



テストとトラブルシューティング

この章では、ASA のトラブルシューティング方法と基本接続のテスト方法について説明します。

- [イネーブルパスワードと Telnet パスワードの回復](#) (1 ページ)
- [Packet Capture Wizard を使用したキャプチャの設定と実行](#) (5 ページ)
- [CPU 使用率とレポート](#) (13 ページ)
- [設定のテスト](#) (19 ページ)
- [パフォーマンスとシステム リソースのモニタリング](#) (28 ページ)
- [接続のモニタリング](#) (31 ページ)
- [ASA Virtual での同意トークンを使用したルートシェルアクセスのサポート](#) (31 ページ)
- [テストおよびトラブルシューティングの履歴](#) (33 ページ)

イネーブルパスワードと Telnet パスワードの回復

ASA 仮想 および ISA 3000 モデルでは、イネーブルパスワードまたは Telnet パスワードを忘れた場合に回復できます。CLI を使用してタスクを実行する必要があります。



- (注) その他のプラットフォームでは、パスワードを忘れた場合に回復することはできません。工場出荷時のデフォルト設定に戻すことは可能で、パスワードをデフォルトにリセットできます。Firepower 4100/9300 の場合は、『[FXOS configuration guide](#)』を参照してください。他のモデルについては、『[FXOS troubleshooting guide](#)』を参照してください。
-

ISA 3000 でのパスワードの回復

ISA 3000 のパスワードの回復には、次の手順を実行します。

手順

- ステップ1** ASA のコンソール ポートに接続します。
- ステップ2** ASA の電源を切ってから、再び電源をオンにします。
- ステップ3** スタートアップ後、ROMMONモードに入るようにプロンプトが表示されたら、**Escape** キーを押します。
- ステップ4** コンフィギュレーション レジスタ値をアップデートするには、次のコマンドを入力します。

```
rommon #1> confreg 0x41
```

```
You must reset or power cycle for new config to take effect
```

ASA で現在のコンフィギュレーションレジスタ値と構成オプションのリストが表示されます。後で回復できるように、現在のコンフィギュレーションのレジスタ値を記録します。

```
Configuration Register: 0x00000041
```

```
Configuration Summary
```

```
[ 0 ] password recovery  
[ 1 ] display break prompt  
[ 2 ] ignore system configuration  
[ 3 ] auto-boot image in disks  
[ 4 ] console baud: 9600  
boot: ..... auto-boot index 1 image in disks
```

- ステップ5** 次のコマンドを入力して、ASA をリロードします。

```
rommon #2> boot
```

```
Launching BootLoader...
```

```
Boot configuration file contains 1 entry.
```

```
Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

ASA は、スタートアップコンフィギュレーションの代わりにデフォルトコンフィギュレーションをロードします。

- ステップ6** 次のコマンドを入力して、特権 EXEC モードにアクセスします。

```
ciscoasa# enable
```

- ステップ7** パスワードの入力を求められたら、**Enter** キーを押します。
パスワードは空白です。

- ステップ8** 次のコマンドを入力して、スタートアップコンフィギュレーションをロードします。

```
ciscoasa# copy startup-config running-config
```

ステップ 9 次のコマンドを入力して、グローバル コンフィギュレーション モードにアクセスします。

```
ciscoasa# configure terminal
```

ステップ 10 次のコマンドを入力して、デフォルト コンフィギュレーションで必要に応じてパスワードを変更します。

```
ciscoasa(config)# password password  
ciscoasa(config)# enable password password  
ciscoasa(config)# username name password password
```

ステップ 11 次のコマンドを入力して、デフォルト コンフィギュレーションをロードします。

```
ciscoasa(config)# no config-register
```

デフォルト コンフィギュレーションのレジスタ値は 0x1 です。コンフィギュレーション レジスタの詳細については、[コマンドリファレンス](#)を参照してください。

ステップ 12 次のコマンドを入力して、新しいパスワードをスタートアップコンフィギュレーションに保存します。

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

ASA 仮想 のパスワードまたはイメージの回復

ASA 仮想 のパスワードまたはイメージを回復するには、次の手順を実行します。

手順

ステップ 1 実行コンフィギュレーションを ASA 仮想 のバックアップ ファイルにコピーします。

```
copy running-config filename
```

例 :

```
ciscoasa# copy running-config backup.cfg
```

ステップ 2 ASA 仮想 を再起動します。

```
reload
```

ステップ 3 [GNUGRUB] メニューから、下矢印を押し、**コンフィギュレーションをロードしないオプション**で <filename> を選択し、Enter キーを押します。ファイル名は、ASA 仮想 のデフォルトのブートイメージのファイル名です。デフォルトのブートイメージは、**fallback** コマンドによっ

て自動的にブートされることはありません。その後、選択したブートイメージをロードします。

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

例：

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

ステップ4 実行コンフィギュレーションにバックアップ コンフィギュレーション ファイルをコピーします。

copy filename running-config

例：

```
ciscoasa (config)# copy backup.cfg running-config
```

ステップ5 パスワードのリセット。

enable password password

例：

```
ciscoasa(config)# enable password cisco123
```

ステップ6 新しい設定を保存します。

write memory

例：

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

ISA 3000 ハードウェアのパスワード回復の無効化



(注) ASA 仮想、Cisco Secure Firewall モデルでパスワード回復をディセーブルにすることはできません。

権限のないユーザーがパスワード回復メカニズムを使用して ASA を危険にさらすことがないように、パスワード回復をディセーブルにするには、次の手順を実行します。

始める前に

ASA で、**no service password-recovery** コマンドを使用すると ROMMON モードに入って、コンフィギュレーションの変更を防ぐことができます。ROMMON モードに入ると、ASA では、すべてのフラッシュ ファイル システムの消去を求めるプロンプトが表示されます。最初に消去を実行しないと、ROMMON モードを開始できません。フラッシュ ファイル システムを消去しない場合、ASA はリロードされます。パスワード回復は ROMMON モードの使用と既存のコンフィギュレーションの保持に依存しているため、この消去によって、パスワードの回復ができなくなります。ただし、パスワードを回復できなくすることで、不正なユーザーがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合、システムを動作可能な状態に回復するには、新しいイメージとバックアップコンフィギュレーション ファイル（入手できる場合）をロードします。

service password-recovery コマンドは、コンフィギュレーション ファイルに通知用としてのみ表示されます。CLI プロンプトに対してコマンドを入力すると、設定は NVRAM に保存されます。設定を変更する唯一の方法は、CLI プロンプトでコマンドを入力することです。このコマンドの異なるバージョンで新規コンフィギュレーションをロードしても、設定は変更されません。（パスワード回復の準備段階で）スタートアップ時にスタートアップ コンフィギュレーションを無視するよう ASA が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、通常どおりスタートアップ コンフィギュレーションをロードするように ASA の設定が変更されます。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スタンバイ装置が設定されている場合は、**no service password-recovery** コマンドでスタンバイ装置に複製したときに、コンフィギュレーション レジスタに同じ変更が加えられます。

手順

パスワード回復をディセーブルにします。

no service password-recovery

例：

