CHAPTER 43

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

ここでは、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 コンテキストに対して接続テストを行う手順について説明します。セキュリティ アプライアンスのインターフェイスに ping を実行する手順、および 1 つのインターフェイス上のホストから他のインターフェイス上のホストに ping を実行する手順を次に示します。

トラブルシューティングでは、ping およびデバッグに関するメッセージだけをイネーブルにすることを推奨します。セキュリティ アプライアンス のテストが終了したら、「テスト設定のディセーブル化」（P.43-6）の手順に従ってください。

この項では、次のトピックについて取り上げます。

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

デバッグ メッセージとシステム メッセージは、ping に失敗した原因を特定する場合に役立ちます。セキュリティ アプライアンス には、セキュリティ アプライアンス のインターフェイスへの ping に関する ICMP デバッグ メッセージだけが表示されます。セキュリティ アプライアンス 経由で他のホストに宛てた ping に関するメッセージは表示されません。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　次のコマンドを入力して、セキュリティ アプライアンス のインターフェイスへの ping に関する ICMP パケット情報を表示します。

```
hostname(config)# debug icmp trace
```

ステップ 2　次のコマンドを入力して、Telnet または SSH セッションにシステム メッセージが送信されるように設定します。

```
hostname(config)# logging monitor debug
```

または、**logging buffer debug** コマンドを使用してメッセージをバッファに送信し、そのあとで **show logging** コマンドを使用して表示することもできます。

ステップ 3　次のコマンドを入力して、Telnet または SSH セッションにシステム メッセージを送信します。

```
hostname(config)# terminal monitor
```

ステップ 4　次のコマンドを入力して、システム メッセージをイネーブルにします。

```
hostname(config)# logging 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
```

この例には、ICMP パケット長（32 バイト）、ICMP パケット ID（1）、および ICMP シーケンス番号（ICMP シーケンス番号は 0 から始まり、要求が送信されるごとに増分されます）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 のインターフェイスが稼働中であり、セキュリティ アプライアンス と接続先ルータが正しくルーティングされているかどうかをテストするには、セキュリティ アプライアンス のインターフェイスに ping を実行します。

（注）　セキュリティ保護のため、セキュリティ アプライアンスは遠端インターフェイスの ping、つまり内部ネットワークから外部インターフェイスの IP アドレスへの ping をサポートしません。

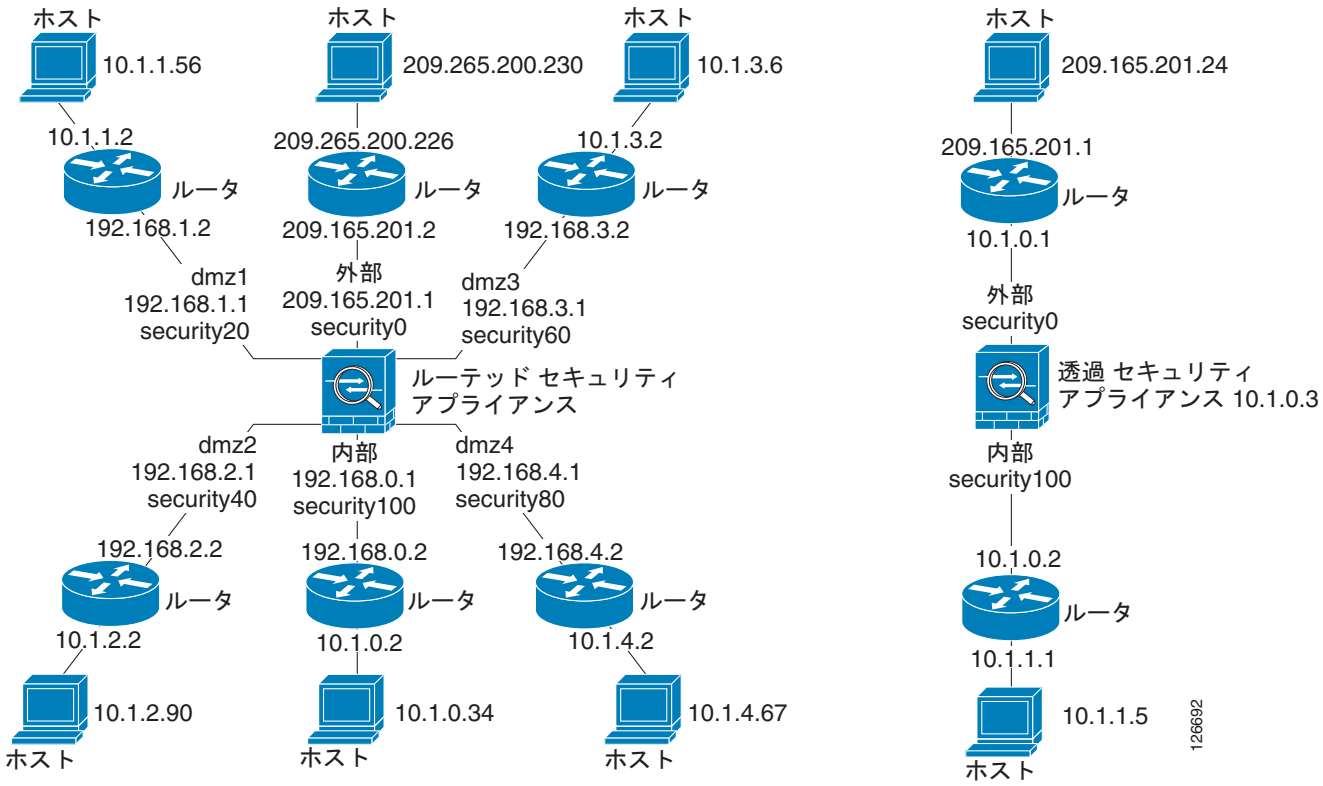
セキュリティ アプライアンス インターフェイスを ping するには、次の手順を実行します。

