CHAPTER 12

IP ロギングの設定

（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、センサーで IP ロギングを設定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。

IP ロギングについて

IP アドレスで指定したホストに関連するすべての IP トラフィックをキャプチャするように、手動でセンサーを設定できます。IP トラフィックをログに記録する期間、および記録するパケット数とバイト数を指定できます。指定したパラメータが 1 つでも該当した時点で、センサーは IP トラフィックのロギングを停止します。

また、特定のシグニチャが起動するたびに IP パケットを記録するように、センサーを設定することもできます。センサーが IP トラフィックをログに記録する期間、および記録するパケット数とバイト数を指定できます。

注意 IP ロギングをイネーブルにすると、システム パフォーマンスは低下します。

（注） IP ログ ファイルを削除したり管理することはできません。**no iplog** コマンドでは、IP ログは削除されません。その IP ログへのパケットの記録が停止されるだけです。IP ログは循環バッファに格納されます。古い IP ログは新しい IP ログによって上書きされるので、循環バッファがいっぱいになることはありません。

センサーから IP ログをコピーし、libpcap 形式のパケット ファイルを読み取りできる Wireshark や TCPDUMP などのツールでそれらのログを解析できます。

（注） 各アラートは、そのアラートが原因となって作成された IP ログを参照します。複数のアラートによって同一の IP アドレスに関する IP ログが作成された場合は、それらすべてのアラートに対して IP ログが 1 つだけ作成されます。各アラートは同じ IP ログを参照します。ただし IP ログ ステータスの出力には、その IP ログをトリガーした最初のアラートのイベント ID だけが表示されます。

自動 IP ロギングの設定

ip-log-packets *number*、**ip-log-time** *number*、および **ip-log-bytes** *number* コマンドを使用して、センサーに自動 IP ロギング パラメータを設定します。

オプション

次のオプションが適用されます。

- **ip-log-packets**：ログに記録するパケットの数を指定します。有効な値は 0 ～ 65535 です。デフォルトは 0 です。
- **ip-log-time**：センサーでパケットを記録する期間を指定します。有効な値は 0 ～ 65535 分です。デフォルトは 30 分です。
- **ip-log-bytes**：ログに記録する最大バイト数を指定します。有効な値は 0 ～ 2147483647 です。デフォルトは 0 です。
- **default**：パラメータをリセットします。

（注） 自動 IP ログは、これらいずれかのパラメータに達するまでパケットのキャプチャを継続します。

自動 IP ロギングはシグニチャ単位で、またはイベント アクション オーバーライドとして設定されます。自動 IP ロギングをトリガーするアクションは次のとおりです。

- log-attacker-packets
- log-victim-packets
- log-pair-packets

自動 IP ロギングの設定

自動 IP ロギング 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　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 CLI にログインします。

ステップ 2　シグニチャ定義 IP ログ コンフィギュレーション サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig0
ips-ssp(config-sig)# ip-log
```

ステップ 3　センサーがログに記録するパケットの数を指定します。

```
ips-ssp(config-sig-ip)# ip-log-packets 200
```

ステップ 4　センサーがパケットを記録する期間を指定します。

```
ips-ssp(config-sig-ip)# ip-log-time 60
```

ステップ 5　記録するバイト数を指定します。

```
ips-ssp(config-sig-ip)# ip-log-bytes 5024
```

ステップ 6　設定を確認できます。

```
ips-ssp(config-sig-ip)# show settings
   ip-log
   -----------------------------------------------
      ip-log-packets: 200 default: 0
      ip-log-time: 60 default: 30
      ip-log-bytes: 5024 default: 0
   -----------------------------------------------
ips-ssp(config-sig-ip)#
```

ステップ 7　IP ロギング サブモードを終了します。

```
ips-ssp(config-sig-ip)# exit
ips-ssp(config-sig)# exit
Apply Changes?:[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- IP ログ ファイルをコピーおよび表示するには、「表示する IP ログ ファイルのコピー」（P.12-8）を参照してください。
- イベント アクションの詳細については、「シグニチャへのアクションの割り当て」（P.7-16）および「イベント アクション オーバーライドの設定」（P.8-16）を参照してください。

特定の IP アドレスに対する手動 IP ロギングの設定

iplog *name ip_address* [**duration** *minutes*] [**packets** *numPackets*] [**bytes** *numBytes*] コマンドを使用して、仮想センサーで特定の IP アドレスの IP パケットを手動で記録します。

オプション

次のオプションが適用されます。

- *name*：ロギングを開始および終了する仮想センサーを指定します。
- *ip_address*：指定された送信元 IP アドレスまたは宛て先 IP アドレス（あるいはその両方）が含まれたパケットをログに記録します。
- *minutes*：ロギングが動作する期間を指定します。有効な範囲は 1 ～ 60 分です。デフォルトは 10 分です。
- *numPackets*：記録するパケットの最大数を指定します。有効な範囲は 0 ～ 4294967295 です。デフォルトは 1000 パケットです。
- *numBytes*：記録する最大バイト数を指定します。有効な範囲は 0 ～ 4294967295 です。0 の値はバイト数が無制限であることを示します。

