CHAPTER 13

インターフェイスのライブ トラフィックの表示とキャプチャ

（注） 現在、Cisco IPS 7.1 をサポートしているプラットフォームは、IPS SSP を搭載した Cisco ASA 5585-X のみです。それ以外の Cisco IPS センサーは、IPS 7.1 を現在サポートしていません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降でサポートされています。ASA 8.3(*x*) ではサポートされていません。

この章では、パケット ファイルを表示、キャプチャ、コピー、消去する方法について説明します。次のような構成になっています。

パケットの表示とキャプチャについて

インターフェイスのライブ トラフィックを表示またはキャプチャし、そのライブ トラフィックや以前にキャプチャされたファイルを画面に直接表示することができます。ストレージは 1 つのローカル ファイルのみに使用でき、後続のキャプチャ要求によって既存のファイルは上書きされます。ストレージ ファイルのサイズはプラットフォームによって異なります。要求された数のパケットがキャプチャされる前に最大ファイル サイズに達すると、メッセージが表示される場合があります。

（注） インターフェイスからライブ トラフィックをキャプチャしても、センサーの機能は中断されません。

注意 インターフェイスの設定を変更すると、そのインターフェイスで実行されている **packet** コマンドが異常終了します。

注意　**packet display** または **capture** コマンドを実行すると、パフォーマンスが大幅に低下します。

インターフェイスのライブ トラフィックの表示

packet display *interface_name* [**snaplen** *length*] [**count** *count*] [**verbose**] [**expression** *expression*] コマンドを使用して、インターフェイスのライブ トラフィックを画面に直接表示します。

（注）　ライブ表示を終了するには、Ctrl キーを押した状態で C キーを押します。

オプション

次のオプションが適用されます。

- *interface_name*：インターフェイス名、インターフェイス タイプ（GigabitEthernet、FastEthernet、Management）、スロット/ポートの順に指定します。システムに存在するインターフェイス名だけを使用できます。
- **snaplen**：（任意）キャプチャする各パケットの最大バイト数を指定します。有効な範囲は 68 ～ 1600 です。デフォルトは 0 です。0 の値は、パケット全体をキャプチャするために必要な長さを使用することを意味します。
- **count**：（任意）キャプチャするパケットの最大数を指定します。有効な範囲は 1 ～ 10000 です。

  （注）　このオプションを指定しない場合、最大ファイル サイズまでキャプチャされるとキャプチャは停止します。

- **verbose**：（任意）1 行のサマリーではなく、各パケットのプロトコル ツリーを表示します。
- **expression**：パケット表示フィルタの式を指定します。この式は TCPDUMP に直接渡されるので、TCPDUMP 式の構文に従う必要があります。

  （注）　式の構文については、TCPDUMP の man ページで説明されています。

- **file-info**：保存されたパケット ファイルに関する情報を表示します。

  file-info で表示される情報は次のとおりです。

  Captured by: *user:id*, Cmd: *cliCmd*

  Start: yyyy/mm/dd hh:mm:ss zone, End: yyyy/mm/dd hh:mm:ss zone or in-progress

  ここで

  user = キャプチャを開始するユーザのユーザ名

  id = ユーザの CLI ID

  cliCmd = キャプチャを実行するために入力されたコマンド

注意　**packet display** コマンドを実行すると、パフォーマンスが大幅に低下します。

インターフェイスのライブ トラフィックの表示

インターフェイスのライブ トラフィックを画面に表示するようにセンサーを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用してセンサーにログインします。