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 アドレスを明記したシングルモードの セキュリティ アプライアンス またはセキュリティ コンテキストの接続図を作成します。

（注）　この手順では IP アドレスを使用しますが、**ping** コマンドでは、DNS 名および **name** コマンドを使用してローカル IP アドレスに割り当てられた名前もサポートされます。

この接続図には、直接接続されたルータ、および セキュリティ アプライアンス への ping の実行元となるルータの反対側のホストも明記する必要があります。この情報は、ここで説明する手順、および「セキュリティ アプライアンスによる ping」（P.43-4）の手順で使用します。次に例を示します。

図 43-1　　インターフェイス、ルータ、およびホストを明記したネットワーク接続図



ステップ 2　*直接接続されたルータ*から セキュリティ アプライアンス の各インターフェイスに ping を実行します。トランスペアレント 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。

ping に失敗した場合は、セキュリティ アプライアンス のインターフェイスがアクティブでないか、インターフェイスが正しく設定されていないか、または セキュリティ アプライアンス とルータ間のスイッチが停止している可能性があります（図 43-2 を参照）。この場合は、パケットが到達しないため、セキュリティ アプライアンス 上にデバッグ メッセージもシステム メッセージも表示されません。

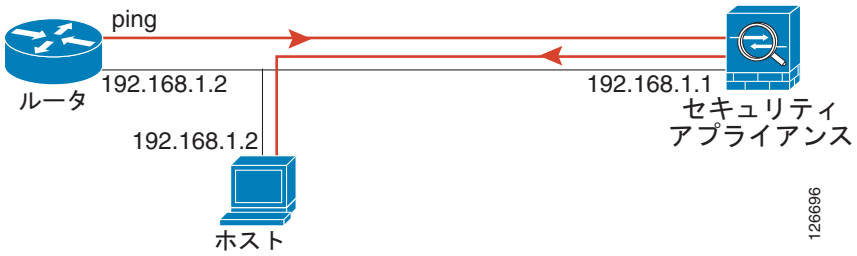
図 43-2　　セキュリティ アプライアンス インターフェイスでの ping の失敗

