDI サーバのサポート

セキュリティ アプライアンスは、VPN 認証に RSA SecureID サーバを使用できます。これらのサーバは、SDI サーバとも呼ばれます。ユーザが VPN アクセスを確立しようとしたとき、適用可能なトンネルグループ レコードによって SDI 認証サーバ グループが指定されている場合、セキュリティ アプライアンスは SDI サーバにユーザ名とワンタイム パスワードを送信し、その後サーバからの応答に基づいてユーザのアクセスを許可または拒否します。

ここでは、次の項目について説明します。

- [SDI バージョンのサポート \(P.10-7\)](#)
- [2 ステップ認証プロセス \(P.10-8\)](#)
- [SDI プライマリ サーバおよびレプリカ サーバ \(P.10-8\)](#)

## SDI バージョンのサポート

セキュリティ アプライアンスでは、次の SDI バージョンがサポートされています。

- **バージョン 5.0 より前のバージョン**：5.0 より前の SDI バージョンは、シングルノード秘密ファイル (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 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。各プライマリおよびそのレプリカは、シングルノード秘密ファイルを共有します。そのノード秘密ファイルの名前は、.sdi が付加された ACE/ サーバ IP アドレスの 16 進数値に基づきます。



セキュリティ アプライアンスに設定するバージョン 5.0 SDI サーバは、プライマリでも、レプリカのいずれか 1 つでもかまいません。ユーザ認証のための SDI エージェントによるサーバの選択方法の詳細については、[P.10-8](#) の「SDI プライマリ サーバおよびレプリカ サーバ」を参照してください。

## 2 ステップ認証プロセス

SDI バージョン 5.0 は 2 ステップのプロセスを使用して、侵入者が RSA SecurID 認証要求から情報を取り込み、それを使用して別のサーバに認証を証明しないように防止します。エージェントはまず、SecurID サーバにロック要求を送信してから、ユーザ認証要求を送信します。サーバはユーザ名をロックして、別の（レプリカ）サーバがユーザ名を受信できないようにします。これは、同じユーザが、同じ認証サーバを同時に使用して、2 つのセキュリティ アプライアンスに認証を証明することができないことを意味します。ユーザ名のロックに成功すると、セキュリティ アプライアンスはパスワードを送信します。

## SDI プライマリ サーバおよびレプリカ サーバ

セキュリティ アプライアンスは、最初のユーザが設定済みサーバ（プライマリでもレプリカでもかまいません）に認証を証明するときに、サーバ リストを取得します。次に、セキュリティ アプライアンスはリスト上の各サーバに優先度を割り当て、その後のサーバ選択では、この割り当てられた優先度のサーバから無作為に抽出します。最も優先度の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

セキュリティ アプライアンスは、NTLM バージョン 1（集合的に NT サーバと呼びます）をサポートしている Microsoft Windows サーバオペレーティングシステムでの VPN 認証をサポートします。ユーザが VPN アクセスを確立しようとしたとき、適用可能なトンネルグループ レコードによって NT 認証サーバグループが指定されている場合、セキュリティ アプライアンスは、Microsoft Windows ドメイン サーバでのユーザ認証に NTLM バージョン 1 を使用します。セキュリティ アプライアンスは、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許可または拒否します。



(注)

NT サーバでは、ユーザ パスワードの最大長は 14 文字です。それより長いパスワードは切り捨てられます。これは、NTLM バージョン 1 の制限です。

## Kerberos サーバのサポート

セキュリティ アプライアンスは、VPN 認証に Kerberos サーバを使用できます。ユーザがセキュリティ アプライアンスを使用して VPN アクセスを確立しようとしたとき、トラフィックが認証文と一致する場合、セキュリティ アプライアンスは Kerberos サーバにユーザ認証について問い合わせ、サーバからの応答に基づいてユーザのアクセスを許可または拒否します。

セキュリティ アプライアンスは、3DES、DES、および RC4 暗号タイプをサポートしています。



(注)

セキュリティ アプライアンスは、トンネル ネゴシエーション中のユーザ パスワードの変更はサポートしていません。この状況が意図せずに発生することを回避するために、セキュリティ アプライアンスに接続するユーザの Kerberos/Active Directory サーバでのパスワード期限切れをディセーブルにします。



単純な Kerberos サーバ コンフィギュレーションの例については、[例 10-2](#) を参照してください。

## LDAP サーバのサポート

LDAP ディレクトリ サーバに対して IPSec VPN ユーザ、SSL VPN クライアント、および WebVPN ユーザを認証し、認可するようにセキュリティ アプライアンスを設定できます。この項では、VPN ユーザの認証と認可にセキュリティ アプライアンスを利用する LDAP ディレクトリの使用について説明します。ここでは、次の項目について説明します。

- [LDAP による認証 \(P.10-9\)](#)
- [LDAP での認可 \(P.10-10\)](#)
- [LDAP アトリビュート マッピング \(P.10-11\)](#)

LDAP による認証または認可を設定するために使用する設定手順の例については、[付録 E「認可および認証用の外部サーバの設定」](#) を参照してください。

## LDAP による認証

認証中、セキュリティ アプライアンスは VPN ユーザの LDAP サーバへのクライアント プロキシとして機能し、プレーンテキストまたは Simple Authentication and Security Layer (SASL) プロトコルのいずれかを使用して LDAP サーバに対する認証を行います。デフォルトでは、セキュリティ アプライアンスは、認証パラメータ（通常、ユーザ名とパスワード）を LDAP サーバにプレーンテキストで渡します。SASL とプレーンテキストのどちらを使用する場合でも、`ldap-over-ssl` コマンドを使用して、セキュリティ アプライアンスと LDAP サーバの間の通信を SSL で保護できます。



(注)

SASL を設定しない場合は、SSL で LDAP 通信を保護することを強くお勧めします。『Cisco Security Appliance Command Reference』の `ldap-over-ssl` コマンドを参照してください。

VPN アクセスのユーザ LDAP 認証が成功すると、LDAP サーバは認証された VPN ユーザのアトリビュートを返します。これらのアトリビュートには、通常、VPN セッションに適用される認可データが含まれています。したがって、LDAP を使用している場合は、1 つのステップで認証と認可が実行されます。

## SASL での LDAP 認証の保護

セキュリティ アプライアンスは、次の SASL メカニズムをサポートします。強度の低い順にそのメカニズムを示します。

- Digest-MD5：セキュリティ アプライアンスは、ユーザ名とパスワードから計算した MD5 値で LDAP サーバに応答します。
- Kerberos：セキュリティ アプライアンスは、Generic Security Services Application Programming Interface (GSSAPI; 汎用セキュリティ サービス API) Kerberos メカニズムを使用してユーザ名と領域を送信することで LDAP サーバに応答します。

これらの SASL メカニズムの任意の組み合わせをサポートするように、セキュリティ アプライアンスと LDAP サーバを設定できます。複数のメカニズムを設定した場合、セキュリティ アプライアンスは、サーバに設定された SASL メカニズムのリストを取得し、セキュリティ アプライアンスとサーバの両方に設定されているメカニズムで最も強力なものを認証メカニズムとして設定します。たとえば、LDAP サーバとセキュリティ アプライアンスの両方がこれらのメカニズムを 2 つともサポートしている場合、セキュリティ アプライアンスは、より強力なメカニズムである Kerberos を選択します。

次の例では、ldap\_dir\_1 という名前の LDAP ディレクトリ サーバに対する認証に digest-MD5 SASL メカニズムを使用し、SSL で保護された接続で通信するように、セキュリティ アプライアンスを設定しています。

```
hostname(config)# aaa-server ldap_dir_1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
hostname(config-aaa-server-host)# sasl-mechanism digest-md5
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)#
```

## LDAP サーバタイプの設定

セキュリティ アプライアンスは LDAP Version 3 をサポートします。そのため、任意の LDAP V3 サーバまたは V2 サーバと互換性があります。ただし、認証機能とパスワード管理機能については、Sun Microsystems JAVA System Directory Server (旧称 Sun ONE Directory Server) および Microsoft Active Directory 上のみでサポートします。たとえば、有効期限が切れたパスワードをシステム管理者の介入なしで自動的にリセットする機能をセキュリティ アプライアンスがサポートするのは、Sun サーバまたは Microsoft LDAP サーバのいずれかを使用した場合です。Novell サーバや OpenLDAP サーバなど、他のタイプの LDAP サーバを使用した場合は、LDAP 認可機能と Certificate Revocation List (CRL; 証明書失効リスト) 取得のみをサポートします。

デフォルトでは、セキュリティ アプライアンスは、Microsoft ディレクトリ サーバと Sun LDAP ディレクトリ サーバのどちらに接続されているかを自動的に検出します。ただし、自動検出による LDAP サーバタイプの判別に失敗しても、そのサーバが Microsoft サーバであるか、Sun サーバであるかがわかっていれば、サーバタイプを手動で設定できます。次の例では、LDAP ディレクトリ サーバ ldap\_dir\_1 を Sun Microsystems タイプに設定しています。

```
hostname(config)# aaa-server ldap_dir_1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
hostname(config-aaa-server-host)# server-type sun
hostname(config-aaa-server-host)#
```

## LDAP での認可

VPN アクセスのためのユーザ LDAP 認証が成功すると、セキュリティ アプライアンスは LDAP サーバに対してクエリーを実行し、その LDAP サーバは LDAP アトリビュートを返します。通常、これらのアトリビュートには、VPN セッションに適用される認可データが含まれています。したがって、LDAP を使用している場合は、1つのステップで認証と認可が実行されます。

ただし、認証メカニズムとは別に、それとは異なる認可を LDAP ディレクトリ サーバから取得しなければならない場合もあります。たとえば、認証に SDI サーバや証明書サーバを使用している場合、認可情報は返されません。この場合のユーザ認可では、認証成功後に LDAP ディレクトリに対してクエリーを実行します。つまり、認証と認可は2つのステップで実行されます。

LDAP を使用する VPN ユーザ認可を設定するには、最初に AAA サーバグループとトンネルグループを作成する必要があります。次に、**tunnel-group general-attributes** コマンドを使用して、サーバとトンネルグループを関連付けます。特定の要件で使用できる認可関連のコマンドおよびオプションは他にもありますが、次の例では、LDAP でのユーザ認可をイネーブルにするための基本のコマンドを示しています。この例では、remote-1 という名前の IPSec リモートアクセストンネルグループを作成し、すでに作成してある認可用の ldap\_dir\_1 AAA サーバにその新しいトンネルグループを割り当てています。

```
hostname(config)# tunnel-group remote-1 type ipsec-ra
hostname(config)# tunnel-group remote-1 general-attributes
hostname(config-general)# authorization-server-group ldap_dir_1
hostname(config-general)#
```

この基本の設定を完了したら、ディレクトリ パスワード、ディレクトリ検索の開始点、ディレクトリ検索の範囲など、追加の LDAP 認可パラメータを次のように設定できます。

```
hostname(config)# aaa-server ldap_dir_1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
hostname(config-aaa-server-host)# ldap-login-dn obscurepassword
hostname(config-aaa-server-host)# ldap-base-dn starthere
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)#
```

詳細については、『Cisco Security Appliance Command Reference』の LDAP コマンドを参照してください。

## LDAP アトリビュート マッピング

既存の LDAP ディレクトリにセキュリティ アプライアンスを導入する場合、既存の LDAP アトリビュートの名前と値は、シスコのアトリビュートの名前および値と異なっているかもしれません。既存のユーザ定義のアトリビュートの名前と値を、セキュリティ アプライアンスと互換性のあるシスコのアトリビュートの名前と値に対応付ける LDAP アトリビュート マップを作成する必要があります。作成後は、それらのアトリビュート マップを LDAP サーバにバインドしたり、必要に応じて削除したりできます。また、アトリビュート マップの表示や消去も可能です。



(注)

アトリビュート マッピング機能を適切に使用するには、シスコの LDAP アトリビュートの名前と値およびユーザ定義のアトリビュートの名前と値を理解する必要があります。

グローバル コンフィギュレーション モードで入力された次のコマンドでは、att\_map\_1 という名前の空の LDAP アトリビュート マップ テーブルを作成しています。

```
hostname(config)# ldap attribute-map att_map_1
hostname(config-ldap-attribute-map)#
```

次のコマンドでは、ユーザ定義のアトリビュート名 department をシスコのアトリビュート名 cVPN3000-IETF-Radius-Class に対応付けています。2 番目のコマンドでは、ユーザ定義のアトリビュート値 Engineering をユーザ定義のアトリビュート department とシスコで定義されているアトリビュート値 group1 に対応付けています。

```
hostname(config)# ldap attribute-map att_map_1
hostname(config-ldap-attribute-map)# map-name department cVPN3000-IETF-Radius-Class
hostname(config-ldap-attribute-map)# map-value department Engineering group1
hostname(config-ldap-attribute-map)#
```

次のコマンドでは、アトリビュート マップ att\_map\_1 を LDAP サーバ ldap\_dir\_1 にバインドしています。

```
hostname(config)# aaa-server ldap_dir_1 host 10.1.1.4
hostname(config-aaa-server-host)# ldap-attribute-map att_map_1
hostname(config-aaa-server-host)#
```



(注)

アトリビュート マップを作成するコマンド (ldap attribute-map) と LDAP サーバにそれをバインドするコマンド (ldap-attribute-map) の違いは、ハイフンの有無とモードだけです。

次のコマンドでは、実行コンフィギュレーション内のすべての LDAP アトリビュート マップを表示または消去しています。

```
hostname# show running-config all ldap attribute-map
hostname(config)# clear configuration ldap attribute-map
hostname(config)#
```

頻繁に対応付けられるシスコの LDAP アトリビュートの名前と、一般に対応付けられることの多いユーザ定義のアトリビュートのタイプには、次のものがあります。

```
cVPN3000-IETF-Radius-Class - Department or user group
cVPN3000-IETF-Radius-Filter-Id - Access control list
cVPN3000-IETF-Radius-Framed-IP-Address - A static IP address
cVPN3000-IPSec-Banner1 - A organization title
cVPN3000-Tunneling-Protocols - Allow or deny dial-in
```

シスコの LDAP アトリビュートの名前と値のリストについては、[付録 E「認可および認証用の外部サーバの設定」](#)を参照してください。または、次の例のように、ldap-attribute-map モードで「?」を入力して、シスコの LDAP アトリビュート名の一覧をすべて表示することもできます。

```
hostname(config)# ldap attribute-map att_map_1
hostname(config-ldap-attribute-map)# map-name att_map_1 ?

ldap mode commands/options:
cisco-attribute-names:
  cVPN3000-Access-Hours
  cVPN3000-Allow-Network-Extension-Mode
  cVPN3000-Auth-Service-Type
  cVPN3000-Authenticated-User-Idle-Timeout
  cVPN3000-Authorization-Required
  cVPN3000-Authorization-Type
  :
  :
  cVPN3000-X509-Cert-Data
hostname(config-ldap-attribute-map)#
```

## HTTP Form での WebVPN に対する SSO サポート

セキュリティ アプライアンスは、WebVPN ユーザの Single Sign-On (SSO; シングル サインオン) 認証だけに HTTP Form プロトコルを使用できます。SSO がサポートされていると、WebVPN ユーザはユーザ名とパスワードを一度入力するだけで、複数の保護されたサービスや Web サーバにアクセスできます。セキュリティ アプライアンス上で実行されている WebVPN サーバは、認証サーバにアクセスするユーザのプロキシとして機能します。ユーザがログインすると、WebVPN サーバは HTTPS を使用して認証サーバに SSO 認証要求を送信します。要求にはユーザ名とパスワードが含まれます。サーバは認証要求を承認した場合、SSO 認証クッキーを WebVPN サーバに返します。セキュリティ アプライアンスは、ユーザの代理としてこのクッキーを保持し、SSO サーバによって保護されているドメイン内のセキュア Web サイトに対してユーザを認証するために使用します。

HTTP Form で SSO を実装するほかに、WebVPN 管理者は Computer Associates eTrust SiteMinder SSO サーバ (旧称 Netegrity SiteMinder) を使用して SSO 認証を設定することも選択できます。HTTP Form または SiteMinder での SSO の設定の詳細については、「[WebVPN の設定](#)」の章を参照してください。

## ローカル データベースのサポート

セキュリティ アプライアンスは、ユーザ プロファイルを取り込むことができるローカル データベースを管理します。

ここでは、次の項目について説明します。

- ユーザ プロファイル (P.10-13)
- ローカル データベースの機能 (P.10-13)
- フォールバック サポート (P.10-14)

## 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ています。通常、パスワードはオプションですが、各ユーザ名にパスワードが割り当てられます。

**username attributes** コマンドによって、ユーザ名モードに移行することができます。このモードでは、特定のユーザ プロファイルにその他の情報を追加できます。追加できる情報には、VPN セッション タイムアウト値など VPN 関連アトリビュートが含まれます。

## ローカル データベースの機能

セキュリティ アプライアンスは、表 10-4 に説明されている機能に関して、ローカル データベースを使用できます。

表 10-4 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 コンソール接続でセキュリティ アプライアンスにアクセスしようとしたとき、トラフィックが認証文と一致する場合、セキュリティ アプライアンスはユーザのユーザ名とパスワードを要求し、クレデンシャルをローカル データベースと照合してチェックし、その結果に基づいてユーザの CLI アクセスを許可または拒否します。 |
| <b>enable</b> コマンドまたは <b>login</b> コマンドのユーザ認証 | ユーザが <b>enable</b> コマンドにアクセスしようとする、セキュリティ アプライアンスはユーザのパスワードを要求し、ユーザ名とパスワードをローカル データベースと照合してチェックし、その結果に基づいてイネーブル モードへのユーザのアクセスを許可または拒否します。                                             |
| 管理コマンドのユーザ認可                                  | ユーザが <b>enable</b> コマンドで認証（または <b>login</b> コマンドでログイン）する場合、セキュリティ アプライアンスはそのユーザを、ローカル データベースによって定義された特権レベルに配置します。各コマンドは、コマンドが 0 ～ 15 の特権レベルに属するように、セキュリティ アプライアンスに設定できます。             |
| ネットワーク アクセスのユーザ認証                             | ユーザがセキュリティ アプライアンスを使用してネットワークにアクセスしようとしたとき、トラフィックが認証文と一致する場合、セキュリティ アプライアンスはユーザのユーザ名とパスワードを要求し、クレデンシャルをローカル データベースと照合してチェックし、その結果に基づいてユーザのネットワーク アクセスを許可または拒否します。                     |
| VPN 認証                                        | ユーザが VPN アクセスを確立しようとしたとき、トラフィックが認証文と一致する場合、セキュリティ アプライアンスは、受信したユーザ名とパスワードをローカル ユーザ データベースと照合してチェックし、その結果に基づいて VPN アクセスを許可または拒否します。                                                    |
| VPN 認可                                        | VPN アクセスのユーザ認証が成功した場合、セキュリティ アプライアンスは、ユーザ名と適用可能なグループポリシーに関連するローカル データベースからのアトリビュートを VPN セッションに適用します。                                                                                  |

## フォールバック サポート

ネットワーク アクセス認証のフォールバックを除き、ローカル データベースは、表 10-4 の機能のフォールバック方式として動作します。この動作は、セキュリティ アプライアンスから誤ってロックアウトされないようにすることを意図しています。

フォールバック サポートを必要とするユーザでは、ローカル データベース内のユーザ名とパスワードと AAA サーバ内のユーザ名とパスワードを一致させることをお勧めします。これにより、透過フォールバックがサポートされます。ユーザは、AAA サーバとローカル データベースのどちらがサービスを提供しているかが判別できないので、ローカル データベースのユーザ名およびパスワードとは異なるユーザ名およびパスワードを AAA サーバで使用する場合は、指定すべきユーザ名とパスワードをユーザが確信できないことを意味します。

ローカル データベースでサポートされているフォールバック機能は次のとおりです。

- **コンソールおよびイネーブル パスワード認証**：aaa authentication console コマンドを使用する場合、AAA サーバ グループ タグの後に **LOCAL** キーワードが追加できます。グループ内のサーバがすべて使用できない場合、セキュリティ アプライアンスはローカル データベースを使用して管理アクセスを認証します。これには、イネーブル パスワード認証も含めることができます。
- **コマンド認可**：aaa authorization command コマンドを使用する場合、AAA サーバ グループ タグの後に **LOCAL** キーワードが追加できます。グループ内の TACACS+ サーバがすべて使用できない場合、特権レベルに基づいてコマンドを認可するためにローカル データベースが使用されます。
- **VPN 認証および認可**：VPN 認証および認可は、通常この VPN サービスをサポートしている AAA サーバが使用できない場合、セキュリティ アプライアンスへのリモートアクセスをイネーブルにするためにサポートされます。authentication-server-group コマンド（トンネルグループ一般アトリビュート モードで使用可能）を使用すると、トンネルグループのアトリビュートを設定するときに、**LOCAL** キーワードが指定できます。管理者である VPN クライアントが、ローカル データベースへのフォールバックを設定されたトンネルグループを指定する場合、AAA サーバ グループが使用できない場合でも、ローカル データベースが必要なアトリビュートで設定されていれば、VPN トンネルが確立できます。

## 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の管理方法について説明します。ローカル データベースは、CLI アクセス認証、特権モード認証、コマンド認可、ネットワーク アクセス認証、および VPN 認証および認可に使用できます。ネットワーク アクセス認証には、ローカル データベースは使用できません。ローカル データベースはアカウンティングをサポートしません。

マルチコンテキスト モードの場合、システム実行スペースでユーザ名を設定し、**login** コマンドを使用して個々のログインを指定できます。しかし、システム実行スペースでは **aaa** コマンドは設定できません。



### 注意

CLI にはアクセスできるが、特権モードに移行することは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、コマンド認可をイネーブルにします（P.33-9 の「[ローカル コマンド認可の設定](#)」を参照してください）。コマンド認可を行わないと、ユーザは、特権レベルが 2 以上（2 がデフォルト）の場合、CLI で自分のパスワードを使用して特権モード（およびすべてのコマンド）にアクセスできます。あるいは、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することも、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特権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。

LOCAL データベースにユーザ アカウントを定義するには、次の手順を実行します。

**ステップ 1** ユーザ アカウントを作成します。これを行うには、次のコマンドを入力します。

```
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 文字の文字列。
- **password password** : 3 ～ 16 文字の文字列。
- **encrypted** : 指定された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特権レベル（0 ～ 15）。デフォルトは 2 です。この特権レベルはコマンド認可で使用されます。
- **nopassword** : パスワードを指定しないユーザ アカウントを作成します。

**ステップ 2** VPN アトリビュートを指定してローカル ユーザ アカウントを設定するには、次の手順を実行します。

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場合は、ユーザ名モードに移行します。このモードで使えるコマンドは、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`
- `webvpn`

必要に応じてこれらのコマンドを使用して、ユーザ プロファイルを設定します。これらのコマンドの詳細については、『*Cisco Security Appliance 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完了したら、**exit**を入力して設定モードに戻ります。

---

たとえば、次のコマンドは、admin ユーザ アカウントに対して特権レベル 15 を割り当てます。

```
hostname/contexta(config)# username admin password passw0rd privilege 15
```

次のコマンドは、パスワードを指定しないユーザ アカウントを作成します。

```
hostname/contexta(config)# username bcham34 nopassword
```

次のコマンドは、パスワードを指定するユーザ アカウントを作成し、ユーザ名モードに移行して、いくつかの VPN アトリビュートを指定します。

```
hostname/contexta(config)# username rwilliams password g0ge0us
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、認可、またはアカウントिंगに外部 AAA サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの AAA サーバグループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。AAA サーバグループは名前で識別されます。各サーバグループは、Kerberos、LDAP、NT、RADIUS、SDI、または TACACS+ というサーバの 1 つのタイプ専用となります。

セキュリティ アプライアンスは、グループ内の最初のサーバにアクセスします。そのサーバが使用できない場合、セキュリティ アプライアンスはグループ内の次のサーバにアクセスします（設定されている場合）。グループ内のすべてのサーバが使用できない場合、セキュリティ アプライアンスは、ローカル データベースがフォールバック方式として設定されていると、ローカル データベースに接続しようとします（管理認証および認可のみ）。フォールバック方式として設定されていない場合、セキュリティ アプライアンスは引き続き AAA サーバにアクセスしようとします。

サーバグループを作成して、AAA サーバを追加するには、次の手順を実行します。

### ステップ 1 作成する必要がある AAA サーバについて、次の手順を実行します。

- a. サーバグループ名とプロトコルを指定します。これを行うには、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、TACACS+ を使用して CLI アクセスを認証するには、RADIUS サーバ用に 1 つ、TACACS+ サーバ用に 1 つというように、最低 2 つのサーバグループを作成する必要があります。

最大 15 のシングルモード サーバグループまたは 4 つのマルチモード サーバグループを指定できます。各サーバグループには、シングルモードで最大 16 台、マルチモードで最大 4 台のサーバを含めることができます。

**aaa-server protocol** コマンドを入力する場合は、グループモードに移行します。

- b. 次のサーバを作成する前に、グループ内の AAA サーバに送信される要求の最大数を指定する場合は、次のコマンドを入力します。

```
hostname/contexta(config-aaa-server-group)# max-failed-attempts number
```

**number** には、1 ～ 5 が指定できます。デフォルトは 3 です。

ローカル データベースを使用してフォールバック方式を設定し（管理アクセスのみの場合は、[P.33-6 の「システム管理者の AAA」](#) および [P.33-12 の「TACACS+ コマンド認可の設定」](#) を参照してフォールバック メカニズムを設定）、グループ内のすべてのサーバが応答できなかった場合、グループは非応答と見なされ、フォールバック方式が試行されます。サーバグループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続いたら、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、セキュリティ アプライアンスは引き続きグループ内のサーバにアクセスしようとします。

- c. グループ内の障害の発生したサーバが再度アクティブ化される方法（再アクティブ化ポリシー）を指定する場合は、**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、『*Cisco Security Appliance 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が単一のサーバに送信されるか（シングルモード）またはグループ内のすべてのサーバに送信されるか（同時モード）を指示する場合は、**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、『*Cisco Security Appliance Command Reference*』を参照してください。
- e. AAA サーバグループの設定が終了したら、**exit** を入力します。

**ステップ 2** ネットワーク上の各 AAA サーバについて、次の手順を実行します。

- a. サーバを、所属する AAA サーバ グループを含めて、指定します。これを行うには、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場合、ホスト モードに移行します。

- b. 必要に応じて、ホスト モード コマンドを使用して、さらに AAA サーバを設定します。

ホスト モードでのコマンドはすべての AAA サーバ タイプに適用されるわけではありません。[表 10-5](#) に、使用可能なコマンド、適用先のサーバタイプ、および新規 AAA サーバ定義にそのコマンドのデフォルト値が指定されているかどうかを示します。コマンドが、指定したサーバタイプに適用可能で、デフォルト値が用意されていない場合は（「—」で示す）、コマンドを使用して値を指定します。これらのコマンドの詳細については、『Cisco Security Appliance Command Reference』を参照してください。

**表 10-5 ホスト モード コマンド、サーバタイプ、およびデフォルト**

| 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           |
| acl-netmask-convert       | RADIUS            | 標準             |
| authentication-port       | RADIUS            | 1645           |
| kerberos-realm            | Kerberos          | —              |
| key                       | RADIUS            | —              |
|                           | TACACS+           | —              |
| ldap-attribute-map        | LDAP              | —              |
| ldap-base-dn              | LDAP              | —              |
| ldap-login-dn             | LDAP              | —              |
| ldap-login-password       | LDAP              | —              |
| ldap-naming-attribute     | LDAP              | —              |
| ldap-over-ssl             | LDAP              | —              |
| ldap-scope                | LDAP              | —              |
| nt-auth-domain-controller | NT                | —              |
| radius-common-pw          | RADIUS            | —              |
| retry-interval            | Kerberos          | 10 秒           |
|                           | RADIUS            | 10 秒           |
|                           | SDI               | 10 秒           |
| sasl-mechanism            | LDAP              | —              |
| sdi-pre-5-slave           | SDI               | —              |
| sdi-version               | SDI               | sdi-5          |
| server-port               | Kerberos          | 88             |
|                           | LDAP              | 389            |
|                           | NT                | 139            |
|                           | SDI               | 5500           |
|                           | TACACS+           | 49             |
| server-type               | LDAP              | auto-discovery |
| timeout                   | すべて               | 10 秒           |

c. AAA サーバ ホストの設定が終了したら、**exit**を入力します。

例 10-1 に、1つのプライマリ サーバと 1つのバックアップ サーバを持つ 1つの TACACS+ グループ、単一のサーバを持つ 1つの RADIUS グループ、および 1つの NT ドメイン サーバを追加するコマンドを示します。

#### 例 10-1 複数の AAA サーバグループおよびサーバ

```
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 NTAAuth protocol nt
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server NTAAuth (inside) host 10.1.1.4
hostname/contexta(config-aaa-server-host)# nt-auth-domain-controller primary1
hostname/contexta(config-aaa-server-host)# exit
```

例 10-2 に、watchdogs という名前の Kerberos AAA サーバグループを設定し、AAA サーバをそのグループに追加し、そのサーバの Kerberos 領域を定義するコマンドを示します。例 10-2 では、リトライ インターバルと Kerberos サーバがリスンするポートを定義していないため、セキュリティ アプライアンスは、これら 2つのサーバ固有のパラメータにデフォルト値を使用します。表 10-5 に、すべての AAA サーバ ホスト モード コマンドのデフォルト値を示します。



(注)

Kerberos 領域名には、数字と大文字だけを使用できます。セキュリティ アプライアンスは、領域名の小文字を受け入れますが、小文字から大文字への変換は実行しません。大文字だけを使用するようにしてください。

#### 例 10-2 Kerberos サーバグループおよびサーバ

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(config)#
```

## 証明書とユーザ ログイン クレデンシャルの使用法

この項では、認証と認可で証明書およびユーザ ログイン クレデンシャル（ユーザ名とパスワード）を使用するさまざまな方法について説明します。この内容は、IPSec と WebVPN の両方に適用されます。

すべての場合において、LDAP 認可では、パスワードはクレデンシャルとして使用されません。RADIUS 認可では、すべてのユーザの共通パスワードかユーザ名のいずれかがパスワードとして使用されます。

### ユーザ ログイン クレデンシャルの使用法

認証と認可のデフォルトの方法では、ユーザ ログイン クレデンシャルが使用されます。

- 認証
  - 認証サーバ グループ設定によってイネーブル化されます。
  - ユーザ名とパスワードがクレデンシャルとして使用されます。
- 認可
  - 認可サーバ グループ設定によってイネーブル化されます。
  - ユーザ名がクレデンシャルとして使用されます。

### 証明書の使用法

ユーザ デジタル証明書が設定されている場合、セキュリティ アプライアンスは最初に証明書を検証します。ただし、証明書の DN は認証用のユーザ名として使用されません。

認証と認可の両方がイネーブルの場合、セキュリティ アプライアンスはユーザの認証と認可の両方にユーザ ログイン クレデンシャルを使用します。

- 認証
  - 認証サーバ グループ設定によってイネーブル化されます。
  - ユーザ名とパスワードがクレデンシャルとして使用されます。
- 認可
  - 認可サーバ グループ設定によってイネーブル化されます。
  - ユーザ名がクレデンシャルとして使用されます。

認証がディセーブルで認可がイネーブルの場合、セキュリティ アプライアンスは認可にプライマリ DN フィールドを使用します。

- 認証
  - 認証サーバ グループ設定によって DISABLED（None に設定）されます。
  - クレデンシャルは使用されません。
- 認可
  - 認可サーバ グループ設定によってイネーブル化されます。
  - 証明書のプライマリ DN フィールドのユーザ名の値がクレデンシャルとして使用されます。



**(注)**

プライマリ DN フィールドが証明書に存在しない場合、セキュリティ アプライアンスはセカンダリ DN フィールドの値を認可要求でユーザ名として使用します。

たとえば、次の Subject DN フィールドと値が含まれているユーザ証明書があるとします。

**Cn=anyuser,OU=sales,O=XYZCorporation,L=boston,S=mass,C=us;ea=anyuser@example.com.**

Primary DN = EA（電子メール アドレス）で、Secondary DN = CN（通常名）である場合、認可要求で使用されるユーザ名は anyuser@example.com となります。





# フェールオーバーの設定

---

この章では、セキュリティ アプライアンスのフェールオーバー機能について説明します。この機能を使用すると、2つのセキュリティ アプライアンスを設定して、一方の装置が故障した場合に、もう一方の装置が動作を引き継ぐようにできます。

次の事項について説明します。

- [フェールオーバーの概要 \(P.11-2\)](#)
- [フェールオーバーの設定 \(P.11-19\)](#)
- [フェールオーバーの制御およびモニタリング \(P.11-49\)](#)
- [フェールオーバー コンフィギュレーションの例 \(P.11-51\)](#)

## フェールオーバーの概要

フェールオーバー設定には、同じセキュリティ アプライアンスが 2 台、専用のフェールオーバー リンク（オプションで、ステートフル フェールオーバー リンク）で相互に接続されている必要があります。アクティブ インターフェイスおよび装置のヘルスが監視されて、所定のフェールオーバー条件に一致しているかどうか判断されます。所定の条件に一致すると、フェールオーバーが行われます。

セキュリティ アプライアンスは、Active/Active フェールオーバーと Active/Standby フェールオーバーの 2 つのフェールオーバーをサポートします。各フェールオーバー コンフィギュレーションには、フェールオーバーを判定および実行する独自の方式があります。

Active/Active フェールオーバーでは、両方の装置がネットワーク トラフィックを渡すことができます。これによって、ネットワークのロードバランシングを設定できます。Active/Active フェールオーバーは、マルチコンテキスト モードで実行中の装置でのみ使用できます。

Active/Standby フェールオーバーでは、1 つの装置だけがトラフィックを渡すことができ、もう 1 つの装置はスタンバイ状態で待機します。Active/Standby フェールオーバーは、シングルコンテキスト モードで実行中の装置とマルチコンテキスト モードで実行中の装置の両方で使用できます。

両フェールオーバー コンフィギュレーションとも、ステートフルまたはステートレス（通常）フェールオーバーをサポートします。



(注)

VPN フェールオーバーは、マルチコンテキスト モードで動作中の装置ではサポートされません。VPN フェールオーバーは、Active/Standby フェールオーバー コンフィギュレーションに限り使用できます。

ここでは、次の項目について説明します。

- [フェールオーバーのシステム要件 \(P.11-2\)](#)
- [フェールオーバー リンクとステートフル フェールオーバー リンク \(P.11-3\)](#)
- [Active/Active フェールオーバーと Active/Standby フェールオーバー \(P.11-7\)](#)
- [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 \(P.11-16\)](#)
- [フェールオーバー ヘルスのモニタリング \(P.11-17\)](#)

## フェールオーバーのシステム要件

ここでは、フェールオーバー コンフィギュレーションにあるセキュリティ アプライアンスのハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。ここでは、次の項目について説明します。

- [ハードウェア要件 \(P.11-2\)](#)
- [ソフトウェア要件 \(P.11-3\)](#)
- [ライセンス要件 \(P.11-3\)](#)

### ハードウェア要件

フェールオーバー コンフィギュレーションでは、2 台の装置が同じハードウェア コンフィギュレーションになっていなければなりません。つまり、同じモデル、同じ数およびタイプのインターフェイス、同じフラッシュ メモリ量、および同じ RAM 量でなければなりません。



## ソフトウェア要件

フェールオーバー コンフィギュレーションの 2 台の装置は同じ動作モード（ルーテッドまたは透過、シングルコンテキストまたはマルチコンテキスト）でなければなりません。ソフトウェアバージョンは、メジャー（最初の番号）およびマイナー（2 番目の番号）ともに同じである必要があります。ただし、アップグレードプロセス中は、異なるバージョンのソフトウェアを使用できます。たとえば、ある装置をバージョン 7.0(1) からバージョン 7.0(2) にアップグレードし、フェールオーバーをアクティブ状態のままにできます。長期的に互換性を維持するために、両方の装置を同じバージョンにアップグレードすることをお勧めします。

## ライセンス要件

PIX セキュリティ アプライアンス プラットフォームでは、少なくとも 1 台の装置に無制限（UR）ライセンスが必要です。もう一方の装置は、Failover Only (FO) ライセンス、Failover Only Active-Active (FO\_AA) ライセンス、または別の UR ライセンスのどれでもかまいません。制限付きライセンスの装置はフェールオーバーには使用できません。FO または FO\_AA ライセンスの装置 2 台をフェールオーバー ペアとして一緒に使用することはできません。

**(注)**

FO ライセンスは、Active/Active フェールオーバーをサポートしません。

FO ライセンスおよび FO\_AA ライセンスは、フェールオーバー コンフィギュレーションの装置にのみ使用することが予定されており、スタンドアロン モードの装置で使用するとは考えられていません。このいずれかのライセンスのフェールオーバー装置をスタンドアロン モードで使用すると、フェールオーバー動作に戻るまで、少なくとも 24 時間に 1 回リブートされます。FO または FO\_AA ライセンスの装置は、UR ライセンスのフェールオーバー ピアに接続されていない状態でブートされると、スタンドアロン モードで動作します。フェールオーバー ペアの UR ライセンスの装置が故障して、コンフィギュレーションから削除された場合、FO または FO\_AA ライセンスの装置は、24 時間ごとに自動的にリブートすることはなくなります。手動でリブートされない限り、中断することなく動作します。

装置が自動的にリブートされると、次のメッセージがコンソールに表示されます。

```
=====NOTICE=====
This machine is running in secondary mode without
a connection to an active primary PIX. Please
check your connection to the primary system.

REBOOTING....
=====
```

ASA プラットフォームには、この制限はありません。

## フェールオーバー リンクとステートフル フェールオーバー リンク

ここでは、フェールオーバー リンクおよびステートフル フェールオーバー リンクについて説明します。これらのリンクは、フェールオーバー コンフィギュレーションで 2 台の装置を接続する専用のリンクです。ここでは、次の項目について説明します。

- [フェールオーバー リンク \(P.11-4\)](#)
- [ステートフル フェールオーバー リンク \(P.11-6\)](#)

## フェールオーバー リンク

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態（アクティブまたはスタンバイ）
- 電源ステータス（ケーブルベースのフェールオーバーのみ：Cisco PIX セキュリティ アプライアンス プラットフォームに限り使用可能）
- hello メッセージ（キープアライブ）
- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期



### 注意

フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

PIX セキュリティ アプライアンスの場合、フェールオーバー リンクは LAN ベースの接続または専用のシリアル フェールオーバー ケーブルです。ASA プラットフォームの場合、フェールオーバー リンクは LAN ベースの接続のみです。

ここでは、次の項目について説明します。

- [LAN ベースのフェールオーバー リンク \(P.11-4\)](#)
- [シリアルケーブル フェールオーバー リンク \(PIX セキュリティ アプライアンスのみ\) \(P.11-5\)](#)

## LAN ベースのフェールオーバー リンク

装置上のイーサネット インターフェイスは、使用されていなければどれでも、フェールオーバー リンクとして使用できます。現在名前が設定されているインターフェイスは指定できません。フェールオーバー リンク インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー通信のためにのみ存在します。このインターフェイスは、フェールオーバー リンク（および、オプションでステートフル フェールオーバー リンク）専用とする必要があります。LAN ベースのフェールオーバー リンクを接続するには、そのリンク上にホストもルータもない専用スイッチを使用することも、装置を直接リンクするクロスオーバー イーサネット ケーブルを使用することもできます。



### (注)

VLAN を使用する場合は、フェールオーバー リンク専用の VLAN を使用します。フェールオーバー リンク VLAN を他の VLAN と共有すると、トラフィックが途切れ途切れになるという問題、あるいは ping 障害や ARP 障害が発生することがあります。スイッチを使用してフェールオーバー リンクを接続する場合は、フェールオーバー リンクには、スイッチおよびセキュリティ アプライアンス上の専用インターフェイスを使用します。このインターフェイスは、通常のネットワーク トラフィックを転送するサブインターフェイスと共有しないでください。

マルチコンテキスト モードで動作中のシステムの場合、フェールオーバー リンクはシステム コンテキストに存在します。このインターフェイスとステートフル フェールオーバー リンク（使用される場合）のみが、システム コンテキストで設定できるインターフェイスです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。



(注)

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、フェールオーバー時に変更されません。

### シリアル ケーブル フェールオーバー リンク (PIX セキュリティ アプライアンスのみ)

シリアル フェールオーバー ケーブル、つまり「ケーブルベースのフェールオーバー」、は PIX セキュリティ アプライアンス プラットフォームでのみ使用できます。2 台の装置の距離が約 1.8 m 以内の場合は、シリアル フェールオーバー ケーブルを使用することをお勧めします。

2 台の装置を接続するケーブルは、117,760 bps (115 Kbps) でデータを転送する修正 RS-232 シリアル リンク ケーブルです。ケーブルの一方の端には「Primary」のラベルが付いています。ケーブルのこの端に接続される装置は、自動的にプライマリ装置になります。ケーブルのもう一方の端には「Secondary」のラベルが付いています。ケーブルのこの端に接続される装置は、自動的にセカンダリ装置になります。PIX セキュリティ アプライアンス ソフトウェアでこれらの指定を上書きすることはできません。PIX セキュリティ アプライアンス フェールオーバー バンドルを購入すると、このケーブルが含まれています。予備を注文する場合は、部品番号 PIX-FO= を使用します。

ケーブルベースのフェールオーバーを使用する利点は次のとおりです。

- PIX セキュリティ アプライアンスは、ピア装置の電源断を即時に検出でき、さらに電源断とケーブルが外れているのを区別できます。
- スタンバイ装置はアクティブ装置と通信でき、またフェールオーバーのブートストラップを行わなくても、コンフィギュレーション全体を受信できます。LAN ベースのフェールオーバーでは、スタンバイ装置がアクティブ装置と通信するには、事前にスタンバイ装置にフェールオーバー リンクを設定しておく必要があります。
- LAN ベースのフェールオーバーで 2 台の装置間のスイッチが、別のハードウェア障害ポイントとなる場合があります。ケーブルベースのフェールオーバーでは、この潜在的な障害ポイントはなくなります。
- イーサネット インターフェイス（およびスイッチ）をフェールオーバー リンク専用にする必要はありません。
- ケーブルによってプライマリ装置とセカンダリ装置が判別されるため、装置コンフィギュレーションでその情報を手動で入力する必要がなくなります。

欠点は次のとおりです。

- 距離の制限：装置は約 1.8 m 以上離せません。
- コンフィギュレーションの複製に時間がかかります。

## ステートフル フェールオーバー リンク

ステートフル フェールオーバーを使用するには、ステートフル フェールオーバー リンクを設定してすべてのステート情報を渡す必要があります。ステートフル フェールオーバー リンクを設定する方法としては、次の 3 つのオプションがあります。

- ステートフル フェールオーバー リンクに、専用のイーサネット インターフェイスを使用できます。
- LAN ベースのフェールオーバーを使用している場合は、フェールオーバー リンクを共有できます。
- 内部インターフェイスなど、通常のデータ インターフェイスを共有できます。しかし、このオプションは推奨しません。

ステートフル フェールオーバー リンクに専用のイーサネット インターフェイスを使用している場合、スイッチまたはクロスオーバー ケーブルを使用して装置を直接接続できます。スイッチを使用している場合、他のホストまたはルータをこのリンクに配置しないでください。



(注)

セキュリティ アプライアンスに直接接続されているシスコ スイッチ ポートの PortFast オプションをイネーブルにします。

フェールオーバー リンクをステートフル フェールオーバー リンクとして使用している場合は、使用可能な最も速いイーサネット インターフェイスを使用します。このインターフェイスでパフォーマンス上の問題が発生した場合は、別のインターフェイスをステートフル フェールオーバー インターフェイス専用にすることを検討してください。

データ インターフェイスをステートフル フェールオーバー リンクとして使用する場合、そのインターフェイスをステートフル フェールオーバー リンクと指定すると、次の警告が表示されます。

```
***** WARNING ***** WARNING ***** WARNING ***** WARNING *****
Sharing Stateful failover interface with regular data interface is not
a recommended configuration due to performance and security concerns.
***** WARNING ***** WARNING ***** WARNING ***** WARNING *****
```

データ インターフェイスとステートフル フェールオーバー インターフェイスを共有すると、リプレイ攻撃を受けやすくなる場合があります。さらに、大量のステートフル フェールオーバー トラフィックがインターフェイスで送信され、そのネットワーク セグメントでパフォーマンス上の問題が発生することがあります。



(注)

データ インターフェイスをステートフル フェールオーバー インターフェイスとして使用するのには、シングルコンテキストのルーテッド モードでのみサポートされます。

マルチコンテキスト モードでは、ステートフル フェールオーバー リンクはシステム コンテキストに存在します。このインターフェイスとフェールオーバー インターフェイスが、システム コンテキスト内にある唯一のインターフェイスです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。



(注)

ステートフル フェールオーバー リンクが通常のデータ インターフェイスに設定されていない限り、ステートフル フェールオーバー リンクの IP アドレスと MAC アドレスは、フェールオーバー時に変更されません。

**注意**

フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

## Active/Active フェールオーバーと Active/Standby フェールオーバー

ここでは、各フェールオーバー コンフィギュレーションについて詳細に説明します。ここでは、次の項目について説明します。

- [Active/Standby フェールオーバー \(P.11-7\)](#)
- [Active/Active フェールオーバー \(P.11-11\)](#)
- [使用するフェールオーバーのタイプの決定 \(P.11-15\)](#)

## Active/Standby フェールオーバー

ここでは、Active/Standby フェールオーバーについて次の項目で説明します。

- [Active/Standby フェールオーバーの概要 \(P.11-7\)](#)
- [Primary/Secondary ステータスと Active/Standby ステータス \(P.11-8\)](#)
- [装置の初期化とコンフィギュレーションの同期 \(P.11-8\)](#)
- [コマンドの複製 \(P.11-9\)](#)
- [フェールオーバーのトリガー \(P.11-9\)](#)
- [フェールオーバーのアクション \(P.11-10\)](#)

## Active/Standby フェールオーバーの概要

Active/Standby フェールオーバーでは、スタンバイ セキュリティ アプライアンスを使用して、障害の発生した装置の機能を引き継ぎます。アクティブ装置が故障すると、スタンバイ状態に変わり、そしてスタンバイ装置がアクティブ状態に変わります。アクティブになる装置が、障害の発生した装置の IP アドレス（または、透過ファイアウォールの場合は管理 IP アドレス）および MAC アドレスを引き継いで、トラフィックの転送を開始します。現在スタンバイになっている装置が、スタンバイの IP アドレスと MAC アドレスを引き継ぎます。ネットワーク装置は、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどこにおいても ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

**(注)**

マルチコンテキスト モードの場合、セキュリティ アプライアンスは装置全体（すべてのコンテキストを含む）をフェールオーバーできますが、個々のコンテキストを別々にフェールオーバーすることはできません。

## Primary/Secondary ステータスと Active/Standby ステータス

フェールオーバー ペアの 2 台の装置の主な相違点は、どちらの装置がアクティブでどちらの装置がスタンバイであるか、つまりどちらの IP アドレスを使用するかおよびどちらの装置がアクティブにトラフィックを渡すかということに関連します。

しかし、プライマリである装置（コンフィギュレーションで指定）とセカンダリである装置との間で、いくつかの相違点があります。

- 両方の装置が同時にスタート アップした場合（さらに動作ヘルスが等しい場合）、プライマリ装置が常にアクティブ装置になります。
- プライマリ装置の MAC アドレスは常に、アクティブ IP アドレスと結び付けられています。この規則の例外は、セカンダリ装置がアクティブであり、フェールオーバー リンク経由でプライマリ MAC アドレスを取得できない場合に発生します。この場合、セカンダリ MAC アドレスが使用されます。

## 装置の初期化とコンフィギュレーションの同期

コンフィギュレーションの同期は、フェールオーバー ペアの一方または両方の装置がブートされると行われます。コンフィギュレーションは常に、アクティブ装置からスタンバイ装置に同期化されます。スタンバイ装置は、その初期スタートアップを完了すると、自分の実行コンフィギュレーションを削除し（アクティブ装置との通信に必要なフェールオーバー コマンドを除く）、アクティブ装置は自分のコンフィギュレーション全体をスタンバイ装置に送信します。

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時にブートされた場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。



(注)

セカンダリ装置がブートされてプライマリ装置を検出できないと、その装置はアクティブ装置になります。アクティブ IP アドレスには、セカンダリ装置自体の MAC アドレスを使用します。しかし、プライマリ装置が使用可能になると、セカンダリ装置は MAC アドレスをプライマリ装置の MAC アドレスに変更します。これによって、ネットワークトラフィックが中断されることがあります。これを回避するには、フェールオーバー ペアを仮想 MAC アドレスで設定します。詳細については、[P.11-19 の「Active/Standby フェールオーバーの設定」](#)を参照してください。

複製が開始されると、アクティブ装置のセキュリティ アプライアンス コンソールに「Beginning configuration replication: Sending to mate」というメッセージが表示され、複製が完了すると、セキュリティ アプライアンスに「End Configuration Replication to mate」というメッセージが表示されます。複製中、アクティブ装置に入力されたコマンドがスタンバイ装置に適切に複製されないことがあり、またスタンバイ装置に入力されたコマンドが、アクティブ装置から複製されているコンフィギュレーションによって上書きされることがあります。コンフィギュレーションの複製処理中には、フェールオーバー ペアのどちらの装置にもコマンドを入力しないでください。コンフィギュレーションのサイズによって、複製は数秒で済むことも数分かかることもあります。

スタンバイ装置の場合、コンフィギュレーションは実行メモリにのみ存在します。同期化後に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には、次のようにします。

- シングルコンテキスト モードの場合は、アクティブ装置で **copy running-config startup-config** コマンドを使用します。コマンドはスタンバイ装置に複製され、コンフィギュレーション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 モードの場合は、システム実行スペースおよびディスク上の各コンテキスト内からアクティブ装置に **copy running-config startup-config** コマンドを入力します。コマンドはスタンバイ装置に複製され、コンフィギュレーションがフラッシュ メモリに書き込まれます。外部のサーバにスタートアップ コンフィギュレーションがあるコンテキストは、ネットワーク経由で両方の装置からアクセスできます。そのため、各装置で個別に保存する必要はありません。または、ディスク上のコンテキストを、アクティブ装置から外部サーバにコピーし、それからスタンバイ装置のディスクにコピーできます。スタンバイ装置で、装置がリロードされると、そのコンテキストが使用可能になります。

## コマンドの複製

コマンドの複製は常に、アクティブ装置からスタンバイ装置の方向に行われます。アクティブ装置にコマンドを入力すると、そのコマンドがフェールオーバー リンクを通してスタンバイ装置に送信されます。コマンドを複製する場合、アクティブ コンフィギュレーションをフラッシュ メモリに保存する必要はありません。



(注)

スタンバイ装置上で行った変更は、アクティブ装置に複製されません。スタンバイ装置にコマンドを入力すると、セキュリティ アプライアンスに \*\*\*\* WARNING \*\*\*\* Configuration Replication is NOT performed from Standby unit to Active unit. Configurations are no longer synchronized というメッセージが表示されます。このメッセージは、コンフィギュレーションに影響しない数多くのコマンドを入力したときにも表示されます。

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

マルチコンテキスト モードの場合、システム実行スペースに **write standby** コマンドを入力すると、すべてのコンテキストが複製されます。あるコンテキスト内で **write standby** コマンドを入力すると、コマンドはそのコンテキスト コンフィギュレーションのみを複製します。

複製されたコマンドは、実行コンフィギュレーションに保存されます。スタンバイ装置のフラッシュ メモリに複製されたコマンドを保存するには、次のように行います。

- シングルコンテキスト モードの場合は、アクティブ装置で **copy running-config startup-config** コマンドを使用します。コマンドはスタンバイ装置に複製され、コンフィギュレーションがフラッシュ メモリに書き込まれます。
- マルチコンテキスト モードの場合は、システム実行スペースおよびディスク上の各コンテキスト内からアクティブ装置に **copy running-config startup-config** コマンドを入力します。コマンドはスタンバイ装置に複製され、コンフィギュレーションがフラッシュ メモリに書き込まれます。外部のサーバにスタートアップ コンフィギュレーションがあるコンテキストは、ネットワーク経由で両方の装置からアクセスできます。そのため、各装置で個別に保存する必要はありません。または、ディスク上のコンテキストを、アクティブ装置から外部サーバにコピーし、それからスタンバイ装置のディスクにコピーできます。

## フェールオーバーのトリガー

次のいずれかのイベントが発生した場合、装置が故障する可能性があります。

- 装置でハードウェア障害または電源断が発生した。
- 装置でソフトウェア障害が発生した。
- 多くの監視対象インターフェイスが故障した。
- no failover active** コマンドがアクティブ装置に入力されたか、**failover active** コマンドがスタンバイ装置に入力された。



## フェールオーバーのアクション

Active/Standby フェールオーバーでは、フェールオーバーは装置ごとに行われます。マルチコンテキスト モードで動作中のシステムでも、個々のコンテキストまたはコンテキストのグループをフェールオーバーすることはできません。

表 11-1 に、各障害イベントに対するフェールオーバー アクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ装置が行うアクション、スタンバイ装置が行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 11-1 フェールオーバー動作

| 障害の状況                         | ポリシー       | アクティブ<br>アクション                    | スタンバイ<br>アクション                    | 注意                                                                               |
|-------------------------------|------------|-----------------------------------|-----------------------------------|----------------------------------------------------------------------------------|
| アクティブ装置が故障（電源またはハードウェア）       | フェールオーバー   | 該当なし                              | アクティブになる<br>アクティブに故障<br>とマークする    | 監視対象インターフェイスまたはフェールオーバー リンクで hello メッセージは受信されません。                                |
| 以前にアクティブであった装置の復旧             | フェールオーバーなし | スタンバイになる                          | 動作なし                              | なし。                                                                              |
| スタンバイ装置が故障（電源またはハードウェア）       | フェールオーバーなし | スタンバイに故障<br>とマークする                | 該当なし                              | スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。                |
| 動作中にフェールオーバーリンクに障害が発生した       | フェールオーバーなし | フェールオーバー<br>インターフェイス<br>に故障とマークする | フェールオーバー<br>インターフェイス<br>に故障とマークする | フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。 |
| スタートアップ時にフェールオーバー リンクに障害が発生した | フェールオーバーなし | フェールオーバー<br>インターフェイス<br>に故障とマークする | アクティブになる                          | スタートアップ時にフェールオーバー リンクがダウンしていると、両方の装置がアクティブになります。                                 |
| ステートフル フェールオーバー リンクに障害が発生した   | フェールオーバーなし | 動作なし                              | 動作なし                              | ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。                                           |
| アクティブ装置におけるしきい値を超えたインターフェイス障害 | フェールオーバー   | アクティブに故障<br>とマークする                | アクティブになる                          | なし。                                                                              |
| スタンバイ装置におけるしきい値を超えたインターフェイス障害 | フェールオーバーなし | 動作なし                              | スタンバイに故障<br>とマークする                | スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。                |



## Active/Active フェールオーバー

ここでは、Active/Active フェールオーバーについて説明します。ここでは、次の項目について説明します。

- [Active/Active フェールオーバーの概要 \(P.11-11\)](#)
- [Primary/Secondary ステータスと Active/Standby ステータス \(P.11-12\)](#)
- [装置の初期化とコンフィギュレーションの同期 \(P.11-12\)](#)
- [コマンドの複製 \(P.11-13\)](#)
- [フェールオーバーのトリガー \(P.11-13\)](#)
- [フェールオーバー アクション \(P.11-14\)](#)

### Active/Active フェールオーバーの概要

Active/Active フェールオーバーは、マルチコンテキスト モードのセキュリティ アプライアンスでのみ使用できます。Active/Active フェールオーバー コンフィギュレーションでは、両方のセキュリティ アプライアンスがネットワーク トラフィックを渡すことができます。

Active/Active フェールオーバーでは、セキュリティ アプライアンスのセキュリティ コンテキストは、フェールオーバー グループに分割されます。フェールオーバー グループは、1 つまたは複数のセキュリティ コンテキストの論理グループにすぎません。セキュリティ アプライアンスには最大 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 のメンバーであり、未割り当てセキュリティ コンテキストもまた、デフォルトでフェールオーバー グループ 1 のメンバーです。

フェールオーバー グループは、Active/Active フェールオーバーにおいてフェールオーバーの基本単位を形成します。インターフェイス障害モニタリング、フェールオーバー、およびアクティブ/スタンバイ ステータスはすべて、フェールオーバー グループのアトリビュートであって、装置のアトリビュートではありません。アクティブ フェールオーバー グループが故障すると、スタンバイ状態に変化し、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が、故障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 アドレスを引き継ぎます。スタンバイ状態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が、スタンバイ MAC アドレスと IP アドレスを引き継ぎます。



(注)

あるフェールオーバー グループが装置上で故障したというのは、装置が故障したという意味ではありません。その装置では、別のフェールオーバー グループが依然としてトラフィックを渡している場合があります。

フェールオーバー グループを作成する場合は、フェールオーバー グループ 1 がアクティブ状態にある装置に作成する必要があります。



(注)

Active/Active フェールオーバーでは、各フェールオーバー グループのインターフェイスに対して仮想 MAC アドレスが生成されます。同じネットワーク上に Active/Active フェールオーバー ペアが複数ある場合は、あるペアのインターフェイスに割り当てられているものと同じデフォルト仮想 MAC アドレスが、他のペアのインターフェイスに割り当てられることがあります。これは、デフォルト仮想 MAC アドレスの決定方法に基づいた動作です。ネットワーク上で MAC アドレスが重複することを回避するには、必ず各物理インターフェイスに仮想のアクティブおよびスタンバイ MAC アドレスを割り当てます。

## Primary/Secondary ステータスと Active/Standby ステータス

Active/Standby フェールオーバーの場合のように、Active/Active フェールオーバー ペアの一方の装置がプライマリ装置に指定され、もう一方の装置がセカンダリ装置に指定されます。Active/Standby フェールオーバーの場合とは異なり、両方の装置が同時に起動された場合、この指定ではどちらの装置がアクティブになるか指示しません。代わりに、プライマリ/セカンダリ指定によって、ペアに実行コンフィギュレーションを提供する装置と、両方の装置が同時に起動された場合に各フェールオーバー グループがアクティブ状態で表示される装置が決定されます。

コンフィギュレーションの各フェールオーバー グループには、プライマリまたはセカンダリ装置プリファレンスが付与されます。このプリファレンスによって、両方の装置が同時に起動された場合に、フェールオーバー ペアのどちらの装置で、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状態で表示されるかが決定されます。両方のフェールオーバー グループをペアのある 1 つの装置でアクティブ状態にして、もう一方の装置にはスタンバイ状態のフェールオーバー グループが含まれるようにできます。しかし、さらに一般的なコンフィギュレーションでは、各フェールオーバー グループに異なる役割プリファレンスを割り当て、装置ごとにそれぞれ 1 つをアクティブにして、装置全体でトラフィックのバランスがとれるようにします。



(注)

セキュリティ アプライアンスには、ロードバランシング サービスは用意されていません。ロードバランシングは、セキュリティ アプライアンスにトラフィックを渡すルータが処理する必要があります。

## 装置の初期化とコンフィギュレーションの同期

コンフィギュレーションの同期がとられるのは、フェールオーバー ペアの一方または両方の装置がブートされたときです。

ピア装置が使用できないときに装置がブートされると、フェールオーバー グループおよび装置のプライマリまたはセカンダリ指定には関係なく、両方のフェールオーバー グループがその装置でアクティブになります。コンフィギュレーションの同期はとられません。ピア装置が使用できない場合があるのは、ピア装置の電源が切断されている、ピア装置が故障状態である、または装置間のフェールオーバー リンクが確立されていない、などの理由が考えられます。

ピア装置がアクティブ（ピア装置で両方のフェールオーバー グループがアクティブ）の間に装置がブートされると、ブートされた装置はアクティブ装置にアクセス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、フェールオーバー グループは、アクティブ装置でアクティブのままです。これは、各フェールオーバー グループのプライマリ プリファレンスまたはセカンダリ プリファレンス、および装置指定には関係ありません。フェールオーバー グループは、フェールオーバーが行われるか、または **no failover active** コマンドでもう一方の装置に手動で強制的にフェールオーバーされるまで、その装置でアクティブのままです。しかし、**preempt** コマンドを使用すると、優先する装置が使用可能になったときに、その装置上でアクティブになるように、各フェールオーバー グループを設定できます。フェールオーバー グループは、**preempt** コマンドで設定されている場合、優先する装置が使用可能になると、その装置上で自動的にアクティブになります。

両方の装置が同時にブートされる場合、プライマリ装置がアクティブ装置になります。セカンダリ装置は、実行コンフィギュレーションをプライマリ装置から取得します。コンフィギュレーションが同期化されると、各フェールオーバー グループが優先する装置上でアクティブになります。

## コマンドの複製

両方の装置が動作中になった後で、次のように、コマンドが一方の装置からもう一方の装置に複製されます。

- セキュリティ コンテキスト内で入力されたコマンドは、そのセキュリティ コンテキストがアクティブ状態で表示される装置からピア装置に複製されます。



(注) あるコンテキストがある装置でアクティブ状態と見なされるのは、そのコンテキストが属するフェールオーバー グループがその装置上でアクティブ状態である場合です。

- 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 がアクティブ状態の装置から、フェールオーバー グループ 1 がスタンバイ状態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 がアクティブ状態の装置から、フェールオーバー グループ 1 がスタンバイ状態の装置に複製されます。

コマンド複製を行うのに適切な装置上でコマンドを入力しなかった場合は、コンフィギュレーションは非同期になります。この変更内容は、次回に初期コンフィギュレーション同期が行われると失われることがあります。

**write standby** コマンドを使用すると、非同期になったコンフィギュレーションを再同期化できます。Active/Active 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。

- システム実行スペースで **write standby** コマンドを入力すると、システム コンフィギュレーションおよびセキュリティ アプライアンス上のセキュリティ コンテキストすべてに対するコンフィギュレーションがピア装置に書き込まれます。これには、スタンバイ状態のセキュリティ コンテキストのコンフィギュレーション情報が含まれています。このコマンドの入力は、フェールオーバー グループ 1 がアクティブ状態の装置上のシステム実行スペースで行う必要があります。
- セキュリティ コンテキストで **write standby** コマンドを入力すると、セキュリティ コンテキストのコンフィギュレーションのみがピア装置に書き込まれます。このコマンドの入力は、セキュリティ コンテキストがアクティブ状態で表示される装置のセキュリティ コンテキストで行う必要があります。

複製されたコマンドは、ピア装置に複製された場合、フラッシュ メモリに保存されません。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、変更を行った装置で **write memory** または **copy running-config startup-config** コマンドを使用します。コマンドはピア装置に複製されて、コンフィギュレーションがピア装置のフラッシュ メモリに保存されます。

## フェールオーバーのトリガー

Active/Active フェールオーバーでは、次のいずれかのイベントが発生すると、フェールオーバーが装置レベルでトリガーされます。

- 装置でハードウェア障害が発生した。
- 装置で電源障害が発生した。
- 装置でソフトウェア障害が発生した。
- **no failover active** または **failover active** コマンドがシステム実行スペースで入力された。

フェールオーバーは、次のいずれかのイベントが発生すると、フェールオーバー グループ レベルでトリガーされます。

- グループ内の多くの監視対象インターフェイスが故障した。
- **no failover active group group\_id** コマンドが入力された。

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することで各フェールオーバー グループにフェールオーバーしきい値を設定し、故障したインターフェイスがこのしきい値（インターフェイスの数または割合）を超えた場合にそのグループは故障したと判断されます。フェールオーバー グループには複数のコンテキストを含めることができ、また各コンテキストには複数のインターフェイスを含めることができるので、1つのコンテキストのインターフェイスがすべて故障しても、そのコンテキストに関連するフェールオーバー グループが故障と判断されない可能性があります。

インターフェイスと装置のモニタリングの詳細については、P.11-17 の「フェールオーバー ヘルス のモニタリング」を参照してください。

## フェールオーバー アクション

Active/Active フェールオーバー コンフィギュレーションでは、フェールオーバーは、システムごとに行うのではなく、フェールオーバー グループごとに行われます。たとえば、プライマリ装置で両方のフェールオーバー グループをアクティブと指定し、フェールオーバー グループ 1 が故障すると、フェールオーバー グループ 2 はプライマリ装置でアクティブのままですが、フェールオーバー グループ 1 はセカンダリ装置でアクティブになります。



(注)

Active/Active フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにしてください。

表 11-2 に、各障害イベントに対するフェールオーバー アクションを示します。各障害イベントに対して、ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ フェールオーバー グループのアクション、およびスタンバイ フェールオーバー グループのアクションを示します。

表 11-2 Active/Active フェールオーバーのフェールオーバー動作

| 障害の状況                                     | ポリシー       | アクティブ<br>グループの<br>アクション | スタンバイ<br>グループの<br>アクション        | 注意                                                                                                 |
|-------------------------------------------|------------|-------------------------|--------------------------------|----------------------------------------------------------------------------------------------------|
| 装置で電源断またはソフトウェア障害が発生した                    | フェールオーバー   | スタンバイになり、故障とマークする       | アクティブになる<br><br>アクティブに故障とマークする | フェールオーバー ペアの装置が故障すると、その装置のアクティブ フェールオーバー グループはすべて故障とマークされ、ピア装置のフェールオーバー グループがアクティブになります。           |
| アクティブ フェールオーバー グループにおけるしきい値を超えたインターフェイス障害 | フェールオーバー   | アクティブ グループに故障とマークする     | アクティブになる                       | なし。                                                                                                |
| スタンバイ フェールオーバー グループにおけるしきい値を超えたインターフェイス障害 | フェールオーバーなし | 動作なし                    | スタンバイ グループに故障とマークする            | スタンバイ フェールオーバー グループが故障とマークされている場合、インターフェイス フェールオーバー障害しきい値を超えても、アクティブ フェールオーバー グループはフェールオーバーを行いません。 |
| 以前にアクティブであったフェールオーバー グループの復旧              | フェールオーバーなし | 動作なし                    | 動作なし                           | <b>preempt</b> コマンドで設定されていない場合、フェールオーバー グループは現在の装置でアクティブのままです。                                     |

表 11-2 Active/Active フェールオーバーのフェールオーバー動作（続き）

| 障害の状況                         | ポリシー        | アクティブグループのアクション | スタンバイグループのアクション | 注意                                                                                                                 |
|-------------------------------|-------------|-----------------|-----------------|--------------------------------------------------------------------------------------------------------------------|
| スタートアップ時にフェールオーバー リンクに障害が発生した | フェールオーバー なし | アクティブになる        | アクティブになる        | スタートアップ時にフェールオーバー リンクがダウンしていると、両方の装置の両方のフェールオーバー グループがアクティブになります。                                                  |
| ステートフル フェールオーバー リンクに障害が発生した   | フェールオーバー なし | 動作なし            | 動作なし            | ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。                                                                             |
| 動作中にフェールオーバー リンクに障害が発生した      | フェールオーバー なし | 該当なし            | 該当なし            | 各装置で、フェールオーバー インターフェイスが故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。 |

## 使用するフェールオーバーのタイプの決定

選択するフェールオーバーのタイプは、セキュリティ アプライアンスのコンフィギュレーションとセキュリティ アプライアンスの使用計画によって決定されます。

セキュリティ アプライアンスをシングルモードで動作させている場合、使用できるのは Active/Standby フェールオーバーのみです。Active/Active フェールオーバーは、マルチコンテキストモードで動作しているセキュリティ アプライアンスでのみ使用できます。

セキュリティ アプライアンスをマルチコンテキスト モードで動作させている場合は、Active/Active フェールオーバーまたは Active/Standby フェールオーバーを設定できます。

- ロードバランシングを提供するには、Active/Active フェールオーバーを使用します。
- ロードバランシングを提供しない場合は、Active/Standby フェールオーバーまたは Active/Active フェールオーバーを使用します。

表 11-3 に、各タイプのフェールオーバー コンフィギュレーションでサポートされる機能を比較して示します。

表 11-3 フェールオーバー コンフィギュレーション機能のサポート

| 機能                           | Active/Active | Active/Standby |
|------------------------------|---------------|----------------|
| シングルコンテキスト モード               | なし            | あり             |
| マルチコンテキスト モード                | あり            | あり             |
| ロードバランシング ネットワーク コンフィギュレーション | あり            | なし             |
| 装置フェールオーバー                   | あり            | あり             |
| コンテキスト グループのフェールオーバー         | あり            | なし             |
| 個別コンテキストのフェールオーバー            | なし            | なし             |

## 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

セキュリティ アプライアンスは、標準およびステートフルという 2 つのタイプのフェールオーバーをサポートします。ここでは、次の項目について説明します。

- [標準フェールオーバー \(P.11-16\)](#)
- [ステートフル フェールオーバー \(P.11-16\)](#)

### 標準フェールオーバー

フェールオーバーが行われると、アクティブ接続はすべてドロップされます。新しいアクティブ装置が引き継ぐ場合、クライアントは接続を再確立する必要があります。

### 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になっている場合、アクティブ装置は接続ごとのステート情報をスタンバイ装置に常に渡しています。フェールオーバーの発生後も、新しいアクティブ装置で同じ接続情報が利用できます。サポートされているエンドユーザのアプリケーションでは、同じ通信セッションを保持するために再接続する必要はありません。

スタンバイ装置に渡されるステート情報は、次のとおりです。

- NAT 変換テーブル
- TCP 接続状態
- UDP 接続状態
- ARP テーブル
- レイヤ 2 ブリッジ テーブル (透過ファイアウォール モードで動作中の場合)
- HTTP 接続状態 (HTTP 複製がイネーブルの場合)
- 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になっている場合にスタンバイ装置に渡されない情報は、次のとおりです。

- HTTP 接続テーブル (HTTP 複製がイネーブルでない場合)
- ユーザ認証 (uauth) テーブル
- ルーティング テーブル
- セキュリティ サービス モジュールのステート情報



(注)

アクティブな Cisco IP SoftPhone セッション中にフェールオーバーが行われると、コールセッションステート情報がスタンバイ装置に複製されているので、コールはアクティブのままになります。コールが終了すると、IP SoftPhone クライアントは CallManager との接続がなくなります。これは、CTIQBE ハングアップ メッセージのセッション情報がスタンバイ装置に存在しないために発生します。IP SoftPhone クライアントが一定の時間内に CallManager から返送される応答を受信しない場合、このクライアントは CallManager を到達不能と見なし、自分自身の登録を解除します。

## フェールオーバー ヘルスのモニタリング

セキュリティ アプライアンスは、各装置について全体的なヘルスおよびインターフェイス ヘルスを監視します。セキュリティ アプライアンスがテストを実行して、各装置の状態を判断する方法の詳細については、次の項を参照してください。

- 装置ヘルスのモニタリング (P.11-17)
- インターフェイスのモニタリング (P.11-17)

### 装置ヘルスのモニタリング

セキュリティ アプライアンスは、フェールオーバー リンクを監視して相手装置のヘルスを判断します。装置がフェールオーバー リンクで hello メッセージを受信しない場合、装置は、フェールオーバー インターフェイスを含むすべてのインターフェイスに ARP 要求を送信します。セキュリティ アプライアンスによる試行回数は、ユーザが設定できます。セキュリティ アプライアンスが行うアクションは、相手装置からの応答によって決まります。次の可能なアクションを参照してください。

- セキュリティ アプライアンスがいずれかのインターフェイスで応答を受信した場合は、フェールオーバーを行いません。
- セキュリティ アプライアンスがどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブ モードに切り替わり、相手装置を故障に分類します。
- セキュリティ アプライアンスがフェールオーバー リンクで応答を受信しなかった場合、装置のフェールオーバーは行われません。フェールオーバー リンクが故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。

**(注)**

障害が発生した装置が回復せず、実際には障害は発生していないと考えられる場合は、**failover reset** コマンドを使用して状態をリセットできます。ただし、フェールオーバー条件が継続している場合、装置は再び障害状態になります。

### インターフェイスのモニタリング

すべてのコンテキスト間に分割された最大 250 のインターフェイスを監視できます。重要なインターフェイスを監視する必要があります。たとえば、共有インターフェイスを監視するように 1 つのコンテキストを設定する場合があります（インターフェイスが共有されているため、すべてのコンテキストがそのモニタリングで監視されます）。

装置が監視対象のインターフェイスで hello メッセージを受信しない場合は、次のテストを実行します。

1. リンク アップ/ダウン テスト：インターフェイスのステータスのテスト。リンク アップ/ダウン テストでインターフェイスが動作していることが示された場合、セキュリティ アプライアンスはネットワーク テストを実行します。一連のテストでは、障害が発生している装置を判別するためのネットワーク トラフィックが生成されます。各テストの開始時に、各装置はインターフェイスの受信パケット カウントをリセットします。各テストの終了時には、各装置はトラフィックを受信したかどうかをチェックします。トラフィックを受信していれば、インターフェイスは正常に動作していると見なされます。いずれか一方の装置だけがテスト用のトラフィックを受信している場合は、トラフィックを受信しなかった装置が故障していると思なわれます。どちらの装置もトラフィックを受信しなかった場合は、次のテストが使用されます。
2. ネットワーク アクティビティ テスト：受信ネットワーク アクティビティ テスト。装置は、最大 5 秒間、すべての受信パケット数をカウントします。この時間間隔の間にパケットが受信されると、インターフェイスが正常に動作しているものと見なされ、テストは停止します。トラフィックが受信されなかった場合、ARP テストが開始します。



3. ARP テスト：取得したエントリの最後の 2 つの装置 ARP キャッシュの読み取り。装置は、ネットワークトラフィックを発生させるために、1 回に 1 つずつ、これらのマシンに ARP 要求を送信します。各要求後、装置は最大 5 秒間受信したトラフィックをすべてカウントします。トラフィックが受信されれば、インターフェイスは正常に動作していると思なされます。トラフィックが受信されなければ、ARP 要求が次のマシンに送信されます。リストの最後まで、まったくトラフィックが受信されなかった場合、ping テストが開始します。
4. ブロードキャスト Ping テスト：ブロードキャスト ping 要求の送信で構成される ping テスト。装置は、最大 5 秒間、すべての受信パケット数をカウントします。この時間間隔の間にパケットが受信されると、インターフェイスが正常に動作しているものと見なされ、テストは停止します。

1 つのインターフェイスに対するネットワーク テストがすべて失敗したが、相手装置のこのインターフェイスが正常にトラフィックを渡し続けている場合、そのインターフェイスは故障していると思なされます。故障したインターフェイスがしきい値を超えている場合は、フェールオーバーが行われます。相手装置のインターフェイスもすべてのネットワーク テストに失敗した場合、両方のインターフェイスが「未知」状態になり、フェールオーバー制限に向けてのカウントは行いません。

インターフェイスは、何らかのトラフィックを受信すると、再度動作状態になります。故障したセキュリティ アプライアンスは、インターフェイス障害しきい値が満たされなくなった場合、スタンバイ モードに戻ります。

**(注)**

障害が発生した装置が回復せず、実際には障害は発生していないと考えられる場合は、**failover reset** コマンドを使用して状態をリセットできます。ただし、フェールオーバー条件が継続している場合、装置は再び障害状態になります。



## フェールオーバーの設定

この項では、フェールオーバーを設定する方法について説明します。次の項目を取り上げます。

- [Active/Standby フェールオーバーの設定 \(P.11-19\)](#)
- [Active/Active フェールオーバーの設定 \(P.11-27\)](#)
- [フェールオーバー通信の認証 / 暗号化の設定 \(P.11-38\)](#)
- [フェールオーバー コンフィギュレーションの確認 \(P.11-39\)](#)

### Active/Standby フェールオーバーの設定

ここでは、Active/Standby フェールオーバーを設定する手順の詳細を説明します。ここでは、次の項目について説明します。

- [前提条件 \(P.11-19\)](#)
- [ケーブルベースの Active/Standby フェールオーバーの設定 \(PIX セキュリティ アプライアンスのみ\) \(P.11-19\)](#)
- [LAN ベースの Active/Standby フェールオーバーの設定 \(P.11-21\)](#)
- [オプションの Active/Standby フェールオーバー設定値の設定 \(P.11-25\)](#)

代表的なフェールオーバー コンフィギュレーションの例については、[P.11-51 の「フェールオーバー コンフィギュレーションの例」](#)を参照してください。

#### 前提条件

始める前に、次の事項を確認してください。

- 両方の装置のハードウェア、ソフトウェア コンフィギュレーション、必要なライセンスが同じである。
- 両方の装置が同じモードである（シングルまたはマルチ、透過またはルーテッド）。

#### ケーブルベースの Active/Standby フェールオーバーの設定 (PIX セキュリティ アプライアンスのみ)

次の手順に従って、シリアル ケーブルをフェールオーバー リンクとして使用して Active/Standby フェールオーバーを設定します。このタスクのコマンドは、フェールオーバー ペアのプライマリ装置で入力します。プライマリ装置は、ケーブルの「Primary」と表記された側が接続されている装置です。マルチコンテキスト モードの装置では、特に注記がない限り、システム実行スペースでコマンドを入力します。

ケーブルベースのフェールオーバーを使用する場合、フェールオーバー ペアのセカンダリ装置をブートストラップする必要はありません。指示があるまで、セカンダリ装置の電源はオフのままにします。

ケーブルベースのフェールオーバーは、PIX セキュリティ アプライアンス プラットフォームでのみ使用できます。

ケーブルベースの Active/Standby フェールオーバーを設定するには、次の手順を実行します。

**ステップ 1** フェールオーバー ケーブルを PIX セキュリティ アプライアンスに接続します。必ず「Primary」とマークされているケーブルの端をプライマリ装置として使用する装置に接続し、「Secondary」とマークされているケーブルの端をもう一方の装置に接続します。

**ステップ 2** プライマリ装置の電源を投入します。

- ステップ 3** まだ行っていない場合、各データ インターフェイス（ルーテッド モード）または管理インターフェイス（透過モード）のアクティブおよびスタンバイ IP アドレスを設定します。スタンバイ IP アドレスは、現在スタンバイ装置になっているセキュリティ アプライアンスで使用します。アクティブ IP アドレスと同じサブネットである必要があります。



(注)

専用のステートフル フェールオーバー インターフェイスを使用する場合は、ステートフル フェールオーバー リンクの IP アドレスは設定しないでください。専用のステートフル フェールオーバー インターフェイスを設定するには、後述のステップの **failover interface ip** コマンドを使用します。

```
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、各コンテキストからインターフェイス 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、コンテキストを切り替えます。コマンド プロンプトが `hostname/context(config-if)#` に変わります。ここで、*context* は、現在のコンテキスト名です。

- ステップ 4** (オプション) 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、ステートフル フェールオーバー リンクを設定します。

- a. ステートフル フェールオーバー リンクとして使用するインターフェイスを指定します。

```
hostname(config)# failover link if_name phy_if
```

*if\_name* 引数は、*phy\_if* 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。*phy\_if* 引数は、物理ポート名 (Ethernet1 など) にすることも、すでに作成されているサブインターフェイス (Ethernet0/2.3 など) にすることもできます。このインターフェイスは、他の目的に使用しないでください。

- b. アクティブおよびスタンバイ IP アドレスをステートフル 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)

ステートフル フェールオーバー リンクがデータ インターフェイスを使用する場合は、このステップをスキップします。インターフェイスのアクティブおよびスタンバイ IP アドレスは、すでに定義しています。

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である必要があります。スタンバイ IP アドレスのサブネット マスクを指定する必要はありません。

ステートフル フェールオーバー リンク IP アドレスおよび MAC アドレスは、データ インターフェイスを使用しない限り、フェールオーバー時に変更されません。アクティブ IP アドレスは、常にプライマリ装置にあります。スタンバイ IP アドレスは、セカンダリ装置にあります。

- c. インターフェイスをイネーブルにします。

```
hostname(config)# interface phy_if
hostname(config-if)# no shutdown
```

**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** セカンダリ装置の電源を投入し、まだイネーブルにしていない場合、装置でフェールオーバーをイネーブルにします。

```
hostname(config)# failover
```

実行メモリのコンフィギュレーションがアクティブ装置からスタンバイ装置に送信されます。コンフィギュレーションが同期すると、メッセージ「Beginning configuration replication: sending to mate」および「End Configuration Replication to mate」がプライマリ コンソールに表示されます。

**ステップ 7** コンフィギュレーションをプライマリ装置のフラッシュ メモリに保存します。プライマリ装置で入力されたコマンドはセカンダリ装置に複製されるため、セカンダリ装置もコンフィギュレーションをフラッシュ メモリに保存します。

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

**LAN ベースの Active/Standby フェールオーバーの設定**

ここでは、イーサネット フェールオーバー リンクを使用して Active/Standby フェールオーバーを設定する方法について説明します。LAN ベースのフェールオーバーを設定するときは、セカンダリ装置がプライマリ装置から実行コンフィギュレーションを取得する前に、セカンダリ装置をブートストラップしてフェールオーバー リンクを認識させる必要があります。

**(注)**

ケーブルベースのフェールオーバーから LAN ベースのフェールオーバーに変更する場合、ケーブルベースのフェールオーバー コンフィギュレーションで完了しているステップ（各インターフェイスのアクティブ IP アドレスおよびスタンバイ IP アドレスの割り当てなど）はスキップできます。

ここでは、次の項目について説明します。

- [プライマリ装置の設定 \(P.11-21\)](#)
- [セカンダリ装置の設定 \(P.11-24\)](#)

**プライマリ装置の設定**

次の手順に従って、LAN ベースの Active/Standby フェールオーバー コンフィギュレーションのプライマリ装置を設定します。この手順では、プライマリ装置でフェールオーバーをイネーブルにするために必要な最小のコンフィギュレーションが用意されています。マルチコンテキスト モードでは、特に注記がない限り、手順はすべてシステム実行スペースで実行します。

Active/Standby フェールオーバー ペアのプライマリ装置を設定するには、次の手順を実行します。

- ステップ 1** まだ行っていない場合、各インターフェイス（ルーテッド モード）または管理インターフェイス（透過モード）のアクティブおよびスタンバイ IP アドレスを設定します。スタンバイ IP アドレスは、現在スタンバイ装置になっているセキュリティ アプライアンスで使用します。アクティブ IP アドレスと同じサブネットである必要があります。



- (注)** 専用のステートフル フェールオーバー インターフェイスを使用する場合は、ステートフル フェールオーバー リンクの IP アドレスは設定しないでください。専用のステートフル フェールオーバー インターフェイスを設定するには、後述のステップの **failover interface ip** コマンドを使用します。

```
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、各コンテキストからインターフェイス 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、コンテキストを切り替えます。コマンド プロンプトが `hostname/context(config-if)#` に変わります。ここで、*context* は、現在のコンテキスト名です。

- ステップ 2** (PIX セキュリティ アプライアンス プラットフォームのみ) LAN ベースのフェールオーバーをイネーブルにします。

```
hostname(config)# failover lan enable
```

- ステップ 3** 装置をプライマリ装置に指定します。

```
hostname(config)# failover lan unit primary
```

- ステップ 4** 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 phy_if
```

*if\_name* 引数は、*phy\_if* 引数で指定されたインターフェイスに名前を割り当てます。*phy\_if* 引数は、物理ポート名 (Ethernet1 など) にすることも、すでに作成されているサブインターフェイス (Ethernet0/2.3 など) にすることもできます。

- b. アクティブおよびスタンバイ 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である必要があります。スタンバイ アドレスのサブネット マスクを指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、フェールオーバー時に変更されません。フェールオーバー リンクのアクティブ IP アドレスは、常にプライマリ装置にあります。スタンバイ IP アドレスは、セカンダリ装置にあります。

- c. インターフェイスをイネーブルにします。

```
hostname(config)# interface phy_if  
hostname(config-if)# no shutdown
```

### ステップ 5 (オプション) 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、ステートフル フェールオーバー リンクを設定します。

- a. ステートフル フェールオーバー リンクとして使用するインターフェイスを指定します。

```
hostname(config)# failover link if_name phy_if
```



(注)

ステートフル フェールオーバー リンクがフェールオーバー リンクまたはデータ インターフェイスを使用する場合は、*if\_name* 引数を指定することだけが必要です。

*if\_name* 引数は、*phy\_if* 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。*phy\_if* 引数は、物理ポート名 (Ethernet1 など) にすることも、すでに作成されているサブインターフェイス (Ethernet0/2.3 など) にすることもできます。このインターフェイスは、他の目的に使用しないでください (オプションのフェールオーバー リンクは除く)。

- b. アクティブおよびスタンバイ IP アドレスをステートフル フェールオーバー リンクに割り当てます。



(注)

ステートフル フェールオーバー リンクがフェールオーバー リンクまたはデータ インターフェイスを使用する場合は、このステップをスキップします。インターフェイスのアクティブおよびスタンバイ IP アドレスは、すでに定義しています。

```
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である必要があります。スタンバイ アドレスのサブネット マスクを指定する必要はありません。

ステートフル フェールオーバー リンク IP アドレスおよび MAC アドレスは、データ インターフェイスを使用しない限り、フェールオーバー時に変更されません。アクティブ IP アドレスは、常にプライマリ装置にあります。スタンバイ IP アドレスは、セカンダリ装置にあります。

- c. インターフェイスをイネーブルにします。



(注)

ステートフル フェールオーバー リンクがフェールオーバー リンクまたはデータ インターフェイスを使用する場合は、このステップをスキップします。インターフェイスは、すでにイネーブルです。

```
hostname(config)# interface phy_if  
hostname(config-if)# no shutdown
```

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

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

**セカンダリ装置の設定**

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

マルチコンテキスト モードでは、特に注記がない限り、手順はすべてシステム実行スペースで実行します。

セカンダリ装置を設定するには、次の手順を実行します。

**ステップ 1** (PIX セキュリティ アプライアンス プラットフォームのみ) LAN ベースのフェールオーバーをイネーブルにします。

```
hostname(config)# failover lan enable
```

**ステップ 2** フェールオーバー インターフェイスを定義します。プライマリ装置に使用している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 phy_if
```

*if\_name* 引数は、*phy\_if* 引数で指定されたインターフェイスに名前を割り当てます。

- b. アクティブおよびスタンバイ 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)**

プライマリ装置にフェールオーバー インターフェイスを設定する場合、プライマリ装置でこのコマンドを入力するときは、正確に入力してください。

- c. インターフェイスをイネーブルにします。

```
hostname(config)# interface phy_if
hostname(config-if)# no shutdown
```

**ステップ 3** (オプション) この装置をセカンダリ装置に指定します。

```
hostname(config)# failover lan unit secondary
```

**(注)**

以前に設定されていない場合、装置はデフォルトでセカンダリに指定されているので、このステップはオプションです。

**ステップ 4** 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、実行メモリのコンフィギュレーションがアクティブ装置からスタンバイ装置に送信されます。コンフィギュレーションが同期すると、メッセージ「Beginning configuration replication: Sending to mate」および「End Configuration Replication to mate」がアクティブ装置のコンソールに表示されます。

**ステップ 5** 実行コンフィギュレーションの複製が完了したら、そのコンフィギュレーションをフラッシュメモリに保存します。

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

---

**オプションの Active/Standby フェールオーバー設定値の設定**

次のオプションの Active/Standby フェールオーバー設定値は、最初にフェールオーバーを設定するときでも、フェールオーバーがすでに設定された後でも設定できます。特に注記がない限り、コマンドはアクティブ装置で入力する必要があります。

ここでは、次の項目について説明します。

- [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 \(P.11-25\)](#)
- [インターフェイス モニタリングのディセーブル化とイネーブル化 \(P.11-25\)](#)
- [インターフェイスと装置のポーリング時間の設定 \(P.11-26\)](#)
- [フェールオーバー基準の設定 \(P.11-26\)](#)
- [仮想 MAC アドレスの設定 \(P.11-27\)](#)

**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**

HTTP 接続がステート情報複製に含まれるようにするには、HTTP 複製をイネーブルにする必要があります。HTTP 接続は通常は存続期間が短く、HTTP クライアントは接続試行が失敗すると通常は再試行するため、HTTP 接続は複製されるステート情報に自動的に含まれません。

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、ステートフル フェールオーバーがイネーブル状態の場合に、HTTP ステート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 モニタリングのディセーブル化とイネーブル化**

デフォルトでは、物理インターフェイスのモニタリングはイネーブルに、サブインターフェイスのモニタリングはディセーブルになっています。1 台の装置で最大 250 のインターフェイスを監視できます。特定のインターフェイスのモニタリングをディセーブルにし、別のモニタリングをイネーブルにすることで、フェールオーバー ポリシーに影響を与えるインターフェイスを制御できます。これによって、重要度の低いネットワークに接続されているインターフェイスがフェールオーバーポリシーに影響を与えないようにできます。

マルチコンフィギュレーション モードの装置の場合は、次のコマンドを使用して特定のインターフェイスのヘルス モニタリングをイネーブルまたはディセーブルにします。

## ■ フェールオーバーの設定

- インターフェイスのヘルス モニタリングをディセーブルにするには、コンテキスト内で次のコマンドを入力します。

```
hostname/context(config)# no monitor-interface if_name
```

- インターフェイスのヘルス モニタリングをイネーブルにするには、コンテキスト内で次のコマンドを入力します。

```
hostname/context(config)# monitor-interface if_name
```

シングルコンフィギュレーション モードの装置の場合は、次のコマンドを使用して特定のインターフェイスのヘルス モニタリングをイネーブルまたはディセーブルにします。

- インターフェイスのヘルス モニタリングをディセーブルにするには、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)# no monitor-interface if_name
```

- インターフェイスのヘルス モニタリングをイネーブルにするには、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)# monitor-interface if_name
```

## インターフェイスと装置のポーリング時間の設定

セキュリティ アプライアンスは、フェールオーバーについて装置とインターフェイス両方のヘルスを監視します。インターフェイスと装置のヘルスを監視する場合、hello メッセージの間の時間間隔を設定できます。ポーリング時間を短縮すると、インターフェイスまたは装置の障害をより迅速に検出できますが、多くのシステム リソースを消費します。

インターフェイスのポーリング時間を変更するには、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
```

装置のポーリング時間を変更するには、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
```

## フェールオーバー基準の設定

デフォルトでは、1 つのインターフェイス障害でフェールオーバーが行われます。インターフェイス数または監視されているインターフェイスの割合を指定して、この数または割合を超えたインターフェイスに障害が発生した場合にフェールオーバーが発生するようにできます。

デフォルトのフェールオーバー基準を変更するには、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[%]
```

インターフェイス数を指定する場合、*num* 引数は 1 ～ 250 です。インターフェイスの割合を指定する場合、*num* 引数は 1 ～ 100 です。



## 仮想 MAC アドレスの設定

Active/Standby フェールオーバーでは、プライマリ装置の MAC アドレスは常にアクティブ IP アドレスに関連付けられています。セカンダリ装置は、最初にブートされてアクティブになると、そのインターフェイスの焼き付け済み MAC アドレスを使用します。プライマリ装置がオンラインになると、セカンダリ装置はプライマリ装置から MAC アドレスを取得します。この変更によって、ネットワークトラフィックが中断することがあります。

各インターフェイスに仮想 MAC アドレスを設定して、セカンダリ装置がプライマリ装置より前にオンラインになっても、セカンダリ装置がアクティブ装置である場合、正しい MAC アドレスを使用するようにします。仮想 MAC アドレスを使用しない場合、フェールオーバー ペアは焼き付け済み NIC アドレスを MAC アドレスとして使用します。



(注)

フェールオーバーまたはステートフル フェールオーバー リンクには、仮想 MAC アドレスは設定できません。これらのリンクの MAC アドレスおよび IP アドレスは、フェールオーバー中に変更されません。

アクティブ装置で次のコマンドを入力して、インターフェイスの仮想 MAC アドレスを設定します。

```
hostname(config)# failover mac address phy_if active_mac standby_mac
```

*phy\_if* 引数は、インターフェイスの物理名 (Ethernet1 など) です。*active\_mac* および *standby\_mac* 引数は、H.H.H 形式 (H は 16 ビットの 16 進数) の MAC アドレスです。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。

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

## Active/Active フェールオーバーの設定

ここでは、Active/Active フェールオーバーの設定方法について説明します。

ここでは、次の項目について説明します。

- [前提条件 \(P.11-27\)](#)
- [ケーブルベースの Active/Active フェールオーバーの設定 \(PIX セキュリティ アプライアンスのみ\) \(P.11-28\)](#)
- [LAN ベースの Active/Active フェールオーバーの設定 \(P.11-30\)](#)
- [オプションの Active/Active フェールオーバー設定値の設定 \(P.11-34\)](#)

代表的なフェールオーバー コンフィギュレーションの例については、[P.11-51 の「フェールオーバー コンフィギュレーションの例」](#)を参照してください。

## 前提条件

始める前に、次の事項を確認してください。

- 両方の装置のハードウェア、ソフトウェア コンフィギュレーション、必要なライセンスが同じである。
- 両方の装置がマルチコンテキスト モードである。

## ケーブルベースの Active/Active フェールオーバーの設定 (PIX セキュリティ アプライアンスのみ)

次の手順に従って、シリアル ケーブルをフェールオーバー リンクとして使用して Active/ Active フェールオーバーを設定します。このタスクのコマンドは、フェールオーバー ペアのプライマリ装置で入力します。プライマリ装置は、ケーブルの「Primary」と表記された側が接続されている装置です。マルチコンテキスト モードの装置では、特に注記がない限り、システム実行スペースでコマンドを入力します。

ケーブルベースのフェールオーバーを使用する場合、フェールオーバー ペアのセカンダリ装置をブートストラップする必要はありません。指示があるまで、セカンダリ装置の電源はオフのままにします。

ケーブルベースのフェールオーバーは、PIX セキュリティ アプライアンス プラットフォームでのみ使用できます。

ケーブルベースの Active/ Active フェールオーバーを設定するには、次の手順を実行します。

- ステップ 1** フェールオーバー ケーブルを PIX セキュリティ アプライアンスに接続します。必ず「Primary」とマークされているケーブルの端をプライマリ装置として使用する装置に接続し、「Secondary」とマークされている端をセカンダリ装置として使用する装置に接続します。
- ステップ 2** プライマリ装置の電源を投入します。
- ステップ 3** まだ行っていない場合、各インターフェイス（ルーテッド モード）または管理インターフェイス（透過モード）のアクティブおよびスタンバイ IP アドレスを設定します。スタンバイ IP アドレスは、現在スタンバイ装置になっているセキュリティ アプライアンスで使用します。アクティブ IP アドレスと同じサブネットである必要があります。



(注)

専用のステートフル フェールオーバー インターフェイスを使用する場合は、ステートフル フェールオーバー リンクの IP アドレスは設定しないでください。専用のステートフル フェールオーバー インターフェイスを設定するには、後述のステップの **failover interface ip** コマンドを使用します。

```
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、各コンテキストからインターフェイス 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、コンテキストを切り替えます。コマンドプロンプトが `hostname/context(config-if)#` に変わります。ここで、*context* は、現在のコンテキスト名です。

- ステップ 4** (オプション) 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、ステートフル フェールオーバー リンクを設定します。
  - a.** ステートフル フェールオーバー リンクとして使用するインターフェイスを指定します。

```
hostname(config)# failover link if_name phy_if
```

*if\_name* 引数は、*phy\_if* 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。*phy\_if* 引数は、物理ポート名 (Ethernet1 など) にすることも、すでに作成されているサブインターフェイス (Ethernet0/2.3 など) にすることもできます。このインターフェイスは、他の目的に使用しないでください (オプションのフェールオーバー リンクは除く)。

- b. アクティブおよびスタンバイ IP アドレスをステートフル 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である必要があります。スタンバイ IP アドレスのサブネット マスクを指定する必要はありません。

ステートフル 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、ステートフル フェールオーバーで標準データ インターフェイスを使用する場合を除き、フェールオーバー時に変更されません。アクティブ IP アドレスは、常にプライマリ装置にあります。スタンバイ IP アドレスは、セカンダリ装置にあります。

- c. インターフェイスをイネーブルにします。

```
hostname(config)# interface phy_if  
hostname(config-if)# no shutdown
```

**ステップ 5** 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 グループを使用できます。**failover group** コマンドは、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はこれを作成し、フェールオーバー グループ コンフィギュレーション モードに移行します。

フェールオーバー グループごとに **primary** または **secondary** コマンドを使用して、フェールオーバー グループがプライマリ プリファレンスとセカンダリ プリファレンスのどちらを持つかを指定する必要があります。同じプリファレンスを両方のフェールオーバー グループに割り当てることができます。ロードバランシング コンフィギュレーションの場合は、各フェールオーバー グループに異なる装置プリファレンスを割り当てる必要があります。

次の例では、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、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 6** 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、各ユーザ 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}  
hostname(config-context)# exit
```

**ステップ 7** 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 8** セカンダリ装置の電源を投入し、まだイネーブルにしていない場合、装置でフェールオーバーをイネーブルにします。

```
hostname(config)# failover
```

実行メモリのコンフィギュレーションがアクティブ装置からスタンバイ装置に送信されます。コンフィギュレーションが同期すると、メッセージ「Beginning configuration replication: Sending to mate」および「End Configuration Replication to mate」がプライマリ コンソールに表示されます。

- ステップ 9** コンフィギュレーションをプライマリ装置のフラッシュ メモリに保存します。プライマリ装置で入力されたコマンドはセカンダリ装置に複製されるため、セカンダリ装置もコンフィギュレーションをフラッシュ メモリに保存します。

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

- ステップ 10** 必要に応じて、プライマリ装置でアクティブなフェールオーバー グループすべてを強制的にセカンダリ装置でアクティブ状態にします。フェールオーバー グループを強制的にセカンダリ装置でアクティブにするには、プライマリ装置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* 引数は、セカンダリ装置でアクティブにするグループを指定します。

## LAN ベースの Active/ Active フェールオーバーの設定

ここでは、イーサネット フェールオーバー リンクを使用して Active/ Active フェールオーバーを設定する方法について説明します。LAN ベースのフェールオーバーを設定するときは、セカンダリ装置がプライマリ装置から実行コンフィギュレーションを取得する前に、セカンダリ装置をブートストラップしてフェールオーバー リンクを認識させる必要があります。

ここでは、次の項目について説明します。

- [プライマリ装置の設定 \(P.11-30\)](#)
- [セカンダリ装置の設定 \(P.11-33\)](#)

### プライマリ装置の設定

Active/ Active フェールオーバー コンフィギュレーションのプライマリ装置を設定するには、次の手順を実行します。

- ステップ 1** 基本フェールオーバー パラメータをシステム実行スペースで設定します。

- a. (PIX セキュリティ アプライアンス プラットフォームのみ) LAN ベースのフェールオーバーをイネーブルにします。

```
hostname(config)# hostname(config)# failover lan enable
```

- b. 装置をプライマリ装置に指定します。

```
hostname(config)# failover lan unit primary
```

- c. フェールオーバー リンクを指定します。

```
hostname(config)# failover lan interface if_name phy_if
```

*if\_name* 引数は、*phy\_if* 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。*phy\_if* 引数は、物理ポート名 (Ethernet1 など) にすることも、すでに作成されているサブインターフェイス (Ethernet0/2.3 など) にすることもできます。このインターフェイスは、他の目的に使用しないでください (オプションのステートフル フェールオーバー リンクは除く)。

- d. フェールオーバー リンクのアクティブ IP アドレスおよびスタンバイ 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である必要があります。スタンバイ IP アドレスのサブネット マスクを指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、フェールオーバー時に変更されません。アクティブ IP アドレスは、常にプライマリ装置にあります。スタンバイ IP アドレスは、セカンダリ装置にあります。

## ステップ 2 (オプション) 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、ステートフル フェールオーバー リンクを設定します。

- a. ステートフル フェールオーバー リンクとして使用するインターフェイスを指定します。

```
hostname(config)# failover link if_name phy_if
```

*if\_name* 引数は、*phy\_if* 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。*phy\_if* 引数は、物理ポート名 (Ethernet1 など) にすることも、すでに作成されているサブインターフェイス (Ethernet0/2.3 など) にすることもできます。このインターフェイスは、他の目的に使用しないでください (オプションのフェールオーバー リンクは除く)。



(注)

ステートフル フェールオーバー リンクがフェールオーバー リンクまたは標準データインターフェイスを使用する場合は、*if\_name* 引数を指定することだけが必要です。

- b. アクティブおよびスタンバイ IP アドレスをステートフル フェールオーバー リンクに割り当てます。



(注)

ステートフル フェールオーバー リンクがフェールオーバー リンクまたは標準データインターフェイスを使用する場合は、このステップをスキップします。インターフェイスのアクティブおよびスタンバイ IP アドレスは、すでに定義しています。

```
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である必要があります。スタンバイ アドレスのサブネット マスクを指定する必要はありません。

状態リンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。アクティブ IP アドレスは、常にプライマリ装置にあります。スタンバイ IP アドレスは、セカンダリ装置にあります。

- c. インターフェイスをイネーブルにします。



(注)

ステートフル フェールオーバー リンクがフェールオーバー リンクまたは標準データ インターフェイスを使用する場合は、このステップをスキップします。インターフェイスは、すでにイネーブルです。

```
hostname(config)# interface phy_if
hostname(config-if)# no shutdown
```

- 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 グループを使用できます。**failover group** コマンドは、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はこれを作成し、フェールオーバー グループ コンフィギュレーション モードに移行します。

フェールオーバー グループごとに **primary** または **secondary** コマンドを使用して、フェールオーバー グループがプライマリ プリファレンスとセカンダリ プリファレンスのどちらを持つかを指定します。同じプリファレンスを両方のフェールオーバー グループに割り当てることができます。ロードバランシング コンフィギュレーションの場合は、各フェールオーバー グループに異なる装置プリファレンスを割り当てする必要があります。

次の例では、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、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、各ユーザ 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}
hostname(config-context)# exit
```

- 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
```

## セカンダリ装置の設定

LAN ベースの Active/Active フェールオーバーを設定するときは、セカンダリ装置をブートストラップしてフェールオーバー リンクを認識させる必要があります。その結果、セカンダリ装置は、プライマリ装置と通信して、実行コンフィギュレーションを受信できるようになります。

Active/ Active 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装置をブートストラップするには、次の手順を実行します。

- ステップ 1** (PIX セキュリティ アプライアンス プラットフォームのみ) LAN ベースのフェールオーバーをイネーブルにします。

```
hostname(config)# failover lan enable
```

- ステップ 2** フェールオーバー インターフェイスを定義します。プライマリ装置に使用している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 phy_if
```

*if\_name* 引数は、*phy\_if* 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。*phy\_if* 引数は、物理ポート名 (Ethernet1 など) にすることも、すでに作成されているサブインターフェイス (Ethernet0/2.3 など) にすることもできます。

- b. アクティブおよびスタンバイ 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)

フェールオーバー インターフェイスを設定する場合、プライマリ装置でこのコマンドを入力するときは、正確に入力してください。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。スタンバイ アドレスのサブネット マスクを指定する必要はありません。

- c. インターフェイスをイネーブルにします。

```
hostname(config)# interface phy_if  
hostname(config-if)# no shutdown
```

- ステップ 3** (オプション) この装置をセカンダリ装置に指定します。

```
hostname(config)# failover lan unit secondary
```



(注)

前に別の設定がされていない限り、装置はデフォルトでセカンダリに指定されているので、このステップはオプションです。

**ステップ 4** 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、実行メモリのコンフィギュレーションがアクティブ装置からスタンバイ装置に送信されます。コンフィギュレーションが同期すると、メッセージ「Beginning configuration replication: Sending to mate」および「End Configuration Replication to mate」がアクティブ装置のコンソールに表示されます。

**ステップ 5** 実行コンフィギュレーションの複製が完了したら、次のコマンドを入力してそのコンフィギュレーションをフラッシュメモリに保存します。

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

**ステップ 6** 必要に応じて、プライマリ装置でアクティブなフェールオーバー グループすべてを強制的にセカンダリ装置でアクティブ状態にします。フェールオーバー グループを強制的にセカンダリ装置でアクティブにするには、プライマリ装置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` 引数は、セカンダリ装置でアクティブにするグループを指定します。

**オプションの Active/ Active フェールオーバー設定値の設定**

次のオプションの Active/Active フェールオーバー設定値は、最初にフェールオーバーを設定するときでも、フェールオーバーがすでに設定された後でも設定できます。特に注記がない限り、コマンドは、フェールオーバー グループ 1 がアクティブ状態の装置で入力する必要があります。

ここでは、次の項目について説明します。

- [フェールオーバー グループのプリエンプションの設定 \(P.11-34\)](#)
- [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 \(P.11-35\)](#)
- [インターフェイス モニタリングのディセーブル化とイネーブル化 \(P.11-35\)](#)
- [インターフェイスと装置のポーリング時間の設定 \(P.11-35\)](#)
- [フェールオーバー基準の設定 \(P.11-36\)](#)
- [仮想 MAC アドレスの設定 \(P.11-36\)](#)
- [非対称ルーティングのサポートの設定 \(P.11-37\)](#)

**フェールオーバー グループのプリエンプションの設定**

プライマリまたはセカンダリの優先順位をフェールオーバー グループに割り当てると、両方の装置が同時にブートされるときに、フェールオーバー グループがどの装置上でアクティブになるかが指定されます。しかし、ある装置がもう一方の装置よりも先にブートした場合、どちらのフェールオーバー グループもその装置上で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、その装置に優先度を認めているフェールオーバー グループはいずれも、その装置ではアクティブになりません。ただし、手動で強制された場合、フェールオーバーが行われた場合、またはそのフェールオーバー グループが **preempt** コマンドで設定されている場合は除きます。**preempt** コマンドによって、フェールオーバー グループは、指定された装置が使用可能になると、その装置で自動的にアクティブになります。



指定されたフェールオーバー グループのプリエン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)# failover group {1 | 2}
hostname(config-fover-group)# preempt [delay]
```

オプションの *delay* 値に秒数を入力して、その時間フェールオーバー グループが現在の装置でアクティブ状態に維持され、その後に指定された装置で自動的にアクティブになるようにできます。

## 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

HTTP 接続をステート情報に含めることができるようにするには、HTTP 複製をイネーブルにする必要があります。HTTP 接続は通常は存続期間が短く、HTTP クライアントは接続試行が失敗すると通常は再試行するため、HTTP 接続は複製されるステート情報に自動的に含まれません。**replication http** コマンドを使用すると、ステートフル フェールオーバーがイネーブルになっている場合に、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 グループの HTTP ステート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、設定されているフェールオーバー グループにのみ影響します。両方のフェールオーバー グループの HTTP ステート複製をイネーブルにするには、各グループで次のコマンドを入力する必要があります。次のコマンドは、システム実行スペースで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 モニタリングのディセーブル化とイネーブル化

1 台の装置で最大 250 のインターフェイスを監視できます。デフォルトでは、物理インターフェイスのモニタリングはイネーブルに、サブインターフェイスのモニタリングはディセーブルになっています。特定のインターフェイスのモニタリングをディセーブルにし、別のモニタリングをイネーブルにすることで、フェールオーバー ポリシーに影響を与えるインターフェイスを制御できます。これによって、重要度の低いネットワークに接続されているインターフェイスがフェールオーバー ポリシーに影響を与えないようにできます。

インターフェイスのヘルス モニタリングをディセーブルにするには、コンテキスト内で次のコマンドを入力します。

```
hostname/context(config)# no monitor-interface if_name
```

インターフェイスのヘルス モニタリングをイネーブルにするには、コンテキスト内で次のコマンドを入力します。

```
hostname/context(config)# monitor-interface if_name
```

## インターフェイスと装置のポーリング時間の設定

フェールオーバー グループ内のインターフェイスのヘルスを監視する場合、hello メッセージ間の時間間隔を設定できます。インターフェイスのポーリング時間を短縮すると、インターフェイスが故障した場合にフェールオーバーを迅速に行うことができますが、多くのシステム リソースを消費します。

インターフェイスのデフォルトのポーリング時間を変更するには、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
```

## ■ フェールオーバーの設定

装置のポーリング時間は、ピア装置のヘルスを判断するために、フェールオーバー リンク全体に送信される hello メッセージ間の時間間隔を指定します。装置のポーリング時間を短縮すると、障害の発生した装置をより迅速に検出できますが、多くのシステム リソースを消費します。装置のポーリング時間を変更するには、システム実行スペースのグローバル 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
```

## フェールオーバー基準の設定

デフォルトでは、1つのインターフェイス障害でフェールオーバーが行われます。インターフェイス数または監視されているインターフェイスの割合を指定して、この数または割合を超えたインターフェイスに障害が発生した場合にフェールオーバーが発生するようにできます。フェールオーバー基準は、フェールオーバー グループごとに指定されます。

指定されたフェールオーバー グループのデフォルト フェールオーバー基準を変更するには、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[%]
```

インターフェイス数を指定する場合、*num* 引数は 1 ～ 250 です。インターフェイスの割合を指定する場合、*num* 引数は 1 ～ 100 です。

## 仮想 MAC アドレスの設定

Active/Active フェールオーバーでは、すべてのインターフェイスで仮想 MAC アドレスを使用します。仮想 MAC アドレスを指定しない場合は、次のように計算されます。

- アクティブ装置のデフォルト MAC アドレス：00a0.c9physical\_port\_number.failover\_group\_id01
- スタンバイ装置のデフォルト MAC アドレス：00a0.c9physical\_port\_number.failover\_group\_id02



(注)

同じネットワーク上に Active/Active フェールオーバー ペアが複数ある場合は、あるペアのインターフェイスに割り当てられているものと同一デフォルト仮想 MAC アドレスが、他のペアのインターフェイスに割り当てられることがあります。これは、デフォルト仮想 MAC アドレスの決定方法に基づいた動作です。ネットワーク上で MAC アドレスが重複することを回避するには、すべてのフェールオーバー グループに対して、必ず各物理インターフェイスに仮想のアクティブおよびスタンバイ MAC アドレスを割り当てます。

インターフェイスの特定のアクティブおよびスタンバイ MAC 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)# failover group {1 | 2}
hostname(config-fover-group)# mac address phy_if active_mac standby_mac
```

*phy\_if* 引数は、インターフェイスの物理名 (Ethernet1 など) です。*active\_mac* および *standby\_mac* 引数は、H.H.H 形式 (H は 16 ビットの 16 進数) の MAC アドレスです。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。

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

## 非対称ルーティングのサポートの設定

Active/Active フェールオーバーで動作中の場合、装置は、ピア装置を経由して送信された接続用の返送パケットを受信することがあります。そのパケットを受信するセキュリティ アプライアンスにはそのパケットの接続情報がないために、パケットはドロップされます。これが最もよく発生するのは、Active/Active フェールオーバー ペアのセキュリティ アプライアンス 2 台が異なるサービス プロバイダーに接続されており、発信接続で NAT アドレスが使用されていない場合です。

返送パケットのドロップは、ドロップが発生する可能性のあるインターフェイスで **asr-group** コマンドを使用することで防止できます。インターフェイスに **asr-group** コマンドが設定されていると、インターフェイス接続情報がフェールオーバー ピアに送信されます。ピアは、アクティブ接続のないパケットを受信した場合、非同期ルーティング グループ内の他のインターフェイスで対応する接続を探します。受信したパケットのアクティブ接続がピアに存在する場合は、そのパケットおよびその接続向けに受信する他のすべてのものを、その接続がアクティブであるピア装置に、接続が終了するまで転送します。



(注)

非対称ルーティングのサポートを設定するために **asr-group** コマンドを使用する方法は、**nailed** オプションを指定して **static** コマンドを使用する方法よりも安全です。

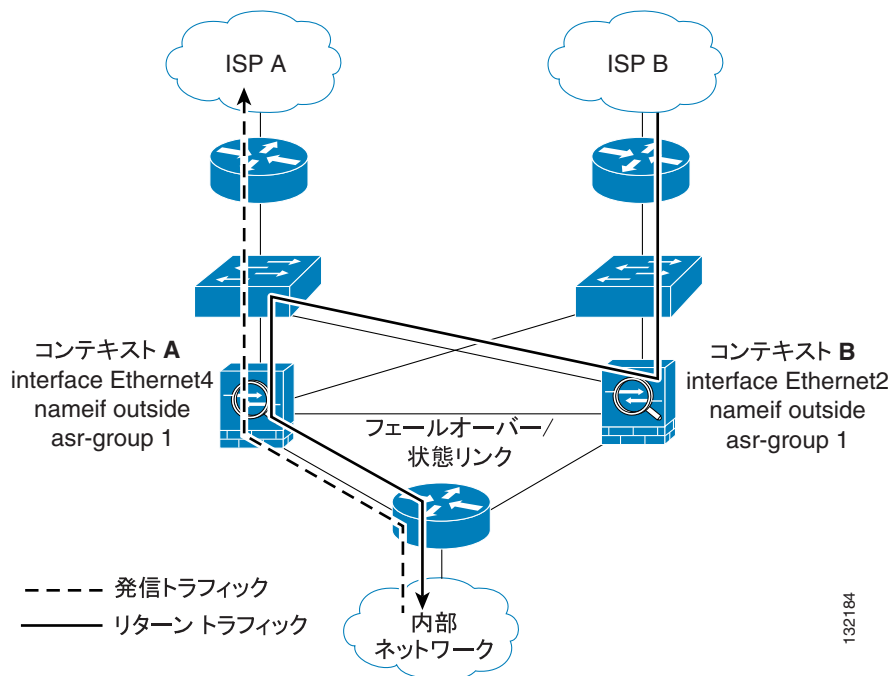
次のコマンドを入力して、非対称ルーティングのサポートを設定します。**asr-group** コマンドは、セキュリティ コンテキストでのみ使用できます。非対称ルーティングが正しく機能するには、ステートフル フェールオーバーがイネーブルになっている必要があります。

```
hostname/ctx1(config)# interface phy_if  
hostname/ctx1(config-if)# asr-group num
```

**num** 範囲に有効な値は、1 ～ 32 です。非対称ルーティング グループに参加するインターフェイスそれぞれにコマンドを入力する必要があります。インターフェイスによって転送、受信、またはドロップされた ASR パケットの数を表示するには、**show interface detail** コマンドを使用します。

図 11-1 に、非対称ルーティングのサポートに対する **asr-group** コマンドの使用例を示します。

図 11-1 ASR の例



コンテキスト A が一方の装置でアクティブであり、コンテキスト B がもう一方の装置でアクティブです。各コンテキストには、「外部」という名前のインターフェイスがあります。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 がアクティブの装置を経由してルーティングされます。しかし、リターントラフィックは、コンテキスト B がアクティブの装置を経由してルーティングされます。通常、リターントラフィックは、その装置上にリターントラフィックに関するセッション情報がないので、ドロップされます。しかし、インターフェイスに **asr-group** 番号が設定されているので、その装置は、同じ **asr-group** が割り当てられている他のインターフェイスすべてのセッション情報を参照します。その装置は、コンテキスト A の外部インターフェイスにセッション情報を検出します。コンテキスト A はその装置ではスタンバイ状態であり、リターントラフィックをコンテキスト A がアクティブである装置に転送します。

トラフィックは、コンテキスト A がスタンバイ状態である装置のコンテキスト 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 がアクティブ状態である装置のコンテキスト A の外部インターフェイスを経由して返送されます。この転送は、必要に応じて、セッションが終了するまで続行されます。

## フェールオーバー通信の認証 / 暗号化の設定

フェールオーバー ピアの間の通信の暗号化および認証は、共有秘密または 16 進数のキーを指定することによって可能になります。



(注)

PIX セキュリティ アプライアンス プラットフォームの場合、専用のシリアル フェールオーバー ケーブルを使用して装置を接続すると、フェールオーバー リンク経由の通信は、フェールオーバー キーが設定されていても、暗号化されません。フェールオーバー キーでは、LAN ベースのフェールオーバー通信のみが暗号化されます。

**注意**

フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

Active/Standby フェールオーバー ペアのアクティブ装置、または Active/Active フェールオーバー ペアのフェールオーバー グループ 1 がアクティブ状態の装置で次のコマンドを入力します。

```
hostname(config)# failover key {secret | hex key}
```

*secret* 引数で、暗号キーの生成に使用される共有秘密を指定します。共有秘密には 1 ～ 63 文字が指定できます。文字としては、数字、英字、句読点のどのような組み合わせでも使用できます。*hex key* 引数で、16 進暗号キーを指定します。キーは、32 桁の 16 進数文字 (0 ～ 9、a ～ f) でなければなりません。

**(注)**

フェールオーバー キーが、ピア装置に既存のフェールオーバー コンフィギュレーション用のクリア テキストとして複製されるのを防止するには、アクティブ装置 (またはフェールオーバー グループ 1 がアクティブ状態の装置のシステム実行スペース) でフェールオーバーをディセーブルにして、両方の装置でフェールオーバー キーを入力し、その後フェールオーバーを再度イネーブルにします。フェールオーバーが再度イネーブルにされると、フェールオーバー通信がそのキーで暗号化されます。

新しい LAN ベースのフェールオーバー コンフィギュレーションの場合、**failover key** コマンドはフェールオーバー ペアのブートストラップ コンフィギュレーションの一部でなければなりません。

## フェールオーバー コンフィギュレーションの確認

この項では、フェールオーバー 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。ここでは、次の項目について説明します。

- [show failover コマンドの使用法 \(P.11-40\)](#)
- [監視対象インターフェイスの表示 \(P.11-47\)](#)
- [実行コンフィギュレーション内のフェールオーバー コマンドの表示 \(P.11-48\)](#)
- [フェールオーバー機能のテスト \(P.11-48\)](#)

## show failover コマンドの使用方法

ここでは、**show failover** コマンドの出力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、Active/Standby フェールオーバーと Active/Active フェールオーバーのどちらを使用しているかによって決まります。

ここでは、次の項目について説明します。

- [show failover : Active/Standby \(P.11-40\)](#)
- [フェールオーバーの表示 : Active/Active \(P.11-44\)](#)

### show failover : Active/Standby

次に、Active/Standby 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 11-4 に、表示される情報についての説明を示します。

```
hostname# show failover

Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: fover Ethernet2 (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 Ethernet2 (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** コマンドを使用して、そのコンテキストのフェールオーバー情報を表示します。この情報は、シングルコンテキスト モードでコマンドを使用した場合に表示される情報に似ています。装置のアクティブ ステータスまたはスタンバイ ステータスを表示する代わりに、コンテキストのアクティブ ステータスまたはスタンバイ ステータスを表示します。表 11-4 に、表示された情報についての説明を示します。

```
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 11-4 show failover の表示の説明

| フィールド                    | オプション                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Failover                 | <ul style="list-style-type: none"> <li>On</li> <li>Off</li> </ul>                                                                                                                                                                                                                                                                                                     |
| Cable status:            | <ul style="list-style-type: none"> <li>Normal: ケーブルは両方の装置に接続されており、両方の装置とも電源が入っています。</li> <li>My side not connected: シリアル ケーブルがこの装置に接続されていません。ケーブルがもう一方の装置に接続されているかどうかは不明です。</li> <li>Other side is not connected: シリアル ケーブルはこの装置に接続されていますが、もう一方の装置には接続されていません。</li> <li>Other side powered off: 相手装置の電源がオフになっています。</li> <li>N/A: LAN ベースのフェールオーバーはイネーブルです。</li> </ul> |
| Failover Unit            | Primary または Secondary                                                                                                                                                                                                                                                                                                                                                 |
| Failover LAN Interface   | フェールオーバー リンクの論理名または物理名が表示されます。                                                                                                                                                                                                                                                                                                                                        |
| Unit Poll frequency      | hello メッセージがピア装置に送信される間隔の秒数と、装置がフェールオーバー リンクで hello メッセージを受信する待機時間の秒数が表示されます。この秒数を超えて hello メッセージを受信しない場合、ピアに障害が発生したと宣言されます。                                                                                                                                                                                                                                          |
| Interface Poll frequency | <p><i>n</i> seconds</p> <p><b>failover polltime interface</b> コマンドで設定した秒数です。デフォルトは、15 秒です。</p>                                                                                                                                                                                                                                                                        |
| Interface Policy         | 数または割合が表示されます。この数または割合を超えたインターフェイスが故障すると、フェールオーバーがトリガーされます。                                                                                                                                                                                                                                                                                                           |

表 11-4 show failover の表示の説明 (続き)

| フィールド                                       | オプション                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitored Interfaces                        | 監視中のインターフェイス数と、監視可能最大インターフェイス数が表示されます。                                                                                                                                                                                                                                                                                                                                                                  |
| failover replication http                   | ステートフル フェールオーバーに対して HTTP ステート複製がイネーブルの場合に表示されます。                                                                                                                                                                                                                                                                                                                                                        |
| Last Failover at:                           | 最後のフェールオーバーの日付と時刻。形式は次のとおりです。<br><br><i>hh:mm:ss UTC DayName Month Day yyyy</i><br><br>UTC (世界標準時) は、GMT (グリニッジ標準時) と同じです。                                                                                                                                                                                                                                                                              |
| This host:                                  | ホストごとに、次の情報が表示されます。                                                                                                                                                                                                                                                                                                                                                                                     |
| Other host:                                 |                                                                                                                                                                                                                                                                                                                                                                                                         |
| Primary または Secondary                       | <ul style="list-style-type: none"> <li>• Active</li> <li>• Standby</li> </ul>                                                                                                                                                                                                                                                                                                                           |
| Active time:                                | <i>n (sec)</i><br><br>装置がアクティブ状態にあった時間。この時間は累積です。したがって、スタンバイ装置にも、過去にアクティブであった場合は値が表示されます。                                                                                                                                                                                                                                                                                                               |
| slot x                                      | スロットのモジュールに関する情報、または空。                                                                                                                                                                                                                                                                                                                                                                                  |
| Interface name (n.n.n.n):                   | <p>インターフェイスごとに、各装置で現在使用している IP アドレス、および次の状態のいずれかが表示されます。</p> <ul style="list-style-type: none"> <li>• Failed: インターフェイスに障害が発生しました。</li> <li>• No Link: インターフェイスの回線プロトコルがダウンしています。</li> <li>• Normal: インターフェイスが正しく動作しています。</li> <li>• Link Down: インターフェイスは管理上シャットダウンされました。</li> <li>• Unknown: セキュリティ アプライアンスがインターフェイスのステータスを判別できません。</li> <li>• Waiting: 相手装置のネットワーク インターフェイスの監視はまだ開始されていません。</li> </ul> |
| Stateful Failover Logical Update Statistics | 次のフィールドは、ステートフル フェールオーバー機能に関係します。Link フィールドにインターフェイス名が表示されている場合、ステートフル フェールオーバー統計情報が表示されます。                                                                                                                                                                                                                                                                                                             |
| Link                                        | <ul style="list-style-type: none"> <li>• <i>interface_name</i>: ステートフル フェールオーバー リンクに使用するインターフェイス。</li> <li>• Unconfigured: ステートフル フェールオーバーを使用していません。</li> <li>• up: インターフェイスは実行中で、機能しています。</li> <li>• down: インターフェイスは管理上シャットダウンされたか、物理的にダウンしています。</li> <li>• failed: インターフェイスに障害が発生し、ステートフル データが渡されていません。</li> </ul>                                                                                    |



表 11-4 show failover の表示の説明 (続き)

| フィールド                            | オプション                                                                                                                                                                                                                                                                                     |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stateful Obj                     | 各フィールド型で、次の統計情報が表示されます。これらは、2 台の装置の間で送信されたステート情報パケットのカウンタです。フィールドは必ずしも、装置を通過するアクティブな接続を示すわけではありません。 <ul style="list-style-type: none"> <li>• xmit：相手装置に送信されたパケットの数</li> <li>• xerr：相手装置にパケットを送信中に発生したエラーの数</li> <li>• rcv：受信されたパケットの数</li> <li>• rerr：相手装置からパケットを受信中に発生したエラーの数</li> </ul> |
| General                          | ステートフル オブジェクトの総数。                                                                                                                                                                                                                                                                         |
| sys cmd                          | 論理更新システム コマンド (LOGIN、Stay Alive など)。                                                                                                                                                                                                                                                      |
| up time                          | アップタイム (アクティブ装置がスタンバイ装置に渡す値)。                                                                                                                                                                                                                                                             |
| RPC services                     | Remote Procedure Call (リモート プロシージャ コール) 接続の情報。                                                                                                                                                                                                                                            |
| TCP conn                         | TCP 接続の情報。                                                                                                                                                                                                                                                                                |
| UDP conn                         | ダイナミック UDP 接続の情報。                                                                                                                                                                                                                                                                         |
| ARP tbl                          | ダイナミック ARP テーブルの情報。                                                                                                                                                                                                                                                                       |
| L2BRIDGE tbl                     | レイヤ 2 ブリッジ テーブルの情報 (透過ファイアウォール モードのみ)。                                                                                                                                                                                                                                                    |
| Xlate_Timeout                    | 接続変換タイムアウトの情報を示します。                                                                                                                                                                                                                                                                       |
| VPN IKE upd                      | IKE 接続の情報。                                                                                                                                                                                                                                                                                |
| VPN IPSEC upd                    | IPSec 接続の情報。                                                                                                                                                                                                                                                                              |
| VPN CTCP upd                     | cTCP トンネル接続の情報。                                                                                                                                                                                                                                                                           |
| VPN SDI upd                      | SDI AAA 接続の情報。                                                                                                                                                                                                                                                                            |
| VPN DHCP upd                     | トンネル DHCP 接続の情報。                                                                                                                                                                                                                                                                          |
| GTP PDP                          | GTP PDP アップデート情報。この情報は、inspect GTP がイネーブルの場合にのみ適用されます。                                                                                                                                                                                                                                    |
| GTP PDPMCB                       | GTP PDPMCB アップデート情報。この情報は、inspect GTP がイネーブルの場合にのみ適用されます。                                                                                                                                                                                                                                 |
| Logical Update Queue Information | 各フィールド型で、次の統計情報が使用されます。 <ul style="list-style-type: none"> <li>• Cur：現在のパケット数</li> <li>• Max：最大パケット数</li> <li>• Total：合計パケット数</li> </ul>                                                                                                                                                  |
| 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。                                                                                                                                                                                                                                                                              |

## フェールオーバーの表示：Active/Active

次に、Active/Active 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 11-5 に、表示される情報についての説明を示します。

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: third GigabitEthernet0/2 (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)

slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.11)S91(0.11)) status (Up)
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)

slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.1)S91(0.1)) status (Up)
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 : third GigabitEthernet0/2 (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、Active/Active 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** コマンドの情報と似ていますが、指定されたグループの情報に限定されています。表 11-5 に、表示される情報についての説明を示します。

```

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 11-5 show failover の表示の説明

| フィールド                    | オプション                                                                                                                        |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Failover                 | <ul style="list-style-type: none"> <li>On</li> <li>Off</li> </ul>                                                            |
| Failover Unit            | Primary または Secondary                                                                                                        |
| Failover LAN Interface   | フェールオーバー リンクの論理名または物理名が表示されます。                                                                                               |
| Unit Poll frequency      | hello メッセージがピア装置に送信される間隔の秒数と、装置がフェールオーバー リンクで hello メッセージを受信する待機時間の秒数が表示されます。この秒数を超えて hello メッセージを受信しない場合、ピアに障害が発生したと宣言されます。 |
| Interface Poll frequency | <p><i>n</i> seconds</p> <p><b>failover polltime interface</b> コマンドで設定した秒数です。デフォルトは、15 秒です。</p>                               |
| Interface Policy         | 数または割合が表示されます。この数または割合を超えたインターフェイスが故障すると、フェールオーバーがトリガーされます。                                                                  |
| Monitored Interfaces     | 監視中のインターフェイス数と、監視可能最大インターフェイス数が表示されます。                                                                                       |

表 11-5 show failover の表示の説明 (続き)

| フィールド                                                  | オプション                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group 1 Last Failover at:<br>Group 2 Last Failover at: | 各グループの最後のフェールオーバーの日付と時刻。形式は次のとおりです。<br><br><i>hh:mm:ss UTC DayName Month Day yyyy</i><br><br>UTC (世界標準時) は、GMT (グリニッジ標準時) と同じです。                                                                                                                                                                                                                                                            |
| This host:<br>Other host:                              | ホストごとに、次の情報が表示されます。                                                                                                                                                                                                                                                                                                                                                                         |
| Role                                                   | Primary または Secondary                                                                                                                                                                                                                                                                                                                                                                       |
| System State                                           | <ul style="list-style-type: none"> <li>Active または Standby Ready</li> <li>アクティブ時間 (秒)</li> </ul>                                                                                                                                                                                                                                                                                             |
| Group 1 State<br>Group 2 State                         | <ul style="list-style-type: none"> <li>Active または Standby Ready</li> <li>アクティブ時間 (秒)</li> </ul>                                                                                                                                                                                                                                                                                             |
| slot x                                                 | スロットのモジュールに関する情報、または空。                                                                                                                                                                                                                                                                                                                                                                      |
| context Interface name<br>(n.n.n.n):                   | <p>インターフェイスごとに、各装置で現在使用している IP アドレス、および次の状態のいずれかが表示されます。</p> <ul style="list-style-type: none"> <li>Failed: インターフェイスに障害が発生しました。</li> <li>No Link: インターフェイスの回線プロトコルがダウンしています。</li> <li>Normal: インターフェイスが正しく動作しています。</li> <li>Link Down: インターフェイスは管理上シャットダウンされました。</li> <li>Unknown: セキュリティ アプライアンスがインターフェイスのステータスを判別できません。</li> <li>Waiting: 相手装置のネットワーク インターフェイスの監視はまだ開始されていません。</li> </ul> |
| Stateful Failover Logical<br>Update Statistics         | 次のフィールドは、ステートフル フェールオーバー機能に関係します。Link フィールドにインターフェイス名が表示されている場合、ステートフル フェールオーバー統計情報が表示されます。                                                                                                                                                                                                                                                                                                 |
| Link                                                   | <ul style="list-style-type: none"> <li><i>interface_name</i>: ステートフル フェールオーバー リンクに使用するインターフェイス。</li> <li>Unconfigured: ステートフル フェールオーバーを使用していません。</li> <li>up: インターフェイスは実行中で、機能しています。</li> <li>down: インターフェイスは管理上シャットダウンされたか、物理的にダウンしています。</li> <li>failed: インターフェイスに障害が発生し、ステートフル データが渡されていません。</li> </ul>                                                                                  |

表 11-5 show failover の表示の説明 (続き)

| フィールド                            | オプション                                                                                                                                                                                                                                                                                     |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stateful Obj                     | 各フィールド型で、次の統計情報が使用されます。これらは、2 台の装置の間で送信されたステート情報パケットのカウンタです。フィールドは必ずしも、装置を通過するアクティブな接続を示すわけではありません。 <ul style="list-style-type: none"> <li>• xmit：相手装置に送信されたパケットの数</li> <li>• xerr：相手装置にパケットを送信中に発生したエラーの数</li> <li>• rcv：受信されたパケットの数</li> <li>• rerr：相手装置からパケットを受信中に発生したエラーの数</li> </ul> |
| General                          | ステートフル オブジェクトの総数。                                                                                                                                                                                                                                                                         |
| sys cmd                          | 論理更新システム コマンド (LOGIN、Stay Alive など)。                                                                                                                                                                                                                                                      |
| up time                          | アップタイム (アクティブ装置がスタンバイ装置に渡す値)。                                                                                                                                                                                                                                                             |
| RPC services                     | Remote Procedure Call (リモート プロシージャ コール) 接続の情報。                                                                                                                                                                                                                                            |
| TCP conn                         | TCP 接続の情報。                                                                                                                                                                                                                                                                                |
| UDP conn                         | ダイナミック UDP 接続の情報。                                                                                                                                                                                                                                                                         |
| ARP tbl                          | ダイナミック ARP テーブルの情報。                                                                                                                                                                                                                                                                       |
| L2BRIDGE tbl                     | レイヤ 2 ブリッジ テーブルの情報 (透過ファイアウォール モードのみ)。                                                                                                                                                                                                                                                    |
| Xlate_Timeout                    | 接続変換タイムアウトの情報を示します。                                                                                                                                                                                                                                                                       |
| VPN IKE upd                      | IKE 接続の情報。                                                                                                                                                                                                                                                                                |
| VPN IPSEC upd                    | IPSec 接続の情報。                                                                                                                                                                                                                                                                              |
| VPN CTCP upd                     | cTCP トンネル接続の情報。                                                                                                                                                                                                                                                                           |
| VPN SDI upd                      | SDI AAA 接続の情報。                                                                                                                                                                                                                                                                            |
| VPN DHCP upd                     | トンネル DHCP 接続の情報。                                                                                                                                                                                                                                                                          |
| GTP PDP                          | GTP PDP アップデート情報。この情報は、inspect GTP がイネーブルの場合にのみ適用されます。                                                                                                                                                                                                                                    |
| GTP PDPMCB                       | GTP PDPMCB アップデート情報。この情報は、inspect GTP がイネーブルの場合にのみ適用されます。                                                                                                                                                                                                                                 |
| Logical Update Queue Information | 各フィールド型で、次の統計情報が使用されます。 <ul style="list-style-type: none"> <li>• Cur：現在のパケット数</li> <li>• Max：最大パケット数</li> <li>• Total：合計パケット数</li> </ul>                                                                                                                                                  |
| 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。                                                                                                                                                                                                                                                                              |

## 監視対象インターフェイスの表示

監視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 モードの場合は、グローバル コンフィギュレーション モードでこのコマンドを入力します。マルチコンテキスト モードの場合は、コンテキスト内でこのコマンドを入力します。

```
primary/context(config)# show monitor-interface
```

次の例を参考にしてください。

```
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
```

## 実行コンフィギュレーション内のフェールオーバー コマンドの表示

実行コンフィギュレーション内のフェールオーバー コマンドを表示するには、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 モードで動作中の装置の場合は、システム実行スペースでこのコマンドを入力します。**show running-config all failover** を入力すると、実行コンフィギュレーション内のフェールオーバー コマンドが表示され、デフォルト値を変更していないコマンドが含まれています。

## フェールオーバー機能のテスト

フェールオーバーの機能をテストするには、次の手順を実行します。

**ステップ 1** アクティブ装置またはフェールオーバー グループが、たとえば FTP を使用して予期したとおりにトラフィックを渡して、異なるインターフェイスのホスト間でファイルを送信することをテストします。

**ステップ 2** 次のコマンドを入力して、スタンバイ装置に強制的にフェールオーバーします。

- Active/Standby フェールオーバーの場合は、アクティブ装置で次のコマンドを入力します。

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

- Active/Active フェールオーバーの場合は、ホストを接続す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である装置で、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** テストに成功しなかった場合は、**show failover** コマンドを入力して、フェールオーバー ステータスをチェックします。

**ステップ 5** 終了したら、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状態に復元できます。

- Active/Standby フェールオーバーの場合は、アクティブ装置で次のコマンドを入力します。

```
hostname(config)# failover active
```

- Active/Active フェールオーバーの場合は、ホストを接続す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である装置で、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およびモニタリング

ここでは、フェールオーバーの制御方法および監視方法について説明します。ここでは、次の項目について説明します。

- [強制フェールオーバー \(P.11-49\)](#)
- [フェールオーバーのディセーブル化 \(P.11-49\)](#)
- [故障した装置またはフェールオーバー グループの復元 \(P.11-50\)](#)
- [フェールオーバーのモニタリング \(P.11-50\)](#)

### 強制フェールオーバー

スタンバイ装置またはフェールオーバー 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。

- Active/Standby フェールオーバーの場合  
スタンバイ装置で次のコマンドを入力します。

```
hostname# failover active
```

アクティブ装置で次のコマンドを入力します。

```
hostname# no failover active
```

- Active/Active フェールオーバーの場合  
フェールオーバー グループがスタンバイ状態の装置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# failover active group group_id
```

または、フェールオーバー グループがアクティブ状態の装置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
```

システム実行スペースで次のコマンドを入力すると、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
```

Active/Standby 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およびスタンバイ状態が、再起動するまで維持されます。たとえば、スタンバイ装置はスタンバイ モードのままなので、両方の装置はトラフィックを渡し始めません。スタンバイ装置をアクティブにするには（フェールオーバーがディセーブル状態でも）、[P.11-49 の「強制フェールオーバー」](#)を参照してください。

Active/Active ペアのフェールオーバーをディセーブルにすると、どの装置が優先に設定されているかに関係なく、どちらの装置が現在アクティブであっても、アクティブ状態の装置においてフェールオーバー グループがアクティブ状態のままになります。システム実行スペースでは、フェールオーバー コマンドを入力しないでください。

## 故障した装置またはフェールオーバー グループの復元

故障した装置を故障していない状態に復元するには、次のコマンドを入力します。

```
hostname(config)# failover reset
```

故障した Active/Active フェールオーバー グループを故障していない状態に復元するには、次のコマンドを入力します。

```
hostname(config)# failover reset group group_id
```

故障した装置またはグループを故障していない状態にしても自動的にアクティブになりません。復元された装置またはグループは、フェールオーバーによってアクティブにされるまで（強制または通常）、スタンバイ状態のままになっています。例外は、**preempt** コマンドで設定されたフェールオーバー グループです。前にアクティブであった場合、フェールオーバー グループは、**preempt** コマンドで設定されていて、故障したときの装置が優先設定の装置であると、アクティブになります。

## フェールオーバーのモニタリング

フェールオーバーが行われると、両方のセキュリティ アプライアンスからシステム メッセージが送信されます。ここでは、次の項目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.11-50)
- デバッグ メッセージ (P.11-50)
- SNMP (P.11-51)

### フェールオーバー システム メッセージ

セキュリティ アプライアンスは、優先度 2 でフェールオーバーに関連したいくつかのシステム メッセージを発行します。優先度 2 は、クリティカルな状態を示します。これらのメッセージを表示するには、『Cisco Security Appliance Logging Configuration and System Log Messages』のロギングのイネーブル化、およびシステム メッセージの説明の表示を参照してください。



(注)

切り替え中に、フェールオーバーが論理的にシャットダウンされ、その後インターフェイスが起動されて、syslog 411001 および 411002 メッセージが生成されます。これは、正常なアクティビティです。

### 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、『Cisco Security Appliance Command Reference』を参照してください。



(注)

デバッグ出力は CPU プロセスで高優先順位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幅に影響することがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティングセッションの間に限り **debug fover** コマンドを使用してください。



## SNMP

フェールオーバー用の SNMP syslog トラップを受信するには、SNMP トラップを SNMP 管理ステーションに送信するように SNMP エージェントを設定し、syslog ホストを定義し、Cisco syslog MIB をコンパイルして SNMP 管理ステーションに組み込みます。詳細については、『Cisco Security Appliance Command Reference』の `snmp-server` コマンドおよび `logging` コマンドのページを参照してください。

## フェールオーバー コンフィギュレーションの例

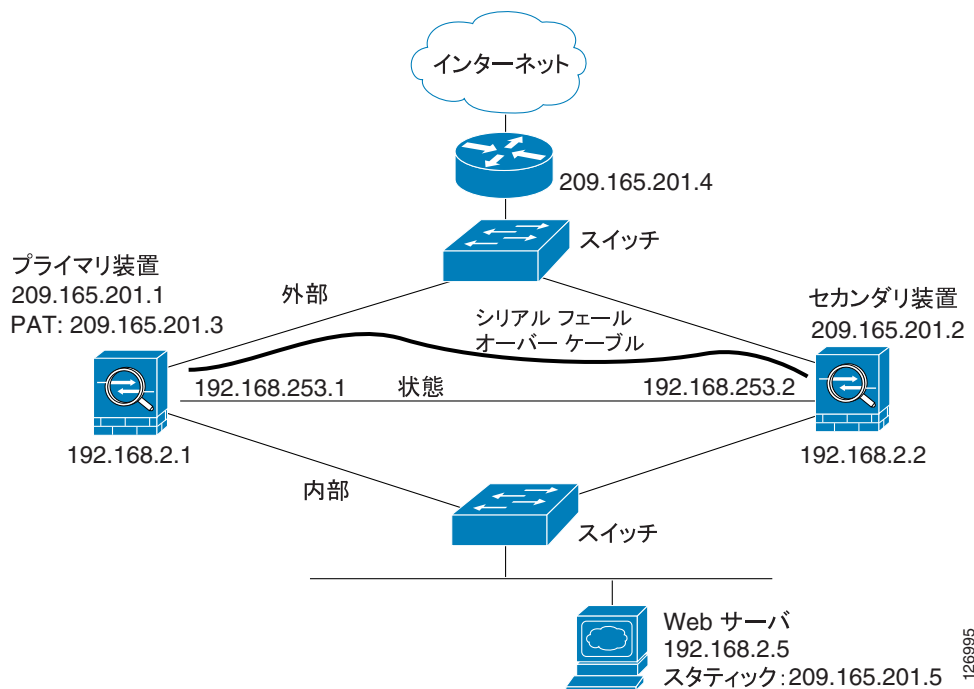
ここでは、コンフィギュレーションおよびネットワーク図のサンプルとして、次の 3 つの例を示します。

- ケーブルベースの Active/Standby フェールオーバーの例 (P.11-51)
- LAN ベースの Active/Standby フェールオーバーの例 (P.11-53)
- LAN ベースの Active/Active フェールオーバーの例 (P.11-55)

## ケーブルベースの Active/Standby フェールオーバーの例

図 11-2 に、シリアル フェールオーバー ケーブルを使用したフェールオーバー コンフィギュレーションのネットワーク図を示します。

図 11-2 ケーブルベースのフェールオーバー コンフィギュレーション



例 11-1 に、ケーブルベースのフェールオーバー コンフィギュレーションにおける代表的なコマンドのリストを示します。

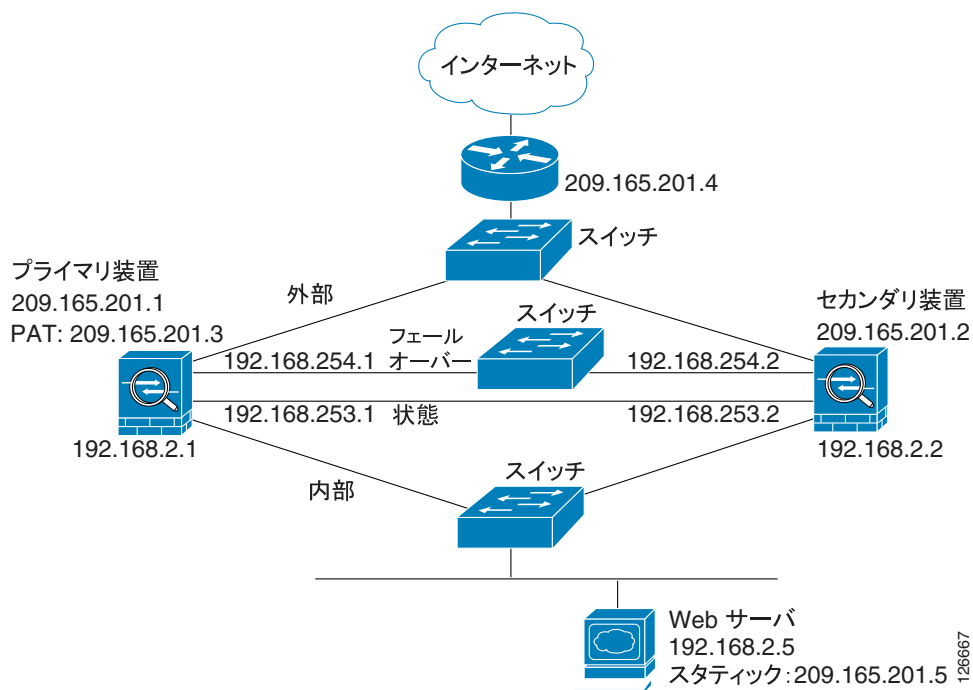
#### 例 11-1 ケーブルベースのフェールオーバー コンフィギュレーション

```
interface Ethernet0
  nameif outside
  speed 100full
  ip address 209.165.201.1 255.255.255.224 standby 209.165.201.2
interface Ethernet1
  nameif inside
  speed 100full
  ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2
interface Ethernet2
  nameif interface2
  security-level 4
  no ip address
interface Ethernet3
  description STATE Failover Interface
  enable password BVKtebKhYT.3gsIp encrypted
passwd iyyymOglaKJgF2fx6 encrypted
telnet 192.168.2.45 255.255.255.255
hostname pixfirewall
access-list acl_out permit tcp any host 209.165.201.5 eq 80
failover
failover link state Ethernet3
failover interface ip state 192.168.253.1 255.255.255.252 standby 192.168.253.2
global (outside) 1 209.165.201.3 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 209.165.201.5 192.168.2.5 netmask 255.255.255.255 0 0
access-group acl_out in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.201.4 1
```

## LAN ベースの Active/Standby フェールオーバーの例

図 11-3 に、イーサネット フェールオーバー リンクを使用したフェールオーバー コンフィギュレーションのネットワーク図を示します。

図 11-3 LAN ベースのフェールオーバー コンフィギュレーション



例 11-2 (プライマリ装置) および 例 11-3 (セカンダリ装置) に、LAN ベースのフェールオーバー コンフィギュレーションにおける代表的なコマンドのリストを示します。



(注)

failover lan enable コマンドは、PIX セキュリティ アプライアンスでのみ必要です。

**例 11-2 LAN ベースのフェールオーバー コンフィギュレーション：プライマリ装置**

```

interface Ethernet0
  nameif outside
  ip address 209.165.201.1 255.255.255.224 standby 209.165.201.2
interface Ethernet1
  nameif inside
  ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2
interface Ethernet2
  description LAN Failover Interface
interface ethernet3
  description STATE Failover Interface
enable password BVKtebKhYT.3gsIp encrypted
passwd iyymOglaKJgF2fx6 encrypted
telnet 192.168.2.45 255.255.255.255
hostname pixfirewall
access-list acl_out permit tcp any host 209.165.201.5 eq 80
failover
failover lan unit primary
failover lan interface failover Ethernet2
failover lan enable
failover key *****
failover link state Ethernet3
failover interface ip failover 192.168.254.1 255.255.255.0 standby 192.168.254.2
failover interface ip state 192.168.253.1 255.255.255.0 standby 192.168.253.2
global (outside) 1 209.165.201.3 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 209.165.201.5 192.168.2.5 netmask 255.255.255.255 0 0
access-group acl_out in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.201.4 1

```

例 11-3 に、セカンダリ装置のコンフィギュレーションを示します。

**例 11-3 LAN ベースのフェールオーバー コンフィギュレーション：セカンダリ装置**

```

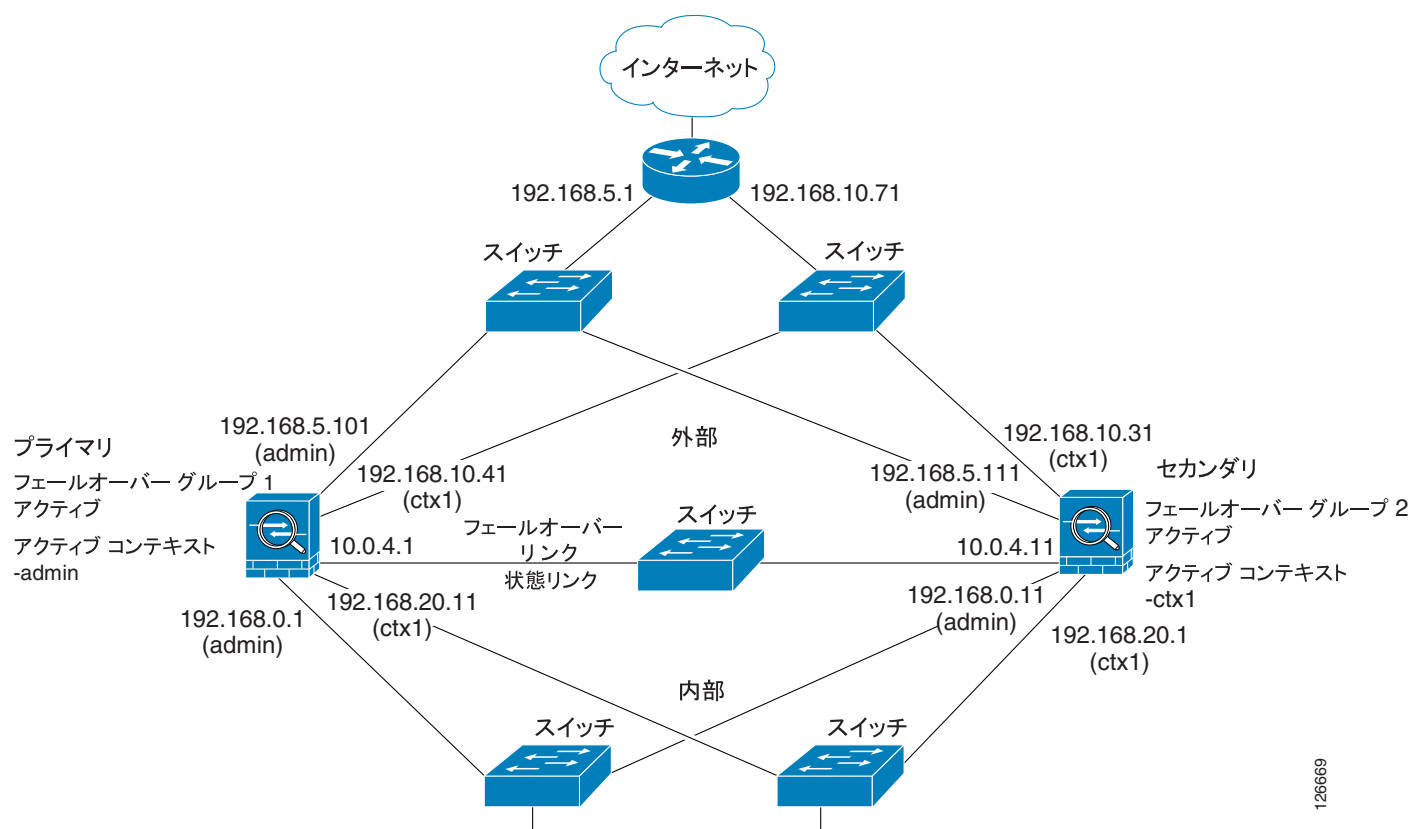
failover
failover lan unit secondary
failover lan interface failover ethernet2
failover lan enable
failover key *****
failover interface ip failover 192.168.254.1 255.255.255.0 standby 192.168.254.2

```

## LAN ベースの Active/ Active フェールオーバーの例

次の例は、Active/Active フェールオーバーの設定方法を示します。この例では、admin と ctx1 という名前の 2 つのコンテキストがあります。図 11-4 に、ネットワーク図の例を示します。

図 11-4 Active/Active フェールオーバー コンフィギュレーション



例 11-4 に、システム コンテキストのコンフィギュレーションを示します。例 11-5 および例 11-6 に、各コンテキストのコンフィギュレーションを示します。

**例 11-4 システム コンテキストのコンフィギュレーション (プライマリ装置)**

```

interface Ethernet0
    description LAN/STATE Failover Interface
interface Ethernet1
interface Ethernet2
interface Ethernet3
interface Ethernet4
interface Ethernet5
interface Ethernet6
interface Ethernet7
interface Ethernet8
interface Ethernet9
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname ciscopix
boot system flash:/cdisk.bin
ftp mode passive
no pager
failover
failover lan unit primary
failover lan interface folink Ethernet0
failover link folink Ethernet0
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
    primary
    preempt
failover group 2
    secondary
    preempt
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h323
0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
console timeout 0
terminal width 80

admin-context admin
context admin
    description admin
    allocate-interface Ethernet1
    allocate-interface Ethernet2
    config-url flash:admin.cfg
    join-failover-group 1

context ctx1
    description context 1
    allocate-interface Ethernet3
    allocate-interface Ethernet4
    config-url flash:ctx1.cfg
    join-failover-group 2

Cryptochecksum:e46a0587966b4c13bf59d7992f994e1e
: end
ciscopix(config)#

ciscopix(config)# changeto context admin
ciscopix/admin(config)#
ciscopix/admin(config)# show running-config
: Saved
:

```

**例 11-5 管理コンテキストのコンフィギュレーション (プライマリ装置)**

```
interface Ethernet1
  nameif outside
  security-level 0
  ip address 192.168.5.101 255.255.255.0 standby 192.168.5.111

interface Ethernet2
  nameif inside
  security-level 100
  ip address 192.168.0.1 255.255.255.0 standby 192.168.0.11

enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname admin
pager lines 24
mtu outside 1500
mtu inside 1500
no vpn-addr-assign aaa
no vpn-addr-assign dhcp
no vpn-addr-assign local
monitor-interface outside
monitor-interface inside
no asdm history enable
arp timeout 14400
route outside 0.0.0.0 0.0.0.0 192.168.5.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h323
0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 outside
fragment chain 24 outside
fragment timeout 5 outside
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
```

**例 11-6 ctx1 コンテキストのコンフィギュレーション (プライマリ装置)**

```

interface Ethernet3
  nameif inside
  security-level 100
  ip address 192.168.20.1 255.255.255.0 standby 192.168.20.11
!
interface Ethernet4
  nameif outside
  security-level 0
  ip address 192.168.10.31 255.255.255.0 standby 192.168.10.41
  asr-group 1
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname ctx1
access-list 201 extended permit ip any any
pager lines 24
logging console informational
mtu inside 1500
mtu outside 1500
no vpn-addr-assign aaa
no vpn-addr-assign dhcp
no vpn-addr-assign local
monitor-interface inside
monitor-interface outside
no asdm history enable
arp timeout 14400
access-group 201 in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.10.71 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h323
0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp

```

**例 11-7 セカンダリ装置のコンフィギュレーション**

セカンダリ セキュリティ アプライアンスについて必要な点は、フェールオーバー リンクを認識するように設定することだけです。セカンダリ セキュリティ アプライアンスは、ブート時またはフェールオーバーが初めてイネーブルになったときに、プライマリ セキュリティ アプライアンスからコンテキスト 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 コンフィギュレーション内の **preempt** コマンドにより、コンフィギュレーションが同期化され、プリエンプション遅延が経過した後に、フェールオーバー グループは指定された装置上でアクティブになります。

```

failover
failover lan unit secondary
failover lan interface folink Ethernet0
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11

```





## PART 2

### ファイアウォールの設定







## ファイアウォール モードの概要

この章では、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を説明します。

セキュリティ アプライアンスは次の 2 つのファイアウォール モードで実行できます。

- ルーテッド モード
- 透過モード

ルーテッド モードでは、セキュリティ アプライアンスはネットワーク内のルータ ホップと見なされます。接続されたネットワーク間で NAT を実行し、(シングルクontext モードで) OSPF または受動 RIP を使用することができます。ルーテッド モードは多数のインターフェイスをサポートしています。インターフェイスはそれぞれ異なるサブネット上に置かれます。コンテキスト間でインターフェイスを共有することもできます。

透過モードでは、セキュリティ アプライアンスは「bump-in-the-wire (BITW)」または「ステルスファイアウォール」のように動作し、ルータ ホップにはなりません。セキュリティ アプライアンスでは、内部インターフェイスと外部インターフェイスに同じネットワークが接続されます。ダイナミック ルーティング プロトコルまたは NAT は使用されません。ただし、ルーテッド モードと同様に、透過モードでも、自動的に許可される ARP パケット以外のトラフィックがセキュリティ アプライアンスを通過できるようにするためにアクセスリストが必要です。透過モードは、サポートされないルーティング プロトコルなど、ルーテッド モードではブロックされるアクセスリスト内の特定のタイプのトラフィックを許可することができます。オプションで、透過モードは EtherType アクセスリストを使用して IP 以外のトラフィックを許可することもできます。透過モードでは、内部インターフェイスと外部インターフェイスの 2 つのインターフェイスだけがサポートされますが、プラットフォームで利用できる場合は専用の管理インターフェイスもサポートされます。



(注)

透過ファイアウォールには管理 IP アドレスが必要です。セキュリティ アプライアンスは、この IP アドレスを、セキュリティ アプライアンスで発信されるパケットの送信元アドレスとして使用します。管理 IP アドレスは、接続されているネットワークと同じサブネット内にある必要があります。

次の事項について説明します。

- [ルーテッド モードの概要 \(P.12-2\)](#)
- [透過モードの概要 \(P.12-9\)](#)

## ルーテッド モードの概要

- IP ルーティングのサポート (P.12-2)
- ネットワーク アドレス変換 (P.12-2)
- ルーテッド ファイアウォール モードでデータがセキュリティ アプライアンスを通過する方法 (P.12-3)

### IP ルーティングのサポート

セキュリティ アプライアンスは、接続されたネットワーク間のルータとして機能します。インターフェイスごとに、異なるサブネット上の IP アドレスが必要です。シングルコンテキスト モードでは、ルーテッド ファイアウォールは OSPF および RIP をサポートします (パッシブ モードで)。マルチコンテキスト モードでは、スタティック ルートだけがサポートされます。過度なルーティングのニーズをセキュリティ アプライアンスに頼るのではなく、アップストリーム ルータとダウンストリーム ルータの拡張ルーティング機能を使用することをお勧めします。

### ネットワーク アドレス変換

NAT は、パケット上のローカル アドレスを、宛先ネットワークでルーティングできるグローバル アドレスに置換します。デフォルトでは、NAT は必要ありません。高セキュリティ インターフェイス (内部) 上のホストに対して、低セキュリティ インターフェイス (外部) と通信する際に NAT を使用することを要求する NAT ポリシーを強制する場合は、NAT 制御をイネーブルにします (**nat-control** コマンドを参照)。

**(注)**

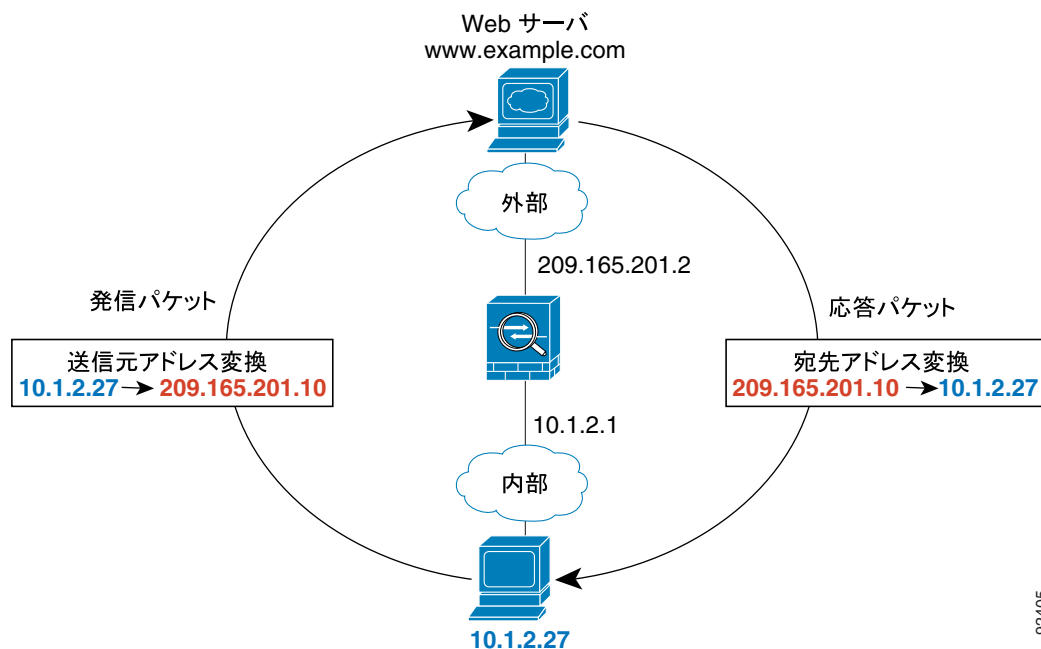
NAT 制御は、バージョン 7.0 より前のソフトウェア バージョンではデフォルトの処理です。セキュリティ アプライアンスを以前のバージョンからアップグレードする場合は、期待される処理を維持するために、**nat-control** コマンドが自動的にコンフィギュレーションに追加されます。

NAT の利点のいくつかを次に示します。

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

図 12-1 は、内部にプライベート ネットワークを持つ一般的な NAT シナリオを示しています。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、パケットのローカル送信元アドレスが、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。Web サーバは応答をグローバル アドレスに送信し、セキュリティ アプライアンスはパケットを受信します。次に、セキュリティ アプライアンスはグローバル アドレスをローカル アドレスに変換してから、それをユーザに送信します。

図 12-1 NAT の例



## ルーテッド ファイアウォール モードでデータがセキュリティ アプライアンスを通過する方法

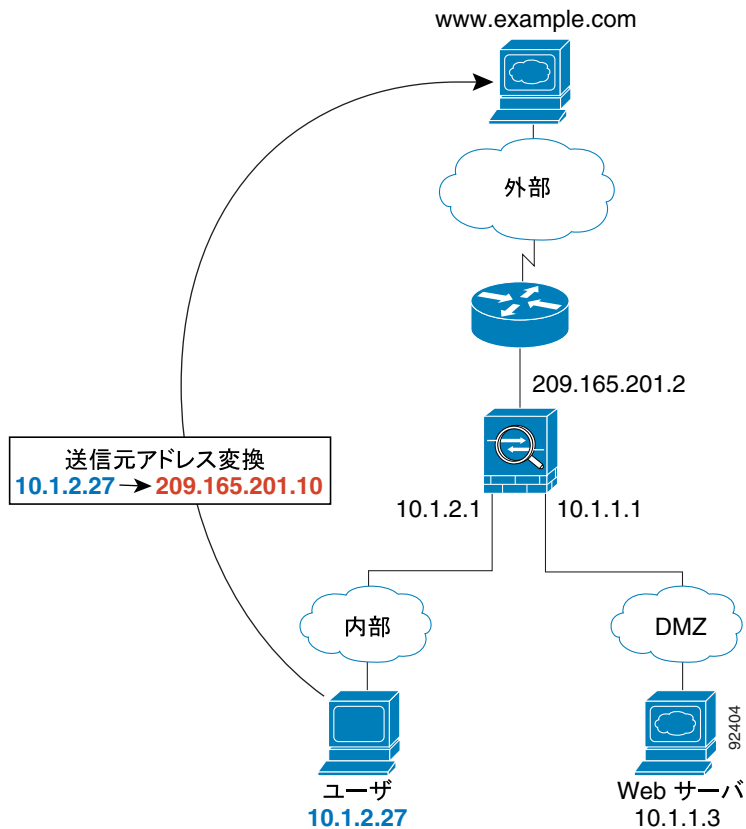
この項では、ルーテッド ファイアウォール モードでデータがセキュリティ アプライアンスをどのように通過するかを説明します。次の項目について説明します。

- 内部ユーザが Web サーバにアクセスする (P.12-4)
- 外部ユーザが DMZ 上の Web サーバにアクセスする (P.12-5)
- 内部ユーザが DMZ 上の Web サーバにアクセスする (P.12-6)
- 外部ユーザが内部ホストにアクセスしようとする (P.12-7)
- DMZ ユーザが内部ホストにアクセスしようとする (P.12-8)

## 内部ユーザが Web サーバにアクセスする

図 12-2 は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 12-2 内部から外部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します (図 12-2 を参照)。

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

マルチコンテキスト モードの場合、セキュリティ アプライアンスは、コンテキストに関連付けられる一意なインターフェイスまたは一意な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、コンテキストでのアドレス変換と照合することによって関連付けられます。この場合、インターフェイスは固有です。www.example.com IP アドレスは、コンテキスト内に最新のアドレス変換を持っていません。

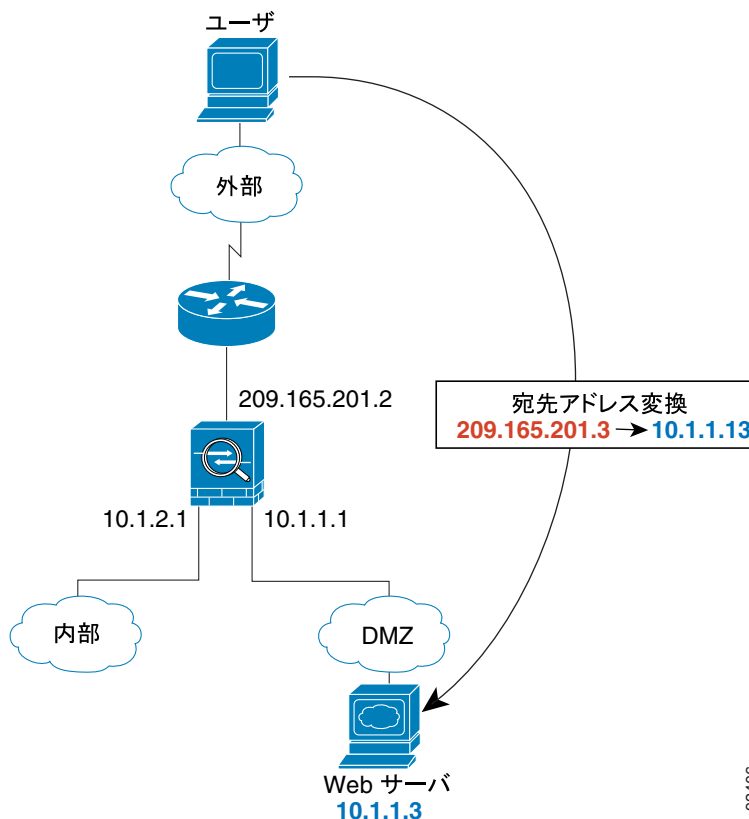
3. セキュリティ アプライアンスは、ローカル送信元アドレス (10.1.2.27) を、外部インターフェイスサブネット上のグローバルアドレス 209.165.201.10 に変換します。  
グローバルアドレスは任意のサブネット上に置くことができますが、外部インターフェイスサブネットに置くとルーティングが簡素化されます。
4. 次に、セキュリティ アプライアンスはセッションが確立されたことを記録し、外部インターフェイスからパケットを転送します。

5. www.example.com が要求に応答すると、パケットはセキュリティ アプライアンスを通過します。これはすでに確立されているセッションであるため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。セキュリティ アプライアンスは、グローバル宛先アドレスをローカル ユーザ アドレス 10.1.2.27 に変換することによって、NAT を実行します。
6. セキュリティ アプライアンスは、パケットを内部ユーザに転送します。

## 外部ユーザが DMZ 上の Web サーバにアクセスする

図 12-3 は、外部ユーザが DMZ Web サーバにアクセスしていることを示しています。

図 12-3 外部から DMZ へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します (図 12-3 を参照)。

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

マルチコンテキスト モードの場合、セキュリティ アプライアンスは、コンテキストに関連付けられる一意なインターフェイスまたは一意な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、コンテキストでのアドレス変換と照合することによって関連付けられます。この場合、分類子は DMZ Web サーバ アドレスがサーバ アドレス変換のため特定のコンテキストに属することを「認識」しています。

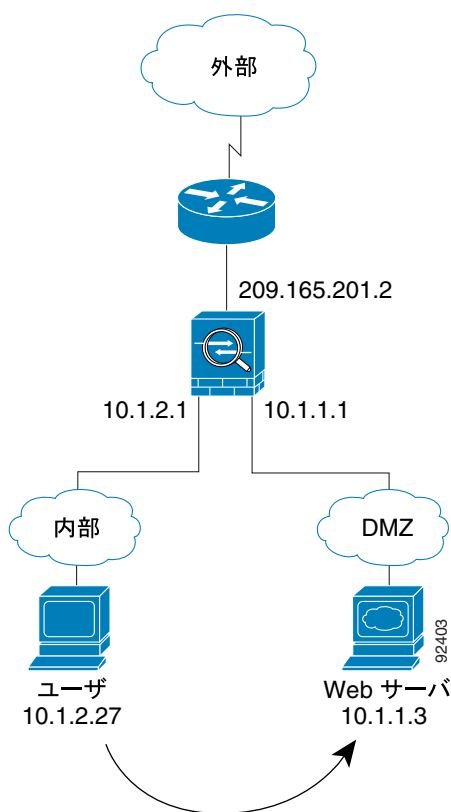
3. セキュリティ アプライアンスは、宛先アドレスをローカル アドレス 10.1.1.3 に変換します。

- 次に、セキュリティ アプライアンスはセッション エントリを高速パスに追加し、DMZ インターフェイスからパケットを転送します。
- DMZ Web サーバが要求に応答すると、パケットはセキュリティ アプライアンスを通過します。また、セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。セキュリティ アプライアンスは、ローカル送信元アドレスを 209.165.201.3 に変換することによって、NAT を実行します。
- セキュリティ アプライアンスは、パケットを外部ユーザに転送します。

## 内部ユーザが DMZ 上の Web サーバにアクセスする

図 12-4 は、内部ユーザが DMZ Web サーバにアクセスしていることを示しています。

図 12-4 内部から DMZ へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します (図 12-4 を参照)。

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

マルチコンテキスト モードの場合、セキュリティ アプライアンスは、コンテキストに関連付けられる一意なインターフェイスまたは一意な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、コンテキストでのアドレス変換と照合することによって関連付けられます。この場合、インターフェイスは固有です。Web サーバ IP アドレスは、最新のアドレス変換を持っていません。

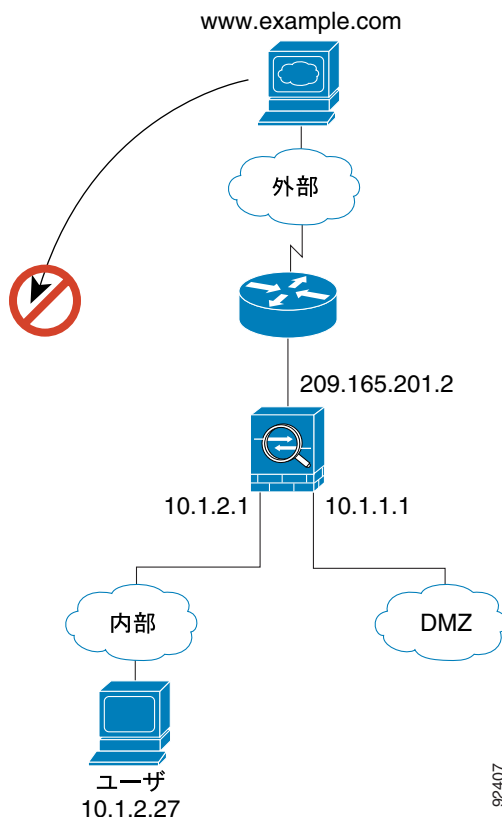


- 次に、セキュリティ アプライアンスはセッションが確立されたことを記録し、DMZ インターフェイスからパケットを転送します。
- DMZ Web サーバが要求に応答すると、パケットは高速パスを通過します。このため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
- セキュリティ アプライアンスは、パケットを内部ユーザに転送します。

## 外部ユーザが内部ホストにアクセスしようとする

図 12-5 は、外部ユーザが内部ネットワークにアクセスしようとしていることを示しています。

図 12-5 外部から内部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します (図 12-5 を参照)。

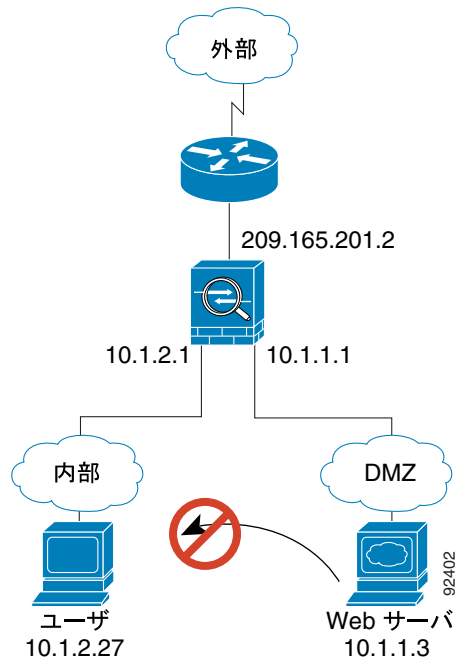
- 外部ネットワーク上のユーザが、内部ホストに到達しようとしています (ホストにルーティング可能な IP アドレスがあると想定します)。  
内部ネットワークがプライベート アドレスを使用している場合、外部ユーザが NAT なしで内部ネットワークに到達することはできません。外部ユーザは既存の NAT セッションを使用して内部ユーザに到達しようとするのが考えられます。
- セキュリティ アプライアンスはパケットを受信します。これは新しいセッションであるため、セキュリティ アプライアンスはセキュリティ ポリシー (アクセスリスト、フィルタ、AAA) に従って、パケットが許可されているかどうかを確認します。
- パケットが拒否され、セキュリティ アプライアンスはパケットをドロップし、接続試行をログに記録します。

外部ユーザが内部ネットワークを攻撃しようとした場合、セキュリティ アプライアンスは多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。

## DMZ ユーザが内部ホストにアクセスしようとする

図 12-6 は、DMZ 内のユーザが内部ネットワークにアクセスしようとしていることを示しています。

図 12-6 DMZ から内部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します (図 12-6 を参照)。

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

## 透過モードの概要

ここでは、透過ファイアウォール モードについて次の項目で説明します。

- 透過ファイアウォールの機能 (P.12-9)
- ネットワークでの透過ファイアウォールの使用 (P.12-10)
- 透過ファイアウォール ガイドライン (P.12-10)
- 透過モードでサポートされない機能 (P.12-11)
- 透過ファイアウォールを通過するデータの動き (P.12-12)

## 透過ファイアウォールの機能

通常、ファイアウォールはルーティングされたホップであり、スクリーニングされたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。一方、透過ファイアウォールは、「bump-in-the-wire (BITW)」または「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとは見なされません。セキュリティ アプライアンスでは、内部ポートと外部ポートに同じネットワークが接続されます。透過ファイアウォールはルーティングされたホップではないので、既存のネットワークに簡単に導入できます。IP 再アドレッシングは必要ありません。

トラブルシューティング用の複雑なルーティング パターンや NAT コンフィギュレーションがないので、保守が容易です。

透過モードはブリッジとして機能しますが、IP トラフィックなどのレイヤ IP 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ない限り、セキュリティ アプライアンスを通過できません。アクセスリストなしで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 検査によって制御されます。

ルーテッド モードでは、アクセスリストで許可しても、いくつかのタイプのトラフィックはセキュリティ アプライアンスを通過できません。一方、透過ファイアウォールは、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) を使用して、どのトラフィックも許可することができます。



(注)

透過モードのセキュリティ アプライアンスは、CDP パケットを通過させません。

たとえば、透過ファイアウォールでルーティング プロトコルの隣接関係を確立できます。つまり、拡張アクセスリストに基づいて、OSPF、RIP、EIGRP、または BGP トラフィックを許可することができます。同様に、HSRP や VRRP などのプロトコルはセキュリティ アプライアンスを通過できます。

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

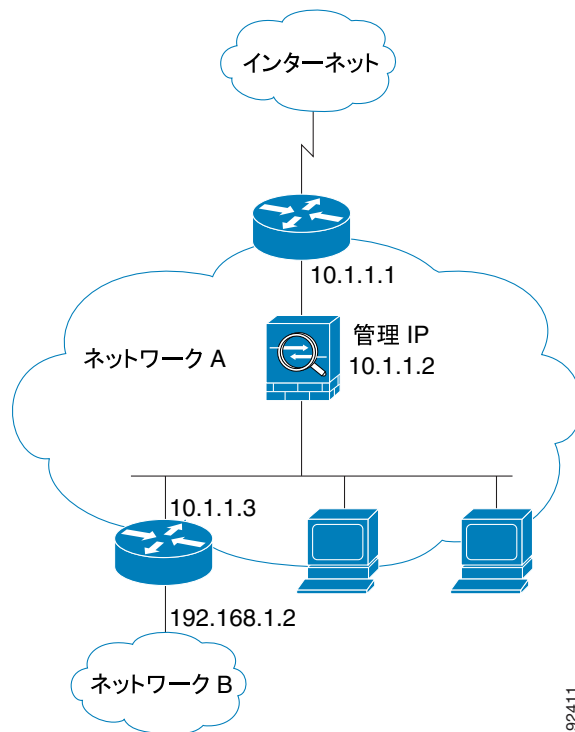
透過ファイアウォールで直接サポートされていない機能の場合は、アップストリーム ルータとダウンストリーム ルータが機能をサポートできるようにトラフィックの通過を許可することができます。たとえば、拡張アクセスリストを使用して、DHCP トラフィック (サポートされない DHCP リレー機能の代わりに) または IP/TV によって作成されたトラフィックなどのマルチキャスト トラフィックを許可できます。

セキュリティ アプライアンスが透過モードで動作している場合、パケットの発信インターフェイスは、ルート ルックアップではなく MAC アドレス ルックアップを実行することによって決定されます。この場合もルート文を設定することはできますが、セキュリティ アプライアンスから発信されたトラフィックだけに適用されます。たとえば、syslog サーバがリモート ネットワークにある場合は、セキュリティ アプライアンスがそのサブネットに到達できるようにスタティック ルートを使用する必要があります。

## ネットワークでの透過ファイアウォールの使用

図 12-7 に、外部デバイスが内部デバイスと同じサブネット上にある一般的な透過ファイアウォール ネットワークを示します。内部ルータとホストは、外部ルータに直接接続されているように見えます。

図 12-7 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 ガイドライン

透過ファイアウォール ネットワークを計画する場合は、次のガイドラインに従ってください。

- 管理 IP アドレスが必要です。マルチコンテキスト モードの場合は、各コンテキストごとに IP アドレスが必要です。

インターフェイスごとに IP アドレスが必要なルーテッドモードと異なり、透過ファイアウォールではデバイス全体に IP アドレスが割り当てられます。セキュリティ アプライアンスは、この IP アドレスを、システム メッセージや AAA 通信など、セキュリティ アプライアンスで発信されるパケットの送信元アドレスとして使用します。

管理 IP アドレスは、接続されているネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。

- 透過セキュリティ アプライアンスは、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。プラットフォームに専用の管理インターフェイスが含まれている場合は、管理トラフィック専用の管理インターフェイスまたはサブインターフェイスを設定することもできます。

シングルモードでは、セキュリティ アプライアンスに 3 つ以上のインターフェイスが含まれている場合でも、2 つのデータ インターフェイス（および使用可能な場合は専用の管理インターフェイス）だけを使用できます。

- 直接に接続された各ネットワークは同一のサブネット上にある必要があります。
- 接続されたデバイス用のデフォルト ゲートウェイとしてセキュリティ アプライアンス管理 IP アドレスを指定しないでください。デバイスはセキュリティ アプライアンスの他方の側の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。
- マルチコンテキスト モードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。
- マルチコンテキスト モードでは、通常、各コンテキストが別個のサブネットを使用します。重複するサブネットを使用することもできますが、ルーティングスタンドポイントから可能にするため、ネットワーク トポロジにルータと NAT コンフィギュレーションが必要です。
- 拡張アクセスリストを使用し、IP トラフィックなどのレイヤ 3 トラフィックがセキュリティ アプライアンスを通過できるようにする必要があります。

オプションで、EtherType アクセスリストを使用して IP 以外のトラフィックの通過を許可することもできます。

## 透過モードでサポートされない機能

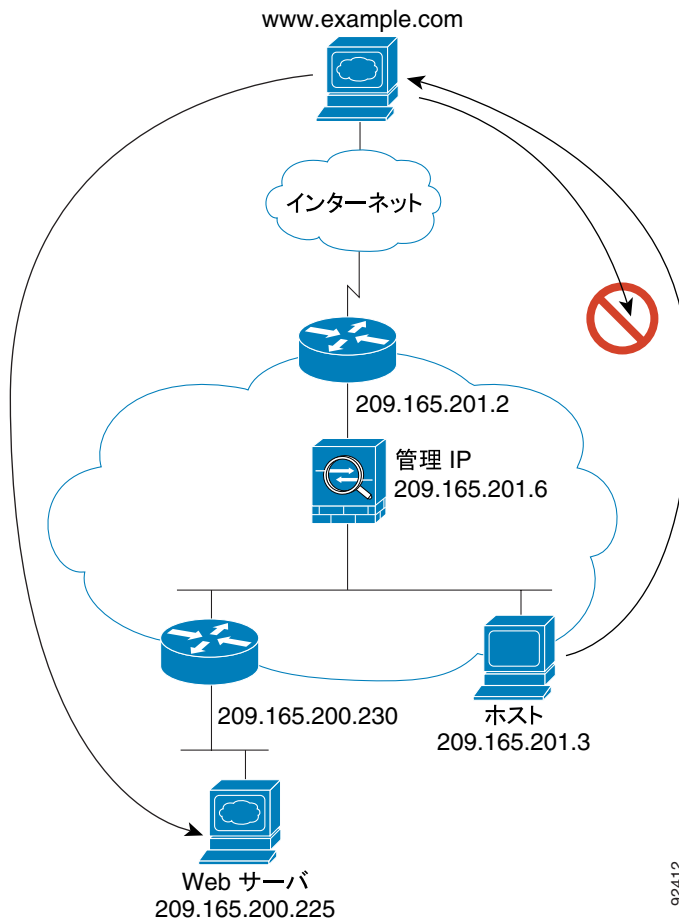
次の機能は透過モードでサポートされていません。

- NAT  
NAT はアップストリーム ルータで実行されます。
- ダイナミック ルーティング プロトコル  
ただし、セキュリティ アプライアンスで発信されたトラフィックのスタティック ルートを追加できます。拡張アクセスリストを使用して、ダイナミック ルーティング プロトコルがセキュリティ アプライアンスを通過できるようにすることもできます。
- IPv6
- 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ができますが、DHCP リレー コマンドはサポートしません。DHCP トラフィックの通過は拡張アクセスリストを使用して許可できるので、DHCP リレーは必要ありません。
- Quality of Service
- 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によって、マルチキャスト トラフィックがセキュリティ アプライアンスを通過できるようにすることができます。
- 通過トラフィック用の VPN ターミネーション  
透過ファイアウォールは、管理接続に対してのみサイトツーサイト VPN トンネルをサポートします。これは、セキュリティ アプライアンスを通過するトラフィックに対して VPN 接続を終端しません。拡張アクセスリストを使用して VPN トラフィックにセキュリティ アプライアンスを通過させることはできませんが、非管理接続は終端されません。

## 透過ファイアウォールを通過するデータの動き

図 12-8 に、パブリック Web サーバを含む内部ネットワークを持つ一般的な透過ファイアウォールの実装を示します。内部ユーザがインターネット リソースにアクセスできるよう、セキュリティ アプライアンスにはアクセスリストがあります。別のアクセスリストによって、外部ユーザは内部ネットワーク上の Web サーバだけにアクセスできます。

図 12-8 一般的な透過ファイアウォールのデータ パス



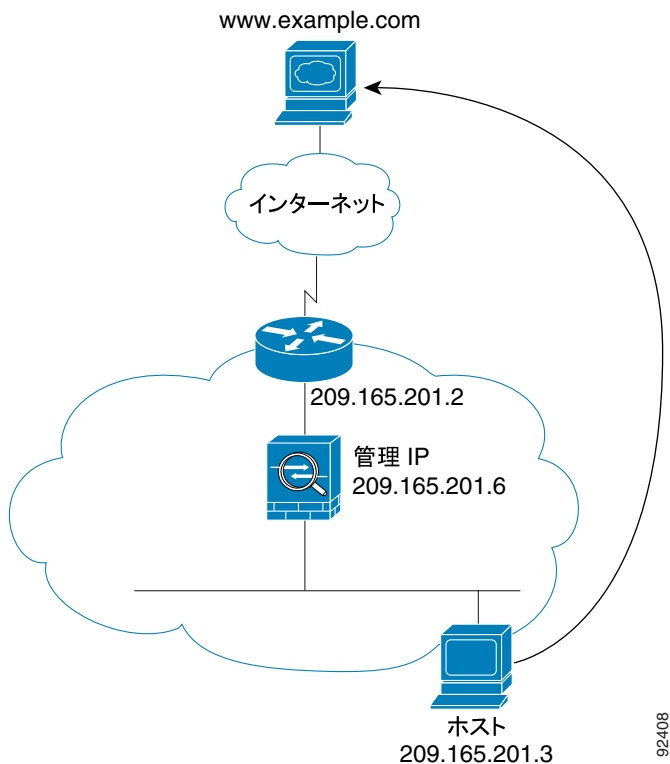
この項では、データがセキュリティ アプライアンスをどのように通過するかを説明します。次の項目について説明します。

- 内部ユーザが Web サーバにアクセスする (P.12-13)
- 外部ユーザが内部ネットワーク上の Web サーバにアクセスする (P.12-14)
- 外部ユーザが内部ホストにアクセスしようとする (P.12-15)

## 内部ユーザが Web サーバにアクセスする

図 12-9 は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 12-9 内部から外部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します (図 12-9 を参照)。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。
2. セキュリティ アプライアンスはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシー (アクセスリスト、フィルタ、AAA) の条件に従って、パケットが許可されていることを確認します。

マルチコンテキスト モードの場合、セキュリティ アプライアンスは、一意なインターフェイスに従ってパケットを分類します。

3. セキュリティ アプライアンスは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、セキュリティ アプライアンス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 209.186.201.2 のアドレスです。

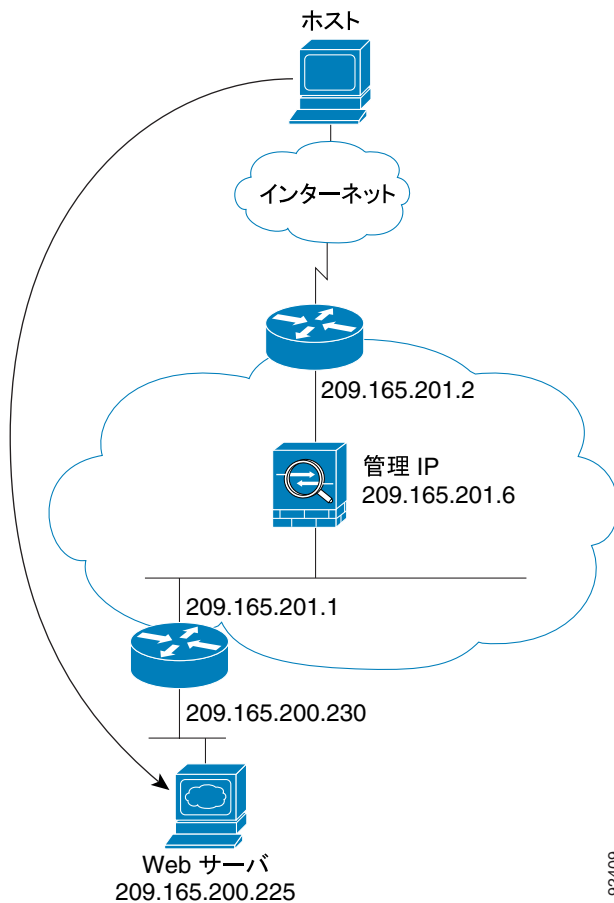
宛先 MAC アドレスがセキュリティ アプライアンスのテーブルにない場合、セキュリティ アプライアンスは、ARP 要求と ping を送信して、MAC アドレスを検出しようとします。最初のパケットはドロップされます。

5. Web サーバが要求に応答すると、必要な場合、セキュリティ アプライアンスは Web サーバの MAC アドレスを MAC アドレス テーブルに追加します。これはすでに確立されているセッションであるため、パケットは、新しい接続に関連付けられる多くのルックアップをバイパスします。
6. セキュリティ アプライアンスは、パケットを内部ユーザに転送します。

## 外部ユーザが内部ネットワーク上の Web サーバにアクセスする

図 12-10 は、外部ユーザが内部 Web サーバにアクセスしていることを示しています。

図 12-10 外部から内部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します(図 12-10 を参照)。

1. 外部ネットワーク上のユーザは、内部 Web サーバから Web ページを要求します。
2. セキュリティ アプライアンスはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシー (アクセスリスト、フィルタ、AAA) の条件に従って、パケットが許可されていることを確認します。

マルチコンテキスト モードの場合、セキュリティ アプライアンスは、一意なインターフェイスに従ってパケットを分類します。

3. セキュリティ アプライアンスは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、セキュリティ アプライアンスは内部インターフェイスからパケットを転送します。宛先 MAC アドレスは、ダウンストリーム ルータ 209.186.201.1 のアドレスです。

宛先 MAC アドレスがセキュリティ アプライアンスのテーブルにない場合、セキュリティ アプライアンスは、ARP 要求と ping を送信して、MAC アドレスを検出しようとします。最初のパケットはドロップされます。

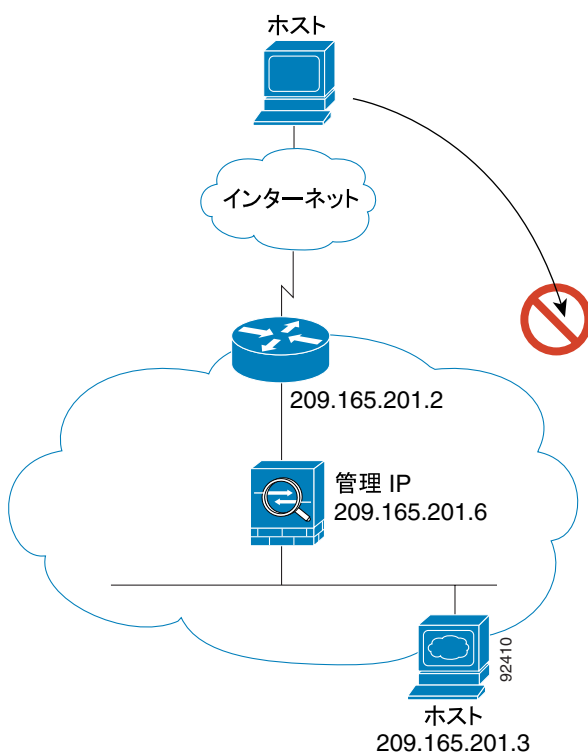


5. Web サーバが要求に応答すると、必要な場合、セキュリティ アプライアンスは Web サーバの MAC アドレスを MAC アドレス テーブルに追加します。これはすでに確立されているセッションであるため、パケットは、新しい接続に関連付けられる多くのルックアップをバイパスします。
6. セキュリティ アプライアンスは、パケットを外部ユーザに転送します。

## 外部ユーザが内部ホストにアクセスしようとする

図 12-11 は、外部ユーザが内部ネットワーク上のホストにアクセスしようとしていることを示しています。

図 12-11 外部から内部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します(図 12-11 を参照)。

1. 外部ネットワーク上のユーザが、内部ホストに到達しようとしています。
2. セキュリティ アプライアンスはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシー (アクセスリスト、フィルタ、AAA) の条件に従って、パケットが許可されているかどうかを確認します。  
マルチコンテキスト モードの場合、セキュリティ アプライアンスは、一意なインターフェイスに従ってパケットを分類します。
3. パケットが拒否され、セキュリティ アプライアンスはパケットをドロップします。
4. 外部ユーザが内部ネットワークを攻撃しようとした場合、セキュリティ アプライアンスは多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判断します。





# アクセスリストによるトラフィックの指定

---

この章では、アクセスリストを使用してトラフィックを指定する方法について説明します。

次の項目について説明します。

- [アクセスリストの概要 \(P.13-2\)](#)
- [拡張アクセスリストの追加 \(P.13-6\)](#)
- [EtherType アクセスリストの追加 \(P.13-9\)](#)
- [標準アクセスリストの追加 \(P.13-11\)](#)
- [Webtype アクセスリストの追加 \(P.13-11\)](#)
- [オブジェクト グループ化機能によるアクセスリストの簡略化 \(P.13-12\)](#)
- [アクセスリストへのコメントの追加 \(P.13-20\)](#)
- [拡張アクセスリストのアクティブ化のスケジュール設定 \(P.13-21\)](#)
- [アクセスリスト アクティビティのロギング \(P.13-23\)](#)

IPv6 アクセスリストについては、[P.9-6](#) の「[IPv6 アクセスリストの設定](#)」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 コントロール エントリ) で構成されます。ACE は、permit 規則または deny 規則を指定するアクセスリスト内の1つのエントリで、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。また、オプションで、送信元ポートおよび宛先ポートに適用される場合もあります。

アクセスリストは、さまざまな機能で使用されます。モジュラ ポリシー フレームワークを使用する機能では、アクセスリストによってトラフィック クラスマップ内のトラフィックを識別できます。モジュラ ポリシー フレームワークの詳細については、[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。

ここでは、次の項目について説明します。

- [アクセスリストのタイプ \(P.13-2\)](#)
- [ACE の順序 \(P.13-3\)](#)
- [アクセス コントロールによる暗黙的な拒否 \(P.13-3\)](#)
- [NAT 使用時にアクセスリストで使用する IP アドレス \(P.13-3\)](#)

## アクセスリストのタイプ

[表13-1](#) に、アクセスリストのタイプと、それらの一般的な使用目的の一部を示します。

**表 13-1 アクセスリストのタイプと一般的な使用目的**

| アクセスリストの使用目的                                  | アクセスリストのタイプ               | 説明                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP トラフィックのネットワーク アクセスの制御 (ルーテッド モード および透過モード) | 拡張                        | <p>セキュリティ アプライアンスは、拡張アクセスリストで明示的に許可されているトラフィックを除き、すべてのトラフィックを許可しません。</p> <p> (注) 管理アクセス用のセキュリティ アプライアンス インターフェイスにアクセスするために、ホスト IP アドレスを許可するアクセスリストを併せて使用する必要はありません。<a href="#">第33章「システム アクセスの管理」</a>に従って管理アクセスを設定するだけで十分です。</p> |
| AAA 規則でのトラフィック識別                              | 拡張                        | AAA 規則では、アクセスリストを使用してトラフィックを識別します。                                                                                                                                                                                                                                                                                  |
| 所定のユーザに関する IP トラフィックのネットワーク アクセス制御            | 拡張、ユーザごとに AAA サーバからダウンロード | ユーザに適用するダイナミック 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。または、セキュリティ アプライアンス上に設定済みのアクセスリストの名前を送信するようにサーバを設定できます。                                                                                                                                                                                                         |
| NAT (ポリシー NAT および NAT 免除) のアドレス識別             | 拡張                        | ポリシー NAT を使用すると、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り、アドレスを変換するローカルトラフィックを指定できます。                                                                                                                                                                                                                                      |
| 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。                                                                                                                                                                                                                                                                                          |
| モジュラ ポリシーのトラフィック クラスマップ内でのトラフィック識別            | 拡張<br>EtherType           | アクセスリストを使用すると、クラスマップ内のトラフィックを識別できます。このマップは、モジュラ ポリシー フレームワークをサポートする機能に使用されます。モジュラ ポリシー フレームワークをサポートする機能には、TCP および一般的な接続設定や検査などがあります。                                                                                                                                                                                |

表 13-1 アクセスリストのタイプと一般的な使用目的（続き）

| アクセスリストの使用目的                                  | アクセスリストのタイプ | 説明                                                               |
|-----------------------------------------------|-------------|------------------------------------------------------------------|
| 透過ファイアウォール モードの場合、IP 以外のトラフィックのネットワーク アクセスの制御 | EtherType   | トラフィックを EtherType に基づいて制御するためのアクセスリストを設定できます。                    |
| OSPF ルート再配布の指定                                | 標準          | 標準アクセスリストには、宛先アドレスだけが含まれています。標準アクセスリストを使用して、OSPF ルートの再配布を制御できます。 |
| WebVPN のフィルタリング                               | Webtype     | URL をフィルタリングするように Webtype アクセスリストを設定できます。                        |

## ACE の順序

アクセスリストは、1 つまたは複数の ACE で構成されます。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。

特定のアクセスリスト名に対して入力した各 ACE は、そのアクセスリストの末尾に追加されます。

ACE の順序は重要です。セキュリティ アプライアンスは、パケットを転送するかドロップするかを決定するとき、エントリがリストされている順序で各 ACE とパケットを照合します。一致が見つかり、ACE はそれ以上チェックされません。たとえば、すべてのトラフィックを明示的に許可する ACE をアクセスリストの先頭に作成した場合、それより後の文はまったくチェックされません。

ACE をディセーブルにするには、`access-list` コマンドで *inactive* キーワードを指定します。

## アクセス コントロールによる暗黙的な拒否

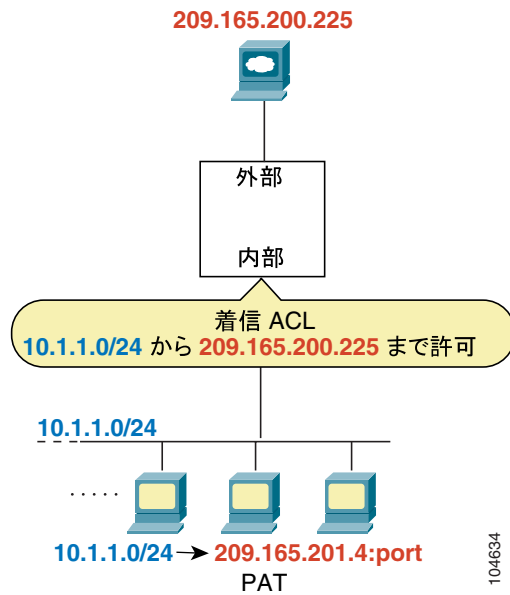
アクセスリストの末尾には、暗黙的な拒否があるため、明示的に許可しない限り、トラフィックは通過できません。たとえば、特定のアドレス以外のすべてのユーザがセキュリティ アプライアンス経由でネットワークにアクセスできるようにするには、特定のアドレスを拒否してから、その他のすべてのアドレスを許可する必要があります。

## NAT 使用時にアクセスリストで使用する 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、アクセスリストが適用されるインターフェイスによって異なります。つまり、そのインターフェイスに接続され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。使用されるアドレスは宛先によって決まるのではなく、インターフェイスによってだけ決まるというガイドラインは、着信アクセスリストと発信アクセスリストの両方に当てはまります。

たとえば、アクセスリストを内部インターフェイスの着信方向に適用するとします。内部の送信元アドレスが外部アドレスにアクセスするときに、内部の送信元アドレスに対して NAT を実行するように、セキュリティ アプライアンスを設定します。アクセスリストは内部インターフェイスに適用されるため、送信元アドレスは変換されていない元のアドレスです。外部アドレスは変換されないため、アクセスリストで使用する宛先アドレスは実際のアドレスです（図 13-1 を参照）。