ステップ 2　PortChannel0/0 など、目的のインターフェイスのライブ トラフィックを表示します。

```
ips-ssp# packet display PortChannel0/0
Warning: This command will cause significant performance degradation
tcpdump: listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes
03:43:05.691883 IP (tos 0x10, ttl  64, id 55460, offset 0, flags [DF], length: 100)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 4233955485:4233955533(48) ack
1495691730 win 8576 <nop,nop,timestamp 44085169 226014949>
03:43:05.691975 IP (tos 0x10, ttl  64, id 55461, offset 0, flags [DF], length: 164)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 48:160(112) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.691998 IP (tos 0x10, ttl  64, id 53735, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 48 win 11704
<nop,nop,timestamp 226014949 44085169>
03:43:05.693165 IP (tos 0x10, ttl  64, id 53736, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 160 win 11704
<nop,nop,timestamp 226014949 44085169>
03:43:05.693351 IP (tos 0x10, ttl  64, id 55462, offset 0, flags [DF], length: 316)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 160:424(264) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.693493 IP (tos 0x10, ttl  64, id 55463, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 424:664(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.693612 IP (tos 0x10, ttl  64, id 55464, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 664:904(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.693628 IP (tos 0x10, ttl  64, id 53737, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 424 win 11704
<nop,nop,timestamp 226014949 44085169>
03:43:05.693654 IP (tos 0x10, ttl  64, id 53738, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 664 win 11704
<nop,nop,timestamp 226014949 44085169>
03:43:05.693926 IP (tos 0x10, ttl  64, id 55465, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 904:1144(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.694043 IP (tos 0x10, ttl  64, id 55466, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 1144:1384(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.694163 IP (tos 0x10, ttl  64, id 55467, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 1384:1624(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.694209 IP (tos 0x10, ttl  64, id 53739, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 1384 win 11704
<nop,nop,timestamp 226014950 44085169>
03:43:05.694283 IP (tos 0x10, ttl  64, id 55468, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 1624:1864(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014950>
03:43:05.694402 IP (tos 0x10, ttl  64, id 55469, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 1864:2104(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014950>
03:43:05.694521 IP (tos 0x10, ttl  64, id 55470, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 2104:2344(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014950>
03:43:05.694690 IP (tos 0x10, ttl  64, id 53740, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 2344 win 11704
<nop,nop,timestamp 226014950 44085169>
```

```
03:43:05.694808 IP (tos 0x10, ttl  64, id 55471, offset 0, flags [DF], length: 300)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 2344:2592(248) ack 1 win 8576
<nop,nop,timestamp 44085169 226014950>
```

ステップ 3　**expression** オプションを使用すると、表示内容を制限できます。たとえば、TCP パケットだけを表示することができます。

（注）　TCPDUMP の man ページで説明されているとおり、プロトコル識別子 tcp、udp、および icmp はキーワードでもあるため、2 つのバック スラッシュ（\\）を使用してエスケープする必要があります。

```
ips-ssp# packet display PortChannel0/1 verbose expression ip proto \\tcp
Warning: This command will cause significant performance degradation
tcpdump: listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes
03:42:02.509738 IP (tos 0x10, ttl  64, id 27743, offset 0, flags [DF], length: 88)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 3449098782:3449098830(48) ack
3009767154 win 8704
03:42:02.509834 IP (tos 0x10, ttl  64, id 27744, offset 0, flags [DF], length: 152)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 48:160(112) ack 1 win 8704
03:42:02.510248 IP (tos 0x0, ttl 252, id 55922, offset 0, flags [none], length: 40)
64.101.182.54.47039 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 160 win 8760
03:42:02.511262 IP (tos 0x10, ttl  64, id 27745, offset 0, flags [DF], length: 264)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 160:384(224) ack 1 win 8704
03:42:02.511408 IP (tos 0x10, ttl  64, id 27746, offset 0, flags [DF], length: 248)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 384:592(208) ack 1 win 8704
03:42:02.511545 IP (tos 0x10, ttl  64, id 27747, offset 0, flags [DF], length: 240)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 592:792(200) ack 1 win 8704
```

ステップ 4　パケット ファイルに関する情報を表示します。

```
ips-ssp# packet display file-info
Captured by: cisco:25579, Cmd: packet capture PortChannel0/1
Start: 2010/02/03 02:56:48 UTC, End: 2010/02/03 02:56:51 UTC
ips-ssp#
```