```
ciscoasa (config)# no service password-recovery
```

Packet Capture Wizard を使用したキャプチャの設定と実行

Packet Capture Wizard を使用して、エラーのトラブルシューティングを行う場合のキャプチャを設定および実行できます。キャプチャでは ACL を使用して、キャプチャされるトラフィックのタイプを、送信元と宛先のアドレスとポート、および1つ以上のインターフェイスで制限できます。このウィザードは、入出力インターフェイスのそれぞれでキャプチャを1回実行します。キャプチャしたパケットは、PC に保存してパケット アナライザで分析できます。



(注) このツールは、クライアントレス SSL VPN キャプチャをサポートしていません。

キャプチャを設定および実行するには、次の手順を実行します。

手順

ステップ 1 [Wizards] > [Packet Capture Wizard] の順に選択します。

[Overview of Packet Capture] 画面には、ウィザードを完了するまでに行うタスクの一覧が表示されます。これらのタスクには、以下が含まれます。

- 入力インターフェイスの選択。
- 出力インターフェイスの選択。
- バッファ パラメータの設定。
- キャプチャの実行。
- (オプション) キャプチャ データの PC への保存。

ステップ 2 [Next] をクリックします。

クラスタ環境では、[Cluster Option] 画面が表示されます。ステップ 3 に進みます。

非クラスタ環境では、[Ingress Traffic Selector] 画面が表示されます。ステップ 4 に進みます。

ステップ 3 [Cluster Option] 画面で、キャプチャの実行対象として [This device only] または [The whole cluster] のいずれかのオプションを選択します。[Next] をクリックして [Ingress Selector] 画面を表示します。

ステップ 4 インターフェイスでパケットをキャプチャするには、[Select Interface] オプション ボタンをクリックします。

クラスタリング環境では、クラスタ コントロール プレーン パケットのみをキャプチャするには、[CP-Cluster] チェックボックスをオンにします。

ステップ 5 ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。

ステップ 6 [Packet Match Criteria] 領域で、次のいずれかを実行します。

- パケットの照合に使用する ACL を指定するには、[アクセスリストの選択 (Select access list)] オプション ボタンをクリックし、[ACL の選択 (Select ACL)] ドロップダウンリストから ACL を選択します。以前設定した ACL を現在のドロップダウンリストに追加するには、[Manage] をクリックして [ACL Manager] ペインを表示します。ACL を選択して [OK] をクリックします。

スイッチパケットキャプチャを有効にすると、アクセスリストオプションは無効になります。詳細については、[入力トラフィック セレクタ \(10 ページ\)](#) を参照してください。

- **[Specify Packet Parameters]** オプション ボタンをクリックして、パケットパラメータを指定します。

a) **[ICMP Capture]** ドロップダウンリストで次のいずれかを実行します。

(注)

[ICMP Capture] フィールドは、前のウィンドウでクラスター オプションとして **[The whole cluster]** を選択した場合にのみ設定されます。

- ファイアウォールデバイスに入った時点で、通常のトラフィックと復号化されたトラフィックの両方を含む復号化された IPsec パケットをキャプチャするには、**[include-decrypted]** を選択します。
- クラスター ユニット上の永続パケットをキャプチャするには、**[persist]** を選択します。

ステップ 7 以降の手順については、[入力トラフィック セレクタ \(10 ページ\)](#) を参照してください。

ステップ 8 **[Next]** をクリックして、**[Egress Traffic Selector]** 画面を表示します。

ステップ 9 インターフェイスでパケットをキャプチャするには、**[Select Interface]** オプション ボタンをクリックします。

クラスタリング環境でクラスター コントロールプレーンパケットみをキャプチャするには、**[CP-Cluster]** チェックボックスをオンにします。

(注)

[Egress Traffic Selector] のフィールドの詳細については[出力トラフィック セレクタ \(11 ページ\)](#) を参照してください。

[Egress Traffic Selector] のフィールドの詳細については[出力トラフィック セレクタ \(11 ページ\)](#) を参照してください。

ステップ 10 **[Next]** をクリックして **[Buffers & Captures]** 画面を表示します。続行するには、「**バッファ**」を参照してください。

ステップ 11 最新のキャプチャを 10 秒ごとに自動的に取得するように、**[Capture Parameters]** 領域で **[Get capture every 10 seconds]** チェックボックスをオンにします。デフォルトでは、このキャプチャは循環バッファを使用します。

ステップ 12 **[Buffer Parameters]** 領域で、バッファサイズとパケットサイズを指定します。バッファサイズは、キャプチャがパケットを保存するために使用可能なメモリの最大容量です。パケットサイズは、キャプチャが保持できる最長のパケットです。できる限り多くの情報をキャプチャするため、最長パケットサイズを使用することを推奨します。

- (オプション。Cisco Secure Firewall 3100 デバイスのみに適用されます) キャプチャされたスイッチパケットを保存するには、**[スイッチ (Switch)]** チェックボックスをオンにします。
- パケットサイズを入力します。有効なサイズ範囲は 14 ~ 1522 バイトです。スイッチパケットキャプチャの場合、有効なサイズの範囲は 64 ~ 9,006 バイトです。
- バッファサイズを入力します。有効なサイズ範囲は 1534 ~ 33554432 バイトです。スイッチパケットキャプチャの場合、有効なサイズの範囲は 256 ~ 2,048 バイトです。

- d) キャプチャされたパケットを保存するには、[Use circular buffer] チェックボックスをオンにします。

(注)

この設定を選択すると、すべてのバッファストレージが使用されている場合、キャプチャは最も古いパケットへの上書きを始めます。

- ステップ 13** [Next] をクリックして、入力したクラスタ内の全装置のクラスタオプション（クラスタを使用している場合）、トラフィックセレクタ、バッファパラメータを表示する [Summary] 画面を表示します。続行するには、「[サマリー](#)」を参照してください。
- ステップ 14** [Next] をクリックして [Run Captures] 画面を表示し、次に [Start] をクリックしてパケットのキャプチャを開始します。[Stop] をクリックしてキャプチャを終了します。以降の手順については、[キャプチャの実行 \(12 ページ\)](#) を参照してください。クラスタリングを使用している場合は、手順 16 に進みます。
- ステップ 15** 残りのバッファスペースを確認するには、[Get Capture Buffer] をクリックします。現在のパケットの内容を削除して、バッファに別のパケットをキャプチャするスペースを確保するには、[Clear Buffer on Device] をクリックします。
- ステップ 16** クラスタ環境では、[Run Captures] 画面で、次の手順の 1 つ以上を実行します。
- [Get Cluster Capture Summary] をクリックすると、クラスタ内の全装置のパケットキャプチャ情報のサマリーに続いて、各装置のパケットキャプチャ情報が表示されます。
 - [Get Capture Buffer] をクリックすると、クラスタの各装置にどの程度バッファスペースが残っているかが表示されます。[Capture Buffer from Device] ダイアログボックスが表示されます。
 - [Clear Capture Buffer] をクリックすると、クラスタ内の特定の装置またはすべての装置の現在のコンテンツを削除し、さらにパケットをキャプチャするためのバッファ容量を確保します。
- ステップ 17** [Save captures] をクリックして、[Save Capture] ダイアログボックスを表示します。入力キャプチャ、出力キャプチャ、またはその両方を保存するオプションを選択できます。続行するには、「[キャプチャの保存](#)」を参照してください。
- ステップ 18** [Save Ingress Capture] をクリックして、[Save capture file] ダイアログボックスを表示します。PC 上の保存場所を指定して、[Save] をクリックします。
- ステップ 19** [Launch Network Sniffer Application] をクリックして、[Tools] > [Preferences] で指定したパケット分析アプリケーションを起動し、入力キャプチャを分析します。
- ステップ 20** [Save Egress Capture] をクリックして、[Save capture file] ダイアログボックスを表示します。PC 上の保存場所を指定して、[Save] をクリックします。
- ステップ 21** [Launch Network Sniffer Application] をクリックして、[Tools] > [Preferences] で指定したパケット分析アプリケーションを起動し、出力キャプチャを分析します。
- ステップ 22** [Close] をクリックし、次に [Finish] をクリックしてウィザードを終了します。

パケットキャプチャのガイドライン

コンテキストモード

- コンテキスト内のクラスタ制御リンクでキャプチャを設定できます。この場合、そのクラスタ制御リンクで送信されるコンテキストに関連付けられているパケットだけがキャプチャされます。
- VLAN ごとに設定できるキャプチャは1つだけです。共有 VLAN の複数のコンテキストでキャプチャを設定した場合は、最後に設定したキャプチャだけが使用されます。