図 13-1 アクセスリスト内の IP アドレス：送信元アドレスに対して使用される NAT

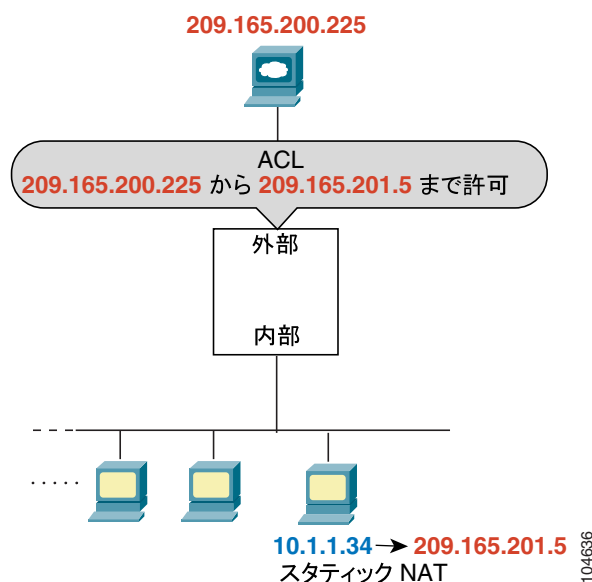


この例について、次のコマンドを参照してください。

```
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
```

内部ホストへのアクセスを外部ホストに許可する場合は、外部インターフェイスに着信アクセスリストを適用します。内部ホストの変換後アドレスは外部ネットワーク上で使用できるアドレスであるため、変換後アドレスをアクセスリストで指定する必要があります（図 13-2 を参照）。

図 13-2 アクセスリスト内の IP アドレス：宛先アドレスに対して使用される NAT

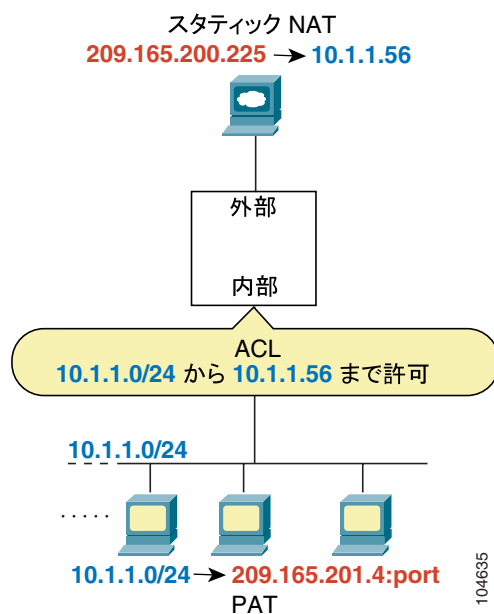


この例について、次のコマンドを参照してください。

```
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に対して NAT を実行する場合は、そのインターフェイスにとって可視のアドレスを使用することに留意してください。図 13-3 では、内部ネットワークで変換後アドレスが示されるように、外部サーバがスタティック NAT を使用しています。

図 13-3 アクセスリスト内の IP アドレス：送信元アドレスと宛先アドレスに対して使用される NAT



この例について、次のコマンドを参照してください。

```
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
```

## 拡張アクセスリストの追加

この項では、アクセスリストを追加する方法について説明します。次の項目を取り上げます。

- 拡張アクセスリストの概要 (P.13-6)
- 拡張 ACE の追加 (P.13-7)

### 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 で構成されます。このリストには、行番号を指定して ACE、送信元アドレス、および宛先アドレスを挿入できます。また、ACE タイプによっては、プロトコル、ポート (TCP または UDP の場合)、または ICMP タイプ (ICMP の場合) も挿入できます。これらのパラメータはすべて、**access-list** コマンドで指定できます。または、各パラメータ用のオブジェクト グループを使用することもできます。この項では、コマンド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 グループの使用方法については、P.13-12 の「オブジェクト グループ化機能によるアクセスリストの簡略化」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、P.13-23 の「アクセスリスト アクティビティのロギング」を参照してください。時間範囲オプションについては、P.13-21 の「拡張アクセスリストのアクティブ化のスケジュール設定」を参照してください。

TCP 接続および UDP 接続については、リターン トラフィックを許可するためのアクセスリストは必要はありません。FWSM は、確立された双方向接続のリターン トラフィックをすべて許可します。ただし、ICMP などのコネクションレス型プロトコルについては、セキュリティ アプライアンスは単方向セッションを確立します。したがって、(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で) アクセスリストで双方向の ICMP を許可するか、ICMP 検査エンジンをイネーブルにする必要があります。ICMP 検査エンジンは、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の各タイプ (拡張および EtherType) に適用できるアクセスリストは 1 つだけです。同一のアクセスリストを複数のインターフェイスに適用できます。アクセスリストをインターフェイスに適用する方法の詳細については、第 15 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 コンフィギュレーションを変更したときに、既存の接続がタイムアウトするまで待機せずに新しいアクセスリスト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できます。

### 透過ファイアウォールを通過する特殊な IP トラフィックの許可

ルーテッド ファイアウォール モードでは、一部のタイプの IP トラフィックは、アクセスリストで許可されている場合でもブロックされます。これには、サポートされていないダイナミック ルーティング プロトコルおよび DHCP (DHCP リレーを設定している場合を除く) が含まれます。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できます。これらの特殊なタイプのトラフィックはコネクションレス型であるため、拡張アクセスリストを両方のインターフェイスに適用して、リターン トラフィックの通過を許可する必要があります。

表 13-2 に、透過ファイアウォールの通過を許可できる一般的なトラフィック タイプを示します。



表 13-2 透過ファイアウォールの特殊トラフィック

| トラフィック タイプ      | プロトコルまたはポート                 | 注意                                                              |
|-----------------|-----------------------------|-----------------------------------------------------------------|
| BGP             | TCP ポート 179                 | —                                                               |
| DHCP            | UDP ポート 67 および 68           | DHCP サーバがイネーブルの場合、セキュリティ アプライアンスは DHCP パケットの通過を拒否します。           |
| 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よって異なります。 | マルチキャスト ストリームは、常に Class D アドレス (224.0.0.0 ~ 239.x.x.x) に送信されます。 |
| RIP (v1 または v2) | UDP ポート 520                 | —                                                               |

## 拡張 ACE の追加

特定のアクセスリスト名に対して **access-list** コマンドを入力するときに、**line** 番号を指定しないと、ACE はアクセスリストの末尾に追加されます。

ACE を追加するには、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} protocol source_address mask [operator port] dest_address mask
[operator port | icmp_type] [inactive]
```



### ヒント

アクセスリスト名は、大文字で入力します。これによって、コンフィギュレーションで名前が見つけやすくなります。アクセスリストには、インターフェイスを表す名前 (INSIDE など) や、作成する目的を表す名前 (NO\_NAT や VPN など) を付けることができます。

通常、プロトコルには **ip** キーワードを指定しますが、他のプロトコルも受け入れられます。プロトコル名のリストについては、[P.D-13 の「プロトコルとアプリケーション」](#)を参照してください。

1 つの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。この場合は、マスクを入力しません。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。

**tcp** プロトコルまたは **udp** プロトコルの場合に限り、送信元ポートおよび宛先ポートを指定できます。使用できるキーワードおよび予約済みポート割り当てのリストについては、[P.D-14 の「TCP ポートと UDP ポート」](#)を参照してください。DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk は、それぞれに TCP の定義と UDP の定義の両方が必要です。TACACS+ では、ポート 49 に対して 1 つの TCP 定義が必要です。

送信元または宛先によって使用されるポート番号を照合するには、**演算子**を使用します。使用できる演算子は、次のとおりです。

- **lt**：小なり。
- **gt**：大なり。
- **eq**：同値。
- **neq**：非同値。

- **range** : 値の包括的な範囲。この演算子を使用する場合は、次のように2つのポート番号を指定します。

```
range 100 200
```

**icmp** プロトコルの場合に限り、ICMP タイプを指定できます。ICMP はコネクションレス型プロトコルであるため、(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で) アクセスリストで両方向の ICMP を許可するか、ICMP 検査エンジンをイネーブルにする必要があります (P.13-16 の「[ICMP タイプ オブジェクト グループの追加](#)」を参照)。ICMP 検査エンジンは、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) (セキュリティ アプライアンスからホストへ) または **echo** (8) (ホストからセキュリティ アプライアンスへ) を指定します。ICMP タイプのリストについては、P.13-16 の「[ICMP タイプ オブジェクト グループの追加](#)」を参照してください。

ネットワーク マスクを指定するときは、指定方法が Cisco IOS ソフトウェアの **access-list** コマンドとは異なることに注意してください。セキュリティ アプライアンスでは、ネットワーク マスク (たとえば、Class C マスクの 255.255.255.0) が使用されます。Cisco IOS マスクでは、ワイルドカード ビット (たとえば、0.0.0.255) が使用されます。

ACE を非アクティブにするには、**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 ACE 全体を入力します。この機能では、再イネーブル化を簡単にするために、非アクティブな ACE のレコードをコンフィギュレーションに保持できます。

次の例を参照してください。

次のアクセスリストでは、すべてのホスト (アクセスリストを適用するインターフェイス上にあるすべてのホスト) に対して、セキュリティ アプライアンスの通過が許可されます。

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

次のサンプル アクセスリストでは、192.168.1.0/24 上のホストが 209.165.201.0/27 ネットワークにアクセスすることが禁止されます。その他のアドレスはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

一部のホストだけにアクセスを制限する場合は、限定的な許可 ACE を入力します。デフォルトでは、明示的に許可しない限り、他のトラフィックはすべて拒否されます。

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

次のアクセスリストでは、すべてのホスト (アクセスリスト適用先のインターフェイス上にあるすべてのホスト) がアドレス 209.165.201.29 の Web サイトにアクセスすることが禁止されます。他のトラフィックはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

## EtherType アクセスリストの追加

### 透過ファイアウォール モードのみ

EtherType ACE は、16 ビットの 16 進数値で指定されるすべての EtherType を制御します。いくつかのタイプは、便宜的にキーワードで指定できます。すべてのトラフィックを特に拒否する EtherType アクセスリストに ACE を追加すると、その ACE により、IP トラフィックおよび ARP トラフィックも拒否されます。これは、IP トラフィックを許可する拡張アクセスリストがある場合も同じです。すべてのアクセスリストの末尾にある暗黙的な拒否では、IP と ARP の通過は許可されます。

EtherType ACE は、IPv6 トラフィックを許可しません。これは、IPv6 EtherType を指定した場合も同じです。

EtherType はコネクションレス型であるため、トラフィックを両方向に通過させる必要がある場合は、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。たとえば、Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット) を許可または拒否できます。デフォルトでは、すべての BPDU が拒否されます。セキュリティ アプライアンスのポートはトランク ポート (シスコ独自) であるため、セキュリティ アプライアンスはトランク ポート BPDU を受信します。トランク BPDU のペイロード内部には VLAN 情報があるため、BPDU を許可した場合、セキュリティ アプライアンスはそのペイロードを発信 VLAN で修正します。フェールオーバーを使用している場合は、EtherType アクセスリストで両方のインターフェイスの BPDU を許可してブリッジンググループを回避する必要があります。

MPLS を許可する場合は、Label Distribution Protocol (LDP; ラベル配布プロトコル) および Tag Distribution Protocol (TDP; タグ配布プロトコル) の TCP 接続がセキュリティ アプライアンスを経由して確立されるようにしてください。これには、セキュリティ アプライアンス インターフェイス上の IP アドレスをラベル配布プロトコルセッションまたは TDP セッションの router-id として使用するよう、セキュリティ アプライアンスに接続されている両方の MPLS ルータを設定します (ラベル配布プロトコルおよび TDP を使用することにより、MPLS ルータは、転送するパケットに使用するラベル (アドレス) をネゴシエートできるようになります)。

Cisco IOS ルータで、使用プロトコル (LDP または TDP) に適したコマンドを入力します。interface は、セキュリティ アプライアンスに接続されている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の各タイプ (拡張および EtherType) に適用できるアクセスリストは 1 つだけです。同一の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 を追加するには、次のコマンドを入力します。

```
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 進数値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> で、RFC 1700 「Assigned Numbers」を参照してください。



(注)

EtherType アクセスリストに **deny all** が設定されている場合、すべてのイーサネット フレームが廃棄されます。その場合でも、自動ネゴシエーションなどの物理プロトコルトラフィックだけは許可されます。

特定のアクセスリスト名に対して **access-list** コマンドを入力すると、ACE はアクセスリストの末尾に追加されます。



*access\_list\_name* は、大文字で入力します。これにより、コンフィギュレーションで名前がつけやすくなります。アクセスリストには、インターフェイスを表す名前（INSIDE など）や、目的を表す名前（MPLS や IPX など）を付けることができます。

たとえば、次のサンプル アクセスリストでは、内部インターフェイスで発信される一般的な EtherType が許可されます。

```
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 はセキュリティ アプライアンスを通過することが許可されますが、IPX は拒否されます。

```
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、両方のインターフェイスで EtherType 0x1256 のトラフィックが拒否されますが、他のトラフィックはすべて許可されます。

```
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

### シングルコンテキスト モードのみ

標準アクセスリストでは、OSPF ルートの宛先 IP アドレスを指定します。このアクセスリストは、OSPF 再配布のルートマップに使用できます。標準アクセスリストをインターフェイスに適用してトラフィックを制御することはできません。

次に、標準 ACE を追加するコマンドを示します。アクセスリストの末尾にもう 1 つ ACE を追加するには、同じアクセスリスト名を指定して別の **access-list** コマンドを入力します。P.8-7 の「[ルートマップの追加](#)」を参照してアクセスリストを適用します。

ACE を追加するには、次のコマンドを入力します。

```
hostname(config)# access-list access_list_name standard {deny | permit} {any | ip_address mask}
```

次のサンプル アクセスリストでは、192.168.1.0/24 へのルートが指定されています。

```
hostname(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

## Webtype アクセスリストの追加

WebVPN のフィルタリングをサポートするコンフィギュレーションにアクセスリストを追加するには、次のコマンドを入力します。

```
hostname(config)# access-list access_list_name webtype {deny | permit} url [url_string | any]
```

ACE の末尾に追加できるロギング オプションについては、P.13-23 の「[アクセスリスト アクティビティのロギング](#)」を参照してください。

## オブジェクト グループ化機能によるアクセスリストの簡略化

この項では、オブジェクト グループ化機能を使用してアクセスリストの作成とメンテナンスを簡略化する方法について説明します。

ここでは、次の項目について説明します。

- オブジェクト グループ化機能の動作 (P.13-12)
- オブジェクト グループの追加 (P.13-13)
- オブジェクト グループのネスト (P.13-17)
- オブジェクト グループの表示 (P.13-19)
- オブジェクト グループの削除 (P.13-19)
- アクセスリストでのオブジェクト グループの使用 (P.13-18)

### オブジェクト グループ化機能の動作

類似オブジェクトをグループにまとめると、オブジェクトごとに ACE を入力する代わりに、ACE でオブジェクト グループを使用できるようになります。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 のタイプ

たとえば、次の3つのオブジェクト グループを考えてみます。

- MyServices: 内部ネットワークへのアクセスが許可されるサービス要求の TCP/UDP ポート番号を含む。
- TrustedHosts: 最大範囲のサービスとサーバへのアクセスが許可されるホスト アドレスとネットワーク アドレスを含む。
- PublicServers: 最大のアクセスが提供されるサーバのホスト アドレスを含む。

上記のグループを作成すると、1つの ACE を使用して、信頼できるホストが公開サーバのグループにサービス要求を許可することが可能になります。

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)

ACE システム制限は、拡張アクセスリストに適用されます。ACE でオブジェクト グループを使用すると、入力する実際の ACE の数は少なくなりますが、拡張 ACE の数はオブジェクト グループがない場合と同じです。多くの場合、オブジェクト グループを使用すると、手動で追加した場合より多くの ACE が作成されます。これは、手動で ACE を作成した場合、オブジェクト グループで作成した場合より多くのアドレスを集約することになるためです。アクセスリストの拡張 ACE の数を表示するには、**show access-list access\_list\_name** コマンドを入力します。

## オブジェクト グループの追加

この項では、オブジェクト グループを追加する方法について説明します。

ここでは、次の項目について説明します。

- [プロトコル オブジェクト グループの追加 \(P.13-13\)](#)
- [ネットワーク オブジェクト グループの追加 \(P.13-14\)](#)
- [サービス オブジェクト グループの追加 \(P.13-15\)](#)
- [ICMP タイプ オブジェクト グループの追加 \(P.13-16\)](#)

### 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には、次の手順を実行します。グループを追加した後、同じグループ名でこの手順を繰り返し、追加のオブジェクトを指定することで、必要に応じてさらにオブジェクトを追加できます。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** 形式で削除するまで残ります。

プロトコル グループを追加するには、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、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 文字のテキスト文字列です。

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** (オプション) 説明を追加するには、次のコマンドを使用します。

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

説明には、最大 200 文字を使用できます。

**ステップ 3** プロトコルごとに次のコマンドを入力して、グループ内にプロトコルを定義します。

```
hostname(config-protocol)# protocol-object protocol
```

protocol は、特定の IP プロトコルの数値識別子 (1 ~ 254) またはキーワード識別子 (たとえば、**icmp**、**tcp**、または **udp**) です。すべての IP プロトコルを含めるには、キーワード **ip** を使用します。指定できるプロトコルのリストについては、[P.D-13 の「プロトコルとアプリケーション」](#)を参照してください。

たとえば、TCP、UDP、および ICMP のプロトコル グループを作成するには、次のコマンドを入力します。

```
hostname(config)# object-group 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には、次の手順を実行します。グループを追加した後、同じグループ名でこの手順を繰り返し、追加のオブジェクトを指定することで、必要に応じてさらにオブジェクトを追加できます。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** 形式で削除するまで残ります。



(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、[P.9-6](#) の「[IPv6 アクセスリストの設定](#)」を参照してください。

ネットワーク グループを追加するには、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、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 文字のテキスト文字列です。

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** (オプション) 説明を追加するには、次のコマンドを使用します。

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

説明には、最大 200 文字を使用できます。

**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、グループ内に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 アドレスを含むネットワーク グループを作成するには、次のコマンドを入力します。

```
hostname(config)# object-group network admins
hostname(config-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には、次の手順を実行します。グループを追加した後、同じグループ名でこの手順を繰り返し、追加のオブジェクトを指定することで、必要に応じてさらにオブジェクトを追加できます。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** 形式で削除するまで残ります。

サービス グループを追加するには、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、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 文字のテキスト文字列です。

**tcp**、**udp**、または **tcp-udp** のいずれかのキーワードで、追加するサービス（ポート）のプロトコルを指定します。同じポート番号で TCP と UDP の両方を使用している場合は、**tcp-udp** キーワードを入力します。たとえば、DNS（ポート 53）の場合です。

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** （オプション）説明を追加するには、次のコマンドを使用します。

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

説明には、最大 200 文字を使用できます。

**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、グループ内に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予約済みポート割り当てのリストについては、[P.D-13 の「プロトコルとアプリケーション」](#)を参照してください。

たとえば、DNS（TCP/UDP）、LDAP（TCP）、および RADIUS（UDP）が含まれたサービス グループを作成するには、次のコマンドを入力します。

```
hostname(config)# object-group 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には、次の手順を実行します。グループを追加した後、同じグループ名でこの手順を繰り返し、追加のオブジェクトを指定することで、必要に応じてさらにオブジェクトを追加できます。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** 形式で削除するまで残ります。

ICMP タイプ グループを追加するには、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、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 文字のテキスト文字列です。

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** (オプション) 説明を追加するには、次のコマンドを使用します。

```
hostname(config-icmp-type)# description text
```

説明には、最大 200 文字を使用できます。

**ステップ 3** タイプごとに次のコマンドを入力して、グループ内に 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、[P.D-18](#) の「[ICMP タイプ](#)」を参照してください。

たとえば、echo-reply および echo (ping を制御するために使用) が含まれる ICMP タイプ グループを作成するには、次のコマンドを入力します。

```
hostname(config)# object-group 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には、まず、[P.13-13](#) の「オブジェクト グループの追加」を参照して、ネストするグループを作成します。その後、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、下位に別のオブジェクト 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、指定したグループをステップ 1 で指定したオブジェクト グループの下位に追加します。

```
hostname(config-group_type)# group-object grp_id
```

ネストするグループは、同じタイプである必要があります。

ネストしたグループ オブジェクトと通常のオブジェクトは、単一のオブジェクト グループ内でさまざまな組み合わせることができます。

たとえば、さまざまな部門に所属する特権ユーザのネットワーク オブジェクト グループを次のように作成します。

```
hostname(config)# object-group network eng  
hostname(config-network)# network-object host 10.1.1.5  
hostname(config-network)# network-object host 10.1.1.9  
hostname(config-network)# network-object host 10.1.1.89
```

```
hostname(config-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
```

その後、3 つすべてのグループを次のようにネストします。

```
hostname(config)# object-group network admin  
hostname(config-network)# group-object eng  
hostname(config-network)# group-object hr  
hostname(config-network)# group-object finance
```

ACE では次のように管理オブジェクト グループを指定するだけです。

```
hostname(config)# access-list ACL_IN extended permit ip object-group admin host  
209.165.201.29
```

## アクセスリストでのオブジェクトグループの使用

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、通常のプロトコル (*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*) の各パラメータを **object-group grp\_id** パラメータで置き換えます。

たとえば、**access-list {tcp | udp}** コマンドで使用可能な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には、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] [log [[level] [interval secs] | disable |
default]] [inactive | time-range time_range_name]
```

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しても、宛先アドレスはアドレスとマスクで指定できます。

次に示す、オブジェクトグループを使用しない通常のアクセスリストでは、内部ネットワーク上のいくつかのホストがいくつかの Web サーバへのアクセスを禁止されます。他のトラフィックはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp 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
```

2つのネットワーク オブジェクトグループ（内部ホスト用に1つ、Web サーバ用に1つ）を作成すると、コンフィギュレーションが簡略化され、簡単に修正してホストを追加できるようになります。

```
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 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、システムは設定されているオブジェクト グループをすべて表示します。

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、次のコマンドを入力します。



(注)

別のアクセスリストで使用されている場合は、オブジェクト グループを削除したり、オブジェクト グループを空に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には、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には、次のコマンドを入力します。

```
hostname(config)# clear object-group [protocol | network | services | icmp-type]
```

タイプを入力しない場合、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含む任意のアクセスリストに、エントリについてのコメントを追加できます。コメントにより、アクセスリストが理解しやすくなります。

最後に入力した **access-list** コマンドの後にコメントを追加するには、次のコマンドを入力します。

```
hostname(config)# access-list access_list_name remark text
```

いずれかの **access-list** コマンドの前にコメントを入力すると、コメントはアクセスリストの最初の行に表示されます。

**no 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 100 文字まで指定できます。テキストの先頭にスペースを入力できます。末尾の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できます。コメントはその場所でアクセスリストに表示されます。コメントの開始位置にダッシュ (-) を入力すると、ACE と区別しやすくなります。

```
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ブ化のスケジュール設定

ACE に時間範囲を適用することで、特定の曜日の特定の時間に ACE がアクティブになるようにスケジュールを設定できます。ここでは、次の項目について説明します。

- [時間範囲の追加 \(P.13-21\)](#)
- [ACE への時間範囲の適用 \(P.13-22\)](#)

### 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、時間範囲の名前を指定します。

```
hostname(config)# time-range name
```

**ステップ 2** 時間範囲は、定期的な時間範囲または絶対的な時間範囲のいずれかとして指定します。

1 つの **time-range** コマンドに両方の時間範囲を指定できます。**time-range** コマンドに **absolute** 値と **periodic** 値の両方が指定されている場合、**periodic** コマンドは **absolute** 開始時間に達した後にのみ評価され、**absolute** 終了時間に達した後は評価されません。

- 定期的な時間範囲を指定する場合

```
hostname(config-time-range)# periodic days-of-the-week time to [days-of-the-week]  
time
```

*days-of-the-week* には次の値を指定できます。

- **monday**、**tuesday**、**wednesday**、**thursday**、**friday**、**saturday**、および **sunday**。
- **daily**
- **weekdays**
- **weekend**

*time* は、*hh:mm* の形式で指定します。たとえば、8:00 は午前 8 時を、20:00 は午後 8 時を意味します。

- 絶対的な時間範囲を指定する場合

```
hostname(config-time-range)# absolute start time date [end time date]
```

*time* は、*hh:mm* の形式で指定します。たとえば、8:00 は午前 8 時を、20:00 は午後 8 時を意味します。

*date* は、*day month year* の形式で指定します。たとえば、**1 january 2006** と指定します。

2006 年 1 月 1 日午前 8 時から始まる絶対的な時間範囲の例を次に示します。終了日時が指定されていないため、時間範囲は無期限で有効です。

```
hostname(config)# time-range for2006  
hostname(config-time-range)# absolute start 8:00 1 january 2006
```

毎週平日午前 8 時から午後 6 時までの定期的な時間範囲の例を次に示します。

```
hostname(config)# time-range workinghours  
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
```

## ACE への時間範囲の適用

ACE に時間範囲を適用するには、次のコマンドを使用します。

```
hostname(config)# access-list access_list_name [extended] {deny |  
permit}...[time-range name]
```

**access-list** コマンドの完全なシンタックスについては、P.13-6 の「[拡張アクセスリストの追加](#)」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は、**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は、**inactive** キーワードを最後のキーワードとして使用します。

---

次の例では、「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バインドしています。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host  
209.165.201.1 time-range New_York_Minute
```



## アクセスリスト アクティビティのロギング

この項では、拡張アクセスリストおよび Webtype アクセスリストのアクセスリスト ロギングを設定する方法について説明します。

ここでは、次の項目について説明します。

- [アクセスリスト ロギングの概要 \(P.13-23\)](#)
- [アクセス コントロール エントリのロギングの設定 \(P.13-24\)](#)
- [拒否フローの管理 \(P.13-25\)](#)

### アクセスリスト ロギングの概要

デフォルトでは、拡張 ACE または Webtype ACE でトラフィックが定義されている場合、セキュリティ アプライアンスは、拒否されたパケットごとに次の形式のシステム メッセージ 106023 を生成します。

```
%ASA|PIX-4-106023: 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
```

セキュリティ アプライアンスが攻撃を受けた場合、拒否されたパケットを示すシステム メッセージの数が非常に大きくなることがあります。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お勧めします。このメッセージは各 ACE の統計情報を示すもので、これを使用することにより、生成されるシステム メッセージの数を制限できます。または、すべてのロギングをディセーブルにする方法もあります。



(注)

ロギング メッセージは、アクセスリストの ACE によってのみ生成されます。アクセスリストの末尾にある暗黙的な拒否によって生成されることはありません。拒否されたすべてのトラフィックによってメッセージが生成されるようにする場合は、次のようにして、手動でアクセスリストの末尾に暗黙的な ACE を追加します。

```
hostname(config)# access-list TEST deny ip any any log
```

拡張 **access-list** コマンドの末尾の **log** オプションを使用すると、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 ロギングに戻る。

システム メッセージ 106100 は次の形式をとります。

```
%ASA|PIX-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で、パケットが ACE と一致した場合、セキュリティ アプライアンスはフロー エントリを作成して、指定された時間内で受信したパケットの数を追跡します。セキュリティ アプライアンスは、最初のヒットがあったとき、および各間隔の終わりにシステム メッセージを生成し、その間隔におけるヒットの合計数を示します。各間隔の終わりに、セキュリティ アプライアンスはヒット数を 0 にリセットします。1 つの間隔内で ACE と一致するパケットがなかった場合、セキュリティ アプライアンスはそのフロー 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、およびポートで定義されます。同じ 2 つのホスト間の新しい接続では、送信元ポートが異なる場合があるため、接続のための新しいフローが作成されると、同じフローの増加は示されない場合があります。ロギングフローの数を制限するには、[P.13-25 の「拒否フローの管理」](#)を参照してください。

確立された接続に属する、許可されたパケットをアクセスリストでチェックする必要はありません。最初のパケットだけがロギングされ、ヒット数に含められます。ICMP などのコネクションレス型プロトコルの場合は、許可されているパケットもすべてロギングされ、拒否されたパケットはすべてロギングされます。

このシステム メッセージの詳細については、『Cisco Security Appliance Logging Configuration and System Log Messages』を参照してください。

## アクセス コントロール エントリのロギングの設定

ACE のロギングを設定するには、**log** オプションに関する次の情報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** コマンドの完全なシンタックスについては、[P.13-6 の「拡張アクセスリストの追加」](#)および [P.13-11 の「Webtype アクセスリストの追加」](#)を参照してください。

引数を指定せずに **log** オプションを入力すると、システム ログメッセージ 106100 はデフォルト レベル (6) とデフォルト間隔 (300 秒) でイネーブルになります。次のオプションを参照してください。

- **level** : 0 ~ 7 の重大度。デフォルトは 6 です。
- **interval secs** : システム メッセージ間の時間間隔 (秒)。1 ~ 600 で指定します。デフォルトは 300 です。この値は、非アクティブ フローを削除するタイムアウト値としても使用されます。
- **disable** : すべてのアクセスリスト ロギングをディセーブルにします。
- **default** : メッセージ 106023 のロギングをイネーブルにします。この設定は、**log** オプションがない場合と同じです。

たとえば、次のアクセスリストを設定します。

```
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
```

パケットが **outside-acl** の最初の ACE によって許可された場合、セキュリティ アプライアンスは次のシステム メッセージを生成します。

```
%ASA|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)
```

この接続の 20 個の後続パケットは、外部インターフェイスに到達しますが、そのトラフィックをアクセスリストでチェックする必要はなく、ヒット数も増加しません。

指定した 10 分間のうちに同じホストによる接続が新たに 1 つ開始された場合 (かつ、送信元ポートと宛先ポートが変わっていない場合)、ヒット数は 1 増加し、10 分間の終わりに次のメッセージが表示されます。

```
%ASA|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)
```

パケットが 3 番目の ACE によって拒否された場合、セキュリティ アプライアンスは次のシステム メッセージを生成します。

```
%ASA|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 分間（デフォルト）のうちにさらに 20 回の試行が行われ、5 分間の終わりに次のメッセージが表示されます。

```
%ASA|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で、パケットが ACE と一致した場合、セキュリティ アプライアンスはフロー エントリを作成して、指定された時間内で受信したパケットの数を追跡します。セキュリティ アプライアンスでは、ACE 用のロギング フローを最大 32 K 保持できます。どの時点でも大量のフローが同時に存在する可能性があります。メモリおよび CPU リソースが無制限に消費されないようにするために、セキュリティ アプライアンスは同時拒否フロー数に制限を設定します。この制限は、拒否フローに対してだけ設定されます（許可フローには設定されません）。これは、拒否フローは攻撃を示している可能性があるためです。制限に達すると、セキュリティ アプライアンスは既存の拒否フローが期限切れにな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、DoS 攻撃（サービス拒絶攻撃）が開始された場合、セキュリティ アプライアンスは大量の拒否フローを短時間のうちに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り、メモリおよび CPU リソースが無制限に消費されないようにします。

拒否フローの最大数に達すると、セキュリティ アプライアンスは次のようなシステム メッセージ 106101 を発行します。

```
%ASA|PIX-1-106101: The number of ACL log deny-flows has reached limit (number).
```

拒否フローの最大数の設定、および拒否フロー アラート メッセージ（106101）間の間隔の設定には、次のコマンドを入力します。

- セキュリティ アプライアンスがロギングを停止するまでの間にコンテキストごとに許可する拒否フローの最大数を設定するには、次のコマンドを入力します。

```
hostname(config)# access-list deny-flow-max number
```

*number* は 1 ～ 4096 で指定します。デフォルトは 4096 です。

- 拒否フローが最大数に達したことを示すシステム メッセージ（番号 106101）間の時間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 で指定します。デフォルトは 300 です。





# NAT の適用

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、セキュリティ アプライアンスは各ネットワーク間の NAT を実行できます。



透過ファイアウォール モードでは、セキュリティ アプライアンスは NAT をサポートしません。

ここでは、次の項目を取り上げます。

- [NAT の概要 \(P.14-2\)](#)
- [NAT 制御の設定 \(P.14-16\)](#)
- [ダイナミック NAT および PAT の使用 \(P.14-17\)](#)
- [スタティック NAT の使用 \(P.14-26\)](#)
- [スタティック PAT の使用 \(P.14-28\)](#)
- [NAT のバイパス \(P.14-31\)](#)
- [NAT の例 \(P.14-35\)](#)

## NAT の概要

この項では、セキュリティ アプライアンスで NAT がどのように機能するかについて説明します。次の項目を取り上げます。

- [NAT の概要 \(P.14-2\)](#)
- [NAT 制御 \(P.14-3\)](#)
- [NAT のタイプ \(P.14-5\)](#)
- [ポリシー NAT \(P.14-10\)](#)
- [NAT および同じセキュリティ レベルのインターフェイス \(P.14-13\)](#)
- [実際のアドレスとの照合に使用される NAT コマンドの順序 \(P.14-13\)](#)
- [マッピング アドレスに関するガイドライン \(P.14-14\)](#)
- [DNS および NAT \(P.14-14\)](#)

## NAT の概要

アドレス変換では、パケット内の実際のアドレスが、宛先ネットワークでルーティング可能なマッピング アドレスに置き換えられます。NAT は 2 つのステップで構成されます。実際のアドレスをマッピング アドレスに変換するプロセスと、その後リターン トラフィック用に変換を元に戻すプロセスです。

セキュリティ アプライアンスは、NAT 規則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。一致する NAT 規則がない場合、そのパケットの処理は続行されます。例外は、NAT 制御をイネーブルにした場合です。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）に移動するパケットが NAT 規則と一致することが要求されます。一致しない場合、パケットの処理は停止されます（セキュリティ レベルの詳細については、[P.6-2 の「セキュリティ レベルの概要」](#)を参照してください。NAT 制御の詳細については、[P.14-3 の「NAT 制御」](#)を参照してください）。



(注)

このマニュアルでは、すべてのタイプの変換を一般に NAT と呼びます。NAT の説明では、*内部* および *外部* という用語は相対的なものであり、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ています。セキュリティ レベルの高い方が内部、セキュリティ レベルの低い方が外部です。たとえば、インターフェイス 1 のセキュリティ レベルが 60 で、インターフェイス 2 のセキュリティ レベルが 50 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」です。

NAT の利点のいくつかを次に示します。

- 内部ネットワークでプライベート アドレスを使用できます。プライベート アドレスは、インターネットにルーティングできません（詳細については、[P.D-2 の「プライベート ネットワーク」](#)を参照してください）。
- NAT は実際のアドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。
- 重複アドレスなど、IP ルーティングの問題を解決できます。

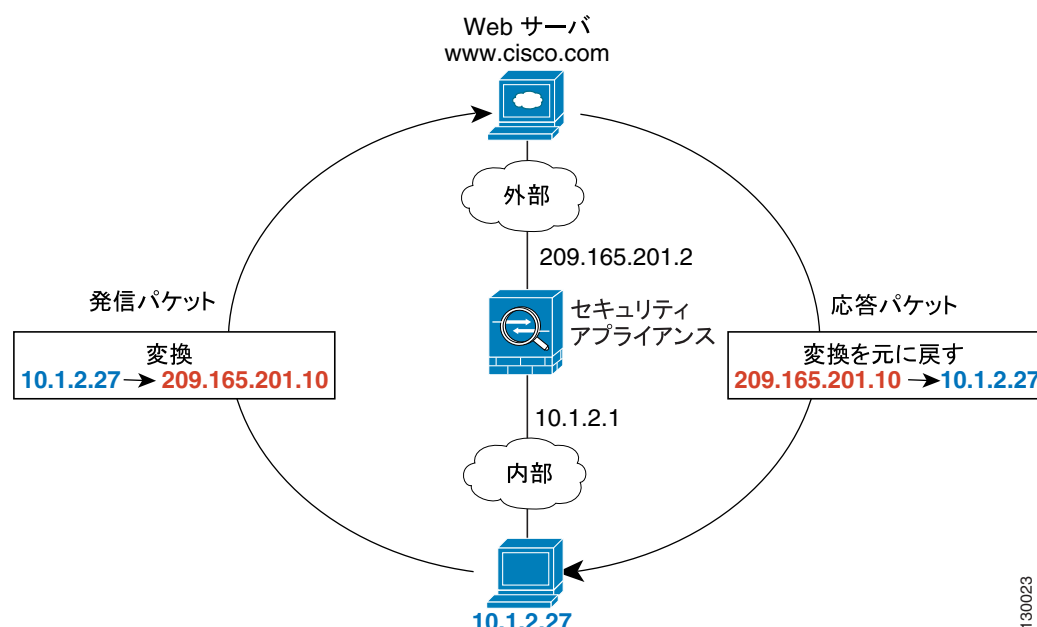


(注)

NAT をサポートしないプロトコルについては、[P.22-3 の表 22-1](#) を参照してください。

図 14-1 に、内部にプライベート ネットワークがある一般的な NAT のシナリオを示します。内部ホスト 10.1.1.27 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.1.27 はマッピング アドレス 209.165.201.10 に変更されます。サーバが応答すると、応答がマッピング アドレス 209.165.201.10 に送信されます。そのパケットをセキュリティ アプライアンスが受信します。セキュリティ アプライアンスはその後、パケットをホストに送信する前に、マッピング アドレス 209.165.201.10 を変換し、実際のアドレス 10.1.1.27 に戻します。

図 14-1 NAT の例



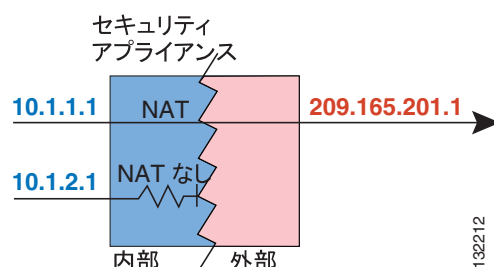
この例について、次のコマンドを参照してください。

```
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

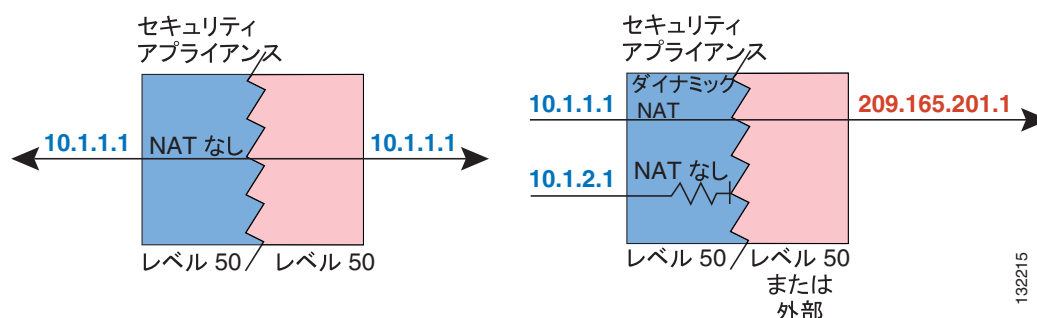
NAT 制御では、内部インターフェイスから外部インターフェイスに移動するパケットが NAT 規則と一致することが要求されます。内部ネットワークの任意のホストが外部ネットワークのホストにアクセスできるようにするには、内部ホスト アドレスが変換されるように NAT を設定する必要があります（図 14-2 を参照）。

図 14-2 NAT 制御と発信トラフィック



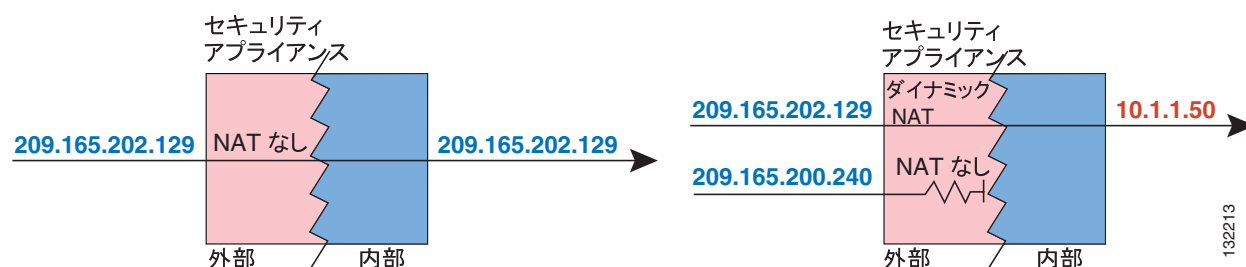
同じセキュリティ レベルのインターフェイスは、NAT を使用して通信することを要求されません。ただし、ダイナミック NAT または PAT を同じセキュリティ レベルのインターフェイス上に設定した場合は、そのインターフェイスから同じセキュリティ レベルのインターフェイス、または外部インターフェイスに向かうすべてのトラフィックは、NAT 規則と一致する必要があります（図 14-3 を参照）。

図 14-3 NAT 制御と同じセキュリティ レベルのトラフィック



同様に、外部のダイナミック NAT または PAT をイネーブルにした場合、すべての外部トラフィックは、内部インターフェイスにアクセスするときに、NAT 規則と一致する必要があります（図 14-4 を参照）。

図 14-4 NAT 制御と着信トラフィック



スタティック NAT では、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、NAT を実行することを選択しない限り、どのネットワークに対しても NAT を実行する必要はありません。ただし、以前のバージョンのソフトウェアからアップグレードした場合は、NAT 制御がシステム上でイネーブルになっている可能性があります。

NAT 制御によってセキュリティを強化し、同時に内部アドレスの変換を回避する必要がある場合は、それらのアドレスに対して NAT 免除規則またはアイデンティティ NAT 規則を適用できます（詳細については、P.14-31 の「NAT のバイパス」を参照してください）。

NAT 制御を設定するには、P.14-16 の「NAT 制御の設定」を参照してください。





(注)

マルチコンテキスト モードでは、パケット分類子が 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ケースもあります。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、分類子によってはネットワーク 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。分類子と NAT の関係の詳細については、[P.3-3 の「セキュリティ アプライアンスによるパケットの分類方法」](#)を参照してください。

## NAT のタイプ

この項では、使用可能な NAT の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の組み合わせとして実装できます。NAT をバイパスする規則を設定することもできます。たとえば、NAT 制御をイネーブルにしている状態で NAT を実行しない場合です。ここでは、次の項目について説明します。

- [ダイナミック NAT \(P.14-5\)](#)
- [PAT \(P.14-7\)](#)
- [スタティック NAT \(P.14-8\)](#)
- [スタティック PAT \(P.14-8\)](#)
- [NAT 制御がイネーブルな状態での NAT のバイパス \(P.14-9\)](#)

## ダイナミック NAT

ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピングアドレスのプールに変換されます。マッピングされたプールにあるアドレスは、実際のグループより少ないことがあります。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、セキュリティ アプライアンスは、マッピングされたプールから IP アドレスをそのホストに割り当てます。変換は、実際のホストが接続を開始したときにだけ追加されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません（『Cisco Security Appliance Command Reference』の `timeout xlate` コマンドを参照してください）。したがって、宛先ネットワークのユーザは、ダイナミック NAT を使用しているホストへの接続を確実に開始できません（アクセスリストでその接続が許可されている場合も同じです）。また、セキュリティ アプライアンスは、実際のホストアドレスに直接接続しようとする試みを拒否します。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](#)」の項または「[スタティック PAT](#)」の項を参照してください。

[図 14-5](#) に、実際のアドレスへの接続を試みているリモート ホストを示します。セキュリティ アプライアンスはマッピングアドレスへのリターン接続だけを許可するため、この接続は拒否されています。

図 14-5 実際のアドレスへの接続を試みているリモート ホスト

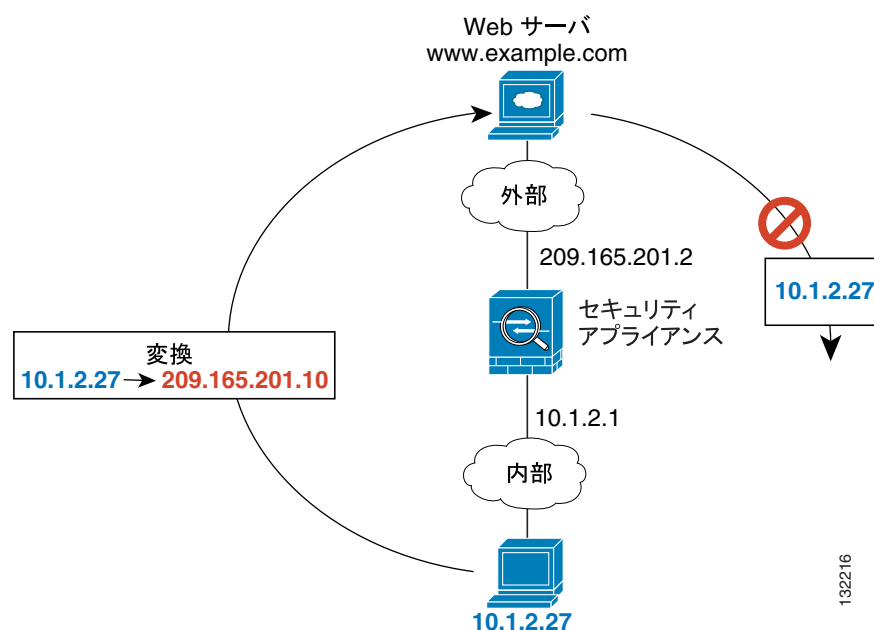
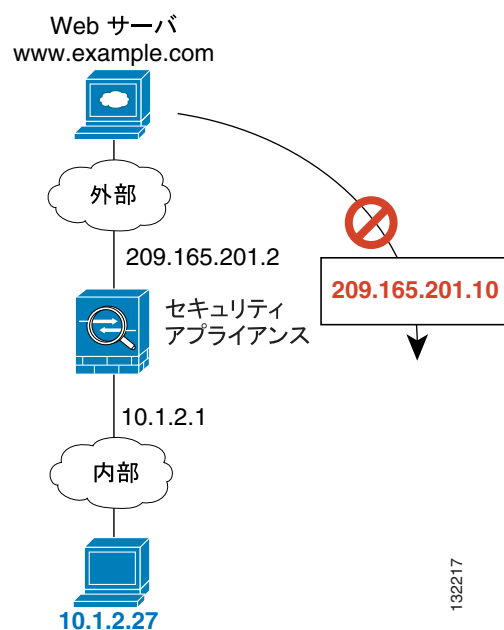


図 14-6 に、マッピングアドレスへの接続開始を試みているリモート ホストを示します。このアドレスは、現時点では変換テーブルにないため、セキュリティ アプライアンスはパケットをドロップしています。

図 14-6 マッピングアドレスへの接続開始を試みているリモート ホスト





(注)

変換が継続している間、アクセスリストで許可されていれば、リモートホストは変換済みホストへの接続を開始できます。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセスリストのセキュリティに依存できます。

ダイナミック NAT には、次の欠点があります。

- マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。

このことが頻繁に起こる場合は、PAT を使用します。PAT では、1 つのアドレスの複数のポートを使用して 64,000 件を超える変換が提供されます。

- マッピングされたプール内のルーティング可能なアドレスを多数使用する必要があります。インターネットなど、宛先ネットワークが登録アドレスを要求する場合は、使用可能なアドレスが不足する可能性があります。

ダイナミック NAT の利点は、一部のプロトコルが 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 などのように、オーバーロードするためのポートがない IP プロトコルでは機能しません。また、PAT は、一部のマルチメディア アプリケーションなどのように、1 つのポート上にデータ ストリームを持ち、別のポート上に制御パスを持ち、公開規格ではない一部のアプリケーションでも機能しません。NAT および PAT のサポートの詳細については、[P.22-2 の「アプリケーション プロトコル検査を使用するタイミング」](#)を参照してください。

## PAT

PAT では、複数の実際のアドレスが 1 つのマッピング IP アドレスに変換されます。具体的には、セキュリティ アプライアンスが複数の実際のアドレスおよび送信元ポート（実際のソケット）を 1 つのマッピング アドレスおよび 1024 より上の一意のポート（マッピング ソケット）に変換します。送信元ポートが接続ごとに異なるため、各接続には別の変換が必要です。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

接続の有効期限が切れると、ポート変換も 30 秒間の非アクティブ状態の後に有効期限切れになります。このタイムアウトは変更できません。宛先ネットワークのユーザは、PAT を使用するホストへの接続を確実に開始できません（アクセスリストでその接続が許可されている場合も同じです）。ユーザがホストの実際のポート番号またはマッピング ポート番号を予測できないだけでなく、変換済みホストが発信側ではない場合、セキュリティ アプライアンスは変換をまったく作成しません。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](#)」の項または「[スタティック PAT](#)」の項を参照してください。

PAT では、1 つのマッピング アドレスを使用できるため、ルーティング可能なアドレスが節約されます。さらに、セキュリティ アプライアンス 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できます。PAT は、制御パスとは異なるデータ ストリームを持つ一部のマルチメディア アプリケーションでは機能しません。NAT および PAT のサポートの詳細については、[P.22-2 の「アプリケーション プロトコル検査を使用するタイミング」](#)を参照してください。



(注)

変換が継続している間、アクセスリストで許可されていれば、リモートホストは変換済みホストへの接続を開始できます。実際のポート アドレスおよびマッピング ポート アドレスはどちらも予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセスリストのセキュリティに依存できます。

## スタティック NAT

スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。ダイナミック NAT および PAT では、各ホストは後続する変換ごとに異なるアドレスまたはポートを使用します。スタティック NAT では、マッピング アドレスは連続する各接続で同じであり、永続的な変換規則が存在するため、宛先ネットワークのホストは変換済みのホストへのトラフィックを開始できます（そのトラフィックを許可するアクセスリストがある場合）。

ダイナミック NAT とスタティック NAT のアドレス範囲との主な違いは、スタティック NAT ではリモート ホストが変換済みのホストへの接続を開始でき（それを許可するアクセスリストがある場合）、ダイナミック NAT では開始できないという点です。スタティック NAT では、実際のアドレスと同数のマッピング アドレスも必要です。

## スタティック PAT

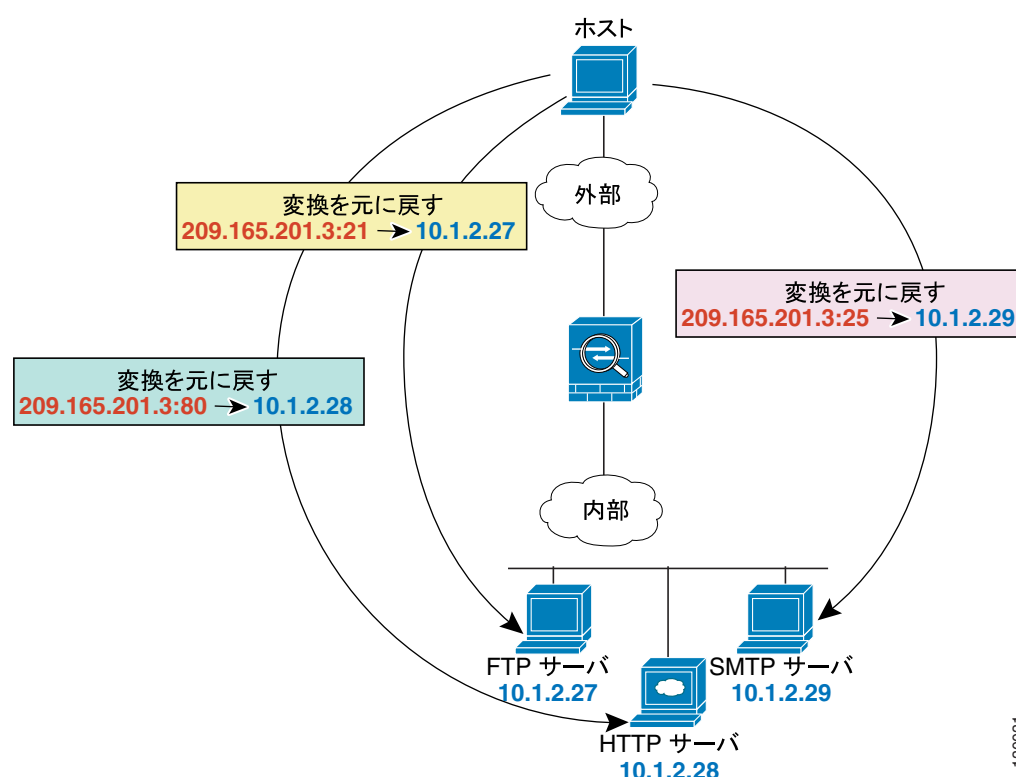
スタティック PAT は、プロトコル（TCP または UDP）および実際のアドレスとマッピング アドレスのポートを指定できる点を除いて、スタティック NAT と同じです。

この機能により、各文のポートが別個である限り、多数の異なるスタティック文にわたって同じマッピング アドレスを指定できます（複数のスタティック NAT 文に対しては、同じマッピング アドレスを使用できません）。

セカンダリ チャネルのアプリケーション検査が必要なアプリケーション（FTP、VoIP など）を使用する場合は、セキュリティ アプライアンスが自動的にセカンダリ ポートを変換します。

たとえば、FTP、HTTP、および SMTP にアクセスするリモート ユーザに 1 つのアドレスを提供する必要があるときに、これらが実際のネットワークでそれぞれ異なるサーバにある場合は、同じマッピング IP アドレスを使用しながら異なるポートを使用する各サーバに対してスタティック PAT 文を指定できます（図 14-7 を参照）。

図 14-7 スタティック PAT



130031

この例について、次のコマンドを参照してください。

```
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 を使用すると、予約済みポートから標準以外のポートへの変換や、その逆の変換も可能です。たとえば、内部 Web サーバがポート 8080 を使用する場合、ポート 80 に接続することを外部ユーザに許可し、その後、変換を元のポート 8080 に戻すことができます。同様に、セキュリティをさらに高めるには、Web ユーザに標準以外のポート 6785 に接続するように指示し、その後、変換をポート 80 に戻すことができます。

## NAT 制御がイネーブルな状態での NAT のバイパス

NAT 制御をイネーブルにすると、外部ホストにアクセスする際に、内部ホストは NAT 規則と一致する必要があります。一部のホストに対して NAT が実行されないようにするには、それらのホストに対する NAT をバイパスします（または、NAT 制御をディセーブルにする方法もあります）。たとえば、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は、NAT のバイパスが必要になることがあります（NAT をサポートしない検査エンジンについては、[P.22-2 の「アプリケーション プロトコル検査を使用するタイミング」](#)を参照してください）。

次の 3 つの方法のいずれかを使用して、トラフィックが NAT をバイパスするように設定できます。どの方法でも、検査エンジンとの互換性が実現されます。ただし、それぞれの方法で提供される機能は、次のようにわずかに異なります。

- アイデンティティ NAT (**nat 0** コマンド)：アイデンティティ NAT (ダイナミック NAT と類似) を設定するときは、変換を特定のインターフェイス上のホストに限定しません。つまり、アイデンティティ NAT は、すべてのインターフェイスを通過する接続に対して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際のアドレスに対して通常の変換を実行し、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 を使用するということは選択できません。一方、標準ダイナミック NAT では、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 を適用する実際のアドレスは、アクセスリストで使用可能となっているすべてのネットワークでルーティング可能である必要があります。

アイデンティティ NAT では、マッピングアドレスは実際のアドレスと同じものになりますが、外部から内部への接続を開始することはできません（インターフェイス アクセスリストでそれが許可されている場合も同じです）。そのような機能が必要な場合は、スタティック アイデンティティ NAT または NAT 免除を使用します。

- スタティック 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 では、インターフェイスを指定して実際のアドレスの表示を許可できるため、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通常の変換を使用できます。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。ポリシー NAT では、変換対象の実際のアドレスを決定するときに、実際のアドレスと宛先アドレスが指定されます（ポリシー NAT の詳細については、[P.14-10 の「ポリシー NAT」](#)を参照してください）。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するとき、宛先がサーバ A である場合は内部アドレスに対してスタティック アイデンティティ NAT を使用し、外部サーバ B にアクセスする場合は通常の変換を使用できます。
- NAT 免除 (**nat 0 access-list** コマンド)：NAT 免除では、変換済みのホストおよびリモート ホストの両方が接続を開始できます。アイデンティティ NAT と同様に、変換を特定のインターフェイス上のホストに限定しません。すべてのインターフェイスを通過する接続に対して NAT 免除を使用する必要があります。ただし、NAT 免除では、変換対象の実際のアドレスを決定するときに実際のアドレスおよび宛先アドレスを指定できます（ポリシー NAT と類似）。したがって、NAT 免除を使用すると制御力が高くなります。しかし、ポリシー NAT とは異なり、NAT 免除では、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および宛先アドレスを指定することにより、アドレス変換対象の実際のアドレスを指定できます。オプションで、送信元ポートおよび宛先ポートを指定することもできます。標準 NAT で考慮されるのは、実際のアドレスだけです。たとえば、サーバ A にアクセスするときは実際のアドレスをマッピング アドレス A に変換し、サーバ B にアクセスするときは実際のアドレスをマッピング アドレス B に変換できます。

セカンダリ チャネルのアプリケーション検査を必要とするアプリケーション (FTP、VoIP など) に対してポリシー NAT のポートを指定すると、セキュリティ アプライアンスは自動的にセカンダリポートを変換します。

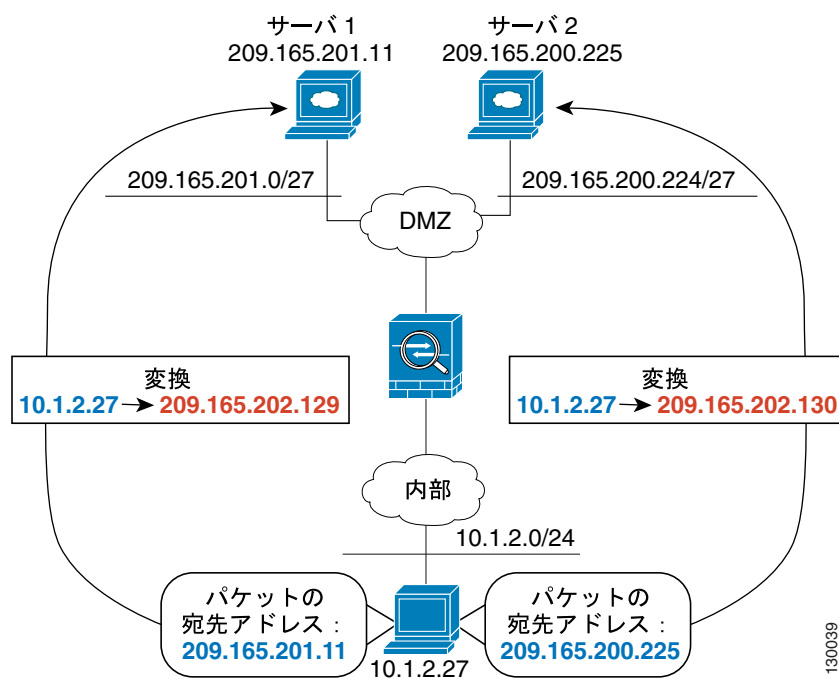


(注)

NAT 免除を除くすべてのタイプの NAT は、ポリシー NAT をサポートします。NAT 免除では、アクセスリストを使用して実際のアドレスを指定しますが、ポートが考慮されない点でポリシー NAT とは異なります。その他の相違点については、[P.14-31 の「NAT のバイパス」](#)を参照してください。ポリシー NAT をサポートするスタティック アイデンティティ NAT を使用することでも、NAT 免除と同じ結果が得られます。

図 14-8 に、2 台の異なるサーバにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129 に変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130 に変換されます。これにより、ホストはサーバと同じネットワークに存在するように見えるようになり、そのことがルーティングに役立ちます。

図 14-8 異なる宛先アドレスを使用するポリシー NAT



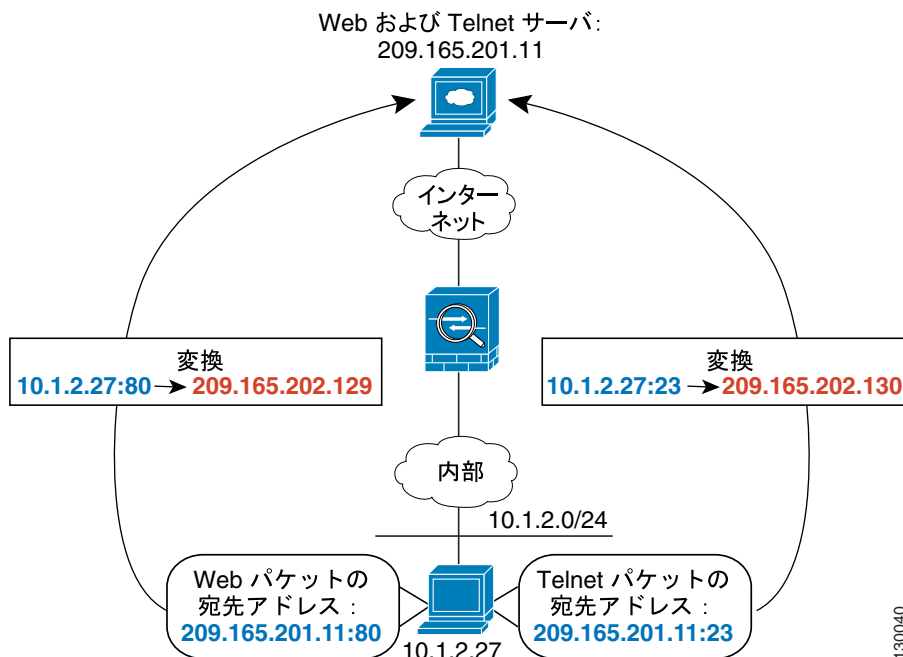


この例について、次のコマンドを参照してください。

```
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 14-9 に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Web サービスを求めてサーバにアクセスすると、実際のアドレスは 209.165.202.129 に変換されます。ホストが Telnet サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130 に変換されます。

図 14-9 異なる宛先ポートを使用するポリシー NAT



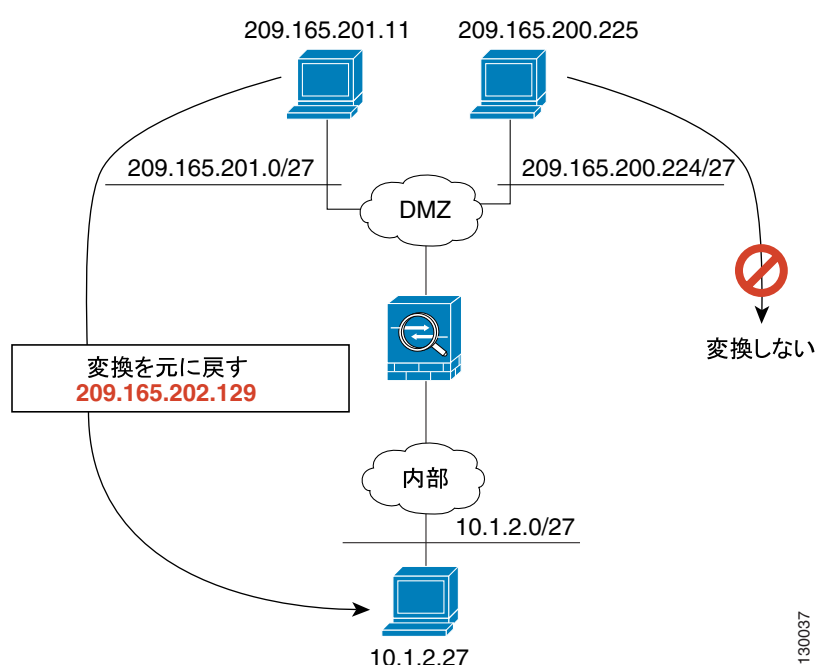
この例について、次のコマンドを参照してください。

```
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（および同じくアクセスリストを使用してトラフィックを指定する NAT 免除）では、変換済みのホストおよびリモート ホストの両方がトラフィックを発信できます。変換済みのネットワークで発信されたトラフィックについては、NAT アクセスリストで実際のアドレスと宛先アドレスが指定されますが、リモート ネットワークで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することを許可されたリモート ホストの実際のアドレスと送信元アドレスがアクセスリストで指定されます。

図 14-10 に、変換済みのホストに接続するリモート ホストを示します。変換済みのホストには、209.165.201.0/27 ネットワークが起点または終点となるトラフィックに限り実際のアドレスを変換するポリシー スタティック NAT 変換があります。209.165.200.224/27 ネットワーク用の変換は存在しません。したがって、変換済みのホストはそのネットワークに接続できず、そのネットワークのホストも変換済みのホストに接続できません。

図 14-10 宛先アドレス変換があるポリシー スタティック NAT



この例について、次のコマンドを参照してください。

```
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 はサポートしています。他のプロトコルに対する NAT サポートについては、P.22-2 の「アプリケーション プロトコル検査を使用する タイミング」を参照してください。



## NAT および同じセキュリティ レベルのインターフェイス

同じセキュリティ レベルのインターフェイス間では、NAT 制御をイネーブルにしている場合であっても、NAT は必要とされません。必要であれば、オプションで NAT を設定できます。ただし、NAT 制御がイネーブルの場合にダイナミック NAT を設定すると、NAT が必要になります。詳細については、[P.14-3 の「NAT 制御」](#)を参照してください。また、同じセキュリティ レベルのインターフェイスのダイナミック NAT または PAT に対して IP アドレスのグループを指定した場合は、それらのアドレスがセキュリティ レベルの低い（または同じ）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（NAT 制御がイネーブルになっていない場合も同じです）。スタティック NAT に対して指定されているトラフィックは影響を受けません。

同じセキュリティ レベルの通信をイネーブルにするには、[P.6-7 の「同一セキュリティ レベルにあるインターフェイス間の通信の許可」](#)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に NAT を設定すると、セキュリティ アプライアンスは VoIP 検査エンジンをサポートしなくなります。このような検査エンジンには、Skinny、SIP、H.323 などがあります。サポートされる検査エンジンについては、[P.22-2 の「アプリケーション プロトコル検査を使用するタイミング」](#)を参照してください。

## 実際のアドレスとの照合に使用される NAT コマンドの順序

セキュリティ アプライアンスは、実際のアドレスと NAT コマンドを次の順序で照合します。

1. NAT 免除 (**nat 0 access-list**) : 順序に従って、最初の一致が見つかるまで続行されます。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 のカテゴリに属します。NAT 免除文でのアドレスの重複はお勧めしません。予期しない結果が発生する可能性があります。
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**) : 順序に従って、最初の一致が見つかるまで続行されます。スタティック アイデンティティ NAT は、このカテゴリに属します。
3. ポリシー ダイナミック NAT (**nat access-list**) : 順序に従って、最初の一致が見つかるまで続行されます。アドレスの重複は許容されます。
4. 標準ダイナミック NAT (**nat**) : 最も適合するものを検出します。標準アイデンティティ NAT は、このカテゴリに属します。NAT コマンドの順序は無関係です。実際のアドレスと最も適合する NAT 文が使用されます。たとえば、インターフェイスですべてのアドレス (0.0.0.0) を変換する汎用文を作成できます。ネットワークのサブネット (10.1.1.1) を別のアドレスに変換する場合は、10.1.1.1 だけを変換する文を作成できます。10.1.1.1 が接続を開始すると、10.1.1.1 用の特定の文が使用されます。これは、その文が実際のアドレスに最も適合するからです。重複する文を使用することはお勧めしません。重複する文により、より多くのメモリが使用され、セキュリティ アプライアンスのパフォーマンスが低下する可能性があります。

## マッピング アドレスに関するガイドライン

実際のアドレスをマッピング アドレスに変換するときは、次のマッピング アドレスを使用できます。

- マッピング インターフェイスと同じネットワーク上のアドレス

マッピング インターフェイス（トラフィックがセキュリティ アプライアンスから出るときに通過するインターフェイス）と同じネットワーク上のアドレスを使用した場合、セキュリティ アプライアンスはプロキシ ARP を使用してすべてのマッピング アドレス要求に応答することにより、実際のアドレスに向かうトラフィックを代行受信します。この方法では、セキュリティ アプライアンスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。ただし、この方法では、変換に使用できるアドレス数に限度があります。

PAT では、マッピング インターフェイスの IP アドレスも使用できます。

- 一意のネットワーク上のアドレス

マッピング インターフェイスで使用可能なアドレスより多くのアドレスが必要な場合は、別のサブネット上のアドレスを指定できます。セキュリティ アプライアンスはプロキシ ARP を使用してすべてのマッピング アドレス要求に応答することにより、実際のアドレスを宛先とするトラフィックを代行受信します。OSPF を使用している場合に、マッピング インターフェイス上のルートをアドバタイズすると、セキュリティ アプライアンスはマッピング アドレスをアドバタイズします。マッピング 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場合）、またはスタティック ルーティングを使用している場合、マッピング アドレスを宛先としてトラフィックを送信するアップストリーム ルータ上のスタティック ルートをセキュリティ アプライアンスに追加する必要があります。

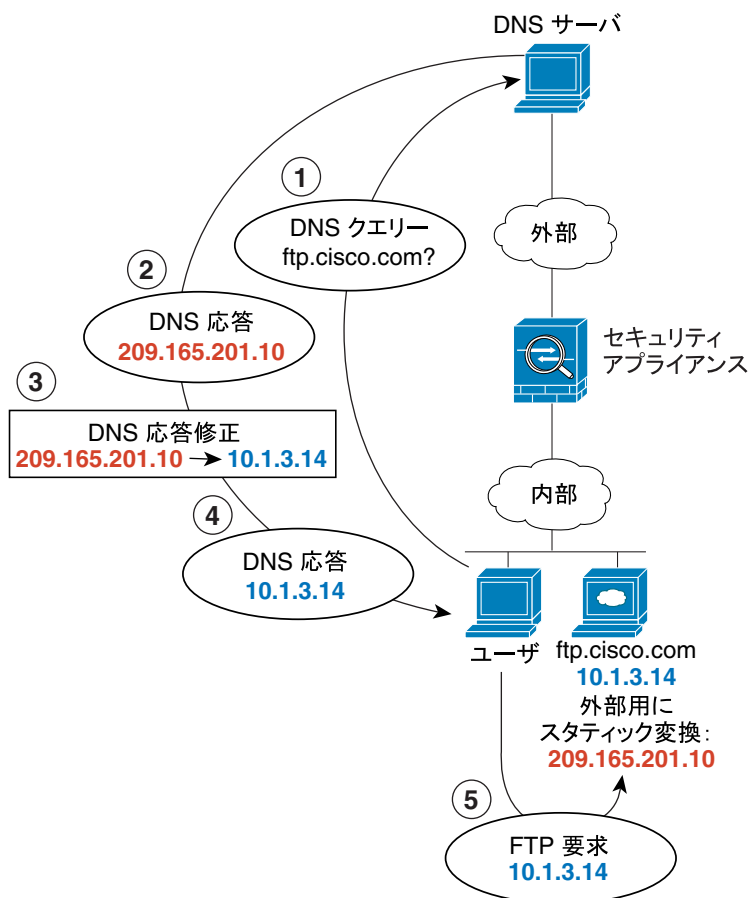
## DNS および NAT

応答内のアドレスを NAT コンフィギュレーションと一致するアドレスに置き換えて、DNS 応答を修正するようにセキュリティ アプライアンスを設定することが必要になる場合があります。DNS 修正は、各変換を設定するときに設定できます。

たとえば、DNS サーバが外部インターフェイスからアクセス可能であるとします。ftp.cisco.com というサーバが内部インターフェイス上にあります。ftp.cisco.com の実際のアドレス（10.1.3.14）を、外部ネットワーク上で可視のマッピング アドレス（209.165.201.10）にスタティックに変換するように、セキュリティ アプライアンスを設定します（図 14-11 を参照）。この場合、このスタティック文で DNS 応答修正をイネーブルにする必要があります。これにより、実際のアドレスを使用して ftp.cisco.com にアクセスすることを許可されている内部ユーザは、マッピング アドレスではなく実際のアドレスを DNS サーバから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバは応答でマッピング アドレス（209.165.201.10）を示します。セキュリティ アプライアンスは、内部サーバのスタティック文を参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正をイネーブルにしない場合、内部ホストは ftp.cisco.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することを試みます。

図 14-11 DNS 応答修正



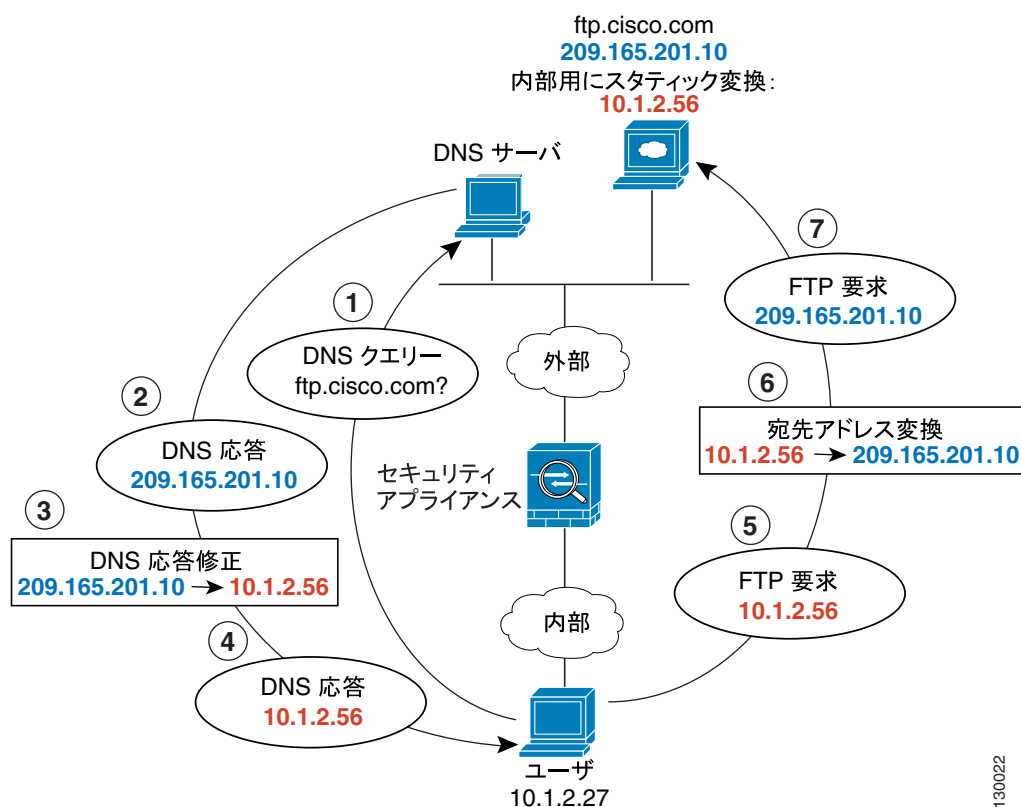
130021

この例について、次のコマンドを参照してください。

```
hostname(config)# static (inside,outside) 209.165.201.10 10.1.3.14 netmask
255.255.255.255 dns
```

図 14-12 に、外部の Web サーバと DNS サーバを示します。セキュリティ アプライアンスには、外部サーバ用のスタティック変換があります。この場合、ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答で実際のアドレス 209.165.20.10 を示します。ftp.cisco.com のマッピングアドレス (10.1.2.56) が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。

図 14-12 外部 NAT を使用する DNS 応答修正



この例について、次のコマンドを参照してください。

```
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 制御は、内部インターフェイスから外部インターフェイスに移動するパケットが NAT 規則に一致することを要求します。詳細については、[P.14-3](#) の「[NAT 制御](#)」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

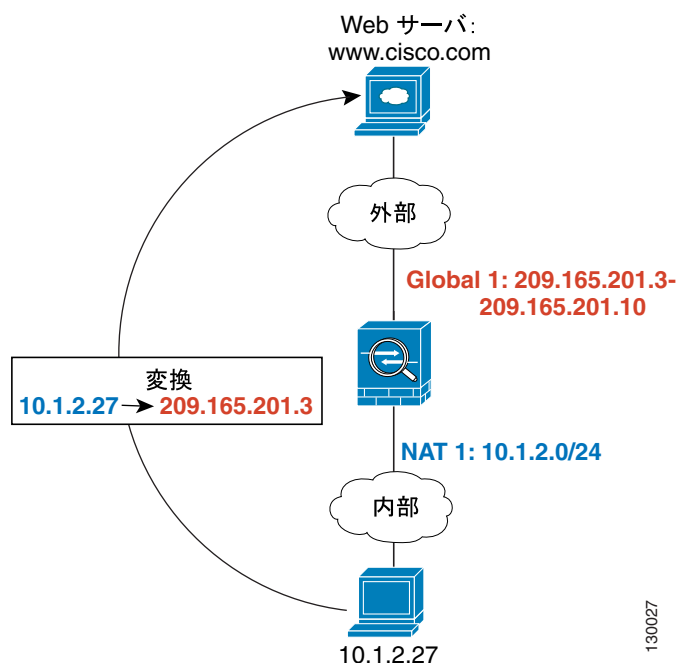
この項では、ダイナミック NAT および PAT を設定する方法について説明します。次の項目を取り上げます。

- [ダイナミック NAT および PAT の実装 \(P.14-17\)](#)
- [ダイナミック NAT または PAT の設定 \(P.14-23\)](#)

### 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 を実装するには、まず特定のインターフェイス上の変換対象の実際のアドレスを指定する **nat** コマンドを設定します。次に、別の **global** コマンドを設定して、別のインターフェイスを出るときのマッピング アドレスを指定します（PAT の場合、これは 1 つのアドレスです）。各 **nat** コマンドは、各コマンドに割り当てた番号である NAT ID を比較することにより、**global** コマンドと照合されます（[図 14-13](#) を参照）。

図 14-13 nat と global の ID 照合

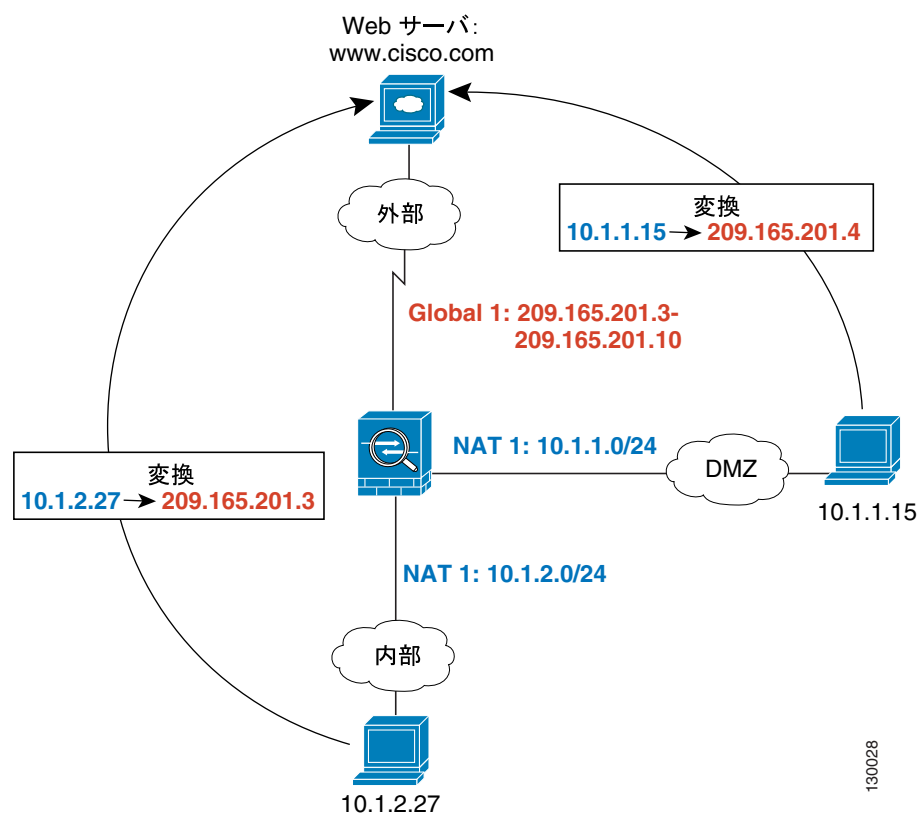


この例について、次のコマンドを参照してください。

```
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 を使用する各インターフェイスに対して、**nat** コマンドを入力できます。これらのインターフェイスはすべて、特定のインターフェイスを出るときに同じ **global** コマンドを使用します。たとえば、どちらも NAT ID 1 である内部インターフェイスおよび DMZ インターフェイスに **nat** コマンドを設定できます。次に、同じく ID 1 の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および 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、マッピングされたプールまたは PAT アドレスを共有します（[図 14-14](#) を参照）。

図 14-14 複数のインターフェイスに対する nat コマンド

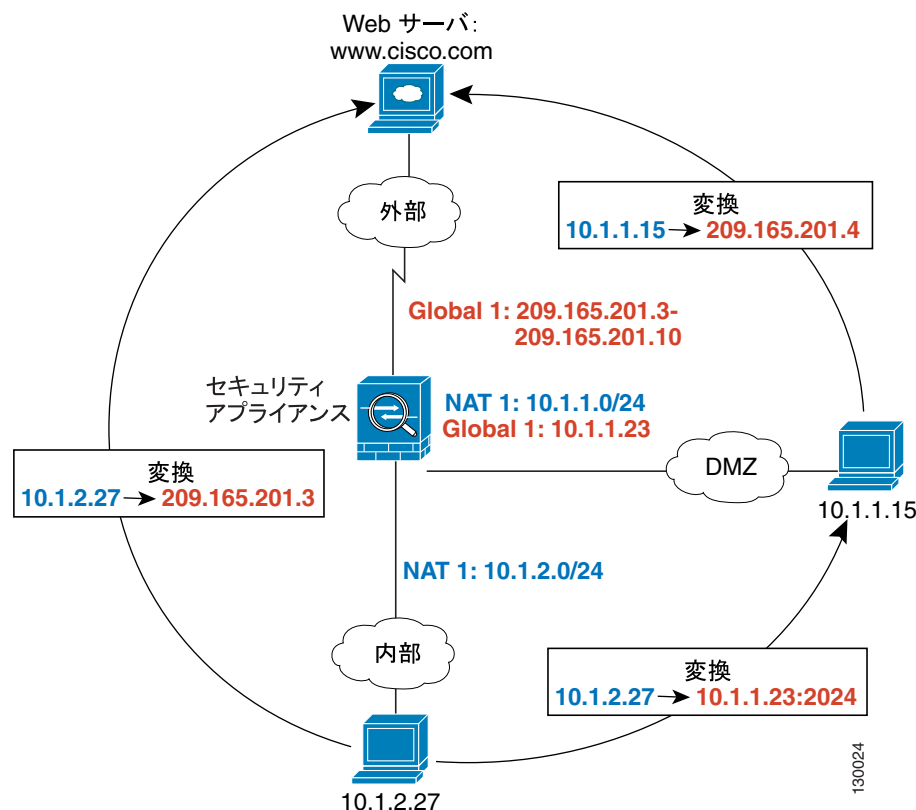


この例について、次のコマンドを参照してください。

```
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
```

また、同じ NAT ID を使用する各インターフェイスに対して **global** コマンドを入力することもできます。ID 1 の外部インターフェイスおよび DMZ インターフェイスに対して **global** コマンドを入力すると、内部 **nat** コマンドは、トラフィックが外部インターフェイスに向かうときも DMZ インターフェイスに向かうときも、変換済みのトラフィックを指定します。同様に、ID 1 の DMZ インターフェイスに対して **nat** コマンドも入力すると、外部インターフェイスに対する **global** コマンドが DMZ トラフィックにも使用されます (図 14-15 を参照)。

図 14-15 複数のインターフェイスに対する global コマンドと nat コマンド

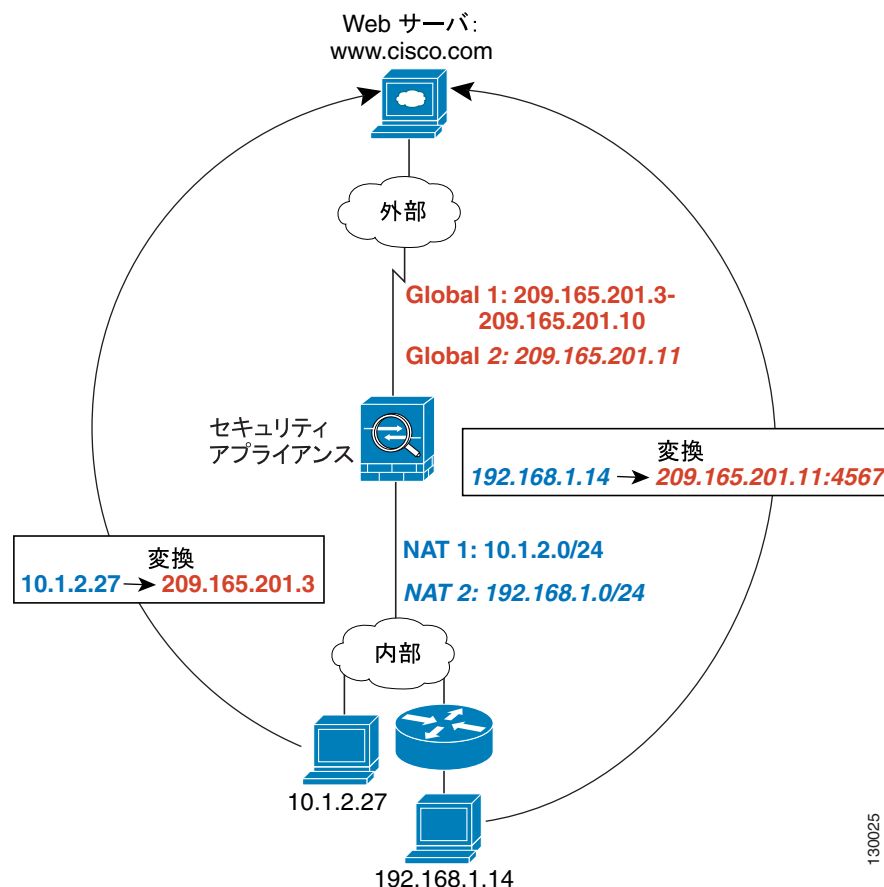


この例について、次のコマンドを参照してください。

```
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
```

異なる NAT ID を使用すると、実際のアドレスの集合を指定して、それぞれが異なるマッピングアドレスを持つようにできます。たとえば、内部インターフェイス上で、異なる 2 つの NAT ID に対して 2 つの **nat** コマンドを設定できます。外部インターフェイス上で、これら 2 つの ID に対して 2 つの **global** コマンドを設定できます。その場合、内部ネットワーク A からのトラフィックが外部インターフェイスを出ると、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 からのトラフィックは、プール B のアドレスに変換されます (図 14-16 を参照)。ポリシー NAT を使用した場合は、宛先のアドレスとポートが各アクセスリスト内で一意であれば、複数の **nat** コマンドに対して同じ実際のアドレスを指定できます。

図 14-16 異なる NAT ID



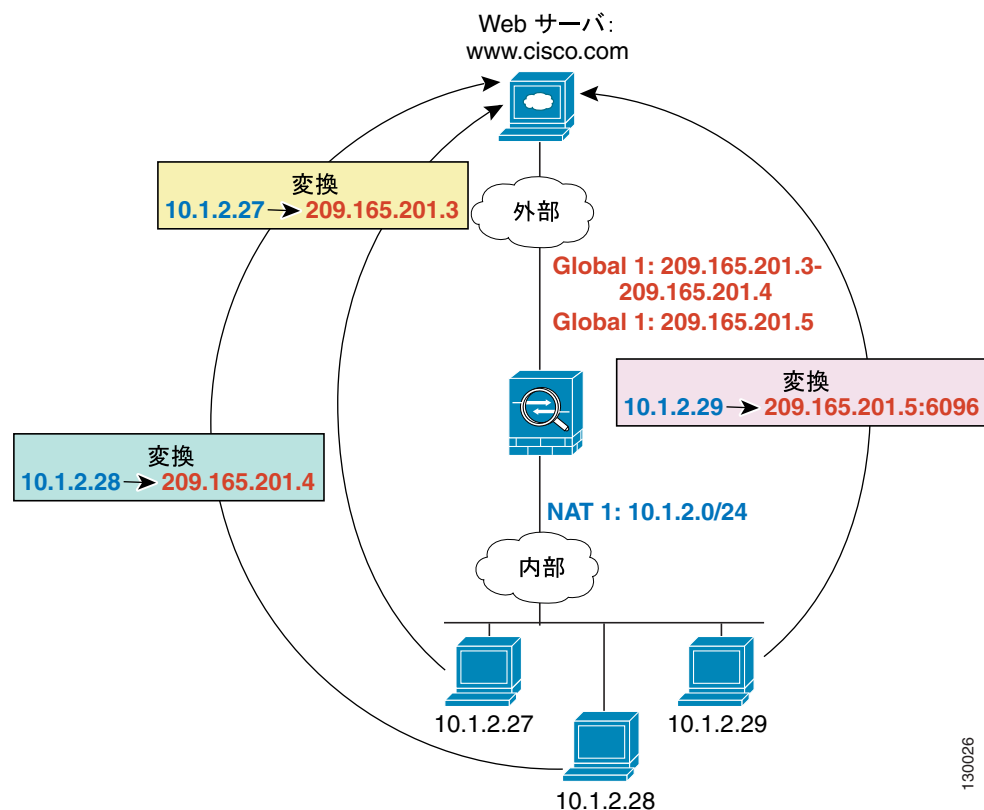
この例について、次のコマンドを参照してください。

```
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対して複数の **global** コマンドを入力できます。セキュリティ アプライアンスは最初にダイナミック NAT **global** コマンドをコンフィギュレーション内の順序で使用し、次に PAT **global** コマンドを順序どおりに使用します。特定のアプリケーションに対してダイナミック NAT を使用する必要があると同時に、ダイナミック NAT アドレスが不足したときに備えてバックアップ PAT 文を用意しておく必要がある場合、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できます。同様に、1 つの PAT がマッピングされた文がサポートする約 64,000 回の PAT セッションより多くのセッションが必要な場合、2 つの PAT 文を入力できます (図 14-17 を参照)。



図 14-17 NAT と PAT の併用

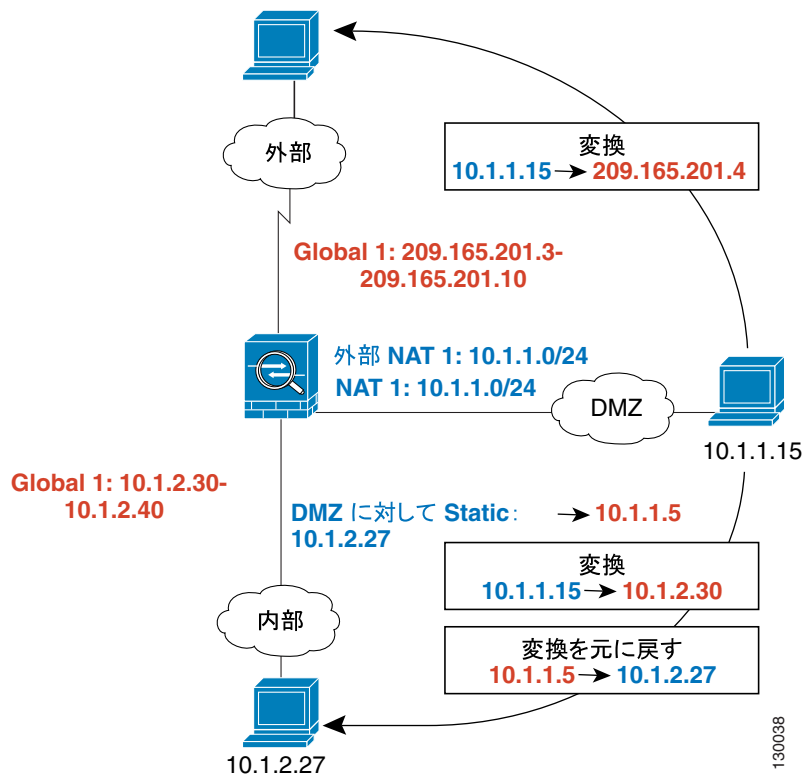


この例について、次のコマンドを参照してください。

```
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 については、外部 NAT 用の **nat** コマンド (**outside** キーワード) を指定する必要があります。内部インターフェイスにアクセスするときにも同じトラフィックを変換する場合（たとえば、DMZ 上のトラフィックを、内部インターフェイスと外部インターフェイスにアクセスするときに変換する場合）は、**outside** オプションなしで別の **nat** コマンドを設定する必要があります。この場合、両方の文で同じアドレスを指定し、同じ NAT ID を使用できます（図 14-18 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へ）では、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します。したがって、送信元アドレスと宛先アドレスの両方が変換されます。

図 14-18 外部 NAT と内部 NAT の併用



この例について、次のコマンドを参照してください。

```
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 アドレスのグループを指定した場合は、そのアドレス グループがセキュリティ レベルの低いまたは同じインターフェイスにアクセスするときに、NAT を実行する必要があります。各インターフェイスに対して同じ NAT ID を使用して **global** コマンドを適用するか、**static** コマンドを使用する必要があります。このグループがセキュリティ レベルの高いインターフェイスにアクセスするときは、NAT は必要とされません。外部から内部への NAT を実行するには、**outside** キーワードを使用する別の **nat** コマンドを作成する必要があるためです。外部 NAT を適用しない場合、このアドレス グループがセキュリティ レベルの高いインターフェイスにアクセスするときは、上記の 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** コマンドで指定されている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

この項では、ダイナミック NAT またはダイナミック PAT を設定する方法について説明します。ダイナミック NAT とダイナミック PAT のコンフィギュレーションはほぼ同じです。NAT の場合はマッピングアドレスの範囲を指定し、PAT の場合は 1 つのアドレスを指定する点だけが異なります。

図 14-19 に、一般的なダイナミック NAT のシナリオを示します。変換済みのホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。マッピングアドレスは、**global** コマンドで定義されたプールからダイナミックに割り当てられます。

図 14-19 ダイナミック NAT

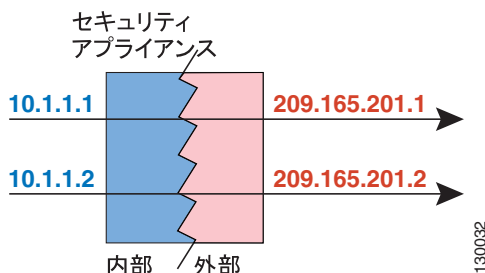
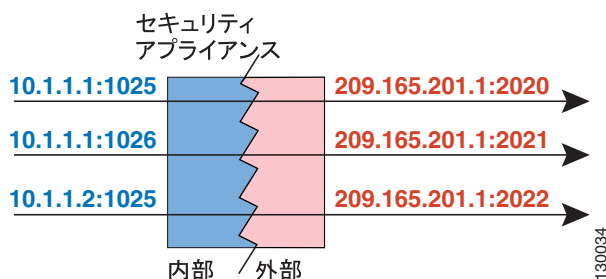


図 14-20 に、一般的なダイナミック PAT のシナリオを示します。変換済みのホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。**global** コマンドで定義されたマッピングアドレスはどの変換でも同じですが、ポートがダイナミックに割り当てられます。

図 14-20 ダイナミック PAT



ダイナミック NAT の詳細については、P.14-5 の「ダイナミック NAT」を参照してください。PAT の詳細については、P.14-7 の「PAT」を参照してください。



(注)

NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待機せずに新しい 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できます。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

ダイナミック NAT またはダイナミック PAT を設定するには、次の手順を実行します。

### ステップ 1 次のコマンドのいずれかを入力して、変換する実際の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]
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

他の **nat** コマンドで重複アドレスを指定できます。たとえば、1 つのコマンドで 10.1.1.0 を指定しても、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序どおりにポリシー NAT コマンドと照合されます。または、標準 NAT の場合は、最も適合するものが使用されます。

このコマンドのオプションについては、次の説明を参照してください。

- **access-list acl\_name** : 拡張アクセスリストを使用して、実際の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 (P.13-6 の「[拡張アクセスリストの追加](#)」を参照)。このアクセスリストには、許可 ACE のみを含めます。**eq** 演算子を使用して、アクセスリストに実際のポートおよび宛先ポートをオプションで指定できます。ポリシー NAT は、**inactive** および **time-range** キーワードを考慮しません。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見なされます。
- **nat\_id** : 1 ~ 65535 の整数。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、P.14-17 の「[ダイナミック NAT および PAT の実装](#)」を参照してください。**0** は、NAT 免除用に予約されています (NAT 免除の詳細については、P.14-33 の「[NAT 免除の設定](#)」を参照してください)。
- **dns** : **nat** コマンドに、DNS サーバ内にエントリを持つホストのアドレスが含まれており、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバでホストのアドレスが異なっている必要があります。一方にはマッピングアドレスが、もう一方には実際のアドレスが必要です。このオプションにより、クライアントに対する DNS 応答内でアドレスが書き換えられます。変換済みのホストは、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ある必要があります。一般に、他のインターフェイスからのアクセスを許可する必要があるホストはスタティック変換を使用するため、このオプションは多くの場合、**static** コマンドで使用されます (詳細については、P.14-14 の「[DNS および NAT](#)」を参照してください)。
- **outside** : このインターフェイスのセキュリティ レベルが、一致する **global** 文で指定したインターフェイスのセキュリティ レベルより低い場合、**outside** を入力して 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。
- **norandomseq**、**tcp tcp\_max\_conns**、**udp udp\_max\_conns**、および **emb\_limit** : これらのキーワードは、接続制限値を設定します。ただし、接続制限値の設定には、より汎用的な方法を使用することをお勧めします。P.20-5 の「[接続の制限値とタイムアウトの設定](#)」を参照してください。

- 標準 NAT :

```
hostname(config)# nat (real_interface) nat_id real_ip [mask [dns] [outside]
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

**nat\_id** は、1 ~ 2147483647 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、P.14-17 の「[ダイナミック NAT および PAT の実装](#)」を参照してください。**0** はアイデンティティ NAT 用に予約されています。アイデンティティ NAT の詳細については、P.14-31 の「[アイデンティティ NAT の設定](#)」を参照してください。

その他のオプションについては、上記のポリシー 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を出るときに実際のアドレスから変換するマッピングアドレスを指定します。

```
hostname(config)# global (mapped_interface) nat_id {mapped_ip[-mapped_ip] | interface}
```

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。一致した **nat** コマンドにより、このインターフェイスを出るときに変換するアドレスが指定されます。

1 つのアドレス（PAT の場合）またはアドレスの範囲（NAT の場合）を指定できます。必要であれば、サブネットの境界を横断する範囲を指定できます。たとえば、次の「スーパーネット」を指定できます。

```
192.168.1.1-192.168.2.254
```

たとえば、内部インターフェイス上の 10.1.1.0/24 ネットワークを変換するには、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) 1 209.165.201.1-209.165.201.30
```

ダイナミック NAT 用のアドレス プールを、NAT プールを使い果たしたときのための PAT アドレスとともに指定するには、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
```

ルーティングの簡略化などのために、セキュリティの低い DMZ（非武装地帯）のネットワーク アドレスを変換して内部ネットワーク（10.1.1.0）と同じネットワーク上に表示するには、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
```

ポリシー NAT を使用して、1 つの実際のアドレスに 2 つの異なる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（これに関する図については、[P.14-10 の図 14-8](#) を参照してください）。

```
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、それぞれが異なるポートを使用する、1 つの実際のアドレスと宛先アドレスのペアを指定するには、次のコマンドを入力します（これに関する図については、[P.14-11 の図 14-9](#) を参照してください）。

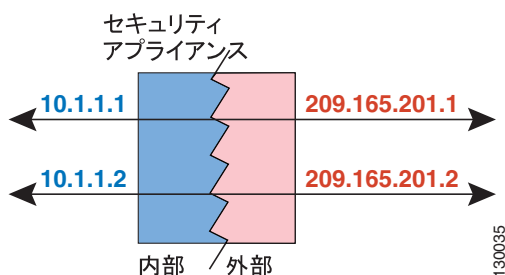
```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11  
255.255.255.255 eq 80  
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11  
255.255.255.255 eq 23  
hostname(config)# nat (inside) 1 access-list WEB  
hostname(config)# global (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

この項では、スタティック変換を設定する方法について説明します。

図 14-21 に、一般的なスタティック NAT のシナリオを示します。この変換は常にアクティブであるので、変換済みのホストとリモート ホストの両方が接続を開始でき、マッピングアドレスは **static** コマンドによってスタティックに割り当てられます。

図 14-21 スタティック NAT



同一の実際のアドレスまたはマッピング アドレスを、同一の 2 つのインターフェイス間の複数の **static** コマンドで使用することはできません。 **static** コマンドで、同じマッピング インターフェイスの **global** コマンドでも定義されているマッピング アドレスを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、P.14-8 の「スタティック NAT」を参照してください。



(注)

**static** コマンドを削除した場合、変換を使用してい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。

**clear xlate** コマンドで変換テーブルからスタティック変換を消去することはできません。 **static** コマンドを削除する必要があります。 **clear xlate** コマンドでは、**nat** コマンドおよび **global** コマンドで作成したダイナミック変換のみを削除できます。

スタティック NAT を設定するには、次のコマンドのいずれかを入力します。

- ポリシー スタティック NAT の場合は、次のコマンドを入力します。

```
hostname(config)# static (real_interface,mapped_interface) {mapped_ip | interface}
access-list acl_name [dns] [norandomseq] [[tcp] tcp_max_conns [emb_limit]]
[udp udp_max_conns]
```

**access-list** コマンドを使用して、アクセスリストを作成します (P.13-6 の「拡張アクセスリストの追加」を参照)。このアクセスリストには、許可 ACE のみを含めます。アクセスリストで使用する送信元サブネット マスクは、マッピング アドレスにも使用されます。 **eq** 演算子を使用して、アクセスリストに実際のポートおよび宛先ポートを指定することもできます。ポリシー NAT は、**inactive** および **time-range** キーワードを考慮しません。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見なされます。詳細については、P.14-10 の「ポリシー NAT」を参照してください。

変換にネットワークを指定すると (10.1.1.0 255.255.255.0 など)、セキュリティ アプライアンスは、.0 および .255 のアドレスを変換します。これらのアドレスへのアクセスを禁止するには、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、P.14-23 の「ダイナミック NAT または PAT の設定」を参照してください。

- 標準スタティック NAT 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) {mapped_ip | interface}  
real_ip [netmask mask] [dns] [norandomseq] [[tcp] tcp_max_conns [emb_limit]]  
[udp udp_max_conns]
```

オプションについては、[P.14-23](#) の「ダイナミック NAT または PAT の設定」を参照してください。

たとえば、次のポリシー スタティック NAT の例では、宛先アドレスに応じて 2 つのマッピングアドレスに変換される 1 つの実際のアドレスを示しています（これに関する図については、[P.14-10](#) の [図 14-8](#) を参照してください）。

```
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
```

次のコマンドは、内部 IP アドレス（10.1.1.3）を外部 IP アドレス（209.165.201.12）にマッピングします。

```
hostname(config)# static (inside,outside) 209.165.201.12 10.1.1.3 netmask  
255.255.255.255
```

次のコマンドは、外部アドレス（209.165.201.15）を内部アドレス（10.1.1.6）にマッピングします。

```
hostname(config)# static (outside,inside) 10.1.1.6 209.165.201.15 netmask  
255.255.255.255
```

次のコマンドは、サブネット全体をスタティックにマッピングします。

```
hostname(config)# static (inside,dmz) 10.1.1.0 10.1.2.0 netmask 255.255.255.0
```

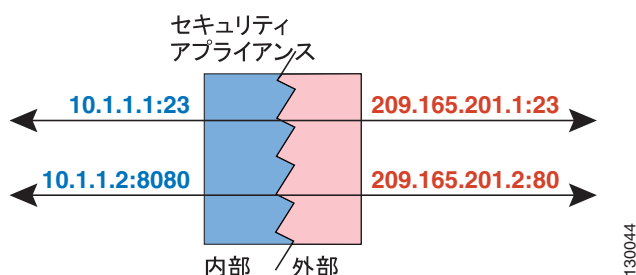


## スタティック PAT の使用

この項では、スタティック ポート変換を設定する方法について説明します。スタティック PAT を使用すると、実際の IP アドレスをマッピング IP アドレスに変換するとともに、実際のポートをマッピングポートに変換できます。実際のポートを同じポートに変換することを選択できます。これにより、特定のタイプのトラフィックだけを変換できます。また、さらに別のポートに変換することもできます。

図 14-22 に、一般的なスタティック PAT のシナリオを示します。この変換は常にアクティブであるため、変換済みのホストとリモート ホストの両方が接続を開始でき、マッピングアドレスとポートは **static** コマンドによってスタティックに割り当てられます。

図 14-22 スタティック PAT



セカンダリ チャネルのアプリケーション検査が必要なアプリケーション（FTP、VoIP など）を使用する場合は、セキュリティ アプライアンスが自動的にセカンダリ ポートを変換します。

同一の実際のアドレスまたはマッピングアドレスを、同一の 2 つのインターフェイス間の複数の **static** 文で使用することはできません。 **static** コマンドで、同じマッピング インターフェイスの **global** コマンドでも定義されているマッピングアドレスを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、P.14-8 の「スタティック PAT」を参照してください。



(注)

**static** コマンドを削除した場合、変換を使用してい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。

**clear xlate** コマンドで変換テーブルからスタティック変換を消去することはできません。**static** コマンドを削除する必要があります。**clear xlate** コマンドでは、**nat** コマンドおよび **global** コマンドで作成したダイナミック変換のみを削除できます。

スタティック PAT を設定するには、次のコマンドのいずれかを入力します。

- ポリシー スタティック PAT の場合は、次のコマンドを入力します。

```
hostname(config)# static (real_interface,mapped_interface) {tcp | udp}
{mapped_ip | interface} mapped_port access-list acl_name [dns] [norandomseq]
[[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```



**access-list** コマンドを使用して、アクセスリストを作成します (P.13-6 の「[拡張アクセスリストの追加](#)」を参照)。アクセスリストのプロトコルは、このコマンドで設定したプロトコルと一致する必要があります。たとえば、**static** コマンドで **tcp** を指定した場合は、アクセスリストで **tcp** を指定する必要があります。**eq** 演算子を使用してポートを指定します。このアクセスリストには、**許可** ACE のみを含めます。アクセスリストで使用する送信元サブネット マスクは、マッピング アドレスにも使用されます。ポリシー NAT は、**inactive** および **time-range** キーワードを考慮しません。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見なされます。

変換にネットワークを指定すると (10.1.1.0 255.255.255.0 など)、セキュリティ アプライアンスは、.0 および .255 のアドレスを変換します。これらのアドレスへのアクセスを禁止するには、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、P.14-23 の「[ダイナミック NAT または PAT の設定](#)」を参照してください。

- スタティック PAT 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) {tcp | udp} {mapped_ip |  
interface} mapped_port real_ip real_port [netmask mask] [dns] [norandomseq] [[tcp]  
tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

オプションについては、P.14-23 の「[ダイナミック NAT または PAT の設定](#)」を参照してください。

たとえば、10.1.3.0 ネットワークのホストから開始された、セキュリティ アプライアンス外部インターフェイス (10.1.2.14) に向かう Telnet トラフィックを、内部ホスト 10.1.1.15 にリダイレクトできます。これには、次のコマンドを入力します。

```
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
```

10.1.3.0 ネットワークのホストから開始された、セキュリティ アプライアンス外部インターフェイス (10.1.2.14) に向かう HTTP トラフィックを、内部ホスト 10.1.1.15 にリダイレクトできます。これには、次のコマンドを入力します。

```
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
```

Telnet トラフィックをセキュリティ アプライアンス外部インターフェイス (10.1.2.14) から内部ホスト 10.1.1.15 にリダイレクトするには、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet  
netmask 255.255.255.255
```

ただし、上記の実際の Telnet サーバが接続を開始することを許可する場合は、変換を追加で指定する必要があります。たとえば、その他のタイプのトラフィックをすべて変換するには、次のコマンドを入力します。元の **static** コマンドでは、サーバに Telnet 用の変換が指定され、**nat** コマンドおよび **global** コマンドでは、サーバからの発信接続用の PAT が指定されます。

```
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
```

すべての内部トラフィック用の別個の変換も設定していて、内部ホストが Telnet サーバと異なるマッピングアドレスを使用する場合でも、サーバへの Telnet トラフィックを許可する **static** 文と同じマッピングアドレスが使用されるように、Telnet サーバから開始されるトラフィックを設定できます。Telnet サーバ専用により限定的な **nat** 文を作成する必要があります。**nat** 文の読み取りでは、最も適合するものが求められるため、より限定的な **nat** 文が一般的な文より先に一致します。次の例は、Telnet サーバから開始されたトラフィック用のより限定的な **nat** 文である Telnet **static** 文を示しています。また、その他の内部ホスト用の文も示しています。後者の文では、異なるマッピングアドレスが使用されています。

```
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
```

予約済みポート（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

この項では、NAT をバイパスする方法について説明します。NAT 制御がイネーブルのときに NAT をバイパスしなければならない場合があります。NAT は、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 免除を使用することでバイパスできます。これらの方法の詳細については、P.14-9 の「NAT 制御がイネーブルな状態での NAT のバイパス」を参照してください。ここでは、次の項目について説明します。

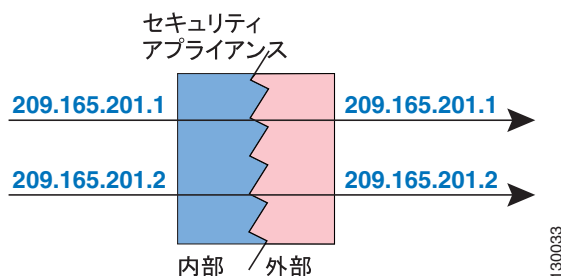
- アイデンティティ NAT の設定 (P.14-31)
- スタティック アイデンティティ NAT の設定 (P.14-32)
- NAT 免除の設定 (P.14-33)

### アイデンティティ NAT の設定

アイデンティティ NAT では、実際の IP アドレスが同じ IP アドレスに変換されます。「変換済み」のホストだけが NAT 変換を作成でき、応答トラフィックが許可されます。

図 14-23 に、一般的なアイデンティティ NAT のシナリオを示します。

図 14-23 NAT の識別



(注)

NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待機せずに新しい 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できます。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

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] [norandomseq]
[[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

オプションについては、P.14-23 の「ダイナミック NAT または PAT の設定」を参照してください。

たとえば、内部 10.1.1.0/24 ネットワークに対してアイデンティティ NAT を使用するには、次のコマンドを使用します。

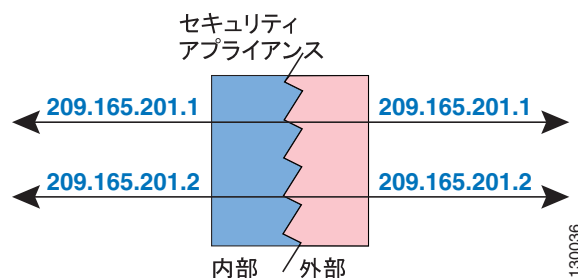
```
hostname(config)# nat (inside) 0 10.1.1.0 255.255.255.0
```

## 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、実際の IP アドレスが同じ IP アドレスに変換されます。この変換は常にアクティブであるため、「変換済み」のホストとリモート ホストの両方が接続を開始できます。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 では、変換する実際のアドレスを決定するときに、実際のアドレスと宛先アドレスを指定できます（ポリシー NAT の詳細については、[P.14-10 の「ポリシー NAT」](#)を参照してください）。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する際に、宛先がサーバ A である場合は内部アドレスに対してポリシー 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 にアクセスする場合は通常の変換を使用できます。

図 14-24 に、一般的なスタティック アイデンティティ NAT のシナリオを示します。

図 14-24 スタティック アイデンティティ NAT



(注)

**static** コマンドを削除した場合、変換を使用してい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。

**clear xlate** コマンドで変換テーブルからスタティック変換を消去することはできません。**static** コマンドを削除する必要があります。**clear xlate** コマンドでは、**nat** コマンドおよび **global** コマンドで作成したダイナミック変換のみを削除できます。

スタティック アイデンティティ NAT を設定するには、次のコマンドのいずれかを入力します。

- ポリシー スタティック アイデンティティ NAT を設定するには、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] [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

**access-list** コマンドを使用して、アクセスリストを作成します（[P.13-6 の「拡張アクセスリストの追加」](#)を参照）。このアクセスリストには、許可 ACE のみを含めます。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** と一致することを確認します。ポリシー NAT は、**inactive** および **time-range** キーワードを考慮しません。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見なされます。詳細については、[P.14-10 の「ポリシー NAT」](#)を参照してください。

その他のオプションについては、[P.14-23 の「ダイナミック NAT または PAT の設定」](#)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] [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

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、P.14-23 の「[ダイナミック NAT または PAT の設定](#)」を参照してください。

たとえば、次のコマンドでは、外部からのアクセスがあった場合に、内部 IP アドレス（10.1.1.3）に対してスタティック アイデンティティ NAT が使用されます。

```
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、内部からのアクセスがあった場合に、外部アドレス（209.165.201.15）に対してスタティック アイデンティティ NAT が使用されます。

```
hostname(config)# static (outside,inside) 209.165.201.15 209.165.201.15 netmask 255.255.255.255
```

次のコマンドは、サブネット全体をスタティックにマッピングします。

```
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 の例は、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何らかの変換を使用する 1 つの実際のアドレスを示しています。

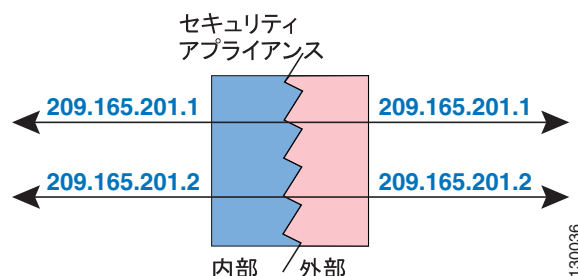
```
hostname(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0 255.255.255.224
hostname(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224 255.255.255.224
hostname(config)# static (inside,outside) 10.1.2.27 access-list NET1
hostname(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

## NAT 免除の設定

NAT 免除を使用すると、アドレスは変換を免除され、実際のホストとリモート ホストの両方が接続を開始できるようになります。NAT 免除では、免除する実際のトラフィックを決定するときに、実際のアドレスと宛先アドレスを指定できます（ポリシー NAT と類似）。そのため、NAT 免除では、アイデンティティ NAT を使用した場合よりも制御力が高くなります。ただし、ポリシー NAT と異なり、NAT 免除は、アクセスリストの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場合は、スタティック アイデンティティ NAT を使用してください。

図 14-25 に、一般的な NAT 免除のシナリオを示します。

図 14-25 NAT 免除



(注)

NAT 免除コンフィギュレーションを削除しても、NAT 免除を使用してい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 免除を設定するには、次のコマンドを入力します。

```
hostname(config)# nat (real_interface) 0 access-list acl_name [outside] [norandomseq]
[[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

**access-list** コマンドを使用して、アクセスリストを作成します (P.13-6 の「[拡張アクセスリストの追加](#)」を参照)。このアクセスリストには、**許可** ACE と **拒否** ACE の両方を含めることができます。このアクセスリストでは、実際のポートおよび宛先ポートを指定しないでください。NAT 免除はポートを考慮しません。NAT 免除は、**inactive** および **time-range** キーワードを考慮しません。すべての ACE が、NAT 免除コンフィギュレーションに対してアクティブであると見なされます。

その他のオプションについては、P.14-23 の「[ダイナミック NAT または PAT の設定](#)」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免除します。外部から内部へのトラフィックが NAT をバイパスするようにするには、別の **nat** コマンドを追加し、**outside** を入力して NAT インスタンスを外部 NAT として指定します。外部インターフェイスに対してダイナミック NAT を設定している場合に、他のトラフィックを免除するときは、外部 NAT 免除を使用できます。

たとえば、任意の宛先アドレスにアクセスするとき、内部ネットワークに対して免除するには、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
```

ある DMZ ネットワークに対してダイナミック外部 NAT を使用し、別の DMZ ネットワークに対して免除するには、次のコマンドを使用します。

```
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、内部アドレスに対して免除するには、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

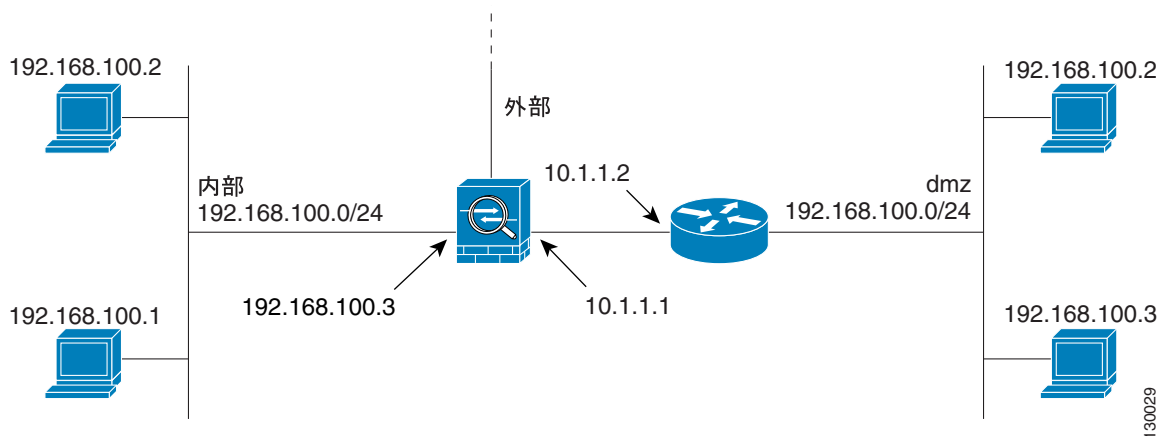
この項では、NAT 解決を使用する一般的なシナリオについて説明します。次の項目について取り上げます。

- アドレスが重複するネットワーク (P.14-35)
- ポートのリダイレクト (P.14-37)

### アドレスが重複するネットワーク

図 14-26 のセキュリティ アプライアンスには、アドレス範囲が重複する 2 つのプライベート ネットワークが接続されています。

図 14-26 アドレスが重複するネットワークでの外部 NAT の使用



2 つのネットワークで、重複するアドレス空間 (192.168.100.0/24) が使用されていますが、各ネットワークのホストは (アクセスリストの許可に従って) 通信する必要があります。NAT がない場合、アドレスが重複する DMZ ネットワークのホストに内部ネットワークのホストがアクセスしようとしても、パケットはセキュリティ アプライアンスを通過できません。セキュリティ アプライアンスはこのパケットを、内部ネットワークの宛先アドレスが含まれているものと見なします。さらに、内部ネットワークの別のホストでこの宛先アドレスが使用されている場合、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指定します。両方の方向でアクセスを許可する場合は、両方のネットワークに対してスタティック NAT を使用します。内部インターフェイスだけに DMZ のホストへのアクセスを許可する場合は、内部アドレスに対してダイナミック NAT を使用し、アクセス先の DMZ アドレスに対してスタティック NAT を使用します。次の例は、スタティック NAT の場合を示しています。

これら 2 つのインターフェイスに対してスタティック NAT を設定するには、次の手順を実行します。DMZ の 10.1.1.0/24 ネットワークは変換されません。

- ステップ 1** 次のコマンドを入力して、DMZ にアクセスする内部の 192.168.100.0/24 を 10.1.2.0 /24 に変換します。

```
hostname(config)# static (inside,dmz) 10.1.2.0 192.168.100.0 netmask 255.255.255.0
```

- ステップ 2** 次のコマンドを入力して、内部にアクセスする DMZ の 192.168.100.0/24 ネットワークを 10.1.3.0/24 に変換します。

```
hostname(config)# static (dmz,inside) 10.1.3.0 192.168.100.0 netmask 255.255.255.0
```

- ステップ 3** DMZ ネットワークへのトラフィックがセキュリティ アプライアンスによって正しくルーティングされるように、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
```

セキュリティ アプライアンスには、内部ネットワーク用に接続されたルートがすでに存在します。これらのスタティック ルートを使用することで、セキュリティ アプライアンスは 192.168.100.0/24 ネットワークへのトラフィックを DMZ インターフェイスからゲートウェイ ルータ 10.1.1.2 に発信できます(接続されたルートとまったく同じネットワークを持つスタティック ルートを作成することはできないため、ネットワークを 2 つに分割する必要があります)。または、デフォルト ルートなど、より広範囲のルートを DMZ トラフィック用に使用することもできます。

DMZ ネットワークのホスト 192.168.100.2 が内部ネットワークのホスト 192.168.100.2 への接続を開始しようとする、次のイベントが発生します。

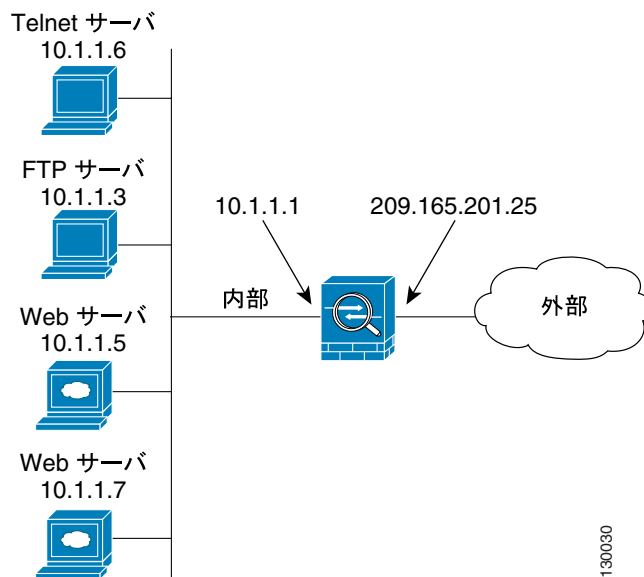
1. DMZ ホスト 192.168.100.2 が IP アドレス 10.1.2.2 にパケットを送信します。
2. セキュリティ アプライアンスがこのパケットを受信すると、セキュリティ アプライアンスは送信元アドレスを 192.168.100.2 から 10.1.3.2 に変換します。
3. 次に、セキュリティ アプライアンスは宛先アドレスを 10.1.2.2 から 192.168.100.2 に変換し、パケットを転送します。



## ポートのリダイレクト

図 14-27 に、ポート リダイレクション機能が効果的であるネットワークの代表例を示します。

図 14-27 スタティック PAT を使用するポート リダイレクション



この項で説明する構成では、ポート リダイレクションは、次のように外部ネットワーク上のホストに対して実行されます。

- IP アドレス 209.165.201.5 に対する Telnet 要求が、10.1.1.6 にリダイレクトされる。
- IP アドレス 209.165.201.5 に対する FTP 要求が、10.1.1.3 にリダイレクトされる。
- セキュリティ アプライアンスの外部 IP アドレス 209.165.201.25 に対する HTTP 要求が、10.1.1.5 にリダイレクトされる。
- PAT アドレス 209.165.201.15 に対する HTTP ポート 8080 の要求が、10.1.1.7 ポート 80 にリダイレクトされる。

この事例を実装するには、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、内部ネットワークに対して PAT を設定します。

```
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** 次のコマンドを入力して、209.165.201.5 に対する Telnet 要求を 10.1.1.6 にリダイレクトします。

```
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** 次のコマンドを入力して、IP アドレス 209.165.201.5 に対する FTP 要求を 10.1.1.3 にリダイレクトします。

```
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** 次のコマンドを入力して、セキュリティ アプライアンス外部インターフェイス アドレスに対する HTTP 要求を 10.1.1.5 にリダイレクトします。

```
hostname(config)# static (inside,outside) tcp interface www 10.1.1.5 www netmask  
255.255.255.255
```

- ステップ 5** 次のコマンドを入力して、PAT アドレス 209.165.201.15 に対するポート 8080 での HTTP 要求を 10.1.1.7 ポート 80 にリダイレクトします。

```
hostname(config)# static (inside,outside) tcp 209.165.201.15 8080 10.1.1.7 www netmask  
255.255.255.255
```

---



# ネットワーク アクセスの許可または拒否

この章では、セキュリティ アプライアンスを経由するネットワーク アクセスを、アクセスリストを使用して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には、[第 13 章「アクセスリストによるトラフィックの指定」](#)を参照してください。



(注)

ルーテッド ファイアウォール モードの場合も透過ファイアウォール モードの場合も、ネットワーク アクセスを制御するには、ACL を使用します。透過モードでは、拡張 ACL（レイヤ 3 トラフィック用）と EtherType ACL（レイヤ 2 トラフィック用）の両方を使用できます。

管理アクセス用のセキュリティ アプライアンス インターフェイスにアクセスするために、ホスト IP アドレスを許可するアクセスリストを併せて使用する必要はありません。[第 33 章「システム アクセスの管理」](#)に従って管理アクセスを設定するだけで十分です。

次の事項について説明します。

- [着信アクセスリストおよび発信アクセスリストの概要（P.15-2）](#)
- [インターフェイスへのアクセスリストの適用（P.15-5）](#)

## 着信アクセスリストおよび発信アクセスリストの概要

セキュリティ アプライアンスのインターフェイスを通過するトラフィックは、2つの方法で制御できます。セキュリティ アプライアンスに入るトラフィックは、着信アクセスリストを発信元インターフェイスに関連付けることで制御できます。セキュリティ アプライアンスから出るトラフィックは、発信アクセスリストを宛先インターフェイスに関連付けることで制御できます。セキュリティ アプライアンスに入るトラフィックを許可するには、着信アクセスリストをインターフェイスに関連付ける必要があります。そのようにしていない場合、セキュリティ アプライアンスは、そのインターフェイスに入るすべてのトラフィックを自動的にドロップします。発信アクセスリストを使用してトラフィックを制限していない限り、デフォルトでは、トラフィックはどのインターフェイス上のセキュリティ アプライアンスでも出ることができます。発信アクセスリストは、着信アクセスリストですでに設定されている制限にさらに制限を追加します。

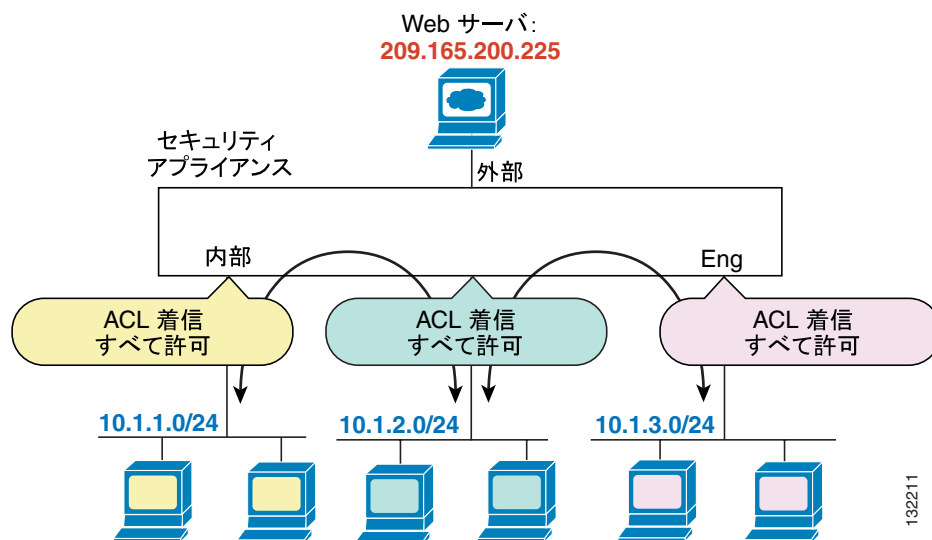


(注)

「着信」および「発信」とは、インターフェイス上のセキュリティ アプライアンスに入るトラフィックまたはインターフェイス上のセキュリティ アプライアンスを出るトラフィックのどちらかにインターフェイス上のアクセスリストが適用されているかを意味します。これらの用語は、一般に着信と呼ばれる、セキュリティ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移動や、一般に発信と呼ばれる、セキュリティの高いインターフェイスから低いインターフェイスへのトラフィックの移動を意味しません。

発信アクセスリストは、アクセスリスト コンフィギュレーションを簡素化するために使用できます。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、すべてのトラフィックを許可する簡単な着信アクセスリストを各内部インターフェイス上に作成できます (図 15-1 を参照)。

図 15-1 着信アクセスリスト



この例について、次のコマンドを参照してください。

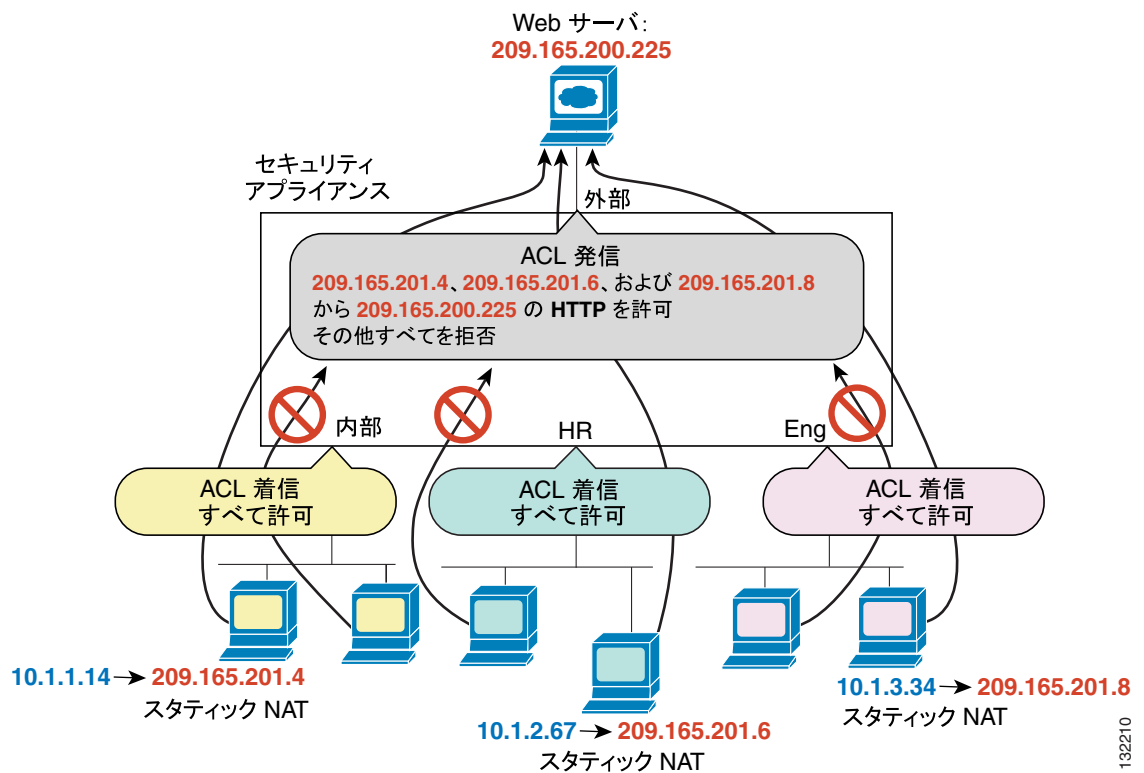
```
hostname(config)# access-list INSIDE extended permit ip any any
hostname(config)# access-group INSIDE in interface inside

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
```

次に、内部ネットワークの特定のホストだけに外部ネットワークの Web サーバへのアクセスを許可する場合、指定したホストだけを許可する、より限定的なアクセスリストを作成し、それを外部インターフェイスの発信方向に適用できます（図 15-2 を参照）。NAT および IP アドレスについては、P.13-3 の「NAT 使用時にアクセスリストで使用する IP アドレス」を参照してください。発信アクセスリストは、他のホストが外部ネットワークに到達することを禁止します。

図 15-2 発信アクセスリスト



132210

この例について、次のコマンドを参照してください。

```
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
```

## インターフェイスへのアクセスリストの適用

拡張アクセスリストをインターフェイスの着信方向または発信方向に適用するには、次のコマンドを入力します。

```
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の方向に適用できるアクセスリストは、タイプ（拡張および EtherType）ごとに 1 つです。アクセスリストの方向の詳細については、[P.15-2 の「着信アクセスリストおよび発信アクセスリストの概要」](#)を参照してください。

**per-user-override** キーワードを使用すると、ユーザ認可用にダウンロードしたダイナミック アクセスリストにより、インターフェイスに割り当てられているアクセスリストを上書きできます。たとえば、インターフェイス アクセスリストが 10.0.0.0 からのトラフィックをすべて拒否し、ダイナミック アクセスリストが 10.0.0.0 からのトラフィックをすべて許可する場合、そのユーザに関しては、ダイナミック アクセスリストによってインターフェイス アクセスリストが上書きされます。ユーザごとのアクセスリストの詳細については、「RADIUS 認可の設定」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限り使用可能です。

コネクションレス型プロトコルの場合、トラフィックをどちらの方向にも通過させるには、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、透過モードでは、EtherType アクセスリストで BGP を許可できますが、その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。

次の例は、IP アドレス 209.165.201.12 の内部 Web サーバへのアクセスをイネーブルにするために必要なコマンドを示しています（この IP アドレスは、NAT 後、外部インターフェイスで可視となるアドレスです）。

```
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
```

この Web サーバ用の NAT も設定する必要があります。

次のアクセスリストでは、すべてのホストが内部ネットワークと hr ネットワークの間で通信することが許可されますが、外部ネットワークへのアクセスは特定のホストだけに許可されます。

```
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、次のサンプル アクセスリストでは、内部インターフェイスで発信される一般的な EtherType が許可されます。

```
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、セキュリティ アプライアンスを通過する一部の EtherType が許可されますが、それ以外はすべて拒否されます。

```
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、両方のインターフェイスで EtherType 0x1256 のトラフィックが拒否されますが、他のトラフィックはすべて許可されます。

```
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
```





# ネットワーク アクセスへの AAA の適用

この章では、ネットワーク アクセスに対して AAA（トリプル エー）をイネーブルにする方法について説明します。

管理アクセスの AAA については、[P.33-6 の「システム管理者の AAA」](#)を参照してください。

ここでは、次の項目を取り上げます。

- [AAA パフォーマンス \(P.16-1\)](#)
- [ネットワーク アクセス認証の設定 \(P.16-2\)](#)
- [ネットワーク アクセス認可の設定 \(P.16-7\)](#)
- [ネットワーク アクセスのアカウンティングの設定 \(P.16-14\)](#)
- [MAC アドレスによるトラフィックの認証と認可の免除 \(P.16-16\)](#)

## AAA パフォーマンス

セキュリティ アプライアンスは「カットスルー プロキシ」を使用します。これにより、従来のプロキシ サーバと比較して、パフォーマンスが大幅に向上します。従来のプロキシ サーバは、OSI 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ため、プロキシ サーバのパフォーマンスに負担がかかります。セキュリティ アプライアンス カットスルー プロキシは、アプリケーション レイヤで最初にユーザ確認を行い、標準 RADIUS、TACACS+、またはローカル データベースで認証します。セキュリティ アプライアンスはユーザを認証した後、セッション フローをシフトするため、セッション ステート情報を維持したまま、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流れます。

## ネットワーク アクセス認証の設定

ここでは、次の項目について説明します。

- 認証の概要 (P.16-2)
- ネットワーク アクセス認証のイネーブル化 (P.16-3)
- Web クライアントのセキュアな認証のイネーブル化 (P.16-4)

### 認証の概要

セキュリティ アプライアンスでは、AAA サーバを使用するネットワーク アクセス認証を設定できます。

所定の IP アドレスのユーザは、認証セッションが期限切れになるまで、すべての規則およびタイプに対して一度だけ認証を受ける必要があります (タイムアウトの値については、『Cisco Security Appliance Command Reference』で **timeout uauth** コマンドを参照してください)。たとえば、Telnet および FTP を認証するようにセキュリティ アプライアンスが設定されていて、ユーザが正常に Telnet 認証を受けた場合、認証セッションが継続している限り、ユーザは FTP 認証を受ける必要はありません。

プロトコルまたはサービスへのネットワーク アクセス認証を要求するようにセキュリティ アプライアンスを設定することは、すべてのプロトコルまたはサービスについて可能ですが、ユーザが直接認証を受けることができるのは、HTTP (S)、Telnet、または FTP だけです。ユーザがこれらのサービスのいずれかの認証を受けないと、セキュリティ アプライアンスは認証が必要な他のトラフィックを許可しません。

HTTP (S)、Telnet、または FTP がセキュリティ アプライアンスを通過することを許可せずに、他のタイプのトラフィックを認証する場合は、仮想 Telnet を設定できます。仮想 Telnet では、セキュリティ アプライアンス上に設定された所定の IP アドレスにユーザが Telnet 接続すると、セキュリティ アプライアンスは Telnet プロンプトを表示します。**virtual telnet** コマンドの詳細については、『Cisco Security Appliance Command Reference』を参照してください。

Telnet、HTTP (S)、および FTP の場合、セキュリティ アプライアンスは認証プロンプトを生成します。宛先サーバにも独自の認証がある場合、ユーザは別のユーザ名とパスワードを入力します。

HTTP 認証では、スタティック NAT が設定されている場合、セキュリティ アプライアンスはローカル ポートをチェックします。セキュリティ アプライアンスは、グローバル ポートにかかわらず、ローカル ポート 80 を宛先とするトラフィックを検出した場合、HTTP 接続を代行受信し、認証を実行します。

たとえば、外部 TCP ポート 889 はポート 80 (www) に変換され、すべての関連 ACL はトラフィックを許可するものとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask
255.255.255.255
```

この場合、ユーザはポート 889 で 10.48.66.155 にアクセスを試み、セキュリティ アプライアンスはそのトラフィックを代行受信し、HTTP 認証を実行します。セキュリティ アプライアンスが HTTP 接続の完了を許可する前に、ユーザの Web ブラウザには HTTP 認証ページが表示されます。

次の例のように、ローカル ポートがポート 80 ではないとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask
255.255.255.255
```

この場合、認証ページはユーザに表示されません。その代わりに、セキュリティ アプライアンスは、要求したサービスを使用するには認証を受ける必要があることを示すエラーメッセージを Web ブラウザに送信します。

**(注)**

**aaa authentication secure-http-client** コマンドを使用しないで HTTP 認証を使用した場合、AAA サーバだけでなく、宛先 Web サーバにもユーザ名とパスワードがクリア テキストで送信されます。たとえば、外部 Web サーバにアクセスする内部ユーザを認証した場合、外部の誰もが有効なユーザ名とパスワードを知ることができます。HTTP 認証をイネーブルにするときは必ず **aaa authentication secure-http-client** コマンドを使用することをお勧めします。**aaa authentication secure-http-client** コマンドの詳細については、P.16-4 の「Web クライアントのセキュアな認証のイネーブル化」を参照してください。

FTP の場合、セキュリティ アプライアンス ユーザ名、アット マーク (@)、FTP ユーザ名 (name1@name2) を入力するオプションがあります。パスワードには、セキュリティ アプライアンス パスワード、アット マーク (@)、FTP パスワード (password1@password2) を入力します。たとえば、次のテキストを入力します。

```
name> jamiec@jchrichton
password> letmein@he110
```

この機能は、複数のログインを必要とするファイアウォールをカスケード接続している場合に有用です。複数の名前およびパスワードは、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には、次の手順を実行します。

**ステップ 1** **aaa-server** コマンドを使用して、AAA サーバを指定します。すでに AAA サーバを指定してある場合は、次の手順に進みます。

AAA サーバの指定方法の詳細については、P.10-17 の「AAA サーバ グループおよびサーバの識別」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、認証するトラフィックの送信元アドレスと宛先アドレスを指定する ACL を作成します。手順については、P.13-6 の「拡張アクセスリストの追加」を参照してください。

許可 ACE は、一致したトラフィックを認証するようにマークします。一方、拒否エントリは、一致したトラフィックを認証から除外します。HTTP、Telnet、または FTP のいずれかの宛先ポートを ACL に必ず含めます。これは、ユーザがこれらのサービスのいずれかの認証を受けないと、他のサービスがセキュリティ アプライアンスの通過を許可されないためです。

**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 ACL の名前、**interface\_name** は **nameif** コマンドで指定したインターフェイスの名前、**server\_group** はステップ 1 で作成した AAA サーバ グループです。



(注)

もう 1 つの方法として、**aaa authentication include** コマンド（コマンド内でトラフィックを指定するコマンド）を使用することもできます。ただし、同一コンフィギュレーション内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、『Cisco Security Appliance Command Reference』を参照してください。

**ステップ 4** （オプション） 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、セキュリティ アプライアンスが所定のユーザ アカウントに対して許可する連続失敗ログイン試行の回数を制限する場合は、**aaa local authentication attempts max-fail** コマンドを使用します。次の例を参考にしてください。

```
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 ステータスを解除するには、**clear aaa local user lockout** コマンドを使用します。

たとえば、次のコマンドは、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
```

次のコマンドは、外部インターフェイスから特定のサーバ（209.165.201.5）への Telnet トラフィックを認証します。

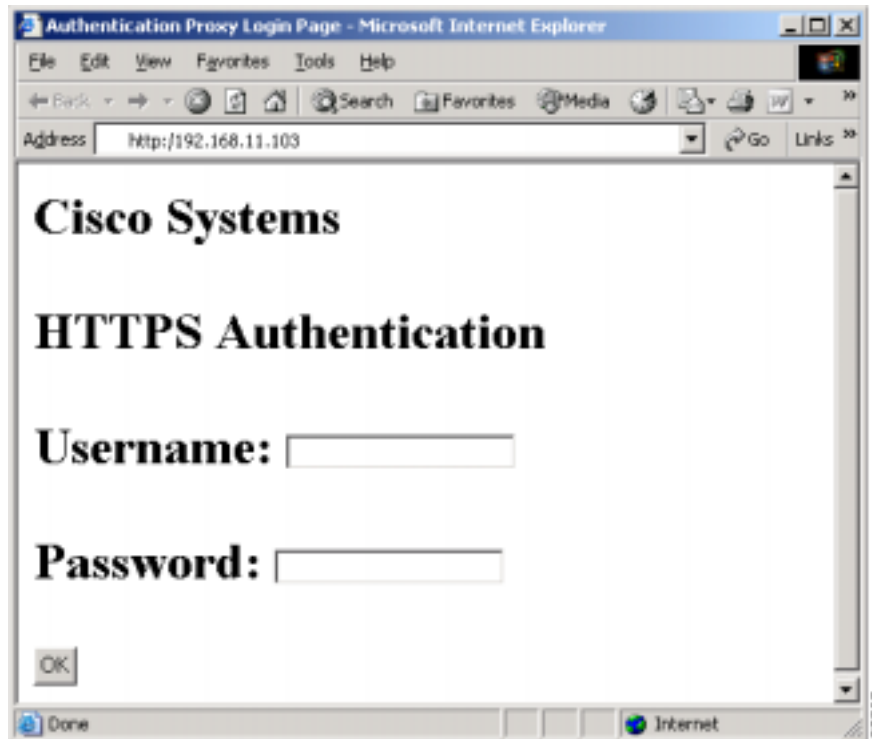
```
hostname/contexta(config)# aaa-server AuthInbound protocol tacacs+
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server AuthInbound (inside) host 10.1.1.1
hostname/contexta(config-aaa-server-host)# key TACPlusUauthKey
hostname/contexta(config-aaa-server-host)# exit
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な認証のイネーブル化

セキュリティ アプライアンスでは、HTTP 認証を保護する方法が提供されます。HTTP 認証を保護しないと、セキュリティ アプライアンスに対して入力されたユーザ名とパスワードは、宛先 Web サーバに渡されます。**aaa authentication secure-http-client** コマンドを使用することにより、Web クライアントとセキュリティ アプライアンスの間の HTTPS によるユーザ名とパスワードの交換をイネーブルにできます。HTTPS は伝送を暗号化し、ユーザ名とパスワードが HTTP で外部 Web サーバに渡されるのを防ぎます。

この機能をイネーブルにすると、認証を必要とする Web ページにユーザがアクセスする場合、セキュリティ アプライアンスによって、図 16-1 に示す Authentication Proxy Login ページが表示されます。

図 16-1 Authentication Proxy Login ページ



(注)

この例で表示されている Cisco Systems テキスト フィールドは、**auth-prompt** コマンドを使用してカスタマイズされています。このコマンドのシンタックスの詳細については、『Cisco Security Appliance Command Reference』を参照してください。**auth-prompt** コマンドを使用して文字列を入力しない場合、このフィールドは空白になります。

ユーザが有効なユーザ名とパスワードを入力すると、「Authentication Successful」ページが自動的に表示され閉じられます。ユーザが有効なユーザ名とパスワードの入力に失敗すると、「Authentication Failed」ページが表示されます。

セキュアな Web クライアント認証では、次の制限事項があります。

- 同時に行うことができる HTTPS 認証セッションは、最大 16 個です。16 個の HTTPS 認証プロセスがすべて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) 場合は、HTTPS 認証が機能しないことがあります。HTTPS 認証を受けた後、ブラウザが複数の TCP 接続を開始して Web ページのロードを試みると、最初の接続はそのまま許可されますが、後続の接続に対しては認証が発生します。その結果、ユーザが認証ページに正しいユーザ名とパスワードを毎回入力しても、繰り返し認証ページが表示されます。この現象を回避するには、**timeout uauth 0:0:1** コマンドを使用して、**uauth timeout** を 1 秒に設定します。ただし、この回避策ではウィンドウが 1 秒間開かれるため、このウィンドウを利用して、同じ送信元 IP アドレスからアクセスしてく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 で発生するため、HTTP クライアントから HTTP サーバに向かうポート 443 上のトラフィックをブロックするように **access-list** コマンド文を設定しないでください。また、ポート 80 上の Web トラフィックに対してスタティック PAT を設定する場合は、SSL ポートに対してもスタティック PAT を設定する必要があります。次の例では、1 行目で 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 行目を追加して、HTTPS 認証コンフィギュレーション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、ブラウザ自身によって生成された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、ユーザ名とパスワードを収集するためのフォームがブラウザにロードされます。どちらの場合でも、ユーザの入力したパスワードが誤っている場合は、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には、次の手順を実行します。

**ステップ 1** HTTP 認証をイネーブルにします。認証をイネーブルにする方法の詳細については、[P.16-3 の「ネットワーク アクセス認証のイネーブル化」](#)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、Web クライアントのセキュアな認証をイネーブルにします。

```
aaa authentication secure-http-client
```



(注)

**aaa authentication secure-http-client** コマンドは、HTTP 認証をイネーブルにする前でもイネーブルにした後でも使用できます。必要に応じて、HTTP 認証をイネーブルにする前にこのコマンドを入力することで、HTTP 認証をイネーブルにした時点でユーザ名とパスワードがセキュアな Web クライアント認証で保護されているようにすることができます。

## ネットワーク アクセス認可の設定

ユーザが所定の接続のための認証を受けると、セキュリティ アプライアンスは認可を使用して、ユーザからのトラフィックをさらに制御できます。

ここでは、次の項目について説明します。

- TACACS+ 認可の設定 (P.16-7)
- RADIUS 認可の設定 (P.16-8)

### TACACS+ 認可の設定

TACACS+ でネットワーク アクセス認可を実行するように、セキュリティ アプライアンスを設定できます。認可規則が一致する必要がある ACL を指定することにより、認可するトラフィックを指定します。または、認可規則自体で直接、トラフィックを指定することもできます。



#### ヒント

ACL を使用して認可するトラフィックを指定すると、入力する必要がある認可コマンドの数を大幅に少なくすることができます。これは、入力した各認可規則では、送信元と宛先のサブネットとサービスを 1 つだけ指定できるのに対して、ACL には多数のエントリを含めることができるためです。

認証文と認可文は互いに依存しませんが、認可文で一致した未認証トラフィックはすべて拒否されます。認可が成功するためには、ユーザは最初にセキュリティ アプライアンスで認証を受ける必要があります。所定の IP アドレスのユーザは、すべての規則およびタイプに対して一度だけ認証を受ければよいので、認証セッションが期限切れになっていなければ、トラフィックが認証文で一致した場合でも、認可が発生することがあります。

ユーザの認証が完了すると、セキュリティ アプライアンスは、一致するトラフィックの認可規則をチェックします。トラフィックが認可文に一致した場合、セキュリティ アプライアンスはユーザ名を TACACS+ サーバに送信します。TACACS+ サーバはセキュリティ アプライアンスに応答し、ユーザ 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を示します。セキュリティ アプライアンスは、その応答内の認可規則を実施します。

ユーザに対するネットワーク アクセス認可の設定については、ご使用の TACACS+ サーバのマニュアルを参照してください。

TACACS+ 認可を設定するには、次の手順を実行します。

**ステップ 1** 認証をイネーブルにします。詳細については、[P.16-3 の「ネットワーク アクセス認証のイネーブル化」](#)を参照してください。すでに認証をイネーブルにしてある場合は、次の手順に進みます。

**ステップ 2** `access-list` コマンドを使用して、認可するトラフィックの送信元アドレスと宛先アドレスを指定する ACL を作成します。手順については、[P.13-6 の「拡張アクセスリストの追加」](#)を参照してください。

許可 ACE は、一致したトラフィックを認可するようにマークします。一方、拒否エントリは、一致したトラフィックを認可から除外します。認可の照合に使用する ACL には、認証の照合に使用する ACL の規則と同じ規則またはその一部が含まれている必要があります。



**(注)**

認証を設定済みで、なおかつ認証されたトラフィックをすべて認可する場合、**aaa authentication match** コマンドで使用するために作成した ACL と同じ ACL を使用できます。

**ステップ 3** 認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 ACL の名前、*interface\_name* は **nameif** コマンドまたはデフォルトで指定したインターフェイスの名前、*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)**

もう 1 つの方法として、**aaa authorization include** コマンド（コマンド内でトラフィックを指定するコマンド）を使用することもできます。ただし、同一コンフィギュレーション内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、*Cisco Security Appliance Command Reference* を参照してください。

次のコマンドは、内部 Telnet トラフィックを認証し、認可します。209.165.201.5 以外のサーバに向かう Telnet トラフィックは認証だけを受けますが、209.165.201.5 に向かうトラフィックには認可が必要です。

```
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 認可の設定

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る access-accept メッセージでユーザ認可を返します。認証の設定の詳細については、[P.16-2 の「ネットワーク アクセス認証の設定」](#)を参照してください。

ネットワーク アクセスについてユーザを認証するようにセキュリティ アプライアンスを設定すると、RADIUS 認可も暗黙的にイネーブルになっています。したがって、この項では、セキュリティ アプライアンス上の RADIUS 認可の設定については取り上げません。ここでは、セキュリティ アプライアンスが RADIUS サーバから受信した ACL 情報をどのように処理するかについて説明します。

ACL をセキュリティ アプライアンスにダウンロードするように RADIUS サーバを設定できます。または、認証時に ACL 名をダウンロードするようにも設定できます。ユーザは、ユーザ固有の ACL で許可された操作だけを認可されます。





(注)

**access-group** コマンドを使用して ACL をインターフェイスに適用した場合は、**per-user-override** キーワードが、ユーザ固有の ACL による認可に対して次のように影響を与えることに注意してください。

- **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 ACL とユーザ固有の ACL の両方によって許可される必要があります。
- **per-user-override** キーワードを使用した場合、ユーザ固有の ACL によって許可される内容が決定されます。

詳細については、『Cisco Security Appliance Command Reference』の **access-group** コマンドの項を参照してください。

ここでは、次の項目について説明します。

- [ダウンロード可能な ACL を送信するための RADIUS サーバの設定 \(P.16-9\)](#)
- [ユーザごとの ACL 名をダウンロードするための RADIUS サーバの設定 \(P.16-13\)](#)

## ダウンロード可能な ACL を送信するための RADIUS サーバの設定

この項では、Cisco Secure ACS およびサードパーティ RADIUS サーバを設定する方法について説明します。次の項目を取り上げます。

- [ダウンロード可能な ACL の機能と Cisco Secure ACS について \(P.16-9\)](#)
- [ダウンロード可能な ACL に関する Cisco Secure ACS の設定 \(P.16-11\)](#)
- [ダウンロード可能な ACL に関する任意の RADIUS サーバの設定 \(P.16-12\)](#)
- [ダウンロード可能な ACL 内のワイルドカード ネットマスク表現の変換 \(P.16-13\)](#)

## ダウンロード可能な ACL の機能と Cisco Secure ACS について

ダウンロード可能な ACL は、Cisco Secure ACS を使用して各サーバに適切な ACL を提供する場合に最もスケーラブルな方法です。次の機能があります。

- 無制限の ACL サイズ：ダウンロード可能な ACL は、完全な ACL を Cisco Secure ACS からセキュリティ アプライアンスに転送するために必要な数の RADIUS パケットを使用して送信されます。
- ACL 管理の簡素化および集中化：ダウンロード可能な ACL により、一度記述した ACL セットを多数のユーザ プロファイルまたはグループ プロファイルに適用することや、多数のセキュリティ アプライアンスに配布することができます。

この方法は、複数の Cisco Secure ACS ユーザまたはグループに適用する非常に大きい ACL セットがある場合に最適ですが、Cisco Secure ACS ユーザおよびグループの管理を簡素化できることから、ACL のサイズを問わず有用です。

セキュリティ アプライアンスは、ダウンロード可能な ACL を Cisco Secure ACS から次のプロセスで受信します。

1. セキュリティ アプライアンスがユーザ セッションのための RADIUS 認証要求パケットを送信します。

2. Cisco Secure ACS がそのユーザを正常に認証した場合、Cisco Secure ACS は、該当するダウンロード可能な ACL の内部名が含まれた RADIUS access-accept メッセージを返します。Cisco IOS cisco-av-pair RADIUS VSA (ベンダー 9、アトリビュート 1) には、ダウンロード可能な ACL セットを特定する次の AV のペアが含まれています。

```
ACS: CiscoSecure-Defined-ACL=acl-set-name
```

`acl-set-name` はダウンロード可能な ACL の内部名です。この名前は、Cisco Secure ACS 管理者が ACL に割り当てた名前と ACL が最後に変更された日時の組み合わせです。

3. セキュリティ アプライアンスはダウンロード可能な ACL の名前を検査し、以前にその名前のダウンロード可能な ACL を受信したことがあるかどうかを判別します。

- セキュリティ アプライアンスが以前にその名前のダウンロード可能な ACL を受信したことがある場合は、Cisco Secure ACS との通信は完了し、セキュリティ アプライアンスは ACL をユーザ セッションに適用します。ダウンロード可能な ACL の名前には最後に変更された日時が含まれているため、Cisco Secure ACS から送信された名前と、以前にダウンロードした ACL の名前が一致するという事は、セキュリティ アプライアンスはダウンロード可能な ACL の最新バージョンを持っていることになります。
- セキュリティ アプライアンスが以前にその名前のダウンロード可能な ACL を受信したことがない場合は、その ACL の古いバージョンを持っているか、その ACL のどのバージョンもダウンロードしたことがないことになります。いずれの場合でも、セキュリティ アプライアンスは、ダウンロード可能な ACL 名を RADIUS 要求内のユーザ名として使用し、ヌル パスワード アトリビュートとともに RADIUS 認証要求を発行します。cisco-av-pair RADIUS VSA では、この要求に次の AV のペアも含まれます。

```
AAA:service=ip-admission
AAA:event=acl-download
```

これに加えて、セキュリティ アプライアンスは Message-Authenticator アトリビュート (IETF RADIUS アトリビュート 80) で要求に署名します。

4. ダウンロード可能な ACL の名前が含まれているユーザ名アトリビュートを持つ RADIUS 認証要求を受信すると、Cisco Secure ACS は Message-Authenticator アトリビュートをチェックして要求を認証します。Message-Authenticator アトリビュートがない場合、または正しくない場合、Cisco Secure ACS はその要求を無視します。Message-Authenticator アトリビュートの存在により、ダウンロード可能な ACL 名がネットワーク アクセスの不正取得に悪用されることが防止されます。Message-Authenticator アトリビュートとその使用方法は、RFC 2869「RADIUS Extensions」で定義されています。この文書は、<http://www.ietf.org> で入手できます。
5. 要求された ACL の長さが約 4 KB 未満の場合、Cisco Secure ACS はその ACL を含めた access-accept メッセージで応答します。メッセージには他の必須アトリビュートを含める必要があるため、1 つの access-accept メッセージに収まる ACL の最大サイズは 4 KB よりわずかに小さくなります。

Cisco Secure ACS はダウンロード可能な ACL を cisco-av-pair RADIUS VSA で送信します。ACL は、一連の AV のペアという形式をとります。各ペアには ACE が 1 つ含まれ、シリアル番号が付けられます。

```
ip:inacl#1=ACE-1
ip:inacl#2=ACE-2
.
.
ip:inacl#n=ACE-n
```

AV のペアの例を次に示します。

```
ip:inacl#1=permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
```

6. 要求された ACL の長さが約 4 KB を超える場合、Cisco Secure ACS は、上記の形式の ACL の一部が含まれた access-challenge メッセージで応答します。メッセージには、State アトリビュート (IETF RADIUS アトリビュート 24) も含まれています。State アトリビュートには、Cisco Secure ACS がダウンロードの進捗を追跡するために使用する制御データが含まれています。Cisco Secure ACS は、RADIUS メッセージの最大サイズ以内で可能な限り多数の完全な AV のペアを cisco-av-pair RADIUS VSA に含めます。

セキュリティ アプライアンスは ACL の一部を受信すると、それを保存し、新しい access-request メッセージで応答します。これには、ダウンロード可能な ACL を求める最初の要求と同じアトリビュートと、access-challenge メッセージで受信した State アトリビュートのコピーが含まれています。

これは、Cisco Secure ACS が ACL の最後の部分を access-accept メッセージで送信するまで続行されます。

### ダウンロード可能な ACL に関する Cisco Secure ACS の設定

Cisco Secure ACS 上のダウンロード可能な ACL を共有プロファイル コンポーネントとして設定し、その ACL をグループまたは個々のユーザに割り当てることができます。

ACL 定義は、次のプレフィックスがない点を除いて拡張 **access-list** コマンド (P.13-6 の「[拡張アクセスリストの追加](#)」を参照) に類似する 1 つまたは複数のセキュリティ アプライアンス コマンドで構成されます。

```
access-list acl_name extended
```

Cisco Secure ACS バージョン 3.3 上のダウンロード可能な ACL 定義の例を次に示します。

```
+-----+
| 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 ACL を作成する方法、およびそれらをユーザと関連付ける方法の詳細については、ご使用のバージョンの Cisco Secure ACS のガイドを参照してください。

セキュリティ アプライアンス上では、ダウンロードされた ACL の名前は次のようになります。

```
#ACSACL#-ip-acl_name-number
```

acl\_name 引数は Cisco Secure ACS で定義された名前 (上記の例では acs\_ten\_acl)、number は Cisco Secure ACS が生成した一意のバージョン ID です。

セキュリティ アプライアンス上にダウンロードされた ACL は、次の行で構成されます。

```
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.253
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.253
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.253
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit ip any any
```

## ダウンロード可能な ACL に関する任意の RADIUS サーバの設定

ユーザ固有の ACL を Cisco IOS RADIUS cisco-av-pair VSA (ベンダー 9、アトリビュート 1) でセキュリティ アプライアンスに送信するように、Cisco IOS RADIUS VSA をサポートする任意の RADIUS サーバを設定できます。

cisco-av-pair VSA で、**access-list extended** コマンド (P.13-6 の「拡張アクセスリストの追加」を参照) と類似する 1 つまたは複数の ACE を設定します。ただし、次のコマンド プレフィックスを置き換える必要があります。

```
access-list acl_name extended
```

次のテキストに置き換えます。

```
ip:inacl#nnn=
```

*nnn* 引数は、0 ～ 999999999 の番号で、セキュリティ アプライアンス上に設定するコマンド文の順序を指定します。このパラメータを省略すると、順番は 0 となり、cisco-av-pair RADIUS VSA 内部の ACE の順序が使用されます。

RADIUS サーバ上の cisco-av-pair VSA に対して設定されている必要のある ACL 定義の例を次に示します。

```
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 ACL をユーザごとに一意にする方法については、ご使用の RADIUS サーバのマニュアルを参照してください。

セキュリティ アプライアンス上では、ダウンロードされた ACL の名前は次の形式になります。

```
AAA-user-username
```

*username* 引数は、認証を受けるユーザの名前です。

セキュリティ アプライアンス上にダウンロードされた ACL は、次の行で構成されます。RADIUS サーバ上で指定された番号に基づいた順序になっています。

```
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
```

ダウンロードされた ACL の「access-list」という単語と名前の間には、2 個のスペースがあります。これらのスペースにより、ダウンロードされた ACL とローカル ACL が区別されます。この例では、「79AD4A08」はセキュリティ アプライアンスが作成したハッシュ値で、RADIUS サーバ上で ACL 定義がいつ変更されたかを判別するために役立ちます。

### ダウンロード可能な ACL 内のワイルドカード ネットマスク表現の変換

RADIUS サーバを使用して、ダウンロード可能な ACL を Cisco VPN 3000 Series Concentrator およびセキュリティ アプライアンスに提供する場合は、ワイルドカード ネットマスク表現を標準のネットマスク表現に変換するようにセキュリティ アプライアンスを設定しなければならない場合があります。これは、Cisco VPN 3000 Series Concentrator はワイルドカード ネットマスク表現をサポートしますが、セキュリティ アプライアンスは標準のネットマスク表現しかサポートしないためです。これらの違いは、RADIUS サーバ上のダウンロード可能な ACL を設定する方法に影響しますが、ワイルドカード ネットマスク表現を変換するようにセキュリティ アプライアンスを設定することで、その影響を最小限に抑えることができます。ワイルドカード ネットマスク表現の変換により、RADIUS サーバ上のダウンロード可能な ACL のコンフィギュレーションを変更することなく、Cisco VPN 3000 Series Concentrator 用に記述されたダウンロード可能な ACL をセキュリティ アプライアンスで使用できます。

ACL ネットマスク変換は、**acl-netmask-convert** コマンドを使用してサーバごとに設定できます。このコマンドは AAA サーバ コンフィギュレーション モードで使用できます。RADIUS サーバの設定方法の詳細については、[P.10-17](#) の「[AAA サーバ グループおよびサーバの識別](#)」を参照してください。**acl-netmask-convert** コマンドの詳細については、『Cisco Security Appliance Command Reference』を参照してください。

### ユーザごとの ACL 名をダウンロードするための RADIUS サーバの設定

ユーザ認証時に、セキュリティ アプライアンスで作成済みの ACL の名前を RADIUS サーバからダウンロードするには、IETF RADIUS filter-id アトリビュート（アトリビュート番号 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、**filter-id=** を省略し、**acl\_name** だけを入力して指定します。

filter-id アトリビュートの値をユーザごとに一意にする方法については、ご使用の RADIUS サーバのマニュアルを参照してください。

セキュリティ アプライアンス上に ACL を作成する方法については、[P.13-6](#) の「[拡張アクセスリストの追加](#)」を参照してください。

## ネットワーク アクセスのアカウントティングの設定

セキュリティ アプライアンスは、セキュリティ アプライアンスを通過する任意の TCP トラフィックまたは UDP トラフィックについてのアカウントティング情報を RADIUS サーバまたは TACACS+ サーバに送信できます。そのトラフィックも認証されている場合、AAA サーバはユーザ名でアカウントティング情報を保持できます。そのトラフィックが認証されていない場合、AAA サーバは IP アドレスでアカウントティング情報を保持できます。アカウントティング情報には、セッションの開始時刻と終了時刻、ユーザ名、そのセッションでセキュリティ アプライアンスを経由したバイト数、使用されたサービス、セッションの継続時間が含まれます。

アカウントティングを設定するには、次の手順を実行します。

**ステップ 1** ユーザごとのアカウントティング データを提供するようにセキュリティ アプライアンスを設定する場合は、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、[P.16-3 の「ネットワーク アクセス認証のイネーブル化」](#)を参照してください。IP アドレスごとのアカウントティング データを提供するようにセキュリティ アプライアンスを設定する場合は、認証をイネーブルにする必要はありません。次のステップに進みます。

**ステップ 2** `access-list` コマンドを使用して、アカウントティング対象のトラフィックの送信元アドレスと宛先アドレスを指定する ACL を作成します。手順については、[P.13-6 の「拡張アクセスリストの追加」](#)を参照してください。

許可 ACE は、一致したトラフィックを認可するようにマークします。一方、拒否エントリは、一致したトラフィックを認可から除外します。



(注)

認証が設定済みで、なおかつ認証されたすべてのトラフィックのアカウントティング データが必要な場合、`aaa authentication match` コマンドで使用するために作成した ACL と同じ ACL を使用できます。

**ステップ 3** アカウント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)

もう 1 つの方法として、`aaa accounting include` コマンド（コマンド内でトラフィックを指定するコマンド）を使用することもできます。ただし、同一コンフィギュレーション内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、『Cisco Security Appliance Command Reference』を参照してください。

次のコマンドは、内部 Telnet トラフィックを認証、認可、アカウントिंगします。209.165.201.5 以外のサーバに向かう Telnet トラフィックは認証だけを受けますが、209.165.201.5 に向かうトラフィックには認可およびアカウントングが必要です。

```
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 アドレスによるトラフィックの認証と認可の免除

セキュリティ アプライアンスは、特定の MAC アドレスからのトラフィックの認証および認可を免除できます。

たとえば、特定のネットワーク上で発信された TCP トラフィックを認証するようにセキュリティ アプライアンスが設定された状態で、特定のサーバからの未認証 TCP 接続を許可するには、まず、**mac-list** コマンドを使用して、そのサーバの MAC アドレスからのトラフィックを許可する規則を作成します。次に、**aaa mac-exempt** コマンドを使用して、その MAC リストで指定したサーバからのすべてのトラフィックの認証および認可を免除します。

これとは逆に、特定のコンピュータからのトラフィックを認証にかかわらず常に許可しない場合は、その MAC アドレスからのトラフィックを拒否する **mac-list** コマンドで、このコンピュータの MAC アドレスを使用できます。このシナリオで使用している **aaa mac-exempt** コマンドにより、これ以外の場合であれば認証規則で許可されるトラフィックでも、このコンピュータからのトラフィックは拒否されます。

MAC アドレスを使用してトラフィックの認証および認可を免除するには、次の手順を実行します。

### 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 リストに割り当てる 16 進数値、*mac* はトラフィックを許可または拒否するコンピュータの MAC アドレス、*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、『Cisco Security Appliance Command Reference』を参照してください。

### ステップ 2 特定の MAC リストで指定されている MAC アドレスのトラフィックに対して免除するには、次のコマンドを入力します。

```
hostname/contexta(config)# aaa mac-exempt match id
```

*id* は、認証および認可を免除するトラフィックの MAC アドレスが含まれている MAC リストを指定する文字列です。

次のコマンドは、2つの MAC リストを作成します。各リストには、1つの MAC アドレスが含まれています。1つのリストは、リストにある MAC アドレスからのトラフィックを許可し、もう1つのリストは、リストにある MAC アドレスからのトラフィックを拒否します。最後の2つのコマンドは、2つのリストにある MAC アドレスから発信されたすべてのトラフィックの認証および認可を免除するようにセキュリティ アプライアンスを設定します。

```
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 リスクを低減したり不適切な使用を防止したりする方法について説明します。ここでは、次の項目を取り上げます。

- [フィルタリングの概要 \(P.17-1\)](#)
- [ActiveX オブジェクトのフィルタリング \(P.17-2\)](#)
- [Java アプレットのフィルタリング \(P.17-4\)](#)
- [外部サーバによる URL および FTP 要求のフィルタリング \(P.17-5\)](#)
- [フィルタリング統計情報とフィルタリング設定の表示 \(P.17-11\)](#)

## フィルタリングの概要

この項では、フィルタリングを適用することにより、セキュリティ アプライアンスを通過するトラフィックをどのように制御できるかについて説明します。フィルタリングは、次の2つの異なる方法で使用できます。

- 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するフィルタリング

アクセスを全面的にブロックする代わりに、ActiveX オブジェクトや Java アプレットなど、特定の状況でセキュリティ上の脅威をもたらす可能性のある特定の不適切なオブジェクトを HTTP トラフィックから取り除くことができます。

URL フィルタリングを使用して、N2H2 Sentian や Websense などの外部フィルタリングサーバに特定のトラフィックを誘導することもできます。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ている特定のサイトまたは特定のタイプのサイトに向かう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 に大きな負荷がかかるため、外部フィルタリングサーバを使用することにより、他のトラフィックのスループットに影響を与えることがなくなります。ただし、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している場合でも、ネットワークの速度および URL フィルタリングサーバのキャパシティによっては、最初の接続に必要な時間が著しく長くなる場合もあります。

## ActiveX オブジェクトのフィルタリング

この項では、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 オブジェクトを取り除く方法について説明します。ここでは、次の項目について説明します。

- [ActiveX フィルタリングの概要 \(P.17-2\)](#)
- [ActiveX フィルタリングのイネーブル化 \(P.17-2\)](#)

### ActiveX フィルタリングの概要

ActiveX オブジェクトは、保護されたネットワーク上のホストとサーバを攻撃するコードを含むことがあるため、セキュリティ リスクを引き起こす可能性があります。ActiveX オブジェクトは、ActiveX フィルタリングで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 ページなど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 フォームやカレンダーなど、情報の収集と表示に使用されるサードパーティ製の多様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、またはサーバへの攻撃に利用される、などの恐れがあります。

**filteractivex** 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、および </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ています。



**注意**

このコマンドは、オブジェクト タグに埋め込まれている Java アプレット、イメージ ファイル、またはマルチメディア オブジェクトもすべてブロックします。

<object> または </object> という HTML タグが複数のネットワーク 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 MTU のバイト数より長い場合、セキュリティ アプライアンスはそのタグをブロックできません。

ActiveX blocking does not occur when users access an IP address referenced by the **alias** command.

### ActiveX フィルタリングのイネーブル化

この項では、セキュリティ アプライアンスを通過する HTTP トラフィック内の ActiveX オブジェクトを取り除く方法について説明します。ActiveX オブジェクトを取り除くには、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)# filteractivex port[-port] local_ip local_mask foreign_ip foreign_mask
```

このコマンドを使用するには、*port* に、フィルタリングを適用する TCP ポートを指定します。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 には **http** または **url** リテラルを使用できます。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ます。

ローカル IP アドレスおよびマスクによって、フィルタリングされるトラフィックの発信元である 1 台以上の内部ホストを指定します。外部アドレスおよびマスクは、フィルタリングされるトラフィックの外部の宛先を指定します。

これらのアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。これらのマスクに **0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。

次の例では、すべての発信接続で ActiveX オブジェクトをブロックすることを指定しています。

```
hostname(config)# filter activex 80 0 0 0 0
```

このコマンドは、ポート 80 上において、あらゆるローカル ホストから来て、あらゆる外部ホスト 接続へ向かう Web トラフィックに ActiveX オブジェクト ブロッキングが適用されることを指定します。

このコンフィギュレーションを削除するには、次の例で示すように、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

この項では、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 アプレットを取り除く方法について説明します。Java アプレットは、保護されたネットワーク上のホストとサーバを攻撃するコードを含むことがあるため、セキュリティ リスクを引き起こす可能性があります。Java アプレットは、**filter java** コマンドで取り除くことができます。

**filter java** コマンドは、発信接続からセキュリティ アプライアンスに戻る 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 ページの送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> タグに埋め込まれた Java アプレットを取り除くには、**filter activex** コマンドを使用します。

ファイアウォールを通過する HTTP トラフィック内の Java アプレットを取り除くには、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] local_ip local_mask foreign_ip foreign_mask
```

このコマンドを使用するには、*port* に、フィルタリングを適用する TCP ポートを指定します。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 には **http** または **url** リテラルを使用できます。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ます。

ローカル IP アドレスおよびマスクによって、フィルタリングされるトラフィックの発信元である 1 台以上の内部ホストを指定します。外部アドレスおよびマスクは、フィルタリングされるトラフィックの外部の宛先を指定します。

これらのアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。これらのマスクに **0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。

これらのアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。これらのマスクに **0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。

次の例では、すべての発信接続で Java アプレットをブロックすることを指定しています。

```
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。

次の例では、保護されたネットワーク上のホストへの Java アプレットのダウンロードをブロックしています。

```
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。

このコンフィギュレーションを削除するには、次の例で示すように、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

この項では、外部サーバを使用して URL および FTP 要求をフィルタリングする方法について説明します。ここでは、次の項目について説明します。

- [URL フィルタリングの概要 \(P.17-5\)](#)
- [フィルタリングサーバの指定 \(P.17-5\)](#)
- [コンテンツ サーバ応答のバッファリング \(P.17-6\)](#)
- [サーバ アドレスのキャッシング \(P.17-7\)](#)
- [HTTP URL のフィルタリング \(P.17-8\)](#)
- [HTTPS URL のフィルタリング \(P.17-9\)](#)
- [FTP 要求のフィルタリング \(P.17-10\)](#)

### URL フィルタリングの概要

フィルタリングは、セキュリティの高いネットワークからセキュリティの低いネットワークに発信される接続要求に対して適用できます。ACL を使用して特定のコンテンツ サーバに対する発信アクセスを禁止することはできますが、サイズおよびインターネットのダイナミックな性質により、このような手段で使用方法を管理することは困難です。次のインターネット フィルタリング製品のいずれかを実行する別個のサーバを使用することにより、コンフィギュレーションを簡素化し、セキュリティ アプライアンスのパフォーマンスを向上できます。

- HTTP、HTTPS、および FTP フィルタリング用の Websense Enterprise
- HTTP フィルタリング専用の N2H2 Sentian (Sentian の一部のバージョンは HTTPS をサポートしますが、セキュリティ アプライアンスでは、Sentian による HTTP フィルタリングだけがサポートされています)

セキュリティ アプライアンスのパフォーマンスへの影響は、外部サーバを使用した方が小さくなりますが、フィルタリングサーバがセキュリティ アプライアンスから離れている場合は、Web サイトまたは FTP サーバへのアクセス時間が長くなることもあります。

フィルタリングがイネーブルで、コンテンツを求める要求がセキュリティ アプライアンスを経由して送信された場合、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がその接続を許可した場合、セキュリティ アプライアンスはコンテンツサーバからの応答を発信元クライアントに転送します。フィルタリングサーバがその接続を拒否した場合、セキュリティ アプライアンスは応答をドロップし、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。

セキュリティ アプライアンス上でユーザ認証がイネーブルの場合、セキュリティ アプライアンスはフィルタリングサーバにユーザ名も送信します。フィルタリングサーバは、ユーザ固有のフィルタリング設定を使用したり、使用方法に関する高度なレポートを提供したりすることができます。

### フィルタリング サーバの指定

コンテキストごとに最大 4 つのフィルタリングサーバを指定できます。セキュリティ アプライアンスは、1 つのサーバが応答するまで、それらのサーバを順番に使用します。コンフィギュレーション内に設定できるサーバのタイプは、1 つだけ (Websense または N2H2) です。



(注)

**filter** コマンドを使用して HTTP または HTTPS のフィルタリングを設定する前に、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、**filter** コマンドもすべて削除されます。

**url-server** コマンドを次のように使用して、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 |  
UDP version 1|4 [connections num_conns] ]
```

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 [connections num_conns]]
```

*if\_name* には、フィルタリングサーバに接続されているセキュリティ アプライアンス インターフェイスの名前を指定します（デフォルトは **inside** です）。*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、セキュリティ アプライアンスがフィルタリングサーバへの接続試行を継続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、N2H2 サーバが TCP または UDP でセキュリティ アプライアンスと通信するために使用するデフォルト ポートです。デフォルト ポートの変更方法については、『*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
```

これは、セキュリティ アプライアンスの境界インターフェイス上の、IP アドレス 10.0.1.1 を持つ Websense フィルタリングサーバを指定しています。この例でイネーブルになっている version 4 は、キャッシュをサポートするため、Websense によって推奨されています。

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
```

これは、2 つの Sentian フィルタリングサーバを指定しています。どちらもセキュリティ アプライアンスの境界インターフェイス上にあります。

## コンテンツ サーバ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した場合、その要求は、セキュリティ アプライアンスによって、コンテンツ サーバとフィルタリングサーバの両方に同時に送信されます。フィルタリングサーバがコンテンツ サーバより早く応答しなかった場合、サーバ応答はドロップされます。これにより、Web クライアント側の視点で Web サーバ応答が表示されます。これは、クライアントが要求を再発行する必要があるためです。

HTTP 応答バッファをイネーブルにすると、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、バッファリングしない場合に発生する可能性のある遅延が回避されます。

HTTP 要求または FTP 要求に対する応答のバッファリングを設定するには、次の手順を実行します。

- ステップ 1** 次のコマンドを入力して、フィルタリング サーバからの応答が保留中である、HTTP 要求または 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 サーバに限りサポートされています。

- ステップ 2** 次のコマンドを入力して、保留中 URL バッファリング（および Websense による長い URL バッファリング）用の最大使用可能メモリを設定します。

```
hostname(config)# url-block url-mempool memory-pool-size
```

最大メモリ割り当ての 2 KB ～ 10 MB に相当する 2 ～ 10240 の範囲の値を、*memory-pool-size* に指定します。

## 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すると、フィルタリング サーバはセキュリティ アプライアンスに対して、サーバアドレスを一定時間キャッシュすることを許可できます。ただし、そのアドレスでホストされているサイトはいずれも、常に許可されるカテゴリに属している必要があります。これにより、そのユーザがそのサーバに再度アクセスするか、別のユーザがそのサーバにアクセスしたときに、セキュリティ アプライアンスがフィルタリング サーバに再度照会する必要がなくなります。



**(注)** キャッシュされた IP アドレス要求は、フィルタリング サーバに渡されず、記録もされません。そのため、このアクティビティはどのレポートにも表示されません。**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、**url-cache** コマンドを使用して、次のように入力します。

```
hostname(config)# url-cache dst | src_dst size
```

範囲 1 ～ 128 (KB) のキャッシュサイズの値を、*size* に指定します。

**dst** キーワードを使用して、URL 宛先アドレスに基づいて、エントリをキャッシュします。このモードは、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選択します。

**src\_dst** キーワードを使用して、URL 要求を開始した送信元アドレスと 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します。このモードは、ユーザが Websense サーバ上で同じ URL フィルタリング ポリシーを共有していない場合に選択します。

## HTTP URL のフィルタリング

この項では、外部フィルタリングサーバを使用する HTTP フィルタリングを設定する方法について説明します。ここでは、次の項目について説明します。

- [HTTP フィルタリングの設定 \(P.17-8\)](#)
- [長い HTTP URL のフィルタリングのイネーブル化 \(P.17-8\)](#)
- [長い HTTP URL の切り捨て \(P.17-8\)](#)
- [トラフィックに対するフィルタリングの免除 \(P.17-9\)](#)

### 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し、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 接続要求を承認した場合、セキュリティ アプライアンスは Web サーバからの応答が発信元クライアントに到達することを許可します。フィルタリングサーバが要求を拒否した場合、セキュリティ アプライアンスは、ユーザをブロック ページにリダイレクトし、アクセスが拒否されたことを示します。

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] 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は、1 つまたは複数のポート番号を、*port* に指定します。*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。

**allow** オプションは、一次フィルタリングサーバが利用できないときに、セキュリティ アプライアンス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。**proxy-block** コマンドを使用して、プロキシサーバへの要求をすべてドロップします。

### 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、セキュリティ アプライアンスは、1159 文字を超える HTTP URL を長い URL と見なします。Websense サーバの場合、最大許容長を大きくすることができます。

(Websense のみ) 次のコマンドを使用して、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
```

最大 2 ～ 4 KB の URL サイズに相当する 2 ～ 4 の範囲の値を、*long-url-size* に指定します。デフォルト値は 2 です。

### 長い HTTP URL の切り捨て

デフォルトでは、URL が最大許容サイズを超えると、その URL はドロップされます。これを回避するには、次のコマンドを入力して、長い URL を切り捨てるようにセキュリティ アプライアンスを設定します。

```
hostname(config)# filter url [longurl-truncate | longurl-deny | cgi-truncate]
```



**longurl-truncate** オプションを指定すると、セキュリティ アプライアンスは URL が最大許容長よりも長い場合に、URL のホスト名または IP アドレス部分だけを、評価のためにフィルタリングサーバに送信します。**longurl-deny** オプションは、URL が最大許容長よりも長い場合、発信 URL トラフィックを拒否します。

パラメータは含まずに CGI スクリプトの場所とスクリプト名だけを含むよう CGI URL を切り捨てるには、**cgi-truncate** オプションを使用します。長い HTTP 要求のほとんどは、CGI 要求です。パラメータ リストが非常に長い場合は、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ことにより、メモリ リソースが使い果たされ、ファイアウォールのパフォーマンスに影響します。

## トラフィックに対するフィルタリングの免除

特定のトラフィックに対してフィルタリングを免除するには、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、次のコマンドは、10.0.2.54 からの HTTP 要求を除くすべての HTTP 要求がフィルタリングサーバに転送されるように設定しています。

```
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し、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に対してだけ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、セキュリティ アプライアンスは、ディレクトリおよびファイル名の情報を付けずに URL ルックアップを送信します。フィルタリングサーバが HTTPS 接続要求を承認した場合、セキュリティ アプライアンスは SSL 接続ネゴシエーションの完了を許可し、Web サーバからの応答が発信元クライアントに到達することを許可します。フィルタリングサーバが要求を拒否した場合、セキュリティ アプライアンスは SSL 接続ネゴシエーションの完了を許可しません。ブラウザに、「The Page or the content cannot be displayed.」のようなエラーメッセージが表示されます。



(注)

セキュリティ アプライアンスは、HTTPS 用の認証プロンプトを表示しないため、ユーザは HTTPS サーバにアクセスする前に、HTTP または FTP を使用してセキュリティ アプライアンスで認証を受ける必要があります。

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は、ポート番号を *port* に指定します。*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。

**allow** オプションは、一次フィルタリングサーバが利用できないときに、セキュリティ アプライアンス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 サーバを指定し、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 サーバに対してだけサポートされています。

フィルタリング サーバが FTP 接続要求を承認した場合、セキュリティ アプライアンスは、成功を示す FTP リターン コードが発信元クライアントに到達することを許可します。たとえば、成功を示すリターン コードは「250: CWD command successful」です。フィルタリング サーバが要求を拒否した場合、FTP リターン コードは接続が拒否されたことを示すように変更されます。たとえば、セキュリティ アプライアンスの場合、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 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は、ポート番号を *port* に指定します。*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。

**allow** オプションは、一次フィルタリングサーバが利用できないときに、セキュリティ アプライアンス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。

完全なディレクトリパスを提供しない対話型の FTP セッションをブロックするには、**interact-block** オプションを使用します。対話型の FTP クライアントでは、ユーザが完全なパスを入力せずにディレクトリを変更できます。たとえば、ユーザは **cd /public/files** ではなく **cd ./files** と入力できます。

## フィルタリング統計情報とフィルタリング設定の表示

この項では、フィルタリング統計情報を監視する方法について説明します。ここでは、次の項目について説明します。

- [フィルタリング サーバ統計情報の表示 \(P.17-11\)](#)
- [バッファ コンフィギュレーションと統計情報の表示 \(P.17-11\)](#)
- [キャッシュ統計情報の表示 \(P.17-12\)](#)
- [フィルタリング性能統計情報の表示 \(P.17-12\)](#)
- [フィルタリング コンフィギュレーションの表示 \(P.17-12\)](#)

### フィルタリング サーバ統計情報の表示

フィルタリング サーバの情報を表示するには、次のコマンドを入力します。

```
hostname# show url-server
```

次に、**show url-server** コマンドの出力例を示します。

```
hostname# show 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、**show url-server stats** コマンドの出力例を示します。このコマンドでは、フィルタリング統計情報が表示されます。

```
hostname# show url-server stats  
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 コンフィギュレーションと統計情報の表示

**show url-block** コマンドは、url-block バッファにあるパケット数、およびバッファ上限を超えたためまたは再送信のためにドロップされたパケット数（ある場合）を表示します。

次に、**show url-block** コマンドの出力例を示します。

```
hostname# show url-block  
url-block url-mempool 128  
url-block url-size 4  
url-block block 128
```

これは、URL ブロック バッファのコンフィギュレーションを示しています。

次に、**show url-block block statistics** コマンドの出力例を示します。

```
hostname# show url-block block statistics

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
```

これは、URL ブロック統計情報を示しています。

## キャッシュ統計情報の表示

次に、**show url-cache stats** コマンドの出力例を示します。

```
hostname# show url-cache stats
URL Filter Cache Stats
-----
      Size :      128KB
  Entries :      1724
    In Use :       456
  Lookups :        45
     Hits :         8
```

This shows how the cache is used.