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 から応答が返されると、次のようなデバッグ メッセージが表示されます。

```
ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
```

ping 応答がルータに返らない場合、スイッチ ループが発生しているか、または IP アドレスが重複している可能性があります（図 43-3 を参照）。

図 43-3　IP アドレッシングの問題による ping の失敗

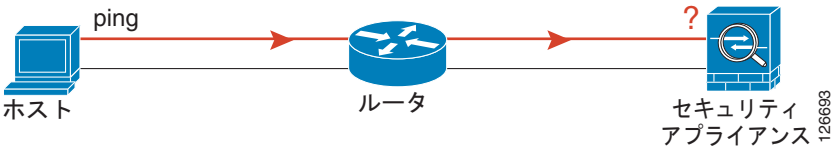


ステップ 3　リモート ホストから各セキュリティ アプライアンス インターフェイスを ping します。トランスペアレント モードでは、管理 IP アドレスを ping します。

このテストでは、直接接続されたルータがホストと セキュリティ アプライアンス 間の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 からホストに返されるパケットが正しくルーティングされていることを確認します。

ping に失敗した場合は、中継ルータを経由したホストまでのルートが セキュリティ アプライアンス に正しく設定されていない可能性があります（図 43-4 を参照）。この場合は、ping に成功したことを示すデバッグ メッセージが表示されますが、システム メッセージ 110001 でルーティング障害が発生していることが示されます。

図 43-4　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 のインターフェイスへの ping に成功したら、セキュリティ アプライアンス 経由でトラフィックを正しく転送できるかどうかを確認する必要があります。ルーテッド モードでは、このテストによって、NAT が設定されている場合に正しく実行されるかどうかを確認できます。NAT を使用しないトランスペアレント モードの場合は、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をこのテストで確認します。トランスペアレント モードで ping に失敗した場合は、Cisco TAC に連絡してください。

異なるインターフェイス上のホスト間で ping 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、任意の送信元ホストからの ICMP を許可するアクセス リストを追加します。

```
hostname(config)# access-list ICMPACL extended permit icmp any any
```

デフォルトでは、ホストが低セキュリティ 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　次のコマンドを入力して、各送信元インターフェイスにアクセス リストを割り当てます。

```
hostname(config)# access-group ICMPACL in interface interface_name
```

各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　次のコマンドを入力して、ICMP 応答が送信元ホストに戻されるように、ICMP インスペクション エンジンをイネーブルにします。

```
hostname(config)# class-map ICMP-CLASS
hostname(config-cmap)# match access-list ICMPACL
hostname(config-cmap)# policy-map ICMP-POLICY
hostname(config-pmap)# class ICMP-CLASS
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# service-policy ICMP-POLICY global
```

または、セキュリティ アプライアンス 経由で ICMP トラフィックを返すことを許可するために、ICMPACL アクセス リストを宛先インターフェイスに適用することもできます。

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 に成功すると、ルーテッド モードのアドレス変換を確認するシステム メッセージ（305009 または 305011）と ICMP 接続が確立されたことを示すメッセージ（302020）が表示されます。**show xlate** コマンドと **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。

トランスペアレント 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 が失敗することがあります（図 43-5 を参照）。この状況は、NAT 制御をイネーブルにしている場合によく発生します。この場合は、NAT 変換に失敗したことを示すシステム メッセージ（305005 または 305006）が表示されます。外部ホストから内部ホストに ping を実行した場合に、スタティック変換（NAT 制御に必要）が設定されていないと、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 には、セキュリティ アプライアンス のインターフェイスへの ping に関する ICMP デバッグ メッセージだけが表示されます。セキュリティ アプライアンス 経由で他のホストに宛てた ping に関するメッセージは表示されません。

図 43-5　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

テスト設定のディセーブル化

テストが完了したら、セキュリティ アプライアンス 宛ての ICMP と FWSM 経由の ICMP を許可し、デバッグ メッセージを出力するテスト設定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 メッセージを生成すると、セキュリティ アプライアンス のパフォーマンスが遅くなります。

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　次のコマンドを入力して、ICMP デバッグ メッセージをディセーブルにします。

```
hostname(config)# no debug icmp trace
```

ステップ 2　必要に応じて、次のコマンドを入力して、ロギングをディセーブルにします。

```
hostname(config)# no logging on
```

ステップ 3　次のコマンドを入力して、ICMPACL アクセス リストを削除し、関連する **access-group** コマンドも削除します。

```
hostname(config)# no access-list ICMPACL
```