（注） *minutes*、n*umPackets*、*numBytes* パラメータは省略可能です。3 つすべてを指定する必要はありません。しかし、複数のパラメータを指定した場合、センサーは最初のしきい値に到達するまでロギングを続行します。たとえば、時間を 5 分に設定し、パケット数を 1000 に設定すると、センサーは 1000 番目のパケットがキャプチャされると、2 分しか経過していなくてもロギングを停止します。

手動 IP ロギングの設定

仮想センサーで特定の IP アドレスのパケットを手動で記録するには、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 CLI にログインします。

ステップ 2　特定の IP アドレスに対する IP ロギングを開始します。

```
ips-ssp# iplog vs0 192.0.2.1 duration 5
Logging started for virtual sensor vs0, IP address 192.0.2.1, Log ID 1
Warning: IP Logging will affect system performance.
ips-ssp#
```

この例で、センサーは IP アドレス 192.0.2.1 との間で送受信されるすべての IP パケットを 5 分間ログに記録しています。

（注） 後で参照するときのために、ログ ID はメモしておいてください。

ステップ 3　**iplog-status** コマンドを使用して IP ログのステータスをモニタします。

```
ips-ssp# iplog-status
Log ID:              1
IP Address 1:        192.0.2.1
Virtual Sensor:      vs0
Status:              added
Event ID:            0
Bytes Captured:      0
Packets Captured:    0
ips-ssp#
```

（注）　各アラートは、そのアラートが原因となって作成された IP ログを参照します。複数のアラートによって同一の IP アドレスに関する IP ログが作成された場合は、それらすべてのアラートに対して IP ログが 1 つだけ作成されます。各アラートは同じ IP ログを参照します。ただし IP ログ ステータスの出力には、その IP ログをトリガーした最初のアラートのイベント ID だけが表示されます。

詳細情報

- 特定の IP アドレスに関する IP パケットのロギングを停止するには、「動作している IP ログの停止」（P.12-6）を参照してください。
- IP パケットをシグニチャに関連付けられたイベントとしてログに記録するには、「自動 IP ロギングの設定」（P.12-2）を参照してください。
- IP ログ ファイルをコピーおよび表示するには、「表示する IP ログ ファイルのコピー」（P.12-8）を参照してください。

IP ログの内容の表示

iplog-status [**log-id** *log_id*] [**brief**] [**reverse**] [| {**begin** *regular_expression* | **exclude** *regular_expression* | **include** *regular_expression* }] コマンドを使用して、使用可能な IP ログの内容を表示します。

ログが作成されると、ステータスは `added` になります。最初のエントリがログに挿入されると、ステータスは `started` に変わります。パケット数の制限に達するなどしてログが完了すると、ステータスは `completed` に変わります。

オプション

次のオプションが適用されます。

- *log_id*：（任意）ステータスを表示したいファイルのログ ID を指定します。
- **brief**：（任意）各ログの IP ログ ステータス情報のサマリーを表示します。
- **reverse**：（任意）リストを逆の日付順で（最新のログから順に）表示します。
- |―：（任意）この後に出力処理の指定が続くことを示します。
- *regular_expression*：IP ログ ステータスの出力に含まれる正規表現。
- **begin**：**more** コマンドの出力を検索し、指定された文字列の最初のインスタンスからの出力を表示します。
- **exclude**：IP ログ ステータスの出力をフィルタリングし、特定の正規表現が含まれた行を除外します。
- **include**：IP ログ ステータスの出力をフィルタリングし、特定の正規表現が含まれた行を挿入します。

IP ログの表示

IP のログの内容を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　すべての IP ログのステータスを表示します。

```
ips-ssp# iplog-status
Log ID:                2425
```

```
IP Address 1:           192.0.2.1
Virtual Sensor:         vs0
Status:                 started
Start Time:             2003/07/30 18:24:18 2002/07/30 12:24:18 CST
Packets Captured:       1039438


Log ID:                 2342
IP Address 1:           192.0.2.10
IP Address 2:           192.0.2.20
Virtual Sensor:         vs0
Status:                 completed
Event ID:               209348
Start Time:             2003/07/30 18:24:18 2002/07/30 12:24:18 CST
End Time:               2003/07/30 18:34:18 2002/07/30 12:34:18 CST
sensor#
```

ステップ 3　すべての IP ログの簡単なリストを表示します。

```
ips-ssp# iplog-status brief
Log ID   VS    IP Address1   Status      Event ID   Start Date
2425     vs0   192.0.2.10    started     N/A        2003/07/30
2342     vs0   192.0.2.20    completed   209348     2003/07/30
ips-ssp#
```