## フィルタリング性能統計情報の表示

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
```

これは、URL フィルタリング性能統計情報とその他の性能統計情報を示しています。フィルタリング統計情報は URL Access 行および URL Server Req 行に表示されます。

## フィルタリング コンフィギュレーションの表示

次に、**show filter** コマンドの出力例を示します。

```
hostname# show filter
filter url http 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```



# 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、一般的な接続設定、検査、IPS、CSC、および QoS に関するセキュリティ ポリシーを作成する方法について説明します。

次の事項について説明します。

- [モジュラ ポリシー フレームワークの概要 \(P.18-2\)](#)
- [クラスマップによるトラフィックの特定 \(P.18-3\)](#)
- [ポリシーマップによるアクションの定義 \(P.18-6\)](#)
- [サービス ポリシーによるインターフェイスへのポリシーの適用 \(P.18-10\)](#)
- [モジュラ ポリシー フレームワークの例 \(P.18-11\)](#)

## 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 ソフトウェアの QoS CLI と同様の方法でセキュリティ アプライアンスの機能を設定できるように、一貫性と柔軟性のある手段を提供します。たとえば、モジュラ ポリシー フレームワークを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。

モジュラ ポリシー フレームワークは、次の機能をサポートします。

- IPS
- CSC
- TCP 正規化、TCP 接続および UDP 接続の制限値とタイムアウト、および TCP シーケンス番号のランダム化
- QoS ポリシング
- QoS プライオリティキュー
- 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は、次の 3 つのタスクで構成されます。

1. アクションを適用するトラフィックを特定します。[P.18-3 の「クラスマップによるトラフィックの特定」](#)を参照。
2. アクションをトラフィックに適用します。[P.18-6 の「ポリシーマップによるアクションの定義」](#)を参照。
3. インターフェイスでアクションをアクティブにします。[P.18-10 の「サービス ポリシーによるインターフェイスへのポリシーの適用」](#)を参照。

## デフォルト グローバル ポリシー

デフォルトでは、すべてのデフォルト アプリケーション検査トラフィックに一致するポリシーがコンフィギュレーションに含まれ、すべての検査がすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。

デフォルト ポリシー コンフィギュレーションには、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
```

## クラスマップによるトラフィックの特定

クラスマップは、アクションを適用するトラフィックを特定します。クラスマップの最大数は、シングルモードで 255、またはマルチモードのコンテキストごとに 255 です。コンフィギュレーションには、デフォルト グローバル ポリシーでセキュリティ アプライアンスが使用するデフォルト クラスマップが含まれます。これは **inspection\_default** と呼ばれ、デフォルト検査トラフィックと一致します。

```
class-map inspection_default
  match default-inspection-traffic
```

クラスマップを定義するには、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、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** (オプション) 次のコマンドを入力して、クラスマップの説明を追加します。

```
hostname(config-cmap)# description string
```

**ステップ 3** 次の特性のいずれかと照合して、クラスに含めるトラフィックを定義します。特に指定がない場合、クラスマップに含めることができる **match** コマンドは 1 つだけです。

- 任意のトラフィック：クラスは、すべてのトラフィックと一致します。

```
hostname(config-cmap)# match any
```

- アクセスリスト：拡張アクセスリストで指定されたトラフィックとクラスを一致させることができます。セキュリティ アプライアンスが透過ファイアウォール モードで動作している場合は、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、[P.13-6 の「拡張アクセスリストの追加」](#)または [P.13-9 の「EtherType アクセスリストの追加」](#)を参照してください。

NAT を使用するアクセスリストの作成については、[P.13-3 の「NAT 使用時にアクセスリストで使用する IP アドレス」](#)を参照してください。

- TCP または UDP 宛先ポート：単一ポートまたは連続したポート範囲とクラスを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

複数の非連続ポートを使用するアプリケーションに対しては、**match access-list** コマンドを使用して、各ポートと一致する ACE を定義します。

指定できるポートのリストについては、[P.D-14 の「TCP ポートと UDP ポート」](#)を参照してください。

たとえば、ポート 80 の TCP パケット (HTTP) と一致させるには、次のコマンドを入力します。

```
hostname(config-cmap)# match tcp eq 80
```

- 検査のデフォルト トラフィック：デフォルトでセキュリティ アプライアンスが検査するトラフィックとクラスを一致させることができます。

```
hostname(config-cmap)# match default-inspection-traffic
```

**match default-inspection-traffic** コマンドは、デフォルトで検査するプロトコルとポートを指定します。デフォルト検査トラフィックのリストについては、『*Cisco Security Appliance Command Reference*』で、このコマンドを参照してください。セキュリティ アプライアンスにはデフォルト検査トラフィックと一致するデフォルト グローバル ポリシーが含まれ、すべてのインターフェイスのトラフィックに検査が適用されます。

**match access-list** コマンドを **match default-inspection-traffic** コマンドとともに指定すると、一致するトラフィックを絞り込むことができます。**match default-inspection-traffic** コマンドによって一致するポートが指定されるため、アクセスリストのポートはすべて無視されます。

- IP ヘッダーの DSCP 値：クラスは、8 個までの DSCP 値と一致します。

```
hostname(config-cmap)# match dscp value1 [value2] [...] [value8]
```

たとえば、次のように入力します。

```
hostname(config-cmap)# match dscp af43 cs1 ef
```

- 優先：クラスは、4 個までの優先値と一致します。優先値は、IP ヘッダーの TOS バイトで表します。

```
hostname(config-cmap)# match precedence value1 [value2] [value3] [value4]
```

*value1* ~ *value4* は 0 ~ 7 になります。この値は該当の優先順位に対応します。

- RTP トラフィック：クラスは、RTP トラフィックと一致します。

```
hostname(config-cmap)# match rtp starting_port range
```

*starting\_port* には、2000 ~ 65534 の偶数番号の UDP 宛先ポートを指定します。*range* には、*starting\_port* よりも上の追加の UDP ポートの数を 0 ~ 16383 で指定します。

- トンネルグループ トラフィック：QoS に適用するトンネルグループのトラフィックと一致します。

```
hostname(config-cmap)# match tunnel-group name
```

トラフィック照合を調整するために、**match** コマンドをもう 1 つ指定できます。上記のコマンドのいずれかを指定できますが、**match any**、**match access-list**、および **match default-inspection-traffic** コマンドは指定できません。次のコマンドを入力して、各フローをポリシングすることもできます。

```
hostname(config-cmap)# match flow ip destination address
```

一意の IP 宛先アドレスに向かうトラフィックは、すべてフローと見なされます。



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
```

## ポリシーマップによるアクションの定義

この項では、ポリシーマップを作成して、アクションをクラスマップに関連付ける方法について説明します。ここでは、次の項目について説明します。

- [ポリシーマップの概要 \(P.18-6\)](#)
- [デフォルト ポリシーマップ \(P.18-7\)](#)
- [ポリシーマップの追加 \(P.18-8\)](#)

### 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識別し、1 つ以上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、次のものがあります。

- IPS
- CSC
- TCP 正規化、TCP 接続および UDP 接続の制限値とタイムアウト、および TCP シーケンス番号のランダム化
- QoS ポリシング
- QoS プライオリティキュー
- アプリケーション検査

パケットは、各機能タイプのポリシーマップで、1 つのクラスマップにのみ一致します。パケットが機能タイプのクラスマップに一致した場合、セキュリティ アプライアンスは、その機能タイプの後続のクラスマップとは照合しません。ただし、パケットが別の機能タイプの後続のクラスマップと一致した場合、セキュリティ アプライアンスは、後続のクラスマップのアクションも適用します。

たとえば、パケットが接続制限値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 番目のクラスマップアクションは適用されません。

アクションは、機能に応じて双方向または単方向にトラフィックに適用されます。双方向に適用される機能の場合、トラフィックが両方向のクラスマップと一致した場合に、ポリシーマップを適用するインターフェイスを出入り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場合は、すべての機能が単方向です。単一インターフェイスに適用する場合に通常双方向の機能は、グローバルに適用される場合、各インターフェイスの入力にのみ適用されます。ポリシーはすべてのインターフェイスに適用されるため、ポリシーは両方向に適用され、この場合の双方向は冗長になります。

QoS など単方向に適用される機能の場合は、ポリシーマップを適用するインターフェイスを出るトラフィックだけが影響を受けます。各機能の方向については、[表 18-1](#) を参照してください。

表 18-1 機能の方向

| 機能                                                        | 単一インターフェイスでの方向 | グローバルでの方向 |
|-----------------------------------------------------------|----------------|-----------|
| TCP 正規化、TCP 接続および UDP 接続の制限値とタイムアウト、および TCP シーケンス番号のランダム化 | 双方向            | 入力        |
| CSC                                                       | 双方向            | 入力        |
| アプリケーション検査                                                | 双方向            | 入力        |
| IPS                                                       | 双方向            | 入力        |
| QoS ポリシング                                                 | 出力             | 出力        |
| QoS プライオリティキュー                                            | 出力             | 出力        |

ポリシーマップの各種のアクションが実行される順序は、ポリシーマップ中に出現する順序とは無関係です。アクションは次の順序で実行されます。

- TCP 正規化、TCP 接続および UDP 接続の制限値とタイムアウト、および TCP シーケンス番号のランダム化
- CSC
- アプリケーション検査
- IPS
- QoS ポリシング
- QoS プライオリティキュー

1 つのインターフェイスに割り当てることができるポリシーマップは 1 つだけですが、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はできます。

## デフォルト ポリシーマップ

コンフィギュレーションには、デフォルト グローバル ポリシーでセキュリティ アプライアンスが使用するデフォルト ポリシーマップが含まれます。これは **global\_policy** と呼ばれ、デフォルト検査トラフィックに対して検査を実行します。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。

デフォルト ポリシーマップ コンフィギュレーションには、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、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** (オプション) 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、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、[P.18-3 の「クラスマップによるトラフィックの特定」](#)を参照してください。

**ステップ 4** このクラスマップに、1 つ以上のアクションを指定します。

- IPS。 [P.19-3 の「AIP SSM へのトラフィックの誘導」](#)を参照してください。
- CSC。 [P.19-14 の「CSC SSM へのトラフィックの誘導」](#)を参照してください。
- TCP の正規化。 [P.20-2 の「TCP の正規化の設定」](#)を参照してください。
- TCP 接続および UDP 接続の制限値とタイムアウト、および TCP シーケンス番号のランダム化。 [P.20-5 の「接続の制限値とタイムアウトの設定」](#)を参照してください。
- QoS ポリシングと QoS プライオリティ。 [第 21 章「QoS ポリシーの適用」](#)を参照してください。
- アプリケーション検査。 [第 22 章「アプリケーション層プロトコル検査の設定」](#)を参照してください。



**(注)**

クラスマップに **match default\_inspection\_traffic** コマンドがない場合、そのクラスに最大 1 つの **inspect** コマンドを設定できます。

**ステップ 5** このポリシーマップに含めるクラスマップごとに、[ステップ 4](#)を繰り返します。

接続ポリシーの **policy-map** コマンドの例を次に示します。このコマンドは、Web サーバ 10.1.1.1 への接続許可数を制限します。

```
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
```

次の例は、ポリシーマップでの複数の照合の動作を示しています。

```
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-c)# class http_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

次の例は、トラフィックが最初の利用可能なクラスマップと一致した場合に、同じ機能ドメインのアクションが指定されている後続のクラスマップと照合されないことを示しています。

```
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-c)# 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-c)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

Telnet 接続は、開始時に **class telnet\_traffic** と一致します。同様に FTP 接続は、開始時に **class ftp\_traffic** と一致します。Telnet および FTP 以外の TCP 接続の場合は、**class tcp\_traffic** と一致します。Telnet 接続または FTP 接続は **class tcp\_traffic** と一致しますが、すでに他のクラスと一致しているため、セキュリティ アプライアンスはこの照合を行いません。

## サービス ポリシーによるインターフェイスへのポリシーの適用

ポリシーマップをアクティブにするには、1 つ以上のインターフェイスに適用するサービス ポリシー、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関連付けてサービス 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
```

デフォルトでは、すべてのデフォルト アプリケーション検査トラフィックに一致するグローバル ポリシーがコンフィギュレーションに含まれ、すべての検査がトラフィックにグローバルに適用されます。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。

デフォルト 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、次のコマンドは、外部インターフェイスで inbound\_policy ポリシーマップをイネーブルにします。

```
hostname(config)# service-policy inbound_policy interface outside
```

次のコマンドは、デフォルト グローバル ポリシーをディセーブルにし、他のすべてのセキュリティ アプライアンス インターフェイスで新しいポリシー new\_global\_policy 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

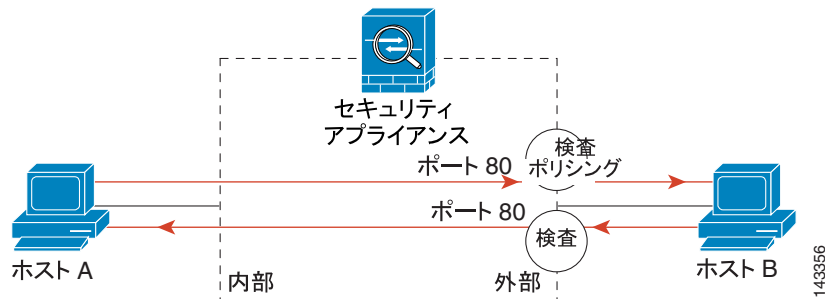
この項では、モジュラ ポリシー フレームワークの例をいくつか示します。次の事項を取り上げます。

- HTTP トラフィックへの検査と QoS ポリシングの適用 (P.18-11)
- HTTP トラフィックへの検査のグローバルな適用 (P.18-11)
- 特定のサーバへの HTTP トラフィックに対する検査と接続制限値の適用 (P.18-12)
- NAT による HTTP トラフィックへの検査の適用 (P.18-13)

### HTTP トラフィックへの検査と QoS ポリシングの適用

この例 (図 18-1) では、外部インターフェイスを通じてセキュリティ アプライアンスを出入りするすべての HTTP 接続 (ポート 80 の TCP トラフィック) が HTTP 検査対象として分類されます。外部インターフェイスを出るすべての HTTP トラフィックがポリシング対象として分類されます。

図 18-1 HTTP 検査と QoS ポリシング



この例について、次のコマンドを参照してください。

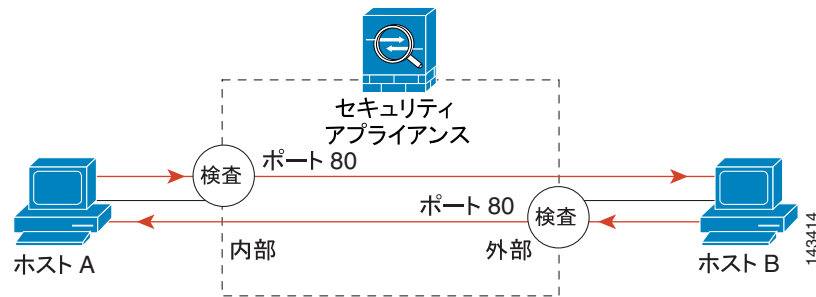
```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# police 250000
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 (図 18-2) では、任意のインターフェイスを通じてセキュリティ アプライアンスに入るすべての HTTP 接続 (ポート 80 の TCP トラフィック) が HTTP 検査対象として分類されます。このポリシーはグローバル ポリシーなので、検査が発生するのは各インターフェイスにトラフィックが入ったときだけです。

図 18-2 グローバル HTTP 検査



この例について、次のコマンドを参照してください。

```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

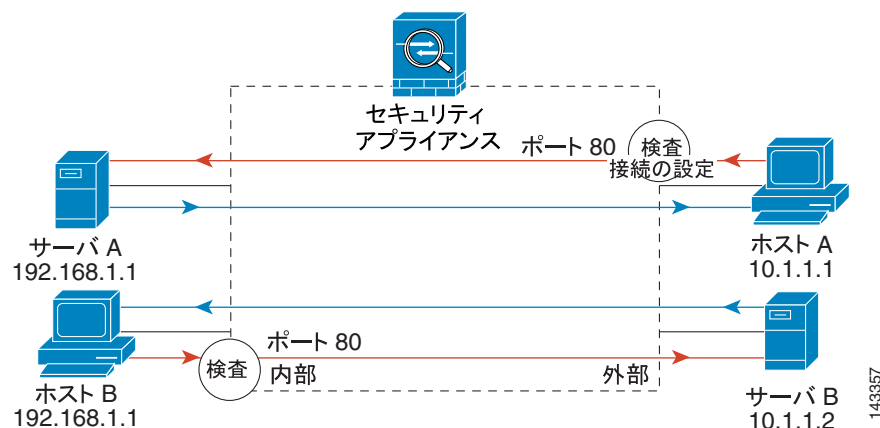
hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config)# service-policy http_traffic_policy global
```

## 特定のサーバへの HTTP トラフィックに対する検査と接続制限値の適用

この例 (図 18-3) では、外部インターフェイスを通じてセキュリティ アプライアンスに入るサーバ A 宛ての HTTP 接続 (ポート 80 の TCP トラフィック) が HTTP 検査および最大接続数制限値の対象として分類されます。サーバ A から発信されたホスト A への接続は、クラスマップのアクセスリストと照合しないので、影響を受けません。

内部インターフェイスを通じてセキュリティ アプライアンスに入るサーバ B 宛てのすべての HTTP 接続は、HTTP 検査対象として分類されます。サーバ B から発信されたホスト B への接続は、クラスマップのアクセスリストと照合しないので、影響を受けません。

図 18-3 特定のサーバに対する HTTP 検査と接続制限値





この例について、次のコマンドを参照してください。

```
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

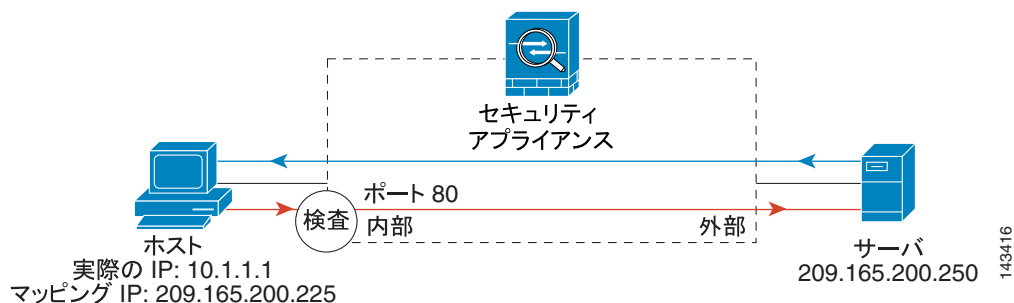
hostname(config)# policy-map policy_serverA
hostname(config-pmap)# class http_serverA
hostname(config-pmap-c)# inspect http http_map_serverA
hostname(config-pmap-c)# set connection conn-max 100
hostname(config)# policy-map policy_serverB
hostname(config-pmap)# class http_serverB
hostname(config-pmap-c)# inspect http http_map_serverB

hostname(config)# service-policy policy_serverB interface inside
hostname(config)# service-policy policy_serverA interface outside
```

## NAT による HTTP トラフィックへの検査の適用

この例では、ネットワーク内のホストに 2 つのアドレスがあります。1 つは、実際の IP アドレスの 10.1.1.1 です。もう 1 つは、外部ネットワークで使用するマッピング IP アドレスの 209.165.200.225 です。ポリシーは、実アドレスを使用する内部インターフェイスに適用されるため、クラスマップのアクセスリストでは、実際の IP アドレスを使用する必要があります。外部インターフェイスに適用する場合は、マッピングアドレスを使用します。

図 18-4 NAT による HTTP 検査



この例について、次のコマンドを参照してください。

```
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
```





# AIP SSM および CSC SSM の管理

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは、さまざまな SSM をサポートします。この章では、AIP SSM または CSC SSM をサポートするように適応型セキュリティ アプライアンスを設定する方法について説明します。また、これらの SSM にトラフィックを送信する方法についても取り上げます。

ASA 5000 シリーズ適応型セキュリティ アプライアンスの 4GE SSM については、[第 4 章「イーサネットとサブインターフェイスの設定」](#)を参照してください。



---

Cisco PIX 500 シリーズセキュリティ アプライアンスは、SSM をサポートしません。

---

次の事項について説明します。

- [AIP SSM の管理 \(P.19-2\)](#)
- [CSC SSM の管理 \(P.19-7\)](#)
- [SSM ステータスのチェック \(P.19-17\)](#)
- [SSM へのイメージの転送 \(P.19-18\)](#)

## AIP SSM の管理

ここでは、次の項目について説明します。

- [AIP SSM について \(P.19-2\)](#)
- [AIP SSM の準備 \(P.19-2\)](#)
- [AIP SSM へのトラフィックの誘導 \(P.19-3\)](#)
- [AIP SSM へのセッションの接続とセットアップの実行 \(P.19-5\)](#)

## AIP SSM について

ASA 5500 シリーズ適応型セキュリティ アプライアンスは、AIP SSM をサポートします。AIP SSM は、セキュリティ検査を強化する高度な IPS ソフトウェアを実行します。適応型セキュリティ アプライアンスは、他のファイアウォール ポリシーが適用された後、パケットが出力インターフェイスを出る直前（または、VPN 暗号化が設定されている場合は、VPN 暗号化が発生する直前）にパケットを AIP SSM に誘導します。たとえば、アクセスリストでブロックされたパケットは、AIP SSM に転送されません。

AIP SSM は、次の 2 つのモードのいずれかで動作できます。

- **インライン モード**：AIP SSM をトラフィック フローに直接配置します。すべてのトラフィックは、まず AIP SSM を通過し、検査されます。その後で、適応型セキュリティ アプライアンスを通過します。このモードは、すべてのパケットが通過前に分析されるため、最も安全です。また、AIP SSM はパケット単位のブロック ポリシーを実装できます。ただし、このモードは、スループットに影響を与えることがあります。このモードは、**ips** コマンドの **inline** キーワードを使用して指定します。
- **無差別モード**：トラフィックの重複ストリームを AIP SSM に送信します。このモードは安全性では劣りますが、トラフィックのスループットにほとんど影響を与えません。インライン モードの動作とは異なり、無差別モードで動作している SSM は、適応型セキュリティ アプライアンスにトラフィックを**排除**するように指示するか、適応型セキュリティ アプライアンス上の接続をリセットすることによってのみトラフィックをブロックできます。また、AIP SSM がトラフィックを分析している間、AIP SSM がブロックする前に、少量のトラフィックが適応型セキュリティ アプライアンスを通過することがあります。このモードは、**ips** コマンドの **inline** キーワードを使用して指定します。

ハードウェア障害やその他の原因で AIP SSM を使用できない場合に適応型セキュリティ アプライアンスがトラフィックを処理する方法を指定できます。この動作は、**ips** コマンドの 2 つのキーワードを使用して制御します。**fail-close** キーワードは、AIP SSM が使用できない場合はすべてのトラフィックをブロックするように、適応型セキュリティ アプライアンスを設定します。**fail-open** キーワードは、AIP SSM が使用できない場合はすべてのトラフィックを検査せずに通過させるように、適応型セキュリティ アプライアンスを設定します。

AIP SSM の動作モードの設定方法および AIP SSM セキュリティ アプライアンスによる障害時のトラフィック処理方法に関する詳細については、[P.19-3 の「AIP SSM へのトラフィックの誘導」](#)を参照してください。

## AIP SSM の準備

AIP SSM を設定するには、まず ASA 5500 シリーズ適応型セキュリティ アプライアンスを設定し、次に AIP SSM を設定します。

1. ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、AIP SSM に誘導するトラフィックを特定します ([P.19-3 の「AIP SSM へのトラフィックの誘導」](#)の説明を参照してください)。

2. AIP SSM では、検査と保護ポリシーを設定することにより、トラフィックの検査方法と侵入検出時の対処を決定します。AIP SSM 上で動作する IPS ソフトウェアは非常に強力であり、このマニュアルの範囲外です。そのため、詳細な設定情報については、以下に示す別のマニュアルを参照してください。

- [Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface](#)
- [Command Reference for Cisco Intrusion Prevention System](#)

## AIP SSM へのトラフィックの誘導

トラフィックを AIP SSM に誘導するように適応型セキュリティ アプライアンスを設定するには、MPF コマンドを使用します。その設定を適応型セキュリティ アプライアンスに行う前に、[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。MPF の概念と一般的なコマンドの概要が説明されています。

適応型セキュリティ アプライアンスから AIP SSM に誘導するトラフィックを特定するには、次の手順を実行します。

- 
- ステップ 1** すべてのトラフィックが一致するアクセスリストを次のように作成します。

```
hostname(config)# access-list acl-name permit ip any any
```

- ステップ 2** AIP SSM に誘導するトラフィックを特定するクラスマップを作成します。これを行うには、**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* には、トラフィック クラスの名前を指定します。**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 モードに移行します。

- ステップ 3** **match access-list** コマンドを [ステップ 1](#) で作成したアクセスリストとともに使用して、スキャンするトラフィックを特定します。

```
hostname(config-cmap)# match access-list acl-name
```

- ステップ 4** AIP SSM へのトラフィックの送信に使用するポリシーマップを作成するか、既存のポリシーマップを修正します。これを行うには、**policy-map** コマンドを使用します。

```
hostname(config-cmap)# policy-map policy_map_name  
hostname(config-pmap)#
```

*policy\_map\_name* には、ポリシーマップの名前を指定します。CLI はポリシーマップ コンフィギュレーション モードに移行し、それに応じてプロンプトが変化します。

- ステップ 5** [ステップ 2](#) で作成した、スキャンするトラフィックを特定するクラスマップを指定します。これを行うには、**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* には、[ステップ 2](#) で作成したクラスマップの名前を指定します。CLI はポリシーマップ クラス コンフィギュレーション モードに移行し、それに応じてプロンプトが変化します。

- ステップ 6** クラスマップによって特定されているトラフィックを、AIP SSM に送信するトラフィックとして割り当てます。これを行うには、**ips** コマンドを次のように使用します。

```
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close | fail-open}
```

**inline** キーワードおよび **promiscuous** キーワードは、AIP SSM の動作モードを制御します。**fail-close** キーワードおよび **fail-open** キーワードは、AIP SSM が使用できない場合に適応型セキュリティ アプライアンスがトラフィックを処理する方法を制御します。動作モードと障害時の動作の詳細については、[P.19-2 の「AIP SSM について」](#)を参照してください。

- ステップ 7** **service-policy** コマンドを次のように使用して、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-pmap-c)# service-policy policy_map_name [global | interface interface_ID]
hostname(config)#
```

**policy\_map\_name** には、[ステップ 4](#)で作成したポリシーマップを指定します。ポリシーマップをすべてのインターフェイスのトラフィックに適用する場合は、**global** キーワードを使用します。ポリシーマップを特定のインターフェイスのトラフィックに適用する場合は、**interface interface\_ID** オプションを使用します。**interface\_ID** には、**nameif** コマンドでインターフェイスに割り当てた名前を指定します。

グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを 1 つだけ適用できます。

適応型セキュリティ アプライアンスは、指定内容に従ってトラフィックを AIP SSM に誘導し始めます。

次の例では、すべての IP トラフィックが AIP SSM に無差別モードで誘導され、何らかの理由で AIP SSM カードに障害が発生した場合にすべての IP トラフィックがブロックされます。

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ids-policy
hostname(config-pmap-c)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

## AIP SSM へのセッションの接続とセットアップの実行

トラフィックを AIP SSM に誘導するように ASA 5500 シリーズ適応型セキュリティ アプライアンスを設定した後、AIP SSM にセッションを接続し、初期コンフィギュレーション用のセットアップユーティリティを実行します。

**(注)**

(**session 1** コマンドを使用して)適応型セキュリティ アプライアンスから SSM にセッションを接続することも、管理インターフェイスで SSH または Telnet を使用して SSM に直接接続することもできます。あるいは、ASDM を使用することもできます。

適応型セキュリティ アプライアンスから AIP SSM にセッションを接続するには、次の手順を実行します。

- ステップ 1** **session 1** コマンドを入力して、ASA 5500 シリーズ適応型セキュリティ アプライアンスから AIP SSM にセッションを接続します。

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

- ステップ 2** ユーザ名とパスワードを入力します。デフォルトのユーザ名とパスワードは、どちらも **cisco** です。

**(注)**

初めて AIP SSM にログインしたときに、デフォルト パスワードの変更を要求するプロンプトが表示されます。パスワードは 8 文字以上で、辞書に載っていない単語にする必要があります。

```
login: cisco
Password:
Last login: Fri Sep  2 06:21:20 from xxx.xxx.xxx.xxx
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
AIP SSM#
```

**(注)**

上記のライセンスの注意が表示された場合(一部のソフトウェアバージョンでのみ表示されます)、AIP SSM でシグニチャ ファイルをアップグレードする必要がなければ、無視してかまいません。有効なライセンス キーがインストールされるまで、AIP SSM は現在のシグニチャ レベルで動作し続けます。ライセンス キーは後でインストールできます。ライセンス キーは、AIP SSM の現在の機能に影響を与えません。

**ステップ 3** **setup** コマンドを入力して、AIP SSM の初期コンフィギュレーション用のセットアップ ユーティリティを実行します。

AIP SSM# **setup**

これで、侵入防御のために AIP SSM を設定する準備ができました。AIP SSM の設定情報については、次のマニュアルを参照してください。

- [Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface](#)
- [Command Reference for Cisco Intrusion Prevention System](#)



## CSC SSM の管理

ここでは、次の項目について説明します。

- [CSC SSM について \(P.19-7\)](#)
- [CSC SSM の準備 \(P.19-9\)](#)
- [スキャンするトラフィックの指定 \(P.19-11\)](#)
- [CSC SSM を通過する接続の制限 \(P.19-13\)](#)
- [CSC SSM へのトラフィックの誘導 \(P.19-14\)](#)

## CSC SSM について

ASA 5500 シリーズ適応型セキュリティ アプライアンスは、CSC SSM をサポートします。CSC SSM は、Content Security and Control ソフトウェアを実行します。CSC SSM により、ウイルス、スパイウェア、スパム、およびその他の不要トラフィックから保護されます。これは、FTP、HTTP、POP3、および SMTP トラフィックをスキャンすることで実現されます。そのためには、これらのトラフィックを CSC SSM に送信するように適応型セキュリティ アプライアンスを設定しておきます。

図 19-1 は、次の構成のセキュリティ アプライアンスを通過するトラフィックのフローを示しています。

- CSC SSM がインストール、設定されている。
- どのトラフィックを SSM に誘導し、スキャンするかを指定するサービス ポリシーがある。

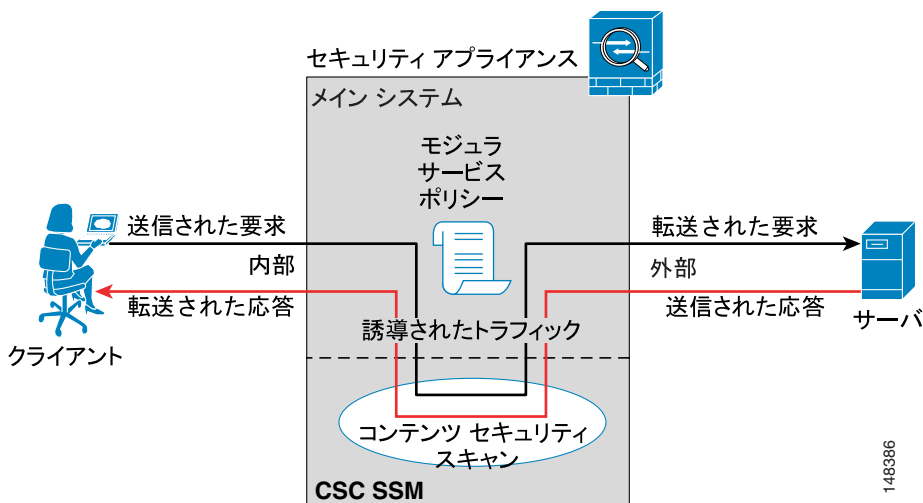
この例では、クライアントのネットワーク ユーザは、Web サイトにアクセスしているか、FTP サーバからファイルをダウンロードしているか、POP3 サーバから電子メールを取得している可能性があります。SMTP スキャンは、適応型セキュリティ アプライアンスによって保護された SMTP サーバに向けて外部から送信されたトラフィックをスキャンするように、適応型セキュリティ アプライアンスを設定する必要がある点で異なります。



(注)

CSC SSM は、適応型セキュリティ アプライアンスで FTP 検査がイネーブルの場合に限り、FTP ファイル転送をスキャンします。デフォルトでは、FTP 検査はイネーブルです。

図 19-1 CSC SSM でスキャンされるトラフィックのフロー



システムの設定と CSC SSM の監視には、ASDM を使用します。CSC SSM ソフトウェアのコンテンツ セキュリティ ポリシーに高度な設定を行うには、ASDM でリンクをクリックして、CSC SSM の Web ベース GUI にアクセスします。CSC SSM GUI の使用方法については、『Cisco Content Security and Control SSM Administrator Guide』を参照してください。



(注)

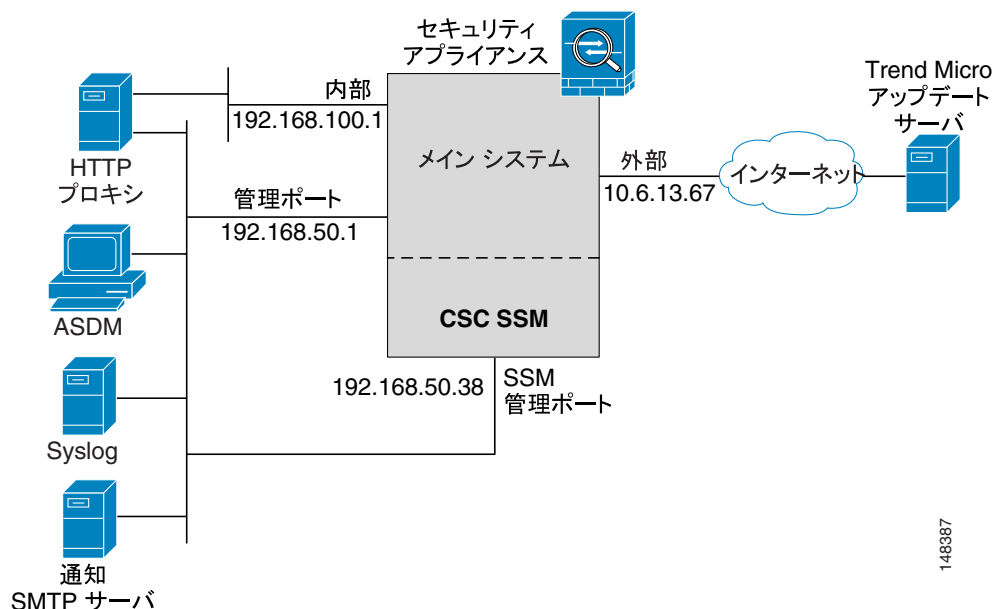
ASDM と CSC SSM では、別個のパスワードが保持されています。それらのパスワードを同一にすることはできますが、2つのパスワードのうち一方を変更しても、もう一方に影響することはありません。

ASDM を実行しているホストと適応型セキュリティ アプライアンスの間の接続は、適応型セキュリティ アプライアンスの管理ポートを通じて確立されます。CSC SSM GUI への接続は、SSM の管理ポートを通じて確立されます。これら 2つの接続は CSC SSM の管理に必要であるため、ASDM を実行しているすべてのホストは適応型セキュリティ アプライアンスの管理ポートと SSM の管理ポートの両方の IP アドレスに到達できる必要があります。

図 19-2 に、専用の管理ネットワークに接続されている CSC SSM を持つ適応型セキュリティ アプライアンスを示します。専用の管理ネットワークの使用は必須ではありませんが、使用することをお勧めします。図 19-2 で特に重要な点は次のとおりです。

- HTTP プロキシ サーバが内部ネットワークと管理ネットワークに接続されている。これにより、CSC SSM は Trend Micro アップデート サーバに接続できます。
- 適応型セキュリティ アプライアンスの管理ポートが管理ネットワークに接続されている。適応型セキュリティ アプライアンスと CSC SSM の管理を可能にするには、ASDM を実行しているホストは管理ネットワークに接続されている必要があります。
- 管理ネットワーク内には、CSC SSM への電子メール通知に使用される SMTP サーバと、CSC SSM が syslog メッセージを送信できる syslog サーバがある。

図 19-2 管理ネットワークを備えた CSC SSM 構成



148387

CSC SSM は、ステートフル フェールオーバーをサポートできません。これは、CSC SSM は接続情報を保持せず、ステートフル フェールオーバーに必要な情報をフェールオーバー装置に提供できないためです。CSC SSM でスキャン中の接続は、その CSC SSM がインストールされているセキュリティ アプライアンスに障害が発生するとドロップされます。スタンバイの適応型セキュリティ アプライアンスがアクティブになると、スキャンされるトラフィックは CSC SSM に転送され、接続はリセットされます。

## CSC SSM の準備

CSC SSM のセキュリティ効果を得るには、SSM のハードウェア インストールだけでなく、他にもいくつかのステップを実行する必要があります。次の手順では、それらのステップの概要を示します。

適応型セキュリティ アプライアンスおよび CSC SSM を設定するには、次の手順を実行します。

**ステップ 1** CSC SSM が Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスにプレインストールされていない場合は、インストールし、ネットワーク ケーブルを SSM の管理ポートに接続します。SSM のインストールと接続については、『[Cisco ASA 5500 Series Hardware Installation Guide](#)』を参照してください。

CSC SSM ソフトウェアの管理と自動アップデートを可能にするには、CSC SSM の管理ポートがネットワークに接続されている必要があります。また、CSC SSM は、電子メール通知と syslog ロギングにも管理ポートを使用します。

**ステップ 2** CSC SSM には、Product Authorization Key (PAK) が付属しています。PAK を使用して、次の URL で CSC SSM を登録します。

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

登録すると、アクティベーション キーが電子メールで届きます。**ステップ 6** を完了するには、アクティベーション キーが必要です。

**ステップ 3** **ステップ 6** で必要となる次の情報を収集します。

- **ステップ 2** を完了した後に受信したアクティベーション キー
- SSM 管理ポートの IP アドレス、ネットマスク、およびゲートウェイ IP アドレス



(注)

SSM 管理ポートの IP アドレスは、ASDM の実行に使用するホストがアクセスできるものである必要があります。SSM 管理ポートの IP アドレスと適応型セキュリティ アプライアンス管理インターフェイスの IP アドレスは、異なるサブネットに属していてもかまいません。

- DNS サーバの IP アドレス
- HTTP プロキシ サーバの IP アドレス（セキュリティ ポリシーで、インターネットへの HTTP アクセスにプロキシ サーバの使用が求められている場合に限り必要）
- SSM のドメイン名とホスト名
- 電子メール通知に使用する、電子メール アドレスおよび SMTP サーバの IP アドレスとポート番号
- CSC SSM を管理できるホストまたはネットワークの IP アドレス

- CSC SSM 用のパスワード

**ステップ 4** Web ブラウザで、CSC SSM がインストールされている適応型セキュリティ アプライアンスの ASDM にアクセスします。



**(注)** 初めて ASDM にアクセスする場合は、『[Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide](#)』の Startup Wizard の説明を参照してください。

ASDM アクセスをイネーブルにする方法の詳細については、[P.33-5](#) の「[ASDM の HTTPS アクセスの許可](#)」を参照してください。

**ステップ 5** 適応型セキュリティ アプライアンス上の時刻設定を確認します。時刻設定が正確であることは、セキュリティ イベントのロギングや CSC SSM ソフトウェアの自動アップデートで重要です。

- 時刻設定を手動で制御する場合は、時間帯を含むクロック設定を確認します。**Configuration > Properties > Device Administration > Clock** を選択します。
- NTP を使用している場合は、NTP 設定を確認します。**Configuration > Properties > Device Administration > NTP** を選択します。

**ステップ 6** ASDM で、Content Security セットアップ ウィザードを実行します。これを行うには、サポートされる Web ブラウザで ASDM GUI にアクセスし、Home ページの **Content Security** タブをクリックします。Content Security セットアップ ウィザードが実行されます。Content Security セットアップ ウィザードについては、**Help** ボタンをクリックしてください。



**(注)** 初めて ASDM にアクセスする場合は、『[Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide](#)』のスタートアップ ウィザードの説明を参照してください。

**ステップ 7** ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、CSC SSM に誘導するトラフィックを特定します ([P.19-14](#) の「[CSC SSM へのトラフィックの誘導](#)」の説明を参照してください)。

**ステップ 8** (オプション) CSC SSM GUI で、デフォルトのコンテンツ セキュリティ ポリシーを確認します。デフォルトのコンテンツ セキュリティ ポリシーは、ほとんどの実装に適しています。このポリシーの修正は高度な設定であるため、必ず『[Cisco Content Security and Control SSM Administrator Guide](#)』を読んでから実行してください。

コンテンツ セキュリティ ポリシーを確認するには、イネーブルになっている機能を CSC SSM GUI で表示します。使用できる機能は、購入したライセンス レベルによって異なります。デフォルトでは、購入したライセンスに含まれているすべての機能がイネーブルです。

基本ライセンスの場合、デフォルトでイネーブルになっている機能は、SMTP ウイルス スキャン、POP3 のウイルス スキャンとコンテンツ フィルタリング、Web メール ウイルス スキャン、HTTP ファイル ブロッキング、FTP のウイルス スキャンとファイル ブロッキング、および自動アップデートです。

Plus ライセンスのデフォルトでイネーブルになっている追加機能は、SMTP アンチスパム、SMTP コンテンツ フィルタリング、POP3 アンチスパム、URL ブロッキング、および URL フィルタリングです。

CSC SSM GUI にアクセスするには、ASDM で **Configuration > Trend Micro Content Security** を選択し、次のいずれかを選択します。**Web**、**Mail**、**File Transfer**、または **Updates**。これらのペインにある、「Configure」という単語で始まる青色のリンクをクリックすると、CSC SSM GUI が開きます。

## スキャンするトラフィックの指定

CSC SSM は、FTP、HTTP、POP3、および SMTP トラフィックをスキャンできます。これらのプロトコルは、接続要求パケットの宛先ポートがそのプロトコルの予約済みポートである場合に限りサポートされます。つまり、CSC SSM がスキャンできる接続は次のものに限られます。

- TCP ポート 21 に対して開かれた FTP 接続
- TCP ポート 80 に対して開かれた HTTP 接続
- TCP ポート 110 に対して開かれた POP3 接続
- TCP ポート 25 に対して開かれた SMTP 接続

これらすべてのプロトコルのトラフィックをスキャンすることも、任意の組み合わせをスキャンすることもできます。たとえば、ネットワーク ユーザに POP3 電子メールの受信を許可しない場合に、POP3 トラフィックを CSC SSM に誘導するように適応型セキュリティ アプライアンスを設定する必要はありません（POP3 トラフィックをブロックするように設定できます）。

適応型セキュリティ アプライアンスと CSC SSM のパフォーマンスを最大化するには、CSC SSM でスキャンするトラフィックだけを CSC SSM に誘導します。信頼できる送信元と宛先の間のトラフィックなど、スキャンする必要のないトラフィックまでも誘導すると、ネットワーク パフォーマンスに悪影響を与える可能性があります。

CSC SSM でトラフィックをスキャンするアクションは、**csc** コマンドを使用してイネーブルにします。このコマンドは、サービス ポリシーに含める必要があります。サービス ポリシーはグローバルに適用することも、特定のインターフェイスに適用することもできるため、**csc** コマンドについても、グローバルにイネーブルにするか、特定のインターフェイスに対してイネーブルにするかを選択できます。

**csc** コマンドをグローバル ポリシーに追加した場合、適応型セキュリティ アプライアンスを通過する暗号化されていないすべての接続は、確実に CSC SSM でスキャンされます。ただし、信頼できる送信元からのトラフィックが不必要にスキャンされることになる場合もあります。

**csc** コマンドをインターフェイス固有のサービス ポリシーでイネーブルにした場合、このコマンドは双方向性を持ちます。つまり、適応型セキュリティ アプライアンスが新しい接続を開くとき、その接続の着信インターフェイスまたは発信インターフェイスのいずれかで **csc** コマンドがアクティブで、ポリシーのクラスマップでスキャン対象のトラフィックが特定されていれば、適応型セキュリティ アプライアンスはそのトラフィックを CSC SSM に誘導します。

ただし、双方向性があることにより、特定のインターフェイスを通過するサポート対象のトラフィック タイプを CSC SSM に誘導した場合に、信頼できる内部ネットワークからのトラフィックに対して CSC SSM が不必要なスキャンを実行することになる可能性があります。たとえば、DMZ ネットワークの Web サーバから要求された URL およびファイルが内部ネットワークのホストに対してコンテンツ セキュリティ リスクをもたらす可能性は低いいため、そのようなトラフィックを適応型セキュリティ アプライアンスで CSC SSM に誘導する必要はほとんどありません。

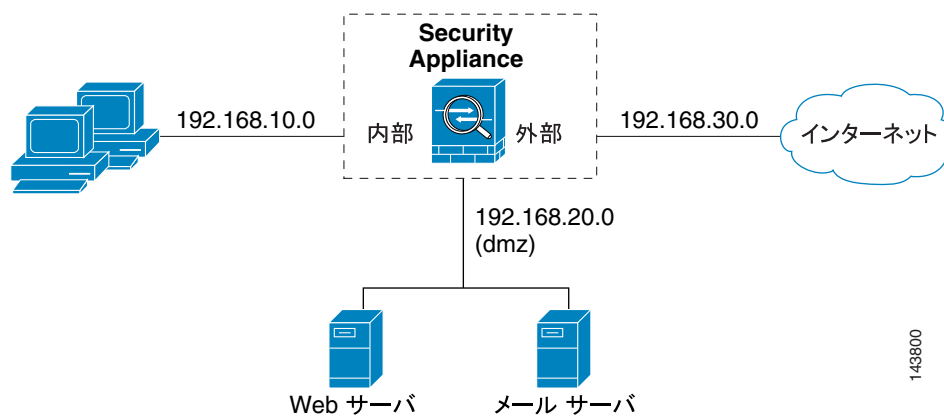
したがって、アクセスリストを使用して、CSC SSM サービス ポリシーのクラスマップによって選択されたトラフィックをさらに制限することを強くお勧めします。特に、次の接続と一致するアクセスリストを使用することをお勧めします。

- 外部ネットワークへの HTTP 接続

- 適応型セキュリティ アプライアンスの内部のクライアントから適応型セキュリティ アプライアンスの外部のサーバへの FTP 接続
- セキュリティ アプライアンスの内部のクライアントから適応型セキュリティ アプライアンスの外部のサーバへの POP3 接続
- 内部メール サーバを宛先とする着信 SMTP 接続

図 19-3 では、適応型セキュリティ アプライアンスは、CSC SSM にトラフィックを誘導するように設定されています。内部ネットワークのクライアントから外部ネットワークへの HTTP、FTP、および POP3 接続要求、および外部ホストから DMZ ネットワークのメール サーバへの着信 SMTP 接続要求が誘導されます。内部ネットワークから DMZ ネットワークの Web サーバへの HTTP 要求はスキャンされません。

図 19-3 CSC SSM スキャンの一般的なネットワーク構成



スキャンするトラフィックを特定するように適応型セキュリティ アプライアンスを設定する方法は多数あります。その 1 つは、内部インターフェイスに対するサービス ポリシーと外部インターフェイスに対するサービス ポリシーの 2 つのサービス ポリシーを定義することです。各サービス ポリシーには、スキャンするトラフィックと一致するアクセスリストを含めます。内部インターフェイスに適用するポリシーでは、次のアクセスリストを使用できます。

```

access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110
  
```

前述のとおり、**csc** コマンドを特定のインターフェイスに適用するポリシーは入力トラフィックと出力トラフィックの両方に対して有効ですが、**csc\_out** アクセスリストで 192.168.10.0 を送信元ネットワークとして指定することにより、内部インターフェイスに適用されたポリシーは、内部ネットワークのホストによって開始された接続のみと一致するようになります。アクセスリストの 2 つ目の ACE では、**deny** キーワードが使用されています。この ACE は、192.168.10.0 ネットワークから 192.168.20.0 ネットワークの TCP ポート 80 に送信されたトラフィックを適応型セキュリティ アプライアンスがブロックするという意味ではありません。これは単に、このトラフィックをポリシーマップによる照合から免除することで、適応型セキュリティ アプライアンスがこのトラフィックを CSC SSM に送信できないようにするという意味です。



アクセスリストで deny 文を使用すると、信頼できる外部ホストとの接続をスキャンから免除できます。たとえば、CSC SSM の負荷を軽減するために、既知の信頼できるサイトへの HTTP トラフィックを免除できます。そのようなサイトにある Web サーバが IP アドレス 209.165.201.7 を持つ場合、次の ACE を csc\_out アクセスリストに追加すると、信頼できる外部 Web サーバと内部ホストの間の HTTP 接続を CSC SSM によるスキャンから除外できます。

```
access-list csc_out deny tcp 192.168.10.0 255.255.255.0 209.165.201.7 255.255.255.255 eq 80
```

この例の 2 つ目のポリシー（外部インターフェイスに適用される）は、次のアクセスリストを使用します。

```
access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
```

このアクセスリストは、任意の外部ホストから DMZ ネットワークの任意のホストへの着信 SMTP 接続を照合します。したがって、外部インターフェイスに適用されるポリシーにより、着信 SMTP 電子メールは確実に CSC SSM に誘導され、スキャンされます。内部ネットワークのホストから DMZ ネットワークのメールサーバへの SMTP 接続は、外部インターフェイスを使用しないため照合されません。

DMZ ネットワークの Web サーバが、外部ホストから HTTP でアップロードされたファイルを受信する場合、次の ACE を csc\_in アクセスリストに追加すると、CSC SSM を使用して Web サーバを感染ファイルから保護できます。

```
access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80
```

この項のアクセスリストを使用するサービス ポリシー コンフィギュレーションの完全な例については、[例 19-1](#) を参照してください。

## CSC SSM を通過する接続の制限

適応型セキュリティ アプライアンスは、CSC SSM と、CSC SSM がスキャンする接続の宛先が必要以上の接続要求を受け入れないようにできます。さらには、受信しないようにすることもできます。これは、初期接続に対しても、完全に確立された接続に対しても可能です。また、class-map 制限および per-client 制限に含まれているすべてのクライアントに対して制限値を指定することもできます。初期接続または完全に確立された接続に対する制限を設定するには、**set connection** コマンドを使用します。

また、class-map 制限および per-client 制限に含まれているすべてのクライアントに対して制限値を指定することもできます。**per-client-embryonic-max** パラメータおよび **per-client-max** パラメータは、個々のクライアントが開くことのできる接続の最大数を制限します。あるクライアントが必要以上のネットワーク リソースを同時に使用する場合、これらのパラメータを使用すると、適応型セキュリティ アプライアンスが各クライアントに許可する接続数を制限できます。

DoS 攻撃（サービス拒絶攻撃）の目的は、接続や接続要求で主要ホストの容量を圧迫することにより、ネットワークを混乱させることです。**set connection** コマンドは、DoS 攻撃を阻止するために使用できます。攻撃対象となる可能性のあるホストがサポートできる per-client 最大値を設定すると、悪意のあるクライアントは、保護されたネットワークのホストを圧迫できなくなります。

**set connection** コマンドを使用して、CSC SSM と、CSC SSM がスキャンする接続の宛先を保護する方法については、[P.19-14](#) の「CSC SSM へのトラフィックの誘導」を参照してください。

## CSC SSM へのトラフィックの誘導

トラフィックを CSC SSM に誘導するように適応型セキュリティ アプライアンスを設定するには、MPF コマンドを使用します。その設定を適応型セキュリティ アプライアンスに行う前に、[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。MPF の概念と一般的なコマンドの概要が説明されています。

適応型セキュリティ アプライアンスから CSC SSM に誘導するトラフィックを特定するには、次の手順を実行します。

**ステップ 1** CSC SSM でスキャンするトラフィックと一致するアクセスリストを作成します。これを行うには、**access-list extended** コマンドを使用します。すべてのトラフィックを一致させるのに必要な数の ACE を作成します。たとえば、FTP、HTTP、POP3、および SMTP トラフィックを指定する場合、4 つの ACE が必要です。スキャンするトラフィックを特定する方法については、[P.19-11 の「スキャンするトラフィックの指定」](#)を参照してください。

**ステップ 2** CSC SSM に誘導するトラフィックを特定するクラスマップを作成します。これを行うには、**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* には、トラフィック クラスの名前を指定します。**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 モードに移行します。

**ステップ 3** **match access-list** コマンドを [ステップ 1](#) で作成したアクセスリストとともに使用して、スキャンするトラフィックを特定します。

```
hostname(config-cmap)# match access-list acl-name
```

**ステップ 4** CSC SSM へのトラフィックの送信に使用するポリシーマップを作成するか、既存のポリシーマップを修正します。これを行うには、**policy-map** コマンドを使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

*policy\_map\_name* には、ポリシーマップの名前を指定します。CLI はポリシーマップ コンフィギュレーション モードに移行し、それに応じてプロンプトが変化します。

**ステップ 5** [ステップ 2](#) で作成した、スキャンするトラフィックを特定するクラスマップを指定します。これを行うには、**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* には、[ステップ 2](#) で作成したクラスマップの名前を指定します。CLI はポリシーマップ クラス コンフィギュレーション モードに移行し、それに応じてプロンプトが変化します。



- ステップ 6** 適応型セキュリティ アプライアンスが CSC SSM に誘導する同時接続の per-client 制限を適用する場合は、**set connection** コマンドを次のように設定します。

```
hostname(config-pmap-c)# set connection per-client-max n
```

*n* には、適応型セキュリティ アプライアンスがクライアントごとに許可する最大同時接続数を指定します。これを指定すると、1つのクライアントが CSC SSM のサービスや SSM で保護されたサーバを必要以上に使用することはできなくなります。また、CSC SSM が保護する HTTP、FTP、POP3、および SMTP の各サーバに対する DoS 攻撃の試みも阻止されます。

- ステップ 7** クラスマップによって特定されているトラフィックを、CSC SSM に送信されるトラフィックとして割り当てます。これを行うには、**csc** コマンドを次のように使用します。

```
hostname(config-pmap-c)# csc {fail-close | fail-open}
```

**fail-close** キーワードおよび **fail-open** キーワードは、CSC SSM が使用できない場合に適応型セキュリティ アプライアンスがトラフィックを処理する方法を制御します。動作モードと障害時の動作の詳細については、[P.19-7 の「CSC SSM について」](#)を参照してください。

- ステップ 8** **service-policy** コマンドを次のように使用して、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-pmap-c)# service-policy policy_map_name [global | interface
interface_ID]
hostname(config)#
```

*policy\_map\_name* には、[ステップ 4](#) で作成したポリシーマップを指定します。ポリシーマップをすべてのインターフェイスのトラフィックに適用する場合は、**global** キーワードを使用します。ポリシーマップを特定のインターフェイスのトラフィックに適用する場合は、**interface interface\_ID** オプションを使用します。*interface\_ID* には、**nameif** コマンドでインターフェイスに割り当てた名前を指定します。

グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを 1 つだけ適用できます。

適応型セキュリティ アプライアンスは、指定内容に従ってトラフィックを CSC SSM に誘導し始めます。

**例 19-1** は、[図 19-3](#) で示したネットワークに基づいています。この例では、2つのサービス ポリシーが作成されています。1つ目のポリシーの *csc\_out\_policy* は、内部インターフェイスに適用されるもので、*csc\_out* アクセスリストを使用して、すべての発信 FTP 要求および発信 POP3 要求がスキャンされることを確実にします。*csc\_out* アクセスリストも、内部から外部インターフェイス上のネットワークへの HTTP 接続がスキャンされることを確実にしますが、deny ACE が含まれているため、内部から DMZ ネットワークのサーバへの HTTP 接続は除外されます。

2つ目のポリシーの *csc\_in\_policy* は、外部インターフェイスに適用されるもので、*csc\_in* アクセスリストを使用して、外部インターフェイスで発信され、DMZ ネットワークを宛先とする SMTP 要求および HTTP 要求が CSC SSM でスキャンされることを確実にします。HTTP 要求のスキャンにより、Web サーバは HTTP ファイルのアップロードから保護されます。

**例 19-1 一般的な CSC SSM スキャン シナリオのサービス ポリシー**

```

hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
hostname(config)# access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110

hostname(config)# class-map csc_outbound_class
hostname(config-cmap)# match access-list csc_out

hostname(config)# policy-map csc_out_policy
hostname(config-pmap)# class csc_outbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config)# service-policy csc_out_policy interface inside

hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80

hostname(config)# class-map csc_inbound_class
hostname(config-cmap)# match access-list csc_in

hostname(config)# policy-map csc_in_policy
hostname(config-pmap)# class csc_inbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config)# service-policy csc_in_policy interface outside

```

**(注)**

FTP で転送されるファイルをスキャンするには、FTP 検査が CSC SSM に対してイネーブルになっている必要があります。デフォルトでは、FTP 検査はイネーブルです。

## SSM ステータスのチェック

SSM のステータスをチェックするには、**show module** コマンドを使用します。

次に示す出力例は、CSC SSM がインストールされた適応型セキュリティ アプライアンスからのものです。Status フィールドには、SSM の動作ステータスが示されています。正常に動作している SSM は、**show module** コマンドの出力で「Up」というステータスで示されます。適応型セキュリティ アプライアンスがアプリケーション イメージを SSM に転送している間は、出力の Status フィールドに「Recover」と示されます。各種ステータスの詳細については、『[Cisco Security Appliance Command Reference](#)』の **show module** コマンドの項を参照してください。

```
hostname# show module 1
Mod Card Type                               Model                Serial No.
-----
 1 ASA 5500 Series Security Services Module-20 ASA-SSM-20          JAB100301NE

Mod MAC Address Range                       Hw Version          Fw Version          Sw Version
-----
 1 0015.c6fa.2c0f to 0015.c6fa.2c0f 1.0                1.0(10)0           CSC SSM 6.0 (Build#1349)

Mod SSM Application Name                    Status              SSM Application Version
-----
 1 CSC SSM                                Down                6.0 (Build#1349)

Mod Status                                Data Plane Status    Compatibility
-----
 1 Up                                    Up
```

コマンドの末尾の引数 **1** は、SSM 専用のスロット番号です。スロット番号がわからない場合は、それを省略すると、適応型セキュリティ アプライアンスを含むすべてのモジュールの情報が表示されます。適応型セキュリティ アプライアンス専用のスロットは、スロット 0（ゼロ）であると見なされます。

details キーワードを使用すると、SSM の追加情報を表示できます。

次に示す出力例は、CSC SSM がインストールされた適応型セキュリティ アプライアンスからのものです。

```
hostname# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:                ASA-SSM-20
Hardware version:     1.0
Serial Number:        JAB100301NE
Firmware version:     1.0(10)0
Software version:     CSC SSM 6.0 (Build#1349)
MAC Address Range:    0015.c6fa.2c0f to 0015.c6fa.2c0f
App. name:            CSC SSM
App. Status:          Up
App. Status Desc:     CSC SSM scan services are available
App. version:         6.0 (Build#1349)
Data plane Status:    Up
Status:               Up
HTTP Service:         Up
Mail Service:         Up
FTP Service:          Up
Activated:            Yes
Mgmt IP addr:         10.23.62.92
Mgmt web port:        8443
Peer IP addr:         <not enabled>
```

## SSM へのイメージの転送

AIP SSM や CSC SSM などのインテリジェント SSM の場合、アプリケーション イメージを TFTP サーバから SSM に転送できます。このプロセスでは、アップグレード イメージと保守イメージがサポートされます。



(注)

SSM のアプリケーションをアップグレードする場合、SSM アプリケーションによっては、コンフィギュレーションのバックアップがサポートされることがあります。SSM アプリケーションのコンフィギュレーションをバックアップしないと、イメージを SSM に転送したときにコンフィギュレーションは失われます。SSM によるバックアップのサポートの詳細については、ご使用の SSM のマニュアルを参照してください。

イメージをインテリジェント SSM に転送するには、次の手順を実行します。

**ステップ 1** SSM のリカバリ コンフィギュレーションを作成または修正します。これを行うには、次の手順を実行します。

- a. SSM のリカバリ コンフィギュレーションが存在するかどうかを確認します。これを行うには、**show module** コマンドを **recover** キーワードとともに次のように使用します。

```
hostname# show module slot recover
```

*slot* には、SSM 専用のスロット番号を指定します。

**recover** キーワードが無効な場合、リカバリ コンフィギュレーションは存在しません。**show module** コマンドの **recover** キーワードは、SSM のリカバリ コンフィギュレーションが存在する場合に限り使用できます。



(注)

適応型セキュリティ アプライアンスがマルチコンテキスト モードで動作している場合、**configure** キーワードは、システム コンテキストのみで使用できます。

SSM のリカバリ コンフィギュレーションが存在する場合、適応型セキュリティ アプライアンスはそれを表示します。リカバリ コンフィギュレーションをよく調べて、正しいことを確認します。特に、Image URL フィールドについて確認します。次の例は、スロット 1 の SSM のリカバリ コンフィギュレーションを示しています。

```
hostname# show module 1 recover
Module 1 recover parameters. . .
Boot Recovery Image: Yes
Image URL:          tftp://10.21.18.1/csc-img
Port IP Address:    10.1.2.10
Port Mask :         255.255.255.0
Gateway IP Address: 10.1.2.254
```

- b. リカバリ コンフィギュレーションを作成または修正する必要がある場合は、**hw-module module recover** コマンドを **configure** キーワードとともに次のように使用します。

```
hostname# hw-module module slot recover configure
```

*slot* には、SSM 専用のスロット番号を指定します。

プロンプトへの応答を必要に応じて完了します。コンフィギュレーションを修正する場合は、**Enter** キーを押すと、以前に設定した値を保持できます。これらのプロンプトの例を次に示します。これらのプロンプトの詳細については、『[Cisco Security Appliance Command Reference](#)』の **hw-module module recover** コマンドの項を参照してください。

```
Image URL [tftp://0.0.0.0/]:  
Port IP Address [0.0.0.0]:  
VLAN ID [0]:  
Gateway IP Address [0.0.0.0]:
```

**(注)**

指定する TFTP サーバが最大 60 MB のファイルを転送できることを確認してください。また、SSM の管理ポート IP アドレスとして指定した IP アドレスに TFTP が接続できることも確認してください。

プロンプトへの応答が完了すると、適応型セキュリティ アプライアンスが指定の URL で検出したイメージを SSM に転送する準備が整います。

**ステップ 2** TFTP サーバから SSM にイメージを転送し、SSM を再起動します。これを行うには、**hw-module module recover** コマンドを **boot** キーワードとともに次のように使用します。

```
hostname# hw-module module slot recover boot
```

*slot* には、SSM 専用のスロット番号を指定します。

**ステップ 3** イメージ転送の進捗と SSM の再起動プロセスを確認します。これを行うには、**show module** コマンドを使用します。詳細については、[P.19-17](#) の「**SSM ステータスのチェック**」を参照してください。

適応型セキュリティ アプライアンスがイメージの転送と SSM の再起動を完了すると、SSM は、新しく転送されたイメージを実行します。

**(注)**

ご使用の SSM がコンフィギュレーションのバックアップをサポートしていて、SSM で実行しているアプリケーションのコンフィギュレーションを復元する必要がある場合の詳細については、その SSM のマニュアルを参照してください。





# ネットワーク攻撃の防止

---

この章では、TCP 正規化の設定、TCP 接続と UDP 接続の制限、およびその他のさまざまな保護機能によるネットワーク攻撃の防止方法について説明します。

次の事項について説明します。

- [TCP の正規化の設定 \(P.20-2\)](#)
- [接続の制限値とタイムアウトの設定 \(P.20-5\)](#)
- [IP スプーフィングの防止 \(P.20-7\)](#)
- [フラグメント サイズの設定 \(P.20-7\)](#)
- [不要な接続のブロック \(P.20-8\)](#)
- [基本 IPS をサポートする IP 監査の設定 \(P.20-9\)](#)

## TCP の正規化の設定

TCP の正規化機能を使用して、異常なパケットを特定する基準を指定できます。このような異常なパケットは、検出時にセキュリティ アプライアンスによってドロップされます。この機能はモジュラ ポリシー フレームワークを使用するため、TCP の正規化の実装は、トラフィックの特定、TCP の正規化基準の指定、およびインターフェイスでの TCP の正規化のアクティブ化で構成されます。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。

TCP の正規化を設定するには、次の手順を実行します。

**ステップ 1** 検索する TCP の正規化基準を指定するには、次のコマンドを入力して TCP マップを作成します。

```
hostname(config)# tcp-map tcp-map-name
```

TCP マップごとに 1 つまたは複数の設定値を指定できます。

**ステップ 2** 次の 1 つ以上のオプションについて、コマンドを入力して TCP マップ基準を設定します。

- 一貫性のない TCP 再送信を防止する。

```
hostname(config-tcp-map)# check-retransmission
```

- チェックサムを確認する。

```
hostname(config-tcp-map)# checksum-verification
```

- データ長が TCP 最大セグメント サイズを超えるパケットを許可する。デフォルトでは、このようなパケットはドロップされるため、次のコマンドで許可します。

```
hostname(config-tcp-map)# exceed-mss {allow | drop}
```

- TCP 接続のキューに入れることができる異常なパケットの最大数を設定する。

```
hostname(config-tcp-map)# queue-limit pkt_num
```

*pkt\_num* には、異常なパケットの最大数を指定します。範囲は 0 ～ 250 で、デフォルトは 0 です。

- TCP ヘッダーの予約ビットを消去するか、または予約ビットが設定されているパケットをドロップする。デフォルトでは、予約ビットは許可されます。そのため、次のコマンドで予約ビットを消去するか、パケットをドロップします。

```
hostname(config-tcp-map)# reserved-bits {allow | clear | drop}
```

**allow** は、TCP ヘッダーの予約ビットが設定されているパケットを許可します。**clear** は、TCP ヘッダーの予約ビットを消去してパケットを許可します。**drop** は、TCP ヘッダーの予約ビットが設定されているパケットをドロップします。

- データが設定されている SYN パケットをドロップする。デフォルトでは、データが設定されている SYN パケットは許可されます。そのため、次のコマンドでパケットをドロップします。

```
hostname(config-tcp-map)# syn-data {allow | drop}
```

- selective-ack、timestamp、window-scale の各 TCP オプションを消去するか、または番号で指定された TCP オプションの範囲をドロップする。デフォルトでは、指定されたオプションが設定されているパケットは許可され、範囲内のオプションは消去されます。そのため、次のコマンドでそれらを消去、許可、またはドロップします。

```
hostname(config-tcp-map)# tcp-options {selective-ack | timestamp | window-scale}
{allow | clear}
```

または

```
hostname(config-tcp-map)# tcp-options range lower upper {allow | clear | drop}
```



**allow** は、指定されたオプションが設定されているパケットを許可します。**clear** は、オプションを消去してパケットを許可します。**drop** は、パケットをドロップします。

**selective-ack** キーワードは、SACK オプションを許可または消去します。デフォルトでは、SACK オプションは許可されます。

**timestamp** キーワードは、タイムスタンプ オプションを許可または消去します。タイムスタンプ オプションを消去すると、PAWS と RTT がディセーブルになります。デフォルトでは、タイムスタンプ オプションは許可されます。

**widow-scale** キーワードは、ウィンドウ スケール メカニズム オプションを許可または消去します。デフォルトでは、ウィンドウ スケール メカニズム オプションは許可されます。

**range** キーワードは、オプションの範囲を指定します。

**lower** 引数は、範囲の下限を設定します。6、7、または 9～255 です。

**upper** 引数は、範囲の上限を設定します。6、7、または 9～255 です。

- TTL 回避保護をディセーブルにする。

```
hostname(config-tcp-map)# ttl-evasion-protection
```

セキュリティ ポリシーを回避しようとする攻撃を防ぐ場合は、このコマンドを入力しないでください。

たとえば、攻撃者は TTL を非常に短くしてポリシーを通過するパケットを送信できます。TTL がゼロになると、セキュリティ アプライアンスとエンドポイントの間のルータはパケットをドロップします。この時点で、攻撃者は TTL を長くした悪意のあるパケットを送信できます。このパケットは、セキュリティ アプライアンスには再送信のように見えるため、通過します。一方、エンドポイント ホストにとっては、このパケットが攻撃者によって受信された最初のパケットになります。この場合、攻撃者はセキュリティによる攻撃の防止を受けず、攻撃に成功します。

- URG ポインタを許可する。

```
hostname(config-tcp-map)# urgent-flag {allow | clear}
```

URG フラグは、ストリーム中の他のデータよりも優先順位の高い情報がこのパケットに含まれていることを示すために使用します。TCP RFC では、URG フラグの正確な解釈が明確にされていません。そのため、エンド システムは緊急オフセットをさまざまな方法で処理しており、これが攻撃に対する脆弱性になることがあります。デフォルトの動作は、URG フラグおよびオフセットの消去です。URG フラグを許可するには、このコマンドを使用します。

- 予想外のウィンドウ サイズの変更が発生した接続をドロップする。デフォルトでは、このような接続は許可されるため、次のコマンドでドロップします。

```
hostname(config-tcp-map)# window-variation {allow | drop}
```

ウィンドウ サイズ メカニズムによって、TCP は大きなウィンドウをアダプタサイズでき、続いて、過剰な量のデータを受け入れずに、はるかに小さなウィンドウをアダプタサイズできます。TCP 仕様により、「ウィンドウの縮小」は極力避けることが推奨されています。この条件が検出された場合に、接続をドロップできます。

**ステップ 3** TCP 正規化を適用するトラフィックを特定するには、**class-map** コマンドを使用してクラスマップを追加します。詳細については、[P.18-3](#) の「[クラスマップによるトラフィックの特定](#)」を参照してください。

**ステップ 4** クラスマップ トラフィックで実行する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 5** 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 6** 次のコマンドを入力して、TCP マップをクラスマップに適用します。

```
hostname(config-pmap-c)# set connection advanced-options tcp-map-name
```

**ステップ 7** 1 つ以上のインターフェイスでポリシーマップをアクティブにするには、次のコマンドを入力します。

```
hostname(config)# service-policy policymap_name {global | interface interface_name}
```

ここで、**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 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを 1 つだけ適用できます。

たとえば、既知の FTP データ ポートと Telnet ポートの間の TCP ポート範囲に送信されるすべてのトラフィックで緊急フラグと緊急オフセット パケットを許可するには、次のコマンドを入力します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config-tcp-map)# class-map urg-class
hostname(config-cmap)# match port tcp range ftp-data telnet
hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap
hostname(config-pmap-c)# service-policy pmap global
```

## 接続の制限値とタイムアウトの設定

この項では、TCP と UDP の最大接続数、最大初期接続数、クライアントごとの最大接続数、接続タイムアウトを設定する方法、および TCP シーケンスのランダム化をディセーブルにする方法について説明します。

接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。セキュリティ アプライアンスでは、クライアントごとの制限値と初期接続制限値を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラグディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

TCP 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ていて、結果としてデータ順序が変わる場合だけにします。各 TCP 接続には、2 つの Initial Sequence Number (ISN; 初期シーケンス番号) があります。1 つはクライアントが生成し、1 つはサーバが生成します。セキュリティ アプライアンスは、ホストとサーバが生成する ISN をランダム化します。少なくとも 1 つの ISN をランダムに生成して、攻撃者が次の ISN を予想してセッションを乗っ取ることができないようにする必要があります。



(注)

最大接続数、最大初期接続数、および TCP シーケンスのランダム化は、NAT コンフィギュレーションでも設定できます。同じトラフィックに対して両方の方法でこれらの設定値を設定した場合、セキュリティ アプライアンスは小さい方の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されている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

接続制限値を設定するには、次の手順を実行します。

**ステップ 1**    トラフィックを特定するには、**class-map** コマンドを使用して、クラスマップを追加します。詳細については、[P.18-3 の「クラスマップによるトラフィックの特定」](#)を参照してください。

**ステップ 2**    クラスマップ    トラフィックで実行する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**    最大接続制限値または TCP シーケンスのランダム化のイネーブル / ディセーブルを設定するには、次のコマンドを入力します。

```
hostname(config-pmap-c)# set connection {conn-max number | embryonic-conn-max number |  
per-client-embryonic-max number | per-client-max number | random-sequence-number  
{enable | disable}}. . .
```

*number* は、0 ～ 65535 の整数です。デフォルトは 0 で、接続を制限しないことを意味します。

このコマンドを 1 行ですべて入力することも（順序は任意）、各アトリビュートを別々のコマンドとして入力することもできます。セキュリティ アプライアンスにより、コマンドは実行コンフィギュレーションで 1 行に結合されます。

**ステップ 5** 接続、初期接続（ハーフオープン接続）、およびハーフクローズ接続のタイムアウトを設定するには、次のコマンドを入力します。

```
hostname(config-pmap-c)# set connection timeout {[embryonic hh[:mm[:ss]]]
[half-closed hh[:mm[:ss]]] [tcp hh[:mm[:ss]]]}
```

**embryonic** *hh[:mm[:ss]]* は、0:0:5 ～ 1192:59:59 の時間です。デフォルトは 0:0:30 です。この値を 0 に設定することもできます。これは、接続がタイムアウトしないことを意味します。

**half-closed** *hh[:mm[:ss]]* の値および **tcp** *hh[:mm[:ss]]* の値は、0:5:0 ～ 1192:59:59 の時間です。**half-closed** のデフォルトは 0:10:0 で、**tcp** のデフォルトは 1:0:0 です。この値を 0 に設定することもできます。これは、接続がタイムアウトしないことを意味します。

このコマンドを 1 行ですべて入力することも（順序は任意）、各アトリビュートを別々のコマンドとして入力することもできます。コマンドは実行コンフィギュレーションで 1 行に結合されます。

**ステップ 6** 1 つ以上のインターフェイスでポリシーマップをアクティブにするには、次のコマンドを入力します。

```
hostname(config)# service-policy policymap_name {global | interface interface_name}
```

ここで、**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 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを 1 つだけ適用できます。

## IP スプーフィングの防止

この項では、インターフェイスで Unicast Reverse Path Forwarding (Unicast RPF; ユニキャスト逆経路転送) をイネーブルにします。Unicast RPF は、ルーティング テーブルに従い、すべてのパケットが正しい発信元インターフェイスと一致する送信元 IP アドレスを持っていることを確認して、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、実際の送信元を隠蔽すること) から保護します。

通常、セキュリティ アプライアンスは、パケットの転送先を判定するときに、宛先アドレスだけを調べます。Unicast RPF は、送信元アドレスも調べるようにセキュリティ アプライアンスに指示します。そのため、逆経路転送 (Reverse Path Forwarding) と呼ばれます。セキュリティ アプライアンスの通過を許可するすべてのトラフィックについて、送信元アドレスに戻るルートを経由するセキュリティ アプライアンスのルーティング テーブルに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。

たとえば、外部トラフィックの場合、セキュリティ アプライアンスはデフォルト ルートを使用して Unicast RPF 保護を満たすことができます。トラフィックが外部インターフェイスから入り、送信元アドレスがルーティング テーブルにない場合、セキュリティ アプライアンスはデフォルト ルートを使用して、外部インターフェイスを発信元インターフェイスとして正しく識別します。

ルーティング テーブルにあるアドレスから外部インターフェイスにトラフィックが入り、このアドレスが内部インターフェイスに関連付けられている場合、セキュリティ アプライアンスはパケットをドロップします。同様に、未知の送信元アドレスから内部インターフェイスにトラフィックが入った場合は、一致するルート (デフォルト ルート) が外部インターフェイスを示しているため、セキュリティ アプライアンスはパケットをドロップします。

Unicast RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP と TCP にはセッションがあるため、最初のパケットは逆ルート ルックアップが必要です。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

Unicast RPF 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、セキュリティ アプライアンスは 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。NFS over UDP など、アプリケーションが日常的にパケットをフラグメント化する場合は、ネットワークでフラグメント化を許可する必要があります。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は、フラグメントがセキュリティ アプライアンスを通過できないようにすることをお勧めします。フラグメント化されたパケットは、DoS 攻撃によく使われます。フラグメントの禁止を設定するには、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禁止する場合は、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。

## 不要な接続のブロック

あるホストがネットワークを攻撃しようとしていることがわかった場合（たとえば、システム ログメッセージで攻撃が示された場合）、送信元 IP アドレスおよびその他の識別パラメータに基づいて、接続をブロック（排除）できます。排除を無効するまで、新しい接続は作成できません。



(注)

トラフィックを監視する IPS（AIP SSM など）がある場合は、IPS で自動的に接続を排除できます。

接続を手動で排除するには、次の手順を実行します。

**ステップ 1** 必要に応じて、次のコマンドを入力し、接続に関する情報を表示します。

```
hostname# show conn
```

セキュリティ アプライアンスは、各接続に関する情報を次のように表示します。

```
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** この送信元 IP アドレスからの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 アドレスだけを入力した場合、以後のすべての接続が排除されます。既存の接続はアクティブのままです。

送信元 IP アドレスからの以後の接続をブロックするだけでなく、既存の接続もドロップするには、宛先 IP アドレス、送信元と宛先のポート、およびプロトコルを入力します。デフォルトでは、プロトコルは IP を表す 0 です。

マルチコンテキスト モードでは、このコマンドは管理コンテキストで入力できます。また、他のコンテキストのインターフェイスに割り当てられている VLAN ID を指定することで、他のコンテキストの接続を排除できます。

**ステップ 3** 排除を無効するには、次のコマンドを入力します。

```
hostname(config)# no shun src_ip [vlan vlan_id]
```

## 基本 IPS をサポートする IP 監査の設定

IP 監査機能は、AIP SSM を使用しないセキュリティ アプライアンスに基本 IPS サポートを提供します。シグニチャの基本リストをサポートし、シグニチャと一致するトラフィックに対して 1 つ以上のアクションを実行するようにセキュリティ アプライアンスを設定できます。

IP 監査をイネーブルにするには、次の手順を実行します。

**ステップ 1** 情報シグニチャに対する IP 監査ポリシーを定義するには、次のコマンドを入力します。

```
hostname(config)# ip audit name name info [action [alarm] [drop] [reset]]
```

ここで、**alarm** はパケットがシグニチャと一致したことを示すシステム メッセージを生成し、**drop** はパケットをドロップし、**reset** はパケットをドロップして接続を閉じます。アクションを定義しない場合、デフォルト アクションはアラームの生成です。

**ステップ 2** 攻撃シグニチャに対する IP 監査ポリシーを定義するには、次のコマンドを入力します。

```
hostname(config)# ip audit name name attack [action [alarm] [drop] [reset]]
```

ここで、**alarm** はパケットがシグニチャと一致したことを示すシステム メッセージを生成し、**drop** はパケットをドロップし、**reset** はパケットをドロップして接続を閉じます。アクションを定義しない場合、デフォルト アクションはアラームの生成です。

**ステップ 3** ポリシーをインターフェイスに割り当てるには、次のコマンドを入力します。

```
ip audit interface interface_name policy_name
```

**ステップ 4** シグニチャをディセーブルにする方法およびシグニチャの詳細については、『Cisco Security Appliance Command Reference』の **ip audit signature** コマンドを参照してください。







# QoS ポリシーの適用

---

この章では、QoS ポリシーを適用する方法について説明します。次の項で構成されています。

- [概要 \(P.21-2\)](#)
- [QoS の概念 \(P.21-3\)](#)
- [QoS の実装 \(P.21-4\)](#)
- [QoS の対象にするトラフィックの特定 \(P.21-6\)](#)
- [QoS ポリシーマップの定義 \(P.21-8\)](#)
- [レート制限の適用 \(P.21-9\)](#)
- [サービス ポリシーのアクティブ化 \(P.21-10\)](#)
- [低遅延キューイングの適用 \(P.21-11\)](#)
- [QoS の設定 \(P.21-13\)](#)
- [QoS コンフィギュレーションの表示 \(P.21-17\)](#)
- [QoS 統計情報の表示 \(P.21-19\)](#)

## 概要

衛星接続を使用した長距離電話では、会話が、短い間ですが認識できる程度に途切れて、不定期に中断されることがあります。このような中断は、ネットワークで送信されるパケットが到着する間隔の時間で、*遅延*と呼ばれます。音声やストリーミング ビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。*Quality of Service (QoS)* は、このようなトラフィックの優先順位を上げることができるネットワーク機能です。

ユーザのインターネット コミュニティのアクセス ポイントが、モデムから DSL やケーブルなどの高速ブロードバンド接続にアップグレードしたことにより、1 人のユーザが、すべてではないにしても、利用可能な帯域幅のほとんどを消費し、他のユーザが使用する帯域幅が欠乏する可能性が高まっています。ユーザまたはサイトツーサイトの接続が適切な割り当て分を超えて帯域幅を消費しないように、QoS は、ユーザが使用できる最大帯域幅を管理するポリシング機能を提供します。

QoS は、基盤となるテクノロジーの限られた帯域幅で全体的に最良のサービスを実現するさまざまなテクノロジーを通じて、特定のネットワーク トラフィックに、より良いサービスを提供するネットワークの機能を指します。

セキュリティ アプライアンスでの QoS の主要目的は、個別のフローまたは VPN トンネル フローの両方で、特定のネットワーク トラフィックのレートを制限し、限られた帯域幅の中ですべてのトラフィックが適切な割り当て分を得ることができるようにすることです。フローは、多くの方法で定義できます。セキュリティ アプライアンスでは、送信元 IP アドレスと宛先 IP アドレスの組み合わせ、送信元ポート番号と宛先ポート番号の組み合わせ、および IP ヘッダーの TOS バイトに QoS を適用できます。

## QoS の概念

QoS は、ネットワーク トラフィックの種類とそのトラフィックに割り当てた優先順位に基づいて、ミッションクリティカルなデータと通常のデータの両方にネットワーク リソースを割り当てることのできるトラフィック管理戦略です。簡単に言えば、QoS はプライオリティ トラフィックの円滑さを保証し、デフォルト トラフィックのレート制限（ポリシング）機能を提供します。

たとえば、転送メカニズムとしてインターネットというインフラストラクチャを使用している地理的に離れたサイト間でのオフィス間通信にとって、Video および Voice over IP（VoIP）はますます重要になっています。ファイアウォールはアクセスを制御することによってネットワークを安全にする鍵であり、VoIP プロトコルの検査も行います。QoS は、デバイスを通過するその他のすべてのトラフィックに対して基本レベルのサービスを提供しながら、明瞭で中断されない音声およびビデオ通信を提供することに焦点を置いています。

セキュアで信頼性が高く、費用効果の高い方法で音声およびビデオが IP ネットワークを通過できるように、ネットワークのすべてのポイントで QoS をイネーブルにする必要があります。QoS を実装すると、次のことができるようになります。

- **ネットワーク オペレーションの単純化。**類似のテクノロジーを使用して、すべてのデータ、音声、およびビデオのネットワーク トラフィックを 1 つのバックボーンにまとめることができます。
- **新しいネットワーク アプリケーションのイネーブル化。**統合コール センタ アプリケーションやビデオベースのトレーニングなどによって、それぞれの市場で企業価値を高め、生産性を上げることができます。
- **リソースの使用率の制御。**どのトラフィックがどのリソースを受け取るかを制御できます。たとえば、最も重要で時間の問題が大きいトラフィックは、必要なだけのネットワーク リソース（利用可能な帯域幅と最小の遅延）を受け取り、リンクを使用するその他のアプリケーションは、ミッションクリティカルなトラフィックを妨害せずに適正なサービスの割り当て分を使用するようにできます。

QoS は、個々のユーザ トンネルおよびサイトツーサイト トンネルごとに、トンネル トラフィックに対して最大レート制御（ポリシング）を提供します。このリリースでは、最低帯域幅の保証はありません。

セキュリティ アプライアンスで、LAN-to-LAN トンネル内の個々のユーザ トラフィックをポリシングするには、トンネルに関連付けるのではなく、最終的にトラフィックが LAN-to-LAN トンネルを通過するようなクラスマップを設定します。その後、LAN-to-LAN トンネルの前のトラフィックは、トンネルを通過するときに個別のポリシングが可能になり、トンネルに適用される集約レートで再びポリシングされます。

セキュリティ アプライアンスは、Low-Latency Queue（LLQ; 低遅延キュー）とデフォルト キューの 2 種類のトラフィック キューを使用して QoS を実現します。デフォルト トラフィックだけが、レート制限の対象になります。

QoS は大量のリソースを消費し、セキュリティ アプライアンスのパフォーマンスを低下させることがあるため、QoS はデフォルトでディセーブルになっています。



(注)

常に変化するネットワーク環境では、QoS は 1 回限りの構成ではなく、ネットワーク設計の継続的で不可欠な要素であることを考慮する必要があります。

## QoS の実装

一般的に、QoS ポリシーをプロビジョニングするには、次の手順が必要です。

1. トラフィック クラスを指定します。
2. アクションをトラフィック クラスに関連付けて、ポリシーを形成します。
3. ポリシーをアクティブにします。

分類ポリシーの指定（トラフィック クラスの定義）は、分類の結果に基づいて動作するポリシーの指定とは区別されています。

トラフィック クラスは、パケットの内容で識別可能なトラフィックのセットです。たとえば、ポートの値が 23 の TCP トラフィックは、Telnet トラフィック クラスに分類できます。

アクションは、情報またはリソースを保護するために実行される特定の動作です。ここでは、QoS 機能が実行されます。アクションは通常、特定のトラフィック クラスに関連付けられます。

セキュリティ アプライアンスの慣例的な QoS ポリシーの設定は、次の手順で構成されます。

- トラフィック クラスを定義します（**class-map** コマンド）。
- ポリシーとアクションを各トラフィック クラスに関連付けます（**policy-map** コマンド）。
- ポリシーを論理インターフェイスまたは物理インターフェイスに関連付けます（**service-policy** コマンド）。



(注)

設定手順の詳細については、[P.21-13 の「QoS の設定」](#)を参照してください。

**class-map** コマンドは、トラフィックのクラスを表す名前付きオブジェクトを定義し、このクラスに属するパケットを識別する基準に一致するパケットを指定します。コマンドの基本形式は次のとおりです。

```
class-map class-map-name-1
    match match-criteria-1
class-map class-map-name-n
    match match-criteria-n
```

**policy-map** コマンドは、トラフィック クラスのセットに適用するポリシーのセットを表す名前付きオブジェクトを定義します。このようなポリシーの例として、ある最大レートへのトラフィック クラスのポリシングがあります。コマンドの基本形式は次のとおりです。

```
policy-map policy-map-name
    class class-map-name-1
        policy-1
        policy-n
    class class-map-name-n
        policy-m
        policy-m+1
```

**service-policy** コマンドは、ポリシーマップとそれに関連付けられているポリシーを、対象の名前付きインターフェイスに関連付けます。



(注)

policy-map-name の下の QoS レート ポリシーは、名前付きインターフェイスの出力トラフィックにのみ適用され、入力トラフィックには適用されません。

このコマンドでは、対象から着信するパケットにポリシーを適用するか、または対象に送信されるパケットにポリシーを適用するかについても指定します。たとえば、出力ポリシー（インターフェイスから出るパケットに適用）は、次のように適用されます。

```
interface GigabitEthernet0/3
  service-policy output policy-map-name
```

また、プライオリティトラフィックとベストエフォートトラフィックを区別する場合は、優先されるトラフィックを伝送する名前付き物理インターフェイスごとに、低遅延キューを定義する必要があります（**priority-queue** コマンド）。

次の例は、デフォルトのプライオリティキューをデフォルトの **queue-limit** と **tx-ring-limit** でイネーブルにします。

```
priority-queue name-interface
```

次の項で、これらの使用方法を詳しく説明します。

## QoS の対象にするトラフィックの特定

**class-map** コマンドは、QoS アクションが関連付けられているトラフィックのセットを分類します。さまざまな種類の一致基準を使用して、トラフィックを分類できます。**match** コマンドで、クラスマップのトラフィック クラスに含まれるトラフィックを指定します。これらのコマンドは、クラスマップに含まれるトラフィックを定義するためのさまざまな基準を保持しています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラスマップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィック クラス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で受信したパケットは、クラスマップの **match** 文で定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに包含され、そのトラフィック クラスに関連付けられているアクションの対象になります。どのトラフィック クラスのどの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

基準の 1 つがアクセスリストです。たとえば、次のシーケンスで、**class-map** コマンドは `tcp_traffic` というアクセスリストを使用して、すべての非トンネル TCP トラフィックを分類します。

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic
```

パケットをクラスマップと照合したとき、結果は一致または不一致です。

次の例では、より限定的な一致基準を使用して、特定のセキュリティ関連のトンネルグループにトラフィックを分類します。これらの特定の一致基準では、トラフィックが特定のトンネルに分類されるために、最初の一致特性としてトンネルグループ（この例では、すでに定義されている Tunnel-Group-1）に一致する必要があります。次に、別の照合行でトラフィックを分類できます（IP DiffServ コード ポイント、緊急転送）。

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group Tunnel-Group-1
hostname(config-cmap)# match dscp ef
```

次の例では、**class-map** コマンドはトンネル トラフィックと非トンネル トラフィックの両方をトラフィック タイプに従って分類します。

```
hostname(config)# access-list tunneled extended permit ip 10.10.34.0 255.255.255.0 20.20.10.0
255.255.255.0
hostname(config)# access-list non-tunneled extended permit tcp any any
hostname(config)# tunnel-group tunnel-grp1 type IPSec_L2L

hostname(config)# class-map browse
hostname(config-cmap)# description "This class-map matches all non-tunneled tcp traffic."
hostname(config-cmap)# match access-list non-tunneled

hostname(config-cmap)# class-map TG1-voice
hostname(config-cmap)# description "This class-map matches all dscp ef traffic for tunnel-grp 1."
hostname(config-cmap)# match dscp ef
hostname(config-cmap)# match tunnel-group tunnel-grp1

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# description "This class-map matches all best-effort traffic for tunnel-grp1."
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address
```

次の例は、クラストラフィックがトンネルとして指定されておらず、トンネルを通過する場合に、トンネル内のフローをポリシングする方法を示します。この例では、192.168.10.10 がリモートトンネルのプライベート側のホストマシンのアドレスで、アクセスリストの名前は「host-over-l2l」です。クラスマップ（名前は「host-specific」）を作成することによって、LAN-to-LAN 接続でトンネルを制御する前に、「host-specific」クラスをポリシングできます。この例では、トンネルの前で「host-specific」トラフィックのレートが制限され、次にトンネルのレートが制限されます。

```
hostname(config)# access-list host-over-l2l extended permit ip any host 192.168.10.10
hostname(config)# class-map host-specific
hostname(config-cmap)# match access-list host-over-l2l
```

次の表に、使用可能で QoS に関係がある **match** コマンドの基準をまとめます。すべての **match** コマンドとそのシンタックスの完全なリストについては、『Cisco Security Appliance Command Reference』を参照してください。

| コマンド                                     | 説明                                                                                                                                                                                                                                                                                                         |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>match access-list</b>                 | 名前または番号によって、クラスマップ内のアクセスリストトラフィックと照合します。                                                                                                                                                                                                                                                                   |
| <b>match any</b>                         | クラスマップ中の任意の基準に一致するトラフィックを識別します。                                                                                                                                                                                                                                                                            |
| <b>match dscp</b>                        | クラスマップ中の IETF 定義の DSCP 値（IP ヘッダー内）を照合します。最大 64 の異なる dscp 値を指定し、指定した値のいずれかと一致するパケットで構成されたクラスを定義できます。                                                                                                                                                                                                        |
| <b>match flow ip destination-address</b> | フローベースのポリシーアクションをイネーブルにします。フローを定義する基準は、宛先 IP アドレスです。一意の IP 宛先アドレスに向かうトラフィックは、すべてフローと見なされます。ポリシーのアクションは、トラフィッククラス全体ではなく各フローに適用されます。このコマンドは常に、 <b>match tunnel group</b> を伴います。リモートアクセス VPN の場合、このコマンドは、各リモートアクセスホストフローに適用されます。LAN-to-LAN VPN の場合、このコマンドは、ローカルとリモートのトンネルアドレスのペアで識別される 1 つの集約 VPN フローに適用されます。 |
| <b>match port</b>                        | このインターフェイスで受信したパケットの比較基準として、TCP/UDP ポートを指定します。                                                                                                                                                                                                                                                             |
| <b>match precedence</b>                  | IP ヘッダーの TOS バイトで表された優先値を照合します。最大 8 の異なる優先値を指定し、指定した値のいずれかと一致するパケットで構成されたクラスを定義できます。                                                                                                                                                                                                                       |
| <b>match rtp</b>                         | 指定された範囲内の特定の RTP ポートを使用するトラフィックが一致します。許可される範囲は、RTP を使用すると考えられるアプリケーションの取得の対象です。パケットは、UDP ポートが指定された範囲内にあり（両端の値を含む）、ポート番号が偶数の場合にのみ、定義されたクラスに一致します。                                                                                                                                                           |
| <b>match tunnel group</b>                | 指定されたトンネルグループ内のすべてのトンネルが一致します。                                                                                                                                                                                                                                                                             |

ユーザ定義のクラスに加え、class-default というシステム定義のクラスもあります。この class-default は、どのユーザ定義クラスとも一致しないすべてのパケットを表すため、このようなパケットにポリシーを定義できます。

## QoS ポリシーマップの定義

**policy-map** コマンドは、セキュリティ ポリシーや QoS ポリシーなど、さまざまなポリシーを設定します。ポリシーは、**class** コマンドで指定されたトラフィック クラスと 1 つ以上のアクションとの関連付けです。この項では、特に **policy-map** コマンドを使用して 1 つ以上のパケットのクラスに QoS ポリシーを定義する方法について説明します。

**policy-map** コマンドを入力すると、ポリシーマップ コンフィギュレーション モードに移行し、プロンプトが変化します。このモードでは、**class** コマンドと **description** コマンドを入力できます。**policy-map** コマンドでは、複数のポリシーを指定できます。ポリシーマップの最大数は 64 です。

**policy-map** コマンドを入力した後、**class** コマンドを入力して、パケット トラフィックの分類を指定します。**class** コマンドは、指定されたクラスマップで指定されているトラフィックのクラスの QoS ポリシーを設定します。トラフィック クラスは、パケットの内容で識別可能なトラフィックのセットです。たとえば、ポートの値が 23 の TCP トラフィックは、Telnet トラフィック クラスに分類できます。**class** コマンドは、以前指定して構築したクラスマップ指定で区別され、関連付けるアクションが直後に付きます。

セキュリティ アプライアンスは、ポリシーマップ コンフィギュレーションで入力された順に、クラスマップを評価します。パケットは、一致した最初のクラスマップに分類されます。



(注)

ポリシーマップの各種のアクションが実行される順序は、このマニュアルのコマンド説明で出現する順序とは無関係です。

**priority** コマンドは、音声など遅延が問題になるトラフィックに、低遅延キューイングを提供します。このコマンドは、関連付けられたクラス（前の例では、TG1-voice）と一致するすべてのパケットを選択し、プライオリティ処理のために低遅延キューに送信します。



## レート制限の適用

各ユーザの Bandwidth Limiting Traffic ストリーム (BLT) は、最大帯域幅制限 (つまり、個別のユーザのデフォルト トラフィックを一定の最大レートにレート制限する厳密なポリシング) に参加できます。これによって、あるユーザの BLT によって他のユーザが圧迫されることを防ぎます。ただし、LLQ トラフィックは、プライオリティキューのダウンストリームでマークされ、処理されます。このトラフィックは、レート制限されません。

ポリシングは、設定した最大レート (ビット / 秒) を超えるトラフィックが発生しないようにして、1 つのトラフィック フローが全体のリソースを占有しないようにする方法です。police コマンドを使用して、最大レート (このトラフィック フローのレート制限) を指定します。この値は、8000 ~ 2000000000 の範囲で、許可される最大速度 (1 秒あたりのビット) を指定します。

制限内のトラフィックと制限を超えたトラフィックに対して実行するアクション (ドロップまたは送信) も指定します。



(注)

ドロップ アクションは指定できますが、機能しません。レートを超えた場合を除き、アクションは常に送信です。レートを超えた場合でも、アクションは、許可される最大速度へのトラフィックの抑制です

police コマンドは、許可されるトラフィックの最大単一バーストも設定します。バースト値は 1000 ~ 512000000 の範囲で、持続したバーストで許可される瞬間的なバイト数を指定します。これを超えると、レート値に適応するためにトラフィックが抑制されます。



(注)

ポリシングは、出力方向にのみ適用されます。

優先順位とポリシングを、両方ともイネーブルにすることはできません。

既存の VPN クライアント トラフィック、LAN-to-LAN トラフィック、または非トンネル トラフィックが確立されているインターフェイスを対象として、サービス ポリシーを適用または削除した場合、QoS ポリシーは適用されず、トラフィック ストリームから削除されません。このような接続を対象として QoS ポリシーを適用または削除するには、接続を消去 (ドロップ) して再確立する必要があります。



(注)

デフォルト クラスマップの class-default でポリシングを指定すると、LAN-to-LAN VPN のトンネルグループに定義された police コマンドがない場合に、集約された LAN-to-LAN VPN フローに class-default のポリシング値が適用されます。つまり、class-default のポリシング値は、暗号化前に存在する LAN-to-LAN VPN の個別のフローには適用されません。

次の例は、前の項で作成したコンフィギュレーションで構築されています。前の例と同様に、tcp\_traffic と TG1-voice という 2 つのクラスマップがあります。3 番目のクラスマップを追加します。

```
hostname(config)# class-map TG1-best-effort
hostname(config-cmap)# match tunnel-group Tunnel-Group-1
hostname(config-cmap)# match flow ip destination-address
```

これによって、次のように、トンネルおよび非トンネル QoS ポリシーを定義する基本が提供されます。トンネルおよび非トンネル トラフィックに対する単純な QoS ポリシーが作成され、クラス TG1-voice のパケットが低遅延キューに割り当てられ、tcp\_traffic および TG1-best-effort フローにレート制限が設定されます。



(注)

「ベストエフォート」は、信頼性の高いパケット配信を保証せず、高度な確認応答システムを使用しません。ただし、宛先にパケットを配信するために「最善の努力 (ベストエフォート)」をします。

この例では、tcp\_traffic クラスのトラフィックの最大レートは 56,000 ビット / 秒で、最大バーストサイズは 10,500 バイト / 秒です。TC1-BestEffort クラスの最大レートは 200,000 ビット / 秒で、最大バーストは 37,500 バイト / 秒です。TC1-voice クラスのトラフィックは、プライオリティ クラスに属しているため、最大速度またはバースト レートでポリシングされません。

```
hostname(config)# policy-map qos
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# police output 56000 10500

hostname(config-pmap-c)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# class TG1-best-effort
hostname(config-pmap-c)# police output 200000 37500

hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)# police output 1000000 37500
```



(注)

最大 256 のポリシーマップを使用でき、1 つのポリシーマップで最大 256 のクラスを使用できます。すべてのポリシーマップのクラスを合計した最大数は、256 です。トンネル クラスを除き、1 つのクラスマップに関連付けることができる **match** 文は 1 つだけです。トンネル クラスの場合、追加の **match tunnel-group** 文が許可されます。



(注)

クラス **class-default** は、常に存在します。宣言する必要はありません。

## サービス ポリシーのアクティブ化

**service-policy** コマンドは、**policy-map** コマンドをすべてのインターフェイスでグローバルにアクティブにするか、または対象のインターフェイスでアクティブにします。インターフェイスは、仮想 (vlan) インターフェイスまたは物理インターフェイスです。グローバル ポリシーマップは 1 つしか適用できません。キーワード **interface** とインターフェイス名を指定すると、ポリシーマップはそのインターフェイスにのみ適用されます。インターフェイス ポリシーマップはグローバル ポリシーマップを上書きします。1 つのインターフェイスに適用できるポリシーマップは 1 つだけです。通常、**service-policy** コマンドは、**nameif** コマンドで定義できる任意のインターフェイスに適用できます。

前の項のポリシーマップの例を使用して、次の **service-policy** コマンドで、前の項で外部インターフェイスのトラフィックに定義したポリシーマップ「qos」をアクティブにします。

```
hostname(config)# service-policy qos interface outside
```

## 低遅延キューイングの適用

セキュリティ アプライアンスでは、2つのクラスのトラフィックを使用できます。優先順位が高く、遅延が問題になるトラフィック（音声やビデオなど）には、低遅延キューイング（LLQ）を使用し、その他のすべてのトラフィックには、デフォルトのベストエフォートを使用します。これらの2つのキューは、システムに組み込まれています。セキュリティ アプライアンスは、QoS プライオリティ トラフィックを認識し、適切な QoS ポリシーを適用します。

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これが「テール ドロップ」です。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。

低遅延（プライオリティ）キューを設定して、送信キューに入れることができるパケットの最大数を調整したり（**tx-ring-limit** コマンドを使用）、プライオリティキューの深さを変更したり（**queue-limit** コマンドを使用）できます。これによって、プライオリティ キューイングの遅延と強固さを制御できます。

**(注)**

**queue-limit** コマンドと **tx-ring-limit** コマンドの値の範囲の上限は、実行時に動的に決まります。この上限値を表示するには、コマンドラインで **help** または **?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。**queue-limit** 値の範囲は、0 ～ 2048 パケットです。**tx-ring-limit** 値の範囲は、PIX プラットフォームでは 3 ～ 128 パケット、ASA プラットフォームでは 3 ～ 256 パケットです。

## プライオリティ キューイングの設定

優先順位の高いトラフィックは、クラス モードで **priority** コマンドを使用して指定します。このコマンドは、クラスマップによって選択されたトラフィックに高い優先順位をマークするように、セキュリティ アプライアンスに指示します。

プライオリティ キューイングが実行されるようにするには、優先順位の高いトラフィックを伝送する名前付き物理インターフェイスのプライオリティキューを作成する必要があります。インターフェイスのプライオリティキューをイネーブルにするには、グローバル コンフィギュレーション モードで **priority-queue** コマンドを使用します。1つの **priority-queue** コマンドを、**nameif** コマンドで定義された各物理インターフェイスに対して適用できます。その他のすべてのトラフィックは、ベストエフォートに基づいて配信されます。

通常、**priority-queue** コマンドは、**nameif** コマンドで定義できるすべての物理インターフェイスに適用できます。**priority-queue** コマンドは、VLAN インターフェイスには適用できません。**priority-queue** コマンドを使用すると、プロンプトで示されるように、プライオリティキュー モードに移行します。このモードでは、送信キューに入れることができるパケットの最大数や、プライオリティキューのサイズを設定できます。

**(注)**

プライオリティ キューイングとポリシングを、両方ともイネーブルにすることはできません。つまり、ポリシングできるのは通常の優先順位のパケットだけで、高い優先順位のパケットはポリシングされません。

## プライオリティキューのサイズの変更

プライオリティキューに指定するサイズは、低遅延キューとベストエフォート キューの両方に適用されます。**queue-limit** コマンドは、プライオリティキューに入れることができるパケットの最大数を指定します。この数を超えると、以後のデータはドロップされます。この制限は、0 ～ 2048 パケットにする必要があります。

## キュー遅延の低減

**tx-ring-limit** コマンドを使用して、任意の時点で、イーサネット送信ドライバリングのキューに入れることができるパケットの最大数（深さ）を設定できます。これによって送信キューを調整して、遅延を低減し、送信ドライバの全体的なパフォーマンスを向上させることができます。この制限の範囲は、PIX プラットフォームでは 3 ～ 128 パケット、ASA プラットフォームでは 3 ～ 256 パケットです。

デフォルトのキュー制限は 256 バイト パケットで、これは、指定されたインターフェイスが上限の 2048 パケットを 500 ms の間隔で送信できる平均値です。ネットワーク ノードに 500 ms を超えて留まるパケットは、エンドツーエンド アプリケーションでタイムアウトをトリガーすることがあります。このようなパケットは、ネットワーク ノードで破棄されることがあります。

デフォルトの **tx-ring-limit** は、指定されたインターフェイスが 10 ms の間隔で送信できる最大値の 1550 バイト パケットです。これによって、ハードウェアベースの送信リングは、優先順位が高いパケットに対して 10 ms を超える余分な遅延を発生させないことが保証されます。

次の例は、デフォルトの **queue-limit** と **tx-ring-limit** を使用して、インターフェイス「outside」（GigabitEthernet0/1 インターフェイス）にプライオリティキューを構築します。

```
hostname(config)# priority-queue outside
```

次の例は、**queue-limit** を 2048 パケット、**tx-ring-limit** を 256 に設定して、インターフェイス「outside」（GigabitEthernet0/1 インターフェイス）にプライオリティキューを構築します。

```
hostname(config)# priority-queue outside
hostname(config-priority-queue)# queue-limit 2048
hostname(config-priority-queue)# tx-ring-limit 256
```



(注)

プライオリティ キューイングをイネーブルにすると、セキュリティ アプライアンスは、優先順位の低いキューのパケットを伝送する前に、優先順位の高いキューのパケットをすべて送出します。

## QoS の設定

QoS ポリシング（レート制限）またはプライオリティ キューイングを実装するトラフィック クラス、ポリシーマップ、およびサービス ポリシーを設定するには、次に示す手順を実行します。プライオリティ キューイングの場合は、インターフェイスのプライオリティキューをイネーブルにするステップも実行します。

QoS を実装するために必要なトラフィック クラス、ポリシーマップ、およびサービス ポリシーの数は、ネットワークの要件によって異なります。ネットワークを分析して、現在設定しているセキュリティ アプライアンスに必要なトラフィック クラス、ポリシーマップ、およびサービス ポリシーの数を確認してから、QoS 構成に応じてこの手順を実行してください。

QoS ポリシングとプライオリティ キューイングを設定するには、次の手順を実行します。

**ステップ 1** ポリシングするトラフィック、またはプライオリティ キューイングのマークを付けるトラフィックを特定します。QoS トラフィックの特定に関する詳細については、[P.21-6 の「QoS の対象にするトラフィックの特定」](#)を参照してください。

**ステップ 2** クラスマップを作成するか、既存のクラスマップを修正して、ポリシングするトラフィックまたはプライオリティ トラフィックとするトラフィックを指定します。これを行うには、**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* には、トラフィック クラスの名前を指定します。**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 モードに移行します。

**ステップ 3** [ステップ 1](#) で特定したトラフィックを指定します。これを行うには、**match** コマンドを使用します。QoS トラフィックの特定に関する詳細については、[P.21-6 の「QoS の対象にするトラフィックの特定」](#)を参照してください。

連続しない複数のポートを指定する必要がある場合は、**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複数の TCP ポートを指定する方法を示しています。

```
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
```

1 つのポートだけを指定する必要がある場合は、**match port** コマンドを次のように使用します。

```
hostname(config-cmap)# match port {tcp | udp} port_number
```

*port\_number* には、セキュリティ アプライアンスでポリシングするトラフィック、またはプライオリティ キューイングのマークを付けるトラフィックの宛先ポートを指定します。

連続した複数のポートを指定する必要がある場合は、**match port** コマンドと **range** キーワードを次のように使用します。

```
hostname(config-cmap)# match port {tcp | udp} range begin_port_number end_port_number
```

*begin\_port\_number* には、ポートの範囲で最小のポート番号を指定し、*end\_port\_number* には、最大のポート番号を指定します。

**ステップ 4** ポリシングまたはプライオリティ キューイングを**ステップ 2** で指定した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、既存のポリシーマップを修正します。QoS ポリシーマップの詳細については、[P.21-8](#) の「[QoS ポリシーマップの定義](#)」を参照してください。

**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* には、ポリシーマップの名前を指定します。CLI はポリシーマップ コンフィギュレーション モードに移行し、それに応じてプロンプトが変化します。

**ステップ 5** [ステップ 2](#) で作成した、ポリシングするトラフィック、またはプライオリティ キューイングのマークを付けるトラフィックを特定するクラスマップを指定します。これを行うには、**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* には、[ステップ 2](#) で作成したクラスマップの名前を指定します。CLI はポリシーマップ クラス コンフィギュレーション モードに移行し、それに応じてプロンプトが変化します。

**ステップ 6** クラスのアクションを設定します。トラフィック クラスをプライオリティ トラフィックとしてマークすること、またはトラフィック クラスのレート制限を指定することが可能です。次のいずれかを実行します。

- クラスマップによって選択されたトラフィックをプライオリティ トラフィックとしてマークする場合は、**priority** コマンドを入力します。

```
hostname(config-pmap-c)# priority
```



**(注)**

プライオリティとしてマークしたトラフィックに対するプライオリティ キューイングは、自動的に実行されません。プライオリティ キューイングをイネーブルにするには、[ステップ 8](#) も実行する必要があります。このステップにより、プライオリティキューがイネーブルになります。

プライオリティ キューイングの詳細については、[P.21-11](#) の「[低遅延キューイングの適用](#)」および『Cisco Security Appliance Command Reference』の **priority** コマンドのページを参照してください。

- クラスマップによって選択されたトラフィックをセキュリティ アプライアンスでポリシングする場合は、**police** コマンドを入力します。

```
hostname(config-pmap-c)# police [output] conform-rate [conform-burst]
[conform-action {drop | transmit}] [exceed-action {drop | transmit}]
```

**police** コマンドの使用方法の詳細については、[P.21-9](#) の「[レート制限の適用](#)」および『Cisco Security Appliance Command Reference』の **police** コマンドのページを参照してください。

**ステップ 7** **service-policy** コマンドを次のように使用して、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-pmap-c)# service-policy policy_map_name [global | interface  
interface_ID]  
hostname(config)#
```

*policy\_map\_name* には、[ステップ 4](#) で作成したポリシーマップを指定します。ポリシーマップをすべてのインターフェイスのトラフィックに適用する場合は、**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のトラフィックに適用する場合は、**interface interface\_ID** オプションを使用します。*interface\_ID* には、**nameif** コマンドでインターフェイスに割り当てた名前を指定します。

セキュリティ アプライアンスが、指定内容に基づいて、トラフィックのポリシングとプライオリティ キューイングのためのマーク付けを開始します。

**ステップ 8** [ステップ 6](#) で **priority** コマンドを入力した場合は、インターフェイスのプライオリティキューをイネーブルにしないと、セキュリティ アプライアンスはプライオリティ キューイングを実行しません。

セキュリティ アプライアンスがプライオリティ キューイングを実行するインターフェイスごとに、次の手順を実行します。

**a. priority-queue** コマンドを入力します。

```
hostname(config)# priority-queue interface  
hostname(config-priority-queue)#
```

*interface* には、プライオリティキューを有効にする物理インターフェイスに割り当てられている名前を指定します。VLAN インターフェイスは、プライオリティ キューイングをサポートしていません。CLI はプライオリティキュー コンフィギュレーション モードに移行し、それに従ってプロンプトが変化します。

**b. (オプション) キューに入れることのできるプライオリティ パケットの non-default 最大数を指定する場合は、queue-limit** コマンドを次のように入力します。

```
hostname(config-priority-queue)# queue-limit number-of-packets
```

デフォルトのキュー サイズは、2048 パケットです。

**c. (オプション) 送信キューに入れることのできるパケットの non-default 最大数を指定する場合は、tx-ring-limit** コマンドを次のように入力します。

```
hostname(config-priority-queue)# tx-ring-limit number-of-packets
```

デフォルトの送信キュー サイズは、128 パケットです。

プライオリティ キューイングをイネーブルにしたインターフェイスで、セキュリティ アプライアンスがプライオリティ キューイングの実行を開始します。

---

次の例では、「tunnel-grp1」という名前の設定済みトンネルグループ用に、優先順位の高いトラフィック (voice) のクラスマップとベストエフォート トラフィックのクラスマップを作成しています。「qos」ポリシーマップには、ベストエフォート トラフィック クラスおよびデフォルト トラフィック クラスに対する **police** コマンドと、voice クラスに対する **priority** コマンドが含まれています。サービス ポリシーは外部インターフェイスに適用され、外部インターフェイスのプライオリティ キューがイネーブルになります。

**例 21-1 QoS ポリシングとプライオリティ キューイングの設定**

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# description "This class-map matches all dscp ef traffic for tunnel-grp 1"
hostname(config-cmap)# match dscp ef
hostname(config-cmap)# match tunnel-group tunnel-grp1

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# description "This class-map matches all best-effort traffic for tunnel-grp1"
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address

hostname(config-cmap)# policy-map qos
hostname(config-pmap)# class TG1-voice
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# class TG1-best-effort
hostname(config-pmap-c)# police output 200000 37500
hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)# police output 1000000 37500

hostname(config-pmap-c)# service-policy qos interface outside
hostname(config)# priority-queue outside
hostname(config-priority-queue)# queue-limit 2048
hostname(config-priority-queue)# tx-ring-limit 256
```



## QoS コンフィギュレーションの表示

ここでは、次の項目について説明します。

- [QoS ポリシーマップ コンフィギュレーションの表示 \(P.21-18\)](#)
- [インターフェイスのプライオリティキュー コンフィギュレーションの表示 \(P.21-18\)](#)

## QoS サービス ポリシー コンフィギュレーションの表示

QoS ポリシーマップを実装するサービス ポリシーを含めて、現在のサービス ポリシーをすべて表示するには、特権 EXEC モードで **show service-policy** コマンドを使用します。**police** キーワードまたは **priority** キーワードを使用すると、**police** コマンドまたは **priority** コマンドが含まれているポリシーに出力を限定できます。



(注)

このコマンドは、プライオリティ統計情報およびポリシング統計情報の表示に使用するコマンドと同じものです。

次の例は、**police** キーワードを使用した **show service-policy** の出力を示しています。

```
hostname# show service-policy police

Global policy:
  Service-policy: global_fw_policy

Interface outside:
  Service-policy: qos
  Class-map: browse
    police Interface outside:
      cir 56000 bps, bc 10500 bytes
      conformed 10065 packets, 12621510 bytes; actions: transmit
      exceeded 499 packets, 625146 bytes; actions: drop
      conformed 5600 bps, exceed 5016 bps
  Class-map: cmap2
    police Interface outside:
      cir 200000 bps, bc 37500 bytes
      conformed 17179 packets, 20614800 bytes; actions: transmit
      exceeded 617 packets, 770718 bytes; actions: drop
      conformed 198785 bps, exceed 2303 bps
```

次の例は、**priority** キーワードを使用した **show service-policy** の出力を示しています。

```
hostname# show service-policy priority

Global policy:
  Service-policy: global_fw_policy

Interface outside:
  Service-policy: qos
  Class-map: TG1-voice
    Priority:
      Interface outside: aggregate drop 0, aggregate transmit 9383
```

## QoS ポリシーマップ コンフィギュレーションの表示

**police** コマンドおよび **priority** コマンドが含まれているポリシーマップを含めて、すべてのポリシーマップを表示するには、特権 EXEC モードで次のコマンドを使用します。

```
hostname# show running-config policy-map
```

上記の例の場合、このコマンドの出力は次のようになります。

```
hostname# show running-config policy-map
!
policy-map test
  class class-default
policy-map inbound_policy
  class ftp-port
    inspect ftp strict inbound_ftp
policy-map qos
  class browse
    police 56000 10500
  class TG1-voice
    priority
  class TG1-BestEffort
    police 200000 37500
```

## インターフェイスのプライオリティキュー コンフィギュレーションの表示

インターフェイスのプライオリティキュー コンフィギュレーションを表示するには、グローバル コンフィギュレーション モードで **show running-config priority-queue** コマンドを入力します。次の例で、「test」というインターフェイスのプライオリティキュー コンフィギュレーションを示します。

```
hostname(config)# show running-config priority-queue test
priority-queue test
  queue-limit 2048
  tx-ring-limit 256
hostname(config)#
```

## QoS 統計情報の表示

ここでは、次の項目について説明します。

- [QoS ポリシング統計情報の表示 \(P.21-19\)](#)
- [QoS プライオリティ統計情報の表示 \(P.21-19\)](#)
- [QoS プライオリティキュー統計情報の表示 \(P.21-20\)](#)

### QoS ポリシング統計情報の表示

トラフィック ポリシングに関する QoS 統計情報を表示するには、特権 EXEC モードで **show service-policy** コマンドと **police** キーワードを次のように使用します。

```
hostname# show service-policy police
```



(注)

このコマンドは、**police** キーワードが含まれているポリシーのコンフィギュレーションの表示に使用するコマンドと同じものです。

たとえば、次のコマンドでは、**police** コマンドと関連統計情報が含まれているサービス ポリシーを表示しています。

```
hostname# show service-policy police

Global policy:
  Service-policy: global_fw_policy

Interface outside:
  Service-policy: qos
  Class-map: browse
    police Interface outside:
      cir 56000 bps, bc 10500 bytes
      conformed 10065 packets, 12621510 bytes; actions: transmit
      exceeded 499 packets, 625146 bytes; actions: drop
      conformed 5600 bps, exceed 5016 bps
  Class-map: cmap2
    police Interface outside:
      cir 200000 bps, bc 37500 bytes
      conformed 17179 packets, 20614800 bytes; actions: transmit
      exceeded 617 packets, 770718 bytes; actions: drop
      conformed 198785 bps, exceed 2303 bps
```

### QoS プライオリティ統計情報の表示

**priority** コマンドを実装するサービス ポリシーの統計情報を表示するには、特権 EXEC モードで **show service-policy** コマンドと **priority** キーワードを使用します。

```
hostname# show service-policy priority
```



(注)

このコマンドは、**priority** キーワードが含まれているポリシーのコンフィギュレーションの表示に使用するコマンドと同じものです。

たとえば、次のコマンドでは、**priority** コマンドと関連統計情報が含まれているサービス ポリシーを表示しています。

```
hostname# show service-policy priority
Global policy:
  Service-policy: global_fw_policy
Interface outside:
  Service-policy: qos
  Class-map: TGI-voice
  Priority:
    Interface outside: aggregate drop 0, aggregate transmit 9383
```



(注)

「aggregate drop」は、このインターフェイスでの合計ドロップ数を示しています。「aggregate transmit」は、このインターフェイスで送信されたパケットの合計数を示しています。

## QoS プライオリティキュー統計情報の表示

インターフェイスのプライオリティキュー統計情報を表示するには、特権 EXEC モードで **show priority-queue statistics** コマンドを実行します。ベストエフォート (BE) キューと低遅延キュー (LLQ) の両方の統計情報が表示されます。次の例で、**test** というインターフェイスに対する **show priority-queue statistics** コマンドの使用方法和、そのコマンド出力を示します。

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type      = BE
Packets Dropped = 0
Packets Transmit = 0
Packets Enqueued = 0
Current Q Length = 0
Max Q Length    = 0

Queue Type      = LLQ
Packets Dropped = 0
Packets Transmit = 0
Packets Enqueued = 0
Current Q Length = 0
Max Q Length    = 0
hostname#
```

この統計情報レポートの項目の意味は、次のとおりです。

- 「Packets Dropped」は、このキューでドロップされたパケットの合計数を示します。
- 「Packets Transmit」は、このキューで送信されたパケットの合計数を示します。
- 「Packets Enqueued」は、このキューに入れられたパケットの合計数を示します。
- 「Current Q Length」は、このキューの現在の深さを示します。
- 「Max Q Length」は、このキューで発生した最大の深さを示します。



# アプリケーション層プロトコル検査の設定

この章では、アプリケーション層プロトコル検査の設定方法について説明します。検査エンジンは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。アプリケーション層プロトコルでは、高速パスでパケットを渡すのではなく、セキュリティ アプライアンスが詳細なパケット検査を行う必要があります（高速パスの詳細については、[P.1-4 の「ステートフル インスペクションの概要」](#)を参照してください）。そのため、検査エンジンはスループット全体に影響することがあります。

いくつかの一般的な検査エンジンはセキュリティ アプライアンス上でデフォルトでイネーブルになっていますが、ネットワークによっては、その他の検査エンジンをイネーブルにしなければならない場合があります。次の事項について説明します。

- [検査エンジンの概要 \(P.22-2\)](#)
  - [アプリケーション プロトコル検査を使用するタイミング \(P.22-2\)](#)
  - [検査に関する制限事項 \(P.22-2\)](#)
  - [デフォルトの検査ポリシー \(P.22-3\)](#)
- [アプリケーション検査の設定 \(P.22-5\)](#)
- [CTIQBE 検査 \(P.22-9\)](#)
- [DNS 検査 \(P.22-12\)](#)
- [FTP 検査 \(P.22-20\)](#)
- [GTP 検査 \(P.22-24\)](#)
- [H.323 検査 \(P.22-31\)](#)
- [HTTP 検査 \(P.22-35\)](#)
- [ICMP 検査 \(P.22-39\)](#)
- [ICMP エラー検査 \(P.22-39\)](#)
- [ILS 検査 \(P.22-40\)](#)
- [MGCP 検査 \(P.22-41\)](#)
- [NetBIOS 検査 \(P.22-45\)](#)
- [PPTP 検査 \(P.22-46\)](#)
- [RSH 検査 \(P.22-46\)](#)
- [RTSP 検査 \(P.22-47\)](#)
- [SIP 検査 \(P.22-49\)](#)

- [Skinny \(SCCP\) 検査 \(P.22-52\)](#)
- [SMTP および拡張 SMTP 検査 \(P.22-54\)](#)
- [SNMP 検査 \(P.22-55\)](#)
- [SQL\\*Net 検査 \(P.22-56\)](#)
- [Sun RPC 検査 \(P.22-57\)](#)
- [TFTP 検査 \(P.22-60\)](#)
- [XDMCP 検査 \(P.22-60\)](#)

## 検査エンジンの概要

ここでは、次の項目について説明します。

- [アプリケーション プロトコル検査を使用するタイミング \(P.22-2\)](#)
- [検査に関する制限事項 \(P.22-2\)](#)
- [デフォルトの検査ポリシー \(P.22-3\)](#)

## アプリケーション プロトコル検査を使用するタイミング

ユーザが接続を確立すると、セキュリティ アプライアンスはアクセスリストと照合してパケットをチェックし、アドレス変換を作成します。次に、高速パスでのセッション用にエントリを作成し、後続のパケットが時間のかかるチェックをバイパスできるようにします。ただし、高速パスは、予測可能なポート番号に基づいており、パケット内部のアドレス変換を実行しません。

多くのプロトコルは、セカンダリの TCP ポートまたは UDP ポートを開きます。予約済みポート上の初期セッションは、ダイナミックに割り当てられたポート番号をネゴシエートするために使用されます。

また、送信元アドレスと一致する必要がある IP アドレスをパケットに埋め込むアプリケーションもあります。送信元アドレスは、通常、セキュリティ アプライアンスを通過するときに変換されます。

これらのアプリケーションを使用する場合は、アプリケーション検査をイネーブルにする必要があります。

IP アドレスを埋め込むサービスに対してアプリケーション検査をイネーブルにすると、セキュリティ アプライアンスは、埋め込まれたアドレスを変換し、チェックサムや変換の影響を受けたその他のフィールドを更新します。

ダイナミックに割り当てられたポートを使用するサービスに対してアプリケーション検査をイネーブルにすると、セキュリティ アプライアンスは、セッションを監視して、ダイナミックに割り当てられたポートを特定し、所定のセッションの間、それらのポートでのデータ交換を許可します。

## 検査に関する制限事項

アプリケーション プロトコル検査では、次の制限事項があります。

- 検査が必要なマルチメディア セッションのステート情報は、ステートフル フェールオーバーのステートリンクで渡されません。
- フラグメント化された IP パケットの場合は、最初のフラグメントだけが検査されます。
- セグメント化された TCP パケットの場合は、メッセージがセグメント間に分かれていると、セキュリティ アプライアンスはパケットを検査できません。
- 一部の検査エンジンは、PAT、NAT、外部 NAT、または同一セキュリティ インターフェイス間の NAT をサポートしません。

## デフォルトの検査ポリシー

デフォルトでは、すべてのデフォルト アプリケーション検査トラフィックに一致するポリシーがコンフィギュレーションに含まれ、すべての検査がすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。デフォルト アプリケーション検査トラフィックには、各プロトコルのデフォルト ポートへのトラフィックが含まれます。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合（たとえば、標準以外のポートに検査を適用する場合や、デフォルトでイネーブルになっていない検査を追加する場合）は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。

表 22-1 に、サポートされているすべての検査、デフォルトのクラスマップで使用されるデフォルトポート、およびデフォルトでオンになっている検査エンジン（太字表記）を示します。NAT に関する制限事項についてもこの表に示します。

表 22-1 サポートされているアプリケーション検査エンジン

| アプリケーション <sup>1</sup>                  | デフォルトポート                                         | NAT に関する制限事項                                                      | 標準 <sup>2</sup>                                   | コメント                                                                                                |
|----------------------------------------|--------------------------------------------------|-------------------------------------------------------------------|---------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| CTIQBE                                 | TCP/2748                                         | —                                                                 | —                                                 | —                                                                                                   |
| DNS over UDP                           | UDP/53                                           | NAT サポートは、WINS 経由の名前解決では使用できません。                                  | RFC 1123                                          | PTR レコードは変更されません。                                                                                   |
| FTP                                    | TCP/21                                           | —                                                                 | RFC 959                                           | —                                                                                                   |
| GTP                                    | UDP/3386<br>UDP/2123                             | —                                                                 | —                                                 | 特別なライセンスが必要。                                                                                        |
| <b>H.323 H.225</b><br>および <b>RAS</b>   | TCP/1720<br>UDP/1718<br>UDP (RAS)<br>1718 ~ 1719 | 同一セキュリティ インターフェイス上の NAT はサポートされません。<br><br>スタティック PAT はサポートされません。 | ITU-T H.323、<br>H.245、<br>H.225.0、<br>Q.931、Q.932 | —                                                                                                   |
| HTTP                                   | TCP/80                                           | —                                                                 | RFC 2616                                          | ActiveX と Java を除去する際の MTU 制限に注意。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、除去の処理は行われません。 |
| ICMP                                   | —                                                | —                                                                 | —                                                 | すべての ICMP トラフィックは、デフォルトのクラスマップで照合されます。                                                              |
| ICMP ERROR                             | —                                                | —                                                                 | —                                                 | すべての ICMP トラフィックは、デフォルトのクラスマップで照合されます。                                                              |
| ILS (LDAP)                             | TCP/389                                          | PAT はサポートされません。                                                   | —                                                 | —                                                                                                   |
| MGCP                                   | UDP/2427、<br>2727                                | —                                                                 | RFC<br>2705bis-05                                 | —                                                                                                   |
| <b>NetBIOS Name<br/>Server over IP</b> | UDP/137、<br>138 (送信元<br>ポート)                     | —                                                                 | —                                                 | NetBIOS は、NBNS UDP ポート 137 および NBDS 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。                   |
| PPTP                                   | TCP/1723                                         | —                                                                 | RFC 2637                                          | —                                                                                                   |
| <b>RSH</b>                             | TCP/514                                          | PAT はサポートされません。                                                   | Berkeley<br>UNIX                                  | —                                                                                                   |

表 22-1 サポートされているアプリケーション検査エンジン（続き）

| アプリケーション <sup>1</sup>   | デフォルトポート             | NAT に関する制限事項                                              | 標準 <sup>2</sup>                      | コメント                                                                                                |
|-------------------------|----------------------|-----------------------------------------------------------|--------------------------------------|-----------------------------------------------------------------------------------------------------|
| RTSP                    | TCP/554              | PAT はサポートされません。<br>外部 NAT はサポートされません。                     | RFC 2326、<br>2327、1889               | HTTP クローキングは処理しません。                                                                                 |
| SIP                     | TCP/5060<br>UDP/5060 | 外部 NAT はサポートされません。<br>同一セキュリティ インターフェイス上の NAT はサポートされません。 | RFC 2543                             | —                                                                                                   |
| SKINNY<br>(SCCP)        | TCP/2000             | 外部 NAT はサポートされません。<br>同一セキュリティ インターフェイス上の NAT はサポートされません。 | —                                    | 一定の条件下で、Cisco IP Phone 設定をアップロード済みの TFTP は処理しません。                                                   |
| SMTP および<br>ESMTP       | TCP/25               | —                                                         | RFC 821, 1123                        | —                                                                                                   |
| SNMP                    | UDP/161、<br>162      | NAT および PAT はサポートされません。                                   | RFC 1155、<br>1157、1212、<br>1213、1215 | v.2 RFC 1902-1908、v.3 RFC 2570-2580                                                                 |
| SQL*Net                 | TCP/1521             | —                                                         | —                                    | v.1 および v.2.                                                                                        |
| Sun RPC over<br>UDP/TCP | UDP/111              | NAT および PAT はサポートされません。                                   | —                                    | デフォルトでイネーブルになっているのは、UDP ポート 111 用の検査だけです。TCP ポート 111 に向かうパケットを検査するには、このポートを検査トラフィックに手動で追加する必要があります。 |
| TFTP                    | UDP/69               | —                                                         | RFC 1350                             | ペイロード IP アドレスは変換されません。                                                                              |
| XDCMP                   | UDP/177              | NAT および PAT はサポートされません。                                   | —                                    | —                                                                                                   |

1. デフォルト ポートに対してデフォルトでイネーブルになっている検査エンジンについては、太字で表記しています。
2. セキュリティ アプライアンスは、これらの標準に準拠していますが、検査対象のパケットには準拠を強制しません。たとえば、FTP コマンドは特定の順序になっている必要がありますが、セキュリティ アプライアンスは、その順序を強制しません。

デフォルト ポリシー コンフィギュレーションには、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
```



## アプリケーション検査の設定

この機能はモジュラ ポリシー フレームワークを使用するため、アプリケーション検査の実装の際には、トラフィックの特定、トラフィックへの検査の適用、およびインターフェイスでの検査のアクティブ化を行います。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。

一部のアプリケーションでは、検査がデフォルトでイネーブルになっています。詳細については、「デフォルトの検査ポリシー」の項を参照してください。検査ポリシーを修正する方法が示されています。

アプリケーション検査を設定するには、次の手順を実行します。

- ステップ 1** 検査を適用するトラフィックを特定するには、**class-map** コマンドを使用してクラスマップを追加します。詳細については、P.18-3 の「クラスマップによるトラフィックの特定」を参照してください。

デフォルトのクラスマップの名前は「inspection\_default」です。このクラスマップは、特殊な **match** コマンド (**match default-inspection-traffic**) を使用してトラフィックと照合することにより、各アプリケーション プロトコルのデフォルト ポートと照合します。

**match access-list** コマンドを **match default-inspection-traffic** コマンドとともに指定すると、照合するトラフィックを特定の IP アドレスに絞り込むことができます。**match default-inspection-traffic** コマンドによって照合するポートが指定されるため、アクセスリストのポートはすべて無視されます。

標準以外のポートと照合する場合は、**match default-inspection-traffic** コマンドを使用しないでください。たとえば、「inspection\_default」クラスマップに追加を行うのではなく、カスタマイズできるクラスマップを新しく作成します。各検査エンジンの標準ポートについては、P.22-3 の「デフォルトの検査ポリシー」を参照してください。

たとえば、デフォルトのクラスマップを使用して、検査を 10.1.1.0 から 192.168.1.0 へのトラフィックに限定するには、次のコマンドを入力します。

```
hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0
hostname(config)# class-map inspection_default
hostname(config-cmap)# match access-list inspect
```

次のコマンドを使用して、クラスマップ全体を表示します。

```
hostname(config-cmap)# show running-config class-map inspection_default
!
class-map inspection_default
  match default-inspection-traffic
  match access-list inspect
!
```

ポート 21 とポート 1056（標準以外のポート）の FTP トラフィックを検査するには、それらのポートを指定するアクセスリストを作成し、新しいクラスマップに割り当てます。検査をイネーブルにするその他のポートも、必ずすべてアクセスリストに含めてください。この例では、ポート 21 とポート 1056 だけを示します。

```
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 21
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 1056
hostname(config)# class-map new_inspection
hostname(config-cmap)# match access-list ftp_inspect
```

**ステップ 2** (オプション) 一部の検査エンジンでは、トラフィックに検査を適用するときに、追加のパラメータを制御できます。ポリシーマップコンフィギュレーションで検査を適用する前に、次のコマンドを使用して追加のパラメータを設定します。

```
hostname(config)# application-map application_map_name
```

*application* には、アプリケーション検査の種類を指定します。次の map コマンドを使用できます。

- **ftp-map**: FTP マップ コンフィギュレーション モードで使えるコマンドの詳細については、[P.22-21](#) の「[検査制御を追加するための FTP マップの設定](#)」を参照してください。
- **gtp-map**: GTP マップ コンフィギュレーション モードで使えるコマンドの詳細については、[P.22-25](#) の「[検査制御を追加するための GTP マップの設定](#)」を参照してください。
- **http-map**: HTTP マップ コンフィギュレーション モードで使えるコマンドの詳細については、[P.22-35](#) の「[検査制御を追加するための HTTP マップの設定](#)」を参照してください。
- **mgcp-map**: MGCP マップ コンフィギュレーション モードで使えるコマンドの詳細については、[P.22-43](#) の「[検査制御を追加するための MGCP マップの設定](#)」を参照してください。
- **snmp-map**: SNMP マップ コンフィギュレーション モードで使えるコマンドの詳細については、[P.22-55](#) の「[SNMP 検査](#)」を参照してください。SNMP 検査をイネーブルにする場合は、拒否する SNMP バージョンを特定する SNMP マップを使用する必要があります。

**ステップ 3** クラスマップ トラフィックで実行する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
```

デフォルトのポリシーマップの名前は「global\_policy」です。このポリシーマップには、[P.22-3](#) の「[デフォルトの検査ポリシー](#)」で示されているデフォルトの検査が含まれています。デフォルトのポリシーを修正する場合（たとえば、検査を追加または削除する場合や、別のクラスマップを特定してアクションを割り当てる場合）は、**global\_policy** を名前として入力します。

**ステップ 4** 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
```

デフォルトのポリシーマップを編集している場合、「inspection\_default」というクラスマップが含まれています。このクラスマップを削除するには、**no class inspection\_default** コマンドを使用します。次に、新しいクラスマップ名を指定して **class** コマンドを新しく入力します。ポリシーマップには、検査アクションを持つクラスを 1 つだけ含めることができます。したがって、デフォルトのクラスを保持したまま、追加の検査を持つ新しいクラスを追加することはできません。

**ステップ 5** 次のコマンドを入力して、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 protocol
```

*protocol* には、次の値のいずれかを指定します。

表 22-2 protocol のキーワード

| キーワード                               | 注意                                                                                                                                                                                                                                                                                                   |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ctiqbe                              | —                                                                                                                                                                                                                                                                                                    |
| dns [maximum-length max-pkt-length] | 最大 DNS パケット長をデフォルト（512）から変更するには、 <b>maximum-length</b> キーワードを使用し、 <b>max-pkt-length</b> に数値を指定します。これよりも長いパケットはドロップされます。DNS パケット長のチェックをディセーブルにするには、 <b>maximum-length</b> キーワードを指定せずに、 <b>inspect dns</b> コマンドを入力します。                                                                                 |
| esmtpt                              | —                                                                                                                                                                                                                                                                                                    |
| ftp [strict [map_name]]             | <b>strict</b> キーワードを使用すると、Web ブラウザが FTP 要求内の埋め込みコマンドを送信できないようにすることで、保護されたネットワークのセキュリティを向上できます。詳細については、 <a href="#">P.22-20 の「strict オプションの使用」</a> を参照してください。<br><br>ステップ 2 で FTP マップを追加した場合は、このコマンドでマップ名を指定します。FTP マップを追加する方法の詳細については、 <a href="#">P.22-21 の「検査制御を追加するための FTP マップの設定」</a> を参照してください。 |
| gtp [map_name]                      | ステップ 2 で GTP マップを追加した場合は、このコマンドでマップ名を指定します。GTP マップを追加する方法の詳細については、 <a href="#">P.22-25 の「検査制御を追加するための GTP マップの設定」</a> を参照してください。                                                                                                                                                                     |
| h323 h225                           | —                                                                                                                                                                                                                                                                                                    |
| h323 ras                            | —                                                                                                                                                                                                                                                                                                    |
| http [map_name]                     | ステップ 2 で HTTP マップを追加した場合は、このコマンドでマップ名を指定します。HTTP マップを追加する方法の詳細については、 <a href="#">P.22-35 の「検査制御を追加するための HTTP マップの設定」</a> を参照してください。                                                                                                                                                                  |
| icmp                                | —                                                                                                                                                                                                                                                                                                    |
| icmp error                          | —                                                                                                                                                                                                                                                                                                    |
| ils                                 | —                                                                                                                                                                                                                                                                                                    |
| mgcp [map_name]                     | ステップ 2 で MGCP マップを追加した場合は、このコマンドでマップ名を指定します。MGCP マップを追加する方法の詳細については、 <a href="#">P.22-43 の「検査制御を追加するための MGCP マップの設定」</a> を参照してください。                                                                                                                                                                  |
| netbios                             | —                                                                                                                                                                                                                                                                                                    |
| pptp                                | —                                                                                                                                                                                                                                                                                                    |
| rsh                                 | —                                                                                                                                                                                                                                                                                                    |
| rtsp                                | —                                                                                                                                                                                                                                                                                                    |
| sip                                 | —                                                                                                                                                                                                                                                                                                    |
| skinny                              | —                                                                                                                                                                                                                                                                                                    |
| snmp map_name                       | SNMP 検査エンジンには、指定した SNMP バージョンを拒否する SNMP マップが必要です。SNMP マップを追加する方法の詳細については、 <a href="#">P.22-55 の「SNMP 検査」</a> を参照してください。                                                                                                                                                                              |

表 22-2 protocol のキーワード (続き)

| キーワード  | 注意                                                                                                                              |
|--------|---------------------------------------------------------------------------------------------------------------------------------|
| sqlnet | —                                                                                                                               |
| sunrpc | デフォルトのクラスマップには、UDP ポート 111 が含まれています。TCP ポート 111 の Sun RPC 検査をイネーブルにする場合は、そのポートをクラスマップに追加する必要があります。その場合、デフォルトのクラスマップは使用しないでください。 |
| tftp   | —                                                                                                                               |
| xdmcp  | —                                                                                                                               |

- ステップ 6** 1 つ以上のインターフェイスでポリシーマップをアクティブにするには、次のコマンドを入力します。

```
hostname(config)# service-policy polycymap_name {global | interface interface_name}
```

ここで、**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 1 つのインターフェイスに適用します。デフォルトでは、デフォルトのポリシーマップ「global\_policy」がグローバルに適用されます。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを 1 つだけ適用できます。

## CTIQBE 検査

この項では、CTIQBE アプリケーション検査について説明します。ここでは、次の項目について説明します。

- [CTIQBE 検査の概要 \(P.22-9\)](#)
- [制限事項 \(P.22-9\)](#)
- [CTIQBE 検査の確認と監視 \(P.22-10\)](#)

### CTIQBE 検査の概要

CTIQBE プロトコル検査では、NAT、PAT、および双方向 NAT がサポートされます。これによって、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが、セキュリティ アプライアンスを越えてコール セットアップを行うために、Cisco CallManager と問題なく連携動作するようになります。

TAPI と 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 TSP が Cisco CallManager と通信するために使用されます。

### 制限事項

CTIQBE アプリケーション検査の使用時に適用される制限を次にまとめます。

- CTIQBE アプリケーション検査は、**alias** コマンドを使用するコンフィギュレーションをサポートしません。
- 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 ctique** 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ます。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、セキュリティ アプライアンスを介して 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 の動作するシステムで Cisco TSP 設定のタイムアウト値を増やしてください。

次に、CTIQBE アプリケーション検査を特定の事例で使用する際に、特別に注意が必要な事項をまとめます。

- 2 つの Cisco IP SoftPhone が異なる Cisco CallManager に登録されていて、各 CallManager がセキュリティ アプライアンス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 つ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いる状態で、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ことが必要のためです。
- 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、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。これは Cisco IP SoftPhone の登録を成功させるためです。CTIQBE 受信ポート (TCP 2748) は固定されていて、Cisco CallManager、Cisco IP SoftPhone、Cisco TSP のいずれにおいてもユーザによる設定はできません。

## CTIQBE 検査の確認と監視

**show ctiqbe** コマンドは、セキュリティ アプライアンスを越えて確立されている CTIQBE セッションに関する情報を表示します。CTIQBE 検査エンジンで割り当てられたメディア接続に関する情報が表示されます。

次の条件における **show ctiqbe** コマンドの出力例を示します。セキュリティ アプライアンス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 CallManager 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、すでに CallManager に登録されています。デバイスの内部アドレスおよび RTP 受信ポートは 172.29.1.99 の UDP ポート 1028 に PAT 変換されています。RTCP 受信ポートは UDP 1029 に PAT 変換されています。

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は、その外部インターフェイスに PAT 変換されている場合に限り表示されます。この行は、CallManager が内部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部インターフェイスに変換されている場合は、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 にある別の電話機の間で確立されていることを示します。他の電話機の RTP および RTCP 受信ポートは、UDP 26822 および 26823 です。セキュリティ アプライアンスは 2 番目の電話機と 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、他の電話機は、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 レッグは、Device ID 27 および Call ID 0 で確認できます。

これらの CTIBQE 接続の **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 検査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

この項では、DNS アプリケーション検査について説明します。ここでは、次の項目について説明します。

- [DNS アプリケーション検査の動作 \(P.22-12\)](#)
- [DNS リライトの動作 \(P.22-13\)](#)
- [DNS リライトの設定 \(P.22-14\)](#)
- [DNS 検査の確認と監視 \(P.22-19\)](#)

### DNS アプリケーション検査の動作

セキュリティ アプライアンスは DNS 応答を転送するとすぐに、DNS クエリーと関連付けられた DNS セッションを切断します。また、セキュリティ アプライアンスはメッセージ交換を監視し、DNS 応答の ID が、DNS クエリーの ID と一致することを確認します。

DNS 検査をイネーブルにすると（デフォルト）、セキュリティ アプライアンスは次の追加のタスクを実行します。

- **alias**、**static**、および **nat** コマンドを使用して作成されたコンフィギュレーションに基づいて、DNS レコードを変換します（DNS リライト）。変換は、DNS 応答の A レコードだけに適用されます。そのため、PTR レコードを必要とする逆ルックアップは、DNS リライトの影響を受けません。



(注)

1 つの A レコードに複数の PAT 規則が適用可能で、使用する PAT 規則があいまいなため、DNS リライトは PAT には適用できません。

- 最大 DNS メッセージ長を指定します（デフォルトは 512 バイト、最大長は 65535 バイト）。セキュリティ アプライアンスが必要に応じてリアセンブリを実行し、設定された最大長よりもパケット長が短いことを確認します。セキュリティ アプライアンスは、最大長を超えるパケットをドロップします。



(注)

**maximum-length** オプションを指定せずに **inspect dns** コマンドを入力した場合、DNS パケットサイズはチェックされません。

- ドメイン名の長さを 255 バイトに制限し、ラベルの長さを 63 バイトに制限します。
- DNS メッセージに圧縮ポインタが出現した場合、ポインタが参照するドメイン名の整合性を確認します。
- 圧縮ポインタのループが終了するかどうかを確認します。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元 / 宛先 IP アドレス、送信元 / 宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つのみ作成されます。DNS ID は *app\_id* で追跡され、各 *app\_id* のアイドルタイマーは独立して実行されます。

*app\_id* の有効期限はそれぞれ独立して満了するため、正当な DNS 応答がセキュリティ アプライアンスを通過できるのは、限られた期間内のみであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力した場合、新しい DNS セッションによってリセットされている 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 接続の性質によるものであり、仕様です。



## DNS リライトの動作

DNS 検査がイネーブルであるとき、DNS リライトは、任意のインターフェイスから送信された DNS メッセージの NAT を完全にサポートします。

内部の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 サーバから送信される内部アドレスの 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 検査エンジンがディセーブルである場合、A レコードは変換されません。

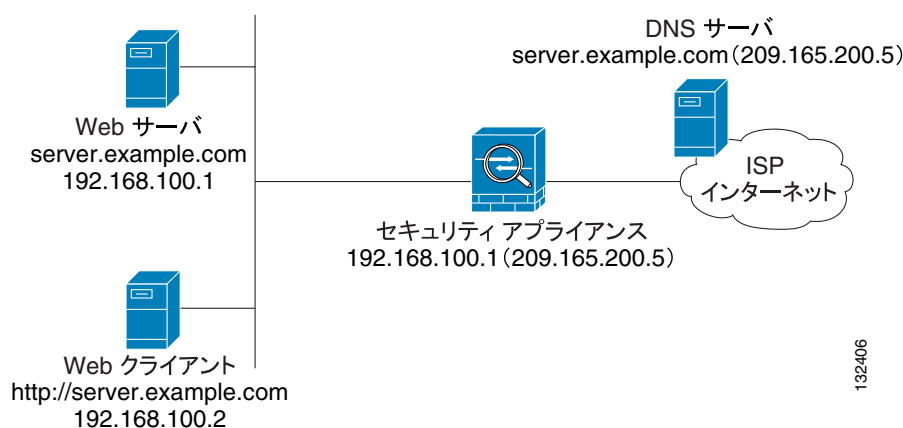
DNS 検査がイネーブルのままである間、**alias**、**static**、または **nat** コマンドを使用して DNS リライトを設定できます。必要なコンフィギュレーションの詳細については、[P.22-14 の「DNS リライトの設定」](#)を参照してください。

DNS リライトは、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」アドレス）をプライベート アドレス（「実際の」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 22-1](#) では、DNS サーバは外部(ISP)ネットワークにあります。サーバの実アドレス(192.168.100.1)は、**static** コマンドで ISP 割り当てアドレス (209.165.200.5) にマッピングされています。内部インターフェイスの Web クライアントが <http://server.example.com> という URL を持つ Web サーバにアクセスを試行する場合、Web クライアントは、Web サーバの IP アドレスの解決を求める DNS 要求を DNS サーバに送信します。セキュリティ アプライアンスは、IP ヘッダーにあるルーティングできない送信元アドレスを変換し、外部インターフェイスの ISP ネットワークに要求を転送します。DNS 応答が返されると、セキュリティ アプライアンスはアドレス変換を宛先アドレスだけではなく、DNS 応答の A レコードに含まれる、埋め込まれた Web サーバの IP アドレスにも適用します。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 サーバとの接続に使用する正しいアドレスを取得します。このような事例の設定手順については、[P.22-15 の「2つの NAT ゾーンを持つ DNS リライトの設定」](#)を参照してください。

図 22-1 DNS 応答のアドレスの変換 (DNS リライト)



DNS リライトは、DNS 要求を作成するクライアントが DMZ ネットワークにあり、DNS サーバが内部インターフェイスにある場合にも機能します。この事例の詳細と設定手順については、[P.22-16 の「3つの NAT ゾーンを持つ DNS リライト」](#)を参照してください。

## DNS リライトの設定

DNS リライトは、**alias**、**static**、または **nat** コマンドを使用して設定します。**alias** コマンドと **static** コマンドは、入れ替えが可能です。ただし、新しく構成するときには、より正確であいまいさがないう **static** コマンドを使用することを推奨します。また、**static** コマンドを使用する場合、DNS リライトは省略可能です。

この項では、**alias** および **static** コマンドを使用して DNS リライトを設定する方法について説明します。単純な事例と、より複雑な事例で、**static** コマンドを使用するための設定手順を示します。**nat** コマンドの使用は、**static** コマンドの使用に似ていますが、DNS リライトはスタティック マッピングではなくダイナミック変換に基づきます。

ここでは、次の項目について説明します。

- DNS リライト用の **static** コマンドの使用 (P.22-14)
- DNS リライト用の **static** コマンドの使用 (P.22-14)
- 2つの NAT ゾーンを持つ DNS リライトの設定 (P.22-15)
- 3つの NAT ゾーンを持つ DNS リライト (P.22-16)
- 3つの NAT ゾーンを持つ DNS リライトの設定 (P.22-18)

**alias**、**nat**、および **static** コマンドの詳細なシンタックスおよびその他の機能については、『Cisco Security Appliance Command Reference』の対応するコマンドのページを参照してください。

### DNS リライト用の **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ある IP ネットワークのアドレスが、異なるインターフェイスの別の IP ネットワークのアドレスに変換されます。このコマンドのシンタックスは次のとおりです。

```
hostname(config)# static (real_ifc,mapped_ifc) mapped-address real-address dns
```

次の例では、内部インターフェイスのアドレス 192.168.100.10 を外部インターフェイスの 209.165.200.5 に変換するように指定しています。

```
hostname(config)# static (inside,outside) 209.165.200.225 192.168.100.10 dns
```



(注)

**nat** コマンドの使用は、**static** コマンドの使用に似ていますが、DNS リライトはスタティック マッピングではなくダイナミック変換に基づきます。

### DNS リライト用の **alias** コマンドの使用

**alias** コマンドを使用すると、セキュリティ アプライアンスは、任意のインターフェイスにある IP ネットワークのアドレスを、異なるインターフェイスを通じて接続されている別の IP ネットワークのアドレスに変換します。このコマンドのシンタックスは次のとおりです。

```
hostname(config)# alias (interface_name) mapped-address real-address
```

次の例では、内部インターフェイス以外の任意のインターフェイスの実アドレス (192.168.100.10) が、内部インターフェイスのマッピング アドレス (209.165.200.225) に変換されています。192.168.100.10 の場所が正確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)

**alias** コマンドを使用して DNS リライトを設定する場合、マッピング アドレスに対してプロキシ ARP が実行されます。これを防ぐには、**alias** コマンドを入力した後、**sysopt noproxyarp** コマンドを入力して、プロキシ ARP をディセーブルにします。

## 2 つの NAT ゾーンを持つ DNS リライトの設定

図 22-1 で示す DNS リライトと類似の事例を実装するには、次の手順を実行します。

**ステップ 1** Web サーバのスタティック変換を次のように作成します。

```
hostname(config)# static (real_ifc,mapped_ifc) mapped-address real-address netmask  
255.255.255.255 dns
```

引数は次のとおりです。

- *real\_ifc* : 実際のアドレスに接続されているインターフェイスの名前。
- *mapped\_ifc* : アドレスのマッピング先とするインターフェイスの名前。
- *mapped-address* : Web サーバの変換後の IP アドレス。
- *real-address* : Web サーバの実際の IP アドレス。

**ステップ 2** Web サーバが HTTP 要求を受信す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 extended 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 サーバの変換後の IP アドレス。

*port* : Web サーバが HTTP 要求を受信する 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マッピング インターフェイスに適用します。これを行うには、**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 mapped_ifc
```

**ステップ 4** DNS 検査がディセーブルの場合、または最大 DNS パケット長を変更する場合は、DNS 検査を設定します。デフォルトで、DNS アプリケーション検査は、最大 DNS パケット長を 512 バイトとしてイネーブルになっています。設定手順については、P.22-5 の「アプリケーション検査の設定」を参照してください。

**ステップ 5** パブリック DNS サーバで、Web サーバの A レコードを次のように追加します。

```
domain-qualified-hostname. IN A mapped-address
```

*domain-qualified-hostname* には、ホスト名をドメイン サフィックスとともに指定します（例、*server.example.com*）。ホスト名の後ろのピリオドは重要です。*mapped-address* には、Web サーバの変換後の IP アドレスを指定します。

次の例では、図 22-1 に示されているシナリオでセキュリティ アプライアンスを設定しています。DNS 検査はすでにイネーブルになっていることが前提です。

```
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
```

このコンフィギュレーションには、DNS サーバの次の A レコードが必要です。

```
server.example.com. IN A 209.165.200.225
```

### 3 つの NAT ゾーンを持つ DNS リライト

図 22-2 では、DNS 検査によってどのようにして NAT が最小コンフィギュレーションの DNS サーバと透過的に連携動作するかを示す、より複雑な事例を示します。このような事例の設定手順については、P.22-18 の「3 つの NAT ゾーンを持つ DNS リライトの設定」を参照してください。

図 22-2 3 つの NAT ゾーンを持つ DNS リライト

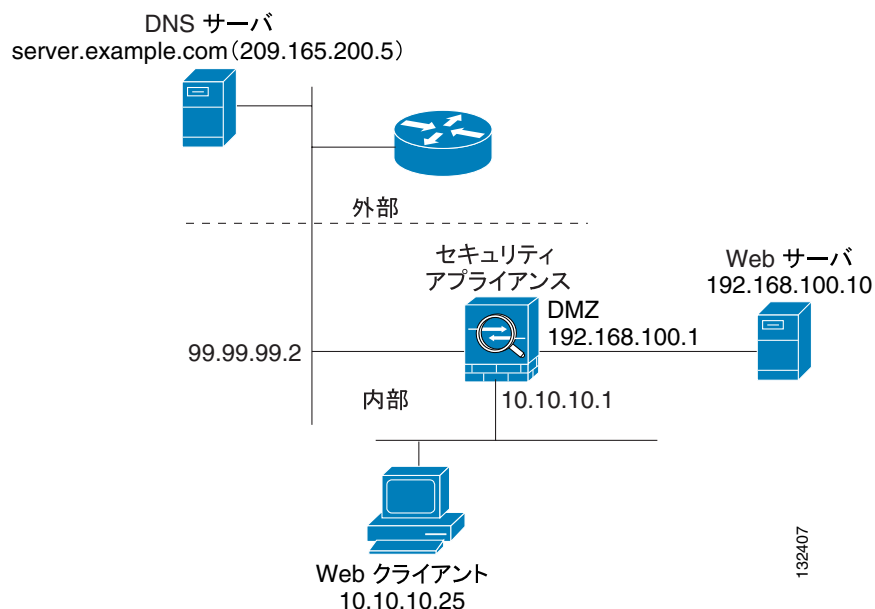


図 22-2 で、Web サーバ *server.example.com* の実アドレスは、セキュリティ アプライアンスの DMZ インターフェイスの 192.168.100.10 です。IP アドレス 10.10.10.25 の Web クライアントが内部インターフェイスにあり、パブリック DNS サーバが外部インターフェイスにあります。サイト NAT ポリシーは次のとおりです。

- 外部 DNS サーバは *server.example.com* の信頼できるアドレス レコードを保持しています。
- 外部ネットワークのホストは、ドメイン名が *server.example.com* の Web サーバに、外部 DNS サーバまたは IP アドレス 209.165.200.5 を使用して接続できます。

- 内部ネットワークのクライアントは、ドメイン名が `server.example.com` の Web サーバに、外部 DNS サーバまたは IP アドレス `192.168.100.10` を使用してアクセスできます。

いずれかのインターフェイスのホストまたはクライアントは、DMZ Web サーバにアクセスするときに、パブリック DNS サーバに対して `server.example.com` の A レコードを問い合わせます。DNS サーバは、`server.example.com` がアドレス `209.165.200.5` にバインドされていることを示す A レコードを返します。

外部ネットワークの Web クライアントが `http://server.example.com` にアクセスを試みたときのイベントシーケンスは次のとおりです。

- Web クライアントを実行しているホストが DNS サーバに、`server.example.com` の IP アドレスを求める要求を送信します。
- DNS サーバが応答で IP アドレス `209.165.200.225` を示します。
- Web クライアントが HTTP 要求を `209.165.200.225` に送信します。
- 外部ホストからのパケットがセキュリティ アプライアンスの外部インターフェイスに到達します。
- スタティック規則によってアドレス `209.165.200.225` が `192.168.100.10` に変換され、セキュリティ アプライアンスがパケットを DMZ の Web サーバに誘導します。

内部ネットワークの Web クライアントが `http://server.example.com` にアクセスを試みたときのイベントシーケンスは次のとおりです。

- Web クライアントを実行しているホストが DNS サーバに、`server.example.com` の IP アドレスを求める要求を送信します。
- DNS サーバが応答で IP アドレス `209.165.200.225` を示します。
- セキュリティ アプライアンスが DNS 応答を受信し、その応答を DNS アプリケーション検査エンジンに送信します。
- DNS アプリケーション検査エンジンは、次の処理を行います。

- 埋め込まれた 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。この例では、次のスタティック コンフィギュレーションが検索されます。

```
static (dmz,outside) 209.165.200.225 192.168.100.10 dns
```

- dns** オプションが含まれているため、次のように A レコードをリライトするスタティック規則が使用されます。

```
[outside]:209.165.200.225 --> [dmz]:192.168.100.10
```



(注)

**static** コマンドに **dns** オプションが含まれていない場合、DNS リライトは実行されず、他のパケット処理が継続されます。

- 内部 Web クライアントと通信するときに、Web サーバアドレス `[dmz]:192.168.100.10` を変換する NAT が検索されます。

適用可能な NAT 規則がない場合、アプリケーション検査は終了します。

NAT 規則 (`nat` または `static`) が適用可能な場合は、**dns** オプションも指定されている必要があります。**dns** オプションが指定されていなかった場合、ステップ **b** の A レコードリライトは取り消され、他のパケット処理が継続されます。

- セキュリティ アプライアンスが DMZ インターフェイスの `server.example.com` に HTTP 要求を送信します。

### 3 つの NAT ゾーンを持つ DNS リライトの設定

図 22-2 の事例の NAT ポリシーをイネーブルにするには、次の手順を実行します。

**ステップ 1** DMZ ネットワークの Web サーバのスタティック変換を次のように作成します。

```
hostname(config)# static (dmz,outside) mapped-address real-address dns
```

引数は次のとおりです。

- *dmz*：セキュリティ アプライアンスの DMZ インターフェイスの名前。
- *outside*：セキュリティ アプライアンスの外部インターフェイスの名前。
- *mapped-address*：Web サーバの変換後の IP アドレス。
- *real-address*：Web サーバの実際の IP アドレス。

**ステップ 2** Web サーバが HTTP 要求を受信す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 extended 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 サーバの変換後の IP アドレス。

*port*：Web サーバが HTTP 要求を受信する 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。これを行うには、**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の場合、または最大 DNS パケット長を変更する場合は、DNS 検査を設定します。デフォルトで、DNS アプリケーション検査は、最大 DNS パケット長を 512 バイトとしてイネーブルになっています。設定手順については、P.22-5 の「アプリケーション検査の設定」を参照してください。

**ステップ 5** たとえば、パブリック DNS サーバで、A レコードを example.com zone に追加します。

```
domain-qualified-hostname. IN A mapped-address
```

*domain-qualified-hostname* には、ホスト名をドメイン サフィックスとともに指定します（例、server.example.com）。ホスト名の後ろのピリオドは重要です。*mapped-address* には、Web サーバの変換後の IP アドレスを指定します。

次の例では、図 22-2 に示されているシナリオでセキュリティ アプライアンスを設定しています。DNS 検査はすでにイネーブルになっていることが前提です。

```
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
```

このコンフィギュレーションには、DNS サーバの次の A レコードが必要です。

```
server.example.com. IN A 209.165.200.225
```

## DNS 検査の確認と監視

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 サーバを使用する接続の場合、show conn コマンド出力で、接続の送信元ポートが DNS サーバの IP アドレスに置き換えられることがあります。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元 / 宛先 IP アドレス、送信元 / 宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つのみ作成されます。DNS ID は app\_id で追跡され、各 app\_id のアイドル タイマーは独立して実行されます。

app\_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答がセキュリティ アプライアンスを通過できるのは、限られた期間内のみであり、リソースの継続使用はできません。ただし、show conn コマンドを入力した場合、新しい DNS セッションによってリセットされている 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 接続の性質によるものであり、仕様です。

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

この項では、FTP 検査エンジンについて説明します。ここでは、次の項目について説明します。

- [FTP 検査の概要 \(P.22-20\)](#)
- [strict オプションの使用 \(P.22-20\)](#)
- [検査制御を追加するための FTP マップの設定 \(P.22-21\)](#)
- [FTP 検査の確認と監視 \(P.22-23\)](#)

### FTP 検査の概要

FTP アプリケーション検査機能は、FTP セッションを検査し、次の 4 つのタスクを実行します。

- ダイナミックなセカンダリ データ接続の準備
- FTP コマンド応答シーケンスの追跡
- 監査証跡の生成
- 埋め込み IP アドレスの変換

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 チャンネルが用意されます。これらのチャンネルのポートは、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。セカンダリ チャンネルは、ファイル アップロード、ファイル ダウンロード、またはディレクトリ リスティング イベントへの応答で割り当てられます。



(注)

**no inspect ftp** コマンドを使用して、FTP 検査エンジンをディセーブルにすると、発信ユーザはパッシブモードだけで接続を開始でき、着信 FTP はすべてディセーブルになります。

### strict オプションの使用

**strict** オプションを **inspect ftp** コマンドで使用すると、Web ブラウザが FTP 要求内の埋め込みコマンドを送信できなくなるため、保護されたネットワークのセキュリティが向上します。



(注)

セキュリティ アプライアンスの通過が許可されない FTP コマンドを指定するには、[P.22-21 の「検査制御を追加するための FTP マップの設定」](#)を参照して FTP マップを作成します。

インターフェイスで **strict** オプションをイネーブルにすると、FTP 検査によって次の動作が強制的に適用されます。

- FTP コマンドが確認応答されてからでないと、セキュリティ アプライアンスは新しいコマンドを許可しません。
- セキュリティ アプライアンスは、埋め込みコマンドを送信する接続をドロップします。
- 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チェックされます。



注意

**strict** オプションを使用すると、FTP RFC に厳密に準拠していない FTP クライアントは失敗することがあります。



**strict** オプションがイネーブルになっている場合、各 FTP コマンドおよび応答シーケンスが追跡され、次の異常なアクティビティがチェックされます。

- 切り捨てられたコマンド：PORT コマンドおよび PASV 応答コマンドのカンマの数が 5 であるかどうかを確認されます。カンマの数が 5 でない場合は、PORT コマンドが切り捨てられていると見なされ、TCP 接続は閉じられます。
- 不正なコマンド：RFC の要求通りに、<CR><LF> 文字で終了しているかを調べるため、FTP コマンドが確認されます。終了していない場合は、接続が閉じられます。
- RETR コマンドと STOR コマンドのサイズ：これらが、固定の定数と比較チェックされます。サイズが定数より大きい場合は、エラーメッセージがロギングされ、接続が閉じられます。
- 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ます。PORT コマンドがサーバから送信される場合、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ます。PASV 応答コマンドがクライアントから送信される場合、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.」を実行する場合のセキュリティホールが予防できます。
- TCP ストリーム編集：セキュリティ アプライアンスは、TCP ストリーム編集を検出した場合に接続を閉じます。
- 無効ポート ネゴシエーション：ネゴシエートされたダイナミック ポート値が、1024 未満であるかどうか調べられます。1 ~ 1024 の範囲のポート番号は、予約済み接続用に指定されているため、ネゴシエートされたポートがこの範囲内であった場合、TCP 接続は解放されます。
- コマンドパイプライン：PORT コマンドと PASV 応答コマンド内のポート番号の後に続く文字数が、定数の 8 と比べられます。8 より大きい場合は、TCP 接続が閉じられます。
- FTP クライアントがサーバのシステム タイプを取得できないように、セキュリティ アプライアンスは、SYST コマンドに対する FTP サーバ応答を X の連続に置き換えます。このデフォルトの動作を無効にするには、FTP マップで、**no mask-syst-reply** コマンドを使用します。

## 検査制御を追加するための FTP マップの設定

FTP クライアントがサーバのシステム タイプを取得することを FTP 検査で許可する場合、および許可する FTP コマンドを制限する場合は、FTP マップを作成し、設定する必要があります。その後、[P.22-5 の「アプリケーション検査の設定」](#)を参照して、FTP 検査をイネーブルにする際に FTP マップを適用できます。

FTP マップを作成するには、次の手順を実行します。

**ステップ 1** FTP マップを作成するには、次のコマンドを入力します。

```
hostname(config)# ftp-map map_name  
hostname(config-ftp-map)#
```

*map\_name* には、FTP マップの名前を指定します。CLI は FTP マップ コンフィギュレーション モードに移行します。

**ステップ 2** この FTP マップにテキスト説明を追加するには、次のコマンドを入力します。

```
hostname(config-ftp-map)# description text
```

- ステップ 3** FTP クライアントが FTP サーバのシステム タイプを SYST メッセージに対する応答から取得することを許可する場合は、**mask-syst-reply** コマンドの **no** 形式を次のように使用します。

```
hostname(config-ftp-map)# no mask-syst-reply
hostname(config-ftp-map)#
```



(注)

デフォルトでは、FTP 検査がイネーブルの場合、SYST メッセージに対する応答はマスク処理されます。SYST 応答のマスク処理をディセーブルにした場合は、**mask-syst-response** コマンドで再度イネーブルにできます。

- ステップ 4** 特定の FTP コマンドを拒否する場合は、次のコマンドを使用します。

```
hostname(config-ftp-map)# request-command deny ftp_command [ftp_command...]
hostname(config-ftp-map)#
```

*ftp\_command* には、制限する 1 つ以上の FTP コマンドを指定します。制限できる FTP コマンドのリストについては、[表 22-3](#) を参照してください。

**表 22-3 FTP マップの request-command deny オプション**

| request-command deny オプション | 目的                                    |
|----------------------------|---------------------------------------|
| <b>appe</b>                | ファイルへの追加を行うコマンドを拒否します。                |
| <b>cdup</b>                | 現在の作業ディレクトリの親ディレクトリに移動するコマンドを拒否します。   |
| <b>dele</b>                | サーバのファイルを削除するコマンドを拒否します。              |
| <b>get</b>                 | サーバからファイルを取得するクライアント コマンドを拒否します。      |
| <b>help</b>                | ヘルプ情報を提供するコマンドを拒否します。                 |
| <b>mkd</b>                 | サーバ上にディレクトリを作成するコマンドを拒否します。           |
| <b>put</b>                 | サーバにファイルを送信するクライアント コマンドを拒否します。       |
| <b>rmd</b>                 | サーバ上のディレクトリを削除するコマンドを拒否します。           |
| <b>rnfr</b>                | 変更元ファイル名を指定するコマンドを拒否します。              |
| <b>rnto</b>                | 変更先ファイル名を指定するコマンドを拒否します。              |
| <b>site</b>                | サーバシステム固有のコマンドを拒否します。通常、リモート管理に使用します。 |
| <b>stou</b>                | 一意のファイル名を使用してファイルを保存するコマンドを拒否します。     |

次の例は、FTP マップの定義方法を示しています。

```
hostname(config-cmap)# ftp-map sample_map
hostname(config-ftp-map)# request-command deny put stou appe
```

## FTP 検査の確認と監視

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。

- An Audit record 302002 is generated for each file that is retrieved or uploaded.
- The ftp command is checked to see if it is RETR or STOR and the retrieve and store commands are logged.
- The username is obtained by looking up a table providing the IP address.
- The username, source IP address, destination IP address, NAT address, and the file operation are logged.
- Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.

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。これは、RFC 959 に詳細に記述されています。

## GTP 検査

この項では、GTP 検査エンジンについて説明します。ここでは、次の項目について説明します。

- GTP 検査の概要 (P.22-24)
- 検査制御を追加するための GTP マップの設定 (P.22-25)
- GTP 検査の確認と監視 (P.22-29)



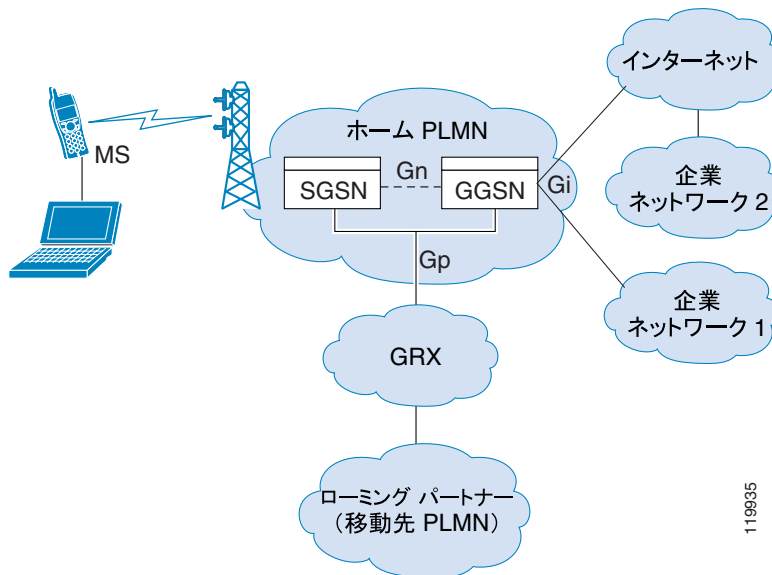
(注)

GTP 検査には、特別なライセンスが必要です。必要なライセンスがないときに、セキュリティ アプライアンスで GTP 関連のコマンドを入力した場合、セキュリティ アプライアンスはエラー メッセージを表示します。

### GTP 検査の概要

GPRS は、モバイル ユーザに対して、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との間で中断しない接続を提供します。GGSN は、GPRS 無線データ ネットワークと他のネットワークとの間のインターフェイスです。SGSN は、モビリティ、データ セッション管理、およびデータ圧縮を実行します (図 22-3 を参照)。

図 22-3 GPRS トンネリング プロトコル



UMTS は、固定回線テレフォニー、モバイル、インターネット、コンピュータ テクノロジーの商用コンバージェンスです。UTRAN は、このシステムで無線ネットワークを実装するためのネットワークング プロトコルです。GTP を使用すると、GGSN、SGSN、および UTRAN 間の UMTS/GPRS バックボーンで、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やユーザ データの暗号化は含まれていませんが、セキュリティ アプライアンスで GTP を使用することによって、これらの危険性からネットワークを保護できます。

SGSN は、GTP を使用する GGSN に論理的に接続されます。GTP を使用すると、GSN 間の GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによって、SGSN は、トンネルの作成、変更、および削除を行い、モバイル ステーションに GPRS ネットワーク アクセスを提供できます。GTP は、トンネリング メカニズムを使用して、ユーザ データ パケットを伝送するためのサービスを提供します。



(注)

GTP をフェールオーバーと同時に使用しているとき、GTP 接続が確立され、データがトンネルを超えて伝送される前にアクティブ装置に障害が発生した場合、GTP データ接続（「j」フラグが設定されています）は、スタンバイ装置に複製されません。これは、アクティブ装置が初期接続をスタンバイ装置に複製しないためです。

## 検査制御を追加するための GTP マップの設定

GTP トラフィックに対して追加のパラメータを実行する場合は、GTP マップを作成し、設定します。**inspect gtp** コマンドでマップを指定しないと、セキュリティ アプライアンスはデフォルトの GTP マップを使用します。デフォルトの GTP マップは次のデフォルト値で事前に設定されています。

- **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**

GTP マップを作成し、設定するには、次の手順を実行します。その後、[P.22-5 の「アプリケーション検査の設定」](#)を参照して、GTP 検査をイネーブルにする際に GTP マップを適用できます。

**ステップ 1** GTP マップを作成するには、次のコマンドを入力します。

```
hostname(config)# gtp-map map_name  
hostname(config-gtp-map)#
```

*map\_name* には、GTP マップの名前を指定します。CLI は GTP マップ コンフィギュレーション モードに移行します。

**ステップ 2** この GTP マップにテキスト説明を追加するには、次のコマンドを入力します。

```
hostname(config-gtp-map)# description text
```

**ステップ 3** 指定した GTP メッセージをドロップするには、次のコマンドを入力します。

```
hostname(config-gtp-map)# drop {apn access_point_name | message message_id | version  
version}
```

**apn** キーワードは、*access\_point\_name* で指定された GTP メッセージをドロップします。

**message** キーワードは、*message\_id* で特定された GTP メッセージをドロップします。*message\_id* には、1 ～ 255 の英数字の識別子を指定します。

**version** キーワードは、*version* で指定された GTP メッセージをドロップします。バージョン 0 を指定するには 0 を、バージョン 1 を指定するには 1 を使用します。GTP のバージョン 0 はポート 2123 を使用し、バージョン 1 はポート 3386 を使用します。

デフォルトでは、有効なメッセージ ID、APN、およびバージョンがある sll メッセージが検査されます。任意の APN が許可されます。

- ステップ 4** IMSI プレフィックス フィルタリングのモバイル国コードおよびモバイル ネットワーク コードを指定するには、次のコマンドを入力します。

```
hostname(config-gtp-map)# mcc country_code mnc network_code
```

**mcc** *country\_code* 引数には、モバイル国コードを表すゼロ以外の 3 桁の値を指定します。1 桁または 2 桁のエントリには、3 桁の値になるように先頭に 0 が付けられます。

**mnc** *network\_code* 引数には、ネットワーク コードを表す 2 桁または 3 桁の値を指定します。

デフォルトでは、セキュリティ アプライアンスは、MCC と MNC の有効な組み合わせがあるかをチェックしません。このコマンドは、IMSI プレフィックス フィルタリングに使用されます。受信パケットの IMSI の MCC と MNC は、このコマンドに設定されている MCC と MNC と比較され、一致しない場合はドロップされます。

このコマンドは、IMSI プレフィックス フィルタリングをイネーブルにするために使用する必要があります。複数の検査を設定して、許可する MCC と MNC の組み合わせを指定できます。デフォルトでは、MNC と MCC の組み合わせが有効であるかはセキュリティ アプライアンスによってチェックされないため、設定した組み合わせが有効であるかどうかを確認する必要があります。MCC と MNC の詳細については、ITU E.212 勧告『*Identification Plan for Land Mobile Stations*』を参照してください。

- ステップ 5** 設定した最大長および最小長と一致しない GTP パケット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-gtp-map)# message-length min min_bytes max max_bytes
```

**min** *min\_bytes* 引数には、UDP ペイロードで許容される最小バイト数を 1 ～ 65536 で指定します。

**max** *max\_bytes* 引数には、UDP ペイロードで許容される最大バイト数を 1 ～ 65536 で指定します。

このコマンドで指定する長さは、メッセージの GTP ヘッダーとそれ以外の部分の合計です。この合計が UDP パケットのペイロードです。

- ステップ 6** 無効な GTP パケット、または、そのままでは解析で失敗するパケットやドロップされるパケットを許可するには、次のコマンドを入力します。

```
hostname(config-gtp-map)# permit errors
```

デフォルトでは、無効なパケットまたは解析中に失敗したパケットはドロップされます。

- ステップ 7** GSN プーリングのサポートをイネーブルにするには、**permit response** コマンドを使用します。

セキュリティ アプライアンスが GTP 検査を実行する場合、デフォルトでセキュリティ アプライアンスは、GTP 要求で指定されていない GSN からの GTP 応答をドロップします。これは、GSN のプール間でロードバランシングを使用して、GPRS の効率とスケーラビリティを高めているときに発生します。

GSN プーリングのサポートをイネーブルにするには、**permit response** コマンドを使用します。このコマンドは、GTP 要求がどの GSN に送信されたかにかかわらず、指定された GSN のセットの中のいずれかからの応答を許可するようにセキュリティ アプライアンスを設定します。ロードバランシング GSN のプールは、ネットワーク オブジェクトとして指定します。同様に、SGSN もネットワーク オブジェクトとして指定します。応答している GSN が GTP 要求の送信先の GSN と同じオブジェクト グループに属している場合、および応答している GSN による GTP 応答の送信が許可されている先のオブジェクト グループに SGSN がある場合、セキュリティ アプライアンスはその応答を許可します。

1. ロードバランシング GSN のプールを表すオブジェクトを作成するには、次の手順を実行します。

- a. **object-group** コマンドを使用して、ロードバランシング GSN のプールを表す新しいネットワーク オブジェクト グループを定義します。

```
hostname(config)# object-group network GSN-pool-name
hostname(config-network)#
```

たとえば、次のコマンドは、gsnpool32 というオブジェクト グループを作成します。

```
hostname(config)# object-group network gsnpool32
hostname(config-network)#
```

- b. **network-object** コマンドを使用して、ロードバランシング GSN を指定します。**host** キーワードを使用して、GSN ごとに 1 つの **network-object** コマンドを使用します。**network-object** コマンドを使用して、ロードバランシングを実行する GSN を含むネットワーク全体を指定することもできます。

```
hostname(config-network)# network-object host IP-address
```

たとえば、次のコマンドは、個別のホストを表す 3 つのネットワーク オブジェクトを作成します。

```
hostname(config-network)# network-object host 192.168.100.1
hostname(config-network)# network-object host 192.168.100.2
hostname(config-network)# network-object host 192.168.100.3
hostname(config-network)#
```

2. ロードバランシング GSN による応答が許可される SGSN を表すオブジェクトを作成するには、次の手順を実行します。

- a. **object-group** コマンドを使用して、GTP 要求を GSN プールに送信する SGSN を表す新しいネットワーク オブジェクト グループを定義します。

```
hostname(config)# object-group network SGSN-name
hostname(config-network)#
```

たとえば、次のコマンドは、sgsn32 というオブジェクト グループを作成します。

```
hostname(config)# object-group network sgsn32
hostname(config-network)#
```

- b. **network-object** コマンドと **host** キーワードを使用して、SGSN を指定します。

```
hostname(config-network)# network-object host IP-address
```

たとえば、次のコマンドは、SGSN を表すネットワーク オブジェクトを作成します。

```
hostname(config-network)# network-object host 192.168.50.100
hostname(config-network)#
```

3. 1. で定義した GSN プールを表すネットワーク オブジェクトの任意の GSN から、2. で定義した SGSN を表すネットワーク オブジェクトへの GTP 応答を許可するには、次のコマンドを入力します。

```
hostname(config)# gtp-map map_name
hostname(config-gtp-map)# permit response to-object-group SGSN-name
from-object-group GSN-pool-name
```

たとえば、次のコマンドは、オブジェクト グループ gsnpool32 からオブジェクト グループ sgsn32 への GTP 応答を許可します。

```
hostname(config-gtp-map)# permit response to-object-group sgsn32 from-object-group
gsnpool32
```

次の例で、GSN プールと SGSN のネットワーク オブジェクトを定義して GSN プーリングをサポートする方法を示します。クラス C ネットワーク全体が GSN プールとして定義されていますが、ネットワーク全体を指定する代わりに、複数の個別の IP アドレスを **network-object** コマンドで 1 つずつ指定できます。この例では、次に、GSN プールから SGSN への応答を許可するように、GTP マップを変更します。

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.100.0 255.255.255.0
hostname(config)# object-group network sgsn32
hostname(config-network)# network-object host 192.168.50.100
hostname(config)# gtp-map gtp-policy
hostname(config-gtp-map)# permit response to-object-group sgsn32 from-object-group
gsnpool32
```

- ステップ 8** 応答を待機するキューに入れることのできる GTP 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(config-gtp-map)# request-queue max_requests
```

**max\_requests** 引数には、応答を待機するキューに入れることのできる GTP 要求の最大数を 1 ～ 4294967295 で指定します。デフォルトは 200 です。

この制限値に達した後新しい要求が到着すると、最も長時間キューに入っていた要求が削除されます。「Version Not Supported」および「SGSN Context Acknowledge」というエラー メッセージは、要求と見なされないため、応答を待機する要求のキューに入れられません。

- ステップ 9** GTP セッションの非アクティビティ タイマーを変更するには、次のコマンドを入力します。

```
hostname(config-gtp-map)# timeout {gsn | pdp-context | request | signaling | tunnel }
hh:mm:ss
```

このコマンドを、タイムアウトごとに別々に入力します。

**gsn** キーワードは、GSN が削除されるまでの非アクティブ期間を指定します。

**pdp-context** キーワードは、PDP コンテキストの受信を開始するまでの最大許容期間を指定します。

**request** キーワードは、GTP メッセージの受信を開始するまでの最大許容期間を指定します。

**signaling** キーワードは、GTP シグナリングが削除されるまでの非アクティブ期間を指定します。

**tunnel** キーワードは、GTP トンネルが切断されるまでの非アクティブ期間を指定します。

**hh:mm:ss** 引数では、タイムアウトを指定します。**hh** には時を、**mm** には分を、**ss** には秒を指定します。値 **0** は、切断しないことを意味します。



**ステップ 10** セキュリティ アプライアンス上でアクティブであることが許容される GTP トンネルの最大数を指定するには、次のコマンドを入力します。

```
hostname(config-gtp-map)# tunnel-limit max_tunnels
```

`max_tunnels` 引数には、許容する最大トンネル数を 1 ～ 4294967295 で指定します。デフォルトは 500 です。

このコマンドで指定したトンネル数に達すると、新しい要求はドロップされます。

次の例は、GTP マップの生成方法を示しています。

```
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
```

## GTP 検査の確認と監視

GTP コンフィギュレーションを表示するには、特権 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シンタックスについては、『*Cisco Security Appliance Command Reference*』のコマンドのページを参照してください。

**show service-policy inspect gtp statistics** コマンドを使用して、GTP 検査の統計情報を表示します。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
```

垂直バー (|) を使用して、表示をフィルタリングできます。?**|** と入力すると、表示フィルタリングオプションが表示されます。

**show service-policy inspect gtp pdp-context** コマンドを使用して、PDP コンテキストに関する情報を表示します。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.cisco.com

user_name (IMSI): 214365870921435    MS address:      1.1.1.1
primary pdp: Y
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、IMSI と NSAPI の値の組み合わせであるトンネル ID によって識別されます。GTP トンネルは、それぞれ別個の GSN ノードにある、2 つの関連する PDP コンテキストによって定義され、トンネル ID によって識別されます。GTP トンネルは、パケットを外部パケット データ ネットワークと MS ユーザの間で転送するために必要なものです。

次の例で示すように、垂直バー (|) を使用して、表示をフィルタリングできます。

```
hostname# show service-policy gtp statistics | grep gsn
```

## H.323 検査

この項では、H.323 アプリケーション検査について説明します。ここでは、次の項目について説明します。

- [H.323 検査の概要 \(P.22-31\)](#)
- [H.323 の動作 \(P.22-31\)](#)
- [制限事項 \(P.22-32\)](#)
- [H.323 および H.225 のタイムアウト値の設定 \(P.22-33\)](#)
- [H.323 検査の確認と監視 \(P.22-33\)](#)

### H.323 検査の概要

H.323 検査は、Cisco CallManager および VocalTec Gatekeeper などの H.323 に準拠したアプリケーションをサポートします。H.323 は、International Telecommunication Union (ITU; 国際電気通信連合) によって定義されている、LAN を介したマルチメディア会議用のプロトコル群です。セキュリティ アプライアンスは、H.323 v3 機能の同一コール シグナリング チャネルでの複数コールを含めて、H.323 を Version 4 までサポートします。

H.323 検査をイネーブルにした場合、セキュリティ アプライアンスは、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、セキュリティ アプライアンスでのポート使用が減少します。

H.323 検査の 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化形式で符号化されているため、セキュリティ アプライアンスでは ASN.1 デコーダを使用して H.323 メッセージを復号化します。
- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。

### H.323 の動作

H.323 のプロトコルのコレクションは、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、RAS は登録、アドミッション、およびステータス用に 1 つの UDP 接続を使用します。

H.323 クライアントは、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 セットアップを要求します。H.323 端末は、コール セットアップ プロセスの一部として、H.245 TCP 接続に使用するため、クライアントに 1 つのポート番号を供給します。H.323 ゲートキーパが使用されている環境では、初期パケットは UDP を使用して送信されます。

H.323 検査は、Q.931 TCP 接続を監視して、H.245 ポート番号を決定します。H.323 端末が、FastConnect を使用していない場合は、セキュリティ アプライアンスが H.225 メッセージの検査に基づいて、H.245 接続をダイナミックに割り当てます。

各 H.245 メッセージ内で、H.323 エンドポイントが、後続の 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 メッセージを調査して、ポート番号を識別し、メディア交換用の接続をダイナミックに作成します。RTP はネゴシエートされたポート番号を使用し、RTCP はその次に高い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 検査では、次のポートが使用されます。

- 1718 : ゲートキーパ検出 UDP ポート
- 1719 : RAS UDP ポート

- 1720：TCP 制御ポート

H.225 コール シグナリング用の予約済み H.323 ポート 1720 のトラフィックを許可する必要があります。ただし、H.245 シグナリング ポートは、H.225 シグナリングのエンドポイント間でネゴシエートされます。H.323 ゲートキーパの使用時には、セキュリティ アプライアンスは、ACF メッセージの検査に基づいて、H.225 接続を開きます。

H.225 メッセージを検査した後、セキュリティ アプライアンスは H.245 チャネルを開き、H.245 チャネルで送信されるトラフィックを検査します。セキュリティ アプライアンスを通過するすべての H.245 メッセージは、H.245 アプリケーション検査を受けます。それによって、埋め込み IP アドレスが変換され、H.245 メッセージでネゴシエートされたメディア チャネルが開かれます。

H.323 ITU 規格では、メッセージ長を定義する TPKT ヘッダーが最初に送信されてから、H.225 と H.245 が信頼できる接続上を送信されることが要求されています。TPKT ヘッダーは、必ずしも H.225 メッセージおよび H.245 メッセージと同一の TCP パケット内で送信される必要はないため、セキュリティ アプライアンスでは、メッセージを正しく処理して復号化するために TPKT 長を記憶しておく必要があります。セキュリティ アプライアンスは、次に届くメッセージに備えて、TPKT 長が格納されたレコードを接続ごとに保持します。

セキュリティ アプライアンスでメッセージ内の IP アドレスを NAT 処理する必要がある場合、チェックサム、UUIE 長、および TPKT (H.225 メッセージを含む TCP パケットに含まれている場合) が変化します。TPKT が別の TCP パケットで送信されている場合は、セキュリティ アプライアンスが TPKT に対する ACK の代理処理を行い、新しい TPKT が新しい長さで H.245 メッセージに追加されます。



(注)

セキュリティ アプライアンスは、TPKT に対する ACK の代理処理では TCP オプションをサポートしていません。

H.323 検査を通過するパケットが通る各 UDP 接続は、H.323 接続としてマークされ、**timeout** コマンドで設定された H.323 タイムアウト値でタイムアウトします。

## 制限事項

H.323 アプリケーション検査の使用に関して、次の既知の問題および制限があります。

- スタティック PAT は、H.323 メッセージのオプション フィールドに埋め込まれた IP アドレスを正しく変換できないことがあります。この問題が発生した場合は、H.323 でスタティック PAT を使用しないでください。
- H.323 アプリケーション検査は、同一セキュリティ レベルのインターフェイス間の NAT ではサポートされていません。
- NetMeeting クライアントが H.323 ゲートキーパーに登録されているときに、同じく H.323 ゲートキーパーに登録されている H.323 ゲートウェイを呼び出そうとすると、接続は確立されますが、どちらの方向でも音声聞こえません。この問題は、セキュリティ アプライアンスの問題ではありません。
- ネットワーク スタティック アドレスを設定した場合、このネットワーク スタティック アドレスが第三者のネットマスクおよびアドレスと同じであると、すべての発信 H.323 接続が失敗します。

## H.323 および H.225 のタイムアウト値の設定

H.225 シグナリング接続を閉じ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は、1 時間です。

H.323 制御接続を閉じ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 検査の確認と監視

ここでは、H.323 セッションに関する情報を表示する方法について説明します。ここでは、次の項目について説明します。

- [H.225 セッションの監視 \(P.22-33\)](#)
- [H.245 セッションの監視 \(P.22-34\)](#)
- [H.323 RAS セッションの監視 \(P.22-34\)](#)

## H.225 セッションの監視

**show h225** コマンドは、セキュリティ アプライアンスを越えて確立されている H.225 セッションの情報を表示します。**debug h323 h225 event**、**debug h323 h245 event**、および **show local-host** コマンドとともに、このコマンドは、H.323 検査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** コマンドを設定することを推奨します。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。異常なほど多くの接続が存在する場合は、デフォルトのタイムアウト値または設定した値に基づいてセッションがタイムアウトしているかどうか確認します。タイムアウトしていなければ問題があるので、調査が必要です。

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
```

この出力は、現在セキュリティ アプライアンス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ています。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 CRV が 9861 であることを示しています。

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、またはコンフィギュレーション内の H.225 タイムアウト値に基づくセッションのタイムアウトが起こるまで、セッションは開いたままになります。

## H.245 セッションの監視

**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セキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します。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。ファースト 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**、および **show local-host** コマンドとともに、このコマンドは、H.323 検査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
```

セキュリティ アプライアンスを越えているアクティブな 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 メッセージの前に送られる 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 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 番目の 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 セッションの監視

**show h323-ras** コマンドは、セキュリティ アプライアンスを越えてゲートキーパーとその H.323 エンドポイントの間に確立されている 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 検査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 検査エンジンの問題のトラブルシューティングに使用される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、ゲートキーパー 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 つあることを示しています。

## HTTP 検査

この項では、HTTP 検査エンジンについて説明します。ここでは、次の項目について説明します。

- [HTTP 検査の概要 \(P.22-35\)](#)
- [検査制御を追加するための HTTP マップの設定 \(P.22-35\)](#)

### HTTP 検査の概要

HTTP 検査エンジンを使用して、特定の攻撃、および HTTP トラフィックに関係する可能性があるその他の脅威から保護します。HTTP 検査は、次のようないくつかの機能を実行します。

- 拡張 HTTP 検査
- N2H2 または Websense を使用する URL のスクリーニング
- Java と ActiveX のフィルタリング

後の 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 17 章「フィルタリングサービスの適用」](#)を参照してください。



(注)

**no fixup protocol http** コマンドは、**filter url** コマンドもディセーブルにします。

拡張 HTTP 検査機能（アプリケーション ファイアウォールとも呼ばれ、HTTP マップ設定時に使用可能。「[検査制御を追加するための HTTP マップの設定](#)」を参照）を使用すると、攻撃者が HTTP メッセージを使用してネットワーク セキュリティ ポリシーを回避することを阻止できます。この機能により、すべての HTTP メッセージについて次のことが確認されます。

- RFC 2616 への準拠
- RFC で定義された方式のみの使用

### 検査制御を追加するための HTTP マップの設定

メッセージがパラメータを違反したときのアクションを指定するには、HTTP マップを作成します。その後、[P.22-5 の「アプリケーション検査の設定」](#)を参照して、HTTP 検査をイネーブルにする際に HTTP マップを適用できます。



(注)

HTTP マップを使用して HTTP 検査をイネーブルにすると、デフォルトでは、アクション **reset** および **log** を使用した厳密な HTTP 検査がイネーブルになります。検査に合格しない場合に実行されるアクションは変更できますが、HTTP マップがイネーブルのままである限り、厳密な検査をディセーブルにすることはできません。

HTTP マップを作成するには、次の手順を実行します。

**ステップ 1** HTTP マップを作成するには、次のコマンドを入力します。

```
hostname(config-cmap)# http-map map_name
hostname(config-http-map)#
```

`map_name` には、HTTP マップの名前を指定します。CLI は HTTP マップ コンフィギュレーション モードに移行します。

**ステップ 2** HTTP メッセージ本文の長さに基づいて HTTP トラフィックを制限するには、次のコマンドを入力します。

```
hostname(config-http-map)# content-length {[min bytes] [max bytes]} action {allow |
reset | drop} [log]
```

**min bytes** 引数には、許容する最小コンテンツ長を 1 ～ 65535 で指定します。

**max bytes** 引数には、許容する最大コンテンツ長を 1 ～ 50000000 で指定します。

**action** キーワードは、メッセージがこの検査に合格しなかったときに実行するアクションを指定します。allow、reset、または drop を指定できます。

**log** キーワードを指定すると、メッセージがこの検査に合格しなかったときのシステム メッセージが生成されます。

**ステップ 3** HTTP メッセージのコンテンツ タイプに基づいて HTTP トラフィックを制限するには、次のコマンドを入力します。

```
hostname(config-http-map)# content-type-verification [match-req-rsp] action {allow |
reset | drop} [log]
```

**match-req-rsp** キーワードは、HTTP 応答の content-type フィールドが対応する HTTP 要求メッセージの accept フィールドと一致することを確認します。

**action** キーワードは、メッセージがこの検査に合格しなかったときに実行するアクションを指定します。allow、reset、または drop を指定できます。

**log** キーワードを指定すると、メッセージがこの検査に合格しなかったときのシステム メッセージが生成されます。

このコマンドにより、次のチェックがイネーブルになります。

- ヘッダーの content-type の値が、サポートされているコンテンツ タイプの内部リストにあることの確認。  
コンテンツ タイプのリストについては、『Cisco Security Appliance Command Reference』を参照してください。
- ヘッダーの content-type が、メッセージのデータ部分または実体本文部分の実際のコンテンツと一致することの確認。
- match-req-rsp キーワードでイネーブルになる追加のチェック。このチェックでは、HTTP 応答の content-type フィールドが、対応する HTTP 要求メッセージの accept フィールドと一致することが確認されます。

**ステップ 4** HTTP ヘッダーの長さに基づいて HTTP トラフィックを制限するには、次のコマンドを入力します。

```
hostname(config-http-map)# max-header-length {[request bytes] [response bytes]} action
{allow | reset | drop} [log]
```

**request bytes** 引数には、要求メッセージの最大ヘッダー長を 1 ～ 65535 で指定します。

**response bytes** 引数には、応答メッセージの最大ヘッダー長を 1 ～ 65535 で指定します。

**action** キーワードは、メッセージがこの検査に合格しなかったときに実行するアクションを指定します。allow、reset、または drop を指定できます。



**log** キーワードを指定すると、メッセージがこの検査に合格しなかったときのシステム メッセージが生成されます。

**ステップ 5** HTTP 要求メッセージ内の URI の長さに基づいて HTTP トラフィックを制限するには、次のコマンドを入力します。

```
hostname(config-http-map)# max-uri-length bytes action {allow | reset | drop} [log]
```

bytes 引数には、最大 URI 長を 1 ～ 65535 で指定します。

**ステップ 6** 制限するアプリケーション カテゴリを指定することで HTTP トラフィックを制限するには、次のコマンドを入力します。

```
hostname(config-http-map)# port-misuse {im | p2p | tunneling | default} action {allow | reset | drop} [log]
```

**im** キーワードは、インスタント メッセージ アプリケーション カテゴリのトラフィックを制限します。チェック対象のアプリケーションは、Yahoo Messenger、AIM、および MSN IM です。

**p2p** キーワードは、ピアツーピア アプリケーション カテゴリのトラフィックを制限します。Kazaa アプリケーションがチェックされます。

**tunneling** キーワードは、トンネリング アプリケーション カテゴリのトラフィックを制限します。チェック対象のアプリケーションは、HTTPPort/HTTHost、GNU Httptunnel、GotoMyPC、Firethru、および Http-tunnel.com Client です。

**default** を指定すると、トラフィックがリストのアプリケーション タイプと一致しない場合にセキュリティ アプライアンスによって実行されるデフォルトのアクションが設定されます。デフォルトのアクションは、ログに記録せずに接続を許可することです。

**action** キーワードは、メッセージがこの検査に合格しなかったときに実行するアクションを指定します。allow、reset、または drop を指定できます。

**log** キーワードを指定すると、メッセージがこの検査に合格しなかったときのシステム メッセージが生成されます。

適用する設定ごとに 1 度、port-misuse コマンドを入力します。

**ステップ 7** HTTP 要求方式に基づいて HTTP トラフィックを制限するには、次のコマンドを入力します。

```
hostname(config-http-map)# request-method {ext {ext_methods | default} | rfc {rfc_methods | default}} action {allow | reset | drop} [log]
```

**ext** キーワードは、拡張方式を指定します。拡張方式のリストについては、CLI ヘルプを参照してください。default を指定すると、トラフィックがリストの拡張方式と一致しない場合にセキュリティ アプライアンスによって実行されるデフォルトのアクションが設定されます。デフォルトのアクションは、ログに記録せずに接続を許可することです。

**rfc** キーワードは、RFC 2616 でサポートされている方式を指定します。RFC 方式のリストについては、CLI ヘルプを参照してください。default を指定すると、トラフィックがリストの RFC 方式と一致しない場合にセキュリティ アプライアンスによって実行されるデフォルトのアクションが設定されます。デフォルトのアクションは、ログに記録せずに接続を許可することです。

**action** キーワードは、メッセージがこの検査に合格しなかったときに実行するアクションを指定します。allow、reset、または drop を指定できます。

**log** キーワードを指定すると、メッセージがこの検査に合格しなかったときのシステム メッセージが生成されます。

適用する設定ごとに 1 度、**request-method** コマンドを入力します。

**ステップ 8** 準拠していない HTTP トラフィックの転送を許可するには、次のコマンドを入力します。

```
hostname(config-http-map)# strict-http action {allow | reset | drop} [log]
```

**action** キーワードは、メッセージがこの検査に合格しなかったときに実行するアクションを指定します。**allow**、**reset**、または **drop** を指定できます。

**log** キーワードを指定すると、メッセージがこの検査に合格しなかったときのシステム メッセージが生成されます。

厳密な HTTP 検査をディセーブルにすることはできませんが、**strict-http action allow** コマンドを使用すると、セキュリティ アプライアンスは、準拠していない HTTP トラフィックの転送を許可します。このコマンドにより、デフォルトの動作は無効になります。デフォルトは、準拠していない HTTP トラフィックの転送を拒否することです。

**ステップ 9** 転送符号化タイプを指定することで HTTP トラフィックを制限するには、次のコマンドを入力します。

```
hostname(config-http-map)# transfer-encoding type {chunked | compress | deflate | gzip | identity | default} action {allow | reset | drop} [log]
```

**chunked** キーワードは、メッセージ本文を一連のチャンクとして転送する転送符号化タイプを指定します。

**compress** キーワードは、メッセージ本文を UNIX ファイル圧縮で転送する転送符号化タイプを指定します。

**deflate** キーワードは、メッセージ本文を zlib 形式 (RFC 1950) および deflate 圧縮 (RFC 1951) で転送する転送符号化タイプを指定します。

**gzip** キーワードは、メッセージ本文を GNU zip (RFC 1952) で転送する転送符号化タイプを指定します。

**identity** キーワードは、メッセージ本文に転送符号化を実行しない接続を指定します。

**default** を指定すると、トラフィックがリストの転送符号化タイプと一致しない場合にセキュリティ アプライアンスによって実行されるデフォルトのアクションが設定されます。デフォルトのアクションは、ログに記録せずに接続を許可することです。

**action** キーワードは、メッセージがこの検査に合格しなかったときに実行するアクションを指定します。**allow**、**reset**、または **drop** を指定できます。

**log** キーワードを指定すると、メッセージがこの検査に合格しなかったときのシステム メッセージが生成されます。

適用する設定ごとに 1 度、**transfer-encoding** コマンドを入力します。

次の例は、HTTP マップの定義方法を示しています。

```
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
```

## ICMP 検査

ICMP 検査エンジンを使用すると、ICMP トラフィックが「セッション」を持つようになるため、TCP トラフィックや UDP トラフィックのように検査することが可能になります。ICMP 検査エンジンを使用しない場合は、アクセスリストで、セキュリティ アプライアンスの通過を ICMP に許可しないことをお勧めします。ステートフルインスペクションを実行しない場合、ICMP がネットワーク攻撃に利用される可能性があります。ICMP 検査エンジンは、1 つの要求への応答が 1 つだけであること、シーケンス番号が正しいことを確認します。

## ICMP エラー検査

この機能がイネーブルの場合、セキュリティ アプライアンスは、NAT コンフィギュレーションに基づいて ICMP エラー メッセージを送信する中間ホップの変換セッションを作成します。セキュリティ アプライアンスは、変換した IP アドレスでパケットを上書きします。

ディセーブルの場合、セキュリティ アプライアンスは、ICMP エラー メッセージを生成する中間ノードの変換セッションを作成しません。内部ホストとセキュリティ アプライアンスの間にある中間ノードによって作成された ICMP エラー メッセージは、NAT リソースをそれ以上消費することなく、外部ホストに到達します。外部ホストが traceroute コマンドを使用して、セキュリティ アプライアンスの内部にある宛先までのホップをトレースしている場合、これは望ましくありません。セキュリティ アプライアンスが中間ホップを変換しない場合、すべての中間ホップは、マッピングされた宛先 IP アドレスとともに表示されます。

ICMP ペイロードをスキャンすることにより、元のパケットから 5 つのタプルが取得されます。クライアントの元のアドレスを確認するには、取得した 5 つのタプルを使用してルックアップを実行します。ICMP エラー検査エンジンは、ICMP パケットに対して次の変更を加えます。

- IP ヘッダー内のマッピング IP を実際の IP（宛先アドレス）に変更し、IP チェックサムを修正する。
- ICMP パケットに変更を加えたため、ICMP ヘッダー内の ICMP チェックサムを修正する。
- ペイロードに次の変更を加える。
  - 元のパケットのマッピング IP を実際の IP に変更する。
  - 元のパケットのマッピング ポートを実際のポートに変更する。
  - 元のパケットの IP チェックサムを再計算する。

## ILS 検査

ILS 検査エンジンは、LDAP を使用してディレクトリ情報を ILS サーバと交換する Microsoft NetMeeting、SiteServer、および Active Directory 製品に対して NAT をサポートします。

セキュリティ アプライアンスは ILS に対して NAT をサポートします。ILS は、ILS または SiteServer Directory のエンドポイントの登録および検索に使用されます。LDAP データベースには IP アドレスしか格納されないため、PAT はサポートされません。

LDAP サーバが外部にある場合は、内部ピアが外部 LDAP サーバに登録された状態でローカルで通信できるように、検索応答に対して NAT を適用することをお勧めします。このような検索応答の場合、最初に xlate が検索され、次に DNAT エントリが検索されて正しいアドレスが取得されます。これらの検索がどちらも失敗した場合、アドレスは変更されません。NAT 0 (NAT なし) を使用していて、DNAT の相互作用を予期していないサイトの場合は、検査エンジンをオフにしてパフォーマンスを向上することをお勧めします。

ILS サーバがセキュリティ アプライアンス境界の内部にある場合は、さらに設定が必要なことがあります。この場合、外部クライアントが所定のポート（通常は TCP 389）で LDAP サーバにアクセスするためのホールが必要となります。

ILS トラフィックはセカンダリ UDP チャンネルだけで発生するため、TCP 接続は非アクティビティ間隔の後に切断されます。デフォルトでは、この間隔は 60 分です。この値は、**timeout** コマンドを使用して調整できます。

ILS/LDAP はクライアント / サーバ モデルに従っており、セッションは 1 つの TCP 接続で処理されます。このようなセッションのいくつかは、クライアントのアクションに応じて作成されます。

接続ネゴシエーション中、クライアントからサーバに BIND PDU が送信されます。サーバから成功を示す BIND RESPONSE を受信すると、その他の操作メッセージ (ADD、DEL、SEARCH、MODIFY など) を交換できるようになり、ILS Directory に対する操作が実行されます。ADD REQUEST PDU および SEARCH RESPONSE PDU には、NetMeeting セッションを確立するために H.323 (SETUP および CONNECT メッセージ) によって使用される NetMeeting ピアの IP アドレスが含まれている場合があります。Microsoft NetMeeting v2.X および v3.X は、ILS をサポートしています。

ILS 検査では、次の操作が実行されます。

- BER 復号化機能による LDAP REQUEST/RESPONSE PDU の復号化
- LDAP パケットの解析
- IP アドレスの抽出
- 必要に応じた IP アドレスの変換
- BER 符号化機能による、変換されたアドレスが含まれる PDU の符号化
- 元の TCP パケットへの、新しく符号化された PDU のコピー
- 差分 TCP チェックサムとシーケンス番号を増分的に調整

ILS 検査では、次の制限事項があります。

- Referral 要求および応答はサポートされません。
- 複数のディレクトリ内のユーザは統合されません。
- 1 人のユーザが複数のディレクトリで複数のアイデンティティを持つ場合、そのユーザは NAT によって認識されません。



(注)

H225 コール シグナリング トラフィックはセカンダリ UDP チャンネルだけで発生するため、TCP 接続は、TCP **timeout** コマンドで指定した間隔の後に切断されます。デフォルトでは、この間隔は 60 分です。

## MGCP 検査

この項では、MGCP アプリケーション検査について説明します。ここでは、次の項目について説明します。

- [MGCP 検査の概要 \(P.22-41\)](#)
- [検査制御を追加するための MGCP マップの設定 \(P.22-43\)](#)
- [MGCP タイムアウト値の設定 \(P.22-44\)](#)
- [MGCP 検査の確認と監視 \(P.22-44\)](#)

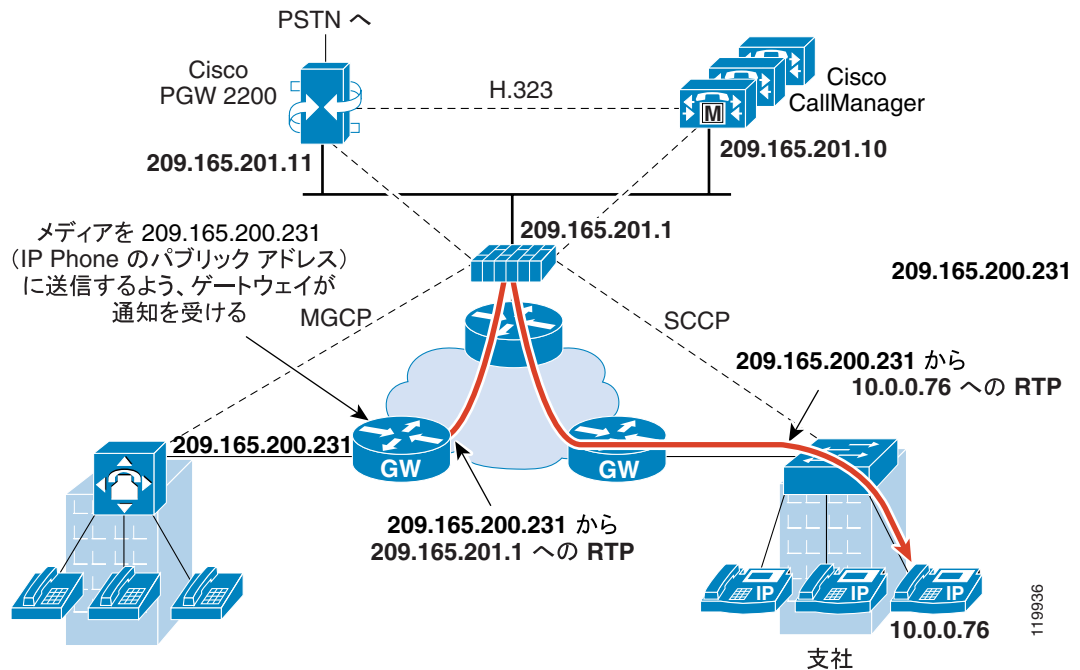
### MGCP 検査の概要

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のコール制御要素からメディア 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に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。NAT および PAT を MGCP とともに使用すると、限られた外部（グローバル）アドレスのセットで、内部ネットワークの多数のデバイスをサポートできます。メディア ゲートウェイの例は次のとおりです。

- トランキング ゲートウェイ。電話ネットワークと Voice over IP ネットワークとの間のインターフェイスです。このようなゲートウェイは通常、大量のデジタル回線を管理します。
- 住宅用ゲートウェイ。従来のアナログ (RJ11) インターフェイスを Voice over IP ネットワークに提供します。住宅用ゲートウェイの例としては、ケーブル モデムやケーブル セットトップボックス、xDSL 装置、ブロードバンド ワイヤレス装置などがあります。
- ビジネス ゲートウェイ。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 soft PBX インターフェイスを Voice over IP ネットワークに提供します。

MGCP メッセージは UDP を介して送信されます。応答はコマンドの送信元アドレス（IP アドレスと UDP ポート番号）に返送されますが、コマンド送信先と同じアドレスからの応答は到達しない場合があります。これは、複数のコール エージェントがフェールオーバー コンフィギュレーションで使用されているときに、コマンドを受信したコール エージェントが制御をバックアップ コール エージェントに引き渡し、バックアップ コール エージェントから応答を送信する場合に起こる可能性があります。[図 22-4](#) で、NAT と MGCP を同時に使用方法を示します。

図 22-4 NAT と MGCP の使用



MGCP エンドポイントは、物理または仮想のデータ送信元および宛先です。メディア ゲートウェイには、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て制御するために、コール エージェントが接続を作成、変更、および削除できるエンドポイントが含まれています。また、コール エージェントは、特定のイベントを検出してシグナルを生成するようにエンドポイントに指示できます。エンドポイントは、サービス状態の変化を自動的にコール エージェントに伝達します。

MGCP トランザクションは、コマンドと必須応答で構成されます。次の 8 種類のコマンドがあります。

- CreateConnection
- ModifyConnection
- DeleteConnection
- NotificationRequest
- Notify
- AuditEndpoint
- AuditConnection
- RestartInProgress

最初の 4 つのコマンドは、コール エージェントからゲートウェイに送信されます。Notify コマンドは、ゲートウェイからコール エージェントに送信されます。ゲートウェイは、DeleteConnection を送信することもあります。MGCP ゲートウェイをコール エージェントに登録するには、RestartInProgress コマンドを使用します。AuditEndpoint コマンドおよび AuditConnection コマンドは、コール エージェントからゲートウェイに送信されます。

すべてのコマンドは、コマンドヘッダーと、その後ろに続くオプションのセッション記述で構成されます。すべての応答は、応答ヘッダーと、その後ろに続くオプションのセッション記述で構成されます。

- ゲートウェイがコール エージェントからのコマンドを受信するポート。通常、ゲートウェイは UDP ポート 2427 をリスンします。
- コール エージェントがゲートウェイからのコマンドを受信するポート。通常、コール エージェントは UDP ポート 2727 をリスンします。

**(注)**

MGCP 検査では、MGCP シグナリングと RTP データで異なる IP アドレスを使用することはサポートされていません。一般的かつ推奨される方法は、ループバック IP アドレスや仮想 IP アドレスなどの回復力のある IP アドレスから RTP データを送信することです。ただし、セキュリティ アプライアンスは、MGCP シグナリングと同じアドレスから RTP データを受信する必要があります。

## 検査制御を追加するための MGCP マップの設定

セキュリティ アプライアンスがピンホールを開ける必要のあるコール エージェントとゲートウェイがネットワークに複数ある場合は、MGCP マップを作成します。その後、[P.22-5 の「アプリケーション検査の設定」](#)を参照して、MGCP 検査をイネーブルにする際に MGCP マップを適用できます。

MGCP マップを作成するには、次の手順を実行します。

**ステップ 1** MGCP マップを作成するには、次のコマンドを入力します。

```
hostname(config-cmap)# mgcp-map map_name  
hostname(config-mgcp-map)#
```

*map\_name* には、MGCP マップの名前を指定します。システムは MGCP マップ コンフィギュレーション モードに移行し、それに応じて CLI プロンプトが変化します。

**ステップ 2** コール エージェントを設定するには、コール エージェントごとに次のコマンドを入力します。

```
hostname(config-mgcp-map)# call-agent ip_address group_id
```

1 つ以上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 エージェントのグループ情報は、どのコール エージェントも応答を送信できるように、グループ内の（ゲートウェイがコマンドを送信する先以外の）コール エージェントに接続を開くために使用されます。同じ *group\_id* のコール エージェントは、同じグループに属します。1 つのコール 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 ～ 4294967295 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。

**(注)**

MGCP コール エージェントは、AUEP メッセージを送信して、MGCP エンドポイントが存在するかどうかを判定します。これによって、セキュリティ アプライアンスを通過するフローが確立され、MGCP エンドポイントをコール エージェントに登録できます。

**ステップ 3** ゲートウェイを設定するには、ゲートウェイごとに次のコマンドを入力します。

```
hostname(config-mgcp-map)# gateway ip_address group_id
```

特定のゲートウェイを管理しているコール エージェントのグループを指定するには、**gateway** コマンドを使用します。**ip\_address** オプションを使用して、ゲートウェイの IP アドレスを指定します。**group\_id** オプションは 0 ～ 4294967295 の数字です。この数字は、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** に対応している必要があります。1 つのゲートウェイは 1 つのグループだけに所属できます。

- ステップ 4** MGCP コマンド キューに入れることができるコマンドの最大数を変更するには、次のコマンドを入力します。

```
hostname(config-mgcp-map)# command-queue command_limit
```

次の例は、MGCP マップの定義方法を示しています。

```
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
```

## MGCP タイムアウト値の設定

**timeout mgcp** コマンドを使用して、MGCP メディア接続を閉じるまでの非アクティビティ間隔を設定できます。デフォルトは 5 分です。

**timeout mgcp-pat** コマンドを使用して、PAT xlate のタイムアウトを設定できます。MGCP にはキープアライブ メカニズムがないため、Cisco 以外の MGCP ゲートウェイ（コール エージェント）を使用すると、デフォルトのタイムアウト間隔（30 秒）の後で PAT xlate は切断されます。