- 最後に設定した（アクティブ）キャプチャを削除した場合は、別のコンテキストで事前に設定したキャプチャがあっても、アクティブになるキャプチャはありません。キャプチャをアクティブにするには、キャプチャを削除して追加し直す必要があります。
- キャプチャを指定したインターフェイスに着信するすべてのトラフィックがキャプチャされます。これには、共有 VLAN 上の他のコンテキストへのトラフィックも含まれます。したがって、ある VLAN のコンテキスト A でのキャプチャをイネーブルにしたときに、その VLAN がコンテキスト B でも使用される場合は、コンテキスト A とコンテキスト B の両方の入力トラフィックがキャプチャされます。
- 出力トラフィックの場合は、アクティブキャプチャのあるコンテキストのトラフィックだけがキャプチャされます。唯一の例外は、ICMP 検査をイネーブルにしない（したがって、ICMP トラフィックのセッションが高速パスにない）場合です。この場合は、共有 VLAN のすべてのコンテキストで入力と出力の ICMP トラフィックがキャプチャされます。

その他のガイドライン

- ASA が不正な形式の TCP ヘッダーを持つパケットを受信し、ASP が *invalid-tcp-hdr-length* であるというドロップ理由でそのパケットをドロップする場合、そのパケットを受信したインターフェイス上の **show capture** コマンド出力は、そのパケットを表示しません。
- IP トラフィックだけをキャプチャできます。ARP などの非 IP パケットはキャプチャできません。
- インライン SGT タグ付きパケットの場合、キャプチャされたパケットに含まれている追加 CMD ヘッダーを、PCAP ビューアが認識しないことがあります。
- パケットキャプチャには、システムを変更する、またはインスペクションのために接続に挿入されるパケット、NAT、TCP の正規化、パケットの内容を調整するその他の機能が含まれます。
- データパスに挿入された仮想パケットの寿命のトレースは、データパスでの物理パケットの処理を正確に反映していません。この違いは、ソフトウェアバージョン、構成、および挿入された仮想パケットのタイプによって異なります。違いが生じる原因となる可能性がある構成の設定を次に示します。
 - 同じホストに対して2つ以上の NAT ステートメントが存在する。

- 接続の順方向と逆方向のフローでプロトコルが異なる（順方向のフローが UDP または TCP で、逆方向のフローが ICMP である場合など）。
- ICMP エラーインスペクションが有効になっている。

入カトラフィック セレクタ

パケットキャプチャの入カインターフェイス、送信元と宛先のホストまたはネットワーク、およびプロトコルを設定するには、次の手順を実行します。

手順

-
- ステップ 1** ドロップダウン リストから入カインターフェイス名を選択します。
- ステップ 2** 入力送信元ホストおよびネットワークを入力します。ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。
- ステップ 3** 入力宛先ホストおよびネットワークを入力します。
- ステップ 4** キャプチャするプロトコル タイプを指定します。指定できるプロトコルは、ah、eigrp、esp、gre、icmp、icmp6、igmp、igrp、ip、ipinip、nos、ospf、pcp、pim、snp、tcp、または udp です。
- ICMP にのみ ICMP タイプを入力します。指定できるタイプは、all、alternate address、conversion-error、echo、echo-reply、information-reply、information-request、mask-reply、mask-request、mobile-redirect、parameter-problem、redirect、router-advertisement、router-solicitation、source-quench、time-exceeded、timestamp-reply、timestamp-request、traceroute、または unreachable です。
 - TCP および UDP プロトコルだけの送信元および宛先ポートのサービスを指定します。指定できるオプションは次のとおりです。
 - すべてのサービスを含めるには、[All Services] を選択します。
 - サービス グループを含めるには、[Service Groups] を選択します。
 特定のサービスを含めるには、aol、bgp、chargen、cifs、citrix-ica、ctiqbe、daytime、discard、domain、echo、exec、finger、ftp、ftp-data、gopher、h323、hostname、http、https、ident、imap4、irc、klogin、kshell、ldap、ldaps、login、lotusnotes、lpd、netbios-ssn、nntp、pcanywhere-data、pim-auto-rp、pop2、pop3、pptp、rsh、rtsp、sip、smtp、sqlnet、ssh、sunrpc、tacacs、talk、telnet、uucp、または whois のいずれかを指定します。
- ステップ 5** Cisco TrustSec サービスのパケットキャプチャを有効にするには、[セキュリティグループタグ (Security Group Tagging)] 領域の [SGT 番号 (SGT number)] チェックボックスをオンにして、セキュリティグループタグ番号を入力します。有効なセキュリティグループタグ番号は 2 ~ 65519 です。
- ステップ 6** (オプション。Cisco Secure Firewall 3100 デバイスおよび Cisco Secure Firewall 4200 モデルデバイスにのみ適用可能)。スイッチパケットキャプチャを有効にするには、[スイッチ制御 (Switch

Control] 領域で [スイッチ (Switch)] チェックボックスをオンにして、内部 VLAN と外部 VLAN の範囲 (1 ~ 4096) を指定します。

(注)

スイッチパケットキャプチャを有効にすると、アクセスリストオプションは無効になります。

- ステップ 7** (オプション。このオプションは、スイッチパケットキャプチャを有効にすると適用できません)。Cisco Secure Firewall 4200 モデルデバイスのパケットキャプチャに対して入力トラフィック方向のパラメータを設定するには、[方向制御 (Direction Control)] 領域で、[方向 (Direction)] ドロップダウンから方向を選択します。

出力トラフィック セレクタ

パケットキャプチャでの出力インターフェイス、送信元と宛先のホストとネットワーク、および送信元と宛先ポートのサービスを設定するには、次の手順を実行します。

手順

- ステップ 1** インターフェイスでパケットをキャプチャするには、[Select Interface] オプション ボタンをクリックします。ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。
- ステップ 2** ドロップダウン リストから出力インターフェイス名を選択します。
- ステップ 3** 出力送信元ホストおよびネットワークを入力します。
- ステップ 4** 出力宛先ホストおよびネットワークを入力します。
- 入力設定時に選択したプロトコルタイプがすでにリストされています。
- ステップ 5** (オプション。Cisco Secure Firewall 3100 デバイスおよび Cisco Secure Firewall 4200 モデルデバイスにのみ適用可能)。スイッチパケットキャプチャを有効にしている場合は、内部 VLAN と外部 VLAN の範囲 (1 ~ 4096) を指定します。スイッチパケットキャプチャを有効にするには、[入力トラフィック セレクタ \(10 ページ\)](#) を参照してください。
- ステップ 6** (オプション。このオプションは、スイッチパケットキャプチャを有効にすると適用できません)。Cisco Secure Firewall 4200 モデルデバイスのパケットキャプチャに対して出力トラフィック方向のパラメータを設定するには、[方向制御 (Direction Control)] 領域で、[方向 (Direction)] ドロップダウンから方向を選択します。

Buffers

パケットキャプチャのパケットサイズ、バッファ サイズ、および循環バッファを使用するかどうかを設定するには、次の手順を実行します。

手順

-
- ステップ 1** キャプチャが保持できる最長のパケットを入力します。できるだけ多くの情報をキャプチャするために、指定可能な最長サイズを使用してください。
 - ステップ 2** パケットを保存するためにキャプチャが使用できるメモリの最大容量を入力します。
 - ステップ 3** パケットの保存には循環バッファを使用します。循環バッファのバッファストレージがすべて使い尽くされると、キャプチャは最も古いパケットから上書きを始めます。
-

要約

[Summary] 画面には、クラスタオプション（クラスタリングを使用している場合）、トラフィックセレクタ、前のウィザード画面で選択したパケットキャプチャのためのバッファパラメータが表示されます。

キャプチャの実行

キャプチャセッションの開始および停止、キャプチャバッファの表示、ネットワークアナライザアプリケーションの起動、パケットキャプチャの保存、およびバッファのクリアを行うには、次の手順を実行します。

手順

-
- ステップ 1** [Start] をクリックして、選択したインターフェイス上でパケットキャプチャセッションを開始します。
 - ステップ 2** [Stop] をクリックして、選択したインターフェイス上のパケットキャプチャセッションを停止します。
 - ステップ 3** [Get Capture Buffer] をクリックして、インターフェイス上でキャプチャされたパケットのスナップショットを取得します。
 - ステップ 4** [Ingress] をクリックして、入力インターフェイスのキャプチャバッファを表示します。
 - ステップ 5** [Egress] をクリックして、出力インターフェイスのキャプチャバッファを表示します。
 - ステップ 6** [Clear Buffer on Device] をクリックして、デバイス上のバッファを消去します。
 - ステップ 7** [Launch Network Sniffer Application] をクリックして、[Tools] > [Preferences] で指定した、入力キャプチャまたは出力キャプチャを分析するためのパケット分析アプリケーションを起動します。