インターフェイスのライブ トラフィックのキャプチャ

packet capture *interface_name* [**snaplen** *length*] [**count** *count*] [**expression** *expression*] コマンドを使用して、インターフェイスのライブ トラフィックをキャプチャします。**packet capture** コマンドを使用できるのは、一度に 1 ユーザだけです。2 番めのユーザ要求が発行されるとエラー メッセージが表示され、現在キャプチャを実行しているユーザに関する情報が示されます。

注意　**packet capture** コマンドを実行すると、パフォーマンスが大幅に低下します。

packet capture コマンドでは、libpcap 出力をローカル ファイルにキャプチャします。**packet display packet-file** [**verbose**] [**expression** *expression*] コマンドを使用して、このローカル ファイルを表示します。ローカル ファイルに関する情報がある場合は、**packet display file-info** を使用して表示できます。

オプション

次のオプションが適用されます。

- *interface_name*：論理インターフェイス名を指定します。システムに存在するインターフェイス名だけを使用できます。
- **snaplen**：キャプチャする各パケットの最大バイト数を指定します（任意）。有効な範囲は 68 ～ 1600 です。デフォルトは 0 です。
- **count**：キャプチャするパケットの最大数を指定します（任意）。有効な範囲は 1 ～ 10000 です。

（注）　このオプションを指定しない場合、最大ファイル サイズまでキャプチャされるとキャプチャは停止します。

- **expression**—パケット キャプチャ フィルタの式を指定します。この式は TCPDUMP に直接渡されるので、TCPDUMP 式の構文に従う必要があります。
- **file-info**：保存されたパケット ファイルに関する情報を表示します。

  file-info で表示される情報は次のとおりです。

  Captured by: *user:id*, Cmd: *cliCmd*

  Start: yyyy/mm/dd hh:mm:ss zone, End: yyyy/mm/dd hh:mm:ss zone or in-progress

  ここで

  user = キャプチャを開始するユーザのユーザ名

  id = ユーザの CLI ID

  cliCmd = キャプチャを実行するために入力されたコマンド
- **verbose**：1 行のサマリーではなく、各パケットのプロトコル ツリーを表示します。このパラメータはオプションです。

インターフェイスのライブ トラフィックのキャプチャ

インターフェイスのライブ トラフィックをキャプチャするようにセンサーを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用してセンサーにログインします。

ステップ 2　PortChannel0/0 など、目的のインターフェイスのライブ トラフィックをキャプチャします。

```
ips-ssp# packet capture PortChannel0/0
Warning: This command will cause significant performance degradation
tcpdump: WARNING: ge0_1: no IPv4 address assigned
tcpdump: listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes
125 packets captured
126 packets received by filter
0 packets dropped by kernel
```