## MGCP 検査の確認と監視

**show mgcp commands** コマンドは、コマンド キュー内の MGCP コマンド数を表示します。**show mgcp sessions** コマンドは、既存の MGCP セッション数を表示します。**detail** オプションは、各コマンド（またはセッション）に関する追加情報を出力に含めます。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、デフォルトでイネーブルになっています。NetBios 検査エンジンは、セキュリティアプライアンス NAT コンフィギュレーションに基づいて、NetBios Name Service (NBNS; NetBios ネーム サービス) パケット内の IP アドレスを変換します。

## PPTP 検査

PPTP は、PPP トラフィックのトンネリングに使用されるプロトコルです。PPTP セッションは、1 つの TCP チャンネルと通常 2 つの PPTP GRE トンネルで構成されます。TCP チャンネルは、PPTP GRE トンネルのネゴシエートと管理に使用される制御チャンネルです。GRE トンネルは、2 つのホスト間の PPP セッションを伝送します。

イネーブルの場合、PPTP アプリケーション検査では、PPTP プロトコルパケットが検査され、PPTP トラフィックを許可するために必要な GRE 接続と xlate がダイナミックに作成されます。RFC 2637 で定義されているバージョン 1 だけがサポートされます。

PAT は、PPTP TCP 制御チャンネルで修正バージョンの GRE [RFC 2637] がネゴシエートされたときに、その GRE に対してのみ実行されます。PAT は、未修正バージョンの GRE [RFC 1701、RFC 1702] に対しては実行されません。

具体的には、セキュリティ アプライアンスは、PPTP のバージョン情報と発信コールの要求 / 応答シーケンスを検査します。RFC 2637 で定義されている PPTP バージョン 1 だけが検査されます。いずれか一方が示すバージョンがバージョン 1 でない場合、TCP 制御チャンネルでのその後の検査はディセーブルになります。また、発信コールの要求と応答のシーケンスは追跡されます。接続と xlate は、後続のセカンダリ GRE データ トラフィックを許可するために、必要に応じてダイナミックに割り当てられます。

PPTP 検査エンジンは、PPTP トラフィックが PAT で変換されるように、イネーブルにする必要があります。また、PAT は、PPTP TCP 制御チャンネルで修正バージョンの GRE (RFC 2637) がネゴシエートされた場合に限り、その GRE に対してのみ実行されます。PAT は、未修正バージョンの GRE (RFC 1701 および RFC 1702) に対しては実行されません。

RFC 2637 で定義されているように、PPTP プロトコルは、主に、モデム バンク PPTP Access Concentrator (PAC; PPTP アクセス コンセントレータ) から開始されたヘッドエンド PPTP Network Server (PNS; PPTP ネットワーク サーバ) への PPP セッションのトンネリングに使用されます。このように使用された場合、PAC がリモート クライアントで PNS がサーバです。

ただし、Windows の VPN で使用された場合、この関係は逆になります。PNS が、中央のネットワークにアクセスするためにヘッドエンド PAC への接続を開始するリモートの単一ユーザ PC です。

## RSH 検査

RSH 検査はデフォルトでイネーブルになっています。RSH プロトコルは、RSH クライアントから RSH サーバへの TCP ポート 514 での TCP 接続を使用します。クライアントとサーバは、クライアントが STDERR 出力ストリームを受信する TCP ポート番号をネゴシエートします。RSH 検査では、ネゴシエートされるポート番号の NAT がサポートされます。

## RTSP 検査

この項では、RTSP アプリケーション検査について説明します。ここでは、次の項目について説明します。

- [RTSP 検査の概要 \(P.22-47\)](#)
- [RealPlayer の使用 \(P.22-48\)](#)
- [制限事項 \(P.22-48\)](#)

### RTSP 検査の概要

RTSP 検査エンジンを使用すると、セキュリティ アプライアンスは RTSP パケットを通過させることができるようになります。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV 接続によって使用されます。

**(注)**

Cisco IP/TV では、RTSP TCP ポート 554 と TCP 8554 を使用します。

RTSP アプリケーションは、制御チャンネルとしての TCP（例外的に UDP）とともに予約済みポート 554 を使用します。セキュリティ アプライアンスは、RFC 2326 に準拠して、TCP だけをサポートします。この TCP 制御チャンネルは、クライアント上で設定されているトランスポート モードに応じて、音声 / ビデオ トラフィックの送信に使用されるデータ チャンネルのネゴシエーションに使用されます。

サポートされている 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。

セキュリティ アプライアンスは、ステータス コード 200 の SETUP 応答メッセージを解析します。SETUP 応答メッセージが、着信方向に移動している場合は、サーバはセキュリティ アプライアンスとの相対位置関係で外部に存在することになるため、サーバから着信する接続に対してダイナミック チャンネルを開くことが必要になります。この応答メッセージが発信方向である場合、セキュリティ アプライアンスは、ダイナミック チャンネルを開く必要はありません。

RFC 2326 では、クライアント ポートとサーバ ポートが、SETUP 応答メッセージ内に含まれていることは必要でないため、セキュリティ アプライアンスでは、状態を維持し、SETUP メッセージ内のクライアント ポートを記憶します。QuickTime が、SETUP メッセージ内にクライアント ポートを設定すると、サーバは、サーバ ポートだけで応答します。

RTSP 検査は、PAT またはデュアル NAT をサポートしていません。また、セキュリティ アプライアンスは、RTSP メッセージが HTTP メッセージ内に隠される HTTP クローキングを認識できません。

## RealPlayer の使用

RealPlayer を使用するときは、転送モードを正しく設定することが重要です。セキュリティ アプライアンスでは、サーバからクライアントに、またはその逆に **access-list** コマンドを追加します。RealPlayer では、**Options > Preferences > Transport > RTSP Settings** をクリックすることで、転送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** チェックボックスおよび **Attempt to use TCP for all content** チェックボックスをオンにします。セキュリティ アプライアンスで、検査エンジンを設定する必要はありません。

RealPlayer 上で UDP モードを使用している場合、**Use TCP to Connect to Server** チェックボックスと **Attempt to use UDP for all content** チェックボックスをオンにします。Multicast 経由で入手できないライブ コンテンツに対しても同様です。セキュリティ アプライアンスで、**inspect rtsp port** コマンドを追加します。

## 制限事項

**inspect rtsp** コマンドには、次の制約事項が適用されます。

- セキュリティ アプライアンスは、マルチキャスト RTSP または UDP による RTSP メッセージをサポートしません。
- PAT はサポートされていません。
- セキュリティ アプライアンスには、RTSP メッセージが HTTP メッセージ内に隠されている HTTP クローキングを認識する機能はありません。
- 埋め込み IP アドレスが HTTP メッセージまたは RTSP メッセージの一部として SDP ファイル内に含まれているため、セキュリティ アプライアンスは、RTSP メッセージに NAT を実行できません。パケットはフラグメント化する可能性があり、セキュリティ アプライアンスはフラグメント化されたパケットに対して NAT を実行できません。
- Cisco IP/TV では、メッセージの SDP 部分についてセキュリティ アプライアンスが実行する変換の数は、Content Manager にあるプログラム リストの数に比例します（各プログラム リストには、少なくとも 6 個の埋め込み IP アドレスを含めることができます）。
- Apple QuickTime 4 または RealPlayer 用の NAT を設定できます。Cisco IP/TV は、ビューアと Content Manager が外部ネットワークにあり、サーバが内部ネットワークにあるときにだけ NAT を使用できます。

## SIP 検査

この項では、SIP アプリケーション検査について説明します。ここでは、次の項目について説明します。

- [SIP 検査の概要 \(P.22-49\)](#)
- [SIP インスタント メッセージ \(P.22-49\)](#)
- [SIP タイムアウト値の設定 \(P.22-50\)](#)
- [SIP 検査の確認と監視 \(P.22-51\)](#)

### SIP 検査の概要

IETF で定義されている SIP により、特に 2 者間の音声会議などのコール処理セッションまたは「コール」が使用可能になります。SIP は、コール シグナリング用の SDP で動作します。SDP は、メディア ストリーム用のポートを指定します。SIP を使用して、セキュリティ アプライアンスは任意の SIP VoIP ゲートウェイおよび 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 に記載されています。

- SIP : Session Initiation Protocol、RFC 2543
- SDP : Session Description Protocol、RFC 2327

セキュリティ アプライアンス経由の SIP コールをサポートする場合は、シグナリング メッセージは予約済みの宛先ポート (UDP/TCP 5060) 経由で送信され、メディア ストリームはダイナミックに割り当てられるため、メディア接続アドレスのシグナリング メッセージ、メディア ポート、およびメディアの初期接続を検査する必要があります。また、SIP は、IP パケットのユーザデータ部分に IP アドレスを埋め込みます。SIP 検査は、それらの埋め込まれた IP アドレスに NAT を適用します。

PAT を SIP で使用する場合、次の制限事項が適用されます。

- セキュリティ アプライアンスで保護されているネットワークの SIP プロキシにリモート エンドポイントを登録しようとする、次のような特定の条件のもとで登録が失敗します。
  - PAT がリモート エンドポイント用に設定されている。
  - SIP レジストラ サーバが外部ネットワークにある。
  - エンドポイントからプロキシ サーバに送信された REGISTER メッセージの接続先フィールドにポートが設定されていない。
- SDP 部分の所有者 / 作成者フィールド (o=) の IP アドレスが接続フィールド (c=) の IP アドレスと異なるパケットを SIP デバイスが送信すると、o= フィールドの IP アドレスが正しく変換されない場合があります。これは、o= フィールドでポート値を提供しない SIP プロトコルの制限によるものです。

### SIP インスタント メッセージ

インスタント メッセージとは、ほぼリアルタイムにユーザ間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 を使用する Windows XP のチャット機能のみをサポートします。次の RFC で定義されているように、MESSAGE/INFO 方式および 202 Accept 応答を使用して IM をサポートします。

- Session Initiation Protocol (SIP) -Specific Event Notification、RFC 3265
- Session Initiation Protocol (SIP) Extension for Instant Messaging、RFC 3428

MESSAGE/INFO 要求は、登録または加入の後、任意の時点で着信する可能性があります。たとえば、2 人のユーザはいつでもオンラインになる可能性があります。何時間もチャットをすることはありません。そのため、SIP 検査エンジンは、設定されている 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、登録継続時間よりも 5 分以上長く設定する必要があります。登録継続時間は Contact Expires 値で定義し、通常 30 分です。

MESSAGE/INFO 要求は、通常、ポート 5060 以外の動的に割り当てられたポートを使用して送信されるため、SIP 検査エンジンを通過する必要があります。



(注)

現在は、チャット機能のみがサポートされています。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 はサポートされていません。

SIP 検査は、テキストベースの SIP メッセージを変換し、メッセージの SDP 部分の内容長を再計算した後、パケット長とチェックサムを再計算します。また、エンドポイントが受信すべきアドレスまたはポートとして、SIP メッセージの SDP 部分に指定されたポートに対するメディア接続をダイナミックに開きます。

SIP 検査では、SIP ペイロードから取得したインデックス CALL\_ID/FROM/TO が格納されたデータベースが使用されます。これらのインデックスにより、コール、送信元、宛先が識別されます。このデータベースには、SDP メディア情報フィールドで見つかったメディア アドレスとメディア ポート、およびメディア タイプが格納されています。1 つのセッションに対して、複数のメディア アドレスとポートが存在することが可能です。セキュリティ アプライアンスは、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に RTP/RTCP 接続を開きます。

初期コール セットアップ (INVITE) メッセージでは、予約済みポート 5060 を使用する必要があります。ただし、後続のメッセージにはこのポート番号がない場合もあります。SIP 検査エンジンはシグナリング接続のピンホールを開き、それらの接続を SIP 接続としてマークします。これは、SIP アプリケーションに到達し、変換すべきメッセージに対して行われます。

コールのセットアップ時に、SIP セッションは、着呼エンドポイントが受信する RTP ポートを示す応答メッセージにおいて、メディア アドレスとメディア ポートが受信されるまで「一時的な」状態にあります。1 分以内に、応答メッセージの受信に障害があった場合は、シグナリング接続は切断されます。

最終的なハンドシェイクが行われると、コール状態はアクティブに移行し、シグナリング接続は、BYE メッセージの受信まで継続されます。

内部エンドポイントが、外部エンドポイントに発呼した場合、メディア ホールが、外部インターフェイスに対して開き、内部エンドポイントから送信された INVITE メッセージで指定された内部エンドポイントのメディア アドレスとメディア ポートに、RTP/RTCP UDP パケットが流れることが許可されます。内部インターフェイスに対する要求外の RTP/RTCP UDP パケットは、セキュリティ アプライアンスのコンフィギュレーションにより特別に許可されない限り、セキュリティ アプライアンスを通過できません。

## SIP タイムアウト値の設定

メディア接続は、接続がアイドル状態になってから 2 分以内に切断されます。ただし、これは設定可能なタイムアウトであり、時間間隔は変更することが可能です。SIP 制御接続のタイムアウトを設定するには、次のコマンドを入力します。

```
hostname(config)# timeout sip hh:mm:ss
```

このコマンドは、SIP 制御接続を閉じるまでのアイドル 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を設定するには、次のコマンドを入力します。

```
hostname(config)# timeout sip_media hh:mm:ss
```

このコマンドは、SIP メディア接続を閉じるまでのアイドル タイムアウトを設定します。

## SIP 検査の確認と監視

**show sip** コマンドは、SIP 検査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** コマンドと一緒に説明されています。**show timeout sip** コマンドは、指示されている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、セキュリティ アプライアンスを超えて確立されている SIP セッションの情報を表示します。**debug sip** と **show local-host** コマンドとともに、このコマンドは、SIP 検査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ることがあります。

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
```

この例は、セキュリティ アプライアンス上の 2 つのアクティブな SIP セッションを示しています (Total フィールドで示されているように)。各 call-id は、コールを表しています。

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、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 番目のセッションは、Active 状態です。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

この項では、SCCP アプリケーション検査について説明します。ここでは、次の項目について説明します。

- [SCCP 検査の概要 \(P.22-52\)](#)
- [Cisco IP Phone のサポート \(P.22-52\)](#)
- [制限事項 \(P.22-53\)](#)
- [SCCP 検査の確認と監視 \(P.22-53\)](#)

### SCCP 検査の概要

Skinny (SCCP) は、VoIP ネットワークで使用される単純化されたプロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境でも使用できます。Cisco CallManager と併用すると、SCCP クライアントは、H.323 準拠端末と同時使用できます。セキュリティ アプライアンスにおけるアプリケーション層機能では、SCCP Version 3.3 が認識されます。SCCP プロトコルのバージョンには 2.4、3.0.4、3.1.1、3.2、および 3.3.2 の 5 つがあります。セキュリティ アプライアンスは、Version 3.3.2 までのすべてのバージョンをサポートします。

セキュリティ アプライアンスは、SCCP に対して PAT と NAT をサポートします。IP 電話用のグローバル IP アドレスより多くの IP 電話を使用する場合は、PAT が必要です。Skinny アプリケーション検査は、SCCP シグナリング パケットの NAT と PAT をサポートすることにより、すべての SCCP シグナリングとメディア パケットが確実にセキュリティ アプライアンスを通過できるようにします。

Cisco CallManager と Cisco IP Phones の間の通常のトラフィックは SCCP を使用しており、特別な設定なしで SCCP 検査によって処理されます。セキュリティ アプライアンスは、DHCP オプション 150 および 66 もサポートします。これは、TFTP サーバの場所を Cisco IP Phones とその他の DHCP クライアントに送信することで達成されます。Cisco IP Phone では、デフォルト ルートを設定する DHCP オプション 3 を要求に含めることもできます。詳細については、[P.8-31 の「DHCP サーバを利用する Cisco IP Phone の使用方法」](#)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に配置されているトポロジにおいて、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。これは、Cisco IP Phone では Cisco CallManager IP アドレスを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ためです。スタティック アイデンティティ エントリを使用して、より高いセキュリティ インターフェイスの Cisco CallManager が Cisco IP Phone からの登録を受け付けるようにできます。

Cisco IP Phone では、TFTP サーバにアクセスして、Cisco CallManager サーバに接続するため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 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 エントリが必要ですが、識別スタティック エントリにする必要はありません。NAT を使用する場合、識別スタティック 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 サーバおよび 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にあるときは、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 エントリも必要ありません。



## 制限事項

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** コマンドを含むコンフィギュレーションでは動作しません。
- 外部 NAT も PAT もサポートされません。

内部の Cisco CallManager のアドレスが NAT または PAT 用に別の IP アドレスかポートを設定している場合、セキュリティ アプライアンスは現在のところ TFTP を経由して転送するファイルの内容に対して NAT または PAT をサポートしていないため、外部の Cisco IP Phone 用の登録は失敗します。セキュリティ アプライアンスは 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、電話の登録中に TFTP を使用して転送された 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することはできません。



(注)

セキュリティ アプライアンスは、コール セットアップ中のコールを除き、SCCP コールのステートフル フェールオーバーをサポートします。

## SCCP 検査の確認と監視

**show skinny** コマンドは、SCCP (Skinny) 検査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。次の条件での **show skinny** コマンドの出力例を示します。セキュリティ アプライアンスを越えて 2 つのアクティブな Skinny セッションがセットアップされています。最初の Skinny 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 の間に確立されています。TCP ポート 2000 は、CallManager です。2 番目の Skinny 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 の間に確立されています。

```
hostname# show skinny
          LOCAL                FOREIGN                STATE
-----
1         10.0.0.11/52238       172.18.1.33/2000                1
    MEDIA 10.0.0.11/22948       172.18.1.22/20798
2         10.0.0.22/52232       172.18.1.33/2000                1
    MEDIA 10.0.0.22/20798       172.18.1.11/22948
```

この出力は、2 つの内部 Cisco IP Phone 間でコールが確立されていることを示します。最初と 2 番目の電話機の RTP リスン ポートは、それぞれ UDP 22948 と 20798 です。

これらの Skinny 接続の **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

ESMTP アプリケーション検査を使用すると、セキュリティ アプライアンスを通過できる SMTP コマンドの種類を制限し、監視機能を追加することによって、SMTP ベースの攻撃からより強固に保護できます。

ESMTP は SMTP プロトコルの拡張で、ほとんどの観点で SMTP に似ています。便宜上、このマニュアルでは、SMTP という用語を SMTP と ESMTP の両方に使用します。拡張 SMTP に対するアプリケーション検査処理は、SMTP アプリケーション検査に似ており、SMTP セッションのサポートが含まれています。拡張 SMTP セッションで使用するほとんどのコマンドは、SMTP セッションで使用するコマンドと同じですが、ESMTP セッションの方が大幅に高速で、配信ステータス通知など信頼性およびセキュリティに関するオプションが増えています。

拡張 SMTP アプリケーション検査では、AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、および VRFY の 8 つの拡張 SMTP コマンドのサポートが追加されます。セキュリティ アプライアンスは、7 つの RFC 821 コマンド (DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET) をサポートするとともに、合計 15 の SMTP コマンドをサポートします。

その他の拡張 SMTP コマンド (ATRN、STARTLS、ONEX、VERB、CHUNKING など)、およびプライベート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、内部サーバにより拒否される X に変換されます。この結果は、「500 Command unknown: 'XXX'」のようなメッセージで表示されます。不完全なコマンドは、廃棄されます。

ESMTP 検査エンジンは、文字「2」、「0」、「0」を除き、サーバ SMTP バナーの文字をアスタリスクに変更します。復帰 (CR)、および改行 (LF) は無視されます。

SMTP 検査をイネーブルにする場合、次の規則に従わないと、対話型の SMTP に使用する Telnet セッションが停止することがあります。SMTP コマンドの長さは 4 文字以上にする必要があります。復帰と改行で終了する必要があります。次の応答を発行する前に現在の応答を待機する必要があります。

SMTP サーバは、数値応答コード、およびオプションの可読文字列でクライアント要求に応答します。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とサーバが返送するメッセージを制御し、その数を減らします。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 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監視します。
- 監査証跡の生成：メール アドレス内に埋め込まれている無効な文字が交換されたときに、監査レコード 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 検査では、次の異常なシグニチャをチェックするため、コマンド応答シーケンスが監視されます。

- 切り捨てられたコマンド
- 不正なコマンド終端 (<CR><LR> で終了していない)
- MAIL コマンドと RCPT コマンドでは、メールの送信者と受信者が指定されます。異常な文字がないか、メール アドレスがスキャンされます。パイプ (|) が削除 (空白スペースに変更) され、「<」および「>」については、メール アドレスの定義に使用される場合だけ許可されます («<」の後には、必ず「>」が使用されている必要があります)。
- SMTP サーバによる不意の移行
- 未知のコマンドに対しては、セキュリティ アプライアンス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、サーバがクライアントに対してエラー コードを生成します。パケット内が変更されているため、TCP チェックサムは、再計算または調節する必要があります。
- TCP ストリーム編集
- コマンドパイプライン

## SNMP 検査

SNMP アプリケーション検査では、SNMP トラフィックを特定のバージョンの SNMP に制限できます。SNMP の以前のバージョンは安全性が低いため、セキュリティ ポリシーによっては、特定の SNMP バージョンを拒否する必要があります。セキュリティ アプライアンスは、SNMP バージョン 1、2、2c、または 3 を拒否できます。許可するバージョンは、SNMP マップを作成することで制御できます。その後、[P.22-5 の「アプリケーション検査の設定」](#)を参照して、SNMP 検査をイネーブルにする際に SNMP マップを適用できます。

SNMP マップを作成するには、次の手順を実行します。

**ステップ 1** SNMP マップを作成するには、次のコマンドを入力します。

```
hostname(config)# snmp-map map_name  
hostname(config-snmp-map)#
```

*map\_name* には、SNMP マップの名前を指定します。CLI は SNMP マップ コンフィギュレーション モードに移行します。

**ステップ 2** 拒否する SNMP のバージョンを指定するには、バージョンごとに次のコマンドを入力します。

```
hostname(config-snmp-map)# deny version version  
hostname(config-snmp-map)#
```

*version* には、1、2、2c、または 3 を指定します。

次の例では、SNMP バージョン 1 および 2 を拒否しています。

```
hostname(config)# snmp-map sample_map  
hostname(config-snmp-map)# deny version 1  
hostname(config-snmp-map)# deny version 2
```

## SQL\*Net 検査

SQL\*Net 検査は、デフォルトでイネーブルになっています。

SQL\*Net プロトコルは、さまざまなパケット タイプで構成されています。セキュリティ アプライアンスはそれら进行处理し、セキュリティ アプライアンスのどちらの側の Oracle アプリケーションにも一貫性のあるデータ ストリームが表示されるようにします。

SQL\*Net のデフォルトのポート割り当ては 1521 です。これは、Oracle が SQL\*Net 用に使用している値ですが、Structured Query Language (SQL; 構造化照会言語) の IANA ポート割り当てとは一致しません。**class-map** コマンドを使用すると、SQL\*Net 検査を一連のポート番号に適用できます。

セキュリティ アプライアンスは、すべてのアドレスを変換し、パケットを調べて、SQL\*Net バージョン 1 用に開くすべての埋め込みポートを見つけます。

SQL\*Net バージョン 2 の場合、データ長ゼロの REDIRECT パケットの直後に続くすべての DATA パケットまたは REDIRECT パケットは、フィックスアップされます。

フィックスアップが必要なパケットには、埋め込まれたホスト アドレスおよびポート アドレスが次の形式で含まれています。

```
(ADDRESS=(PROTOCOL=tcp) (DEV=6) (HOST=a.b.c.d) (PORT=a))
```

SQL\*Net バージョン 2 TNSFrame タイプ (Connect、Accept、Refuse、Resend、および Marker) は、NAT 処理するアドレスがあるかどうかをスキャンされず、パケット内の埋め込みポートのダイナミック接続も開かれません。

SQL\*Net バージョン 2 TNSFrame、Redirect パケット、および Data パケットは、ペイロードのデータ長がゼロの REDIRECT TNSFrame タイプの後に続く場合、開くポートおよび NAT 処理するアドレスがあるかどうかをスキャンされます。データ長ゼロの Redirect メッセージがセキュリティ アプライアンスを通過すると、接続データ構造にフラグが設定され、後に続く Data メッセージまたは Redirect メッセージを変換するため、およびポートをダイナミックに開くために備えられます。先行するパラグラフの TNS フレームのいずれかが Redirect メッセージの後に到着した場合、フラグはリセットされます。

SQL\*Net 検査エンジンは、チェックサムを再計算し、IP および TCP の長さを変更し、新旧のメッセージの長さの差を使用してシーケンス番号と確認応答番号を再調整します。

SQL\*Net バージョン 1 では、その他のすべての場合を想定しています。TNSFrame タイプ (Connect、Accept、Refuse、Resend、Marker、Redirect、および Data) とすべてのパケットは、ポートおよびアドレスを見つけるためにスキャンされます。アドレスが変換され、ポート接続が開かれます。

## Sun RPC 検査

この項では、Sun RPC アプリケーション検査について説明します。ここでは、次の項目について説明します。

- [Sun RPC 検査の概要 \(P.22-57\)](#)
- [Sun RPC サービスの管理 \(P.22-57\)](#)
- [Sun RPC 検査の確認と監視 \(P.22-58\)](#)

### Sun RPC 検査の概要

Sun RPC 検査エンジンは、Sun RPC プロトコルのアプリケーション検査をイネーブ爾またはディセーブルにします。Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスは、任意のポート上で実行できます。サーバ上の Sun RPC サービスにアクセスしようとするクライアントは、そのサービスが実行されているポートを知る必要があります。そのためには、予約済みポート 111 でポート マッパー プロセス（通常、rpcbind）にクエリーを送信します。

クライアントがサービスの Sun RPC プログラム番号を送信すると、ポート マッパー プロセスは応答でサービスのポート番号を示します。クライアントは、ポート マッパー プロセスによって特定されたポートを指定して、Sun RPC クエリーをサーバに送信します。サーバが応答すると、セキュリティ アプライアンスはこのパケットを代行受信し、そのポートで初期 TCP および UDP 接続の両方を開きます。



(注)

Sun RPC ペイロード情報の NAT または PAT はサポートされていません。

### Sun RPC サービスの管理

Sun RPC サービス テーブルを使用して、確立された Sun RPC セッションに基づいてセキュリティ アプライアンスを経由する Sun RPC トラフィックを制御します。Sun RPC サービス テーブルの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** コマンドを次のように使用します。

```
hostname(config)# sunrpc-server interface_name ip_address mask service service_type  
protocol {tcp | udp} port[-port] timeout hh:mm:ss
```

このコマンドを使用して、Sun RPC アプリケーション検査で開いたピンホールを閉じるまでのタイムアウトを指定できます。たとえば、IP アドレスが 192.168.100.2 の Sun RPC サーバに対して 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で開いたピンホールが 30 分後に閉じるように指定します。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にあります。UDP、別のポート番号、ポート範囲を指定することもできます。ポート範囲を指定するには、範囲の開始ポート番号と終了ポート番号をハイフンで区切ります（111-113 など）。

サービス タイプは、特定のサービス タイプとそのサービスに使用するポート番号の間のマッピングを特定します。サービス タイプ（この例では 100003）を判定するには、Sun RPC サーバ マシンの 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
```

これによって、**sunrpc-server** コマンドを使用して実行されるコンフィギュレーションが削除されます。**sunrpc-server** コマンドを使用して、指定したタイムアウト値を持つピンホールを作成できます。

アクティブな 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
```

これによって、そのサービス（NFS、NIS など）で Sun RPC アプリケーション検査が開いたピンホールが消去されます。

## Sun RPC 検査の確認と監視

この項の出力例では、Sun RPC サーバの IP アドレスは 192.168.100.2 で内部インターフェイスにあり、Sun RPC クライアントの IP アドレスは 209.168.200.5 で外部インターフェイスにあるものとします。

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、IP アドレスが 192.168.100.2 で内部インターフェイスにある Sun RPC サーバの UDP ポート 111 で、タイムアウト間隔が 30 分に設定されていることが示されています。

Sun RPC サービスで開かれている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 サーバで実行されている 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 が UDP 上で実行されている mountd デーモンに対応しています。mountd プロセスは、通常、ポート 32780 を使用します。この例では、TCP 上で実行されている mountd プロセスがポート 650 を使用しています。

## TFTP 検査

TFTP 検査は、デフォルトでイネーブルになっています。

RFC 1350 で定義されているように、TFTP は TFTP サーバとクライアントの間のファイルの読み書きに使用される簡易プロトコルです。

セキュリティ アプライアンスは、TFTP トラフィックを検査し、ダイナミックに接続と変換（必要な場合）を作成し、TFTP クライアントとサーバの間のファイル転送を許可します。具体的には、検査エンジンは TFTP 読み取り要求（RRQ）、書き込み要求（WRQ）、およびエラー通知（ERROR）を検査します。

必要に応じて、ダイナミックなセカンダリ チャネルと PAT 変換が、有効な RRQ または WRQ の受信に割り当てられます。次に、このセカンダリ チャネルが、ファイル転送またはエラー通知用に TFTP によって使用されます。

TFTP サーバだけがセカンダリ チャネルのトラフィックを開始できます。また、TFTP クライアントとサーバの間に存在できる不完全なセカンダリ チャネルは 1 つまでです。サーバからのエラー通知があると、セカンダリ チャネルは閉じます。

TFTP トラフィックのリダイレクトにスタティック PAT が使用されている場合は、TFTP 検査をイネーブルにする必要があります。

## XDMCP 検査

XDMCP 検査はデフォルトでイネーブルですが、XDMCP 検査エンジンは、**established** コマンドが適切に構成されていないと使用できません。

XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションが確立される場合は、TCP が使用されます。

XWindows セッションを正常にネゴシエートして、開始するために、セキュリティ アプライアンスは、Xhosted コンピュータからの TCP 戻り接続を許可する必要があります。戻り接続を許可するには、セキュリティ アプライアンスに対して **established** コマンドを使用します。XDMCP がディスプレイを送信するポートをネゴシエートすると、**established** コマンドが参照され、この戻り接続を許可すべきかどうかを確認されます。

XWindows セッション中、マネージャは予約済みポート 6000 | n でディスプレイ Xserver と通信します。次の端末設定を行うと、各ディスプレイは別々の接続で Xserver と接続します。

```
setenv DISPLAY Xserver:n
```

n には、ディスプレイ番号を指定します。

XDMCP が使用されている場合、ディスプレイは IP アドレスを使用してネゴシエートされます。IP アドレスは、セキュリティ アプライアンスが必要に応じて NAT 処理できる要素です。XDMCP 検査では、PAT はサポートされません。





# 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 モードのみ

この章では、ARP 検査をイネーブルにする方法と、セキュリティ アプライアンスのブリッジング オペレーション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システムではなくセキュリティ コンテキストで入力します。

次の事項について説明します。

- [ARP 検査の設定 \(P.23-2\)](#)
- [MAC アドレス テーブルのカスタマイズ \(P.23-4\)](#)

## ARP 検査の設定

この項では、ARP 検査について説明し、これをイネーブルにする方法について説明します。次の事項を取り上げます。

- [ARP 検査の概要 \(P.23-2\)](#)
- [スタティック ARP エントリの追加 \(P.23-3\)](#)
- [ARP 検査のイネーブル化 \(P.23-3\)](#)

### ARP 検査の概要

デフォルトでは、すべての ARP パケットがセキュリティ アプライアンスを通過できます。ARP パケットのフローを制御するには、ARP 検査をイネーブルにします。

ARP 検査をイネーブルにすると、セキュリティ アプライアンスはすべての ARP パケットの MAC アドレス、IP アドレス、および発信元インターフェイスを ARP テーブルのスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および発信元インターフェイスが ARP エントリと一致した場合、パケットは通過します。
- MAC アドレス、IP アドレス、またはインターフェイス間でミスマッチがある場合、セキュリティ アプライアンスはパケットをドロップします。
- ARP パケットがスタティック ARP テーブルのどのエントリとも一致しない場合は、パケットをすべてのインターフェイスに転送するか（フラッド）、パケットをドロップするようにセキュリティ アプライアンスを設定できます。



(注)

専用の管理インターフェイスがある場合、このインターフェイスは、このパラメータがフラッドに設定されていてもパケットをフラッドしません。

ARP 検査は、悪意のあるユーザが他のホストまたはルータになりすますこと（ARP スプーフィング）を防ぎます。ARP スプーフィングは、「man-in-the-middle」攻撃（中間者攻撃）を可能にすることがあります。たとえば、ホストは ARP 要求をゲートウェイ ルータに送信し、ゲートウェイ ルータはゲートウェイ ルータ MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスの代わりに攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これによって、攻撃者は、すべてのホスト トラフィックを傍受してからルータに転送できます。

ARP 検査を行うと、正しい MAC アドレスとそれに関連付けられている IP アドレスがスタティック ARP テーブルにある限り、攻撃者は、攻撃者の MAC アドレスで ARP 応答を送信することができなくなります。

## スタティック ARP エントリの追加

ARP 検査は、ARP パケットを ARP テーブルのスタティック ARP エントリと比較します。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
```

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

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



(注)

透過ファイアウォールは、セキュリティ アプライアンスとの間のトラフィック（管理トラフィックなど）に、ARP テーブルのダイナミック ARP エントリを使用します。

## 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]
```

**flood** は、一致しない ARP パケットをすべてのインターフェイスに転送し、**no-flood** は、一致しないパケットをドロップします。



(注)

デフォルト設定では、一致しないパケットはフラッドします。スタティック エントリにある ARP だけがセキュリティ アプライアンスを通過するように制限するには、このコマンドを **no-flood** に設定します。

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

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

すべてのインターフェイスについて、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

この項では、MAC アドレス テーブルについて説明します。次の事項を取り上げます。

- [MAC アドレス テーブルの概要 \(P.23-4\)](#)
- [スタティック MAC アドレスの追加 \(P.23-4\)](#)
- [MAC アドレス タイムアウトの設定 \(P.23-5\)](#)
- [MAC アドレス ラーニングのディセーブル化 \(P.23-5\)](#)
- [MAC アドレス テーブルの表示 \(P.23-5\)](#)

### MAC アドレス テーブルの概要

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

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

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

元のパケットはドロップされます。

### スタティック MAC アドレスの追加

通常、MAC アドレスは、特定の MAC アドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。必要に応じて、スタティック MAC アドレスを MAC アドレス テーブルに追加できます。スタティック エントリを追加する利点の 1 つとして、MAC スプーフィングの防止があります。スタティック エントリと同じ MAC アドレスを持つクライアントが、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した場合、セキュリティ アプライアンスはトラフィックをドロップし、システム メッセージを生成します。

スタティック MAC アドレスを MAC アドレス テーブルに追加するには、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、発信元インターフェイスです。

## MAC アドレス タイムアウトの設定

ダイナミック MAC アドレス テーブルのデフォルトのタイムアウト値は 5 分ですが、タイムアウトは変更できます。タイムアウトを変更するには、次のコマンドを入力します。

```
hostname(config)# mac-address-table aging-time timeout_value
```

*timeout\_value* (分) は、5 ～ 720 (12 時間) です。5 分がデフォルトです。

## MAC アドレス ラーニングのディセーブル化

デフォルトでは、各インターフェイスは入ってきたトラフィックの MAC アドレスを自動的にラーニングして、セキュリティ アプライアンスは対応するエントリを MAC アドレス テーブルに追加します。必要に応じて MAC アドレス ラーニングをディセーブルにできますが、この場合、MAC アドレスをテーブルにスタティックに追加しないと、トラフィックがセキュリティ アプライアンスを通過できなくなります。

MAC アドレス ラーニングをディセーブルにするには、次のコマンドを入力します。

```
hostname(config)# mac-learn interface_name disable
```

このコマンドの **no** 形式を使用すると、MAC アドレス ラーニングが再度イネーブルになります。**clear configure mac-learn** コマンドは、すべてのインターフェイスで MAC アドレス ラーニングを再度イネーブルにします。

## MAC アドレス テーブルの表示

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

```
hostname# show mac-address-table [interface_name]
```

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

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

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

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





## PART 3

### VPN の設定









# IPSec と ISAKMP の設定

この章では、バーチャル プライベート ネットワークを構築するための IPSec と ISAKMP の標準の設定方法について説明します。ここでは、次の項目について説明します。

- [トンネリングの概要 \(P.24-1\)](#)
- [IPSec の概要 \(P.24-2\)](#)
- [ISAKMP の設定 \(P.24-3\)](#)
- [証明書グループ照合の設定 \(P.24-12\)](#)
- [IPSec の設定 \(P.24-14\)](#)
- [セキュリティ アソシエーションのクリア \(P.24-30\)](#)
- [暗号マップ コンフィギュレーションのクリア \(P.24-30\)](#)

## トンネリングの概要

トンネリングは、インターネットなどのパブリック TCP/IP ネットワークを使用して、リモート ユーザとプライベートな企業ネットワークとの間でセキュアな接続を構築することを可能にします。それぞれのセキュアな接続は、トンネルと呼ばれます。

セキュリティ アプライアンスは、ISAKMP と IPSec のトンネリング標準を使用してトンネルの構築と管理を行っています。ISAKMP と IPSec は、次の処理を実行できます。

- トンネル パラメータのネゴシエーション
- トンネルの確立
- ユーザとデータの認証
- セキュリティ キーの管理
- データの暗号化と復号化
- トンネル経由のデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理

セキュリティ アプライアンスは、双方向のトンネル エンドポイントとして機能します。プライベート ネットワークからプレーン パケットを受信してカプセル化し、トンネルを作成して、カプセル化したパケットをトンネルのもう一方の終端に送信します。トンネルの終端では、パケットのカプセル化が解除されて最終的な宛先に送信されます。また、カプセル化されたパケットをパブリック ネットワークから受信してカプセル化を解除し、プライベート ネットワーク上の最終的な宛先に送信します。

## IPSec の概要

最もセキュアなプロトコルであるとされている IPSec は、VPN トンネルの最も完全なアーキテクチャを提供します。IPSec は、ネットワーク内のデータを権限のないビューや修正から保護するため、およびデータがパブリック インターネットなどの保護されていないネットワークを通して転送されたときのために、認証サービスおよび暗号化サービスを提供します。当社の IPSec 標準の実装では、ESP セキュリティ プロトコルを使用して認証サービス、暗号化サービス、リプレイ攻撃防止サービスを提供しています。

セキュリティ アプライアンスは、次の 2 種類のコンフィギュレーションで IPSec を実装します。

- LAN-to-LAN コンフィギュレーションは、2 つの IPSec セキュリティ ゲートウェイ間、たとえばセキュリティ アプライアンス装置やその他のプロトコル準拠の VPN デバイスのコンフィギュレーションです。LAN-to-LAN VPN は、地理的に異なる場所にあるネットワークを接続します。
- リモートアクセス コンフィギュレーションは、セキュアなリモートアクセスをモバイル ユーザなどの Cisco VPN クライアントに提供します。リモートアクセス VPN を使用することで、リモート ユーザは中央集中型ネットワーク リソースに安全にアクセスできます。Cisco VPN クライアントは IPSec プロトコルに準拠し、特にセキュリティ アプライアンスと連携して動作するように設計されています。一方、セキュリティ アプライアンスは、さまざまなプロトコル準拠クライアントとの IPSec 接続を確立できます。

IPSec LAN-to-LAN 接続では、セキュリティ アプライアンスは発信側または応答側として機能します。IPSec リモートアクセス接続では、セキュリティ アプライアンスは応答側としてだけ機能します。発信側は SA を提案し、応答側は、設定されたセキュリティ アソシエーション (SA) パラメータに従って、SA の提示を受け入れるか、拒否するか、または対案を提示します。接続を確立するには、両方のエンティティで SA が一致する必要があります。

IPSec 用語では、ピアとは、リモートアクセス クライアントまたは別のセキュアなゲートウェイを意味します。

## ISAKMP の設定

この項では、Internet Key Exchange (IKE; インターネット キー エクスチェンジ) プロトコルについて説明します。このプロトコルは Internet Security Association and Key Management Protocol とも呼ばれます。セキュリティ アプライアンスの IKE コマンドは、ISAKMP をキーワードとして使用します。このマニュアルでも同様です。ISAKMP は、IPSec と連携することで、VPN をよりスケーラブルなものにします。ここでは、次の項目について説明します。

- [ISAKMP の概要 \(P.24-3\)](#)
- [ISAKMP ポリシーの設定 \(P.24-6\)](#)
- [外部インターフェイスでの ISAKMP のイネーブル化 \(P.24-7\)](#)
- [Aggressive モードでの ISAKMP のディセーブル化 \(P.24-7\)](#)
- [ISAKMP ピアの識別方式の決定 \(P.24-8\)](#)
- [IPSec over NAT-T のイネーブル化 \(P.24-8\)](#)
- [IPSec over TCP のイネーブル化 \(P.24-9\)](#)
- [リブートの前にアクティブセッションの終了を待機 \(P.24-10\)](#)
- [接続解除の前にピアに警告する \(P.24-11\)](#)

## ISAKMP の概要

IKE は ISAKMP と呼ばれ、2 台のホストで IPSec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーション プロトコルです。ISAKMP のネゴシエーションは 2 つのフェーズ (フェーズ 1 とフェーズ 2) に分かれています。

フェーズ 1 は、以後の ISAKMP ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ 2 は、データを保護するトンネルを作成します。

ISAKMP ネゴシエーションの条件を設定するには、以下を含む ISAKMP ポリシーを作成します。

- ピアの ID を確認する認証方式。
- データを保護し、プライバシーを守る暗号化方式。
- 送信者を特定し、搬送中にメッセージが変更されていないこと保証する Hashed Message Authentication Code (HMAC) 方式。
- 暗号キー決定アルゴリズムの強度を決定する Diffie-Hellman グループ。このアルゴリズムを使用して、セキュリティ アプライアンスは暗号キーとハッシュ キーを導出します。
- セキュリティ アプライアンスが暗号キーを置き換える前に、この暗号キーを使用する最長時間の制限。

表 24-1 に、ISAKMP ポリシー キーワードとそれらの値を示します。

表 24-1 CLI コマンド用の ISAKMP ポリシー キーワード

| コマンド                         | キーワード                | 意味                                    | 説明                                                                                                                                                                   |
|------------------------------|----------------------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| isakmp policy authentication | rsa-sig              | RSA シグニチャ アルゴリズムによって生成されたキー付きのデジタル証明書 | 各 IPsec ピアの ID を確立するためにセキュリティ アプライアンスが使用する認証方式を指定します。                                                                                                                |
|                              | dsa-sig              | DSA シグニチャ アルゴリズムによって生成されたキー付きのデジタル証明書 | 認証方式として、デジタル署名アルゴリズムのシグニチャを指定します。                                                                                                                                    |
|                              | pre-share<br>(デフォルト) | 事前共有キー                                | 事前共有キーは拡大するネットワークに対応して拡張が困難ですが、小規模ネットワークではセットアップが容易です。                                                                                                               |
| isakmp policy encryption     | des                  | 56 ビット DES-CBC                        | 2 つの IPsec ピア間で伝送されるユーザ データを保護する対称暗号化アルゴリズムを指定します。デフォルトは 168 ビット Triple DES です。Advanced Encryption Standard (AES; 高度暗号規格) は、128 ビット、192 ビット、256 ビットの長さのキーをサポートしています。 |
|                              | 3des (デフォルト)         | 168 ビット Triple DES                    |                                                                                                                                                                      |
|                              | aes                  |                                       |                                                                                                                                                                      |
|                              | aes-192<br>aes-256   |                                       |                                                                                                                                                                      |
| isakmp policy hash           | sha (デフォルト)          | SHA-1 (HMAC バリエーション)                  | データ整合性の確保のために使用するハッシュ アルゴリズムを指定します。パケットがそのパケットに記されている発信元から発信されたこと、また搬送中に変更されていないことを保証します。                                                                            |
|                              | md5                  | MD5 (HMAC バリエーション)                    | デフォルト値は SHA-1 です。MD5 は、SHA-1 よりもダイジェストが小さく、わずかに速いとされています。しかし、MD5 に対する攻撃が成功 (これは非常に困難) しても、IKE が使用する HMAC バリエーションがこの攻撃を防ぎます。                                          |

表 24-1 CLI コマンド用の ISAKMP ポリシー キーワード (続き)

| コマンド                   | キーワード                  | 意味                              | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------|------------------------|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| isakmp policy group    | 1                      | Group 1 (768 ビット)               | Diffie-Hellman グループ ID を指定します。この ID は、2 つの IPSec ピアが、相互に共有秘密情報を転送するのではなく、共有秘密情報を取り出すために使用します。<br><br>グループ 7 以外は、Diffie-Hellman グループ番号が小さいほど、実行に必要な CPU 時間も少なくなります。Diffie-Hellman のグループ番号が大きいほど、セキュリティも高くなります。<br><br>Cisco VPN クライアント バージョン 3.x 以降では、少なくともグループ 2 が必要です (DH グループ 1 を設定すると、Cisco VPN クライアントは接続できません)。<br><br>AES は、VPN-3DES のライセンスがあるセキュリティ アプライアンスに限りサポートされます。AES で必要なより大きいキー長をサポートするには、ISAKMP ネゴシエーションで Diffie-Hellman (DH) のグループ 5 を使用する必要があります。<br><br>グループ 7 は、PDA や携帯電話など処理能力の低いデバイス用に設計されていて、最高のセキュリティを提供します。Cercicom Movian クライアントにはグループ 7 が必要です。 |
|                        | 2 (デフォルト)              | Group 2(1024 ビット)               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                        | 5                      | Group 5(1536 ビット)               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                        | 7                      | グループ 7 (楕円曲線フィールドのサイズが 163 ビット) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| isakmp policy lifetime | 整数値<br>(86400 = デフォルト) | 120 ~ 2147483647 秒              | SA ライフタイムを指定します。デフォルトは 86,400 秒、つまり 24 時間です。原則として、ライフタイムが短いほど、ISAKMP ネゴシエーションの安全性は (ある程度まで) 高くなります。ただし、ライフタイムが短いほど、セキュリティ アプライアンスによる IPSec SA のセットアップ機能が高速になります。                                                                                                                                                                                                                                                                                                                                                                                                        |

各コンフィギュレーションは最大 20 個の ISAKMP ポリシーをサポートし、ポリシーごとに値セットが異なります。作成するポリシーごとに一意のプライオリティを割り当てます。プライオリティ番号が小さいほど、プライオリティが高くなります。

ISAKMP ネゴシエーションが始まると、ネゴシエーションを開始したピアはそのすべてのポリシーをリモートピアに送信し、リモートピアは一致するポリシーを探します。リモートピアは、一致するポリシーを見つけるまで、設定済みのポリシーに対してピアのすべてのポリシーを 1 つずつプライオリティ順に (最も高いプライオリティから) 照合します。

2 つのピアのポリシーの両方に、同一の暗号化、ハッシュ、認証、および Diffie-Hellman パラメータ値が含まれ、さらにリモートピアのポリシーで指定されているライフタイムが、発信側が送信したポリシーのライフタイム以下である場合、一致しているとされます。ライフタイムが等しくない場合、セキュリティ アプライアンスは短い方のライフタイムを使用します。一致するポリシーがない場合、ISAKMP はネゴシエーションを拒否し、SA は確立されません。

各パラメータに対して特定の値を選択するときは、セキュリティとパフォーマンスの間に暗黙のトレードオフが発生します。デフォルト値で得られるセキュリティ レベルは、ほとんどの組織のセキュリティ要件に十分に対応します。パラメータに対し 1 つの値だけをサポートしているピアと相互運用する場合は、相手のピアがサポートしている値に選択が制限されます。



(注)

新しい ASA コンフィギュレーションには、デフォルトの ISAKMP ポリシーはありません。

## ISAKMP ポリシーの設定

ISAKMP ポリシーを設定するには、グローバル コンフィギュレーション モードで、**isakmp policy** コマンドにさまざまな引数を指定します。ISAKMP ポリシー コマンドのシンタックスは次のとおりです。

**isakmp policy priority attribute\_name [attribute\_value | integer]**

ISAKMP コマンドには、それぞれプライオリティを指定する必要があります。プライオリティ番号によってポリシーが一意に識別され、ISAKMP ネゴシエーションにおけるポリシーのプライオリティが決定されます。

ISAKMP を設定してイネーブルにするには、例を参考にして、次の手順を実行します。



(注)

所定のポリシー パラメータに値を指定しない場合、デフォルト値が適用されます。

- ステップ 1** 暗号化アルゴリズムを指定します。デフォルトは Triple DES です。この例では、暗号化を DES に設定します。

```
isakmp policy priority encryption [aes | aes-192 | aes-256 | des | 3des]
```

次の例を参考にしてください。

```
hostname(config)# isakmp policy 2 encryption des
```

- ステップ 2** ハッシュ アルゴリズムを指定します。デフォルトは SHA-1 です。この例では、MD5 を設定します。

```
isakmp policy priority hash [md5 | sha]
```

次の例を参考にしてください。

```
hostname(config)# isakmp policy 2 hash md5
```

- ステップ 3** 認証方式を指定します。デフォルトは事前共有キーです。この例では、RSA シグニチャを設定します。

```
isakmp policy priority authentication [pre-share | dsa-sig | rsa-sig]
```

次の例を参考にしてください。

```
hostname(config)# isakmp policy 2 authentication rsa-sig
```

- ステップ 4** Diffie-Hellman グループ識別番号を指定します。デフォルトはグループ 2 です。この例では、グループ 5 を設定します。

```
isakmp policy priority group [1 | 2 | 5 | 7]
```

次の例を参考にしてください。

```
hostname(config)# isakmp policy 2 group 5
```

- ステップ 5** SA ライフタイムを指定します。この例では、4 時間（14400 秒）のライフタイムを設定します。デフォルトは 86400 秒（24 時間）です。

```
isakmp policy priority lifetime seconds
```

次の例を参考にしてください。

```
hostname(config)# isakmp policy 2 lifetime 14400
```

## 外部インターフェイスでの ISAKMP のイネーブル化

VPN トンネルを終端するインターフェイスでは、ISAKMP をイネーブルにする必要があります。通常は外部（つまり、パブリック）インターフェイスです。

ISAKMP をイネーブルにするには、次のコマンドを入力します。

```
isakmp enable interface-name
```

次の例を参考にしてください。

```
hostname(config)# isakmp enable outside
```

## Aggressive モードでの ISAKMP のディセーブル化

フェーズ 1 の ISAKMP ネゴシエーションでは、Main モードまたは Aggressive モードのいずれかを使用できます。どちらのモードも同じサービスを提供しますが、Aggressive モードでは、ピア間で 3 回の合計 6 つのメッセージ交換ではなく、2 回の合計 3 つのメッセージ交換だけですみます。Aggressive モードの方が高速ですが、通信パーティの ID は保護されません。このため、セキュアな SA を確立する前に、ピア間で ID 情報を交換する必要があります。Aggressive モードはデフォルトでイネーブルになっています。

- 交換回数の多い Main モードは低速ですが、通信しているピアの ID を保護します。
- Aggressive モードは高速ですが、ピアの ID を保護しません。

Aggressive モードの ISAKMP をディセーブルにするには、次のコマンドを入力します。

```
isakmp am-disable
```

次の例を参考にしてください。

```
hostname(config)# isakmp am-disable
```

Aggressive モードをいったんディセーブルにした後でイネーブルに戻すには、**no** 形式でコマンドを使用します。次の例を参考にしてください。

```
hostname(config)# no isakmp am-disable
```



(注)

Agressive モードをディセーブルにすると、Cisco VPN クライアントは、セキュリティ アプライアンスへのトンネルを確立するための事前共有キー認証を使用できなくなります。ただし、証明書に基づく認証（つまり ASA または RSA）を使用してトンネルを確立できます。

## ISAKMP ピアの識別方式の決定

フェーズ I の ISAKMP ネゴシエーションでは、ピアは相互に相手を識別する必要があります。この識別方法は、次のオプションから選択できます。

|       |                                                                                                                           |
|-------|---------------------------------------------------------------------------------------------------------------------------|
| アドレス  | ISAKMP の識別情報を交換するホストの IP アドレスを使用します。                                                                                      |
| 自動    | 接続タイプによって ISAKMP ネゴシエーションが決まります。 <ul style="list-style-type: none"> <li>事前共有キーの IP アドレス</li> <li>証明書認証の証明書認定者名</li> </ul> |
| ホスト名  | ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。                                                      |
| キー ID | リモート ピアが事前共有キーの検索に使用する文字列を使用します。                                                                                          |

セキュリティ アプライアンスは、ピアに送信するフェーズ I の ID を使用します。これは、事前共有キーで認証を行う Main モードでの LAN-to-LAN 接続を除いて、すべての VPN シナリオで行われます。

デフォルト設定は hostname です。

ピア識別方式を変更するには、次のコマンドを入力します。

```
isakmp identity {address | hostname | key-id id-string | auto}
```

たとえば、次のコマンドはピア識別方法を「自動」に設定します。

```
hostname(config)# isakmp identity auto
```

## IPsec over NAT-T のイネーブル化

NAT-T を使用すると、IPsec ピアは NAT デバイスを介した接続を確立できます。NAT-T は UDP データグラムの IPsec トラフィックをカプセル化し、ポート 4500 を使用して、NAT デバイスにポート情報を提供します。NAT-T はすべての NAT デバイスを自動検出し、必要な場合だけ IPsec トラフィックをカプセル化します。この機能は、デフォルトでディセーブルになっています。

セキュリティ アプライアンスは、データ交換を行うクライアントに応じて、標準の IPsec、IPsec over TCP、NAT-T、および IPsec over UDP を同時にサポートできます。NAT-T と IPsec over UDP の両方がイネーブルになっている場合、NAT-T が優先されます。IPsec over TCP は、イネーブルになっている場合、その他のすべての接続方式よりも優先されます。

NAT-T をイネーブルにすると、セキュリティ アプライアンスは、IPsec がイネーブルになっているすべてのインターフェイス上で自動的にポート 4500 を開きます。

セキュリティ アプライアンスは、次の両方のネットワークではなく、どちらか一方のネットワークで動作する単一の NAT/PAT デバイスの背後にある複数の IPsec ピアをサポートします。

- LAN-to-LAN
- リモートアクセス



混合環境では、リモートアクセス トンネルはネゴシエーションに失敗します。これは、すべてのピアが同じパブリック IP アドレス、つまり同じ NAT デバイスから発信されたように見えるためです。また、リモートアクセス トンネルは、LAN-to-LAN トンネルグループ（つまり NAT デバイスの IP アドレス）と同じ名前を使用することが多いため、混合環境では失敗します。この名前の一致により、NAT デバイスの背後にあるピアの LAN-to-LAN とリモートアクセスの混合ネットワークでは、複数のピア間のネゴシエーションが失敗する場合があります。

## NAT-T の使用

NAT-T を使用するには、次の作業を実行する必要があります。

- ステップ 1** セキュリティ アプライアンスでグローバルに IPSec over NAT-T をイネーブルにするには、次のコマンドを入力します。

```
isakmp nat-traversal natkeepalive
```

natkeepalive は 10 ～ 3600 秒の範囲です。デフォルトは、20 秒です。

たとえば、次のコマンドを入力して、NAT-T をイネーブルにし、キープアライブ値を 1 時間に設定します。

```
hostname(config)# isakmp nat-traversal 3600
```

- ステップ 2** IPSec フラグメンテーション ポリシーに「before-fragmentation」オプションを選択します。

このオプションは、IP フラグメンテーションをサポートしていない NAT デバイス間をトラフィックが通過できるようにします。このオプションを使用しても、IP フラグメンテーションをサポートしていない NAT デバイスの動作を妨げることはありません。

## IPSec over TCP のイネーブル化

IPSec over TCP を使用すると、標準 ESP や標準 ISAKMP が機能できない環境、または既存のファイアウォール規則を変更した場合に限って機能できる環境で、Cisco VPN クライアントが動作できるようになります。IPSec over TCP は TCP のようなパケット内で ISAKMP プロトコルと IPSec プロトコルをカプセル化し、NAT と PAT の両方のデバイスとファイアウォールを通過するセキュアなトンネリングを実現します。この機能は、デフォルトでディセーブルになっています。



(注)

この機能は、プロキシ ベースのファイアウォールでは動作しません。

IPSec over TCP は、リモートアクセス クライアントで動作します。IPSec over TCP をグローバルにイネーブルにすると、ISAKMP がイネーブルにされたすべてのインターフェイスで動作します。これは、セキュリティ アプライアンス機能に対応するクライアントに限られます。LAN-to-LAN 接続では機能しません。

セキュリティ アプライアンスは、データ交換を行うクライアントに応じて、標準の IPSec、IPSec over TCP、NAT-Traversal、および IPSec over UDP を同時にサポートできます。IPSec over TCP は、イネーブルになっている場合、その他のすべての接続方式よりも優先されます。

1 度に 1 つのトンネルをサポートする VPN 3002 ハードウェア クライアントは、標準の IPSec、IPSec over TCP、NAT-Traversal、または IPSec over UDP を使用して接続できます。

セキュリティ アプライアンスとその接続先のクライアントの両方で IPSec over TCP をイネーブルにします。

最大 10 個のポートを指定して、それらのポートに対して IPSec over TCP をイネーブルにできます。ポート 80 (HTTP) やポート 443 (HTTPS) などの周知のポートを入力すると、そのポートに関連付けられているプロトコルがパブリック インターフェイスで機能しなくなることを示すアラートが表示されます。その結果、パブリック インターフェイスを介してセキュリティ アプライアンスを管理するためにブラウザを使用することができなくなります。この問題を解決するには、HTTP/HTTPS 管理を別のポートに再設定します。

デフォルト ポートは 10000 です。

セキュリティ アプライアンスだけでなく、クライアントでも TCP ポートを設定する必要があります。クライアントの設定には、セキュリティ アプライアンス用に設定したポートを少なくとも 1 つ含める必要があります。

セキュリティ アプライアンスでグローバルに IPSec over TCP をイネーブルにするには、次のコマンドを入力します。

```
isakmp ipsec-over-tcp [port port 1...port0]
```

次の例では、IPSec over TCP をポート 45 でイネーブルにしています。

```
hostname(config)# isakmp ctcp port 45
```

## リブートの前にアクティブ セッションの終了を待機

すべてのアクティブセッションが自発的に終了した場合に限り、セキュリティ アプライアンスがリブートするようにスケジュールを設定できます。この機能は、デフォルトでディセーブルになっています。

セキュリティ アプライアンスのリブートの前にすべてのアクティブ セッションが自発的に終了するまで待機する機能をイネーブルにするには、次のコマンドを入力します。

```
isakmp reload-wait
```

次の例を参考にしてください。

```
hostname(config)# isakmp reload-wait
```

**reload** コマンドを使用して、セキュリティ アプライアンスをリブートします。**reload-wait** コマンドを設定すると、**reload quick** コマンドを使用して **reload-wait** 設定を無効にできます。**reload** コマンドと **reload-wait** コマンドは特権 EXEC モードで使用できます。どちらにも **isakmp** プレフィックスは付けません。

## 接続解除の前にピアに警告する

セキュリティ アプライアンスのシャットダウンまたはリブート、セッション アイドル タイムアウト、最大接続時間の超過、管理者による停止などいくつかの理由で、リモートアクセス セッションまたは LAN-to-LAN セッションがドロップすることがあります。

セキュリティ アプライアンスは、限定されたピア、つまり Cisco VPN クライアントと VPN 3002 ハードウェア クライアントに対して、セッションが接続解除される直前に通知できます (LAN-to-LAN コンフィギュレーションの場合)。アラートを受信したピアまたはクライアントは、その理由をデコードしてイベント ログまたはポップアップ パネルに表示します。この機能は、デフォルトでディセーブルになっています。

限定されたクライアントとピアには次のものが含まれます。

- アラートがイネーブルになっているセキュリティ アプライアンス
- バージョン 4.0 以降のソフトウェアを実行している Cisco VPN クライアント (アラート設定は不要)
- バージョン 4.0 以降のソフトウェアを実行し、アラートがイネーブルになっている VPN 3002 ハードウェア クライアント
- バージョン 4.0 以降のソフトウェアを実行し、アラートがイネーブルになっている VPN 3000 シリーズ コンセントレータ

IPsec ピアに対する接続解除の通知をイネーブルにするには、**isakmp disconnect-notify** コマンドを入力します。

次の例を参考にしてください。

```
hostname(config)# isakmp disconnect-notify
```

## 証明書グループ照合の設定

トンネルグループは、ユーザの接続条件とアクセス権を定義します。証明書グループ照合では、ユーザ証明書のサブジェクト DN または発行者 DN を使用して、ユーザとトンネルグループを照合します。

証明書のこれらのフィールドに基づいてユーザをトンネルグループと照合するには、まず一致基準を定義した規則を作成し、次に各規則を目的のトンネルグループに関連付ける必要があります。

証明書マップを作成するには、**crypto ca certificate map** コマンドを使用します。トンネルグループを定義するには、**tunnel-group** コマンドを使用します。

また、証明書ユーザの許可グループを識別するための方法として、次のいずれか 1 つを設定する証明書グループ照合ポリシーも設定する必要があります。

- 規則からグループを照合する。
- organizational unit (OU) フィールドからグループを照合する。
- すべての証明書ユーザにデフォルトのグループを使用する。

上記の方法のいずれか、またはすべてを使用できます。

## 証明書グループ照合の規則とポリシーの作成

証明書ベースの ISAKMP セッションをトンネルグループにマッピングするためのポリシーと規則を設定し、証明書マップ エントリをトンネルグループに関連付けるには、グローバル コンフィギュレーション モードで **tunnel-group-map** コマンドを入力します。

このコマンドのシンタックスは次のとおりです。

```
tunnel-group-map enable {rules | ou | ike-id | peer ip}
```

```
tunnel-group-map [rule-index] enable policy
```

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>policy</i>     | <p>証明書からトンネルグループ名を取得するためのポリシーを指定します。<br/><i>policy</i> には、次のいずれか 1 つを指定できます。</p> <p><b>ike-id</b>：トンネルグループを規則検索によって決定しない、または <i>ou</i> から取得しない場合、証明書ベースの ISAKMP セッションは、フェーズ 1 の ISAKMP ID の内容に基づいてトンネルグループにマッピングされることを示します。</p> <p><b>ou</b>：トンネルグループを規則検索によって決定しない場合、サブジェクト認定者名 (DN) の OU の値を使用することを示します。</p> <p><b>peer-ip</b>：トンネルグループを規則検索によって決定しない、OU から取得しない、または <i>ike-id</i> 方式によって取得しない場合、ピアの IP アドレスを使用することを示します。</p> <p><b>rules</b>：証明書ベースの ISAKMP セッションが、このコマンドによって設定された証明書マップの関連付けに基づいて、トンネルグループにマッピングされることを示します。</p> |
| <i>rule index</i> | <p>オプション。<b>crypto ca certificate map</b> コマンドで指定したパラメータを参照します。値は、1 ～ 65,535 です。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                |

次のことに注意してください。

- このコマンドの起動が他と重複せず、マップ インデックスの参照が 1 度だけであれば、このコマンドを何度でも起動できる。
- 規則は 255 文字以下である。
- 1 つのグループに複数の規則を割り当てられる。複数の規則を割り当てるには、まず規則のプライオリティを追加し、グループ化します。次に、各グループに必要な数だけ基準文を定義します。1 つのグループに複数の規則を割り当てた場合、テストされる最初の規則の照合結果は一致します。
- ユーザを特定のトンネルグループに割り当てる前にすべての一致基準が必要な場合は、単一の規則を作成する。すべての一致基準が必要であることは、論理 AND 操作に相当します。または、ユーザを特定のトンネルグループに割り当てる前にすべての一致基準が必要な場合は、基準ごとに 1 つの規則を作成します。一致基準が 1 つだけ必要であることは、論理 OR 操作に相当します。

次の例では、フェーズ 1 の ISAKMP ID の内容に基づいて、証明書ベースの ISAKMP セッションをトンネルグループにマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable ike-id
hostname(config)#
```

次の例では、ピアの IP アドレスに基づいて、証明書ベースの ISAKMP セッションをトンネルグループにマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable peer-ip
hostname(config)#
```

次の例では、サブジェクト認定者名 (DN) の組織ユニット (OU) に基づいて、証明書ベースの ISAKMP セッションをマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable ou
hostname(config)#
```

次の例では、設定された規則に基づいて、証明書ベースの ISAKMP セッションをマッピングする機能をイネーブルにします。

```
hostname(config)# tunnel-group-map enable rules
hostname(config)#
```

## tunnel-group-map default-group コマンドの使用

このコマンドは、コンフィギュレーションでトンネルグループが指定されていない場合に使用する、デフォルトのトンネルグループを指定します。

コマンドのシンタックスは、**tunnel-group-map [rule-index] default-group tunnel-group-name** です。**rule-index** は規則のプライオリティで、**tunnel-group name** は既存のトンネルグループである必要があります。

## IPsec の設定

この項では、IPsec に関する背景情報と、IPsec を使用して VPN を実装するときにセキュリティ アプライアンスを設定する手順について説明します。次の項目について説明します。

- [IPsec トンネルの理解 \(P.24-14\)](#)
- [トランスフォーム セットの概要 \(P.24-14\)](#)
- [暗号マップの定義 \(P.24-15\)](#)
- [インターフェイスへの暗号マップの適用 \(P.24-21\)](#)
- [インターフェイス アクセスリストの使用 \(P.24-22\)](#)
- [IPsec SA のライフタイムの変更 \(P.24-24\)](#)
- [基本的な IPsec コンフィギュレーションの作成 \(P.24-24\)](#)
- [ダイナミック暗号マップの使用 \(P.24-26\)](#)
- [サイトツーサイト冗長性の定義 \(P.24-29\)](#)
- [IPsec コンフィギュレーションの表示 \(P.24-29\)](#)

### IPsec トンネルの理解

IPsec トンネルとは、セキュリティ アプライアンスがピア間に確立する SA のセットのことです。SA は機密データに適用するプロトコルとアルゴリズムを定義し、ピアが使用するキー関連情報を指定します。IPsec SA は、ユーザ トラフィックの実際の伝送を制御します。SA は単方向ですが、通常ペア（着信と発信）で確立されます。

ピアは SA ごとに使用する設定をネゴシエートします。各 SA は次のもので構成されます。

- トランスフォーム セット
- 暗号マップ
- アクセスリスト
- トンネルグループ
- 事前フラグメンテーション ポリシー

### トランスフォーム セットの概要

トランスフォーム セットとは、セキュリティ アプライアンスによるデータの保護方法を定義したセキュリティ プロトコルとアルゴリズムの組み合わせのことです。複数のトランスフォーム セットを作成し、最大 6 個のトランスフォーム セットを暗号マップに指定します。

IPsec SA のネゴシエート中、2 つのピアは、両方のピアで一致しているトランスフォーム セットを識別する必要があります。次にセキュリティ アプライアンスは一致しているトランスフォームを使用して、暗号マップに対するアクセスリストのデータ フローを保護する SA を作成します。

トランスフォーム セット定義を変更すると、セキュリティ アプライアンスはトンネルを切り離します。詳細については「[セキュリティ アソシエーションのクリア](#)」を参照してください。



(注)

トランスフォーム セットの要素を 1 つだけ消去または削除すると、セキュリティ アプライアンスはその要素を参照する暗号マップを自動的に削除します。

## 暗号マップの定義

暗号マップは、IPsec SA でネゴシエートされる IPsec ポリシーを定義します。暗号マップには、次のものが含まれます。

- IPsec 接続が許可および保護するパケットを識別するためのアクセスリスト
- ピア ID
- IPsec トラフィックのローカル アドレス（詳細については、「[インターフェイスへの暗号マップの適用](#)」を参照）
- ピアのセキュリティ設定の照合に使用される最大 6 個のトランスフォーム セット

暗号マップセットは、同じマップ名を持つ 1 つまたは複数の暗号マップで構成されます。最初の暗号マップを作成したときに、暗号マップセットを作成します。暗号マップを作成または追加するコマンドのシンタックスは、次のとおりです。

```
crypto map map-name seq-num match address access-list-name
```

このコマンドを続けて入力すると、暗号マップを暗号マップ セットに追加できます。次の例では、暗号マップを追加する暗号マップセットの名前は「mymap」です。

```
crypto map mymap 10 match address 101
```

同じ名前を持つ暗号マップの中で、上記のシンタックスで示されているシーケンス番号 (seq-num) はそれぞれ異なります。暗号マップに割り当てられているシーケンス番号によって、暗号マップセット内の暗号マップ間のプライオリティが決まります。シーケンス番号が小さいほど、プライオリティが高くなります。暗号マップ セットをインターフェイスに割り当てると、セキュリティ アプライアンスは、そのインターフェイスを通過するすべての IP トラフィックと暗号マップ セット内の暗号マップを、シーケンス番号が低い順に照合して評価します。

暗号マップに割り当てられている Access Control List (ACL; アクセス コントロール リスト) は、同じアクセスリスト名を持つすべての Access Control Entry (ACE; アクセス コントロール エントリ) で構成されます。コマンドのシンタックスは、次のとおりです。

```
access-list access-list-name {deny | permit} ip source source-netmask destination destination-netmask
```

各 ACL は、同じアクセスリスト名を持つ 1 つまたは複数の ACE で構成されます。最初の ACE を作成したときに、ACL を作成します。ACL を作成または追加するコマンドのシンタックスは、次のとおりです。

```
access-list access-list-name {deny | permit} ip source source-netmask destination destination-netmask
```

次の例では、セキュリティ アプライアンスは、10.0.0.0 サブネットから 10.1.1.0 サブネットまでのすべてのトラフィック フローに対して、暗号マップに割り当てられている IPsec 保護を適用します。

```
access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

パケットが一致する暗号マップによって、SA ネゴシエーションで使用されるセキュリティ設定が決定します。ローカルのセキュリティ アプライアンスがネゴシエーションを開始する場合は、スタティック暗号マップで指定されたポリシーを使用して、指定のピアに送信するオファーを作成します。ピアがネゴシエーションを開始する場合、セキュリティ アプライアンスはポリシーをスタティック暗号マップと照合しますが、これが失敗した場合は、暗号マップセットのダイナミック暗号マップと照合して、ピアのオファーを受け入れるか拒否するかを決定します。

2 つのピアが SA の確立に成功するには、両方のピアが互換性のある暗号マップを少なくとも 1 つ持っている必要があります。互換性が成立するには、暗号マップが次の条件を満たす必要があります。

- 暗号マップに、互換性を持つ暗号 ACL（たとえば、ミラー イメージ ACL）が含まれている。応答するピアがダイナミック暗号マップを使用する場合、IPsec を適用するための要件として、セキュリティ アプライアンスもダイナミック暗号マップを使用する必要があります。
- 各暗号マップが他のピアを識別する（応答するピアがダイナミック暗号マップを使用していない場合）。
- 暗号マップに、共通のトランスフォーム セットが少なくとも 1 つある。

1 つのインターフェイスに適用できる暗号マップ セットは 1 つだけです。次の条件のいずれかが当てはまる場合は、セキュリティ アプライアンス上の特定のインターフェイスに対して複数の暗号マップを作成します。

- 特定のピアに異なるデータ フローを処理させる。
- さまざまなタイプのトラフィックにさまざまな IPsec セキュリティを適用する。

たとえば、暗号マップを 1 つ作成し、2 つのサブネット間のトラフィックを識別する ACL を割り当て、トランスフォーム セットを 1 つ割り当てます。別の暗号マップを作成し、別の 2 つのサブネット間のトラフィックを識別する ACL を割り当て、VPN パラメータが異なるトランスフォーム セットを適用します。

1 つのインターフェイスに複数の暗号マップを作成する場合は、暗号マップ セット内のプライオリティを決めるシーケンス番号 (seq-num) を各暗号マップ エントリに指定します。

各 ACE には permit 文または deny 文が含まれます。表 24-2 に、暗号マップに適用される ACL での ACE の許可と拒否の特別な意味を示します。

**表 24-2 発信トラフィックに適用されるアクセスリストにおける許可と拒否の特別な意味**

| 暗号マップ評価の結果                       | 対応                                                                                                                                                                                                                             |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| permit 文が含まれている ACE の基準と一致       | パケットを暗号マップ セットの残りの ACE と照合して評価することを停止し、パケット セキュリティ設定を、暗号マップに割り当てられているトランスフォーム セットと照合して評価します。セキュリティ設定がトランスフォーム セットのセキュリティ設定と一致すると、セキュリティ アプライアンスは関連する IPsec 設定を適用します。一般に発信トラフィックの場合、IPsec 設定の適用とはパケットの復号化、認証、ルーティングを行うことを意味します。 |
| deny 文が含まれている ACE の基準と一致         | パケットを評価中の暗号マップの残りの ACE と照合して評価することを中断し、次の暗号マップ（暗号マップに割り当てられているシーケンス番号で判断する）の ACE との照合と評価を再開します。                                                                                                                                |
| 暗号マップ セット内のテスト済みのすべての許可 ACE と不一致 | パケットを暗号化せずにルーティングします。                                                                                                                                                                                                          |

deny 文が含まれている ACE は、IPsec 保護が不要な発信トラフィック（たとえば、ルーティング プロトコルトラフィックなど）をフィルタリングして除外します。したがって、暗号アクセスリストの permit 文と照合して評価する必要のない発信トラフィックをフィルタリングするために、最初の deny 文を挿入します。



暗号化された着信パケットに対しては、セキュリティ アプライアンスは送信元アドレスと ESP SPI を使用して、パラメータの復号化を決定します。セキュリティ アプライアンスは、パケットを復号化した後で、復号化されたパケットの内部ヘッダーを、そのパケットの SA に関連付けられている ACL の許可 ACE と比較します。内部ヘッダーがプロキシと一致しない場合、セキュリティ アプライアンスはそのパケットをドロップします。内部ヘッダーがプロキシと一致する場合、セキュリティ アプライアンスはそのパケットをルーティングします。

暗号化されていない着信パケットの内部ヘッダーを比較する場合は、セキュリティ アプライアンスはすべての拒否規則を無視します。これは、拒否規則によってフェーズ 2 の SA の確立が妨げられるためです。

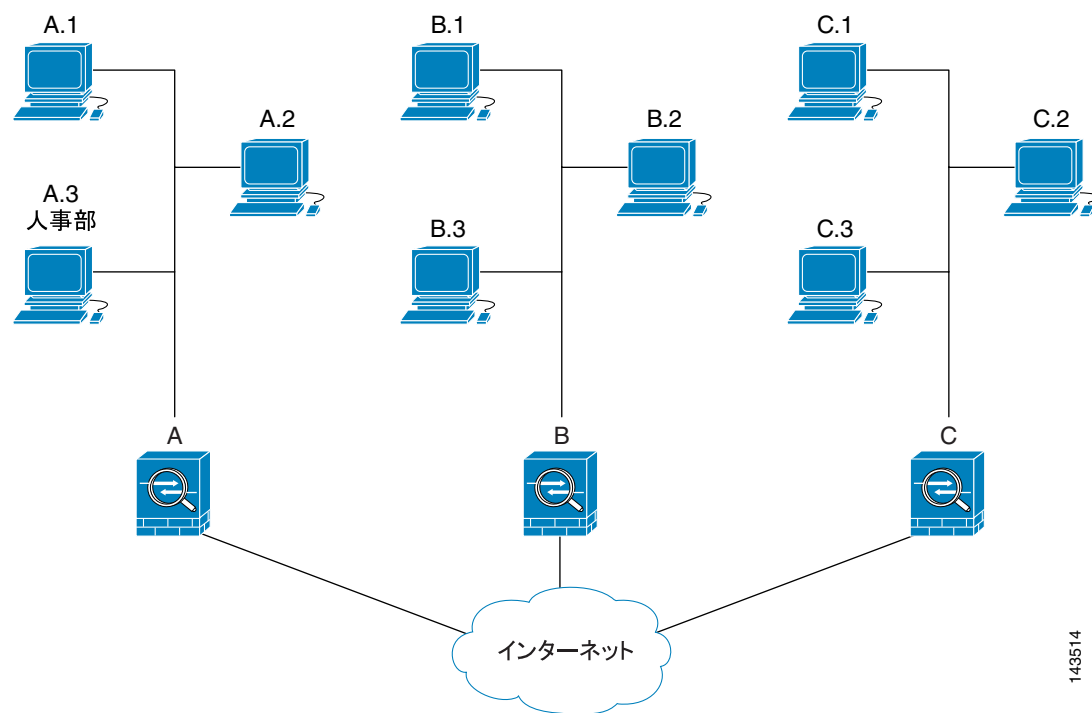


(注)

暗号化されていない着信トラフィックをクリア テキストとしてルーティングするには、ACE の許可の前に ACE の拒否を挿入します。

図 24-1 に、セキュリティ アプライアンスの LAN-to-LAN ネットワークの例を示します。

図 24-1 ACE の許可と拒否がトラフィックに及ぼす影響（概念上のアドレス）



この図に示され、また以下の説明で使用されている単純なアドレス表記は、抽象化したものです。実際の IP アドレスを使用した例は、この説明の後に示します。

この LAN-to-LAN ネットワーク例において、セキュリティ アプライアンス A、B、および C を設定する目的は、図 24-1 に示したホストのいずれか 1 台から発信されるすべてのトラフィックのトンネリングを許可することです。ただし、ホスト A.3 から発信されるトラフィックには人事部の機密データが含まれるため、他のトラフィックよりも強固な暗号化と頻繁なキー再生が必要です。そのため、ホスト A.3 から発信されるトラフィックには特別なトランスフォーム セットを割り当てます。

セキュリティ アプライアンス A の発信トラフィックを設定するために、2つの暗号マップを作成します。1つはホスト A.3 の発信トラフィック用で、もう1つはネットワーク A の別のホストの発信トラフィック用です。次に例を示します。

```
Crypto Map Seq_No_1
  deny packets from A.3 to B
  deny packets from A.3 to C
  permit packets from A to B
  permit packets from A to C
Crypto Map Seq_No_2
  permit packets from A.3 to B
  permit packets from A.3 to C
```

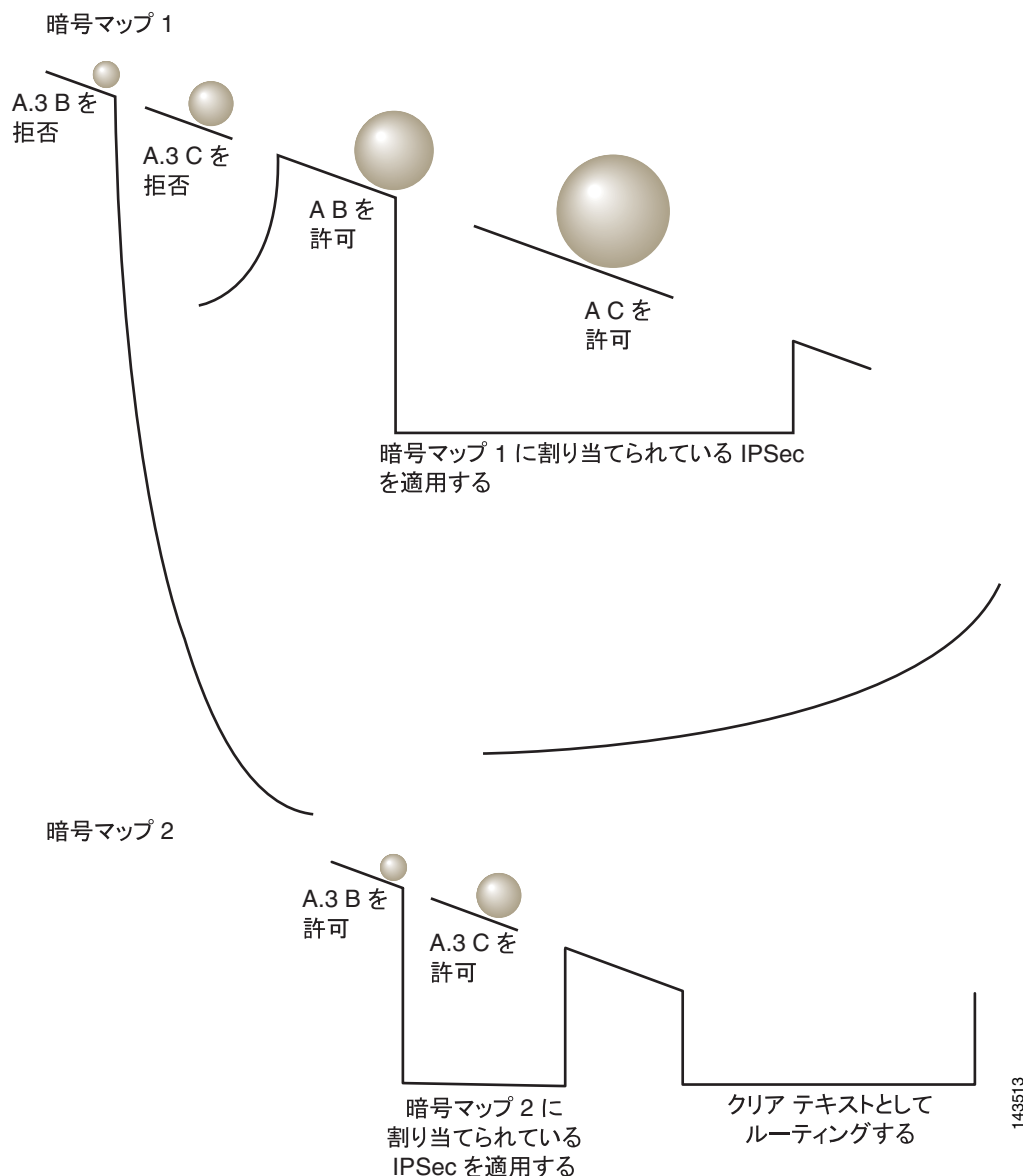
ACL を作成したら、一致するパケットごとに必要な IPSec を適用するためのトランスフォーム セットを各暗号マップに割り当てます。

カスケード ACL とは、拒否 ACE を挿入することで、ACL との照合と評価をバイパスし、暗号マップセット内の次の ACL との照合と評価を再開するものです。暗号マップごとに異なる IPSec 設定を関連付けることができるため、拒否 ACE を使用することで、特別なトラフィックを対応する暗号マップでの以後の評価から除外し、異なるセキュリティを提供する別の暗号マップ、または異なるセキュリティを必要とする別の暗号マップの permit 文と特別なトラフィックを照合することができます。暗号 ACL に割り当てられているシーケンス番号によって、暗号マップセット内の評価の順序が決まります。

図 24-2 に、上記のイメージ ACE から作成されたカスケード ACL を示します。この図の各記号の意味は次のとおりです。

|                                                                                     |                                                                                                      |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
|  | 暗号マップセット内の暗号マップ。                                                                                     |
|  | (すき間がある直線) パケットが ACE に一致した時点で暗号マップの照合を終了します。                                                         |
|  | 1つの ACE の説明と一致したパケット。それぞれの大きさのボールは、図中の別々の ACE に一致する異なるパケットを表しています。大きさの違いは、各パケットの発信元と宛先が異なることを示しています。 |
|  | 暗号マップセット内での次の暗号マップへのリダイレクション。                                                                        |
|  | パケットが ACE に一致するか、または暗号マップセット内のすべての許可 ACE に一致しない場合の応答。                                                |

図 24-2 暗号マップセット内のカスケード ACL



セキュリティ アプライアンス A は、ホスト A.3 から発信されたパケットが許可 ACE と一致するまで評価し、暗号マップに関連付けられている IPsec セキュリティの割り当てを試行します。このパケットが拒否 ACE と一致すると、セキュリティ アプライアンスはこの暗号マップの残りの ACE を無視し、次の暗号マップ（暗号マップに割り当てられているシーケンス番号で判断する）との照合と評価を再開します。この例では、セキュリティ アプライアンス A がホスト A.3 から発信されたパケットを受信すると、このパケットを最初の暗号マップの拒否 ACE と照合し、次の暗号マップでの照合と評価を再開します。パケットが 2 番目の暗号マップの許可 ACE と一致すると、関連付けられた IPsec セキュリティ（強固な暗号化と頻繁なキー再生）がパケットに適用されます。

このネットワーク例におけるセキュリティ アプライアンスの設定を完了するために、ミラー暗号マップをセキュリティ アプライアンス B と C に割り当てます。しかし、セキュリティ アプライアンスは、暗号化された着信トラフィックの評価では拒否 ACE を無視するため、拒否 A.3 B と拒否 A.3 C の ACE のミラーに相当するものを無視できます。したがって、暗号マップ 2 のミラーに相当するものを無視できます。このため、セキュリティ アプライアンス B と C のカスケード ACL の設定は不要です。

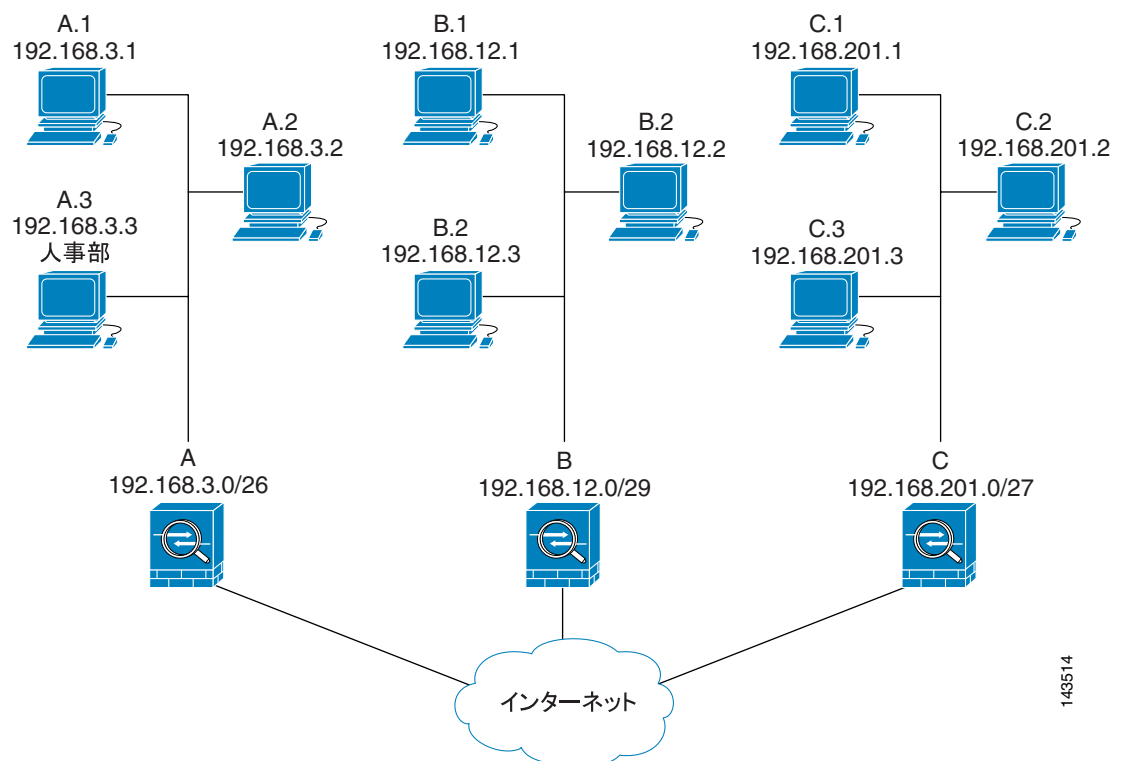
表 24-3 に、図 24-1 の 3 台のセキュリティ アプライアンス用に設定された暗号マップに割り当てられている ACL を示します。

表 24-3 許可文と拒否文の例（概念図）

| セキュリティ アプライアンス A     |           | セキュリティ アプライアンス B     |          | セキュリティ アプライアンス C     |          |
|----------------------|-----------|----------------------|----------|----------------------|----------|
| 暗号マップ<br>シーケンス<br>番号 | ACE パターン  | 暗号マップ<br>シーケンス<br>番号 | ACE パターン | 暗号マップ<br>シーケンス<br>番号 | ACE パターン |
| 1                    | A.3 B を拒否 | 1                    | B A を許可  | 1                    | C A を許可  |
|                      | A.3 C を拒否 |                      | B C を許可  |                      | C B を許可  |
|                      | A B を許可   |                      |          |                      |          |
|                      | A C を許可   |                      |          |                      |          |
| 2                    | A.3 B を許可 |                      |          |                      |          |
|                      | A.3 C を許可 |                      |          |                      |          |

図 24-3 では、図 24-1 の概念アドレスを実際の IP アドレスにマッピングしています。

図 24-3 ACE の許可と拒否がトラフィックに及ぼす影響（実際のアドレス）



次の表は、図 24-3 の IP アドレスを表 24-3 の概念と結合したものです。これらの表に示されている実際の ACE によって、このネットワーク内で評価を受けたすべての IPsec パケットに適切な IPsec 設定が適用されます。

表 24-4 セキュリティ アプライアンス A の permit 文と deny 文の例

| セキュリティ<br>アプライアンス | 暗号マップ<br>シーケンス番号 | ACE パターン  | 実際の ACE                                                           |
|-------------------|------------------|-----------|-------------------------------------------------------------------|
| A                 | 1                | A.3 B を拒否 | deny 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248     |
|                   |                  | A.3 C を拒否 | deny 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224    |
|                   |                  | A B を許可   | permit 192.168.3.0 255.255.255.192 192.168.12.0 255.255.255.248   |
|                   |                  | A C を許可   | permit 192.168.3.0 255.255.255.192 192.168.201.0 255.255.255.224  |
|                   | 2                | A.3 B を許可 | permit 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248   |
|                   |                  | A.3 C を許可 | permit 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224  |
| B                 | 必要なし             | B A を許可   | permit 192.168.12.0 255.255.255.248 192.168.3.0 255.255.255.192   |
|                   |                  | B C を許可   | permit 192.168.12.0 255.255.255.248 192.168.201.0 255.255.255.224 |
| C                 | 必要なし             | C A を許可   | permit 192.168.201.0 255.255.255.224 192.168.3.0 255.255.255.192  |
|                   |                  | C B を許可   | permit 192.168.201.0 255.255.255.224 192.168.12.0 255.255.255.248 |

このネットワーク例で示されている論法を応用して、カスケード ACL を使用することにより、Cisco セキュリティ アプライアンスで保護されているさまざまなホストまたはサブネットにさまざまなセキュリティ設定を割り当てることができます。



(注)

デフォルトでは、セキュリティ アプライアンスは、トラフィックが入ってきたインターフェイスと同じインターフェイスを宛先とするトラフィックをサポートしません（このタイプのトラフィックには、U ターン、ハブアンドスポーク、ヘアピニングなどの名称があります）。ただし、IPsec で U ターン トラフィックをサポートすることもできます。そのためには、同じネットワークの発信トラフィックと着信トラフィックを許可する ACE を挿入します。たとえば、セキュリティ アプライアンス B で U ターン トラフィックをサポートするには、概念上の「permit B B」ACE を ACL1 に追加します。実際の ACE は次のようになります。

```
permit 192.168.12.0 255.255.255.248 192.168.12.0 255.255.255.248
```

## インターフェイスへの暗号マップの適用

暗号マップセットは、IPsec トラフィックが通過する各インターフェイスに割り当てする必要があります。セキュリティ アプライアンスは、すべてのインターフェイスで IPsec をサポートします。暗号マップセットをインターフェイスに割り当てると、セキュリティ アプライアンスは、すべてのトラフィックを暗号マップセットと照合して評価し、接続中またはネゴシエーション中は指定されたポリシーを使用します。

暗号マップをインターフェイスに割り当てると、SA データベースやセキュリティ ポリシー データベースなどのランタイム データ構造も初期設定されます。暗号マップを修正してインターフェイスに再割り当てすると、ランタイム データ構造は暗号マップ設定と再同期化されます。また、新しいシーケンス番号を使用して新しいピアを追加し、暗号マップを再割り当てしても、既存の接続が切断されることはありません。

## インターフェイス アクセスリストの使用

セキュリティ アプライアンスでは、デフォルトで IPsec パケットがインターフェイス ACL をバイパスするようになっています。インターフェイス アクセスリストを IPsec トラフィックに適用する場合は、**no** 形式の **sysopt connection permit-ipsec** コマンドを使用します。

発信インターフェイスにバインドされている暗号マップ アクセスリストは、VPN トンネルを通過する IPsec パケットの許可と拒否を行います。IPsec は、IPsec トンネルから来たパケットの認証と解読を行い、トンネルに関連付けられている ACL とパケットを照合して評価します。

アクセスリストは、どの IP トラフィックを保護するかを定義します。たとえば、2つのサブネット間または 2 台のホスト間のすべての IP トラフィックを保護するためのアクセスリストを作成できます（これらのアクセスリストは、**access-group** コマンドで使用されるアクセスリストとよく似ています。ただし、**access-group** コマンドでは、アクセスリストがインターフェイスで転送するトラフィックと阻止するトラフィックを決めます）。

暗号マップを割り当てるまで、アクセスリストは IPsec の使用に限定されません。各暗号マップはアクセスリストを参照し、パケットがアクセスリストのいずれか 1 つで **permit** と一致した場合に適用する IPsec プロパティを決めます。

IPsec 暗号マップに割り当てられているアクセスリストには、次の 4 つの主要機能があります。

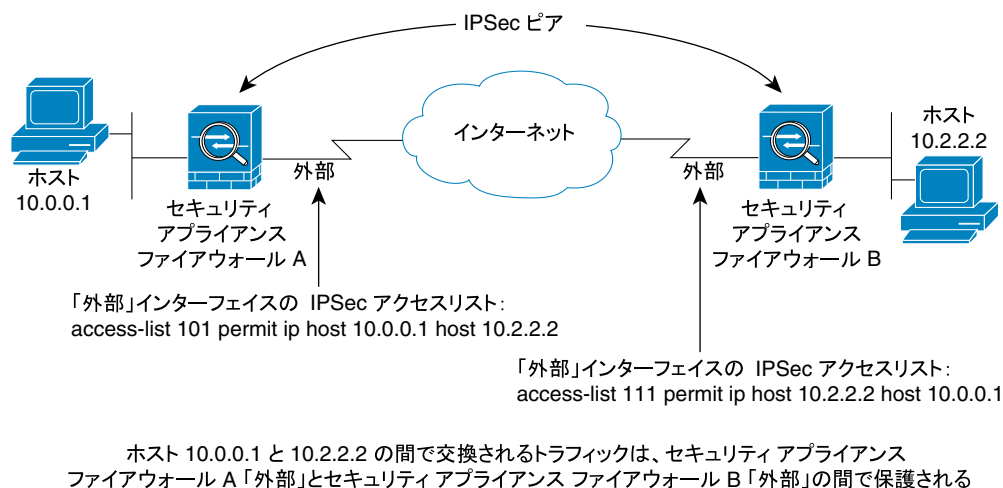
- IPsec で保護する発信トラフィックを選択する（**permit** に一致したものが保護の対象）。
- 確立された SA がない状態で移動するデータに対して ISAKMP ネゴシエーションをトリガーする。
- 着信トラフィックを処理して、IPsec で保護すべきであったトラフィックをフィルタリングして廃棄する。
- ピアからの IKE ネゴシエーションを処理するときに、IPsec SA の要求を受け入れるかどうかを決定する（ネゴシエーションは **ipsec-isakmp crypto map** エントリだけに適用されます）。ピアは **ipsec-isakmp crypto map** コマンド エントリに関連付けられているデータ フローを「許可」し、ネゴシエーション中に要求を受け入れられるようにする必要があります。

トラフィックが着信か発信かに関係なく、セキュリティ アプライアンスは、インターフェイスに割り当てられているアクセスリストとトラフィックを照合して評価します。インターフェイスに IPsec を割り当てるには、次の手順を実行します。

- 
- ステップ 1** IPsec に使用するアクセスリストを作成します。
  - ステップ 2** 作成したアクセスリストを、同じ暗号マップ名を使用して 1 つまたは複数の暗号マップにマッピングします。
  - ステップ 3** データ フローに IPsec を適用するために、トランスフォーム セットを暗号マップにマッピングします。
  - ステップ 4** 共有する暗号マップ名を割り当てて、暗号マップを一括して「暗号マップセット」としてインターフェイスに適用します。
- 

図 24-4 では、データがセキュリティ アプライアンス A 上の外部インターフェイスを出てホスト 10.2.2.2 に向かうときに、ホスト 10.0.0.1 とホスト 10.2.2.2 の間のトラフィックに IPsec 保護が適用されます。

図 24-4 暗号アクセスリストを IPsec に適用する方法



セキュリティ アプライアンス A は、ホスト 10.0.0.1 からホスト 10.2.2.2 へのトラフィックを次のように評価します。

- 送信元 = ホスト 10.00.00.1
- 宛先 = ホスト 10.20.20.2

またセキュリティ アプライアンス A は、ホスト 10.2.2.2 からホスト 10.0.0.1 へのトラフィックを次のように評価します。

- 送信元 = ホスト 10.20.20.2
- 宛先 = ホスト 10.00.00.1

評価中のパケットと最初に一致した permit 文によって、IPsec SA のスコープが決まります。



(注)

アクセスリストの要素を 1 つだけ削除すると、セキュリティ アプライアンスは関連付けられている暗号マップも削除します。

現在 1 つまたは複数の暗号マップが参照しているアクセスリストを修正する場合は、**crypto map interface** コマンドを使用して SA データベースのランタイムを再初期化します。詳細については、**crypto map** コマンドを参照してください。

ローカル ピアで定義するスタティック暗号マップに指定したすべてのアクセスリストに対して、リモート ピアで「ミラー イメージ」暗号アクセスリストを定義することを推奨します。また、暗号マップは共通トランスフォームをサポートし、他のシステムをピアとして参照する必要があります。これにより、両方のピアで IPsec が正しく処理されます。



(注)

すべてのスタティック暗号マップでアクセスリストと IPsec ピアを定義する必要があります。どちらかが定義されていないと、暗号マップは不完全なものになり、セキュリティ アプライアンスは、前の完全な暗号マップにまだ一致していないトラフィックをドロップします。**show conf** コマンドを使用して、すべての暗号マップが完全なものになるようにします。不完全な暗号マップを修正するには、いったん暗号マップを削除し、不足しているエントリを追加してから再適用します。

暗号アクセスリストで送信元アドレスまたは宛先アドレスの指定に **any** キーワードを使用すると問題が発生するため、このキーワードの使用は避けてください。**permit any any** コマンド文を使用すると次の現象が発生するため、使用は極力避けてください。

- すべての発信トラフィックが保護されます。これには、対応する暗号マップで指定されているピアに送信される保護済みのトラフィックも含まれます。
- すべての着信トラフィックに対する保護が必要になります。

このシナリオでは、セキュリティ アプライアンスは IPSec 保護されていないすべての着信パケットを通知なしでドロップします。

保護するパケットを定義したことを必ず確認してください。**permit** 文に **any** キーワードを使用する場合は、その文の前に一連の **deny** 文をおき、保護対象外のトラフィックをすべてフィルタリングして排除します。これを行わないと、その **permit** 文に保護対象外のトラフィックが含まれることになります。

## IPSec SA のライフタイムの変更

セキュリティ アプライアンスが新しい IPSec SA とネゴシエートするときに使用する、グローバル ライフタイム値を変更できます。特定の暗号マップのグローバル ライフタイム値を無効にできます。

IPSec SA では、取得された共有秘密キーが使用されます。共有秘密キーは SA に不可欠な要素で、共有秘密キーにリフレッシュが必要な場合、SA と同時にタイムアウトします。各 SA には、「時間」ライフタイムと「トラフィック量」ライフタイムの2つがあります。それぞれのライフタイムとネゴシエーションが新しい SA 用に開始されると、前の SA は期限満了になります。デフォルトのライフタイムは、28,800 秒 (8 時間) および 4,608,000 キロバイト (10 メガバイト / 秒で 1 時間) です。

グローバル ライフタイムを変更すると、セキュリティ アプライアンスはトンネルをドロップします。変更後に確立された SA のネゴシエーションでは、新しい値が使用されます。

暗号マップに設定されたライフタイム値がなく、セキュリティ アプライアンスから新しい SA を要求された場合、暗号マップは、ピアに送信される新しい SA 要求に、既存の SA で使用されているグローバル ライフタイム値を挿入します。ピアがネゴシエーション要求を受け取ると、このピアが提案するライフタイム値とローカルに設定されているライフタイム値のうち小さい方の値を、新しい SA のライフタイム値として使用します。

既存 SA のライフタイムのしきい値を超える前に、ピアは新しい SA をネゴシエートします。このようにして、既存 SA の有効期限が切れる前に、新しい SA の準備が整います。既存 SA の残りのライフタイムが約 5 ～ 15% になると、ピアは新しい SA をネゴシエートします。

## 基本的な IPSec コンフィギュレーションの作成

次の手順は、基本的な IPSec コンフィギュレーション（スタティック暗号マップ付き）の作成について説明しています。

### ステップ 1 アクセスリストを作成して、保護するトラフィックを定義します。

```
access-list access-list-name {deny | permit} ip source source-netmask destination
destination-netmask
```

次の例を参考にしてください。

```
access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```



この例では、**permit** キーワードによって、指定の条件に一致するトラフィックすべてが暗号で保護されます。

**ステップ 2**    トラフィックを保護する方法を定義するトランスフォームを設定します。複数のトランスフォームセットを設定し、暗号マップでこれらのトランスフォーム セットの 1 つまたは複数を指定します (ステップ 3c)。

```
crypto ipsec transform-set transform-set-name transform1 [ttransform2, transform3]
```

次の例を参考にしてください。

```
crypto ipsec transform-set myset1 esp-des esp-sha-hmac
crypto ipsec transform-set myset2 esp-3des esp-sha-hmac
crypto ipsec transform-set aes_set esp-md5-hmac esp-aes-256
```

この例では、「myset1」、「myset2」、「aes\_set」がトランスフォーム セットの名前です。

**ステップ 3**    暗号マップを作成するには、次の手順を実行します。

- a. アクセスリストを暗号マップに割り当てます。

```
crypto map map-name seq-num match address access-list-name
```

次の例では、「mymap」が暗号マップ セットの名前です。マップ セットのシーケンス番号は 10 です。シーケンス番号は、1 つの暗号マップ セット内の複数のエントリにリンクを付けるために使用します。シーケンス番号が小さいほど、プライオリティが高くなります。

```
crypto map mymap 10 match address 101
```

この例では、アクセスリスト 101 が暗号マップ 「mymap」に割り当てられます。

- b. IPsec で保護されたトラフィックの転送先となるピアを指定します。

```
crypto map map-name seq-num set peer ip-address
```

次の例を参考にしてください。

```
crypto map mymap 10 set peer 192.168.1.100
```

セキュリティ アプライアンスは、ピアに IP アドレス 192.168.1.100 が割り当てられている SA をセットアップします。このコマンドを繰り返して、複数のピアを指定します。

- c. この暗号マップに対して許可するトランスフォーム セットを指定します。複数のトランスフォーム セットをプライオリティ順（最高のプライオリティのものが最初）に列挙します。トランスフォーム セットは最大 6 つ指定できます。

```
crypto map map-name seq-num set transform-set transform-set-name1
[transform-set-name2, ...transform-set-name6]
```

次の例を参考にしてください。

```
crypto map mymap 10 set transform-set myset1 myset2
```

この例では、トラフィックがアクセスリスト 101 に一致すると、SA は、どのトランスフォーム セットがピアのトランスフォーム セットに一致するかによって、「myset1」（第 1 プライオリティ）と「myset2」（第 2 プライオリティ）のいずれかを使用できます。

- d. (オプション) グローバル ライフタイムを上書きする場合は、暗号マップの SA ライフタイムを指定します。

```
crypto map map-name seq-num set security-association lifetime {seconds seconds |
kilobytes kilobytes}
```

次の例を参考にしてください。

```
crypto map mymap 10 set security-association lifetime seconds 2700
```

この例では、暗号マップ「mymap 10」の時間ライフタイムを 2700 秒に短縮します。(45 分)。トラフィック量ライフタイムは変更されません。

- e. (オプション) IPSec がこの暗号マップに対して新しい SA を要求するときに Perfect Forward Secrecy (PFS; 完全転送秘密) を要求するか、または IPSec ピアから受け取る要求に PFS を要求するかを指定します。

```
crypto map map-name seq-num set pfs [group1 | group2 | group5 | group7]
```

次の例を参考にしてください。

```
crypto map mymap 10 set pfs group2
```

この例では、暗号マップ「mymap 10」に対して新しい SA をネゴシエートするときに、PFS を要求しています。セキュリティ アプライアンスは、新しい SA で 1024 ビットの Diffie-Hellman プライム モジュラス グループを使用します。

#### ステップ 4 IPSec トラフィックを評価するために、暗号マップセットをインターフェイスに適用します。

```
crypto map map-name interface interface-name
```

次の例を参考にしてください。

```
crypto map mymap interface outside
```

この例では、セキュリティ アプライアンスは外部インターフェイスを通過するトラフィックを暗号マップ「mymap」と照合して評価し、保護が必要かどうかを判断します。

## ダイナミック暗号マップの使用

ダイナミック暗号マップは、パラメータがまったく設定されていない暗号マップです。ダイナミック暗号マップは、不足しているパラメータが、ピアの要件に合うように後でダイナミックに取得される (IPSec ネゴシエーションの結果として) ポリシー テンプレートの役割を果たします。セキュリティ アプライアンスは、IP アドレスがまだスタティック暗号マップで指定されていない場合に、ダイナミック暗号マップを適用してピアにトンネルをネゴシエートさせます。これは、次のタイプのピアで発生します。

- ダイナミックに割り当てられるパブリック IP アドレスを持つピア  
LAN-to-LAN およびリモートアクセス ピアはいずれも、DHCP を使用してパブリック IP アドレスを取得できます。セキュリティ アプライアンスは、このアドレスをトンネルの開始にだけ使用します。
- ダイナミックに割り当てられるプライベート IP アドレスを持つピア  
通常、リモートアクセス トンネルを要求するピアには、ヘッドエンドによって割り当てられたプライベート IP アドレスがあります。一般に、LAN-to-LAN トンネルには、スタティックマップの設定に使用され、IPsec SA の確立に使用されるプライベート ネットワークの事前設定済みのセットがあります。

スタティック暗号マップを設定する管理者は、割り当てられた方法には関係なく、ダイナミックに割り当てられる IP アドレス (DHCP またはその他の方法による) や、他のクライアントのプライベート IP アドレスを知らない場合もあります。通常、VPN クライアントには、スタティック IP アドレスがなく、IPSec ネゴシエーションを発生させるためのダイナミック暗号マップが必要です。たとえば、ヘッドエンドは IKE ネゴシエーション中に IP アドレスを Cisco VPN Client に割り当てますが、クライアントはこれを使用して IPSec SA をネゴシエートします。



(注)

ダイナミック暗号マップには **transform-set** パラメータだけが必要です。

ダイナミック暗号マップは、IPsec コンフィギュレーションを容易にするので、ピアが必ずしも事前設定されていないネットワークで使用するのに適しています。ダイナミック暗号マップは、ダイナミックに割り当てられた IP アドレスを取得する Cisco VPN クライアント（たとえば、モバイルユーザ）およびルータに使用します。



ヒント

ダイナミック暗号マップの **permit** エントリで **any** キーワードを使用する場合は、注意が必要です。そのような **permit** エントリの対象となるトラフィックに、マルチキャスト トラフィックまたはブロードキャスト トラフィックが含まれる可能性がある場合は、適切なアドレス範囲に対する **deny** エントリをアクセスリストに挿入する必要があります。ネットワークとサブネットブロードキャスト トラフィックに対して、また IPsec で保護しないその他のトラフィックに対しては、必ず **deny** エントリを挿入してください。

ダイナミック暗号マップは、接続を開始するリモートピアと SA をネゴシエートするためだけに機能します。セキュリティ アプライアンスは、ダイナミック暗号マップを使用して、リモートピアへの接続を開始することはできません。ダイナミック暗号マップ エントリでは、発信トラフィックがアクセスリストの **permit** エントリと一致しても、対応する SA がまだ存在しない場合、セキュリティ アプライアンスはそのトラフィックをドロップします。

暗号マップセットにはダイナミック暗号マップを含めることができます。ダイナミック暗号マップには、暗号マップセット内の暗号マップの中で最も低いプライオリティを設定し（つまり最も大きいシーケンス番号を付ける）、セキュリティ アプライアンスが他の暗号マップを最初に評価するようにする必要があります。他の（スタティック）マップ エントリが一致しなかった場合にだけ、ダイナミック暗号マップセットが評価されます。

スタティック暗号マップセットと同様に、ダイナミック暗号マップセットも同じ名前を持つダイナミック暗号マップで構成されます。ダイナミック暗号マップセット内のダイナミック暗号マップは、シーケンス番号によって区別されます。ダイナミック暗号マップを設定する場合は、IPsec ピアのデータ フローを暗号アクセスリストで識別するために、ACL の許可を挿入します。この処理を行わないと、セキュリティ アプライアンスはピアから提案されたデータ フロー ID をすべて受け入れます。



注意

ダイナミック暗号マップセットが設定されたセキュリティ アプライアンスインターフェイスにトンネリングされるトラフィックには、スタティック（デフォルトの）ルートを割り当てないでください。トンネリングされるトラフィックを識別するには、ダイナミック暗号マップに ACL を追加します。リモートアクセス トンネルに関連付けられている ACL を設定する場合は、適切なアドレス プールを指定するように注意する必要があります。トンネルの確立を待ってから、逆ルート注入を使用してルートをインストールします。

ダイナミック暗号マップ エントリを使用するための手順は、スタティック暗号マップを作成する代わりにダイナミック暗号マップ エントリを作成するという点を除いて、「[基本的な IPsec コンフィギュレーションの作成](#)」で説明した基本的なコンフィギュレーションと同じです。1 つの暗号マップセットの中でスタティック マップ エントリとダイナミック マップ エントリを組み合わせることもできます。

暗号ダイナミック マップ エントリを作成するには、次の手順を実行します。

### ステップ 1 (オプション) アクセスリストをダイナミック暗号マップに割り当てます。

```
crypto dynamic-map dynamic-map-name dynamic-seq-num match address access-list-name
```

これによって、保護するトラフィックと保護しないトラフィックが決まります。

次の例を参考にしてください。

```
crypto dynamic-map dyn1 10 match address 101
```

この例では、アクセスリスト 101 がダイナミック暗号マップ「dyn1」に割り当てられます。この暗号マップのシーケンス番号は 10 です。

### ステップ 2 このダイナミック暗号マップに対して許可するトランスフォーム セットを指定します。複数のトランスフォーム セットをプライオリティ順（最高のプライオリティのものが最初）に列挙します。

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set transform-set  
transform-set-name1, [transform-set-name2, ...transform-set-name9]
```

次の例を参考にしてください。

```
crypto dynamic-map dyn 10 set transform-set myset1 myset2
```

この例では、トラフィックがアクセスリスト 101 に一致すると、SA は、どのトランスフォーム セットがピアのトランスフォーム セットに一致するかによって、「myset1」（第 1 プライオリティ）と「myset2」（第 2 プライオリティ）のいずれかを使用できます。

### ステップ 3 (オプション) グローバル ライフタイムを無効にする場合は、ダイナミック暗号マップの SA ライフタイムを指定します。

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set security-association lifetime  
{seconds seconds | kilobytes kilobytes}
```

次の例を参考にしてください。

```
crypto dynamic-map dyn1 10 set security-association lifetime seconds 2700
```

この例では、ダイナミック暗号マップ「dyn1 10」の時間ライフタイムを 2700 秒に短縮します。(45 分)。トラフィック量ライフタイムは変更されません。

### ステップ 4 (オプション) IPSec がこのダイナミック暗号マップに対して新しい SA を要求するときに PFS を要求するか、または IPSec ピアから受け取る要求に PFS を要求するかを指定します。

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set pfs [group1 | group2 | group5  
| group7]
```

次の例を参考にしてください。

```
crypto dynamic-map dyn1 10 set pfs group5
```

**ステップ 5** ダイナミック暗号マップセットをスタティック暗号マップセットに追加します。

ダイナミック マップを参照する暗号マップは、必ず暗号マップ セットの中でプライオリティ エントリを最低（シーケンス番号が最大）に設定してください。

```
crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name
```

次の例を参考にしてください。

```
crypto map mymap 200 ipsec-isakmp dynamic dyn1
```

## サイトツーサイト冗長性の定義

暗号マップを使用して、複数のピアに冗長性を定義できます。このコンフィギュレーションはサイトツーサイト VPN に便利です。

あるピアが失敗すると、セキュリティ アプライアンスは、暗号マップに関連付けられている次のピアへのトンネルを確立します。ネゴシエーションが成功したピアにセキュリティ アプライアンスからデータが送信されると、そのピアは「アクティブな」ピアになります。「アクティブな」ピアとは、後続のネゴシエーションに対して、ネゴシエーションが失敗するまでセキュリティ アプライアンスが常に最初に試みるピアのことです。ネゴシエーションが失敗した時点で、セキュリティ アプライアンスは次のピアに移ります。暗号マップに関連付けられているすべてのピアが失敗すると、セキュリティ アプライアンスのサイクルは最初のピアに戻ります。

## IPsec コンフィギュレーションの表示

表 24-5 に、IPsec コンフィギュレーションに関する情報の表示に使用できるコマンドのリストを示します。

**表 24-5 IPsec コンフィギュレーション情報を表示するためのコマンド**

| コマンド                                   | 目的                                                       |
|----------------------------------------|----------------------------------------------------------|
| show running-configuration crypto      | IPsec、暗号マップ、ダイナミック暗号マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。 |
| show running-config crypto ipsec       | IPsec コンフィギュレーション全体を表示します。                               |
| show running-config crypto isakmp      | ISAKMP コンフィギュレーション全体を表示します。                              |
| show running-config crypto map         | 暗号マップ コンフィギュレーション全体を表示します。                               |
| show running-config crypto dynamic-map | ダイナミック暗号マップ コンフィギュレーションを表示します。                           |
| show all crypto map                    | すべてのコンフィギュレーション パラメータ（デフォルト値を持つパラメータも含む）を表示します。          |

## セキュリティ アソシエーションのクリア

一部のコンフィギュレーション変更は、後続の SA をネゴシエートするときまで有効になりません。新しい設定をただちに有効にするには、既存の SA をクリアして、変更後のコンフィギュレーションで SA を再確立します。セキュリティ アプライアンスがアクティブに IPSec トラフィックを処理している場合は、SA データベースのうち、コンフィギュレーション変更の影響を受ける部分だけをクリアします。SA データベースを完全にクリアするのは、大規模な変更の場合や、セキュリティ アプライアンスが処理している IPSec トラフィック量が少ない場合に限定するようにしてください。

表 24-6 に、IPSec SA のクリアと再初期設定に使用できるコマンドのリストを示します。

**表 24-6 IPSec SA のクリアおよび再初期設定用のコマンド**

| コマンド                                              | 目的                                                       |
|---------------------------------------------------|----------------------------------------------------------|
| <code>clear configure crypto</code>               | IPSec、暗号マップ、ダイナミック暗号マップ、ISAKMP など、暗号コンフィギュレーション全体を削除します。 |
| <code>clear configure crypto ca trustpoint</code> | すべてのトラストポイントを削除します。                                      |
| <code>clear configure crypto dynamic-map</code>   | すべてのダイナミック暗号マップを削除します。特定のダイナミック暗号マップを削除できるキーワードもあります。    |
| <code>clear configure crypto map</code>           | すべての暗号マップを削除します。特定の暗号マップを削除できるキーワードもあります。                |
| <code>clear configure isakmp</code>               | ISAKMP コンフィギュレーション全体を削除します。                              |
| <code>clear configure isakmp policy</code>        | すべての ISAKMP ポリシーまたは特定のポリシーを削除します。                        |
| <code>clear isakmp sa</code>                      | ISAKMP SA データベース全体を削除します。                                |

## 暗号マップ コンフィギュレーションのクリア

`clear configure crypto` コマンドには、IPSec、暗号マップ、ダイナミック暗号マップ、CA トラストポイント、すべての証明書、証明書マップ コンフィギュレーション、ISAKMP など、暗号コンフィギュレーションの要素を削除できる引数が含まれます。

引数を指定しないで `clear configure crypto` コマンドを入力すると、暗号コンフィギュレーション全体（すべての認証も含む）が削除されることに注意してください。

詳細については、『Cisco Security Appliance Command Reference』の `clear configure crypto` コマンドを参照してください。



# IPSec VPN の一般パラメータの設定

バーチャル プライベート ネットワークのセキュリティ アプライアンスの実装には、カテゴリの枠を越えた便利な機能があります。この章では、これらの機能のいくつかについて説明します。ここでは、次の項目について説明します。

- [単一のルーテッド モードでの VPN の設定 \(P.25-1\)](#)
- [ACL をバイパスするための IPSec の設定 \(P.25-2\)](#)
- [インターフェイス内トラフィックの許可 \(P.25-3\)](#)
- [アクティブな IPSec VPN セッションの最大数の設定 \(P.25-4\)](#)
- [許可されるクライアント リビジョン レベル確認のためのクライアント アップデートの使用 \(P.25-5\)](#)
- [ロードバランシングの概要 \(P.25-8\)](#)
- [ロードバランシングの設定 \(P.25-12\)](#)
- [VPN セッション制限の設定 \(P.25-15\)](#)

## 単一のルーテッド モードでの VPN の設定

VPN は、単一のルーテッド モードでのみ動作します。セキュリティ コンテキストが含まれるコンフィギュレーション (マルチモード ファイアウォールとも呼ばれる)、または Active/Active ステートフル フェールオーバーが含まれるコンフィギュレーションでは、VPN 機能は利用できません。

例外として、管理上の目的で、透過モードでのセキュリティ アプライアンスへの接続 (通過はしない) を 1 つ設定して使用することができます。

## ACL をバイパスするための IPsec の設定

IPsec トンネルから送信されるすべてのパケットに対して、ACL で発信元インターフェイスと宛先インターフェイスをチェックせずに許可するには、グローバル コンフィギュレーション モードで **sysopt connection permit-ipsec** コマンドを入力します。

IPsec トラフィックのインターフェイス ACL をバイパスする必要があるのは、セキュリティ アプライアンスの背後で別の VPN コンセントレータを使用し、なおかつセキュリティ アプライアンスのパフォーマンスを最大限にする場合などです。通常、IPsec パケットを許可する ACL を **access-list** コマンドを使用して作成し、これを発信元インターフェイスに適用します。ACL を使用すると、セキュリティ アプライアンスを通過できるトラフィックを正確に指定できるため、セキュリティが向上します。

シンタックスは、**sysopt connection permit-ipsec** です。このコマンドには、キーワードも引数もありません。

次の例では、ACL をチェックせずにセキュリティ アプライアンスを通過する IPsec トラフィックをイネーブルにします。

```
hostname(config)# sysopt connection permit-ipsec
```



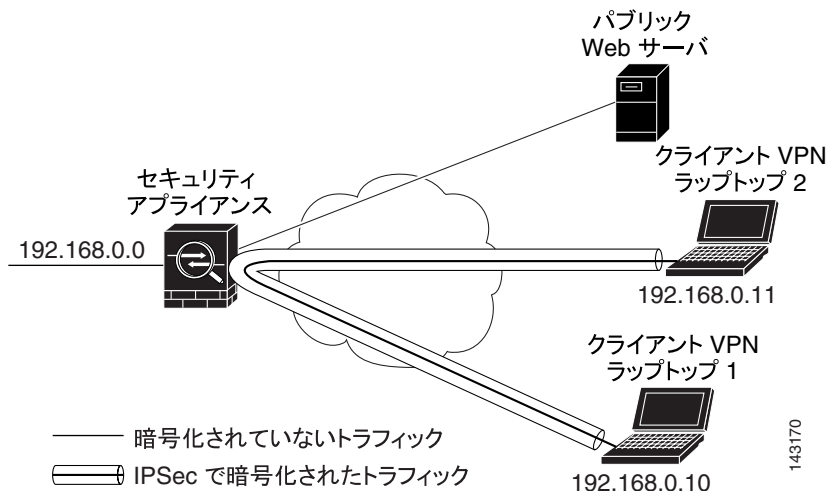
## インターフェイス内トラフィックの許可

セキュリティ アプライアンスには、IPsec で保護されたトラフィックに対して、同じインターフェイスの出入りを許可することにより、VPN クライアントが別の VPN ユーザに IPsec で保護されたトラフィックを送信できる機能があります。「ヘアピンング」とも呼ばれるこの機能は、VPN ハブ（セキュリティ アプライアンス）を介して接続している VPN スポーク（クライアント）と見なすことができます。

別のアプリケーションでは、この機能により、着信 VPN トラフィックを同じインターフェイスを介して暗号化されていないトラフィックとしてリダイレクトできます。この機能は、たとえば、スプリット トネリングがない状態で、VPN へのアクセスと Web のブラウズの両方を行う必要がある VPN クライアントに役立ちます。

図 25-1 では、VPN クライアント 1 が VPN クライアント 2 に対してセキュアな IPsec トラフィックを送信し、パブリック Web サーバに対しては暗号化されていないトラフィックを送信していることを示しています。

図 25-1 ヘアピンングにインターフェイス内機能を使用する VPN クライアント



この機能を設定するには、グローバル コンフィギュレーション モードで **intra-interface** 引数を指定して **same-security-traffic** コマンドを実行します。

コマンドのシンタックスは、**same-security-traffic permit {inter-interface | intra-interface}** です。

次の例では、インターフェイス内トラフィックをイネーブルにする方法を示しています。

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



(注)

**same-security-traffic** コマンドに **inter-interface** 引数を指定すると、セキュリティ レベルが同一のインターフェイス間の通信を許可します。この機能は、IPsec 接続に固有のものではありません。詳細については、このマニュアルの「[インターフェイス パラメータの設定](#)」の章を参照してください。

ヘアピンングを使用するには、次の項で説明するように、適切な NAT 規則をセキュリティ アプライアンスに適用する必要があります。

## インターフェイス内トラフィックにおける NAT の注意事項

セキュリティ アプライアンスがインターフェイスを介して暗号化されていないトラフィックを送信するには、そのインターフェイスに対する NAT をイネーブルにし、プライベート IP アドレスをパブリックにルーティング可能なアドレスに変換する必要があります（ただし、ローカル IP アドレス プールですでにパブリック IP アドレスを使用している場合は除きます）。次の例では、クライアント IP プールから発信されたトラフィックに、インターフェイス PAT 規則を適用しています。

```
hostname(config)# ip local pool clientpool 192.168.0.10-192.168.0.100
hostname(config)# global (outside) 1 interface
hostname(config)# nat (outside) 1 192.168.0.0 255.255.255.0
```

ただし、セキュリティ アプライアンスがこの同じインターフェイスから暗号化された VPN トラフィックを送信する場合、NAT は任意です。VPN 間へアピニングは、NAT を使用してもしなくても機能します。すべての発信トラフィックに NAT を適用するには、上記のコマンドを実装するだけです。VPN 間トラフィックを NAT から免除するには、次のように、VPN 間トラフィックの NAT 免除を実装するコマンドを（上記のコマンドに）追加します。

```
hostname(config)# access-list nonat permit ip 192.168.0.0 255.255.255.0 192.168.0.0
255.255.255.0
hostname(config)# nat (outside) 0 access-list nonat
```

NAT 規則の詳細については、このマニュアルの「[NAT の適用](#)」の章を参照してください。

## アクティブな IPsec VPN セッションの最大数の設定

VPN セッションの数をセキュリティ アプライアンスが許可する数よりも小さい値に制限するには、グローバル コンフィギュレーション モードで `vpn-sessiondb max-session-limit` コマンドを入力します。

- このコマンドは、WebVPN を含むあらゆるタイプの VPN セッションに適用されます。
- このセッション数の制限は、VPN ロードバランシング用に算出されたロード率に影響します。

シンタックスは、`vpn-sessiondb max-session-limit {session-limit}` です。

次の例では、VPN セッションの最大数を 450 に設定する方法を示しています。

```
hostname (config)# vpn-sessiondb max-session-limit 450
hostname (config)#
```

## 許可されるクライアント リビジョン レベル確認のためのクライアント アップデートの使用

クライアント アップデート機能を使用すると、中央にいる管理者は、VPN クライアント ソフトウェアをアップデートする時期と VPN 3002 ハードウェア クライアント イメージを、VPN クライアント ユーザに自動的に通知できます。

リモート ユーザは、旧式の VPN ソフトウェアまたはハードウェア クライアント バージョンを使用している可能性もあります。**client-update** コマンドを使用すると、いつでもクライアント リビジョンのアップデートをイネーブルにして、アップデートが適用されるクライアントのタイプおよびリビジョン番号を指定し、アップデートを取得する URL または IP アドレスを提供できます。また Windows クライアントの場合は、オプションとして VPN クライアント バージョンをアップデートする必要があることをユーザに通知できます。Windows クライアントの場合は、アップデートを実行するメカニズムをユーザに提供できます。VPN 3002 ハードウェア クライアントのユーザの場合、アップデートは通知せずに自動的に行われます。このコマンドは、IPsec リモートアクセス トンネルグループのタイプだけに適用されます。

クライアント アップデートを実行するには、一般コンフィギュレーション モードまたはトンネルグループ ipsec アトリビュート コンフィギュレーション モードで **client-update** コマンドを入力します。クライアントがリビジョン番号リストにあるソフトウェア バージョンをすでに実行している場合、ソフトウェアをアップデートする必要はありません。クライアントがリストにあるソフトウェア バージョンを実行していない場合、アップデートする必要があります。次の手順は、クライアント アップデートの実行方法です。

- 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、コマンドを入力してクライアント アップデートをイネーブルにします。

```
hostname(config)# client-update enable
hostname(config)#
```

- ステップ 2** グローバル コンフィギュレーション モードで、特定のタイプのすべてのクライアントに適用するクライアント アップデートのパラメータを指定します。つまり、クライアントのタイプ、アップデートされたイメージを取得する URL または IP アドレス、およびそのクライアントの許可されるリビジョン番号を指定します。リビジョン番号は、カンマで区切って最大 4 つまで指定できます。

ユーザのクライアントのリビジョン番号が、指定されているリビジョン番号のいずれかと一致している場合、クライアントをアップデートする必要はありません。このコマンドは、セキュリティ アプライアンス全体にわたって指定されているタイプのすべてのクライアントの **client-update** 値を指定します。

これを行うコマンドのシンタックスは次のとおりです。

```
hostname(config)# client-update type type url url-string rev-nums rev-numbers
hostname(config)#
```

使用可能なクライアント タイプは、**win9X**（Windows 95、Windows 98、および Windows ME プラットフォーム）、**winnt**（Windows NT 4.0、Windows 2000、および Windows XP プラットフォーム）、**windows**（すべての Windows ベースのプラットフォーム）、および **vpn3002**（VPN 3002 ハードウェア クライアント）です。

クライアントがリビジョン番号リストにあるソフトウェア バージョンをすでに実行している場合、ソフトウェアをアップデートする必要はありません。クライアントがリストにあるソフトウェア バージョンを実行していない場合、アップデートする必要があります。これらのクライアント アップデート エントリから 3 つまで指定することができます。キーワード **windows** は、許可されるすべての Windows プラットフォームを網羅します。**windows** を指定する場合は、個々の Windows クラ イアント タイプは指定しません。



(注)

すべての Windows クラ イアントでは、URL のプレフィックスとしてプロトコル `http://` または `https://` を使用する必要があります。VPN 3002 ハードウェア クラ イアントの場合は、代わりにプロトコル `tftp://` を指定する必要があります。

次の例では、リモートアクセス トンネルグループのクライアント アップデート パラメータを設定しています。リビジョン番号は 4.6.1、アップデートを取得するための URL は `https://support/updates` を指定しています。

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums
4.6.1
hostname(config)#
```

あるいは、特定のタイプのすべてのクライアントではなく、個々のトンネルグループ専用クライアント アップデートを設定できます（手順 3 を参照）。

VPN 3002 クラ イアントは、ユーザの介入なしにアップデートされるため、ユーザは通知メッセージを受け取りません。次の例は、VPN 3002 ハードウェア クラ イアントだけに適用されます。トンネルグループの ipsec アトリビュート コンフィギュレーション モードに入ると、IPsec リモートアクセス トンネルグループ「salesgrp」のクライアント アップデート パラメータが設定されます。ここでは、リビジョン番号 4.7 を指定し、アップデートされたソフトウェアを IP アドレス 192.168.1.1 のサイトから取得するために TFTP プロトコルを使用します。

```
hostname(config)# tunnel-group salesgrp type ipsec-ra
hostname(config)# tunnel-group salesgrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type vpn3002 url tftp:192.168.1.1
rev-nums 4.7
hostname(config-tunnel-ipsec)#
```



(注)

たとえば `https://support/updates/vpnclient.exe` のように、URL の最後にアプリケーション名を含めると、ブラウザは自動的にアプリケーションを起動します。

**ステップ 3** 特定の ipsec-ra トンネルグループに対して client-update パラメータのセットを定義するには、次の手順を実行します。トンネルグループの ipsec アトリビュート モードで、トンネルグループ名とそのタイプ、アップデートされたイメージを取得する URL または IP アドレス、およびリビジョン番号を指定します。ユーザのクライアントのリビジョン番号が、指定されているリビジョン番号のいずれかと一致している場合は、Windows クラ イアントなどのクライアントをアップデートする必要はありません。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type windows url https://support/updates/
rev-nums 4.6.1
hostname(config-tunnel-ipsec)#
```

**ステップ 4** オプションとして、クライアントのアップデートが必要な旧式の Windows クライアントを持つアクティブなユーザに通知を送信できます。これらのユーザにはポップアップ ウィンドウが表示され、ブラウザを起動して URL に指定したサイトからアップデートされたソフトウェアをダウンロードする機会を提供します。このメッセージのうち設定できる部分は URL だけです（手順 2 または 3 を参照してください）。アクティブでないユーザは、次にログインしたときに通知メッセージを受け取ります。この通知は、すべてのトンネルグループのすべてのアクティブなクライアントに送信するか、または特定のトンネルグループのクライアントに送信することができます。たとえば、すべてのトンネルグループのすべてのアクティブなクライアントに通知するには、特権 EXEC モードで次のコマンドを入力します。

```
hostname# client-update all
hostname#
```

ユーザのクライアントのリビジョン番号が、指定されているリビジョン番号のいずれかと一致している場合、クライアントをアップデートする必要はなく、通知メッセージはユーザに送信されません。VPN 3002 クライアントは、ユーザの介入なしにアップデートされるため、ユーザは通知メッセージを受け取りません。



(注)

client-update タイプを **windows** として指定（すべての Windows ベースのプラットフォームを指定）した後、同じエントリに **win9x** または **winnt** の client-update タイプを入力する場合、最初にこのコマンドの **no** 形式を使用して windows クライアント タイプを削除してから、新しく client-update コマンドを使用して新しいクライアント タイプを指定する必要があります。

## ロードバランシングの概要

リモート セッションを処理するために同じネットワーク上に接続されている 2 つ以上のセキュリティ アプライアンスまたは VPN コンセントレータを使用しているリモートアクセス コンフィギュレーションがある場合、これらのデバイスは、セッション ロードを共有するように設定できます。この機能は、ロードバランシングと呼ばれます。ロードバランシングを実装するには、同じプライベート LAN-to-LAN ネットワーク、プライベート サブネット、およびパブリック サブネット上の 2 つ以上のデバイスを論理的に仮想クラスタとしてグループ化します。

仮想クラスタ内のすべてのデバイスはセッション ロードを伝送します。ロードバランシングは、クラスタ内で最もロードの低いデバイスにセッショントラフィックを転送して、ロードをすべてのデバイス間で分散します。これにより、システム リソースが効率的に使用され、パフォーマンスの向上と高い可用性がもたらされます。

仮想クラスタ内の 1 つのデバイスである仮想クラスタ マスターは、着信トラフィックをセカンダリ デバイスと呼ばれる他のデバイスに転送します。仮想クラスタ マスターは、クラスタ内のすべてのデバイスを監視し、各デバイスのビジー状態を把握して、適宜セッション ロードを分散します。仮想クラスタ マスターの役割は、1 つの物理デバイスに結び付けられることなく、デバイス間でシフトできます。たとえば、現在の仮想クラスタ マスターが故障した場合、クラスタ内のセカンダリ デバイスがその役割を引き継いで、ただちに新しい仮想クラスタ マスターになります。

**(注)**

`show` コマンドの出力は、クラスタ内のセカンダリ デバイスをバックアップ デバイスとして表示する場合があります。

仮想クラスタは、外部のクライアントには単一の仮想クラスタ IP アドレスとして表示されます。この IP アドレスは、特定の物理デバイスに結び付けられていません。これは、現在の仮想クラスタ マスターに属しているため、仮想です。接続を確立しようと試みる VPN クライアントは、最初にこの仮想クラスタ IP アドレスに接続します。仮想クラスタ マスターは、クラスタ内でロードが最小の使用可能なホストのパブリック IP アドレスをクライアントに送り返します。クライアントは、第 2 のトランザクション（ユーザには意識されない）で、そのホストに直接接続します。このようにして、仮想クラスタ マスターは、リソース全体にわたって均一かつ効率的にトラフィックを転送します。

**(注)**

Cisco VPN クライアントまたは Cisco 3002 ハードウェア クライアント以外のすべてのクライアントは、通常どおりにセキュリティ アプライアンスに直接接続する必要があります。これらのクライアントは、仮想クラスタ IP アドレスを使用しません。

クラスタ内のマシンに障害が発生すると、終了したセッションはただちに仮想クラスタ IP アドレスに再接続できます。その後、仮想クラスタ マスターは、これらの接続をクラスタ内の別のアクティブ デバイスに転送します。仮想クラスタ マスター自体に障害が発生した場合、クラスタ内のセカンダリ デバイスがただちに新しい仮想セッション マスターの役割を自動的に引き継ぎます。たとえクラスタ内の複数のデバイスに障害が発生しても、ユーザは、クラスタ内のいずれか 1 つのデバイスが実行中で使用可能である限り、クラスタに引き続き接続できます。

## ロードバランシングの実装

ロードバランシングをイネーブルにするには、次の手順を実行します。

- 共通仮想クラスタ IP アドレス、UDP ポート（必要に応じて）、およびクラスタの IPSec 共有秘密情報を確立することにより、ロードバランシングクラスタを設定する。これらの値は、クラスタ内のすべてのデバイスで同一に設定する必要があります。
- デバイスでロードバランシングをイネーブル化してデバイス固有のプロパティを定義することにより、参加デバイスを設定する。これらの値は、デバイスごとに異なります。



(注)

VPN ロードバランシングには、アクティブな 3DES/AES ライセンスが必要です。セキュリティ アプライアンスは、ロードバランシングをイネーブル化する前に、この暗号ライセンスの存在をチェックします。アクティブな 3DES または AES ライセンスを検出できなかった場合、セキュリティ アプライアンスは、ロードバランシングのイネーブル化を回避し、さらにライセンスがこの使用を許可していない限り、ロードバランシング システムによる 3DES の内部コンフィギュレーションも回避します。

## 前提条件

ロードバランシングは、デフォルトではディセーブルになっています。ロードバランシングは明示的にイネーブルにする必要があります。

最初にパブリック（外部）インターフェイスおよびプライベート（内部）インターフェイスを設定し、さらに仮想クラスタ IP アドレスが参照するインターフェイスを事前に設定しておく必要があります。これらのインターフェイスに異なる名前を設定するには、**interface** および **nameif** コマンドを使用します。この項ではこれ以降の参照に外部および内部の名前を使用します。

クラスタに参加するすべてのデバイスは、同じクラスタ固有の値である IP アドレス、暗号設定、暗号キー、およびポートを共有する必要があります。

## 適格なプラットフォーム

ロードバランシングクラスタには、ASA Release 7.1(1) ソフトウェアまたは ASA Release 7.0(x) ソフトウェアを実行しているセキュリティ アプライアンス モデル ASA 5520 以上を含めることができます。VPN 3000 シリーズ コンセントレータをクラスタに含めることもできます。混在のコンフィギュレーションは可能ですが、一般にクラスタが同種であれば管理は容易になります。

## 適格なクライアント

ロードバランシングは、次のクライアントで開始されるリモートセッションだけに有効です。

- Cisco VPN クライアント（Release 3.0 以上）
- Cisco VPN 3002 ハードウェア クライアント（Release 3.5 以上）
- Easy VPN クライアントとして動作している場合、Cisco PIX 501/506E

ロードバランシングは、IPSec クライアントおよび WebVPN セッションの両方で機能します。LAN-to-LAN 接続を含む他のすべてのクライアントは、ロードバランシングがイネーブルになっているセキュリティ アプライアンスに接続できますが、ロードバランシングに参加することはできません。

## VPN ロードバランシング クラスタ コンフィギュレーション

ロードバランシング クラスタは、次の制限に従って、すべての ASA Release 7.0(x) セキュリティ アプライアンス、すべての ASA Release 7.1(1) セキュリティ アプライアンス、すべての VPN 3000 コンセントレータ、またはこれらの混在で構成することができます。

- すべての ASA 7.0(x) セキュリティ アプライアンス、すべての ASA 7.1(1) セキュリティ アプライアンス、またはすべての VPN 3000 コンセントレータで構成されるロードバランシング クラスタは、IPsec および WebVPN セッションの混在に対してロードバランシングを実行できます。
- ASA 7.0(x) セキュリティ アプライアンスおよび VPN 3000 コンセントレータで構成されるロードバランシング クラスタは、IPsec および WebVPN セッションの混在に対してロードバランシングを実行できます。
- ASA 7.1(1) セキュリティ アプライアンスおよび ASA 7.0(x) または VPN 3000 コンセントレータのいずれか、またはその両方を含むロードバランシング クラスタは、IPsec セッションだけをサポートできます。しかし、このようなコンフィギュレーションでは、ASA 7.1(1) セキュリティ アプライアンスは IPsec キャパシティに完全に到達しない可能性もあります。[P.11 の「シナリオ 1：WebVPN 接続のない混在クラスタ」](#)に、この状況を示します。

Release 7.1(1) を使用すると、IPsec および WebVPN セッションは、クラスタ内の各デバイスが伝送するロードを決定するときに均等にカウントまたは重み付けします。このことは、これらのプラットフォームが共に一部のハードウェア プラットフォーム上で IPsec セッション ロードとは異なる方法で WebVPN セッションロードを計算する重み付けアルゴリズムを使用するという点において、ASA Release 7.0(x) ソフトウェアおよび VPN 3000 コンセントレータのロードバランシング計算からの脱却を意味しています。

クラスタの仮想マスターは、クラスタのメンバーにセッション要求を割り当てます。ASA Release 7.1(1) セキュリティ アプライアンスはすべてのセッション、WebVPN または IPsec を同等と見なし、これらを適宜割り当てます。ASA Release 7.0(x) セキュリティ アプライアンスまたは VPN 3000 コンセントレータは、セッション ロードを割り当てる際に重み付け計算を実行します。



(注)

IPsec および WebVPN セッションの数は、コンフィギュレーションとライセンスで許可されている最大数まで設定できます。これら制限の設定方法については、[P.25-15 の「VPN セッション制限の設定」](#)を参照してください。

## 一部の一般的な混在クラスタのシナリオ

混在のコンフィギュレーション、つまりロードバランシング クラスタに ASA ソフトウェア リリースの混在を実行しているデバイス、または ASA Release 7.1(1) および VPN 3000 コンセントレータを実行しているセキュリティ アプライアンスが少なくとも 1 つ含まれる場合、最初のクラスタ マスターに障害が発生して別のデバイスがマスターを引き継ぐときに、重み付けアルゴリズムの相異が問題になります。

次のシナリオは、ASA Release 7.1(1) および ASA Release 7.0(x) ソフトウェアを実行しているセキュリティ アプライアンスと VPN 3000 シリーズ コンセントレータの混在で構成されるクラスタでの VPN ロードバランシングの使用を示しています。



## シナリオ 1：WebVPN 接続のない混在クラスタ

このシナリオでは、クラスタはセキュリティ アプライアンスおよび VPN 3000 コンセントレータの混在で構成されます。セキュリティ アプライアンス クラスタ ピアには、ASA Release 7.0(x) を実行しているものも、Release 7.1(1) を実行しているものもあります。7.1(1) 以前の VPN 3000 ピアには、SSL VPN 接続がなく、7.1(1) クラスタ ピアは、2 つの WebVPN セッションを許可する基本 SSL VPN ライセンスだけを備えています。この場合、すべての接続は IPsec であり、ロードバランシングは良好に機能します。

2 つの WebVPN ライセンスは、ユーザの最大 IPsec セッション制限の利用にはほんのわずかな影響しか及ぼしません。またそれは VPN 3000 コンセントレータがクラスタ マスターである場合に限られます。一般に、混在クラスタ内のセキュリティ アプライアンスの WebVPN ライセンスの数が少なくなると、それに応じて IPsec セッションしかないシナリオにおいてその IPsec セッションの制限に到達できる ASA 7.1(1) デバイスへの影響も小さくなります。

## シナリオ 2：WebVPN 接続を処理する混在クラスタ

たとえば、ASA Release 7.1(1) ソフトウェアを実行しているセキュリティ アプライアンスが最初のクラスタ マスターであり、そのデバイスに障害が発生したとします。クラスタ内の別のデバイスがマスターを自動的に引き継ぎ、クラスタ内のプロセッサ ロードを決定するためにそのデバイスのロードバランシング アルゴリズムを適用します。ASA Release 7.1(1) ソフトウェアを実行しているクラスタ マスターは、そのソフトウェアが提供する方法以外ではセッション ロードを重み付けすることができません。したがって、クラスタ マスターは、IPsec および WebVPN セッション ロードの組み合わせを、以前のバージョンを実行する ASA デバイスにも VPN 3000 コンセントレータにも適切に割り当てることができません。これとは逆に、クラスタ マスターとして動作している VPN 3000 コンセントレータは、ASA Release 7.1(1) セキュリティ アプライアンスにロードを適切に割り当てられません。次のシナリオは、このジレンマを示しています。

このシナリオは、クラスタがセキュリティ アプライアンスおよび VPN 3000 コンセントレータの混在で構成されているという点において、前述のシナリオと類似しています。セキュリティ アプライアンス クラスタ ピアには、ASA Release 7.0(x) を実行しているものも、Release 7.1(1) を実行しているものもあります。しかし、この場合、クラスタは SSL VPN 接続だけでなく IPsec 接続も処理しています。

ASA Release 7.1(1) 以前のソフトウェアを実行しているデバイスがクラスタ マスターである場合、マスターは実質的に Release 7.1(1) 以前のプロトコルとロジックを適用します。つまり、セッションは、セッション制限を超えているロードバランシング ピアに転送される場合もあります。その場合、ユーザはアクセスを拒否されます。

クラスタ マスターが ASA Release 7.0(x) ソフトウェアを実行しているデバイスである場合、以前のセッション重み付けアルゴリズムはクラスタ内の 7.1(1) 以前のピアにだけ適用されます。この場合、アクセスを拒否されることはありません。7.1(1) 以前のピアはセッション重み付けアルゴリズムを使用するため、はるかにロードが軽くなっています。

しかし、7.1(1) ピアが常にクラスタ マスターであることは保証できないため、問題が生じます。クラスタ マスターに障害が発生すると、別のピアがマスターの役割を引き継ぎます。新しいマスターは、適格なピアのいずれかになります。結果が本質的に予測不能であるため、このタイプのクラスタを構成しないことをお勧めします。

## ロードバランシングの設定

ASA Release 7.1(1) ソフトウェアを実行しているセキュリティ アプライアンスでロードバランシングを設定するには、クラスタに参加するデバイスごとに次の要素を設定します。

- パブリックおよびプライベート インターフェイス
- VPN ロードバランシング クラスタ アトリビュート



(注)

クラスタ内のすべての参加デバイスは、クラスタ内のデバイス プライオリティの場合を除いて、同一のクラスタ コンフィギュレーションを持つ必要があります。

## ロードバランシング用のパブリックおよびプライベート インターフェイスの設定

ロードバランシング クラスタ デバイス用にパブリック（外部）およびプライベート（内部）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** vpn-load-balancing コンフィギュレーション モードで **lbpublic** キーワードを指定して **interface** コマンドを入力し、セキュリティ アプライアンスにパブリック インターフェイスを設定します。このコマンドは、このデバイスのロードバランシングのためのパブリック インターフェイスの名前または IP アドレスを指定します。

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic outside
hostname(config-load-balancing)#
```

- ステップ 2** vpn-load-balancing コンフィギュレーション モードで **lbprivate** キーワードを指定して **interface** コマンドを入力し、セキュリティ アプライアンスにプライベート インターフェイスを設定します。このコマンドは、このデバイスのロードバランシングのためのプライベート インターフェイスの名前または IP アドレスを指定します。

```
hostname(config-load-balancing)# interface lbprivate inside
hostname(config-load-balancing)#
```

- ステップ 3** クラスタ内のこのデバイスに割り当てるようにプライオリティを設定します。範囲は 1～10 です。プライオリティは、このデバイスが、起動時または既存のマスターに障害が発生したときに仮想クラスタ マスターになる可能性を示します。プライオリティを高く設定すると（たとえば 10）、それに応じてこのデバイスが仮想クラスタ マスターになる可能性も高くなります。

```
hostname(config-load-balancing)# priority number
hostname(config-load-balancing)#
```

たとえば、このデバイスにクラスタ内で 6 のプライオリティを割り当てるには、次のコマンドを入力します。

```
hostname(config-load-balancing)# priority 6
hostname(config-load-balancing)#
```

- ステップ 4** このデバイスのネットワーク アドレス変換を適用する場合は、デバイスの NAT 割り当てアドレスを指定して **nat** コマンドを入力します。

```
hostname(config-load-balancing)# nat ip_address  
hostname(config-load-balancing)#
```

たとえば、このデバイスに 192.168.30.3 の NAT アドレスを割り当てるには、次のコマンドを入力します。

```
hostname(config-load-balancing)# nat 192.168.30.3  
hostname(config-load-balancing)#
```

## ロードバランシング クラスタ アトリビュートの設定

クラスタ内の各デバイスのロードバランシング クラスタ アトリビュートを設定するには、次の手順を実行します。

- 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 **vpn load-balancing** コマンドを入力して、VPN ロードバランシングをセットアップします。

```
hostname(config)# vpn load-balancing  
hostname(config-load-balancing)#
```

これで VPN ロードバランシング コンフィギュレーション モードに移行し、ここで残りのロードバランシング アトリビュートを設定できます。

- ステップ 2** このデバイスが属しているクラスタの IP アドレスを設定します。このコマンドは、仮想クラスタ全体を表す単一の IP アドレスを指定します。仮想クラスタ内のすべてのセキュリティ アプライアンスが共有しているパブリックサブネット アドレスの範囲内にある IP アドレスを選択します。

```
hostname(config-load-balancing)# cluster ip address ip_address  
hostname(config-load-balancing)#
```

たとえば、クラスタ IP アドレスを 192.168.10.10 に設定するには、次のコマンドを入力します。

```
hostname(config-load-balancing)# cluster ip address 192.168.10.10  
hostname(config-load-balancing)#
```

- ステップ 3** クラスタ ポートを設定します。このコマンドは、このデバイスが参加している仮想クラスタの UDP ポートを指定します。デフォルト値は 9023 です。他のアプリケーションがこのポートを使用している場合は、ロードバランシングに使用する UDP 宛先ポート番号を入力します。

```
hostname(config-load-balancing)# cluster port port_number  
hostname(config-load-balancing)#
```

たとえば、クラスタ ポートを 4444 に設定するには、次のコマンドを入力します。

```
hostname(config-load-balancing)# cluster port 4444  
hostname(config-load-balancing)#
```

**ステップ 4** オプションで、クラスタの IPsec 暗号化をイネーブルにします。デフォルトでは暗号化は使用されません。このコマンドは、IPsec 暗号化をイネーブルまたはディセーブルにします。このチェックアトリビュートを設定する場合、最初に共有秘密情報を指定して確認する必要があります。仮想クラスタ内のセキュリティ アプライアンスは、IPsec を使用して LAN-to-LAN トンネルを介して通信します。デバイス間で通信されるすべてのロードバランシング情報が暗号化されるようにするには、このアトリビュートをイネーブルにします。

```
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)#
```



**(注)** 暗号化を使用する場合、インターフェイス内でロードバランシングを事前に設定しておく必要があります。ロードバランシング内部インターフェイスでそのインターフェイスがイネーブルになっていない場合、クラスタ暗号化を設定しようと試みるとエラー メッセージが表示されます。

クラスタ暗号化を設定したときにロードバランシング内部インターフェイスがイネーブルになっていたが、仮想クラスタへのデバイスの参加を設定する前にディセーブルにされた場合、**participate** コマンドを入力すると（または ASDM で Participate in Load Balancing Cluster チェックボックスを選択すると）エラー メッセージが表示され、そのクラスタに対して暗号化はイネーブルにはなりません。

クラスタ暗号化を使用するには、内部インターフェイスを指定して **crypto isakmp enable** コマンドを使用し、内部インターフェイス上の isakmp インターフェイスをイネーブルにする必要があります。

**ステップ 5** クラスタ暗号化をイネーブルにする場合は、さらに **cluster key** コマンドを入力して IPsec 共有秘密情報を指定する必要があります。このコマンドは、IPsec 暗号化をイネーブルにしてある場合、IPsec ピア間に共有秘密情報を指定します。ボックスに入力する値は、連続するアスタリスク文字として表示されます。

```
hostname(config-load-balancing)# cluster key shared_secret
hostname(config-load-balancing)#
```

たとえば、共有秘密情報を 123456789 に設定するには、次のコマンドを入力します。

```
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)#
```

**ステップ 6** **participate** コマンドを入力して、このデバイスのクラスタへの参加をイネーブルにします。

```
hostname(config-load-balancing)# participate
hostname(config-load-balancing)#
```

## VPN セッション制限の設定

IPsec セッションおよび WebVPN セッションは、セキュリティ アプライアンスのプラットフォームおよびライセンスがサポートする数だけ実行することができます。セキュリティ アプライアンスのライセンス情報を表示するには、グローバル コンフィギュレーション モードで **show version** コマンドを入力します。次の例で、コマンドと、このコマンドの出力からのライセンス情報の抜粋を示します。

```
hostname(config)# show version
```

```
Cisco Adaptive Security Appliance Software Version 7.1(0)182  
Device Manager Version 5.1(0)128
```

```
Licensed features for this platform:  
Maximum Physical Interfaces : Unlimited  
Maximum VLANs              : 100  
Inside Hosts                : Unlimited  
Failover                    : Active/Active  
VPN-DES                     : Enabled  
VPN-3DES-AES                : Enabled  
Security Contexts           : 10  
GTP/GPRS                    : Enabled  
VPN Peers                   : 750  
WebVPN Peers                : 500
```

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

アクティブな IPsec VPN セッションの最大数を、セキュリティ アプライアンスが許可する数よりも小さい値に制限するには、グローバル コンフィギュレーション モードで

**vpn-sessiondb max-session-limit** コマンドを入力します。このセッション数の制限は、VPN ロードバランシング用に算出されたロード率に影響します。

```
hostname(config)# vpn-sessiondb max-session-limit number_of_sessions  
hostname(config)#
```

たとえば、セキュリティ アプライアンス ライセンスが 750 の IPsec セッションを許可しており、IPsec セッションの数を 500 に制限したい場合は、次のコマンドを入力します。

```
hostname(config)# vpn-sessiondb max-session-limit 500  
hostname(config)#
```

このセッション制限を削除するには、このコマンドの **no** バージョンを使用します。

```
hostname(config)# no vpn-sessiondb max-session-limit  
hostname(config)#
```

WebVPN セッションの数をセキュリティ アプライアンスが許可する数よりも小さい値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb max-webvpn-session-limit** コマンドを使用します。このセッション制限を削除するには、このコマンドの **no** バージョンを使用します。

```
hostname(config)# vpn-sessiondb max-webvpn-session-limit number_of_sessions  
hostname(config)#
```

たとえば、セキュリティ アプライアンス ライセンスが 500 の WebVPN セッションを許可しており、WebVPN セッションの数を 250 に制限したい場合は、次のコマンドを入力します。

```
hostname(config)# vpn-sessiondb max-webvpn-session-limit 250  
hostname(config)#
```

このセッション制限を削除するには、このコマンドの **no** バージョンを使用します。

```
hostname(config)# no vpn-sessiondb max-webvpn-session-limit  
hostname(config)#
```

このライセンスで使用可能な機能の詳細な説明は、付録 A「機能のライセンスと仕様」を参照してください。



# トンネルグループ、グループポリシー、およびユーザの設定

この章では、VPN のトンネルグループ、グループポリシー、およびユーザの設定方法について説明します。次の事項について説明します。

- [トンネルグループ、グループポリシー、およびユーザの概要 \(P.26-2\)](#)
- [トンネルグループの設定 \(P.26-6\)](#)
- [グループポリシー \(P.26-24\)](#)
- [ユーザ アトリビュートの設定 \(P.26-60\)](#)

要約すると次のようになります。最初にトンネルグループを設定して、接続用の値を設定します。次に、グループポリシーを設定します。グループポリシーでは、ユーザの集合に関する値が設定されます。その後、ユーザを設定します。ユーザはグループの値を継承でき、さらに個別のユーザ単位に特定の値を設定することができます。この章では、これらのエンティティを設定する方法と理由について説明します。

## トンネルグループ、グループポリシー、およびユーザの概要

グループとユーザは、バーチャル プライベート ネットワーク (VPN) のセキュリティ管理とセキュリティ アプライアンスの設定における中核的な概念です。グループとユーザで指定されるアトリビュートによって、VPN へのユーザ アクセスと VPN の使用方法が決定されます。グループは、ユーザの集合を 1 つのエンティティとして扱うものです。ユーザのアトリビュートは、グループポリシーから取得されます。トンネルグループは、特定の接続用のグループポリシーを指定します。ユーザに特定のグループポリシーを割り当てない場合は、その接続のデフォルトのグループポリシーが適用されます。

トンネルグループとグループポリシーを使用すると、システム管理が簡略化されます。コンフィギュレーション タスクを効率化するために、セキュリティ アプライアンスには、デフォルトの LAN-to-LAN トンネルグループ、デフォルトのリモートアクセス トンネルグループ、デフォルトの WebVPN トンネルグループ、およびデフォルトのグループポリシー (DfltGrpPolicy) が用意されています。デフォルトのトンネルグループとグループポリシーでは、多くのユーザに共通すると考えられる設定が提供されます。ユーザを追加するときは、ユーザがグループポリシーからパラメータを「継承」するように指定できます。この指定により、多数のユーザの VPN アクセスを迅速に設定することができます。

すべての VPN ユーザに同一の権限を許可する場合は、特定のトンネルグループやグループポリシーを設定する必要はありませんが、VPN がそのように使用されることはほとんどありません。たとえば、経理グループ、カスタマー サポート グループ、および MIS (経営情報システム) グループが、プライベート ネットワークのそれぞれ異なる部分にアクセスできるようにする場合が考えられます。また、MIS の特定のユーザにシステムへのアクセスを許可し、その他の MIS ユーザはアクセスできないようにする場合もあります。トンネルグループとグループポリシーにより、このような柔軟な設定を安全に実行することができます。



(注)

セキュリティ アプライアンスには、オブジェクト グループという概念もあります。これは、ネットワーク リストのスーパーセットです。オブジェクト グループを使用すると、ポートやネットワークに対する VPN アクセスを定義することができます。オブジェクト グループは、グループポリシーやトンネルグループよりも、ACL と関連があります。オブジェクト グループを使用する方法の詳細については、[第 13 章「アクセスリストによるトラフィックの指定」](#)を参照してください。



## トンネルグループ

トンネルグループは、トンネル接続ポリシーを決定するレコードのセットで構成されます。これらのレコードでは、トンネル ユーザーが認証されるサーバ、およびアカウントिंग サーバがある場合は接続情報の送信先となるサーバが指定されます。また、これらのレコードには、接続用のデフォルト グループポリシーも指定され、さらにプロトコル固有の接続パラメータも含まれています。トンネルグループには、トンネル自体の作成に関連する少数のアトリビュートが含まれます。また、トンネルグループには、ユーザー関連のアトリビュートを定義するグループポリシーへのポイントも含まれます。

セキュリティ アプライアンスには、LAN-to-LAN 接続用の DefaultL2LGroup とリモートアクセス接続用の DefaultRAGroup、および WebVPN 接続用の DefaultWEBVPNGroup のデフォルト トンネルグループが用意されています。これらのデフォルト トンネルグループは変更できますが、削除はできません。また、環境に固有のトンネルグループを 1 つ以上作成することもできます。トンネルグループは、セキュリティ アプライアンスのローカルな設定であり、外部サーバでは設定できません。

トンネルグループでは、次のアトリビュートが指定されます。

- [トンネルグループの一般接続パラメータ \(P.26-3\)](#)
- [トンネルグループの IPSec 接続パラメータ \(P.26-4\)](#)
- [トンネルグループの WebVPN 接続パラメータ \(P.26-5\)](#)

### トンネルグループの一般接続パラメータ

一般パラメータは、IPSec および WebVPN 接続の両方に共通です。一般パラメータには、次のものがあります。

- トンネルグループ名：トンネルグループを追加または編集する場合にトンネルグループ名を指定します。次の考慮事項が適用されます。
  - 認証に事前共有キーを使用するクライアントの場合、トンネルグループ名は IPSec クライアントがセキュリティ アプライアンスに渡すグループ名と同じです。
  - 認証に証明書を使用するクライアントはこの名前を証明書の一部として渡し、セキュリティ アプライアンスが証明書からこの名前を抽出します。
- 接続タイプ：接続タイプには、IPSec リモートアクセス、IPSec LAN-to-LAN、および WebVPN があります。トンネルグループでは、接続タイプを 1 つだけ指定できます。
- 認証、認可、アカウントिंग サーバ：これらのパラメータでは、セキュリティ アプライアンスが次の目的で使用するサーバのグループまたはリストを指定します。
  - ユーザーの認証
  - ユーザーがアクセスを認可されたサービスに関する情報の取得
  - アccounting レコードの保存

サーバ グループは、1 つ以上のサーバで構成されます。

- 接続用のデフォルト グループポリシー：グループポリシーは、ユーザー関連のアトリビュートのセットです。デフォルト グループポリシーは、セキュリティ アプライアンスがトンネル ユーザーを認証または認可する際にデフォルトで使用するアトリビュートを含んだグループポリシーです。
- クライアント アドレスの割り当て方式：この方式には、セキュリティ アプライアンスがクライアントに割り当てる 1 つ以上の DHCP サーバまたはアドレス プールの値が含まれます。
- account-disabled の上書き：このパラメータにより、AAA サーバから受信した「account-disabled」インジケータを上書きできます。
- パスワード管理：このパラメータにより、現在のパスワードが指定された日数（デフォルトでは 14 日）で有効期限が切れることをユーザーに警告して、パスワードを変更する機会をユーザーに提供できます。

- グループの除去と領域の除去：これらのパラメータは、セキュリティ アプライアンスが受信したユーザ名を処理する方法を指示します。これらが適用されるのは、`user@realm` という形式で受信したユーザ名だけです。領域とは、ユーザ名に `@` デリミタが負荷されている管理ドメインです (`user@abc`)。

**strip-group** コマンドを指定する場合、セキュリティ アプライアンスは、VPN クライアントによって提示されるユーザ名からグループ名を取得してユーザ接続のトンネルグループを選択します。その後、セキュリティ アプライアンスは認可 / 認証のためにユーザ名のユーザ部分だけを送信します。それ以外の場合（ディセーブルになっている場合）、セキュリティ アプライアンスは領域を含むユーザ名全体を送信します。

**strip-realm** コマンドの処理は、ユーザ名を認証または認可サーバに送信するときにユーザ名から領域を削除します。コマンドがイネーブルになっている場合、セキュリティ アプライアンスはユーザ名認可 / 認証のユーザ部分だけを送信します。それ以外の場合、セキュリティ アプライアンスはユーザ名全体を送信します。

- 認可の要求：このパラメータにより、ユーザのアクセス前に認可を要求するか、またはその要求を取り下げることができます。
- 認可 DN アトリビュート：このパラメータは、認可の実行時に使用する認定者名アトリビュートを指定します。

## トンネルグループの IPsec 接続パラメータ

IPsec パラメータには、次のものがあります。

- クライアント認証方式：事前共有キー、証明書、またはその両方。
  - 事前共有キーに基づく IKE 接続の場合は、接続ポリシーに関連付けられている英数字キー自体（長さ 128 文字まで）。
  - ピア ID 確認要求：このパラメータはピアの証明書を使用してピアの ID を確認することを要求するかどうかを指定します。
- ISAKMP (IKE) キープアライブの設定。この機能により、セキュリティ アプライアンスはリモート ピアの継続的な存在を監視し、自分自身の存在をピアに報告します。ピアが応答なくなると、セキュリティ アプライアンスは接続を削除します。IKE キープアライブをイネーブルにすると、IKE ピアが接続を失ったときに接続がハングしません。

IKE キープアライブにはさまざまな形式があります。この機能が動作するには、セキュリティ アプライアンスとリモート ピアが共通の形式をサポートしている必要があります。この機能は、次のピアに対して動作します。

- Cisco VPN Client (Release 3.0 以上)
- Cisco VPN 3000 Client (Release 2.x)
- Cisco VPN 3002 ハードウェア クライアント
- Cisco VPN 3000 シリーズ コンセントレータ
- Cisco IOS ソフトウェア
- Cisco Secure PIX Firewall

シスコ以外の VPN クライアントは IKE キープアライブをサポートしません。

IKE キープアライブをサポートするピアとサポートしないピアが混在するグループを設定する場合は、グループ全体に対して IKE キープアライブをイネーブルにします。この機能をサポートしないピアに影響はありません。

IKE キープアライブをディセーブルにすると、応答しないピアとの接続はタイムアウトになるまでアクティブのままになるため、アイドル タイムアウトを短くすることを推奨します。アイドル タイムアウトを変更するには、[P.26-26 の「グループポリシーの設定」](#)を参照してください。



(注)

ISDN 回線経由で接続するクライアントがグループに含まれる場合は、接続コストを削減するために IKE キープアライブをディセーブルにしてください。通常、ISDN 接続はアイドルになると切断されますが、IKE キープアライブのメカニズムによって接続がアイドル状態にならないために、切断されなくなります。

IKE キープアライブをディセーブルにすると、クライアントは IKE キーと IPSec キーのどちらかの期限が満了した場合にのみ切断されます。IKE キープアライブがイネーブルになっている場合とは異なり、障害が発生したトラフィックは Peer Timeout Profile 値を持つトンネルから切断されません。



(注)

IKE メイン モードを使用する LAN-to-LAN コンフィギュレーションの場合は、2 つのピアの IKE キープアライブの設定が同じであることを確認してください。両方のピアで IKE キープアライブがイネーブルになっているか、または両方のピアで IKE キープアライブがディセーブルになっている必要があります。

- デジタル証明書を使用して認証を設定する場合、(ID 証明書とすべての発行証明書をピアに送信する) 証明書チェーン全体を送信するか、または発行証明書 (ルート証明書とすべての下位 CA 証明書を含む) だけを送信するかを指定できます。
- Windows クライアント ソフトウェアの古いバージョンを使用しているユーザに、クライアントをアップデートする必要があることを通知できるため、アップデートされたクライアントバージョンを取得するためのメカニズムを提供できます。VPN 3002 ハードウェア クライアントのユーザの場合、自動アップデートをトリガーできます。すべてのトンネルグループまたは特定のトンネルグループに対して、クライアント アップデートを設定および変更できます。
- デジタル証明書を使用して認証を設定する場合、IKE ピアに送信する証明書を識別するトラストポイントの名前を指定できます。

## トンネルグループの WebVPN 接続パラメータ

次のアトリビュートは WebVPN 接続に固有です。

- AAA または証明書の認証方式。
- 適用するカスタマイゼーションの名前。カスタマイゼーションは、ログイン時にユーザに表示されるウィンドウの内容を決定します。カスタマイゼーション パラメータは、WebVPN 設定の一部として設定します。
- DNS サーバ グループ名。DNS サーバ グループは、DNS サーバ名、ドメイン名、ネーム サーバ、リトライ回数、および DNS サーバがトンネルグループに使用するタイムアウト値を指定します。
- 1 つ以上のグループ エイリアス。これらはサーバがトンネルグループを参照できる代替名です。ログイン時に、ユーザはドロップダウン メニューからグループ名を選択します。
- 1 つ以上のグループ URL。このパラメータを設定する場合、指定されている URL に加わるユーザは、ログイン時にグループを選択する必要はありません。
- デフォルトのグループポリシーとは異なる WebVPN ユーザ アクセス権を許可するグループポリシー。
- CIFS 名前解決に使用する NetBIOS ネーム サービス サーバ (nbns-server) の名前。

## トンネルグループの設定

次の各項では、トンネルグループの内容とコンフィギュレーションについて説明します。

- デフォルトの IPsec リモートアクセス トンネルグループのコンフィギュレーション (P.26-6)
- トンネルグループの IPsec 一般パラメータの設定 (P.26-6)
- IPsec リモートアクセス トンネルグループの設定 (P.26-7)
- LAN-to-LAN トンネルグループの設定 (P.26-12)
- WebVPN トンネルグループの設定 (P.26-15)
- WebVPN ユーザ用のログイン ウィンドウのカスタマイズ (P.26-22)

デフォルト トンネルグループは変更可能です。また、3つのトンネルグループ タイプの1つとして新しいトンネルグループを設定することもできます。トンネルグループのアトリビュートを明示的に設定しない場合、そのアトリビュートは、値をデフォルト トンネルグループから取得します。デフォルト トンネルグループのタイプは ipsec-ra です。その後のパラメータは、選択したトンネル タイプによって異なります。デフォルト トンネルグループも含めて、すべてのトンネルグループの現在のコンフィギュレーションとデフォルトのコンフィギュレーションを確認するには、**show running-config all tunnel-group** コマンドを入力します。

### デフォルトの IPsec リモートアクセス トンネルグループのコンフィギュレーション

デフォルトのリモートアクセス トンネルグループの内容は、次のとおりです。

```
tunnel-group DefaultRAGroup general-attributes
no address-pool
authentication-server-group LOCAL
no authorization-server-group
no accounting-server-group
default-group-policy DfltGrpPolicy
no dhcp-server
no strip-realm
password-management password-expire-in-days 14
no override-account-disable
no strip-group
no authorization-required
authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup ipsec-attributes
no pre-shared-key
peer-id-validate req
no chain
no trust-point
isakmp keepalive threshold 300 retry 2
```

### トンネルグループの IPsec 一般パラメータの設定

一般パラメータは、複数のトンネルグループ タイプにわたって共通です。IPsec リモートアクセス および WebVPN トンネルは、同じ一般パラメータの大部分を共有します。IPsec LAN-to-LAN トンネルはサブセットを使用します。すべてのコマンドの詳細な説明については、『Cisco Security Appliance Command Reference』を参照してください。次の各項では、IPsec リモートアクセス トンネルグループ、IPsec LAN-to-LAN トンネルグループ、および WebVPN トンネルグループの設定方法について説明します。

## IPSec リモートアクセス トンネルグループの設定

ハードウェアまたはソフトウェア クライアントを使用して、リモート クライアントと中央サイトのセキュリティ アプライアンスとの間の接続をセットアップする場合は、IPSec リモートアクセス トンネルグループを使用します。IPSec リモートアクセス トンネルグループを設定するには、最初にトンネルグループ一般アトリビュートを設定してから、IPSec リモートアクセスアトリビュートを設定します。IPSec リモートアクセス VPN トンネルグループは、リモートアクセス IPSec クライアント接続にのみ適用されます。

### IPSec リモートアクセス トンネルグループの名前とタイプの指定

トンネルグループを作成し、**tunnel-group** コマンドを入力してその名前とタイプを指定します。IPSec リモートアクセス トンネルの場合、タイプは **ipsec-ra** になります。

```
hostname(config)# tunnel-group tunnel_group_name type ipsec-ra
hostname(config)#
```

たとえば、TunnelGroup1 という名前の IPSec リモートアクセス トンネルグループを作成するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group TunnelGroup1 type ipsec-ra
hostname(config)#
```

### IPSec リモートアクセス トンネルグループの一般アトリビュートの設定

トンネルグループの一般アトリビュートを設定または変更するには、次の手順でパラメータを指定します。

- ステップ 1** 一般アトリビュートを設定するには、**tunnel-group general-attributes** コマンドを入力して、トンネルグループの一般アトリビュート コンフィギュレーション モードに入ります。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

- ステップ 2** 認証サーバグループがある場合、使用するグループの名前を指定します。指定したグループに障害が発生したときにローカル データベースを認証に使用する場合は、**LOCAL** というキーワードを追加します。

```
hostname(config-tunnel-general)# authentication-server-group [(interface_name)]
groupname [LOCAL]
hostname(config-tunnel-general)#
```

グループ名の後ろにインターフェイス名を指定することにより、インターフェイス固有の認証をオプションで設定することができます。IPSec トンネルの終端位置を指定するインターフェイス名は丸カッコで囲む必要があります。次のコマンドは、**test** という名前のインターフェイスで **servergroup1** という名前のサーバを認証に使用するように、インターフェイス固有の認証を設定しています。

```
hostname(config-tunnel-general)# authentication-server-group (test) servergroup1
hostname(config-tunnel-general)#
```

- ステップ 3** 認可サーバグループがある場合、使用するグループの名前を指定します。この値を設定する場合、接続する認可データベースにユーザが存在する必要があります。

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

たとえば、次のコマンドは、認可サーバグループ FinGroup を使用することを指定しています。

```
hostname(config-tunnel-general)# authorization-server-group FinGroup
hostname(config-tunnel-general)#
```

- ステップ 4** アカウンティングサーバグループがある場合、使用するグループの名前を指定します。

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

たとえば、次のコマンドは、comptroller という名前のアカウンティングサーバグループを使用することを指定しています。

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

- ステップ 5** デフォルトグループポリシーの名前を指定します。

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

次の例では、デフォルトグループポリシーの名前として DfltGrpPolicy を設定しています。

```
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
hostname(config-tunnel-general)#
```

- ステップ 6** DHCP サーバ（最大 10 サーバ）の名前または IP アドレス、および DHCP アドレスプール（最大 6 プール）の名前を指定します。デフォルトでは、DHCP サーバとアドレスプールは使用されません。

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```



**(注)** インターフェイス名は丸カッコで囲む必要があります。

アドレスプールは、グローバルコンフィギュレーションモードで **ip local pool** コマンドを使用して設定します。

- ステップ 7** ユーザ名を AAA サーバに渡す前に、ユーザ名からグループまたは領域を除去するかどうかを指定します。デフォルトでは、グループ名も領域も除去されません。

```
hostname(config-tunnel-general)# strip-group
hostname(config-tunnel-general)# strip-realm
hostname(config-tunnel-general)#
```

領域は管理ドメインです。領域を除去すると、セキュリティ アプライアンスは、ユーザ名とグループ（ある場合）認証を使用します。グループを除去すると、セキュリティ アプライアンスは認証にユーザ名と領域（ある場合）を使用します。領域修飾子を削除するには **strip-realm** コマンドを入力し、認証時にユーザ名からグループ修飾子を削除するには **strip-group** コマンドを使用します。両方の修飾子を削除すると、認証は **username** だけに基ついて実行されます。それ以外の場合は、**username@realm** または **username<delimiter> group** 文字列全体に基ついて認証が行われます。サーバでデリミタを解析できない場合は、**strip-realm** を指定する必要があります。

**ステップ 8** オプションで、サーバが RADIUS、RADIUS with NT、または LDAP サーバである場合、パスワード管理をイネーブルにできます。この機能は、デフォルトでイネーブルになっていますが、現在のパスワードがまもなく有効期限切れになる場合にユーザに警告します。デフォルトでは、期限切れの 14 日前にユーザへの警告を開始します。

```
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

サーバが LDAP サーバの場合、期限切れが迫っていることをユーザに警告し始める有効期限までの日数（0 ～ 180）を指定できます。

```
hostname(config-tunnel-general)# password-management [password-expire in days n]
hostname(config-tunnel-general)#
```

**(注)**

トンネルグループの一般アトリビュート コンフィギュレーション モードで入力される **password-management** コマンドは、トンネルグループの ipsec アトリビュート モードで以前入力された非推奨の **radius-with-expiry** コマンドに置き換えられます。

このコマンドを設定する場合、セキュリティ アプライアンスはログイン時に、ユーザの現在のパスワードがまもなく期限切れになるか、または期限切れであることをリモート ユーザに通知します。その後セキュリティ アプライアンスは、パスワードを変更する機会をユーザに提供します。現在のパスワードの期限がまだ切れていない場合、ユーザは引き続きそのパスワードを使用してログインできます。RADIUS または LDAP 認証が設定されていない場合、セキュリティ アプライアンスはこのコマンドを無視します。

これはパスワードの期限切れまでの日数を変更するのではなく、まもなく期限切れになることをセキュリティ アプライアンスがユーザに警告し始めるまでの期限前の日数を変更することに注意してください。

**password-expire-in-days** キーワードを指定する場合、日数も指定する必要があります。

日数を 0 にしてこのコマンドを指定すると、このコマンドはディセーブルになります。セキュリティ アプライアンスは、期限切れが迫っていることをユーザに通知しませんが、ユーザは期限が切れた後にパスワードを変更できます。

**ステップ 9** オプションで、**override-account-disable** コマンドを入力して、AAA サーバから account-disabled インジケータを上書きする機能を設定します。

```
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

**(注)**

**override-account-disable** を許可すると、セキュリティ上のリスクが発生する可能性があります。

- ステップ 10** 証明書から認可クエリ用の名前を得るために使用する 1 つまたは複数のアトリビュートを指定します。このアトリビュートにより、サブジェクト DN フィールドのどの部分を認可用のユーザ名として使用するかが指定されます。

```
hostname(config-tunnel-ipsec)# authorization-dn-attributes {primary-attribute
[secondary-attribute] | use-entire-name}
```

たとえば、次のコマンドは、CN アトリビュートを認可用のユーザ名として使用することを指定しています。

```
hostname(config-tunnel-ipsec)# hostname(config-ipsec)# authorization-dn-attributes CN
hostname(config-tunnel-ipsec)#
```

authorization-dn-attributes には、**C** (国)、**CN** (通常名)、**DNQ** (DN 修飾子)、**EA** (電子メール アドレス)、**GENQ** (世代修飾子)、**GN** (名)、**I** (イニシャル)、**L** (地名)、**N** (名前)、**O** (組織)、**OU** (組織ユニット)、**SER** (シリアル番号)、**SN** (姓)、**SP** (州または都道府県)、**T** (役職)、**UID** (ユーザ ID) があります。

- ステップ 11** ユーザに接続を許可する前に、そのユーザが正常に認可されている必要があるかどうかを指定します。デフォルトでは認可は要求されません。

```
hostname(config-tunnel-ipsec)# authorization-required
hostname(config-tunnel-ipsec)#
```

## IPSec リモートアクセス トンネルグループの IPSec アトリビュートの設定

リモートアクセス トンネルグループに IPSec アトリビュートを設定するには、次の手順を実行します。次の説明では、すでに IPSec リモートアクセス トンネルグループが作成済みであると仮定しています。IPSec リモートアクセス トンネルグループには、IPSec LAN-to-LAN トンネルグループよりも多くのアトリビュートがあります。

- ステップ 1** IPSec リモートアクセス トンネルグループのアトリビュートを指定するには、次のコマンドを入力してトンネルグループ ipsec アトリビュート モードに入ります。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

このコマンドによりトンネルグループ ipsec アトリビュート コンフィギュレーションモードに入ります。リモートアクセス トンネルグループの IPSec アトリビュートは、このモードで設定します。

たとえば、次のコマンドは、TG1 という名前のトンネルグループに関するトンネルグループ ipsec アトリビュート モードのコマンドが続くことを指定しています。プロンプトが変化して、トンネルグループ ipsec アトリビュート モードに入ったことがわかります。

```
hostname(config)# tunnel-group TG1 type ipsec-ra
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```



- ステップ 2** 事前共有キーに基づく IKE 接続をサポートするために、事前共有キーを指定します。たとえば、次のコマンドは、IPSec リモートアクセス トンネルグループの IKE 接続をサポートするために、事前共有キー `xyzx` を指定しています。

```
hostname(config-tunnel-ipsec)# pre-shared-key xyzx  
hostname(config-tunnel-ipsec)#
```

- ステップ 3** ピアの証明書を使用してピアの ID を検証するかどうかを指定します。

```
hostname(config-tunnel-ipsec)# peer-id-validate option  
hostname(config-tunnel-ipsec)#
```

使用できるオプションは、**req** (必須)、**cert** (証明書でサポートされている場合)、**nocheck** (調べない) です。デフォルトは **req** です。

- ステップ 4** 証明書チェーンを送信できるかどうかを指定します。次のコマンドは、ルート証明書とすべての下位 CA 証明書を送信しています。

```
hostname(config-tunnel-ipsec)# chain  
hostname(config-tunnel-ipsec)#
```

このアトリビュートは、すべての IPSec トンネルグループ タイプに適用されます。

- ステップ 5** IKE ピアに送信する証明書を識別するトラストポイントの名前を指定します。

```
hostname(config-tunnel-ipsec)# trust-point trust-point-name  
hostname(config-tunnel-ipsec)#
```

次のコマンドは、IKE ピアに送信する証明書の名前として `mytrustpoint` を指定しています。

```
hostname(config-ipsec)# trust-point mytrustpoint
```

- ステップ 6** ISAKMP (IKE) キープアライブのしきい値と許可されるリトライ回数を指定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold <number> retry <number>  
hostname(config-tunnel-ipsec)#
```

**threshold** パラメータは、ピアがキープアライブ モニタリングを開始するまでの最長アイドル時間を秒数で指定します (10 ~ 3600)。**retry** パラメータは、キープアライブ応答が受信されなくなった後のリトライ間のインターバルです (2 ~ 10 秒)。IKE キープアライブは、デフォルトでイネーブルです。IKE キープアライブをディセーブルにするには、**isakmp** コマンドの **no** 形式を入力します。

たとえば、次のコマンドは、IKE キープアライブのしきい値を 15 秒に設定し、リトライ インターバルを 10 秒に設定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10  
hostname(config-tunnel-ipsec)#
```

**threshold** パラメータのデフォルト値は、リモートアクセスの場合は 300、LAN-to-LAN の場合は 10 です。また、**retry** パラメータのデフォルト値は 2 です。

**(注)**

以前トンネルグループ ipsec-ra コンフィギュレーションの一部として設定されていた **radius-with-expiry** コマンドは、推奨しません。トンネルグループ一般アトリビュート モードで入力される **password-management** コマンドが、これに代わります。

## LAN-to-LAN トンネルグループの設定

IPSec LAN-to-LAN VPN トンネルグループは、LAN-to-LAN IPSec クライアント接続だけに適用されます。設定するパラメータの多くは IPSec リモートアクセス トンネルグループの場合と同じですが、LAN-to-LAN トンネルのほうがパラメータの数は少なくなっています。LAN-to-LAN トンネルグループを設定するには、この項の手順を実行します。

### デフォルトの LAN-to-LAN トンネルグループのコンフィギュレーション

デフォルトの LAN-to-LAN トンネルグループの内容は、次のとおりです。

```
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
no accounting-server-group
default-group-policy DfltGrpPolicy
tunnel-group DefaultL2LGroup ipsec-attributes
no pre-shared-key
peer-id-validate req
no chain
no trust-point
isakmp keepalive threshold 10 retry 2
```

LAN-to-LAN トンネルグループのパラメータはリモートアクセス トンネルグループのパラメータより少なく、そのほとんどはどちらのグループでも同じです。実際に接続を設定する場合の利便性を考え、ここではこのグループのパラメータを個別に説明します。明示的に設定しないパラメータは、値をデフォルトのトンネルグループから継承します。

### LAN-to-LAN トンネルグループの名前とタイプの指定

トンネルグループの名前とタイプを指定するには、次のように **tunnel-group** コマンドを入力します。

```
hostname(config)# tunnel-group tunnel_group_name type tunnel_type
```

LAN-to-LAN トンネルの場合、タイプは **ipsec-l2l** になります。たとえば、docs という名前の LAN-to-LAN トンネルグループを作成するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group docs type ipsec-l2l
hostname(config)#
```

## LAN-to-LAN トンネルグループの一般アトリビュートの設定

トンネルグループの一般アトリビュートを設定するには、次の手順を実行します。

**ステップ 1** general-attributes キーワードを指定して、トンネルグループ一般アトリビュート モードに入ります。

```
hostname(config)# tunnel-group tunnel-group-name general-attributes  
hostname(config-tunnel-general)#
```

プロンプトが変化して、config-general モードに入ったことがわかります。トンネルグループの一般アトリビュートは、このモードで設定します。

たとえば、docs という名前のトンネルグループの場合、次のコマンドを入力します。

```
hostname(config)# tunnel-group docs general-attributes  
hostname(config-tunnel-general)#
```

**ステップ 2** アカウンティングサーバ グループがある場合、使用するグループの名前を指定します。

```
hostname(config-tunnel-general)# accounting-server-group groupname  
hostname(config-tunnel-general)#
```

たとえば、次のコマンドは、アカウンティングサーバ グループ acctgserv1 の使用を指定しています。

```
hostname(config-tunnel-general)# accounting-server-group acctgserv1  
hostname(config-tunnel-general)#
```

**ステップ 3** デフォルト グループポリシーの名前を指定します。

```
hostname(config-tunnel-general)# default-group-policy policyname  
hostname(config-tunnel-general)#
```

たとえば、次のコマンドは、デフォルト グループポリシーの名前に MyPolicy を指定しています。

```
hostname(config-tunnel-general)# default-group-policy MyPolicy  
hostname(config-tunnel-general)#
```

## LAN-to-LAN IPSec アトリビュートの設定

IPSec アトリビュートを設定するには、次の手順を実行します。

- ステップ 1** トンネルグループ IPSec アトリビュートを設定するには、IPSec アトリビュート キーワードとともに `tunnel-group` コマンドを入力して、トンネルグループ ipsec アトリビュート コンフィギュレーション モードに入ります。

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、`config-ipsec` モードに入り、TG1 という名前のトンネルグループのパラメータを設定できます。

```
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

プロンプトが変化して、トンネルグループ ipsec アトリビュート コンフィギュレーション モードに入ったことがわかります。

- ステップ 2** 事前共有キーに基づく IKE 接続をサポートするために、事前共有キーを指定します。

```
hostname(config-tunnel-ipsec)# pre-shared-key key
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、IPSec LAN-to-LAN トンネルグループの IKE 接続をサポートするために、事前共有キー XYZX を指定しています。

```
hostname(config-tunnel-ipsec)# pre-shared-key xyzx
hostname(config-tunnel-general)#
```

- ステップ 3** ピアの証明書を使用してピアの ID を検証するかどうかを指定します。

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

使用できるオプションは、**req** (必須)、**cert** (証明書でサポートされている場合)、**nocheck** (調べない) です。デフォルトは **req** です。たとえば、次のコマンドは、`peer-id-validate` オプションを **nocheck** に設定しています。

```
hostname(config-tunnel-ipsec)# peer-id-validate nocheck
hostname(config-tunnel-ipsec)#
```

- ステップ 4** 証明書チェーンを送信できるかどうかを指定します。次のアクションは、ルート証明書とすべての下位 CA 証明書を送信しています。

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

すべてのトンネルグループ タイプにこのアトリビュートを適用できます。

**ステップ 5** IKE ピアに送信する証明書を識別するトラストポイントの名前を指定します。

```
hostname(config-tunnel-ipsec)# trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、トラストポイント名を mytrustpoint に設定しています。

```
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
hostname(config-tunnel-ipsec)#
```

すべてのトンネルグループタイプにこのアトリビュートを適用できます。

**ステップ 6** ISAKMP (IKE) キープアライブのしきい値と許可されるリトライ回数を指定します。**threshold** パラメータは、ピアがキープアライブ モニタリングを開始するまでの最長アイドル時間を秒数で指定します (10 ~ 3600)。**retry** パラメータは、キープアライブ応答が受信されなくなった後のリトライ間のインターバルです (2 ~ 10 秒)。IKE キープアライブは、デフォルトでイネーブルです。IKE キープアライブをディセーブルにするには、**isakmp** コマンドの **no** 形式を入力します。

```
hostname(config)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、ISAKMP キープアライブのしきい値を 15 秒に設定し、リトライ インターバルを 10 秒に設定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

**threshold** パラメータのデフォルト値は、LAN-to-LAN の場合は 10 です。また、**retry** パラメータのデフォルト値は 2 です。

## WebVPN トンネルグループの設定

WebVPN トンネルグループは、WebVPN 接続だけに適用されます。WebVPN トンネルグループのトンネルグループ一般アトリビュートは IPsec リモートアクセス トンネルグループの場合と同じですが、トンネルグループのタイプが webvpn であり、**strip-group** および **strip-realm** コマンドが適用されない点が異なります。WebVPN 固有のアトリビュートは個別に定義します。次の各項では、WebVPN トンネルグループの設定方法について説明します。

### WebVPN トンネルグループの名前とタイプの指定

トンネルグループを作成し、グローバル コンフィギュレーション モードで **tunnel-group** コマンドを入力してその名前とタイプを指定します。IPsec リモートアクセス トンネルの場合、タイプは **webvpn** になります。

```
hostname(config)# tunnel-group tunnel_group_name type webvpn
hostname(config)#
```

たとえば、TunnelGroup3 という名前の WebVPN トンネルグループを作成するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group TunnelGroup3 type webvpn
hostname(config)#
```

## WebVPN トンネルグループの一般アトリビュートの設定

トンネルグループの一般アトリビュートを設定または変更するには、次の手順でパラメータを指定します。

- ステップ 1** 一般アトリビュートを設定するには、**tunnel-group general-attributes** コマンドを入力して、トンネルグループ一般アトリビュート コンフィギュレーション モードに入ります。プロンプトが次のように変化します。

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

以前の項で作成した TunnelGroup3 の一般アトリビュートを設定するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group TunnelGroup3 general-attributes
hostname(config-tunnel-general)#
```

- ステップ 2** 認証サーバグループがある場合、使用するグループの名前を指定します。指定したグループに障害が発生したときにローカル データベースを認証に使用する場合は、キーワード **LOCAL** を追加します。

```
hostname(config-tunnel-general)# authentication-server-group groupname [LOCAL]
hostname(config-tunnel-general)#
```

グループ名の後ろにインターフェイス名を指定することにより、インターフェイス固有の認証を設定することもできます。次のコマンドは、test という名前のインターフェイスでサーバ servergroup1 を認証に使用するよう、インターフェイス固有の認証を設定しています。

```
hostname(config-tunnel-general)# authentication-server-group test servergroup1
hostname(config-tunnel-general)#
```

- ステップ 3** オプションで、認可サーバグループがある場合、使用するグループの名前を指定します。認可を使用しない場合は、ステップ 6 に進みます。この値を設定する場合、接続する認可データベースにユーザが存在する必要があります。

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

たとえば、次のコマンドは、認可サーバグループ FinGroup を使用することを指定しています。

```
hostname(config-tunnel-general)# authorization-server-group FinGroup
hostname(config-tunnel-general)#
```

- ステップ 4** ユーザに接続を許可する前に、そのユーザが正常に認可されている必要があるかどうかを指定します。デフォルトでは認可は要求されません。

```
hostname(config-tunnel-ipsec)# authorization-required
hostname(config-tunnel-ipsec)#
```

- ステップ 5** 証明書から認可クエリー用の名前を得るために使用する 1 つまたは複数のアトリビュートを指定します。このアトリビュートにより、サブジェクト DN フィールドのどの部分を認可用のユーザ名として使用するかが指定されます。

```
hostname(config-tunnel-ipsec)# authorization-dn-attributes {primary-attribute
[secondary-attribute] | use-entire-name}
```

たとえば、次のコマンドは、CN アトリビュートを認可用のユーザ名として使用することを指定しています。

```
hostname(config-tunnel-ipsec)# hostname(config-ipsec)# authorization-dn-attributes CN
hostname(config-tunnel-ipsec)#
```

authorization-dn-attributes には、**C** (国)、**CN** (通常名)、**DNQ** (DN 修飾子)、**EA** (電子メール アドレス)、**GENQ** (世代修飾子)、**GN** (名)、**I** (イニシャル)、**L** (地名)、**N** (名前)、**O** (組織)、**OU** (組織ユニット)、**SER** (シリアル番号)、**SN** (姓)、**SP** (州または都道府県)、**T** (役職)、**UID** (ユーザ ID) があります。

- ステップ 6** オプションで、アカウントिंग サーバ グループがある場合、使用するグループの名前を指定します。アカウントングを使用しない場合は、ステップ 7 に進みます。

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

たとえば、次のコマンドは、アカウントング サーバ グループ comptroller の使用を指定しています。

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

- ステップ 7** オプションで、デフォルト グループポリシーの名前を指定します。デフォルト値は DfltGrpPolicy です。

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

次の例では、デフォルト グループポリシーの名前として MyDfltGrpPolicy を設定しています。

```
hostname(config-tunnel-general)# default-group-policy MyDfltGrpPolicy
hostname(config-tunnel-general)#
```

- ステップ 8** オプションで DHCP サーバ (最大 10 サーバ) の名前または IP アドレス、および DHCP アドレス プール (最大 6 プール) の名前を指定します。リスト項目をスペースで区切ります。デフォルトでは、DHCP サーバとアドレス プールは使用されません。

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```



(注)

インターフェイス名は丸カッコで囲む必要があります。

アドレス プールは、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用し  
て設定します。アドレス プールの設定については、第 27 章「VPN の IP アドレスの設定」を参照  
してください。

- ステップ 9** オプションで、サーバが RADIUS、RADIUS with NT、または LDAP サーバである場合、パスワー  
ド管理をイネーブルまたはディセーブルにできます。この機能は、デフォルトでイネーブルになっ  
ていますが、現在のパスワードがまもなく有効期限切れになる場合にユーザに警告します。デフォ  
ルトでは、期限切れの 14 日前にユーザへの警告を開始します。

```
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

サーバが LDAP サーバの場合、期限切れが迫っていることをユーザに警告し始める有効期限までの  
日数を指定できます。



**(注)** トンネルグループ一般アトリビュート コンフィギュレーション モードで入力される  
**password-management** コマンドは、トンネルグループ ipsec アトリビュート モードで以前  
入力された非推奨の **radius-with-expiry** コマンドに置き換えられます。

- ステップ 10** オプションで、**override-account-disable** コマンドを入力して、AAA サーバから account-disabled イ  
ンジケータを上書きする機能を設定します。

```
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

## WebVPN トンネルグループの WebVPN アトリビュートの設定

WebVPN トンネルグループに固有のパラメータを設定するには、この項の手順を実行します。

- ステップ 1** WebVPN トンネルグループのアトリビュートを指定するには、次のコマンドを入力してトンネルグ  
ループの webvpn アトリビュート モードに入ります。プロンプトが変化して、モードが変更された  
ことがわかります。

```
hostname(config)# tunnel-group tunnel-group-name webvpn-attributes
hostname(config-tunnel-ipsec)#
```

たとえば、sales という名前の WebVPN トンネルグループに webvpn アトリビュートを指定するに  
は、次のコマンドを入力します。

```
hostname(config)# tunnel-group sales webvpn-attributes
hostname(config-tunnel-webvpn)#
```

- ステップ 2** 使用する認証方式 AAA、デジタル署名、またはその両方を指定するには、**authentication** コマンド  
を入力します。aaa または certificate あるいはその両方を、任意の順序で指定できます。

```
hostname(config-tunnel-webvpn)# authentication authentication_method
hostname(config-tunnel-webvpn)#
```



たとえば、AAA と証明書認証の両方を許可するには、次のコマンドを入力します。

```
hostname(config-tunnel-webvpn)# authentication aaa certificate
hostname(config-tunnel-webvpn)#
```

**ステップ 3** 以前定義した Web ページ カスタマイゼーションを適用して、ログイン時にユーザに表示される Web ページのルックアンドフィールを変更するには、`customization` コマンドを入力します。

```
hostname(config-tunnel-webvpn)# customization customization_name
hostname(config-tunnel-webvpn)#
```

たとえば、`blueborder` という名前のカスタマイゼーションを使用する場合、次のコマンドを入力します。

```
hostname(config-tunnel-webvpn)# customization blueborder
hostname(config-tunnel-webvpn)#
```

カスタマイゼーション自体を WebVPN モードで設定します。

**ステップ 4** セキュリティ アプライアンスは、NetBIOS 名を IP アドレスにマップするために NBNS サーバにクエリーを行います。WebVPN は、リモート システム上のファイルをアクセスまたは共有することを NetBIOS に要求します。WebVPN は、NetBIOS および CIFS プロトコルを使用して、リモート システム上のファイルをアクセスまたは共有します。コンピュータ名を使用して Windows コンピュータへのファイル共有接続を試みる場合、指定するファイル サーバは、ネットワーク上のリソースを識別する特定の NetBIOS 名に対応します。

セキュリティ アプライアンスは、NetBIOS 名を IP アドレスにマップするために NetBIOS ネーム サーバにクエリーを行います。WebVPN は、リモート システム上のファイルをアクセスまたは共有することを NetBIOS に要求します。

NBNS 機能を正常に動作させるには、少なくとも 1 つの NetBIOS サーバ (ホスト) を設定する必要があります。冗長性を確保するため、最大 3 つの NBNS サーバを設定できます。セキュリティ アプライアンスは、リストにある最初のサーバを NetBIOS/CIFS の名前解決に使用します。クエリーが失敗すると、次のサーバを使用します。

CIFS の名前解決に使用する NBNS (NetBIOS ネーム サービス) サーバの名前を指定するには **nbns-server** コマンドを使用します。サーバ エントリは最大 3 つまで入力できます。設定する最初のサーバはプライマリ サーバであり、その他のサーバは冗長性を確保するためのバックアップです。これが (単なる WINS サーバではなく) マスター ブラウザであるかどうかと、タイムアウト間隔、およびリトライ回数を指定することもできます。通常、WINS サーバまたはマスター ブラウザは、セキュリティ アプライアンスと同じネットワーク上にあるか、またはそのネットワークから到達可能です。リトライ回数より先にタイムアウト間隔を指定する必要があります。

```
hostname(config-tunnel-webvpn)# nbns-server {host-name | IP_address} [master]
[timeout seconds] [retry number]
hostname(config-tunnel-webvpn)#
```

たとえば、`nbnsprimary` という名前のサーバをプライマリ サーバとし、サーバ 192.168.2.2 をセカンダリ サーバとして設定し、それぞれ 3 回のリトライを許可し、タイムアウトを 5 秒にするには、次のコマンドを入力します。

```
hostname(config)# name 192.168.2.1 nbnsprimary
hostname(config-tunnel-webvpn)# nbns-server nbnsprimary master timeout 5 retry 3
hostname(config-tunnel-webvpn)# nbns-server 192.168.2.2 timeout 5 retry 3
hostname(config-tunnel-webvpn)#
```

タイムアウト間隔は 1 ～ 30 秒の範囲（デフォルトは 2）に、リトライ回数は 0 ～ 10 の範囲（デフォルトは 2）にすることができます。

トンネルグループの `webvpn` アトリビュート コンフィギュレーション モードの `nbns-server` コマンドは、`webvpn` コンフィギュレーション モードの非推奨のコマンドに置き換えられます。

**ステップ 5** グループに代替の名前を指定するには、`group-alias` コマンドを使用します。グループ エイリアスを指定すると、ユーザがトンネルグループを参照できる代替名が 1 つ以上作成されます。ここで指定するグループ エイリアスは、ユーザのログイン ページでドロップダウン リストに表示されます。各グループには、それぞれ別個のコマンドで指定された複数のエイリアスを持つようにすることも、エイリアスを持たないようにすることもできます。この機能は、「Devtest」と「QA」のように、複数の通常名によって同じグループが認識される場合に便利です。

グループ エイリアスごとに、`group-alias` コマンドを入力します。各エイリアスは、デフォルトではイネーブルになっています。オプションで、各エイリアスを明示的にイネーブルまたはディセーブルにできます。

```
hostname(config-tunnel-webvpn)# group-alias alias [enable | disable]
hostname(config-tunnel-webvpn)#
```

たとえば、QA という名前のトンネルグループに対して エイリアス QA および Devtest 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-tunnel-webvpn)# group-alias QA enable
hostname(config-tunnel-webvpn)# group-alias Devtest enable
hostname(config-tunnel-webvpn)#
```



(注)

WebVPN トンネルグループ リストは、(ドロップダウン) グループ リストが表示されるようにイネーブルにしておく必要があります。

**ステップ 6** グループに着信 URL または IP アドレスを指定するには、`group-url` コマンドを使用します。グループ URL または IP アドレスを指定すると、ユーザはログイン時にグループを選択する必要がなくなります。ユーザがログインするとき、セキュリティ アプライアンスは、ユーザの着信 URL またはアドレスを `tunnel-group-policy` テーブルで探します。URL またはアドレスが検出され、`group-url` がトンネルグループでイネーブルになっている場合、セキュリティ アプライアンスは、関連付けられているトンネルグループを自動的に選択して、ユーザ名フィールドとパスワード フィールドだけをログイン ウィンドウでユーザに提示します。これにより、ユーザ インターフェイスは簡略化され、さらにグループのリストがユーザに公開されないという利点が加わります。ユーザに表示されるログイン ウィンドウでは、そのトンネルグループに設定されたカスタマイゼーションが使用されます。

URL またはアドレスがディセーブルになっており、グループ エイリアスが設定されている場合、グループのドロップダウン リストも表示されるため、ユーザはグループを選択する必要があります。

グループに複数の URL またはアドレスを設定（あるいは設定しないことも）できます。各 URL またはアドレスは、個別にイネーブルまたはディセーブルにすることができます。指定した各 URL またはアドレスごとに別個の `group-url` コマンドを使用する必要があります。http または https プロトコルのいずれかを含む URL またはアドレス全体を指定する必要があります。

同じ URL またはアドレスを複数のグループに関連付けることはできません。セキュリティ アプライアンスは、トンネルグループの URL またはアドレスを受け入れる前に、URL またはアドレスが一意であることを確認します。