 - ステップ 8** [Save Captures] をクリックして、入力キャプチャおよび出力キャプチャを ASCII または PCAP 形式で保存します。
-

キャプチャの保存

パケットをさらに分析するために、入力および出力パケットキャプチャを ASCII または PCAP ファイル形式で保存するには、次の手順を実行します。

手順

-
- ステップ1 キャプチャバッファを ASCII 形式で保存するには、[ASCII] をクリックします。
 - ステップ2 キャプチャバッファを PCAP 形式で保存するには、[PCAP] をクリックします。
 - ステップ3 入力パケットキャプチャを保存するファイルを指定するには、[Save ingress capture] をクリックします。
 - ステップ4 出力パケットキャプチャを保存するファイルを指定するには、[Save egress capture] をクリックします。
-

CPU 使用率とレポート

CPU 使用率レポートには、指定された時間内に使用された CPU の割合の要約が表示されます。通常、コアはピーク時以外には合計 CPU 容量の約 30 ~ 40% で動作し、ピーク時は約 60 ~ 70% の容量で動作します。

の vCPU 使用率 ASA 仮想

CPU 使用率の統計を表示するには、ASA 仮想で **show cpu usage** コマンドを使用します。ASA 仮想の vCPU 使用率では、データパス、制御ポイント、および外部プロセスで使用されている vCPU の量を表示します。

(VMware、Azure、OCI などの) クラウドサービスプロバイダーによって報告される vCPU 使用率には、示されている ASA 仮想使用率に加えて、以下が含まれます。

- ASA 仮想のアイドル時間
- ASA VM に使用された %SYS オーバーヘッド
- vSwitch、vNIC および pNIC の間を移動するパケットのオーバーヘッド。このオーバーヘッドは非常に大きくなる場合があります。

CPU 使用率の例

報告された vCPU の使用率が大幅に異なる例を次に示します。

- ASA 仮想のレポート：40%

- DP : 35%
- 外部プロセス : 5%
- vSphere のレポート : 95%
- ASA (ASA 仮想 レポートとして) : 40%
- ASA アイドル ポーリング : 10%
- オーバーヘッド : 45%

オーバーヘッドは、ハイパーバイザ機能の実行、および vSwitch を使用した NIC と vNIC の間のパケット転送に使用されています。

ASA 仮想のためのオーバーヘッドとして、ESXi サーバが追加のコンピューティングリソースを使用する場合があるため、使用率は 100% を超えることがあります。

VMware の CPU 使用率のレポート

vSphere で [VM Performance] タブをクリックし、[Advanced] をクリックすると [Chart Options] ドロップダウンリストが表示されます。ここには VM の各ステート (%USER、%IDLE、%SYS など) の vCPU 使用率が表示されます。この情報は、VMware の観点から CPU リソースが使用されている場所を理解するのに役立ちます。

ESXi サーバのシェル (ホストへの接続に SSH を使用してシェルにアクセスします) では、esxtop を使用できます。Esxtop は Linux の **top** コマンドに似た操作性と外観を持ち、次の内容を含む vSphere のパフォーマンスに関する VM のステート情報を提供します。

- vCPU、メモリ、ネットワーク使用率の詳細
- 各 VM のステートごとの vCPU 使用率
- メモリ (実行中に「M」と入力) とネットワーク (実行中に「N」と入力) に加えて、統計情報と RX ドロップ数

ASA 仮想 と vCenter のグラフ

ASA 仮想 と vCenter の CPU 使用率の数値には違いがあります。

- vCenter のグラフの数値は常に ASA 仮想 の数値よりも大きくなります。
- vCenter ではこの値は %CPU usage と呼ばれ、ASA 仮想 ではこの値は %CPU utilization と呼ばれます。

用語「%CPU utilization」と「%CPU usage」は別のものを意味しています。

- CPU utilization は、物理 CPU の統計情報を提供します。

- CPU usage は CPU のハイパースレッディングに基づいた論理 CPU の統計情報を提供します。しかし、1 つの vCPU のみが使用されるため、ハイパースレッディングは動作しません。

vCenter は CPU % usage を次のように計算します。

アクティブに使用された仮想 CPU の量。使用可能な CPU の合計に対する割合として指定されます。

この計算は、ホストから見た CPU 使用率であり、ゲストオペレーティングシステムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率 / 仮想 CPU の数 x コア周波数」として計算されます。

使用率を MHz で比較すると、vCenter と ASA 仮想 両方の数値は一致します。vCenter グラフから、MHz % CPU 使用率は $60 / (2499 \times 1 \text{ vCPU}) = 2.4$ と求められます。

Amazon CloudWatch CPU 使用率レポート

メトリックエクスペローラを表示して、タグとプロパティでリソースをモニターできます。特定のインスタンスの CPU 使用率の統計を表示するには、次の手順を実行します。

手順

- ステップ 1** [CloudWatch] コンソールを開き、ナビゲーションペインで [メトリクス (Metrics)] を選択します。
- ステップ 2** EC2 メトリクスの名前空間を選択し、[インスタンスごとのメトリクス (Per-instance Metrics)] ディメンションを選択します。
- ステップ 3** 検索フィールドに **CPUUtilization** と入力して Enter を押します。必要なインスタンスの行を選択し、そのインスタンスの **CPUUtilization** メトリックのグラフを表示します。

詳細については、[Amazon CloudWatch のドキュメント](#)を参照してください。

ASA 仮想 と Amazon CloudWatch のグラフ

Amazon CloudWatch のグラフの数値は、CPU 使用率の計算方法が ASA 仮想 と CloudWatch で異なるため、数値よりも大きくなっています。

ASA 仮想 がポーリングモードで実行されている場合、各 CPU は、省電力モードやその他のアイドル状態に入る代わりに、軽量コマンドのループを実行します。これにより、インテルの電

源状態によってオンオフを切り替えたりクロックを調整したりするのではなく、各コアが常にアクティブに保たれてパフォーマンスが向上します。

ASA 仮想内では、このアクティビティはアイドル動作であると認識され、CPU 使用率が正しく計算されます。ただし、Amazon CloudWatch では、すべての CPU サイクルに実行する命令があるため、アイドル状態の動作は通常の CPU アクティビティのように見えます。これにより、CloudWatch では高い CPU 使用率（85 ～ 90%）が表示されます。

Azure の CPU 使用率レポート

Azure Monitor から VM Insights を使用して、監視対象の VM すべての CPU 使用率を表示するには、次の手順を実行します。

手順

-
- ステップ 1** Azure ポータルに移動し、[監視 (Monitor)] を選択してから [ソリューション (Solutions)] セクションで [仮想マシン (Virtual Machines)] を選択します。
 - ステップ 2** [パフォーマンス (Performance)] タブを選択して [CPU 使用率 (CPU Utilization %)] グラフを表示します。このグラフには、平均プロセッサ使用率が最も高い上位 5 つのマシンが表示されます。
-

特定の Azure VM から直接 CPU 使用率グラフを表示するには、次の手順を実行します。

手順

-
- ステップ 1** Azure ポータルに移動し、[仮想マシン (Virtual Machines)] を選択します。
 - ステップ 2** VM のリストから VM を選択します。
 - ステップ 3** [モニタリング (Monitoring)] セクションで、[Insights] を選択します。
 - ステップ 4** [パフォーマンス (Performance)] タブを選択します。

詳細については、「[How to chart performance with VM insights](#)」[英語] を参照してください。

ASA 仮想 と Azure のグラフ

ASA 仮想 と Azure の CPU 使用率の数値には違いがあります。Azure は、使用可能な CPU の合計に対する割合として指定される、アクティブに使用されている仮想 CUP の量として CPU 使用率を計算するため、Azure のグラフの数値は常に ASA 仮想 の数値より高くなります。

この計算は、ホストから見た CPU 使用率であり、ゲストオペレーティングシステムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率/仮想 CPU の数 X コア周波数」として計算されます。

Azure は、ゲスト OS によって要求される CPU の量にもレート制限を適用します。ASA 仮想が 40% の CPU 使用率を報告し、ハイパーバイザが 90% の CPU 使用率を報告しているシナリオについて考えてみましょう。ここで ASA 仮想がさらなる処理能力を求めた場合、CPU 使用率が 80% を超え、ハイパーバイザが 95% を超える CPU 使用率を報告する可能性があります。これにより、ASA 仮想がポーリングモードで軽量コマンドのループを実行しているだけでアイドルリング動作を示していたとしても、ハイパーバイザは ASA 仮想 CPU をスロットリングすることになります。

Hyper-V CPU 使用率レポート

使用可能なクラウドサーバーの CPU、RAM、およびディスク容量の構成情報の表示に加えて、ディスク、I/O、およびネットワーク情報も表示できます。この情報を使用して、ニーズに適したクラウドサーバーを決定してください。コマンドライン nova クライアントまたは **Cloud Control Panel** インターフェイスを使用して、使用可能なサーバーを表示できます。

コマンドラインで、次のコマンドを実行します。