ステップ 4　（任意）ICMP インスペクション エンジンをディセーブルにする場合には、次のコマンドを入力します。

```
hostname(config)# no service-policy ICMP-POLICY
```

traceroute

パケットのルートは、トレースルート機能を使用してトレースできます。この機能には、**traceroute** コマンドでアクセスできます。トレースルートは、無効なポート上の宛先に UDP パケットを送信することで機能します。ポートが有効ではないため、宛先までの間にあるルータは ICMP Time Exceeded Message を表示して応答し、セキュリティ アプライアンスにエラーを報告します。

パケット トレーサ

パケットのキャプチャとトレースルート機能に加えて、パケット トレーサ ツールを使用して意図したとおりに動作しているかどうかを確認するために、セキュリティ アプライアンスを通過するパケットのライフ スパンをトレースすることができます。パケット トレーサ ツールでは次のことができます。

- 実働ネットワークにおけるすべてのパケット ドロップをデバッグします。
- コンフィギュレーションが意図したとおりに機能しているかを確認する。
- パケットに適用可能なすべてのルールと、ルールの追加に使用した CLI ラインを表示します。
- データ パス内でのパケット変化を時系列で表示する。
- データ パスにトレーサ パケットを挿入する。

packet-tracer コマンドは、パケットに関する詳細情報、およびセキュリティ アプライアンスによるパケットの処理方法を提供します。コンフィギュレーションからのコマンドでパケットがドロップしなかった場合、**packet-tracer** コマンドは、原因に関する情報を判読しやすい方法で提供します。たとえば、無効なヘッダー検証が原因でパケットがドロップされた場合、「packet dropped due to bad ip header (reason)」というメッセージが表示されます。

（注）　**packet-tracer** コマンドは、送信元 IP、宛先 IP、送信元ポート、宛先ポート、およびプロトコルの 5 つのタプル情報に基づいてパケットを生成できます。パケット トレーサでは、パケットのデータ部分に入力せず、その結果、エンジンのチェックの一部は適用されません。パケット トレーサは、インスペクション チェックに合格しなかったからではなく、インスペクション チェックをテストするための十分なデータがないために、パケットがドロップされることを示します。たとえば、DNS インスペクションがイネーブルの場合、パケット トレーサは不適切な DNS トラフィックのドロップを示します。

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 設定が原因でロック アウトが発生した場合の回復方法について説明します。高いセキュリティ保護のために、パスワード回復をディセーブルにすることもできます。この項では、次のトピックについて取り上げます。

- 「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.43-7）
- 「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.43-8）
- 「パスワード回復のディセーブル化」（P.43-10）
- 「SSM ハードウェア モジュールのパスワードのリセット」（P.43-10）

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

パスワードを回復するには、次の手順を実行します。

ステップ 1　「コマンドライン インターフェイスへのアクセス」（P.2-5）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　起動メッセージ中、ROMMON を開始するように促されたときに、Escape キーを押します。

ステップ 4　リロード時、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が尋ねられます。

```
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　「disable system configuration?」値を除くすべての設定のデフォルト値を受け入れます。プロンプトで **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 モードを開始します。

```
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。

パスワードは空白です。

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 モードを開始します。

```
hostname# configure terminal
```

ステップ 13　必要に応じて、次のコマンドを入力して、コンフィギュレーションの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
```

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、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、login password、enable password、および **aaa authentication console** コマンドが削除されます。デフォルトのパスワードでログインできるようにこれらのコマンドを削除するは、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 の『Password Recovery Procedure for the PIX』のマニュアル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　「コマンドライン インターフェイスへのアクセス」（P.2-5）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?」プロンプトに対して、**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。

次に、外部インターフェイス上の TFTP サーバでの PIX パスワード回復の例を示します。