グループ URL またはアドレスごとに、**group-url** コマンドを入力します。オプションで、各 URL またはエイリアスを明示的にイネーブル（デフォルト）またはディセーブルにできます。

```
hostname(config-tunnel-webvpn)# group-url url [enable | disable]
hostname(config-tunnel-webvpn)#
```

たとえば、RadiusServer という名前のトンネルグループのグループ URL、http://www.cisco.com および http://192.168.10.10 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)# tunnel-group RadiusServer type webvpn
hostname(config)# tunnel-group RadiusServer general-attributes
hostname(config-tunnel-general)# authentication server-group RADIUS
hostname(config-tunnel-general)# accounting-server-group RADIUS
hostname(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias "Cisco Remote Access" enable
hostname(config-tunnel-webvpn)# group-url http://www.cisco.com enable
hostname(config-tunnel-webvpn)# group-url http://192.168.10.10 enable
hostname(config-tunnel-webvpn)#
```

さらに詳細な例については、P.26-22 の「WebVPN ユーザ用のログイン ウィンドウのカスタマイズ」を参照してください。

**ステップ 7** WebVPN トンネルグループに使用する DNS サーバを指定するには、**dns-group** コマンドを入力します。デフォルト値は DefaultDNS です。

```
hostname(config-tunnel-webvpn)# dns-group {hostname | ip_address}
hostname(config-tunnel-webvpn)#
```

**dns-group** コマンドは、ホスト名をトンネルグループの適切な DNS サーバに解決します。たとえば、server1 という名前の DNS サーバの使用を指定する場合、次のコマンドを入力します。

```
hostname(config)# name 10.10.10.1 server1
hostname(config-tunnel-webvpn)# dns-group server1
hostname(config-tunnel-webvpn)#
```

**ステップ 8** （オプション）Cisco Secure Desktop Manager を使用してグループベース ポリシー アトリビュートを「Use Failure Group-Policy」または「Use Success Group-Policy, if criteria match」に設定する場合、VPN 機能ポリシーを指定するには、**hic-fail-group-policy** コマンドを使用します。デフォルト値は DfltGrpPolicy です。

```
hostname(config-tunnel-webvpn)# hic-fail-group-policy name
hostname(config-tunnel-webvpn)#
```

*Name* は、WebVPN トンネルグループに作成されたグループポリシーの名前です。

このポリシーは、次の CSD クライアントのアクセス権を区別するための代替グループポリシーです。

- 「Use Failure Group-Policy」に設定されている CSD ロケーション エントリと一致するクライアント。
- 「Use Success Group-Policy, if criteria match」に設定された CSD ロケーション エントリと一致し、設定されているグループベース ポリシー基準と一致しないクライアント。詳細については、『Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators』を参照してください。

次の例は、group2 という名前の代替グループポリシーを指定します。

```
hostname(config-tunnel-webvpn)# hic-fail-group-policy group2
hostname(config-tunnel-webvpn)#
```



(注)

VPN 機能ポリシーを「Always use Success Group-Policy」に設定した場合、セキュリティ アプライアンスはこのアトリビュートを使用しません。

詳細については、『Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators』を参照してください。

## WebVPN ユーザ用のログイン ウィンドウのカスタマイズ

カスタマイゼーション プロファイルとトンネルグループの組み合わせを使用して、さまざまなグループに異なるログイン ウィンドウをセットアップできます。たとえば、salesgui と呼ばれるカスタマイゼーション プロファイルを作成したとすれば、次の例で示すように、そのカスタマイゼーション プロファイルを使用する sales という名前の WebVPN トンネルグループを作成できます。

- ステップ 1** webvpn モードで、WebVPN カスタマイゼーション（この場合は salesgui という名前）を定義して、デフォルトのロゴを mycompanylogo.gif に変更します。あらかじめ mycompanylogo.gif をセキュリティ アプライアンスのフラッシュ メモリにロードしてコンフィギュレーションを保存しておく必要があります。詳細については、WebVPN の章を参照してください。

```
hostname# webvpn
hostname (config-webvpn)# customization value salesgui
hostname(config-webvpn-custom)# logo file disk0:\mycompanylogo.gif
hostname(config-webvpn-custom)#
```

- ステップ 2** グローバル コンフィギュレーション モードで、ユーザ名をセットアップして、それを定義した WebVPN カスタマイゼーションに関連付けます。

```
hostname# username seller attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# customization value salesgui
hostname(config-username-webvpn)# exit
hostname(config-username)# exit
hostname#
```

- ステップ 3** グローバル コンフィギュレーション モードで、sales という名前の WebVPN トンネルグループを作成します。

```
hostname# tunnel-group sales type webvpn
hostname(config-tunnel-webvpn)#
```

- ステップ 4** このトンネルグループに salesgui カスタマイゼーションを使用することを指定します。

```
hostname# tunnel-group sales webvpn-attributes
hostname(config-tunnel-webvpn)# customization salesgui
```

**ステップ 5** セキュリティ アプライアンスへのログイン時にユーザがブラウザに入力するアドレスに、グループ URL を設定します。たとえば、セキュリティ アプライアンスの IP アドレスが 192.168.3.3 の場合、グループ URL を https://192.168.3.3 に設定します。

```
hostname(config-tunnel-webvpn)# group-url https://192.168.3.3.  
hostname(config-tunnel-webvpn)#
```

正常にログインするためにポート番号が必要になる場合は、コロンを前に付けてポート番号を含めます。セキュリティ アプライアンスは、この URL を sales トンネルグループにマップし、salesgui カスタマイゼーション プロファイルを、ユーザが https://192.168.3.3 にログインするときに表示されるログイン画面に適用します。

---

## グループポリシー

この項では、グループポリシーとその設定方法について説明します。ここでは、次の項目について説明します。

- デフォルトのグループポリシー (P.26-24)
- グループポリシーの設定 (P.26-26)

グループポリシーは、IPSec 接続用のユーザ関連の属性と値のペアがセットになったもので、デバイスに内部的（ローカル）に保存されるか、外部の RADIUS サーバ上に保存されます。トンネルグループは、トンネルの確立後、ユーザ接続の条件を設定するグループポリシーを使用します。グループポリシーを使用すると、属性のセット全体をユーザまたはユーザのグループに適用することができ、各ユーザに各属性を個別に指定する必要がなくなります。

ユーザにグループポリシーを割り当てたり、特定のユーザのグループポリシーを変更したりするには、グローバル コンフィギュレーション モードで **group-policy** コマンドを入力します。

セキュリティ アプライアンスには、デフォルトのグループポリシーが含まれています。変更は可能でも削除できないデフォルト グループポリシーだけでなく、環境に固有のグループポリシーを 1 つ以上作成することもできます。

内部グループポリシーと外部グループポリシーを設定できます。内部グループは、セキュリティ アプライアンスの内部データベースに設定されます。外部グループは、RADIUS のような外部認証サーバに設定されます。グループポリシーには、次の属性があります。

- ID
- サーバ定義
- クライアント ファイアウォールの設定
- トンネリング プロトコル
- IPSec の設定
- ハードウェア クライアントの設定
- フィルタ
- クライアント コンフィギュレーションの設定
- WebVPN の機能
- 接続の設定

## デフォルトのグループポリシー

セキュリティ アプライアンスでは、デフォルトのグループポリシーが提供されます。このデフォルト グループポリシーは変更できますが、削除はできません。デフォルト グループポリシーは、DfltGrpPolicy という名前で必ずセキュリティ アプライアンス上に存在していますが、このデフォルト グループポリシーは、セキュリティ アプライアンスで使用するよう設定しないと有効になりません。他のグループポリシーを設定する場合、明示的に指定しない任意の属性がその値をデフォルト グループポリシーから受け継ぎます。デフォルト グループポリシーを表示するには、次のコマンドを入力します。

```
hostname(config)# show running-config all group-policy DfltGrpPolicy
hostname(config)#
```

デフォルト グループポリシーを設定するには、次のコマンドを入力します。

```
hostname(config)# group-policy DfltGrpPolicy internal
hostname(config)#
```



(注)

デフォルトのグループポリシーは、常に内部（internal）です。コマンドのシンタックスは、`hostname(config)# group-policy DfltGrpPolicy {internal | external}` となっていますが、タイプを `external` に変更することはできません。

デフォルト グループポリシーの任意のアトリビュートを変更する場合は、次のように `group-policy attributes` コマンドを使用してアトリビュート モードに入り、その後、目的の任意のアトリビュートを変更するためのコマンドを指定します。

```
hostname(config)# group-policy DfltGrpPolicy attributes
```



(注)

アトリビュート モードは内部グループポリシーだけに適用されます。

セキュリティ アプライアンスが提供するデフォルトのグループポリシー `DfltGrpPolicy` は、次のとおりです。

```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
wins-server none
dns-server none
vpn-access-hours none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-session-timeout none
vpn-filter none
vpn-tunnel-protocol IPSec
password-storage disable
ip-comp disable
re-xauth disable
group-lock none
pfs disable
banner none
ipsec-udp disable
ipsec-udp-port 10000
split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
secure-unit-authentication disable
user-authentication disable
user-authentication-idle-timeout 30
ip-phone-bypass disable
leap-bypass disable
nem disable
backup-servers keep-client-config
client-firewall none
client-access-rule none
webvpn
functions url-entry
no html-content-filter
no homepage
no filter
no url-list
no port-forward
port-forward-name value Application Access
```

デフォルト グループポリシーは変更可能です。また、環境に固有の 1 つ以上のグループポリシーを作成することもできます。

## グループポリシーの設定

グループポリシーはあらゆる種類のトンネルに適用できます。どちらの場合も、パラメータが明示的に指定されていなければ、そのグループはデフォルト グループポリシーの値を使用します。グループポリシーを設定するには、次の項の手順を実行します。

### 外部グループポリシーの設定

外部グループポリシーは、指定した外部サーバからアトリビュート値を取得します。外部グループポリシーの場合は、セキュリティ アプライアンスがアトリビュートのクエリーを実行できる AAA サーバ グループを指定し、その外部 AAA サーバ グループからアトリビュートを取得するときに使用するパスワードを指定します。外部認証サーバを使用している場合、ユーザ名とグループ名は一意でなければならないことに留意してください。グループに名前を付ける場合、外部ユーザの名前と一致する名前を選択しないようにします。これとは逆に、外部ユーザに名前を割り当てる場合、外部グループの名前を選択しないようにします。

セキュリティ アプライアンスは、外部 LDAP または RADIUS サーバでのユーザ認可をサポートします。外部サーバを使用するようにセキュリティ アプライアンスを設定する前に、正しいセキュリティ アプライアンス認可アトリビュートでサーバを設定し、これらのアトリビュートのサブセットから個々のユーザに固有のアクセス権を割り当てる必要があります。[付録 E「認可および認証用の外部サーバの設定」](#)の手順に従って、外部サーバを設定します。

外部グループポリシーを設定するには、次の手順を実行し、サーバ グループ名とパスワードとともにグループポリシーの名前とタイプを指定します。

```
hostname(config)# group-policy group_policy_name type server-group server_group_name
password server_password
hostname(config)#
```



(注)

外部グループポリシーの場合、サポートされる AAA サーバ タイプは RADIUS のみです。

たとえば、次のコマンドは、ExtRAD という名前の外部 RADIUS サーバからアトリビュートを取得する ExtGroup という名前の外部グループポリシーを作成し、アトリビュートを取得するときに使用するパスワードが newpassword パスワードであることを指定します。

```
hostname(config)# group-policy ExtGroup external server-group ExtRAD password
newpassword
hostname(config)#
```



(注)

[付録 E「認可および認証用の外部サーバの設定」](#)で説明しているように、複数のベンダー固有のアトリビュート (VSA) を設定できます。RADIUS サーバが Class アトリビュート (#25) を返すように設定されている場合、セキュリティ アプライアンスは、そのアトリビュートを使用してグループ名を認証します。RADIUS サーバで、アトリビュートは OU=groupname の形式をとる必要があります。ここで groupname は、たとえば OU=Finance のように、セキュリティ アプライアンスで設定されているグループ名と同じです。



## 内部グループポリシーの設定

内部グループポリシーを設定するには、グループポリシーの名前とタイプを指定します。

```
hostname(config)# group-policy group_policy_name type
hostname(config)#
```

たとえば、次のコマンドは、GroupPolicy1 という名前の内部グループポリシーを作成します。

```
hostname(config)# group-policy GroupPolicy1 internal
hostname(config)#
```

デフォルトのタイプは **internal** です。

キーワード **from** を追加して既存のポリシーの名前を指定することにより、内部グループポリシーのアトリビュートをその既存のグループポリシーの値に初期設定することができます。

```
hostname(config)# group-policy group_policy_name internal from group_policy_name
hostname(config-group-policy)#
hostname(config-group-policy)#
```

## グループポリシー アトリビュートの設定

内部グループポリシーの場合は、特定のアトリビュート値を指定できます。最初に、グローバル コンフィギュレーション モードで **group-policy attributes** コマンドを入力して、グループポリシーのアトリビュート モードに入ります。

```
hostname(config)# group-policy name attributes
hostname(config-group-policy)#
```

プロンプトが変化して、モードが変更されたことがわかります。グループポリシー アトリビュート モードでは、指定したグループポリシーのアトリビュートと値のペアを設定することができます。グループポリシー アトリビュート モードで、デフォルト グループから継承しないアトリビュートと値のペアを明示的に設定します。このためのコマンドを、次の各項で説明します。

## WINS サーバおよび DNS サーバの設定

プライマリとセカンダリの WINS サーバおよび DNS サーバを指定できます。それぞれの場合のデフォルト値は **none** です。これらのサーバを設定するには、次の手順を実行します。

### ステップ 1 プライマリとセカンダリの WINS サーバを指定します。

```
hostname(config-group-policy)# wins-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

最初に指定する IP アドレスがプライマリ WINS サーバの IP アドレスです。2 番目（オプション）の IP アドレスはセカンダリ WINS サーバの IP アドレスです。IP アドレスではなく **none** キーワードを指定すると、WINS サーバにヌル値が設定されます。この設定により、WINS サーバは許可されず、デフォルトまたは指定のグループポリシーから値が継承されなくなります。

**wins-server** コマンドを入力するたびに、既存の設定が上書きされます。たとえば、WINS サーバ x.x.x.x を設定し、その後 WINS サーバ y.y.y.y を設定すると、2 番目のコマンドで最初のコマンドが上書きされ、y.y.y.y が単独の WINS サーバになります。サーバを複数設定する場合も同様です。以前に設定したサーバを上書きせずに WINS サーバを追加するには、このコマンドを入力するときにすべての WINS サーバの IP アドレスを指定します。

次の例は、FirstGroup という名前のグループポリシーに、IP アドレスが 10.10.10.15 と 10.10.10.30 である WINS サーバを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30
hostname(config-group-policy)#
```

## ステップ 2 プライマリとセカンダリの DNS サーバを指定します。

```
hostname(config-group-policy)# dns-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

最初に指定する IP アドレスがプライマリ DNS サーバの IP アドレスです。2 番目（オプション）の IP アドレスはセカンダリ DNS サーバの IP アドレスです。IP アドレスではなく **none** キーワードを指定すると、DNS サーバにヌル値が設定されます。この設定により、DNS サーバは許可されず、デフォルトまたは指定のグループポリシーから値が継承されなくなります。

**dns-server** コマンドを入力するたびに、既存の設定が上書きされます。たとえば、DNS サーバ x.x.x.x を設定し、その後 DNS サーバ y.y.y.y を設定すると、2 番目のコマンドで最初のコマンドが上書きされ、y.y.y.y が単独の DNS サーバになります。サーバを複数設定する場合も同様です。以前に設定したサーバを上書きせずに DNS サーバを追加するには、このコマンドを入力するときにすべての DNS サーバの IP アドレスを指定します。

次の例は、「FirstGroup」という名前のグループポリシーに、IP アドレスが 10.10.10.15 と 10.10.10.30 である DNS サーバを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dns-server value 10.10.10.15 10.10.10.30
hostname(config-group-policy)#
```

## VPN 固有アトリビュートの設定

VPN アトリビュートの値を設定するアトリビュートを設定するには、この項の手順を実行します。これらのアトリビュートは、アクセス時間、許可される同時ログイン数、タイムアウト、VPN 接続に使用する ACL の名前、およびトンネル プロトコルを制御します。

### ステップ 1 VPN アクセス時間を設定します。これには、グループポリシー コンフィギュレーション モードで **vpn-access-hours** コマンドを使用して、グループポリシーを設定済みの time-range ポリシーに関連付けます。

```
hostname(config-group-policy)# vpn-access-hours value {time-range | none}
```

グループポリシーは、デフォルトまたは指定されたグループポリシーの time-range の値を継承することができます。この継承が発生しないようにするには、このコマンドで time-range の名前ではなく **none** キーワードを入力します。このキーワードにより、VPN アクセス時間がヌル値に設定され、time-range ポリシーは許可されなくなります。

time-range 変数は、グローバル コンフィギュレーション モードで **time-range** コマンドを使用して定義されたアクセス時間のセットの名前です。次の例は、FirstGroup という名前のグループポリシーを 824 と呼ばれる time-range ポリシーに関連付ける方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-access-hours value 824
```

**ステップ 2** グループポリシー コンフィギュレーション モードで **vpn-simultaneous-logins** コマンドを使用して、任意のユーザに許可される同時ログイン数を指定します。

```
hostname(config-group-policy)# vpn-simultaneous-logins integer
```

デフォルト値は 3 です。値の範囲は 0 ～ 2147483647 の整数です。グループポリシーは、別のグループポリシーからこの値を継承することができます。ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。次の例は、FirstGroup という名前のグループポリシーで最大 4 つの同時ログインを許可する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes  
hostname(config-group-policy)# vpn-simultaneous-logins 4  
hostname(config-group-policy)#
```



(注)

同時ログインの最大数の制限は非常に大きいですが、複数の同時ログインの許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼす恐れがあります。

**ステップ 3** グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-idle-timeout** コマンドを入力して、ユーザ タイムアウト期間を設定します。

```
hostname(config-group-policy)# vpn-idle-timeout {minutes | none}  
hostname(config-group-policy)#
```

最小時間は 1 分で、最大時間は 35791394 分です。デフォルトは 30 分です。この期間中に接続上で通信アクティビティがまったくなかった場合、セキュリティ アプライアンスは接続を終了します。

グループポリシーは、別のグループポリシーからこの値を継承できます。値を継承しないようにするには、分を指定する代わりに **none** キーワードを使用して、このコマンドを入力します。また、**none** キーワードを指定すると、無制限のアイドル タイムアウト期間が許可されます。このキーワードにより、アイドル タイムアウトにヌル値が設定され、アイドル タイムアウトが拒否されます。

次の例は、FirstGroup という名前のグループポリシーに 15 分の VPN アイドル タイムアウトを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes  
hostname(config-group-policy)# vpn-idle-timeout 15  
hostname(config-group-policy)#
```

**ステップ 4** グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-session-timeout** コマンドを使用して、VPN 接続の最大時間を設定します。

```
hostname(config-group-policy)# vpn-session-timeout {minutes | none}  
hostname(config-group-policy)#
```

最小時間は 1 分で、最大時間は 35791394 分です。デフォルト値はありません。この期間が終了すると、セキュリティ アプライアンスは接続を終了します。

グループポリシーは、別のグループポリシーからこの値を継承できます。値を継承しないようにするには、分を指定する代わりに **none** キーワードを使用して、このコマンドを入力します。**none** キーワードを指定すると、無制限のセッション タイムアウト期間が許可されます。セッション タイムアウトにはヌル値が設定され、セッション タイムアウトが拒否されます。

次の例は、FirstGroup という名前のグループポリシーに 180 分の VPN セッション タイムアウトを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

**ステップ 5** グループポリシー モードで **vpn-filter** コマンドを使用して、VPN 接続に使用する ACL の名前を指定します（このアトリビュートはユーザ名モードでも設定できます。その場合、グループポリシー値はユーザ名のもとで設定された値に置き換えられます）。

```
hostname(config-group-policy)# vpn-filter {value ACL name | none}
hostname(config-group-policy)#
```

ACL を設定して、このグループポリシーについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**vpn-filter** コマンドを入力して、これらの ACL を適用します。

**vpn-filter none** コマンドを入力して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。

グループポリシーは、別のグループポリシーからこの値を継承できます。値を継承しないようにするには、ACL 名を指定する代わりに、**none** キーワードを入力します。**none** キーワードは、アクセスリストがないことを示します。このキーワードにより、ヌル値が設定され、アクセスリストが拒否されます。

次の例は、FirstGroup という名前のグループポリシーに対して **acl\_vpn** という名前のアクセスリストを呼び出すフィルタを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter acl_vpn
hostname(config-group-policy)#
```

**ステップ 6** このグループポリシーの VPN トンネル タイプ（IPSec または WebVPN）を指定します。

```
hostname(config-group-policy)# vpn-tunnel-protocol {webvpn | IPSec}
hostname(config-group-policy)#
```

デフォルトは IPSec です。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no vpn-tunnel-protocol [webvpn | IPSec]
hostname(config-group-policy)#
```

このコマンドのパラメータの値は、次のとおりです。

- **IPSec**：2 つのピア（リモートアクセス クライアントまたは別のセキュア ゲートウェイ）間の IPSec トンネルをネゴシエートします。認証、暗号化、カプセル化、キー管理を制御するセキュリティ アソシエーションを作成します。
- **webvpn**：HTTP 対応 Web ブラウザ経由でリモート ユーザに VPN サービスを提供します。クライアントは不要です。

このコマンドを入力して、1 つ以上のトンネリング モードを設定します。VPN トンネルで接続するユーザに対して、1 つ以上のトンネリング モードを設定する必要があります。

次の例は、FirstGroup という名前のグループポリシーに IPSec トンネリング モードを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol IPSec
hostname(config-group-policy)#
```

## セキュリティ アトリビュートの設定

この項のアトリビュートは、グループの特定のセキュリティ設定を指定します。

- ステップ 1** グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **password-storage** コマンドを使用し、ユーザがログイン パスワードをクライアント システムに保存するかどうかを指定します。パスワード保存をディセーブルにするには、**disable** キーワードを指定して **password-storage** コマンドを使用します。

```
hostname(config-group-policy)# password-storage {enable | disable}
hostname(config-group-policy)#
```

セキュリティ上の理由から、パスワード保存はデフォルトでディセーブルになっています。パスワード保存は、セキュアなサイトにあることがわかっているシステムでのみ、イネーブルにします。

**password-storage** アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no password-storage
hostname(config-group-policy)#
```

**no** 形式を指定すると、**password-storage** の値を別のグループポリシーから継承することができます。

このコマンドは、対話的なハードウェア クライアント 認証やハードウェア クライアントの個別 ユーザ認証には適用されません。

次の例は、FirstGroup という名前のグループポリシーでパスワード保存をイネーブルにする方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
hostname(config-group-policy)#
```

- ステップ 2** デフォルトではディセーブルになっている IP 圧縮をイネーブルにするかどうかを指定します。

```
hostname(config-group-policy)# ip-comp {enable | disable}
hostname(config-group-policy)#
```

LZS IP 圧縮をイネーブルにするには、グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **ip-comp** コマンドを入力します。IP 圧縮をディセーブルにするには、**disable** キーワードを指定して **ip-comp** コマンドを入力します。

**ip-comp** アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、値を別のグループポリシーから継承できます。

```
hostname(config-group-policy)# no ip-comp
hostname(config-group-policy)#
```

データ圧縮をイネーブルにすることにより、モデムで接続するリモート ダイアルイン ユーザのデータ伝送レートが高くなる可能性があります。



### 注意

データ圧縮を使用すると、ユーザセッションごとのメモリ要求と CPU 使用率が増加し、結果としてセキュリティ アプライアンスのスループット全体が低下します。そのため、データ圧縮はモデムで接続するリモート ユーザについてのみイネーブルにすることを推奨します。モデム ユーザ専用のグループポリシーを設計して、そのようなユーザに対してのみ圧縮をイネーブルにしてください。

**ステップ 3** グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **re-xauth** コマンドを使用し、IKE キーの再生成時にユーザが再認証を受ける必要があるかどうかを指定します。IKE キーが再生成される際の再認証をイネーブルにすると、セキュリティ アプライアンスは初回のフェーズ 1 PKE ネゴシエーションでユーザにユーザ名とパスワードの入力を求めるプロンプトを表示し、IKE キーの再生成が発生するたびに同様にユーザ認証のプロンプトを表示します。再認証によりセキュリティがより強固になります。

設定されているキーの再生成インターバルが短い場合、ユーザは繰り返し認可要求を受けるため、不便を感じる場合があります。認可要求が何度も繰り返されないようにするには、再認証をディセーブルにします。設定されているキーの再生成インターバルを確認するには、モニタリング モードで **show crypto ipsec sa** コマンドを入力して、セキュリティ アソシエーションの秒単位のライフタイム、およびデータのキロバイト単位のライフタイムを表示します。IKE キーが再生成される際のユーザの再認証をディセーブルにするには、**disable** キーワードを入力します。IKE キーが再生成される際の再認証は、デフォルトでディセーブルになっています。

```
hostname(config-group-policy)# re-xauth {enable | disable}
hostname(config-group-policy)#
```

IKE キーが再生成される際の再認証の値を他のグループポリシーから継承できるようにするには、このコマンドの **no** 形式を入力して、**re-xauth** アトリビュートを実行コンフィギュレーションから削除します。

```
hostname(config-group-policy)# no re-xauth
hostname(config-group-policy)#
```



(注) 接続先にユーザが存在しない場合、再認証は失敗します。

**ステップ 4** グループポリシー コンフィギュレーション モードで **group-lock** コマンドを使用することにより、トンネルグループだけを介してアクセスするようにリモート ユーザを制限するかどうかを指定します。

```
hostname(config-group-policy)# group-lock {value tunnel-grp-name | none}
hostname(config-group-policy)# no group-lock
hostname(config-group-policy)#
```

**tunnel-grp-name** 変数は、セキュリティ アプライアンスがユーザの接続に関して要求する既存のトンネルグループの名前を指定します。**group-lock** は、VPN クライアントで設定されたグループが、そのユーザが割り当てられているトンネルグループと同じかどうかをチェックすることによって、ユーザを制限します。同じでない場合、セキュリティ アプライアンスはそのユーザによる接続を禁

止します。group-lock を設定しない場合、セキュリティ アプライアンスは割り当てられているグループを考慮せずに、ユーザを認証します。グループ ロックはデフォルトでディセーブルになっています。

**group-lock** アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、値を別のグループポリシーから継承できます。

group-lock をディセーブルにするには、**none** キーワードを指定して **group-lock** コマンドを入力します。none キーワードにより、group-lock はヌル値に設定され、group-lock の制限が拒否されます。また、デフォルトまたは指定されたグループポリシーから group-lock の値が継承されなくなります。

**ステップ 5** 完全転送秘密をイネーブルにするかどうかを指定します。IPSec ネゴシエーションでは、完全転送秘密により、新しい各暗号キーは以前のどのキーとも関連性がないことが保証されます。グループポリシーは、別のグループポリシーから完全転送秘密の値を継承できます。完全転送秘密は、デフォルトではディセーブルになっています。完全転送秘密をイネーブルにするには、グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **pfs** コマンドを使用します。

```
hostname(config-group-policy)# pfs {enable | disable}
hostname(config-group-policy)#
```

完全転送秘密をディセーブルにするには、**disable** キーワードを指定して **pfs** コマンドを入力します。

完全転送秘密アトリビュートを実行コンフィギュレーションから削除して、値を継承しないようにするには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no pfs
hostname(config-group-policy)#
```

## バナー メッセージの設定

バナーまたは初期メッセージを表示する場合は、それを指定します。デフォルトではバナーは表示されません。指定したメッセージは、リモート クライアントが接続したときに、そのクライアントに表示されます。バナーを指定するには、グループポリシー コンフィギュレーション モードで **banner** コマンドを入力します。バナー テキストの長さは 510 文字までです。復帰を入力するには、「\n」シーケンスを入力します。



(注)

バナー内の復帰改行は、2 文字として数えられます。

バナーを削除するには、このコマンドの **no** 形式を入力します。このコマンドの **no** 形式を使用すると、グループポリシーのすべてのバナーが削除されることに注意してください。

グループポリシーは、別のグループポリシーからこの値を継承できます。値を継承しないようにするには、次のように、バナー文字列の値を指定する代わりに **none** キーワードを入力します。

```
hostname(config-group-policy)# banner {value banner_string | none}
```

次の例は、FirstGroup という名前のグループポリシーにバナーを作成する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems 7.0.
```

## IPSec-UDP アトリビュートの設定

IPSec over UDP (IPSec through NAT と呼ばれることもあります) を使用すると、Cisco VPN クライアントまたはハードウェア クライアントは、NAT を実行しているセキュリティ アプライアンスに UDP 経由で接続することができます。この機能はデフォルトでディセーブルになっています。IPSec over UDP は、リモートアクセス接続にのみ適用される専用の機能で、モード コンフィギュレーションが必要です。セキュリティ アプライアンスは、SA のネゴシエート時にクライアントとの間でコンフィギュレーション パラメータをやり取りします。IPSec over UDP を使用すると、システムのパフォーマンスがわずかに低下する場合があります。

IPSec over UDP をイネーブルにするには、グループポリシー コンフィギュレーション モードで、**ipsec-udp** コマンドに **enable** キーワードを指定します。

```
hostname(config-group-policy)# ipsec-udp {enable | disable}
hostname(config-group-policy)# no ipsec-udp
```

IPSec over UDP を使用するには、次のように **ipsec-udp-port** コマンドも設定する必要があります。

IPSec over UDP をディセーブルにするには、**disable** キーワードを入力します。IPSec over UDP のアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、IPSec over UDP の値を別のグループポリシーから継承できます。

また、IPSec over UDP を使用するように Cisco VPN クライアントを設定しておく必要があります (Cisco VPN クライアントは、デフォルトで IPSec over UDP を使用するように設定されています)。VPN 3002 では、IPSec over UDP を使用するためのコンフィギュレーションは必要ありません。

次の例は、FirstGroup という名前のグループポリシーに IPSec over UDP を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

IPSec over UDP をイネーブルにした場合は、グループポリシー コンフィギュレーション モードで **ipsec-udp-port** コマンドも設定する必要があります。このコマンドにより、IPSec over UDP 用の UDP ポート番号が設定されます。IPSec ネゴシエーションでは、セキュリティ アプライアンスは設定されたポートでリスンし、他のフィルタ規則で UDP トラフィックがドロップされていても、そのポート宛ての UDP トラフィックを転送します。ポート番号の範囲は 4001 ~ 49151 です。デフォルトのポート値は 10000 です。

UDP ポート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。これにより、IPSec over UDP のポート値を別のグループポリシーから継承できます。

```
hostname(config-group-policy)# ipsec-udp-port port
```

次の例は、FirstGroup という名前のグループポリシーの IPSec UDP ポートをポート 4025 に設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```



## スプリット トンネリング アトリビュートの設定

スプリット トンネリングを使用すると、リモートアクセス IPsec クライアントは、条件に応じて、パケットを暗号化された形式で IPsec トンネルを介して誘導したり、クリア テキスト形式でネットワーク インターフェイスに誘導したりすることができます。スプリット トンネリングがイネーブルになっている場合、IPsec トンネルの相手側を宛先としないパケットを暗号化する必要はありません。このようなパケットはトンネル上を復号化された状態で送信され、その後、最終的な宛先にルーティングされます。このコマンドは、このスプリット トンネリング ポリシーを特定のネットワークに適用します。

### スプリット トンネリング ポリシーの設定

スプリット トンネリング ポリシーを指定して、トラフィックのトンネリング規則を設定します。

```
hostname(config-group-policy)# split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}  
hostname(config-group-policy)# no split-tunnel-policy
```

デフォルトでは、すべてのトラフィックがトンネリングされます。スプリット トンネリング ポリシーを設定するには、グループポリシー コンフィギュレーション モードで **split-tunnel-policy** コマンドを入力します。**split-tunnel-policy** アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、スプリット トンネリングの値を別のグループポリシーから継承できます。

トラフィックがクリア テキストで送信されるネットワークのリストは、**excludespecified** キーワードで定義します。この機能は、トンネル経由で企業ネットワークに接続しながら、プリンタなどのローカル ネットワーク デバイスにアクセスするリモート ユーザにとって便利です。このオプションは、Cisco VPN クライアントに対してのみ適用されます。

**tunnelall** キーワードを指定すると、すべてのトラフィックがクリア テキストとして送信されなくなるか、セキュリティ アプライアンス以外の宛先に送信されなくなります。この指定では、実質的にスプリット トンネリングはディセーブルになります。リモート ユーザは企業ネットワークを経由してインターネットにアクセスしますが、ローカル ネットワークにはアクセスできません。これがデフォルトのオプションです。

**tunnelspecified** キーワードでは、指定されたネットワークとの間のすべてのトラフィックがトンネリングされます。このオプションにより、スプリット トンネリングはイネーブルになります。このオプションでは、トンネリングするアドレスのネットワーク リストを作成することができます。これ以外のすべてのアドレスに対するデータは、クリア テキストで送信され、リモート ユーザのインターネット サービス プロバイダーによってルーティングされます。



(注)

スプリット トンネリングは主としてトラフィック管理機能であり、セキュリティ機能ではありません。最大限のセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

次の例は、FirstGroup という名前のグループポリシーで、指定されたネットワークのトンネリングに関してだけ、スプリット トンネリング ポリシーを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes  
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
```

## スプリット トンネリング用ネットワーク リストの作成

グループポリシー コンフィギュレーション モードで **split-tunnel-network-list** コマンドを使用して、スプリット トンネリング用のネットワーク リストを作成します。

```
hostname(config-group-policy)# split-tunnel-network-list {value access-list_name | none}
hostname(config-group-policy)# no split-tunnel-network-list value [access-list_name]
```

スプリット トンネリングのネットワーク リストは、トラフィックをトンネル経由で送信する必要のあるネットワークと、トンネリングが不要なネットワークを区別します。セキュリティ アプライアンスは、ネットワーク リストに基づいてスプリット トンネリングを実行するかどうかを決定します。ネットワーク リストは、プライベート ネットワーク上のアドレスのリストで構成された ACL です。標準タイプの ACL のみが許可されます。

**value access-list name** パラメータは、トンネリングを実行する、または実行しないネットワークを列挙したアクセスリストを指定します。

**none** キーワードは、スプリット トンネリング用のネットワーク リストが存在しないことを示し、セキュリティ アプライアンスはすべてのトラフィックをトンネリングします。**none** キーワードを指定すると、スプリット トンネリングのネットワーク リストにヌル値が設定され、スプリット トンネリングが拒否されます。また、これにより、デフォルトまたは指定されたグループポリシーから、デフォルトのスプリット トンネリング ネットワーク リストが継承されなくなります。

ネットワーク リストを削除するには、このコマンドの **no** 形式を入力します。すべてのスプリット トンネリング ネットワーク リストを削除するには、引数を指定せずに **no split-tunnel-network-list** コマンドを入力します。このコマンドにより、**none** キーワードを入力して作成したヌル リストがあればそれも含めて、設定済みのすべてのネットワーク リストが削除されます。

スプリット トンネリングのネットワーク リストが存在しない場合、ユーザはデフォルトまたは指定されたグループポリシー内に存在するネットワーク リストを継承します。ユーザがこのようなネットワーク リストを継承しないようにするには、**split-tunnel-network-list none** コマンドを入力します。

次の例は、FirstGroup という名前のグループポリシーに FirstList という名前のネットワーク リストを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list FirstList
```

## トンネリング用ドメイン アトリビュートの設定

トンネリングされたパケットのデフォルトのドメイン名またはスプリット トンネルを介して解決されるドメインのリストを指定できます。次の各項では、これらのドメインの設定方法について説明します。

### トンネリングされたパケットのデフォルト ドメイン名の設定

セキュリティ アプライアンスは、ドメイン フィールドが省略される DNS クエリーにドメインを追加するために、IPSec クライアントにデフォルトのドメイン名を渡します。デフォルトのドメイン名が存在しない場合、ユーザはデフォルト グループポリシーのドメイン名を継承します。グループポリシーのユーザにデフォルトのドメイン名を指定するには、グループポリシー コンフィギュレーション モードで **default-domain** コマンドを入力します。ドメイン名を削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# default-domain {value domain-name | none}
hostname(config-group-policy)# no default-domain [domain-name]
```

**value domain-name** パラメータは、そのグループのデフォルト ドメイン名を示します。デフォルト ドメイン名が存在しないことを示すには、**none** キーワードを入力します。このコマンドにより、デフォルト ドメイン名にヌル値が設定され、デフォルト ドメイン名が拒否されます。また、デフォルトまたは指定されたグループポリシーからデフォルト ドメイン名が継承されなくなります。

すべてのデフォルト ドメイン名を削除するには、引数を指定せずに **no default-domain** コマンドを入力します。このコマンドにより、**none** キーワードとともに **default-domain** コマンドを入力して作成したヌル リストがあればそれも含めて、設定済みのすべてのデフォルト ドメイン名が削除されます。**no** 形式を使用すると、ドメイン名の継承が許可されます。

次の例は、FirstGroup という名前のグループポリシーに FirstDomain というデフォルト ドメイン名を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

## スプリット トンネリング用ドメインのリストの定義

スプリット トンネルを介して解決されるドメインのリストを入力します。グループポリシー コンフィギュレーション モードで **split-dns** コマンドを入力します。リストを削除するには、このコマンドの **no** 形式を入力します。

スプリット トンネリングのドメイン リストが存在しない場合、ユーザはデフォルト グループポリシー内に存在するリストを継承します。ユーザがこのようなスプリット トンネリング ドメイン リストを継承しないようにするには、**none** キーワードを指定して **split-dns** コマンドを入力します。

すべてのスプリット トンネリング ドメイン リストを削除するには、引数を指定せずに **no split-dns** コマンドを入力します。これにより、**none** キーワードとともに **split-dns** コマンドを発行して作成したヌルリストを含めて、設定済みのすべてのスプリット トンネリング ドメイン リストが削除されます。

パラメータ **value domain-name** は、セキュリティ アプライアンスがスプリット トンネルを介して解決するドメイン名を指定します。**none** キーワードは、スプリット DNS リストが存在しないことを示します。また、このキーワードにより、スプリット DNS リストにヌル値が設定されます。そのため、スプリット DNS リストは拒否され、デフォルトまたは指定されたグループポリシーのスプリット DNS リストが継承されなくなります。このコマンドのシンタックスは次のとおりです。

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2...
domain-nameN] | none}
hostname(config-group-policy)# no split-dns [domain-name domain-name2 domain-nameN]
```

ドメインのリスト内で各エントリを区切るには、スペースを1つ入力します。エントリ数に制限はありませんが、文字列全体で 255 文字を超えることはできません。英数字、ハイフン (-)、およびピリオド (.) のみを使用できます。デフォルトのドメイン名がトンネルを介して解決される場合、その名前をこのリストに明示的に含める必要があります。

次の例は、FirstGroup という名前のグループポリシーで、Domain1、Domain2、Domain3、Domain4 の各ドメインがスプリット トンネリングを介して解決されるように設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

## VPN ハードウェア クライアント用アトリビュートの設定

この項にあるコマンドは、セキュア ユニット認証とユーザ認証をイネーブルまたはディセーブルにし、VPN ハードウェア クライアントのユーザ認証のタイムアウト値を設定します。また、これらのコマンドを使用すると、Cisco IP Phone と LEAP パケットが個々のユーザ認証をバイパスでき、ネットワーク拡張モードを使用するハードウェア クライアントが接続できるようになります。

### セキュア ユニット認証の設定

セキュア ユニット認証は、VPN ハードウェア クライアントがトンネルを開始するたびにユーザ名とパスワードを使用して認証されるようにすることにより、セキュリティを強化します。この機能がイネーブルの場合、ハードウェア クライアントはユーザ名とパスワードを保存しません。セキュア ユニット認証はデフォルトでディセーブルになっています。



(注)

この機能がイネーブルの場合、VPN トンネルを起動するには、ユーザがユーザ名とパスワードを入力する必要があります。

セキュア ユニット認証では、ハードウェア クライアントが使用するトンネルグループに対して認証サーバグループが設定されている必要があります。プライマリ セキュリティ アプライアンスでセキュア ユニット認証を使用する必要がある場合は、すべてのバックアップ サーバにも必ず同じ設定を行ってください。

グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **secure-unit-authentication** コマンドを入力し、セキュア ユニット認証をイネーブルにするかどうかを指定します。

```
hostname(config-group-policy)# secure-unit-authentication {enable | disable}
hostname(config-group-policy)# no secure-unit-authentication
```

セキュア ユニット認証をディセーブルにするには、**disable** キーワードを入力します。セキュア ユニット認証のアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、セキュア ユニット認証の値を別のグループポリシーから継承できます。

次の例は、FirstGroup という名前のグループポリシーでセキュア ユニット認証をイネーブルにする方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

### ユーザ認証の設定

ユーザ認証はデフォルトでディセーブルになっています。ユーザ認証がイネーブルの場合、ハードウェア クライアントの背後の個々のユーザは、トンネルを介してネットワークにアクセスするために認証を受ける必要があります。個々のユーザは、設定した認証サーバの順序に従って認証されます。

グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **user-authentication** コマンドを入力し、ユーザ認証をイネーブルにするかどうかを指定します。

```
hostname(config-group-policy)# user-authentication {enable | disable}
hostname(config-group-policy)# no user-authentication
```

ユーザ認証をディセーブルにするには、**disable** キーワードを入力します。ユーザ認証アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、ユーザ認証の値を別のグループポリシーから継承できます。

プライマリ セキュリティ アプライアンスでユーザ認証を使用する必要がある場合は、すべてのバックアップ サーバにも必ず同じ設定を行ってください。

次の例は、FirstGroup という名前のグループポリシーでユーザ認証をイネーブルにする方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
```

## アイドル タイムアウトの設定

グループポリシー コンフィギュレーション モードで **user-authentication-idle-timeout** コマンドを入力して、ハードウェア クライアントの背後の個々のユーザにアイドル タイムアウトを設定します。アイドル タイムアウト期間中にハードウェア クライアントの背後のユーザによる通信アクティビティがない場合、セキュリティ アプライアンスはそのクライアントのアクセスを終了します。

```
hostname(config-group-policy)# user-authentication-idle-timeout {minutes | none}
hostname(config-group-policy)# no user-authentication-idle-timeout
```



(注)

**user-authentication-idle-timeout** コマンドで終了されるのは、VPN トンネルを経由したクライアントのアクセスだけであり、VPN トンネル自体は終了されません。

*minutes* パラメータには、アイドル タイムアウト期間の長さを分単位で指定します。最小値は 1 分、デフォルト値は 30 分、最大値は 35791394 分です。

アイドル タイムアウト値を削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、アイドル タイムアウト値を別のグループポリシーから継承できます。

アイドル タイムアウト値を継承しないようにするには、**none** キーワードを指定して **user-authentication-idle-timeout** コマンドを入力します。このコマンドにより、アイドル タイムアウトにヌル値が設定されます。この設定によってアイドル タイムアウトが拒否され、デフォルトまたは指定されたグループポリシーからユーザ認証のアイドル タイムアウト値が継承されなくなります。

次の例は、FirstGroup という名前のグループポリシーに 45 分の アイドル タイムアウト値を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication-idle-timeout 45
```

## IP Phone Bypass の設定

Cisco IP Phone は、ハードウェア クライアントの背後の個々のユーザ認証をバイパスさせることができます。IP Phone Bypass をイネーブルにするには、グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **ip-phone-bypass** コマンドを入力します。IP Phone Bypass を使用すると、ハードウェア クライアントの背後の IP Phone はユーザ認証プロセスを実行しなくても接続が可能になります。IP Phone Bypass は、デフォルトでディセーブルになっています。イネーブルの場合、セキュア ユニット認証は有効なままになります。

IP Phone Bypass をディセーブルにするには、**disable** キーワードを入力します。IP Phone Bypass アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、IP Phone Bypass の値を別のグループポリシーから継承できます。

```
hostname(config-group-policy)# ip-phone-bypass {enable | disable}
hostname(config-group-policy)# no ip-phone-bypass
```

## LEAP Bypass の設定

LEAP Bypass がイネーブルの場合、VPN 3002 ハードウェア クライアントの背後の無線デバイスからの LEAP パケットは、ユーザ認証の前に VPN トンネルを通過します。このアクションにより、シスコの無線アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立し、その後、ユーザ単位で再度認証を実行することができます。LEAP Bypass は、デフォルトでディセーブルになっています。

シスコの無線アクセス ポイントからの LEAP パケットが個々のユーザ認証をバイパスできるようにするには、グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **leap-bypass** コマンドを入力します。LEAP Bypass をディセーブルにするには、**disable** キーワードを入力します。LEAP Bypass のアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、LEAP Bypass の値を別のグループポリシーから継承できます。

```
hostname(config-group-policy)# leap-bypass {enable | disable}
hostname(config-group-policy)# no leap-bypass
```



(注)

IEEE 802.1X は、有線および無線ネットワークにおける認証規格です。この規格では、クライアントと認証サーバの間で強力な相互認証を実現し、ユーザ単位およびセッション単位のダイナミックな無線暗号化秘密 (WEP) キーの使用を可能にして、スタティックな WEP キーの場合に介在する面倒な管理作業やセキュリティ上の問題を軽減することができます。

シスコシステムズは、Cisco LEAP と呼ばれる 802.1X 無線認証タイプを開発しました。LEAP (Lightweight Extensible Authentication Protocol) は、無線クライアントと RADIUS サーバの間の接続における相互認証を実装します。パスワードなど、認証に使用されるクレデンシャルは、無線メディア上で送信される前に必ず暗号化されます。

Cisco LEAP では、無線クライアントを RADIUS サーバに対して認証します。RADIUS アカウンティングサービスは提供されません。

対話的なハードウェア クライアント認証をイネーブルにしている場合、この機能は意図したように動作しません。



注意

認証されていないトラフィックがトンネルを通過できるようにすると、ネットワークにセキュリティ リスクを招く恐れがあります。

次の例は、FirstGroup という名前のグループポリシーに LEAP Bypass を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# leap-bypass enable
```

## ネットワーク拡張モードのイネーブル化

ネットワーク拡張モードを使用すると、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することができます。ハードウェア クライアントの背後のプライベート ネットワークからセキュリティ アプライアンスの背後のネットワークへのすべてのトラフィックは、IPSec でカプセル化されます。PAT は適用されません。したがって、セキュリティ アプライアンスの背後のデバイスは、トンネル経由でのみハードウェア クライアントの背後にあるプライベート ネットワーク上のデバイスに直接アクセスでき、逆方向の場合も同様にトンネル経由の場合にのみ可能になります。トンネルは、ハードウェア クライアントから開始する必要がありますが、トンネルの確立後はどちらの側からデータ交換を開始してもかまいません。

グループポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **nem** コマンドを入力し、ハードウェア クライアントの ネットワーク拡張モードをイネーブルにします。

```
hostname(config-group-policy)# nem {enable | disable}
hostname(config-group-policy)# no nem
```

NEM をディセーブルにするには、**disable** キーワードを入力します。この NEM のアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、値を別のグループポリシーから継承できます。

次の例は、FirstGroup という名前のグループポリシーに NEM を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
```

## バックアップ サーバアトリビュートの設定

バックアップ サーバを設定します（使用する予定がある場合）。IPSec バックアップ サーバを使用すると、VPN クライアントはプライマリ セキュリティ アプライアンスが使用不可の場合も接続が可能になります。バックアップサーバを設定すると、セキュリティ アプライアンスは、IPSec トンネルを確立するときにクライアントにサーバリストを渡します。バックアップサーバは、クライアントまたはプライマリ セキュリティ アプライアンスにその設定を行うまでは存在しません。

バックアップサーバは、クライアントまたはプライマリ セキュリティ アプライアンスのいずれかに設定します。セキュリティ アプライアンスにバックアップサーバを設定すると、セキュリティ アプライアンスはバックアップサーバ ポリシーをグループ内のクライアントに配信し、クライアントにバックアップサーバリストが設定されている場合はそのリストを置き換えます。



(注)

ホスト名を使用している場合は、バックアップ用の DNS サーバおよび WINS サーバを、プライマリの DNS サーバおよび WINS サーバと異なるネットワーク上に配置することを推奨します。このようにしないと、ハードウェア クライアントの背後のクライアントが DHCP 経由でそのハードウェア クライアントから DNS および WINS の情報を取得している場合に、プライマリ サーバへの接続が失われると、バックアップサーバに別の DNS および WINS の情報があっても、クライアントは DHCP リースの期限が満了するまではアップデートされなくなります。また、ホスト名を使用している場合に DNS サーバが使用不可になると、大幅な遅延が発生する恐れがあります。

バックアップサーバを設定するには、グループポリシー コンフィギュレーション モードで **backup-servers** コマンドを入力します。

```
hostname(config-group-policy)# backup-servers {server1 server2... server10 |
clear-client-config | keep-client-config}
```

バックアップサーバを削除するには、バックアップサーバを指定してこのコマンドの **no** 形式を入力します。backup-servers アトリビュートを実行コンフィギュレーションから削除し、backup-servers の値を他のグループポリシーから継承できるようにするには、引数を指定せずにこのコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no backup-servers [server1 server2... server10 |
clear-client-config | keep-client-config]
```

**clear-client-config** キーワードは、クライアントでバックアップサーバを使用しないことを指定します。セキュリティ アプライアンスはヌルのサーバリストを配信します。

**keep-client-config** キーワードは、セキュリティ アプライアンスがバックアップサーバ情報をクライアントに送信しないことを指定します。クライアントは、そのクライアントのサーバリストを使用します（設定されている場合）。これがデフォルトです。

server1 server 2.... server10 パラメータ リストは、プライマリ セキュリティ アプライアンスが使用不可の場合に VPN クライアントが使用するサーバを、プライオリティ順にスペースで区切ったリストです。このリストには、サーバを IP アドレスまたはホスト名で指定します。このリストの長さは 500 文字までで、格納できるエントリは 10 個までです。

次の例は、FirstGroup という名前のグループポリシーに、IP アドレスが 10.10.10.1 と 192.168.10.14 であるバックアップサーバを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

## ファイアウォール ポリシーの設定

ファイアウォールは、データの個々の着信パケットと発信パケットをそれぞれ検査して、パケットを許可するかドロップするかどうか決定することにより、コンピュータをインターネットから分離して保護します。ファイアウォールは、グループのリモート ユーザがスプリット トンネリングを設定してある場合、セキュリティの向上をもたらします。この場合、ファイアウォールは、インターネットまたはユーザのローカル LAN を経由する侵入からユーザの PC を保護することで、企業ネットワークを保護します。VPN クライアントを使用してセキュリティ アプライアンスに接続しているリモート ユーザは、適切なファイアウォール オプションを選択できます。

グループポリシー コンフィギュレーション モードで **client-firewall** コマンドを使用して、セキュリティ アプライアンスが IKE トンネル ネゴシエーション中に VPN クライアントに配信するパーソナル ファイアウォール ポリシーを設定します。ファイアウォール ポリシーを削除するには、このコマンドの **no** 形式を入力します。

すべてのファイアウォール ポリシーを削除するには、引数を指定せずに **no client-firewall** コマンドを入力します。このコマンドにより、**none** キーワードとともに **client-firewall** コマンドを入力して作成したヌル ポリシーがあればそれも含めて、設定済みのすべてのファイアウォール ポリシーが削除されます。

ファイアウォール ポリシーが存在しない場合、ユーザはデフォルトまたはその他のグループポリシー内に存在するファイアウォール ポリシーを継承します。ユーザがこのようなファイアウォール ポリシーを継承しないようにするには、**none** キーワードを指定して **client-firewall** コマンドを入力します。

Add or Edit Group Policy ウィンドウ、Client Firewall タブでは、追加または変更するグループポリシーに対して VPN クライアントのファイアウォール設定を指定できます。





(注)

これらのファイアウォール機能を使用できるのは、Microsoft Windows を実行する VPN クライアントだけです。現在、ハードウェア クライアントまたは他の（Windows 以外の）ソフトウェア クライアントでは、これらの機能は使用できません。

最初のシナリオでは、リモート ユーザの PC 上にパーソナル ファイアウォールがインストールされています。VPN クライアントは、ローカル ファイアウォールで定義されているファイアウォールポリシーを適用し、そのファイアウォールが実行されていることを確認するために監視します。ファイアウォールの実行が停止すると、VPN クライアントはセキュリティ アプライアンスへの通信をドロップします（このファイアウォール適用メカニズムは、*Are You There (AYT)* と呼ばれます。VPN クライアントが、定期的に「are you there?」メッセージを送信することによってファイアウォールを監視するからです。応答が返されない場合、VPN クライアントは、ファイアウォールがダウンしてセキュリティ アプライアンスへの接続が終了したことを認識します）。ネットワーク管理者がこれらの PC ファイアウォールを独自に設定する場合がありますが、この方法を使用すれば、ユーザは各自の設定をカスタマイズできます。

第 2 のシナリオでは、VPN クライアント PC のパーソナル ファイアウォールに中央集中型ファイアウォールポリシーを適用することが選択されることがあります。一般的な例としては、スプリットトンネリングを使用してグループのリモート PC へのインターネットトラフィックをブロックすることがあげられます。この方法は、トンネルが確立されている間、インターネット経由の侵入から PC を保護するので、中央サイトも保護されます。このファイアウォールのシナリオは、*プッシュポリシー*または *Central Protection Policy (CPP)* と呼ばれます。セキュリティ アプライアンスでは、VPN クライアントに適用するトラフィック管理規則のセットを作成し、これらの規則をフィルタに関連付けて、そのフィルタをファイアウォールポリシーに指定します。セキュリティ アプライアンスは、このポリシーを VPN クライアントまで配信します。その後、VPN クライアントはポリシーをローカル ファイアウォールに渡し、そこでポリシーが適用されます。

次のコマンドを入力して、適切なクライアント ファイアウォールのパラメータを設定します。このコマンドに設定できるインスタンスは 1 つだけです。この一連のコマンドの後に記載された表 26-1 で、これらのコマンドのシンタックス要素について説明します。

## Cisco 統合ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-integrated acl-in ACL  
acl-out ACL
```

## Cisco Security Agent

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-security-agent
```

## ファイアウォールなし

```
hostname(config-group-policy)# client-firewall none
```

## カスタム ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} custom vendor-id num  
product-id num policy {AYT | CPP acl-in ACL acl-out ACL} [description string]
```

## ZoneLabs ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarm policy
{AYT | CPP acl-in ACL acl-out ACL}

hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarmpro
policy {AYT | CPP acl-in ACL acl-out ACL}

client-firewall {opt | req} zonelabs-zonealarmpro policy {AYT | CPP acl-in ACL acl-out
ACL}
```

## Sygate Personal ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal

hostname(config-group-policy)# client-firewall {opt | req} sygate-personal-pro

hostname(config-group-policy)# client-firewall {opt | req} sygate-security-agent
```

## Network ICE、Black ICE ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} networkkice-blackkice
```

表 26-1 client-firewall コマンドのキーワードと変数

| パラメータ                 | 説明                                                                                                                                                                 |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acl-in ACL            | クライアントが着信トラフィックに使用するポリシーを指定します。                                                                                                                                    |
| acl-out ACL           | クライアントが発信トラフィックに使用するポリシーを指定します。                                                                                                                                    |
| AYT                   | クライアント PC のファイアウォール アプリケーションがファイアウォール ポリシーを制御するように指定します。セキュリティ アプライアンスはファイアウォールが実行されていることを確認します。セキュリティ アプライアンスは、確認のために「Are You There?」という質問を行い、応答がない場合はトンネルを切断します。 |
| cisco-integrated      | Cisco 統合ファイアウォール タイプを指定します。                                                                                                                                        |
| cisco-security-agent  | Cisco Intrusion Prevention Security Agent ファイアウォール タイプを指定します。                                                                                                      |
| CPP                   | VPN クライアントのファイアウォール ポリシーのソースとして Policy Pushed を指定します。                                                                                                              |
| custom                | カスタム ファイアウォール タイプを指定します。                                                                                                                                           |
| description string    | ファイアウォールの説明です。                                                                                                                                                     |
| networkkice-blackkice | Network ICE Black ICE ファイアウォール タイプを指定します。                                                                                                                          |
| none                  | クライアント ファイアウォール ポリシーが存在しないことを示します。ファイアウォール ポリシーにヌル値を設定して、ファイアウォール ポリシーを拒否します。デフォルトのグループポリシーまたは指定されているグループポリシーからファイアウォール ポリシーを継承しないようにします。                          |
| opt                   | オプションのファイアウォール タイプを示します。                                                                                                                                           |
| product-id            | ファイアウォール製品を指定します。                                                                                                                                                  |
| req                   | 必要なファイアウォール タイプを示します。                                                                                                                                              |
| sygate-personal       | Sygate Personal ファイアウォール タイプを指定します。                                                                                                                                |

表 26-1 client-firewall コマンドのキーワードと変数 (続き)

| パラメータ                          | 説明                                              |
|--------------------------------|-------------------------------------------------|
| sygate-personal-pro            | Sygate Personal Pro ファイアウォール タイプを指定します。         |
| sygate-security-agent          | Sygate Security Agent ファイアウォール タイプを指定します。       |
| vendor-id                      | ファイアウォール ベンダーを指定します。                            |
| zonelabs-zonealarm             | Zone Labs ZoneAlarm ファイアウォール タイプを指定します。         |
| zonelabs-zonealarmorpro policy | Zone Labs ZoneAlarm または Pro ファイアウォール タイプを指定します。 |
| zonelabs-zonealarmpro policy   | Zone Labs ZoneAlarm Pro ファイアウォール タイプを指定します。     |

次の例は、FirstGroup という名前のグループポリシーで、Cisco Intrusion Prevention Security Agent を必要とするクライアント ファイアウォール ポリシーを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
hostname(config-group-policy)#
```

## クライアント アクセス規則の設定

グループポリシー コンフィギュレーション モードで **client-access-rule** コマンドを使用して、セキュリティ アプライアンスを介して IPSec で接続できるリモートアクセス クライアントのタイプとバージョンを制限する規則を指定します。次のガイドラインに従って規則を作成します。

- 規則を定義しない場合、セキュリティ アプライアンスはすべての接続タイプを許可します。
- クライアントがどの規則にも一致しない場合、セキュリティ アプライアンスは接続を拒否します。拒否規則を定義する場合は、許可規則も 1 つ以上定義しないと、セキュリティ アプライアンスはすべての接続を拒否します。
- ソフトウェア クライアントとハードウェア クライアントのどちらでも、タイプとバージョンは **show vpn-sessiondb remote** で表示される内容と完全に一致している必要があります。
- \* 文字はワイルドカードです。各規則で複数回入力することができます。たとえば、**client-access rule 3 deny type \* version 3.\*** では、バージョン 3.x のソフトウェア リリースを実行しているすべてのクライアント タイプを拒否する、プライオリティ 3 のクライアント アクセス規則が作成されます。
- グループポリシーごとに最大 25 の規則を作成できます。
- 規則のセット全体で 255 文字の制限があります。
- クライアントのタイプまたはバージョン (あるいはその両方) を送信しないクライアントには、n/a を入力できます。

規則を削除するには、このコマンドの **no** 形式を入力します。このコマンドは、次のコマンドと同等です。

```
hostname(config-group-policy)# client-access-rule 1 deny type "Cisco VPN Client"
version 4.0
```

すべての規則を削除するには、引数を指定せずに **no client-access-rule** コマンドを入力します。これにより、**none** キーワードとともに **client-access-rule** コマンドを発行して作成したヌル規則があればそれも含めて、設定済みのすべての規則が削除されます。

デフォルトでは、アクセス規則はありません。クライアント アクセス規則が存在しない場合、ユーザはデフォルト グループポリシー内に存在する規則を継承します。

ユーザがクライアント アクセス規則を継承しないようにするには、**none** キーワードを指定して **client-access-rule** コマンドを入力します。このコマンドの結果、すべてのタイプとバージョンのクライアントが接続できるようになります。

```
hostname(config-group-policy)# client-access rule priority {permit | deny} type type version {version | none}
```

```
hostname(config-group-policy)# no client-access rule [priority {permit | deny} type type version version]
```

表 26-2 で、これらのコマンドのキーワードとパラメータの意味を説明します。

**表 26-2 client-access rule コマンドのキーワードと変数**

| パラメータ                  | 説明                                                                                                                                                 |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>deny</b>            | 特定のタイプまたはバージョン（あるいはその両方）のデバイスの接続を拒否します。                                                                                                            |
| <b>none</b>            | クライアント アクセス規則を許可しません。client-access-rule をヌル値に設定して、制限を拒否します。デフォルトのグループポリシーまたは指定されているグループポリシーから値を継承しないようにします。                                        |
| <b>permit</b>          | 特定のタイプまたはバージョン（あるいはその両方）のデバイスの接続を許可します。                                                                                                            |
| <b>priority</b>        | 規則のプライオリティを決定します。最小の整数値を持つ規則のプライオリティが最も高くなります。したがって、クライアントのタイプまたはバージョン（あるいはその両方）に一致し、最小の整数値を持つ規則が適用されます。それよりもプライオリティの低い規則は、セキュリティ アプライアンスでは無視されます。 |
| <b>type type</b>       | デバイス タイプを、「VPN 3002」などの自由形式の文字列で指定します。文字列は、 <b>show vpn-sessiondb remote</b> で表示される内容と完全に一致している必要があります。ただし、ワイルドカードとして * 文字を入力できます。                 |
| <b>version version</b> | デバイスのバージョンを、「7.0」などの自由形式の文字列で指定します。文字列は、 <b>show vpn-sessiondb remote</b> で表示される内容と完全に一致している必要があります。ただし、ワイルドカードとして * 文字を入力できます。                    |

次の例は、FirstGroup という名前のグループポリシーにクライアント アクセス規則を作成する方法を示しています。これらの規則は、バージョン 4.x のソフトウェアを実行する Cisco VPN クライアントを許可し、すべての Windows NT クライアントを拒否します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 deny type WinNT version *
hostname(config-group-policy)# client-access-rule 2 permit "Cisco VPN Client" version 4.*
```



**(注)**

「type」フィールドは、任意の値が許可される自由形式の文字列ですが、その値は、クライアントが接続時にセキュリティ アプライアンスに送信する固定値と一致している必要があります。

## グループポリシーの WebVPN アトリビュートの設定

WebVPN によってユーザは、ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモートアクセス VPN トンネルを確立できます。ソフトウェア クライアントもハードウェア クライアントも必要ありません。WebVPN を使用することで、HTTPS インターネット サイトにアクセスできるほとんどすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできます。WebVPN は SSL およびその後継である TLS1 を使用して、リモートユーザと、中央サイトで設定した特定のサポートされている内部リソースとの間で、セキュアな接続を提供します。セキュリティ アプライアンスはプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。WebVPN は、デフォルトではディセーブルになっています。

特定の内部グループポリシー用の WebVPN コンフィギュレーションをカスタマイズできます。



(注)

グローバル コンフィギュレーション モードで `webvpn` モードを入力することによって、WebVPN のグローバル設定を構成できます。この項で説明する `webvpn` モード（グループポリシー コンフィギュレーション モードから入る `webvpn` モード）を使用すると、特定のグループポリシーの WebVPN コンフィギュレーションをカスタマイズできます。

グループポリシーの `webvpn` コンフィギュレーション モードでは、すべての機能の設定を継承するか、または次のパラメータをカスタマイズするかどうかを指定できます。各パラメータについては、後述のステップで説明します。

- `functions`
- `customizations`
- `html-content-filter`
- `homepage`
- `filter`
- `url-list`
- `port-forward`
- `port-forward-name`
- `sso server` (single-signon server)
- `auto-signon`
- `deny message`
- `SSL VPN Client` (SVC)
- `keep-alive ignore`

多くの場合、WebVPN の設定の一部として WebVPN アトリビュートを定義した後、グループポリシーの `webvpn` アトリビュートを設定するときにこれらの定義を特定のグループに適用します。グループポリシーの コンフィギュレーション モードで `webvpn` コマンドを使用して、グループポリシーの `webvpn` コンフィギュレーション モードに入ります。グループポリシー用の `webvpn` コマンドは、ファイル、MAPI プロキシ、URL、および TCP アプリケーションへの WebVPN 経由のアクセスを定義します。フィルタリングする ACL とトラフィックの種類も特定します。WebVPN は、デフォルトではディセーブルになっています。WebVPN アトリビュートの設定の詳細については、『Cisco Security Appliance Command Line Configuration Guide』および『Cisco Security Appliance Command Reference』を参照してください。

グループポリシーの webvpn コンフィギュレーション モードで入力されたすべてのコマンドを削除するには、このコマンドの **no** 形式を入力します。これらの webvpn コマンドは、設定を行ったユーザ名またはグループポリシーに対して適用されます。

```
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# no webvpn
```

電子メール プロキシを使用するために WebVPN を設定する必要はありません。

次の例は、FirstGroup という名前のグループポリシーの webvpn コンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#
```

## グループポリシーの WebVPN 機能アトリビュートの設定

イネーブルにする WebVPN 機能を設定します。グループポリシーに対して、WebVPN を使用した、ファイル アクセスとファイル ブラウジング、HTTP プロキシ、MAPI プロキシ、および URL エントリを設定するには、webvpn モードで **functions** コマンドを入力します。これらの機能は、デフォルトではディセーブルです。

```
hostname(config-group-webvpn)# functions {auto-download | citrix | file-access |
file-browsing | file-entry | filter | http-proxy | mapi | none | port-forward |
url-entry}
```

設定した機能を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。機能の値を継承しないようにするには、**functions none** コマンドを入力します。

**functions none** コマンドを発行して作成したヌル値を含めて、設定済みのすべての機能を削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。

```
hostname(config-group-webvpn)# no functions [auto-download | citrix | file-access |
file-browsing | file-entry | filter | http-proxy | mapi | none | port-forward |
url-entry]
```

このコマンドで使用するキーワードの意味を、[表 26-3](#) で説明します。

**表 26-3 functions コマンドのキーワード**

| キーワード                | 意味                                                                                                                                         |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>auto-download</b> | ポート転送アプレットを自動的にダウンロードします。                                                                                                                  |
| <b>citrix</b>        | Citrix をイネーブルにします。                                                                                                                         |
| <b>file-access</b>   | ファイル アクセスをイネーブルまたはディセーブルにします。イネーブルにすると、WebVPN ホーム ページにサーバリストのファイル サーバが表示されます。ファイル ブラウジングまたはファイル エントリをイネーブルにするには、ファイル アクセスをイネーブルにする必要があります。 |
| <b>file-browsing</b> | ファイル サーバとファイル共有のブラウジングをイネーブルまたはディセーブルにします。ファイル サーバのユーザ エントリを許可するには、ファイル ブラウジングをイネーブルにする必要があります。                                            |
| <b>file-entry</b>    | ユーザがファイル サーバの名前を入力する機能をイネーブルまたはディセーブルにします。                                                                                                 |
| <b>filter</b>        | webtype アクセスリストを適用します。                                                                                                                     |

表 26-3 functions コマンドのキーワード (続き)

| キーワード               | 意味                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>http-proxy</b>   | HTTP アプレット プロキシのクライアントへの転送をイネーブルまたはディセーブルにします。プロキシは、Java、ActiveX、Flash など、適切なマングリングを妨げる技術に対して有用です。セキュリティ アプライアンスの使用を継続しながら、マングリングをバイパスします。転送プロキシは、ブラウザの古いプロキシ コンフィギュレーションを自動的に変更し、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、Java など、実質的にすべてのクライアント サイド技術をサポートします。サポートされるブラウザは Microsoft Internet Explorer だけです。 |
| <b>mapi</b>         | Microsoft Outlook/Exchange のポート転送をイネーブルまたはディセーブルにします。                                                                                                                                                                                                                                                                                                           |
| <b>none</b>         | すべての WebVPN の <b>functions</b> にヌルを設定します。デフォルトのグループポリシーまたは指定されているグループポリシーから機能を継承しないようにします。                                                                                                                                                                                                                                                                      |
| <b>port-forward</b> | ポート転送をイネーブルにします。                                                                                                                                                                                                                                                                                                                                                |
| <b>url-entry</b>    | ユーザの URL エントリをイネーブルまたはディセーブルにします。イネーブルにしても、セキュリティ アプライアンスは設定されている URL またはネットワーク ACL で、URL を制限します。URL エントリをディセーブルにすると、セキュリティ アプライアンスは、WebVPN ユーザがホームページの URL にのみアクセスできるように制限します。                                                                                                                                                                                 |

次の例は、FirstGroup という名前のグループポリシーに対して、ファイル アクセス、ファイル ブラウジング、および MAPI プロキシを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# functions file-access file-browsing MAPI
hostname(config-group-webvpn)#
```

## カスタマイゼーションの適用

カスタマイゼーションは、ログイン時にユーザに表示されるウィンドウの内容を決定します。カスタマイゼーション パラメータは、WebVPN 設定の一部として指定します。以前定義した Web ページ カスタマイゼーションを適用して、ログイン時にユーザに表示される Web ページのルックアンドフィールを変更するには、ユーザ名の webvpn コンフィギュレーション モードで customization コマンドを入力します。

```
hostname(config-group-webvpn)# customization customization_name
hostname(config-group-webvpn)#
```

たとえば、blueborder という名前のカスタマイゼーションを使用する場合、次のコマンドを入力します。

```
hostname(config-group-webvpn)# customization blueborder
hostname(config-group-webvpn)#
```

## 「拒否」メッセージの指定

Web VPN に正しくログインしたリモート ユーザに送信されるメッセージを指定できます。リモート ユーザが VPN 特権を持たない場合は、グループポリシーの webvpn コンフィギュレーションモードで **deny-message** コマンドを入力すると、リモート ユーザに送信されるメッセージを指定できます。

```
hostname(config-group-webvpn)# deny-message value "message"
hostname(config-group-webvpn)# no deny-message value "message"
hostname(config-group-webvpn)# deny-message none
```

**no deny-message value** コマンドは、リモート ユーザがメッセージを受信しないように、メッセージ文字列を削除します。

**no deny-message none** コマンドは、トンネルグループのポリシー コンフィギュレーションからアトリビュートを削除します。このポリシーはアトリビュート値を継承します。

メッセージには、最長で特殊文字、スペース、および句読点を含めて英数字 491 文字を使用できますが、囲みの引用符はカウントされません。ログイン時には、リモート ユーザのブラウザにテキストが表示されます。**deny-message value** コマンドに文字列を入力しているときは、コマンドがラップしても入力が続けてください。

デフォルトの拒否メッセージは、「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features.Contact your IT administrator for more information.」です。

次の例の最初のコマンドは、Group2 という名前の内部グループポリシーを作成します。後続のコマンドは、そのポリシーに関連付けられている webvpn 拒否メッセージが含まれたアトリビュートを変更します。

```
hostname(config)# group-policy group2 internal
hostname(config)# group-policy group2 attributes
hostname(config-group)# webvpn
hostname(config-group-webvpn)# deny-message value "Your login credentials are OK.
However, you have not been granted rights to use the VPN features. Contact your
administrator for more information."
hostname(config-group-webvpn)
```

## グループポリシーの WebVPN フィルタ アトリビュートの設定

webvpn モードで **html-content-filter** コマンドを使用して、このグループポリシーの WebVPN セッションの Java、ActiveX、イメージ、スクリプト、およびクッキーをフィルタリングするかどうかを指定します。HTML フィルタリングは、デフォルトでディセーブルです。

コンテンツ フィルタを削除するには、このコマンドの **no** 形式を入力します。**none** キーワードとともに **html-content-filter** コマンドを発行して作成したヌル値を含めて、すべてのコンテンツ フィルタを削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。HTML コンテンツ フィルタを継承しないようにするには、**none** キーワードを指定して **html-content-filter** コマンドを入力します。

コマンドを 2 回使用すると、先行する設定値が上書きされます。

```
hostname(config-group-webvpn)# html-content-filter {java | images | scripts | cookies
| none}

hostname(config-group-webvpn)# no html-content-filter [java | images | scripts |
cookies | none]
```



このコマンドで使用するキーワードの意味を、表 26-4 で説明します。

表 26-4 filter コマンドのキーワード

| キーワード          | 意味                                                                   |
|----------------|----------------------------------------------------------------------|
| <b>cookies</b> | イメージからクッキーを削除して、アドバタイズメント フィルタリングを制限し、プライバシーを保持します。                  |
| <b>images</b>  | イメージへの参照を削除します (<IMG> タグを削除)。                                        |
| <b>java</b>    | Java および ActiveX への参照を削除します (<EMBED>、<APPLET>、および <OBJECT> の各タグを削除)。 |
| <b>none</b>    | フィルタリングを実行しないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリングの値を継承しないようにします。  |
| <b>scripts</b> | スクリプトへの参照を削除します (<SCRIPT> タグを削除)。                                    |

次の例は、FirstGroup という名前のグループポリシーに、Java と ActiveX、クッキー、およびイメージのフィルタリングを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# html-content-filter java cookies images
hostname(config-group-webvpn)#
```

## ユーザ ホームページの指定

グループポリシーの webvpn コンフィギュレーション モードで **homepage** コマンドを使用して、このグループのユーザのログイン時に表示される Web ページの URL を指定します。デフォルトのホーム ページはありません。

**homepage none** コマンドを発行して作成したヌル値を含めて、設定されているホームページを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。ホーム ページを継承しないようにするには、**homepage none** コマンドを入力します。

**none** キーワードは、WebVPN ホームページがないことを示します。これにより、ヌル値が設定されてホーム ページが拒否され、ホーム ページが継承されなくなります。

キーワード **value** の後ろの **url-string** 変数で、ホームページの URL を指定します。文字列の先頭は、**http://** または **https://** にする必要があります。

```
hostname(config-group-webvpn)# homepage {value url-string | none}
hostname(config-group-webvpn)# no homepage
hostname(config-group-webvpn)#
```

## 自動サインオンの設定

**auto-signon** コマンドは、WebVPN ユーザ用のシングル サインオン方式です。NTLM 認証、基本認証、またはその両方を使用する認証のために WebVPN ログイン クレデンシャル（ユーザ名とパスワード）を内部サーバに渡します。複数の **auto-signon** コマンドを入力でき、コマンドは入力順序に従って処理されます（先に入力されたコマンドが優先されます）。

自動サインオン機能は、webvpn コンフィギュレーション、webvpn グループ コンフィギュレーション、または webvpn ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。ユーザ名はグループに優先し、グループはグローバルに優先するという標準的な優先動作が適用されます。選択するモードは、使用する認証の対象範囲によって異なります。

特定のサーバへの特定のユーザの自動サインオンをディセーブルにするには、元の IP ブロックまたは URI を指定してこのコマンドの **no** 形式を使用します。すべてのサーバへの認証をディセーブルにするには、引数を指定しないで **no** 形式を使用します。**no** オプションを使用すると、値をグループポリシーから継承できます。

次の例では、webvpn コンフィギュレーション モードで入力し、基本認証を使用して、10.1.1.0 から 10.1.1.255 の範囲の IP アドレスを持つサーバへの anyuser という名前のユーザの自動サインオンを設定します。

次の例では、基本認証または NTLM 認証を使用して、Web VPN ユーザの ExamplePolicy グループに対し、URI マスク https://\*.example.com/\* で定義されたサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type
all
hostname(config-group-webvpn)#
```

次の例では、基本認証または NTLM 認証を使用して、Web VPN ユーザの ExamplePolicy2 グループに対し、サブネット マスク 255.255.255.0 を使用する IP アドレス 10.1.1.0 のサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type
all
hostname(config-group-webvpn)#
```

## WebVPN 接続に使用するアクセスリストの指定

webvpn モードで **filter** コマンドを使用して、このグループポリシーまたはユーザ名で WebVPN 接続に使用するアクセスリストの名前を指定します。**filter** コマンドを入力して指定するまで、WebVPN アクセスリストは適用されません。

**filter none** コマンドを発行して作成したヌル値を含めて、アクセスリストを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。フィルタの値を継承しないようにするには、**filter value none** コマンドを入力します。

**filter** コマンドを入力して指定するまで、WebVPN アクセスリストは適用されません。

ACL を設定して、このグループポリシーについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**filter** コマンドを入力して、これらの ACL を WebVPN トラフィックに適用します。

```
hostname(config-group-webvpn)# filter {value ACLname | none}
hostname(config-group-webvpn)# no filter
```

**none** キーワードは、webvpntype アクセスリストがないことを示します。これにより、ヌル値が設定されてアクセスリストが拒否され、別のグループポリシーからアクセスリストが継承されなくなります。

キーワード **value** の後ろの ACLname 文字列で、すでに設定されているアクセスリストの名前を指定します。



(注)

**functions** コマンドでは、**filter** を選択しておく必要があります。WebVPN は、**vpn-filter** コマンドで定義されている ACL を使用しません。

次の例は、FirstGroup という名前のグループポリシーに対して `acl_in` という名前のアクセスリストを呼び出すフィルタを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# filter acl_in
hostname(config-group-webvpn)#
```

## URL リストの適用

グループポリシーの WebVPN ホームページに URL のリストを表示するように指定できます。最初に、グローバル コンフィギュレーション モードで `url-list` コマンドを入力して 1 つ以上の名前付きリストを作成する必要があります。特定のグループポリシーに WebVPN サーバと URL のリストを適用して、特定のグループポリシーのリストにある URL にアクセスできるようにするには、グループポリシーの `webvpn` コンフィギュレーションモードに入って、`url-list` コマンドを実行する際に、作成するリストの名前を使用します。デフォルトの URL リストはありません。

`url-list none` コマンドを使用して作成したヌル値を含めて、リストを削除するには、このコマンドの `no` 形式を使用します。`no` オプションを使用すると、値を別のグループポリシーから継承できます。URL リストを継承しないようにするには、`url-list none` コマンドを入力します。コマンドを 2 回使用すると、先行する設定値が上書きされます。

```
hostname(config-group-webvpn)# url-list {value name | none} [index]
hostname(config-group-webvpn)# no url-list
```

表 26-5 に、`url-list` コマンドのパラメータと意味を示します。

表 26-5 url-list コマンドのキーワードと変数

| パラメータ                   | 意味                                                                                                    |
|-------------------------|-------------------------------------------------------------------------------------------------------|
| <code>index</code>      | ホームページでの表示優先順位を示します。                                                                                  |
| <code>none</code>       | URL リストにヌル値を設定します。デフォルトのグループポリシーまたは指定されているグループポリシーからリストを継承しないようにします。                                  |
| <code>value name</code> | 事前に設定されている URL のリストの名前を指定します。そのようなリストを設定するには、グローバル コンフィギュレーション モードで <code>url-list</code> コマンドを使用します。 |

次の例では、FirstGroup という名前のグループポリシーに FirstGroupURLs という名前の URL リストを設定し、これがホームページに表示される最初の URL リストになるように指定します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# url-list value FirstGroupURLs 1
hostname(config-group-webvpn)#
```

## グループポリシーの WebVPN アプリケーション アクセスのイネーブル化

このユーザの WebVPN アプリケーション アクセスをイネーブルにするには、グループポリシーの `webvpn` コンフィギュレーション モードで `port-forward` コマンドを入力します。ポート転送は、デフォルトではディセーブルになっています。

グループポリシーの `webvpn` コンフィギュレーション モードで `port-forward` コマンドを入力し、アプリケーション アクセスをイネーブルにする前に、WebVPN 接続でユーザが使用できるアプリケーションのリストを定義する必要があります。グローバル コンフィギュレーション モードで `port-forward` コマンドを入力し、このリストを定義します。

`port-forward none` コマンドを発行して作成したヌル値を含めて、コンフィギュレーションからポート転送アトリビュートを削除するには、このコマンドの `no` 形式を入力します。`no` オプションを使用すると、リストを別のグループポリシーから継承できます。ポート転送リストを継承しないようにするには、`none` キーワードを指定して `port-forward` コマンドを入力します。`none` キーワードは、フィルタリングが実行されないことを示します。これにより、ヌル値が設定されてフィルタリングが拒否され、フィルタリング値が継承されなくなります。

このコマンドのシンタックスは次のとおりです。

```
hostname(config-group-webvpn)# port-forward {value listname | none}
hostname(config-group-webvpn)# no port-forward
```

キーワード **value** の後ろの *listname* 文字列で、WebVPN ユーザがアクセスできるアプリケーションのリストを指定します。`webvpn` コンフィギュレーション モードで `port-forward` コマンドを入力し、このリストを定義します。

コマンドを 2 回使用すると、先行する設定値が上書きされます。

次の例は、*FirstGroup* という名前の内部グループポリシーに *ports1* というポート転送リストを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward value ports1
hostname(config-group-webvpn)#
```

## ポート転送表示名の設定

グループポリシーの `webvpn` コンフィギュレーション モードで `port-forward-name` コマンドを使用して、特定のユーザまたはグループポリシーでエンド ユーザへの TCP ポート転送を識別する表示名を設定します。`port-forward-name none` コマンドを使用して作成したヌル値を含めて、表示名を削除するには、コマンドの `no` 形式を入力します。`no` オプションは、デフォルト名の Application Access を復元します。表示名を使用しないようにするには、`port-forward none` コマンドを入力します。このコマンドのシンタックスは次のとおりです。

```
hostname(config-group-webvpn)# port-forward-name {value name | none}
hostname(config-group-webvpn)# no port-forward-name
```

次の例は、*FirstGroup* という名前の内部グループポリシーに Remote Access TCP Applications という名前を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
hostname(config-group-webvpn)#
```

## セッション タイマー更新のために無視する最大オブジェクト サイズの設定

ネットワーク デバイスは、短いキープアライブ メッセージを交換して、デバイス間の仮想回線が引き続きアクティブであることを確認します。これらのメッセージの長さは異なる可能性があります。**keep-alive-ignore** コマンドを使用すると、指定したサイズ以下のすべてのメッセージをキープアライブ メッセージと見なし、セッション タイマーの更新時にトラフィックと見なさないようセキュリティ アプライアンスに指示できます。範囲は 0 ～ 900 KB です。デフォルトは 4 KB です。

トランザクションごとに無視する HTTP/HTTPS トラフィックの上限を指定するには、グループポリシー アトリビュートの webvpn コンフィギュレーション モードで **keep-alive-ignore** コマンドを使用します。

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#
```

The **no** form of the command removes this specification from the configuration:

```
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

次の例では、無視するオブジェクトの最大サイズを 5 KB に設定します。

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

## SSO サーバの指定

WebVPN だけに使用できるシングル サインオンのサポートを使用すると、ユーザはユーザ名とパスワードを複数回入力しなくても、さまざまなサーバのセキュア各種のサービスにアクセスできます。**sso-server value** コマンドをグループポリシーの webvpn モードで入力すると、SSO サーバをグループポリシーに割り当てることができます。

SSO サーバをグループポリシーに割り当てするには、グループポリシーの webvpn コンフィギュレーション モードで **sso-server value** コマンドを入力します。このコマンドは、コンフィギュレーションに CA SiteMinder コマンドが含まれていることを必要とします。

```
hostname(config-group-webvpn)# sso-server value server_name
hostname(config-group-webvpn)#
```

この割り当てを削除してデフォルト ポリシーを使用するには、このコマンドの **no** 形式を使用します。デフォルト ポリシーを継承しないようにするには、**sso-server none** コマンドを入力します。

```
hostname(config-group-webvpn)# sso-server {value server_name | none}
hostname(config-group-webvpn)# [no] sso-server value server_name
```

SSO サーバに割り当てられているデフォルト ポリシーは DfltGrpPolicy です。

次の例では、グループポリシー「my-sso-grp-pol」を作成して、「example」という名前の SSO サーバに割り当てます。

```
hostname(config)# group-policy my-sso-grp-pol internal
hostname(config)# group-policy my-sso-grp-pol attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# sso-server value example
hostname(config-group-webvpn)#
```

## SVC の設定

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 をインストールして設定しなくても、リモート ユーザが IPSec VPN クライアントの利点を活用できる VPN トンネリング テクノロジーです。SVC は、リモート コンピュータの既存の 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。

SVC セッションを確立するには、リモート ユーザはセキュリティ アプライアンスの WebVPN インターフェイスの IP アドレスをブラウザに入力します。ブラウザはそのインターフェイスに接続して WebVPN のログイン画面を表示します。ユーザがログインと認証を完了し、ユーザが SVC を必要としていることをセキュリティ アプライアンスが確認すると、セキュリティ アプライアンスは SVC をリモート コンピュータにダウンロードします。セキュリティ アプライアンスが、SVC を使用するオプションがユーザにあると確認した場合、セキュリティ アプライアンスは、SVC のインストールをスキップするリンクをユーザ画面に表示するとともに、SVC をリモート コンピュータにダウンロードします。

ダウンロードが完了すると、SVC は自動的にインストールと設定を実行します。接続が切断されると (設定に応じて)、SVC はリモート コンピュータに保持されるか、またはリモート コンピュータからアンインストールされます。

セキュリティ アプライアンスは、さまざまなリモート コンピュータのオペレーティング システム用に、複数の独自の SVC イメージをキャッシュ メモリ内に備えている場合もあります。ユーザが接続を試みると、セキュリティ アプライアンスは、イメージとオペレーティング システムが一致するまで引き続きこれらのイメージの部分をリモート コンピュータにダウンロードできます。一致した時点で、SVC 全体をダウンロードします。接続のセットアップ時間を短縮するため、ダウンロードされる最初のイメージが、最もよく遭遇するリモート コンピュータのオペレーティング システムになるように SVC イメージの順序を指定できます。SVC のインストールと使用の詳細については、第 31 章「SSL VPN クライアントの設定」を参照してください。

第 31 章「SSL VPN クライアントの設定」に示すように、SVC をイネーブルにした後は、特定のグループの SVC 機能をイネーブルまたは必須にできます。この機能は、デフォルトでディセーブルになっています。SVC をイネーブルまたは必須にすると、この項で説明している一連の svc コマンドをイネーブルにできます。SVC とその関連する svc コマンドをイネーブルにするには、グループポリシーの webvpn コンフィギュレーション モードで次の手順を実行します。

- ステップ 1** セキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードできるようにするには、**svc enable** コマンドを入力します。このコマンドは、デフォルトではディセーブルになっています。セキュリティ アプライアンスは SVC ファイルをダウンロードしません。このコンフィギュレーションから **svc enable** コマンドを削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-webvpn) # svc {none | enable | required}
hostname(config-group-webvpn) #
```



(注)

**no svc enable** コマンドを入力しても、アクティブな SVC セッションは終了しません。

```
hostname(config) # group-policy sales attributes
hostname(config-group-policy) # webvpn
hostname(config-group-webvpn) # svc enable
hostname(config-group-webvpn) #
```

**ステップ 2** SVC 接続経由で特定のグループについて HTTP データの圧縮をイネーブルにするには、`svc compression` コマンドを入力します。SVC 圧縮は、デフォルトで **deflate**（イネーブル）に設定されています。特定のグループの圧縮をディセーブルにするには、**none** キーワードを使用します。`svc compression` コマンドを削除して値が継承されるようにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-webvpn)# svc compression {deflate | none}
hostname(config-group-webvpn)#
```

次の例では、`sales` という名前のグループポリシーの SVC 圧縮をディセーブルにします。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc compression none
hostname(config-group-webvpn)#
```

**ステップ 3** セキュリティ アプライアンスで `dead-peer-detection` (DPD) をイネーブルにして、SVC またはセキュリティ アプライアンスが DPD を実行する頻度を設定するには、`svc dpd-interval` コマンドを使用します。このコンフィギュレーションから `svc dpd-interval` コマンドを削除するには、このコマンドの **no** 形式を使用します。このグループの SVC DPD をディセーブルにするには、**none** キーワードを使用します。

```
hostname(config-group-webvpn)# svc dpd-interval {[gateway {seconds | none}] | [client {seconds | none}]}
hostname(config-group-webvpn)#
```

DPD チェックは、デフォルトでディセーブルになっています。

ゲートウェイは、セキュリティ アプライアンスのことです。セキュリティ アプライアンスが DPD テストを実行する頻度を、30 ～ 3600 秒（1 時間）の範囲で指定できます。**none** を指定すると、セキュリティ アプライアンスが実行する DPD テストはディセーブルになります。

クライアントは、SVC のことです。クライアントが DPD テストを実行する頻度を、30 ～ 3600 秒（1 時間）の範囲で指定できます。**none** を指定すると、クライアントが実行する DPD テストはディセーブルになります。

次の例では、`sales` という名前の既存のグループポリシーについて、セキュリティ アプライアンス（ゲートウェイ）によって実行される DPD の頻度を 3000 秒に設定し、クライアントによって実行される DPD の頻度を 1000 秒に設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc dpd-interval gateway 3000
hostname(config-group-webvpn)# svc dpd-interval client 1000
hostname(config-group-webvpn)#
```

**ステップ 4** 接続のアイドル状態を維持できる時間をデバイスが制限している場合でも、プロキシ、ファイアウォール、または NAT デバイスを通じて SVC 接続のオープン状態を維持するように、キープアライブ メッセージの頻度を調整できます（`seconds` で指定）。

頻度を調整することで、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケットベースのアプリケーションをアクティブに実行していない場合でも、SVC が切断して再接続をしないようにできます。

リモート コンピュータ上の SVC がキープアライブ メッセージをセキュリティ アプライアンスに送信する頻度（15 ～ 600 秒）を設定するには、**svc keepalive** コマンドを使用します。コンフィギュレーションからこのコマンドを削除して値が継承されるようにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-webvpn)# svc keepalive {none | seconds}
hostname(config-group-webvpn)# no svc keepalive {none | seconds}
hostname(config-group-webvpn)#
```

SVC キープアライブは、デフォルトでディセーブルになっています。キーワード **none** を使用すると SVC キープアライブ メッセージがディセーブルになります。

次の例では、SVC がキープアライブ メッセージを 300 秒（5 分）の頻度で送信できるようにセキュリティ アプライアンスを設定します。

```
hostname(config-group-webvpn)# svc keepalive 300
hostname(config-group-webvpn)#
```

**ステップ 5** SVC がリモート コンピュータに永続的にインストールされた状態を保つには、**installed** キーワードを指定して **svc keep-installer** コマンドを使用します。コマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-webvpn)# svc keep-installer {installed | none}
hostname(config-group-webvpn)# no svc keep-installer {installed | none}
hostname(config-group-webvpn)#
```

デフォルトでは、SVC の永続的インストールがディセーブルになっています。SVC セッションの終わりに、SVC はリモートコンピュータからアンインストールされます。

次の例では、このグループのリモート コンピュータの SVC インストール状態を維持するようにセキュリティ アプライアンスを設定します。

```
hostname(config-group-webvpn)# svc keep-installer installed
hostname(config-group-webvpn)#
```

**ステップ 6** SVC が SVC セッションでキーの再生成を実行できるようにするには、**svc rekey** コマンドを使用します。キーの再生成をディセーブルにして、コマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-webvpn)# svc rekey {method {ssl | new-tunnel} | time minutes | none}
hostname(config-group-webvpn)# no svc rekey {method {ssl | new-tunnel} | time minutes | none}
hostname(config-group-webvpn)#
```

SVC キーの再生成は、デフォルトでディセーブルになっています。

方式を **new-tunnel** に指定すると、SVC キーの再生成中に SVC が新しいトンネルを確立することが指定されます。方式を **none** に指定すると、SVC キーの再生成はディセーブルになります。方式を **ssl** に指定すると、SSL の再ネゴシエーションは SVC キーの再生成中に行われます。方式を指定する代わりに、セッションの開始からキーの再生成が行われるまでの時間を 1 ～ 10080（1 週間）の分数で指定できます。

次の例で示すように、コマンドが **no** 形式の場合は、必要なのは最小限だけです。

```
hostname(config-username-webvpn)# no svc rekey method
hostname(config-username-webvpn)#
```



ただし、方式を `new-tunnel` に指定する場合は、次のようになります。

```
hostname(config-username-webvpn)# no svc rekey method new-tunnel  
hostname(config-username-webvpn)#
```

しかし、現在の方式は `ssl` であり、値が一致しないためにコマンドは失敗します。

次の例では、キーの再生成中に SVC が SSL と再ネゴシエートするように設定し、キーの再生成がセッション開始の 30 分後に発生するように設定します。

```
hostname(config-group-webvpn)# svc rekey method ssl  
hostname(config-group-webvpn)# svc rekey time 30  
hostname(config-group-webvpn)#
```

---

## ユーザアトリビュートの設定

この項では、ユーザアトリビュートとその設定方法について説明します。ここでは、次の項目について説明します。

- [ユーザ名のコンフィギュレーションの表示 \(P.26-60\)](#)
- [特定ユーザのアトリビュートの設定 \(P.26-61\)](#)

デフォルトでは、ユーザは、割り当てられているグループポリシーからすべてのユーザアトリビュートを継承します。また、セキュリティアプライアンスでは、ユーザレベルで個別にアトリビュートを割り当て、そのユーザに適用されるグループポリシーの値を上書きすることができます。たとえば、すべてのユーザに営業時間内のアクセスを許可し、特定のユーザに 24 時間のアクセスを許可するグループポリシーを指定することができます。

## ユーザ名のコンフィギュレーションの表示

すべてのユーザ名のコンフィギュレーションを、グループポリシーから継承したデフォルト値も含めて表示するには、次のように、**all** キーワードを指定して **show running-config username** コマンドを入力します。

```
hostname# show running-config all username
hostname#
```

**all** キーワードを省略すると、明示的に設定された値だけがリストに表示されます。この例では、ユーザ名は **testuser** と **ppurkm** です。継承した値も含めて、これらの設定済みのユーザのコンフィギュレーションは、次のとおりです。

```
username testuser password 12RsxXQnphyr/I9Z encrypted privilege 15
username testuser attributes
  vpn-group-policy testing
  vpn-access-hours value averylongtime
  vpn-simultaneous-logins 4
  vpn-idle-timeout 30
  vpn-session-timeout none
  vpn-filter value tunneled
  no vpn-framed-ip-address
  group-lock value test
webvpn
  no functions
  html-content-filter java images scripts cookies
  no homepage
  no filter
  no url-list
  no port-forward
  no port-forward-name

username ppurkm password vt/qqEzfgfrXXya4 encrypted privilege 2
username ppurkm attributes
  no vpn-group-policy
  vpn-tunnel-protocol webvpn
  no vpn-framed-ip-address
webvpn
  functions url-entry file-access file-entry file-browsing
  no html-content-filter
  no homepage
  no filter
  no url-list
  no port-forward
  no port-forward-name

username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15
username newuser nopassword privilege 15
```

## 特定ユーザのアトリビュートの設定

特定のユーザを設定するには、**username** コマンドを使用してユーザ名モードに入り、ユーザにパスワード（パスワードなしも可）とアトリビュートを割り当てます。指定しなかったすべてのアトリビュートは、グループポリシーから継承されます。

内部ユーザ認証データベースは、**username** コマンドを使用して入力されたユーザで構成されています。**login** コマンドは、このデータベースを認証に使用します。セキュリティ アプライアンスのデータベースにユーザを追加するには、グローバル コンフィギュレーション モードで **username** コマンドを入力します。ユーザを削除するには、このコマンドの **no** 形式を使用して削除するユーザ名を指定します。すべてのユーザ名を削除するには、ユーザ名を指定せずに **clear configure username** コマンドを使用します。

## ユーザのパスワードと特権レベルの設定

ユーザにパスワードと特権レベルを割り当てるには、**username** コマンドを入力します。**nopassword** キーワードを入力して、そのユーザにパスワードが不要であることを指定することもできます。パスワードを指定する場合は、そのパスワードを暗号化形式で保存するかどうかを指定できます。

オプションの **privilege** キーワードにより、そのユーザの特権レベルを設定できます。特権レベルの範囲は 0（最低）～ 15 です。一般に、システム管理者は最高の特権レベルを持ちます。デフォルトのレベルは 2 です。

```
hostname(config)# username name {nopassword | password password [encrypted]}  
[privilege priv_level]  
  
hostname(config)# no username [name]
```

表 26-6 で、このコマンドで使用するキーワードと変数の意味を説明します。

表 26-6 username コマンドのキーワードと変数

| キーワード / 変数                  | 意味                                                                                                                          |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>encrypted</b>            | パスワードの暗号化を指定します。                                                                                                            |
| <b>name</b>                 | ユーザの名前を指定します。                                                                                                               |
| <b>nopassword</b>           | このユーザにパスワードが不要であることを指定します。                                                                                                  |
| <b>password password</b>    | このユーザにパスワードが存在することを示し、パスワードを指定します。                                                                                          |
| <b>privilege priv_level</b> | このユーザの特権レベルを設定します。範囲は 0 ～ 15 です。この数値が低いほど、コマンドの使用やセキュリティ アプライアンスの管理に関する機能が限定されます。デフォルトの特権レベルは 2 です。システム管理者の通常の特権レベルは 15 です。 |

デフォルトでは、このコマンドで追加する VPN ユーザにはアトリビュートやグループポリシーは関連付けられません。すべての値を明示的に設定する必要があります。

次の例は、暗号化されたパスワードが pw\_12345678 で、特権レベルが 12 の anyuser という名前のユーザを設定する方法を示しています。

```
hostname(config)# username anyuser password pw_12345678 encrypted privilege 12  
hostname(config)#
```

## ユーザアトリビュートの設定

ユーザのパスワード（存在する場合）と特権レベルの設定後は、その他のアトリビュートを設定します。これらは任意の順序で設定できます。任意のアトリビュートと値のペアを削除するには、該当コマンドの **no** 形式を入力します。

**attributes** キーワードを指定して **username** コマンドを入力し、ユーザ名モードに入ります。

```
hostname(config)# username name attributes
hostname(config-username)#
```

プロンプトが変化し、新しいモードになったことが示されます。これでアトリビュートを設定できます。

## VPN ユーザアトリビュートの設定

VPN ユーザアトリビュートは、次の項で説明するように、VPN 接続に固有の値を設定します。

### 継承の設定

ユーザが、それまでにユーザレベルで設定されていないアトリビュートの値をグループポリシーから継承するようにできます。このユーザがアトリビュートを継承するグループポリシーの名前を指定するには、**vpn-group-policy** コマンドを入力します。デフォルトでは、VPN ユーザにはグループポリシーが関連付けられていません。

```
hostname(config-username)# vpn-group-policy group-policy-name
hostname(config-username)# no vpn-group-policy group-policy-name
```

ユーザ名モードで利用できるアトリビュートの場合、ユーザ名モードでアトリビュートを設定すると、特定のユーザに関してグループポリシーにおけるそのアトリビュートの値を上書きできます。

次の例は、anyuser という名前のユーザが FirstGroup という名前のグループポリシーのアトリビュートを使用するように設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
hostname(config-username)#
```

### アクセス時間の設定

設定済みの time-range ポリシーの名前を指定して、このユーザがシステムへのアクセスを許可される時間を関連付けます。

このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。このオプションを使用すると、time-range の値を別のグループポリシーから継承できます。値を継承しないようにするには、**vpn-access-hours none** コマンドを入力します。デフォルトでは、アクセスは無制限です。

```
hostname(config-username)# vpn-access-hours value {time-range | none}
hostname(config-username)# vpn-access-hours value none
hostname(config)#
```

次の例は、anyuser という名前のユーザを 824 と呼ばれる time-range ポリシーに関連付ける方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-access-hours 824
hostname(config-username)#
```

## 最大同時ログイン数の設定

このユーザに許可される同時ログインの最大数を指定します。範囲は 0 ～ 2147483647 です。デフォルトの同時ログイン数は 3 です。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。

```
hostname(config-username)# vpn-simultaneous-logins integer
hostname(config-username)# no vpn-simultaneous-logins
hostname(config-username)#
```



(注)

同時ログインに最大数の制限はありませんが、複数の同時ログインの許可がセキュリティの低下を招き、パフォーマンスに影響を及ぼす恐れがあります。

次の例は、anyuser という名前のユーザに最大 4 つの同時ログインを許可する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-simultaneous-logins 4
hostname(config-username)#
```

## アイドル タイムアウトの設定

アイドル タイムアウト期間を分単位で指定するか、**none** を入力してアイドル タイムアウトをディセーブルにします。この期間中に接続上で通信アクティビティがまったくなかった場合、セキュリティ アプライアンスは接続を終了します。

範囲は 1 ～ 35791394 分です。デフォルトは 30 分です。無制限のタイムアウト期間を許可し、タイムアウト値を継承しないようにするには、**none** キーワードを指定して **vpn-idle-timeout** コマンドを入力します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-idle-timeout {minutes | none}
hostname(config-username)# no vpn-idle-timeout
hostname(config-username)#
```

次の例は、anyuser という名前のユーザに 30 分の VPN アイドル タイムアウトを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout 30
hostname(config-username)#
```

## 最大接続時間の設定

ユーザの最大接続時間を分単位で指定するか、**none** を入力して無制限の接続時間を許可し、このアトリビュートの値を継承しないようにします。この期間が終了すると、セキュリティ アプライアンスは接続を終了します。

範囲は 1 ～ 35791394 分です。デフォルトのタイムアウトはありません。無制限のタイムアウト期間を許可し、タイムアウト値を継承しないようにするには、**none** キーワードを指定して **vpn-session-timeout** コマンドを入力します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-session-timeout {minutes | none}
hostname(config-username)# no vpn-session-timeout
hostname(config-username)#
```

次の例は、anyuser という名前のユーザに 180 分の VPN セッション タイムアウトを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180
hostname(config-username)#
```

## ACL フィルタの適用

VPN 接続用のフィルタとして使用する、事前に設定されたユーザ固有の ACL の名前を指定します。アクセスリストを拒否し、グループポリシーからアクセスリストを継承しないようにするには、**none** キーワードを指定して **vpn-filter** コマンドを入力します。**vpn-filter none** コマンドを発行して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループポリシーから継承できます。このコマンドには、デフォルトの動作や値はありません。

ACL を設定して、このユーザについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**vpn-filter** コマンドを使用して、これらの ACL を適用します。

```
hostname(config-username)# vpn-filter {value ACL name | none}
hostname(config-username)# no vpn-filter
hostname(config-username)#
```



(注)

**functions** コマンドには、**filter** を選択しておく必要があります。WebVPN は、**vpn-filter** コマンドで定義されている ACL を使用しません。

次の例は、anyuser という名前のユーザに対して acl\_vpn という名前のアクセスリストを呼び出すフィルタを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-filter value acl_vpn
hostname(config-username)#
```

## IP アドレスとネットマスクの指定

特定のユーザに割り当てる IP アドレスとネットマスクを指定します。IP アドレスを削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-framed-ip-address {ip_address}
hostname(config-username)# no vpn-framed-ip-address
hostname(config-username)
```

次の例は、anyuser という名前のユーザに IP アドレス 10.92.166.7 を設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
hostname(config-username)
```

前の手順で指定した IP アドレスに使用するネットワーク マスクを指定します。

**no vpn-framed-ip-address** コマンドを使用した場合は、ネットワーク マスクを指定しないでください。サブネット マスクを削除するには、このコマンドの **no** 形式を入力します。デフォルトの動作や値はありません。

```
hostname(config-username)# vpn-framed-ip-netmask {netmask}
hostname(config-username)# no vpn-framed-ip-netmask
hostname(config-username)
```

次の例は、anyuser という名前のユーザに、サブネット マスク 255.255.255.254 を設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
hostname(config-username)
```

## トンネル プロトコルの指定

このユーザが使用できる VPN トンネル タイプ (IPSec または WebVPN) を指定します。デフォルトは、デフォルト グループポリシーから取得される値で、IPSec になります。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-username)# vpn-tunnel-protocol {webvpn | IPSec}
hostname(config-username)# no vpn-tunnel-protocol [webvpn | IPSec]
hostname(config-username)
```

このコマンドのパラメータの値は、次のとおりです。

- **IPSec** : 2 つのピア (リモートアクセス クライアントまたは別のセキュア ゲートウェイ) 間の IPSec トンネルをネゴシエートします。認証、暗号化、カプセル化、キー管理を制御するセキュリティ アソシエーションを作成します。
- **webvpn** : HTTP 対応 Web ブラウザ経由でリモート ユーザに VPN サービスを提供します。クライアントは不要です。

このコマンドを入力して、1 つ以上のトンネリング モードを設定します。VPN トンネルで接続するユーザに対して、1 つ以上のトンネリング モードを設定する必要があります。

次の例は、anyuser という名前のユーザに WebVPN および IPSec トンネリング モードを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-tunnel-protocol webvpn
hostname(config-username)# vpn-tunnel-protocol IPSec
hostname(config-username)
```

## リモート ユーザ アクセスの制限

**value** キーワードを指定して **group-lock** アトリビュートを設定することにより、指定した既存のトンネルグループだけを介してアクセスするようにリモート ユーザを制限します。**group-lock** は、VPN クライアントで設定されたグループが、そのユーザが割り当てられているトンネルグループと同じかどうかをチェックすることによって、ユーザを制限します。同じでない場合、セキュリティ アプライアンスはそのユーザによる接続を禁止します。**group-lock** を設定しない場合、セキュリティ アプライアンスは割り当てられているグループを考慮せずに、ユーザを認証します。

**group-lock** アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、値をグループポリシーから継承できます。**group-lock** をディセーブルにし、デフォルトまたは指定されたグループポリシーから **group-lock** の値を継承しないようにするには、**none** キーワードを指定して **group-lock** コマンドを入力します。

```
hostname(config-username)# group-lock {value tunnel-grp-name | none}
hostname(config-username)# no group-lock
hostname(config-username)
```

次の例は、anyuser という名前のユーザにグループ ロックを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# group-lock value tunnel group name
hostname(config-username)
```

## ソフトウェア クライアント ユーザのパスワード保存のイネーブル化

ユーザがログイン パスワードをクライアント システム上に保存するかどうかを指定します。パスワード保存は、デフォルトでディセーブルになっています。パスワード保存は、セキュアなサイトにあることがわかっているシステムでだけ、イネーブルにします。パスワード保存をディセーブルにするには、**disable** キーワードを指定して **password-storage** コマンドを入力します。**password-storage** アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。これにより、**password-storage** の値をグループポリシーから継承できます。

```
hostname(config-username)# password-storage {enable | disable}
hostname(config-username)# no password-storage
hostname(config-username)
```

このコマンドは、対話的なハードウェア クライアント認証やハードウェア クライアントの個別ユーザ認証では動作しません。

次の例は、anyuser という名前のユーザでパスワード保存をイネーブルにする方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# password-storage enable
hostname(config-username)
```

## 特定ユーザの WebVPN の設定

次の各項では、特定のユーザの WebVPN 設定をカスタマイズする方法について説明します。ユーザ名のコンフィギュレーション モードで **webvpn** コマンドを使用して、ユーザ名の **webvpn** コンフィギュレーション モードに入ります。WebVPN によってユーザは、ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモートアクセス VPN トンネルを確立できます。ソフトウェア クライアントもハードウェア クライアントも必要ありません。WebVPN を使用することで、HTTPS インターネット サイトにアクセスできるほとんどすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできます。WebVPN は SSL およびその後継である TLS1 を使用して、リモート ユーザと、中央サイトで設定した特定のサポートされて



いる内部リソースとの間で、セキュアな接続を提供します。セキュリティ アプライアンスはプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

ユーザ名の webvpn コンフィギュレーション モード コマンドは、ファイル、MAPI プロキシ、URL、および TCP アプリケーションへの WebVPN 経由のアクセスを定義します。フィルタリングする ACL とトラフィックの種類も特定します。WebVPN は、デフォルトではディセーブルになっています。これらの **webvpn** コマンドは、設定を行ったユーザ名に適用されます。プロンプトが変化して、ユーザ名の webvpn コンフィギュレーション モードに入ったことがわかります。

```
hostname(config-username)# webvpn  
hostname(config-username-webvpn)#
```

ユーザ名の webvpn コンフィギュレーション モードで入力されたすべてのコマンドを削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-username)# no webvpn  
hostname(config-username)#
```

電子メール プロキシを使用するために WebVPN を設定する必要はありません。



(注)

グローバル コンフィギュレーション モードで webvpn モードを入力することによって、WebVPN のグローバル設定を構成できます。この項で説明した、ユーザ名モードから入ったユーザ名の webvpn コンフィギュレーション モードを使用すると、特定のユーザの WebVPN コンフィギュレーション をカスタマイズできます。

ユーザ名の webvpn コンフィギュレーション モードでは、次のパラメータをカスタマイズできます。各パラメータについては、後述のステップで説明します。

- functions
- customizations
- deny message
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- sso server (single-signon server)
- auto-signon
- SSL VPN Client (SVC)
- keep-alive ignore

次の例は、ユーザ名 anyuser のアトリビュートのユーザ名の webvpn コンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# username anyuser attributes  
hostname(config-username)# webvpn  
hostname(config-username-webvpn)#
```

## イネーブルにする WebVPN 機能の設定

このユーザに対して、WebVPN を使用した、WebVPN 機能のファイル アクセスとファイル ブラウジング、HTTP プロキシ、MAPI プロキシ、および URL エントリを設定するには、ユーザ名の webvpn コンフィギュレーション モードで **functions** コマンドを入力します。設定した機能を削除するには、このコマンドの **no** 形式を入力します。これらの機能は、デフォルトではディセーブルです。

**functions none** コマンドを発行して作成したヌル値を含めて、設定済みのすべての機能を削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。機能の値を継承しないようにするには、**functions none** コマンドを入力します。

```
hostname(config-username-webvpn)# functions {auto-download | citrix | file-access |
file-browsing | file-entry | filter | http-proxy | mapi | none | port-forward |
url-entry}
```

```
hostname(config-username-webvpn)# no functions [auto-download | citrix | file-access |
file-browsing | file-entry | filter | http-proxy | mapi | none | port-forward |
url-entry]
```

表 26-7 で、このコマンドで使用するキーワードの意味を次の表で説明します。

表 26-7 functions コマンドのキーワード

| キーワード         | 意味                                                                                                                                                                                                                                                                                                                                                              |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| auto-download | ポート転送アプレットを自動的にダウンロードします。                                                                                                                                                                                                                                                                                                                                       |
| citrix        | Citrix をイネーブルにします。                                                                                                                                                                                                                                                                                                                                              |
| file-access   | ファイル アクセスをイネーブルまたはディセーブルにします。イネーブルにすると、WebVPN ホーム ページにサーバリストのファイル サーバが表示されます。ファイル ブラウジングまたはファイル エントリをイネーブルにするには、ファイル アクセスをイネーブルにする必要があります。                                                                                                                                                                                                                      |
| file-browsing | ファイル サーバとファイル共有のブラウジングをイネーブルまたはディセーブルにします。ファイル サーバのユーザ エントリを許可するには、ファイル ブラウジングをイネーブルにする必要があります。                                                                                                                                                                                                                                                                 |
| file-entry    | ユーザがファイル サーバの名前を入力する機能をイネーブルまたはディセーブルにします。                                                                                                                                                                                                                                                                                                                      |
| filter        | webtype アクセスリストを適用します。                                                                                                                                                                                                                                                                                                                                          |
| http-proxy    | HTTP アプレット プロキシのクライアントへの転送をイネーブルまたはディセーブルにします。プロキシは、Java、ActiveX、Flash など、適切なマングリングを妨げる技術に対して有効です。セキュリティ アプライアンスの使用を継続しながら、マングリングをバイパスします。転送プロキシは、ブラウザの古いプロキシ コンフィギュレーションを自動的に変更し、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、Java など、実質的にすべてのクライアント サイド技術をサポートします。サポートされるブラウザは Microsoft Internet Explorer だけです。 |
| mapi          | Microsoft Outlook/Exchange のポート転送をイネーブルまたはディセーブルにします。                                                                                                                                                                                                                                                                                                           |
| none          | すべての WebVPN の <b>functions</b> にヌルを設定します。デフォルトのグループポリシーまたは指定されているグループポリシーから機能を継承しないようにします。                                                                                                                                                                                                                                                                      |

表 26-7 functions コマンドのキーワード (続き)

| キーワード        | 意味                                                                                                                                                                               |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| port-forward | ポート転送をイネーブルにします。                                                                                                                                                                 |
| url-entry    | ユーザの URL エントリをイネーブルまたはディセーブルにします。イネーブルにしても、セキュリティ アプライアンスは設定されている URL またはネットワーク ACL で、URL を制限します。URL エントリをディセーブルにすると、セキュリティ アプライアンスは、WebVPN ユーザがホーム ページの URL にのみアクセスできるように制限します。 |

このコマンドで使用するキーワードは、次のとおりです。

- **file-access** : ファイル アクセスをイネーブルまたはディセーブルにします。イネーブルにすると、WebVPN ホーム ページにサーバリストのファイル サーバが表示されます。ファイル ブラウジングまたはファイル エントリをイネーブルにするには、ファイル アクセスをイネーブルにする必要があります。
- **file-browsing** : ファイル サーバとファイル共有のブラウジングをイネーブルまたはディセーブルにします。ファイル サーバのユーザ エントリを許可するには、ファイル ブラウジングをイネーブルにする必要があります。
- **file-entry** : ユーザがファイル サーバの名前を入力する機能をイネーブルまたはディセーブルにします。
- **http-proxy** : HTTP アプレット プロキシのクライアントへの転送をイネーブルまたはディセーブルにします。プロキシは、Java、ActiveX、Flash など、適切なマングリングを妨げる技術に対して有効です。セキュリティ アプライアンスの使用を継続しながら、マングリングをバイパスします。転送プロキシは、ブラウザの古いプロキシ コンフィギュレーションを自動的に変更し、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、Java など、実質的にすべてのクライアント サイド技術をサポートします。サポートされるブラウザは Microsoft Internet Explorer だけです。
- **mapi** : Microsoft Outlook/Exchange のポート転送をイネーブルまたはディセーブルにします。
- **none** : すべての WebVPN の **functions** にヌルを設定します。デフォルトのグループポリシーまたは指定されているグループポリシーから機能を継承しないようにします。
- **url-entry** : ユーザの URL エントリをイネーブルまたはディセーブルにします。イネーブルにしても、セキュリティ アプライアンスは設定されている URL またはネットワーク ACL で、URL を制限します。URL エントリをディセーブルにすると、セキュリティ アプライアンスは、WebVPN ユーザがホーム ページの URL にのみアクセスできるように制限します。

次の例は、anyuser という名前のユーザに対して、ファイル アクセス、ファイル ブラウジング、HTTP プロキシ、および MAPI プロキシを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# functions file-access file-browsing MAPI
hostname(config-username-webvpn)#
```

## HTML からフィルタリングするコンテンツとオブジェクトの指定

このユーザの WebVPN セッションの Java、ActiveX、イメージ、スクリプト、およびクッキーをフィルタリングするには、ユーザ名の webvpn コンフィギュレーション モードで **html-content-filter** コマンドを入力します。コンテンツ フィルタを削除するには、このコマンドの **no** 形式を入力します。**html-content-filter none** コマンドを発行して作成したヌル値を含めて、設定済みのすべてのコンテンツ フィルタを削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループポリシーから継承できます。HTML コンテンツ フィルタを継承しないようにするには、**html-content-filter none** コマンドを入力します。HTML フィルタリングは、デフォルトでディセーブルです。

コマンドを 2 回使用すると、先行する設定値が上書きされます。

```
hostname(config-username-webvpn)# html-content-filter {java | images | scripts | cookies | none}

hostname(config-username-webvpn)# no html-content-filter [java | images | scripts | cookies | none]
```

このコマンドで使用するキーワードは、次のとおりです。

- **cookies**：イメージからクッキーを削除して、アドバタイズメント フィルタリングを制限し、プライバシーを保持します。
- **images**：イメージへの参照を削除します（<IMG> タグを削除）。
- **java**：Java および ActiveX への参照を削除します（<EMBED>、<APPLET>、および <OBJECT> の各タグを削除）。
- **none**：フィルタリングを実行しないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリングの値を継承しないようにします。
- **scripts**：スクリプトへの参照を削除します（<SCRIPT> タグを削除）。

次の例は、anyuser という名前のユーザに、Java と ActiveX、クッキー、およびイメージのフィルタリングを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# html-content-filter java cookies images
hostname(config-username-webvpn)#
```

## ユーザ ホームページの指定

この WebVPN ユーザのログイン時に表示される Web ページの URL を指定するには、ユーザ名の webvpn コンフィギュレーション モードで **homepage** コマンドを入力します。**homepage none** コマンドを発行して作成したヌル値を含めて、設定されているホーム ページを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループポリシーから継承できます。ホーム ページを継承しないようにするには、**homepage none** コマンドを入力します。

**none** キーワードは、WebVPN ホームページがないことを示します。これにより、ヌル値が設定されてホーム ページが拒否され、ホーム ページが継承されなくなります。

キーワード **value** の後ろの *url-string* 変数で、ホームページの URL を指定します。文字列の先頭は、http:// または https:// にする必要があります。

デフォルトのホーム ページはありません。

```
hostname(config-username-webvpn)# homepage {value url-string | none}
hostname(config-username-webvpn)# no homepage
hostname(config-username-webvpn)#
```

次の例は、「anyuser」という名前のユーザのホームページとして www.example.com を指定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# homepage value www.example.com
hostname(config-username-webvpn)#
```

## カスタマイゼーションの適用

カスタマイゼーションは、ログイン時にユーザに表示されるウィンドウの内容を決定します。カスタマイゼーション パラメータは、WebVPN 設定の一部として設定します。以前定義した Web ページ カスタマイゼーションを適用して、ログイン時にユーザに表示される Web ページのルックアンドフィールを変更するには、ユーザ名の webvpn コンフィギュレーション モードで customization コマンドを入力します。

```
hostname(config-username-webvpn)# customization customization_name
hostname(config-username-webvpn)#
```

たとえば、blueborder という名前のカスタマイゼーションを使用する場合、次のコマンドを入力します。

```
hostname(config-username-webvpn)# customization blueborder
hostname(config-username-webvpn)#
```

## 「拒否」メッセージの指定

ユーザ名の webvpn コンフィギュレーション モードで **deny-message** コマンドを入力すると、WebVPN に正常なログインが可能でも VPN 特権を持たないリモート ユーザに送信されるメッセージを指定できます。

```
hostname(config-username-webvpn)# deny-message value "message"
hostname(config-username-webvpn)# no deny-message value "message"
hostname(config-username-webvpn)# deny-message none
```

**no deny-message value** コマンドは、リモート ユーザがメッセージを受信しないように、メッセージ文字列を削除します。

**no deny-message none** コマンドは、トンネルグループ ポリシー コンフィギュレーションからアトリビュートを削除します。ポリシーはアトリビュート値を継承します。

メッセージは、特殊文字、スペース、および句読点を含む、英数字最大 491 文字の長さにできますが、囲みの引用符はカウントされません。テキストは、ログイン時にリモート ユーザのブラウザに表示されます。**deny-message value** コマンドに文字列を入力しているときは、たとえコマンドがラップしても入力が続けます。

デフォルトの拒否メッセージは、「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features.Contact your IT administrator for more information.」です。

次の例の最初のコマンドは、ユーザ名モードに入り、anyuser という名前のユーザにアトリビュートを設定します。後続のコマンドは、ユーザ名の webvpn コンフィギュレーション モードに入り、そのユーザに関連付けられている拒否メッセージを変更します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# deny-message value "Your login credentials are OK.
However, you have not been granted rights to use the VPN features. Contact your
administrator for more information."
hostname(config-username-webvpn)
```

## WebVPN 接続に使用するアクセスリストの指定

このユーザの WebVPN 接続に使用するアクセスリストの名前を指定するには、ユーザ名の webvpn コンフィギュレーション モードで **filter** コマンドを入力します。**filter none** コマンドを発行して作成したヌル値を含めて、アクセスリストを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループポリシーから継承できます。フィルタの値を継承しないようにするには、**filter value none** コマンドを入力します。

**filter** コマンドを入力して指定するまで、WebVPN アクセスリストは適用されません。

ACL を設定して、このユーザについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**filter** コマンドを入力して、これらの ACL を WebVPN トラフィックに適用します。

```
hostname(config-username-webvpn)# filter {value ACLname | none}
hostname(config-username-webvpn)# no filter
hostname(config-username-webvpn)#
```

**none** キーワードは、**webvpntype** アクセスリストがないことを示します。これにより、ヌル値が設定されてアクセスリストが拒否され、別のグループポリシーからアクセスリストが継承されなくなります。

キーワード **value** の後ろの **ACLname** 文字列で、すでに設定されているアクセスリストの名前を指定します。



(注)

WebVPN は、**vpn-filter** コマンドで定義されている ACL を使用しません。

次の例は、anyuser という名前のユーザに対して **acl\_in** という名前のアクセスリストを呼び出すフィルタを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# filter acl_in
hostname(config-username-webvpn)#
```

## URL リストの適用

ユーザの WebVPN ホームページに URL のリストを表示するように指定できます。最初に、グローバル コンフィギュレーション モードで **url-list** コマンドを入力して 1 つ以上の名前付きリストを作成する必要があります。特定のユーザに WebVPN サーバと URL のリストを適用するには、ユーザ名の webvpn コンフィギュレーション モードで **url-list** コマンドを入力します。

**url-list none** コマンドを使用して作成したヌル値を含めて、リストを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値をグループポリシーから継承できます。URL リストを継承しないようにするには、**url-list none** コマンドを入力します。

```
hostname(config-username-webvpn)# url-list {listname displayname url | none}
hostname(config-username-webvpn)# no url-list
```

このコマンドで使用するキーワードと変数は、次のとおりです。

- **displayname** : URL の名前を指定します。この名前は、WebVPN のエンドユーザ インターフェイスに表示されます。
- **listname** : URL をグループ化する名前を指定します。
- **none** : URL のリストが存在しないことを示します。ヌル値を設定して、URL リストを拒否します。URL リストの値を継承しないようにします。
- **url** : WebVPN ユーザがアクセスできる URL を指定します。

デフォルトの URL リストはありません。

コマンドを 2 回使用すると、先行する設定値が上書きされます。

次の例は、anyuser という名前のユーザに AnyuserURLs という URL リストを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# url-list value AnyuserURLs
hostname(config-username-webvpn)#
```

## WebVPN アプリケーション アクセスのイネーブル化

このユーザの WebVPN アプリケーション アクセスをイネーブルにするには、ユーザ名の webvpn コンフィギュレーション モードで **port-forward** コマンドを入力します。ポート転送は、デフォルトではディセーブルになっています。

**port-forward none** コマンドを発行して作成したヌル値を含めて、コンフィギュレーションからポート転送アトリビュートを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、リストをグループポリシーから継承できます。フィルタリングを拒否してポート転送リストを継承しないようにするには、**none** キーワードを指定して **port-forward** コマンドを入力します。

```
hostname(config-username-webvpn)# port-forward {value listname | none}
hostname(config-username-webvpn)# no port-forward
hostname(config-username-webvpn)#
```

キーワード **value** の後ろの *listname* 文字列で、WebVPN ユーザがアクセスできるアプリケーションのリストを指定します。コンフィギュレーション モードで **port-forward** コマンドを入力し、このリストを定義します。

コマンドを 2 回使用すると、先行する設定値が上書きされます。

ユーザ名の webvpn コンフィギュレーション モードで **port-forward** コマンドを入力し、アプリケーション アクセスをイネーブルにする前に、WebVPN 接続でユーザが使用できるアプリケーションのリストを定義する必要があります。グローバル コンフィギュレーション モードで **port-forward** コマンドを入力し、このリストを定義します。

次の例は、ports1 というポート転送リストを設定する方法を示しています。

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward value ports1
hostname(config-username-webvpn)#
```

## ポート転送表示名の設定

ユーザ名の webvpn コンフィギュレーション モードで **port-forward-name** コマンドを使用して、特定のユーザでエンド ユーザへの TCP ポート転送を識別する表示名を設定します。

**port-forward-name none** コマンドを使用して作成したヌル値を含めて、表示名を削除するには、コマンドの **no** 形式を入力します。**no** オプションは、デフォルト名の Application Access を復元します。表示名を使用しないようにするには、**port-forward none** コマンドを入力します。

```
hostname(config-username-webvpn)# port-forward-name {value name | none}
hostname(config-username-webvpn)# no port-forward-name
```

次の例は、ポート転送名 test を設定する方法を示しています。

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward-name value test
hostname(config-username-webvpn)#
```

## セッション タイマー更新のために無視する最大オブジェクト サイズの設定

デットワーク デバイスは、短いキープアライブ メッセージを交換して、デバイス間の仮想回線が引き続きアクティブであることを確認します。これらのメッセージの長さは異なる可能性があります。**keep-alive-ignore** コマンドを使用すると、指定したサイズ以下のすべてのメッセージをキープアライブ メッセージと見なし、セッション タイマーの更新時にトラフィックと見なさないようセキュリティ アプライアンスに指示できます。範囲は 0 ～ 900 KB です。デフォルトは 4 KB です。

無視する HTTP/HTTPS トラフィックの上限をトランザクションごとに指定するには、グループポリシー アトリビュート **webvpn** コンフィギュレーション モードで **keep-alive-ignore** コマンドを使用します。

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#
```

このコマンドの **no** 形式を使用すると、コンフィギュレーションから指定を削除します。

```
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

次の例では、無視するオブジェクトの最大サイズを 5 KB に設定します。

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

## 自動サインオンの設定

NTLM、基本 HTTP 認証、またはその両方を使用する内部サーバに、特定の WebVPN ユーザの WebVPN ログイン クレデンシャルを自動的に渡すには、ユーザ名の **webvpn** コンフィギュレーション モードで **auto-signon** コマンドを入力します。

**auto-signon** コマンドは、WebVPN ユーザ用のシングル サインオン方式です。NTLM 認証、基本認証、またはその両方を使用する認証のために WebVPN ログイン クレデンシャル（ユーザ名とパスワード）を内部サーバに渡します。複数の **auto-signon** コマンドを入力でき、コマンドは入力順序に従って処理されます（先に入力されたコマンドが優先されます）。

自動サインオン機能は、**webvpn** コンフィギュレーション、**webvpn** グループ コンフィギュレーション、または **webvpn** ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。ユーザ名がグループに優先し、グループがグローバルに優先するという標準的な優先動作が適用されます。選択するモードは、望ましい認証の範囲によって異なります。

特定のサーバへの特定のユーザの自動サインオンをディセーブルにするには、元の IP ブロックまたは URI を指定してこのコマンドの **no** 形式を使用します。すべてのサーバへの認証をディセーブルにするには、引数を指定しないで **no** 形式を使用します。**no** オプションを使用すると、値をグループポリシーから継承できます。

次の例では、基本認証または NTLM 認証を使用して、anyuser という名前の Web VPN ユーザに対し、URI マスク **https://\*.example.com/\*** で定義されたサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow uri https://*.example.com/*
auth-type all
```



次の例では、基本認証または NTLM 認証を使用して、anyuser という名前の Web VPN ユーザに対し、サブネット マスク 255.255.255.0 を使用する IP アドレス 10.1.1.0 のサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0
auth-type all
hostname(config-username-webvpn)#
```

## SSO サーバの指定

WebVPN だけに使用できるシングル サインオンのサポートを使用すると、ユーザはユーザ名とパスワードを複数回入力しなくても、さまざまなサーバのセキュアな各種のサービスにアクセスできます。**sso-server value** コマンドをユーザ名の webvpn モードで入力すると、SSO サーバをユーザに割り当てることができます。

SSO サーバをユーザに割り当てするには、ユーザ名の webvpn コンフィギュレーション モードで **sso-server value** コマンドを入力します。このコマンドでは、コンフィギュレーションに CA SiteMinder コマンドが含まれている必要があります。

```
hostname(config-username-webvpn)# sso-server value server_name
hostname(config-username-webvpn)#
```

この割り当てを削除してデフォルト ポリシーを使用するには、このコマンドの **no** 形式を使用します。デフォルト ポリシーを継承しないようにするには、**sso-server none** コマンドを入力します。

```
hostname(config-username-webvpn)# sso-server {value server_name | none}
hostname(config-username-webvpn)# [no] sso-server value server_name
```

SSO サーバに割り当てられているデフォルト ポリシーは DfltGrpPolicy です。

次の例では、example という名前の SSO サーバを anyuser という名前のユーザに割り当てます。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# sso-server value example
hostname(config-username-webvpn)#
```

## SVC の設定

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 をインストールして設定しなくても、リモート ユーザが IPSec VPN クライアントの利点を活用できる VPN トンネリング テクノロジーです。SVC では、リモート コンピュータにすでにある 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。

SVC セッションを確立するには、リモート ユーザはセキュリティ アプライアンスの WebVPN インターフェイスの IP アドレスをブラウザに入力します。ブラウザはそのインターフェイスに接続して WebVPN のログイン画面を表示します。ユーザがログインと認証を完了し、ユーザが SVC を必要としていることをセキュリティ アプライアンスが確認すると、セキュリティ アプライアンスは SVC をリモート コンピュータにダウンロードします。セキュリティ アプライアンスが、SVC を使用するオプションがユーザにあると確認した場合、セキュリティ アプライアンスは、SVC のインストールをスキップするリンクをユーザ画面に表示するとともに、SVC をリモート コンピュータにダウンロードします。

ダウンロードが完了すると、SVC は自動的にインストールと設定を実行します。接続が切断されると（設定に応じて）、SVC はリモート コンピュータに保持されるか、またはリモート コンピュータからアンインストールされます。

セキュリティ アプライアンスは、さまざまなリモート コンピュータのオペレーティング システム用に、複数の独自の SVC イメージをキャッシュ メモリ内に備えている場合もあります。ユーザが接続を試みると、セキュリティ アプライアンスは、イメージとオペレーティング システムが一致するまで引き続きこれらのイメージの部分をリモート コンピュータにダウンロードできます。一致した時点で、SVC 全体をダウンロードします。接続のセットアップ時間を短縮するため、ダウンロードされる最初のイメージが、最もよく遭遇するリモート コンピュータのオペレーティング システムになるように SVC イメージの順序を指定できます。SVC のインストールと使用の詳細については、第 31 章「SSL VPN クライアントの設定」を参照してください。

第 31 章「SSL VPN クライアントの設定」に示すように、SVC をイネーブルにした後は、特定のグループの SVC 機能をイネーブルまたは必須にできます。この機能は、デフォルトでディセーブルになっています。SVC をイネーブルまたは必須にすると、この項で説明している一連の svc コマンドをイネーブルにできます。SVC とその関連する svc コマンドをイネーブルにするには、ユーザ名の webvpn コンフィギュレーション モードで次の手順を実行します。

- ステップ 1** セキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードできるようにするには、**svc enable** コマンドを入力します。このコマンドは、デフォルトではディセーブルになっています。セキュリティ アプライアンスは SVC ファイルをダウンロードしません。このコンフィギュレーションから **svc enable** コマンドを削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-username-webvpn)# svc {none | enable | required}
hostname(config-username-webvpn)#
```



(注)

**no svc enable** コマンドを入力しても、アクティブな SVC セッションは終了しません。

```
hostname(config)# username sales attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# svc enable
hostname(config-username-webvpn)#
```

- ステップ 2** SVC 接続経由で特定のユーザについて HTTP データの圧縮をイネーブルにするには、**svc compression** コマンドを入力します。SVC 圧縮は、デフォルトで **deflate**（イネーブル）に設定されています。特定のユーザの圧縮をディセーブルにするには、**none** キーワードを使用します。svc compression コマンドを削除して値が継承されるようにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-username-webvpn)# svc compression {deflate | none}
hostname(config-username-webvpn)#
```

次の例では、sales という名前のユーザ SVC 圧縮をディセーブルにします。

```
hostname(config)# username sales attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# svc compression none
hostname(config-username-webvpn)#
```

**ステップ 3** セキュリティ アプライアンスで dead-peer-detection (DPD) をイネーブルにして、SVC またはセキュリティ アプライアンスが DPD を実行する頻度を設定するには、**svc dpd-interval** コマンドを使用します。このコンフィギュレーションから **svc dpd-interval** コマンドを削除するには、このコマンドの **no** 形式を使用します。このユーザの SVC DPD をディセーブルにするには、**none** キーワードを使用します。

```
hostname(config-username-webvpn)# svc dpd-interval {[gateway {seconds | none}] | [client {seconds | none}]}
```

```
hostname(config-username-webvpn)#
```

DPD チェックは、デフォルトでディセーブルになっています。

ゲートウェイは、セキュリティ アプライアンスのことです。セキュリティ アプライアンスが DPD テストを実行する頻度を、30 ～ 3600 秒（1 時間）の範囲で指定できます。**none** を指定すると、セキュリティ アプライアンスが実行する DPD テストはディセーブルになります。

クライアントは、SVC のことです。クライアントが DPD テストを実行する頻度を、30 ～ 3600 秒（1 時間）の範囲で指定できます。**none** を指定すると、クライアントが実行する DPD テストはディセーブルになります。

次の例では、sales という名前の既存のユーザについて、セキュリティ アプライアンス（ゲートウェイ）によって実行される DPD の頻度を 3000 秒に設定し、クライアントによって実行される DPD の頻度を 1000 秒に設定しています。

```
hostname(config)# username sales attributes
```

```
hostname(config-username)# webvpn
```

```
hostname(config-username-webvpn)# svc dpd-interval gateway 3000
```

```
hostname(config-username-webvpn)# svc dpd-interval client 1000
```

```
hostname(config-username-webvpn)#
```

**ステップ 4** 接続のアイドル状態を維持できる時間をデバイスが制限している場合でも、プロキシ、ファイアウォール、または NAT デバイスを通じて SVC 接続のオープン状態を維持するように、キープアライブ メッセージの頻度を調整できます (*seconds* で指定)。

頻度を調整することで、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケットベースのアプリケーションをアクティブに実行していない場合でも、SVC が切断して再接続をしないようにできます。

リモート コンピュータ上の SVC がキープアライブ メッセージをセキュリティ アプライアンスに送信する頻度（15 ～ 600 秒）を設定するには、**svc keepalive** コマンドを使用します。コンフィギュレーションからこのコマンドを削除して値が継承されるようにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-username-webvpn)# svc keepalive {none | seconds}
```

```
hostname(config-username-webvpn)# no svc keepalive {none | seconds}
```

```
hostname(config-username-webvpn)#
```

SVC キープアライブは、デフォルトでディセーブルになっています。キーワード **none** を使用すると SVC キープアライブ メッセージがディセーブルになります。

次の例では、ユーザは、SVC がキープアライブ メッセージを 300 秒（5 分）の頻度で送信できるようにセキュリティ アプライアンスを設定します。

```
hostname(config-username-webvpn)# svc keepalive 300
```

```
hostname(config-username-webvpn)#
```

- ステップ 5** SVC がリモート コンピュータに永続的にインストールされた状態を保つには、*installed* キーワードを指定して **svc keep-installer** コマンドを使用します。コマンドをこのコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-username-webvpn)# svc keep-installer {installed | none}
hostname(config-username-webvpn)# no svc keep-installer {installed | none}
hostname(config-username-webvpn)#
```

デフォルトでは、SVC の常時インストールがディセーブルになっています。SVC セッションの終わりに、SVC はリモートコンピュータからアンインストールされます。

次の例では、このユーザのリモート コンピュータの SVC インストール状態を維持するようにセキュリティ アプライアンスを設定します。

```
hostname(config-username-webvpn)# svc keep-installer installed
hostname(config-username-webvpn)#
```

- ステップ 6** SVC が SVC セッションでキーの再生成を実行できるようにするには、**svc rekey** コマンドを使用します。

```
hostname(config-username-webvpn)# svc rekey {method {ssl | new-tunnel} | time minutes | none}}
```

キーの再生成をディセーブルにして、コマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-username-webvpn)# no svc rekey [method {ssl | new-tunnel} | time minutes | none}]
hostname(config-username-webvpn)#
```

SVC キーの再生成は、デフォルトでディセーブルになっています。

method を new-tunnel に指定すると、SVC キーの再生成中に SVC が新しいトンネルを確立することが指定されます。method を none に指定すると、SVC キーの再生成はディセーブルになります。method を ssl に指定すると、SSL の再ネゴシエーションは SVC キーの再生成中に行われます。method を指定する代わりに、セッションの開始からキーの再生成が行われるまでの時間を 1 ～ 10080（1 週間）の分数で指定できます。

コマンドの **no** 形式の場合は、必要最小限の指定をします。適正な例は、次のとおりです。

```
hostname(config-username-webvpn)# no svc rekey method
hostname(config-username-webvpn)#
```

ただし、method を次のように new-tunnel に指定し、

```
hostname(config-username-webvpn)# no svc rekey method new-tunnel
hostname(config-username-webvpn)#
```

現在の method が ssl である場合、値が一致しないためにコマンドは失敗します。

次の例では、ユーザは、キーの再生成中に SVC が SSL と再ネゴシエートするように設定し、キーの再生成がセッション開始の 30 分後に発生するように設定します。

```
hostname(config-username-webvpn)# svc rekey method ssl
hostname(config-username-webvpn)# svc rekey time 30
hostname(config-username-webvpn)#
```



## VPN の IP アドレスの設定

この章では、IP アドレスの割り当て方式について説明します。

インターネットワーク接続は、IP アドレスによって可能になります。IP アドレスは、送信者と受信者の両方に接続用の番号が割り当てられている必要があるという点で、電話番号に似ています。ただし、VPN では、実際には 2 セットのアドレスが存在します。最初のセットは、パブリック ネットワーク上でクライアントとサーバを接続します。この接続が確立されると、2 番目のセットが VPN トンネル経由でクライアントとサーバを接続します。

セキュリティ アプライアンスのアドレス管理では、この IP アドレスの 2 番目のセットを扱います。これらのプライベート IP アドレスは、クライアントをトンネル経由でプライベート ネットワーク上のリソースに接続し、プライベート ネットワークに直接接続されているかのようなクライアント機能を提供します。また、ここでは、クライアントに割り当てられたプライベート IP アドレスのみを扱います。プライベート ネットワーク上のその他のリソースに割り当てられた IP アドレスは、VPN 管理ではなく、ネットワーク管理業務の一部に位置づけられます。したがって、ここで IP アドレスに言及する場合は、クライアントをトンネルのエンドポイントとして機能させる、プライベート ネットワークのアドレッシング方式で取得される IP アドレスを意味します。

次の事項について説明します。

- [IP アドレスの割り当て方式の設定 \(P.27-2\)](#)
- [ローカル IP アドレス プールの設定 \(P.27-2\)](#)
- [AAA アドレッシングの設定 \(P.27-3\)](#)
- [DHCP アドレッシングの設定 \(P.27-4\)](#)

## IP アドレスの割り当て方式の設定

セキュリティ アプライアンスでは、リモートアクセス クライアントに IP アドレスを割り当てる際に、次の 1 つ以上の方式を使用することができます。複数のアドレス割り当て方式を設定すると、セキュリティ アプライアンスは IP アドレスが見つかるまで各オプションを検索します。デフォルトでは、すべての方式がイネーブルになっています。現在のコンフィギュレーションを表示するには、**show running-config all vpn-addr-assign** コマンドを入力します。

- **aaa**：ユーザ単位で外部認証サーバからアドレスを取得します。IP アドレスが設定された認証サーバを使用している場合は、この方式を使用することを推奨します。
- **dhcp**：DHCP サーバから IP アドレスを取得します。DHCP を使用する場合は、DHCP サーバを設定する必要があります。また、DHCP サーバで使用可能な IP アドレスの範囲も定義する必要があります。
- **local**：内部アドレス プールを使用します。内部的に設定されたアドレス プールは、最も設定が簡単なアドレス プール割り当て方式です。local を選択する場合は、**ip-local-pool** コマンドを使用して、使用する IP アドレスの範囲も定義する必要があります。

リモートアクセス クライアントへの IP アドレス割り当て方式を指定するには、グローバル コンフィギュレーション モードで **vpn-addr-assign** コマンドを入力します。シンタックスは、**vpn-addr-assign {aaa | dhcp | local}** です。

## ローカル IP アドレス プールの設定

VPN リモートアクセス トンネルに使用する IP アドレス プールを設定するには、グローバル コンフィギュレーション モードで **ip local pool** コマンドを入力します。アドレス プールを削除するには、このコマンドの **no** 形式を入力します。

セキュリティ アプライアンスは、該当の接続用のトンネルグループに基づいたアドレス プールを使用します。1 つのトンネルグループに複数のアドレス プールを設定する場合は、セキュリティ アプライアンスは設定された順にそれらのプールを使用します。

ローカルでないサブネットのアドレスを割り当てる場合は、そのようなネットワーク用のルートの追加が容易になるように、サブネットの境界を担当するプールを追加することを推奨します。

ローカルアドレス プールのコンフィギュレーションの概要は、次のようになります。

```
hostname(config)# vpn-addr-assign local
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
hostname(config)
```

**ステップ 1** アドレス割り当て方式として IP アドレス プールを設定するには、**local** 引数を指定して **vpn-addr-assign** コマンドを入力します。

```
hostname(config)# vpn-addr-assign local
hostname(config)#
```

**ステップ 2** アドレス プールを設定するには、**ip local pool** コマンドを使用します。シンタックスは、**ip local pool poolname first-address—last-address mask mask** です。

次の例では、firstpool という名前の IP アドレス プールを設定しています。開始アドレスは 10.20.30.40 で、終了アドレスは 10.20.30.50 です。ネットワーク マスクは 255.255.255.0 です。

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
hostname(config)
```

## AAA アドレッシングの設定

AAA サーバを使用して VPN リモートアクセス クライアントにアドレスを割り当てるには、まず AAA サーバまたは AAA サーバ グループを設定する必要があります。『Cisco Security Appliance Command Reference』の **aaa-server protocol** コマンドと、このマニュアルの第 10 章「AAA サーバとローカル データベースの設定」の「AAA サーバ グループおよびサーバの識別」を参照してください。

また、ユーザは RADIUS 認証用に設定されたトンネルグループと一致している必要があります。

次の例は、firstgroup という名前のトンネルグループに、RAD2 という AAA サーバ グループを定義する方法を示しています。例の中に 1 つ余分な手順が入っていますが、これは以前にそのトンネルグループに名前を付け、トンネルグループ タイプを定義していた場合のためです。この手順が次の例に記載されているのは、これらの値を設定しない限り、後続の tunnel-group コマンドにアクセスできないので、注意を促すためです。

この例で作成されるコンフィギュレーションの概要は、次のとおりです。

```
hostname(config)# vpn-addr-assign aaa
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)# authentication-server-group RAD2
```

IP アドレッシング用に AAA を設定するには、次の手順を実行します。

- ステップ 1** アドレス割り当て方式として AAA を設定するには、**aaa** 引数を指定して **vpn-addr-assign** コマンドを入力します。

```
hostname(config)# vpn-addr-assign aaa
hostname(config)#
```

- ステップ 2** firstgroup というトンネルグループをリモートアクセスまたは LAN-to-LAN トンネルグループとして確立するには、**type** キーワードを指定して **tunnel-group** コマンドを入力します。次の例は、リモートアクセス トンネルグループを設定します。

```
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)#
```

- ステップ 3** 一般アトリビュート コンフィギュレーション モードに入り、firstgroup というトンネルグループの AAA サーバ グループを定義するには、**general-attributes** 引数を指定して **tunnel-group** コマンドを入力します。

```
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)#
```

- ステップ 4** 認証に使用する AAA サーバ グループを指定するには、**authentication-server-group** コマンドを入力します。

```
hostname(config-general)# authentication-server-group RAD2
hostname(config-general)#
```

このコマンドには、この例で示すより多くの引数があります。詳細については、『Cisco Security Appliance Command Reference』を参照してください。

## DHCP アドレッシングの設定

DHCP を使用して VPN クライアントのアドレスを割り当てるには、まず DHCP サーバ、およびその DHCP サーバで使用可能な IP アドレスの範囲を設定する必要があります。その後、トンネルグループ単位で DHCP サーバを定義します。また、オプションとして、該当のトンネルグループまたはユーザ名に関連付けられたグループポリシー内に、DHCP ネットワーク スコープも定義できます。このスコープは、使用する IP アドレス プールを DHCP サーバに指定するための、IP ネットワーク番号または IP アドレスです。

次の例では、firstgroup という名前のトンネルグループに、IP アドレス 172.33.44.19 の DHCP サーバを定義しています。また、この例では、remotegroup というグループポリシーに対して、192.86.0.0 という DHCP ネットワーク スコープも定義しています（remotegroup というグループポリシーは、firstgroup というトンネルグループに関連付けられています）。ネットワーク スコープを定義しない場合、DHCP サーバはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

次のコンフィギュレーションには、本来不要な手順が含まれています。これらは、以前にそのトンネルグループに名前を付け、トンネルグループ タイプをリモートアクセスとして定義していたり、グループポリシーに名前を付け、内部または外部として指定していた場合のためです。これらの手順が次の例に記載されているのは、これらの値を設定しない限り、後続の tunnel-group コマンドおよび group-policy コマンドにアクセスできないので、注意を促すためです。

この例で作成されるコンフィギュレーションの概要は、次のとおりです。

```
hostname(config)# vpn-addr-assign dhcp
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)# group-policy remotegroup internal
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 192.86.0.0
```

IP アドレッシング用に DHCP サーバを設定するには、次の手順を実行します。

- ステップ 1** アドレス割り当て方式として DHCP を設定するには、**dhcp** 引数を指定して **vpn-addr-assign** コマンドを入力します。

```
hostname(config)# vpn-addr-assign dhcp
hostname(config)#
```

- ステップ 2** firstgroup というトンネルグループをリモートアクセスまたは LAN-to-LAN トンネルグループとして確立するには、**type** キーワードを指定して **tunnel-group** コマンドを入力します。次の例は、リモートアクセス トンネルグループを設定します。

```
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)#
```

- ステップ 3** 一般アトリビュート コンフィギュレーション モードに入って DHCP サーバを定義するには、**general-attributes** 引数を指定して **tunnel-group** コマンドを入力します。

```
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config)#
```



- ステップ 4** DHCP サーバを定義するには、**dhcp-server** コマンドを入力します。次の例では、IP アドレス 172.33.44.19 の DHCP サーバを設定しています。

```
hostname(config-general)# dhcp-server 172.33.44.19  
hostname(config-general)#
```

- ステップ 5** トンネルグループ モードを終了します。

```
hostname(config-general)# exit  
hostname(config)#
```

- ステップ 6** remotegroup というグループポリシーを、内部的または外部的に設定されたグループとして定義するには、**internal** 引数または **external** 引数を指定して **group-policy** コマンドを入力します。次の例では、内部グループを設定しています。

```
hostname(config)# group-policy remotegroup internal  
hostname(config)#
```

- ステップ 7** (オプション) グループポリシー アトリビュート コンフィギュレーション モードに入り、DHCP サーバで使用する IP アドレスのサブネットワークを設定するには、**attributes** キーワードを指定して **group-policy** コマンドを入力します。

```
hostname(config)# group-policy remotegroup attributes  
hostname(config-group-policy)#
```

- ステップ 8** (オプション) remotegroup というグループポリシーのユーザにアドレスを割り当てるために DHCP サーバで使用する IP アドレスの範囲を指定するには、**dhcp-network-scope** コマンドを入力します。次の例では、192.86.0.0 というネットワーク スコープを設定しています。

```
hostname(config-group-policy)# dhcp-network-scope 192.86.0.0  
hostname(config-group-policy)#
```

---





## リモートアクセス IPsec VPN の設定

リモートアクセス VPN を使用すると、インターネットなどの TCP/IP ネットワーク上のセキュアな接続を介して、単一ユーザを中央サイトに接続することができます。

この章では、リモートアクセス VPN 接続の構築方法について説明します。ここでは、次の項目について説明します。

- [コンフィギュレーションのまとめ \(P.28-2\)](#)
- [インターフェイスの設定 \(P.28-3\)](#)
- [ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化 \(P.28-4\)](#)
- [アドレス プールの設定 \(P.28-5\)](#)
- [ユーザの追加 \(P.28-6\)](#)
- [トランスフォーム セットの作成 \(P.28-6\)](#)
- [トンネルグループの定義 \(P.28-7\)](#)
- [ダイナミック暗号マップの作成 \(P.28-8\)](#)
- [ダイナミック暗号マップを使用するための暗号マップ エントリの作成 \(P.28-9\)](#)

## コンフィギュレーションのまとめ

この章では、次のコンフィギュレーションを使用して、リモートアクセス接続の設定方法について説明します。後の項で、手順の詳細を説明します。

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)# nameif outside
hostname(config)# no shutdown
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)# isakmp policy 1 hash sha
hostname(config)# isakmp policy 1 group 2
hostname(config)# isakmp policy 1 lifetime 43200
hostname(config)# isakmp enable outside
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# tunnel-group testgroup type ipsec-ra
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# pre-shared-key 44kkaol59636jnfX
hostname(config)# crypto dynamic-map dyn1 1 set transform-set FirstSet
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)# crypto map mymap interface outside
hostname(config)# write memory
```

## インターフェイスの設定

セキュリティ アプライアンスには、少なくとも 2 つのインターフェイスがあり、これらをここでは外部と内部と言います。一般に、外部インターフェイスは、パブリック インターネットに接続されます。一方、内部インターフェイスは、プライベート ネットワークに接続され、一般のアクセスから保護されます。

最初に、セキュリティ アプライアンスの 2 つのインターフェイスを設定し、イネーブルにします。次に、名前、IP アドレス、およびサブネット マスクを割り当てます。オプションで、セキュリティ レベル、速度、およびセキュリティ アプライアンスでの二重操作を設定します。

インターフェイスを設定するには、例で示すコマンド シンタックスを使用して、次の手順を実行します。

- ステップ 1** インターフェイス コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで、設定するインターフェイスのデフォルト名を指定して **interface** コマンドを入力します。次の例で、インターフェイスは ethernet0 です。

```
hostname(config)# interface ethernet0
hostname(config-if)#
```

- ステップ 2** インターフェイスの IP アドレスとサブネット マスクを設定するには、**ip address** コマンドを入力します。次の例で、IP アドレスは 10.10.4.100、サブネット マスクは 255.255.0.0 です。

```
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)#
```

- ステップ 3** インターフェイスに名前を付けるには、**nameif** コマンドを入力します。最大 48 文字です。この名前は、設定した後で変更することはできません。次の例で、ethernet0 インターフェイスの名前は outside です。

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

- ステップ 4** インターフェイスをイネーブルにするには、**shutdown** コマンドの **no** 形式を入力します。デフォルトでは、インターフェイスはディセーブルです。

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

- ステップ 5** 変更を保存するには、**write memory** コマンドを入力します。

```
hostname(config-if)# write memory
hostname(config-if)#
```

- ステップ 6** 同じ手順で、2 番目のインターフェイスを設定します。

## ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化

Internet Security Association and Key Management Protocol は IKE と呼ばれ、2 台のホストで IPsec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーション プロトコルです。各 ISAKMP ネゴシエーションは、フェーズ 1 とフェーズ 2 と呼ばれる 2 つの部分に分かれます。

フェーズ 1 は、以後の ISAKMP ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ 2 は、セキュアな接続を移動するデータを保護するトンネルを作成します。

ISAKMP ネゴシエーションの条件を設定するには、ISAKMP ポリシーを作成します。ここでは、次の項目について説明します。

- ピアの ID を確認する認証方式。
- データを保護し、プライバシーを守る暗号化方式。
- Hashed Message Authentication Code 方式。送信者の身元を保証し、搬送中にメッセージが変更されていないことを保証します。
- 暗号キーのサイズを設定する Diffie-Hellman グループ。
- セキュリティ アプライアンスが暗号キーを置き換える前に、この暗号キーを使用する最長時間の制限。

IKE ポリシーのキーワードとその値の詳細については、このマニュアルの「IPsec と ISAKMP の設定」の章の [P.24-4 の表 24-1](#) を参照してください。

ISAKMP ポリシーを設定するには、グローバル コンフィギュレーション モードで、各種の引数を指定して **isakmp policy** コマンドを入力します。isakmp policy コマンドのシンタックスは次のとおりです。

**isakmp policy priority attribute\_name [attribute\_value | integer].**

次の手順を実行し、ガイドとして次の例で示すコマンド シンタックスを使用します。

**ステップ 1** 認証方式を設定します。次の例では、事前共有キーを設定します。このステップおよび後続のすべてのステップで、プライオリティは 1 です。

```
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)#
```

**ステップ 2** 暗号方式を設定します。次の例では、3DES に設定します。

```
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)#
```

**ステップ 3** HMAC 方式を設定します。次の例では、SHA-1 に設定します。

```
hostname(config)# isakmp policy 1 hash sha
hostname(config)#
```

**ステップ 4** Diffie-Hellman グループを設定します。次の例では、グループ 2 に設定します。

```
hostname(config)# isakmp policy 1 group 2
hostname(config)#
```

**ステップ 5** 暗号キーのライフタイムを設定します。次の例では、43,200 秒（12 時間）に設定します。

```
hostname(config)# isakmp policy 1 lifetime 43200  
hostname(config)#
```

**ステップ 6** outside というインターフェイス上の ISAKMP をイネーブルにします。

```
hostname(config)# isakmp enable outside  
hostname(config)#
```

**ステップ 7** 変更を保存するには、**write memory** コマンドを入力します。

```
hostname(config)# write memory  
hostname(config)#
```

---

## アドレス プールの設定

セキュリティ アプライアンスでは、ユーザに IP アドレスを割り当てる方式が必要です。一般的な方式では、アドレス プールを使用します。また、DHCP サーバや AAA サーバでアドレスを割り当てる場合もあります。次の例では、アドレス プールを使用します。

**ステップ 1** アドレス プールを設定するには、**ip local pool** コマンドを使用します。シンタックスは、**ip local pool poolname first\_address-last\_address** です。次の例では、プール名は testpool です。

```
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15  
hostname(config)#
```

**ステップ 2** 変更を保存します。

```
hostname(config)# write memory  
hostname(config)#
```

---

## ユーザの追加

セキュリティ アプライアンスに対するリモートアクセス ユーザを特定するには、ユーザ名とパスワードを設定します。

- ステップ 1** ユーザを追加するには、**username** コマンドを入力します。シンタックスは、**username username password password** です。次の例では、ユーザ名は **testuser**、パスワードは **12345678** です。

```
hostname(config)# username testuser password 12345678
hostname(config)#
```

- ステップ 2** 追加するユーザごとに、ステップ 1 を繰り返します。

## トランスフォーム セットの作成

トランスフォーム セットは、暗号化方式と認証方式を組み合わせたものです。特定のデータ フローを保護する場合、ピアは、ISAKMP との IPsec セキュリティ アソシエーションのネゴシエート中に、特定のトランスフォーム セットを使用することに同意します。トランスフォーム セットは、両方のピアで同じである必要があります。

トランスフォーム セットを複数作成して、暗号マップ エントリでそれらのトランスフォーム セットを 1 つまたはそれ以上指定することもできます。セキュリティ アプライアンスは、トランスフォーム セットを使用して、その暗号マップ エントリ アクセスリストのデータ フローを保護します。有効な暗号化方式と認証方式をリストしたテーブルなど、さらに詳細な情報については、このマニュアルの第 29 章「LAN-to-LAN IPsec VPN の設定」の「トランスフォーム セットの作成」を参照してください。

- ステップ 1** トランスフォーム セットを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec transform-set** コマンドを入力します。シンタックスは次のとおりです。

```
crypto ipsec transform-set transform-set-name encryption-method authentication-method
```

次の例では、名前が **FirstSet** で、暗号化と認証にそれぞれ **esp-3des** と **esp-md5-hmac** を使用するトランスフォーム セットを設定しています。

```
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

- ステップ 2** 変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```



## トンネルグループの定義

トンネルグループは、トンネル接続ポリシーを格納したレコードのセットです。AAA サーバを識別するトンネルグループを設定し、接続パラメータを指定し、デフォルトのグループポリシーを定義します。セキュリティ アプライアンスは、トンネルグループを内部的に保存します。

セキュリティ アプライアンス システムには、2 つのデフォルト トンネルグループがあります。1 つはデフォルトの IPSec リモートアクセス トンネルグループである DefaultRAGroup で、もう 1 つはデフォルトの IPSec LAN-to-LAN トンネルグループである DefaultL2Lgroup です。これらは、変更可能ですが、削除することはできません。トンネル ネゴシエーション中に特定のトンネルグループが指定されなかった場合、セキュリティ アプライアンスは、これらのグループを使用してリモートアクセスおよび LAN-to-LAN トンネルグループのデフォルト トンネル パラメータを設定します。

基本的なリモートアクセス接続を確立するには、次のように 3 つのアトリビュートをトンネルグループに設定する必要があります。

- 接続タイプを IPSec リモートアクセスに設定します。
- アドレス割り当て方式を設定します。次の例では、アドレス プールを使用します。
- 認証方式を設定します。次の例では、事前共有キーを使用します。

**ステップ 1** 接続タイプを IPSec リモートアクセスに設定するには、**tunnel-group** コマンドを入力します。コマンドシンタックスは、**tunnel-group name type type** です。ここで、*name* はトンネルグループに割り当てる名前であり、*type* はトンネルのタイプです。CLI で入力するトンネル タイプには、次のものがあります。

- ipsec-ra (IPSec リモートアクセス)
- ipsec-l2l (IPSec LAN-to-LAN)

次の例では、トンネルグループの名前は testgroup です。

```
hostname(config)# tunnel-group testgroup type ipsec-ra
hostname(config)#
```

**ステップ 2** トンネルグループの認証方式を設定するには、一般アトリビュート モードに入り、**address-pool** コマンドを入力してアドレス プールを作成します。次の例では、グループの名前は testgroup で、アドレス プールの名前は testpool です。

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
```

**ステップ 3** 認証方式を設定するには、ipsec アトリビュート モードに入り、**pre-shared-key** コマンドを入力して事前共有キーを作成します。セキュリティ アプライアンスとクライアントの両方で同じ事前共有キーを使用する必要があります。



(注)

事前共有キーは、VPN クライアントで使用される事前共有キーの長さを超えることはできません。事前共有キーのサイズが異なる Cisco VPN Client がセキュリティ アプライアンスに接続しようとすると、クライアントはピアの認証に失敗したことを示すエラー メッセージをログに記録します。

キーは、1 ～ 128 文字の英数字文字列です。次の例で、事前共有キーは 44kkaol59636jnfx です。

```
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# pre-shared-key 44kkaol59636jnfx
```

#### ステップ 4 変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```

## ダイナミック暗号マップの作成

セキュリティ アプライアンスは、ダイナミック暗号マップを使用してポリシー テンプレートを定義します。ポリシー テンプレートには、すべてのパラメータを設定する必要はありません。このようなダイナミック暗号マップにより、セキュリティ アプライアンスは IP アドレスが不明なピアからの接続を受信することができます。リモートアクセス クライアントは、このカテゴリに入ります。

ダイナミック暗号マップのエントリは、接続のトランスフォーム セットを指定します。また、逆ルーティングもイネーブルにします。これにより、セキュリティ アプライアンスは接続されたクライアントのルーティング情報を取得し、それを RIP または OSPF 経由でアドバタイズします。

#### ステップ 1 ダイナミック暗号マップ エントリにトランスフォーム セットを指定するには、**crypto dynamic-map set transform-set** コマンドを入力します。

シンタックスは、**crypto dynamic-map dynamic-map-name seq-num set transform-set transform-set-name** です。次の例では、ダイナミック マップの名前は dyn1、シーケンス番号は 1、トランスフォーム セット名は FirstSet です。

```
hostname(config)# crypto dynamic-map dyn1 1 set transform-set FirstSet
hostname(config)#
```

#### ステップ 2 この暗号マップ エントリに基づく任意の接続で RRI をイネーブルにするには、**crypto dynamic-map set reverse route** コマンドを入力します。

```
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)#
```

#### ステップ 3 変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```

## ダイナミック暗号マップを使用するための暗号マップ エントリの作成

次に、暗号マップ エントリを作成します。これにより、セキュリティ アプライアンスは、ダイナミック暗号マップを使用して IPSec セキュリティ アソシエーションのパラメータを設定することができます。

このコマンドに関する次の例では、暗号マップ名は mymap、シーケンス番号は 1、ダイナミック暗号マップ名は dyn1 です。この名前は、前の項「[ダイナミック暗号マップの作成](#)」で作成したものです。これらのコマンドは、グローバル コンフィギュレーション モードで入力します。

- ステップ 1** ダイナミック暗号マップを使用する暗号マップ エントリを作成するには、**crypto map** コマンドを入力します。シンタックスは、**crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name** です。

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1  
hostname(config)#
```

- ステップ 2** 暗号マップを外部インターフェイスに適用するには、**crypto map interface** コマンドを入力します。

シンタックスは、**crypto map map-name interface interface-name** です。

```
hostname(config)# crypto map mymap interface outside  
hostname(config)#
```

## ■ ダイナミック暗号マップを使用するための暗号マップ エントリの作成



# LAN-to-LAN IPSec VPN の設定

LAN-to-LAN VPN は、IPSec セキュリティ ゲートウェイ（セキュリティ アプライアンスやプロトコル準拠のその他の VPN デバイスなど）の間のコンフィギュレーションです。LAN-to-LAN VPN は、地理的に異なる場所にあるネットワークを接続します。

この章では、LAN-to-LAN VPN 接続の構築方法について説明します。ここでは、次の項目について説明します。

- [コンフィギュレーションのまとめ \(P.29-1\)](#)
- [インターフェイスの設定 \(P.29-2\)](#)
- [ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化 \(P.29-3\)](#)
- [トランスフォーム セットの作成 \(P.29-5\)](#)
- [ACL の設定 \(P.29-6\)](#)
- [トンネルグループの定義 \(P.29-7\)](#)
- [暗号マップの作成とインターフェイスへの適用 \(P.29-8\)](#)

## コンフィギュレーションのまとめ

ここでは、この章で作成するサンプルの LAN-to-LAN コンフィギュレーションの概要を説明します。後の項で、手順の詳細を説明します。

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)# no shutdown
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)# isakmp policy 1 hash sha
hostname(config)# isakmp policy 1 group 2
hostname(config)# isakmp policy 1 lifetime 43200
hostname(config)# isakmp enable outside
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# access-list 121_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# pre-shared-key 44kkaol59636jnfxf
hostname(config)# crypto map abcmap 1 match address 121_list
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
hostname(config)# crypto map abcmap interface outside
hostname(config)# write memory
```

## インターフェイスの設定

セキュリティ アプライアンスには、少なくとも 2 つのインターフェイスがあり、これらをここでは外部と内部と言います。一般に、外部インターフェイスは、パブリック インターネットに接続されます。一方、内部インターフェイスは、プライベート ネットワークに接続され、一般のアクセスから保護されます。

最初に、セキュリティ アプライアンスの 2 つのインターフェイスを設定し、イネーブルにします。次に、名前、IP アドレス、およびサブネット マスクを割り当てます。オプションで、セキュリティ レベル、速度、およびセキュリティ アプライアンスでの二重操作を設定します。

インターフェイスを設定するには、例で示すコマンド シNTAX を使用して、次の手順を実行します。

- ステップ 1** インターフェイス コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで、設定するインターフェイスのデフォルト名を指定して **interface** コマンドを入力します。次の例で、インターフェイスは ethernet0 です。

```
hostname(config)# interface ethernet0
hostname(config-if)#
```

- ステップ 2** インターフェイスの IP アドレスとサブネット マスクを設定するには、**ip address** コマンドを入力します。次の例で、IP アドレスは 10.10.4.100、サブネット マスクは 255.255.0.0 です。

```
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)#
```

- ステップ 3** インターフェイスに名前を付けるには、**nameif** コマンドを入力します。最大 48 文字です。この名前は、設定した後で変更することはできません。次の例で、ethernet0 インターフェイスの名前は outside です。

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

- ステップ 4** インターフェイスをイネーブルにするには、**shutdown** コマンドの **no** 形式を使用します。デフォルトでは、インターフェイスはディセーブルです。

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

- ステップ 5** 変更を保存するには、**write memory** コマンドを入力します。

```
hostname(config-if)# write memory
hostname(config-if)#
```

- ステップ 6** 同じ手順で、2 番目のインターフェイスを設定します。

## ISAKMP ポリシーの設定と外部インターフェイスでの ISAKMP のイネーブル化

Internet Security Association and Key Management Protocol は IKE と呼ばれ、2 台のホストで IPSec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーション プロトコルです。各 ISAKMP ネゴシエーションは、フェーズ 1 とフェーズ 2 と呼ばれる 2 つの部分に分かれます。

フェーズ 1 は、以後の ISAKMP ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ 2 は、セキュアな接続を移動するデータを保護するトンネルを作成します。

ISAKMP ネゴシエーションの条件を設定するには、以下を含む ISAKMP ポリシーを作成します。

- ピアの ID を確認する認証方式。
- データを保護し、プライバシーを守る暗号化方式。
- Hashed Message Authentication Code 方式。送信者の身元を保証し、搬送中にメッセージが変更されていないことを保証します。
- 暗号キー判別アルゴリズムを強化する Diffie-Hellman グループ。このアルゴリズムを使用して、セキュリティ アプライアンスは暗号キーとハッシュ キーを導出します。
- セキュリティ アプライアンスが暗号キーを置き換える前に、この暗号キーを使用する最長時間の制限。

IKE ポリシーのキーワードとその値の詳細については、このマニュアルの「IPSec と ISAKMP の設定」の章の [P.24-4 の表 24-1](#) を参照してください。

ISAKMP ポリシーを設定するには、グローバル コンフィギュレーション モードで、各種の引数を指定して **isakmp policy** コマンドを使用します。ISAKMP ポリシー コマンドのシンタックスは次のとおりです。

```
isakmp policy priority attribute_name [attribute_value | integer]
```

次の手順を実行し、ガイドとして次の例で示すコマンド シンタックスを使用します。

**ステップ 1** 認証方式を設定します。次の例では、事前共有キーを設定します。このステップおよび後続のすべてのステップで、プライオリティは 1 です。

```
hostname(config)# isakmp policy 1 authentication pre-share  
hostname(config)#
```

**ステップ 2** 暗号方式を設定します。次の例では、3DES に設定します。

```
hostname(config)# isakmp policy 1 encryption 3des  
hostname(config)#
```

**ステップ 3** HMAC 方式を設定します。次の例では、SHA-1 に設定します。

```
hostname(config)# isakmp policy 1 hash sha  
hostname(config)#
```

**ステップ 4** Diffie-Hellman グループを設定します。次の例では、グループ 2 に設定します。

```
hostname(config)# isakmp policy 1 group 2  
hostname(config)#
```

**ステップ 5** 暗号キーのライフタイムを設定します。次の例では、43,200 秒（12 時間）に設定します。

```
hostname(config)# isakmp policy 1 lifetime 43200  
hostname(config)#
```

**ステップ 6** outside というインターフェイス上の ISAKMP をイネーブルにします。

```
hostname(config)# isakmp enable outside  
hostname(config)#
```

**ステップ 7** 変更を保存するには、**write memory** コマンドを入力します。

```
hostname(config)# write memory  
hostname(config)#
```

---



## トランスフォーム セットの作成

トランスフォーム セットは、暗号化方式と認証方式を組み合わせたものです。特定のデータ フローを保護する場合、ピアは、ISAKMP との IPSec セキュリティ アソシエーションのネゴシエート中に、特定のトランスフォーム セットを使用することに同意します。トランスフォーム セットは、両方のピアで同じである必要があります。

トランスフォーム セットを複数作成して、暗号マップ エントリでそれらのトランスフォーム セットを 1 つまたはそれ以上指定することもできます。セキュリティ アプライアンスは、トランスフォーム セットを使用して、その暗号マップ エントリ アクセスリストのデータ フローを保護します。

表 29-1 に、有効な暗号化方式と認証方式を示します。

**表 29-1 暗号化方式と認証方式**

| 有効な暗号化方式             | 有効な認証方式              |
|----------------------|----------------------|
| esp-des              | esp-md5-hmac         |
| esp-3des (デフォルト)     | esp-sha-hmac (デフォルト) |
| esp-aes (128 ビット暗号化) |                      |
| esp-aes-192          |                      |
| esp-aes-256          |                      |
| esp-null             |                      |

パブリック インターネットなどの非信頼ネットワークを介して接続された 2 つのセキュリティ アプライアンス間で、IPSec を実装する通常の方法は、トンネル モードです。トンネル モードはデフォルトであり、設定は必要ありません。

トランスフォーム セットを設定するには、次の手順を実行します。

- 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、**crypto ipsec transform-set** コマンドを入力します。次の例では、名前が FirstSet で、暗号化と認証にそれぞれ esp-3des と esp-md5-hmac を使用するトランスフォーム セットを設定しています。シンタックスは次のとおりです。

**crypto ipsec transform-set transform-set-name encryption-method authentication-method**

```
hostname(config)# crypto ipsec transform-set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

- ステップ 2** 変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```

## ACL の設定

セキュリティ アプライアンスは、アクセスコントロール リストを使用してネットワーク アクセスを制御します。デフォルトでは、セキュリティ アプライアンスはすべてのトラフィックを拒否します。トラフィックを許可する ACL を設定する必要があります。

この LAN-to-LAN VPN 制御接続で設定する ACL は、送信元と宛先の IP アドレスに基づいています。接続の両側に、互いにミラーリングする ACL を設定します。

ACL を設定するには、次の手順を実行します。

- ステップ 1** **access-list extended** コマンドを入力します。次の例では、192.168.0.0 のネットワーク内にある IP アドレスから 150.150.0.0 のネットワークにトラフィックを送信する、l2l\_list という名前の ACL を設定します。シンタックスは、**access-list listname extended permit ip source-ipaddress source-netmask destination-ipaddress destination-netmask** です。

```
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0  
150.150.0.0 255.255.0.0  
hostname(config)#
```

- ステップ 2** 接続のもう一方の側のセキュリティ アプライアンスに、上記の ACL をミラーリングする ACL を設定します。次の例では、該当ピアのプロンプトは hostname2 です。

```
hostname2(config)# access-list l2l_list extended permit ip 150.150.0.0 255.255.0.0  
192.168.0.0 255.255.0.0  
hostname2(config)#
```

## トンネルグループの定義

トンネルグループは、トンネル接続ポリシーを格納したレコードのセットです。AAA サーバを識別するトンネルグループを設定し、接続パラメータを指定し、デフォルトのグループポリシーを定義します。セキュリティ アプライアンスは、トンネルグループを内部的に保存します。

セキュリティ アプライアンス システムには、2つのデフォルト トンネルグループがあります。1つはデフォルトの IPSec リモートアクセス トンネルグループである DefaultRAGroup で、もう 1つはデフォルトの IPSec LAN-to-LAN トンネルグループである DefaultL2Lgroup です。これらは、変更可能ですが、削除することはできません。また、環境に合った新しいトンネルグループを 1つ以上作成することもできます。トンネル ネゴシエーション中に特定のトンネルグループが指定されなかった場合、セキュリティ アプライアンスは、これらのグループを使用してリモートアクセスおよび LAN-to-LAN トンネルグループのデフォルト トンネルパラメータを設定します。

基本的な LAN-to-LAN 接続を確立するには、次のように 2つのアトリビュートをトンネルグループに設定する必要があります。

- 接続タイプを IPSec LAN-to-LAN に設定します。
- 認証方式を設定します。次の例では、事前共有キーを使用します。

**ステップ 1** 接続タイプを IPSec LAN-to-LAN に設定するには、**tunnel-group** コマンドを入力します。シンタックスは、**tunnel-group name type type** です。ここで、*name* はトンネルグループに割り当てた名前であり、*type* はトンネルのタイプです。CLI で入力するトンネルタイプは、次のとおりです。

- **ipsec-ra** (IPSec リモートアクセス)
- **ipsec-l2l** (IPSec LAN-to-LAN)

次の例では、トンネルグループの名前は、LAN-to-LAN ピアの IP アドレスである 10.10.4.108 です。

```
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)#
```

**ステップ 2** 認証方式を事前共有キーに設定するには、ipsec アトリビュート モードに入り、**pre-shared-key** コマンドを入力して事前共有キーを作成します。この LAN-to-LAN 接続の両方のセキュリティ アプライアンスで、同じ事前共有キーを使用する必要があります。

キーは、1 ～ 128 文字の英数字文字列です。次の例で、事前共有キーは 44kkaol59636jnfxx です。

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# pre-shared-key 44kkaol59636jnfxx
```

**ステップ 3** 変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```

## 暗号マップの作成とインターフェイスへの適用

暗号マップ エントリは、IPSec セキュリティ アソシエーションの次のような各種要素をまとめたものです。

- IPSec で保護する必要のあるトラフィック（アクセスリストで定義）
- IPSec で保護されたトラフィックの送信先（ピアで指定）
- トラフィックに適用される IPSec セキュリティ（トランスフォーム セットで指定）
- IPSec トラフィックのローカル アドレス（インターフェイスに暗号マップを適用して指定）

IPSec が成功するためには、両方のピアに互換性のあるコンフィギュレーションを持つ暗号マップ エントリが存在する必要があります。2つの暗号マップ エントリが互換性を持つためには、両者が少なくとも次の基準を満たす必要があります。

- 暗号マップ エントリに、互換性を持つ暗号アクセスリスト（たとえば、ミラー イメージ アクセスリスト）が含まれている。応答するピアがダイナミック暗号マップを使用している場合は、セキュリティ アプライアンスの暗号アクセスリストのエントリがピアの暗号アクセスリストによって「許可」されている必要があります。
- 各暗号マップ エントリが他のピアを識別する（応答するピアがダイナミック暗号マップを使用していない場合）。
- 暗号マップ エントリに、共通のトランスフォーム セットが少なくとも 1つ存在する。

所定のインターフェイスに対して複数の暗号マップ エントリを作成する場合は、各エントリのシーケンス番号 (seq-num) を使用して、エントリにランクを付けます。seq-num が小さいほど、プライオリティが高くなります。暗号マップ セットを持つインターフェイスでは、セキュリティ アプライアンスはまずトラフィックをプライオリティの高いマップ エントリと照合して評価します。

次の条件のいずれかに当てはまる場合は、所定のインターフェイスに対して複数の暗号マップ エントリを作成します。

- 複数のピアで異なるデータ フローを処理する場合。
- 異なるタイプのトラフィック（同一または個別のピアへの）に異なる IPSec セキュリティを適用する場合。たとえば、あるサブネット セット間のトラフィックは認証し、別のサブネット セット間のトラフィックは認証および暗号化するような場合です。この場合は、異なるタイプのトラフィックを 2つの個別のアクセスリストで定義し、各暗号アクセスリストに対して個別に暗号マップ エントリを作成します。

暗号マップを作成して外部インターフェイスに割り当てるには、グローバル コンフィギュレーション モードで **crypto map** コマンドをいくつか入力します。これらのコマンドではさまざまな引数を使用しますが、シンタックスはすべて **crypto map map-name-seq-num** で始まります。次の例では、マップ名は abcmap で、シーケンス番号は 1 です。

これらのコマンドは、グローバル コンフィギュレーション モードで入力します。

**ステップ 1** アクセスリストを暗号マップ エントリに割り当てるには、**crypto map match address** コマンドを入力します。

シンタックスは、**crypto map map-name seq-num match address aclname** です。次の例では、マップ名は abcmap、シーケンス番号は 1、アクセスリスト名は 121\_list です。

```
hostname(config)# crypto map abcmap 1 match address 121_list
hostname(config)#
```

**ステップ 2** IPSec 接続用のピアを指定するには、**crypto map set peer** コマンドを入力します。

シンタックスは、**crypto map map-name seq-num set peer {ip\_address1 | hostname1} [... ip\_address10 | hostname10]** です。次の例では、ピア名は 10.10.4.108 です。

```
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108  
hostname(config)#
```

**ステップ 3** 暗号マップ エントリにトランスフォーム セットを指定するには、**crypto map set transform-set** コマンドを入力します。

シンタックスは、**crypto map map-name seq-num set transform-set transform-set-name** です。次の例では、トランスフォーム セット名は FirstSet です。

```
hostname(config)# crypto map abcmap 1 set transform-set FirstSet  
hostname(config)#
```

## 暗号マップのインターフェイスへの適用

暗号マップセットは、IPSec トラフィックが通過する各インターフェイスに適用する必要があります。セキュリティ アプライアンスは、すべてのインターフェイスで IPSec をサポートします。暗号マップ セットをインターフェイスに適用すると、セキュリティ アプライアンスはすべてのインターフェイス トラフィックを暗号マップ セットと照合して評価し、接続時やセキュリティ アソシエーションのネゴシエート時に、指定されたポリシーを使用します。

また、暗号マップをインターフェイスにバインドすると、セキュリティ アソシエーション データベースやセキュリティ ポリシー データベースなどのランタイム データ構造も初期化されます。暗号マップを後から変更すると、セキュリティ アプライアンスは自動的にその変更を実行コンフィギュレーションに適用します。既存の接続はすべてドロップされ、新しい暗号マップの適用後に再確立されます。

**ステップ 1** 設定済みの暗号マップを外部インターフェイスに適用するには、**crypto map interface** コマンドを入力します。シンタックスは、**crypto map map-name interface interface-name** です。

```
hostname(config)# crypto map abcmap interface outside  
hostname(config)#
```

**ステップ 2** 変更を保存します。

```
hostname(config)# write memory  
hostname(config)#
```





# WebVPN の設定

---

次の事項について説明します。

- [WebVPN の準備 \(P.30-2\)](#)
- [WebVPN ポリシーの作成と適用 \(P.30-17\)](#)
- [WebVPN トンネルグループ アトリビュートの定義 \(P.30-19\)](#)
- [WebVPN グループポリシーとユーザ アトリビュートの設定 \(P.30-20\)](#)
- [Application Access の設定 \(P.30-21\)](#)
- [ファイル アクセスの設定 \(P.30-25\)](#)
- [Citrix MetaFrame サービスへのアクセスの設定 \(P.30-28\)](#)
- [PDA での WebVPN の使用 \(P.30-29\)](#)
- [WebVPN を介した電子メールの使用 \(P.30-30\)](#)
- [WebVPN のパフォーマンスの最適化 \(P.30-32\)](#)
- [WebVPN エンド ユーザ設定の概要 \(P.30-36\)](#)
- [WebVPN データのキャプチャ \(P.30-55\)](#)

## WebVPN の準備

WebVPN によってユーザは、ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモートアクセス VPN トンネルを確立できます。ソフトウェアやハードウェア クライアントは必要ありません。

WebVPN を使用することで、インターネット上のほぼすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションへのセキュアで容易なアクセスが可能になります。次のようなアクセス先があります。

- 内部 Web サイト
- Web 対応アプリケーション
- NT/Active Directory ファイル共有
- POP3S、IMAP4S、および SMTPS などの電子メール プロキシ
- MS Outlook Web Access
- MAPI
- Application Access（他の TCP ベースのアプリケーションにアクセスするためのポート転送）

WebVPN は Secure Sockets Layer プロトコルおよびその後継である Transport Layer Security を使用して、リモート ユーザと、中央サイトで設定した特定のサポートされている内部リソースとの間で、セキュアな接続を提供します。セキュリティ アプライアンスはプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

ネットワーク管理者は、ユーザに対してグループ単位で WebVPN リソースへのアクセスを提供します。ユーザは、内部ネットワーク上のリソースに直接アクセスすることはできません。

次の項では、WebVPN アクセスを設定するための準備について説明します。

- [WebVPN セキュリティ対策の順守](#)
- [WebVPN でサポートされていない機能の概要](#)
- [中央サイトにアクセスするための SSL の使用](#)
- [デジタル証明書による認証](#)
- [Web VPN 用にブラウザのクッキーをイネーブルにする](#)
- [パスワードの管理](#)
- [WebVPN でのシングル サインオンの使用](#)
- [デジタル証明書による認証](#)

## WebVPN セキュリティ対策の順守

セキュリティ アプライアンス上の WebVPN 接続は、リモートアクセス IPSec 接続とはまったく異なっています。特に SSL 対応サーバとの対話方法やセキュリティ上のリスクを減らすための対策に大きな違いがあります。

WebVPN 接続では、セキュリティ アプライアンスは、エンド ユーザの Web ブラウザとターゲット Web サーバとの間のプロキシとして機能します。WebVPN ユーザが SSL 対応 Web サーバに接続すると、セキュリティ アプライアンスはセキュアな接続を確立し、SSL 証明書を検証します。エンドユーザのブラウザは提示された SSL 証明書を受信しないため、この証明書を検証することはできません。

セキュリティ アプライアンス上の現在の WebVPN 実装では、有効期限が切れた証明書を提示するサイトとの通信は許可しません。また、セキュリティ アプライアンスは信頼できる CA 証明書の検証も実行しません。このため、WebVPN ユーザは、SSL 対応の Web サーバと通信する前に相手が提示する証明書を分析することができません。



SSL 証明書に関するリスクを最小限にするには、次のようにします。

1. WebVPN アクセスを必要とするすべてのユーザからなるグループポリシーを設定し、そのグループポリシーに対してだけ WebVPN 機能をイネーブルにします。
2. WebVPN ユーザに対してインターネット アクセスを制限します。その方法の 1 つは、URL エントリをディセーブルにすることです。次に、WebVPN ユーザがアクセス可能なプライベートネットワーク内の特定のターゲットへのリンクを設定します。
3. ユーザに適切な情報を提供します。SSL 対応サイトがプライベート ネットワーク内部にない場合、ユーザは WebVPN 接続を介してこのサイトにアクセスすることはできません。そのようなサイトにアクセスする場合、ユーザは別のブラウザ ウィンドウを開き、そのブラウザを使用して、提示された証明書を表示する必要があります。

## WebVPN でサポートされていない機能の概要

セキュリティ アプライアンスは、WebVPN 接続では次の機能をサポートしていません。

- モジュラ ポリシー フレームワークの検査機能。コンフィギュレーション制御を検査する機能です。
- **vpn-filter** コマンドなどのフィルタ設定コマンドが持つ機能。
- NAT。グローバルに一意の IP アドレスの必要性を減らす機能です。
- PAT。複数の発信セッションが 1 つの IP アドレスから発信されているように見せることができる機能です。
- QoS。 **police** コマンドと **priority-queue** コマンドを使用してレートを制限する機能です。
- 接続制限。スタティックまたはモジュラ ポリシー フレームワークの **set connection** コマンドを使用して、接続をチェックする機能です。
- **established** コマンド。このコマンドを使用すると、高セキュリティ ホストから低セキュリティ ホストへの接続が確立済みの場合に、低セキュリティ ホストから高セキュリティ ホストへのリターン接続が可能になります。

## 中央サイトにアクセスするための SSL の使用

WebVPN は SSL およびその後継である TLS1 を使用して、リモート ユーザと、中央サイトにある特定のサポートされている内部リソースとの間で、セキュアな接続を提供します。ここでは、次の項目について説明します。

- [WebVPN セッションでの HTTPS の使用](#)
- [同一インターフェイス上での WebVPN と ASDM の設定](#)
- [WebVPN HTTP/HTTPS プロキシの設定](#)
- [SSL/TLS 暗号化プロトコルの設定](#)

## WebVPN セッションでの HTTPS の使用

WebVPN セッションの確立には、次のことが必要です。

- セキュリティ アプライアンスまたはロードバランシング クラスターへのアクセスに HTTPS を使用する。Web ブラウザには、セキュリティ アプライアンスの IP アドレスを `https:// address` 形式で入力します。`address` はセキュリティ アプライアンス インターフェイスの IP アドレスまたは DNS ホスト名です。
- ユーザの接続先のセキュリティ アプライアンス インターフェイス上で WebVPN セッションをイネーブルにする。

インターフェイス上で WebVPN セッションを許可するには、次の手順を実行します。

**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 **webvpn** コマンドを入力して、webvpn モードに入ります。

**ステップ 2** WebVPN セッションに使用するインターフェイス名を指定して **enable** コマンドを入力します。

たとえば、外部のインターフェイス上で WebVPN セッションをイネーブルにするには、次のように入力します。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

## 同一インターフェイス上での WebVPN と ASDM の設定

セキュリティ アプライアンスは、同一インターフェイスで WebVPN と ASDM の両方の管理セッションを同時にサポートできます。このためには、これらの機能に別々のポート番号を割り当てる必要があります。あるいは、WebVPN を設定して異なるインターフェイス上で ASDM にアクセスします。

## WebVPN HTTP/HTTPS プロキシの設定

セキュリティ アプライアンスは HTTPS 接続を終了して、HTTP/HTTPS 要求を HTTP プロキシ サーバや HTTPS プロキシ サーバに転送できます。これらのサーバは、ユーザとインターネットの仲介役として機能します。すべてのインターネット アクセスが組織によって制御されているサーバを経由するように指定することで、別のフィルタリングが可能になり、セキュアなインターネット アクセスと管理制御が保証されます。

HTTP プロキシと HTTPS プロキシに対する値を設定するには、webvpn モードで **http-proxy** コマンドと **https-proxy** コマンドを使用します。これらのコマンドを使用すると、HTTP や HTTPS のプロキシ サーバとポートを指定できます。

## SSL/TLS 暗号化プロトコルの設定

SSL/TLS 暗号化プロトコルを設定するときは、次のことに注意してください。

- 使用しているセキュリティ アプライアンスとブラウザが、同じ SSL/TLS 暗号化プロトコルを利用していることを確認してください。
- 電子メールプロキシを設定する場合は、セキュリティ アプライアンス SSL バージョンを TLSv1 Only に設定しないでください。  
MS Outlook と MS Outlook Express は TLS をサポートしていません。
- TCP ポート転送には、Sun Microsystems Java Runtime Environment (JRE) バージョン 1.4.x と 1.5.x が必要です。WebVPN ユーザが次の SSL バージョンで接続している場合、ポート転送は機能しません。

|                       |                  |
|-----------------------|------------------|
| Negotiate SSLv3       | Java がダウンロードされる  |
| Negotiate SSLv3/TLSv1 | Java がダウンロードされる  |
| Negotiate TLSv1       | Java がダウンロードされない |
| TLSv1Only             | Java がダウンロードされない |
| SSLv3Only             | Java がダウンロードされない |

## デジタル証明書による認証

SSL はデジタル証明書を使用して認証を行います。セキュリティ アプライアンスは、ブート時に自己署名の SSL サーバ証明書を作成します。または、PKI コンテキストで発行された SSL 証明書をセキュリティ アプライアンスにインストールすることもできます。HTTPS の場合、この証明書をクライアントにインストールする必要があります。証明書のインストールは、特定のセキュリティ アプライアンスから 1 度だけ行います。

デジタル証明書によるユーザ認証には、次のような制限事項があります。

- デジタル証明書を使用して認証を行う WebVPN ユーザに対して、Application Access は機能しません。JRE には、Web ブラウザ キーストアにアクセスする機能はありません。このため、JAVA はブラウザがユーザ認証に使用する証明書を使用できず、起動できません。
- 電子メールプロキシは、Netscape 7.x の電子メール クライアントの証明書認証だけをサポートします。MS Outlook、MS Outlook Express、Eudora など、他の電子メール クライアントは、証明書ストアにアクセスできません。

デジタル証明書を使用する認証と認可の詳細については、「[AAA サーバとローカル データベースの設定](#)」の「[証明書とユーザ ログイン クレデンシャルの使用方法](#)」を参照してください。

## Web VPN 用にブラウザのクッキーをイネーブルにする

WebVPN が正しく動作するためには、ブラウザのクッキーが必要です。ブラウザでクッキーがディセーブルになっていると、Web ポータル ホームページからのリンクによって新しいウィンドウが開き、ユーザはもう一度ログインするように要求されます。

## パスワードの管理

パスワードの期限切れが近づくとにエンド ユーザに警告するようにセキュリティ アプライアンスを設定することができます。これを設定するには、トンネルグループの一般アトリビュート モードで、**password-management** コマンドを指定します。

このコマンドを設定すると、セキュリティ アプライアンスは、リモート ユーザのログイン時に、現在のパスワードの期限切れが近づいているか、または期限が切れていることを通知します。次に、セキュリティ アプライアンスからパスワード変更の機会がユーザに提供されます。現在のパスワードの期限がまだ切れていない場合は、ユーザはこのパスワードで引き続きログインできます。このコマンドは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。RADIUS 認証または LDAP 認証が設定されていない場合、セキュリティ アプライアンスはこのコマンドを無視します。

このコマンドは、パスワードが期限切れになるまでの日数は変更しませんが、パスワードの期限切れが近づいていることをセキュリティ アプライアンスがユーザに警告する期限切れまでの日数を指定します。デフォルト値は 14 日間です。

LDAP サーバ認証だけの場合は、キーワード **password-expire-in-days** を使用すると特定の日数を指定できます。**password-expire-in-days** を使用する場合は、日数も指定する必要があります。

日数を 0 にしてこのコマンドを指定すると、このコマンドがディセーブルになります。セキュリティ アプライアンスは期限切れが迫っていることをユーザに通知しませんが、ユーザは期限切れ後にパスワードを変更することができます。

次の例は、トンネルグループ「testgroup」についてパスワードの期限切れが迫っていることをユーザに警告し始めるまでの日数を 90 日間に設定しています。

```
hostname(config)# tunnel-group testgroup type webvpn
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# password-management password-expire-in-days 90
```

## WebVPN でのシングル サインオンの使用

シングル サインオン サポートは、WebVPN ユーザがパスワードを 1 回入力するだけで複数の保護されたサービスや Web サーバにアクセスできるシステムです。一般に、SSO のメカニズムは、AAA プロセスの一部として開始されるか、または AAA サーバのユーザ認証に成功した直後に開始されます。セキュリティ アプライアンスで実行する WebVPN サーバは、認証サーバに対するユーザのプロキシとして動作します。ユーザがログインすると、WebVPN サーバは、ユーザ名およびパスワードを含む SSO 認証要求を HTTPS を使用して認証サーバに送信します。サーバが認証要求を受け入れた場合は、WebVPN サーバに SSO 認証クッキーを返信します。セキュリティ アプライアンスは、ユーザに代わってこのクッキーを保持し、ユーザ認証でこのクッキーを使用して、SSO サーバで保護されているドメイン内部の Web サイトの安全を確保します。

この項では、WebVPN でサポートされる 3 種類の SSO 認証方法について説明します。これらの認証方法には、HTTP Basic 認証と NTLMv1 (NT LAN Manager) 認証、Computer Associates の eTrust SiteMinder SSO サーバ（前 Netegrity SiteMinder）による認証、および HTTP Form プロトコルによる認証があります。

この項の内容は次のとおりです。

- [HTTP Basic 認証または NTLM 認証による SSO の設定](#)
- [SiteMinder による SSO 認証の設定](#)
- [HTTP Form プロトコルを使用した SSO の設定](#)

## HTTP Basic 認証または NTLM 認証による SSO の設定

この項では、HTTP Basic 認証または NTLM 認証を使用するシングル サインオンについて説明します。この方法のいずれかまたは両方を使用して SSO を実装するようにセキュリティ アプライアンスを設定することができます。**auto-signon** コマンドを使用すると、セキュリティ アプライアンスは WebVPN ユーザのログインのクレデンシャル（ユーザ名およびパスワード）を内部サーバに自動的に渡すように設定されます。**auto-signon** コマンドは 2 回以上入力することができます。コマンドを複数回入力すると、セキュリティ アプライアンスは入力順（先に入力されたコマンドを優先）にこれらを処理します。IP アドレスと IP マスク、または URI マスクのいずれかを使用してログインのクレデンシャルを受信するようにサーバに指定します。

**auto-signon** コマンドは、webvpn コンフィギュレーション モード、webvpn グループポリシー モード、webvpn ユーザ名モードのすべてで使用できます。ユーザ名はグループより優先され、グループはグローバルより優先されます。モードは、次のように、必要な認証の範囲に応じて選択します。

| モード                     | 範囲                              |
|-------------------------|---------------------------------|
| Webvpn コンフィギュレーション      | WebVPN ユーザ全員に対するグローバルな範囲        |
| Webvpn グループ コンフィギュレーション | グループポリシーで定義される WebVPN ユーザのサブセット |
| Webvpn ユーザ名コンフィギュレーション  | 個々の WebVPN ユーザ                  |

次の例では、モードと引数の組み合わせが可能なさまざまなコマンドについて説明します。

### すべてのユーザ、IP アドレス範囲、NTLM

NTLM 認証を使用し、10.1.1.0 から 10.1.1.255 の IP アドレス範囲に存在するサーバに対するすべての WebVPN ユーザからのアクセスに **自動サインオン**を設定するには、次のようなコマンドを入力します。

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow ip 10.1.1.1 255.255.255.0 auth-type ntlm
```

### すべてのユーザ、URI 範囲、HTTP Basic

基本の HTTP 認証を使用するすべての Web VPN ユーザに対し、URI マスク `https://*.example.com/*` で定義されたサーバへのアクセスに **自動サインオン**を設定するには、次のようなコマンドを入力します。

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
```

### グループ、URI 範囲、HTTP Basic および NTLM

基本認証または NTLM 認証を使用して、Web VPN ユーザの ExamplePolicy グループに対し、URI マスク `https://*.example.com/*` で定義されたサーバへのアクセスに**自動サインオン**を設定するには、次のコマンドを入力します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type all
```

### 特定のユーザ、IP アドレス範囲、HTTP Basic

HTTP Basic 認証を使用し、10.1.1.0 から 10.1.1.255 の IP アドレス範囲に存在するサーバに対する Anyuser と名付けられたユーザからのアクセスに **自動サインオン**を設定するには、次のようなコマンドを入力します。

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.1 255.255.255.0
auth-type basic
```

## SiteMinder による SSO 認証の設定

ここでは、SiteMinder を使用して SSO をサポートするためのセキュリティ アプライアンスの設定について説明します。ユーザの Web サイトのセキュリティ インフラストラクチャにすでに SiteMinder を組み込んでいる場合は、SSO に SiteMinder を使用するのが普通です。この方式により、SSO 認証は AAA から切り離され、AAA プロセスが完了するとこの認証が 1 回実施されます。WebVPN ユーザまたはグループに SSO を設定する場合は、まず RADIUS サーバまたは LDAP サーバなどの AAA サーバを設定する必要があります。その後で、WebVPN の SSO サポートをセットアップできます。この項の内容は次のとおりです。

- [タスクの概要：Siteminder による SSO の設定](#)
- [タスクの詳細：Siteminder による SSO の設定](#)
- [シスコの認証スキームの SiteMinder への追加](#)

## タスクの概要：Siteminder による SSO の設定

この項では、SiteMinder SSO を使用して SSO を設定するために必要なタスクの概要について説明します。必要なタスクは次のとおりです。

- SSO サーバの指定
- セキュリティ アプライアンスが SSO 認証要求を作成するための SSO サーバの URL の指定
- セキュリティ アプライアンスと SSO サーバとの間でセキュアな通信を確立するための秘密キーの指定。このキーはパスワードのようなもので、ユーザが作成および保管し、Cisco Java プラグイン認証スキームを使用してセキュリティ アプライアンスおよび SiteMinder Policy Server の両方で入力します。

これらの必須タスクに加えて、次のようなオプションの設定タスクを行うことができます。

- 認証要求のタイムアウトの設定
- 認証要求のリトライ回数の設定

設定タスクの完了後、ユーザまたはグループポリシーに SSO サーバを割り当てます。

## タスクの詳細：Siteminder による SSO の設定

ここでは、CA SiteMinder による SSO 認証をサポートするためのセキュリティ アプライアンスの特定の設定手順について説明します。SiteMinder を使用して SSO を設定するには、次の手順を実行します。

- ステップ 1** webvpn コンフィギュレーション モードで、次の **sso-server** コマンドと **type** オプションを入力して SSO サーバを作成します。たとえば、Example of type siteminder という名前の SSO サーバを作成するには、次のように入力します。

```
hostname(config)# webvpn
hostname(config-webvpn)# sso-server Example type siteminder
hostname(config-webvpn-sso-siteminder)#
```



(注)

現時点では、セキュリティ アプライアンスは、SSO サーバタイプ siteminder のみサポートします。

- ステップ 2** webvpn-sso-siteminder コンフィギュレーション モードで次のように **web-agent-url** コマンドを入力して SSO サーバの認証 URL を指定します。たとえば、http://www.Example.com/webvpn という URL に認証要求を送信するには、次のように入力します。

```
hostname(config-webvpn-sso-siteminder)# web-agent-url http://www.Example.com/webvpn
hostname(config-webvpn-sso-siteminder)#
```

- ステップ 3** セキュリティ アプライアンスと SiteMinder との間の認証通信をセキュアにする秘密キーを webvpn-sso-siteminder コンフィギュレーション モードで **policy-server-secret** コマンドを使用して指定します。キーの長さは、標準またはシフト式英数字を使用した任意の文字長にできますが、セキュリティ アプライアンスと SSO サーバの両方で同じキーを使用する必要があります。

たとえば、AtaL8rD8! という秘密キーを作成するには、次のように入力します。

```
hostname(config-webvpn-sso-siteminder)# policy-server-secret AtaL8rD8!
hostname(config-webvpn-sso-siteminder)#
```

**ステップ 4** また、オプションで、webvpn-sso-siteminder コンフィギュレーション モードから **request-timeout** コマンドを使用すると、失敗した SSO 認証がタイムアウトを試行するまでの秒数を設定することができます。デフォルトの秒数は 5 秒で、1 秒から 30 秒までの範囲で指定できます。要求がタイムアウトするまでの秒数を 8 に変更するには、次のように入力します。

```
hostname(config-webvpn-sso-siteminder)# request-timeout 8  
hostname(config-webvpn-sso-siteminder)#
```

**ステップ 5** また、オプションで、webvpn-sso-siteminder コンフィギュレーション モードから **max-retry-attempts** コマンドを使用すると、セキュリティ アプライアンスがタイムアウトするまでに、失敗した SSO 認証をリトライする回数を設定することができます。デフォルトのリトライ回数は 3 で、1 回から 5 回までの範囲で指定できます。たとえば、リトライの回数を 4 に設定するには、次のように入力します。

```
hostname(config-webvpn-sso-siteminder)# max-retry-attempts 4  
hostname(config-webvpn-sso-siteminder)#
```

**ステップ 6** SSO サーバの設定後、グループまたはユーザのいずれかに対して SSO 認証を指定する必要があります。グループに SSO を指定するには、group-policy-webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用して SSO サーバをグループポリシーに割り当てます。ユーザに SSO を指定するには、同じ **sso-server value** コマンドを使用して SSO サーバをユーザに割り当てますが、この場合は username-webvpn コンフィギュレーション モードで実行します。たとえば、Example という名前の SSO サーバをユーザ名 Anyuser に割り当てるには、次のように入力します。