```
nova flavor-list
```

使用可能なすべてのサーバー構成が表示されます。リストには、次の情報が含まれています。

- ID : サーバー構成 ID
- 名前 : RAM サイズとパフォーマンスタイプでラベル付けされた構成名
- Memory_MB : 構成の RAM の量
- ディスク : GB 単位のディスクサイズ (汎用クラウドサーバーの場合、システムディスクのサイズ)
- エフェメラル : データディスクのサイズ
- スワップ : スワップ領域のサイズ
- VCPU : 構成に関連付けられた仮想 CPU の数
- RXTX_Factor : サーバーに接続された PublicNet ポート、ServiceNet ポート、および分離されたネットワーク (クラウドネットワーク) に割り当てられる帯域幅の量 (Mbps 単位)
- Is_Public : 未使用

ASA Virtual と Hyper-V のグラフ

ASA Virtual と Hyper-V の CPU 使用率の数値には違いがあります。

- Hyper-V のグラフの数値は ASA Virtual の数値よりも常に大きくなります。
- Hyper-V ではこの値は %CPU usage と呼ばれ、ASA Virtual ではこの値は %CPU utilization と呼ばれます。

用語「%CPU utilization」と「%CPU usage」は別のものを意味しています。

- CPU utilization は、物理 CPU の統計情報を提供します。
- CPU usage は CPU のハイパースレッディングに基づいた論理 CPU の統計情報を提供します。しかし、1つの vCPU のみが使用されるため、ハイパースレッディングは動作しません。

Hyper-V では %CPU usage は次のように計算されます。

アクティブに使用された仮想 CPU の量。使用可能な CPU の合計に対する割合として指定されます。

この計算は、ホストから見た CPU 使用率であり、ゲストオペレーティングシステムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率 / 仮想 CPU の数 x コア周波数」として計算されます。



(注) 正確な CPU 使用率を得るには、ASA Virtual レポートを調べることをお勧めします。

OCI CPU 使用率レポート

コンピューティング インスタンス メトリック `oci_computeagent` を使用して、OCI の CPU 使用率を表示できます。CpuUtilization メトリックは、CPU からのアクティビティレベルを表示し、合計時間に対する割合として表されます。単一のコンピューティング インスタンスのメトリック グラフを表示するには、次の手順を実行します。

手順

- ステップ 1** ナビゲーションメニューを開き、[コンピューティング (Compute)] の下の [インスタンス (Instances)] をクリックします。

- ステップ2** インスタンスをクリックし、[リソース (Resources)] の下の [メトリック (Metrics)] をクリックします。
- ステップ3** メトリック名前空間リストで [oci_computeagent] を選択します。
- 詳細については、[コンピューティング インスタンス メトリック](#) を参照してください。

ASA 仮想 と OCI のグラフ

OCI は、使用可能な CPU の合計に対する割合として指定される、アクティブに使用されている仮想 CUP の量として CPU 使用率を計算するため、OCI のグラフの数値は常に ASA 仮想の数値より高くなります。

この計算は、ホストから見た CPU 使用率であり、ゲストオペレーティングシステムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率/仮想 CPU の数 X コア周波数」として計算されます。

設定のテスト

ここでは、シングルモード ASA または各セキュリティ コンテキストの接続性のテスト方法、ASA インターフェイスを ping する方法、およびある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 できるようにする方法について説明します。

基本接続のテスト：アドレス向けの ping の実行

ping は、特定のアドレスが使用可能で、応答するかどうかを確認するための単純なコマンドです。次のトピックでは、このコマンドの詳細とそれを使って実行可能なテストについて説明します。

ping で実行可能なテスト

デバイスを ping すると、そのデバイスにパケットが送信され、デバイスが応答を返します。このプロセスを使用して、ネットワークデバイスは、相互に検出、識別、およびテストすることができます。

ping を使用して、次のテストを実行できます。

- 2 つのインターフェイスのループバック テスト：同じ ASA で一方のインターフェイスからもう一方のインターフェイスに ping を外部ループバック テストとして起動すると、双方のインターフェイスの基本的な「アップ」ステータスおよび動作を検証できます。

- ASA の ping : 別の ASA のインターフェイスを ping し、そのインターフェイスがアップしていて応答することを確認できます。
- ASA 経由の ping : ASA の反対側のデバイスを ping することによって、中間 ASA 経由で ping することができます。パケットは、それぞれの方向に移動するときに、2つの中間 ASA のインターフェイスを通過します。このアクションは、中間ユニットのインターフェイス、動作、および応答時間の基本テストになります。
- ネットワーク デバイスの疑わしい動作をテストするための ping : ASA インターフェイスから、正常に機能していないと思われるネットワーク デバイスに ping することができます。インターフェイスが正しく設定されているにもかかわらずエコーが受信されない場合は、デバイスに問題があると考えられます。
- 中間通信をテストするための ping : ASA インターフェイスから、正常に機能することがわかっているネットワーク デバイスに ping することができます。エコーを受信した場合、中間にあるデバイスがすべて正常に動作し、物理的に正しく接続されていることが確認されたこととなります。

ICMP ping と TCP ping の選択

ASA には、ICMP エコー要求パケットを送信して、エコー応答パケットを受信する従来の ping が付属しています。これは、標準ツールで、すべての仲介ネットワークデバイスで ICMP トラフィックが許可される場合にうまく機能します。ICMP ping を使用して、IPv4/IPv6 アドレスまたはホスト名を ping することができます。

ただし、ICMP を禁止しているネットワークもあります。ご使用のネットワークがこれに該当する場合は、代わりに、TCP ping を使用してネットワーク接続をテストできます。TCP ping では、ping から TCP SYN パケットが送信され、応答で SYN-ACK が受信された段階でその ping が成功したと見なされます。また、TCP ping では、IPv4 アドレスまたはホスト名は ping できますが、IPv6 アドレスは ping できません。

正常な ICMP または TCP ping とは、使用されているアドレスが有効で特定のタイプのトラフィックに反応することを意味しているにすぎません。これは基本接続が機能していることを意味します。デバイス上で動作する他のポリシーで、特定のタイプのトラフィックがデバイスを通過できないようにすることができます。

ICMP の有効化

デフォルトでは、セキュリティの高いインターフェイスからセキュリティの低いインターフェイスへの ping を実行できます。リターントラフィックを通過させるように ICMP インспекションをイネーブルにすることだけが必要です。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に ping するには、トラフィックを許可する ACL を適用する必要があります。

ASA インターフェイスを ping する場合は、そのインターフェイスに適用された ICMP ルールによって、エコー要求パケットとエコー応答パケットが許可される必要があります。ICMP ルールは省略可能です。このルールを設定しなかった場合は、インターフェイスへのすべての ICMP トラフィックが許可されます。

この手順では、ASA インターフェイスの ICMP ping をイネーブルにするため、または、ASA 経由の ping 用に構成する必要がある ICMP コンフィギュレーションのすべてについて説明します。

手順

ステップ 1 ICMP ルールでエコー要求/エコー応答が許可されることを確認します。

ICMP ルールは、省略可能で、インターフェイスに直接送信される ICMP パケットに適用されます。ICMP ルールを適用しなかった場合は、すべての ICMP アクセスが許可されます。この場合は、アクションが不要です。

ただし、ICMP ルールを実装する場合は、エコー要求メッセージとエコー応答メッセージのアドレスを許可するルールが各インターフェイスに含まれていることを確認します。[Configuration] > [Device Management] > [Management Access] > [ICMP] ペインで ICMP ルールを設定します。

ステップ 2 アクセスルールで ICMP が許可されることを確認します。

ASA 経由でホストを ping する場合は、アクセスルールで ICMP トラフィックの送受信が許可される必要があります。アクセスルールは、少なくとも、エコー要求/エコー応答 ICMP パケットを許可する必要があります。これらのルールはグローバルルールとして追加することができます。

アクセスルールを使用しない場合は、必要な他のタイプのトラフィックも許可する必要があります。これは、インターフェイスにアクセスルールを適用すると、暗黙の deny が追加されるため、他のすべてのトラフィックが破棄されるためです。

[Configuration] > [Firewall] > [Access Rules] ペインでアクセスルールを設定します。単にテスト目的でルールを追加する場合は、テストの終了後にそのルールを削除できます。

ステップ 3 ICMP インспекションをイネーブルにします。

インターフェイスの ping とは対照的に、ASA 経由で ping する場合は、ICMP インспекションが必要です。インспекションを使用すれば、リターントラフィック（つまり、エコー応答パケット）を ping を開始したホストに返すことができるうえ、パケットあたり 1 つの応答の存在が保証されるため、特定のタイプの攻撃を防止することができます。

ICMP インспекションは、デフォルトのグローバルインспекションポリシーでイネーブルにできます。

- a) [Configuration] > [Firewall] > [Service Policy Rules] の順に選択します。
- b) **inspection_default** グローバルルールを編集します。
- c) [Rule Actions] > [Protocol Inspection] タブで、ICMP を選択します。
- d) [OK] をクリックし、さらに [Apply] をクリックします。

ホストの ping

デバイスを ping するには、[Tools] > [Ping] を選択して、ping する宛先の IP アドレスまたはホスト名を入力し、[Ping] をクリックするだけです。TCP ping の場合は、[TCP] を選択して、宛先ポートも含めます。通常は、実行する必要があるテストの範囲にします。

成功した ping の出力例：

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ping が失敗した場合は、失敗した試行が ? で示され、成功率が 100% 未満になります（すべて失敗した場合は 0% になります）。

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
????
Success rate is 0 percent (0/5)
```