動作している IP ログの停止

no iplog [**log-id** *log_id* | **name** *name*] コマンドを使用して、`started` 状態のログの記録を停止し、`added` 状態のログを削除します。

（注）　added 状態の IP ログで **no iplog** コマンドを使用すると、IP ログが停止します。added 状態は、IP ログがまだ空である（パケットがない）ことを示しています。パケットがない状態での停止は、空の IP ログを停止することを意味します。空の IP ログは、停止の際に削除されます。

（注）　**no iplog** コマンドでは、IP ログは削除されません。このコマンドは、その IP ログでそれ以上パケットをキャプチャしないようセンサーに通知するだけです。

オプション

次のオプションが適用されます。

- *log_id* : 停止するロギング セッションのログ ID。ログ ID を検索するには **iplog-status** コマンドを使用します。
- *name* : ロギングを開始または終了する仮想センサー。

IP ロギング セッションのディセーブル化

1 つまたはすべての IP ロギング セッ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　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 CLI にログインします。

ステップ 2　特定の IP ロギング セッションを停止します。

a. 停止するセッションのログ ID を検索します。

```
ips-ssp# iplog-status
Log ID:              1
IP Address 1:        192.0.2.1
Virtual Sensor:      vs0
Status:              added
Event ID:            0
Bytes Captured:      0
Packets Captured:    0
ips-ssp#
```

（注）　各アラートは、そのアラートが原因となって作成された IP ログを参照します。複数のアラートによって同一の IP アドレスに関する IP ログが作成された場合は、それらすべてのアラートに対して IP ログが 1 つだけ作成されます。各アラートは同じ IP ログを参照します。ただし IP ログ ステータスの出力には、その IP ログをトリガーした最初のアラートのイベント ID だけが表示されます。

b. IP ログ セッションを停止します。

```
ips-ssp# no iplog log-id 137857512
```

ステップ 3　仮想センサーでのすべての IP ロギング セッションを停止します。

```
ips-ssp# no iplog name vs0
```

ステップ 4　IP ロギングが停止されたことを確認します。ログが停止されると、completed ステータスが表示されます。

```
ips-ssp# iplog-status
Log ID:              1
IP Address 1:        192.0.2.1
Virtual Sensor:      vs0
Status:              completed
Event ID:            0
Bytes Captured:      0
Packets Captured:    0
ips-ssp#
```

表示する IP ログ ファイルのコピー

copy iplog *log_id destination_url* コマンドを使用して、IP ログを FTP または SCP サーバにコピーし、Ethereal や tcpdump などのスニフィング ツールで表示できるようにします。

オプション

次のオプションが適用されます。

- *log_id* : ロギング セッションのログ ID を指定します。ログ ID は **iplog-status** コマンドを使用して検索できます。
- *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。

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。有効なタイプは次のとおりです。

- 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

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。

IP ログ ファイルのコピー

IP ログ 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　CLI にログインします。

ステップ 2　コピーするログ ファイルのログ ID のステータスが completed になるまで、**iplog-status** コマンドを使用して IP ログ ステータスをモニタします。

```
ips-ssp# iplog-status
Log ID:              2425
IP Address:          192.0.2.1
Virtual Sensor:      vs0
Status:              started
Start Time:          2010/07/30 18:24:18 2002/07/30 12:24:18 CST
Packets Captured:    1039438

Log ID:              2342
IP Address:          192.0.2.2
Virtual Sensor:      vs0
Status:              completed
Event ID:            209348
Start Time:          2010/07/30 18:24:18 2002/07/30 12:24:18 CST
End Time:            2010/07/30 18:34:18 2002/07/30 12:34:18 CST
ips-ssp#
```

ステップ 3　IP ログを FTP または SCP サーバにコピーします。

```
ips-ssp# copy iplog 2342 ftp://root@209.165.200.225/user/iplog1
Password: ******** Connected to 209.165.200.225 (209.165.200.225). 220 linux.machine.com
FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30 :36 EST 2000) ready. ftp> user (username)
root 331 Password required for root. Password:230 User root logged in. ftp> 200 Type set
to I. ftp> put iplog.8518.tmp iplog1 local: iplog.8518.tmp remote: iplog1 227 Entering
Passive Mode (2,4,6,8,179,125) 150 Opening BINARY mode data connection for iplog1. 226
Transfer complete. 30650 bytes sent in 0.00246 secs (1.2e+04 Kbytes/sec) ftp>
```

ステップ 4　Wireshark や TCPDUMP などのスニファ プログラムを使用して IP ログを開きます。Wireshark の詳細については、http://www.wireshark.org を参照してください。TCPDUMP の詳細については、http://www.tcpdump.org/ 参照してください。