```
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 アプライアンスでは、**no service password-recovery** コマンドを使用すると、ユーザが ROMMON を開始することを防止でき、コンフィギュレーションも変更されないままとすることができます。ユーザが ROMMON を開始すると、ユーザは、セキュリティ アプライアンスによって、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られます。ユーザは、最初に消去を実行しないと、ROMMON を開始できません。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。パスワードの回復は ROMMON の使用と既存のコンフィギュレーションを維持することに依存しているため、フラッシュ ファイル システムを消去することによってパスワードを回復できなくなります。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。この場合に、システムを動作ステートに回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（使用可能な場合）をロードします。**service password-recovery** コマンドは、コンフィギュレーション ファイルに情報提供の目的でのみ表示されます。CLI プロンプトでこのコマンドを入力すると、設定は NVRAM に保存されます。設定を変更する唯一の方法は、CLI プロンプトでコマンドを入力することです。このコマンドの異なるバージョンで新規コンフィギュレーションをロードしても、設定は変更されません。セキュリティ アプライアンスが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の回復をディセーブルにすると（パスワードの回復準備のために）、セキュリティ アプライアンスによって設定が変更され、通常どおりにスタートアップ コンフィギュレーションが起動されます。フェールオーバーを使用し、スタートアップ コンフィギュレーションを無視するようにスタンバイ装置が設定されている場合は、**no service password recovery** コマンドでスタンバイ装置に複製したときにコンフィギュレーション レジスタに同じ変更が加えられます。

PIX 500 シリーズ セキュリティ アプライアンスでは、**no service password-recovery** コマンドを使用すると、ユーザは、PIX パスワード ツールによって、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られます。ユーザは、最初に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。パスワードの回復は既存のコンフィギュレーションを維持することに依存しているため、フラッシュ ファイル システムを消去することによってパスワードを回復できなくなります。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。この場合に、システムを動作ステートに回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（使用可能な場合）をロードします。

SSM ハードウェア モジュールのパスワードのリセット

SSM ハードウェア モジュールのパスワードをデフォルトの「cisco」にリセットするには、次の手順を実行します。

ステップ 1　SSM ハードウェア モジュールがアップ状態にあり、パスワードのリセットがサポートされていることを確認します。

ステップ 2　次のコマンドを入力します。

```
hostname (config)# hw-module module 1 password-reset
```

ここで、*1* は、SSM ハードウェア モジュール上の指定したスロット番号です。

（注）　AIP SSM で、このコマンドを入力するとハードウェア モジュールがリブートされます。モジュールはリブートが終了するまでオフラインです。モジュールのステータスをモニタするには、**show module** コマンドを入力します。AIP SSM では、バージョン 6.0 以降でこのコマンドがサポートされています。

CSC SSM で、このコマンドを入力すると、パスワードがリセットされた後でハードウェア モジュールの Web サービスがリセットされます。ASDM への接続が失われる、またはハードウェア モジュールからログ アウトされることがあります。CSC SSM では、2006 年 11 月の最新バージョン 6.1 でこのコマンドがサポートされています。

```
Reset the password on module in slot 1? [confirm]
```

ステップ 3　確認のために **y** を入力します。

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 から支援を受ける際に役立つ他のトラブルシューティング ツールが用意されています。

- 「デバッグ メッセージの表示」（P.43-11）
- 「パケットのキャプチャ」（P.43-12）
- 「クラッシュ ダンプの表示」（P.43-12）

デバッグ メッセージの表示

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、debug コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。デバッグ メッセージをイネーブルにする場合は、『*Cisco Security Appliance Command Reference*』の **debug** コマンドの説明を参照してください。

パケットのキャプチャ

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モニタ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。

症状　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。

症状　セキュリティ アプライアンス のインターフェイスに Telnet も SSH（セキュア シェル）も接続できない。

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 をイネーブルにしていません。

推奨処置　「Telnet アクセスの許可」（P.40-1）または「SSH アクセスの許可」（P.40-2）の説明に従って セキュリティ アプライアンス への Telnet 接続または SSH 接続をイネーブルにします。

症状　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ています。

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。

症状　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 経由で ping を実行できない。

考えられる原因　ICMP インスペクション エンジン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は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 インスペクション エンジンをイネーブルにします。

症状　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　同じセキュリティ レベルのインターフェイス間のトラフィックを許可する機能が、イネーブルに設定されていません。

推奨処置　「同一セキュリティ レベルにあるインターフェイス間の通信の許可」（P.7-6）の説明に従って、この機能をイネーブルにします。