```
hostname(config)# username Anyuser attributes  
hostname(config-username)# webvpn  
hostname(config-username-webvpn)# sso-server value Example  
hostname(config-group-webvpn)#
```

**ステップ 7** 最後に、特権 EXEC モードで、**test sso-server** コマンドを使用すると SSO サーバの設定をテストできます。たとえば、Example という名前の SSO サーバをユーザ名 Anyuser でテストするには、次のように入力します。

```
hostname# test sso-server Example username Anyuser  
INFO: Attempting authentication request to sso-server Example for user Anyuser  
INFO: STATUS: Success  
hostname#
```

## シスコの認証スキームの SiteMinder への追加

SiteMinder による SSO を使用するためのセキュリティ アプライアンスの設定に加え、Java プラグインとして提供されている、シスコの認証スキームを使用するようにユーザの CA SiteMinder Policy Server を設定する必要もあります。



(注)

- SiteMinder Policy Server を正しく設定するには、SiteMinder の経験が必要です。
- この項では、手順のすべてではなく、一般的なタスクを取り上げます。
- カスタム認証スキームを追加するための完全な手順については、CA SiteMinder のマニュアルを参照してください。



ユーザの SiteMinder Policy Server にシスコの認証スキームを設定するには、次のタスクを実行します。

**ステップ 1** Siteminder Administration ユーティリティを使用して、次の特定の引数を使用できるようにカスタム認証スキームを作成します。

- Library フィールドに、**smjavaapi** と入力します。
- Secret フィールドに、セキュリティ アプライアンスに設定したものと同一秘密キーを入力します。  
コマンドライン インターフェイスから **policy-server-secret** コマンドを入力するか、ASDM の Add SSO Server ダイアログの Secret Key フィールドに入力するか、いずれかの方法でセキュリティ アプライアンスにこれを設定します。
- Parameter フィールドに、**CiscoAuthAPI** と入力します。

**ステップ 2** CD から **cisco\_vpn\_auth.jar** ファイルを SiteMinder サーバのデフォルトのライブラリ ディレクトリにコピーします。

## HTTP Form プロトコルを使用した SSO の設定

この項では、SSO における HTTP Form プロトコルの使用方法について説明します。HTTP Form プロトコルは SSO 認証を実行するための一般的な手段で、AAA 方式としても使用できます。このプロトコルは、WebVPN ユーザおよび認証を行う Web サーバの間で認証情報を交換するセキュアな方法を提供します。HTTP Form は一般的なプロトコルとして、Web サーバや Web ベースの SSO 製品との高度な互換性を持ち、RADIUS サーバや LDAP サーバなど他の AAA サーバと共に使用することができます。



(注)

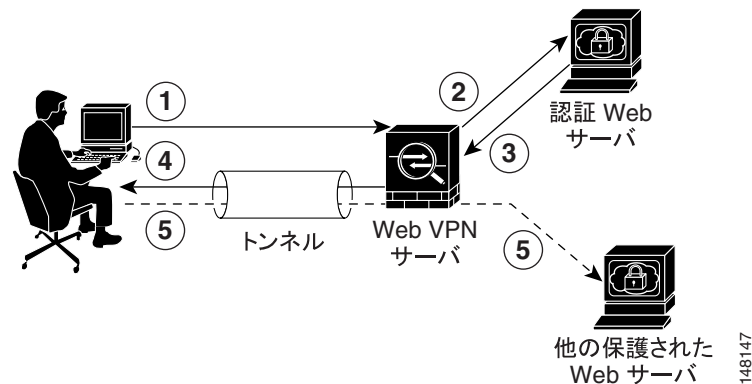
HTTP プロトコルを使用して SSO を正しく設定するには、認証および HTTP プロトコル交換に関する実用的な知識が必要です。

セキュリティ アプライアンスは、ここでも認証 Web サーバに対する WebVPN ユーザのプロキシとして動作しますが、この場合は、要求に対して HTTP Form プロトコルと POST 方式を使用します。フォーム データを送受信するためにセキュリティ アプライアンスを設定する必要があります。[図 30-1](#) は、次の SSO 認証の手順を示したものです。

1. 最初に、WebVPN ユーザは、ユーザ名とパスワードを入力してセキュリティ アプライアンス上の WebVPN サーバにログインします。
2. ユーザのプロキシとして動作する WebVPN サーバは、このフォーム データ（ユーザ名およびパスワード）を、POST 認証要求によって認証する Web サーバに転送します。
3. 認証する Web サーバがユーザのデータを承認した場合は、ユーザの代行で保管していた認証クッキーを WebVPN サーバに戻します。
4. WebVPN サーバはユーザまでのトンネル接続を確立します。
5. これでユーザは、ユーザ名やパスワードを再入力しなくても、保護された SSO 環境内の他の Web サイトにアクセスできるようになります。



図 30-1 HTTP Form による SSO 認証



セキュリティ アプライアンスでユーザ名やパスワードなどの POST データを含めるようにするフォームパラメータを設定するときに、Web サーバが追加的に要求する非表示パラメータの中には、ユーザ側で当初認識できないものがある場合があります。認証アプリケーションによっては、ユーザ側に表示されず、ユーザが入力もしない非表示データを要求する場合があります。しかし、認証 Web サーバが要求する非表示パラメータを見つけることは可能です。これは、セキュリティ アプライアンスを仲介役のプロキシとして使用せずに、ユーザのブラウザから Web サーバに直接認証要求を出す方法で行います。HTTP ヘッダー アナライザを使用して Web サーバの応答を分析すると、非表示パラメータが次のような形式で表示されます。

```
<param name>=<URL encoded value>&<param name>=<URL encoded>
```

非表示パラメータには、必須のパラメータとオプションのパラメータとがあります。Web サーバが非表示パラメータのデータを要求した場合は、そのデータを省略するすべての認証 POST 要求を拒否します。非表示パラメータが必須かオプションかについてはヘッダー アナライザでは分からないので、必須であることが判別できるまではすべての非表示パラメータを含めることを推奨します。

この項の内容は次のとおりです。

- [HTTP Form データの収集](#)
- [タスクの概要：HTTP Form プロトコルによる SSO の設定](#)
- [タスクの詳細：HTTP Form プロトコルによる SSO の設定](#)

## HTTP Form データの収集

この項では、必要な HTTP Form データを検出および収集する手順を示します。認証 Web サーバが要求するパラメータが何か分からない場合は、次の手順を実行して認証交換を分析するとパラメータデータを収集することができます。



(注)

これらの手順では、ブラウザと HTTP ヘッダー アナライザが必要です。

- ステップ 1** ユーザのブラウザと HTTP ヘッダー アナライザを起動して、セキュリティ アプライアンスを経由せずに Web サーバのログイン ページに直接接続します。
- ステップ 2** Web サーバのログイン ページがユーザのブラウザにロードされてから、ログイン シーケンスを検証して交換時にクッキーが設定されているかどうか判別します。Web サーバによってログイン ページにクッキーがロードされている場合は、このログイン ページの URL を *start-URL* として設定します。

**ステップ 3** Web サーバにログインするためのユーザ名とパスワードを入力して、Enter キーを押します。この動作によって、ユーザが検証する認証 POST 要求が HTTP ヘッダー アナライザで生成されます。

次に、ホストの HTTP ヘッダーおよび本文が記載された POST 要求の例を示します。

```
POST
/emco/myemco/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000430e1-7443-125c-ac0
5-83846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5Fzmjnk3DRNwNjk2KcqVCFb
IrNT9%2bJ0H0KpshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.com%2Femco%2F
myemco%2F HTTP/1.1
Host: www.example.com
(BODY)
SMENC=ISO-8859-1&SMLOCALE=US-EN&USERID=Anyuser&USER_PASSWORD=XXXXXX&target=https%3A%2F
%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0
```

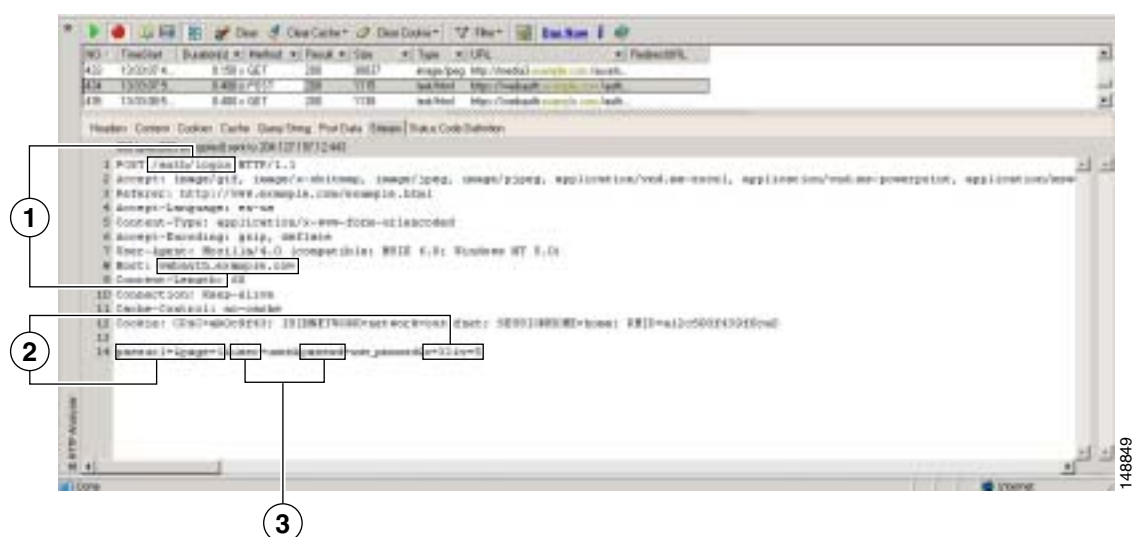
**ステップ 4** POST 要求を検証してプロトコル、ホストをコピーし、URL を入力して、action-uri パラメータを設定します。

**ステップ 5** POST 要求の本文を検証して、次の情報をコピーします。

- ユーザ名パラメータ。上記の例では、このパラメータは USERID で、値は anyuser ではありません。
- パスワードパラメータ。上記の例では、このパラメータは USER\_PASSWORD です。
- 非表示パラメータ。このパラメータは、POST 本文からユーザ名パラメータとパスワードパラメータを除くすべてです。上記の例で言うと、非表示パラメータは、SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0 の部分です。

図 30-2 に、HTTP アナライザの出力例に表示される action URI、非表示データ、ユーザ名、パスワードの各種パラメータを示します。これは一例です。出力は Web サイトによって大幅に異なることがあります。

図 30-2 action-uri、非表示、ユーザ名、パスワードの各種パラメータ



|   |                      |
|---|----------------------|
| 1 | action URI パラメータ     |
| 2 | 非表示パラメータ             |
| 3 | ユーザ名パラメータとパスワードパラメータ |

**ステップ 6** Web サーバへのログインが成功したら、HTTP ヘッダー アナライザを使用して、サーバからユーザのブラウザ内に設定されているセッションのクッキー名を見つけ出すことによって、サーバの応答を検証します。ここで **auth-cookie-name** パラメータを使用します。

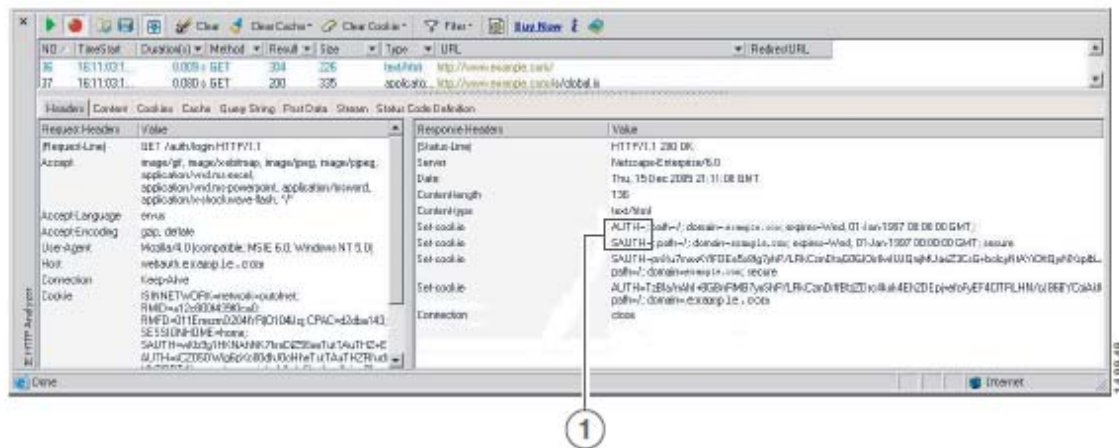
次のサーバ応答ヘッダーでは、SMSESSION がセッションのクッキーの名前です。必要なのはこの名前だけです。値は不要です。

Set-Cookie:

```
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+ltwie0gqnjbhkTkUnR8XWP3hvDH6PZPBHIHTWLD
KTA8ngDB/1bYtjIxrBdX8WPWwG3CxVa3adOxHFR8yJD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw
+MGiW0o88uHa2t4l+SillqfJvcpuXfiIAO06D/gtDF40Ow5YKHE12KhDEvv+yQzxfEz2cl7Ef5iMr8LgGcDK7
qvMcvrgUqx68JQOK2+RSwtHQ15bCZmsDU5vQVCvSQWC8OMHNGwps253XwRLvd/h6S/tM0k98QMv+i3N8oOdj1V
7f1BqecH7+kVrU01F6oFzr0zM1kMyLr5Hh1VDh7B0k9wp0dUFZiAzaf43jupD5f6CEkuLeudYW1xgNzsR8eqtP
K6t1gFJyOn0s7QdNQ7q9knsPJsekRAH9hrLBhWBLTU/3B1QS94wEGD2YTuiW36TiP14hYw0lCAYRj2/bY3+lyz
Vu7EmzMQ+UefYxh4cF2gYD8RZL2Rwmp9JV5148I3XBFPNUw/3V5jf7nRuLr/CdfK3008+Pa3V6/nNhokErSgyx
jzMd88DVzM41LxxaUDhbcmkOHT9ImzBvKzJX0J+o7FoUDFOxEdIq1AN4GNqk49cpi2sXDbIarALp6B13+tbB4M
lHGH+0CPscZXqoi/kon9YmGauHyRs+0m6wthdlAmCnvlJCDfDoXtn8DpabgiW6VDTrvl3SGPyQtUv7Wdahug5S
xbUzjY2JxQnrUtwB977NCzYu2sOtN+dsEReWJ6ueyJBbMzKyzUB4L3i5uSYN50B4PCv1w5KdRka5p3N0Nfq6RM
6dfipMEJw0Ny1sZ7ohz3fbvQ/YZ7lw/k7ods/8VbaR15ivkE8dSCzuf/AInHtCzuQ6wApzEp9CUoG8/dapWriH
jNoi41lJOGCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma5dc/emWor9vWr0HnTQaHP5rg5dTNqunkDEd
MIHfibeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.example.com;Path=/
```

図 30-3 に、HTTP アナライザによる認可クッキーの出力例を示します。これは一例です。出力は Web サイトによって大きく異なります。

図 30-3 HTTP アナライザの出力例に表示された認可クッキー



## 1 認可クッキー

**ステップ 7** この場合は、認証の成否に関わらず同じクッキーがサーバによって設定される可能性があり、このようなクッキーは SSO の目的上、認められません。クッキーが異なっていることを確認するには、無効なログイン クレデンシャルを使用して、「失敗した」クッキーと「成功した」クッキーとを **ステップ 1** から **ステップ 6** を繰り返して比較します。

これで、HTTP Form プロトコルによる SSO をセキュリティ アプライアンスに設定するために必要なパラメータ データを入手できました。

## タスクの概要：HTTP Form プロトコルによる SSO の設定

この項では、HTTP Form プロトコルを使用した SSO の設定の概要について説明します。HTTP によって SSO をイネーブルにするには、次のタスクを実行します。

- フォーム データ (**action-uri**) を受信および処理するために、認証 Web サーバの Uniform Resource Identifier (URI; ユニフォーム リソース識別子) を設定する。
- ユーザ名パラメータ (**user-parameter**) を設定する。
- ユーザ パスワード パラメータ (**password-parameter**) を設定する。

認証 Web サーバの要件によっては次のタスクが必要になる場合もあります。

- 認証サーバがログイン前のクッキー交換を必要とする場合は、開始 URL (**start-url**) を設定する。
- 認証 Web サーバが要求する任意の非表示認証パラメータ (**hidden-parameter**) を設定する。
- 認証 Web サーバによって設定される認証クッキーの名前 (**auth-cookie-name**) を設定する。

## タスクの詳細：HTTP Form プロトコルによる SSO の設定

この項では、HTTP Form プロトコルを使用した SSO を設定するために必要な詳細タスクを取り上げます。セキュリティ アプライアンスが HTTP Form プロトコルを使用した SSO を実行するように設定するには、次の手順を実行します。

- ステップ 1** 認証 Web サーバが要求する場合は、aaa-server-host コンフィギュレーション モードで **start-url** コマンドを入力して、認証 Web サーバから事前ログイン クッキーを取得するための URL を指定します。たとえば、`http://example.com/east/Area.do?Page-Grp1` の URL 認証 Web サーバを、IP アドレス 10.0.0.2 の testgrp1 サーバ グループに指定するには、次のように入力します。

```
hostname(config)# aaa-server testgrp1 host 10.0.0.2
hostname(config-aaa-server-host)# start-url http://example.com/east/Area.do?Page-Grp1
hostname(config-aaa-server-host)#
```

- ステップ 2** 認証 Web サーバに認証プログラム用の URI を指定するには、aaa-server-host コンフィギュレーション モードで **action-uri** コマンドを入力します。1 つの URI を連続する複数行にわたって入力することができます。1 行あたりの最大文字数は 255 です。URI 全体の合計の最大文字数は 2048 です。action URI の出力例は次のとおりです。

```
http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxxHqLw%3d%3d&TARGET=https%3A%2F%2Fauth.example.com
```

この action URI を指定するには、次のコマンドを入力します。

```
hostname(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
hostname(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
hostname(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
hostname(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
hostname(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
hostname(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
hostname(config-aaa-server-host)# action-uri B1UV2PxxHqLw%3d%3d&TARGET=https%3A%2F
hostname(config-aaa-server-host)# action-uri %2Fauth.example.com
hostname(config-aaa-server-host)#
```



(注)

action URI には、ホスト名およびプロトコルを含めることができます。上記の例では、これらは、`http://www.example.com` の URI の最初に表示されます。

- ステップ 3** HTTP POST 要求のユーザ名パラメータを設定するには、aaa-server-host コンフィギュレーション モードで、**user-parameter** コマンドを入力します。たとえば、次のようにコマンドを入力すると、ユーザ名パラメータ `userid` が設定されます。

```
hostname(config-aaa-server-host)# user-parameter userid
hostname(config-aaa-server-host)#
```

- ステップ 4** HTTP POST 要求のユーザ パスワード パラメータを設定するには、aaa-server-host コンフィギュレーション モードで、**password-parameter** コマンドを入力します。たとえば、次のようにコマンドを入力すると、ユーザ パスワード パラメータ名として `user_password` が設定されます。

```
hostname(config-aaa-server-host)# password-parameter user_password
hostname(config-aaa-server-host)#
```

- ステップ 5** 認証 Web サーバと交換する非表示パラメータを指定するには、aaa-server-host コンフィギュレーション モードで、**hidden-parameter** コマンドを入力します。次に、POST 要求から抜粋した非表示パラメータの例を示します。

```
SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2F
appdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0
```

この非表示パラメータには、間を & で区切った 4 つの Form エントリとその値が含まれています。4 つのエントリとその値は次のとおりです。

- SMENC エントリおよび値 ISO-8859-1
- SMLOCALE エントリおよび値 US-EN
- target エントリと値 `https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG`
- smauthreason エントリと値 0

この非表示パラメータを指定するには、次のコマンドを入力します。

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# hidden-parameter
SMENC=ISO-8859-1&SMLOCALE=US-EN&target=
hostname(config-aaa-server-host)# hidden-parameter
t=https%3A%2F%2Fwww.example.com%2Femc
hostname(config-aaa-server-host)# hidden-parameter
o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
hostname(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
hostname(config-aaa-server-host)#
```

**ステップ 6** 認証クッキーの名前を指定するには、aaa-server-host コンフィギュレーション モードで、**auth-cookie-name** コマンドを入力します。このコマンドをはオプションです。次に、SsoAuthCookie という名前の認証クッキーを指定する例を示します。

```
hostname(config-aaa-server-host)# auth-cookie-name SsoAuthCookie  
hostname(config-aaa-server-host)#
```

---

## デジタル証明書による認証

デジタル証明書を使用して認証を行う WebVPN ユーザは、グローバルな認証と認可の設定を使用しません。その代わり、証明書の検証が完了すると、ユーザは認可サーバを使用して認証します。デジタル証明書を使用する認証と認可の詳細については、「[AAA サーバとローカル データベースの設定](#)」の「[証明書とユーザ ログイン クレデンシャルの使用方法](#)」を参照してください。

## WebVPN ポリシーの作成と適用

中央にあるリソースへのアクセスを制御する WebVPN ポリシーを作成および適用するには、次の作業を実行します。

- グローバル コンフィギュレーション モードでのポート転送、URL、およびアクセスリストの作成
- グループポリシー モードまたはユーザ モードでのグループポリシーとユーザへのリストの割り当て
- グループポリシーとユーザ用の機能のイネーブル化
- グループポリシーへのユーザの割り当て

第 26 章「トンネルグループ、グループポリシー、およびユーザの設定」では、これらのタスクについて詳細な手順で説明しています。

### グローバル コンフィギュレーション モードでのポート転送、URL、およびアクセスリストの作成

転送するポートと WebVPN ユーザに提示する URL のリストを設定し、これらのアクセス レベルを設定するには、グローバル コンフィギュレーション モードで **port forward** コマンド、**url-list** コマンド、および **access-list** コマンドを使用します。

### グループポリシー モードまたはユーザ モードでのグループポリシーとユーザへのリストの割り当て

ポート転送と URL リストを設定したら、webvpn グループポリシー モードまたはユーザ モードで **port forward** コマンド、**url-list** コマンド、および **filter** コマンドを使用して、グループポリシーやユーザにリストを割り当てます。

### グループポリシーとユーザ用の機能のイネーブル化

グループポリシーとユーザ用の機能をイネーブルにするには、グループポリシー モードまたはユーザ コンフィギュレーション モードで **functions** コマンドを発行します。

### グループポリシーへのユーザの割り当て

ユーザをグループポリシーに割り当てると、複数のユーザにポリシーを適用することで設定が容易になります。ユーザをグループポリシーに割り当てするには、内部の認証サーバまたは RADIUS サーバを使用することができます。グループポリシーを使用して設定を簡略化する説明の詳細については、第 26 章「トンネルグループ、グループポリシー、およびユーザの設定」を参照してください。

### セキュリティ アプライアンス認証サーバを使用する

セキュリティ アプライアンスの内部認証サーバでユーザを認証するように設定し、これらのユーザをセキュリティ アプライアンス上でグループポリシーに割り当てることもできます。

## RADIUS サーバを使用する

RADIUS サーバをユーザ認証に使用する場合は、次の手順を実行して、ユーザをグループポリシーに割り当てます。

---

**ステップ 1** RADIUS でユーザ認証を行い、Class アトリビュートを使用してそのユーザを特定のグループポリシーに割り当てます。

**ステップ 2** OU=group\_name 形式で Class アトリビュートをグループポリシー名に設定します。

たとえば、WebVPN ユーザを SSL\_VPN グループに割り当てるには、RADIUS Class アトリビュートを `OU=SSL_VPN;`（セミコロンは省略不可）の値に設定します。

---



## WebVPN トンネルグループ アトリビュートの定義

表 30-1 は、WebVPN に特有のトンネルグループ アトリビュートをリストで示したものです。これらのアトリビュートに加えて、すべての VPN 接続に共通する一般的なトンネルグループ アトリビュートを設定します。トンネルグループを設定するための詳細な手順については、第 26 章「トンネルグループ、グループポリシー、およびユーザの設定」の「WebVPN トンネルグループの設定」を参照してください。

表 30-1 WebVPN トンネルグループ アトリビュート

| コマンド                         | 機能                                                                                                                                                              |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>authentication</b>        | 認証方式を設定します。                                                                                                                                                     |
| <b>customization</b>         | 以前に定義した、適用対象のカスタマイゼーションの名前を指定します。                                                                                                                               |
| <b>nbns-server</b>           | CIFS 名前解決用の NetBIOS ネーム サービス サーバの名前（nbns-server）を指定します。                                                                                                         |
| <b>group-alias</b>           | サーバがトンネルグループの参照に使用できる代替名を指定します。                                                                                                                                 |
| <b>group-url</b>             | 1 つ以上のグループの URL を指定します。このアトリビュートを設定すると、指定した URL に着信するユーザはログイン時にグループを選択する必要がありません                                                                                |
| <b>dns-group</b>             | DNS サーバ名、ドメイン名、ネーム サーバ、リトライの回数、およびタイムアウト値を指定する DNS サーバグループを指定します。                                                                                               |
| <b>hic-fail-group-policy</b> | Cisco Secure Desktop Manager を使用してグループベースのポリシー アトリビュートを「Use Failure Group-Policy」または「Use Success Group-Policy, if criteria match」に設定する場合の VPN フィーチャ ポリシーを指定します。 |

## WebVPN グループポリシーとユーザアトリビュートの設定

表 30-2 に、WebVPN グループポリシーアトリビュートとユーザアトリビュートをリストで示します。グループポリシーアトリビュートとユーザアトリビュートの詳細な設定手順については、第 26 章「トンネルグループ、グループポリシー、およびユーザの設定」の「グループポリシーの設定」および「特定ユーザのアトリビュートの設定」を参照してください。

**表 30-2 WebVPN グループポリシーアトリビュートとユーザアトリビュート**

| コマンド                       | 機能                                                                                                                    |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>auto-signon</b>         | 自動サインオンの値を設定します。設定では WebVPN への初回の接続のみユーザ名およびパスワードのクレデンシャルが必要です。                                                       |
| <b>customization</b>       | カスタマイゼーションオブジェクトをグループポリシーまたはユーザに割り当てます。                                                                               |
| <b>deny-message</b>        | WebVPN へのログインに成功したが VPN 特権を持たないリモートユーザに送信されるメッセージを指定します。                                                              |
| <b>filter</b>              | webtype アクセスリストの名前を設定します。                                                                                             |
| <b>functions</b>           | WebVPN 機能（自動ダウンロード、Citrix、ファイルアクセス、ファイルブラウジング、ファイルエントリ、フィルタリング、HTTP プロキシ、URL エントリ、MAPI プロキシ、ポート転送）の一部または全部をイネーブルにします。 |
| <b>homepage</b>            | ログイン時に表示される Web ページの URL を設定します。                                                                                      |
| <b>html-content-filter</b> | このグループポリシー用の HTML からフィルタリングするコンテンツとオブジェクトを設定します。                                                                      |
| <b>http-comp</b>           | 圧縮を設定します。                                                                                                             |
| <b>keep-alive-ignore</b>   | セッションタイマーのアップデートを無視する最大オブジェクトサイズを設定します。                                                                               |
| <b>port-forward</b>        | 転送する WebVPN TCP ポートのリストを適用します。ユーザインターフェイスにこのリスト上のアプリケーションが表示されます。                                                     |
| <b>port-forward-name</b>   | ポート転送アプレットの名前を設定します。                                                                                                  |
| <b>sso-server</b>          | SSO サーバの名前を設定します。                                                                                                     |
| <b>svc</b>                 | SSL VPN クライアントのアトリビュートを設定します。                                                                                         |
| <b>url-list</b>            | エンドユーザのアクセス用にユーザインターフェイスで表示される WebVPN サーバと URL のリストを適用します。                                                            |

## Application Access の設定

次の各項では、Application Access の設定について説明します。

[ポート転送アプレットの自動ダウンロード](#)

[hosts ファイル エラーを回避するための Application Access の終了](#)

[Application Access 使用時の hosts ファイル エラーの回復](#)

### ポート転送アプレットの自動ダウンロード

WebVPN を介してリモート アプリケーションを実行するには、WebVPN ホームページの **Start Application Access** をクリックしてポート転送 Java アプレットをダウンロードし、起動します。アプリケーションのアクセスを簡略化して起動時間を短縮するには、WebVPN にユーザが最初にログインした時点で、このポート転送アプレットを自動的にダウンロードするように WebVPN を設定できます。

ポート転送アプレットの自動ダウンロードをイネーブルにするには、webvpn モードから **auto-download** オプションと共に **functions** コマンドを入力します。



(注)

自動ダウンロード機能を設定する前に、ポート転送、Outlook/Exchange プロキシまたは HTTP プロキシなどのアプレットを使用するアプリケーションを最初にイネーブルにする必要があります。

### hosts ファイル エラーを回避するための Application Access の終了

Application Access の実行の妨げになる hosts ファイル エラーを回避するために、Application Access を使用し終わったら Application Access ウィンドウを正しく閉じるようにします。終了するには、close アイコンをクリックします。

### Application Access 使用時の hosts ファイル エラーの回復

Application Access ウィンドウを正しく閉じないと次のエラーが発生することがあります。

- 次に Application Access を起動しようとしたときに、Application Access がディセーブルになっていて、Backup HOSTS File Found エラー メッセージが表示される。
- アプリケーションをローカルで実行している場合でも、アプリケーション自体がディセーブルになっているか、または動作しない。

このようなエラーは、Application Access ウィンドウを不適切な方法で終了したことが原因です。次の例を参考にしてください。

- Application Access の使用中に、ブラウザがクラッシュした。
- Application Access の使用中に、停電またはシステム シャットダウンが発生した。
- 作業中に Application Access ウィンドウを最小化し、このウィンドウがアクティブな状態（ただし最小化されている）でコンピュータをシャットダウンした。

ここでは、次の項目について説明します。

- [hosts ファイルの概要](#)
- [不正な Application Access の終了](#)
- [hosts ファイルの再設定](#)

## hosts ファイルの概要

ローカル システム上の hosts ファイルは、IP アドレスをホスト名にマッピングしています。Application Access を起動すると、WebVPN は hosts ファイルを修正し、WebVPN 固有のエントリを追加します。Application Access ウィンドウを正しく閉じて Application Access を終了すると、hosts ファイルは元の状態に戻ります。

|                         |                                                                                                                                                                  |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Access の起動前 | hosts ファイルは元の状態です。                                                                                                                                               |
| Application Access の起動時 | <ul style="list-style-type: none"> <li>WebVPN は hosts ファイルを hosts.webvpn にコピーして、バックアップを作成します。</li> <li>次に WebVPN は hosts ファイルを編集し、WebVPN 固有の情報を挿入します。</li> </ul> |
| Application Access の終了時 | <ul style="list-style-type: none"> <li>WebVPN はバックアップ ファイルを hosts ファイルにコピーして、hosts ファイルを元の状態に戻します。</li> <li>WebVPN は hosts.webvpn を削除します。</li> </ul>             |
| Application Access の終了後 | hosts ファイルは元の状態です。                                                                                                                                               |



(注)

Microsoft アンチスパイウェア ソフトウェアは、ポート転送 JAVA アプレットによる hosts ファイルの変更をブロックします。アンチスパイウェア ソフトウェアの使用時に hosts ファイルの変更を許可する方法の詳細については、[www.microsoft.com](http://www.microsoft.com) を参照してください。

## 不正な Application Access の終了

Application Access が正しく終了しなかった場合、hosts ファイルは WebVPN 用にカスタマイズされた状態のままになっています。ユーザが次に Application Access を起動するときに、WebVPN は hosts.webvpn ファイルを検索することで、Application Access の状態をチェックします。hosts.webvpn ファイルが検出されると、Backup HOSTS File Found エラー メッセージ (図 30-4) が表示され、Application Access が一時的にディセーブルになります。

Application Access を正しくシャットダウンしないと、リモートアクセス クライアント / サーバ アプリケーションが不安定な状態のままになります。WebVPN を使用せずにこれらのアプリケーションを起動しようとすると、正しく動作しない場合があります。通常の接続先のホストが使用できなくなる場合があります。一般にこのような状況は、自宅からリモートでアプリケーションを実行し、Application Access ウィンドウを終了せずにコンピュータをシャットダウンし、その後職場でそのアプリケーションを実行しようとした場合に発生します。

## hosts ファイルの再設定

Application Access または正しく動作しないアプリケーションを再度イネーブルにするには、次の手順を実行します。

- リモートアクセス サーバに接続できる場合は、「[WebVPN による hosts ファイルの自動再設定](#)」の項で説明されている手順を実行してください。
- 現在の場所からリモートアクセス サーバに接続できない場合や、hosts ファイルをカスタム編集した場合は、「[手動による hosts ファイルの再設定](#)」で説明されている手順に従ってください。

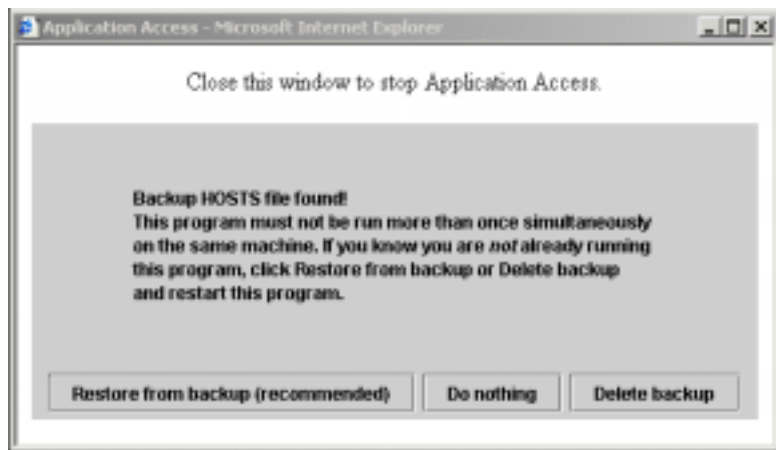
## WebVPN による hosts ファイルの自動再設定

リモートアクセス サーバに接続できる場合は、hosts ファイルを再設定し、Application Access やアプリケーションを再度イネーブルにするために、次の手順を実行します。

**ステップ 1** WebVPN を起動してログインします。ホームページが開きます。

**ステップ 2** Applications Access リンクをクリックします。Backup HOSTS File Found メッセージが表示されます（図 30-4 を参照）。

図 30-4 Backup HOSTS File Found メッセージ



**ステップ 3** 次のいずれかのオプションを選択します。

- **Restore from backup** : WebVPN は強制的に正しくシャットダウンされます。WebVPN は hosts.webvpn backup ファイルを hosts ファイルにコピーし、hosts ファイルを元の状態に戻してから、hosts.webvpn を削除します。その後、Application Access を再起動する必要があります。
- **Do nothing** : Application Access は起動しません。リモートアクセスのホームページが再び表示されます。
- **Delete backup** : WebVPN は hosts.webvpn ファイルを削除し、hosts ファイルを WebVPN 用にカスタマイズされた状態にしておきます。元の hosts ファイル設定は失われます。Application Access は、WebVPN 用にカスタマイズされた hosts ファイルを新しいオリジナルとして使用して起動します。このオプションは、hosts ファイル設定が失われても問題がない場合にだけ選択してください。Application Access が不適切にシャットダウンされた後に、ユーザまたはユーザが使用するプログラムによって hosts ファイルが編集された可能性がある場合は、他の 2 つのオプションのどちらかを選択するか、または hosts ファイルを手動で編集します（「[手動による hosts ファイルの再設定](#)」を参照）。

## 手動による hosts ファイルの再設定

現在の場所からリモートアクセス サーバに接続できない場合や、カスタマイズした hosts ファイルの編集内容を失いたくない場合は、次の手順に従って、hosts ファイルを再設定し、Application Access とアプリケーションを再度イネーブルにします。

**ステップ 1** hosts ファイルを見つけて編集します。最も一般的な場所は、c:\windows\system32\drivers\etc\hosts です。

**ステップ 2** # added by WebVpnPortForward という文字列が含まれている行があるかどうかをチェックします。この文字列を含む行がある場合、hosts ファイルは WebVPN 用にカスタマイズされています。hosts ファイルが WebVPN 用にカスタマイズされている場合、次の例のようになっています。

```
123.0.0.3 server1 # added by WebVpnPortForward
123.0.0.3 server1.example.com vpn3000.com # added by WebVpnPortForward
123.0.0.4 server2 # added by WebVpnPortForward
123.0.0.4 server2.example.com vpn3000.com # added by WebVpnPortForward
123.0.0.5 server3 # added by WebVpnPortForward
123.0.0.5 server3.example.com vpn3000.com # added by WebVpnPortForward

# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       cisco.example.com          # source server
#       38.25.63.10       x.example.com              # x client host

123.0.0.1                localhost
```

**ステップ 3** # added by WebVpnPortForward という文字列が含まれている行を削除します。

**ステップ 4** hosts ファイルを保存してから閉じます。

**ステップ 5** WebVPN を起動してログインします。

ホームページが開きます。

**ステップ 6** Application Access リンクをクリックします。

Application Access ウィンドウが表示されます。これで Application Access がイネーブルになります。

## ファイル アクセスの設定

Common Internet File System (CIFS; 共通インターネット ファイル システム) プロトコルは、ファイル、プリンタ、および他のマシン リソースへのネットワーク アクセスをユーザに提供します。Microsoft では、Windows コンピュータのネットワークで CIFS を実装しています。一方、CIFS のオープン ソース実装では、Linux、UNIX、および Mac OS X など他のオペレーティング システムを実行するサーバへのファイル アクセスも提供しています。

WebVPN は、リモート ユーザに HTTPS ポータル ページを提供しています。このページは、セキュリティ アプライアンス上で稼動するプロキシ CIFS クライアントとのインターフェイスになっています。WebVPN は、このクライアントを使用して、ユーザが認証の要件を満たしてファイルのプロパティがアクセスを制限しない限り、ネットワーク上のファイルへのネットワーク アクセスをユーザに提供します。クライアントは透過的です。WebVPN から送信されるポータル ページでは、ファイル システムに直接アクセスしているかのように見えます。

ユーザがファイルのリストを要求すると、WebVPN は、そのリストが含まれるサーバの IP アドレスをマスター ブラウザに指定されているサーバに照会します。セキュリティ アプライアンスはリストを入手してポータル ページ上のリモート ユーザに送信します。

WebVPN は、ユーザの認証要求とファイルのプロパティに応じて、ユーザが次の CIFS の機能と呼び出すことができるようにします。

- ドメインおよびワークグループへの移動とリスト、ドメインまたはワークグループ内のサーバへの移動とリスト、サーバ内部の共有、共有部分またはディレクトリ内でのファイルの共有
- ディレクトリの作成
- ファイルのダウンロード、アップロード、移動、削除

セキュリティ アプライアンスは、通常、同じネットワーク上か、またはこのネットワークからアクセス可能な場所にマスター ブラウザまたは WINS サーバが必要です。これは、リモート ユーザが WebVPN ホームページまたはツールバー上の Browse Networks をクリックしたときにサーバ リストのクエリーがネットワークに送信されるようにするためです (図 30-5)。

図 30-5 WebVPN ホームページとフローティング ツールバーのネットワークのブラウズ





マスター ブラウザには、セキュリティ アプライアンス上の CIFS クライアントと、Web VPN がリモート ユーザに提供するネットワーク リソースのリストが表示されます。マスター ブラウザに DNS サーバを使用することはできません。WebVPN は、WINS サーバを使用した Active Native Directory 環境でのファイル アクセスをサポートしますが、ダイナミック DNS サーバでのアクセスはサポートしません。

次に示す手順 1 は、マスター ブラウザと WINS サーバの指定方法について説明します。手順 1 の代わりに、グローバル コンフィギュレーション モードか、グループポリシーまたはユーザ名モードから入る webvpn モードで **url-list** コマンドを使用して、File Folder Bookmark にサーバ共有を設定することができます。次の例を参考にしてください。

```
url-list listname displayname cifs://ServerA/ShareX/
```

この方法(共有を追加)では、マスター ブラウザまたは WINS サーバは不要ですが、Browse Networks リンクはサポートされません。このコマンドの入力時に ServerA を参照するためのホスト名または IP アドレスが使用できます。ホスト名を使用する場合、セキュリティ アプライアンスには IP アドレスを解決するための DNS サーバが必要です。



(注)

ファイル アクセスを設定する前に、ユーザ アクセス用のサーバに共有を設定する必要があります。

次の手順を実行して CIFS のファイル アクセスをサポートするようにします。

- ステップ 1** NetBIOS Name Server (NBNS) ごとに 1 回ずつ、トンネルグループの webvpn コンフィギュレーション モードで、**nbns-server** コマンドを使用します。

```
nbns-server {IPaddress | hostname} [master] [timeout timeout] [retry retries]
```

**master** は、マスター ブラウザに指定されるコンピュータです。マスター ブラウザは、コンピュータと共有リソースのリストを保持します。コマンドのマスター部分を入力せずにこのコマンドで指定する任意の NBNS サーバは、Windows Internet Naming Server (WINS) である必要があります。まずマスター ブラウザを指定してから、WINS サーバを指定してください。トンネルグループ用のマスター ブラウザを含め、サーバは最大 3 つまで指定できます。

**retries** は、NBNS サーバに対するクエリーのリトライ回数です。セキュリティ アプライアンスは、この回数だけサーバのリストを再利用してからエラー メッセージを送信します。デフォルト値は 2 で、範囲は 1 ～ 10 です。

**timeout** は、セキュリティ アプライアンスが、クエリーを再度サーバに送信する前に待機する秒数です。このとき、サーバが 1 つしかない場合は同じサーバに送信し、サーバが複数存在する場合は別のサーバに送信します。デフォルトのタイムアウトは 2 秒で、範囲は 1 ～ 30 秒です。

次に例を示します。

```
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.20 master
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.41
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.47
```



(注)

トンネルグループのコンフィギュレーションにすでに存在する NBNS サーバを表示する場合は、**tunnel-group webvpn-attributes** コマンドを使用します。



**ステップ 2** (オプション) WebVPN のポータル ページをリモート ユーザに送信するために符号化する文字セットを指定する **character-encoding** コマンドを使用します。デフォルトでは、リモート ブラウザ上の符号化タイプセットで WebVPN ポータル ページの文字セットが決定されるため、ユーザは、ブラウザで符号化を適切に実行するために必要となる場合に限り、文字の符号化を設定する必要があります。

#### **character-encoding charset**

Charset は、最大 40 文字からなる文字列で、<http://www.iana.org/assignments/character-sets> で指定されたいずれかの有効文字セットと同じです。このページのリストにある名前またはエイリアスのいずれかを使用できます。例には、iso-8859-1、shift\_jis、および ibm850 が含まれています。



(注)

character-encoding 値および file-encoding 値では、ブラウザが使用するフォント ファミリを除外しません。これらの値のいずれかに対し、次の例で示すように日本語の Shift JIS 文字符号化を使用する場合は、webvpn カスタマイゼーション コマンド モードの **page style** コマンドを使用してフォント ファミリを置き換えるか、webvpn カスタマイゼーション コマンド モードで **no page style** コマンドを入力してフォント ファミリを削除することにより、設定を補う必要があります。

次に、日本語の Shift JIS 文字をサポートしてフォント ファミリを削除し、さらにデフォルトの背景色を保持するための character-encoding アトリビュートを設定する例を示します。

```
hostname(config-webvpn)# character-encoding shift_jis
hostname(config-webvpn)# customization DfltCustomization
hostname(config-webvpn-custom)# page style background-color:white
hostname(config-webvpn-custom)#
```

**ステップ 3** (オプション) 特定の CIFS サーバの Web VPN ポータル ページの符号化を指定する **file-encoding** コマンドを使用します。このため、これ以外の文字の符合化が必要な各 CIFS サーバに対し、異なるファイル符号化値を使用できます。

#### **file-encoding {server-name | server-ip-address} charset**

次の例では、IBM860 (エイリアス「CP860」) 文字をサポートするために、CIFS サーバ 10.86.5.174 にファイル符号化アトリビュートを設定しています。

```
hostname(config-webvpn)# file-encoding 10.86.5.174 cp860
hostname(config-webvpn)#
```

**ステップ 4** ファイル アクセス、ファイルのブラウジング、およびファイル サーバ エントリをサポートするようにセキュリティ アプライアンスを設定するために、グループポリシー モードまたはユーザ名モードから入る webvpn モードで、**functions** コマンドを使用します。

#### **functions file-access file-browsing file-entry**

次の例を参考にしてください。

```
hostname(config-group-webvpn)# functions file-access file-browsing file-entry
hostname(config-group-policy)#
```

これらのコマンドの詳細については、『Cisco Security Appliance Command Reference』を参照してください。

## Citrix MetaFrame サービスへのアクセスの設定

WebVPN ユーザは、セキュリティ アプライアンスとの接続を通じて Citrix MetaFrame サービスにアクセスすることができます。この設定では、セキュリティ アプライアンスは Citrix のセキュアなゲートウェイとして機能します。次の手順を実行して、Citrix MetaFrame サービスのサポートを設定します。

**ステップ 1** セキュア ゲートウェイを使用しないモードで動作するように Citrix Web Interface ソフトウェアを設定します。

**ステップ 2** リモート ユーザが接続のために Fully-Qualified Domain Name (FQDN; 完全修飾ドメイン名) を使用するセキュリティ アプライアンスのインターフェイスに SSL 証明書をインストールします。



(注)

SSL 証明書の Common Name (CN; 通常名) に IP アドレスを指定しないでください。リモート ユーザは FQDN を使用してセキュリティ アプライアンスとの通信を試みます。リモート PC は、FQDN を解決するために System32\drivers\etc\hosts ファイル内の DNS またはエントリを使用できる必要があります。

**ステップ 3** Citrix サポートをイネーブルにするグループポリシーまたはユーザに対し、**functions citrix** コマンドを 1 回ずつ実行します。

次の例は、FirstGroup という名前のグループポリシーに Citrix を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# functions citrix
hostname(config-group-webvpn)#
```

## PDA での WebVPN の使用

Pocket PC または他の認定された携帯情報端末から WebVPN にアクセスすることができます。セキュリティ アプライアンスの管理者や WebVPN ユーザは、特に何もしなくても、認定された PDA で WebVPN を使用することができます。

シスコでは次の PDA プラットフォームを認定しています。

HP iPaq H4150  
Pocket PC 2003  
Windows CE 4.20.0、ビルド 14053  
Pocket Internet Explorer (PIE)  
ROM バージョン 1.10.03ENG  
ROM 日付：7/16/2004

PDA のバージョンによって、WebVPN に次のような相違点があります。

- ポップアップの WebVPN ウィンドウはバナー Web ページに置き換わっている
- 標準の WebVPN フローティング ツールバーがアイコン バーに置き換わっている。このバーには、Go、Home、および Logout の各種ボタンが表示されます。
- メインの WebVPN ポータル ページに Show Toolbar アイコンがない
- WebVPN のログアウト時に、警告メッセージで PIE ブラウザを正しく閉じる手順が表示される。この手順に従わないで通常の方法でブラウザのウィンドウを閉じると、WebVPN または HTTPS を使用するすべてのセキュアな Web サイトから PIE が切断されません。
- WebVPN は OWA 2000 版および OWA 2003 版の基本認証をサポートする。OWA サーバに基本認証を設定せずに WebVPN ユーザがこのサーバにアクセスしようとするアクセスは拒否されます。
- サポートされていない WebVPN の機能
  - Application Access（ポート転送）および他の Java 依存の各種機能
  - MAPI プロキシ
  - HTTP プロキシ
  - Cisco Secure Desktop（CSD は Microsoft Windows CE 用のサポートは限定的に提供）
  - Microsoft Outlook Web Access (OWA) 5.5
  - Citrix Metaframe 機能（PDA に対応する Citrix ICA クライアント ソフトウェアが装備されていない場合）

## WebVPN を介した電子メールの使用

WebVPN は、電子メールにアクセスする方法をいくつかサポートしています。ここでは、次の方式について説明します。

- [電子メール プロキシの設定](#)
- [MAPI の設定](#)
- [Web 電子メール MS Outlook Web Access の設定](#)

### 電子メール プロキシの設定

WebVPN は IMAP4S、POP3S、および SMTPS 電子メール プロキシをサポートしています。表 30-3 に、電子メール プロキシ ユーザにグローバルに適用されるアトリビュートを示します。

表 30-3 グローバル電子メール プロキシ アトリビュート

| 機能                                            | コマンド                                     | デフォルト値                                             |
|-----------------------------------------------|------------------------------------------|----------------------------------------------------|
| 電子メール プロキシで使用するよう事前に設定されているアカウントिंगサーバを指定します。 | <code>accounting-server-group</code>     | なし                                                 |
| 電子メール プロキシ ユーザ用の認証方式（複数可）を指定します。              | <code>authentication</code>              | IMAP4S：メールホスト（必須）<br>POP3S メールホスト（必須）<br>SMTPS：AAA |
| 電子メール プロキシで使用するよう事前に設定されている認証サーバを指定します。       | <code>authentication-server-group</code> | LOCAL                                              |
| WebVPN で使用するよう事前に設定されている認可サーバを指定します。          | <code>authorization-server-group</code>  | なし                                                 |
| ユーザが接続するには、正常に認可される必要があります。                   | <code>authorization-required</code>      | ディセーブル                                             |
| 認可のユーザ名として使用するピア証明書の DN を指定します。               | <code>authorization-dn-attributes</code> | プライマリ アトリビュート：CN<br>セカンダリ アトリビュート：OU               |
| 使用するグループポリシーの名前を指定します。                        | <code>default-group-policy</code>        | DfltGrpPolicy                                      |
| 指定したインターフェイスで電子メール プロキシをイネーブルにします。            | <code>enable</code>                      | ディセーブル                                             |
| 電子メールと VPN のユーザ名とパスワードとの間の区切り記号を定義します。        | <code>name-separator</code>              | 「:」（コロン）                                           |
| 未処理の未承認セッションの最大数を設定します。                       | <code>outstanding</code>                 | 20                                                 |
| 電子メール プロキシがリスンするポートを設定します。                    | <code>port</code>                        | IMAP4S：993<br>POP3S：995<br>SMTPS：988 <sup>1</sup>  |
| デフォルトの電子メール サーバを指定します。                        | <code>server</code>                      | なし。                                                |
| 電子メールとサーバ名との間の区切り記号を定義します。                    | <code>server-separator</code>            | 「@」                                                |

1. Eudora 電子メール クライアントでは、SMTPS 接続のデフォルトのポートが 988 の場合でも、SMTPS はポート 465 でだけ動作します。

## 電子メールプロキシの証明書認証

電子メール プロキシ接続の証明書認証は、Netscape 7x 電子メール クライアントで機能します。MS Outlook、MS Outlook Express、Eudora など、他の電子メール クライアントは、証明書ストアにアクセスできません。

## MAPI の設定

MS Outlook Exchange プロキシとも呼ばれる MAPI には、次の要件があります。

- MS Outlook Exchange がリモート コンピュータにインストールされている必要があります。
- セキュリティ アプライアンス インターフェイス上で、MS Outlook Exchange プロキシをイネーブルにします。これには、グループポリシー webvpn コマンドの 1 つである **functions** コマンドを入力します。次の例を参考にしてください。

```
hostname(config)# group-policy group_policy_name attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# functions mapi
```

- Exchange サーバの NetBIOS 名を指定します。この Exchange サーバは、セキュリティ アプライアンス DNS サーバと同じドメイン上にあることが必要です。次の例を参考にしてください。

```
hostname(config)# domain domain_name
hostname(config)#
```



(注)

MS Outlook Exchange Mail Proxy を経由して接続されているオープンな MS Outlook クライアントは、Exchange Server 上で定期的にメール チェックを行っているため、接続がオープン状態に保たれます。Outlook がオープンである限り、接続がタイムアウトすることはありません。これは、設定には関係ありません。

## Web 電子メール MS Outlook Web Access の設定

Web 電子メールとは、MS Outlook Web Access for Exchange 2000、Exchange 5.5、および Exchange 2003 のことです。中央サイトに MS Outlook Exchange Server が必要です。また、ユーザが次の作業を行う必要があります。

- WebVPN セッションで、ブラウザに電子メール サーバの URL を入力する。
- プロンプトが表示されたら、電子メール サーバのユーザ名を `domain\username` 形式で入力する。
- 電子メールのパスワードを入力する。

## WebVPN のパフォーマンスの最適化

セキュリティ アプライアンスには、WebVPN のパフォーマンスと機能性を最適化するいくつかの方法があります。パフォーマンスの改善には、キャッシングと Web オブジェクトの圧縮が含まれます。機能性の調整には、コンテンツの変換およびプロキシのバイパスが含まれます。APCF は、コンテンツの変換を調整するための追加的な方法を提供します。この項では、次のトピックを取り上げます。

- [キャッシングの設定](#)
- [コンテンツの変換の設定](#)

### キャッシングの設定

キャッシングを行うと WebVPN のパフォーマンスが向上します。キャッシングによって頻繁に再利用されるオブジェクトはシステム キャッシュに保存され、コンテンツを繰り返しリライトしたり圧縮する必要性を減らすことができます。また、WebVPN とリモート サーバとのトラフィックが軽減されるため、多くのアプリケーションが今までよりはるかに効率的に実行できるようになります。

デフォルトでは、キャッシングはイネーブルになっています。次のように、webvpn モードからキャッシング コマンドを入力すると、ユーザの環境に応じてキャッシング動作をカスタマイズできます。

```
hostname(config)#
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#
```

次に、キャッシング コマンドとその機能のリストを示します。

| キャッシング コマンド      | 機能                                |
|------------------|-----------------------------------|
| cache-compressed | 圧縮したコンテンツをキャッシングします。              |
| disable          | キャッシングをディセーブルにします。                |
| expiry-time      | キャッシング オブジェクトの期限切れの時刻を設定します。      |
| lmfactor         | キャッシングされたオブジェクトを再検証するための用語を設定します。 |
| max-object-size  | キャッシュに入れるオブジェクトの最大サイズを設定します。      |
| min-object-size  | キャッシュに入れるオブジェクトの最小サイズを設定します。      |

### コンテンツの変換の設定

デフォルトでは、セキュリティ アプライアンスは、コンテンツ変換およびリライト エンジンを通じ、JavaScript および Java などの高度な要素からプロキシ HTTP へのトラフィックを含む、すべての WebVPN トラフィックを処理します。このようなトラフィックでは、ユーザがアプリケーションにアクセスするのに SSL VPN デバイス内部からアクセスしているか、これらに依存せずにアクセスしているかによって、セマンティックやアクセス コントロールのルールが異なる場合があります。

Web リソースによっては高度に個別の処理が要求される場合があります。次の各項では、このような処理を提供する機能について説明します。

- [コンテンツのリライトのディセーブル化](#)
- [プロキシのバイパスの使用](#)

- アプリケーション プロファイル カスタマイゼーション フレームワークの設定

組織や関係する Web コンテンツの要件に応じてこれらの機能のいずれかを使用する場合があります。

## コンテンツのリライトのディセーブル化

公開 Web サイトなどの一部のアプリケーションや Web リソースによっては、セキュリティ アプライアンスを通過しない設定が求められる場合があります。このため、セキュリティ アプライアンスでは、特定のサイトやアプリケーションをセキュリティ アプライアンスを通過せずにブラウズできるリライト ルールを作成できます。これは、IPSec VPN 接続のスプリット トンネリングと同様の機能です。

webvpn モードで **rewrite** コマンドと **disable** オプションを使用して、WebVPN トンネル外部にアクセスするためのアプリケーションとリソースを指定します。

この rewrite コマンドは複数回使用できます。セキュリティ アプライアンスはリライト ルールを順序番号に従って検索するため、ルールの順序番号は重要です。このとき、最下位の番号から順に検索して行き、最初に一致したルールが適用されます。

## プロキシのバイパスの使用

ユーザはプロキシ バイパスを使用するようにセキュリティ アプライアンスを設定できます。これは、プロキシ バイパスが提供する特殊なコンテンツ リライト機能を使用した方が、アプリケーションや Web リソースをより有効活用できる場合に設定します。プロキシ バイパスはコンテンツ リライトに代わる手法で、元のコンテンツへの変更を最小限にします。多くの場合、カスタム Web アプリケーションでこれを使用すると有効です。

このコマンドは複数回使用できます。エントリを設定する順序は重要ではありません。インターフェイスとパス マスク、またはインターフェイスとポートを組み合わせることで、プロキシ バイパスのルールを一意に指定できます。

ネットワーク設定に応じてパス マスクではなくポートを使用してプロキシ バイパスを設定する場合、これらのポートからセキュリティ アプライアンスにアクセスできるようにファイアウォール設定を変更する必要がある場合があります。この制約を回避するにはパス マスクを使用します。ただし、このパス マスクは変更される場合があるため、複数の pathmask 文を使用して可能性を排除する必要があることに注意してください。

パスとは URL の中で .com、.org、または他のドメイン名以降に記述されているすべてを指します。たとえば、www.mycompany.com/hrbenefits という URL では、*hrbenefits* がパスになります。同様に、www.mycompany.com/hrinsurance という URL では、*hrinsurance* がパスです。すべての hr サイトでプロキシ バイパスを使用する場合は、/hr\* のように \* をワイルドカードとして使用すると、コマンドを何度も入力しなくても済みます。

プロキシ バイパスを設定するには、webvpn モードで **proxy-bypass** コマンドを使用します。

## アプリケーション プロファイル カスタマイゼーション フレームワークの設定

WebVPN 用の Application Profile Customization Framework (APCF; アプリケーション プロファイル カスタマイゼーション フレームワーク) プロファイルを使用すると、セキュリティ アプライアンスは、標準以外のアプリケーションや Web リソースを処理できるようになり、WebVPN 接続を介してこれらが正しく表示されます。APCF プロファイルには、特定のアプリケーションに送信するデータの送信時刻（処理前、処理後）、送信部分（ヘッダー、本文、要求、応答）、および送信内容を指定したスクリプトが含まれています。スクリプトは XML 形式で記述され、ストリングおよびテキストの変換では sed（ストリーム エディタ）のシンタックスが使用されます。APCF プロファイルは、セキュリティ アプライアンス上で数種類を同時に実行することができます。1 つの APCF プロファイルのスクリプト内に複数の APCF ルールを適用することができます。この場合、セキュリティ アプライアンスは、最も古いルール（設定履歴に基づいて）を最初に処理し、次に 2 番目に古いルール、その次は 3 番目という順序で処理します。

APCF プロファイルは、セキュリティ アプライアンスのフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、または TFTP サーバに保存できます。webvpn モードで **apcf** コマンドを使用すると、セキュリティ アプライアンス上にロードする APCF プロファイルを指定し、検索することができます。

次の例は、フラッシュ メモリに保存されている apcf1.xml という名前の APCF プロファイルのイネーブル化を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml
hostname(config-webvpn)#
```

この例では、ポート番号 1440、パスが /apcf の myserver という名前の https サーバにある APCF プロファイル apcf2.xml をイネーブルにする手順を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
hostname(config-webvpn)#
```

## APCF シンタックス

次の項では、APCF シンタックスについて説明します。



### 注意

APCF プロファイルの使い方を誤ると、パフォーマンスが低下したり、好ましくない表現のコンテンツになる場合があります。シスコのエンジニアリング部では、ほとんどの場合、APCF プロファイルを提供することで特定アプリケーションの表現上の問題を解決しています。

APCF プロファイルは、XML フォーマットおよび sed スクリプト シンタックスを使用します。表 30-4 に、この場合に使用する XML タグを示します。

表 30-4 APCF XML タグ

| タグ                             | 用途                                         |
|--------------------------------|--------------------------------------------|
| <APCF>...</APCF>               | すべての APCF XML ファイルを開くための必須のルート要素。          |
| <version>1.0</version>         | APCF の実装バージョンを指定する必須タグ。現在のバージョンは 1.0 だけです。 |
| <application>...</application> | XML 記述の本文を囲む必須タグ。                          |
| <id> text </id>                | この特定の APCF 機能を記述する必須タグ。                    |



表 30-4 APCF XML タグ (続き)

| タグ                                                         | 用途                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <apcf-entities>...</apcf-entities>                         | 単一または複数の APCF エンティティを囲む必須タグ。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <js-object>...</js-object>                                 | コンテンツの種類または実施される APCF 処理の段階を指定するこれらのタグのうち 1 つは必須です。                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <html-object>...</html-object>                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <process-request-header>...</process-request-header>       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <process-response-header>...</process-response-header>     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <preprocess-request-body>...</preprocess-request-body>     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <postprocess-request-body>...</postprocess-request-body>   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <preprocess-response-body>...</preprocess-response-body>   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <postprocess-response-body>...</postprocess-response-body> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <conditions>... </conditions>                              | <p>処理前および処理後の子要素タグで、次の処理基準を指定します。</p> <p>http-version (1.1, 1.0, 0.9 など)</p> <p>http-method (get、put、post、webdav)</p> <p>http-scheme (http、https、other)</p> <p>("a".. "z"   "A".. "Z"   "0".. "9"   ".-_*[]?") を含む server-regexp 正規表現</p> <p>("a".. "z"   "A".. "Z"   "0".. "9"   ".-_*[]?+()\\{\\},") を含む server-fnmatch 正規表現</p> <p>user-agent-regexp</p> <p>user-agent-fnmatch</p> <p>request-uri-regexp</p> <p>request-uri-fnmatch</p> <p>条件タグのうち 2 つ以上が存在する場合は、セキュリティ アプライアンスはすべてのタグに対して論理 AND を実行します。</p> |
| <action> ... </action>                                     | 指定の条件以下のコンテンツで実行する 1 つまたは複数のアクションを囲みます。つまり、これらのアクションのそれぞれを下記の <do> タグまたは <sed-script> タグで定義します。                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <do>...</do>                                               | <p>次のいずれかのアクションを定義します。</p> <p>&lt;no-rewrite/&gt;</p> <p>&lt;no-toolbar/&gt;</p> <p>&lt;no-gzip/&gt;</p> <p>&lt;force-cache/&gt;</p> <p>&lt;force-no-cache/&gt;</p>                                                                                                                                                                                                                                                                                                                                             |
| <sed-script> TEXT </sed-script>                            | アクション タグの子要素です。TEXT は有効な Sed スクリプトである必要があります。<sed-script> は、これより前に定義された <conditions> タグに適用されます。                                                                                                                                                                                                                                                                                                                                                                                                                 |

## APCF の例

APCF プロファイルの例を次に示します。

```
<APCF>
<version>1.0</version>
<application>
  <id>Do not compress content from notsogood.com</id>
  <apcf-entities>
    <process-request-header>
      <conditions>
        <server-fnmatch>*.notsogood.com</server-fnmatch>
      </conditions>
      <action>
        <do><no-gzip/></do>
      </action>
    </process-request-header>
  </apcf-entities>
</application>
</APCF>
```

## WebVPN エンド ユーザ設定の概要

この項は、エンド ユーザのために WebVPN を設定するシステム管理者を対象にしています。ここでは、エンド ユーザ インターフェイスをカスタマイズする方法について説明します。

この項では、リモート システムの設定要件と作業の概要を説明します。ユーザが WebVPN の使用を開始するために、ユーザに伝える必要のある情報を明確にします。次の項目について説明します。

- [エンド ユーザ インターフェイスの定義](#)
- [WebVPN ページのカスタマイズ](#)
- [ユーザ名とパスワードの要求](#)
- [セキュリティのヒントの通知](#)
- [WebVPN 機能を使用するためのリモート システムの設定](#)

## エンド ユーザ インターフェイスの定義

WebVPN エンド ユーザ インターフェイスは一連の HTML パネルで構成されます。ユーザは、セキュリティ アプライアンス インターフェイスの IP アドレスを `https://address` 形式で入力することにより、WebVPN にログインします。最初に表示されるパネルは、ログイン画面です (図 30-6)。

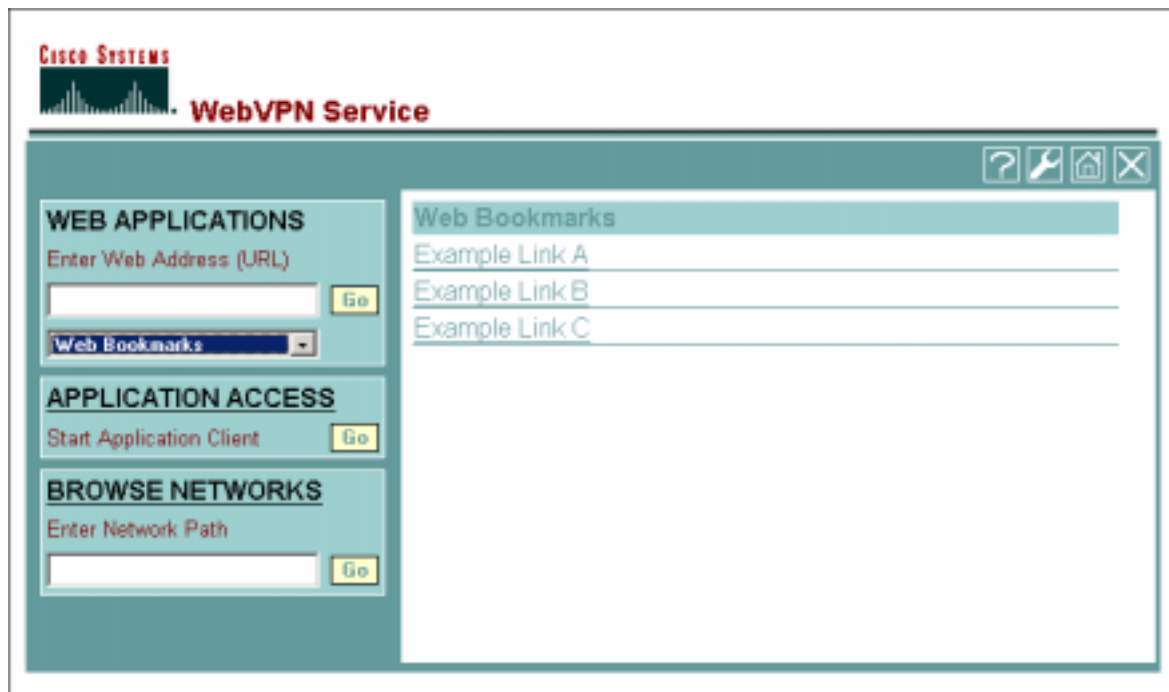
図 30-6 WebVPN の Login 画面



## WebVPN ホームページの表示

ユーザがログインすると、WebVPN ホームページが開きます (図 30-7)。

図 30-7 WebVPN ホームページ

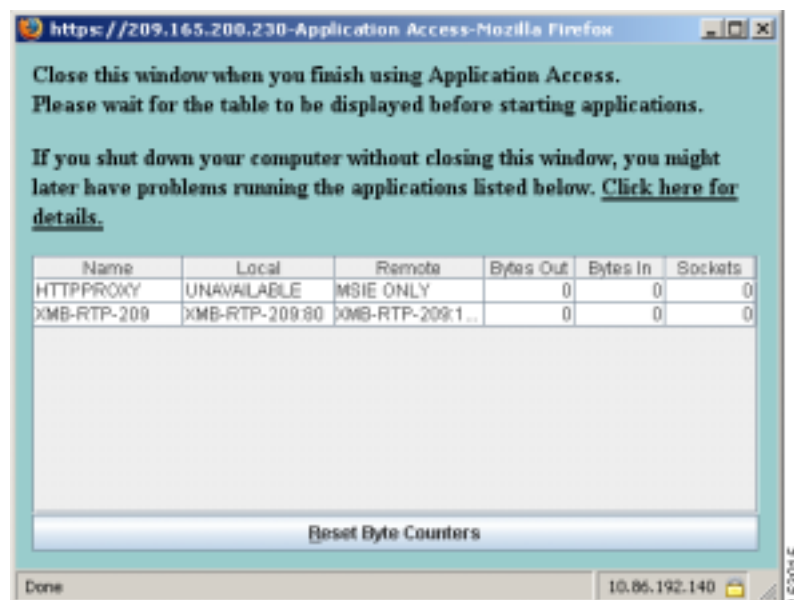


ホームページには設定済みの WebVPN 機能がすべて表示され、選択済みのロゴ、テキスト、および色が外観に反映されています。このサンプル ホームページには、特定のファイル共有の指定機能以外のすべての WebVPN 機能が表示されています。ユーザはこのホームページを使用して、ネットワークのブラウズ、URL の入力、特定の Web サイトへのアクセス、およびポート転送による TCP アプリケーションへのアクセスを実行できます。

## WebVPN Application Access パネルの表示

ポート転送(アプリケーション アクセスとも呼ばれる)を開始するには、ユーザは Application Access ボックスの Go ボタンをクリックします。Application Access ウィンドウが開きます (図 30-8)。

図 30-8 WebVPN Application Access ウィンドウ



このウィンドウには、この WebVPN 接続用に設定された TCP アプリケーションが表示されます。アプリケーションを使用する場合は、このパネルを開いたまま、通常の方法でアプリケーションを起動します。

## フローティング ツールバーの表示

図 30-9 に示すフローティング ツールバーは、現在の WebVPN セッションを表します。

図 30-9 WebVPN フローティング ツールバー



フローティング ツールバーの次の特性に注意してください。

- ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。
- ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。
- ツールバーを閉じると、セキュリティ アプライアンスは WebVPN セッションの終了を確認するプロンプトを表示します。

WebVPN の使用方法については、P.30-50 の表 30-6 を参照してください。

## WebVPN ページのカスタマイズ

WebVPN ユーザに表示される WebVPN ページの外観を変えることができます。変更できる外観には、ユーザによるセキュリティ アプライアンスへの接続時に表示される Login ページ、セキュリティ アプライアンスのユーザ承認後に表示されるホームページ、ユーザによるアプリケーション起動時に表示される Application Access ウィンドウ、さらにはユーザによる Web VPN サービスのログオフ時に表示される Logout ページがあります。

WebVPN ページのカスタマイズ後は、このカスタマイズを保存して特定のトンネルグループ、グループ、ユーザに適用できます。いくつかのカスタマイゼーションを作成、保存して、ユーザ個人やユーザグループに応じて Web VPN ページの外観を変更するようにセキュリティ アプライアンスをイネーブル化できます。

ここでは、次の項目とタスクについて説明します。

- [Cascading Style Sheet パラメータの使用 \(P.30-39\)](#)
- [WebVPN Login ページのカスタマイズ \(P.30-40\)](#)
- [WebVPN Logout ページのカスタマイズ \(P.30-42\)](#)
- [WebVPN ホームページのカスタマイズ \(P.30-43\)](#)
- [Application Access ウィンドウのカスタマイズ \(P.30-45\)](#)
- [プロンプト ダイアログのカスタマイズ \(P.30-46\)](#)
- [トンネルグループ、グループ、およびユーザへのカスタマイゼーションの適用 \(P.30-47\)](#)

## Cascading Style Sheet パラメータの使用

多くの WebVPN カスタマイゼーション コマンドには、**style** オプションが含まれています。この値は、任意の有効な Cascading Style Sheet (CSS) パラメータで表されます。これらのパラメータの説明は、このマニュアルの範囲外です。CSS パラメータの詳細については、World Wide Web Consortium (W3C) の Web サイト、[www.w3.org](http://www.w3.org) で CSS 仕様を参照してください。CSS 2.1 Specification の Appendix F には、CSS パラメータのリストが分かりやすく一覧されています。

[www.w3.org/TR/CSS21/propidx.html](http://www.w3.org/TR/CSS21/propidx.html) で参照できます。

次に、WebVPN ページの最も一般的な変更である、ページ色の変更についてヒントを示します。

- カンマで区切った RGB 値、HTML の色値、または HTML で認識されている場合はその色の名前を使用することができます。
- RGB の形式は 0,0,0 で、赤、緑、青の各色にはそれぞれ 0 から 255 までの範囲の 10 進数を指定できます。カンマで区切ったエントリは、各色を他の色と組み合わせる場合の強度を示します。
- HTML 形式は #000000 です。6 桁の 10 進数で構成され、最初と 2 番目の数字が赤、3 番目と 4 番目が緑、残りの 2 つが青をそれぞれ表します。



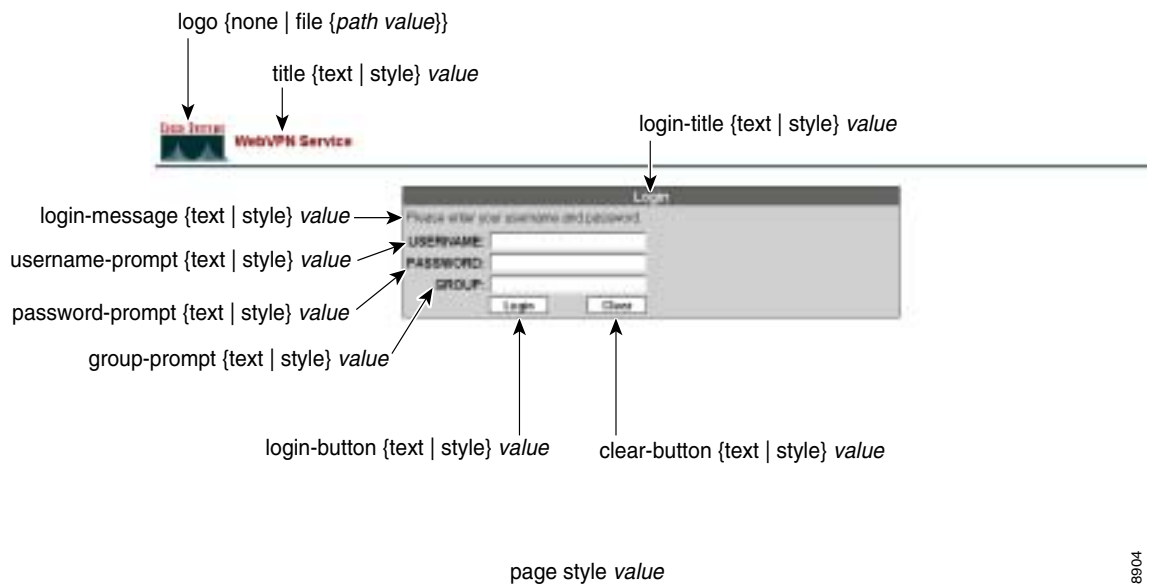
(注)

WebVPN ページのカスタマイズを簡略化するには ASDM を使用することをお勧めします。ASDM には、色見本などのスタイル要素の設定やプレビューなどの便利な機能があります。

## WebVPN Login ページのカスタマイズ

図 30-10 に、WebVPN Login ページと、このページをカスタマイズするのに使用可能な関連する CLI コマンドを示します。

図 30-10 WebVPN Login ページと関連する CLI コマンド



148904

次の手順に従うと、CLI コマンドを使用して WebVPN Login ページのすべての要素をカスタマイズできます。各種コマンドの使用例も示します。

**ステップ 1** webvpn モードから **customization** コマンドを使用して、WebVPN カスタマイゼーション モードに入ります。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

**ステップ 2** **page style** コマンドを使用して WebVPN Login ページの CSS のスタイルを変更します。

```
[no] page style value
hostname(config-webvpn-custom)# page style font-size:large
```

**ステップ 3** **title** コマンドを使用してタイトルを変更します。

```
[no] title {text | style} value
hostname(config-webvpn-custom)# title text Cisco WebVPN Service
```

**ステップ 4** **logo** コマンドを使用して、ロゴをフラッシュ メモリに常駐するロゴに変えます。

```
[no] logo {none | file {path value}}
```

ロゴを拒否して、ロゴが継承されないようにするには、**none** オプションを使用してヌル値を設定します。

```
hostname(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

**ステップ 5** Login ボックスのタイトルを **login-title** コマンドを使用して変更します。

```
[no] login-title {text | style} value
```

```
hostname(config-webvpn-custom)# login-title style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt;
font-style: italic; font-weight: bold
```

**ステップ 6** Login ボックスのメッセージを **login-message** コマンドを使用して変更します。

```
[no] login-message {text | style} value
```

```
hostname(config-webvpn-custom)# login-message text username and password
```

**ステップ 7** Login ボックスに表示されるユーザ名のプロンプトを **username-prompt** コマンドを使用して変更します。

```
[no] username-prompt {text | style} value
```

```
hostname(config-webvpn-custom)# username-prompt text Corporate Username:
hostname(config-webvpn-custom)# username-prompt style font-weight:bolder
```

**ステップ 8** Login ボックスに表示されるパスワードのプロンプトを **password-prompt** コマンドを使用して変更します。

```
[no] password-prompt {text | style} value
```

```
hostname(config-webvpn-custom)# password-prompt text Corporate Username:
hostname(config-webvpn-custom)# password-prompt style font-weight:bolder
```

**ステップ 9** Login ボックスに表示されるグループ プロンプトを **group-prompt** コマンドを使用して変更します。

```
[no] group-prompt {text | style} value
```

```
hostname(config-webvpn-custom)# group-prompt text Corporate Group:
hostname(config-webvpn-custom)# group-prompt style font-weight:bolder
```

**ステップ 10** Login ボックスの Login ボタンの内容または外観を **login-button** コマンドを使用して変更します。

```
[no] login-button {text | style} value
```

```
hostname(config-webvpn-custom)# login-button text OK
```

**ステップ 11** Login ボックスの Clear ボタンの内容または外観を **clear-button** コマンドを使用して変更します。

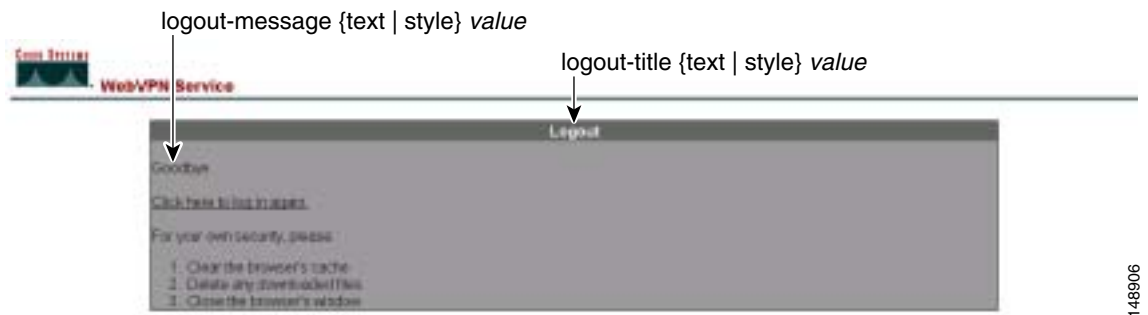
[no] **clear-button** {text | style} value

```
hostname(config-webvpn-custom)# clear-button background-color:blue
```

## WebVPN Logout ページのカスタマイズ

セキュリティ アプライアンスは、WebVPN ユーザが WebVPN のサービスをログアウトするときに WebVPN Logout ページを表示します。図 30-11 に、WebVPN Logout ページとこのページをカスタマイズするのに使用可能な関連する CLI コマンドを示します。

図 30-11 WebVPN Logout ページ



次の手順に従うと、CLI コマンドを使用して WebVPN Logout ページをカスタマイズできます。各種コマンドの使用例も示します。

**ステップ 1** webvpn モードから **customization** コマンドを使用して、WebVPN カスタマイゼーション モードに入ります。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

**ステップ 2** Logout ボックスのタイトルを **logout-title** コマンドを使用して変更します。

[no] **logout-title** {text | style} value

```
hostname(config-webvpn-custom)# logout-title style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt;
font-style: italic; font-weight: bold
```

**ステップ 3** Logout ボックスのメッセージを **logout-message** コマンドを使用して変更します。

[no] **logout-message** {text | style} value

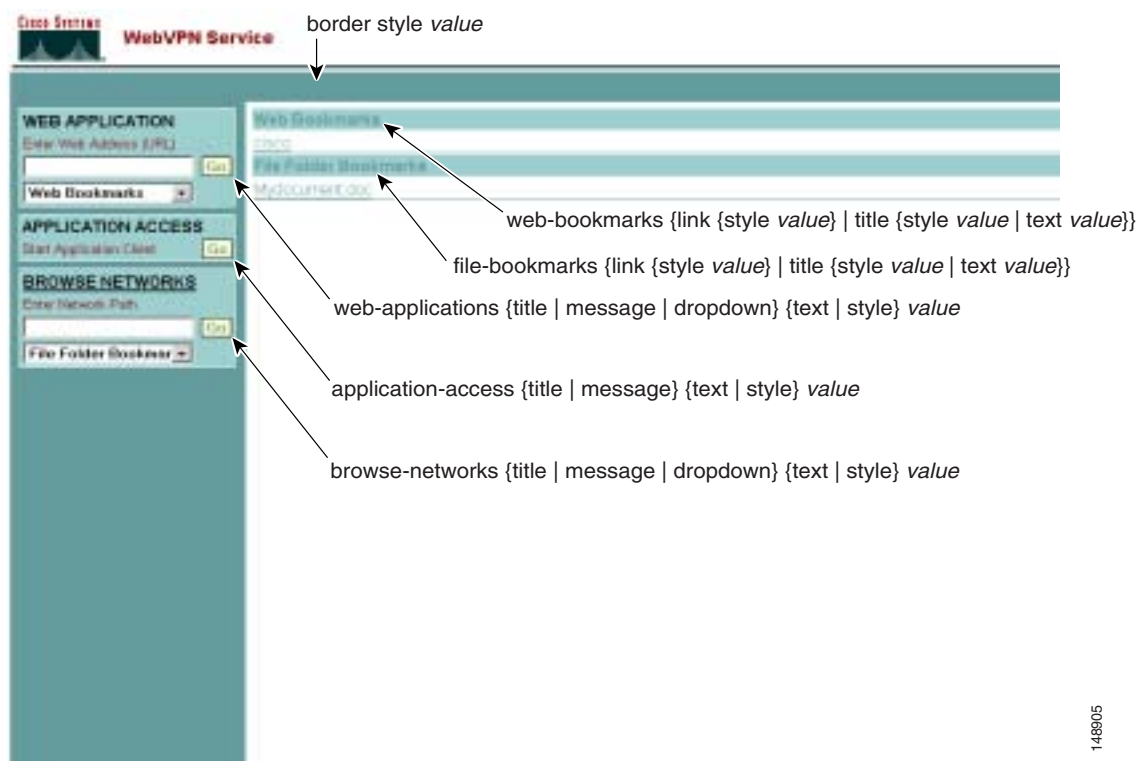
```
hostname(config-webvpn-custom)# login-title style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt;
font-style: italic; font-weight: bold
```



## WebVPN ホームページのカスタマイズ

セキュリティ アプライアンスが認証済み WebVPN ユーザに表示する WebVPN ホームページの外観をカスタマイズできます。図 30-12 に、WebVPN ホームページと、このページをカスタマイズするのに使用可能な関連する CLI コマンドを示します。

図 30-12 WebVPN ホームページと関連する CLI コマンド



次の手順に従うと、CLI コマンドを使用して WebVPN ホームページのすべての要素をカスタマイズできます。各種コマンドの使用例も示します。

- ステップ 1** webvpn モードから **customization** コマンドを使用して、WebVPN カスタマイゼーション モードに入ります。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

- ステップ 2** **border style** コマンドと CSS パラメータを使用して WebVPN ページの外枠のスタイルを変更します。

```
[no] border style value
hostname(config-webvpn-custom)# border style background-color:66FFFF
```

**ステップ 3** **web-applications** コマンドを使用して、Web Applications ボックスの外観を変更します。

**[no] web-applications {title | message | dropdown} {text | style} value**

```
hostname(config-webvpn-custom)# web-applications title text WWW Applications
hostname(config-webvpn-custom)# web-applications title style color:blue
hostname(config-webvpn-custom)# web-applications message text Enter URL
hostname(config-webvpn-custom)# web-applications message style color:blue
hostname(config-webvpn-custom)# web-applications dropdown text URLs to Browse
hostname(config-webvpn-custom)# web-applications dropdown style color:red
```

**ステップ 4** **application-access** コマンドを使用して、Application Access ボックスの外観を変更します。

**[no] application-access {title | message} {text | style} value**

```
hostname(config-webvpn-custom)# application-access title text Applications
hostname(config-webvpn-custom)# application-access title style color:blue
hostname(config-webvpn-custom)# application-access message text Start Application
hostname(config-webvpn-custom)# application-access message style color:blue
```

**ステップ 5** **browse-networks** コマンドを使用して、Browse Networks ボックスの外観を変更します。

**[no] browse-networks {title | message | dropdown} {text | style} value**

```
hostname(config-webvpn-custom)# browse-networks title text Corporate Nets
hostname(config-webvpn-custom)# browse-networks title style color:blue
hostname(config-webvpn-custom)# browse-networks message text Enter URL
hostname(config-webvpn-custom)# browse-networks message style color:blue
hostname(config-webvpn-custom)# browse-networks dropdown text URLs to Browse
hostname(config-webvpn-custom)# browse-networks dropdown style color:red
```

**ステップ 6** **web-bookmarks** コマンドを使用して、Web Bookmarks タイトルまたはリンクを変更します。

**[no] web-bookmarks {link {style value} | title {style value | text value}}**

```
hostname(config-webvpn-custom)# web-bookmarks link style color:black
hostname(config-webvpn-custom)# web-bookmarks title style color:black
hostname(config-webvpn-custom)# web-bookmarks title text Corporate Web Bookmarks
```

**ステップ 7** **file-bookmarks** コマンドを使用して、File Bookmarks タイトルまたは File Bookmarks リンクを変更します。

**[no] file-bookmarks {link {style value} | title {style value | text value}}**

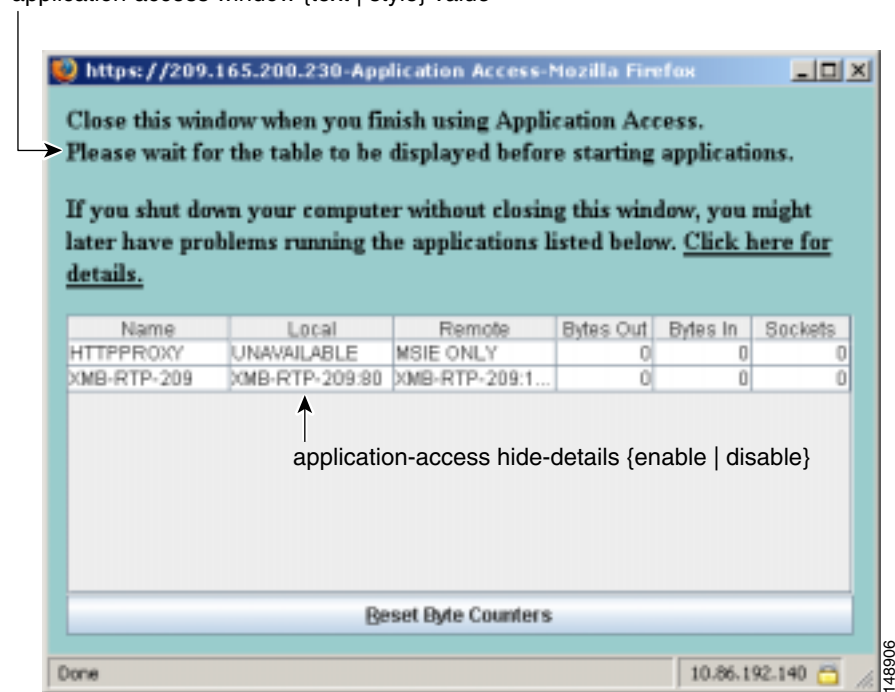
```
hostname(config-webvpn-custom)# file-bookmarks link style color:blue
hostname(config-webvpn-custom)# file-bookmarks title style color:blue
hostname(config-webvpn-custom)# file-bookmarks title text Corporate File Bookmarks
```

## Application Access ウィンドウのカスタマイズ

リモート ユーザがアプリケーションを選択すると起動される Application Access ウィンドウをカスタマイズすることができます。図 30-13 に、Application Access ウィンドウとカスタマイズで使用可能な関連する CLI コマンドを示します。

図 30-13 Application Access ウィンドウ

application-access window {text | style} value



次の手順に従うと、CLI コマンドを使用して Application Access ウィンドウをカスタマイズできます。各種コマンドの使用例も示します。

- ステップ 1** webvpn モードから **customization** コマンドを使用して、WebVPN カスタマイゼーション モードに入ります。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

- ステップ 2** application-access window コマンドを使用して、Application Access ウィンドウを変更します。

[no] application-access window {text | style} value

```
hostname(config-webvpn-custom)# application-access window text URLs to Browse
hostname(config-webvpn-custom)# application-access window style color:red
```

**ステップ 3** `application-access hide-details` コマンドを使用して、WebVPN Applications Access ウィンドウへのアプリケーション詳細の非表示をイネーブル化またはディセーブル化します。

**[no] application-access hide-details {enable | disable}**

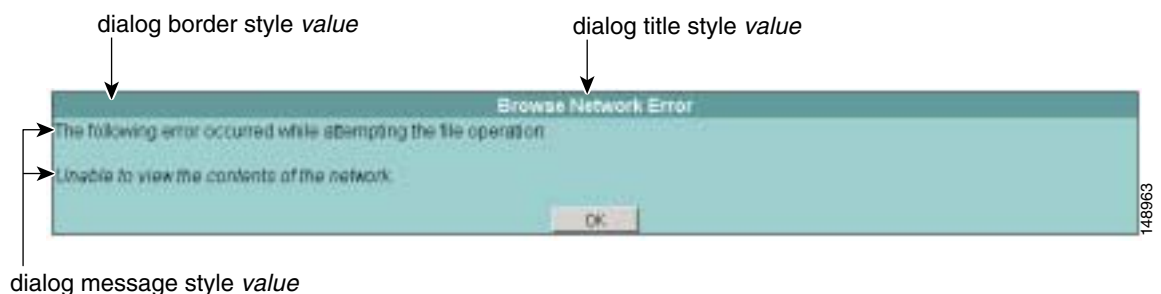
デフォルトではディセーブルになっています。アプリケーションの詳細は非表示にならず、Application Access ウィンドウに表示されます。

```
hostname(config-webvpn-custom)# application-access hide-details enable
```

## プロンプト ダイアログのカスタマイズ

セキュリティ アプライアンスは、通知や警告などのさまざまなプロンプト ダイアログ メッセージを WebVPN ユーザに送信します。図 30-14 に、ダイアログ メッセージと、これらのメッセージの外観をカスタマイズするのに使用可能な関連する CLI コマンドを示します。

図 30-14 ダイアログ メッセージと関連する CLI コマンド



次の手順で、ダイアログ メッセージのすべての要素のカスタマイズと、各種コマンドの使用例を示します。

**ステップ 1** `webvpn` モードから `customization` コマンドを使用して、WebVPN カスタマイゼーション モードに入ります。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

**ステップ 2** `dialog border` コマンドを使用して、ダイアログ メッセージの外枠をカスタマイズします。

**[no] dialog border style value**

```
hostname(config-webvpn-custom)# dialog border style color:blue
```

**ステップ 3** `dialog title` コマンドを使用してタイトルの外観を変更します。

**[no] dialog title style value**

```
hostname(config-webvpn-custom)# dialog title style font:bolder
```

**ステップ 4** `dialog message` コマンドを使用してメッセージの外観を変更します。

**[no] dialog message style value**

```
hostname(config-webvpn-custom)# dialog message style font:italic
```

## トンネルグループ、グループ、およびユーザへのカスタマイゼーションの適用

カスタマイゼーションを作成したら、このカスタマイゼーションを **customization** コマンドを使用して、トンネルグループ、グループ、またはユーザに適用することができます。このコマンドで表示されるオプションは、現在のモードの種類によって異なります。

トンネルグループ、グループポリシー、およびユーザの設定の詳細については、[第 26 章「トンネルグループ、グループポリシー、およびユーザの設定」](#)を参照してください。

### トンネルグループへのカスタマイゼーションの適用

トンネルグループにカスタマイゼーションを適用するには、トンネルグループの `webvpn` モードで、次のように **customization** コマンドを使用します。

**[no] customization name**

*name* は、トンネルグループに適用するカスタマイゼーションの名前です。

コンフィギュレーションからコマンドを削除して、トンネルグループからカスタマイゼーションを削除するには、コマンドの **no** 形式を使用します。

**customization** コマンドと直後に疑問符 (?) を入力して、既存のカスタマイゼーションのリストを表示します。

次の例では、トンネルグループの `webvpn` モードに入ってから、トンネルグループ `cisco_telecommuters` のカスタマイゼーション `cisco` をイネーブルにしています。

```
hostname(config)# tunnel-group cisco_telecommuters webvpn-attributes  
hostname(tunnel-group-webvpn)# customization cisco
```

### グループおよびユーザへのカスタマイゼーションの適用

グループまたはユーザにカスタマイゼーションを適用するにはグループポリシー `webvpn` モードまたはユーザ名 `webvpn` モードで、**customization** コマンドを使用します。これらのモードには、**none** および **value** のオプションが含まれています。

**[no] customization {none | value name}**

**none** は、グループまたはユーザのカスタマイゼーションをディセーブルにして値が継承されないようにするオプションで、デフォルトの WebVPN ページを表示します。

**value name** は、グループまたはユーザに適用するカスタマイゼーションの名前です。

コンフィギュレーションからコマンドを削除して値が継承されるようにするには、コマンドの **no** 形式を使用します。

**customization value** コマンドと直後に疑問符 (?) を入力して、既存のカスタマイゼーションのリストを表示します。

次の例では、グループポリシーの webvpn モードに入ってから、セキュリティ アプライアンスにカスタマイゼーションのリストを照会し、グループポリシー *cisco\_sales* のカスタマイゼーション *cisco* をイネーブルにしています。

```
hostname(config)# group-policy cisco_sales attributes
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# customization value ?

config-username-webvpn mode commands/options:
Available configured customization profiles:
    DfltCustomization
    cisco
hostname(config-group-webvpn)# customization value cisco
```

次の例では、ユーザ名の webvpn モードに入ってから、ユーザ *cisco\_employee* のカスタマイゼーション *cisco* をイネーブルにしています。

```
hostname(config)# username cisco_employee attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# customization value cisco
```

## ユーザ名とパスワードの要求

ネットワークによっては、リモートセッション中にユーザが、コンピュータ、インターネット サービス プロバイダー、WebVPN、メール サーバ、ファイル サーバ、企業アプリケーションのうち、それらの一部またはすべてにログインする必要があることがあります。ユーザはさまざまなコンテキストで認証を行うために、一意のユーザ名、パスワード、PIN などさまざまな情報が要求される場合があります。

表 30-5 に、WebVPN ユーザが知っておく必要のあるユーザ名とパスワードのタイプを示します。

表 30-5 WebVPN ユーザに通知するユーザ名とパスワード

| ログイン ユーザ名/パスワード タイプ | 目的                           | 入力するタイミング                                           |
|---------------------|------------------------------|-----------------------------------------------------|
| コンピュータ              | コンピュータへのアクセス                 | コンピュータの起動                                           |
| インターネット サービス プロバイダー | インターネットへのアクセス                | インターネット サービス プロバイダーへの接続                             |
| WebVPN              | リモート ネットワークへのアクセス            | WebVPN の起動                                          |
| ファイル サーバ            | リモート ファイル サーバへのアクセス          | WebVPN ファイル ブラウジング機能を使用して、リモート ファイル サーバにアクセスするとき    |
| 企業アプリケーションへのログイン    | ファイアウォールで保護された内部サーバへのアクセス    | WebVPN Web ブラウジング機能を使用して、保護されている内部 Web サイトにアクセスするとき |
| メール サーバ             | WebVPN 経由によるリモートメールサーバへのアクセス | 電子メール メッセージの送受信                                     |

## セキュリティのヒントの通知

必ず WebVPN セッションからログアウトするようにユーザに通知してください（WebVPN からログアウトするには、WebVPN ツールバーの logout アイコンをクリックするか、またはブラウザを閉じます）。

WebVPN を使用してもすべてのサイトとの通信がセキュアであるとは限らないことを、ユーザに通知してください。WebVPN は、企業ネットワーク上のリモート PC やワークステーションとセキュリティ アプライアンスとの間のデータ転送のセキュリティを保証するものです。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるもの）にアクセスする場合、企業のセキュリティ アプライアンスから目的の Web サーバまでの通信はセキュアではありません。

## WebVPN 機能を使用するためのリモート システムの設定

表30-6 に、WebVPN を使用するためのリモート システムの設定に関する、次の各種情報を示します。

- WebVPN の起動
- WebVPN フローティング ツールバーの使用
- Web ブラウジング
- ネットワーク ブラウジングとファイル管理
- アプリケーションの使用（ポート転送）
- ポート転送を介した電子メールの使用
- Web アクセスを介した電子メールの使用
- 電子メール プロキシを介した電子メールの使用

また、表 30-6 には、次の項目に関する情報も記載されています。

- WebVPN の要件（機能別）
- WebVPN をサポートするアプリケーション
- クライアント アプリケーションのインストールとコンフィギュレーションの要件
- エンド ユーザに提供する必要のある情報
- エンド ユーザのためのヒントや使用上の推奨事項

ユーザ アカウントを別々に設定し、各ユーザがそれぞれ異なる WebVPN 機能を使用できるようにすることが可能です。表 30-6 には機能別の情報をまとめてあります。利用できない機能の情報についてはスキップしてください。

表 30-6 WebVPN リモート システム コンフィギュレーションとエンド ユーザの要件

| 作業         | リモート システムまたはエンド ユーザの要件 | 仕様または使用上の推奨事項                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WebVPN の起動 | インターネットへの接続            | <p>サポートされているインターネット接続は、次のとおりです。</p> <ul style="list-style-type: none"> <li>• 家庭の DSL、ケーブル、ダイヤルアップ</li> <li>• 公共のキオスク</li> <li>• ホテルの回線</li> <li>• 空港の無線ノード</li> <li>• インターネット カフェ</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|            | WebVPN 対応のブラウザ         | <p>WebVPN には次のブラウザを推奨します。他のブラウザでは、WebVPN 機能を完全にはサポートできない場合があります。</p> <p>Microsoft Windows の場合：</p> <ul style="list-style-type: none"> <li>• Internet Explorer バージョン 6.0</li> <li>• Netscape バージョン 7.2</li> <li>• Mozilla バージョン 1.7 以降</li> <li>• Firefox 1.x</li> </ul> <p>Linux の場合：</p> <ul style="list-style-type: none"> <li>• Mozilla バージョン 1.7</li> <li>• Netscape バージョン 7.2</li> <li>• Firefox 1.x</li> </ul> <p>Solaris の場合：</p> <ul style="list-style-type: none"> <li>• Netscape バージョン 7.2</li> </ul> <p>Macintosh OS X の場合：</p> <ul style="list-style-type: none"> <li>• Safari バージョン 1.0</li> <li>• Firefox 1.x</li> </ul> |
|            | ブラウザでのクッキーのイネーブル化      | <p>ポート転送を介してアプリケーションにアクセスするために、ブラウザでクッキーをイネーブルにする必要があります。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|            | WebVPN 用の URL          | <p>https アドレスの形式は次のとおりです。</p> <p>https://address</p> <p>address は、WebVPN がイネーブルになっているセキュリティ アプライアンスのインターフェイスの IP アドレスまたは DNS ホスト名（またはロードバランシング クラスター）です。たとえば、https://10.89.192.163 または https://cisco.example.com のようになります。</p>                                                                                                                                                                                                                                                                                                                                                                                                         |
|            | WebVPN のユーザ名とパスワード     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|            | (オプション) ローカル プリンタ      | <p>WebVPN は、Web ブラウザからネットワーク プリンタへの印刷をサポートしていません。ローカル プリンタへの印刷はサポートされています。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



表 30-6 WebVPN リモート システム コンフィギュレーションとエンド ユーザの要件 (続き)

| 作業                      | リモート システムまたはエンド ユーザの要件     | 仕様または使用上の推奨事項                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WebVPN フローティング ツールバーの使用 |                            | <p>フローティング ツールバーを使用すると、WebVPN を簡単に使用できます。ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。</p> <p>ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。</p> <p>フローティング ツールバーは、現在の WebVPN セッションを表します。<b>Close</b> ボタンをクリックすると、セキュリティ アプライアンスは WebVPN セッションの終了を確認するプロンプトを表示します。</p> <p> <b>ヒント</b> ヒント：テキストをテキスト フィールドに貼り付けるには、Ctrl+V キーを使用します (WebVPN ツールバーでは右クリックはディセーブルになっています)。</p>                                                                                                                                                                               |
| Web ブラウジング              | 保護されている Web サイトのユーザ名とパスワード | <p>WebVPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。「<a href="#">セキュリティのヒントの通知</a>」を参照してください。</p> <p>WebVPN での Web ブラウジングのルックアンドフィールは、ユーザが見慣れたものではない場合があります。次の例を参考にしてください。</p> <ul style="list-style-type: none"> <li>WebVPN タイトル バーが各 Web ページの上部に表示される</li> <li>Web サイトへのアクセス方法： <ul style="list-style-type: none"> <li>WebVPN ホームページ上の Enter Web Address フィールドに URL を入力する</li> <li>WebVPN ホームページ上にある設定済みの Web サイトリンクをクリックする</li> <li>上記 2 つのどちらかの方法でアクセスした Web ページ上のリンクをクリックする</li> </ul> </li> </ul> <p>また、特定のアカウントの設定によっては、次のようになる場合もあります。</p> <ul style="list-style-type: none"> <li>一部の Web サイトがブロックされている</li> <li>使用可能な Web サイトが、WebVPN ホームページ上にリンクとして表示されるものに限られる</li> </ul> |

表 30-6 WebVPN リモート システム コンフィギュレーションとエンド ユーザの要件 (続き)

| 作業                                          | リモート システムまたはエンド ユーザの要件                                                                                                                                                                                                                                                                                                         | 仕様または使用上の推奨事項                                                                                                |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| ネットワーク ブラウジングとファイル管理                        | 共有リモートアクセス用に設定されたファイルアクセス権                                                                                                                                                                                                                                                                                                     | WebVPN を介してアクセスできるのは、共有フォルダと共有ファイルに限られます。                                                                    |
|                                             | 保護されているファイル サーバのサーバ名とパスワード                                                                                                                                                                                                                                                                                                     | —                                                                                                            |
|                                             | フォルダとファイルが存在するドメイン、ワークグループ、およびサーバ名                                                                                                                                                                                                                                                                                             | ユーザは、組織ネットワークを介してファイルを見つける方法に慣れていない場合があります。                                                                  |
|                                             | —                                                                                                                                                                                                                                                                                                                              | コピー処理の進行中は、 <b>Copy File to Server</b> コマンドを中断したり、別の画面に移動したりしないでください。コピー処理を中断すると、不完全なファイルがサーバに保存される可能性があります。 |
| アプリケーションの使用<br>(ポート転送またはアプリケーション アクセスと呼ばれる) |  (注) Macintosh OS X の場合、この機能をサポートしているのは Safari ブラウザだけです。                                                                                                                                                                                      |                                                                                                              |
|                                             |  (注) この機能を使用するには、Sun Microsystems Java™ Runtime Environment をインストールしてローカル クライアントを設定する必要があります。これには、ローカル システムで管理者の許可が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。                                                              |                                                                                                              |
|                                             |  注意 ユーザは、 <b>Close</b> アイコンをクリックしてアプリケーションを終了したら、必ず Application Access ウィンドウを閉じる必要があります。このウィンドウを正しく閉じないと、Application Access またはアプリケーション自体がディセーブルになる可能性があります。詳細については、「 <a href="#">Application Access 使用時の hosts ファイル エラーの回復</a> 」を参照してください。 |                                                                                                              |
|                                             | インストール済みのクライアント アプリケーション                                                                                                                                                                                                                                                                                                       | —                                                                                                            |
|                                             | ブラウザでイネーブルにされているクッキー                                                                                                                                                                                                                                                                                                           | —                                                                                                            |
|                                             | 管理者特権                                                                                                                                                                                                                                                                                                                          | ユーザが DNS 名を使用してサーバを指定する場合、そのユーザは PC の管理者用アクセス特権を持つ必要があります。これは、hosts ファイルを修正するのにこの特権が必要なためです。                 |

表 30-6 WebVPN リモート システム コンフィギュレーションとエンド ユーザの要件 (続き)

| 作業 | リモート システムまたはエンド ユーザの要件                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 仕様または使用上の推奨事項                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>インストール済みの Sun Microsystems Java Runtime Environment (JRE) バージョン 1.4.x と 1.5.x</p> <p>ブラウザで Javascript をイネーブルにする必要があります。デフォルトでは、イネーブルになっています。</p>                                                                                                                                                                                                                                                                                                                                          | <p>JRE がインストールされていない場合は、ポップアップ ウィンドウが表示され、ユーザに対して使用可能なサイトが示されます。</p> <p>まれに、JAVA 例外エラーで WebVPN ポート転送 アプレットが失敗することがあります。このような状況が発生した場合は、次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. ブラウザのキャッシュをクリアして、ブラウザを閉じます。</li> <li>2. JAVA アイコンがコンピュータのタスク バーに表示されていないことを確認します。JAVA のインスタンスをすべて閉じます。</li> <li>3. WebVPN セッションを確立し、ポート転送 JAVA アプレットを起動します。</li> </ol>                                                             |
|    | <p>設定済みのクライアント アプリケーション (必要な場合)</p> <p> <b>(注)</b> Microsoft Outlook クライアントの場合、この設定手順は不要です。</p> <p>Windows 以外のすべてのクライアント アプリケーションでは、設定が必要です。</p> <p>Windows アプリケーションの設定が必要かどうかを確認するには、Remote Server の値をチェックします。</p> <ul style="list-style-type: none"> <li>Remote Server にサーバ ホスト名が含まれている場合、クライアント アプリケーションの設定は不要です。</li> <li>Remote Server フィールドに IP アドレスが含まれている場合、クライアント アプリケーションを設定する必要があります。</li> </ul> | <p>クライアント アプリケーションを設定するには、ローカルにマッピングされたサーバの IP アドレスとポート番号を使用します。この情報を見つけるには、次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. リモート システム上で WebVPN を起動し、WebVPN ホームページの Application Access リンクをクリックします。Application Access ウィンドウが表示されます。</li> <li>2. Name カラムで、使用するサーバ名を確認し、このサーバに対応するクライアント IP アドレスとポート番号を Local カラムで確認します。</li> <li>3. この IP アドレスとポート番号を使用して、クライアント アプリケーションを設定します。設定手順は、クライアント アプリケーションによって異なります。</li> </ol> |
|    | <p> <b>(注)</b> WebVPN でアプリケーションを実行している場合、アプリケーションで表示される URL (電子メール内の URL など) をクリックしても、WebVPN ではそのサイトは開きません。WebVPN でこのようなサイトを開くには、Enter WebVPN (URL) Address フィールドに URL をカット アンド ペーストします。</p>                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                     |

表 30-6 WebVPN リモート システム コンフィギュレーションとエンド ユーザの要件 (続き)

| 作業                              | リモート システムまたはエンド ユーザの要件                                                                                                                                                          | 仕様または使用上の推奨事項                                                                                                                                                                                                                                                                                          |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Access を介した電子メールの使用 | Application Access の要件を満たす (「アプリケーションの使用」を参照)                                                                                                                                   | 電子メールを使用するには、WebVPN ホームページから Application Access を起動します。これにより、メール クライアントが使用できるようになります。                                                                                                                                                                                                                  |
|                                 |  <b>(注)</b> IMAP クライアントの使用中にメール サーバとの接続が中断し、新しく接続を確立できない場合は、IMAP アプリケーションを終了して WebVPN を再起動します。 |                                                                                                                                                                                                                                                                                                        |
|                                 | その他のメール クライアント                                                                                                                                                                  | <p>Microsoft Outlook Express バージョン 5.5 および 6.0 はテスト済みです。</p> <p>WebVPN は、Netscape Mail、Lotus Notes、および Eudora などの、ポート転送を介したその他の SMTPS、POP3S、または IMAP4S 電子メール プログラムをサポートしますが、動作確認は行っていません。</p>                                                                                                          |
| Web アクセスを介した電子メールの使用            | インストールされている Web ベースの電子メール製品                                                                                                                                                     | <p>次の製品がサポートされています。</p> <ul style="list-style-type: none"> <li>Outlook Web Access</li> </ul> <p>最適な結果を得るために、Internet Explorer 6.x 以上、Mozilla 1.7、または Firefox 1.x. で OWA を使用してください。</p> <ul style="list-style-type: none"> <li>Louts iNotes</li> </ul> <p>その他の Web ベースの電子メール製品も動作しますが、動作確認は行っていません。</p> |
| 電子メール プロキシを介した電子メールの使用          | インストール済みの SSL 対応メール アプリケーション                                                                                                                                                    | <p>サポートされているメール アプリケーションは次のとおりです。</p> <ul style="list-style-type: none"> <li>Microsoft Outlook</li> <li>Microsoft Outlook Express バージョン 5.5 および 6.0</li> <li>Netscape Mail バージョン 7</li> <li>Eudora 4.2 for Windows 2000</li> </ul> <p>その他の SSL 対応クライアントも動作しますが、動作確認は行っていません。</p>                       |
|                                 | 設定済みのメール アプリケーション                                                                                                                                                               | メール アプリケーションの使用方法与例については、「 <a href="#">WebVPN を介した電子メールの使用</a> 」を参照してください。                                                                                                                                                                                                                             |

## WebVPN データのキャプチャ

CLI キャプチャ コマンドにより、WebVPN 接続では正しく表示されない Web サイトに関する情報を記録できます。このデータは、Cisco カスタマー サポート エンジニアによる問題のトラブルシューティングに役立ちます。次の各項では、キャプチャ コマンドの使用方法について説明します。

- [キャプチャ ファイルの作成](#)
- [キャプチャ データを表示するためのブラウザの使用](#)



(注)

WebVPN キャプチャをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスに影響します。トラブルシューティングに必要なキャプチャ ファイルを生成したら、WebVPN キャプチャを必ずディセーブルにしてください。

### キャプチャ ファイルの作成

次の手順を実行して WebVPN セッションに関するデータをファイルにキャプチャします。

- ステップ 1** WebVPN キャプチャ ユーティリティを開始するには、特権 EXEC モードで **capture** コマンドを使用します。

```
capture capture_name type webvpn user webvpn_username
```

パラメータは次のとおりです。

- *capture\_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。
- *webvpn\_user* は、キャプチャの対象となるユーザ名です。

キャプチャ ユーティリティが開始されます。

- ステップ 2** WebVPN ユーザが WebVPN セッションを開始するためにログインします。キャプチャ ユーティリティは、パケットをキャプチャしています。

コマンドの **no** バージョンを使用してキャプチャを停止します。

```
no capture capture_name
```

キャプチャ ユーティリティは *capture\_name.zip* ファイルを作成し、このファイルはパスワード **koleso** で暗号化されます。

- ステップ 3** .zip ファイルをシスコシステムズに送信するか、Cisco TAC サービス リクエストに添付します。

- ステップ 4** .zip ファイルの内容を確認するには、パスワード **koleso** を使用してファイルを解凍します。

次の例では、*hr* という名前のキャプチャを作成します。これは、*user2* への WebVPN トラフィックを次のようにファイルにキャプチャします。

```
hostname# capture hr type webvpn user user2
WebVPN capture started.
  capture name    hr
  user name      user2
hostname# no capture hr
```

## キャプチャ データを表示するためのブラウザの使用

次の手順を実行して WebVPN セッションに関するデータをキャプチャし、これをブラウザに表示します。

- ステップ 1** WebVPN キャプチャ ユーティリティを開始するには、特権 EXEC モードで **capture** コマンドを使用します。

```
capture capture_name type webvpn user webvpn_username
```

パラメータは次のとおりです。

- *capture\_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。
- *webvpn\_user* は、キャプチャの対象となるユーザ名です。

キャプチャ ユーティリティが開始されます。

- ステップ 2** WebVPN ユーザが WebVPN セッションを開始するためにログインします。キャプチャ ユーティリティは、パケットをキャプチャしています。

コマンドの **no** バージョンを使用してキャプチャを停止します。

- ステップ 3** ブラウザをオープンし、アドレスを指定するボックスに次のように入力します。

```
https://IP_address またはセキュリティ アプライアンスのホスト名/webvpn_capture.html
```

キャプチャされたコンテンツが sniffer 形式で表示されます。

- ステップ 4** コンテンツをキャプチャし終わったら、コマンドの **no** バージョンを使用してキャプチャを停止します。



## SSL VPN クライアントの設定

SSL VPN クライアント (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 クライアントをインストールおよび設定しなくても、リモート ユーザが IPsec VPN クライアントを活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、リモート コンピュータの既存の SSL 暗号化を使用したり、セキュリティ アプライアンスの WebVPN ログインと認証を使用します。

SVC セッションを確立するには、リモート ユーザはブラウザで、セキュリティ アプライアンスの WebVPN インターフェイスの IP アドレスを入力します。すると、ブラウザはこのインターフェイスとの接続を確立し、WebVPN ログイン画面を表示します。ユーザがログインして認証され、セキュリティ アプライアンスは、ユーザが SVC を要求していると識別した場合、セキュリティ アプライアンスは SVC をリモート コンピュータにダウンロードします。SVC を使用するためのオプションがユーザ側にあるとセキュリティ アプライアンスが識別した場合は、セキュリティ アプライアンスはユーザ画面に SVC のインストールをスキップするリンクを表示する一方で、SVC をリモートコンピュータにダウンロードします。

ダウンロード終了後、SVC は自身のインストールと設定を行い、接続終了時に SVC は設定内容に応じてリモート コンピュータ上に留まるか、自身をアンインストールします。

この項では、次の項目について説明します。

- [SVC のインストール \(P.31-2\)](#)
- [SVC のイネーブル化 \(P.31-4\)](#)
- [相手先固定 SVC のインストールのイネーブル化 \(P.31-6\)](#)
- [キーの再生成のイネーブル化 \(P.31-6\)](#)
- [デッド ピア検知のイネーブル化と調整 \(P.31-7\)](#)
- [キープアライブのイネーブル化 \(P.31-8\)](#)
- [SVC 圧縮の使用 \(P.31-9\)](#)
- [SVC セッションの表示 \(P.31-10\)](#)
- [SVC セッションのログオフ \(P.31-11\)](#)
- [SVC のアップデート \(P.31-12\)](#)

## SVC のインストール

この項では、SVC をインストールするためのプラットフォーム要件と手順について説明します。

### プラットフォームの要件

SVC を使用するには、リモート コンピュータで Windows 2000 または Windows XP が稼動している必要があります。

### SVC ソフトウェアのインストール

SVC のインストールは、SVC のイメージをセキュリティ アプライアンスにコピーする手順と、このイメージに順序を割り当てる手順で構成されています。SVC をインストールするには、次の手順を実行します。

- ステップ 1** 特権 EXEC モードで **copy** コマンドを実行するか別の方法で SVC イメージをセキュリティ アプライアンスにコピーします。この例では、イメージは **copy tftp** コマンドを使用して tftp サーバからコピーされます。

```
hostname# copy tftp flash
Address or name of remote host []? 209.165.200.226
Source filename []? sslclient-win-1.0.2.127.pkg
Destination filename []? sslclient-win-1.0.2.127.pkg
Accessing
tftp://209.165.200.226/sslclient-win-1.0.2.127.pkg...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file
disk0:/cdisk71...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
319662 bytes copied in 3.695 secs (86511 bytes/sec)
```

- ステップ 2** 次のように、webvpn モードで **svc image** コマンドを使用して、SVC イメージに順序を割り当てます。

#### svc image ファイル名の順序

SVC イメージに番号付けを行うと、セキュリティ アプライアンスがリモート コンピュータにイメージをダウンロードする順序が確立されます。最小の番号が付いた SVC イメージから順にダウンロードされます。このため、最も一般的なオペレーティングシステムが使用するイメージに最小の番号を割り当てるようにします。

次の例では、**show webvpn svc** コマンドの出力によって、windows.pkg イメージに順序番号 1 が付けられていることが分かり、また、windows2.pkg イメージには順序番号 2 が割り当てられています。リモート コンピュータが SVC 接続を確認しようとする、windows.pkg イメージが最初にダウンロードされます。イメージがオペレーティングシステムと一致しない場合、windows2.pkg イメージが次のようにダウンロードされます。

```
hostname(config)# webvpn
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows.pkg 1
   CISCO STC win2k+ 1.0.0
   1,0,2,132
   Thu 08/25/2005 21:51:30.43

2. disk0:/windows2.pkg 2
   CISCO STC win2k+ 1.0.0
   1,0,0,164
   Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```



その後、windows2.pkg イメージが最初にリモート PC にダウンロードされるように **svc image** コマンドを使用して SVC アーカイブのイメージに再度順序付けすると、次のように、windows.pkg イメージが 2 番目にダウンロードされるようになります。

```
hostname(config-webvpn)# no svc image
hostname(config-webvpn)# svc image windows2.pkg 1
hostname(config-webvpn)# svc image windows.pkg 2
```

**show webvpn svc** コマンドを再入力すると、イメージの新しい順序が表示されます。

```
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows2.pkg 1
   CISCO STC win2k+ 1.0.0
   1,0,2,132
   Thu 08/25/2005 21:51:30.43

2. disk0:/windows.pkg 2
   CISCO STC win2k+ 1.0.0
   1,0,0,164
   Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

---

## SVC のイネーブル化

SVC のインストール後、次の手順を実行して SVC をイネーブルにできます。

- ステップ 1** webvpn モードで、次のように **enable** コマンドを使用して、WebVPN をインターフェイス上でイネーブルにします。

**enable interface**

次の例を参考にしてください。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

- ステップ 2** webvpn モードで、次のように **svc enable** コマンドを入力すると、セキュリティ アプライアンスからリモート コンピュータへの SVC イメージのダウンロードがイネーブルになります。

**svc enable**

次の例を参考にしてください。

```
hostname(config-webvpn)# svc enable
```

- ステップ 3** アドレス割り当て方式を設定します。DHCP とユーザ割り当てアドレッシングのいずれかまたは両方が使用できます。また、webvpn モードで次のように **ip local pool** コマンドを使用してローカル IP アドレス プールを作成することもできます。

**ip local pool poolname startaddr-endaddr mask mask**

次に、ローカルの IP アドレス プール、*vpn\_users* を作成する例を示します。

```
hostname(config-webvpn)# ip local pool vpn_users 209.165.200.225-209.165.200.254
mask 255.255.255.224
```

- ステップ 4** トンネルグループに IP アドレスを割り当てます。割り当て方法の 1 つは、次のように、一般アトリビュート モードで **address-pool** コマンドを使用してローカル IP アドレス プールを設定することです。

**address-pool poolname**

これを実行するには、最初に **tunnel-group name general-attributes** コマンドを入力して一般アトリビュート モードに入ります。その後、**address-pool** コマンドを使用してローカル IP アドレス プールを指定します。

次の例では、手順 3 で作成されたアドレス プール *vpn\_users* が既存トンネルグループの *telecommuters* を使用するように設定しています。

```
hostname(config)# tunnel-group telecommuters general-attributes
hostname(config-tunnel-general)# address-pool vpn_users
```

- ステップ 5** 一般アトリビュート モードで、次のように **default-group-policy** コマンドを使用して、デフォルトのグループポリシーをトンネルグループに割り当てます。

**default-group-policy name**

次の例では、グループポリシー *sales* をトンネルグループ *telecommuters* に割り当てています。

```
hostname(config-tunnel-general)# default-group-policy sales
```

- ステップ 6** 次に、トンネルグループの `webvpn` アトリビュート モードで `group-alias` コマンドを使用して、WebVPN ログイン ページのグループ リストに表示されるグループ エイリアスを作成しイネーブルにします。

**group-alias name enable**

ここでは、まずグローバル コンフィギュレーション モードを終了してから、`tunnel-group name webvpn-attributes` コマンドを入力して、トンネルグループの `webvpn` 属性モードに入ります。

次の例では、トンネルグループ `telecommuters` を対象とする `webvpn` アトリビュート コンフィギュレーション モードに入り、その後、グループ エイリアス `sales_department` を作成します。

```
hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias sales_department enable
```

- ステップ 7** `webvpn` モードで、次のように WebVPN ログイン ページ上のトンネルグループのリスト表示をイネーブルにします。

**tunnel-group-list enable**

まずグローバル コンフィギュレーション モードを終了してから、`webvpn` モードに入ります。

次の例では、`webvpn` モードに入ってからトンネルグループ リストをイネーブルにします。

```
hostname(config)# webvpn
hostname(config-webvpn)# tunnel-group-list enable
```

- ステップ 8** グループまたはユーザに対して許可される VPN トンネリング プロトコルとして WebVPN を指定します。これは、グループポリシー モードまたはユーザ名モードで `vpn-tunnel-protocol webvpn` コマンドを使用して実行します。

**vpn-tunnel-protocol webvpn**

これを実行するには、最初にグローバル コンフィギュレーション モードを終了してから、`group-policy name attributes` コマンドを入力してグループポリシー モードに入るか、`username name attributes` コマンドを入力してユーザ名モードに入り、その後、`webvpn` コマンドを使用して `webvpn` モードに入る方法のいずれかを使用して、グループまたはユーザの WebVPN 設定を変更します。

次の例では、グループポリシー `sales` に許可されるトンネリング プロトコルとして WebVPN を指定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# vpn-tunnel-protocol webvpn
```

- ステップ 9** グループポリシー `webvpn` モードまたはユーザ名 `webvpn` モードのいずれかに入ってから、次のように `svc` コマンドを使用して、特定のグループに対して SVC をイネーブル化または要求します。

**svc {none | enable | required}**

次の例では、既存のグループポリシー `sales` に対して、SVC を `required` に設定しています。

```
hostname(config-group-webvpn)# svc required
```

ユーザをグループポリシーに割り当てる詳細については、[第 26 章「トンネルグループ、グループポリシー、およびユーザの設定」](#)を参照してください。

## 相手先固定 SVC のインストールのイネーブル化

相手先固定 SVC のインストールをイネーブルにすると、SVC の自動アンインストール機能はディセーブルになります。以降の SVC 接続では、リモート コンピュータ上に SVC がインストールされたままになるため、リモート ユーザの SVC への接続時間が短縮されます。

特定のグループまたはユーザに対して相手先固定 SVC インストールをイネーブル化するには、グループポリシー モードまたはユーザ名 webvpn モードで次の **svc keep-installer** コマンドを使用します。

```
svc keep-installer {installed | none}
no svc keep-installer {installed | none}
```

パラメータは次のとおりです。

**installed** は、SVC が相手先を固定してリモート コンピュータにインストールされるように指定します。

**none** は、SVC のアクティブ接続の終了後、SVC がリモート コンピュータから削除されるように指定します。

デフォルトでは、SVC の相手先固定インストールはディセーブルになっています。リモート コンピュータでの SVC のアンインストールは、SVC セッションが終了するたびに実行されます。

次の例では、リモート コンピュータに SVC をインストールし続けるように、既存のグループポリシー *sales* を設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc keep-installer installed
```

## キーの再生成のイネーブル化

セキュリティ アプライアンスと SVC がキーを再生成するときは、暗号キーと初期ベクトルを再ネゴシエーションして接続のセキュリティを強化します。

特定のグループまたはユーザの SVC セッションでキーの再生成を実行するように SVC をイネーブル化するには、グループポリシー モードおよびユーザ名 webvpn モードで **svc rekey** コマンドを使用します。

```
svc rekey {method {new-tunnel | none | ssl} | time minutes}
no svc rekey {method {new-tunnel | none | ssl} | time minutes}
```

パラメータは次のとおりです。

**method new-tunnel** は、SVC キー再生成中に新規トンネルを確立するように SVC を指定します。

**method none** は、SVC のキー再生成をディセーブルにします。

**method ssl** は、SVC のキー再生成中に SSL の再ネゴシエーションを実施するように指定します。

**time minutes** は、セッション開始からキーの再生成までの時間に 1 から 10080（1 週間）を分単位で指定します。

次の例では、セッション開始 30 分後に実施されるキーの再生成中に、既存のグループポリシー *sales* に関する SSL との再ネゴシエーションを実施するように SVC を設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc rekey method ssl
hostname(config-group-policy)# svc rekey time 30
```

## デッド ピア検知のイネーブル化と調整

Dead Peer Detection (DPD; デッド ピア検知) は、ピアが応答していない場合または失敗した接続をセキュリティ アプライアンス (ゲートウェイ) または SVC で迅速に検出できるようにします。

特定のグループまたはユーザに対してセキュリティ アプライアンスまたは SVC で DPD をイネーブルにし、セキュリティ アプライアンスまたは SVC が実施する DPD の頻度を指定するには、次のように、グループポリシー モードまたはユーザ名 webvpn モードで **svc dpd-interval** コマンドを使用します。

```
svc dpd-interval {[gateway {seconds | none}} | [client {seconds | none}]]  
no svc dpd-interval {[gateway {seconds | none}} | [client {seconds | none}]]
```

パラメータは次のとおりです。

**gateway seconds** は、セキュリティ アプライアンス (ゲートウェイ) での DPD をイネーブルにして、セキュリティ アプライアンス (ゲートウェイ) で実施する DPD の頻度の間隔を 30 秒から 3600 秒に指定します。

**gateway none** は、セキュリティ アプライアンスによる DPD をディセーブルにします。

**client seconds** は、SVC (クライアント) での DPD をイネーブルにし、SVC で DPD を実施する間隔を 30 秒から 3600 秒に指定します。

**client none** は、SVC での DPD をディセーブルにします。

コンフィギュレーションから **svc dpd-interval** コマンドを削除するには、コマンドの **no** 形式を使用します。

次の例では、既存のグループポリシー *sales* に対してセキュリティ アプライアンスが実施する DPD の間隔を 3000 秒に設定し、SVC が実施する DPD の間隔を 10 秒に設定しています。

```
hostname(config)# group-policy sales attributes  
hostname(config-group-policy)# webvpn  
hostname(config-group-policy)# svc dpd-interval gateway 3000  
hostname(config-group-policy)# svc dpd-interval client 1000
```

## キープアライブのイネーブル化

プロキシ、ファイアウォール、NAT デバイスを通じた SVC 接続をオープンにしておくためのキープアライブ メッセージを送信する頻度を調整することができます。これは、接続のアイドル状態を維持できる時間がデバイスで制限される場合も有効です。頻度を調整することにより、リモートユーザが Microsoft Outlook または Microsoft Internet Explorer などソケットベースのアプリケーションをアクティブに実行していないときに、SVC が接続を切断して再接続しないように設定することもできます。

キープアライブ メッセージの頻度を設定するには、グループポリシー モードまたは webvpn モードで、次のように **svc keepalive** コマンドを使用します。

```
svc keepalive {none | seconds}
no svc keepalive {none | seconds}
```

パラメータは次のとおりです。

**none** は SVC キープアライブ メッセージをディセーブルにします。

**seconds** は、SVC から送信するキープアライブ メッセージをイネーブルにし、メッセージを送信する間隔を 15 秒から 600 秒の範囲に指定します。

デフォルトでは、キープアライブ メッセージはディセーブルです。

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、コマンドの **no** 形式を使用します。

次の例では、既存のグループポリシー *sales* に対し、SVC からキープアライブ メッセージが 300 秒 (5 分) 間隔で送信されるようにセキュリティ アプライアンスの設定をイネーブルにしています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc keepalive 300
```

## SVC 圧縮の使用

SVC 圧縮は、転送されるパケットのサイズを減らすことによって、セキュリティ アプライアンスと SVC 間の通信パフォーマンスを向上させる技術です。デフォルトでは、すべての SVC 接続のセキュリティ アプライアンスでの圧縮は、グローバル レベルおよび、特定のグループまたはユーザのレベルの両方でイネーブルになっています。

SVC 圧縮は、グローバル コンフィギュレーション モードで **compression svc** コマンドを使用すると設定できます。また、グループポリシー モードおよびユーザ名 webvpn モードで **svc compression** コマンドを使用すると、特定のグループまたはユーザに対して圧縮を設定することもできます。グローバル設定は、グループポリシー設定およびユーザ名設定を上書きします。

### SVC 圧縮のグローバルな変更

グローバル SVC 圧縮設定を変更するには、グローバル コンフィギュレーション モードで、次の **compression svc** コマンドを使用します。

```
compression svc
no compression svc
```

コンフィギュレーションからコマンドを削除するには、コマンドの **no** 形式を使用します。

次の例では、すべての SVC 接続の圧縮は、グローバルにディセーブルになっています。

```
hostname(config)# no compression svc
```

### SVC 圧縮のグループ別およびユーザ別の変更

特定のグループまたはユーザに対して圧縮の設定を変更するには、グループポリシー モードおよびユーザ名 webvpn モードで、次の **svc compression** コマンドを使用します。

```
svc compression {deflate | none}
no svc compression {deflate | none}
```

デフォルトでは、グループおよびユーザに対し、SVC 圧縮は *deflate*（イネーブル）に設定されています。

コンフィギュレーションから **svc compression** コマンドを削除し、グローバル設定から値が継承されるようにするには、コマンドの **no** 形式を使用します。

次の例では、グループポリシー sales に対し、SVC 圧縮がディセーブルになっています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc compression none
```



(注)

グローバル コンフィギュレーション モードで設定された **compression svc** コマンドは、グループポリシー モードまたはユーザ名 webvpn モードで設定された **svc compression** コマンドを上書きします。

## SVC セッションの表示

特権 EXEC モードで、次の **show vpn-sessiondb** コマンドを使用すると、アクティブな SVC セッションに関する情報を表示することができます。

### **show vpn-sessiondb svc**

次の例では、**show vpn-sessiondb svc** コマンドの出力が表示されます。

```
hostname# show vpn-sessiondb svc

Session Type: SSL VPN Client

Username      : lee
Index         : 1
Protocol      : SSL VPN Client
Hashing       : SHA1
TCP Dst Port  : 443
Bytes Tx      : 20178
Pkts Tx       : 27
Client Ver    : Cisco STC 1.1.0.117
Client Type   : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Q312461)
Group         : DfltGrpPolicy
Login Time    : 14:32:03 UTC Wed Apr 20 2005
Duration      : 0h:00m:04s
Filter Name   :
```



## SVC セッションのログオフ

すべての SVC セッションをログオフするには、グローバル コンフィギュレーション モードで次のように **vpn-sessiondb logoff svc** コマンドを使用します。

**vpn-sessiondb logoff svc**

次の例では、すべての SVC セッションがログオフされます。

```
hostname# vpn-sessiondb logoff svc
INFO: Number of sessions of type "svc" logged off : 1
```

次の **name** オプションまたは **index** オプションを使用すると、SVC セッションを個別にログオフすることができます。

**vpn-session-db logoff name name**

**vpn-session-db logoff index index**

次の **show vpn-sessiondb svc** コマンドを使用すると、コマンドの出力からユーザ名およびインデックス番号（SVC イメージの順序で確立される番号）の両方を検索することができます。次の例は、ユーザ名 *lee* およびインデックス番号 *1* を示します。

```
hostname# show vpn-sessiondb svc

Session Type: SSL VPN Client

Username      : lee
Index         : 1
Protocol      : SSL VPN Client
Hashing       : SHA1
TCP Dst Port  : 443
Bytes Tx      : 20178
Pkts Tx       : 27
Client Ver    : Cisco STC 1.1.0.117
Client Type   : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Q312461)
Group         : DfltGrpPolicy
Login Time    : 14:32:03 UTC Wed Apr 20 2005
Duration      : 0h:00m:04s
Filter Name   :
```

次の例は、**vpn-session-db logoff** コマンドの **name** オプションを使用してセッションを終了します。

```
hostname# vpn-session-db logoff name lee
INFO: Number of sessions with name "lee" logged off : 1
```

## SVC のアップデート

次の手順を実行すると、セキュリティ アプライアンスの SVC イメージを任意の時点でアップデートすることができます。

- 
- ステップ 1** 特権 EXEC モードで **copy** コマンドを実行するか別の方法で新規 SVC イメージをセキュリティ アプライアンスにコピーします。
- ステップ 2** この新規 SVC イメージ ファイルのファイル名がすでにロードされているファイルと同じ場合は、コンフィギュレーションにある **svc image** コマンドを再入力します。新しいファイル名が同じでなければ **no svc image** コマンドで古いファイルをアンインストールします。次に、**svc image** コマンドを使用して SVC イメージに順序を割り当て、セキュリティ アプライアンスで新規 SVC イメージがロードされるようにします。
-



## 証明書の設定

---

この章では、証明書の設定方法について説明します。CA は、証明書要求の管理とデジタル証明書の発行を行います。デジタル証明書には、ユーザまたはデバイスを識別する情報が含まれています。これらの情報には、名前、シリアル番号、社名、部署、IP アドレスなどがあります。デジタル証明書には、ユーザまたは装置の公開キーのコピーが含まれています。CA は、信頼できる第三者（VeriSign など）の場合もあれば、組織内に設置したプライベート CA（インハウス CA）の場合もあります。

次の事項について説明します。

- [公開キー暗号化（P.32-2）](#)
- [証明書の設定（P.32-5）](#)

## 公開キー暗号化

ここでは、次の項目について説明します。

- 公開キー暗号化について (P.32-2)
- 証明書のスケーラビリティ (P.32-2)
- キー ペアについて (P.32-3)
- トラストポイントについて (P.32-3)
- CRL について (P.32-4)
- サポート対象の CA サーバ (P.32-4)

### 公開キー暗号化について

デジタル署名は、公開キー暗号化によってイネーブルになり、デバイスおよびユーザを認証する手段です。RSA 暗号化システムをはじめとする公開キー暗号化では、各ユーザが公開キーと秘密キーの両方を含むキー ペアを持ちます。両キーは補完的に動作し、片方のキーで暗号化されたものはすべて他方のキーで解読できます。

簡単に言えば、データが秘密キーで暗号化されたとき、シグニチャが形成されます。シグニチャはデータに付加されて受信者に送信されます。受信者は送信者の公開キーをデータに適用します。データとともに送信されたシグニチャが、公開キーをデータに適用した結果と一致した場合、メッセージの有効性が確立されます。

このプロセスは、受信者が送信者の公開キーのコピーを持っていること、およびその公開キーが送信者になりすました別人のものではなく、送信者本人のものであることを受信者が強く確信していることに依存しています。

通常、送信者の公開キーは、アウトオブバンドで取得するか、インストール時の操作によって取得します。たとえば、ほとんどの Web ブラウザでは、いくつかの CA のルート証明書がデフォルトで設定されています。VPN の場合、IKE プロトコルは IPSec のコンポーネントであり、デジタル署名を使用してピア デバイスを認証した後で、セキュリティ アソシエーションをセットアップできます。

### 証明書のスケーラビリティ

デジタル証明書がない場合は、通信相手のピアごとに各 IPSec ピアを手動で設定する必要があります。また、ネットワークに新しいピアを追加するたびに、セキュアに通信する必要のあるピアごとの設定変更が必要になります。

デジタル証明書を使用している場合、各ピアは CA に登録されます。2 つのピアは、通信を試みるときに、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアがネットワークに追加された場合は、そのピアを CA に登録するだけで済みます。他のピアを修正する必要はありません。新しいピアが IPSec 接続を試みると、証明書が自動的に交換され、そのピアの認証ができます。

CA を使用した場合、ピアはリモート ピアに証明書を送り、公開キー暗号化を実行することによって、そのリモート ピアに対して自分自身を認証します。各ピアは、CA によって発行および検証された一意の証明書を送ります。このプロセスが機能を果たすのは、各証明書が関連付けられているピアの公開キーをカプセル化し、各証明書が CA によって認証され、参加しているピアすべてが CA を認証権限者として認識しているためです。このプロセスは、RSA シグニチャ付きの IKE と呼ばれます。

ピアは、証明書が期限満了になるまで、複数の IPSec セッションに対して、および複数の IPSec ピア宛てに証明書を送り続けることができます。証明書が期限満了になったときは、ピアの管理者は新しい証明書を CA から入手する必要があります。

CA は、IPSec に参加しなくなったピアの証明書を無効にすることもできます。無効にされた証明書は、他のピアからは有効な証明書とは認識されなくなります。無効にされた証明書は CRL に記載され、各ピアは別のピアの証明書を受け取る前に、CRL をチェックします。

CAの中には、実装の一部として RA を持つものもあります。RA は CA のプロキシの役割を果たすサーバであるため、CA が使用できないときも CA 機能は継続しています。

## キー ペアについて

キー ペアとは、RSA キーまたは DSA キーのことです。これら 2 つのタイプのキーのサポートには、次のような違いがあります。

- DSA キーは SSH や SSL には使用できません。セキュリティ アプライアンスへの SSH アクセスまたは SSL アクセスをイネーブルにするには、RSA キーを使用する必要があります。
- SCEP 登録は、RSA キーの認証用のみにサポートされています。DSA キーを使用する場合は、手動で登録を行う必要があります。
- キーを生成する目的では、RSA キーの最大キー係数は 2048、DSA キーの最大キー係数は 1024 です。キーを生成する場合、どちらのキー タイプもデフォルト サイズは 1024 です。
- シグニチャ操作でサポートされるキーの最大サイズは、RSA キーの場合は 4096 ビットで、DSA キーの場合は 1024 ビットです。
- 署名にも暗号化にも使用できる汎用 RSA キー ペアを生成することも、署名用と暗号化用に別々の RSA キー ペアを生成することもできます。DSA キー ペアは署名用のみに生成します。

署名用と暗号化用にキーを分けると、キーが公開される頻度を少なくすることができます。これは、SSL は署名用ではなく暗号化用にキー使用しますが、IKE は暗号化用ではなく署名用にキーを使用するためです。キーを用途別に分けることで、キーの公開頻度が最小化されます。

## トラストポイントについて

トラストポイントを使用すると、CA と証明書の管理とトレースができます。トラストポイントとは、CA または ID ペアを表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。

トラストポイントの定義が完了したら、CA の指定を必要とするコマンドで、名前によってトラストポイントを参照できます。トラストポイントは複数設定できます。



(注)

セキュリティ アプライアンスに同じ CA を共有するトラストポイントが複数ある場合、CA を共有するトラストポイントでユーザ証明書の検証に使用できるのは 1 つだけです。

**support-user-cert-validation** コマンドで、CA を共有するどのトラストポイントを使用して、その CA が発行したユーザ証明書を検証するかを制御します。

自動登録の場合は、登録 URL がトラストポイントに設定されている必要があり、また、トラストポイントが示す CA がネットワーク上で使用可能であり、SCEP をサポートしている必要があります。

キー ペアと、トラストポイントに関連付けられている発行済み証明書は、PKCS12 形式でエクスポートとインポートができます。これは、異なるセキュリティ アプライアンス上のトラストポイント コンフィギュレーションを手動でコピーする場合に便利です。

## CRL について

CRL は、有効期間内の証明書が発行元の CA によって無効にされているかどうかを、セキュリティ アプライアンスが判断できるようにするものです。証明書を認証するときに必ず CRL チェックを行うように、セキュリティ アプライアンスを設定することができます。CRL チェックはオプションにすることもできます。このようにすると、CA から更新された CRL データが提供されない場合でも、証明書認証は成功します。

CRL コンフィギュレーションは、定義した各トラストポイントのコンフィギュレーションの一部です。セキュリティ アプライアンスは HTTP、SCEP、または LDAP を使用して、CA から CRL を取得できます。トラストポイントごとに取得された CRL は、トラストポイントごとに設定可能な長さの時間だけキャッシュされます。

設定されたキャッシュ時間を超過してセキュリティ アプライアンスにキャッシュされている CRL がある場合、セキュリティ アプライアンスはその CRL を、古すぎて信頼できない、つまり「失効した」と見なします。セキュリティ アプライアンスは、次の証明書の認証によって失効した CRL のチェックが必要になったときに、より新しいバージョンの CRL を取得しようとします。

セキュリティ アプライアンスが CRL をキャッシュしておく時間の長さは、次の 2 つの要素によって決まります。

- **cache-time** コマンドで指定される分数。デフォルト値は 60 分です。
- 取得した CRL 中の NextUpdate フィールド。このフィールドが CRL にない場合もあります。セキュリティ アプライアンスが NextUpdate フィールドを必要とするかどうか、およびこのフィールドを使用するかどうかは、**enforcenextupdate** コマンドで制御します。

セキュリティ アプライアンスは、これら 2 つの要素を次のように使用します。

- NextUpdate フィールドが不要の場合、**cache-time** コマンドで指定された時間が経過すると、セキュリティ アプライアンスは CRL に失効のマークを付けます。
- NextUpdate フィールドが必要な場合、**cache-time** コマンドと NextUpdate フィールドで指定されている 2 つの時間のうち短い方の時間で、CRL に失効のマークを付けます。たとえば、cache-time コマンドによってキャッシュ時間が 100 分に設定され、NextUpdate フィールドによって次のアップデートが 70 分後に指定されている場合、セキュリティ アプライアンスは 70 分後に CRL に失効のマークを付けます。

セキュリティ アプライアンスがメモリ不足で、特定のトラストポイント用にキャッシュされた CRL をすべて保存することができない場合、使用頻度が最も低い CRL が削除され、新しく取得した CRL 用の空き領域が確保されます。

トラストポイント用の CRL 動作を設定する方法の詳細については、[P.32-13 の「トラストポイントの CRL の設定」](#)を参照してください。

## サポート対象の CA サーバ

セキュリティ アプライアンスは次の CA サーバをサポートしています。

- Cisco IOS CS
- Baltimore Technologies
- Entrust
- Microsoft Certificate Services
- Netscape CMS
- RSA Keon
- VeriSign

## 証明書の設定

この項では、セキュリティ アプライアンスにおける証明書の設定方法と、証明書の使用と管理に関するその他の手順について説明します。

ここでは、次の項目について説明します。

- 証明書の準備 (P.32-5)
- キー ペアの設定 (P.32-5)
- トラストポイントの設定 (P.32-7)
- 証明書の取得 (P.32-9)
- トラストポイントの CRL の設定 (P.32-13)
- トラストポイントのエクスポートとインポート (P.32-15)
- CA 証明書マップ規則の設定 (P.32-16)

## 証明書の準備

セキュリティ アプライアンスの証明書を設定する前に、セキュリティ アプライアンスが証明書をサポートするように正しく設定されていることを確認してください。セキュリティ アプライアンスが正しく設定されていないと、登録が失敗したり、不正確な情報が含まれる証明書を登録時に要求したりする可能性があります。

セキュリティ アプライアンスの証明書を準備するには、次の手順を実行します。

---

**ステップ 1** セキュリティ アプライアンスのホスト名とドメイン名が正しく設定されていることを確認します。**show running-config** コマンドを使用すると、現在設定されているホスト名とドメイン名を表示できます。

ホスト名を設定する方法の詳細については、[P.7-2 の「ホスト名の設定」](#)を参照してください。

ドメイン名を設定する方法の詳細については、[P.7-2 の「ドメイン名の設定」](#)を参照してください。

**ステップ 2** CA を設定する前に、セキュリティ アプライアンスのクロックが正しく設定されていることを確認します。証明書には、有効になる日時と満了になる日時が指定されています。セキュリティ アプライアンスが CA に登録して証明書を取得するとき、セキュリティ アプライアンスは現在の時刻が証明書の有効期間の範囲内であるかどうかをチェックします。現在の時刻が有効期間の範囲外の場合、登録は失敗します。

クロックを設定する方法の詳細については、[P.7-3 の「日付と時刻の設定」](#)を参照してください。

---

## キー ペアの設定

ここでは、次の項目について説明します。

- キー ペアの生成 (P.32-6)
- キー ペアの削除 (P.32-7)

## キー ペアの生成

P.32-3 の「キー ペアについて」で説明したように、キー ペアとは RSA キーまたは DSA キーのことです。使用する証明書のタイプに応じてキー ペアを生成する必要があります。

キー ペアを生成するには、次の手順を実行します。

**ステップ 1** PKI 実装に必要なタイプのキー ペアを生成します。これには、必要に応じて次の手順を実行します。

- a. RSA キー ペアを生成する場合は、**crypto key generate rsa** コマンドを使用します。

```
hostname/contexta(config)# crypto key generate rsa
```

追加のキーワードを使用しない場合、このコマンドは汎用 RSA キー ペアを 1 つ生成します。キー係数が指定されないため、デフォルトのキー係数である 1024 が使用されます。その他の係数サイズを指定するには、**modulus** キーワードを使用します。**label** キーワードを使用すると、各キー ペアにラベルを割り当てることもできます。このラベルは、キー ペアを使用するトラストポイントによって参照されます。ラベルを割り当てなかった場合、キー ペアには <Default-RSA-Key> というラベルが自動的に付けられます。

- b. DSA キー ペアを生成する場合は、**crypto key generate dsa label key-pair-label** コマンドを使用します。

```
hostname/contexta(config)# crypto key generate dsa label key-pair-label
```

このコマンドは、1 つの DSA キー ペアを生成します。キー係数が指定されないため、デフォルトのキー係数である 1024 が使用されます。その他の係数サイズを指定するには、**modulus** キーワードを使用します。**label** キーワードを使用して、キー ペアにラベルを割り当てる必要があります。トラストポイントを設定する場合、ラベルを使用してキー ペアを指定できます。



(注)

DSA キーの生成時に、遅延が発生することがあります。Cisco PIX 515E Firewall では、この遅延が最大で 5 分になることもあります。

**ステップ 2** (オプション) **show crypto key mypubkey** コマンドを使用して、キー ペアを表示します。どちらのタイプのキーを表示するかを指定するには、**rsa** キーワードと **dsa** キーワードを使用します。次の例では、汎用 RSA キーを表示します。

```
hostname/contexta(config)# show crypto key mypubkey rsa
Key pair was generated at: 16:39:47 central Feb 10 2005
Key name: <Default-RSA-Key>
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:

30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ea51b7
0781848f 78bccac2 4a1b5b8d 2f3e30b4 4cae9f86 f4485207 159108c9 f5e49103
9eeb0f5d 45fd1811 3b4aafce 292b3b64 b4124a6f 7a777b08 75b88df1 8092a9f8
5508e9e5 2c271245 7fd1c0c3 3aaf1e04 c7c4efa4 600f4c4a 6afe56ad c1d2c01c
e08407dd 45d9e36e 8cc0bfef 14f9e6ac eca141e4 276d7358 f7f50d13 79020301 0001
Key pair was generated at: 16:34:54 central Feb 10 2005
```

**ステップ 3** 生成したキー ペアを保存します。これを行うには、**write memory** コマンドを入力して、実行コンフィギュレーションを保存します。



## キー ペアの削除

キー ペアを削除するには、グローバル コンフィギュレーション モードで **crypto key zeroize** コマンドを使用します。

次の例では、RSA キー ペアを削除します。

```
hostname(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All device certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
hostname(config)#
```

## トラストポイントの設定

トラストポイントについては、[P.32-3](#) の「[トラストポイントについて](#)」を参照してください。

トラストポイントを設定するには、次の手順を実行します。

- ステップ 1** セキュリティ アプライアンスが証明書を受け取る必要のある CA に対応するトラストポイントを作成します。

```
hostname/contexta(config)# crypto ca trustpoint trustpoint
```

たとえば、Main という名前のトラストポイントを宣言するには、次のようにします。

```
hostname/contexta(config)# crypto ca trustpoint Main
hostname/contexta(config-ca-trustpoint)#
```

このコマンドを入力すると、Crypto ca トラストポイント コンフィギュレーション モードに入ります。

- ステップ 2** このトラストポイントで使用する登録方式を指定します。



(注)

トラストポイントが DSA キーを使用する場合は、手動で登録を行う必要があります。セキュリティ アプライアンスは、DSA キーを持つ証明書の自動登録をサポートしていません。

登録方式を指定するには、次のいずれかを実行します。

- SCEP 登録を指定するには、**enrollment url** コマンドを使用して、宣言したトラストポイントで SCEP 登録に使用する URL を設定します。たとえば、セキュリティ アプライアンスが URL `http://10.29.67.142:80/certsrv/mscep/mscep.dll` を使用してトラストポイント Main に証明書を要求する場合、コマンドは次のようになります。

```
hostname/contexta(config-ca-trustpoint)# enrollment url
http://10.29.67.142:80/certsrv/mscep/mscep.dll
```

- 手動登録を指定するには、**enrollment terminal** コマンドを使用して、CA から取得した証明書を端末に貼り付けることを指定します。

**ステップ 3** 必要に応じて、別の特性をトラストポイントに指定できます。定義する必要のある特性は、CA とそのコンフィギュレーションによって異なります。トラストポイントの特性を指定するには、次のコマンドを使用します。これらのコマンドの完全な説明と使用上のガイドラインについては、『Cisco Security Appliance Command Reference』を参照してください。

- **crl required | optional | nocheck** : CRL コンフィギュレーションのオプションを指定します。**optional** キーワードを使用して **crl** コマンドを入力すると、セキュリティ アプライアンスが CRL にアクセスできない場合でも、セキュリティ アプライアンスはピアからの証明書を受け入れることができます。



(注)

必須またはオプションの CRL チェックをイネーブルにする場合、必ず CRL 管理用のトラストポイントを設定してください。これは、証明書を取得した後に実行する必要があります。トラストポイントの CRL 管理を設定する方法の詳細については、[P.32-13 の「トラストポイントの CRL の設定」](#)を参照してください。

- **crl configure** : CRL コンフィギュレーション モードに入ります。
- **default enrollment** : すべての登録パラメータをシステム デフォルト値に戻します。このコマンドの呼び出しは、アクティブなコンフィギュレーションの一部になりません。
- **enrollment retry period** : (オプション) リトライ間隔を分単位で指定します。この特性は、SCEP 登録を使用している場合にのみ適用されます。
- **enrollment retry count** : (オプション) 許可されるリトライの最大回数を指定します。この特性は、SCEP 登録を使用している場合にのみ適用されます。
- **enrollment terminal** : このトラストポイントで使用するカット アンド ペースト登録を指定します。
- **enrollment url URL** : このトラストポイントで使用する自動登録 (SCEP) を指定し、登録 URL を設定します。
- **fqdn fqdn** : 登録時に、指定された完全修飾ドメイン名を、証明書の Subject Alternative Name 拡張子に含めるように CA に要求します。
- **email address** : 登録時に、指定された電子メール アドレスを、証明書の Subject Alternative Name 拡張子に含めるように CA に要求します。
- **subject-name X.500 name** : 登録時に、指定されたサブジェクト DN を、証明書に含めるように CA に要求します。
- **serial-number** : 登録時に、セキュリティ アプライアンスのシリアル番号を証明書に含めるように CA に要求します。
- **ip-address ip-address** : 登録時に、セキュリティ アプライアンスの IP アドレスを証明書に含めるように CA に要求します。
- **password string** : 登録時に CA に登録されるチャレンジ フレーズを指定します。CA は、通常、このフレーズを使用して、その後の失効要求を認証します。
- **keypair name** : 公開キーが認証の対象となるキー ペアを指定します。
- **id-cert-issuer** : このトラストポイントに関連付けられている CA が発行したピア証明書を、システムが受け入れるかどうかを示します。
- **accept-subordinates** : このトラストポイントに関連付けられている CA よりも下位の CA 証明書が、事前にデバイスにインストールされていない状態でフェーズ 1 の IKE 交換時に配信された場合に、受け入れられるかどうかを示します。
- **support-user-cert-validation** : イネーブルになっている場合、リモート ユーザ証明書を検証するコンフィギュレーション設定が、このトラストポイントから取得されます。ただし、このトラストポイントが、そのリモート ユーザ証明書を発行した CA に認証されることが前提です。
- **exit** : このモードを終了します。

- ステップ 4**    トラストポイント コンフィギュレーションを保存します。これを行うには、**write memory** コマンドを入力して、実行コンフィギュレーションを保存します。

## 証明書の取得

セキュリティ アプライアンスは、トラストポイントごとに 1 つの CA 証明書が必要で、セキュリティ アプライアンス自体には、トラストポイントで使用するキーのコンフィギュレーションに応じて 1 つまたは 2 つの証明書が必要です。トラストポイントが署名と暗号化に別々の RSA キーを使用する場合、セキュリティ アプライアンスには署名用と暗号化用の 2 つの証明書が必要になります。署名用と暗号化用のキーが同じである場合、必要な証明書は 1 つです。

セキュリティ アプライアンスは、SCEP を使用した登録と、base-64-encoded 証明書を直接端末に貼り付けられる手動登録をサポートしています。サイトツーサイト VPN の場合は、各セキュリティ アプライアンスを登録する必要があります。リモートアクセス VPN の場合は、各セキュリティ アプライアンスと各リモートアクセス VPN クライアントを登録する必要があります。

ここでは、次の項目について説明します。

- [SCEP を使用した証明書の取得 \(P.32-9\)](#)
- [手動での証明書の取得 \(P.32-11\)](#)

## SCEP を使用した証明書の取得

この手順では、SCEP を使用して証明書を設定するための手順について説明します。自動登録を設定したトラストポイントごとに、これらの手順を繰り返す必要があります。この手順を完了したときに、セキュリティ アプライアンスはトラストポイントの CA 証明書と、署名と暗号化の目的で 1 つまたは 2 つの証明書を受信しています。DSA キーを使用する場合は、署名用の証明書のみを受信します。汎用 RSA キーを使用する場合は、署名用と暗号化用の証明書を受信します。署名と暗号化に別々の RSA キーを使用する場合は、セキュリティ アプライアンスは署名用と暗号化用の別々の証明書を受信します。



(注)

トラストポイントが証明書の取得に SCEP を使用するかどうかは、そのトラストポイントを設定するときに **enrollment url** コマンドを使用するかどうかによって決まります ([P.32-7 の「トラストポイントの設定」](#)を参照)。

SCEP を使用して証明書を取得するには、次の手順を実行します。

- ステップ 1**    設定したトラストポイントの CA 証明書を取得します。

```
hostname/contexta(config)# crypto ca authenticate trustpoint
```

たとえば、下位 CA を表す Main という名前のトラストポイントを使用する場合は、次のようになります。

```
hostname/contexta(config)# crypto ca authenticate Main
```

```
INFO: Certificate has the following attributes:  
Fingerprint:      3736ffc2 243ecf05 0c40f2fa 26820675  
Do you accept this certificate? [yes/no]: y
```

```
Trustpoint 'Main' is a subordinate CA and holds a non self signed cert.  
Trustpoint CA certificate accepted.
```

**ステップ 2** このトラストポイントを持つセキュリティ アプライアンスを登録します。このプロセスでは、署名データの証明書を取得し、設定したキーのタイプによっては暗号化データの証明書も取得します。

**ステップ 3** 登録を行うには、**crypto ca enroll** コマンドを使用します。CA の管理者は、CA が証明書を付与する前に手動で登録要求を認証しなければならない場合があるため、このコマンドを入力する前に CA の管理者に連絡してください。

```
hostname(config)# crypto ca enroll trustpoint
```

セキュリティ アプライアンスが証明書要求を送信してから 1 分（デフォルト）以内に CA から証明書を受け取らなかった場合は、証明書要求を再送信します。セキュリティ アプライアンスは、証明書を受信するまで、1 分ごとに証明書要求を送信し続けます。



**(注)** トラストポイントの完全修飾ドメイン名がセキュリティ アプライアンスの完全修飾ドメイン名と一致しなかった場合（完全修飾ドメイン名が文字の場合も含む）、警告が表示されます。必要に応じて、登録プロセスを終了し、必要な修正を行ってから、再度 **crypto ca enroll** コマンドを入力します。

次の例では、Main という名前のトラストポイントで登録を実行しています。

```
hostname(config)# crypto ca enroll Main
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
% password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
Password: 2b0rn0t2b
Re-enter password: 2b0rn0t2b
% The subject name in the certificate will be: securityappliance.example.com
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com
% Include the device serial number in the subject name? [yes/no]: no
Request certificate from CA [yes/no]: yes
% Certificate request sent to Certificate authority.
```



**(注)** セキュリティ アプライアンスの証明書を無効にする場合はパスワードが必要になるため、このパスワードを覚えておくことが不可欠です。パスワードは書き留めて安全な場所に保管してください。

セキュリティ アプライアンスが登録する必要があるトラストポイントごとに、**crypto ca enroll** コマンドを入力する必要があります。



**(注)** **crypto ca enroll** コマンドを発行した後、証明書を受信する前にセキュリティ アプライアンスがリブートされた場合は、**crypto ca enroll** コマンドを再発行して、CA 管理者に連絡してください。

- ステップ 4** **show crypto ca certificate** コマンドを使用して、登録プロセスが成功したことを確認します。たとえば、トラストポイント Main から受信した証明書を表示するには、次のように入力します。

```
hostname/contexta(config)# show crypto ca certificate Main
```

このコマンドの出力で、セキュリティ アプライアンスに対して発行された証明書とトラストポイントの CA 証明書の詳細が表示されます。

- ステップ 5** **write memory** コマンドを使用して、コンフィギュレーションを保存します。

```
hostname/contexta(config)# write memory
```

## 手動での証明書の取得

ここでは、手動による証明書要求を設定するための手順について説明します。手動登録を設定したトラストポイントごとに、この手順を繰り返す必要があります。この手順を完了したときに、セキュリティ アプライアンスはトラストポイントの CA 証明書と、署名と暗号化の目的で 1 つまたは 2 つの証明書を受信しています。DSA キーを使用する場合は、署名用の証明書のみを受信します。汎用 RSA キーを使用する場合は、署名用と暗号化用の証明書を受信します。署名と暗号化に別々の RSA キーを使用する場合、受信した証明書はそれぞれ署名専用と暗号化専用で使用されます。



(注)

トラストポイントが手動で証明書を取得する必要があるかどうかは、そのトラストポイントを設定するときに **enrollment terminal** コマンドを使用するかどうかによって決まります（P.32-7 の「[トラストポイントの設定](#)」を参照）。

証明書を手動で取得するには、次の手順を実行します。

- ステップ 1** トラストポイントで示されている CA から、base-64 encoded CA 証明書を取得します。

- ステップ 2** CA 証明書をインポートします。これを行うには、**crypto ca authenticate** コマンドを使用します。次の例は、トラストポイント Main の CA 証明書要求を示しています。

```
hostname (config)# crypto ca authenticate Main
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVCqP/KW74VP0NZzL+JbRTANBgqhkiG9w0BAQUFADCB
[ certificate data omitted ]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint:      24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
hostname (config)#
```

- ステップ 3** 証明書要求を生成します。これを行うには、**crypto ca enroll** コマンドを使用します。次の例は、トラストポイント Main の証明書と暗号化キーの要求を示しています。トラストポイント Main は、手動登録を使用し、署名用と暗号化用の汎用 RSA キーを使用するように設定されています。

```
hostname (config)# crypto ca enroll Main
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be:
securityappliance.example.com

% Include the device serial number in the subject name? [yes/no]: n

Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:

MIIBoDCCAQkCAQAwIzEhMB8GCSqGSIb3DQEJAhYSRmVyYWxQaXguY2l2Y28uY29t
[ certificate request data omitted ]
jF4waw68eOxQxVmdgMWeQ+RbIOYmvt8g6hnBTrd0GdqjjVLt

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: n
hostname (config)#
```

**(注)**

署名と暗号化に別々の RSA キーを使用する場合、**crypto ca enroll** コマンドは各キーに対する 2 つの証明書要求を表示します。登録を完了するには、**crypto ca enroll** コマンドで生成されたすべての証明書要求に対する証明書を取得します。

- ステップ 4** **crypto ca enroll** コマンドで生成される要求ごとに、該当するトラストポイントで示される CA から証明書を取得します。証明書が base-64 形式であることを確認してください。

- ステップ 5** CA から受信した証明書ごとに、**crypto ca import certificate** コマンドを使用します。セキュリティアプライアンスは、証明書を base-64 形式で端末に貼り付けることを求めるプロンプトを表示します。

**(注)**

署名と暗号化に別々の RSA キー ペアを使用する場合は、証明書ごとにこのステップを実行してください。セキュリティアプライアンスは、証明書が署名キー ペア用か暗号化キー ペア用かを自動的に判断します。2 つの証明書をインポートする順序は、どちらが先でも関係ありません。

次の例では、トラストポイント Main 用の証明書を手動でインポートします。

```
hostname (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
hostname (config)#
```

- ステップ 6** `show crypto ca certificate` コマンドを使用して、登録プロセスが成功したことを確認します。たとえば、トラストポイント Main から受信した証明書を表示するには、次のように入力します。

```
hostname/contexta(config)# show crypto ca certificate Main
```

このコマンドの出力で、セキュリティ アプライアンスに対して発行された証明書とトラストポイントの CA 証明書の詳細が表示されます。

- ステップ 7** `write memory` コマンドを使用して、コンフィギュレーションを保存します。

```
hostname/contexta(config)# write memory
```

## トラストポイントの CRL の設定

証明書の認証時に必須またはオプションの CRL チェックを行う場合は、トラストポイントごとに CRL を設定する必要があります。CRL の詳細については、[P.32-4 の「CRL について」](#)を参照してください。

トラストポイントの CRL を設定するには、次の手順を実行します。

- ステップ 1** CRL コンフィギュレーションを変更するトラストポイントに対して、Crypto ca トラストポイント コンフィギュレーション モードに入ります。これを行うには、`crypto ca trustpoint` コマンドを入力します。

- ステップ 2** まだ CRL をイネーブルにしていない場合は、`crl` コマンドに `required` キーワードまたは `optional` キーワードを指定して、イネーブルにします。`required` キーワードを指定すると、CRL が使用できない場合、このトラストポイントの証明書認証は失敗します。

- ステップ 3** `crl configure` コマンドを入力します。

```
hostname/contexta(config-ca-trustpoint)# crl configure
hostname/contexta(config-ca-crl)#
```

このコマンドを入力すると、現在のトラストポイントに対して `crl` コンフィギュレーション モードに入ります。



### ヒント

すべての CRL コンフィギュレーションのオプションをデフォルト値に設定するには、`default` コマンドを使用します。CRL の設定中に、やり直す必要がある場合は、いつでもこのコマンドを入力して、この手順を再度開始できます。

- ステップ 4** `policy` コマンドで、取得ポリシーを設定します。このコマンドの次のキーワードによって、取得ポリシーが決まります。

- `cdp` : CRL は、認証済みの証明書で指定されている CRL 分散ポイントだけから取得できます。



### (注)

SCEP の取得は、証明書で指定されている分散ポイントではサポートされていません。



- **static** : CRL は、設定した URL だけから取得できます。
- **both** : CRL は、認証済みの証明書で指定されている CRL 分散ポイントと、設定した URL の両方から取得できます。

**ステップ 5** CRL ポリシーを設定したときに **static** キーワードまたは **both** キーワードを使用した場合は、**url** コマンドを使用して、CRL 取得用の URL を設定する必要があります。1 ～ 5 のランクを付けて、最大 5 つの URL を入力できます。

```
hostname/contexta(config-ca-crl)# url n URL
```

*n* は、URL に割り当てられるランクです。URL を削除するには、**no url *n*** コマンドを使用します。

**ステップ 6** **protocol** コマンドで、取得方式を設定します。このコマンドの次のキーワードによって、取得方式が決まります。

- **http** : CRL 取得方式として HTTP を指定します。
- **ldap** : CRL 取得方式として LDAP を指定します。
- **scep** : CRL 取得方式として SCEP を指定します。

**ステップ 7** セキュリティ アプライアンスが現在のトラストポイントの CRL をキャッシュしている時間を設定します。セキュリティ アプライアンスが CRL を失効と判断するまで待機する時間を分数で指定するには、次のコマンドを入力します。

```
hostname/contexta(config-ca-crl)# cache-time n
```

*n* は分数です。たとえば、CRL を 7 時間キャッシュする必要がある場合は、次のコマンドを入力します。

```
hostname/contexta(config-ca-crl)# cache-time 420
```

**ステップ 8** セキュリティ アプライアンスに CRL の NextUpdate フィールドが必要かどうかを設定します。セキュリティ アプライアンスが NextUpdate フィールドをどのように使用するかについては、[P.32-4 の「CRL について」](#)を参照してください。

次のいずれかを実行します。

- NextUpdate フィールドが必要な場合は、**enforcenextupdate** コマンドを入力します。これはデフォルトの設定です。
- CRL の NextUpdate フィールドが不要な場合は、**no enforcenextupdate** コマンドを入力します。

**ステップ 9** 取得プロトコルとして LDAP を指定した場合は、次の手順を実行します。

- 次のコマンドを入力して、セキュリティ アプライアンスが LDAP サーバを認識するようにします。

```
hostname/contexta(config-ca-crl)# ldap-defaults server
```

LDAP サーバは、DNS ホスト名または IP アドレスで指定できます。LDAP サーバがデフォルトの 389 以外のポートで LDAP クエリを受信する場合は、ポート番号も指定できます。たとえば、次のコマンドは、ホスト名が **ldap1** の LDAP サーバから CRL を取得するようにセキュリティ アプライアンスを設定します。

```
hostname/contexta(config-ca-crl)# ldap-defaults ldap1
```



**(注)**

LDAP サーバの指定に IP アドレスではなくホスト名を使用する場合は、DNS を使用するようにセキュリティ アプライアンスを設定していることを確認してください。DNS を設定する方法については、『Cisco Security Appliance Command Reference』の **dns** コマンドを参照してください。

- b. LDAP サーバに CRL 取得を許可するクレデンシャルが必要な場合は、次のコマンドを入力します。

```
hostname/contexta(config-ca-crl)# ldap-dn admin-DN password
```

次の例を参考にしてください。

```
hostname/contexta(config-ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering  
c001RunZ
```

**ステップ 10** 現在のトラストポイントの CRL コンフィギュレーションをテストするには、**crypto ca crl request** コマンドを使用します。このコマンドは、指定したトラストポイントによって示される CA から現在の CRL を取得します。

**ステップ 11** 実行コンフィギュレーションを保存します。**write memory** コマンドを入力します。

## トラストポイントのエクスポートとインポート

キー ペアと、トラストポイントに関連付けられている発行済み証明書は、エクスポートおよびインポートできます。セキュリティ アプライアンスは、トラストポイントのエクスポートとインポートにおいて、PKCS12 形式をサポートしています。

ここでは、次の項目について説明します。

- [トラストポイント コンフィギュレーションのエクスポート \(P.32-15\)](#)
- [トラストポイント コンフィギュレーションのインポート \(P.32-16\)](#)

## トラストポイント コンフィギュレーションのエクスポート

関連付けられているすべてのキーや証明書とともに、トラストポイント コンフィギュレーションを PKCS12 形式でエクスポートするには、**crypto ca export** コマンドを使用します。セキュリティ アプライアンスは PKCS12 データを端末に表示します。この表示されたデータはコピーできます。トラストポイント データはパスワードで保護されますが、このデータをファイルに保存する場合は、そのファイルが安全な場所にあることを確認してください。

次の例では、パスフレーズとして Wh0zits を使用して、PKCS12 データをトラストポイント Main にエクスポートしています。

```
hostname (config)# crypto ca export Main pkcs12 Wh0zits  
  
Exported pkcs12 follows:  
  
[ PKCS12 data omitted ]  
  
---End - This line not part of the pkcs12---  
  
hostname (config)#
```

## トラストポイント コンフィギュレーションのインポート

トラストポイント コンフィギュレーションに関連付けられているキー ペアと発行済み証明書をインポートするには、グローバル コンフィギュレーション モードで **crypto ca import pkcs12** コマンドを使用します。セキュリティ アプライアンスは、テキストを base-64 形式で端末に貼り付けることを求めるプロンプトを表示します。

トラストポイントとともにインポートされたキー ペアには、作成するトラストポイントの名前と一致するラベルが割り当てられます。たとえば、エクスポートされたトラストポイントが <Default-RSA-Key> というラベルの付いた RSA キーを使用していた場合、PKCS12 をインポートして **Main** という名前のトラストポイントを作成すると、作成されるキー ペアの名前は <Default-RSA-Key> ではなく **Main** になります。



(注)

セキュリティ アプライアンスに同じ CA を共有するトラストポイントが複数ある場合、CA を共有するトラストポイントでユーザ証明書の検証に使用できるのは 1 つだけです。**crypto ca import pkcs12** コマンドを使用すると、このような状況を構成できます。**support-user-cert-validation** コマンドで、CA を共有するどのトラストポイントを使用して、その CA が発行したユーザ証明書を検証するかを制御します。

次の例では、パスフレーズ **Wh0zits** とともに PKCS12 データを手動でトラストポイント **Main** にインポートしています。

```
hostname (config)# crypto ca import Main pkcs12 Wh0zits

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
hostname (config)#
```

## CA 証明書マップ規則の設定

証明書の Issuer フィールドと Subject フィールドに基づいて、規則を設定できます。作成した規則を使用すると、**tunnel-group-map** コマンドによって、IPSec ピアの証明書をトンネルグループにマッピングできます。セキュリティ アプライアンスは CA 証明書マップを 1 つサポートしています。これには、複数の規則を設定できます。トンネルグループで CA 証明書マップ規則を使用する方法の詳細については、[P.24-12 の「証明書グループ照合の規則とポリシーの作成」](#)を参照してください。

CA 証明書マップ規則を設定するには、次の手順を実行します。

- ステップ 1** 設定する規則に対して CA 証明書マップ コンフィギュレーション モードに入ります。これには、**crypto ca certificate map** コマンドを入力し、規則インデックス番号を指定します。次の例では、インデックス番号 1 の規則に対して CA 証明書マップ モードに入っています。

```
hostname(config)# crypto ca certificate map 1
hostname(config-ca-cert-map)#
```

**ステップ 2** 規則を設定するには、**issuer-name** コマンドと **subject-name** コマンドを使用します。これらのコマンドは、セキュリティ アプライアンスが証明書の Issuer フィールドまたは Subject フィールドの値に適用できるテストを指定します。これらのテストは、特定のアトリビュートに適用することや、Issuer フィールドまたは Subject フィールド全体に適用することができます。規則ごとに複数のテストを設定できますが、これらのコマンドで指定するすべてのテストは、証明書と一致する規則で真である必要があります。**issuer-name** コマンドと **subject-name** コマンドの有効な演算子は、次のとおりです。

| 演算子 | 意味                                 |
|-----|------------------------------------|
| eq  | フィールドまたはアトリビュートが所定の値と一致する。         |
| ne  | フィールドまたはアトリビュートが所定の値と一致しない。        |
| co  | フィールドまたはアトリビュートの一部または全部が所定の値と一致する。 |
| nc  | フィールドまたはアトリビュートの全部が所定の値と一致しない。     |

**issuer-name** コマンドと **subject-name** コマンドの詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。

次の例では、Issuer フィールド内のアトリビュートに文字列 `cisco` が含まれるように指定しています。

```
hostname(config-ca-cert-map)# issuer-name co cisco
hostname(config-ca-cert-map)#
```

次の例では、Subject フィールド内の Organizational Unit アトリビュートが文字列 `Engineering` と完全に一致しなければならないことを指定しています。

```
hostname(config-ca-cert-map)# subject-name attr ou eq Engineering
hostname(config-ca-cert-map)#
```

マップ規則は、**show running-config** コマンドの出力に表示されます。

```
crypto ca certificate map 1
  issuer-name co cisco
  subject-name attr ou eq Engineering
```

**ステップ 3** マップ規則の設定が完了したら、作業内容を保存します。**write memory** コマンドを入力します。





## PART 4

### システム管理







## システム アクセスの管理

---

この章では、Telnet、SSH、および HTTPS を介してシステム管理のためにセキュリティ アプライアンスにアクセスする方法について説明します。また、ユーザを認証および認可する方法とログイン バナーを作成する方法についても説明します。

次の事項について説明します。

- [Telnet アクセスの許可 \(P.33-2\)](#)
- [SSH アクセスの許可 \(P.33-3\)](#)
- [ASDM の HTTPS アクセスの許可 \(P.33-5\)](#)
- [システム管理者の AAA \(P.33-6\)](#)
- [ログイン バナーの設定 \(P.33-19\)](#)



(注)

管理アクセスのためにセキュリティ アプライアンス インターフェイスにアクセスする場合、ホスト IP アドレスを許可するアクセスリストは不要です。この章の各項で説明する手順に従って、管理アクセスのみ設定する必要があります。

---

## Telnet アクセスの許可

セキュリティ アプライアンスは、管理目的でセキュリティ アプライアンスへの Telnet 接続を許可します。IPSec トンネル内で Telnet を使用する場合を除き、最も低いセキュリティ インターフェイスに対して Telnet を使用することはできません。

セキュリティ アプライアンスは、コンテキストごとに最大 5 つの同時 Telnet 接続を許可し、可能な場合は、最大 100 の接続がすべてのコンテキストの間で分割されます。

セキュリティ アプライアンスへの Telnet アクセスを設定するには、次の手順を実行します。

- ステップ 1** セキュリティ アプライアンスが接続を受け入れる送信元 IP アドレスを指定するには、アドレスまたはサブネットごとに、次のコマンドを入力します。

```
hostname(config)# telnet source_IP_address mask source_interface
```

インターフェイスが 1 つしかない場合は、インターフェイスのセキュリティ レベルが 100 である限り、そのインターフェイスにアクセスするように Telnet を設定することができます。

- ステップ 2** (オプション) セキュリティ アプライアンスが Telnet セッションを切断するまでに、セッションがアイドル状態を維持する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
```

タイムアウトは 1 ～ 1440 分に設定します。デフォルトは 5 分です。デフォルト値では一般に短すぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定しておいてください。

たとえば、192.168.1.2 というアドレスを持つ内部インターフェイス上のホストからセキュリティ アプライアンスにアクセスするには、次のように入力します。

```
hostname(config)# telnet 192.168.1.2 255.255.255.255 inside  
hostname(config)# telnet timeout 30
```

192.168.3.0 ネットワーク上のすべてのユーザが内部インターフェイス上のセキュリティ アプライアンスにアクセスできるようにするには、次のコマンドを入力します。

```
hostname(config)# telnet 192.168.3.0 255.255.255.0 inside
```



## SSH アクセスの許可

セキュリティ アプライアンスは、管理目的でセキュリティ アプライアンスへの SSH 接続を許可します。セキュリティ アプライアンスは、コンテキストごとに最大 5 つの同時 SSH 接続を許可し、可能な場合は、最大 100 の接続がすべてのコンテキストの間で分割されます。

SSH は、強力な認証と暗号化機能を提供する TCP/IP など、信頼性の高いトランスポート層で実行されるアプリケーションです。セキュリティ アプライアンスは SSH バージョン 1 および 2 で提供されている SSH リモート シェル機能をサポートし、DES 暗号および 3DES 暗号をサポートします。

**(注)**

SSL および SSH での XML 管理は、PIX Version 7.0 および 7.0 ではサポートされていません。

ここでは、次の項目について説明します。

- [SSH アクセスの設定 \(P.33-3\)](#)
- [SSH クライアントの使用 \(P.33-4\)](#)

## SSH アクセスの設定

セキュリティ アプライアンスへの SSH アクセスを設定するには、次の手順を実行します。

**ステップ 1** SSH に必要な RSA キー ペアを生成するには、次のコマンドを入力します。

```
hostname(config)# crypto key generate rsa modulus modulus_size
```

係数（ビット単位）は 512、768、1024、または 2048 です。指定するキー係数のサイズが大きいほど、RSA の生成にかかる時間は長くなります。値は 1024 にすることを推奨します。

**ステップ 2** 永続的なフラッシュ メモリに RSA キーを保存するには、次のコマンドを入力します。

```
hostname(config)# write mem
```

**ステップ 3** セキュリティ アプライアンスが接続を受け入れる送信元 IP アドレスを指定するには、アドレスまたはサブネットごとに、次のコマンドを入力します。

```
hostname(config)# ssh source_IP_address mask source_interface
```

セキュリティ アプライアンスは、最も低いセキュリティ レベルの接続も含め、すべてのインターフェイスから SSH 接続を受け入れます。

**ステップ 4** (オプション) セキュリティ アプライアンスが SSH セッションを切断するまでに、セッションがアイドル状態を維持する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
```

タイムアウトは 1 ～ 60 分に設定します。デフォルトは 5 分です。デフォルト値では一般に短かすぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定してください。

たとえば、RSA キーを生成し、192.168.1.2 というアドレスを持つ内部インターフェイス上のホストからセキュリティ アプライアンスにアクセスするには、次のように入力します。

```
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
```

192.168.3.0 ネットワーク上のすべてのユーザが内部インターフェイス上のセキュリティ アプライアンスにアクセスできるようにするには、次のコマンドを入力します。

```
hostname(config)# ssh 192.168.3.0 255.255.255.0 inside
```

デフォルトでは、SSH はバージョン 1 とバージョン 2 の両方を許可します。バージョン番号を指定するには、次のコマンドを入力します。

```
hostname(config)# ssh version version_number
```

*version\_number* には 1 または 2 を指定します。

## SSH クライアントの使用

SSH を使用してセキュリティ アプライアンス コンソールにアクセスするには、SSH クライアントでユーザ名 **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 (P.33-4 の「ログインパスワードの変更」を参照してください)。

SSH セッションを開始すると、次のように SSH ユーザ認証プロンプトが表示される前に、セキュリティ アプライアンス コンソール上にドット (.) が表示されます。

```
hostname(config)# .
```

ドットが表示されても、SSH の機能には影響を与えません。コンソールにドットが表示されるのは、ユーザ認証が始まる前で、サーバ キーを生成する場合か、または SSH キー交換中に秘密キーを使用してメッセージを暗号化する場合です。これらのタスクには 2 分以上かかることがあります。ドットは、セキュリティ アプライアンスがビジー状態で、ハングしていないことを示す進捗インジケータです。

## ログインパスワードの変更

ログインパスワードは Telnet 接続と SSH 接続に使用されます。デフォルトでは、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** と入力します。パスワードは、最大 16 文字の英数字および特殊文字で、大文字と小文字の区別があります。パスワードには疑問符 (?) とスペースを除く任意の文字を使用できます。

パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。パスワードをデフォルト設定に戻すには、**no password** コマンドを使用します。

## ASDM 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、セキュリティ アプライアンスへの 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、これらのタスクがすべて完了します。この項では、ASDM アクセスを手動で設定する方法について説明します。

セキュリティ アプライアンスは、コンテキストごとに最大 5 つの同時 ASDM インスタンスを許可し、可能な場合は、最大 32 の ASDM インスタンスがすべてのコンテキストの間で許可されます。



(注)

WebVPN と ASDM 管理を同じインターフェイス上でイネーブルにすることはできません。あるインターフェイス上で WebVPN をイネーブルにした場合、そのインターフェイスを ASDM に使用することはできません。

ASDM アクセスを設定するには、次の手順を実行します。

- ステップ 1** セキュリティ アプライアンスが HTTPS 接続を受け入れる送信元 IP アドレスを指定するには、アドレスまたはサブネットごとに、次のコマンドを入力します。

```
hostname(config)# http source_IP_address mask source_interface
```

- ステップ 2** HTTPS サーバ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)# http server enable
```

- ステップ 3** ASDM イメージのロケーションを指定するには、次のコマンドを入力します。

```
hostname(config)# asdm image disk0:/asdmfile
```

たとえば、HTTPS サーバをイネーブルにして、192.168.1.2 というアドレスを持つ内部インターフェイス上のホストから ASDM にアクセスするには、次のように入力します。

```
hostname(config)# crypto key generate rsa modulus 1024  
hostname(config)# write mem  
hostname(config)# http server enable  
hostname(config)# http 192.168.1.2 255.255.255.255 inside
```

192.168.3.0 ネットワーク上のすべてのユーザが内部インターフェイス上の ASDM にアクセスできるようにするには、次のコマンドを入力します。

```
hostname(config)# http 192.168.3.0 255.255.255.0 inside
```

## システム管理者の AAA

この項では、システム管理者の認証とコマンド認可をイネーブルにする方法について説明します。システム管理者の AAA を設定する前に、まず第 10 章「AAA サーバおよびローカル データベースのサポート」に従ってローカル データベースまたは AAA サーバを設定します。

ここでは、次の項目について説明します。

- CLI アクセスの認証の設定 (P.33-6)
- 特権 EXEC モードにアクセスするための認証の設定 (P.33-7)
- コマンド認可の設定 (P.33-8)
- コマンド アカウンティングの設定 (P.33-16)
- 現在のログイン ユーザの表示 (P.33-17)
- ロックアウトからの回復 (P.33-17)

### CLI アクセスの認証の設定

CLI 認証をイネーブルにすると、セキュリティ アプライアンスはログインのためユーザ名とパスワードの入力を求めるプロンプトを表示します。情報を入力した後、ユーザ EXEC モードにアクセスできるようになります。

特権 EXEC モードに入るには、**enable** コマンドまたは **login** コマンドを入力します（ローカル データベースを使用している場合のみ）。

イネーブル認証を設定する場合（P.33-7 の「**enable** コマンドの認証の設定」を参照）は、セキュリティ アプライアンスによってユーザ名とパスワードの入力を求めるプロンプトが表示されます。イネーブル認証を設定しない場合は、**enable** コマンドを入力する際にシステム イネーブル パスワードを入力します（**enable password** コマンドで設定）。ただし、イネーブル認証を使用しない場合、**enable** コマンドを入力した後、特定のユーザとしてログインする必要はありません。ユーザ名を保持するには、イネーブル認証を使用します。

ローカル データベースを使用して認証する場合は、**login** コマンドを使用できます。これにより、ユーザ名が保持されますが、認証をオンにする設定は必要ありません。



(注)

セキュリティ アプライアンスで Telnet、SSH、または HTTP ユーザを認証できるようにするには、まず **telnet**、**ssh**、および **http** コマンドを使用してセキュリティ アプライアンスへのアクセスを設定する必要があります。これらのコマンドは、セキュリティ アプライアンスとの通信が許可された IP アドレスを識別します。

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** キーワードは、HTTPS を使用してセキュリティ アプライアンスにアクセスする ASDM クライアントを認証します。HTTP 認証を設定する必要があるのは、RADIUS または TACACS+ サーバを使用する場合だけです。デフォルトでは、このコマンドを設定しない場合でも、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は、AAA サーバが使用できないときにローカル データベースをフォールバック方式として使用するようにセキュリティ アプライアンスを設定できます。サーバグループ名の後ろに **LOCAL** を指定します (**LOCAL** は大文字と小文字を区別します)。セキュリティ アプライアンスは、どちらの方式を使用しているかを示すプロンプトを表示しないため、ローカル データベースと AAA サーバで同じユーザ名とパスワードを使用することをお勧めします。

**LOCAL** だけを入力して、ローカル データベースを認証の主要方式として (フォールバックなしで) 使用することもできます。

## 特権 EXEC モードにアクセスするための認証の設定

ユーザが **enable** コマンドを入力したときに AAA サーバまたはローカル データベースでそれらのユーザを認証するようにセキュリティ アプライアンスを設定することができます。あるいは、ユーザは **login** コマンドを入力したときにローカル データベースで自動的に認証されます。この場合も、ローカル データベース内のユーザ レベルに応じて特権 EXEC モードにアクセスします。

ここでは、次の項目について説明します。

- [enable コマンドの認証の設定 \(P.33-7\)](#)
- [login コマンドによるユーザの認証 \(P.33-8\)](#)

### enable コマンドの認証の設定

ユーザが **enable** コマンドを入力したときに認証されるようにセキュリティ アプライアンスを設定できます。**enable** コマンドを認証しない場合は、**enable** を入力したときに、セキュリティ アプライアンスがシステム イネーブルパスワード (**enable password** コマンドで設定) の入力を求めるプロンプトを表示します。この場合、特定のユーザとしてログインする必要はありません。**enable** コマンドに認証を適用すると、ユーザ名が保持されます。この機能は、ユーザが入力できるコマンドを判別するためにユーザ名が重要な役割を果たすコマンド認可を実行する場合に特に役立ちます。

**enable** コマンドを入力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 enable console {LOCAL | server_group [LOCAL]}
```

ユーザ名とパスワードの入力を求めるプロンプトがユーザに対して表示されます。

認証に TACACS+ または RADIUS サーバグループを使用する場合は、AAA サーバが使用できないときにローカル データベースをフォールバック方式として使用するようにセキュリティ アプライアンスを設定できます。サーバグループ名の後ろに **LOCAL** を指定します (**LOCAL** は大文字と小文字を区別します)。セキュリティ アプライアンスは、どちらの方式を使用しているかを示すプロンプトを表示しないため、ローカル データベースと AAA サーバで同じユーザ名とパスワードを使用することをお勧めします。

**LOCAL** だけを入力して、ローカル データベースを認証の主要方式として (フォールバックなしで) 使用することもできます。

## login コマンドによるユーザの認証

ユーザ EXEC モードから、**login** コマンドを使用してローカル データベース内のユーザ名でログインすることができます。

この機能を使用すると、ユーザは独自のユーザ名とパスワードでログインして特権 EXEC モードにアクセスすることができるので、システム イネーブル パスワードを全員に提供する必要がなくなります。ユーザがログインしたときに特権 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、ユーザ特権レベルを 2（デフォルト）～ 15 に設定します。ローカル コマンド認可を設定した場合、ユーザはその特権レベルまたはそれ以下のレベルに割り当てられたコマンドだけを入力できます。詳細については、[P.33-9](#) の「[ローカル コマンド認可の設定](#)」を参照してください。



### 注意

CLI へのアクセス権を取得できるユーザを特権 EXEC モードに入れられないようにするには、そのユーザをローカル データベースに追加する際にコマンド認可を設定する必要があります。コマンド認可がない場合、ユーザは、特権レベルが 2 以上（デフォルトは 2）であれば、CLI で独自のパスワードを使用して特権 EXEC モード（およびすべてのコマンド）にアクセスすることができます。あるいは、RADIUS または TACACS+ 認証を使用するか、またはすべてのローカル ユーザをレベル 1 に設定することにより、誰がシステム イネーブル パスワードで特権 EXEC モードにアクセスできるかを制御できます。

ローカル データベースからユーザとしてログインするには、次のコマンドを入力します。

```
hostname> login
```

セキュリティ アプライアンスにより、ユーザ名とパスワードの入力を求めるプロンプトが表示されます。パスワードを入力すると、セキュリティ アプライアンスにより、ユーザはローカル データベースで指定されている特権レベルに置かれます。

## コマンド認可の設定

デフォルトでは、ログイン時に、最小限のコマンドだけが提供されるユーザ EXEC モードにアクセスできます。**enable** コマンド（またはローカル データベースを使用する場合は **login** コマンド）を入力すると、特権 EXEC モードおよびコンフィギュレーション コマンドなどの拡張コマンドにアクセスできます。コマンドへのアクセスを制御する場合は、セキュリティ アプライアンスでコマンド認可を設定し、ユーザが使用できるコマンドを決定することができます。

ここでは、次の項目について説明します。

- [コマンド認可の概要 \(P.33-9\)](#)
- [ローカル コマンド認可の設定 \(P.33-9\)](#)
- [TACACS+ コマンド認可の設定 \(P.33-12\)](#)

## コマンド認可の概要

次の 2 つのコマンド認可方法のいずれかを使用します。

- ローカル データベース：セキュリティ アプライアンスでコマンド特権レベルを設定します。ローカル ユーザが **enable** コマンドで認証（または **login** コマンドでログイン）すると、セキュリティ アプライアンスにより、そのユーザはローカル データベースで定義されている特権レベルに置かれます。その後、ユーザはそのユーザの特権レベルおよびそれ以下のレベルのコマンドにアクセスできます。



(注)

ローカル データベース内のユーザが存在しない場合、および CLI 認証やイネーブル認証がない場合でも、ローカル コマンド認可は使用できます。代わりに、**enable** コマンドを入力するときにシステム イネーブルパスワードを入力すると、セキュリティ アプライアンスによってレベル 15 に置かれます。次に、すべてのレベルのイネーブルパスワードを作成します。これにより、**enable n** (2 ~ 15) を入力したときに、セキュリティ アプライアンスによってレベル *n* に置かれるようになります。これらのレベルは、ローカル コマンド認可をオンにするまで使用されません（後述の「[ローカル コマンド認可の設定](#)」を参照してください）。（**enable** の詳細については、『Cisco Security Appliance Command Reference』を参照してください）

- TACACS+ サーバ：TACACS+ サーバで、ユーザまたはグループが CLI アクセスの認証後に使用できるコマンドを設定します。CLI でユーザが入力するコマンドはすべて TACACS+ サーバでチェックされます。

## ローカル コマンド認可の設定

ローカル コマンド認可では、各ユーザが特権レベルに置かれます。各ユーザは、自分の特権レベルまたはそれ以下のレベルのコマンドを入力できます。セキュリティ アプライアンスで、コマンドを 16 の特権レベル (0 ~ 15) のいずれかに割り当てることができます。デフォルトでは、各コマンドは特権レベル 0 または 15 に割り当てられます。

ここでは、次の項目について説明します。

- [ローカル コマンド認可の前提条件 \(P.33-9\)](#)
- [デフォルトのコマンド特権レベル \(P.33-10\)](#)
- [コマンドへの特権レベルの割り当てと認可のイネーブル化 \(P.33-10\)](#)
- [コマンド特権レベルの表示 \(P.33-12\)](#)

## ローカル コマンド認可の前提条件

コマンド認可コンフィギュレーションの一部として、次のタスクを実行します。

- enable** 認証を設定します (P.33-7 の「[特権 EXEC モードにアクセスするための認証の設定](#)」を参照してください)。

あるいは、設定を必要としない **login** コマンド（これは、認証のある **enable** コマンドと同じです）を使用することもできます。このオプションはイネーブル認証ほど安全ではないので、お勧めしません。

CLI 認証を使用することもできますが、必須ではありません。

- ローカル データベース内の各ユーザを特権レベル 0 ~ 15 で設定します。



## デフォルトのコマンド特権レベル

デフォルトでは、次のコマンドが特権レベル 0 に割り当てられます。その他のコマンドはすべてレベル 15 です。

- **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**

設定モード コマンドを 15 より低いレベルに移動する場合は、**configure** コマンドも同じレベルに移動してください。このようにしないと、ユーザはコンフィギュレーション モードに入ることができません。

すべての特権レベルを表示する方法は、[P.33-12 の「コマンド特権レベルの表示」](#)を参照してください。

## コマンドへの特権レベルの割り当てと認可のイネーブル化

コマンドを新しい特権レベルに割り当て、認可をイネーブル化するには、次の手順を実行します。

**ステップ 1** 特権レベルにコマンドを割り当てるには、次のコマンドを入力します。

```
hostname(config)# privilege [show | clear | cmd] level level [mode {enable | cmd}]  
command command
```

再割り当てする各コマンドに対してこのコマンドを繰り返します。

このコマンド内のオプションについては、次の情報を参照してください。

- **show | clear | cmd** : これらのオプション キーワードを使用すると、コマンドの show、clear、または configure 形式に対してのみ特権を設定できます。コマンドの configure 形式は、通常、未修正コマンド (**show** または **clear** プレフィックスなしで) または **no** 形式として、コンフィギュレーションの変更を引き起こす形式です。これらのキーワードのいずれかを使用しない場合は、コマンドのすべての形式が影響を受けます。
- **level level** : 0 ~ 15 のレベル。
- **mode {enable | configure}** : ユーザ EXEC/ 特権 EXEC モードおよびコンフィギュレーション モードでコマンドを入力することができ、そのコマンドが各モードで異なるアクションを実行する場合は、それらのモードの特権レベルを個別に設定することができます。
  - **enable** : ユーザ EXEC モードと特権 EXEC モードの両方を指定します。
  - **configure** : **configure terminal** コマンドを使用してアクセスされるコンフィギュレーション モードを指定します。



- **command command** : 設定しているコマンド。設定できるのは、**main** コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定することはできませんが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルを別個に設定することはできません。

また、サブコマンドの特権レベルをメイン コマンドと別に設定することもできません。たとえば、**context** コマンドを設定することはできませんが、**context** コマンドから設定を継承する **allocate-interface** コマンドを設定することはできません。

**ステップ 2** ローカル コマンド認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(config)# aaa authorization command LOCAL
```

コマンド特権レベルを設定しても、このコマンドでコマンド認可をイネーブルにしない限り、コマンド認可は実行されません。

たとえば、**filter** コマンドには次の形式があります。

- **filter** (**configure** オプションで表されます)
- **show running-config filter**
- **clear configure filter**

特権レベルを形式ごとに個別に設定することができます。または、このオプションを省略してすべての形式に同じ特権レベルを設定することもできます。たとえば、次のように、各形式を個別に設定します。

```
hostname(config)# privilege show level 5 command filter  
hostname(config)# privilege clear level 10 command filter  
hostname(config)# privilege cmd level 10 command filter
```

または、すべての **filter** コマンドを同じレベルに設定することもできます。

```
hostname(config)# privilege level 5 command filter
```

**show privilege** コマンドは、形式を分けて表示します。

次の例では、**mode** キーワードの使用方法を示します。**enable** コマンドはユーザ EXEC モードから入力する必要がありますが、コンフィギュレーション モードでアクセスできる **enable password** コマンドには最も高い特権レベルが必要です。

```
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
```

次の例では、**mode** キーワードを使用する追加コマンドである **configure** コマンドを示します。

```
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)

この最後の行は、**configure terminal** コマンドに対するものです。

## コマンド特権レベルの表示

次のコマンドを使用すると、コマンドの特権レベルを表示できます。

- すべて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 all privilege all
```

- 特定の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 privilege command command
```

たとえば、**show running-config all privilege all** コマンドの場合、システムは特権レベルに対する各 CLI コマンドの現在の割り当てを表示します。次に、このコマンドの出力例を示します。

```
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
....
```

次のコマンドを使用すると、特権レベル 10 のコマンド割り当てが表示されます。

```
hostname(config)# show running-config privilege level 10
privilege show level 10 command aaa
```

次のコマンドを使用すると、**access-list** コマンドのコマンド割り当てが表示されます。

```
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+ コマンド認可の設定

TACACS+ コマンド認可をイネーブルにし、ユーザが CLI でコマンドを入力すると、セキュリティ アプライアンスはそのコマンドとユーザ名を TACACS+ サーバに送信し、コマンドが認可されているかどうかを判別します。

TACACS+ サーバでコマンド認可を設定するときは、設定どおりに動作することを確認するまで、コマンド認可機能の設定を保存しないでください。誤ってロックアウトされた場合は、通常、セキュリティ アプライアンスを再起動することによってアクセスを回復できます。それでもロックアウトされたままの場合は、[P.33-17 の「ロックアウトからの回復」](#)を参照してください。

使用している TACACS+ システムが完全に安定していて、高い信頼性があることを確認してください。通常、必要なレベルの信頼性を得るには、完全冗長の TACACS+ サーバシステムと、セキュリティ アプライアンスに対する完全な冗長接続が確立されていることが必要です。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続されたサーバと、インターフェイス 2 に接続された別のサーバを組み込みます。また、TACACS+ サーバを使用できない場合は、ローカル コマンド認可をフォールバック方式として設定できます。この場合は、P.33-8 の「コマンド認可の設定」に従ってローカル ユーザとコマンド特権レベルを設定する必要があります。

ここでは、次の項目について説明します。

- TACACS+ コマンド認可の前提条件 (P.33-13)
- TACACS+ サーバでのコマンドの設定 (P.33-13)
- TACACS+ コマンド認可のイネーブル化 (P.33-16)

### TACACS+ コマンド認可の前提条件

コマンド認可コンフィギュレーションの一部として、次のタスクを実行します。

- CLI 認証を設定する (P.33-9 の「ローカル コマンド認可の設定」を参照)。
- **enable** 認証を設定する (P.33-7 の「特権 EXEC モードにアクセスするための認証の設定」を参照)。

### TACACS+ サーバでのコマンドの設定

グループまたは個々のユーザの共有プロファイル コンポーネントとしての Cisco Secure Access Control サーバ (ACS) TACACS+ サーバでコマンドを設定できます。サードパーティの TACACS+ サーバの場合は、コマンド認可サポートの詳細については、ご使用のサーバのマニュアルを参照してください。

Cisco Secure ACS バージョン 3.1 でコマンドを設定する場合は、次のガイドラインを参照してください。

- セキュリティ アプライアンスは、「シェル」コマンドとして認可するコマンドを送信し、TACACS+ サーバでシェル コマンドとしてコマンドを設定します。



(注)

Cisco Secure ACS には、「pix-shell」と呼ばれるコマンド タイプが含まれている場合があります。このタイプはセキュリティ アプライアンス コマンド認可に使用しないでください。

- コマンドの最初のワードは、メイン コマンドと見なされます。その他のワードはすべて引数と見なされます。これは、**permit** または **deny** の後に置く必要があります。  
たとえば、**show running-configuration aaa-server** コマンドを許可するには、**show running-configuration** をコマンド ボックスに追加し、**permit aaa-server** を引数ボックスに入力します。
- **Permit Unmatched Args** チェックボックスを選択することによって、明示的に拒否していないコマンドのすべての引数を許可することができます。  
たとえば、特定の **show** コマンドを設定するだけで、すべての **show** コマンドが許可されます。CLI の使用法を示す ? や省略形など、コマンドの変形をすべて予想する必要がなくなるので、この方法を使用することをお勧めします (図 33-1 を参照)。

図 33-1 関連するすべてのコマンドの許可

- **enable** や **help** など、単一ワードのコマンドについては、そのコマンドに引数がない場合でも、一致しない引数を許可する必要があります（図 33-2 を参照）。

図 33-2 単一ワードのコマンドの許可

- 引数を拒否するには、その引数の前に **deny** を入力します。  
たとえば、**enable** を許可し、**enable password** を許可しない場合は、コマンド ボックスに **enable** と入力し、引数ボックスに **deny password** と入力します。**enable** だけが許可されるように、Permit Unmatched Args チェックボックスを選択してください（図 33-3 を参照）。

図 33-3 引数の拒否

- コマンドラインでコマンドを省略形で入力した場合、セキュリティ アプライアンスはプレフィックスとメイン コマンドを完全なテキストに展開しますが、その他の引数は入力したとおりに TACACS+ サーバに送信します。

たとえば、**sh log** と入力すると、セキュリティ アプライアンスは完全なコマンド **show logging** を TACACS+ サーバに送信します。一方、**sh log mess** と入力すると、セキュリティ アプライアンスは展開されたコマンド **show logging message** ではなく、**show logging mess** を TACACS+ サーバに送信します。省略形を予想して同じ引数に複数のスペルを設定することができます (図 33-4 を参照)。

図 33-4 省略形の指定

- すべてのユーザに対して次の基本コマンドを許可することをお勧めします。
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**
  - **logout**
  - **pager**
  - **show pager**