ステップ 3　キャプチャされたパケット ファイルを表示します。

```
ips-ssp# packet display packet-file
reading from file /usr/cids/idsRoot/var/packet-file, link-type EN10MB (Ethernet)
03:03:13.216768 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:13.232881 IP 64.101.182.244.1978 > 192.0.2.3.23: . ack 3266153791 win
64328
03:03:13.232895 IP 192.0.2.3.23 > 64.101.182.244.1978: P 1:157(156) ack 0 wi
n 5840
```

```
03:03:13.433136 IP 64.101.182.244.1978 > 192.0.2.3.23: . ack 157 win 65535
03:03:13.518335 IP 10.89.130.134.42342 > 255.255.255.255.42342: UDP, length: 76
03:03:15.218814 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:15.546866 IP 64.101.182.244.1978 > 192.0.2.3.23: P 0:2(2) ack 157 win
65535
03:03:15.546923 IP 192.0.2.3.23 > 64.101.182.244.1978: P 157:159(2) ack 2 wi
n 5840
03:03:15.736377 IP 64.101.182.244.1978 > 192.0.2.3.23: . ack 159 win 65533
03:03:17.219612 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:19.218535 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:19.843658 IP 64.101.182.143.3262 > 10.89.130.23.445: P 3749577803:37495778
56(53) ack 3040953472 win 64407
03:03:20.174835 IP 161.44.55.250.1720 > 10.89.130.60.445: S 3147454533:314745453
3(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:21.219958 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:21.508907 IP 161.44.55.250.1809 > 10.89.130.61.445: S 3152179859:315217985
9(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:23.221004 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:23.688099 IP 161.44.55.250.1975 > 10.89.130.63.445: S 3160484670:316048467
0(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:25.219054 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:25.846552 IP 172.20.12.10.2984 > 10.89.130.127.445: S 1345848756:134584875
6(0) win 64240 <mss 1460,nop,nop,sackOK>
03:03:26.195342 IP 161.44.55.250.2178 > 10.89.130.65.445: S 3170518052:317051805
2(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:27.222725 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:27.299178 IP 161.44.55.250.2269 > 10.89.130.66.445: S 3174717959:317471795
9(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:27.308798 arp who-has 161.44.55.250 tell 10.89.130.66
03:03:28.383028 IP 161.44.55.250.2349 > 10.89.130.67.445: S 3178636061:317863606
1(0) win 65520 <mss 1260,nop,nop,sackOK>
--MORE--
```

ステップ 4　パケット ファイルに関する情報を表示します。

```
ips-ssp# packet display file-info
Captured by: cisco:8874, Cmd: packet capture PortChannel0/0
Start: 2010/01/07 00:12:50 UTC, End: 2010/01/07 00:15:30 UTC
ips-ssp#
```

パケット ファイルのコピー

copy packet-file *destination_url* コマンドを使用してパケット ファイルを FTP または SCP サーバにコピーし、そのファイルを保存したり Wireshark や TCPDUMP など他のツールを使って解析したりします。

オプション

次のオプションが適用されます。

- **packet-file**：**packet capture** コマンドを使用してキャプチャし、ローカルに保存された libpcap ファイルを指定します。
- *destination_url*：コピー先ファイルの場所を指定します。URL またはキーワードを使用できます。

（注） コピー元およびコピー先 URL の正確な形式は、ファイルによって異なります。

  - ftp:：FTP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、次のとおりです。

    ftp:[//[username@] location]/relativeDirectory]/filename

    ftp:[//[username@]location]//absoluteDirectory]/filename
  - scp:：SCP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、次のとおりです。

    scp:[//[username@] location]/relativeDirectory]/filename

    scp:[//[username@] location]//absoluteDirectory]/filename

（注） FTP または SCP プロトコルを使用すると、パスワードの入力を求められます。

パケット ファイルのコピー

パケット ファイルを FTP または SCP サーバにコピーするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　パケット ファイルを FTP または SCP サーバにコピーします。

```
ips-ssp# copy packet-file scp://jbrown@209.165.200.225/work/
Password: *********
packet-file               100% 1670     0.0KB/s   00:00
ips-ssp#
```

ステップ 3　Wireshark または TCPDUMP を使用してパケット ファイルを表示します。

パケット ファイルの消去

erase packet-file コマンドを使用してパケット ファイルを消去します。パケット ファイルは 1 つしかありません。サイズは 16 MB で、**packet capture** コマンドが実行されるたびに上書きされます。

パケット ファイルを消去するには、次の手順を実行します。

ステップ 1　現在キャプチャされているパケット ファイルに関する情報を表示します。

```
ips-ssp# packet display file-info
Captured by: cisco:1514, Cmd: packet capture GigabitEthernet0/1
Start: 2005/02/15 03:55:00 CST, End: 2005/02/15 03:55:05 CST
ips-ssp#
```

ステップ 2　パケット ファイルを消去します。

```
ips-ssp# erase packet-file
ips-ssp#
```

ステップ 3　パケット ファイルが消去されたことを確認します。

```
ips-ssp# packet display file-info
No packet-file available.
ips-ssp#
```