ただし、ping の一部の側面を制御するパラメータを追加することもできます。以下に基本オプションを示します。

- ICMP ping：送信元 IP アドレスに使用するインターフェイスを選択できます。ただし、出力インターフェイスは、データルーティングテーブルを使用したルートルックアップによって決定されます。IPv4/IPv6 アドレスまたはホスト名を ping することができます。
- TCP ping：ping する宛先の TCP ポートを選択する必要もあります。たとえば、HTTP ポートを ping するには **www.example.com 80** とします。IPv4 アドレスまたはホスト名を ping することはできますが、IPv6 アドレスを ping することはできません。

送信元 IP アドレスに使用するインターフェイスを指定するオプションもあります。ただし、出力インターフェイスは、データルーティングテーブルを使用したルートルックアップによって決定されます。

最後に、ping を繰り返す回数（デフォルトは 5 回）または各試行のタイムアウト（デフォルトは 2 秒）を指定できます。

ASA 接続の体系的なテスト

ASA 接続のさらに体系的なテストを実行する場合は、次の一般的な手順を使用できます。

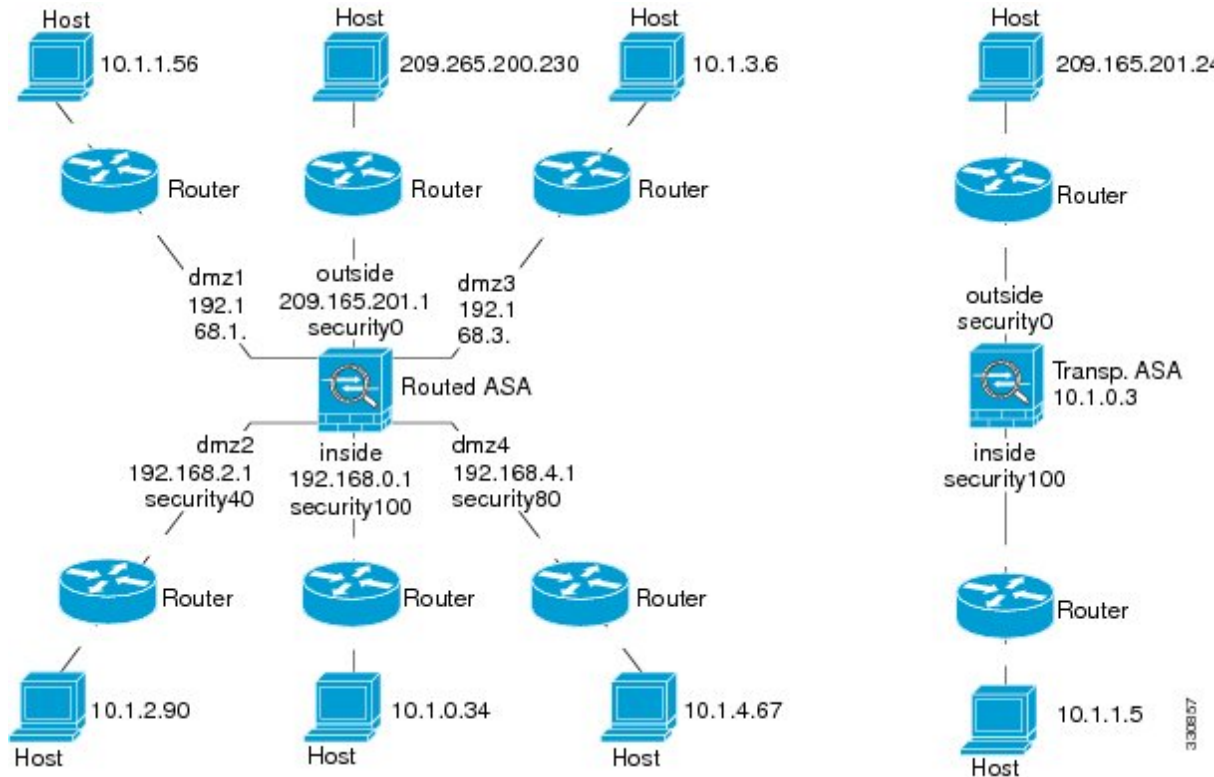
始める前に

手順で説明した syslog メッセージを確認する場合は、ロギングをイネーブルにします（**logging enable** コマンドまたは ASDM の [Configuration] > [Device Management] > [Logging] > [Logging Setup]）。

手順

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 ASA またはセキュリティ コンテキストの図を作成します。図には、直接接続されたすべてのルータ、および ASA 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。

図 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図



ステップ 2 直接接続されたルータから各 ASA 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、BVI IP アドレスを ping します。このテストでは、ASA 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。

ASA 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 ASA 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 (次の図を参照)。この場合は、パケットが ASA に到達しないので、デバッグメッセージや syslog メッセージは表示されません。

図 2: ASA インターフェイスでの ping の失敗

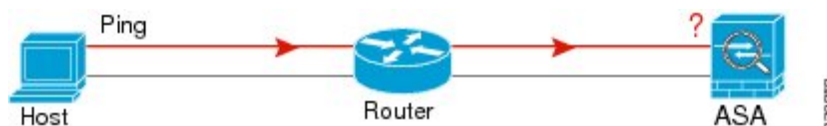
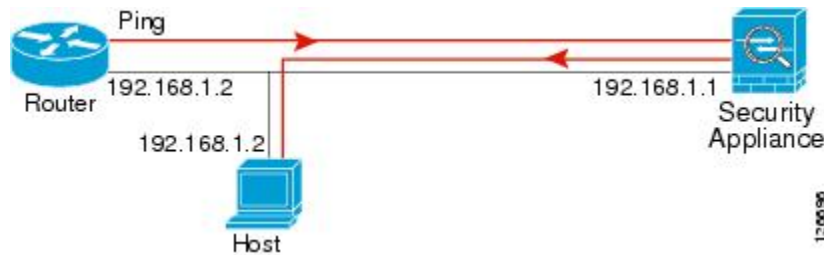


図 3: IP アドレッシングの問題による ping の失敗



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 アドレスが存在する可能性があります（次の図を参照）。

ステップ 3 リモートホストから各 ASA 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、BVI 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 ASA の間でパケットをルーティングできるかどうか、および ASA がパケットを正確にルーティングしてホストに戻せるかどうかを確認します。

中間ルータを通してホストに戻るルートが ASA がない場合、ping は失敗する可能性があります（次の図を参照）。この場合は、デバッグメッセージは ping が成功したことを示しますが、ルーティングの失敗を示す syslog メッセージ 110001 が表示されます。

図 4: ASA の戻りルート未設定による ping の失敗



ステップ 4 ASA インターフェイスから既知のネットワークデバイスへの ping は正しく機能しています。

- ping を受信しない場合は、送信ハードウェアまたはインターフェイスのコンフィギュレーションに問題がある可能性があります。
- ASA のインターフェイスが正しく設定されているにもかかわらず、「既知の正常な」デバイスからエコー応答を受信しない場合は、インターフェイスハードウェアの受信機能に問題があると考えられます。「既知の正常な」受信機能を持つ別のインターフェイスで、同じ「既知の正常な」デバイスに対して ping を送信してエコーを受信できる場合、最初のインターフェイスのハードウェアの受信機能に問題があると確認されたことになります。

ステップ 5 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。NAT を使用する場合は、このテストを行うと NAT が正しく動作していることがわかります。

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 syslog メッセージが表示されます。show xlate コマンドまたは show conns コマンドを入力してこの情報を表示することもできます。

NAT が正しく設定されていないことが原因で、ping に失敗することもあります。この場合、NAT が失敗したことを示す syslog メッセージが表示されます (305005 または 305006)。ping

が外部ホストから内部ホストへ送信され、スタティック変換が存在しない場合は、メッセージ 106010 が表示されます。

図 5: ASA のアドレス変換の問題による ping の失敗



ホストまでのルートの追跡

IP アドレスへのトラフィックの送信で問題が発生している場合は、ホストまでのルートを追跡することによってネットワークパスに問題がないかどうかを確認できます。

手順

- ステップ 1 [トレースルート上の ASA の表示 \(25 ページ\)](#) を使用して無効にすることができます。
- ステップ 2 [パケットルートの決定 \(26 ページ\)](#) を使用して無効にすることができます。

トレースルート上の ASA の表示

デフォルトで、ASA はトレースルート上にホップとして表示されません。これを表示するには、ASA を通過するパケットの存続可能時間を減らして、ICMP 到達不能メッセージのレート制限を増やす必要があります。

手順

- ステップ 1 サービスポリシーを使用して TTL を減らします。
 - a) [Configuration] > [Firewall] > [Service Policy Rules] の順に選択します。
 - b) ルールを追加または編集します。たとえば、TTL を減らすためのオプションを追加可能なルールがすでに存在する場合は、新しいルールを作成する必要はありません。
 - c) ルールをグローバルまたはインターフェイスに適用し、トラフィック照合を指定する [Rule Actions] ページまでウィザードを進めます。たとえば、グローバル match any ルールを作成できます。
 - d) [Rule Actions] ページで、[Connection Settings] タブをクリックして、[Decrement time to live for a connection] を選択します。
 - e) [OK] または [Finish] をクリックしてから、[Apply] をクリックします。
- ステップ 2 ICMP 到達不能レート制限を増やします。