- clear pager
- quit
- show version

## TACACS+ コマンド認可のイネーブル化

TACACS+ コマンド認可をイネーブルにする前に、TACACS+ サーバで定義されたユーザとしてセキュリティ アプライアンスにログインしていること、およびセキュリティ アプライアンスの設定を続けるために必要なコマンド認可があることを確認してください。たとえば、すべてのコマンドが認可された管理ユーザとしてログインする必要があります。このようにしないと、意図せずロックアウトされる可能性があります。

TACACS+ サーバを使用したコマンド認可を実行するには、次のコマンドを入力します。

```
hostname(config)# aaa authorization command tacacs+_server_group [LOCAL]
```

TACACS+ サーバを使用できない場合は、ローカル データベースをフォールバック方式として使用するようにセキュリティ アプライアンスを設定できます。フォールバックをイネーブルにするには、サーバ グループ名の後ろに **LOCAL** を指定します (**LOCAL** は大文字と小文字を区別します)。セキュリティ アプライアンスは、どちらの方式を使用しているかを示すプロンプトを表示しないため、ローカル データベースと TACACS+ サーバで同じユーザ名とパスワードを使用することをお勧めします。必ずローカル データベースのユーザ ([P.33-8 の「コマンド認可の設定」](#)を参照) とコマンド特権レベル ([P.33-9 の「ローカル コマンド認可の設定」](#)を参照) を設定してください。

## 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によって発行されたコマンドに対して、TACACS+ サーバ アカウンティング記録を送信するようにセキュリティ アプライアンスを設定することができます。指定する特権レベルを最小にすると、セキュリティ アプライアンスがアカウンティングするコマンドを制限できます。セキュリティ アプライアンスは、最初の特権レベル未満のコマンドはアカウンティングしません。

コマンドの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、最小の特権レベルで、*server-tag* は、セキュリティ アプライアンスがコマンド アカウンティング メッセージを送信する TACACS+ サーバ グループの名前です。TACACS+ サーバ グループはすでに設定済みである必要があります。AAA サーバ グループを設定する方法の詳細については、[P.10-17 の「AAA サーバ グループおよびサーバの識別」](#)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
```

次の **show curpriv** コマンドの出力例を参照してください。各フィールドの説明については、下記を参照してください。

```
hostname# show curpriv
Username : admin
Current privilege level : 15
Current Mode/s : P_PRIV
```

表 33-1 は、**show curpriv** コマンドの出力について説明しています。

**表 33-1 show curpriv の表示の説明**

| フィールド                   | 説明                                                                                                                                                                           |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username                | ユーザ名。デフォルト ユーザとしてログインすると、名前は enable_1 (ユーザ EXEC) または enable_15 (特権 EXEC) になります。                                                                                              |
| Current privilege level | 0 ～ 15 のレベル。ローカル コマンド認可を設定してコマンドを中間特権レベルに割り当てない限り、使用されるレベルはレベル 0 と 15 だけです。                                                                                                  |
| Current Mode/s          | アクセス モードを表示します。 <ul style="list-style-type: none"><li>• P_UNPR：ユーザ EXEC モード (レベル 0 と 1)</li><li>• P_PRIV：特権 EXEC モード (レベル 2 ～ 15)</li><li>• P_CONF：コンフィギュレーション モード</li></ul> |

## ロックアウトからの回復

状況によっては、コマンド認可や CLI 認証をオンにすると、セキュリティ アプライアンス CLI からロックアウトされる場合があります。通常は、セキュリティ アプライアンスを再起動することによってアクセスを回復できます。ただし、すでにコンフィギュレーションを保存した場合は、ロックアウトされたままになる可能性があります。表 33-2 に、一般的なロックアウト条件と回復方法を示します。

表 33-2 CLI 認証およびコマンド認可のロックアウト シナリオ

| 機能                                                | ロックアウト条件                             | 説明                                              | 対応策：シングルモード                                                                                                                                              | 対応策：マルチモード                                                                                                                                                                                                                                                        |
|---------------------------------------------------|--------------------------------------|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ローカル CLI 認証                                       | ローカル データベース内にユーザが存在しない。              | ローカル データベース内にユーザが存在しない場合は、ログインできず、ユーザの追加もできません。 | ログインし、パスワードと <b>aaa</b> コマンドをリセットします。                                                                                                                    | スイッチからセキュリティ アプライアンスへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザを追加することができます。                                                                                                                                                                                       |
| TACACS+ コマンド認可<br>TACACS+ CLI 認証<br>RADIUS CLI 認証 | サーバがダウンしているか到達不能で、フォールバック方式を設定していない。 | サーバが到達不能である場合は、ログインもコマンドの入力もできません。              | <ol style="list-style-type: none"> <li>1. ログインし、パスワードと AAA コマンドをリセットします。</li> <li>2. サーバがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。</li> </ol> | <ol style="list-style-type: none"> <li>1. セキュリティ アプライアンスでネットワーク コンフィギュレーションが正しくないためサーバが到達不能である場合は、スイッチからセキュリティ アプライアンスへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてネットワークを再設定することができます。</li> <li>2. サーバがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。</li> </ol> |
| TACACS+ コマンド認可                                    | 十分な特権のないユーザまたは存在しないユーザとしてログインした。     | コマンド認可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できません。        | <p>TACACS+ サーバのユーザ アカウントを修正します。</p> <p>TACACS+ サーバへのアクセス権がなく、セキュリティ アプライアンスをすぐに設定する必要がある場合は、メンテナンス パーティションにログインして、パスワードと <b>aaa</b> コマンドをリセットします。</p>    | スイッチからセキュリティ アプライアンスへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてコンフィギュレーションの変更を完了することができます。また、TACACS+ コンフィギュレーションを修正するまでコマンド認可をディセーブルにすることもできます。                                                                                                                       |
| ローカル コマンド認可                                       | 十分な特権のないユーザとしてログインしている。              | コマンド認可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できません。        | ログインし、パスワードと <b>aaa</b> コマンドをリセットします。                                                                                                                    | スイッチからセキュリティ アプライアンスへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザ レベルを変更することができます。                                                                                                                                                                                   |



## ログイン バナーの設定

ユーザがセキュリティ アプライアンスに接続し、ユーザがログインする前または特権 EXEC モードに入る前に表示されるメッセージを設定できます。

ログイン バナーを設定するには、システム実行スペース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 {exec | login | motd} text
```

ユーザが最初に接続したとき（「今日のお知らせ」（**motd**））、ユーザがログインしたとき（**login**）、ユーザが特権 EXEC モードにアクセスしたとき（**exec**）のいずれかに表示するバナーを追加します。ユーザがセキュリティ アプライアンスに接続すると、まず「今日のお知らせ」バナーが表示され、その後にログイン バナーとプロンプトが表示されます。ユーザがセキュリティ アプライアンスに正常にログインすると、exec バナーが表示されます。

バナー テキストには、スペースは許可されますが、タブは CLI を使用して入力できません。セキュリティ アプライアンスのホスト名またはドメイン名は、**\$(hostname)** スtringと **\$(domain)** スtringを組み込むことによって動的に追加できます。システム コンフィギュレーションでバナーを設定する場合は、コンテキスト コンフィギュレーションで **\$(system)** スtring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。

複数の行を追加する場合は、各行の前に **banner** コマンドを置きます。

たとえば、「今日のお知らせ」バナーを追加するには、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.
```





# ソフトウェア、ライセンス、および コンフィギュレーションの管理

この章では、セキュリティ アプライアンスのソフトウェア、ライセンス、およびコンフィギュレーションの管理について説明します。この章では、次の項目について説明します。

- [ライセンスの管理 \(P.34-2\)](#)
- [フラッシュ メモリ内のファイルの表示 \(P.34-3\)](#)
- [フラッシュ メモリへのソフトウェアまたはコンフィギュレーションのダウンロード \(P.34-4\)](#)
- [ブートするアプリケーション イメージと ASDM イメージの設定 \(P.34-6\)](#)
- [スタートアップ コンフィギュレーションとしてブートするファイルの設定 \(P.34-7\)](#)
- [フェールオーバー ペアのゼロ ダウンタイム アップグレードの実行 \(P.34-8\)](#)
- [コンフィギュレーション ファイルのバックアップ \(P.34-11\)](#)
- [Auto Update サポートの設定 \(P.34-13\)](#)

## ライセンスの管理

ソフトウェアをインストールすると、元のイメージから既存のアクティベーション キーが抽出され、セキュリティ アプライアンス ファイル システムのファイル内に保存されます。

### アクティベーション キーの取得

アクティベーション キーを取得するには、シスコの代理店から購入できる Product Authorization Key が必要になります。Product Authorization Key を入手したら Web 上でキーを登録し、次の手順を実行してアクティベーション キーを取得します。

**ステップ 1** 次のコマンドを入力して、セキュリティ アプライアンスのシリアル番号を取得します。

```
hostname> show version | include Number
```

パイプ文字 (|) をコマンドの一部として入力します。

**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 は大文字と小文字を区別します)。

Cisco.com の登録ユーザの場合は、次の Web サイトを使用します。

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

Cisco.com の登録ユーザ以外の場合は、次の Web サイトを使用します。

```
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。

- Product Authorization Key
- セキュリティ アプライアンスのシリアル番号
- 電子メール アドレス

アクティベーション キーが自動的に生成され、指定した電子メール アドレスに送信されます。

### 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
```

キーは、4 つまたは 5 つのエレメントからなる 16 進文字列です。各エレメントは 1 つのスペースで区切られます。たとえば、正しい形式のキーは次のようになります。

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

先頭部分の 0x 指定子は省略できます。値は、すべて 16 進数であると見なされます。

すでにマルチコンテキスト モードに入っている場合は、システム実行スペースにこのコマンドを入力します。

アクティベーション キーを入力する前に、フラッシュ メモリ内のイメージと実行イメージが同一であることを確認します。これは、セキュリティ アプライアンスをリブートしてからアクティベーション キーを入力することで確認できます。

**(注)**

アクティベーション キーは、コンフィギュレーション ファイルには保存されません。キーはデバイスのシリアル番号に結び付けられます。

実行イメージで変更内容を有効にするには、新しいアクティベーション キーを入力した後でセキュリティ アプライアンスをリブートする必要があります。

次の例は、セキュリティ アプライアンスでアクティベーション キーを変更する方法を示しています。

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

## フラッシュ メモリ内のファイルの表示

フラッシュ メモリ内のファイルを表示して、そのファイルに関する情報を参照できます。

- 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 [flash: | disk0: | disk1:]
```

**flash:** キーワードは、PIX 500 シリーズ セキュリティ アプライアンスの内部フラッシュ メモリを表します。ASA 5500 シリーズ 適応型 セキュリティ アプライアンスの内部フラッシュ メモリの場合は、**flash:** または **disk0:** を使用できます。**disk1:** キーワードは、ASA の外部フラッシュ メモリを表します。内部フラッシュ メモリがデフォルトです。

次の例を参考にしてください。

```
hostname# dir
```

```
Directory of disk0:/
500  -rw- 4958208    22:56:20 Nov 29 2004  cdisk.bin
2513 -rw-  4634      19:32:48 Sep 17 2004  first-backup
2788 -rw-  21601    20:51:46 Nov 23 2004  backup.cfg
2927 -rw- 8670632    20:42:48 Dec 08 2004  asdmfile.bin
```

- 特定のファイルに関する拡張情報を表示するには、次のコマンドを入力します。

```
hostname# show file information [path/] filename
```

デフォルト パスは、内部フラッシュ メモリ (flash:/ または disk0:/) のルート ディレクトリです。

次の例を参考にしてください。

```
hostname# show file information cdisk.bin
```

```
disk0:/cdisk.bin:
  type is image (XXX) []
  file size is 4976640 bytes version 7.0(1)
```

示されているファイルサイズは例にすぎません。

## フラッシュメモリへのソフトウェアまたはコンフィギュレーションのダウンロード

アプリケーション イメージ、ASDM イメージ、コンフィギュレーション ファイル、および他のファイルを TFTP、FTP、HTTP、または HTTPS サーバから内部フラッシュメモリに、あるいは ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合は外部フラッシュメモリに、ダウンロードできます。

ここでは、次の項目について説明します。

- 特定の場所へのファイルのダウンロード (P.34-4)
- スタートアップ コンフィギュレーションまたは実行コンフィギュレーションへのファイルのダウンロード (P.34-5)

### 特定の場所へのファイルのダウンロード

この項では、アプリケーション イメージ、ASDM ソフトウェア、コンフィギュレーション ファイル、またはフラッシュメモリへのダウンロードが必要な他のファイルのダウンロード方法について説明します。ファイルを実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにダウンロードする場合は、P.34-5 の「スタートアップ コンフィギュレーションまたは実行コンフィギュレーションへのファイルのダウンロード」を参照してください。

Cisco SSL VPN クライアントのインストールの詳細については、P.31-2 の「SVC ソフトウェアのインストール」を参照してください。セキュリティ アプライアンスへの Cisco Secure Desktop のインストールについては、『Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators』を参照してください。

複数のイメージがインストールされている場合、または外部フラッシュメモリにイメージがインストールされている場合に特定のアプリケーション イメージまたは ASDM イメージを使用するようにセキュリティ アプライアンスを設定する場合は、P.34-6 の「ブートするアプリケーション イメージと ASDM イメージの設定」を参照してください。

特定の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使用するようにセキュリティ アプライアンスを設定する場合は、P.34-7 の「スタートアップ コンフィギュレーションとしてブートするファイルの設定」を参照してください。

マルチコンテキスト モードの場合は、システム実行スペース内にいる必要があります。

ファイルをフラッシュメモリにダウンロードするには、各ダウンロード サーバタイプ用の次のコマンドを参照してください。

- 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:/ | disk0:/ | disk1:/}[/path]/filename
```

**flash:/** キーワードは、PIX 500 シリーズセキュリティ アプライアンスの内部フラッシュメモリを表します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの内部フラッシュメモリの場合は、**flash:/** または **disk0:/** を使用できます。**disk1:/** キーワードは、ASA の外部フラッシュメモリを表します。

- 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:/ | disk0:/ | disk1:/}[/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 {flash:/ | disk0:/ | disk1:/} [path/] filename
```

- セキュア コピーを使用するには、まず 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
```

その後、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@fwsn_address
```

-v は冗長を表します。-pw が指定されていない場合は、パスワードの入力を求めるプロンプトが表示されます。

## スタートアップ コンフィギュレーションまたは実行コンフィギュレーションへのファイルのダウンロード

TFTP、FTP、または HTTP(S) サーバから、またはフラッシュ メモリから、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにテキスト ファイルをダウンロードできます。

スタートアップ コンフィギュレーションまたは実行コンフィギュレーションにファイルをコピーするには、適切なダウンロード サーバに対して次のコマンドのいずれかを入力します。



(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には、2 つのコンフィギュレーションをマージします。マージは、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドを追加します。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生すること、予期できない結果が生じることもあります。

- 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 {startup-config | 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 {startup-config | running-config}
```

- 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 {flash:/ | disk0:/ | disk1:/} [path/] filename {startup-config | running-config}
```

たとえば、TFTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
hostname# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

FTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
hostname# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg startup-config
```

HTTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
hostname# copy http://209.165.200.228/configs/startup.cfg startup-config
```

## ブートするアプリケーションイメージと ASDM イメージの設定

デフォルトでは、セキュリティ アプライアンスは内部フラッシュ メモリ内で見つけた最初のアプリケーション イメージをブートします。また、内部フラッシュ メモリ内で見つけた最初の ASDM イメージをブートするか、内部フラッシュ メモリ内にない場合は外部フラッシュ メモリ内の ASDM イメージをブートします。複数のイメージがある場合は、ブートするイメージを指定する必要があります。ASDM イメージの場合は、ブートするイメージを指定しないと、インストールされているイメージが1つしかなくても、セキュリティ アプライアンスは **asdm image** コマンドを実行コンフィギュレーションに挿入します。Auto Update（設定されている場合）の問題を避けるため、また起動時ごとのイメージ検索を回避するため、ブートする ASDM イメージをスタートアップ コンフィギュレーションで指定する必要があります。

- ブートするアプリケーション イメージを設定するには、次のコマンドを入力します。

```
hostname(config)# boot system url
```

ここで、*url* は次のいずれかです。

— **{flash:/ | disk0:/ | disk1:/}**[*path/*]*filename*

**flash:/** キーワードは、PIX 500 シリーズ セキュリティ アプライアンスの内部フラッシュ メモリを表します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの内部フラッシュ メモリの場合は、**flash:/** または **disk0:/** を使用できます。**disk1:/** キーワードは、ASA の外部フラッシュ メモリを表します。

— **tftp://**[*user[:password]*]**@**[*server[:port]*]**/**[*path/*]*filename*

このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスでのみサポートされています。

最大 4 つの **boot system** コマンド エントリを入力して、ブートする別々のイメージを順番に指定することができます。セキュリティ アプライアンスは、最初に見つけたイメージをブートします。設定できる **boot system tftp:** コマンドは 1 つだけです。これは、最初に設定する必要があります。

- ブートする ASDM イメージを設定するには、次のコマンドを入力します。

```
hostname(config)# asdm image {flash:/ | disk0:/ | disk1:/}[path/]filename
```



## スタートアップ コンフィギュレーションとしてブートするファイルの設定

デフォルトでは、セキュリティ アプライアンスは、隠しファイルであるスタートアップ コンフィギュレーションからブートします。あるいは、次のコマンドを入力して、任意の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設定することもできます。

```
hostname(config)# boot config {flash:/ | disk0:/ | disk1:/}[path/]filename
```

**flash:/** キーワードは、PIX 500 シリーズ セキュリティ アプライアンスの内部フラッシュ メモリを表します。ASA 5500 シリーズ 適応型 セキュリティ アプライアンスの内部フラッシュ メモリの場合は、**flash:/** または **disk0:/** を使用できます。**disk1:/** キーワードは、ASA の外部フラッシュ メモリを表します。

## フェールオーバー ペアのゼロ ダウンタイム アップグレードの実行

フェールオーバー コンフィギュレーション内の2つの装置は、同一のメジャー（最初の番号）およびマイナー（2番目の番号）ソフトウェア バージョンを持っている必要があります。ただし、アップグレード処理中に装置のバージョン パリティを維持する必要はなく、各装置でそれぞれ異なるバージョンのソフトウェアを実行しても、フェールオーバー サポートを維持することができます。互換性と安定性を長期間確保するためには、両装置をできるだけ早期に同じバージョンにアップグレードすることをお勧めします。

表 34-1 に、フェールオーバー ペアに対してゼロダウンタイム アップグレードをサポートするシナリオを示します。

**表 34-1 ゼロダウンタイム アップグレード サポート**

| アップグレードの種類  | サポートの内容                                                                                                                                                                                        |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| メンテナンス リリース | 任意のメンテナンス リリースから、マイナー リリースの範囲で他のメンテナンス リリースにアップグレードできます。<br><br>たとえば、7.0(1) から 7.0(4) の範囲であれば、最初にメンテナンス リリースをインストールしなくてもアップグレードが可能です。                                                          |
| マイナー リリース   | マイナー リリースから次のマイナー リリースにアップグレードできます。途中のマイナー リリースをスキップしてアップグレードすることはできません。<br><br>たとえば、7.0 からは 7.1 にアップグレードできます。ゼロダウンタイム アップグレードでは 7.0 から 7.2 への直接のアップグレードはサポートされていません。まず 7.1 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   | 直前のバージョンの最終マイナー 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。<br><br>たとえば、7.x リリースにおける最終のマイナー バージョンが 7.9 であると想定される場合、7.9 から 8.0 にアップグレードできます。                                                                 |

フェールオーバー ペアに対するソフトウェアのアップグレードの詳細については、次の項目を参照してください。

- [Active/Standby フェールオーバー コンフィギュレーションのアップグレード \(P.34-8\)](#)
- [Active/Active フェールオーバー コンフィギュレーションのアップグレード \(P.34-9\)](#)

### Active/Standby フェールオーバー コンフィギュレーションのアップグレード

Active/Standby フェールオーバー コンフィギュレーションの2つの装置をアップグレードするには、次の手順を実行します。

**ステップ 1** 両方の装置に新規ソフトウェアをダウンロードし、ロードする新規イメージを **boot system** コマンド（[P.34-6](#) の「ブートするアプリケーション イメージと ASDM イメージの設定」を参照）で指定します。

**ステップ 2** アクティブ装置に次のコマンドを入力して、スタンバイ装置をリロードして新規イメージをブートします。

```
active# failover reload-standby
```

- ステップ 3** スタンバイ装置がリロードを終了し、Standby Ready 状態になったら、アクティブ装置で次のコマンドを入力して、アクティブ装置をスタンバイ装置に強制的にフェールオーバーします。



**(注)** `show failover` コマンドを使用して、スタンバイ装置が Standby Ready 状態にあることを確認します。

```
active# no failover active
```

- ステップ 4** 次のコマンドを入力して、前のアクティブ装置（現在の新規スタンバイ装置）をリロードします。

```
newstandby# reload
```

- ステップ 5** 新規スタンバイ装置がリロードを終了し、この装置が Standby Ready 状態になったら、次のコマンドを入力して元のアクティブ装置をアクティブな状態に戻します。

```
newstandby# failover active
```

## Active/Active フェールオーバー コンフィギュレーションのアップグレード

Active/Active フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

- ステップ 1** 両方の装置に新規ソフトウェアをダウンロードし、ロードする新規イメージを `boot system` コマンド（P.34-6 の「ブートするアプリケーション イメージと ASDM イメージの設定」を参照）で指定します。

- ステップ 2** プライマリ装置のシステム実行スペースで次のコマンドを入力して、プライマリ装置の両方のフェールオーバー グループをアクティブにします。

```
primary# failover active
```

- ステップ 3** プライマリ装置のシステム実行スペースで次のコマンドを入力して、セカンダリ装置をリロードして新規イメージをブートします。

```
primary# failover reload-standby
```

- ステップ 4** セカンダリ装置のリロードが終了し、その装置で両方のフェールオーバー グループが Standby Ready 状態になったら、プライマリ装置のシステム実行スペースで次のコマンドを実行して、セカンダリ装置で両方のフェールオーバー グループをアクティブにします。

**(注)**

**show failover** コマンドを使用して、両方のフェールオーバー グループがセカンダリ装置で Standby Ready 状態にあることを確認します。

```
primary# no failover active
```

**ステップ 5** 両方のフェールオーバー グループがプライマリ装置で Standby Ready 状態にあ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装置をリロードします。

```
primary# reload
```

**ステップ 6** 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る場合は、これらはプリエンプション遅延の経過後、指定された装置で自動的にアクティブになります。フェールオーバー グループを **preempt** コマンドで設定していない場合、**failover active group** コマンドを使用すると、これらのグループを指定された装置でアクティブな状態に戻すことができます。

## コンフィギュレーション ファイルのバックアップ

コンフィギュレーションをバックアップするには、次のいずれかの方法で行います。

- 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のシステム コンフィギュレーションのバックアップ (P.34-11)
- コンテキスト コンフィギュレーションのフラッシュ メモリへのバックアップ (P.34-11)
- コンテキスト内でのコンテキスト コンフィギュレーションのバックアップ (P.34-12)
- 端末の表示からのコンフィギュレーションのコピー (P.34-12)

### 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のシステム コンフィギュレーションのバックアップ

シングルコンテキスト モードで、またはマルチモードのシステム コンフィギュレーションから、スタートアップ コンフィギュレーションまたは実行コンフィギュレーションを外部サーバまたはローカルのフラッシュ メモリにコピーできます。

- 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
```

- ローカルのフラッシュ 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} {flash:/ | disk0:/ |
disk1:/} [path/] filename
```

宛先のディレクトリが存在することを確認してください。存在しない場合は、最初に、**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 コンフィギュレーションのフラッシュ メモリへのバックアップ

マルチコンテキスト モードで、システム実行スペースで次のコマンドのいずれかを入力して、ローカルのフラッシュ メモリにあるコンテキスト コンフィギュレーションをコピーします。

- 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
```

- ローカルのフラッシュ 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 {flash:/ | disk0:/ | disk1:/} [path/] filename {flash:/ | disk0:/ |
disk1:/} [path/] newfilename
```

宛先のディレクトリが存在することを確認してください。存在しない場合は、最初に、**mkdir** コマンドを使用してディレクトリを作成します。

## コンテキスト内でのコンテキスト コンフィギュレーションのバックアップ

マルチコンテキスト モードでは、コンテキスト内から次のバックアップを実行できます。

- (admin コンテキストに接続された) スタートアップ コンフィギュレーション サーバに実行コンフィギュレーションをコピーするには、次のコマンドを入力します。

```
hostname/contexta# copy running-config startup-config
```

- コンテキスト ネットワークに接続された TFTP サーバに実行コンフィギュレーションをコピーするには、次のコマンドを入力します。

```
hostname/contexta# copy running-config tftp://server[/path]/filename
```

## 端末の表示からのコンフィギュレーションのコピー

コンフィギュレーションを端末に表示するには、次のコマンドを入力します。

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

このコマンドの出力内容をコピーし、テキスト ファイルにコンフィギュレーションを貼り付けます。

## Auto Update サポートの設定

Auto Update は、Auto Update Server がコンフィギュレーションとソフトウェア イメージを多数のセキュリティ アプライアンスにダウンロードすることを許可し、中央からのセキュリティ アプライアンスの基本的なモニタリングを提供するプロトコル仕様です。セキュリティ アプライアンスは、ソフトウェア イメージおよびコンフィギュレーション ファイルへのアップデートのため、Auto Update Server を定期的にポーリングします。



(注)

Auto Update は、シングルコンテキスト モードでのみサポートされます。

ここでは、次の項目について説明します。

- [Auto Update Server との通信の設定 \(P.34-13\)](#)
- [Auto Update ステータスの表示 \(P.34-14\)](#)

### Auto Update Server との通信の設定

Auto Update を設定するには、次の手順を実行します。

**ステップ 1** AUS の URL を指定するには、次のコマンドを使用します。

```
hostname(config)# auto-update server url [source interface] [verify-certificate]
```

ここで、*url* には次のシンタックスがあります。

```
http[s]://[user:password@]server_ip[:port]/pathname
```

設定できるサーバは 1 つだけです。**https** を指定すると、SSL が使用されます。URL の *user* 引数と *password* 引数は、サーバにログインするときの基本認証に使用されます。**write terminal**、**show configuration**、または **show tech-support** コマンドを使用してコンフィギュレーションを表示した場合、ユーザとパスワードは「\*\*\*\*\*」に置換されます。

HTTP のデフォルト ポートは 80、HTTPS のデフォルト ポートは 443 です。

**source interface** 引数は、AUS に要求を送信するときに使用するインターフェイスを指定します。**management-access** コマンドで指定したインターフェイスと同じインターフェイスを指定すると、Auto Update 要求は管理アクセスに使用されるのと同じ IPSec VPN トンネルを通過します。

**verify-certificate** キーワードは、AUS によって戻される証明書を確認します。

**ステップ 2** (オプション) AUS と通信する際に送信するデバイス ID を識別するには、次のコマンドを入力します。

```
hostname(config)# auto-update device-id {hardware-serial | hostname | ipaddress | if-name} | mac-address [if-name] | string text}
```

使用する ID は、次のいずれかのパラメータによって決まります。

- **hardware-serial**：セキュリティ アプライアンスのシリアル番号を使用します。
- **hostname**：セキュリティ アプライアンス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い場合、AUS との通信に使用するインターフェイスの IP アドレスを使用します。

- **mac-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い場合、AUS との通信に使用するインターフェイスの MAC アドレスを使用します。
- **string**：指定されたテキスト識別子を使用します。空白や、`、`、`>`、`&`、`?` は使用できません。

**ステップ 3** (オプション) コンフィギュレーション、またはイメージの更新を要求するために AUS がポーリングする回数を指定するには、次のコマンドを入力します。

```
hostname(config)# auto-update poll-period poll-period [retry-count [retry-period]]
```

**poll-period** 引数は、更新を確認する間隔(分単位)を指定します。デフォルトは 720 分(12 時間)です。

**retry-count** 引数は、サーバへの最初の接続に失敗した場合に、再試行する回数を指定します。デフォルトは 0 です。

**retry-period** 引数は、リトライの間の待機時間(分単位)を指定します。デフォルトは 5 です。

**ステップ 4** (オプション) Auto Update Server に一定期間アクセスがなかった場合にトラフィックの通過を中断するには、次のコマンドを使用します。

```
hostname(config)# auto-update timeout period
```

ここで、**period** は 1 ～ 35791 の分単位のタイムアウト期間を指定します。デフォルトはタイムアウトなし (0) です。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスに最新のイメージとコンフィギュレーションがあることを確認するには、このコマンドを使用します。この状態は、システム ログ メッセージ 201008 で報告されます。

次の例では、セキュリティ アプライアンスが外部インターフェイスから証明書の検証付きで、IP アドレス 209.165.200.224、ポート番号 1742 で AUS をポーリングするように設定されています。

また、セキュリティ アプライアンスのホスト名をデバイス ID として使用するよう設定されています。ポーリング期間はデフォルトの 720 分から 600 分に減らされます。ポーリングが失敗した場合は、AUS への再接続を 3 分おきに 10 回試行します。

```
hostname(config)# auto-update server  
https://jcrichon: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
```

## Auto Update ステータスの表示

Auto Update のステータスを表示するには、次のコマンドを入力します。

```
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
```





# セキュリティ アプライアンスのモニタリング

この章では、セキュリティ アプライアンスのモニタリングの方法について説明します。次の項で構成されています。

- [システム ログ メッセージの使用 \(P.35-1\)](#)
- [SNMP の使用方法 \(P.35-1\)](#)

## システム ログ メッセージの使用

セキュリティ アプライアンスには、多数のシステム ログ メッセージがあります。ロギングを設定する方法、およびシステム ログ メッセージの説明を表示する方法については、『*Cisco Security Appliance Logging Configuration and System Log Messages*』を参照してください。

## SNMP の使用方法

この項では、SNMP を使用する方法について説明します。次の項目を取り上げます。

- [SNMP の概要 \(P.35-1\)](#)
- [SNMP のイネーブル化 \(P.35-3\)](#)

## SNMP の概要

セキュリティ アプライアンスは、SNMP V1 および V2c でのネットワーク モニタリングに対するサポートを提供します。セキュリティ アプライアンスはトラップと SNMP 読み取りアクセスをサポートしますが、SNMP 書き込みアクセスはサポートしません。

トラップ（イベント通知）を Network Management Station（NMS; ネットワーク管理ステーション）に送信するようにセキュリティ アプライアンスを設定することができます。また、NMS を使用してセキュリティ アプライアンスで MIB をブラウズすることもできます。MIB は定義の集合であり、セキュリティ アプライアンスは各定義に対応する値のデータベースを保持しています。MIB のブラウズは、NMS からの SNMP get 要求の発行を伴います。SNMP トラップを受信して MIB を参照（ブラウジング）するには、CiscoWorks for Windows またはその他の SNMP V1、MIB-II 互換ブラウザを使用してください。

表 35-1 は、セキュリティ アプライアンスでサポートされる MIB とトラップ、およびマルチモードの場合に各コンテキストでサポートされる MIB とトラップを示しています。次の Web サイトから Cisco MIB をダウンロードできます。

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

MIB をダウンロードした後、NMS 用にそれらをコンパイルします。

表 35-1 SNMP MIB とトラップのサポート

| MIB またはトラップのサポート                | 説明                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP コア トラップ                    | <p>セキュリティ アプライアンスは、次のコア SNMP トラップを送信します。</p> <ul style="list-style-type: none"> <li>authentication：NMS が正しいコミュニティ スtring で認証しなかったため、SNMP 要求は失敗します。</li> <li>linkup：インターフェイスが「up」状態に移行しました。</li> <li>linkdown：インターフェイスがダウンします（たとえば、<b>nameif</b> コマンドを削除した場合）。</li> <li>coldstart：セキュリティ アプライアンスがリロード後に動作しています。</li> </ul> |
| MIB-II                          | <p>セキュリティ アプライアンスは、次のグループおよびテーブルのブラウジングをサポートします。</p> <ul style="list-style-type: none"> <li>system</li> </ul>                                                                                                                                                                                                             |
| IF-MIB                          | <p>セキュリティ アプライアンスは、次のテーブルのブラウジングをサポートします。</p> <ul style="list-style-type: none"> <li>ifTable</li> <li>ifXTable</li> </ul>                                                                                                                                                                                                 |
| RFC1213-MIB                     | <p>セキュリティ アプライアンスは、次のテーブルのブラウジングをサポートします。</p> <ul style="list-style-type: none"> <li>ip.ipAddrTable</li> </ul>                                                                                                                                                                                                            |
| SNMPv2-MIB                      | <p>セキュリティ アプライアンスは、次のブラウジングをサポートします。</p> <ul style="list-style-type: none"> <li>snmp</li> </ul>                                                                                                                                                                                                                           |
| ENTITY-MIB                      | <p>セキュリティ アプライアンスは、次のグループおよびテーブルのブラウジングをサポートします。</p> <ul style="list-style-type: none"> <li>entPhysicalTable</li> <li>entLogicalTable</li> </ul> <p>セキュリティ アプライアンスは、次のトラップのブラウジングをサポートします。</p> <ul style="list-style-type: none"> <li>snmp-server enable traps entity {config-change fru-insert fru-remove}</li> </ul>    |
| CISCO-IPSEC-FLOW-MONITOR-MIB    | <p>セキュリティ アプライアンスは、MIB のブラウジングをサポートします。</p> <p>セキュリティ アプライアンスは、次のトラップのブラウジングをサポートします。</p> <ul style="list-style-type: none"> <li>snmp-server enable traps ipsec {start stop}</li> </ul>                                                                                                                                   |
| CISCO-REMOTE-ACCESS-MONITOR-MIB | <p>セキュリティ アプライアンスは、MIB のブラウジングをサポートします。</p> <p>セキュリティ アプライアンスは、次のトラップのブラウジングをサポートします。</p> <ul style="list-style-type: none"> <li>snmp-server enable traps remote-access {session-threshold-exceeded}</li> </ul>                                                                                                           |

表 35-1 SNMP MIB とトラップのサポート (続き)

| MIB またはトラップのサポート             | 説明                                                                                                                                                                                           |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-CRYPTO-ACCELERATOR-MIB | セキュリティ アプライアンスは、MIB のブラウジングをサポートします。                                                                                                                                                         |
| ALTIGA-GLOBAL-REG            | セキュリティ アプライアンスは、MIB のブラウジングをサポートします。                                                                                                                                                         |
| Cisco Firewall MIB           | セキュリティ アプライアンスは、次のグループのブラウジングをサポートします。 <ul style="list-style-type: none"> <li>cfwSystem<br/>情報は cfwSystem.cfwStatus です。これは、フェールオーバー ステータスに関連する情報であり、シングルコンテキストだけでなく、デバイス全体に関係します。</li> </ul> |
| Cisco Memory Pool MIB        | セキュリティ アプライアンスは、次のテーブルのブラウジングをサポートします。 <ul style="list-style-type: none"> <li>ciscoMemoryPoolTable：このテーブルに示されているメモリ使用量は、セキュリティ アプライアンス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。</li> </ul>       |
| Cisco Process MIB            | セキュリティ アプライアンスは、次のテーブルのブラウジングをサポートします。 <ul style="list-style-type: none"> <li>cpmCPUTotalTable</li> </ul>                                                                                    |
| Cisco Syslog MIB             | セキュリティ アプライアンスは、次のトラップをサポートします。 <ul style="list-style-type: none"> <li>clogMessageGenerated</li> </ul> この MIB はブラウズできません。                                                                    |

## SNMP のイネーブル化

セキュリティ アプライアンスで動作する SNMP エージェントは、次の 2 つの機能を実行します。

- NMS からの SNMP 要求に応答する。
- トラップ（イベント通知）を NMS に送信する。

SNMP エージェントをイネーブルにし、セキュリティ アプライアンスに接続できる NMS を識別するには、次の手順を実行します。

**ステップ 1** セキュリティ アプライアンスに接続できる NMS の IP アドレスを識別するには、次のコマンドを入力します。

```
hostname(config)# snmp-server host interface_name ip_address [trap | poll] [community text] [version 1 | 2c] [udp-port port]
```

トラップのみ、またはブラウジング（ポーリング）のみを受信するように NMS を制限する場合は、**trap** または **poll** を指定します。デフォルトでは、NMS は両方の機能を使用します。

SNMP トラップは、デフォルトでは UDP ポート 162 で送信されます。ポート番号は **udp-port** キーワードを使用して変更できます。

**ステップ 2** コミュニティ スtring を指定するには、次のコマンドを入力します。

```
hostname(config)# snmp-server community key
```

SNMP コミュニティ スtring は、セキュリティ アプライアンスと NMS の間の共有秘密情報です。キーは、大文字と小文字が区別される最大 32 文字の値です。スペースは使用できません。

**ステップ 3** (オプション) SNMP サーバの位置または接点情報を設定するには、次のコマンドを入力します。

```
hostname(config)# snmp-server {contact | location} text
```

**ステップ 4** セキュリティ アプライアンスでトラップを NMS に送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)# snmp-server enable [traps [all | feature [trap1] [trap2]] [...]]
```

デフォルトでは、SNMP コア トラップがイネーブルになっています (**snmp**)。コマンドにトラップ タイプを入力しない場合は、**syslog** がデフォルトで使用されます。すべてのトラップをイネーブルまたはディセーブルにするには、**all** オプションを入力します。**snmp** の場合は、各トラップ タイプを個別に識別できます。トラップのリストについては、[P.35-2 の表 35-1](#) を参照してください。

**ステップ 5** システム メッセージをトラップとして NMS に送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)# logging history level
```

また、先行する **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する必要があります。

**ステップ 6** ログイングをイネーブルにして、生成されたシステム メッセージを NMS に送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)# logging on
```

---

次の例では、内部インターフェイス上のホスト 192.168.3.2 から要求を受信するようにセキュリティ アプライアンスを設定します。

```
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
```



# セキュリティ アプライアンスのトラブルシューティング

---

この章では、セキュリティ アプライアンスのトラブルシューティングの方法について説明します。次の項で構成されています。

- [コンフィギュレーションのテスト \(P.36-2\)](#)
- [セキュリティ アプライアンスのリロード \(P.36-7\)](#)
- [パスワード回復の実行 \(P.36-8\)](#)
- [その他のトラブルシューティング ツール \(P.36-12\)](#)
- [一般的な問題 \(P.36-13\)](#)

## コンフィギュレーションのテスト

この項では、シングルモードのセキュリティ アプライアンスまたは各セキュリティ コンテキストの接続性をテストする方法について説明します。次の手順では、セキュリティ アプライアンス インターフェイスを ping する方法と、あるインターフェイス上のホストが別のインターフェイス上のホストに ping できるようにする方法について説明します。

ping およびデバッグ メッセージはトラブルシューティング時に限りイネーブルにしてください。セキュリティ アプライアンスのテストが終了したら、[P.36-6 の「テスト コンフィギュレーションのディセーブル化」](#)の手順を実行します。

この項の内容は次のとおりです。

- [ICMP デバッグ メッセージとシステム メッセージのイネーブル化 \(P.36-2\)](#)
- [セキュリティ アプライアンス インターフェイスの ping \(P.36-3\)](#)
- [セキュリティ アプライアンスによる ping \(P.36-5\)](#)
- [テスト コンフィギュレーションのディセーブル化 \(P.36-6\)](#)

### ICMP デバッグ メッセージとシステム メッセージのイネーブル化

デバッグ メッセージとシステム メッセージは、ping が成功しない理由をトラブルシューティングするのに役立ちます。セキュリティ アプライアンスは、セキュリティ アプライアンス インターフェイスへの ping に対する ICMP デバッグ メッセージのみを表示します。セキュリティ アプライアンスを経由する他のホストへの ping に対する ICMP デバッグ メッセージは表示しません。デバッグ メッセージとシステム メッセージをイネーブルにするには、次の手順を実行します。

- ステップ 1** セキュリティ アプライアンス インターフェイスへの ping の ICMP パケット情報を表示するには、次のコマンドを入力します。

```
hostname(config)# debug icmp trace
```

- ステップ 2** Telnet セッションまたは SSH セッションに送信するシステム メッセージを設定するには、次のコマンドを入力します。

```
hostname(config)# logging monitor debug
```

あるいは、**logging buffer debug** を使用してメッセージをバッファに送信してから、後で **show logging** コマンドを使用してそれらを表示することもできます。

- ステップ 3** システム メッセージを Telnet または SSH セッションに送信するには、次のコマンドを入力します。

```
hostname(config)# terminal monitor
```

- ステップ 4** システム メッセージ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)# logging on
```

次に、外部ホスト (209.165.201.2) からセキュリティ アプライアンスの外部インターフェイス (209.165.201.1) への ping が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
```

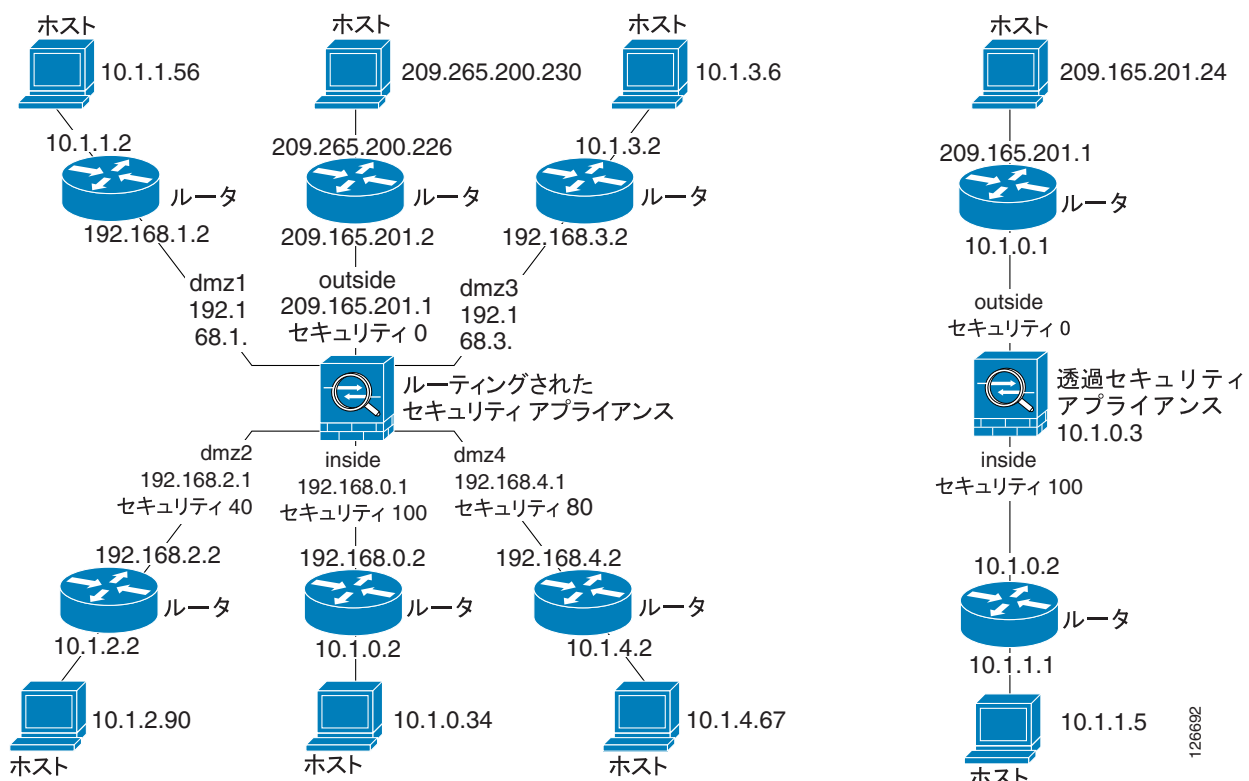
この例では、ICMP パケット長 (32 バイト)、ICMP パケット識別子 (1)、および ICMP シーケンス番号 (ICMP シーケンス番号は 0 から始まり、要求が送信されるたびに増分されます) が示されています。

## セキュリティ アプライアンス インターフェイスの ping

セキュリティ アプライアンス インターフェイスが起動して動作していること、およびセキュリティ アプライアンスと接続ルータが正しくルーティングされていることをテストするには、セキュリティ アプライアンス インターフェイスを ping します。セキュリティ アプライアンス インターフェイスを ping するには、次の手順を実行します。

- ステップ 1** インターフェイス名、セキュリティ レベル、および IP アドレスを示すシングルモードのセキュリティ アプライアンスまたはセキュリティ コンテキストの概略図を作成します。概略図には、直接接続されたすべてのルータ、およびセキュリティ アプライアンスを ping するルータの反対側にあるホストも含める必要があります。この手順と P.36-5 の「セキュリティ アプライアンスによる ping」の手順の情報を使用してください。次の例を参考にしてください。

図 36-1 インターフェイス、ルータ、およびホストを含むネットワーク概略図



**ステップ 2** 直接接続されたルータから各セキュリティ アプライアンス インターフェイスを ping します。透過モードでは、管理 IP アドレスを ping します。

このテストは、セキュリティ アプライアンス インターフェイスがアクティブであること、およびインターフェイス コンフィギュレーションが正しいことを確認します。

セキュリティ アプライアンス インターフェイスがアクティブではない場合、インターフェイス コンフィギュレーションが正しくない場合、またはセキュリティ アプライアンスとルータの間でスイッチがダウンしている場合、ping は失敗する可能性があります (図 36-2 を参照)。この場合、パケットが到達しないので、デバッグ メッセージやシステム メッセージはセキュリティ アプライアンスに表示されません。

図 36-2 セキュリティ アプライアンス インターフェイスでの ping の失敗

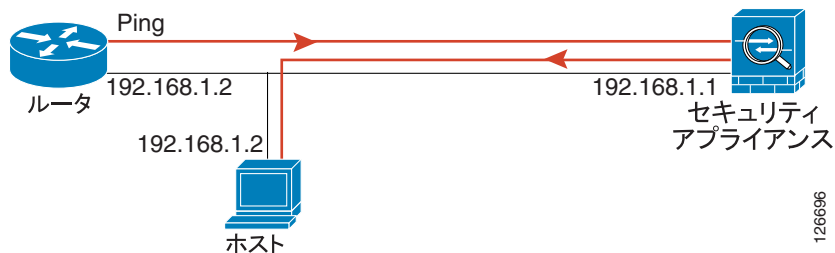


ping がセキュリティ アプライアンスに到達し、セキュリティ アプライアンスが応答すると、次のようなデバッグ メッセージが表示されます。

```
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 応答がルータに戻されない場合は、スイッチ ループまたは冗長 IP アドレスの可能性がありま (図 36-3 を参照)。

図 36-3 IP アドレッシングの問題による ping の失敗



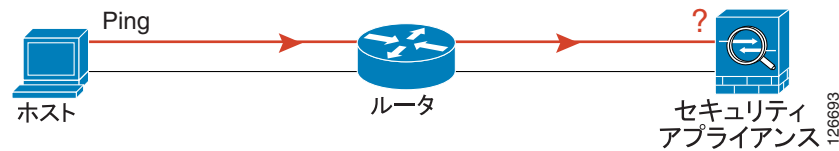
**ステップ 3** リモート ホストから各セキュリティ アプライアンス インターフェイスを ping します。透過モードでは、管理 IP アドレスを ping します。

このテストは、直接接続されたルータがホストとセキュリティ アプライアンスの間でパケットをルーティングできること、およびセキュリティ アプライアンスがパケットを正確にルーティングしてホストに戻せることを確認します。

中間ルータを通してホストに戻るルートがセキュリティ アプライアンスにない場合、ping は失敗する可能性があります (図 36-4 を参照)。この場合、デバッグ メッセージには ping が成功したことが示されますが、ルーティングの失敗を示すシステム メッセージ 110001 が表示されます。



図 36-4 セキュリティ アプライアンスにルートがないことによる ping の失敗



## セキュリティ アプライアンスによる ping

セキュリティ アプライアンス インターフェイスを正常に ping した後、トラフィックがセキュリティ アプライアンスを正常に通過できること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 が正しく機能していることが示されます（設定されている場合）。透過モードの場合は、NAT を使用しないので、このテストではセキュリティ アプライアンスが正しく動作していることが確認されます。透過モードで ping が失敗した場合は、Cisco TAC にお問い合わせください。

異なるインターフェイス上のホスト間で ping するには、次の手順を実行します。

- ステップ 1** 発信元ホストから ICMP を許可するアクセスリストを追加するには、次のコマンドを入力します。

```
hostname(config)# access-list ICMPACL extended permit icmp any any
```

デフォルトでは、ホストが低セキュリティ インターフェイスにアクセスすると、すべてのトラフィックが通過を許可されます。ただし、高セキュリティ インターフェイスにアクセスするには、先行するアクセスリストが必要です。

- ステップ 2** 各発信元インターフェイスにアクセスリストを割り当てるには、次のコマンドを入力します。

```
hostname(config)# access-group ICMPACL in interface interface_name
```

各発信元インターフェイスに対してこのコマンドを繰り返します。

- ステップ 3** ICMP 応答が発信元ホストに戻されるように ICMP 検査エンジン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)# 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
```

あるいは、ICMPACL アクセスリストを宛先インターフェイスに適用し、セキュリティ アプライアンスを介して ICMP トラフィックを戻すこともできます。

- ステップ 4** ホストまたはルータから発信元インターフェイスを介して別のインターフェイス上の別のホストまたはルータに ping します。

確認が必要なすべてのインターフェイス ペアに対して、このステップを繰り返します。

ping が成功すると、ルーテッド モードのアドレス変換（305009 または 305011）と ICMP 接続が確立されたこと（302020）を確認するシステム メッセージが表示されます。show xlate および 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。

透過モードの ping が失敗した場合は、Cisco TAC にお問い合わせください。

ルーテッド モードでは、NAT が正しく設定されていないために ping が失敗する可能性があります（図 36-5 を参照）。これは、NAT 制御をイネーブルにした場合に発生する可能性があります。この場合、NAT 変換が失敗したことを示すシステム メッセージが表示されます（305005 または 305006）。外部ホストから内部ホストに ping し、スタティック変換（NAT 制御を必要とする）がない場合は、メッセージ 106010: deny inbound icmp が表示されます。



(注)

セキュリティ アプライアンスは、セキュリティ アプライアンス インターフェイスへの ping に対する ICMP デバッグ メッセージのみを表示します。セキュリティ アプライアンスを経由する他のホストへの ping に対する ICMP デバッグ メッセージは表示しません。

図 36-5 セキュリティ アプライアンスがアドレスを変換しないことによる ping の失敗



## テスト コンフィギュレーションのディセーブル化

テストの完了後、ICMP のセキュリティ アプライアンスへの送信および通過を許可し、デバッグ メッセージを表示するテスト コンフィギュレーションをディセーブルにします。このコンフィギュレーションをそのままにしておくと、深刻なセキュリティ リスクが生じる可能性があります。また、デバッグ メッセージはセキュリティ アプライアンスのパフォーマンスを低下させます。

テスト コンフィギュレーションをディセーブルにするには、次の手順を実行します。

**ステップ 1** ICMP デバッグ 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)# no debug icmp trace
```

**ステップ 2** 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 on
```

**ステップ 3** ICMPACL アクセスリストを削除し、関連する access-group コマンドも削除するには、次のコマンドを入力します。

```
hostname(config)# no access-list ICMPACL
```

**ステップ 4** （オプション）ICMP 検査エンジ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 service-map ICMP-POLICY
```

---

## セキュリティ アプライアンスのリロード

マルチモードでは、システム実行スペースからしかリロードできません。セキュリティ アプライアンスをリロードするには、次のコマンドを入力します。

```
hostname# reload
```

## パスワード回復の実行

この項では、パスワードを忘れた場合、または AAA 設定のためロックアウト状態を生み出した場合に回復する方法について説明します。セキュリティの向上のためパスワードの回復をディセーブルにすることもできます。ここでは、次の項目について説明します。

- [ASA 5500 シリーズ適応型セキュリティ アプライアンスのパスワード回復の実行 \(P.36-8\)](#)
- [PIX 500 シリーズ セキュリティ アプライアンスのパスワード回復 \(P.36-9\)](#)
- [パスワード回復のディセーブル化 \(P.36-11\)](#)

### ASA 5500 シリーズ適応型セキュリティ アプライアンスのパスワード回復の実行

パスワードの喪失から回復するには、次の手順を実行します。

**ステップ 1** [P.2-2 の「コマンドライン インターフェイスへのアクセス」](#)に従って、セキュリティ アプライアンスのコンソール ポートに接続します。

**ステップ 2** セキュリティ アプライアンスの電源を切ってから、投入します。

**ステップ 3** スタートアップ メッセージで、ROMMON を入力するように求めるプロンプトが表示されたら、**Escape** キーを押します。

**ステップ 4** リロード時にスタートアップ コンフィギュレーションを無視するようにセキュリティ アプライアンスを設定するには、次のコマンドを入力します。

```
rommon #1> confreg
```

セキュリティ アプライアンスによって現在のコンフィギュレーションのレジスタ値が表示され、その値を変更するかどうか尋ねられます。

```
Current Configuration Register: 0x00000011
Configuration Summary:
  boot TFTP image, boot default image from Flash on netboot failure
Do you wish to change this configuration? y/n [n]:
```

**ステップ 5** 後で回復できるように、現在のコンフィギュレーションのレジスタ値を記録します。

**ステップ 6** 値を変更する場合は、プロンプトに対して **Y** を入力します。

セキュリティ アプライアンスによって、新しい値の入力を求めるプロンプトが表示されます。

**ステップ 7** すべての設定についてデフォルト値を受け入れます。ただし、「disable system configuration?」値のプロンプトに対しては **Y** を入力します。

**ステップ 8** 次のコマンドを入力して、セキュリティ アプライアンスをリロードします。

```
rommon #2> boot
```

セキュリティ アプライアンスは、スタートアップ コンフィギュレーションの代わりにデフォルト コンフィギュレーションをロードします。

**ステップ 9** 次のコマンドを入力して、特権 EXEC モードに入ります。

```
hostname> enable
```

**ステップ 10** パスワードの入力を求められたら、**Return** キーを押します。

パスワードはブランクです。

**ステップ 11** 次のコマンドを入力して、スタートアップ コンフィギュレーションをロードします。

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

**ステップ 12** 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 モードに入ります。

```
hostname# configure terminal
```

**ステップ 13** 必要に応じて次のコマンドを入力し、コンフィギュレーションでパスワードを変更します。

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

**ステップ 14** 次のコマンドを入力して、次回のリロード時にスタートアップ コンフィギュレーションをロードするようにコンフィギュレーション レジスタを変更します。

```
hostname(config)# config-register value
```

ここで、*value* は**ステップ 5** でメモしたコンフィギュレーション レジスタ値です。0x1 はデフォルト コンフィギュレーション レジスタです。コンフィギュレーション レジスタの詳細については、『Cisco Security Appliance Command Reference』を参照してください。

**ステップ 15** 次のコマンドを入力して、新しいパスワードをスタートアップ コンフィギュレーションに保存します。

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

## PIX 500 シリーズ セキュリティ アプライアンスのパスワード回復

セキュリティ アプライアンスでパスワード回復を実行すると、ログイン パスワード、イネーブル パスワード、および **aaa authentication console** コマンドが消去されます。これらのコマンドを消去してデフォルト パスワードでログインできるようにするには、次の手順を実行します。

**ステップ 1** Cisco.com から、セキュリティ アプライアンスでアクセス可能な TFTP サーバに PIX パスワード ツールをダウンロードします。次の URL で「Password Recovery Procedure for the PIX」の資料内のリンクを参照してください。

```
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_password_recovery09186a008009478b.shtml
```

**ステップ 2** P.2-2 の「コマンドライン インターフェイスへのアクセス」に従って、セキュリティ アプライアンスのコンソール ポートに接続します。

**ステップ 3** セキュリティ アプライアンスの電源を切ってから、投入します。

**ステップ 4** スタートアップ メッセージが表示された直後に、**Escape** キーを押してモニタ モードに入ります。

**ステップ 5** 次のコマンドを入力して、TFTP サーバにアクセスするインターフェイスのネットワーク設定値を設定します。

```
monitor> interface interface_id
monitor> address interface_ip
monitor> server tftp_ip
monitor> file pw_tool_name
monitor> gateway gateway_ip
```

**ステップ 6** 次のコマンドを入力して、TFTP サーバから PIX パスワード ツールをダウンロードします。

```
monitor> tftp
```

サーバに到達できない場合は、**ping address** コマンドを入力して接続をテストします。

**ステップ 7** 「Do you wish to erase the passwords?」 プロンプトで、**Y** を入力します。

これで、デフォルト ログイン パスワード「cisco」とブランクのイネーブル パスワードでログインできるようになります。

---

次の例は、外部インターフェイス上の TFTP サーバによる PIX パスワード回復を示しています。

```
monitor> interface 0
0: i8255X @ PCI(bus:0 dev:13 irq:10)
1: i8255X @ PCI(bus:0 dev:14 irq:7 )

Using 0: i82559 @ PCI(bus:0 dev:13 irq:10), MAC: 0050.54ff.82b9
monitor> address 10.21.1.99
address 10.21.1.99
monitor> server 172.18.125.3
server 172.18.125.3
monitor> file np70.bin
file np52.bin
monitor> gateway 10.21.1.1
gateway 10.21.1.1
monitor> ping 172.18.125.3
Sending 5, 100-byte 0xf8d3 ICMP Echoes to 172.18.125.3, timeout is 4 seconds:
!!!!
Success rate is 100 percent (5/5)
monitor> tftp
tftp np52.bin@172.18.125.3 via 10.21.1.1.....
Received 73728 bytes

Cisco PIX password tool (4.0) #0: Tue Aug 22 23:22:19 PDT 2005
Flash=i28F640J5 @ 0x300
BIOS Flash=AT29C257 @ 0xd8000

Do you wish to erase the passwords? [yn] y
Passwords have been erased.

Rebooting....
```

## パスワード回復のディセーブル化

権限のないユーザがパスワード回復メカニズムを使用してセキュリティ アプライアンスを危険にさらすことがないように、パスワード回復をディセーブルにすることができます。パスワード回復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 service password-recovery
```

ASA 5500 シリーズ適応型セキュリティ アプライアンスで、**no service password-recovery** コマンドは、ユーザが ROMMON を入力しないようにして、コンフィギュレーションが変更されないようにします。ユーザが ROMMON を入力すると、セキュリティ アプライアンスはユーザに対し、すべてのフラッシュ ファイル システムを消去するように求めるプロンプトを表示します。ユーザはこの消去をまず実行しないと、ROMMON を入力できません。ユーザがフラッシュ ファイル システムを消去しない場合、セキュリティ アプライアンスはリロードします。パスワード回復は ROMMON の使用と既存のコンフィギュレーションの保持に依存しているので、この消去によって、パスワードを回復することはできなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合、システムを動作可能な状態まで回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（入手できる場合）をロードします。**service password-recovery** コマンドは、情報提供の目的に限りコンフィギュレーション ファイルに表示されます。CLI プロンプトでこのコマンドを入力すると、設定が NVRAM に保存されます。設定を変更する唯一の方法は、CLI プロンプトでコマンドを入力することです。このコマンドの異なるバージョンで新規コンフィギュレーションをロードしても、設定は変更されません。セキュリティ アプライアンスが（パスワード回復の準備で）起動時にスタートアップ コンフィギュレーションを無視するように設定されている場合にパスワード回復をディセーブルにすると、セキュリティ アプライアンスは通常どおりスタートアップ コンフィギュレーションをブートするように設定を変更します。フェールオーバーを使用し、スタートアップ コンフィギュレーションを無視するようにスタンバイ装置が設定されている場合は、**no service password recovery** コマンドがスタンバイ装置に複製したときにコンフィギュレーション レジスタに同じ変更が加えられます。

PIX 500 シリーズ セキュリティ アプライアンスで、**no service password-recovery** コマンドは、すべてのフラッシュ ファイル システムの消去をユーザに求めるプロンプトを表示するように PIX パスワード ツールに強制します。ユーザは、まずこの消去を実行しないと、PIX パスワード ツールを使用できません。ユーザがフラッシュ ファイル システムを消去しない場合、セキュリティ アプライアンスはリロードします。パスワード回復は既存のコンフィギュレーションの保持に依存しているので、この消去によって、パスワードを回復することはできなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合、システムを動作可能な状態まで回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（入手できる場合）をロードします。

## その他のトラブルシューティング ツール

セキュリティ アプライアンスには、Cisco TAC とともに使用するその他のトラブルシューティング ツールがあります。

- デバッグ メッセージの表示 (P.36-12)
- パケットの取得 (P.36-12)
- クラッシュ ダンプの表示 (P.36-12)

### デバッグ メッセージの表示

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、debug コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。デバッグ メッセージをイネーブルにする方法は、『Cisco Security Appliance Command Reference』の **debug** コマンドを参照してください。

### パケットの取得

パケットの取得は、接続障害のトラブルシューティングや不審なアクティビティの監視を行う場合に便利です。パケット取得機能を使用する場合は、Cisco TAC に連絡することをお勧めします。『Cisco Security Appliance Command Reference』の **capture** コマンドを参照してください。

### クラッシュ ダンプの表示

セキュリティ アプライアンスがクラッシュした場合に、クラッシュ ダンプ情報を表示できます。クラッシュ ダンプの内容を調べる必要がある場合は、Cisco TAC に連絡することをお勧めします。『Cisco Security Appliance Command Reference』の **show crashdump** コマンドを参照してください。



## 一般的な問題

この項では、セキュリティ アプライアンスの一般的な問題とそれらを解決する方法について説明します。

**現象** コンテキスト コンフィギュレーションが保存されておらず、リロード時に失われました。

**考えられる原因** コンテキスト実行スペース内で各コンテキストを保存しませんでした。コマンドラインでコンテキストを設定している場合、次のコンテキストに切り替える前にコンテキストを保存しませんでした。

**推奨処置** `copy run start` コマンドを使用して、コンテキスト実行スペース内で各コンテキストを保存します。システム実行スペースからはコンテキストを保存できません。

**現象** セキュリティ アプライアンス インターフェイスへの Telnet 接続または SSH を確立できません。

**考えられる原因** セキュリティ アプライアンスへの Telnet または SSH をイネーブルにしませんでした。

**推奨処置** P.33-2 の「Telnet アクセスの許可」または P.33-3 の「SSH アクセスの許可」に従って、セキュリティ アプライアンスへの Telnet または SSH をイネーブルにします。

**現象** セキュリティ アプライアンス インターフェイスを ping できません。

**考えられる原因** セキュリティ アプライアンスへの ICMP をディセーブルにしました。

**推奨処置** `icmp` コマンドを使用して、IP アドレス用にセキュリティ アプライアンスへの 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にもかかわらず、セキュリティ アプライアンスを介して ping することができません。

**考えられる原因** ICMP 検査エンジンをイネーブルにしていないか、入力インターフェイスと出力インターフェイスの両方でアクセスリストを適用していません。

**推奨処置** ICMP はコネクションレス型プロトコルなので、セキュリティ アプライアンスはトラフィックが戻ること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ために、入力インターフェイスだけでなく出力インターフェイスにもアクセスリストを適用するか、あるいは ICMP 接続がステートフル接続として扱われるように ICMP 検査エンジンをイネーブルにします。

**現象** 同一セキュリティ レベルにある 2 つのインターフェイス間をトラフィックが通過しません。

**考えられる原因** 同一セキュリティ レベルにあるインターフェイス間をトラフィックが通過できるようにする機能をイネーブルにしていません。

**推奨処置** P.6-7 の「同一セキュリティ レベルにあるインターフェイス間の通信の許可」に従って、この機能をイネーブルにします。





## PART 5

### 參考資料







## 機能のライセンスと仕様

---

この付録では、機能のライセンスと仕様について説明します。この付録では、次の項目について説明します。

- サポートされているプラットフォーム (P.A-1)
- プラットフォームの機能のライセンス (P.A-2)
- セキュリティ サービス モジュール サポート (P.A-6)
- VPN 仕様 (P.A-7)

### サポートされているプラットフォーム

このソフトウェア バージョンは、次のプラットフォームをサポートしています。

- ASA 5510
- ASA 5520
- ASA 5540
- PIX 515/515E
- PIX 525
- PIX 535

## プラットフォームの機能のライセンス

次の表に、各プラットフォーム ライセンスの機能サポートを示します。



(注)

イタリック体で示された項目は、基本ライセンスに追加できる個別のオプション ライセンスです。ライセンスは、混合し組み合わせることができます。たとえば、10 セキュリティ コンテキスト ライセンスと Strong Encryption ライセンス、VPN Plus ライセンスと GTP/GPRS ライセンス、または 4 つのライセンスを同時に使用することができます。

表 A-1 ASA 5500 シリーズ適応型セキュリティ アプライアンス ライセンスの機能

| プラットフォームおよび機能             | ライセンス                                                           |          |                          |    |     |     |                         |          |                          |    |     |     |
|---------------------------|-----------------------------------------------------------------|----------|--------------------------|----|-----|-----|-------------------------|----------|--------------------------|----|-----|-----|
| ASA 5510                  | 基本ライセンス                                                         |          |                          |    |     |     | Security Plus           |          |                          |    |     |     |
| セキュリティ コンテキスト             | サポートしない                                                         |          |                          |    |     |     | サポートしない                 |          |                          |    |     |     |
| VPN セッション <sup>1</sup>    | IPSec と WebVPN の合計で 250                                         |          |                          |    |     |     | IPSec と WebVPN の合計で 250 |          |                          |    |     |     |
| 最大 IPSec セッション            | 250                                                             |          |                          |    |     |     | 250                     |          |                          |    |     |     |
| 最大 WebVPN セッション           | 2                                                               | 追加ライセンス： |                          |    |     |     | 2                       | 追加ライセンス： |                          |    |     |     |
|                           |                                                                 | 10       | 25                       | 50 | 100 | 250 |                         | 10       | 25                       | 50 | 100 | 250 |
| VPN ロードバランシング             | サポートしない                                                         |          |                          |    |     |     | サポートしない                 |          |                          |    |     |     |
| フェールオーバー                  | なし                                                              |          |                          |    |     |     | Active/Standby          |          |                          |    |     |     |
| GTP/GPRS                  | サポートされていない                                                      |          |                          |    |     |     | サポートされていない              |          |                          |    |     |     |
| 最大 VLAN                   | 10                                                              |          |                          |    |     |     | 25                      |          |                          |    |     |     |
| 同時ファイアウォール接続 <sup>2</sup> | 50 K                                                            |          |                          |    |     |     | 130 K                   |          |                          |    |     |     |
| 最大物理インターフェイス              | 10/100 に 3 つと、管理トラフィック専用の管理インターフェイス (to-the-security-appliance) |          |                          |    |     |     | 制限なし                    |          |                          |    |     |     |
| 暗号化                       | 基本 (DES)                                                        |          | アドオン ライセンス：強化 (3DES/AES) |    |     |     | 基本 (DES)                |          | アドオン ライセンス：強化 (3DES/AES) |    |     |     |
| 最小 RAM                    | 256 MB                                                          |          |                          |    |     |     | 256 MB                  |          |                          |    |     |     |
| ASA 5520                  | 基本ライセンス                                                         |          |                          |    |     |     |                         |          |                          |    |     |     |
| セキュリティ コンテキスト             | 2                                                               | 追加ライセンス： |                          |    |     |     |                         |          |                          |    |     |     |
|                           |                                                                 | 5        | 10                       | 20 |     |     |                         |          |                          |    |     |     |
| VPN セッション <sup>1</sup>    | IPSec と WebVPN の合計で 750                                         |          |                          |    |     |     |                         |          |                          |    |     |     |
| 最大 IPSec セッション            | 750                                                             |          |                          |    |     |     |                         |          |                          |    |     |     |
| 最大 WebVPN セッション           | 2                                                               | 追加ライセンス： |                          |    |     |     |                         |          |                          |    |     |     |
|                           |                                                                 | 10       | 25                       | 50 | 100 | 250 | 500                     | 750      |                          |    |     |     |
| VPN ロードバランシング             | サポート対象                                                          |          |                          |    |     |     |                         |          |                          |    |     |     |
| フェールオーバー                  | Active/Standby<br>Active/Active                                 |          |                          |    |     |     |                         |          |                          |    |     |     |
| GTP/GPRS                  | なし                                                              |          | 追加ライセンス：イネーブル            |    |     |     |                         |          |                          |    |     |     |
| 最大 VLAN                   | 100                                                             |          |                          |    |     |     |                         |          |                          |    |     |     |
| 同時ファイアウォール接続 <sup>2</sup> | 280 K                                                           |          |                          |    |     |     |                         |          |                          |    |     |     |
| 最大物理インターフェイス              | 制限なし                                                            |          |                          |    |     |     |                         |          |                          |    |     |     |
| 暗号化                       | 基本 (DES)                                                        |          | アドオン ライセンス：強化 (3DES/AES) |    |     |     |                         |          |                          |    |     |     |

表 A-1 ASA 5500 シリーズ適応型セキュリティ アプライアンス ライセンスの機能 (続き)

| プラットフォームおよび機能             | ライセンス                    |                         |    |    |     |     |     |     |      |      |
|---------------------------|--------------------------|-------------------------|----|----|-----|-----|-----|-----|------|------|
| 最小 RAM                    | 512 MB                   |                         |    |    |     |     |     |     |      |      |
| ASA 5540                  | 基本ライセンス                  |                         |    |    |     |     |     |     |      |      |
| セキュリティ コンテキスト             | 2                        | 追加ライセンス：                |    |    |     |     |     |     |      |      |
|                           |                          | 5                       | 10 | 20 | 50  |     |     |     |      |      |
| VPN セッション <sup>1</sup>    | IPSec と WebVPN の合計で 5000 |                         |    |    |     |     |     |     |      |      |
| 最大 IPSec セッション            | 5000                     |                         |    |    |     |     |     |     |      |      |
| 最大 WebVPN セッション           | 2                        | 追加ライセンス：                |    |    |     |     |     |     |      |      |
|                           |                          | 10                      | 25 | 50 | 100 | 250 | 500 | 750 | 1000 | 2500 |
| VPN ロードバランシング             | サポート対象                   |                         |    |    |     |     |     |     |      |      |
| フェールオーバー                  | Active/Standby           |                         |    |    |     |     |     |     |      |      |
|                           | Active/Active            |                         |    |    |     |     |     |     |      |      |
| GTP/GPRS                  | なし                       | 追加ライセンス：イネーブル           |    |    |     |     |     |     |      |      |
| 最大 VLAN                   | 200                      |                         |    |    |     |     |     |     |      |      |
| 同時ファイアウォール接続 <sup>2</sup> | 400 K                    |                         |    |    |     |     |     |     |      |      |
| 最大物理インターフェイス              | 制限なし                     |                         |    |    |     |     |     |     |      |      |
| 暗号化                       | 基本（DES）                  | アドオン ライセンス：強化（3DES/AES） |    |    |     |     |     |     |      |      |
| 最小 RAM                    | 1024 MB                  |                         |    |    |     |     |     |     |      |      |

1. IPSec および WebVPN のセッションの最大数には、VPN セッションの最大数を超える数のセッションを追加できますが、両セッションの合計が VPN セッションの上限を超えることはできません。VPN セッションの最大数を超過した場合は、セキュリティ アプライアンスをオーバーロードできるため、ネットワーク サイズを適切に設定するようにしてください。
2. 同時ファイアウォール接続は、4 つの接続すべてに対して 1 つのホストと 1 つのダイナミック変換を持つ 80% TCP と 20% UDP のトラフィック混合に基づいています。

## ■ プラットフォームの機能のライセンス

表 A-2 PIX 500 シリーズ セキュリティ アプライアンス ライセンスの機能

| プラットフォームおよび機能              | ライセンス   |                            |                                     |                                 |                            |                                     |                           |                            |                                     |                                            |                            |                                     |          |  |  |
|----------------------------|---------|----------------------------|-------------------------------------|---------------------------------|----------------------------|-------------------------------------|---------------------------|----------------------------|-------------------------------------|--------------------------------------------|----------------------------|-------------------------------------|----------|--|--|
| PIX 515/515E <sup>1</sup>  | R（制限付き） |                            |                                     | UR（制限なし）                        |                            |                                     | FO（フェールオーバー） <sup>2</sup> |                            |                                     | FO-AA（フェールオーバー Active/Active） <sup>2</sup> |                            |                                     |          |  |  |
| セキュリティ コンテキスト              | サポートしない |                            |                                     | 2                               | 追加ライセンス：                   |                                     |                           | 2                          | 追加ライセンス：                            |                                            |                            | 2                                   | 追加ライセンス： |  |  |
|                            |         |                            |                                     |                                 | 5                          |                                     |                           |                            | 5                                   |                                            |                            |                                     | 5        |  |  |
| IPSec セッション                | 2000    |                            |                                     | 2000                            |                            |                                     | 2000                      |                            |                                     | 2000                                       |                            |                                     |          |  |  |
| フェールオーバー                   | サポートしない |                            |                                     | Active/Standby<br>Active/Active |                            |                                     | Active/Standby            |                            |                                     | Active/Standby<br>Active/Active            |                            |                                     |          |  |  |
| GTP/GPRS                   | なし      | アドオン ライセン<br>ス：イネーブル       |                                     | なし                              | アドオン ライセン<br>ス：イネーブル       |                                     | なし                        | アドオン ライセン<br>ス：イネーブル       |                                     | なし                                         | アドオン ライセン<br>ス：イネーブル       |                                     |          |  |  |
| 最大 VLAN                    | 10      |                            |                                     | 25                              |                            |                                     | 25                        |                            |                                     | 25                                         |                            |                                     |          |  |  |
| 同時 ファイアウォール接続 <sup>3</sup> | 48 K    |                            |                                     | 130 K                           |                            |                                     | 130 K                     |                            |                                     | 130 K                                      |                            |                                     |          |  |  |
| 最大物理インターフェイス               | 3       |                            |                                     | 6                               |                            |                                     | 6                         |                            |                                     | 6                                          |                            |                                     |          |  |  |
| 暗号化                        | なし      | アドオン ライ<br>センス：基本<br>(DES) | アドオン ライ<br>センス：強化<br>(3DES/<br>AES) | なし                              | アドオン ライ<br>センス：基本<br>(DES) | アドオン ライ<br>センス：強化<br>(3DES/<br>AES) | なし                        | アドオン ライ<br>センス：基本<br>(DES) | アドオン ライ<br>センス：強化<br>(3DES/<br>AES) | なし                                         | アドオン ライ<br>センス：基本<br>(DES) | アドオン ライ<br>センス：強化<br>(3DES/<br>AES) |          |  |  |
| 最小 RAM                     | 64 MB   |                            |                                     | 128 MB                          |                            |                                     | 128 MB                    |                            |                                     | 128 MB                                     |                            |                                     |          |  |  |
| PIX 525 <sup>1</sup>       | R（制限付き） |                            |                                     | UR（制限なし）                        |                            |                                     | FO（フェールオーバー） <sup>2</sup> |                            |                                     | FO-AA（フェールオーバー Active/Active） <sup>2</sup> |                            |                                     |          |  |  |
| セキュリティ コンテキスト              | サポートしない |                            |                                     | 2                               | 追加ライセンス：                   |                                     |                           | 2                          | 追加ライセンス：                            |                                            |                            | 2                                   | 追加ライセンス： |  |  |
|                            |         |                            |                                     |                                 | 5                          | 10                                  | 20                        | 50                         |                                     | 5                                          | 10                         | 20                                  | 50       |  |  |
| IPSec セッション                | 2000    |                            |                                     | 2000                            |                            |                                     | 2000                      |                            |                                     | 2000                                       |                            |                                     |          |  |  |
| フェールオーバー                   | サポートしない |                            |                                     | Active/Standby<br>Active/Active |                            |                                     | Active/Standby            |                            |                                     | Active/Standby<br>Active/Active            |                            |                                     |          |  |  |
| GTP/GPRS                   | なし      | アドオン ライセン<br>ス：イネーブル       |                                     | なし                              | アドオン ライセン<br>ス：イネーブル       |                                     | なし                        | アドオン ライセン<br>ス：イネーブル       |                                     | なし                                         | アドオン ライセン<br>ス：イネーブル       |                                     |          |  |  |
| 最大 VLAN                    | 25      |                            |                                     | 100                             |                            |                                     | 100                       |                            |                                     | 100                                        |                            |                                     |          |  |  |
| 同時 ファイアウォール接続 <sup>3</sup> | 140 K   |                            |                                     | 280 K                           |                            |                                     | 280 K                     |                            |                                     | 280 K                                      |                            |                                     |          |  |  |
| 最大物理インターフェイス               | 6       |                            |                                     | 10                              |                            |                                     | 10                        |                            |                                     | 10                                         |                            |                                     |          |  |  |
| 暗号化                        | なし      | アドオン ライ<br>センス：基本<br>(DES) | アドオン ライ<br>センス：強化<br>(3DES/<br>AES) | なし                              | アドオン ライ<br>センス：基本<br>(DES) | アドオン ライ<br>センス：強化<br>(3DES/<br>AES) | なし                        | アドオン ライ<br>センス：基本<br>(DES) | アドオン ライ<br>センス：強化<br>(3DES/<br>AES) | なし                                         | アドオン ライ<br>センス：基本<br>(DES) | アドオン ライ<br>センス：強化<br>(3DES/<br>AES) |          |  |  |
| 最小 RAM                     | 128 MB  |                            |                                     | 256 MB                          |                            |                                     | 256 MB                    |                            |                                     | 256 MB                                     |                            |                                     |          |  |  |



表 A-2 PIX 500 シリーズ セキュリティ アプライアンス ライセンスの機能 (続き)

| プラットフォームおよび機能             | ライセンス   |                                |                                         |                                 |                                |                                         |    |                                |                                         |          |                                |                                            |    |    |          |  |  |  |
|---------------------------|---------|--------------------------------|-----------------------------------------|---------------------------------|--------------------------------|-----------------------------------------|----|--------------------------------|-----------------------------------------|----------|--------------------------------|--------------------------------------------|----|----|----------|--|--|--|
| PIX 535 <sup>1</sup>      | R（制限付き） |                                |                                         | UR（制限なし）                        |                                |                                         |    | FO（フェールオーバー） <sup>2</sup>      |                                         |          |                                | FO-AA（フェールオーバー Active/Active） <sup>2</sup> |    |    |          |  |  |  |
| セキュリティ コンテキスト             | サポートしない |                                |                                         | 2                               | 追加ライセンス：                       |                                         |    |                                | 2                                       | 追加ライセンス： |                                |                                            |    | 2  | 追加ライセンス： |  |  |  |
|                           |         |                                |                                         | 5                               | 10                             | 20                                      | 50 | 5                              | 10                                      | 20       | 50                             | 5                                          | 10 | 20 | 50       |  |  |  |
| IPSec セッション               | 2000    |                                |                                         | 2000                            |                                |                                         |    | 2000                           |                                         |          |                                | 2000                                       |    |    |          |  |  |  |
| フェールオーバー                  | サポートしない |                                |                                         | Active/Standby<br>Active/Active |                                |                                         |    | Active/Standby                 |                                         |          |                                | Active/Standby<br>Active/Active            |    |    |          |  |  |  |
| GTP/GPRS                  | なし      | アドオン ライセン<br>ス：イネーブル           |                                         | なし                              | アドオン ライセン<br>ス：イネーブル           |                                         | なし | アドオン ライセン<br>ス：イネーブル           |                                         | なし       | アドオン ライセン<br>ス：イネーブル           |                                            |    |    |          |  |  |  |
| 最大 VLAN                   | 50      |                                |                                         | 150                             |                                |                                         |    | 150                            |                                         |          |                                | 150                                        |    |    |          |  |  |  |
| 同時ファイアウォール接続 <sup>3</sup> | 250 K   |                                |                                         | 500 K                           |                                |                                         |    | 500 K                          |                                         |          |                                | 500 K                                      |    |    |          |  |  |  |
| 最大物理インターフェイス              | 8       |                                |                                         | 14                              |                                |                                         |    | 14                             |                                         |          |                                | 14                                         |    |    |          |  |  |  |
| 暗号化                       | なし      | アドオン ライ<br>センス：<br>基本<br>(DES) | アドオン ライ<br>センス：<br>強化<br>(3DES/<br>AES) | なし                              | アドオン ライ<br>センス：<br>基本<br>(DES) | アドオン ライ<br>センス：<br>強化<br>(3DES/<br>AES) | なし | アドオン ライ<br>センス：<br>基本<br>(DES) | アドオン ライ<br>センス：<br>強化<br>(3DES/<br>AES) | なし       | アドオン ライ<br>センス：<br>基本<br>(DES) | アドオン ライ<br>センス：<br>強化<br>(3DES/<br>AES)    |    |    |          |  |  |  |
| 最小 RAM                    | 512 MB  |                                |                                         | 1024 MB                         |                                |                                         |    | 1024 MB                        |                                         |          |                                | 1024 MB                                    |    |    |          |  |  |  |

- PIX 500 シリーズ セキュリティ アプライアンスは、WebVPN または VPN ロードバランシングをサポートしません。
- このライセンスは、UR ライセンスを持つ別の装置とのフェールオーバー ペアでのみ使用できます。どちらの装置も同じモデルである必要があります。
- 同時ファイアウォール接続は、4つの接続すべてに対して1つのホストと1つのダイナミック変換を持つ80% TCP と20% UDP のトラフィック混合に基づいています。

## セキュリティ サービス モジュール サポート

表 A-3 に、各プラットフォームでサポートされる SSM を示します。

**表 A-3 SSM サポート**

| プラットフォーム     | SSM モジュール               |
|--------------|-------------------------|
| ASA 5510     | AIP SSM 10              |
|              | CSC SSM 10              |
|              | CSC SSM 20              |
|              | 4GE SSM                 |
| ASA 5520     | AIP SSM 10              |
|              | AIP SSM 20              |
|              | CSC SSM 10              |
|              | CSC SSM 20              |
|              | 4GE SSM                 |
| ASA 5540     | AIP SSM 10              |
|              | AIP SSM 20              |
|              | CSC SSM 10 <sup>1</sup> |
|              | CSC SSM 20 <sup>1</sup> |
|              | 4GE SSM                 |
| PIX 515/515E | サポートしない                 |
| PIX 525      | サポートしない                 |
| PIX 535      | サポートしない                 |

1. CSC SSM ライセンスでは、最大 1000 人のユーザをサポートしますが、Cisco ASA 5540 シリーズのアプライアンスでは、それよりはるかに多数のユーザをサポートできます。ASA 5540 適応型セキュリティ アプライアンスに CSC SSM を導入する場合は、スキャン対象のトラフィックに対してのみ CSC SSM が送信されるようにセキュリティ アプライアンスを設定してください。スキャンするトラフィックを決定するためのガイドラインについては、P.19-13 の「CSC SSM を通過する接続の制限」を参照してください。

## VPN 仕様

この項では、セキュリティ アプライアンスの VPN 仕様について説明します。ここでは、次の項目について説明します。

- [Cisco VPN クライアント サポート \(P.A-7\)](#)
- [Cisco Secure Desktop のサポート \(P.A-7\)](#)
- [サイトツーサイト VPN 互換性 \(P.A-7\)](#)
- [暗号化標準 \(P.A-8\)](#)

### Cisco VPN クライアント サポート

セキュリティ アプライアンスは、[表 A-4](#) に示されているように、広範なソフトウェアおよびハードウェアベースの Cisco VPN クライアントをサポートしています。

**表 A-4 Cisco VPN クライアント サポート**

| クライアント タイプ                                      | クライアント バージョン                                      |
|-------------------------------------------------|---------------------------------------------------|
| SSL VPN クライアント                                  | Cisco SSL VPN client バージョン 1.1 以降                 |
| ソフトウェア IPSec VPN クライアント                         | Cisco VPN client for Windows バージョン 3.6 以降         |
|                                                 | Cisco VPN client for Linux バージョン 3.6 以降           |
|                                                 | Cisco VPN client for Solaris バージョン 3.6 以降         |
|                                                 | Cisco VPN client for Mac OS X バージョン 3.6 以降        |
| ハードウェア IPSec VPN クライアント (Cisco Easy VPN remote) | Cisco VPN 3002 hardware client バージョン 3.0 以降       |
|                                                 | Cisco IOS Software Easy VPN remote リリース 12.2(8)YJ |
|                                                 | Cisco PIX 500 シリーズ セキュリティ アプライアンス バージョン 6.2 以降    |
|                                                 | Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス バージョン 7.0 以降 |

### Cisco Secure Desktop のサポート

セキュリティ アプライアンスでは、CSD ソフトウェアのバージョン 3.1.1.16 をサポートしています。

### サイトツーサイト VPN 互換性

多数のサードパーティ VPN 製品に対する相互運用性に加え、セキュリティ アプライアンスは、[表 A-5](#) に示されているサイトツーサイト VPN 接続用の Cisco VPN 製品との相互運用性を提供します。

**表 A-5 サイトツーサイト VPN 互換性**

| プラットフォーム                             | ソフトウェア バージョン     |
|--------------------------------------|------------------|
| Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス | バージョン 7.0(1) 以降  |
| Cisco IOS ルータ                        | リリース 12.1(6)T 以降 |
| Cisco PIX 500 シリーズ セキュリティ アプライアンス    | バージョン 5.1(1) 以降  |
| Cisco VPN 3000 シリーズ コンセントレータ         | バージョン 3.6(1) 以降  |

## 暗号化標準

セキュリティ アプライアンスは、表 A-6 に示されているものを含め、多数の暗号化標準と、関連するサードパーティ製品およびサービスをサポートしています。

**表 A-6 暗号化標準**

| タイプ                                | 説明                                                                                                                                                  |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 非対称（公開キー）暗号化アルゴリズム                 | RSA 公開キー / 秘密キー ペア、512 ～ 4096 ビット<br>DSA 公開キー / 秘密キー ペア、512 ～ 1024 ビット                                                                              |
| 対称暗号化アルゴリズム                        | AES：128、192、および 256 ビット<br>DES：56 ビット<br>3DES：168 ビット<br>RC4：40、56、64、および 128 ビット                                                                   |
| 完全転送秘密（Diffie-Hellman キー ネゴシエーション） | Group 1：768 ビット<br>Group 2：1024 ビット<br>Group 5：1536 ビット<br>Group 7：163 ビット（Elliptic Curve Diffie-Hellman）                                           |
| ハッシュ アルゴリズム                        | MD5：128 ビット<br>SHA-1：160 ビット                                                                                                                        |
| X.509 認証局                          | Cisco IOS ソフトウェア<br>Baltimore UniCERT<br>Entrust Authority<br>iPlanet/Netscape CMS<br>Microsoft Certificate Services<br>RSA Keon<br>VeriSign OnSite |
| X.509 証明書登録方法                      | SCEP<br>PKCS #7 および #10                                                                                                                             |



## 設定例

---

この付録では、セキュリティ アプライアンスを実装するいくつかの一般的な方法について、図を使用して説明します。次の事項を取り上げます。

- [例 1：外部アクセスのあるマルチモード ファイアウォール \(P.B-2\)](#)
- [例 2：同じセキュリティ レベルを使用したシングルモード ファイアウォール \(P.B-6\)](#)
- [例 3：マルチコンテキストの共有リソース \(P.B-8\)](#)
- [例 4：外部アクセスのあるマルチモード、透過ファイアウォール \(P.B-13\)](#)
- [例 5：WebVPN コンフィギュレーション \(P.B-17\)](#)

フェールオーバーの例は、[第 11 章「フェールオーバー コンフィギュレーションの例」](#)を参照してください。

## 例 1：外部アクセスのあるマルチモード ファイアウォール

このコンフィギュレーションでは、3つのセキュリティ コンテキストに加え、管理コンテキストを作成します。各コンテキストは、内部インターフェイスと外部インターフェイスを持ちます。顧客 C コンテキストには DMZ インターフェイスが含まれています。この DMZ インターフェイスでは、HTTP フィルタリング用の Websense サーバがサービス プロバイダー社内にあります（図 B-1 を参照）。

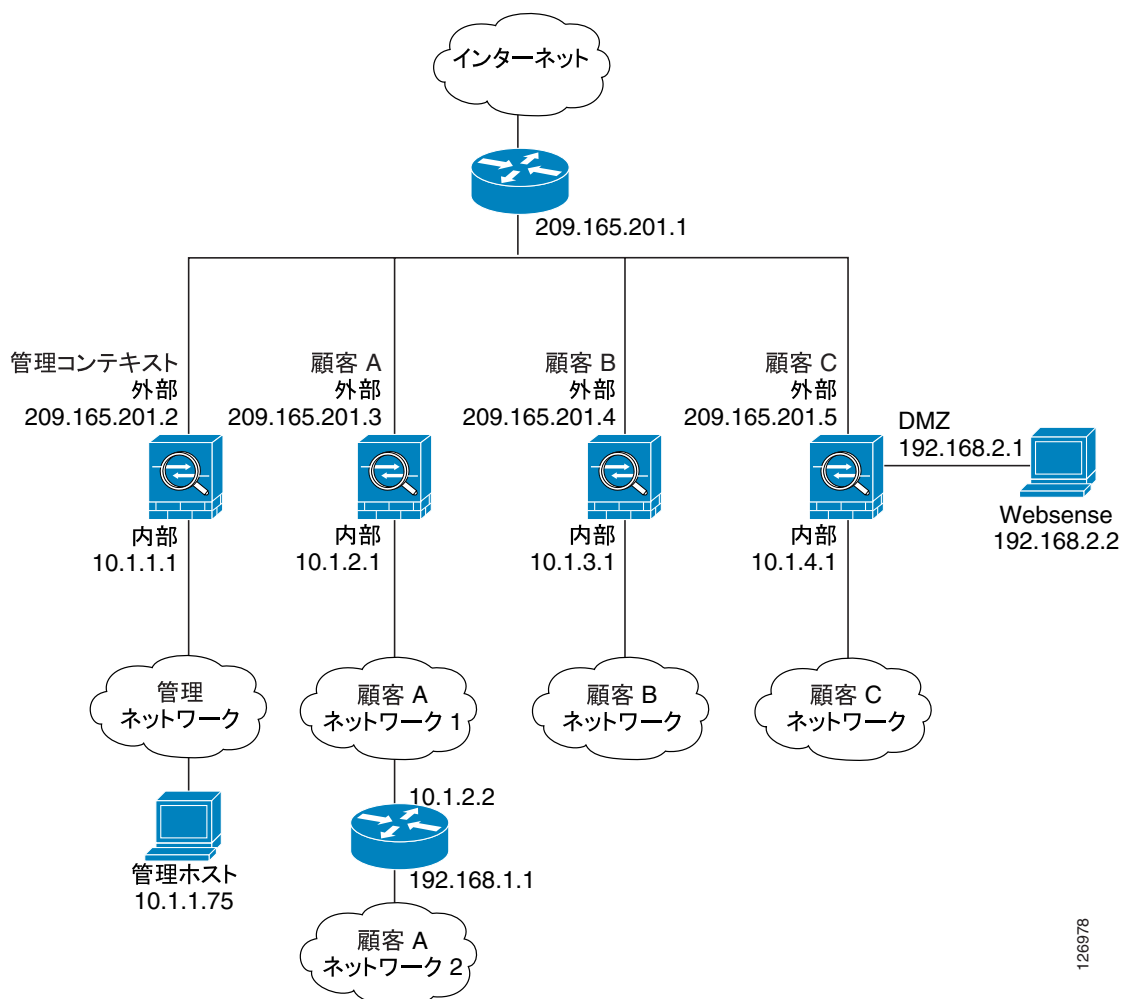
内部ホストはダイナミック NAT または PAT を使用して外部を通じインターネットにアクセスすることができますが、外部ホストは内部にアクセスできません。

顧客 A コンテキストは内部ルータの背後に 2 番目のネットワークを持っています。

管理コンテキストは、1 台のホストからセキュリティ アプライアンスへの SSH セッションを許可します。

インターフェイスが固有である場合、内部 IP アドレスはコンテキスト間で同一にすることができますが、それぞれを固有にした方が管理が容易です。

図 B-1 例 1



126978

この事例のコンフィギュレーションについては、次の項を参照してください。

- [例 1：システム コンフィギュレーション \(P.B-3\)](#)
- [例 1：管理コンテキスト コンフィギュレーション \(P.B-4\)](#)
- [例 1：顧客 A コンテキスト コンフィギュレーション \(P.B-4\)](#)
- [例 1：顧客 B コンテキスト コンフィギュレーション \(P.B-5\)](#)
- [例 1：顧客 C コンテキスト コンフィギュレーション \(P.B-5\)](#)

## 例 1：システム コンフィギュレーション

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する必要があります。モードはリブートしても保持されますが、コンフィギュレーション ファイルには保存されません。**write terminal**、**show startup-config**、または **show running-config** コマンドを使用してセキュリティ アプライアンスでコンフィギュレーションを表示した場合、モードはセキュリティ アプライアンスのバージョンの後ろに表示されます（空白はシングルモードを意味し、「<system>」はシステム コンフィギュレーションでのマルチモードを意味し、<context> はコンテキストでのマルチモードを意味します）。

```
hostname Farscape
password passw0rd
enable password chr1cht0n
admin-context admin
interface gigabitethernet 0/0
    shutdown
interface gigabitethernet 0/0.3
    vlan 3
    no shutdown
interface gigabitethernet 0/1
    no shutdown
interface gigabitethernet 0/1.4
    vlan 4
    no shutdown
interface gigabitethernet 0/1.5
    vlan 5
    no shutdown
interface gigabitethernet 0/1.6
    vlan 6
    no shutdown
interface gigabitethernet 0/1.7
    vlan 7
    no shutdown
interface gigabitethernet 0/1.8
    vlan 8
    no shutdown
context admin
    allocate-interface gigabitethernet 0/0.3
    allocate-interface gigabitethernet 0/1.4
    config-url disk0://admin.cfg
context customerA
    description This is the context for customer A
    allocate-interface gigabitethernet 0/0.3
    allocate-interface gigabitethernet 0/1.5
    config-url disk0://contexta.cfg
context customerB
    description This is the context for customer B
    allocate-interface gigabitethernet 0/0.3
    allocate-interface gigabitethernet 0/1.6
    config-url disk0://contextb.cfg
context customerC
    description This is the context for customer C
    allocate-interface gigabitethernet 0/0.3
    allocate-interface gigabitethernet 0/1.7-gigabitethernet 0/1.8
    config-url disk0://contextc.cfg
```

## 例 1：管理コンテキスト コンフィギュレーション

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します。そのためには、**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。

```
hostname Admin
domain isp
interface gigabitethernet 0/0.3
    nameif outside
    security-level 0
    ip address 209.165.201.2 255.255.255.224
    no shutdown
interface gigabitethernet 0/1.4
    nameif inside
    security-level 100
    ip address 10.1.1.1 255.255.255.0
    no shutdown
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, so
! 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
```

## 例 1：顧客 A コンテキスト コンフィギュレーション

```
interface gigabitethernet 0/0.3
    nameif outside
    security-level 0
    ip address 209.165.201.3 255.255.255.224
    no shutdown
interface gigabitethernet 0/1.5
    nameif inside
    security-level 100
    ip address 10.1.2.1 255.255.255.0
    no shutdown
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
```



## 例 1：顧客 B コンテキスト コンフィギュレーション

```
interface gigabitethernet 0/0.3
  nameif outside
  security-level 0
  ip address 209.165.201.4 255.255.255.224
  no shutdown
interface gigabitethernet 0/1.6
  nameif inside
  security-level 100
  ip address 10.1.3.1 255.255.255.0
  no shutdown
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
```

## 例 1：顧客 C コンテキスト コンフィギュレーション

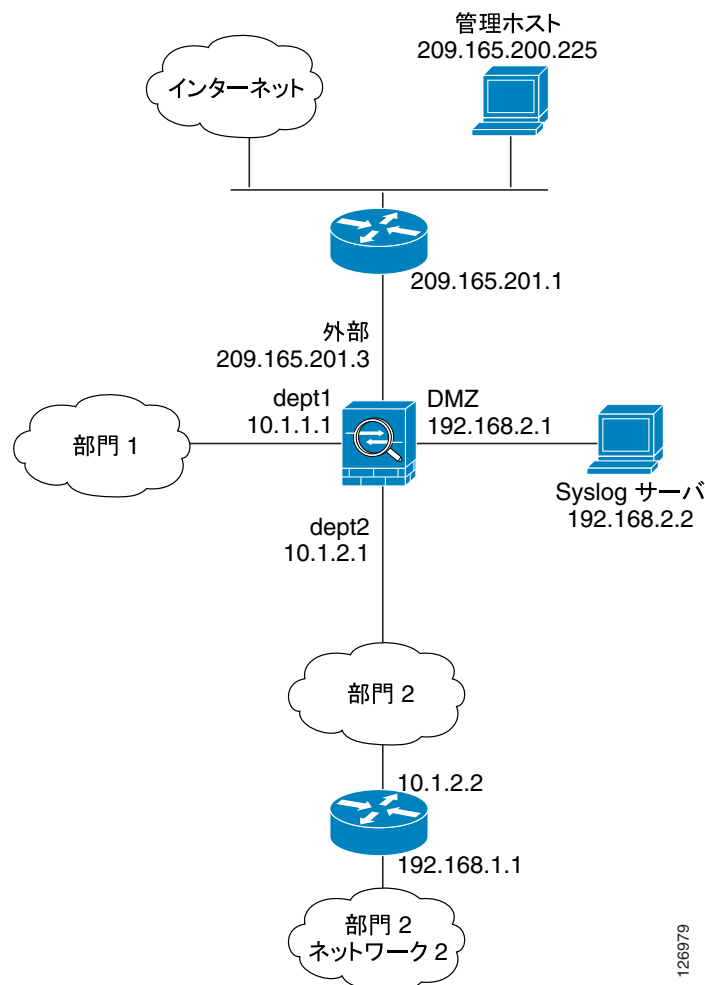
```
interface gigabitethernet 0/0.3
  nameif outside
  security-level 0
  ip address 209.165.201.5 255.255.255.224
  no shutdown
interface gigabitethernet 0/1.7
  nameif inside
  security-level 100
  ip address 10.1.4.1 255.255.255.0
  no shutdown
interface gigabitethernet 0/1.8
  nameif dmz
  security-level 50
  ip address 192.168.2.1 255.255.255.0
  no shutdown
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, the security appliance 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 MANAGE remark Allows the management host to use pcAnywhere on the 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
```

## 例 2：同じセキュリティ レベルを使用したシングルモード ファイアウォール

このコンフィギュレーションでは、3つの内部インターフェイスを作成します。2つのインターフェイスは同じセキュリティレベルの部門に接続します。これにより、すべてのホストがアクセスリストを使用せずに通信できます。DMZ インターフェイスは Syslog サーバをホスティングします。外部インターフェイス上の管理ホストは、Syslog サーバとセキュリティ アプライアンスにアクセスする必要があります。セキュリティ アプライアンスに接続するため、ホストは VPN 接続を使用します。セキュリティ アプライアンスは内部インターフェイス上の RIP を使用してルートを認識します。セキュリティ アプライアンスはルートを RIP でアドバタイズしないので、アップストリームルータはセキュリティ アプライアンス トラフィック用のスタティック ルートを使用する必要があります（図 B-2 を参照）。

部門ネットワークは、インターネットへのアクセスと PAT の使用を許可されています。

図 B-2 例 2



```
interface gigabitethernet 0/0
  nameif outside
  security-level 0
  ip address 209.165.201.3 255.255.255.224
  no shutdown
```

```

interface gigabitethernet 0/1
    nameif dept2
    security-level 100
    ip address 10.1.2.1 255.255.255.0
    no shutdown
interface gigabitethernet 0/2
    nameif dept1
    security-level 100
    ip address 10.1.1.1 255.255.255.0
    no shutdown
interface gigabitethernet 0/3
    nameif dmz
    security-level 50
    ip address 192.168.2.1 255.255.255.0
    no shutdown
passwd g00fball
enable password genlu$
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 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 security appliance IP address as the default gateway for the
downstream
! router. The security appliance 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. The security appliance 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 security appliance 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 on

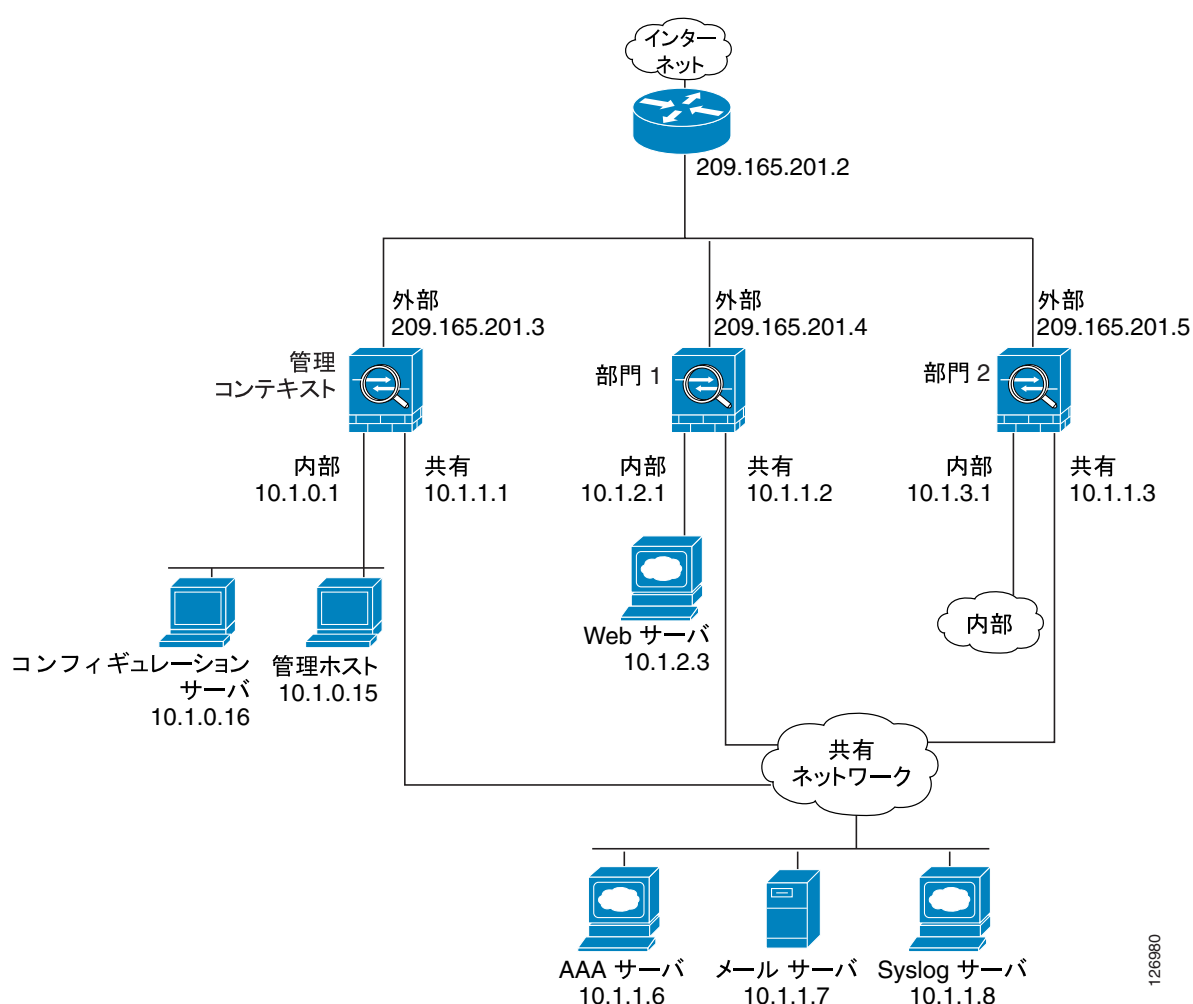
```

## 例 3：マルチコンテキストの共有リソース

このコンフィギュレーションには、社内の複数の部門用のマルチコンテキストが含まれています。それぞれの部門が独自のセキュリティ ポリシーを持つことができるように、各部門には独自のセキュリティ コンテキストがあります。ただし、syslog サーバ、メール サーバ、および AAA サーバはすべての部門で共有されます。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 サーバで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



この事例のコンフィギュレーションについては、次の項を参照してください。

- [例 3：システム コンフィギュレーション（P.B-9）](#)
- [例 3：管理コンテキスト コンフィギュレーション（P.B-10）](#)
- [例 3：部門 1 コンテキスト コンフィギュレーション（P.B-11）](#)
- [例 3：部門 2 コンテキスト コンフィギュレーション（P.B-12）](#)

## 例 3：システム コンフィギュレーション

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する必要があります。モードはリブートしても保持されますが、コンフィギュレーション ファイルには保存されません。**write terminal**、**show startup-config**、または **show running-config** コマンドを使用してセキュリティ アプライアンスでコンフィギュレーションを表示した場合、モードはセキュリティ アプライアンスのバージョンの後ろに表示されます（空白はシングルモードを意味し、「<system>」はシステム コンフィギュレーションでのマルチモードを意味し、<context> はコンテキストでのマルチモードを意味します）。

```
hostname Ubik
password pkd55
enable password deckard69
admin-context admin
interface gigabitethernet 0/0
    no shutdown
interface gigabitethernet 0/0.200
    vlan 200
    no shutdown
interface gigabitethernet 0/1
    shutdown
interface gigabitethernet 0/1.201
    vlan 201
    no shutdown
interface gigabitethernet 0/1.202
    vlan 202
    no shutdown
interface gigabitethernet 0/1.300
    vlan 300
    no shutdown
context admin
    allocate-interface gigabitethernet 0/0.200
    allocate-interface gigabitethernet 0/1.201
    allocate-interface gigabitethernet 0/1.300
    config-url disk0://admin.cfg
context department1
    allocate-interface gigabitethernet 0/0.200
    allocate-interface gigabitethernet 0/1.202
    allocate-interface gigabitethernet 0/1.300
    config-url ftp://admin:passw0rd@10.1.0.16/dept1.cfg
context department2
    allocate-interface gigabitethernet 0/0.200
    allocate-interface gigabitethernet 0/1.203
    allocate-interface gigabitethernet 0/1.300
    config-url ftp://admin:passw0rd@10.1.0.16/dept2.cfg
```

## 例 3：管理コンテキスト コンフィギュレーション

```

hostname Admin
interface gigabitethernet 0/0.200
    nameif outside
    security-level 0
    ip address 209.165.201.3 255.255.255.224
    no shutdown
interface gigabitethernet 0/0.201
    nameif inside
    security-level 100
    ip address 10.1.0.1 255.255.255.0
    no shutdown
interface gigabitethernet 0/0.300
    nameif shared
    security-level 50
    ip address 10.1.1.1 255.255.255.0
    no shutdown
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 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
aaa authorization command AAA-SERVER LOCAL
aaa accounting command 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

```

## 例 3：部門 1 コンテキスト コンフィギュレーション

```
interface gigabitethernet 0/0.200
  nameif outside
  security-level 0
  ip address 209.165.201.4 255.255.255.224
  no shutdown
interface gigabitethernet 0/0.202
  nameif inside
  security-level 100
  ip address 10.1.2.1 255.255.255.0
  no shutdown
interface gigabitethernet 0/0.300
  nameif shared
  security-level 50
  ip address 10.1.1.2 255.255.255.0
  no shutdown
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 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
```

### 例 3：部門 2 コンテキスト コンフィギュレーション

```
interface gigabitethernet 0/0.200
  nameif outside
  security-level 0
  ip address 209.165.201.5 255.255.255.224
  no shutdown
interface gigabitethernet 0/0.203
  nameif inside
  security-level 100
  ip address 10.1.3.1 255.255.255.0
  no shutdown
interface gigabitethernet 0/0.300
  nameif shared
  security-level 50
  ip address 10.1.1.3 255.255.255.0
  no shutdown
passwd mazlrlan
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 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
```



## 例 4：外部アクセスのあるマルチモード、透過ファイアウォール

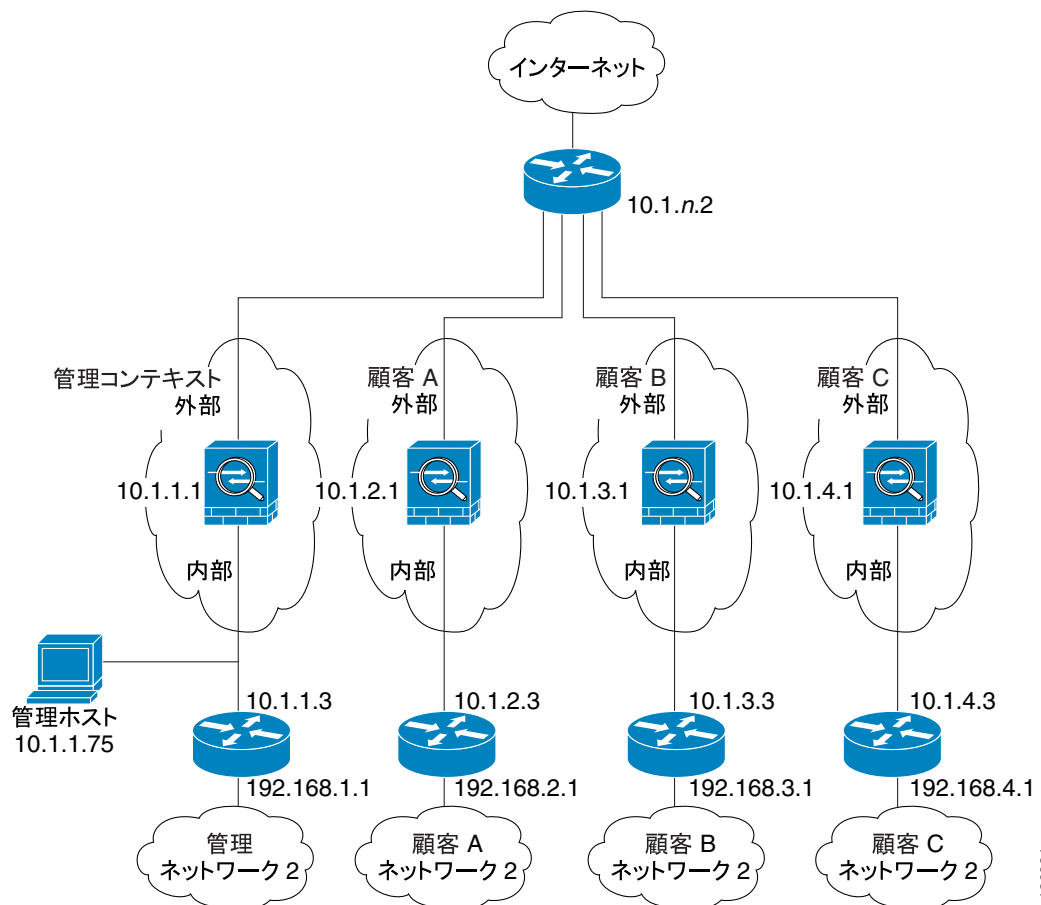
このコンフィギュレーションでは、3つのセキュリティ コンテキストに加え、管理コンテキストを作成します。各コンテキストは、内部ルータと外部ルータの間で OSPF トラフィックの通過を許可します（図 B-4 を参照）。

内部ホストは外部を介して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。

管理コンテキストは、1 台のホストからセキュリティ アプライアンスへの SSH セッションを許可します。

内部 IP アドレスはコンテキスト間で同一にすることができますが、それぞれを固有にした方が管理が容易です。

図 B-4 例 4



この事例のコンフィギュレーションについては、次の項を参照してください。

- 例 4：システム コンフィギュレーション (P.B-14)
- 例 4：管理コンテキスト コンフィギュレーション (P.B-15)
- 例 4：顧客 A コンテキスト コンフィギュレーション (P.B-15)
- 例 4：顧客 B コンテキスト コンフィギュレーション (P.B-15)
- 例 4：顧客 C コンテキスト コンフィギュレーション (P.B-16)

## 例 4：システム コンフィギュレーション

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する必要があります。モードはリブートしても保持されますが、コンフィギュレーション ファイルには保存されません。**write terminal**、**show startup-config**、または **show running-config** コマンドを使用してセキュリティ アプライアンスでコンフィギュレーションを表示した場合、モードはセキュリティ アプライアンスのバージョンの後ろに表示されます（空白はシングルモードを意味し、「<system>」はシステム コンフィギュレーションでのマルチモードを意味し、<context> はコンテキストでのマルチモードを意味します）。

```
firewall transparent
hostname Farscape
password passw0rd
enable password chr1cht0n
admin-context admin
interface gigabitethernet 0/0
    no shutdown
interface gigabitethernet 0/0.150
    vlan 150
    no shutdown
interface gigabitethernet 0/0.151
    vlan 151
    no shutdown
interface gigabitethernet 0/0.152
    vlan 152
    no shutdown
interface gigabitethernet 0/0.153
    vlan 153
    no shutdown
interface gigabitethernet 0/1
    shutdown
interface gigabitethernet 0/1.4
    vlan 4
    no shutdown
interface gigabitethernet 0/1.5
    vlan 5
    no shutdown
interface gigabitethernet 0/1.6
    vlan 6
    no shutdown
interface gigabitethernet 0/1.7
    vlan 7
    no shutdown
context admin
    allocate-interface gigabitethernet 0/0.150
    allocate-interface gigabitethernet 0/1.4
    config-url disk0://admin.cfg
context customerA
    description This is the context for customer A
    allocate-interface gigabitethernet 0/0.151
    allocate-interface gigabitethernet 0/1.5
    config-url disk0://contexta.cfg
context customerB
    description This is the context for customer B
    allocate-interface gigabitethernet 0/0.152
    allocate-interface gigabitethernet 0/1.6
    config-url disk0://contextb.cfg
context customerC
    description This is the context for customer C
    allocate-interface gigabitethernet 0/0.153
    allocate-interface gigabitethernet 0/1.7
    config-url disk0://contextc.cfg
```

## 例 4：管理コンテキスト コンフィギュレーション

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します。そのためには、**crypto key generate** コマンドを使用してキー ペアを生成する必要があります。

```
hostname Admin
domain isp
interface gigabitethernet 0/0.150
    nameif outside
    security-level 0
    no shutdown
interface gigabitethernet 0/1.4
    nameif inside
    security-level 100
    no shutdown
passwd secret1969
enable password hlandl0
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
access-list OSPF remark -Allows OSPF
access-list OSPF extended permit 89 any any
access-group OSPF in interface outside
```

## 例 4：顧客 A コンテキスト コンフィギュレーション

```
interface gigabitethernet 0/0.151
    nameif outside
    security-level 0
    no shutdown
interface gigabitethernet 0/1.5
    nameif inside
    security-level 100
    no shutdown
passwd hell0!
enable password enter55
ip address 10.1.2.1 255.255.255.0
route outside 0 0 10.1.2.2 1
access-list OSPF remark -Allows OSPF
access-list OSPF extended permit 89 any any
access-group OSPF in interface outside
```

## 例 4：顧客 B コンテキスト コンフィギュレーション

```
interface gigabitethernet 0/0.152
    nameif outside
    security-level 0
    no shutdown
interface gigabitethernet 0/1.6
    nameif inside
    security-level 100
    no shutdown
passwd tenac10us
enable password defen$e
ip address 10.1.3.1 255.255.255.0
route outside 0 0 10.1.3.2 1
access-list OSPF remark -Allows OSPF
access-list OSPF extended permit 89 any any
access-group OSPF in interface outside
```

## 例 4：顧客 C コンテキスト コンフィギュレーション

```
interface gigabitethernet 0/0.153
  nameif outside
  security-level 0
  no shutdown
interface gigabitethernet 0/1.7
  nameif inside
  security-level 100
  no shutdown
passwd fl0wer
enable password treeh0u$e
ip address 10.1.4.1 255.255.255.0
route outside 0 0 10.1.4.2 1
access-list OSPF remark -Allows OSPF
access-list OSPF extended permit 89 any any
access-group OSPF in interface outside
```

## 例 5 : WebVPN コンフィギュレーション

このコンフィギュレーションは、セキュリティ アプライアンスへの WebVPN 接続を作成するために必要なコマンドを示しています。

WebVPN によってユーザは、ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモートアクセス VPN トンネルを確立できます。ソフトウェア クライアントもハードウェア クライアントも必要ありません。WebVPN を使用することで、HTTP(S) インターネット サイトにアクセスできるほとんどすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできます。WebVPN は Secure Sockets Layer (SSL) プロトコルおよびその後継である Transport Layer Security (SSL/TLS1) を使用して、リモート ユーザと、中央サイトで設定した特定のサポートされている内部リソースとの間で、セキュアな接続を提供します。セキュリティ アプライアンスはプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

### ステップ 1 WebVPN に対してセキュリティ アプライアンスを設定します。

```
webvpn
! WebVPN sessions are allowed on the outside and dmz1 interfaces, ASDM is not allowed.
enable outside
enable dmz161
title-color green
secondary-color 200,160,0
text-color black
default-idle-timeout 3600
! The NetBios Name server used for CIFS resolution.
nbns-server 172.31.122.10 master timeout 2 retry 2
accounting-server-group RadiusACS1
! WebVPN sessions are authenticated to a RADIUS aaa server.
authentication-server-group RadiusACS2
```

### ステップ 2 WebVPN アクセスリストをグループポリシーまたはユーザ ポリシーで実施できるようにする必要があります。アクセスリストは、グループ コンフィギュレーションまたはユーザ コンフィギュレーションの **filter value** コマンドと **functions** コマンドで定義されます。

```
access-list maia2 remark -deny access to url and send a syslog every 300 seconds
access-list maia2 remark -containing the hit-count (how many times the url was
accessed)
access-list maia2 webtype deny url https://sales.example.com log informational
interval 300
access-list maia2 remark -Permits access to the URL.
access-list maia2 webtype permit url http://employee-connection.example.com
access-list maia2 remark -Permits access to the site using ssh.
access-list maia2 remark -To be enforced via Port-Forwarding application.
access-list maia2 webtype permit tcp asa-35.example.com 255.255.255.255 eq ssh
access-list maia2 remark -Denies access to the application on port 1533.
access-list maia2 webtype deny tcp im.example.com 255.255.255.255 eq 1533
access-list maia2 remark -Permits access to files on this file share via
access-list maia2 remark -WebVPN Common Internet File System (CIFS).
access-list maia2 webtype permit url cifs://server-bos/people/mkting log informational
3600
```

## 例 5: WebVPN コンフィギュレーション

**ステップ 3** ログイン後、WebVPN ユーザのホーム ページに示されている事前設定の URL のリストを設定することができます。これは、ユーザまたはグループごとに定義されています。

```
url-list HomeURL "Sales" https://sales.example.com
url-list HomeURL "VPN3000-1" http://vpn3k-1.example.com
url-list HomeURL "OWA-2000" http://10.160.105.2/exchange
url-list HomeURL "Exchange5.5" http://10.86.195.113/exchange
url-list HomeURL " Employee Benefits" http://benefits.example.com
url-list HomeURL "Calendar" http://http://eng.example.com/cal.html
```

**ステップ 4** WebVPN でポート転送され、ユーザまたはグループポリシーごとに実施される非 Web TCP アプリケーションのリストを設定します。これらはグローバルに定義されますが、ユーザまたはグループポリシーごとに実施できます。

```
port-forward Appsl 4001 10.148.1.81 telnet term-servr
port-forward Appsl 4008 router1-example.com ssh
port-forward Appsl 10143 flask.example.com imap4
port-forward Appsl 10110 flask.example.com pop3
port-forward Appsl 10025 flask.example.com smtp
port-forward Appsl 11533 sametime-im.example.com 1533
port-forward Appsl 10022 secure-term.example.com ssh
port-forward Appsl 21666 tuscan.example.com 1666 perforce-fl
port-forward Appsl 1030 sales.example.com https
```

**ステップ 5** SSLVPNusers グループポリシーのユーザに対して実施するポリシー アトリビュートを設定します。

```
group-policy SSLVPNusers internal
group-policy SSLVPNusers attributes
  banner value Welcome to Web Services !!!
  vpn-idle-timeout 2
  vpn-tunnel-protocol IPSec webvpn
  webvpn
    functions url-entry file-access file-entry file-browsing port-forward filter
    url-list value HomeURL
    port-forward value Appsl
```

**ステップ 6** 次に、ASDM および WebVPN HTTPS セッションが終了するインターフェイスを設定します。同一インターフェイスでの ASDM/WebVPN の併用はサポートされていません。

```
! Enables the HTTP server to allow ASDM and WebVPN HTTPS sessions.
http server enable
! Allows ASDM session(s) from host 10.20.30.47 on the inside interface ; WebVPN
sessions
! are not allowed on this interface.
http 10.10.10.45 inside
! Allows WebVPN sessions on outside interfce using HTTP to be re-directed to HTTPS.
! ASDM session is not allowed on this interface.
http redirect outside 80
! Allows WebVPN sessions on dmz1 interfce using HTTP to be re-directed to HTTPS.
! ASDM session is not allowed on this interface.
http redirect dmz161 80
```

**ステップ 7** 次に、3DES-sha1 暗号化を使用して、セキュリティ アプライアンスでの HTTPS ASDM および WebVPN セッションの終了を許可します。適切な 3DES アクティベーション キーが事前にインストールされている必要があります。

```
ssl encryption 3des-sha1
ssl trust-point CA-MS inside
```

**ステップ 8** 最後に、電子メール プロキシを設定します。

```
imap4s
  enable outside
  enable inside
  enable dmz161
  default-group-policy DfltGrpPolicy
pop3s
  enable outside
  enable inside
  enable dmz161
  default-group-policy DfltGrpPolicy
smtps
  enable outside
  enable inside
  enable dmz161
  default-group-policy DfltGrpPolicy
```

---

## ■ 例 5 : WebVPN コンフィギュレーション





# コマンドライン インターフェイスの使用

この付録では、セキュリティ アプライアンスでの CLI の使用方法について説明します。この章には、次の項があります。

- [ファイアウォール モードとセキュリティ コンテキスト モード \(P.C-2\)](#)
- [コマンドのモードとプロンプト \(P.C-3\)](#)
- [シンタックスの書式 \(P.C-4\)](#)
- [コマンドの省略形 \(P.C-4\)](#)
- [コマンドラインの編集 \(P.C-4\)](#)
- [コマンドの完成 \(P.C-5\)](#)
- [コマンドのヘルプ \(P.C-5\)](#)
- [show コマンド出力のフィルタリング \(P.C-6\)](#)
- [コマンド出力のページング \(P.C-7\)](#)
- [コメントの追加 \(P.C-7\)](#)
- [テキスト コンフィギュレーション ファイル \(P.C-8\)](#)



(注)

CLI は、Cisco IOS CLI と類似したシンタックスおよび異なる表記法を使用しますが、セキュリティ アプライアンスのオペレーティング システムが、Cisco IOS ソフトウェアのバージョンの 1 つとは限りません。Cisco IOS CLI コマンドは、セキュリティ アプライアンスで動作する、またはセキュリティ アプライアンスと同じ機能を持っているとは限らないことに注意してください。

## ファイアウォール モードとセキュリティ コンテキスト モード

セキュリティ アプライアンスは、次のモードの組み合わせで動作します。

- 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 モードは、セキュリティ アプライアンスがレイヤ 2 ファイアウォールまたはレイヤ 3 ファイアウォールとして動作するかどうかを決定します。
- マルチコンテキスト モードまたはシングルコンテキスト モード  
セキュリティ コンテキスト モードは、セキュリティ アプライアンスが単一のデバイスとして動作するか、またはマルチセキュリティ コンテキストとして動作する（仮想デバイスのように動作する）かを決定します。

特定のモードでしか使用できないコマンドもあります。

## コマンドのモードとプロンプト

セキュリティ アプライアンスの CLI にはコマンド モードが含まれています。特定のモードでしか入力できないコマンドもあります。たとえば、機密情報を表示するコマンドを入力するには、パスワードを入力して特権モードに入る必要があります。次に、コンフィギュレーション変更が誤って入力されないようにするために、コンフィギュレーション モードに入る必要があります。下位のコマンドはすべて、高位のモードで入力できます。たとえば、グローバル コンフィギュレーション モードで特権 EXEC コマンドを入力することができます。

システム コンフィギュレーション モードまたはシングルコンテキスト モードに入っている場合、プロンプトはホスト名で始まります。

```
hostname
```

コンテキスト内に入っている場合、プロンプトはホスト名で始まり、その後にコンテキスト名が続きます。

```
hostname/context
```

プロンプトは、アクセス モードに応じて変化します。

- ユーザ EXEC モード

ユーザ EXEC モードでは、最小限のセキュリティ アプライアンス設定が表示されます。初めてセキュリティ アプライアンスにアクセスしたとき、ユーザ EXEC モード プロンプトは次のように表示されます。

```
hostname>
```

```
hostname/context>
```

- 特権 EXEC モード

特権 EXEC モードでは、ユーザの特権レベルまでの現在の設定がすべて表示されます。すべてのユーザ EXEC モード コマンドは、特権 EXEC モードで動作します。特権 EXEC モードを開始するには、ユーザ EXEC モードで **enable** コマンドを入力します。これにはパスワードが必要です。プロンプトにはシャープ記号 (#) が含まれています。

```
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、セキュリティ アプライアンス コンフィギュレーションを変更できます。このモードでは、ユーザ EXEC、特権 EXEC、およびグローバル コンフィギュレーションのコマンドをすべて使用できます。グローバル コンフィギュレーション モードを開始するには、特権 EXEC モードで **configure terminal** コマンドを入力します。プロンプトが次のように変化します。

```
hostname(config)#
```

```
hostname/context(config)#
```

- コマンド固有のコンフィギュレーション モード

いくつかのコマンドは、グローバル コンフィギュレーション モードから、コマンド固有のコンフィギュレーション モードに移行します。このモードでは、ユーザ EXEC、特権 EXEC、グローバル コンフィギュレーション、およびコマンド固有のコンフィギュレーションのコマンドをすべて使用できます。たとえば、**interface** コマンドを使用すると、インターフェイス コンフィギュレーション モードに入ります。プロンプトが次のように変化します。

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

```
hostname/context(config-if)#
```

## シンタックスの書式

コマンド シンタックスの説明では、次の表記法を使用しています。

表 C-1 シンタックスの表記法

| 表記法         | 説明                                                                                                       |
|-------------|----------------------------------------------------------------------------------------------------------|
| 太字          | 記載されているとおりに入力するコマンドおよびキーワードは、太字で示しています。                                                                  |
| イタリック体      | ユーザが値を指定する引数は、イタリック体で示しています。                                                                             |
| [x]         | 省略可能な要素(キーワードまたは引数)は、角カッコで囲んで示しています。                                                                     |
|             | 省略可能または必須のキーワードや引数の中から選択する場合は、縦棒で区切って示しています。                                                             |
| [x   y]     | どれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。                                                       |
| {x   y}     | 必ずどれか 1 つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。                                                  |
| [x {y   z}] | 省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。 |

## コマンドの省略形

ほとんどのコマンドは、コマンドに固有の最小文字数まで短縮できます。たとえば、コンフィギュレーションを表示するには、完全なコマンド **write terminal** を入力する代わりに、**wr t** と入力できます。または、イネーブル モードを開始するには **en**、コンフィギュレーション モードを開始するには **conf t** と入力できます。さらに、**0** を入力して、**0.0.0.0** を表すことができます。

## コマンドラインの編集

セキュリティ アプライアンスでは、Cisco IOS ソフトウェアと同じコマンドライン編集規則が使用されます。**show history** コマンドを使用して以前入力した全コマンドを表示することも、↑キーまたは **^p** コマンドで 1 つずつ前のコマンドを表示することもできます。前に入力したコマンドを確認したら、↓キーまたは **^n** コマンドでリスト内で前に進むことができます。再利用するコマンドに到達したら、そのコマンドを編集することも、**Enter** キーを押して実行することもできます。**^w** でカーソルの左側にある単語を削除することも、**^u** でカーソルのある行を消去することもできます。

セキュリティ アプライアンスでは、1 つのコマンドに 512 文字まで入力できます。512 文字を超えて入力した文字は無視されます。

## コマンドの完成

部分的なストリングを入力してからコマンドまたはキーワードを完成させるには、**Tab** キーを押します。セキュリティ アプライアンスは、部分的なストリングがコマンドまたはキーワード 1 つだけと一致する場合のみ、コマンドまたはキーワードを完成させます。たとえば、**s** と入力して **Tab** キーを押した場合は、一致するコマンドが複数あるため、セキュリティ アプライアンスはコマンドを完成させません。一方、**dis** と入力して **Tab** キーを押すと、コマンド **disable** が完成します。

## コマンドのヘルプ

次のコマンドを入力すると、コマンドラインからヘルプ情報を利用できます。

- **help** *command\_name*  
特定のコマンドのヘルプを表示します。
- *command\_name* ?  
使用可能な引数のリストを表示します。
- *string*? (スペースなし)  
そのストリングで始まるコマンドをリストします。
- ? および +?  
使用できるすべてのコマンドをリストします。? と入力すると、セキュリティ アプライアンスは現在のモードで使用できるコマンドだけを表示します。下位モードのコマンドも含め、使用できるすべてのコマンドを表示するには、+? と入力します。



(注)

コマンド ストリングに疑問符 (?) を組み込む場合は、誤って CLI ヘルプを起動しないよう、疑問符を入力する前に **Ctrl+V** キーを押す必要があります。

## show コマンド出力のフィルタリング

垂直バー (|) はどの **show** コマンドでも使用できます。これには、フィルタ オプションとフィルタリング式を組み込むことができます。フィルタリングは、Cisco IOS ソフトウェアと同様に、各出力行を正規表現と照合することによって行われます。選択するフィルタ オプションによって、正規表現に一致するすべての出力を含めたり除外したりできます。また、正規表現に一致する行で始まるすべての出力を表示することもできます。

**show** コマンドでフィルタリング オプションを使用する場合のシンタックスは、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の最初の垂直バー (|) は演算子であり、コマンド内に含める必要があります。この演算子は、**show** コマンドの出力をフィルタに誘導します。シンタックス ダイアグラムのその他の垂直バー (|) は、代替オプションを示しており、コマンドの一部ではありません。

**include** オプションを指定すると、正規表現に一致するすべての出力行が表示されます。**-v** を付けずに **grep** オプションを使用する場合も、同じ結果となります。**exclude** オプションを指定すると、正規表現に一致するすべての出力行が除外されます。**-v** を付けて **grep** オプションを使用する場合も、同じ結果となります。**begin** オプションを指定すると、正規表現に一致する行で始まるすべての出力行が表示されます。

**regexp** には、Cisco IOS の正規表現を指定します。正規表現は一重引用符または二重引用符で囲まれていません。したがって、末尾の空白スペースが正規表現の一部と解釈されるため、末尾の空白スペースに注意してください。

正規表現を作成する場合は、照合する任意の文字または数字を使用できます。また、正規表現で使用する特別な意味を持つキーボード文字もあります。表 C-2 に、特別な意味を持つキーボード文字を示します。

**表 C-2 正規表現での特殊文字の使用**

| 文字の種類  | 文字             | 特別な意味                                                                      |
|--------|----------------|----------------------------------------------------------------------------|
| ピリオド   | .              | 空白スペースを含め、任意の 1 文字と一致する。                                                   |
| アスタリスク | *              | パターンの 0 個以上のシーケンスと一致する。                                                    |
| プラス記号  | +              | パターンの 1 個以上のシーケンスと一致する。                                                    |
| 疑問符    | ? <sup>1</sup> | 0 個またはそれ以上のパターンと一致する。                                                      |
| カレット   | ^              | 入力文字列の先頭と一致する。                                                             |
| ドル記号   | \$             | 入力文字列の末尾と一致する。                                                             |
| 下線     | _              | カンマ (,), 左中カッコ ({), 右中カッコ (}), 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する。 |
| 角カッコ   | []             | 1 文字のパターンの範囲を指定する。                                                         |
| ハイフン   | -              | 範囲のエンド ポイントを区切る。                                                           |

1. 疑問符がヘルプ コマンドとして解釈されないよう、疑問符の前に **Ctrl+V** キーを押してください。

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 (\) を置いて特殊な意味を除去します。

## コマンド出力のページング

**help** または **?**、**show**、**show xlate** など、長いリストが出力されるコマンドでは、1 画面分ずつ表示して停止させるか、リストの最後まで表示させるかを決めることができます。**pager** コマンドを使用すると、画面上に表示する行数を選択して、その行数を表示した後に More プロンプトを表示するようにできます。

ページングがイネーブルになっているときには、次のプロンプトが表示されます。

```
<--- More --->
```

More プロンプトのシンタックスは、UNIX の **more** コマンドと似ています。

- 次の 1 画面分の情報を表示するには、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

行の先頭にコロン (:) を置いて、コメントを作成できます。しかし、コメントが表示されるのはコマンド ヒストリ バッファだけで、コンフィギュレーションには表示されません。したがって、コメントは、**show history** コマンドを使用するか、矢印キーを押して前のコマンドを取得することによって表示できますが、コンフィギュレーションには含まれないので、**write terminal** コマンドでは表示できません。

## テキスト コンフィギュレーション ファイル

この項では、セキュリティ アプライアンスにダウンロードできるテキスト コンフィギュレーション ファイルをフォーマットする方法について説明します。次の項目を取り上げます。

- テキスト ファイルでコマンドと行が対応する仕組み (P.C-8)
- コマンド固有のコンフィギュレーション モード コマンド (P.C-8)
- 自動テキスト入力 (P.C-8)
- 行の順序 (P.C-9)
- 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-9)
- パスワード (P.C-9)
- マルチセキュリティ コンテキスト ファイル (P.C-9)

### テキスト ファイルでコマンドと行が対応する仕組み

テキスト コンフィギュレーション ファイルには、このガイドで説明するコマンドに対応する行が含まれています。

例では、コマンドの前に CLI プロンプトがあります。次の例のプロンプトは、「hostname(config)#」です。

```
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、コマンドの入力を求めるプロンプトが表示されないで、プロンプトは省略されています。

```
context a
```

### コマンド固有のコンフィギュレーション モード コマンド

コマンド固有のコンフィギュレーション モード コマンドは、コマンドラインで入力されたときに、メイン コマンドの下に字下げして表示されます。テキスト ファイルの行は、コマンドがメイン コマンドのすぐ後に表示される限り、字下げする必要はありません。たとえば、次のテキストは字下げされていませんが、字下げしたテキストと同じように読み取られます。

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
    nameif outside
```

### 自動テキスト入力

コンフィギュレーションをセキュリティ アプライアンスにダウンロードすると、セキュリティ アプライアンスによっていくつかの行が自動的に挿入されます。たとえば、セキュリティ アプライアンスは、デフォルト設定のため、またはコンフィギュレーションが変更されたときのための行を挿入します。テキスト ファイルを作成するときは、これらの自動入力を行う必要はありません。



## 行の順序

ほとんどの場合、コマンドはファイル内で任意の順序に置くことができます。ただし、ACE などいくつかの行は表示された順に処理されるので、順序がアクセスリストの機能に影響する場合があります。その他のコマンドでも、順序の要件がある場合があります。たとえば、あるインターフェイスの名前を多数の後続コマンドが使用する場合は、そのインターフェイスの **nameif** コマンドをまず入力する必要があります。また、コマンド固有のコンフィギュレーション モードのコマンドは、メイン コマンドの直後に置く必要があります。

## テキスト コンフィギュレーションに含まれないコマンド

いくつかのコマンドは、コンフィギュレーションに行を挿入しません。たとえば、**show running-config** などのランタイム コマンドは、テキスト ファイル内に対応する行があります。

## パスワード

ログインパスワード、イネーブルパスワード、およびユーザパスワードは、コンフィギュレーションに保存される前に自動的に暗号化されます。たとえば、パスワード「cisco」の暗号化された形式は jMorNbK0514fadBh のようになります。コンフィギュレーション パスワードを暗号化された形式で別のセキュリティ アプライアンスにコピーすることはできますが、パスワードの暗号を自分で解除することはできません。

暗号を解除したパスワードをテキスト ファイルに入力すると、コンフィギュレーションをセキュリティ アプライアンスにコピーしたときに、セキュリティ アプライアンスはパスワードを自動的に暗号化しません。セキュリティ アプライアンスがパスワードを暗号化するのは、コマンドラインから **copy running-config startup-config** コマンドまたは **write memory** コマンドを使用して実行コンフィギュレーションを保存したときだけです。

## マルチセキュリティ コンテキスト ファイル

マルチセキュリティ コンテキスト では、コンフィギュレーション全体が次の複数の部分で構成されます。

- セキュリティ コンテキスト コンフィギュレーション
- コンテキストのリストなど、セキュリティ アプライアンスの基本設定を示すシステム コンフィギュレーション
- システム コンフィギュレーション用のネットワーク インターフェイスを提供する管理コンテキスト

システム コンフィギュレーションには、それ自体のインターフェイスまたはネットワーク設定は含まれていません。代わりに、システムは、ネットワーク リソースにアクセスする必要があるときに（サーバからコンテキストをダウンロードするときなど）、管理コンテキストとして指定されたコンテキストを使用します。

各コンテキストは、シングルコンテキスト モード コンフィギュレーションに似ています。システム コンフィギュレーションにはシステムのみのコマンド（全コンテキストのリストなど）が含まれており、その他の一般的なコマンド（多数のインターフェイス パラメータなど）は存在しない点で、システム コンフィギュレーションは、コンテキスト コンフィギュレーションとは異なっています。





# アドレス、プロトコル、およびポート

---

この付録では、IP アドレス、プロトコル、およびアプリケーションのクイック リファレンスを提供します。この付録では、次の項目について説明します。

- [IPv4 アドレスとサブネット マスク \(P.D-2\)](#)
- [IPv6 アドレス \(P.D-6\)](#)
- [プロトコルとアプリケーション \(P.D-13\)](#)
- [TCP ポートと UDP ポート \(P.D-14\)](#)
- [ローカル ポートとプロトコル \(P.D-17\)](#)
- [ICMP タイプ \(P.D-18\)](#)

## IPv4 アドレスとサブネット マスク

この項では、セキュリティ アプライアンスで IPv4 アドレスを使用する方法について説明します。IPv4 アドレスはドット付き 10 進数表記の 32 ビットの数値であり、バイナリから 10 進数に変換されドットで区切られた 4 つの 8 ビット フィールド（オクテット）で構成されます。IP アドレスの最初の部分はホストが常駐するネットワークを示し、2 番目の部分は所定のネットワーク上の特定のホストを示します。ネットワーク番号フィールドは、ネットワーク プレフィックスと呼ばれます。所定のネットワーク上のホストはすべて、同じネットワーク プレフィックスを共有しますが、固有のホスト番号を持つ必要があります。クラスフル IP では、アドレスのクラスがネットワーク プレフィックスとホスト番号の間の境界を決定します。

ここでは、次の項目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、Class A、Class B、および Class C の 3 つの異なるアドレス クラスに分割されます。各クラスは、32 ビット アドレス内の異なるポイントで、ネットワーク プレフィックスとホスト番号の間の境界を修正します。Class D アドレスは、マルチキャスト IP 用に予約されています。

- Class A アドレス (1.xxx.xxx.xxx ~ 126.xxx.xxx.xxx) は、最初のオクテットだけをネットワーク プレフィックスとして使用します。
- Class B アドレス (128.0.xxx.xxx ~ 191.255.xxx.xxx) は、最初の 2 つのオクテットをネットワーク プレフィックスとして使用します。
- Class C アドレス (192.0.0.xxx ~ 223.255.255.xxx) は、最初の 3 つのオクテットをネットワーク プレフィックスとして使用します。

Class A アドレスには 16,777,214 個のホスト アドレス、Class B アドレスには 65,534 個のホストがあるので、サブネット マスクを使用してこれらの膨大なネットワークを小さいサブネットに分割することができます。

### プライベート ネットワーク

ネットワーク上に多数のアドレスが必要な場合、それらをインターネットでルーティングする必要がないときは、Internet Assigned Numbers Authority (IANA; インターネット割り当て番号局) が推奨するプライベート IP アドレスを使用できます (RFC 1918 を参照)。次のアドレス範囲が、アドバタイズされないプライベート ネットワークとして指定されています。

- 10.0.0.0 ~ 10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0 ~ 192.168.255.255

## サブネット マスク

サブネット マスクを使用すると、Class A、B、または C の単一のネットワークを複数のネットワークに変換できます。サブネット マスクを使用して、ホスト番号からネットワーク プレフィックスにビットを追加する拡張ネットワーク プレフィックスを作成することができます。たとえば、Class C ネットワーク プレフィックスは常に、IP アドレスの最初の 3 つのオクテットで構成されます。一方、Class C 拡張ネットワーク プレフィックスは、4 番目のオクテットの一部も使用します。

ドット付き 10 進数の代わりにバイナリ表記を使用している場合は、サブネット マスクを容易に理解できます。サブネット マスク内のビットには、インターネット アドレスとの 1 対 1 の対応関係があります。

- IP アドレス内の対応するビットが拡張ネットワーク プレフィックスの一部である場合、ビットは 1 に設定されます。
- ビットがホスト番号の一部である場合、ビットは 0 に設定されます。

**例 1：**Class B アドレスが 129.10.0.0 の場合に 3 番目のオクテット全体をホスト番号ではなく拡張ネットワーク プレフィックスとして使用するには、サブネット マスクとして 11111111.11111111.11111111.00000000 を指定する必要があります。このサブネット マスクによって、Class B アドレスは、ホスト番号が最後のオクテットだけで構成される Class C アドレスに相当するものに変換されます。

**例 2：**3 番目のオクテットの一部だけを拡張ネットワーク プレフィックスに使用する場合は、11111111.11111111.11111000.00000000 のようなサブネット マスクを指定する必要があります。ここでは、3 番目のオクテットのうち 5 ビットだけが拡張ネットワーク プレフィックスに使用されます。

サブネット マスクは、ドット付き 10 進数マスクまたは / ビット（「スラッシュ ビット」）マスクとして記述できます。例 1 では、ドット付き 10 進数マスクに対して、各バイナリ オクテットを 10 進数の 255.255.255.0 に変換します。/ ビットマスクの場合は、1s: /24 の数値を追加します。例 2 では、10 進数は 255.255.248.0 で、/ ビットは /21 です。

3 番目のオクテットの一部を拡張ネットワーク プレフィックスに使用して、複数の Class C ネットワークを大規模なネットワークにスーパーネット化することもできます。たとえば、192.168.0.0/20 と入力できます。

ここでは、次の項目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

必要なホストの数に基づいてサブネット 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 <sup>1</sup> | / ビット マスク | ドット付き 10 進数マスク             |
|------------------|-----------|----------------------------|
| 16,777,216       | /8        | 255.0.0.0 Class A ネットワーク   |
| 65,536           | /16       | 255.255.0.0 Class B ネットワーク |
| 32,768           | /17       | 255.255.128.0              |
| 16,384           | /18       | 255.255.192.0              |
| 8192             | /19       | 255.255.224.0              |
| 4096             | /20       | 255.255.240.0              |
| 2048             | /21       | 255.255.248.0              |

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 <sup>1</sup> | /ビット マスク | ドット付き 10 進数マスク               |
|------------------|----------|------------------------------|
| 1024             | /22      | 255.255.252.0                |
| 512              | /23      | 255.255.254.0                |
| 256              | /24      | 255.255.255.0 Class C ネットワーク |
| 128              | /25      | 255.255.255.128              |
| 64               | /26      | 255.255.255.192              |
| 32               | /27      | 255.255.255.224              |
| 16               | /28      | 255.255.255.240              |
| 8                | /29      | 255.255.255.248              |
| 4                | /30      | 255.255.255.252              |
| 使用不可             | /31      | 255.255.255.254              |
| 1                | /32      | 255.255.255.255 単一ホスト アドレス   |

1. 単一のホストを示す /32 を除き、サブネットの最初と最後の数は予約されています。

## サブネット マスクで使用するアドレスの判別

次の各項では、Class C サイズおよび Class B サイズのネットワークに対してサブネット マスクで使用するネットワーク アドレスを判別する方法について説明します。ここでは、次の項目について説明します。

- [Class C サイズのネットワーク アドレス \(P.D-4\)](#)
- [Class B サイズのネットワーク アドレス \(P.D-5\)](#)

## Class C サイズのネットワーク アドレス

F2 ~ 254 のホストを持つネットワークの場合、4 番目のオクテットは、0 から始まるホスト アドレスの数の倍数になります。たとえば、8 つのホストを持つサブネット (/29)、192.168.0.x は次のようになります。

| マスク /29 (255.255.255.248) でのサブネット | アドレス範囲 <sup>1</sup>           |
|-----------------------------------|-------------------------------|
| 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されています。最初のサブネットの例では、192.168.0.0 と 192.168.0.7 は使用できません。

## Class B サイズのネットワーク アドレス

254 ～ 65,534 のホストを持つネットワークのサブネット マスクで使用するネットワーク アドレスを判別するには、可能な拡張ネットワーク プレフィックスそれぞれについて 3 番目のオクテットの値を判別する必要があります。たとえば、10.1.x.0 のようなアドレスをサブネット化することができます。ここで、最初の 2 つのオクテットは拡張ネットワーク プレフィックスで使用されるため固定されています。4 番目のオクテットは、すべてのビットがホスト番号に使用されるため、0 です。

3 番目のオクテットの値を判別するには、次の手順を実行します。

**ステップ 1** 65,536（3 番目と 4 番目のオクテットを使用するアドレスの合計）を必要なホスト アドレスの数で割って、ネットワークから作成できるサブネットの数を計算します。

たとえば、65,536 を 4096 のホストで割ると、16 になります。

したがって、Class B サイズのネットワークでは、それぞれ 4096 個のアドレスを持つサブネットが 16 個できます。

**ステップ 2** 256（3 番目のオクテットの値の数）をサブネットの数で割って、3 番目のオクテット値の倍数を判別します。

この例では、 $256/16 = 16$  です。

3 番目のオクテットは、0 から始まる 16 の倍数になります。

したがって、ネットワーク 10.1 の 16 個のサブネットは次のようになります。

| マスク /29 (255.255.240.0) でのサブネット | アドレス範囲 <sup>1</sup>       |
|---------------------------------|---------------------------|
| 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されています。最初のサブネットの例では、10.1.0.0 と 10.1.15.255 は使用できません。

## IPv6 アドレス

IPv6 は、IPv4 後の次世代インターネット プロトコルです。これにより、アドレス スペースの拡張、ヘッダー形式の簡略化、拡張子とオプションのサポートの向上、フロー ラベル機能、および認証とプライバシーの機能が提供されます。IPv6 については RFC 2460 で説明されています。IPv6 アドレッシング アーキテクチャについては RFC 3513 で説明されています。

この項では、IPv6 アドレス形式およびアーキテクチャについて説明します。次の項目を取り上げます。

- [IPv6 アドレス形式 \(P.D-6\)](#)
- [IPv6 アドレス タイプ \(P.D-7\)](#)
- [IPv6 アドレス プレフィックス \(P.D-12\)](#)



(注)

この項では、IPv6 アドレス形式、タイプ、およびプレフィックスについて説明します。IPv6 を使用するためのセキュリティ アプライアンスの設定については、[第 6 章「インターフェイス パラメータの設定」](#)を参照してください。

### IPv6 アドレス形式

IPv6 アドレスは、x:x:x:x:x:x:x:x のように、コロン (:) で区切られた 8 つの一連の 16 ビット 16 進数フィールドとして表されます。次に、IPv6 アドレスの例を 2 つ示します。

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A



(注)

IPv6 アドレス内の 16 進数文字には大文字と小文字の区別がありません。

アドレスの個々のフィールドに先行ゼロを含める必要はありません。ただし、各フィールドに少なくとも 1 桁を含める必要があります。したがって、例のアドレス

2001:0DB8:0000:0000:0008:0800:200C:417A は、左から 3 番目～6 番目のフィールドから先行ゼロを削除して、2001:0DB8:0:0:8:800:200C:417A のように短縮することができます。ゼロだけを含むフィールド（左から 3 番目と 4 番目のフィールド）は、単一のゼロに短縮されています。左から 5 番目のフィールドでは、3 つの先行ゼロが削除され、単一の 8 がフィールドに残されています。左から 6 番目のフィールドでは、1 つの先行ゼロが削除され、800 がフィールドに残されています。

IPv6 アドレスには、ゼロの 16 進数フィールドがいくつか連続して含まれていることがよくあります。IPv6 アドレスの先頭、中間、または末尾で 2 つのコロン (::) を使用して、ゼロの連続フィールドを圧縮することができます（コロンは、ゼロの 16 進数フィールドが連続していることを表します）。[表 D-2](#) に、さまざまなタイプの IPv6 アドレスでのアドレス圧縮の例をいくつか示します。

**表 D-2 IPv6 アドレスの圧縮例**

| アドレスの種類 | 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                    |
| 指定なし    | 0:0:0:0:0:0:0:0             | ::                     |





(注)

ゼロのフィールドが連続することを表す 2 つのコロン (::) は、IPv6 アドレスの中で一度だけ使用できます。

IPv4 アドレスと IPv6 アドレスの両方を含む環境に対処するため、別の IPv6 形式がよく使用されます。その形式は `x:x:x:x:x:y.y.y.y` です。ここで、`x` は IPv6 アドレスの 6 つの高次の部分の 16 進数値を表し、`y` はアドレスの 32 ビット IPv4 部分 (IPv6 アドレスの残りの 2 つの 16 ビット部分を占める) の 10 進数値を表します。たとえば、IPv4 アドレス `192.168.1.1` は、IPv6 アドレス `0:0:0:0:0:FFFF:192.168.1.1` または `::FFFF:192.168.1.1` として表すことができます。

## IPv6 アドレス タイプ

次に、IPv6 アドレスの 3 つの主なタイプを示します。

- **ユニキャスト**：ユニキャスト アドレスは、単一インターフェイスの識別子です。ユニキャスト アドレスに送信されたパケットは、そのアドレスで示されたインターフェイスに送信されます。1 つのインターフェイスに複数のユニキャスト アドレスが割り当てられている場合もあります。
- **マルチキャスト**：マルチキャスト アドレスは、インターフェイスのセットを表す識別子です。マルチキャスト アドレスに送信されたパケットは、そのアドレスで示されたすべてのアドレスに送信されます。
- **エニーキャスト**：エニーキャスト アドレスは、インターフェイスのセットを表す識別子です。マルチキャスト アドレスと違い、エニーキャスト アドレスに送信されたパケットは、ルーティング プロトコルの距離測定によって判別された「最も近い」インターフェイスにのみ送信されます。



(注)

IPv6 には、ブロードキャスト アドレスがありません。マルチキャスト アドレスにブロードキャスト機能があります。

ここでは、次の項目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

この項では、IPv6 ユニキャスト アドレスについて説明します。ユニキャスト アドレスは、ネットワーク ノード上のインターフェイスを識別します。

ここでは、次の項目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的な形式では、グローバルルーティングプレフィックス、サブネット ID、インターフェイス ID の順に並んでいます。グローバルルーティングプレフィックスは、別の IPv6 アドレスタイプによって予約されていない任意のプレフィックスです (IPv6 アドレスタイププレフィックスについては、P.D-12 の「IPv6 アドレスプレフィックス」を参照してください)。

バイナリ 000 で始まるものを除くすべてのグローバルユニキャストアドレスが、Modified EUI-64 形式で 64 ビットのインターフェイス ID を持っています。インターフェイス識別子用の Modified EUI-64 形式の詳細については、P.D-9 の「インターフェイス識別子」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には、アドレスのインターフェイス ID 部分のサイズまたは構造に対する制約がありません。このタイプのアドレスの一例として、IPv4 アドレスが埋め込まれた IPv6 アドレスがあります (P.D-8 の「IPv4 互換 IPv6 アドレス」を参照してください)。

## サイトローカルアドレス

サイトローカルアドレスは、サイト内のアドレッシングに使用されます。このアドレスを使用すると、グローバルに固有なプレフィックスを使用せずにサイト全体をアドレッシングすることができます。サイトローカルアドレスでは、Modified EUI-64 形式で、プレフィックス FEC0::/10、54 ビットサブネット ID、64 ビットインターフェイス ID の順に並んでいます。

サイトローカルルータは、サイト外の送信元または宛先にサイトローカルアドレスを持つパケットを転送しません。したがって、サイトローカルアドレスは、プライベートアドレスと見なされます。

## リンクローカルアドレス

すべてのインターフェイスに、少なくとも 1 つのリンクローカルアドレスが必要です。IPv6 アドレスはインターフェイスごとに複数設定できますが、リンクローカルアドレスは 1 つだけです。

リンクローカルアドレスは、Modified EUI-64 形式でリンクローカルプレフィックス FE80::/10 とインターフェイス識別子を使用して任意のインターフェイスで自動的に設定できる IPv6 ユニキャストアドレスです。リンクローカルアドレスは、近隣探索プロトコルとステートレスな自動設定プロセスで使用されます。リンクローカルアドレスを持つノードは、通信が可能です。これらのノードは通信にサイトローカルアドレスまたはグローバルに固有なアドレスを必要としません。

ルータは、送信元または宛先にリンクローカルアドレスを持つパケットを送信しません。したがって、リンクローカルアドレスは、プライベートアドレスと見なされます。

## IPv4 互換 IPv6 アドレス

IPv4 アドレスを組み込むことができる IPv6 アドレスのタイプは 2 つあります。

最初のタイプは、「IPv4 互換 IPv6 アドレス」です。IPv6 移行メカニズムには、ホストとルータが IPv4 ルーティングインフラストラクチャで IPv6 パケットを動的にトンネリングする技術が含まれています。この技術を使用する IPv6 ノードには、低次 32 ビットでグローバル IPv4 アドレスを伝送する特別な IPv6 ユニキャストアドレスが割り当てられます。このタイプのアドレスは「IPv4 互換 IPv6 アドレス」と呼ばれ、形式は ::y.y.y.y です。ここで、y.y.y.y は IPv4 ユニキャストアドレスです。

**(注)**

「IPv4 互換 IPv6 アドレス」で使用する IPv4 アドレスは、グローバルに固有な IPv4 ユニキャスト アドレスである必要があります。

埋め込み IPv4 アドレスを保持する 2 番目のタイプの IPv6 アドレスは、「IPv4 マッピング IPv6 アドレス」と呼ばれます。このアドレス タイプは、IPv4 ノードのアドレスを IPv6 アドレスとして表すために使用されます。このタイプのアドレス形式は ::FFFF:y.y.y.y です。ここで、y.y.y.y は IPv4 ユニキャスト アドレスです。

## 未指定アドレス

未指定アドレス 0:0:0:0:0:0:0:0 は、IPv6 アドレスがないことを示しています。たとえば、IPv6 ネットワーク上で新しく初期化されたノードは、IPv6 アドレスを受信するまで、パケットで未指定アドレスを送信元アドレスとして使用できます。

**(注)**

IPv6 未指定アドレスは、インターフェイスに割り当てることができません。未指定 IPv6 アドレスを IPv6 パケットまたは IPv6 ルーティング ヘッダーで宛先アドレスとして使用することはできません。

## ループバック アドレス

ループバック アドレス 0:0:0:0:0:0:0:1 は、ノードが IPv6 パケットをそれ自体に送信するために使用できます。IPv6 におけるループバック アドレスは、IPv4 のループバック アドレス (127.0.0.1) と同じように機能します。

**(注)**

IPv6 ループバック アドレスは、物理インターフェイスに割り当てることができません。IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットは、そのパケットを作成したノード内に留まっている必要があります。IPv6 ルータは、IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットを転送しません。

## インターフェイス識別子

IPv6 ユニキャスト アドレス内のインターフェイス識別子は、リンク上でインターフェイスを識別するために使用されます。これらの識別子は、サブネット プレフィックス内で固有である必要があります。多くの場合、インターフェイス識別子はインターフェイス リンク層アドレスから導出されます。各インターフェイスが異なるサブネットに接続されていれば、単一ノードの複数のインターフェイスで同一のインターフェイス識別子を使用することもできます。

バイナリ 000 で始まるものを除くすべてのユニキャスト アドレスで、インターフェイス識別子は、64 ビットの長さで Modified EUI-64 形式で構築されている必要があります。Modified EUI-64 形式は、アドレス内のユニバーサル / ローカル ビットを逆にし、MAC アドレスの上の 3 つのバイトと下の 3 つのバイトの間に 16 進数 FFFE を挿入することによって、48 ビット MAC アドレスから作成されます。

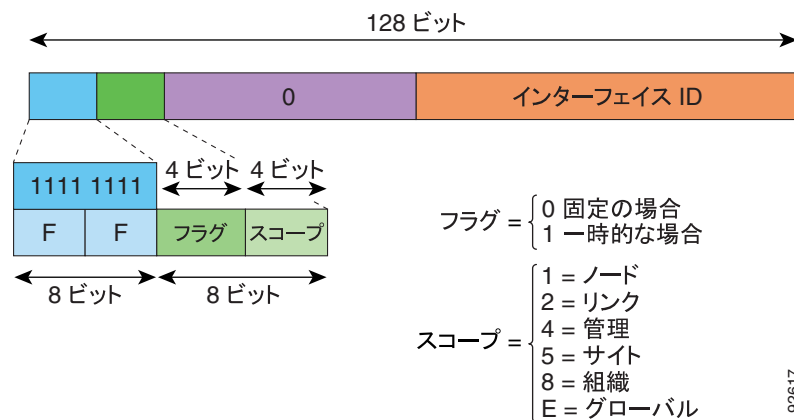
たとえば、MAC アドレスが 00E0.b601.3B7A のインターフェイスの場合、64 ビット インターフェイス ID は 02E0:B6FF:FE01:3B7A になります。

## マルチキャスト アドレス

IPv6 マルチキャスト アドレスは、通常は異なるノード上にある、インターフェイスのグループの識別子です。マルチキャスト アドレスに送信されたパケットは、そのマルチキャスト アドレスで示されたすべてのインターフェイスに送信されます。1 つのインターフェイスが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ックスは FF00::/8 (1111 1111) です。オクテットとそれに続くプレフィックスは、マルチキャスト アドレスのタイプとスコープを定義します。永続的に割り当てられた（「周知の」）マルチキャスト アドレスには、0 に等しいフラグパラメータがあり、一時的な（「過渡」）マルチキャスト アドレスには 1 に等しいフラグパラメータがあります。ノード、リンク、サイト、または組織のスコープを持つマルチキャスト アドレスのスコープパラメータは、それぞれ 1、2、5、8、または E です。たとえば、プレフィックス FF02::/16 を持つマルチキャスト アドレスは、リンク スコープを持つ永続的なマルチキャスト アドレスです。図 D-1 に、IPv6 マルチキャスト アドレスの形式を示します。

図 D-1 IPv6 マルチキャスト アドレス形式



IPv6 ノード（ホストとルータ）は、次のマルチキャスト グループに参加する必要があります。

- All Nodes マルチキャスト アドレス：
  - FF01::（インターフェイスローカル）
  - FF02::（リンクローカル）
- ノード：FF02:0:0:0:1:FFXX:XXXX/104 上の各 IPv6 ユニキャスト アドレスおよびエニーキャスト アドレスの送信要求ノード アドレス。ここで、XX:XXXX は低次 24 ビットのユニキャスト アドレスまたはエニーキャスト アドレスです。



**(注)** 送信要求ノード アドレスは、ネイバー送信要求メッセージで使用されます。

IPv6 ルータは、次のマルチキャスト グループに参加する必要があります。

- FF01::2（インターフェイスローカル）
- FF02::2（リンクローカル）
- FF05::2（サイトローカル）

マルチキャスト アドレスを IPv6 パケットで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 アドレスがありません。ブロードキャスト アドレスの代わりに IPv6 マルチキャスト アドレスが使用されます。

## エニーキャスト アドレス

IPv6 エニーキャスト アドレスは、複数のインターフェイス（通常は異なるノードに属す）に割り当てられたユニキャスト アドレスです。エニーキャスト アドレスにルーティングされたパケットは、そのアドレスを持ち、有効なルーティング プロトコルによって最も近いと判別されたインターフェイスにルーティングされます。

エニーキャスト アドレスは、ユニキャスト アドレス 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 アドレスにすぎません。インターフェイスは、アドレスをエニーキャスト アドレスとして認識するように設定されている必要があります。

エニーキャスト アドレスには次の制限が適用されます。

- エニーキャスト アドレスを 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ができません。IPv6 ルータにのみ割り当てることができます。

**(注)**

エニーキャスト アドレスは、セキュリティ アプライアンスではサポートされていません。

## 必須アドレス

IPv6 ホストには、少なくとも次のアドレスが（自動または手動で）設定されている必要があります。

- 各インターフェイスのリンクローカル アドレス
- ループバック アドレス
- All-Nodes マルチキャスト アドレス
- 各ユニキャスト アドレスまたはエニーキャスト アドレスの送信要求ノード マルチキャスト アドレス

IPv6 ルータには、少なくとも次のアドレスが（自動または手動で）設定されている必要があります。

- 必須ホスト アドレス
- ルータとして動作するように設定されているすべてのインターフェイスのサブネットルータ エニーキャスト アドレス
- All-Routers マルチキャスト アドレス

## IPv6 アドレス プレフィックス

IPv6 アドレス プレフィックスは、ipv6-prefix/prefix-length の形式で、アドレス スペース全体のビット連続ブロックを表すために使用できます。IPv6-prefix は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス（アドレスのネットワーク部分）を構成しているかを指定する 10 進数値です。たとえば、2001:0DB8:8086:6502::/32 は有効な IPv6 プレフィックスです。

IPv6 プレフィックスは、IPv6 アドレスのタイプを示します。表 D-3 に、各 IPv6 アドレス タイプのプレフィックスを示します。

**表 D-3 IPv6 アドレス タイプのプレフィックス**

| アドレスの種類          | バイナリ プレフィックス              | IPv6 表記   |
|------------------|---------------------------|-----------|
| 指定なし             | 000...0 (128 ビット)         | ::/128    |
| ループバック           | 000..0.1 (128 ビット)        | ::1/128   |
| マルチキャスト          | 11111111                  | FF00::/8  |
| リンクローカル (ユニキャスト) | 1111111010                | FE80::/10 |
| サイトローカル (ユニキャスト) | 1111111111                | FEC0::/10 |
| グローバル (ユニキャスト)   | その他すべてのアドレス。              |           |
| エニーキャスト          | ユニキャスト アドレス スペースから取得されます。 |           |

## プロトコルとアプリケーション

表 D-4 に、プロトコルのリテラル値とポート番号を示します。どちらもセキュリティ アプライアンスのコマンドで入力できます。

**表 D-4 プロトコルのリテラル値**

| リテラル   | 値   | 説明                                                                                                                  |
|--------|-----|---------------------------------------------------------------------------------------------------------------------|
| ah     | 51  | IPv6 の認証ヘッダー (RFC 1826)。                                                                                            |
| eigrp  | 88  | Enhanced Interior Gateway Routing Protocol (Enhanced IGRP)。                                                         |
| esp    | 50  | IPv6 の 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 (総称ルーティング カプセル化)。                                                                     |
| icmp   | 1   | Internet Control Message Protocol (インターネット制御メッセージ プロトコル) (RFC 792)。                                                 |
| icmp6  | 58  | IPv6 の Internet Control Message Protocol (インターネット制御メッセージ プロトコル) (RFC 2463)。                                         |
| igmp   | 2   | Internet Group Management Protocol (インターネット グループ管理プロトコル) (RFC 1112)。                                                |
| igrp   | 9   | Interior Gateway Routing Protocol (内部ゲートウェイ ルーティング プロトコル)。                                                          |
| ip     | 0   | Internet Protocol (インターネット プロトコル)。                                                                                  |
| ipinip | 4   | IP-in-IP カプセル化。                                                                                                     |
| ipsec  | 50  | IP セキュリティ。ipsec プロトコル リテラルを入力すると、esp プロトコル リテラルを入力した場合と同じ結果が得られます。                                                  |
| nos    | 94  | Network Operating System (ネットワーク OS) (Novell の NetWare)。                                                            |
| ospf   | 89  | OSPF ルーティング プロトコル (RFC 1247)。                                                                                       |
| pcp    | 108 | Payload Compression Protocol (ペイロード圧縮プロトコル)。                                                                        |
| 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 リテラルを入力すると、gre プロトコル リテラルを入力した場合と同じ結果が得られます。 |
| snp    | 109 | Sitara Networks Protocol。                                                                                           |
| tcp    | 6   | Transmission Control Protocol (伝送制御プロトコル) (RFC 793)。                                                                |
| udp    | 17  | User Datagram Protocol (ユーザ データグラム プロトコル) (RFC 768)。                                                                |

プロトコル番号は、次の IANA Web サイトで確認できます。

<http://www.iana.org/assignments/protocol-numbers>

## TCP ポートと UDP ポート

表 D-5 に、リテラル値とポート番号を示します。どちらもセキュリティ アプライアンスのコマンドで入力できます。次の警告を参照してください。

- セキュリティ アプライアンスは、SQL\*Net 用にポート 1521 を使用します。これは、Oracle が SQL\*Net に使用するデフォルトのポートです。ただし、この値は IANA ポート割り当てとは一致しません。
- セキュリティ アプライアンスは、ポート 1645 と 1646 で RADIUS をリスンしています。RADIUS サーバが標準ポート 1812 と 1813 を使用している場合は、**authentication-port** コマンドと **accounting-port** コマンドを使用して、それらのポートでリスンするようにセキュリティ アプライアンスを設定できます。
- DNS アクセスにポートを割り当てるには、**dns** ではなく **domain** リテラル値を使用します。**dns** を使用した場合、セキュリティ アプライアンスでは、**dnsix** リテラル値を使用すると見なされます。

ポート番号は、次の URL で IANA の Web サイトにアクセスしてオンラインで参照できます。

<http://www.iana.org/assignments/port-numbers>

表 D-5 ポートのリテラル値

| リテラル       | TCP または UDP? | 値    | 説明                                                                             |
|------------|--------------|------|--------------------------------------------------------------------------------|
| aol        | TCP          | 5190 | America Online (アメリカ オンライン)。                                                   |
| bgp        | TCP          | 179  | Border Gateway Protocol (ボーダー ゲートウェイ プロトコル) (RFC 1163)。                        |
| biff       | UDP          | 512  | 新しいメールの受信をユーザに通知するために、メール システムが使用します。                                          |
| bootpc     | UDP          | 68   | Bootstrap Protocol Client (ブートストラップ プロトコル クライアント)。                             |
| bootps     | UDP          | 67   | Bootstrap Protocol Server (ブートストラップ プロトコル サーバ)。                                |
| chargen    | TCP          | 19   | Character Generator (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  | <b>cmd</b> は自動認証機能がある点を除いて、 <b>exec</b> と同様です。                                 |
| ctiqbe     | TCP          | 2748 | Computer Telephony Interface Quick Buffer Encoding。                            |
| daytime    | TCP          | 13   | Day time (日時) (RFC 867)。                                                       |
| discard    | TCP、UDP      | 9    | 廃棄。                                                                            |
| domain     | TCP、UDP      | 53   | DNS                                                                            |
| dnsix      | UDP          | 195  | DNSIX Session Management Module Audit Redirector (DNSIX セッション管理モジュール監査リダイレクタ)。 |
| echo       | TCP、UDP      | 7    | エコー。                                                                           |
| exec       | TCP          | 512  | リモート プロセスの実行。                                                                  |
| finger     | TCP          | 79   | Finger。                                                                        |
| ftp        | TCP          | 21   | File Transfer Protocol (ファイル転送プロトコル) (コンソール ポート)。                              |



表 D-5 ポートのリテラル値 (続き)

| リテラル              | TCP または UDP? | 値    | 説明                                                                      |
|-------------------|--------------|------|-------------------------------------------------------------------------|
| ftp-data          | TCP          | 20   | File Transfer Protocol (ファイル転送プロトコル) (データ ポート)。                         |
| gopher            | TCP          | 70   | Gopher。                                                                 |
| https             | TCP          | 443  | HTTP over SSL。                                                          |
| h323              | TCP          | 1720 | H.323 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  | ID 認証サービス。                                                              |
| imap4             | TCP          | 143  | Internet Message Access Protocol バージョン 4。                               |
| irc               | TCP          | 194  | Internet Relay Chat Protocol (インターネット リレーチャット プロトコル)。                   |
| isakmp            | UDP          | 500  | Internet Security Association and Key Management Protocol。              |
| kerberos          | TCP、UDP      | 750  | Kerberos。                                                               |
| klogin            | TCP          | 543  | KLOGIN。                                                                 |
| kshell            | TCP          | 544  | Korn Shell (Korn シェル)。                                                  |
| ldap              | TCP          | 389  | Lightweight Directory Access Protocol (ライトウェイトディレクトリ アクセス プロトコル)。       |
| ldaps             | TCP          | 636  | Lightweight Directory Access Protocol (ライトウェイトディレクトリ アクセス プロトコル) (SSL)。 |
| lpd               | TCP          | 515  | Line Printer Daemon (ライン プリンタ デーモン) (プリンタ スプーラー)。                       |
| login             | TCP          | 513  | リモート ログイン。                                                              |
| lotusnotes        | TCP          | 1352 | IBM Lotus Notes。                                                        |
| mobile-ip         | UDP          | 434  | MobileIP-Agent (モバイル IP エージェント)。                                        |
| nameserver        | UDP          | 42   | Host Name Server (ホスト ネーム サーバ)。                                         |
| netbios-ns        | UDP          | 137  | NetBIOS Name Service (NetBIOS ネーム サービス)。                                |
| netbios-dgm       | UDP          | 138  | NetBIOS Datagram Service (NetBIOS データグラム サービス)。                         |
| netbios-ssn       | TCP          | 139  | NetBIOS Session Service (NetBIOS セッション サービス)。                           |
| nntp              | TCP          | 119  | Network News Transfer Protocol。                                         |
| ntp               | UDP          | 123  | Network Time Protocol (ネットワーク タイム プロトコル)。                               |
| pcanywhere-status | UDP          | 5632 | pcAnywhere ステータス。                                                       |
| pcanywhere-data   | TCP          | 5631 | pcAnywhere データ。                                                         |
| pim-auto-rp       | TCP、UDP      | 496  | Protocol Independent Multicast、逆パス フラッド、稠密モード。                          |
| pop2              | TCP          | 109  | Post Office Protocol (POP) Version 2。                                   |
| pop3              | TCP          | 110  | Post Office Protocol (POP) Version 3。                                   |
| pptp              | TCP          | 1723 | 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)。            |

表 D-5 ポートのリテラル値 (続き)

| リテラル         | TCP または UDP? | 値    | 説明                                                                                              |
|--------------|--------------|------|-------------------------------------------------------------------------------------------------|
| radius       | UDP          | 1645 | Remote Authentication Dial-In User Service (リモート認証ダイヤルイン ユーザ サービス)。                             |
| radius-acct  | UDP          | 1646 | Remote Authentication Dial-In User Service (リモート認証ダイヤルイン ユーザ サービス) (アカウントティング)。                 |
| rip          | UDP          | 520  | Routing Information Protocol (ルーティング情報プロトコル)。                                                   |
| secureid-udp | UDP          | 5510 | SecureID over UDP。                                                                              |
| smtp         | TCP          | 25   | Simple Mail Transport Protocol (シンプル メール転送プロトコル)。                                               |
| snmp         | UDP          | 161  | Simple Network Management Protocol (簡易ネットワーク管理プロトコル)。                                           |
| snmptrap     | UDP          | 162  | Simple Network Management Protocol (簡易ネットワーク管理プロトコル) (トラップ)。                                    |
| sqlnet       | TCP          | 1521 | Structured Query Language Network (構造化照会言語ネットワーク)。                                              |
| ssh          | TCP          | 22   | Secure Shell (セキュア シェル)。                                                                        |
| sunrpc (rpc) | TCP、UDP      | 111  | Sun Remote Procedure Call (リモート プロシージャ コール)。                                                    |
| syslog       | UDP          | 514  | System Log (システム ログ)。                                                                           |
| tacacs       | TCP、UDP      | 49   | Terminal Access Controller Access Control System Plus (ターミナル アクセス コントローラ アクセス コントロール システム プラス)。 |
| talk         | TCP、UDP      | 517  | Talk。                                                                                           |
| telnet       | TCP          | 23   | Telnet (RFC 854)。                                                                               |
| tftp         | UDP          | 69   | Trivial File Transfer Protocol (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 (UNIX 間コピー プログラム)。                                                    |
| who          | UDP          | 513  | Who。                                                                                            |
| whois        | TCP          | 43   | Who Is。                                                                                         |
| www          | TCP          | 80   | World Wide Web (ワールドワイド ウェブ)。                                                                   |
| xdmcp        | UDP          | 177  | X Display Manager Control Protocol (X DMCP)。                                                    |

## ローカル ポートとプロトコル

表 D-6 に、セキュリティ アプライアンスに向かうトラフィックを処理するためにセキュリティ アプライアンスが開くプロトコル、TCP ポート、および UDP ポートを示します。表 D-6 に記載されている機能とサービスをイネーブルにしない限り、セキュリティ アプライアンスは、TCP または UDP ポートでローカル プロトコルを開きません。セキュリティ アプライアンスがデフォルトのリスニング プロトコルまたはポートを開くように機能またはサービスを設定する必要があります。多くの場合、機能またはサービスをイネーブルにすると、デフォルト ポート以外のポートを設定できます。

**表 D-6 機能とサービスによって開かれるプロトコルとポート**

| 機能またはサービス                              | プロトコル | ポート番号      | コメント                                                     |
|----------------------------------------|-------|------------|----------------------------------------------------------|
| DHCP                                   | UDP   | 67,68      | —                                                        |
| フェールオーバー制御                             | 108   | 該当なし       | —                                                        |
| HTTP                                   | TCP   | 80         | —                                                        |
| HTTPS                                  | TCP   | 443        | —                                                        |
| ICMP                                   | 1     | 該当なし       | —                                                        |
| IGMP                                   | 2     | 該当なし       | プロトコルは宛先 IP アドレス 224.0.0.1 でのみ開かれます。                     |
| ISAKMP/IKE                             | UDP   | 500        | 設定可能。                                                    |
| IPSec (ESP)                            | 50    | 該当なし       | —                                                        |
| IPSec over UDP (NAT-T)                 | UDP   | 4500       | —                                                        |
| IPSec over UDP (Cisco VPN 3000 シリーズ互換) | UDP   | 10000      | 設定可能。                                                    |
| IPSec over TCP (CTCP)                  | TCP   | —          | デフォルト ポートは使用されません。IPSec over TCP の設定時にポート番号を指定する必要があります。 |
| NTP                                    | UDP   | 123        | —                                                        |
| OSPF                                   | 89    | 該当なし       | プロトコルは宛先 IP アドレス 224.0.0.5 および 224.0.0.6 でのみ開かれます。       |
| PIM                                    | 103   | 該当なし       | プロトコルは宛先 IP アドレス 224.0.0.13 でのみ開かれます。                    |
| RIP                                    | UDP   | 520        | —                                                        |
| RIPv2                                  | UDP   | 520        | ポートは宛先 IP アドレス 224.0.0.9 でのみ開かれます。                       |
| SNMP                                   | UDP   | 161        | 設定可能。                                                    |
| SSH                                    | TCP   | 22         | —                                                        |
| ステートフル アップデート                          | 105   | 該当なし       | —                                                        |
| Telnet                                 | TCP   | 23         | —                                                        |
| VPN ロードバランシング                          | UDP   | 9023       | 設定可能。                                                    |
| VPN 個別ユーザ認証プロキシ                        | UDP   | 1645, 1646 | ポートは VPN トンネルでのみアクセスできます。                                |

## ICMP タイプ

表 D-7 に、セキュリティ アプライアンスのコマンドで入力できる ICMP タイプの番号と名前を示します。

**表 D-7 ICMP タイプ**

| ICMP 番号 | ICMP 名               |
|---------|----------------------|
| 0       | echo-reply           |
| 3       | unreachable          |
| 4       | source-quench        |
| 5       | redirect             |
| 6       | alternate-address    |
| 8       | echo                 |
| 9       | router-advertisement |
| 10      | router-solicitation  |
| 11      | time-exceeded        |
| 12      | parameter-problem    |
| 13      | timestamp-request    |
| 14      | timestamp-reply      |
| 15      | information-request  |
| 16      | information-reply    |
| 17      | mask-request         |
| 18      | mask-reply           |
| 31      | conversion-error     |
| 32      | mobile-redirect      |



## 認可および認証用の外部サーバの設定

この付録では、セキュリティ アプライアンス、VPN3000、および PIX ユーザを認証および認可するための外部 LDAP サーバまたは RADIUS サーバの設定方法について説明します。認証ではユーザの本人確認を行い、認可ではこのユーザが実行できるアクションを決定します。セキュリティ アプライアンスを設定して外部サーバを使用する前に、このサーバに正しいセキュリティ アプライアンスの認可アトリビュートを設定する必要があります。また、このアトリビュートのサブセットから、特定の権限を個々のユーザに割り当てます。

この付録では、次の項目について説明します。

- [LDAP、RADIUS、またはローカルの認証および認可の選択](#)
- [権限およびアトリビュートのポリシー実施の概要](#)
- [外部 LDAP サーバの設定](#)
- [外部 RADIUS サーバの設定](#)

## LDAP、RADIUS、またはローカルの認証および認可の選択

ユーザのプラットフォームに適した認証および認可が何かを判別するための支援として、この項では、セキュリティ アプライアンス (ASA)、PIX、および VPN 3000 の各プラットフォームに提供されている LDAP および RADIUS のサポートについて説明します。

- LDAP 認証

PIX 7.1.x およびセキュリティ アプライアンスでのみサポートされています。VPN 3000 ではネイティブ LDAP 認証はサポートしません。LDAP サーバはユーザ名を取得および検索し、定義されている任意のアトリビュートを権限付与機能の一部として使用します。

- LDAP 認可

PIX、VPN 3000、およびセキュリティ アプライアンスでサポートされています。LDAP サーバは、ユーザ名を取得および検索し、定義されている任意のアトリビュートを使用します。

- RADIUS 認証

PIX、VPN 3000、およびセキュリティ アプライアンスでサポートされています。RADIUS サーバはユーザ名を取得および検索し、定義されている任意のアトリビュートを権限付与機能として使用します。

- RADIUS 認可

PIX、VPN 3000、およびセキュリティ アプライアンスでサポートされています。RADIUS サーバは、ユーザ名を取得および検索し、定義されている任意のアトリビュートを使用します。

- ローカル認証

PIX、VPN 3000、およびセキュリティ アプライアンスでサポートされています。ローカルの内部サーバは、ユーザ名を取得および検索し、定義されている任意のアトリビュートを権限付与機能として使用します。

- ローカル認可

PIX 7.1.x およびセキュリティ アプライアンスでのみサポートされています。ローカルの内部サーバは、ユーザ名を取得および検索し、定義されている任意のアトリビュートを使用します。

## 権限およびアトリビュートのポリシー実施の概要

セキュリティ アプライアンスを設定することにより、ローカルまたは内部のデータベース、RADIUS および LDAP の各認証サーバ、または RADIUS または LDAP の各認可サーバからユーザアトリビュートが受信されるようにできます。また、ユーザにさまざまなアトリビュートを持つグループポリシーを適用することもできます。ただし、ユーザのアトリビュートが常に優先されます。デバイスがユーザとグループ（複数可）を認証すると、セキュリティ アプライアンスがユーザとグループアトリビュートセットを組み合わせて1つの集約アトリビュートセットにします。セキュリティ アプライアンスは、次の順序でアトリビュートを使用して、認証済みユーザに集約アトリビュートセットを適用します。

1. ユーザ アトリビュート：ユーザの認証または認可が成功すると、サーバはこれらを返します。このアトリビュートは他のすべてに優先します。
2. グループポリシー アトリビュート：ユーザに関連付けられているグループポリシーのアトリビュートです。ユーザのグループポリシー名は、ローカル データベースの 'vpn-group-policy' アトリビュートで識別するか、外部 RADIUS/LDAP サーバから、'OU=GroupName;' 形式の値 RADIUS CLASS attribute (25) で識別します。グループポリシーはユーザアトリビュートで不足している任意のアトリビュートを提供します。ユーザアトリビュートとグループポリシーアトリビュートの両方に値がある場合、ユーザアトリビュートがグループポリシーアトリビュートを上書きします。
3. トンネルグループの default-group-policy アトリビュート：これらは、トンネルグループに関連付けられている default-group-policy（基本グループ）のアトリビュートです。このグループポリシーを検索後、トンネルグループの default-group-policy は、ユーザアトリビュートまたはグループポリシーで不足している任意のアトリビュートを提供します。ユーザアトリビュートとグループポリシーアトリビュートの両方に値がある場合、ユーザアトリビュートがグループポリシーアトリビュートを上書きします。
4. システムのデフォルトアトリビュート：システムのデフォルトアトリビュートは、ユーザ、グループ、またはトンネルグループの各アトリビュートで不足している任意のアトリビュートを提供します。

## 外部 LDAP サーバの設定

**(注)**

LDAP プロトコルの詳細については、RFC 1777、2251、および 2849 を参照してください。

この項では、LDAP サーバの構造、スキーマ、およびアトリビュートについて説明します。次の項目について説明します。

- [LDAP ディレクトリ構造の確認と設定の手順](#)
- [セキュリティ アプライアンスで使用する LDAP スキーマの構成](#)
- [セキュリティ アプライアンスの LDAP スキーマの定義](#)
- [LDAP サーバへのスキーマのロード](#)
- [ユーザ権限の定義](#)
- [Active Directory の設定の確認](#)

### LDAP ディレクトリ構造の確認と設定の手順

LDAP サーバは、情報をエントリとしてディレクトリに保存します。LDAP スキーマはこのようなエントリが保存する情報の種類を定義します。スキーマは、クラスと各クラスのオブジェクトに含めることができるアトリビュートのセット（必須およびオプション）を示します。

セキュリティ アプライアンスと相互運用するように LDAP サーバを設定するには、セキュリティ アプライアンス認可スキーマを定義します。セキュリティ アプライアンス認可スキーマでは、セキュリティ アプライアンスでサポートするクラスとそのクラスのアトリビュートを定義します。具体的には、セキュリティ アプライアンスユーザにアクセス時間やプライマリ DNS などの権限を付与するために使用できる、オブジェクト クラス（cVPN3000-User-Authorization）およびそのクラスで可能なすべてのアトリビュートです。各アトリビュートは、アトリビュート名、アトリビュートの番号（オブジェクト ID または OID と呼ばれる）、タイプ、および可能な値で構成されます。

セキュリティ アプライアンス認可スキーマを定義し、これを使用するサーバにロードし終わったら、セキュリティ アプライアンスのアトリビュートと権限、およびサーバの使用が認可される各ユーザに相当する値を定義します。

要約すると、LDAP サーバをセットアップするには、次のように実行します。

- ユーザの企業の階層型セットアップに従ってセキュリティ アプライアンス LDAP 認可スキーマを設計する
- セキュリティ アプライアンス認可スキーマを定義する
- LDAP サーバにスキーマをロードする
- LDAP サーバを使用する各ユーザの権限を定義する

使用する LDAP サーバのタイプによって、上記のプロセスの手順が異なります。



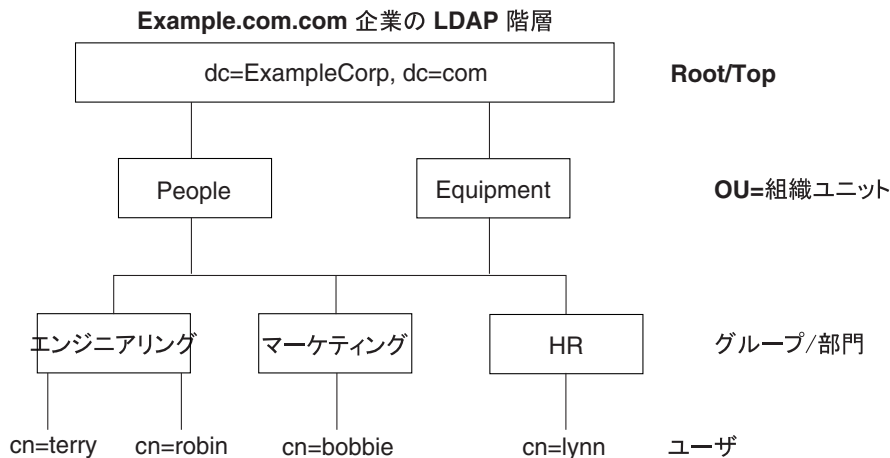
## セキュリティ アプライアンスで使用する LDAP スキーマの構成

スキーマを実際に作成する前に、自分の会社の構造について検討します。LDAP スキーマは、企業の論理階層が反映されたものにする必要があります。

たとえば、Example Corporation という企業の従業員、Terry を例に考えてみます。Terry はエンジニアリング グループに従事しています。この企業の LDAP 階層は 1 つ以上のレベルを持つことができます。Terry を Example Corporation のメンバーと想定し、浅い単一レベルの階層をセットアップすると決定することができます。あるいは、マルチレベルの階層をセットアップすることもできます。この場合、Terry は、エンジニアリング部門のメンバーであると想定され、この部門は、People と呼ばれる組織ユニットのメンバーであり、Example Corporation のメンバーです。図 E-1 に、マルチレベルの階層の例を示します。

マルチレベル階層はさらに細かく設定できますが、シングルレベル階層の方が迅速に検索できます。

図 E-1 マルチレベルの LDAP 階層



148997

## 階層の検索

セキュリティ アプライアンスでは、LDAP 階層内での検索を調整することができます。セキュリティ アプライアンスに次の 3 種類のフィールドを設定すると、LDAP 階層での検索開始場所とその範囲、および検索する情報のタイプを定義することができます。これらのフィールドを組み合わせることで、ユーザーの権限が含まれているツリーの部分だけを検索するように階層の検索を限定できます。

- LDAP Base DN には、サーバがセキュリティ アプライアンスから認可要求を受信したときにユーザー情報の検索を開始すべき LDAP の階層を定義します。
- Search Scope には、LDAP 階層の検索範囲を定義します。この指定では、LDAP Base DN よりもかなり下位のレベルまで検索します。サーバが行う検索を直下の 1 レベルだけにするか、サブツリー全体を検索するかを選択することができます。単一レベルの検索の方が高速ですが、サブツリー検索の方が広範囲に検索できます。
- Naming Attribute には、LDAP サーバのエントリを一意に識別する Relative Distinguished Name (RDN; 相対識別名) を定義します。一般的な名前アトリビュートは、cn (共通名) および uid (ユーザー ID) です。

図 E-1 に、Example Corporation で可能な LDAP 階層の例を示します。この階層が指定されると、複数の方法で検索を定義できます。表 E-1 に、2 種類の可能な検索の設定を示します。

## ■ 外部 LDAP サーバの設定

最初の設定例では、Terry が必要な LDAP 認可を得て自身の IPsec トンネル接続を確立すると、セキュリティ アプライアンスは、LDAP サーバに検索要求を送信します。この要求では、サーバが Terry を代行して エンジニアリング グループの検索を実行する必要があることを指定します。この検索は短時間でできます。

2 番目の設定例では、セキュリティ アプライアンスは、Terry を代行してサーバが Example Corporation 全体を検索するよう指示する検索要求を送信します。この検索には時間がかかります。

表 E-1 検索設定の例

| # | LDAP Base DN                                               | Search Scope | Naming Attribute | 結果          |
|---|------------------------------------------------------------|--------------|------------------|-------------|
| 1 | group= Engineering,ou=People,dc=ExampleCorporation, dc=com | 1 レベル        | cn=Terry         | 検索に時間がかからない |
| 2 | dc=ExampleCorporation,dc=com                               | サブツリー        | cn=Terry         | 検索に時間がかかる   |

## セキュリティ アプライアンスと LDAP サーバのバインディング

一部の LDAP サーバ（Microsoft Active Directory サーバなど）は、セキュリティ アプライアンスに対し、他のあらゆる LDAP 操作の要求を受け入れる前に、認証済みバインディングを介してハンドシェイクを確立することを要求します。セキュリティ アプライアンスは、ユーザの認証要求に Login DN フィールドを付加することにより、自身が認証バインディングされていることを示します。Login DN フィールドには、セキュリティ アプライアンスの認証特性を定義します。これらの特性は、管理者特権を持つユーザの特性に対応している必要があります。たとえば、次のような Login DN フィールドを定義することができます。cn=Administrator, cn=users, ou=people, dc=example, dc=com

## セキュリティ アプライアンスの LDAP スキーマの定義

ユーザ情報の LDAP 階層での構成方法を決定したら、この組織をスキーマとして定義します。スキーマを定義するには、最初に、オブジェクトのクラス名を定義します。セキュリティ アプライアンス ディレクトリのクラス名は、cVPN3000-User-Authorization です。このクラスには、オブジェクト ID (OID) の 1.2.840.113556.1.8000.795.1.1 を持ちます。ディレクトリ内のすべてのエントリまたはユーザは、このクラスのオブジェクトになります。

一部の LDAP サーバ（Microsoft Active Directory LDAP サーバなど）では、定義済みのクラス OID の再利用を許可されません。この場合は、次に大きい OID を使用します。たとえば、クラス名 cVPN3000-Usr-Authorization に誤って 1.2.840.113556.1.8000.795.1.1 という OID を定義した場合、クラス名 cVPN3000-User-Authorization には次の OID である 1.2.840.113556.1.8000.795.1.2 を入力することができます。

Microsoft Active Directory LDAP サーバを使用する場合は、LDAP Data Interchange Format (LDIF) を使用したテキスト フォームでスキーマを定義します。このフォーマットのファイルには、schema.ldif のように拡張子 .ldif が付きます。他の LDAP サーバでは、グラフィカル ユーザ インターフェイスまたはスクリプト ファイルを使用してオブジェクト クラスとそのアトリビュートを定義します。LDIF の詳細については、RFC -2849 を参照してください。



(注)

- 3 種類すべてのアプライアンスでは、すべての LDAP アトリビュートが cVPN3000-Access-Hours のように cVPN3000 で始まります。
- アプライアンスは、数字の ID ではなくアトリビュート名に基づいて LDAP アトリビュートを使用します。一方、RADIUS アトリビュートには、名前ではなく数字の ID が使用されます。
- 認可では、権限またはアトリビュートを使用するプロセスを参照します。認証サーバまたは認可サーバとして定義されている LDAP サーバは、権限またはアトリビュートが設定されている場合はこれらを使用します。

表 E-2 に、セキュリティ アプライアンス、PIX Firewall および VPN 3000 の全アトリビュートのリストを示します。

すべての文字列では大文字と小文字が区別され、テーブル内ではアトリビュート名を大文字にする必要があります。用語の一般的な記述方式と矛盾する場合でも、この表記法に従ってください。たとえば、cVPN3000-IETF-RADIUS-Class ではなく、cVPN3000-IETF-Radius-Class を使用します。

**表 E-2 セキュリティ アプライアンスでサポートされる LDAP Cisco スキーマのアトリビュート**

| アトリビュート名 /OID (オブジェクト ID)         | VPN 3000 | ASA | PIX | アトリビュート OID <sup>1</sup> | シンタックス/タイプ | 単値または多値 | 取り得る値                                                                                                                                   |
|-----------------------------------|----------|-----|-----|--------------------------|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------|
| cVPN3000-Access-Hours             | Y        | Y   | Y   | 1                        | 文字列        | 単値      | time-range の名前 (Business-Hours など)                                                                                                      |
| cVPN3000-Simultaneous-Logins      | Y        | Y   | Y   | 2                        | 整数         | 単値      | 0-2147483647                                                                                                                            |
| cVPN3000-Primary-DNS              | Y        | Y   | Y   | 3                        | 文字列        | 単値      | IP アドレス                                                                                                                                 |
| cVPN3000-Secondary-DNS            | Y        | Y   | Y   | 4                        | 文字列        | 単値      | IP アドレス                                                                                                                                 |
| cVPN3000-Primary-WINS             | Y        | Y   | Y   | 5                        | 文字列        | 単値      | IP アドレス                                                                                                                                 |
| cVPN3000-Secondary-WINS           | Y        | Y   | Y   | 6                        | 文字列        | 単値      | IP アドレス                                                                                                                                 |
| cVPN3000-SEP-Card-Assignment      |          |     |     | 7                        | 整数         | 単値      | 使用しない                                                                                                                                   |
| cVPN3000-Tunneling-Protocols      | Y        | Y   | Y   | 8                        | 整数         | 単値      | 1 = PPTP<br>2 = L2TP<br>4 = IPSec<br>8 = L2TP/IPSec<br>16 = WebVPN<br>8 と 4 は相互排他値<br>(0 - 11、16 - 27 は有効値)                             |
| cVPN3000-IPSec-Sec-Association    | Y        |     |     | 9                        | 文字列        | 単値      | セキュリティ関連の名前                                                                                                                             |
| cVPN3000-IPSec-Authentication     | Y        |     |     | 10                       | 整数         | 単値      | 0 = なし<br>1 = RADIUS<br>2 = LDAP (認可のみ)<br>3 = NT ドメイン<br>4 = SDI<br>5 = 内部<br>6 = RADIUS での Expiry 認証<br>7 = Kerberos/Active Directory |
| cVPN3000-IPSec-Banner1            | Y        | Y   | Y   | 11                       | 文字列        | 単値      | バナー文字列                                                                                                                                  |
| cVPN3000-IPSec-Allow-Passwd-Store | Y        | Y   | Y   | 12                       | ブーリアン      | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                                                                 |
| cVPN3000-Use-Client-Address       | Y        |     |     | 13                       | ブーリアン      | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                                                                 |

## ■ 外部 LDAP サーバの設定

表 E-2 セキュリティ アプライアンスでサポートされる LDAP Cisco スキーマのアトリビュート (続き)

| アトリビュート名 /OID (オブジェクト ID)        | VPN 3000 | ASA | PIX | アトリビュート OID <sup>1</sup> | シンタックス/タイプ | 単値または多値 | 取り得る値                                                                                                    |
|----------------------------------|----------|-----|-----|--------------------------|------------|---------|----------------------------------------------------------------------------------------------------------|
| cVPN3000-PPTP-Encryption         | Y        |     |     | 14                       | 整数         | 単値      | ビットマップ：<br>1 = 暗号化が必要<br>2 = 40 ビット<br>4 = 128 ビット<br>8 = ステートレスが必要<br>例：15 = 40/128 ビットで暗号化 / ステートレスが必要 |
| cVPN3000-L2TP-Encryption         | Y        |     |     | 15                       | 整数         | 単値      | ビットマップ：<br>1 = 暗号化が必要<br>2 = 40 ビット<br>4 = 128 ビット<br>8 = ステートレスが必要<br>5 = 40/128 ビットで暗号化 / ステートレスが必要    |
| cVPN3000-IPSec-Split-Tunnel-List | Y        | Y   | Y   | 16                       | 文字列        | 単値      | スプリット トンネルの包含リストを表すネットワーク名またはアクセスリストを指定します。                                                              |
| cVPN3000-IPSec-Default-Domain    | Y        | Y   | Y   | 17                       | 文字列        | 単値      | クライアントに送信する単一のデフォルトのドメイン名 (1 ~ 255 文字) を指定します。                                                           |
| cVPN3000-IPSec-Split-DNS-Name    | Y        | Y   | Y   | 18                       | 文字列        | 単値      | クライアントに送信する単一のセカンダリ ドメイン名 (1 ~ 255 文字) のリストを指定します。                                                       |
| cVPN3000-IPSec-Tunnel-Type       | Y        | Y   | Y   | 19                       | 整数         | 単値      | 1 = LAN-to-LAN<br>2 = リモートアクセス                                                                           |
| cVPN3000-IPSec-Mode-Config       | Y        | Y   | Y   | 20                       | ブーリアン      | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                                  |
| cVPN3000-IPSec-User-Group-Lock   | Y        |     |     | 21                       | ブーリアン      | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                                  |
| cVPN3000-IPSec-Over-UDP          | Y        | Y   | Y   | 22                       | ブーリアン      | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                                  |
| cVPN3000-IPSec-Over-UDP-Port     | Y        | Y   | Y   | 23                       | 整数         | 単値      | 4001 ~ 49151、デフォルトは 10000                                                                                |
| cVPN3000-IPSec-Banner2           | Y        | Y   | Y   | 24                       | 文字列        | 単値      | バナー文字列                                                                                                   |
| cVPN3000-PPTP-MPPC-Compression   | Y        |     |     | 25                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                                  |

表 E-2 セキュリティ アプライアンスでサポートされる LDAP Cisco スキーマのアトリビュート (続き)

| アトリビュート名 /OID (オブジェクト ID)                      | VPN 3000 | ASA | PIX | アトリビュート OID <sup>1</sup> | シンタックス/タイプ | 単値または多値 | 取り得る値                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------|----------|-----|-----|--------------------------|------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cVPN3000-L2TP-MPPC-Compression                 | Y        |     |     | 26                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                                                                                                                                                                                                                                                          |
| cVPN3000-IPSec-IP-Compression                  | Y        | Y   | Y   | 27                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                                                                                                                                                                                                                                                          |
| cVPN3000-IPSec-IKE-Peer-ID-Check               | Y        | Y   | Y   | 28                       | 整数         | 単値      | 1 = 必須<br>2 = ピア証明書でサポートされる場合<br>3 = チェックしない                                                                                                                                                                                                                                                                                     |
| cVPN3000-IKE-Keep-Alives                       | Y        | Y   | Y   | 29                       | ブーリアン      | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                                                                                                                                                                                                                                                          |
| cVPN3000-IPSec-Auth-On-Rekey                   | Y        | Y   | Y   | 30                       | ブーリアン      | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                                                                                                                                                                                                                                                          |
| cVPN3000-Required-Client-Firewall-Vendor-Code  | Y        | Y   | Y   | 31                       | 整数         | 単値      | 1 = シスコシステムズ (Cisco Integrated Client を使用)<br>2 = Zone Labs<br>3 = NetworkICE<br>4 = Sygate<br>5 = シスコシステムズ (Cisco Intrusion Prevention Security Agent を使用)                                                                                                                                                                      |
| cVPN3000-Required-Client-Firewall-Product-Code | Y        | Y   | Y   | 32                       | 整数         | 単値      | シスコシステムズの製品：<br>1 = Cisco Intrusion Prevention Security Agent または Cisco Integrated Client (CIC)<br>Zone Labs の製品：<br>1 = Zone Alarm<br>2 = Zone AlarmPro<br>3 = Zone Labs Integrity<br>NetworkICE の製品：<br>1 = BlackIce Defender/Agent<br>Sygate の製品：<br>1 = Personal Firewall<br>2 = Personal Firewall Pro<br>3 = Security Agent |
| cVPN3000-Required-Client-Firewall-Description  | Y        | Y   | Y   | 33                       | 文字列        | 単値      | 文字列                                                                                                                                                                                                                                                                                                                              |