- a) [Configuration] > [Device Management] > [Management Access] > [ICMP] を選択します。
- b) ページの下部にある [IPv4 ICMP Unreachable Message Limits] > [Rate Limit] の値を増やします。たとえば、50 に増やします。
- c) [Apply] をクリックします。

パケットルートの決定

tracert を使用すれば、パケットが宛先に到着するまでのルートを特定できます。tracert は、無効なポート上の宛先に UDP パケットまたは ICMPv6 エコーを送信することで機能します。ポートが有効でないため、宛先への途中にあるルータは ICMP または ICMPv6 Time Exceeded Message で応答し、そのエラーを ASA に報告します。

tracert は送信された各プローブの結果を表示します。出力の各行が 1 つの TTL 値に対応します (昇順)。次の表に、出力記号の説明を示します。

| 出力記号 | 説明 |
|---------|---|
| * | タイムアウトの期間内にプローブへの応答を受信しませんでした。 |
| U | 宛先へのルートが存在しません。 |
| nn msec | 各ノードで、指定した数のプローブのラウンドトリップにかかる時間 (ミリ秒)。 |
| !N. | ICMP ネットワークに到達できません。ICMPv6 では、アドレスは対象外です。 |
| !H | ICMP ホストに到達できません。 |
| !P | ICMP に到達できません。ICMPv6 では、ポートが到達不能です。 |
| !A | ICMP が管理者によって禁止されています。 |
| ? | 原因不明の ICMP エラーが発生しました。 |

手順

- ステップ 1 Tools > Tracert** の順に選択します。
- ステップ 2** ルートを追跡する宛先ホスト名または IP アドレスを入力します。ホスト名を使用するように DNS サーバーを設定します。
- ステップ 3** (オプション) トレースの特性を設定します。デフォルトがほとんどのケースに適合します。
 - [Timeout] : タイムアウトするまで応答を待機する時間。デフォルトは 3 秒です。
 - [Port] : 使用する UDP ポート。デフォルトは 33434 です。
 - [Probe] : 各 TTL レベルで送信するプローブの数。デフォルトは 3 です。

- [TTL] : プローブの最小および最大存続可能時間。デフォルトの最小値は1ですが、この値を増やして、既知のホップの表示を抑制することができます。デフォルトの最大値は30です。トレースルートは、パケットが宛先に到達するか、または最大値に達すると終了します。
- [Specify source interface or IP address] : トレースの送信元として使用するインターフェイス。インターフェイスは、名前またはIPアドレスで指定できます。IPv6では、送信元インターフェイスを指定できません。送信元IPアドレスだけを指定できます。IPv6アドレスは、ASAインターフェイスでIPv6を有効にしている場合にのみ有効です。トランスペアレントモードでは、管理アドレスを使用する必要があります。
- [Reverse Resolve] : DNS名前解決が設定されている場合に検出されたホップの名前を出力に表示するかどうか。IPアドレスのみを表示するオプションを選択解除します。
- [Use ICMP] : UDPプローブパケットの代わりにICMPプローブパケットを送信するかどうか。

ステップ4 [Trace Route] をクリックしてトレースルートを開始します。

[Traceroute Output] 領域に、トレースルートの結果についての詳細なメッセージが表示されます。

パケットトレーサを使用したポリシー設定のテスト

送信元と宛先のアドレスおよびプロトコルの特性に基づいてパケットをモデル化することによってポリシー設定をテストできます。トレースは、ポリシー参照を実行してアクセスルールやNATなどをテストし、パケットを許可するか、拒否するかを確認します。

このようにパケットをテストすることによって、ポリシーの結果を確認し、必要に応じて、許可または拒否するトラフィックのタイプが処理されるかどうかをテストできます。設定の確認に加えて、トレーサを使用して許可すべきパケットが拒否されるなどの予期せぬ動作をデバッグできます。

手順

ステップ1 [Tools] > [Packet Tracer] の順に選択します。

ステップ2 パケットトレースの送信元インターフェイスを選択します。

ステップ3 パケットトレースのパケットタイプを指定します。指定できるプロトコルタイプは、ICMP、IP、TCP、UDP、およびSCTPです。

ステップ4 (オプション)。セキュリティグループタグの値がレイヤ2 CMD ヘッダーに埋め込まれたパケットを追跡する (Trustsec) 場合は、[SGT number] をオンにして、セキュリティグループタグの番号 (0 ~ 65533) を入力します。

ステップ 5 (トランスペアレントモード) パケット トレーサが (後でサブインターフェイスにリダイレクトされる) 親インターフェイスに入るようにするには、[VLAN ID] をオンにして、1 ~ 4096 の範囲の ID を入力します。VLAN ID は、入力インターフェイスがサブインターフェイスでない場合にのみ使用できます。

ステップ 6 (トランスペアレントモード) 宛先 MAC アドレスを指定します。

ステップ 7 パケットの送信元と宛先を指定します。

Cisco TrustSec を使用する場合は、IPv4 または IPv6 アドレス、完全修飾ドメイン名 (FQDN)、またはセキュリティグループの名前あるいはタグを指定できます。送信元アドレスに対して、Domain\username 形式でユーザー名を指定することもできます。

ステップ 8 プロトコルの特性を指定します。

- [ICMP] : ICMP タイプ、ICMP コード (0 ~ 255)、およびオプションで ICMP 識別子を入力します。
- [TCP/UDP/SCTP] : 送信元および宛先のポート番号を入力します。
- [Raw IP] : プロトコル番号(0 ~ 255) を入力します。

ステップ 9 クラスタ ユニット全体でパケットをデバッグするには、パケット トレーサを使用します。[Cluster Capture] ドロップダウンリストから、次の項目を選択します。

- a) **decrypted** : VPN トンネルで復号化されたパケットを注入し、さらに、VPN トンネルを経由して到着するパケットをシミュレートします。
- b) **persist** : クラスタ ユニット全体で追跡するパケットを注入します。
- c) **bypass-checks**—Skips security checks like ACL, VPN filters, IPsec spoof, and uRPF.
- d) **transmit** : シミュレートされたパケットが ASA から出られるようにします。

ステップ 10 [Start] をクリックして、パケットをトレースします。

[Information Display Area] に、パケット トレースの結果に関する詳細情報が表示されます。

パフォーマンスとシステム リソースのモニタリング

さまざまなシステムリソースをモニターすることによって、パフォーマンス上の問題またはその他の潜在的な問題を特定することができます。

パフォーマンスのモニタリング

ASA のパフォーマンス情報をグラフ形式または表形式で表示できます。

手順

ステップ 1 [Monitoring] > [Properties] > [Connection Graphs] > [Perfmon] の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Available Graphs] リストから最大 4 つのエントリを選択してから、[Add] をクリックしてそれらのエントリを [Selected Graphs] リストに移動します。使用可能なオプションは次のとおりです。

- [AAA Perfmon] : 認証、許可、およびアカウントリング要求に関する秒単位の要求数。
- [Inspection Perfmon] : HTTP、FTP、および TCP インスペクションに関する秒単位のパケット数。
- [Web Perfmon] : URL アクセス要求と URL サーバー要求に関する秒単位の要求数。
- [Connections Perfmon] : すべての接続、UDP 接続、TCP 接続、および TCP 代行受信に関する秒単位の接続数。
- [Xlate Perfmon] : 秒単位の NAT xlate。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間でそれぞれの表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

メモリ ブロックのモニタリング

空きメモリ ブロックと使用中のメモリ ブロックをグラフ形式または表形式で表示できます。

手順

ステップ 1 [Monitoring] > [Properties] > [System Resources Graphs] > [Blocks] の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Available Graphs] リストからエントリを選択してから、[Add] をクリックしてそれらのエントリを [Selected Graphs] リストに移動します。使用可能なオプションは次のとおりです。

- [Blocks Used] : ASA で使用中のメモリ ブロックを表示します。
- [Blocks Free] : ASA の空きメモリ ブロックを表示します。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間でそれぞれの表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

CPU のモニタリング

CPU 使用率を表示できます。

手順

ステップ 1 [Monitoring] > [Properties] > [System Resources Graphs] > [CPU] の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Selected Graphs] リストに [CPU Utilization] を追加します。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間で表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

メモリのモニタリング

メモリ使用量情報をグラフ形式または表形式で表示できます。

手順

ステップ 1 [Monitoring] > [Properties] > [System Resources Graphs] > [Memory] の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Available Graphs] リストからエントリを選択してから、[Add] をクリックしてそれらのエントリを [Selected Graphs] リストに移動します。使用可能なオプションは次のとおりです。

- [Free Memory] : ASA の空きメモリを表示します。
- [Used Memory] : ASA の使用中のメモリを表示します。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間でそれぞれの表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

プロセス単位の CPU 使用率のモニタリング

CPU で実行されているプロセスをモニターできます。特定のプロセスで使用される CPU の使用率に関する情報を取得できます。CPU 使用率の統計情報は降順で並べられ、使用率の最も高いプロセスが先頭に表示されます。また、プロセスごとの CPU に対する負荷に関する情報（記録時間の 5 秒前、1 分前、および 5 分前の情報）も含まれています。この情報は 5 秒おきに自動的に更新され、リアルタイムの統計情報が表示されます。ASDM では、30 秒おきに更新されます。

プロセス単位の CPU 使用率を表示するには、**[Monitoring] > [Properties] > [Per-Process CPU Usage]** の順に選択します。

自動更新を停止して、情報を手動で更新し、ファイルに保存することができます。**[Configure CPU Usage Colors]** をクリックして、使用率に基づいて背景色と前景色を選択することによって、使用率の高いプロセスのスキャンを実行しやすくすることもできます。

接続のモニタリング

現在の接続を表形式で表示するには、ASDM メイン ウィンドウで、**[Monitoring] > [Properties] > [Connections]** の順に選択します。各接続に関する情報には、プロトコル、送信元アドレスと宛先アドレスの特性、最後のパケットが送信または受信されてからのアイドル時間、および接続中のトラフィック量が含まれます。

ASA Virtual での同意トークンを使用したルートシェルアクセスのサポート

ASA Virtual は、承認ユーザーが管理者パスワードなしでトラブルシューティングまたは診断の目的で Linux ルートシェルにワンタイムアクセスできるようにする新しい同意トークンメカニズムをサポートします。



- (注)
- ユーザーは、コンソールのシリアル端末またはホストの仮想シリアルコンソール経由で、チャレンジを開始し、応答を送信できます。応答が正常に検証されると、ルートシェルが対応するコンソールで開かれます。
 - ユーザーは、SSH または Telnet 端末でチャレンジを生成し、応答を受け入れることができます。応答が確認されると、ルートシェルはコンソール端末でのみ使用可能になり、SSH や Telnet 端末では使用できなくなります。
 - ルートシェルにアクセスするための推奨される方法は、仮想シリアルコンソール経由です。このコンソールでは、ユーザーがチャレンジを生成し、応答を検証し、シリアル端末内で直接ルートシェルを開くことができます。

Consent Token を使用して Linux ルートシェルにアクセスする手順

次の手順を実行して、チャレンジを生成し、Cisco TAC からの応答を取得し、ルートシェルを開きます。

1. チャレンジを生成する

Cisco ASA Virtual で次の CLI コマンドを実行するとチャレンジ文字列を生成できます。

```
ciscoasa# consent-token generate-challenge shell-access 1
```

出力例：

```
Generating Challenge.....
```

```
Challenge String (Please copy everything between the asterisk lines exclusively):
```

```
*****
wzC0AAQ0FPAQAAEFgAEAAAAAACITkRfSL0EBAQzOyEFWlp7wGirO8-SUQABAAJYCARQMBwPHMFTQVDAgABFTQXJAs5QV5SzRNOERg=
*****
```

2. このチャレンジを Cisco TAC と共有します。

生成されたチャレンジ文字列を Cisco TAC チームに送信します。TAC エンジニアは、要求と承認を確認した後、対応する承認応答を提供します。

3. 応答を受け入れる

Cisco TAC から受け入れ応答を受信したら、次のコマンドを使用して適用します。

```
ciscoasa# consent-token accept-response shell-access
```

プロンプトが表示されたら、制限時間内で受け入れ応答を貼り付けます。

```
Please input the response within 37 seconds when you are ready .....
/CYANQAAAQYBAAQAAAABAgAEAAAAAAMBYkFrdDkydBUMXlCMStNSWNlMElteUJ6VzhRMVViv05NSX$
Response Signature Verified successfully !
```

検証が成功すると、ルートシェルがコンソール端末で開きます。



重要 安全でシームレスな運用のために、すべての Consent Token 交換が Cisco TAC チームと調整され、実行されていることを確認します。

テストおよびトラブルシューティングの履歴

| 機能名 | プラットフォームリリース | 説明 |
|-------------------------------------|--------------|---|
| tracerouteのIPv6サポート | 9.7(1) | traceroute コマンドが変更され、IPv6 実行されるようになりました。 次の画面が変更されました。[Tools] > [Tools] |
| ブリッジグループメンバーインターフェイス用のパケットトレーサのサポート | 9.7(1) | ブリッジグループメンバーインターフェイスのパケットトレーサを使用できるようになりました。 パケットトレーサの画面に[VLAN ID]および[MAC Address]フィールドが追加されました。 [Packet Tracer] |
| 手動によるパケットキャプチャの開始と停止 | 9.7(1) | キャプチャを手動で停止および開始できるようにしました。 追加/変更された画面：[Wizards] > [Packet Tracer Wizard] > [Run Captures] 追加/変更されたオプション：[Start] ボタン |

| 機能名 | プラットフォームリリース | 説明 |
|-----------------------------|--------------|--|
| 強化されたパケットトレーサおよびパケットキャプチャ機能 | 9.9(1) | <p>パケット トレーサは次の機能で強化されました。</p> <ul style="list-style-type: none"> • パケットがクラスタユニット間を通過するパケットを追跡します。 • シミュレートされたパケットが ASA から通過するようにします。 • シミュレートされたパケットのセキュリティチェックをバイパスします。 • シミュレートされたパケットを IPsec/SSL によって暗号化されたパケットとして扱います。 <p>パケット キャプチャは次の機能で強化されました。</p> <ul style="list-style-type: none"> • パケットを復号化した後にキャプチャします。 • トレースをキャプチャし、永続リストに追加します。 <p>新規または変更された画面：</p> <p>[Tools] > [Packet Tracer]</p> <p>次のオプションをサポートする [Cluster Capture] ツールを追加しました：[decrypted]、[persist]、[bypass-checks]、[transmit]</p> <p>[All Sessions] ドロップダウンリストの下で [Sessions] ビューに 2 つの新しいオプションを追加しました：[Origin] および [Origin-ID]</p> <p>[Monitoring] > [VPN] > [VPN Statistics] > [Packet Capture and Capture]</p> <p>[Packet Capture Wizard] 画面に [ICMP Capture] ツールを追加しました：[Wizards] > [Packet Capture Wizard]</p> <p>ICMP キャプチャをサポートする 2 つのオプション include-decrypted および persist を追加しました。</p> |

| 機能名 | プラットフォームリリース | 説明 |
|--|--------------|---|
| ACL を使用せず IPv6 トラフィックを一致させるためのパケットキャプチャのサポート | 9.10(1) | <p>capture コマンドの match キーワードを伴った any キーワードは IPv4 トラフィックのみをキャプチャし、IPv4 または IPv6 トラフィックをキャプチャするには any4 と any6 キーワードを指定する必要があります。any キーワードでは、引き続き IPv4 トラフィックのみが一致されます。</p> <p>新規/変更されたコマンド：capture match any</p> <p>ASDM サポートはありません。</p> |
| Forepower 9300/4100 の新しい debug telemetry コマンド | 9.14(1) | <p>debug telemetry コマンドを使用すると、関連するデバッグメッセージが表示されませんが、テレメトリレポートの生成時にエラーを発生させるために役立ちます。</p> <p>変更された画面はありません。</p> |
| ping コマンドの変更 | 9.18(2) | <p>ループバック インターフェイスの ping コマンドのために、ping コマンドの動作が変更され、指定されたインターフェイスでインターフェイスを指定する場合、指定されたインターフェイスの IP アドレスが使用されます。ただし、実際の出カインターフェイスはルーティングテーブルを使用したルートルックアップで決定されます。</p> <p>新規/変更されたコマンド：ping</p> |
| スイッチのパケットキャプチャ | 9.20(1) | <p>スイッチの出力および入力トラフィックをキャプチャするように設定できるようになりました。この機能は、Secure Firewall 4200 モデルでのみ使用できます。</p> <p>新規/変更された画面：[ウィザード (Wizard)]>[パケットキャプチャ ウィザード (Packet Capture Wizard)]>[入力トラフィックセレクタ (Ingress Traffic Selector)]および[ウィザード (Wizard)]>[パケットキャプチャ ウィザード (Packet Capture Wizard)]>[出力トラフィックセレクタ (Egress Traffic Selector)]</p> |
| ASA Virtual での同意トークンを使用したルートシェルアクセスのサポート | 9.24(1) | <p>ASA Virtual は、承認ユーザーが管理者パトロール、トラブルシューティングまたは診断の目的でルートシェルにワンタイムアクセスできるように同意トークンメカニズムをサポートしました。</p> <p>変更された画面はありません。</p> |

翻訳について

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

翻訳について

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