## ■ 外部 LDAP サーバの設定

表 E-2 セキュリティ アプライアンスでサポートされる LDAP Cisco スキーマのアトリビュート (続き)

| アトリビュート名 /OID (オブジェクト ID)                          | VPN 3000 | ASA | PIX | アトリビュート OID <sup>1</sup> | シンタックス/タイプ | 単値または多値 | 取り得る値                                                                                             |
|----------------------------------------------------|----------|-----|-----|--------------------------|------------|---------|---------------------------------------------------------------------------------------------------|
| cVPN3000-Require-Individual-User-Auth              | Y        | Y   | Y   | 34                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                           |
| cVPN3000-Require-HW-Client-Auth                    | Y        | Y   | Y   | 35                       | ブーリアン      | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                           |
| cVPN3000-Authenticated-User-Idle-Timeout           | Y        | Y   | Y   | 36                       | 整数         | 単値      | 1 ~ 35791394 分                                                                                    |
| cVPN3000-Cisco-IP-Phone-Bypass                     | Y        | Y   | Y   | 37                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                           |
| cVPN3000-IPSec-Split-Tunneling-Policy              | Y        | Y   | Y   | 38                       | 整数         | 単値      | 0 = すべてをトンネリング<br>1 = スプリット トンネリング<br>2 = ローカル LAN を許可                                            |
| cVPN3000-IPSec-Required-Client-Firewall-Capability | Y        | Y   | Y   | 39                       | 整数         | 単値      | 0 = なし<br>1 = リモート FW Are-You-There (AYT) で定義されているポリシー<br>2 = Policy Pushed CPP<br>4 = サーバからのポリシー |
| cVPN3000-IPSec-Client-Firewall-Filter-Name         | Y        |     |     | 40                       | 文字列        | 単値      | ファイアウォール ポリシーとしてクライアントに配信が必要なフィルタの名前を指定します。                                                       |
| cVPN3000-IPSec-Client-Firewall-Filter-Optional     | Y        | Y   | Y   | 41                       | 整数         | 単値      | 0 = 必須<br>1 = オプション                                                                               |
| cVPN3000-IPSec-Backup-Servers                      | Y        | Y   | Y   | 42                       | 文字列        | 単値      | 1 = Client-Configured リストを使用する<br>2 = クライアント リストをディセーブルにして消去する<br>3 = バックアップ サーバ リストを使用する         |
| cVPN3000-IPSec-Backup-Server-List                  | Y        | Y   | Y   | 43                       | 文字列        | 単値      | サーバ アドレス (スペースで区切る)                                                                               |
| cVPN3000-Client-Intercept-DHCP-Configure-Msg       | Y        | Y   | Y   | 44                       | ブーリアン      | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                           |
| cVPN3000-MS-Client-Subnet-Mask                     | Y        | Y   | Y   | 45                       | 文字列        | 単値      | IP アドレス                                                                                           |
| cVPN3000-Allow-Network-Extension-Mode              | Y        | Y   | Y   | 46                       | ブーリアン      | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                           |
| cVPN3000-Strip-Realm                               | Y        | Y   | Y   | 47                       | ブーリアン      | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                           |

表 E-2 セキュリティ アプライアンスでサポートされる LDAP Cisco スキーマのアトリビュート (続き)

| アトリビュート名 /OID (オブジェクト ID)                    | VPN 3000 | ASA | PIX | アトリビュート OID <sup>1</sup> | シンタックス/タイプ | 単値または多値 | 取り得る値                                                                                                                                                                                                                                             |
|----------------------------------------------|----------|-----|-----|--------------------------|------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cVPN3000-Cisco-AV-Pair                       | Y        | Y   | Y   | 48                       | 文字列        | 多値      | 次の形式のオクテット文字列<br>[Prefix] [Action] [Protocol]<br>[Source] [Source Wildcard Mask]<br>[Destination] [Destination Wildcard Mask] [Established]<br>[Log] [Operator] [Port]<br><br>詳細については、「 <a href="#">Cisco -AV-Pair アトリビュートのシンタックス</a> 」を参照してください。 |
| cVPN3000-User-Auth-Server-Name               | Y        |     |     | 49                       | 文字列        | 単値      | IP アドレスまたはホスト名                                                                                                                                                                                                                                    |
| cVPN3000-User-Auth-Server-Port               | Y        |     |     | 50                       | 整数         | 単値      | サーバ プロトコルのポート番号                                                                                                                                                                                                                                   |
| cVPN3000-User-Auth-Server-Secret             | Y        |     |     | 51                       | 文字列        | 単値      | サーバのパスワード                                                                                                                                                                                                                                         |
| cVPN3000-Confidence-Interval                 | Y        | Y   | Y   | 52                       | 整数         | 単値      | 10 ～ 300 秒                                                                                                                                                                                                                                        |
| cVPN3000-Cisco-LEAP-Bypass                   | Y        | Y   | Y   | 53                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                                                                                                                                                                           |
| cVPN3000-DHCP-Network-Scope                  | Y        | Y   | Y   | 54                       | 文字列        | 単値      | IP アドレス                                                                                                                                                                                                                                           |
| cVPN3000-Client-Type-Version-Limiting        | Y        | Y   | Y   | 55                       | 文字列        | 単値      | IPsec VPN クライアントのバージョン番号を示す文字列                                                                                                                                                                                                                    |
| cVPN3000-WebVPN-Content-Filter-Parameters    | Y        | Y   |     | 56                       | 整数         | 単値      | 1 = Java および ActiveX<br>2 = Java スクリプト<br>4 = イメージ<br>8 = イメージのクッキー<br><br>複数のパラメータをフィルタリングするには、上記の値を加算します。たとえば、Java スクリプトとクッキーの両方をフィルタリングするには、10 と入力します。(10 = 2 + 8)                                                                             |
| cVPN3000-WebVPN-Enable-functions             |          |     |     | 57                       | 整数         | 単値      | 未使用 - 推奨しない                                                                                                                                                                                                                                       |
| cVPN3000-WebVPN-Exchange-Server-Address      |          |     |     | 58                       | 文字列        | 単値      | 未使用 - 推奨しない                                                                                                                                                                                                                                       |
| cVPN3000-WebVPN-Exchange-Server-NETBIOS-Name |          |     |     | 59                       | 文字列        | 単値      | 未使用 - 推奨しない                                                                                                                                                                                                                                       |
| cVPN3000-Port-Forwarding-Name                | Y        | Y   |     | 60                       | 文字列        | 単値      | 名前を示す文字列<br>("Corporate-Apps" など)                                                                                                                                                                                                                 |
| cVPN3000-IETF-Radius-Framed-IP-Address       | Y        | Y   | Y   | 61                       | 文字列        | 単値      | IP アドレス                                                                                                                                                                                                                                           |
| cVPN3000-IETF-Radius-Framed-IP-Netmask       | Y        | Y   | Y   | 62                       | 文字列        | 単値      | IP アドレス                                                                                                                                                                                                                                           |

## ■ 外部 LDAP サーバの設定

表 E-2 セキュリティ アプライアンスでサポートされる LDAP Cisco スキーマのアトリビュート (続き)

| アトリビュート名 /OID (オブジェクト ID)                   | VPN 3000 | ASA | PIX | アトリビュート OID <sup>1</sup> | シンタックス/タイプ | 単値または多値 | 取り得る値                                                                                        |
|---------------------------------------------|----------|-----|-----|--------------------------|------------|---------|----------------------------------------------------------------------------------------------|
| cVPN3000-IETF-Radius-Session-Timeout        | Y        | Y   | Y   | 63                       | 整数         | 単値      | 1 ~ 35791394 分<br>0 = 制限なし                                                                   |
| cVPN3000-IETF-Radius-Idle-Timeout           | Y        | Y   | Y   | 64                       | 整数         | 単値      | 1 ~ 35791394 分<br>0 = 制限なし                                                                   |
| cVPN3000-IETF-Radius-Class                  | Y        | Y   | Y   | 65                       | 文字列        | 単値      | グループ名を示す文字列。次の 3 種類のうちいずれかの形式を使用します。<br><br>OU=Engineering<br>OU=Engineering;<br>Engineering |
| cVPN3000-IETF-Radius-Filter-Id              | Y        | Y   | Y   | 66                       | 文字列        | 単値      | アクセスリスト                                                                                      |
| cVPN3000-Authorization-Required             | Y        |     |     | 67                       | 整数         | 単値      | 0 = No<br>1 = Yes                                                                            |
| cVPN3000-Authorization-Type                 | Y        |     |     | 68                       | 整数         | 単値      | 0 = なし<br>1 = RADIUS<br>2 = LDAP                                                             |
| cVPN3000-DN-Field                           | Y        | Y   | Y   | 69                       | 文字列        | 単値      | 取り得る値: UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER、use-entire-name。                       |
| cVPN3000-WebVPN-URL-List                    |          | Y   |     | 70                       | 文字列        | 単値      | URL リスト名                                                                                     |
| cVPN3000-WebVPN-Forwarded-Ports             |          | Y   |     | 71                       | 文字列        | 単値      | ポート転送リスト名                                                                                    |
| cVPN3000-WebVPN-ACL-Filters                 |          | Y   |     | 72                       | 文字列        | 単値      | アクセスリスト名                                                                                     |
| cVPN3000-WebVPN-Homepage                    | Y        | Y   |     | 73                       | 文字列        | 単値      | http://example-portal.com などの URL                                                            |
| cVPN3000-WebVPN-Single-Sign-On-Server-Name  |          | Y   |     | 74                       | 文字列        | 単値      | SSO サーバの名前(1 ~ 31 文字)                                                                        |
| cVPN3000-WebVPN-URL-Entry-Enable            | Y        | Y   |     | 75                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                      |
| cVPN3000-WebVPN-File-Access-Enable          | Y        | Y   |     | 76                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                      |
| cVPN3000-WebVPN-File-Server-Entry-Enable    | Y        | Y   |     | 77                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                      |
| cVPN3000-WebVPN-File-Server-Browsing-Enable | Y        | Y   |     | 78                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                      |
| cVPN3000-WebVPN-Port-Forwarding-Enable      | Y        | Y   |     | 79                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                                                                      |



表 E-2 セキュリティ アプライアンスでサポートされる LDAP Cisco スキーマのアトリビュート (続き)

| アトリビュート名 /OID (オブジェクト ID)                             | VPN 3000 | ASA | PIX | アトリビュート OID <sup>1</sup> | シンタックス/タイプ | 単値または多値 | 取り得る値                                         |
|-------------------------------------------------------|----------|-----|-----|--------------------------|------------|---------|-----------------------------------------------|
| cVPN3000-WebVPN-Port-Forwarding-Exchange-Proxy-Enable | Y        | Y   |     | 80                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                       |
| cVPN3000-WebVPN-Port-Forwarding-HTTP-Proxy-Enable     | Y        | Y   |     | 81                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                       |
| cVPN3000-WebVPN-Port-Forwarding-Auto-Download-Enable  | Y        | Y   |     | 82                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                       |
| cVPN3000-WebVPN-Citrix-Support-Enable                 | Y        | Y   |     | 83                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                       |
| cVPN3000-WebVPN-Apply-ACL-Enable                      | Y        | Y   |     | 84                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                       |
| cVPN3000-WebVPN-SVC-Enable                            | Y        | Y   |     | 85                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                       |
| cVPN3000-WebVPN-SVC-Required-Enable                   | Y        | Y   |     | 86                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                       |
| cVPN3000-WebVPN-SVC-Keep-Enable                       | Y        | Y   |     | 87                       | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル                       |
| cVPN3000-IE-Proxy-Server                              | Y        |     |     | 88                       | 文字列        | 単値      | IP アドレス                                       |
| cVPN3000-IE-Proxy-Method                              | Y        |     |     | 89                       | 整数         | 単値      | 1 = 変更なし<br>2 = プロキシなし<br>3 = 自動検出<br>4 = その他 |
| cVPN3000-IE-Proxy-Exception-List                      | Y        |     |     | 90                       | 文字列        | 単値      | 改行 (\n) で区切られた DNS ドメインのリスト                   |
| cVPN3000-IE-Proxy-Bypass-Local                        | Y        |     |     | 91                       | 整数         | 単値      | 0 = なし<br>1 = ローカル                            |
| cVPN3000-Tunnel-Group-Lock                            |          | Y   | Y   | 92                       | 文字列        | 単値      | トンネルグループの名前または「none」                          |
| cVPN3000-Firewall-ACL-In                              |          | Y   | Y   | 93                       | 文字列        | 単値      | アクセスリストの ID                                   |
| cVPN3000-Firewall-ACL-Out                             |          | Y   | Y   | 94                       | 文字列        | 単値      | アクセスリストの ID                                   |
| cVPN3000-PFS-Required                                 | Y        | Y   | Y   | 95                       | ブーリアン      | 単値      | 0 = No<br>1 = Yes                             |
| cVPN3000-WebVPN-SVC-Keepalive                         | Y        | Y   |     | 96                       | 整数         | 単値      | 0 = ディセーブル<br>n = キープアライブ値 (15 ~ 600 秒)       |

## ■ 外部 LDAP サーバの設定

表 E-2 セキュリティ アプライアンスでサポートされる LDAP Cisco スキーマのアトリビュート (続き)

| アトリビュート名 /OID (オブジェクト ID)        | VPN 3000 | ASA | PIX | アトリビュート OID <sup>1</sup> | シンタックス/タイプ | 単値または多値 | 取り得る値                                               |
|----------------------------------|----------|-----|-----|--------------------------|------------|---------|-----------------------------------------------------|
| cVPN3000-WebVPN-SVC-Client-DPD   | Y        | Y   |     | 97                       | 整数         | 単値      | 0 = ディセーブル<br>n = デッド ピア 検知 値 (30 ～ 3600 秒)         |
| cVPN3000-WebVPN-SVC-Gateway-DPD  | Y        | Y   |     | 98                       | 整数         | 単値      | 0 = ディセーブル<br>n = デッド ピア 検知 値 (30 ～ 3600 秒)         |
| cVPN3000-WebVPN-SVC-Rekey-Period | Y        | Y   |     | 99                       | 整数         | 単値      | 0 = ディセーブル<br>n = リトライ間隔(4 ～ 10080 分)               |
| cVPN3000-WebVPN-SVC-Rekey-Method | Y        | Y   |     | 100                      | 整数         | 単値      | 0 = なし<br>1 = SSL<br>2 = 新規トンネル<br>3 = 任意 (SSL に設定) |
| cVPN3000-WebVPN-SVC-Compression  | Y        | Y   |     | 101                      | 整数         | 単値      | 0 = なし<br>1 = デフレート圧縮                               |

1. 各アトリビュートの完全なオブジェクト ID を取得するには、1.2.840.113556.8000.795.2 の最後にこのカラムの数字を追加します。すなわち、テーブルの最初のアトリビュートの cVPN3000-Access-Hours の OID は、1.2.840.113556.8000.795.2.1 です。同様に、テーブルの最後のアトリビュートである cVPN3000-WebVPN-SVC-Compression の OID は、1.2.840.113556.8000.795.2.115 になります。

## Cisco -AV-Pair アトリビュートのシンタックス

各 Cisco-AV-Pair ルールのシンタックスは次のとおりです。

[Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask]  
[Established] [Log] [Operator] [Port]:

| フィールド                     | 説明                                                                                                                       |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Prefix                    | AV ペアの固有の識別子。たとえば、ip:inacl#1= (標準 ACL で使用) または webvpn:inacl# (WebVPN ACL で使用)。このフィールドが表示されるのは、フィルタが AV ペアとして送信されている場合です。 |
| Action                    | ルールが一致した場合に実行するアクション: deny、permit。                                                                                       |
| Protocol                  | IP プロトコルを示す番号またはその名前。0 ～ 255 の整数値、またはキーワード: icmp、igmp、ip、tcp、udp。                                                        |
| Source                    | パケットの送信元のネットワークまたはホスト。IP アドレス、ホスト名、またはキーワード「any」を指定します。IP アドレスを指定する場合には、下記の Source Wildcard Mask も続けて指定する必要があります。        |
| Source Wildcard Mask      | ソース アドレスに適用されるワイルドカード マスク。                                                                                               |
| Destination               | パケットの送信先のネットワークまたはホスト。IP アドレス、ホスト名、またはキーワード「any」を指定します。IP アドレスを指定する場合には、下記の Destination Wildcard Mask も続けて指定する必要があります。   |
| Destination Wildcard Mask | 宛先アドレスに適用されるワイルドカード マスク。                                                                                                 |

| フィールド    | 説明                                                               |
|----------|------------------------------------------------------------------|
| Log      | FILTER ログ メッセージを生成します。重大度レベル 9 のイベントを生成するには、このキーワードを使用する必要があります。 |
| Operator | 論理演算子：greater than、less than、equal to、not equal to。              |
| Port     | TCP ポート番号または UDP ポート番号 (0 ～ 65535)。                              |

次の例を参考にしてください。

```
ip:inacl#1=deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
ip:inacl#2=permit TCP any host 10.160.0.1 eq 80 log
```

```
webvpn:inacl#1=permit url http://www.cnn.com
webvpn:inacl#2=deny smtp any host 10.1.3.5
webvpn:inacl#3=permit url cifs://mar_server/peopleshare1
```



(注)

- リモートの IPsec および SSL VPN クライアント (SVC) トンネルの場合、Cisco-AV ペア エントリにプレフィックス ip:inacl# を付けて ACL を使用してください。
- WebVPN クライアントレス (ブラウザモード) のトンネルの場合、Cisco-AV ペア エントリにプレフィックス webvpn:inacl# を付けて ACL を使用してください。

表 E-3 では、Cisco-AV-Pair アトリビュートのトークンをリストで示します。

表 E-3 セキュリティ アプライアンスでサポートするトークン

| トークン              | シンタックスのフィールド | 説明                                                                                                    |
|-------------------|--------------|-------------------------------------------------------------------------------------------------------|
| ip:inacl#Num=     | なし (識別子)     | (Num は一意の整数。) AV ペアによるアクセス コントロール リストをすべて開始します。リモート IPsec および SSL VPN (SVC) トンネルに強制的に ACL を適用します。     |
| webvpn:inacl#Num= | なし (識別子)     | (Num は一意の整数。) WebVPN AV ペアによるアクセス コントロール リストをすべて開始します。WebVPN クライアントレス (ブラウザモード) トンネルに強制的に ACL を適用します。 |
| deny              | Action       | アクションを拒否します (デフォルト)。                                                                                  |
| permit            | Action       | アクションを許可します。                                                                                          |
| icmp              | Protocol     | Internet Control Message Protocol (ICMP; インターネット制御メッセージ プロトコル)。                                       |
| 1                 | Protocol     | Internet Control Message Protocol (ICMP; インターネット制御メッセージ プロトコル)。                                       |
| IP                | Protocol     | Internet Protocol (IP; インターネット プロトコル)。                                                                |
| 0                 | Protocol     | Internet Protocol (IP; インターネット プロトコル)。                                                                |
| TCP               | Protocol     | Transmission Control Protocol (TCP; 伝送制御プロトコル)。                                                       |
| 6                 | Protocol     | Transmission Control Protocol (TCP; 伝送制御プロトコル)。                                                       |
| UDP               | Protocol     | User Datagram Protocol (UDP; ユーザ データグラム プロトコル)。                                                       |
| 17                | Protocol     | User Datagram Protocol (UDP; ユーザ データグラム プロトコル)。                                                       |
| any               | Hostname     | すべてのホストにルールを適用します。                                                                                    |
| host              | Hostname     | ホスト名を示す任意の英数字による文字列。                                                                                  |

## ■ 外部 LDAP サーバの設定

表 E-3 セキュリティ アプライアンスでサポートするトークン

| トークン  | シンタックスのフィールド | 説明                                                        |
|-------|--------------|-----------------------------------------------------------|
| log   | Log          | イベントが該当すると、フィルタ ログ メッセージが表示されます。(イベント許可または拒否によるログに記録と同様)。 |
| lt    | Operator     | 指定された値より小さい                                               |
| gt    | Operator     | 指定された値より大きい                                               |
| eq    | Operator     | 指定された値と等しい                                                |
| neq   | Operator     | 指定された値と等しくない                                              |
| range | Operator     | 含まれる値の範囲。range の後に、2 つの値が続きます。                            |

## セキュリティ アプライアンスの認可スキーマの例

この項では、LDAP スキーマの例を示します。このスキーマは、セキュリティ アプライアンスのクラスとアトリビュートをサポートしています。このスキーマは、Microsoft Active Directory LDAP サーバに固有です。ユーザ自身の LDAP サーバのスキーマを定義するために、表 E-2 をモデルとして使用してください。

## Schema 3k\_schema.ldif

```
dn:
CN=cVPN3000-Access-Hours,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
changetype: add
adminDisplayName: cVPN3000-Access-Hours
attributeID: 1.2.840.113556.1.8000.795.2.1
attributeSyntax: 2.5.5.3
cn: cVPN3000-Access-Hours
instanceType: 4
isSingleValued: TRUE
LDAPDisplayName: cVPN3000-Access-Hours
distinguishedName:

CN=cVPN3000-Access-Hours,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectCategory:
CN=Attribute-Schema,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectClass: attributeSchema
oMSyntax: 27
name: cVPN3000-Access-Hours
showInAdvancedViewOnly: TRUE

....
.... (define subsequent security appliance authorization attributes here)
....

dn:
CN=cVPN3000-Primary-DNS,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
changetype: add
adminDisplayName: cVPN3000-Primary-DNS
attributeID: 1.2.840.113556.1.8000.795.2.3
attributeSyntax: 2.5.5.3
cn: cVPN3000-Primary-DNS
instanceType: 4
isSingleValued: TRUE
LDAPDisplayName: cVPN3000-Primary-DNS
distinguishedName:
```

```

CN=cVPN3000-Primary-DNS,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectCategory:
  CN=Attribute-Schema,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectClass: attributeSchema
oMSyntax: 27
name: cVPN3000-Primary-DNS
showInAdvancedViewOnly: TRUE

.....
.... (define subsequent security appliance authorization attributes here)
....

dn:
CN=cVPN3000-Confidence-Interval,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
changetype: add
adminDisplayName: cVPN3000-Confidence-Interval
attributeID: 1.2.840.113556.1.8000.795.2.52
attributeSyntax: 2.5.5.9
cn: cVPN3000-Confidence-Interval
instanceType: 4
isSingleValued: TRUE
LDAPDisplayName: cVPN3000-Confidence-Interval
distinguishedName:

CN=cVPN3000-Confidence-Interval,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectCategory:

DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-

dn:
CN=cVPN3000-User-Authorization,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
changetype: add
adminDisplayName: cVPN3000-User-Authorization
adminDescription: Cisco Class Schema
cn: cVPN3000-User-Authorization
defaultObjectCategory:

CN=cVPN3000-User-Authorization,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
defaultSecurityDescriptor:
  D: (A;;RPWPCCDCLCLORCWOWSDDDTDTSW;;;DA) (A;;RPWPCCDCLCLORCWOWSDDDTDTSW;;;SY)
  (A;;RPLCLORC;;;AU)
governsID: 1.2.840.113556.1.8000.795.1.1
instanceType: 4
LDAPDisplayName: cVPN3000-User-Authorization

mustContain: cn
mayContain: cVPN3000-Access-Hours
mayContain: cVPN3000-Simultaneous-Logins
mayContain: cVPN3000-Primary-DNS
...
mayContain: cVPN3000-Confidence-Interval
mayContain: cVPN3000-Cisco-LEAP-Bypass

distinguishedName:

CN=cVPN3000-User-Authorization,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectCategory:
  CN=Class-Schema,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com

```

```
objectClass: classSchema
objectClassCategory: 1
possSuperiors: organizationalUnit
name: cVPN3000-User-Authorization
rDNAttID: cn
showInAdvancedViewOnly: TRUE
subClassOf: top
systemOnly: FALSE
```

```
DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
systemOnly: FALSE
```

```
DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

## LDAP サーバへのスキーマのロード



(注)

この項の手順は、Microsoft Active Directory LDAP サーバに固有のものです。別のタイプのサーバを使用している場合、スキーマをロードするときの詳細についてはサーバのマニュアルを参照してください。

LDAP サーバ上にスキーマをロードするには、スキーマ ファイルが常駐しているディレクトリから `ldifde -i -f Schema Name` とコマンドを入力します。例：`ldifde -i -f 3k_schema.ldif`

## ユーザ権限の定義



(注)

この項の手順は、Microsoft Active Directory LDAP サーバに固有のものです。別のタイプのサーバを使用している場合は、サーバのマニュアルを参照してユーザの属性を定義およびロードしてください。

LDAP サーバへのユーザの認可については、ユーザ ファイルを定義します。ユーザ ファイルは、すべてのセキュリティ アプライアンスの属性および特定のユーザに関連付けられている値を定義します。各ユーザは、クラス `cVPN3000-User-Authorization` のオブジェクトです。ユーザ ファイルを定義するには、テキスト エディタを使用しますファイルの拡張子は `.ldif` にします (ユーザ ファイルの例については、[Robin.ldif](#) を参照してください)。

LDAP サーバ上にユーザ ファイルをロードするには、`ldap_user.ldif` ファイルが常駐しているディレクトリで、`ldifde -i -f ldap_user.ldif` とコマンドを入力します。例：`ldifde -i -f Robin.ldif`

スキーマとユーザ ファイルの両方を作成してロードすると、LDAP サーバは、セキュリティ アプライアンスの認可要求を処理することができるようになります。

## ユーザ ファイルの例

この項では、ユーザ Robin に対するユーザ ファイルの例について説明します。

### Robin.ldif

```
dn: cn=Robin,OU=People,DC=ExampleCorporation,DC=com
changetype: add
cn: Robin
CVPN3000-Access-Hours: Corporate_time
cVPN3000-Simultaneous-Logins: 2
cVPN3000-IPSec-Over-UDP: TRUE
CVPN3000-IPSec-Over-UDP-Port: 12125
cVPN3000-IPSec-Banner1: Welcome to the Example Corporation!!!
cVPN3000-IPSec-Banner2: Unauthorized access is prohibited!!!!!!
cVPN3000-Primary-DNS: 10.10.4.5
CVPN3000-Secondary-DNS: 10.11.12.7
CVPN3000-Primary-WINS: 10.20.1.44
CVPN3000-SEP-Card-Assignment: 1
CVPN3000-IPSec-Tunnel-Type: 2
CVPN3000-Tunneling-Protocols: 7
cVPN3000-Confidence-Interval: 300
cVPN3000-IPSec-Allow-Passwd-Store: TRUE
objectClass: cVPN3000-User-Authorization
```

## Active Directory の設定の確認

この項では、Microsoft Active Directory サーバを使用するセキュリティ アプライアンスで認証および認可を設定する手順について説明します。次の項目について説明します。

- [例 1：Microsoft Active Directory を使用した LDAP 認可の設定（ASA/PIX）](#)
- [例 2: Microsoft Active Directory を使用した LDAP 認可の設定](#)
- [例 3: Microsoft Active Directory を使用した LDAP 認証および LDAP 認可](#)

### 例 1：Microsoft Active Directory を使用した LDAP 認可の設定（ASA/PIX）

この例では、SDI を使用した認証の手順、および LDAP と Microsoft Active Directory（AD）を使用した認可の手順について示します。このサンプル手順を実行するには、次の手順を実行します。

- ステップ 1** LDIF ファイルを使用して、Microsoft AD データベースに cVPN3000-User-Authorization レコードを作成します。このレコードには、ユーザの Cisco VPN 認可アトリビュートが含まれています。



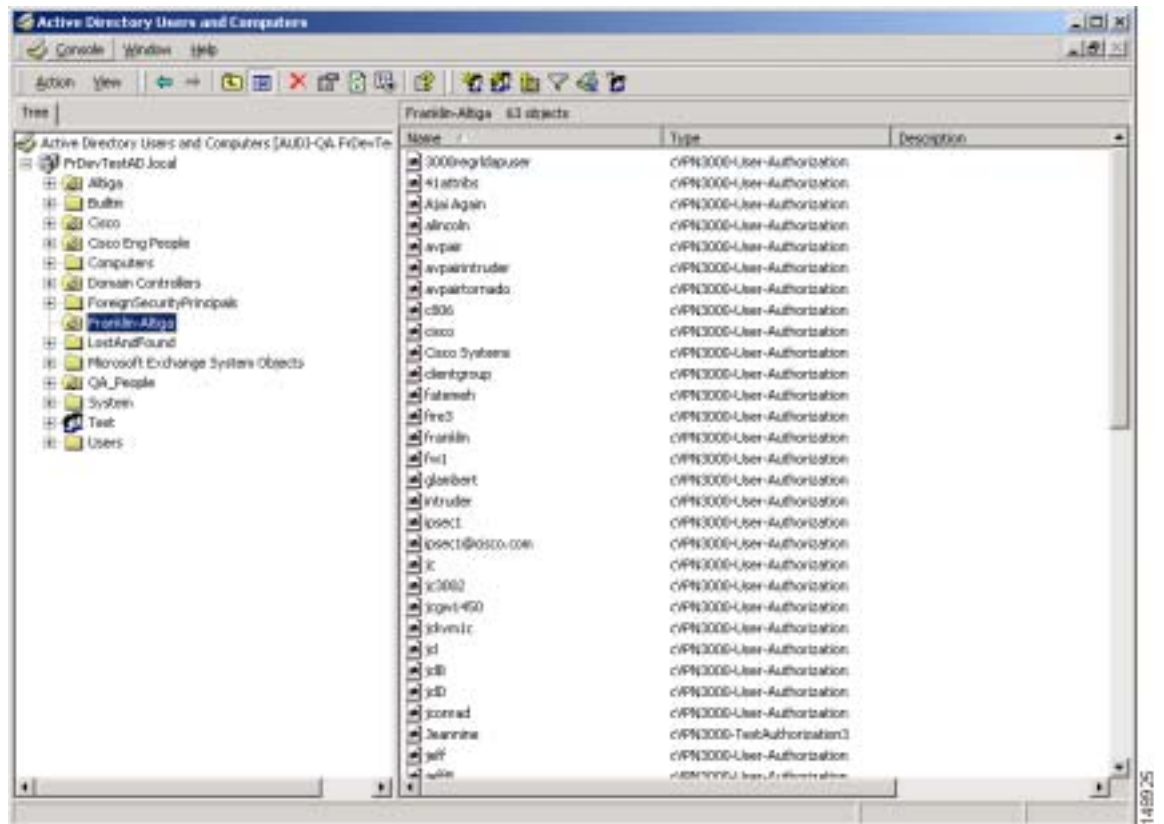
(注)

Cisco TAC に問い合せて、Cisco VPN アトリビュート用の Microsoft AD LDAP スキーマを入手します。

- ステップ 2** 新規レコードを確認するには、**Start > Settings > Control Panel > Administrative Tools > Active Directory Users and Computers** の順にクリックします。

[図 E-2](#) に示すように、Active Directory Users and Computers ウィンドウが表示されます。

図 E-2 Active Directory Users and Computers ウィンドウ



**ステップ 3** セキュリティ アプライアンスで、LDAP サーバ用の aaa-server レコードを作成します。例では、これらの認可レコードは Franklin-Altiga フォルダに保存されます。ここで必要な手順は、次のコマンドで示すとおりです。

```
hostname(config)# aaa-server ldap-authorize-grp protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap-authorize-grp host 10.1.1.4
hostname(config-aaa-server-host)# ldap-base-dn ou=Franklin-Altiga,dc=frdevtestad,dc=local
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)# ldap-login-password anypassword
hostname(config-aaa-server-host)# ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
hostname(config-aaa-server-host)# ldap-attribute-map LdapSvrName
hostname(config-aaa-server-host)#
```

**ステップ 4** 次のコマンド例のとおりに実行して、SDI 認証および LDAP 認可を指定するトンネルグループを作成します。

```
hostname(config)# tunnel-group ipsec-tunnelgroup type ipsec-ra
hostname(config)# tunnel-group ipsec-tunnelgroup general-attributes
hostname(config)# authentication-server-group sdi-group
hostname(config)# authorization-server-group ldap-authorize-group
hostname(config)#
```



(注)

この例では、sdi-group の設定は示していません。

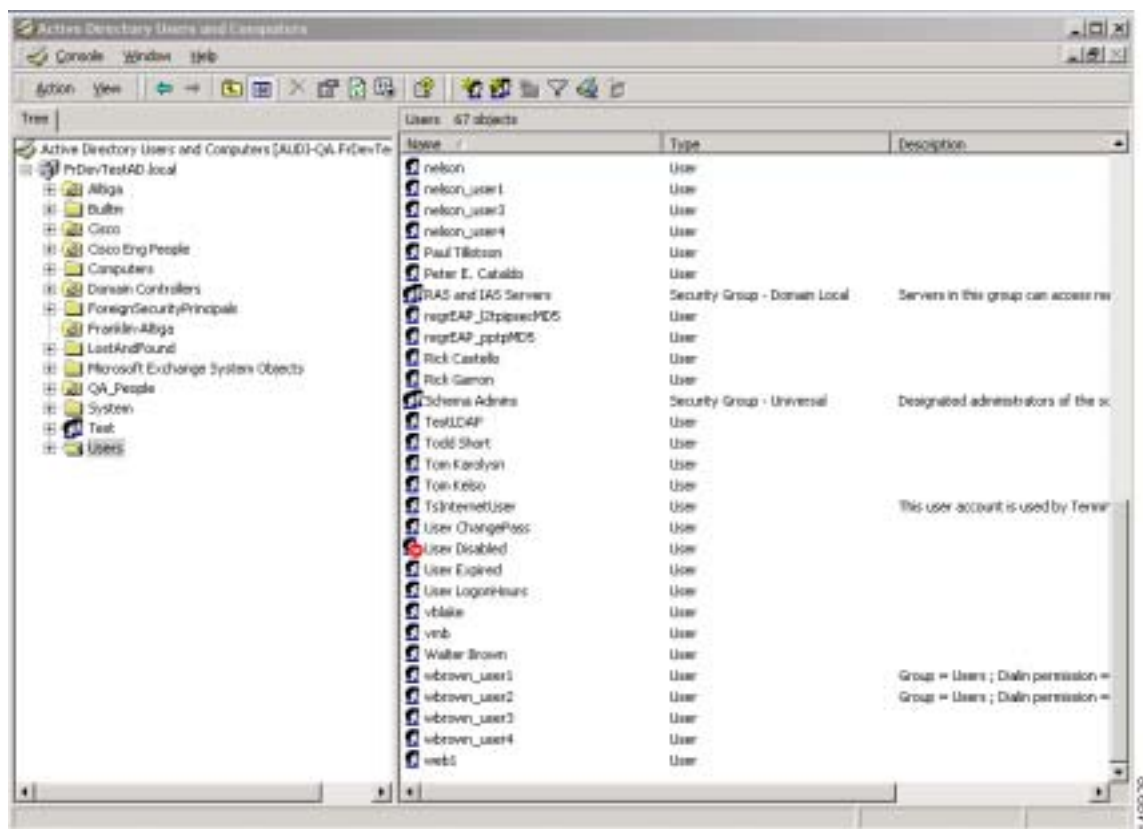


## 例 2: Microsoft Active Directory を使用した LDAP 認可の設定

この例では、Microsoft Active Directory を使用した LDAP 認証の手順について例を示します。伝送中のユーザ クレデンシャルを確保するため、この手順では、SSL 接続を介して LDAP ディレクトリとのメッセージ交換を行うようにセキュリティ アプライアンスを設定します。また、ユーザに割り当てられるグループポリシーとしての Microsoft AD ユーザ レコードの部署アトリビュートを解釈するようにセキュリティ アプライアンスを設定します。このグループの認可アトリビュートは RADIUS サーバから取得します。

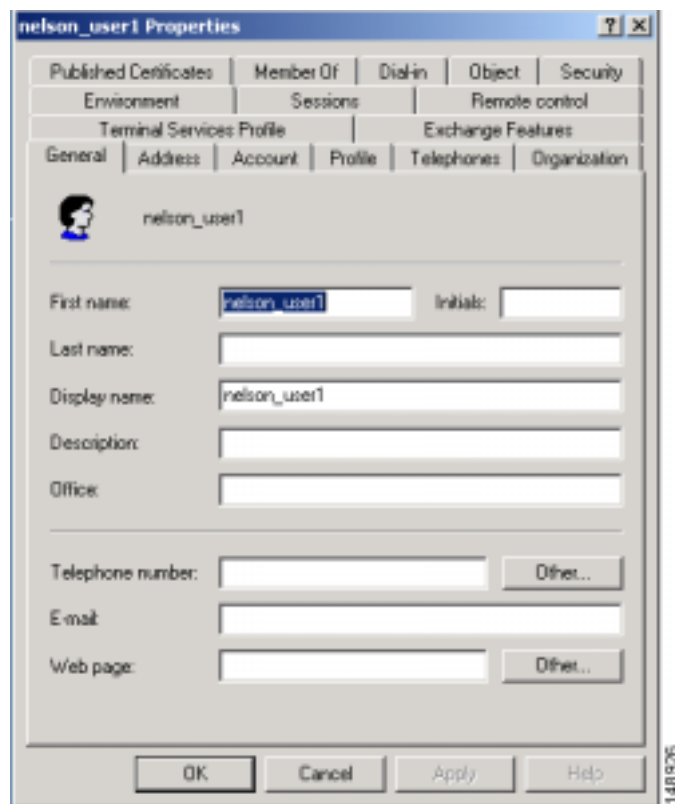
図 E-3 の Active Directory Users and Computers ウィンドウに表示されている Users フォルダをクリックすると、ユーザ レコードを確認できます。

図 E-3 Users フォルダが表示された Active Directory Users and Computers ウィンドウ



特定のユーザ アトリビュートや値を確認するには、ユーザ名を右クリックしてから Properties をクリックします。図 E-4 に、ユーザ名のプロパティ ダイアログボックスを示します。

図 E-4 ユーザ名のプロパティ ダイアログボックス



(注)

部署アトリビュートは、Active Directory Users and Computers ウィンドウの Organization タブで設定されています。

この例のとおり設定するには、セキュリティ アプライアンスで次の手順を実行します。

- ステップ 1** LDAP 認証サーバ用の aaa-server レコードを作成し、ldap-base-dn を使用して、Active Directory ユーザ レコードの検索場所を次のコマンド例のとおり指定します。

```
hostname(config)# aaa-server ldap-authenticate-grp protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap-authenticate-grp host 10.1.1.4
hostname(config-aaa-server-host)# ldap-base-dn cn=Users,dc=frdevtestad,dc=local
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)# ldap-login-password anypassword
hostname(config-aaa-server-host)# ldap-login-dn cn=Administrator,cn=Users,
dc=frdevtestad,dc=local
hostname(config-aaa-server-host)#
```

- ステップ 2** 次のコマンド例のとおり実行して、AD アトリビュート department をシスコのアトリビュート cVPN3000-IETF-Radius-Class にマッピングするための LDAP マッピング テーブルを作成します。

```
hostname(config)# ldap attribute-map ActiveDirectoryMapTable
hostname(config-ldap-attribute-map)# map-name department cVPN3000-IETF-Radius-Class
hostname(config-ldap-attribute-map)#
```

**ステップ 3** 次のコマンド例のとおり実行して、LDAP アトリビュート マップの名前を設定します。

```
hostname(config-aaa-server-host)# ldap-attribute-map ActiveDirectoryMapTable  
hostname(config-aaa-server-host)#
```

**ステップ 4** セキュアな LDAP 接続を次のように指定します。

```
hostname(config-aaa-server-host)# ldap-over-ssl enable  
hostname(config-aaa-server-host)#
```

**ステップ 5** グループ名と RADIUS サーバとを関連付ける外部グループポリシーを作成します。例では、次のコマンドで示すように、ユーザはグループ Engineering に関連付けられます。

```
hostname(config-aaa-server-host)# group-policy Engineering external server-group  
radius-group password anypassword  
hostname(config-aaa-server-host)#
```

**ステップ 6** 次のコマンド例のとおり実行して、LDAP 認証を指定するトンネルグループを作成します。

```
hostname(config)# tunnel-group ipsec-tunnelgroup type ipsec-ra  
hostname(config)# tunnel-group ipsec-tunnelgroup general-attributes  
hostname(config-tunnel-general)# authentication-server-group ldap-authenticate-grp  
hostname(config-tunnel-general)#
```



(注)

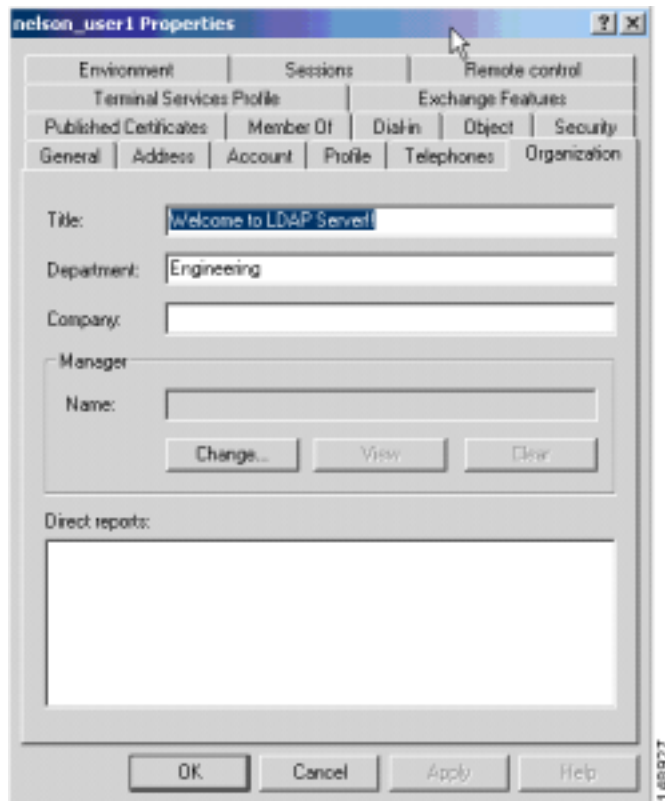
この例では、radius-group の設定は示していません。

### 例 3: Microsoft Active Directory を使用した LDAP 認証および LDAP 認可

この例では、LDAP と Microsoft Active Directory を使用して、認証と認可の両方を設定する手順を示します。Microsoft ユーザレコードでは、部署アトリビュートはユーザの group-name として解釈されます。この group-name の認可アトリビュートは Active Directory サーバから取得します。

部署アトリビュートは、[図 E-5](#) に示すように、Active Directory Users and Computers ウィンドウの Organization タブで設定されます。

図 E-5 Active Directory Users and Computer ダイアログの Organization タブ



この例のとおり設定するには、セキュリティアプライアンスで次の手順を実行します。

- ステップ 1** 次のコマンド例のとおり実行して、Active Directory アトリビュート department をシスコのアトリビュート cVPN3000-IETF-Radius-Class にマッピングするための LDAP マッピングテーブルを作成します。

```
hostname(config)# ldap attribute-map ActiveDirectoryMapTable
hostname(config-ldap-attribute-map)# map-name department cVPN3000-IETF-Radius-Class
```

- ステップ 2** LDAP 認証サーバ用の aaa-server レコードを作成し、ldap-base-dn を使用して、Active Directory ユーザ レコードの検索場所を次のコマンド例のとおり指定します。

```
hostname(config)# aaa-server ldap-authenticate protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap-authenticate host 10.1.1.4
hostname(config-aaa-server-host)# ldap-base-dn cn=Users,dc=frdevtestad,dc=local
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)# ldap-login-password anypassword
hostname(config-aaa-server-host)# ldap-login-dn cn=Administrator,cn=Users,
dc=frdevtestad,dc=local
hostname(config-aaa-server-host)#
```

- ステップ 3** 次のコマンド例のとおり実行して、LDAP アトリビュート マップの名前を設定します。

```
hostname(config-aaa-server-host)# ldap-attribute-map ActiveDirectoryMapTable
hostname(config-aaa-server-host)#
```

- ステップ 4** セキュアな LDAP 接続を次のように指定します。

```
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)#
```

- ステップ 5** LDAP 認可を設定するための aaa-server レコードを作成し、ldap-base-dn を使用して、シスコの cVPN3000-User-Authorization レコードの検索場所を次のコマンド例のとおり指定します。

```
hostname(config-aaa-server-host)# aaa-server ldap-authorize protocol ldap
hostname(config-aaa-server-host)# aaa-server ldap-authorize host 10.1.1.4
hostname(config-aaa-server-host)# ldap-base-dn ou=Franklin-Altiga,dc=frdevtestad,
dc=local
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)# ldap-login-password anypassword
hostname(config-aaa-server-host)# ldap-login-dn cn=Administrator,cn=Users,
dc=frdevtestad,dc=local
hostname(config-aaa-server-host)#
```

- ステップ 6** group-name と LDAP 認可サーバとを関連付ける外部グループポリシーを作成します。次のコマンドで示すように、ユーザはグループ Engineering に関連付けられます。

```
hostname(config-aaa-server-host)# group-policy engineering external server-group
ldap-authorize
hostname(config-aaa-server-host)#
```

- ステップ 7** 次のコマンド例のとおり実行して、LDAP 認証を指定するトンネルグループを作成します。

```
hostname(config)# tunnel-group ipsec-tunnelgroup type ipsec-ra
hostname(config)# tunnel-group ipsec-tunnelgroup general-attributes
hostname(config-tunnel-general)# authentication-server-group ldap-authenticate
hostname(config-tunnel-general)#
```

## 外部 RADIUS サーバの設定

この項では、RADIUS を設定する手順の概要を示し、Cisco RADIUS アトリビュートを定義します。次の項目について説明します。

- [RADIUS 設定の手順の確認](#)
- [セキュリティ アプライアンスの RADIUS 認可アトリビュート](#)

### RADIUS 設定の手順の確認

この項では、セキュリティ アプライアンスのユーザの認証および認可をサポートするために必要な RADIUS 設定の手順を示します。次の手順に従って、セキュリティ アプライアンスと相互作用する RADIUS サーバをセットアップします。

**ステップ 1** セキュリティ アプライアンスのアトリビュートを RADIUS サーバにロードします。アトリビュートをロードするために使用する方法は、使用する RADIUS サーバのタイプによって異なります。

- Cisco ACS を使用している場合：サーバにはこれらのアトリビュートがすでに統合されています。この場合は、この手順を省略できます。
- FUNK RADIUS サーバを使用している場合：シスコでは、セキュリティ アプライアンスのアトリビュートがすべて含まれているディクショナリ ファイルを提供しています。このディクショナリ ファイル `cisco3k.dct` は、CCO のソフトウェア センターまたはセキュリティ アプライアンスの CD-ROM から入手してください。ディクショナリ ファイルをサーバにロードします。
- 他のベンダーの RADIUS サーバ（Microsoft Internet Authentication Service など）：セキュリティ アプライアンスの各アトリビュートを手作業で定義する必要があります。アトリビュートを定義するには、アトリビュート名または番号、タイプ、値、ベンダー コード（3076）が必要です。セキュリティ アプライアンス RADIUS 認可アトリビュートと値のリストについては、[表 E-4](#) を参照してください。

**ステップ 2** 権限のあるユーザまたはグループをセットアップし、IPSec/WebVPN トンネル確立時に送信します。権限またはアトリビュートには、アクセス時間、プライマリ DNS、バナーなどが含まれていることがあります。

### セキュリティ アプライアンスの RADIUS 認可アトリビュート



(注)

認可では、権限またはアトリビュートを使用するプロセスを参照します。認証サーバとして定義されている RADIUS サーバは、権限またはアトリビュートが設定されている場合はこれらを使用します。

[表 E-4](#) は、ユーザ認可に使用可能で、セキュリティ アプライアンス対応の取り得るすべてのアトリビュートをリスト表示したものです。

表 E-4 セキュリティ アプライアンスがサポートしている RADIUS のアトリビュートと値

| アトリビュート名                 | VPN<br>3000 | ASA | PIX | アトリ<br>ビュート<br>番号 # | シンタッ<br>クス/<br>タイプ | 単値<br>または<br>多値 | 単値または多値                                                                                                                                 |
|--------------------------|-------------|-----|-----|---------------------|--------------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Access-Hours             | Y           | Y   | Y   | 1                   | 文字列                | 単値              | 時間の範囲の名前。<br>例: Business-hours                                                                                                          |
| Simultaneous-Logins      | Y           | Y   | Y   | 2                   | 整数                 | 単値              | 0 ~ 2147483647 の整数                                                                                                                      |
| Primary-DNS              | Y           | Y   | Y   | 5                   | 文字列                | 単値              | IP アドレス                                                                                                                                 |
| Secondary-DNS            | Y           | Y   | Y   | 6                   | 文字列                | 単値              | IP アドレス                                                                                                                                 |
| Primary-WINS             | Y           | Y   | Y   | 7                   | 文字列                | 単値              | IP アドレス                                                                                                                                 |
| Secondary-WINS           | Y           | Y   | Y   | 8                   | 文字列                | 単値              | IP アドレス                                                                                                                                 |
| SEP-Card-Assignment      |             |     |     | 9                   | 整数                 | 単値              | 使用しない                                                                                                                                   |
| Tunneling-Protocols      | Y           | Y   | Y   | 11                  | 整数                 | 単値              | 1 = PPTP<br>2 = L2TP<br>4 = IPSec<br>8 = L2TP/IPSec<br>16 = WebVPN<br>4 と 8 は相互排他値 (0-11、16-27<br>は有効値)                                 |
| IPSec-Sec-Association    | Y           |     |     | 12                  | 文字列                | 単値              | セキュリティ関連の名前                                                                                                                             |
| IPSec-Authentication     | Y           |     |     | 13                  | 整数                 | 単値              | 0 = なし<br>1 = RADIUS<br>2 = LDAP (認可のみ)<br>3 = NT ドメイン<br>4 = SDI<br>5 = 内部<br>6 = RADIUS での Expiry 認証<br>7 = Kerberos/Active Directory |
| IPSec-Banner1            | Y           | Y   | Y   | 15                  | 文字列                | 単値              | バナー文字列                                                                                                                                  |
| IPSec-Allow-Passwd-Store | Y           | Y   | Y   | 16                  | ブーリ<br>アン          | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                                                 |
| Use-Client-Address       | Y           |     |     | 17                  | ブーリ<br>アン          | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                                                 |

## ■ 外部 RADIUS サーバの設定

表 E-4 セキュリティ アプライアンスがサポートしている RADIUS のアトリビュートと値 (続き)

| アトリビュート名                | VPN<br>3000 | ASA | PIX | アトリ<br>ビュート<br>番号 # | シンタッ<br>クス/<br>タイプ | 単値<br>または<br>多値 | 単値または多値                                                                                                  |
|-------------------------|-------------|-----|-----|---------------------|--------------------|-----------------|----------------------------------------------------------------------------------------------------------|
| PPTP-Encryption         | Y           |     |     | 20                  | 整数                 | 単値              | ビットマップ：<br>1 = 暗号化が必要<br>2 = 40 ビット<br>4 = 128 ビット<br>8 = ステートレスが必要<br>例：15 = 40/128 ビットで暗号化 / ステートレスが必要 |
| L2TP-Encryption         | Y           |     |     | 21                  | 整数                 | 単値              | ビットマップ：<br>1 = 暗号化が必要<br>2 = 40 ビット<br>4 = 128 ビット<br>8 = ステートレスが必要<br>5 = 40/128 ビットで暗号化 / ステートレスが必要    |
| IPSec-Split-Tunnel-List | Y           | Y   | Y   | 27                  | 文字列                | 単値              | スプリット トンネルの包含リストを表すネットワークおよびアクセスリストを指定します。                                                               |
| IPSec-Default-Domain    | Y           | Y   | Y   | 28                  | 文字列                | 単値              | クライアントに送信する単一のデフォルトのドメイン名 (1 ~ 255 文字) を指定します                                                            |
| IPSec-Split-DNS-Names   | Y           | Y   | Y   | 29                  | 文字列                | 単値              | クライアントに送信する単一のセカンダリ ドメイン名 (1 ~ 255 文字) のリストを指定します                                                        |
| IPSec-Tunnel-Type       | Y           | Y   | Y   | 30                  | 整数                 | 単値              | 1 = LAN-to-LAN<br>2 = リモートアクセス                                                                           |
| IPSec-Mode-Config       | Y           | Y   | Y   | 31                  | ブーリアン              | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                  |
| IPSec-User-Group-Lock   | Y           |     |     | 33                  | ブーリアン              | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                  |
| IPSec-Over-UDP          | Y           | Y   | Y   | 34                  | ブーリアン              | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                  |
| IPSec-Over-UDP-Port     | Y           | Y   | Y   | 35                  | 整数                 | 単値              | 4001 ~ 49151、デフォルトは 10000                                                                                |
| IPSec-Banner2           | Y           | Y   | Y   | 36                  | 文字列                | 単値              | バナー文字列                                                                                                   |
| PPTP-MPPC-Compression   | Y           |     |     | 37                  | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                  |



表 E-4 セキュリティ アプライアンスがサポートしている RADIUS のアトリビュートと値 (続き)

| アトリビュート名                              | VPN<br>3000 | ASA | PIX | アトリ<br>ビュート<br>番号 # | シンタッ<br>クス/<br>タイプ | 単値<br>または<br>多値 | 単値または多値                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------|-------------|-----|-----|---------------------|--------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L2TP-MPPC-Compression                 | Y           |     |     | 38                  | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                                                                                                                                                                                                                                                                            |
| IPSec-IP-Compression                  | Y           | Y   | Y   | 39                  | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                                                                                                                                                                                                                                                                            |
| IPSec-IKE-Peer-ID-Check               | Y           | Y   | Y   | 40                  | 整数                 | 単値              | 1 = 必須<br>2 = ピア証明書でサポートされ<br>る場合<br>3 = チェックしない                                                                                                                                                                                                                                                                                                                   |
| IKE-Keep-Alives                       | Y           | Y   | Y   | 41                  | ブーリ<br>アン          | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                                                                                                                                                                                                                                                                            |
| IPSec-Auth-On-Rekey                   | Y           | Y   | Y   | 42                  | ブーリ<br>アン          | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                                                                                                                                                                                                                                                                            |
| Required-Client- Firewall-Vendor-Code | Y           | Y   | Y   | 45                  | 整数                 | 単値              | 1 = シスコシステムズ (Cisco<br>Integrated Client を使用)<br>2 = Zone Labs<br>3 = NetworkICE<br>4 = Sygate<br>5 = シスコシステムズ (Cisco<br>Intrusion Prevention Security Agent<br>を使用)                                                                                                                                                                                               |
| Required-Client-Firewall-Product-Code | Y           | Y   | Y   | 46                  | 整数                 | 単値              | シスコシステムズの製品：<br><br>1 = Cisco Intrusion Prevention<br>Security Agent または Cisco<br>Integrated Client (CIC)<br><br>Zone Labs の製品：<br><br>1 = Zone Alarm<br>2 = Zone AlarmPro<br>3 = Zone Labs Integrity<br><br>NetworkICE の製品：<br><br>1 = BlackIce Defender/Agent<br><br>Sygate の製品：<br><br>1 = Personal Firewall<br>2 = Personal Firewall Pro<br>3 = Security Agent |
| Required-Client-Firewall-Description  | Y           | Y   | Y   | 47                  | 文字列                | 単値              | 文字列                                                                                                                                                                                                                                                                                                                                                                |

## ■ 外部 RADIUS サーバの設定

表 E-4 セキュリティ アプライアンスがサポートしている RADIUS のアトリビュートと値 (続き)

| アトリビュート名                                  | VPN<br>3000 | ASA | PIX | アトリ<br>ビュート<br>番号 # | シンタッ<br>クス/<br>タイプ | 単値<br>または<br>多値 | 単値または多値                                                                                                   |
|-------------------------------------------|-------------|-----|-----|---------------------|--------------------|-----------------|-----------------------------------------------------------------------------------------------------------|
| Require-HW-Client-Auth                    | Y           | Y   | Y   | 48                  | ブーリ<br>アン          | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                   |
| Required-Individual-User-Auth             | Y           | Y   | Y   | 49                  | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                   |
| Authenticated-User-Idle-Timeout           | Y           | Y   | Y   | 50                  | 整数                 | 単値              | 1 ~ 35791394 分                                                                                            |
| Cisco-IP-Phone-Bypass                     | Y           | Y   | Y   | 51                  | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                   |
| IPSec-Split-Tunneling-Policy              | Y           | Y   | Y   | 55                  | 整数                 | 単値              | 0 = スプリット トンネリングなし<br>1 = スプリット トンネリング<br>2 = ローカル LAN を許可                                                |
| IPSec-Required-Client-Firewall-Capability | Y           | Y   | Y   | 56                  | 整数                 | 単値              | 0 = なし<br>1 = リモート FW Are-You-<br>There (AYT) で定義されている<br>ポリシー<br>2 = Policy Pushed CPP<br>4 = サーバからのポリシー |
| IPSec-Client-Firewall-Filter-Name         | Y           |     |     | 57                  | 文字列                | 単値              | ファイアウォール ポリシーとしてクライアントに配信が必要なフィルタの名前を指定します                                                                |
| IPSec-Client-Firewall-Filter-Optional     | Y           | Y   | Y   | 58                  | 整数                 | 単値              | 0 = 必須<br>1 = オプション                                                                                       |
| IPSec-Backup-Servers                      | Y           | Y   | Y   | 59                  | 文字列                | 単値              | 1 = Client-Configured リストを使用する<br>2 = クライアント リストをディ<br>セーブルにして消去する<br>3 = バックアップ サーバ リスト<br>を使用する         |
| IPSec-Backup-Server-List                  | Y           | Y   | Y   | 60                  | 文字列                | 単値              | サーバ アドレス (スペースで区<br>切る)                                                                                   |
| DHCP-Network-Scope                        | Y           | Y   | Y   | 61                  | 文字列                | 単値              | IP アドレス                                                                                                   |
| Intercept-DHCP-Configure-Msg              | Y           | Y   | Y   | 62                  | ブーリ<br>アン          | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                   |
| MS-Client-Subnet-Mask                     | Y           | Y   | Y   | 63                  | ブーリ<br>アン          | 単値              | IP アドレス                                                                                                   |
| Allow-Network-Extension-Mode              | Y           | Y   | Y   | 64                  | ブーリ<br>アン          | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                   |

表 E-4 セキュリティ アプライアンスがサポートしている RADIUS のアトリビュートと値 (続き)

| アトリビュート名                          | VPN<br>3000 | ASA | PIX | アトリ<br>ビュート<br>番号 # | シンタッ<br>クス/<br>タイプ | 単値<br>または<br>多値 | 単値または多値                                                                                                            |
|-----------------------------------|-------------|-----|-----|---------------------|--------------------|-----------------|--------------------------------------------------------------------------------------------------------------------|
| Authorization-Type                | Y           | Y   | Y   | 65                  | 整数                 | 単値              | 0 = なし<br>1 = RADIUS<br>2 = LDAP                                                                                   |
| Authorization-Required            | Y           |     |     | 66                  | 整数                 | 単値              | 0 = No<br>1 = Yes                                                                                                  |
| Authorization-DN-Field            | Y           | Y   | Y   | 67                  | 文字列                | 単値              | 取り得る値: UID、OU、O、<br>CN、L、SP、C、EA、T、N、<br>GN、SN、I、GENQ、DNQ、<br>SER、use-entire-name                                  |
| IKE-KeepAlive-Confidence-Interval | Y           | Y   | Y   | 68                  | 整数                 | 単値              | 10 ~ 300 秒                                                                                                         |
| WebVPN-Content-Filter-Parameters  | Y           | Y   |     | 69                  | 整数                 | 単値              | 1 = Java ActiveX<br>2 = Java スクリプト<br>4 = イメージ<br>8 = イメージのクッキー                                                    |
| WebVPN-URL-List                   |             | Y   |     | 71                  | 文字列                | 単値              | URL リスト名                                                                                                           |
| WebVPN-Port-Forward-List          |             | Y   |     | 72                  | 文字列                | 単値              | ポート転送リスト名                                                                                                          |
| WebVPN-Access-List                |             | Y   |     | 73                  | 文字列                | 単値              | アクセスリスト名                                                                                                           |
| Cisco-LEAP-Bypass                 | Y           | Y   | Y   | 75                  | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル                                                                                            |
| WebVPN-Homepage                   | Y           | Y   |     | 76                  | 文字列                | 単値              | http://example-portal.com などの<br>URL                                                                               |
| Client-Type-Version-Limiting      | Y           | Y   | Y   | 77                  | 文字列                | 単値              | IPsec VPN のバージョン番号を<br>示す文字列                                                                                       |
| WebVPN-Port-Forwarding-Name       | Y           | Y   |     | 79                  | 文字列                | 単値              | 文字列による名前<br>("Corporate-Apps" など)。<br><br>このテキストは WebVPN ホーム<br>ページ上のデフォルトの文字列<br>「Application Access」を置き換え<br>ます。 |
| IE-Proxy-Server                   | Y           |     |     | 80                  | 文字列                | 単値              | IP アドレス                                                                                                            |
| IE-Proxy-Server-Policy            | Y           |     |     | 81                  | 整数                 | 単値              | 1 = 変更なし<br>2 = プロキシなし<br>3 = 自動検出<br>4 = コンセントレータの設定を<br>使用                                                       |
| IE-Proxy-Exception-List           | Y           |     |     | 82                  | 文字列                | 単値              | 改行 (\n) で区切られた DNS ド<br>メインのリスト                                                                                    |

## ■ 外部 RADIUS サーバの設定

表 E-4 セキュリティ アプライアンスがサポートしている RADIUS のアトリビュートと値 (続き)

| アトリビュート名                             | VPN<br>3000 | ASA | PIX | アトリ<br>ビュート<br>番号 # | シンタッ<br>クス/<br>タイプ | 単値<br>または<br>多値 | 単値または多値                  |
|--------------------------------------|-------------|-----|-----|---------------------|--------------------|-----------------|--------------------------|
| IE-Proxy-Bypass-Local                | Y           |     |     | 83                  | 整数                 | 単値              | 0 = なし<br>1 = ローカル       |
| IKE-Keepalive-Retry-Interval         | Y           | Y   | Y   | 84                  | 整数                 | 単値              | 2 ~ 10 秒                 |
| Tunnel-Group-Lock                    |             | Y   | Y   | 85                  | 文字列                | 単値              | トンネルグループの名前または<br>「none」 |
| Access-List-Inbound                  |             | Y   | Y   | 86                  | 文字列                | 単値              | アクセスリストの ID              |
| Access-List-Outbound                 |             | Y   | Y   | 87                  | 文字列                | 単値              | アクセスリストの ID              |
| Perfect-Forward-Secrecy-Enable       | Y           | Y   | Y   | 88                  | ブーリ<br>アン          | 単値              | 0 = No<br>1 = Yes        |
| NAC-Enable                           | Y           |     |     | 89                  | 整数                 |                 | 0 = No<br>1 = Yes        |
| NAC-Status-Query-Timer               | Y           |     |     | 90                  | 整数                 |                 | 30 ~ 1800 秒              |
| NAC-Revalidation-Timer               | Y           |     |     | 91                  | 整数                 |                 | 300 ~ 86400 秒            |
| NAC-Default-ACL                      | Y           |     |     | 92                  | 文字列                |                 | アクセスリスト                  |
| WebVPN-URL-Entry-Enable              | Y           | Y   |     | 93                  | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル  |
| WebVPN-File-Access-Enable            | Y           | Y   |     | 94                  | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル  |
| WebVPN-File-Server-Entry-Enable      | Y           | Y   |     | 95                  | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル  |
| WebVPN-File-Server-Browsing-Enable   | Y           | Y   |     | 96                  | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル  |
| WebVPN-Port-Forwarding-Enable        | Y           | Y   |     | 97                  | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル  |
| WebVPN-Outlook-Exchange-Proxy-Enable | Y           | Y   |     | 98                  | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル  |
| WebVPN-Port-Forwarding-HTTP-Proxy    | Y           | Y   |     | 99                  | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル  |
| WebVPN-Auto-Applet-Download-Enable   | Y           | Y   |     | 100                 | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル  |
| WebVPN-Citrix-Metaframe-Enable       | Y           | Y   |     | 101                 | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル  |
| WebVPN-Apply-ACL                     | Y           | Y   |     | 102                 | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル  |
| WebVPN-SSL-VPN-Client-Enable         | Y           | Y   |     | 103                 | 整数                 | 単値              | 0 = ディセーブル<br>1 = イネーブル  |

表 E-4 セキュリティ アプライアンスがサポートしている RADIUS のアトリビュートと値 (続き)

| アトリビュート名                                | VPN 3000 | ASA | PIX | アトリビュート番号 # | シンタックス/タイプ | 単値または多値 | 単値または多値                 |
|-----------------------------------------|----------|-----|-----|-------------|------------|---------|-------------------------|
| WebVPN-SSL-VPN-Client-Required          | Y        | Y   |     | 104         | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル |
| WebVPN-SSL-VPN-Client-Keep-Installation | Y        | Y   |     | 105         | 整数         | 単値      | 0 = ディセーブル<br>1 = イネーブル |
| Strip-Realm                             | Y        | Y   | Y   | 135         | ブーリアン      | 単値      | 0 = ディセーブル<br>1 = イネーブル |



(注)

RADIUS アトリビュート名には、VPN 3000、PIX、および ASA の 3 種類すべてのセキュリティ アプライアンスのサポートをよりよく反映するために、cVPN3000 プレフィックスは含まれていません。Cisco Secure ACS 4.x は、この新しい名前をサポートしますが、4.0 以前の ACS のアトリビュート名にはまだ VPN3000 プレフィックスが含まれています。アプライアンスは、アトリビュート名ではなく数字のアトリビュート ID に基づいて、RADIUS アトリビュートを使用します。LDAP アトリビュートは、ID ではなくアトリビュート名で使います。





## GLOSSARY

### 数字

**3DES** 「[DES](#)」を参照。

### A

**AAA** Authentication, Authorization, and Accounting（認証、認可、アカウントिंग）。「[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](#)における、複数エリアへのインターフェイスを備えたルータです。

**ACE** Access Control Entry（アクセス コントロール エントリ）。コンフィギュレーションに入力される情報です。この情報を使用して、[インターフェイス](#)上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ことができます。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。

**ACL** Access Control List（アクセス コントロール リスト）。[ACE](#)の集合。ACLを使用して、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することができます。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。ACLは、通常、着信トラフィックの送信元である[インターフェイス](#)に対して適用されます。「[規則](#)」および「[発信 ACL](#)」も参照してください。

**ActiveX** モバイルまたはポータブル プログラムの作成に使用される、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 アプレットとほぼ同等のものです。

**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 サイファです。AES アルゴリズムでは、128、192、および 256 ビットの暗号キーを使用して、データを 128 ビットのブロックで暗号化および復号化できます。「[DES](#)」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、およびリプレイ検出を保証する IP プロトコル（タイプ 51）です。AHは、保護対象のデータ（完全 IP データグラムなど）に埋め込まれます。AHは、単体でも[ESP](#)と組み合わせても使用できます。AHは旧式の[IPSec](#)プロトコルで、ほとんどのネットワークでは[ESP](#)ほど重要ではありません。AHは認証サービスを提供しますが、暗号化サービスは提供しません。AHは、[認証と暗号化](#)の両方を提供する[ESP](#)をサポートしない[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](#)」も参照してください。RFC 2402を参照してください。

**A レコード アドレス** 「A」はアドレスを表します。[DNS](#)で名前からアドレスにマッピングされたレコードを指します。

**APCF** Application Profile Customization Framework（アプリケーション プロファイル カスタマイゼーション フレームワーク）。セキュリティ アプライアンスが標準以外のアプリケーションを処理できるようにする機能で、これによって WebVPN 接続を介して正しく表示できるようになります。

**ARP** Address Resolution Protocol（アドレス レゾリューション プロトコル）。ハードウェア アドレスまたは MAC アドレスを IP アドレスにマッピングする低レベルの TCP/IP プロトコルです。ハードウェア アドレスの例として、00:00:a6:00:01:ba があります。最初の 3 つの文字グループ（00:00:a6）は製造元を示し、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)。セキュリティ アプライアンスで検査の実行に使用されます。ASA では、内部システムおよびアプリケーションそれぞれに対して明示的に設定を行わなくても、単方向 (内部から外部へ) の接続が可能です。「 <a href="#">検査エンジン</a> 」も参照してください。 |
| ASA         | 適応型セキュリティ アプライアンス。                                                                                                                                                                       |
| ASDM        | Adaptive Security Device Manager。単一のセキュリティ アプライアンスを管理および設定するためのアプリケーションです。                                                                                                               |
| auto-signon | このコマンドを実行すると、WebVPN ユーザはシングル サインオン方式が使用できます。これによって WebVPN ログイン クレデンシャル (ユーザ名およびパスワード) が内部サーバに渡され、サーバは NTLM 認証および基本認証のいずれかまたは両方で認証を行います。                                                  |

---

## B

|           |                                                                                                                                                                                                                                                  |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BGP       | Border Gateway Protocol (ボーダー ゲートウェイ プロトコル)。BGP は、TCP/IP ネットワーク内のドメイン間ルーティングを実行します。BGP はエクステリア ゲートウェイ プロトコルです。つまり、複数の自律システムまたはドメイン間のルーティングを実行し、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。セキュリティ アプライアンスは BGP をサポートしません。「 <a href="#">EGP</a> 」も参照してください。 |
| BLT ストリーム | Bandwidth Limited Traffic ストリーム。帯域幅が制限されたストリームまたはパケット フローです。                                                                                                                                                                                     |
| 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がネットワークを介してブートできるプロトコルで、RFC 951 および RFC 1542 で定義されています。                                                                                                                                      |
| BPDU      | Bridge Protocol Data Unit (ブリッジ プロトコル データ ユニット)。ネットワーク内のブリッジ間で情報を交換するために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 用語です。                                                                                             |

---

## C

|        |                                                                                                                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CA     | Certificate Authority、Certification Authority (認証局)。証明書の発行と無効化に責任を負う第三者機関です。CA の公開キーを持つ各デバイスは、その CA によって発行された証明書を持つデバイスを認証できます。CA という用語が CA サービスを提供するソフトウェアを指す場合もあります。「 <a href="#">証明書</a> 」、「 <a href="#">CRL</a> 」、「 <a href="#">公開キー</a> 」、「 <a href="#">RA</a> 」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術です。CBC には、暗号化を開始するための Initialization Vector (IV; 初期ベクトル) が必要です。IV は、 <a href="#">IPSec</a> パケットで明示的に与えられます。                                                                                                                |
| CHAP   | Challenge Handshake Authentication Protocol (チャレンジ ハンドシェイク 認証プロトコル)。                                                                                                                                                                                                            |
| CIFS   | Common Internet File System (共通インターネット ファイル システム)。プラットフォームに依存しないファイル共有システムで、ファイル、プリンタ、および他のマシン リソースにネットワークを介してアクセスする機能をユーザに提供します。Microsoft では、Windows コンピュータのネットワークで CIFS を実装しています。一方、CIFS のオープン ソース実装では、Linux、UNIX、および Mac OS X など他のオペレーティング システムを実行するサーバへのファイル アクセスも提供しています。  |
| Citrix | クライアント サーバ型アプリケーションの仮想化を実現し、Web アプリケーションを最適化するアプリケーション。                                                                                                                                                                                                                         |
| CLI    | Command Line Interface (コマンドライン インターフェイス)。セキュリティ アプライアンスに対するコンフィギュレーション コマンドやモニタリング コマンドを入力するための主要インターフェイス。                                                                                                                                                                     |
| CPU    | Central Processing Unit (中央演算処理装置)。メイン プロセッサです。                                                                                                                                                                                                                                 |



|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CRC</b>    | Cyclical Redundancy Check (巡回冗長検査)。エラーチェック手法。この手法では、フレームの受信側がフレームの内容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。                                                                                                                                                                                                                                                                                                                             |
| <b>CRL</b>    | Certificate Revocation List (証明書失効リスト)。特定の <b>CA</b> が発行する、最新の無効化されたすべての証明書をリストしたデジタル署名メッセージです。これは、店舗が盗難に遭ったカード番号の帳簿を使用して、悪用されたクレジットカードを拒否するしくみに似ています。証明書は、無効にされると CRL に追加されます。証明書を使用する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、証明書が期限満了になる前に簡単に無効にできますが、一般に CRL は、 <b>CA</b> または <b>RA</b> だけが管理します。CRL を使用している場合は、認証要求時に <b>CA</b> または <b>RA</b> への接続が使用できないと、認証要求が失敗します。「 <b>CA</b> 」、「 <b>証明書</b> 」、「 <b>公開キー</b> 」、「 <b>RA</b> 」も参照してください。 |
| <b>CRV</b>    | Call Reference Value。H.225.0 によって、2つのエンティティ間でシグナリングされるコール レッグの区別に使用されます。                                                                                                                                                                                                                                                                                                                                                                         |
| <b>CTIQBE</b> | Computer Telephony Interface Quick Buffer Encoding。Cisco CallManager と CTI の <b>TAPI</b> および <b>JTAPI</b> アプリケーションの間の IP テレフォニーで使用されるプロトコルです。CTIQBE は、TAPI/JTAPI プロトコルの検査モジュールで使用され、 <b>NAT</b> 、 <b>PAT</b> 、および双方向の <b>NAT</b> をサポートします。これにより、Cisco IP SoftPhone や他の Cisco TAPI/JTAPI アプリケーションは、セキュリティ アプライアンスを越えて Cisco CallManager とコール セットアップおよび音声トラフィックの通信を行うことができます。                                                                      |

## D

|                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DES</b>                                                           | Data Encryption Standard (データ暗号規格)。DES は 1977 年に National Bureau of Standards (米国商務省標準局) から発表された秘密キー暗号化スキームで、IBM の Lucifer アルゴリズムをベースにしています。シスコは、従来の暗号化 (40 ビットおよび 56 ビットのキー)、 <b>IPSec</b> 暗号化 (56 ビット キー)、および、56 ビット キーを使用して 3 倍の暗号化を実行する 3DES (トリプル DES) で DES を使用しています。3DES は DES よりもセキュアですが、暗号化と復号化には、より多くの処理を必要とします。「 <b>AES</b> 」および「 <b>ESP</b> 」も参照してください。                                |
| <b>DHCP</b>                                                          | Dynamic Host Configuration Protocol (ダイナミック ホスト コンフィギュレーション プロトコル)。ホストに IP アドレスをダイナミックに割り当て、ホストが必要としなくなったアドレスを再利用できるようにして、ラップトップなどのモバイル コンピュータが接続先の <b>LAN</b> に対して適切な IP アドレスを取得できるようにするメカニズムを提供します。                                                                                                                                                                                              |
| <b>Diffie-Hellman</b>                                                | セキュアでない通信チャネル上で 2 者が共有秘密を確立できるようにする公開キー暗号化プロトコル。Diffie-Hellman は <b>IKE</b> 内部で使用され、セッション キーを確立します。Diffie-Hellman は、 <b>Oakley</b> キー交換のコンポーネントです。                                                                                                                                                                                                                                                 |
| <b>Diffie-Hellman<br/>グループ 1、<br/>グループ 2、<br/>グループ 5、<br/>グループ 7</b> | Diffie-Hellman は、フェーズ 1 とフェーズ 2 の両方の <b>SA</b> を確立するための、大きな素数に基づく非対称暗号化を使用した公開キー暗号化の一種です。グループ 1 はグループ 2 よりも小さな素数を提供しますが、一部の <b>IPSec</b> ピアではこのバージョンのみがサポートされている場合があります。Diffie-Hellman グループ 5 は 1536 ビットの素数を使用し、最もセキュアであるため、 <b>AES</b> で使用することが推奨されています。163 ビットの楕円曲線フィールド サイズを持つグループ 7 は、Movian VPN クライアントで使用するためのものですが、グループ 7 (ECC) をサポートする任意のピアで動作します。「 <b>VPN</b> 」および「 <b>暗号化</b> 」も参照してください。 |
| <b>DMZ</b>                                                           | 「 <b>インターフェイス</b> 」を参照。                                                                                                                                                                                                                                                                                                                                                                            |
| <b>DN</b>                                                            | Distinguished Name (認定者名)。OSI ディレクトリ (X.500) 内のグローバルな正規のエントリ名です。                                                                                                                                                                                                                                                                                                                                   |
| <b>DNS</b>                                                           | Domain Name System (ドメイン ネーム システム) または 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 サービスです。                                                                                                                                                                                                                                                                                      |
| <b>DoS</b>                                                           | Denial of Service (サービス拒絶)。ネットワーク攻撃の一種です。ネットワーク サービスを使用できないようにすることを目的とします。                                                                                                                                                                                                                                                                                                                         |

|            |                                                                                                                                                                                                                                                                                              |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DSL</b> | Digital Subscriber Line (デジタル加入者線)。従来の銅線ケーブル配線を介して限られた距離で高い帯域幅を提供するパブリック ネットワーク テクノロジーです。DSL のサービスは、中央オフィスと顧客サイトに 1 つずつ配置されたモデムのペアを介して提供されます。ほとんどの DSL テクノロジーではツイストペアの帯域幅全体を使用することはないため、音声チャネル用の部分は残されています。                                                                                  |
| <b>DSP</b> | Digital Signal Processor (デジタル信号プロセッサ)。DSP は音声信号をフレームに分割し、ボイス パケットに格納します。                                                                                                                                                                                                                    |
| <b>DSS</b> | Digital Signature Standard (デジタル シグニチャ規格)。US National Institute of Standards and Technology (国立標準技術研究所) によって設計された、公開キー暗号化に基づくデジタル署名アルゴリズムです。DSS はユーザ データグラムの暗号化は実行しません。DSS は従来の暗号化や Redcreek <a href="#">IPSec</a> 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 <a href="#">IPSec</a> には含まれていません。 |

---

## E

|               |                                                                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>echo</b>   | <a href="#">「ping」</a> および <a href="#">「ICMP」</a> を参照してください。 <a href="#">「検査エンジン」</a> も参照してください。                                                |
| <b>EGP</b>    | Exterior Gateway Protocol (エクステリア ゲートウェイ プロトコル)。BGP に置き換えられました。セキュリティ アプライアンスは EGP をサポートしません。 <a href="#">「BGP」</a> も参照してください。                  |
| <b>EIGRP</b>  | Enhanced Interior Gateway Routing Protocol (Enhanced IGRP)。セキュリティ アプライアンスは EIGRP をサポートしません。                                                     |
| <b>EMBLEM</b> | Enterprise Management BaseLine Embedded Manageability。Cisco IOS システムのログ形式との一貫性を持たせるために設計された syslog 形式。CiscoWorks の管理アプリケーションとの互換性が高められています。     |
| <b>ESMTP</b>  | 拡張 <a href="#">SMTP</a> 。SMTP の拡張バージョン。送達通知やセッション配信などの追加機能が含まれます。ESMTP は、RFC 1869 「SMTP Service Extensions」 で定義されています。                          |
| <b>ESP</b>    | Encapsulating Security Payload。IPSec プロトコルの 1 つです。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

|                  |                                                                                                                           |
|------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>FQDN/IP</b>   | Fully Qualified Domain Name (完全修飾ドメイン名) /IP アドレス。セキュリティ ゲートウェイとなるピアを指定する <a href="#">IPSec</a> パラメータです。                   |
| <b>FragGuard</b> | IP フラグメント保護を可能にし、すべての <a href="#">ICMP</a> エラー メッセージの完全リアセンブリ、およびセキュリティ アプライアンスを介してルーティングされる残りの IP フラグメントの仮想リアセンブリを実行します。 |
| <b>FTP</b>       | File Transfer Protocol (ファイル転送プロトコル)。ホスト間のファイル転送に使用される TCP/IP プロトコル スタックの一部です。                                            |

---

## G

|             |                                                                                                                                              |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>GGSN</b> | Gateway <a href="#">GPRS</a> Support Node (ゲートウェイ GPRS サポート ノード)。モバイル セルラー電話ユーザがパブリック データ ネットワークや指定されたプライベート IP ネットワークに接続できるようにする無線ゲートウェイです。 |
| <b>GMT</b>  | Greenwich Mean Time (グリニッジ標準時)。1967 年に、Coordinated Universal Time (UTC; 世界標準時) に置き換えられました。                                                   |

|             |                                                                                                                                                                                                                                                                                                          |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>GPRS</b> | General Packet Radio Service（グローバル パケット ラジオ サービス）。European Telecommunication Standards Institute（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です。 <a href="#">GSM</a> ネットワークを IP パケットベースで拡張した GPRS は、モバイル無線データ通信を可能にします。                                                                                                  |
| <b>GRE</b>  | Generic Routing Encapsulation（総称ルーティング カプセル化）。RFC 1701 および 1702 で定義されています。GRE は、広範なタイプのプロトコル パケットをトンネル内でカプセル化できるトンネリング プロトコルであり、リモート ポイントのルータに対して IP ネットワークを介した仮想のポイントツーポイント リンクを作成します。複数のマルチプロトコル サブネットワークを 1 つの単一プロトコル バックボーン環境で接続することにより、GRE を使用する IP トンネリングでは、単一プロトコルのバックボーン環境を越えたネットワークの拡張が可能になります。 |
| <b>GSM</b>  | 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 モバイル無線の規格。                                                                                                                                                                                                                                 |
| <b>GTP</b>  | GPRS Tunneling Protocol（GPRS トンネリング プロトコル）。GTP は、 <a href="#">GPRS</a> ネットワークで <a href="#">SGSN</a> と <a href="#">GGSN</a> の間でユーザ パケット データとシグナリング情報のフローを処理します。GTP は、 <a href="#">GPRS</a> ネットワークの Gn と Gp の両方のインターフェイス上で定義されます。                                                                          |

---

## H

|                  |                                                                                                                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>H.225</b>     | テレビ会議などのアプリケーションで TCP シグナリングに使用されるプロトコル。「 <a href="#">H.323</a> 」および「 <a href="#">検査エンジン</a> 」も参照してください。                                                                          |
| <b>H.225.0</b>   | H.225.0 セッションの確立とパケット化を規定する ITU 標準。H.225.0 では、実際には、RAS、Q.931 の使用、 <a href="#">RTP</a> の使用など、いくつかの異なるプロトコルが定められています。                                                               |
| <b>H.245</b>     | H.245 エンドポイントの制御を規定する ITU 標準。                                                                                                                                                     |
| <b>H.320</b>     | ISDN、フラクショナル T1、スイッチド 56 回線などの回線交換メディアを使用したテレビ会議について定めた一連の ITU-T 標準仕様。ITU-T 標準 H.320 の拡張機能により、LAN やその他の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 <a href="#">インターネット</a> を使用したテレビ会議が可能になります。     |
| <b>H.323</b>     | 異種の通信デバイスが、標準化された通信プロトコルを使用して、相互に通信できます。H.323 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の手順、および基本的なデータ転送方法を定義しています。                                                                       |
| <b>H.323 RAS</b> | Registration, Admission, and Status シグナリング プロトコル。デバイスが、登録、許可、帯域幅の変更、および <a href="#">VoIP</a> ゲートウェイとゲートキーパー間のステータスと接続解除手順を実行できるようにします。                                            |
| <b>H.450.2</b>   | <a href="#">H.323</a> のコール転送補足サービス。                                                                                                                                               |
| <b>H.450.3</b>   | <a href="#">H.323</a> のコール宛先変更補足サービス。                                                                                                                                             |
| <b>HMAC</b>      | <a href="#">SHA-1</a> や <a href="#">MD5</a> などの暗号化ハッシュを使用するメッセージ認証メカニズム。                                                                                                          |
| <b>HTTP</b>      | Hypertext Transfer Protocol（ハイパーテキスト転送プロトコル）。ファイルを転送するためにブラウザや Web サーバで使用されるプロトコルです。ユーザが Web ページを表示する場合、ブラウザは HTTP を使用してその Web ページで使用されるファイルを要求し、受信することができます。HTTP による伝送は暗号化されません。 |
| <b>HTTPS</b>     | Hypertext Transfer Protocol Secure。 <a href="#">SSL</a> 暗号化バージョンの HTTP です。                                                                                                        |

|                        |                                                                                                                                                                                                                                                                                                                                                             |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IANA                   | Internet Assigned Number Authority (インターネット割り当て番号局)。インターネットで使用されるすべての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 (インターネット制御メッセージ プロトコル)。ネットワーク レイヤのインターネット プロトコルであり、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します。                                                                                                                                                                                                                                     |
| IDS                    | Intrusion Detection System (侵入検知システム)。シグニチャによって悪意のあるネットワーク アクティビティを検出し、そのシグニチャに対してポリシーを実装する手段です。                                                                                                                                                                                                                                                            |
| IETF                   | Internet Engineering Task Force (インターネット技術特別調査委員会)。インターネット用のプロトコルを定義する RFC 文書を作成する技術標準団体です。                                                                                                                                                                                                                                                                 |
| IGMP                   | Internet Group Management Protocol (インターネット グループ管理プロトコル)。IGMP は、IP マルチキャスト メンバシップを隣接するマルチキャスト ルータに報告するために 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 エクスチェンジ)。IKE は共有セキュリティ ポリシーを確立し、キーを要求するサービス (IPSec など) に対してキーを認証します。IPSec トラフィックが通過する前に、各セキュリティ アプライアンスはピアの ID を確認する必要があります。確認は、両方のホストに手動で事前共有キーを入力するか、CA サービスを使用して実行します。IKE は、Oakley を部分的に使用し、また、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も部分的に使用する、ハイブリッド プロトコルです。これは、以前は ISAKMP/Oakley と呼ばれていたプロトコルであり、RFC 2409 で定義されています。 |
| IKE Mode Configuration | IKE Mode Configuration は、IETF draft-ietf-ipsec-isakmp-mode-cfg-04.txt に従って実装されます。IKE Mode Configuration は、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 (およびその他のネットワーク レベル コンフィギュレーション) をダウンロードする手段をセキュリティ ゲートウェイに提供します。                                                                                                                                           |
| IKE 拡張認証               | IKE 拡張認証 (Xauth) は、IETF draft-ietf-ipsec-isakmp-xauth-04.txt (「拡張認証」草案) に従って実装されます。このプロトコルは、TACACS+ または RADIUS を使用して IKE 内のユーザを認証する機能を提供します。                                                                                                                                                                                                                |
| ILS                    | Internet Locator Service。ILS は LDAP をベースとし、ILSv2 に準拠しています。ILS は、NetMeeting、SiteServer、および Active Directory の各製品と使用するために、Microsoft 社によって独自に開発されたものです。                                                                                                                                                                                                        |
| IMAP                   | Internet Message Access Protocol。共有可能なメール サーバに保持されている電子メールや掲示板のメッセージにアクセスする方式です。IMAP により、クライアントの電子メール アプリケーションは、実際にメッセージを転送することなく、ローカルであるかのようにリモート メッセージストアにアクセスすることができます。                                                                                                                                                                                  |
| IMSI                   | International Mobile Subscriber Identity。GTP トンネル ID の 2 つのコンポーネントの 1 つです。もう 1 つのコンポーネントは NSAPI です。「NSAPI」も参照してください。                                                                                                                                                                                                                                        |
| inside                 | セキュリティ アプライアンスによって保護された内部の「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」および「インターフェイス名」も参照してください。                                                                                                                                                                                                                                                      |
| intfn                  | 名前と構成をカスタマイズできるユーザ設計のサブセット ネットワークに接続する任意のインターフェイス。通常はポート 2 から始まります。                                                                                                                                                                                                                                                                                         |
| IP                     | Internet Protocol (インターネット プロトコル)。IP プロトコルは、相互接続されたネットワークの任意のセット間の通信に使用でき、LAN 通信にも WAN 通信にも同様に適していることから、最も広く使用されている公開プロトコルです。                                                                                                                                                                                                                               |

|                           |                                                                                                                                                                                                                                                                          |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IPS</b>                | Intrusion Prevention System（侵入防御システム）。広範なネットワーク攻撃の軽減に役立つ、インラインの詳細なパケット検査に基づいたソリューションです。                                                                                                                                                                                  |
| <b>IPSec</b>              | IP セキュリティ。関係するピア間のデータ機密性、データ整合性、およびデータ認証を提供する、公開規格のフレームワークです。IPSec はこのようなセキュリティ サービスを IP レイヤで提供します。IPSec は、IKE を使用してローカル ポリシーに基づ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 で使用される暗号キーと認証キーを生成します。IPSec では、一対のホスト間、一対のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホストの間で 1 つ以上のデータ フローを保護できます。 |
| <b>IPSec トランスフォーム セット</b> | トランスフォーム セットは、IPSec ポリシーに一致するトラフィックに対して使用する、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。1 つの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。ほぼすべて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、認証のために DES アルゴリズムと HMAC-SHA を持つ ESP です。                                    |
| <b>IPSec フェーズ 1</b>       | IPSec をネゴシエートする最初のフェーズ。キー交換、および IPSec の ISAKMP の部分が含まれます。                                                                                                                                                                                                                |
| <b>IPSec フェーズ 2</b>       | IPSec をネゴシエートする 2 番目のフェーズ。フェーズ 2 では、ペイロードに使用される暗号化規則のタイプ、暗号化に使用される送信元と宛先、アクセスリストに従って処理対象とするトラフィックの定義、および IPSec ピアが決定されます。IPSec はフェーズ 2 でインターフェイスに適用されます。                                                                                                                 |
| <b>IP アドレス</b>            | IP プロトコル アドレス。セキュリティ アプライアンスのインターフェイスの ip_address です。IP バージョン 4 のアドレスの長さは、32 ビットです。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 バイナリ ビット）にグループ化され、ピリオドまたはドットで区切られた 4 つの 10 進数値として表現されます。4 つのオクテットのそれぞれの意味は、そのネットワークでの使用方法によって決定されます。    |
| <b>IP プール</b>             | ローカル IP アドレスの一定の範囲。名前、および開始 IP アドレスと終了 IP アドレスを持つ範囲によって指定されます。IP プールは、内部インターフェイス上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 と VPN で使用されます。                                                                                                                                       |
| <b>ISAKMP</b>             | Internet Security Association and Key Management Protocol。ペイロード形式、キー交換プロトコル実装の方法、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 フレームワークです。「IKE」を参照。                                                                                                                               |
| <b>ISP</b>                | 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や DSL などのサービスを介してインターネットへの接続を提供する組織です。                                                                                                                                                                |

---

**J**

|              |                                                                                                                                           |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>JTAPI</b> | Java Telephony Application Programming Interface（Java テレフォニー アプリケーション プログラミング インターフェイス）。テレフォニー機能をサポートする Java ベースの API です。「TAPI」も参照してください。 |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------|

---

**L**

|             |                                                                                                                               |
|-------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>LAN</b>  | Local Area Network（ローカルエリア ネットワーク）。1 つのビルや敷地内など、一定の場所に配置されたネットワーク。「インターネット」、「イントラネット」、および「ネットワーク」も参照してください。                   |
| <b>LCN</b>  | Logical Channel Number（論理チャネル番号）。                                                                                             |
| <b>LDAP</b> | Lightweight Directory Access Protocol（ライトウェイト ディレクトリ アクセス プロトコル）。LDAP は、管理アプリケーションやブラウザ アプリケーションが X.500 ディレクトリにアクセスできるようにします。 |



---

**M**

|                                 |                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MCR</b>                      | 「 <a href="#">マルチキャスト</a> 」を参照。                                                                                                                                                                                                                                                                                                                                                      |
| <b>MC ルータ</b>                   | マルチキャスト (MC) ルータは、マルチキャスト データ伝送を、インターネットワーク内の各 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やその他のブロードキャストを受信するように登録されています。「 <a href="#">マルチキャスト</a> 」も参照してください。                                                                                                                                                                                                                            |
| <b>MD5</b>                      | Message Digest 5。128 ビット ハッシュを作成する一方向のハッシュ アルゴリズム。MD5 と <a href="#">SHA-1</a> は両方とも MD4 のバリエーションであり、MD4 のハッシュ アルゴリズムを強化するように設計されています。 <a href="#">SHA-1</a> は MD4 および MD5 よりもセキュアです。シスコでは、 <a href="#">IPSec</a> フレームワーク内の認証にハッシュを使用しています。また、SNMP v.2 のメッセージ認証にも使用します。MD5 は通信の整合性を確認し、発信元を認証して、適時性をチェックします。 <a href="#">MD5</a> は <a href="#">SHA-1</a> よりもダイジェストが小さく、わずかに速いとされています。 |
| <b>MDI</b>                      | Media Dependent Interface (メディア依存インターフェイス)。                                                                                                                                                                                                                                                                                                                                          |
| <b>MDIX</b>                     | Media Dependent Interface Crossover (メディア依存インターフェイス クロスオーバー)。                                                                                                                                                                                                                                                                                                                        |
| <b>MGCP</b>                     | Media Gateway Control Protocol (メディア ゲートウェイ コントロール プロトコル)。MGCP は、メディア ゲートウェイ コントローラやコール エージェントと呼ばれる外部コール制御要素によって VoIP コールを制御するためのプロトコルです。MGCP は IPDC プロトコルと <a href="#">SGCP</a> プロトコルを統合したものです。                                                                                                                                                                                     |
| <b>Mode Config</b>              | 「 <a href="#">IKE Mode Configuration</a> 」を参照。                                                                                                                                                                                                                                                                                                                                       |
| <b>Modular Policy Framework</b> | モジュラ ポリシー フレームワーク。Cisco IOS ソフトウェアのモジュラ <a href="#">QoS</a> CLI と同様の方法でセキュリティ アプライアンスの機能を設定するための手段です。                                                                                                                                                                                                                                                                                |
| <b>MS</b>                       | Mobile Station (モバイル ステーション)。モバイル ハンドセットやモバイル コンピュータなど、ネットワーク サービスにアクセスするために使用される任意のモバイル デバイスの総称です。 <a href="#">GPRS</a> 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、 <a href="#">GPRS</a> および <a href="#">GSM</a> 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、Class A の MS は、 <a href="#">GPRS</a> サービスと <a href="#">GSM</a> サービスの同時操作をサポートします。                                            |
| <b>MS-CHAP</b>                  | Microsoft <a href="#">CHAP</a> 。                                                                                                                                                                                                                                                                                                                                                     |
| <b>MTU</b>                      | Maximum Transmission Unit (最大伝送ユニット)。最適な応答時間で効率的にネットワーク上を転送できる 1 パケットあたり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、各ネットワークに応じてその値は異なり、シリアル接続では最小のバイト数となります。MTU は RFC 1191 で定義されています。                                                                                                                                                                                                   |

---

**N**

|             |                                                                                                                                                                                                       |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>N2H2</b> | セキュリティ アプライアンスと連携動作してユーザの Web アクセスを制御する、サードパーティ製のポリシー型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 <a href="#">HTTP</a> 要求をフィルタリングできます。N2H2 社は 2003 年 10 月に Secure Computing に買収されました。 |
| <b>NAT</b>  | Network Address Translation (ネットワーク アドレス変換)。グローバルに一意的な 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、グローバルに一意的でない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って、このようなアドレスを持つ組織を <a href="#">インターネット</a> に接続できます。    |
| <b>NEM</b>  | Network Extension Mode (ネットワーク拡張モード)。これを使用すると、 <a href="#">VPN</a> ハードウェア クライアントは、 <a href="#">VPN</a> 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。                                   |

|                |                                                                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NetBIOS</b> | 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 のプロトコルです。セキュリティ アプライアンスは、NBNS UDP ポート 137 および NBDS UDP ポート 138 のパケットの <b>NAT</b> 処理を実行することにより、NetBIOS をサポートします。 |
| <b>NMS</b>     | 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。一般に 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 はエージェントと通信して、ネットワークの統計情報やリソース情報を把握します。                            |
| <b>NSAPI</b>   | Network Service Access Point Identifier。 <b>GTP</b> トンネル ID の 2 つのコンポーネントの 1 つです。もう 1 つのコンポーネントは <b>IMSI</b> です。「 <b>IMSI</b> 」も参照してください。                                                           |
| <b>NSSA</b>    | Not-So-Stubby Area。RFC 1587 で定義されている OSPF 機能です。NSSA は Cisco IOS ソフトウェア リリース 11.2 で初めて導入されました。既存のスタブ エリア機能をシスコ独自でない方法で拡張した機能であり、限定的な方法でスタブ エリアに外部ルートを注入することができます。                                    |
| <b>NTLM</b>    | NT LAN Manager。Microsoft Windows のチャレンジ / レスポンス認証方式です。                                                                                                                                              |
| <b>NTP</b>     | Network Time Protocol（ネットワーク タイム プロトコル）。                                                                                                                                                            |

---

## O

|                |                                                                                                                                                                                   |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Oakley</b>  | 認証済みキー関連情報の取得方法を定義するキー交換プロトコル。Oakley の基本メカニズムは <b>Diffie-Hellman</b> 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。                                                                    |
| <b>OSPF</b>    | 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効率的に使用し、かつトポロジ変更後のコンバージェンスが高速であるため、大規模なネットワークに広く展開されているルーティング プロトコルです。セキュリティ アプライアンスは OSPF をサポートしています。 |
| <b>OU</b>      | Organizational Unit（組織ユニット）。X.500 ディレクトリのアトリビュートです。                                                                                                                               |
| <b>outside</b> | セキュリティ アプライアンスの外部（ <b>インターネット</b> ）にある他の「非信頼」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 0 です。「 <b>インターフェイス</b> 」、「 <b>インターフェイス名</b> 」、「 <b>発信</b> 」も参照してください。                                  |

---

## P

|                |                                                                                                                                                                                                                                 |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PAC</b>     | <b>PPTP</b> Access Concentrator（PPTP アクセス コンセントレータ）。 <b>PPP</b> 操作と <b>PPTP</b> プロトコル処理の機能を持つ 1 つ以上の PSTN 回線または ISDN 回線に接続されたデバイスです。PAC では、トラフィックを 1 つ以上の <b>PNS</b> に渡すための TCP/IP のみを実装する必要があります。PAC は IP 以外のプロトコルもトンネリングできます。 |
| <b>PAT</b>     | 「 <b>ダイナミック PAT</b> 」、「 <b>インターフェイス PAT</b> 」、および「 <b>スタティック PAT</b> 」を参照。                                                                                                                                                      |
| <b>PDP</b>     | Packet Data Protocol（パケット データ プロトコル）。                                                                                                                                                                                           |
| <b>Perfmon</b> | セキュリティ アプライアンスの機能。接続数 / 秒や xlate 数 / 秒など、広範な機能統計情報を収集し、報告します。                                                                                                                                                                   |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PFS           | Perfect Forward Secrecy (完全転送秘密)。PFS は、 <a href="#">IPSec</a> のフェーズ 1 とフェーズ 2 の <a href="#">SA</a> で異なるセキュリティ キーを使用することにより、セキュリティを強化します。PFS を使用しない場合は、両方のフェーズで同じセキュリティ キーを使用して <a href="#">SA</a> が確立されます。PFS は、特定の <a href="#">IPSec SA</a> キーが他のシークレット (他のキーなど) から導出されたものでないことを保証します。つまり、PFS では、攻撃者があるキーを突破しても、そこから他のキーを導出することはできないことが保証されます。PFS がイネーブルになっていない場合は、 <a href="#">IKE SA</a> の秘密キーが突破されると、その攻撃者は、 <a href="#">IPSec</a> のすべての保護データをコピーし、 <a href="#">IKE SA</a> のシークレットの知識を使用して、その <a href="#">IKE SA</a> によって設定された <a href="#">IPSec SA</a> のセキュリティを侵すことができると推測されます。PFS を使用すると、攻撃者が <a href="#">IKE</a> を突破しても、直接 <a href="#">IPSec</a> にアクセスすることはできません。その場合、攻撃者は各 <a href="#">IPSec SA</a> を個別に突破する必要があります。 |
| PIM           | Protocol Independent Multicast。PIM は、特定のマルチキャスト伝送をホストのグループに配信するための最適なパスを決定する、スケーラブルな手段を提供します。伝送を受信するために、各ホストは <a href="#">IGMP</a> を使用して登録されます。「 <a href="#">PIM-SM</a> 」も参照してください。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| PIM-SM        | Protocol Independent Multicast-Sparse Mode (PIM 希薄モード)。PIM-SM はシスコ ルータのデフォルトであり、マルチキャスト伝送の送信元がブロードキャストを開始すると、パケットが登録されたホストすべてに到達するまで、トラフィックは MC ルータ間を順次転送されていきます。「 <a href="#">PIM</a> 」も参照してください。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ping          | ホストが別のホストにアクセス可能かどうかを判別するために送信する <a href="#">ICMP</a> 要求。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| PIX           | Private Internet eXchange。Cisco PIX 500 シリーズのセキュリティ アプライアンスには、小規模 / ホーム オフィス向けのコンパクトなプラグアンドプレイ デスクトップ モデルから、きわめて要求の厳しい企業やサービス プロバイダーの環境に適したキャリアクラスのギガビット モデルまで、広い範囲の製品があります。Cisco PIX セキュリティ アプライアンスは、変化の速いネットワーク環境に対応した強固なマルチレイヤ防御機能を構築するための、堅牢な企業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        | 秘密キーや証明書などのデータをはじめとする PKI 関連データの転送規格。この規格をサポートするデバイスを使用すると、管理者は単一セットの個人 ID 情報を維持することができます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| PNS           | <a href="#">PPTP</a> Network Server (PPTP ネットワーク サーバ)。PNS は、汎用コンピューティング / サーバ プラットフォームで動作するように設計されています。PNS は <a href="#">PPTP</a> のサーバ側の処理を担当します。 <a href="#">PPTP</a> は、TCP/IP に完全に依存し、インターフェイス ハードウェアに依存しないため、PNS では <a href="#">LAN</a> デバイスや <a href="#">WAN</a> 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することができます。                                                                                                                                                                                                                                                                                                                                                                                                        |
| POP           | Post Office Protocol。クライアント電子メール アプリケーションが、メール サーバからメールを取得する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したダイヤルアップの <a href="#">ISP</a> アクセス用に開発されました。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 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、Microsoft によって、Windows ネットワークへのセキュアなリモートアクセスを可能にするために導入されました。ただし、攻撃に対して脆弱であるため、一般に PPTP が使用されるのは、より強力なセキュリティ方式が使用できない場合や、それが必要でない場合だけです。PPTP ポートは、 <a href="#">pptp</a> 、1723/tcp、および 1723/udp です。PPTP の詳細については、RFC 2637 を参照してください。また、「 <a href="#">PAC</a> 」、「 <a href="#">PPTP GRE</a> 」、「 <a href="#">PPTP GRE トンネル</a> 」、「 <a href="#">PNS</a> 」、「 <a href="#">PPTP セッション</a> 」、および「 <a href="#">PPTP TCP</a> 」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バージョン 1 の GRE。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| PPTP GRE トンネル | <a href="#">PNS</a> と <a href="#">PAC</a> のペアで定義されるトンネル。このトンネル プロトコルは、 <a href="#">GRE</a> の修正バージョンによって定義されています。このトンネルでは、 <a href="#">PAC</a> と <a href="#">PNS</a> の間で <a href="#">PPP</a> データグラムが伝送されます。多数のセッションが 1 つのトンネルに多重化されます。 <a href="#">TCP</a> 上で動作する制御接続により、セッションおよびトンネル自体の確立、解放、および維持が制御されます。                                                                                                                                                                                                                                                                                                                                                                                                                   |



**PPTP TCP** PPTP のコール制御情報と管理情報の受け渡しに使用される標準の 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ているセッションに論理的に関連付けられていますが、これとは別に存在しています。

**PPTP セッション** PPTP はコネクション型です。PAC に接続された各ユーザの状態は、PNS と PAC で維持されます。ダイヤル ユーザと PNS の間でエンドツーエンドの PPP 接続が試行されると、セッションが作成されます。セッションに関連するデータグラムは、PAC と PNS の間でトンネル経由で送信されます。

## Q

**QoS** Quality of Service。伝送システムのパフォーマンスを基に、その伝送品質とサービスの可用性を表します。

## R

**RA** Registration Authority (登録局)。CA の認可されたプロキシ。RA は証明書登録を実行し、CRL を発行することができます。「CA」、「証明書」、「公開キー」も参照してください。

**RADIUS** Remote Authentication Dial-In User Service (リモート認証ダイヤルイン ユーザ サービス)。RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント / サーバ システムです。RADIUS プロトコルの規格は、RFC 2058 と RFC 2059 で定義されています。「AAA」および「TACACS+」も参照してください。

**RFC** Request for Comments (コメント要求)。RFC 文書は、インターネットを使用した通信用のプロトコルや規格を定義します。RFC は IETF によって作成および発行されます。

**RIP** Routing Information Protocol (ルーティング情報プロトコル)。UNIX BSD システムに付属の Interior Gateway Protocol (IGP) です。インターネットで最も広く使用される IGP です。RIP 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 (予約済みリンク ローカル アドレス)。マルチキャスト アドレスは 224.0.0.0 ~ 239.255.255.255 の範囲ですが、ユーザが使用できるのは 224.0.1.0 ~ 239.255.255.255 だけです。マルチキャスト アドレス範囲の最初の 224.0.0.0 ~ 224.0.0.255 の部分は予約済みであり、RLLA と呼ばれます。これらのアドレスは使用できません。224.0.1.0 ~ 239.255.255.255 を指定することによって、RLLA の範囲を除外することができます。または、224.0.0.0 ~ 239.255.255.255 を指定して、224.0.0.0 ~ 224.0.0.255 を除外します。これで、224.0.1.0 ~ 239.255.255.255 を指定した場合と同じになります。

**RPC** Remote Procedure Call (リモート プロシージャ コール)。RPC は、クライアントで作成または指定されるプロシージャ コールで、サーバで実行され、結果はネットワーク経由でクライアントに返されます。

**RSA** 可変長キーを使用した公開キー暗号化アルゴリズム (名前は発明者である Rivest、Shamir、Adelman の名前に由来する)。RSA の主な欠点は、DES などの一般的な秘密キーアルゴリズムと比較すると、大幅に計算が遅いことです。シスコの IKE の実装では、秘密キーの取得には Diffie-Hellman 交換が使用されています。この交換は、RSA (または事前共有キー) を使用して認証できます。Diffie-Hellman 交換では、DES キーは (暗号化された形式であっても) ネットワークを越えませんが、RSA の暗号化および署名の手法では越えます。RSA はパブリック ドメインではないため、RSA Data Security からライセンスを取得する必要があります。

**RSH** リモート シェル。ユーザがリモート システムにログインせずにその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複数のアクセス サーバのステータスを確認し、コマンドを実行して、通信サーバとの接続を切断することができます。

**RTCP** RTP Control Protocol。IPv6 RTP 接続の QoS を監視し、実行中のセッションに関する情報を伝達するプロトコルです。「RTP」も参照してください。

|             |                                                                                                                                                                                                                                                                                              |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RTP</b>  | Real-Time Transport Protocol (リアルタイム転送プロトコル)。一般に、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のネットワーク サービスとして、アプリケーションがリアルタイムにデータを転送できるように、エンドツーエンドのネットワーク転送機能を提供するように設計されています。RTP は、ペイロード タイプの識別、シーケンス番号付け、タイムスタンプの付加、およびリアルタイム アプリケーションへのモニタリング送信などのサービスを提供します。 |
| <b>RTSP</b> | Real Time Streaming Protocol (リアルタイム ストリーミングプロトコル)。音声やビデオなど、リアルタイム データの制御配信を可能にします。RTSP は、 <a href="#">RTP</a> や <a href="#">HTTP</a> などの主要プロトコルと連携動作するように設計されています。                                                                                                                          |

## S

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SA</b>    | Security Association (セキュリティ アソシエーション)。データ フローに適用されるセキュリティ ポリシーとキー関連情報のインスタンスです。SA は、 <a href="#">IPSec</a> の 2 つのフェーズにおいて、 <a href="#">IPSec</a> 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の作成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 ( <a href="#">IKE SA</a> ) は、フェーズ 2 の SA をネゴシエートする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 ( <a href="#">IPSec SA</a> ) 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。 <a href="#">IKE</a> と <a href="#">IPSec</a> の両方で SA を使用しますが、これらは互いに独立しています。 <a href="#">IPSec</a> SA は単方向であり、各セキュリティ プロトコル内で一意です。保護されたデータ パイプでは 1 組の SA が必要であり、プロトコルごとに 1 方向あたり 1 つずつ必要です。たとえば、ピア間で <a href="#">ESP</a> をサポートしているパイプの場合は、各方向に 1 つの <a href="#">ESP SA</a> が必要です。SA は、宛先 ( <a href="#">IPSec</a> エンドポイント) アドレス、セキュリティ プロトコル ( <a href="#">AH</a> または <a href="#">ESP</a> )、および Security Parameter Index (SPI; 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。 <a href="#">IKE</a> は <a href="#">IPSec</a> に代わって SA のネゴシエーションと確立を行います。ユーザは手動で <a href="#">IPSec SA</a> を確立することもできます。 <a href="#">IKE SA</a> は、 <a href="#">IKE</a> のみによって使用され、 <a href="#">IPSec SA</a> の場合とは異なり双方向です。 |
| <b>SCCP</b>  | Skinny Client Control Protocol。Cisco CallManager と Cisco <a href="#">VoIP</a> 電話の間で使用される Cisco の専用プロトコルです。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>SCEP</b>  | Simple Certificate Enrollment Protocol。 <a href="#">CA</a> から証明書を要求および受信する(登録とも呼ばれる)手段です。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>SDP</b>   | Session Definition Protocol。マルチメディア サービスを定義するための <a href="#">IETF</a> プロトコルです。SDP メッセージは、 <a href="#">SGCP</a> メッセージや <a href="#">MGCP</a> メッセージの一部である場合があります。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>SGCP</b>  | Simple Gateway Control Protocol (簡易ゲートウェイ コントロール プロトコル)。外部コール制御要素(コール エージェントと呼ばれる)によって <a href="#">VoIP</a> ゲートウェイを制御します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>SGSN</b>  | Serving GPRS Support Node。SGSN は、モバイル管理機能、セッション管理機能、およびパケット リレー機能を保証します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>SHA-1</b> | Secure Hash Algorithm 1。SHA-1 [NIST94c] は、1994 年に公開された SHA の修正版です。SHA は MD4 をモデルとした、それにきわめて近い設計であり、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ので、128 ビットのハッシュ ( <a href="#">MD5</a> など) よりも Brute-Force アタックへの抵抗力が強化されます。SHA 1 は、National Institute of Standards and Technology (国立標準技術研究所) と National Security Agency (国家安全保障局) によって共同開発されました。このアルゴリズムは、他のハッシュ アルゴリズムと同様に、ハッシュ値(メッセージ ダイジェストとも呼ばれる)を生成するために使用されます。メッセージ ダイジェストは、下位レイヤのプロトコルでメッセージの内容が伝送中に変更されないように保証するために使用される <a href="#">CRC</a> と同様の動作をします。SHA-1 は、一般に <a href="#">MD5</a> より安全であるとされています。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>SIP</b>   | Session Initiation Protocol (セッション開始プロトコル)。特に二者間の音声会議、または「コール」のコール処理セッションをイネーブルにします。SIP は <a href="#">SDP</a> と連携動作してコール シグナリングを行います。 <a href="#">SDP</a> はメディア ストリーム用のポートを指定します。SIP の使用により、セキュリティ アブライアンスは任意の SIP <a href="#">VoIP</a> ゲートウェイと <a href="#">VoIP</a> プロキシ サーバをサポートすることができます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|                |                                                                                                                                                                                                                                                                                                                                                             |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SKEME</b>   | 認証済みキー関連情報の導出方法を定義するキー交換プロトコル。キー リフレッシュが迅速です。                                                                                                                                                                                                                                                                                                               |
| <b>SMR</b>     | Stub Multicast Routing (スタブ マルチキャスト ルーティング)。SMR により、セキュリティ アプライアンスは「スタブ ルータ」として動作します。スタブ ルータは <b>IGMP</b> プロキシ エージェントとして動作するデバイスです。 <b>IGMP</b> は、マルチキャスト ルータを備えた特定の <b>LAN</b> 上のマルチキャスト グループに特定のホストを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 データ伝送を、特定のマルチメディアやその他のブロードキャストを受信するように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 <b>MC ルータ</b> との間で <b>IGMP</b> メッセージを転送します。 |
| <b>SMTP</b>    | Simple Mail Transfer Protocol (シンプル メール転送プロトコル)。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。                                                                                                                                                                                                                                                                    |
| <b>SNMP</b>    | Simple Network Management Protocol (簡易ネットワーク管理プロトコル)。Management Information Base (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。                                                                                                                                                                                                                        |
| <b>SQL*Net</b> | Structured Query Language (SQL; 構造化照会言語) プロトコル。クライアントとサーバのプロセス間通信に使用される Oracle のプロトコル。                                                                                                                                                                                                                                                                      |
| <b>SSH</b>     | Secure Shell (セキュア シェル)。強力な認証と暗号化機能を提供する、TCP/IP などの信頼性の高いトランスポート レイヤで実行されるアプリケーション。                                                                                                                                                                                                                                                                         |
| <b>SSL</b>     | Secure Socket Layer。アプリケーション レイヤと 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。                                                                                                                                                                                                                                                                               |

---

**T**

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>TACACS+</b>  | Terminal Access Controller Access Control System Plus (ターミナル アクセス コントローラ アクセス コントロール システム プラス)。コマンド認可も含めて <b>AAA</b> サービスをサポートするクライアント / サーバ プロトコルです。「 <b>AAA</b> 」および「 <b>RADIUS</b> 」も参照してください。                                                                                                                                                                                                                                         |
| <b>TAPI</b>     | Telephony Application Programming Interface (テレフォニー アプリケーション プログラミング インターフェイス)。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 インターフェイスです。                                                                                                                                                                                                                                                                                                     |
| <b>TCP</b>      | Transmission Control Protocol (伝送制御プロトコル)。信頼性の高い全二重データ伝送を可能にする、コネクション型トランスポート層プロトコル。                                                                                                                                                                                                                                                                                                                                                      |
| <b>TCP 代行受信</b> | TCP 代行受信機能では、オプションの初期接続制限値に到達すると、初期接続カウントがしきい値未満になるまで、影響を受けるサーバに向けられたすべての SYN が代行受信されます。各 SYN に対して、セキュリティ アプライアンスは、サーバの代わりに空の SYN/ACK セグメントで応答します。セキュリティ アプライアンスは、該当するステート情報を保持し、パケットをドロップして、クライアントの ACK を待ちます。ACK が受信されると、クライアントの SYN セグメントのコピーがサーバに送信され、セキュリティ アプライアンスとサーバの間で <b>TCP</b> 3 ウェイ ハンドシェイクが実行されます。この 3 ウェイ ハンドシェイクが完了した場合は、通常どおり接続を再開できます。接続フェーズのいずれかの部分でクライアントが応答しない場合、セキュリティ アプライアンスは指数バックオフを使用して必要なセグメントを再送信します。         |
| <b>TDP</b>      | Tag Distribution Protocol (タグ配布プロトコル)。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布、要求、および解放するために、タグ スイッチング デバイスによって使用されます。TDP はルーティング プロトコルを置き換えません。代わりに、TDP はルーティング プロトコルから取得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 セッションをオープン、監視、クローズしたり、これらのセッション中に発生したエラーを示したりする目的でも使用されます。TDP は、順次配信が保証されたコネクション型のトランスポート レイヤ プロトコル ( <b>TCP</b> など) で動作します。TDP を使用しても、タグ バインディング情報 (他のプロトコルに関するピギーバックング情報など) を配布するその他のメカニズムの使用は妨げられません。 |

|               |                                                                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Telnet</b> | <a href="#">インターネット</a> などの TCP/IP ネットワーク用のターミナル エミュレーション プロトコル。Telnet はリモートから Web サーバを制御するための一般的な方法ですが、セキュリティ上の脆弱性により、 <a href="#">SSH</a> が使用されるようになってきています。 |
| <b>TFTP</b>   | Trivial File Transfer Protocol (簡易ファイル転送プロトコル)。TFTP は、ファイル転送用のシンプルなプロトコルです。このプロトコルは UDP 上で実行され、RFC 1350 で詳細に説明されています。                                          |
| <b>TID</b>    | Tunnel Identifier (トンネル識別子)。                                                                                                                                   |
| <b>TLS</b>    | Transport Layer Security。SSL に代わる将来の IETF プロトコルです。                                                                                                             |
| <b>TSP</b>    | TAPI Service Provider (TAPI サービス プロバイダー)。「 <a href="#">TAPI</a> 」も参照してください。                                                                                    |

---

## U

|                    |                                                                                                                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>UDP</b>         | User Datagram Protocol (ユーザ データグラム プロトコル)。IP プロトコル スタックにおけるコネクションレス型トランスポート レイヤ プロトコルです。UDP は、確認応答や送達保証を行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、エラー処理や再送信は他のプロトコルによって行う必要があります。UDP は RFC 768 で定義されています。                             |
| <b>UMTS</b>        | Universal Mobile Telecommunication System。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、固定、無線、および衛星ネットワーク経由でモバイル ユーザに配信することにより、オール IP ネットワークを目指す、 <a href="#">GPRS</a> を拡張したネットワーク。                                                           |
| <b>Unicast RPF</b> | Unicast Reverse Path Forwarding (ユニキャスト逆経路転送)。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発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するガードを行います。                                                                         |
| <b>URL</b>         | Uniform Resource Locator (ユニフォーム リソース ロケータ)。ハイパーテキスト文書やその他のサービスにブラウザを使用してアクセスするための標準アドレッシング方式です。たとえば、 <a href="http://www.cisco.com">http://www.cisco.com</a> などです。                                                        |
| <b>UTC</b>         | Coordinated Universal Time (世界標準時)。経度ゼロのタイムゾーンです。以前はグリニッジ標準時 (GMT) およびズールー時と呼ばれていました。UTC は 1967 年に GMT の代わりに世界標準時となりました。UTC は、天文時ではなく、原子時間に基づいています。                                                                        |
| <b>UTRAN</b>       | Universal Terrestrial Radio Access Network。UMTS で無線ネットワークを実装するために使用されるネットワークング プロトコルです。GTP を使用すると、 <a href="#">GGSN</a> 、 <a href="#">SGSN</a> 、および <a href="#">UTRAN</a> の間で、UMTS/GPRS バックボーン経由でマルチプロトコル パケットをトンネリングできます。 |
| <b>UUIE</b>        | User-User Information Element (ユーザ対ユーザ情報要素)。メッセージ内の関連ユーザを識別する <a href="#">H.225</a> パケットの要素です。                                                                                                                             |

---

## V

|             |                                                                                                                                                                                                                                  |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VLAN</b> | Virtual <a href="#">LAN</a> (バーチャル LAN)。実際には複数の異なる <a href="#">LAN</a> セグメント上に配置されていながら、同一のネットワーク ケーブルに接続されているかのように通信できるように (管理ソフトウェアを使用して) 設定された、1 つまたは複数の <a href="#">LAN</a> 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おり、非常に柔軟です。 |
| <b>VoIP</b> | Voice over IP。VoIP は、電話による通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 が音声信号をフレームにセグメント化し、2 つからなるグループにカップリングしてボイス パケットに格納します。これらのボイス パケットは、ITU-T 仕様 <a href="#">H.323</a> に準拠する IP を使用して伝送されます。                              |

|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VPN</b> | Virtual Private Network（バーチャル プライベート ネットワーク）。パブリック ネットワークを使用した 2 つのピア間のネットワーク接続を、厳密なユーザ認証とすべてのデータ トラフィックの暗号化によってプライベート化したものです。VPN は、PC などのクライアント間、またはセキュリティ アプライアンスなどの <b>ヘッドエンド</b> 間で確立することができます。                                                                                                                                                                                                                                                |
| <b>VSA</b> | Vendor-Specific Attribute（ベンダー固有アトリビュート）。 <b>RADIUS</b> の RFC ではなく、ベンダーによって定義された <b>RADIUS</b> パケットのアトリビュートです。 <b>RADIUS</b> プロトコルは、IANA によって割り当てられたベンダー番号を VSA の識別に利用します。これにより、異なるベンダーで同じ番号の VSA の使用が可能になります。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、ベンダー番号 9 に関連付けられた VSA セットでは、cisco-av-pair VSA はアトリビュート 1 になります。ベンダーごとに最大 256 の VSA を定義できます。1 つの <b>RADIUS</b> パケットに、任意の VSA アトリビュート 26（Vendor-specific）が格納されます。VSA はサブアトリビュートと呼ばれる場合もあります。 |

---

## W

|                 |                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WAN</b>      | Wide-Area Network（ワイドエリア ネットワーク）。広い地域にいるユーザ間を接続するデータ通信ネットワークであり、多くの場合、コモン キャリアによって提供される伝送デバイスを使用します。                                                                                                                                                                                                                                                                                                   |
| <b>Websense</b> | 社員による <b>インターネット</b> への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 では、ポリシー エンジンと <b>URL</b> データベースを使用して Web サイトへのユーザ アクセスを管理します。                                                                                                                                                                                                                                                                           |
| <b>WEP</b>      | Wired Equivalent Privacy。無線 <b>LAN</b> 用のセキュリティ プロトコルであり、IEEE 802.11b 規格で定義されています。                                                                                                                                                                                                                                                                                                                     |
| <b>WINS</b>     | Windows Internet Naming Service。特定のネットワーク デバイスに関連付けられた IP アドレスを確認する Windows システムであり、「名前解決」とも呼ばれます。WINS は、現在使用可能なネットワーク デバイスの <b>NetBIOS</b> 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アップデートされる分散データベースを使用します。WINS は、ルーティング型ネットワーク環境で <b>NetBIOS</b> 名から IP アドレスへのダイナミック マッピングを登録し、クエリーを実行するための分散データベースを提供します。WINS は、複雑なネットワークにおける名前解決で発生する問題を解決できるように設計されているため、このようなルーティング型ネットワークでの <b>NetBIOS</b> の名前解決には最適な選択肢です。 |

---

## X

|              |                                                                                        |
|--------------|----------------------------------------------------------------------------------------|
| <b>X.509</b> | デジタル証明書の定義に広く使用されている規格。X.509 は実際には ITU 勧告であり、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。           |
| <b>xauth</b> | 「 <b>IKE 拡張認証</b> 」を参照。                                                                |
| <b>xlate</b> | xlate は変換エントリとも呼ばれ、1 つの IP アドレスから別の IP アドレス、または 1 つの IP アドレスとポートのペアから別のペアへのマッピングを表します。 |

---

## あ

|                 |                                                                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>アクセス モード</b> | セキュリティ アプライアンスの CLI では複数のコマンド モードが使用されます。各モードで使用可能なコマンドが異なります。「 <b>ユーザ EXEC モード</b> 」、「 <b>特権 EXEC モード</b> 」、「 <b>グローバル コンフィギュレーション モード</b> 」、「 <b>コマンド固有のコンフィギュレーション モード</b> 」も参照してください。 |
| <b>圧縮</b>       | より少ないビット数で表現したり、符号化しない表現で使用する以外の情報関連装置を使用する符号化のプロセス。圧縮を行うことにより、転送パケットのサイズを小さくし、通信のパフォーマンスを向上させることができます。                                                                                   |



|                     |                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アドレス変換              | ネットワーク アドレスまたはポート（あるいはその両方）から別のネットワーク アドレスまたはポートへの変換。「 <a href="#">IP アドレス</a> 」、「 <a href="#">インターフェイス PAT</a> 」、「 <a href="#">NAT</a> 」、「 <a href="#">PAT</a> 」、「 <a href="#">スタティック PAT</a> 」、「 <a href="#">xlate</a> 」も参照してください。                                                                                                                |
| アドレス レゾリューション プロトコル | 「 <a href="#">ARP</a> 」を参照。                                                                                                                                                                                                                                                                                                                         |
| アプレットの自動ダウンロード      | ユーザが最初に Web VPN にログインしたときに、WebVPN ポート転送アプレットを自動的に転送します。                                                                                                                                                                                                                                                                                             |
| 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、キーなどのサービス。「 <a href="#">VPN</a> 」および「 <a href="#">IPSec</a> 」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そのデータを理解できない状態にすること。「 <a href="#">復号化</a> 」も参照してください。                                                                                                                                                                                                                                                     |
| 暗号マップ               | セキュリティ アプライアンスで 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、セキュリティ処理が必要なデータ フローを選択し、そのようなフロー、およびそのトラフィックを送信する必要のある暗号化ピアに対する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対して適用されます。暗号マップには、 <a href="#">IKE</a> と <a href="#">IPSec</a> を使用する <a href="#">VPN</a> 用のセキュリティポリシーを指定するために必要な、 <a href="#">ACL</a> 、暗号規格、ピアなどのパラメータが含まれます。「 <a href="#">VPN</a> 」も参照してください。 |
| 暗黙の規則               | デフォルト規則に基づいて、またはユーザ定義規則の結果として、セキュリティ アプライアンスによって自動的に作成されるアクセス規則。                                                                                                                                                                                                                                                                                    |

---

**い**

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| インターネット              | <a href="#">IP</a> を使用したグローバル ネットワーク。 <a href="#">LAN</a> ではありません。「 <a href="#">イントラネット</a> 」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セキュリティ アプライアンスの間の物理的な接続。                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| インターフェイス PAT         | <a href="#">PAT</a> の IP アドレスが外部インターフェイスの IP アドレスでもあるという状態で使用される <a href="#">PAT</a> 。「 <a href="#">ダイナミック PAT</a> 」および「 <a href="#">スタティック PAT</a> 」を参照してください。                                                                                                                                                                                                                                                                                                                      |
| インターフェイスの ip_address | セキュリティ アプライアンスのネットワーク インターフェイスの IP アドレス。各インターフェイスの IP アドレスは、一意である必要があります。複数のインターフェイスに対して、同じ IP アドレスや、同じ IP ネットワーク上に存在する IP アドレスを指定することはできません。                                                                                                                                                                                                                                                                                                                                        |
| インターフェイス名            | セキュリティ アプライアンスのネットワーク インターフェイスに割り当てられた、読んで理解できる形式の名前。内部インターフェイスと外部インターフェイスのデフォルト名は、それぞれ「inside」と「outside」です。境界インターフェイスのデフォルト名は「 <a href="#">intfn</a> 」で、最初のインターフェイスが <a href="#">intf2</a> 、2 番目が <a href="#">intf3</a> という順序で最後のインターフェイスまで続きます。 <a href="#">intf</a> 文字列に指定される数字は、セキュリティ アプライアンス内のインターフェイス カードの位置に対応します。デフォルトの名前を使用することもできますが、経験のあるユーザの場合は、各インターフェイスに意味のある名前を付けてもかまいません。「 <a href="#">inside</a> 」、「 <a href="#">intfn</a> 」、「 <a href="#">outside</a> 」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。 <a href="#">IP</a> を使用した LAN です。「 <a href="#">ネットワーク</a> 」および「 <a href="#">インターネット</a> 」も参照してください。                                                                                                                                                                                                                                                                                                                                                                       |

---

**お**

|                 |                                                                                    |
|-----------------|------------------------------------------------------------------------------------|
| オブジェクト グループ ピング | ネットワーク オブジェクト（プロトコル、サービス、ホスト、ネットワークなど）のグループにアクセス制御文を適用できるようにすることにより、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。

**カットスルー プロキシ** セキュリティ アプライアンスで、ユーザ認証後のトラフィック フローの高速化を可能にします。カットスルー プロキシは、最初にアプリケーション レイヤでユーザの身分証明を要求します。ユーザの認証が終わると、セキュリティ アプライアンスはセッション フローをシフトし、すべてのトラフィック フローがセッション ステート情報を維持したまま送信元と宛先の間で直接かつ迅速にやり取りされるようにします。

## 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。

**規則** 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、セキュリティ アプライアンスのコンフィギュレーションに追加される条件文。[「ACE」](#)、[「ACL」](#)、[「NAT」](#) も参照してください。

**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りポジトリ。これにより、タスクの実行に必要な時間が短縮されます。キャッシングによって頻繁に再利用されるオブジェクトはシステム キャッシュに保存され、コンテンツを繰り返しライトしたり圧縮する必要性を少なくすることができます。

## く

**クッキー** ブラウザによって保存されるオブジェクト。クッキーは、ユーザ プリファレンスなどの情報を永続的なストレージに格納したものです。

**クライアント / サーバ コンピューティング** トランザクションをクライアント（フロントエンド）とサーバ（バックエンド）の2つの部分で分担す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」](#) も参照してください。

**クライアントのアップデート** これによってユーザは、アップデートを適用するクライアントのリビジョンのアップデートができます。具体的には、アップデートするための URL または IP アドレスが提供されたり、Windows クライアントの場合は、VPN クライアントのバージョンをアップデートする必要についてオプションで通知を受けたりします。

**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 モードを使用すると、セキュリティ アプライアンス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、ユーザ EXEC、特権 EXEC、およびグローバル コンフィギュレーションのコマンドをすべて使用できます。[「ユーザ EXEC モード」](#)、[「特権 EXEC モード」](#)、[「コマンド固有のコンフィギュレーション モード」](#) も参照してください。

## け

**検査エンジン** セキュリティ アプライアンスは、トラフィック内に埋め込まれたアドレッシング情報の位置を確認するために、一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、このような埋め込みアドレスを [NAT](#) で変換したり、変換の影響を受けるチェックサムやその他のフィールドをアップデートすることができます。多くのプロトコルでは、セカンダリの [TCP](#) または [UDP](#) ポートを開いているため、各アプリケーション検査エンジンはセッションを監視して、セカンダリ チャネルのポート番号も確認します。予約済みポート上の初期セッションは、ダイナミックに割り当てられたポート番号をネゴシエートするために使用されます。アプリケーション検査エンジンは、この初期セッションを監視し、ダイナミックに割り当てられたポートを特定し、所定のセッションの間、それらのポート上でのデータ交換を許可します。セキュリティ アプライアンスで検査が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。

## こ

- 公開キー** 公開キーは、Public Key Infrastructure (PKI; 公開キー インフラストラクチャ) に関連するデバイスによって生成されるキー ペアの 1 つです。公開キーで暗号化されたデータは、それに関連付けられた秘密キーを使用した場合にのみ復号化できます。デジタル署名が秘密キーを使用して作成されている場合、受信者は送信者の公開キーを使用して、メッセージがその送信者によって署名されていることを確認することができます。このようなキー 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で、スケーラブルかつセキュアな認証方式が可能になります。
- コマンド固有のコンフィギュレーション モード** いくつかのコマンドは、グローバル コンフィギュレーション モードから、コマンド固有のコンフィギュレーション モードに移行します。このモードでは、ユーザ EXEC、特権 EXEC、グローバル コンフィギュレーション、およびコマンド固有のコンフィギュレーションのコマンドをすべて使用できます。「[グローバル コンフィギュレーション モード](#)」、「[特権 EXEC モード](#)」、「[ユーザ EXEC モード](#)」も参照してください。
- コンテンツのリライトまたは変換** アプリケーションを解釈および変更することにより、WebVPN 接続を介して正しく表示できるようになります。
- コンフィギュレーション、コンフィギュレーション ファイル** ASDM や CLI で管理される設定、プリファレンス、およびプロパティと同等の内容を表すセキュリティ アプライアンス上のファイル。

## 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 として接続する 2 つの IPSec ピア間に確立されます。このタイプの VPN では、どちらの IPSec ピアもトラフィックの宛先や送信元ではありません。各 IPSec ピアは、その IPSec ピアに接続されている LAN 上のホストに暗号化と認証のサービスを提供します。各 LAN 上のホストは、一対の IPSec ピア間に確立されたセキュアなトンネル経由でデータを送受信します。
- サブネット マスク** 「[マスク](#)」を参照。

## し

- 事前共有キー** 事前共有キーは、限定された一定数の IPSec ピアを持つネットワークに適した IKE 認証方式を可能にします。この方式では、IPSec ピアの各ペアにキーを設定する必要があるため、スケーラビリティに限界があります。新しい IPSec ピアをネットワークに追加するときには、そのピアと通信するすべての IPSec ピアに対して事前共有キーを設定する必要があります。証明書と CA を使用すると、よりスケーラブルな IKE 認証方式を実現できます。
- 実行コンフィギュレーション** セキュリティ アプライアンスの RAM で現在実行中のコンフィギュレーション。セキュリティ アプライアンスの動作特性を決定しているコンフィギュレーションです。
- 証明書** ユーザまたはデバイスの ID と、その証明書を発行した CA の公開キーを格納した署名付き暗号オブジェクト。証明書には有効期限があり、攻撃を受けたことがわかった場合は CRL に配置することもできます。また、証明書は IKE ネゴシエーションの否認防止を行います。つまり、特定のピアとの IKE ネゴシエーションが完了したことを第三者に証明できます。
- シリアル伝送** データ キャラクタのビットを 1 つのチャンネルで順次伝送するデータ伝送方式。



## す

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| スタティック PAT       | スタティック Port Address Translation (ポート アドレス変換)。スタティック PAT は、ローカル ポートからグローバル ポートへのマッピングも行うスタティック アドレスです。「 <a href="#">ダイナミック PAT</a> 」および「 <a href="#">NAT</a> 」も参照してください。                                                                                                                                                                                                                                                                                                                          |
| スタンバイ装置          | 「 <a href="#">セカンダリ装置</a> 」を参照。                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ステートフル インспекション | ネットワーク プロトコルは、ステート情報と呼ばれる特定のデータを、2つのホスト間のネットワーク接続の各エンドポイントで保持しています。ステート情報は、パケットの送達保証、データのシーケンス指定、フロー制御、トランザクション ID やセッション ID などのプロトコルの機能を実装するために必要な情報です。プロトコルのステート情報の一部は、各プロトコルの使用中にパケットに格納されて送信されます。たとえば、Web サーバに接続されたブラウザは <a href="#">HTTP</a> を使用し、TCP/IP プロトコルをサポートします。各プロトコル レイヤは、そのレイヤで送受信するパケット内にステート情報を保持します。セキュリティ アプライアンスとその他の一部のファイアウォールは、各パケット内のステート情報を検査し、パケットに格納されたすべてのプロトコルについてその情報が最新で有効であることを確認します。この検査はステートフル インспекションと呼ばれ、コンピュータ セキュリティの特定のタイプの脅威に対して強力な防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 メカニズムを乱すことを目的としたタイプの攻撃。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 <a href="#">VPN</a> 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 <a href="#">インターネット</a> への非暗号化アクセス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ていない場合、 <a href="#">VPN</a> クライアントとセキュリティ アプライアンスの間のすべてのトラフィックが <a href="#">IPSec</a> トンネル経由で送信されます。 <a href="#">VPN</a> クライアントから発信されるすべてのトラフィックがトンネル経由で外部インターフェイスに送信され、リモート サイトから <a href="#">インターネット</a> へのクライアント アクセスは拒否されます。                                                                                                                                   |

## せ

|               |                                                                                                                                                                             |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| セカンダリ装置       | 2 台のセキュリティ アプライアンス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。                                                                                                                            |
| セキュリティ コンテキスト | 1 台のセキュリティ アプライアンスを、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パーティション化することができます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したファイアウォールです。マルチコンテキストは、複数のスタンドアロン ファイアウォールを使用することに似ています。 |
| セキュリティ サービス   | 「 <a href="#">暗号</a> 」を参照。                                                                                                                                                  |

## た

|         |                                                                                                                                                              |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ターボ ACL | <a href="#">ACL</a> をコンパイルして複数のルックアップ テーブルのセットにすることにより、ルックアップを高速化します。元の <a href="#">ACL</a> エントリ数とは無関係に、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。 |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|

|            |                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ダイナミック NAT | 「 <a href="#">NAT</a> 」および「 <a href="#">アドレス変換</a> 」を参照。                                                                                                                                                                                                                                                                                                                                                       |
| 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 を使用すると、複数の発信セッションが 1 つの IP アドレスから発信されているように見えます。PAT がイネーブルになっていると、セキュリティ アプライアンスは、各発信変換スロット（ <a href="#">xlate</a> ）用に 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 が発信接続に十分な数の一意の IP アドレスを割り当てられない場合に役立ちます。グローバル プール アドレスは、常に PAT アドレスが使用されるよりも前に使用されます。「 <a href="#">NAT</a> 」、「 <a href="#">スタティック PAT</a> 」、および「 <a href="#">xlate</a> 」も参照してください。 |

## て

|          |                                                                                                                                                 |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| データ機密性   | 攻撃者から読み取られないようにデータを操作するすべての方式を表します。一般に、このような操作は、データの暗号化、および通信の関係者のみが入手できる <a href="#">キー</a> によって実現されます。                                        |
| データ整合性   | <a href="#">秘密キー</a> または <a href="#">公開キー</a> のアルゴリズムに基づく暗号化を使用して、保護されたデータの一部を受信するユーザが、そのデータが搬送中に変更されていないことを確認できるメカニズム。                         |
| データ発信者認証 | 保護されたデータがその送信者のみから発信されていることを受信者が確認できるセキュリティ サービス。このサービスには、データ整合性サービスと、 <a href="#">秘密キー</a> が送信者と受信者の間だけで共有される <a href="#">キー</a> 配布メカニズムが必要です。 |
| デジタル証明書  | 「 <a href="#">証明書</a> 」を参照。                                                                                                                     |
| 転送モード    | 各パケットのデータ部分（ペイロード）のみを暗号化し、ヘッダーはそのままの状態にする <a href="#">IPSec</a> 暗号化モード。転送モードはトンネル モードより安全性が低くなります。                                              |

## と

|               |                                                                                                                                                                                                                                                                        |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 透過ファイアウォールモード | セキュリティ アプライアンスがルータ ホップとにならないモード。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 コンフィギュレーションを簡略化したり、セキュリティ アプライアンスが攻撃者から認識されないように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、 <a href="#">ルーテッド ファイアウォール モード</a> ではブロックされる経路をトラフィックが通過するようにすることもできます。「 <a href="#">ルーテッド ファイアウォール モード</a> 」も参照してください。 |
| 登録局           | 「 <a href="#">RA</a> 」を参照。                                                                                                                                                                                                                                             |
| 特権 EXEC モード   | 特権 EXEC モードでは、現在の設定を変更することができます。すべてのユーザ EXEC モード コマンドは、特権 EXEC モードで動作します。「 <a href="#">コマンド固有のコンフィギュレーション モード</a> 」、「 <a href="#">グローバル コンフィギュレーション モード</a> 」、「 <a href="#">ユーザ EXEC モード</a> 」も参照してください。                                                               |
| 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、各トラフィックが設定されている最大レート（ビット / 秒）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証します。                                                                                                                                                                 |
| トランスフォーム セット  | 「 <a href="#">IPSec トランスフォーム セット</a> 」を参照。                                                                                                                                                                                                                             |
| 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、トンネルにより、リモート <a href="#">VPN</a> 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 <a href="#">IPSec</a> 暗号化モード。トンネルモードは転送モードより安全性が高くなります。                                                                                                                                                                               |

## に

**認証** ユーザの ID とデータの整合性を検証する暗号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 つです。認証により、データストリームの整合性が確保され、搬送中に改ざんされないことが保証されます。また、認証により、データストリームの発信元が確認されます。「[AAA](#)」、「[暗号化](#)」、および「[VPN](#)」も参照してください。

## ね

**ネットマスク** 「[マスク](#)」を参照。

**ネットワーク** セキュリティ アプライアンスのコンフィギュレーションから見ると、ネットワークは 1 つのホストではなく、特定の 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です。ネットワークは複数のノードと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](#)」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デバイス。「[ホスト](#)」および「[ネットワーク](#)」も参照してください。

## は

**バックアップサーバ** IPSec バックアップサーバを使用すると、VPN クライアントはプライマリのセキュリティ アプライアンスが使用不可の場合も接続が可能になります。

**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に対して動作する単方向の機能であり、暗号化サービスがデータの整合性を保証するために使用す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](#) よりもダイジェストが小さく、わずかに速いとされています。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](#)」も参照してください。

**発信** 発信元インターフェイスよりもセキュリティ レベル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** 公開キー システムとも呼ばれます。非対称暗号化では、他の任意のユーザの公開キーに誰でもアクセスすることができます。公開キーにアクセスしたユーザは、その公開キーを使用してキー所有者に暗号化メッセージを送信することができます。「[暗号化](#)」および「[公開キー](#)」も参照してください。

**秘密キー** 秘密キーは、送信者と受信者の間だけで共有されるキーです。「[キー](#)」および「[公開キー](#)」を参照してください。

## ふ

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| フィックスアップ             | 「 <a href="#">検査エンジン</a> 」を参照。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| プール                  | 「 <a href="#">IP プール</a> 」を参照。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| フェーズ 1               | 「 <a href="#">IPSec フェーズ 1</a> 」を参照。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| フェーズ 2               | 「 <a href="#">IPSec フェーズ 2</a> 」を参照。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| フェールオーバー、フェールオーバーモード | フェールオーバーを使用すると、2 台のセキュリティ アプライアンスを設定して、一方に障害が発生した場合にもう一方がその動作を引き継ぐようにすることができます。セキュリティ アプライアンスは、Active/Active フェールオーバーと Active/Standby フェールオーバーの 2 つのフェールオーバーをサポートします。各フェールオーバー コンフィギュレーションには、フェールオーバーを判定および実行する独自の方式があります。Active/Active 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渡すことができます。これによって、ネットワークのロードバランシングを設定できます。Active/Active フェールオーバーは、マルチコンテキスト モードで実行中の装置でのみ使用できます。Active/Standby フェールオーバーでは、1 つの装置だけがトラフィックを渡すことができ、もう 1 つの装置はスタンバイ状態で待機します。Active/Standby フェールオーバーは、シングルコンテキスト モードで実行中の装置とマルチコンテキスト モードで実行中の装置の両方で使用できます。 |
| 不揮発性ストレージ、メモリ        | RAM とは異なり、電源が入っていない場合でも内容を保持しているストレージまたはメモリ。不揮発性ストレージ デバイス内のデータは、パワーオフ / パワーオン（電源再投入）やリブートを実行しても失われません。                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 復号化                  | 暗号化された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たユーザがそのデータを理解できる状態にすること。「 <a href="#">暗号化</a> 」も参照してください。                                                                                                                                                                                                                                                                                                                                                                                                                             |
| プライマリ、プライマリ装置        | 2 台のセキュリティ アプライアンス（プライマリとセカンダリ）がフェールオーバー モードで動作している場合に、通常動作している方の装置。                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| フラッシュ、フラッシュメモリ       | セキュリティ アプライアンスの電源がダウンしている場合にコンフィギュレーション ファイルを保存するために使用される不揮発性ストレージ デバイス。                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| プロキシ ARP             | セキュリティ アプライアンスが、グローバル プール内の IP アドレスに対する <a href="#">ARP</a> 要求に応答できるようにします。「 <a href="#">ARP</a> 」も参照してください。                                                                                                                                                                                                                                                                                                                                                                                                                  |
| プロトコル、プロトコルのリテラル     | ネットワーク ノード間の通信用のパケット交換について定義した規格。プロトコルはレイヤ構造で連携動作します。セキュリティ アプライアンスのコンフィギュレーションでは、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、リテラル値またはポート番号で指定されます。セキュリティ アプライアンスで指定可能なプロトコルのリテラル値は、ahp、eigrp、esp、gre、icmp、igmp、igrp、ip、ipinip、ipsec、nos、ospf、pcp、snp、tcp、および udp です。                                                                                                                                                                                                                                                                          |

## へ

|        |                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ヘッドエンド | パブリック ネットワーク経由の <a href="#">VPN</a> クライアント接続に対して、プライベート ネットワークへのエントリ ポイントとして機能するファイアウォール、コンセントレータ、またはその他のホスト。「 <a href="#">ISP</a> 」および「 <a href="#">VPN</a> 」も参照してください。 |
| 変換     | 「 <a href="#">xlate</a> 」を参照。                                                                                                                                            |

## ほ

|     |                                                                                                     |
|-----|-----------------------------------------------------------------------------------------------------|
| ポート | <a href="#">TCP</a> および <a href="#">UDP</a> プロトコルのパケット ヘッダー内で、パケットの送信元または宛先である上位レベルのサービスを識別するフィールド。 |
|-----|-----------------------------------------------------------------------------------------------------|

|              |                                                                                                                                                      |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| ホスト          | TCP/IP ネットワーク上で IP アドレスを持つ任意のデバイスの名前。「 <a href="#">ネットワーク</a> 」および「 <a href="#">ノード</a> 」も参照してください。                                                  |
| ホスト / ネットワーク | アドレス変換 ( <a href="#">xlate</a> ) や <a href="#">ACE</a> など、セキュリティ アプライアンスのコンフィギュレーションにおいて、1 つのホストまたはネットワーク サブネットを識別するために他の情報とともに使用される IP アドレスとネットマスク。 |
| ポリシー NAT     | アクセスリストに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り、アドレス変換の対象となるローカルトラフィックを識別します。                                                                                  |

---

## ま

|         |                                                                                                                                                                                                                |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| マスク     | <a href="#">インターネット</a> アドレスが、ネットワーク、サブネット、およびホストの部分にどのように分割されているかを示す 32 ビットのマスク。マスク内では、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にビットが指定され、ホストの部分にはゼロが指定されます。マスクには少なくとも標準ネットワークの部分が必要であり、サブネット フィールドはネットワークの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 アドレッシング方式を指します。「 <a href="#">PIM</a> 」および「 <a href="#">SMR</a> 」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、メッセージの整合性を保証するために使用される <a href="#">MD5</a> や <a href="#">SHA-1</a> などのハッシュ アルゴリズムによって作成されます。 |
|--------------|------------------------------------------------------------------------------------------------------------|

---

## も

|     |                                  |
|-----|----------------------------------|
| モード | 「 <a href="#">アクセス モード</a> 」を参照。 |
|-----|----------------------------------|

---

## ゆ

|              |                                                                                                                                                                                                                                    |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ユーザ EXEC モード | ユーザ EXEC モードを使用すると、セキュリティ アプライアンスの設定を表示できます。初めてセキュリティ アプライアンスにアクセスしたとき、ユーザ EXEC モード プロンプトが表示されます。「 <a href="#">コマンド固有のコンフィギュレーション モード</a> 」、「 <a href="#">グローバル コンフィギュレーション モード</a> 」、および「 <a href="#">特権 EXEC モード</a> 」も参照してください。 |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## り

|        |                                                                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| リプレイ検出 | 受信者がリプレイ攻撃を無効にするために、古いパケットまたは重複したパケットを拒否できるセキュリティ サービス。リプレイ攻撃は、攻撃者が古いパケットまたは重複したパケットを受信者に送信し、受信者がその偽のパケットを正当なものと認識するというしくみの攻撃です。リプレイ検出は、シーケンス番号と認証を組み合わせることで実行され、 <a href="#">IPSec</a> の標準機能となっています。 |
| リフレッシュ | セキュリティ アプライアンスから実行コンフィギュレーションを取得して、画面をアップデートします。アイコンとボタンで同じ機能が実行されます。                                                                                                                                 |

---

## 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 モードでは、セキュリティ アプライアンスはネットワーク内でルータホップとして数えられます。接続されたネットワークの間で [NAT](#) を実行し、[OSPF](#) または [RIP](#) を使用することができます。「[透過ファイアウォール モード](#)」も参照してください。

**ルート、ルーティング** [ネットワーク](#)を通過するパス。

---

## れ

**レイヤ** ネットワーキング モデルは、異なるプロトコルと関連付けられた複数のレイヤを実装しています。最も一般的なネットワーキング モデルは OSI モデルです。これは7つのレイヤで構成されます。これらのレイヤの順番は、物理、データリンク、ネットワーク、トランスポート、セッション、プレゼンテーション、およびアプリケーションです。



## INDEX

### Symbols

/ビットサブネットマスク D-3  
?  
    コマンド文字列 C-5  
    ヘルプ C-5

### Numerics

4GE SSM  
    SFP 4-4  
    コネクタ タイプ 4-2  
    ファイバ 4-4

### A

#### AAA

Web クライアントの使用 16-4  
アカウントिंग 16-14  
アドレッシング、設定 27-3  
概要 10-2  
サーバ  
    タイプ 10-4  
    追加 10-17  
サポートの要約 10-4  
認可  
    コマンド 33-8  
    ダウンロード可能なアクセスリス 16-8  
    ネットワーク アクセス 16-7  
認証  
    CLI アクセス 33-6  
    特権 EXEC モード 33-7  
    ネットワーク アクセス 16-2  
パフォーマンス 16-1  
ローカル データベースのサポート 10-13  
ACE  
    ロギング 13-23

#### ACL

IPSec 24-22  
WebVPN ユーザ名アトリビュート 26-72  
    グループポリシーの WebVPN フィルタ 26-52  
ACL フィルタ  
    ユーザ名アトリビュート 26-64  
Active/Active フェールオーバー  
    アクション 11-14  
    概要 11-11  
    コマンドの複製 11-13  
    コンフィギュレーションの同期 11-12  
    セカンダリ ステータス 11-12  
    設定  
        HTTP 複製 11-35  
        LAN ベースのフェールオーバー 11-30  
        インターフェイスのポーリング時間 11-35  
        インターフェイスのモニタリング 11-35  
        仮想 MAC アドレス 11-36  
        ケーブルベースのフェールオーバー 11-28  
        前提条件 11-27  
        装置のポーリング時間 11-35  
        非同期ルーティングのサポート 11-37  
        フェールオーバー グループのプリエンブショ  
            ン 11-34  
        フェールオーバーの基準 11-36  
    装置の初期化 11-12  
    重複 MAC アドレスの回避 11-11, 11-36  
    トリガー 11-13  
    プライマリ ステータス 11-12  
Active Directory の手順 E-19 - E-24  
Active/Standby フェールオーバー  
    アクション 11-10  
    概要 11-7  
    コマンドの複製 11-9  
    コンフィギュレーションの同期 11-8  
    セカンダリ装置 11-8

- 設定
    - HTTP 複製 11-25
    - LAN ベース 11-21
    - インターフェイスのポーリング時間 11-26
    - インターフェイスのモニタリング 11-25
    - 仮想 MAC アドレス 11-27
    - ケーブルベース 11-19
    - 前提条件 11-19
    - 装置のポーリング時間 11-26
    - フェールオーバーの基準 11-26
    - 装置の初期化 11-8
    - トリガー 11-9
    - プライマリ装置 11-8
  - Advanced Encryption Standard (AES) 24-4
  - AIP SSM
    - イメージのロード 19-18
    - 概要 19-2
    - コンフィギュレーション 19-2
    - 初期セットアップ 19-5
    - ステータスのチェック 19-1, 19-17
    - ～へのトラフィックの送信 19-3
  - Application Access パネル、WebVPN 30-38
  - ARP
    - 検査
      - イネーブル化 23-3
      - 概要 23-2
      - スタティック エントリ 23-3
      - テスト、フェールオーバー 11-18
  - ARP 検査
    - 概要 23-2
    - スタティック ARP エントリ、追加 23-3
    - 設定 23-2
  - ARP スプーフィング 23-2
  - ASA 1-4
  - ASDM ソフトウェア
    - インストール 34-4
  - ASR 11-37
    - 「非対称ルーティングのサポート」を参照
  - Auto-MDI/MDIX 4-2
  - Auto-Update
    - 設定 34-13 - ??
- B**
- Baltimore Technologies
    - CA サーバのサポート 32-4
  - Bandwidth Limiting Traffic ストリーム (BLT) 21-9
  - BGP 13-7
  - BPDU
    - ACL、EtherType 13-9
- C**
- CA
    - CR と～ 32-3
    - 公開キー暗号化 32-2
    - サーバのサポート 32-4
    - サポート対象のサーバ 32-4
    - 無効になった証明書 32-3
  - CA 証明書検証、WebVPN では実行されない 30-2
  - Certificate Revocation List
    - 「CRL」を参照
  - Cisco 32-4
  - Cisco IP Phone
    - DHCP 8-31
    - アプリケーション検査 22-52
  - Cisco LDAP アトリビュート E-7
  - Cisco-AV-Pair LDAP アトリビュート E-14
  - Class A、B、および C のアドレス D-2
  - CLI
    - コマンド出力のページング C-7
    - コマンドラインの編集 C-4
    - コメントの追加 C-7
    - 省略形のコマンド C-4
    - シンタックスの書式 C-4
    - 表示 C-7
    - ページング C-7
    - ヘルプ C-5
  - crypto show コマンド 24-29
  - CSC SSM
    - イメージのロード 19-18
    - 概要 19-7
    - 準備 19-9
    - スキャン対象 19-11
    - ステータスのチェック 19-1, 19-17
    - フェールオーバー 19-9
    - ～へのトラフィックの送信 19-14
  - CSD サポート A-7



## D

deny-message  
     ユーザ名の webvpn アトリビュート 26-71  
     グループポリシーの WebVPN アトリビュート 26-50

## DES

IKE ポリシーのキーワード (表) 24-4

DfltGrpPolicy 26-24

## DHCP

アドレッシング、設定 27-4

サーバ

    Cisco IP Phone 8-31

    概要 8-28

    設定 8-28

透過ファイアウォール 13-7

リレー 8-32

## Diffie-Hellman

グループ 5 24-5

サポートされるグループ 24-5

DMZ、定義 1-2

## DNS

～に対する NAT の影響 14-14

DNS、WebVPN 用の設定 30-17

## DNS 検査

概要 22-12

管理 22-12

リライト、概要 22-13

リライト、設定 22-14

DNS サーバ、設定 26-27

## DSA キー

生成 32-6

## E

ECMP 8-3

EIGRP 13-7

## enable

アクセス 2-2

## Entrust

CA サーバのサポート 32-4

ESP セキュリティ プロトコル 24-2

## established コマンド

セキュリティ レベルの要件 6-2

## EtherType

割り当て番号 13-9

## F

FO (フェールオーバー) ライセンス 11-3

FO\_AA ライセンス 11-3

## FTP 検査

概要 22-20

設定 22-20

## G

## group-lock

ユーザ名アトリビュート 26-66

## GTP 検査

概要 22-24

設定 22-24

## H

## H.225

タイムアウト 22-33

## H.245

トラブルシューティング 22-34

## H.323

トラブルシューティング 22-33, 22-34

## H.323 検査

概要 22-31

制限 22-32

設定 22-31

HMAC ハッシュ方式 24-3

## hosts ファイル

WebVPN 30-22

エラー 30-21

hosts ファイル、再設定 30-22

HSRP 12-9

## html-content-filter

ユーザ名の WebVPN アトリビュート 26-69

グループポリシーの WebVPN アトリビュート 26-50

## HTTP

認証 33-6

フィルタリング 17-5

## HTTP 検査

概要 22-35

設定 22-35

HTTP/HTTPS Web VPN プロキシ、設定 30-5

- HTTPS
  - WebVPN セッションでの 30-3
- I
- ICMP
  - 接続のテスト 36-2
  - タイプ番号 D-18
- IKE
  - 「ISAKMP」も参照 28-4
  - ポリシーの作成 24-5
  - 利点 24-3
- IKE キープアライブの設定
  - トンネルグループ 26-4
- ILS
  - アプリケーション検査 22-40
- IM 22-49
- Internet Security Association and Key Management Protocol
  - 「ISAKMP」を参照
- IP Phone Bypass、グループポリシー 26-39
- IP アドレス
  - VPN 用の設定 27-1
  - 管理、透過ファイアウォール 7-6
  - クラス D-2
  - コンテキスト間の重複 3-4
  - サブネット マスク D-5
  - プライベート D-2
  - ローカル IP アドレス プールの設定 27-2
  - 割り当て方式の設定 27-2
- IP スプーフィング
  - 防止 20-7
- IPS コンフィギュレーション 19-2
- IPSec
  - ACL 24-22
  - Cisco VPN Client 24-2
  - LAN-to-LAN コンフィギュレーション 24-2
  - over NAT-T、イネーブル化 24-8
  - over TCP、イネーブル化 24-9
  - SA ライフタイム、変更 24-24
  - アクティブな VPN セッションの最大数の設定 25-4
  - 暗号マップ エントリ 24-15
  - 概要 24-2
  - コンフィギュレーションの表示 24-29
  - スタティック暗号マップ付きの基本的なコンフィギュレーション 24-24
  - 設定 24-1, 24-14
  - トンネル 24-14
  - フラグメンテーション ポリシー 24-9
  - リモートアクセス設定 24-2
- IPSec over UDP、グループポリシー、アトリビュートの設定 26-34
- IPSec パラメータ、トンネルグループ 26-4
- IPSec リモートアクセス トンネルグループ 26-7
- IPv6
  - IPv4 とともに設定 9-8
  - アクセスリスト 9-6
  - イネーブル化 9-3
  - 確認 9-7
  - コマンド 9-2
  - スタティック ルート 9-5
  - デフォルト ルート 9-5
  - デュアル IP スタック 9-8
- IPv6 アドレス
  - エニーキャスト D-11
  - 形式 D-6
  - ～のタイプ D-7
  - 必須 D-11
  - プレフィックス D-12
  - マルチキャスト D-10
  - ユニキャスト D-7
  - ～をサポートするコマンド 9-2
- ISAKMP
  - Aggressive モードでのディセーブル化 24-7
  - 「IKE」も参照 28-4
  - 外部インターフェイスでのイネーブル化 24-7, 28-4
  - 概要 24-3
  - 設定 24-1, 24-3
  - ピアの識別方式の決定 24-8
  - ポリシー、設定 24-6
- ISAKMP キープアライブの設定
  - トンネルグループ 26-4
- ISAKMP ピアの識別方式、決定 24-8
- J
- Java アプレット
  - フィルタリング 17-2

- K**
- keep-alive-ignore
    - グループポリシーの WebVPN アトリビュート 26-55
    - ユーザ名の webvpn アトリビュート 26-74
  - Kerberos
    - サポート 10-8
    - 設定 10-17
- L**
- LAN-to-LAN トンネルグループ、設定 26-12
  - LDAP
    - AAA サーバの設定 E-4 - E-19
    - AAA サポート 10-9
    - Cisco アトリビュート E-7
    - Cisco-AV ペア E-14
    - SASL 10-9
    - アトリビュート マッピング 10-11
    - アプリケーション検査 22-40
    - 階層の例 E-5
    - 権限ポリシー E-3
    - サーバタイプ 10-10
    - サーバ設定の概要 E-4
    - スキーマの計画 E-4 - E-6
    - スキーマの例 E-16
    - スキーマのロード E-18
    - 設定 10-17
    - 設定手順の例 E-19 - E-24
    - ディレクトリの概要 E-4
    - ディレクトリの検索 E-5
    - ユーザ権限 E-18
    - ユーザ認可 10-10
    - ユーザ認証 10-9
  - LEAP Bypass、グループポリシー 26-40
  - LLQ
    - 「低遅延キュー」を参照
- M**
- MAC アドレス テーブル 23-4
    - MAC ラーニング、ディセーブル化 23-5
    - エントリ タイムアウト 23-5
    - 概要 12-12
    - スタティック エントリ 23-4
  - MAC アドレス、フェールオーバー 11-8
  - MAC ラーニング、ディセーブル化 23-5
  - MAPI、設定 30-31
  - mask
    - 応答、ICMP メッセージ D-18
    - 要求、ICMP メッセージ D-18
  - MD5
    - IKE ポリシーのキーワード (表) 24-4
  - MGCP 検査
    - 概要 22-41
    - 設定 22-41
  - MIB 35-2
  - Microsoft Windows 2000 CA
    - サポート対象 32-4
  - More プロンプト C-7
  - MPLS
    - LDP 13-9
    - router-id 13-9
    - TDP 13-9
- N**
- N2H2 フィルタリング サーバ
    - Web サイトの URL 17-5
    - サポート対象 17-5
  - NAT
    - DNS 14-14
    - NAT ID 14-17
    - NAT による免除
      - 概要 14-9
      - コンフィギュレーション 14-33
    - NAT の識別
      - 概要 14-9
      - コンフィギュレーション 14-31
    - NAT のバイパス
      - 概要 14-9
      - コンフィギュレーション 14-31
    - PAT
      - 概要 14-7
      - 実装 14-17
      - 設定 14-23
    - RPC でサポートされていない 22-57
    - 同じセキュリティ レベル 14-13
    - 概要 14-2
    - スタティック NAT
      - 概要 14-8

- 設定 14-26
    - スタティック PAT
      - 概要 14-8
      - 設定 14-28
    - スタティック アイデンティティ、設定 14-32
    - セキュリティ レベルの要件 6-2
    - ダイナミック NAT
      - 概要 14-5
      - 実装 14-17
      - 設定 14-23
    - タイプ 14-5
    - 重複するアドレス 14-35
    - 透過ファイアウォール 12-11
    - 文の順序 14-13
    - ポート リダイレクション 14-37
    - ポリシー NAT
      - 概要 14-10
    - 例 14-35
  - NAT-T
    - IPSec over NAT-T のイネーブル化 24-8
    - 使用方法 24-9
  - Netscape CMS
    - CA サーバのサポート 32-4
  - NT サーバ
    - サポート 10-8
    - 設定 10-17
  - NTLM サポート 10-8
- O
- OSPF
- cost 8-10
  - dead interval 8-10
  - hello interval 8-10
  - MD5 認証 8-10, 8-12
  - NSSA 8-12
  - アップデート パケット ペーシングの表示 8-16
  - イネーブル化 8-6
  - インターフェイスのパラメータ 8-9
  - エリア パラメータ 8-11
  - エリアの認証 8-12
  - 概要 8-5
  - サマリー 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
  - 認証キー 8-9
  - ネイバーの状態のロギング 8-16
  - パケット ペーシング 8-16
  - プロセス 8-5
  - モニタリング 8-17
  - リンクステート アドバタイズメント 8-6
  - ルート計算タイマー 8-15
  - ルート集約 8-13
  - ルートの再配布 8-7
  - ルートマップ 8-7
  - Outlook Exchange プロキシ、設定 30-31
  - Outlook Web Access (OWA) および WebVPN 30-54
  - Outlook 接続、終了 30-31
- P
- password-storage、ユーザ名アトリビュート 26-66
  - PAT
    - スタティック 14-28
  - PAT (Port Address Translation)
    - 「NAT」も参照
    - 制限 22-48
  - ping
    - 「ICMP」を参照
  - PKI プロトコル 32-7
  - port-forward
    - ユーザ名の webvpn アトリビュート 26-73
  - port-forward-name
    - ユーザ名の webvpn アトリビュート 26-73
  - port-forward
    - グループポリシーの WebVPN アトリビュート 26-54
  - port-forward-name
    - グループポリシーの WebVPN アトリビュート 26-54
- Q
- QoS
- match コマンドの基準 21-7
  - アクション 21-4
  - 概念 21-3
  - 概要 21-2
  - (定義) 21-2
  - 統計情報 21-19
  - 統計情報の表示 21-19
  - トラフィック クラス 21-4

- トラフィックの分類 21-6
  - ポリシー 21-1
  - ポリシー、設定 21-4
  - ポリシーマップの定義 21-8
  - ポリシング 21-3
- QoS 統計情報の表示 21-19
- QoS 用のトラフィックの分類 21-6
- Quality of Service、「QoS」を参照
- R
- RADIUS
  - AAA サーバの設定 E-26
  - Cisco AV ペア E-14
  - アトリビュート E-26
  - アトリビュート ポリシー E-3
  - 権限ポリシー E-3
  - サーバの設定 10-17
  - サポート 10-5
  - ダウンロード可能なアクセスリスト 16-9
  - ネットワーク アクセス認証 16-3
  - ネットワーク アクセスの認可 16-8
- RAS
  - H.323 のトラブルシューティング 22-34
- RealPlayer 22-47
- RIP
  - イネーブル化 8-19
  - 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
- RS-232 ケーブル
  - 「フェールオーバー」を参照 11-5
- RSA
  - KEON
    - CA サーバのサポート 32-4
  - キー
    - 生成 32-6, 33-3
  - シグニチャ
    - IKE 認証方式 32-2
- RTSP 検査
  - 概要 22-47
  - 設定 22-47
- S
- SA
  - ライフタイム 24-24
- SCCP (Skinny) 検査
  - 概要 22-52
  - コンフィギュレーション 22-52
  - 設定 22-52
- SDI
  - サポート 10-7
  - 設定 10-17
- SHA
  - IKE ポリシーのキーワード (表) 24-4
- show コマンド、フィルタリング出力 C-6
- SIP
  - トラブルシューティング 22-51
- SIP 検査
  - インスタント メッセージ 22-49
  - 概要 22-49
  - 設定 22-49
  - タイムアウト 22-50
- SMTP 検査
  - 設定 22-54
- SNMP
  - MIB 35-2
  - 概要 35-1
  - トラップ 35-2
- SSH
  - RSA キー 33-3
  - 同時接続 33-3
  - 認証 33-6
  - ユーザ名 33-4
  - ログイン 33-4
- SSL
  - VPN コンセントレータにアクセスするために使用 30-3
  - 証明書 30-5
- SSL VPN Client (SVC)
  - グループポリシーの WebVPN アトリビュート 26-56
  - ユーザ名の webvpn アトリビュート 26-75
- SSL VPN クライアント
  - DPD 31-7
  - 圧縮 31-9
  - イネーブル化 31-4
    - 相手先固定インストール 31-6
    - アドレス割り当て 31-4

- グループおよびユーザ 31-5
- トンネルグループ 31-4
- インストール 31-2
- イメージ 31-2
- 順序 31-2
- キープアライブ メッセージ 31-8
- セッションの表示 31-10
- セッションのログオフ 31-11
- 利点 31-1
- SSL を使用した VPN コンセントレータへのアクセス 30-3
- SSL/TLS 暗号化プロトコル
  - WebVPN 30-4
  - 設定 30-4
- SSM
  - 「AIP SSM」も参照
  - 「CSC SSM」も参照
  - イメージのロード 19-18
  - コンフィギュレーション
    - AIP SSM 19-2
    - CSC SSM 19-9
  - ステータスのチェック 19-1, 19-17
- sso-server
  - グループポリシーの WebVPN アトリビュート 26-55
  - ユーザ名の webvpn アトリビュート 26-75
- Stub Multicast Routing
  - 「SMR」を参照
- Sun Microsystems Java™ Runtime Environment (JRE) と WebVPN 30-52, 30-53
- Sun RPC 検査
  - 概要 22-57
  - 設定 22-57
- SVC
  - グループポリシーの WebVPN アトリビュート 26-56
  - ユーザ名の webvpn アトリビュート 26-75
- T
- TACACS+
  - サーバの設定 10-17
  - サポート 10-6
  - ネットワーク アクセスの認可 16-7
- TACACS+ コマンド認可
  - 設定 33-12
- TCP
  - シーケンス番号のランダム化
  - ディセーブル化
    - ルーテッド モード 14-24
  - ポートとリテラル値 D-13
- TCP の正規化
  - 設定 20-2
- Telnet
  - 同時接続 33-2
  - 認証 33-6
- TKS1 を使用した VPN コンセントレータへのアクセス 30-3
- TLS1
  - VPN コンセントレータにアクセスするために使用 30-3
- tx-ring-limit 21-11
- U
- U ターン 24-21
- UDP
  - コネクション ステート情報 1-5
  - ポートとリテラル値 D-13
- UR (無制限) ライセンス 11-3
- URL
  - コンテキスト コンフィギュレーション、設定 5-4
  - コンテキスト コンフィギュレーション、変更 5-8
  - フィルタリング 17-5
  - フィルタリング、設定 17-7
- url-list
  - グループポリシーの WebVPN アトリビュート 26-53
  - ユーザ名の webvpn アトリビュート 26-72
- V
- VeriSign
  - CA の設定、例 32-4
- VLAN 4-5
  - 共有 3-7
  - コンテキストの割り当て 5-2
  - マッピング インターフェイス名 5-3
- VoIP
  - トラブルシューティング 22-33
  - プロキシ サーバ 22-49

- VPN
  - IPSec セッションの最大数の設定 25-4
  - クライアント、IPSec アトリビュート 24-2
  - パラメータ、一般、設定 25-1
  - vpn-filter ユーザ名アトリビュート 26-64
  - vpn-framed-ip-address ユーザ名アトリビュート 26-65
  - vpn-idle-timeout ユーザ名アトリビュート 26-63
  - vpn-session-timeout ユーザ名アトリビュート 26-64
  - vpn-tunnel-protocol ユーザ名アトリビュート 26-65
  - VPN アトリビュート、グループポリシー 26-28
  - VPN ハードウェア クライアント、グループポリシー アトリビュート 26-38
  - vpn ロードバランシング、「ロードバランシング」を参照 25-8
  - vpn-filter ユーザ名アトリビュート 26-64
  - VRRP 12-9
- W
- WebVPN での SSO 30-6 - 30-16
  - HTTP Basic 認証および NTLM 認証の設定 30-6
  - HTTP Form プロトコルの設定 30-10
  - SiteMinder の設定 30-7
- Web クライアント
  - セキュア認証 16-4
- web 電子メール (Outlook Web Access)
  - Outlook Web Access 30-31
- WebVPN
  - CA 証明書検証は実行されない 30-2
  - hosts ファイル 30-22
  - hosts ファイル、再設定 30-22
  - HTTP/HTTPS プロキシ、設定 30-5
  - HTTPS の使用 30-3
  - SSL/TLS 暗号化プロトコル 30-4
  - URL 30-50
  - 印刷と～ 30-50
  - エンド ユーザ インターフェイスの定義 30-36
  - エンド ユーザ設定 30-36
  - クッキー 30-5
  - クライアント アプリケーション要件 30-49
  - クライアント要件 30-49
    - Web ブラウジング用の 30-51
    - アプリケーションを使用するための 30-52
    - 起動 30-50
    - ネットワーク ブラウジング用の 30-52
    - ファイル管理用の 30-52
    - ポート転送用の 30-52
  - グループポリシー アトリビュート、設定 30-20
  - グループポリシーへのユーザの割り当て 30-18
  - サポートされていない機能 30-3
  - サポートされるアプリケーション 30-49
  - サポートされているインターネット接続のタイプ 30-50
  - サポートされているブラウザ 30-50
  - 使用上の推奨事項 30-36, 30-49
  - セキュリティ対策 30-2, 30-6
  - セキュリティのヒント 30-49
  - セッションの確立 30-3
  - 設定
    - グローバル DNS 30-17
    - 電子メール 30-30
  - 設定、HTTP/HTTPS プロキシの 30-4
  - 定義 30-2
  - デジタル証明書による認証 30-16
  - デジタル証明書認証の制限事項 30-5
  - 電子メール 30-30
  - 電子メール プロキシ 30-30
  - 特定ユーザの設定 26-66
  - トラブルシューティング 30-21
  - ～のためにクッキーをイネーブルにする 30-52
  - 必要なユーザ名とパスワード 30-50
  - フローティング ツールバー 30-38
  - ユーザ名とパスワード 30-48
  - リモート システム コンフィギュレーションとエンド ユーザの要件 30-50
- WebVPN、Application Access パネル 30-38
- webvpn アトリビュート
  - グループポリシー 26-47
  - トンネルグループ 26-5
- WebVPN グループポリシー アトリビュート
  - 機能 26-48
- WebVPN での Web ブラウジング 30-51
- WebVPN の PDA サポート 30-29
- WebVPN ユーザ用のログイン ウィンドウのカスタマイズ 26-22
- WINS サーバ、設定 26-27
- あ
- アイドル タイムアウト
  - ハードウェア クライアント ユーザ、グループポリシー 26-39

- ユーザ名アトリビュート 26-63
  - アクセス時間
    - ユーザ名アトリビュート 26-62
  - アクセスリスト
    - ACE ロギング、設定 13-23
    - EtherType、追加 13-9
    - IP アドレスのガイドライン 13-3
    - NAT アドレス 13-3
    - NAT ガイドライン 13-3
    - QoS トラフィック分類での使用 21-6
    - アクティビティのロギング 13-23
    - アクティブ化のスケジュール設定 13-21
    - 暗黙的な拒否 13-3
    - インターフェイス、適用 15-5
    - オブジェクト グループ ping 13-12
    - オブジェクト グループ 13-19
    - 概要 13-2
    - 拡張、概要 13-6
    - 拡張、追加 13-7
    - 拒否フロー、管理 13-25
    - コメント 13-20
    - タイプ 13-2
    - ダウンロード可能 16-9
    - 着信 15-2
    - 発信 15-2
    - 標準、追加 13-11
    - ロギング 13-23
  - アクティブな IPSec VPN セッションの最大数、設定 25-4
  - アトリビュート
    - LDAP E-7
    - RADIUS E-26
    - ポリシー E-3
    - ユーザ名 26-62
  - アトリビュートと値のペア (AVP) 26-24
  - アドレス
    - 範囲、サブネット D-5
    - プール、設定 28-5
  - アプリケーション アクセス
    - IMAP クライアントで 30-54
    - クライアント アプリケーションの設定 30-53
    - クライアントでの設定 30-52
    - グループポリシーの WebVPN アトリビュート 26-54
    - 再度イネーブルにする 30-23
    - 正しい終了方法 30-22, 30-52
    - 電子メールの使用 30-54
    - 〜と hosts ファイル エラー 30-21
    - 〜と Web アクセス 30-54
    - 特権 30-52
    - 〜と電子メール プロキシ 30-54
    - ブラウザでのクッキーのイネーブル化 30-52
    - ユーザ名の webvpn アトリビュート 26-73
  - アプリケーション プロファイル カスタマイゼーション フレームワーク 30-34
  - アプリケーション 検査
    - セキュリティ レベルの要件 6-2
    - 設定 22-1, ?? - 22-60
    - 適用 22-5
  - 暗号マップ
    - ACL 24-22
    - インターフェイスへの適用 24-21, 29-9
    - エントリ 24-15
    - コンフィギュレーションのクリア 24-30
    - ダイナミック 24-27
    - ダイナミック、作成 28-8
    - ダイナミック暗号マップを使用するためのエントリの作成 28-9
    - 定義 24-15
    - ポリシー 24-15
    - 例 24-23
  - 暗号マップ内の許可 24-18
  - 暗号マップ内の拒否 24-18
- ## い
- イーサネット
    - Auto-MDI/MDIX 4-2
    - 速度 4-2
    - 二重通信 4-2
  - 一般アトリビュート、トンネルグループ 26-3
  - 一般パラメータ、トンネルグループ 26-3
  - インスタント メッセージ
    - 「IM」を参照
  - インターフェイス
    - ID 4-2
    - SFP 4-4
    - イネーブル化 4-2, 4-3
    - イネーブルになった状態 4-2, 4-4, 6-3
    - 監視対象インターフェイスの表示 11-47
    - 共有 3-7
    - グローバル アドレス 14-25
    - サブインターフェイス 4-5



- 速度 4-2
- ～での IPv6 の設定 9-3
- 二重通信 4-2
- ネーミング 6-4
- ファイバ 4-4
- フェールオーバーのモニタリング 11-17
- リモートアクセス用の設定 28-3
- インターフェイスの共有 3-7
- インターフェイスのネーミング 6-4

## え

- エコー応答、ICMP メッセージ D-18
- エンド ユーザ インターフェイス、WebVPN、定義 30-36

## お

- オープン ポート D-17
- 同じセキュリティ レベルの通信
  - NAT 14-13
- オブジェクト グループ
  - 削除 13-19
  - ネスト 13-17

## か

- 介入者攻撃 23-2
- 外部、定義 1-2
- 外部グループポリシー、設定 26-26
- カスケード ACL 24-18
- カスタマイゼーション
  - グループポリシーの WebVPN アトリビュート 26-49
  - ユーザ名の WebVPN アトリビュート 26-71
- 仮想クラスタ 25-8
  - IP アドレス 25-8
  - マスター 25-8
- 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 16-1
- 管理 IP アドレス、透過ファイアウォール 7-6
- 管理コンテキスト
  - 概要 1-7, 3-2
  - 変更 5-7

- 管理ディスタンス
  - 概要 8-3

## き

- 機能
  - WebVPN グループポリシー アトリビュート 26-48
  - ユーザ名の WebVPN アトリビュート 26-68
- 基本設定 7-1
- 疑問符
  - コマンド文字列 C-5
  - ヘルプ C-5
- キャッシング 30-32
- キュー
  - 制限 21-11
  - 遅延、低減 21-12
  - プライオリティ、設定 21-8, 21-11
- 「今日のお知らせ」バナー 33-19
- 共有 VLAN 3-7
- 拒否フロー、ロギング 13-25

## く

- クッキー、WebVPN 用にイネーブル化 30-5
- クライアント
  - VPN 3002 ハードウェア、強制クライアントアップ デート 25-5
  - Windows、クライアント アップデート通知 25-5
- クライアント アクセス規則、グループポリシー 26-45
- クライアント アップデート、実行 25-5
- クライアント ファイアウォール、グループポリシー 26-42
- クラスタ
  - 混在のシナリオ 25-10
  - ロードバランシング コンフィギュレーション 25-10
- クラスタ IP アドレス、ロードバランシング 25-8
- クラスタ、仮想 25-8
- クラッシュ ダンプ 36-12
- グループポリシー
  - IP Phone Bypass 26-39
  - IPSec over UDP アトリビュート 26-34
  - LEAP Bypass 26-40
  - VPN アトリビュート 26-28

VPN ハードウェア クライアント アトリビュート 26-38

webvpn アトリビュート 26-47

WINS サーバと DNS サーバ 26-27

アトリビュート 26-27

外部、設定 26-26

クライアント アクセス規則 26-45

スプリット トンネリング アトリビュート 26-35

スプリット トンネリング ドメイン 26-37

セキュリティ アトリビュート 26-31

設定 26-26

定義 26-2, 26-24

ドメイン アトリビュート 26-36

トンネリングされたパケットのデフォルト ドメイン名 26-36

内部、設定 26-27

ネットワーク拡張モード 26-41

ハードウェア クライアント ユーザ アイドル タイムアウト 26-39

バックアップ サーバ アトリビュート 26-41

ファイアウォール ポリシー 26-42

ユーザ認証 26-38

グループポリシー、セキュア ユニット認証 26-38

グループポリシー、デフォルト 26-24

グループポリシーの WebVPN アトリビュート

- deny-message 26-50
- HTML コンテンツ フィルタ 26-50
- keep-alive-ignore 26-55
- port-forward-name 26-54
- sso-server 26-55
- SVC 26-56
- url-list 26-53
- アプリケーション アクセス 26-54
- カスタマイゼーション 26-49
- 自動サインオン 26-51
- フィルタ 26-52
- ポート転送 26-54
- ホームページ 26-51

グローバル IPSec SA ライフタイム、変更 24-24

グローバル アドレス

- 指定 14-25
- 推奨事項 14-14

グローバル電子メールプロキシ アトリビュート 30-30

## け

### 継承

トンネルグループ 26-2

ユーザ名アトリビュート 26-62

### 検査エンジン

「アプリケーション検査」を参照

概要 22-2

## こ

公開キー暗号化 32-2

コマンド プロンプト C-3

### コマンド認可

概要 33-9

設定 33-8

コマンドラインの編集 C-4

コメント 13-20

アクセスリスト 13-20

コンフィギュレーション C-7

混在クラスタのシナリオ、ロードバランシング 25-10

### コンテキスト

「セキュリティ コンテキスト」を参照

リソースの使用 5-11

コンテキスト間の切り替え 5-7

コンテンツのリライトのディセーブル化 30-33

コンテンツ変換、WebVPN 30-32

### コンフィギュレーション

クリア 2-5

コメント C-7

コンテキスト ファイル 3-3

コンテキストの URL 5-4

テキスト ファイル 2-6

表示 2-5

保存 2-4

コンフィギュレーションのテスト 36-2

## さ

### 最大セッション

IPSec 25-15

最大接続時間、ユーザ名アトリビュート 26-64

サイトツーサイト VPN、冗長性 24-29

リブート、アクティブセッションの終了まで待機 24-10

- サブインターフェイス
    - 追加 4-5
  - サブコマンド モード プロンプト C-3
  - 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
    - 判別 D-3
    - ホストの数 D-3
- ## し
- 時間超過、ICMP メッセージ D-18
  - 時間範囲
    - アクセスリスト 13-21
  - システム コンフィギュレーション
    - 概要 1-7, 3-2
    - ネットワーク設定 3-3
  - 自動サインオン
    - グループポリシーの WebVPN アトリビュート 26-51
    - ユーザ名の webvpn アトリビュート 26-74
  - 照合
    - QoS 用のコマンド基準 21-7
  - 照合、証明書グループ 24-12
  - 状態リンク 11-6
  - 冗長性、サイトツーサイト VPN で、暗号マップを使用 24-29
  - 情報
    - 応答、ICMP メッセージ D-18
    - 要求、ICMP メッセージ D-18
  - 証明書グループ照合
    - 規則とポリシー、作成 24-12
    - 設定 24-12
  - 証明書登録プロトコル 32-7
  - 証明書認証
    - 電子メール プロキシ 30-31
  - 省略形のコマンド C-4
  - 初期メッセージ、グループポリシー 26-33
  - シリアル ケーブル
    - 「フェールオーバー」を参照
  - シングル サインオン
    - 「SSO」を参照
  - シングルサインオン
    - グループポリシーの WebVPN アトリビュート 26-55
    - ユーザ名の webvpn アトリビュート 26-75
  - シングルモード
    - イネーブル化 3-10
    - コンフィギュレーション 3-10
    - コンフィギュレーションのバックアップ 3-10
    - 復元 3-11
  - シンタックスの書式 C-4
  - 侵入防御コンフィギュレーション 19-2
- ## す
- スタートアップ コンフィギュレーション 3-3
  - スタティック ARP エントリ 23-3
  - スタティック NAT
    - 「NAT」を参照
  - スタティック PAT
    - 「NAT」を参照
  - スタティック ブリッジ エントリ 23-4
  - スタティック ルート
    - 概要 8-2
    - 設定 8-3
  - ステート情報 11-16
  - ステートフル インスペクション 1-4
  - ステートフル フェールオーバー
    - 概要 11-16
    - 状態リンク 11-6
    - ステート情報 11-16
    - 統計情報 11-42, 11-46
  - 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
  - スプリット トンネリング
    - グループポリシー 26-35
    - グループポリシー、ドメイン 26-37
- ## せ
- 生成
    - DSA キー 32-6
    - RSA キー 32-6
  - セカンダリ デバイス、仮想クラスター 25-8
  - セカンダリ装置、フェールオーバー 11-8
  - セキュア ユニット認証、グループポリシー 26-38

## セキュリティ

WebVPN 30-2, 30-6

## セキュリティ アソシエーション

「SA」も参照

クリア 24-30

セキュリティ アトリビュート、グループポリシー  
26-31

## セキュリティ アプライアンス

接続 2-2

リロード 36-7

## セキュリティ コンテキスト

VLAN の割り当て 5-2

概要 3-2

カスケード接続 3-8

～間の切り替え 5-7

管理 5-1

管理コンテキスト

概要 1-7, 3-2

変更 5-7

## コンフィギュレーション

URL、設定 5-4

URL、変更 5-8

ファイル 3-3

削除 5-6

サポートされていない機能 3-2

追加 5-2

ネストまたはカスケード接続 3-9

プロンプト C-3

分類子 3-3

マッピング インターフェイス名 5-3

マルチモード、イネーブル化 3-10

モニタリング 5-10

リロード 5-9

ログイン 3-9

## セキュリティ レベル

概要 6-2

## セッション管理パス 1-4

## 接続

ブロック 20-8

接続時間、最大、ユーザ名アトリビュート 26-64

## 接続の制限値

設定 20-5

## 設定モード

アクセス 2-3

プロンプト C-3

## そ

送信キュー リング制限 21-11

ソース クエンチ、ICMP メッセージ D-18

速度、設定 4-2

## た

代替アドレス、ICMP メッセージ D-18

ダイナミック NAT

「NAT」を参照

ダイナミック暗号マップ 24-27

「暗号マップ」も参照

作成 28-8

タイムスタンプ

応答、ICMP メッセージ D-18

要求、ICMP メッセージ D-18

ダウンロード可能なアクセスリスト

設定 16-9

ネットマスク表現の変換 16-13

## ち

遅延 21-2, 21-11

低減 21-12

遅延が問題になるトラフィック、プライオリティ  
21-8

着信アクセスリスト 15-2

## つ

ツールバー、フローティング、WebVPN 30-38

## て

低遅延キュー 21-3

適用 21-11

ディレクトリ階層検索 E-5

データ フロー

透過ファイアウォール 12-12

ルーテッド ファイアウォール 12-3

テール ドロップ 21-11

デジタル証明書

SSL 30-5

WebVPN 認証上の制限事項 30-5

WebVPN ユーザの認証 30-16

- デバッグ メッセージ 36-12
- デフォルト
  - DefaultL2Lgroup 26-2
  - DefaultRAGroup 26-2
  - キュー 21-3
  - トンネルグループ 24-13
- デフォルト グループポリシー 26-24
- デフォルト ドメイン名、グループポリシー 26-36
- デフォルト ルート
  - 概要 8-4
  - 設定 8-4
  - 等コスト ルートの定義 8-4
- デフォルトの LAN-to-LAN トンネルグループ 26-12
- デフォルトのグループポリシー 26-2
- デフォルトのトンネルグループ 26-3
- デフォルトのリモートアクセス トンネルグループ、設定 26-6
- デュアル IP スタック
  - 設定 9-8
- 電子メール
  - Outlook 接続の終了 30-31
  - WebVPN、設定 30-30
  - WebVPN 用の設定 30-30
  - プロキシ、WebVPN 30-30
- 電子メール プロキシ
  - 証明書認証 30-31
  - 〜と WebVPN 30-54
- と
- 透過ファイアウォール
  - ARP 検査
    - イネーブル化 23-3
    - 概要 23-2
    - スタティック エントリ 23-3
  - DHCP パケット、許可 13-7
  - HSRP 12-9
  - MAC アドレス タイムアウト 23-5
  - MAC ラーニング、ディセーブル化 23-5
  - NAT 12-11
  - VRRP 12-9
  - ガイドライン 12-10
  - 概要 12-9
  - 管理 IP アドレス 7-6
  - スタティック ブリッジ エントリ 23-4
  - データ フロー 12-12
  - パケットの処理 13-6
  - マルチキャスト トラフィック 12-9
  - 透過モード
    - ガイドライン 12-10
    - 概要 12-9
    - サポートされていない機能 12-11
  - 統計情報
    - QoS 21-19
    - QoS の表示 21-19
  - 同時ログイン
    - ユーザ名アトリビュート 26-63
  - 到達不能、ICMP メッセージ D-18
  - 登録局
    - 説明 32-3
  - 特権モード
    - アクセス 2-2
    - プロンプト C-3
  - 特権レベル、ユーザ名、設定 26-61
  - ドット付き 10 進数サブネット マスク D-3
  - ドメインアトリビュート、グループポリシー 26-36
  - ドメイン名 7-2
  - トラストポイント 32-3
  - トラップ、SNMP 35-2
  - トラフィック
    - QoS 用の分類 21-6
    - トラフィック クラス、QoS 21-4
    - トラフィック フロー
      - 透過ファイアウォール 12-12
      - ルーテッド ファイアウォール 12-3
  - トラフィック ポリシング
    - コンフィギュレーションの確認 21-18
  - トラフィック ポリシング コンフィギュレーションの確認 21-18
  - トラブルシューティング
    - H.323 22-33
    - H.323 RAS 22-34
    - SIP 22-51
  - トランスフォーム セット
    - 作成 28-6
    - 定義 24-14
  - トンネリング
    - 概要 24-1
  - トンネル
    - IPSec 24-14
    - トンネル エンドポイントとしてのセキュリティ アプライアンス 24-1

## トンネルグループ

- IPSec パラメータ 26-4
- LAN-to-LAN、設定 26-12
- webvpn アトリビュート 26-5
- 一般アトリビュート 26-3
- 一般パラメータ 26-3
- 継承 26-2
- 設定 26-6
- 定義 26-2, 26-3
- デフォルト 24-13, 26-2, 26-3
- デフォルト、リモートアクセス、設定 26-6
- デフォルトの LAN-to-LAN、設定 26-12
- リモートアクセス
  - 設定 28-7
  - リモートアクセス、設定 26-7
- トンネルグループの WebVPN 接続パラメータ 26-5
- トンネルグループの ISAKMP/IKE キープアライブの設定 26-4
- トンネルグループの一般接続パラメータ 26-3

## な

- 内部、定義 1-2
- 内部グループポリシー、設定 26-27

## に

- 二重通信、設定 4-2
- 認可
  - 概要 10-2
  - ネットワーク アクセス 16-7
- 認証
  - FTP 16-3
  - HTTP 16-2
  - Telnet 16-2
  - Web クライアント 16-4
  - 概要 10-2
  - デジタル証明書による WebVPN ユーザ 30-16
  - ネットワーク アクセス 16-2
- 認証局
  - 「CA」を参照
- 認証上の制限事項、WebVPN 30-5

## ね

- ネットワーク アクティビティ テスト 11-17

## ネットワーク アドレス変換

- 「NAT」を参照
- ネットワーク、重複 14-35
- ネットワーク拡張モード、グループポリシー 26-41

## は

- ハードウェア クライアント
  - グループポリシー アトリビュート 26-38
- パケット
  - キャプチャ 36-12
  - フロー、透過ファイアウォール 12-12
  - 分類子 3-3
- パケット フロー
  - ルーテッド ファイアウォール 12-3
- パケット取得 36-12
- パスワード
  - WebVPN 30-48
  - 回復 36-8
  - 変更 7-1
  - ユーザ名、設定 26-61
- バックアップ サーバアトリビュート、グループポリシー 26-41
- バックアップ デバイス
  - ロードバランシング 25-8
- 発信アクセスリスト 15-2
- バナー メッセージ、グループポリシー 26-33
- ハブアンドスポーク 24-21
- パフォーマンス、WebVPN 用の最適化 30-32
- パラメータの問題、ICMP メッセージ D-18

## ひ

- ピア
  - ISAKMP、識別方式の決定 24-8
  - 接続解除の前に警告 24-11
- ビット サブネット マスク D-3
- 非同期ルーティングのサポート 11-37
- 表示
  - RMS 34-14
- 表示画面のページ設定 C-7

## ふ

- ファースト パス 1-5

- ファイアウォール ポリシー、グループポリシー 26-42
- ファイアウォール モード
  - 概要 12-1
  - 設定 2-3
- ファイバ インターフェイス 4-4
- フィルタ (ACL)
  - グループポリシーの WebVPN アトリビュート 26-52
  - ユーザ名の webvpn アトリビュート 26-72
- フィルタリング
  - ActiveX 17-2
  - show コマンド出力 C-6
  - URL 17-5
  - 概要 17-1
  - サポートされるサーバ 17-5
  - セキュリティ レベルの要件 6-2
- プール
  - アドレス
    - グローバル NAT 14-25
- プール、アドレス
  - DHCP 8-28
- フェールオーバー
  - Active/Active、「Active/Active フェールオーバー」を参照
  - Active/Active、設定 11-27
  - Active/Standby、「Active/Standby フェールオーバー」を参照
  - Active/Standby 設定 11-19
  - MAC アドレス 11-8
  - SNMP syslog トラップ 11-51
  - イーサネット フェールオーバー ケーブル 11-4
  - インターフェイス テスト 11-17
  - インターフェイスのヘルス 11-17
  - インターフェイスのモニタリング 11-17
  - 概要 11-2
  - 強制 11-49
  - 故障したグループの復元 11-50
  - 故障した装置の復元 11-50
  - コマンドの表示 11-48
  - コンテキスト 11-7
  - コンフィギュレーション ファイル
    - 端末メッセージ 11-8
  - コンフィギュレーションの確認 11-39
  - システム メッセージ 11-50
  - システム要件 11-2
  - 状態リンク 11-6
  - シリアル ケーブル 11-5
  - 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」を参照
  - 制御 11-49
  - セカンダリ装置 11-8
  - 設定 11-19
  - 装置ヘルス 11-17
  - ソフトウェア バージョン 11-3
  - タイプの選択 11-15
  - ディセーブル化 11-49
  - テスト 11-48
  - デバッグ メッセージ 11-50
  - ネットワーク テスト 11-17
  - フェールオーバー リンク 11-4
  - フェールオーバー通信の暗号化 11-38
  - プライマリ装置 11-8
  - ヘルスのモニタリング 11-17
  - モニタリング 11-17, 11-49
  - ライセンス 11-3
  - リンクの通信 11-4
  - 例
    - Active/ Active LAN ベースのフェールオーバー 11-55
    - Active/Standby LAN ベースのフェールオーバー 11-53
    - Active/Standby ケーブルベースのフェールオーバー 11-51
- プライオリティキュー
  - インターフェイスのコンフィギュレーション、表示 21-18
  - サイズの変更 21-12
  - 設定 21-11
  - 遅延が問題になるトラフィックの 21-8
  - プライオリティキューのサイズの変更 21-12
- プライベート ネットワーク D-2
- プライマリ装置、フェールオーバー
  - 概要 11-8
- フラグメンテーション ポリシー、IPSec 24-9
- フラグメント サイズ
  - 設定 20-7
- ブリッジ
  - エントリ タイムアウト 23-5
  - テーブル
    - 「MAC アドレス テーブル」を参照
- ブロードキャスト Ping テスト 11-18
- プロキシ
  - 「電子メール プロキシ」を参照

## プロキシ サーバ

SIP と～ 22-49

プロキシ バイパス 30-33

プロトコル番号とリテラル値 D-13

## プロンプト

more C-7

コマンド C-3

分類ポリシー、トラフィック 21-4

## へ

ヘアピニング 24-21

ヘルプ、コマンドライン C-5

変換エラー、ICMP メッセージ D-18

## ほ

## ポート

装置でオープン D-17

リダイレクション、NAT 14-37

## ポート転送

アプレットの自動ダウンロード 30-21

クライアント アプリケーションの設定 30-53

## ホームページ

グループポリシーの WebVPN アトリビュート  
26-51

ユーザ名の WebVPN アトリビュート 26-70

ホストのサブネット マスク D-3

## ホスト名

設定 7-2

## ポリシー NAT

概要 14-10

スタティック PAT、設定 14-28

スタティック、設定 14-26

ダイナミック、設定 14-24

ポリシー、QoS 21-1

## ポリシーマップ

QoS での使用 21-10

QoS 用の定義 21-8

## ポリシング

QoS 21-3

厳密な 21-9

コンフィギュレーションの確認 21-18

トンネル内のフロー 21-7

## ま

マッピング インターフェイス名 5-3

マルチキャスト トラフィック 12-9

マルチコンテキスト モード 5-1

マルチモード、イネーブル化 3-10

## む

無効になった証明書 32-3

## も

## モード

コンテキスト 3-10

## モニタリング

OSPF 8-17

SNMP 35-1

フェールオーバー 11-17

モバイル リダイレクション、ICMP メッセージ D-18

## ゆ

## ユーザ

定義 26-2

特定の設定 26-61

リモートアクセス

追加 28-6

ユーザ アクセス、制限 26-66

## ユーザ モード

プロンプト C-3

ユーザ認証、グループポリシー 26-38

## ユーザ名

WebVPN 30-48

## ユーザ名アトリビュート

group-lock 26-66

password-storage 26-66

vpn-filter 26-64

vpn-framed-ip-address 26-65

vpn-idle タイムアウト 26-63

vpn-session-timeout 26-64

vpn-tunnel-protocol 26-65

アクセス時間 26-62

継承 26-62

設定 26-60, 26-62

同時ログイン 26-63



- 特権レベル、設定 26-61
- パスワード、設定 26-61
- ユーザ名コンフィギュレーション、表示 26-60
- ユーザ名の WebVPN アトリビュート
  - html-content-filter 26-69
  - カスタマイゼーション 26-71
  - 機能 26-68
  - ホームページ 26-70
- ユーザ名の webvpn アトリビュート
  - port-forward 26-73
  - port-forward-name 26-73
  - sso-server 26-75
  - SVC 26-75
  - url-list 26-72
  - キープアライブ無視 26-74
  - 拒否メッセージ 26-71
  - 自動サインオン 26-74
  - フィルタ (ACL) 26-72
- ユーザ名の webvpn アトリビュートを無視する最大オブジェクトサイズ 26-74
- ユーザ名の WebVPN モード 26-66

## ら

- ライセンス
  - FO 11-3
  - FO\_AA 11-3
  - UR 11-3
  - 管理 34-2

## り

- リソースの使用 5-11
  - リソース タイプ 5-12
- リダイレクト、ICMP メッセージ D-18
- リモートアクセス
  - IPSec トンネルグループ、設定 26-7
  - VPN、設定 28-1
  - コンフィギュレーションの概要 28-2
  - 制限 26-66
  - トンネルグループ、デフォルトの設定 26-6
  - ユーザ
    - 追加 28-6
- リライト、ディセーブル化 30-33
- リロード
  - コンテキスト 5-9

- リンク アップ/ダウン テスト 11-17

## る

- ルータ
  - アドバタイズメント、ICMP メッセージ D-18
  - 送信要求、ICMP メッセージ D-18
- ルーティング
  - OSPF 8-18
  - RIP 8-19
  - その他のプロトコル 13-6
- ルーテッド モード
  - 設定 2-3
- ルート
  - IPv6 スタティックへの設定 9-5
  - IPv6 デフォルトへの設定 9-5
  - スタティック ルートの設定 8-3
  - スタティックについて 8-2
  - デフォルト ルートの設定 8-4
  - デフォルトについて 8-4

## 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
- レート制限 21-9

## ろ

- ローカル ユーザ データベース
  - サポート 10-13
  - 設定 10-15
  - ユーザの追加 10-15
  - ログイン 33-8
- ロードバランシング
  - 概念 25-8
  - 混在クラスタのシナリオ 25-10
  - 実装 25-9
  - 前提条件 25-9
  - 適格なクライアント 25-9
  - 適格なプラットフォーム 25-9
  - プラットフォーム 25-9

クラスタ コンフィギュレーション      25-10  
ロギング  
    アクセスリスト      13-23  
ログイン  
    FTP      16-3  
    ローカル ユーザ      33-8  
ログイン ウィンドウ、WebVPN ユーザ用にカスタマイズ      26-22  
ログイン、同時、ユーザ名アトリビュート      26-63  
ログイン バナー  
    設定      33-19  
ロックアウト  
    回復      33-17