IP ロギングの設定

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。この章は、次の項で構成されています。

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付けられている IP トラフィックをすべて取り込むように、センサーを手動で設定することができます。IP トラフィックのログを記録する期間、記録する IP パケット数、および記録するバイト数を指定できます。センサーは、指定した最初のパラメータで 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反応するたびに、IP パケットをログに記録するようセンサーを設定することもできます。センサーで IP トラフィックのログを記録する期間、および記録する IP パケット数とバイト数を指定できます。

注意　IP ロギングをオンにすると、システムのパフォーマンスが低下します。

（注）　IP ログ ファイルは、削除したり、管理したりすることはできません。**no iplog** コマンドでは、該当の IP ログにそれ以上パケットが記録されないようになるだけで、IP ログは削除されません。IP ログは、一杯になることのない循環バッファに格納されます。これは、新しい IP ログが古いログを上書きするためです。

IP ログをセンサーからコピーして、libpcap 形式のパケット ファイルを読み取る Ethereal や tcpdump などのツールで分析することができます。

（注）　各アラートは、そのアラートのために作成された IP ログを参照します。複数のアラートにより同一の IP アドレスに対して IP ログが作成される場合は、すべてのアラートについて IP ログが 1 つだけ作成されます。各アラートは、同一の IP ログを参照します。しかし、IP ログ ステータスの出力は、IP ログをトリガーした最初のアラートのイベント ID だけを表示します。

自動 IP ロギングの設定

センサーで自動 IP ロギング パラメータを設定するには、**ip-log-packets** *number*、**ip-log-time** *number*、**ip-log-bytes** *number* の各コマンドを使用します。

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**：センサーでログ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。

（注）　自動 IP ログは、これらのパラメータのいずれかに達するまでパケットの取り込みを継続します。

パラメータをリセットするには、**default** キーワードを使用します。IP ログ ファイルのコピーと表示については、P.8-9 の「IP ログ ファイルのコピーと表示」を参照してください。

自動 IP ロギングは、シグニチャ単位で設定するか、イベント アクション オーバーライドとして設定します。自動 IP ロギングは、次のアクションによってトリガーされます。

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

詳細については、第 6 章「イベント アクション ルールの設定」を参照してください。

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　管理者特権またはオペレータ特権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 IP ログ コンフィギュレーション サブモードに入ります。

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

ステップ 3　センサーでログに記録するパケット数を設定します。

```
sensor(config-sig-ip)# ip-log-packets 200
```

ステップ 4　センサーでパケットをログに記録する期間を設定します。

```
sensor(config-sig-ip)# ip-log-time 60
```

ステップ 5　ログに記録するバイト数を設定します。

```
sensor(config-sig-ip)# ip-log-bytes 5024
```

ステップ 6　設定を確認します。

```
sensor(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
   -----------------------------------------------
sensor(config-sig-ip)#
```

ステップ 7　IP ロギング モードを終了します。

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

ステップ 8　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

特定の IP アドレスの手動 IP ロギングの設定

特定の IP アドレスの仮想センサーで IP パケットを手動でログに記録するには、**iplog** *name ip-address* [**duration** *minutes*] [**packets** *numPackets*] [**bytes** *numBytes*] コマンドを使用します。

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停止する仮想センサー。

（注）　IPS 5.0 バージョン 0 では仮想センサーは 1 つだけです。

- *ip-address*：指定された送信元 IP アドレスまたは宛先 IP アドレス（あるいはその両方）を含むパケットをログに記録します。
- *minutes*：ロギングをアクティブにする期間。
  有効な範囲は 1 ～ 60 分です。デフォルトは 10 分です。
- *numPackets*：ログに記録する最大パケット数。
  有効な範囲は 0 ～ 4294967295 です。デフォルトは 1000 パケットです。
- *numBytes*：ログに記録する最大バイト数。
  有効な範囲は 0 ～ 4294967295 です。値 0 はバイト数に制限がないことを示します。

（注）　*minutes*、*numPackets*、および *numBytes* の各パラメータはオプションです。3 つすべてを指定する必要はありません。ただし、2 つ以上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達するまでしかロギングを継続しません。たとえば、期間を 5 分、パケット数を 1000 と指定した場合、センサーは 2 分しか経過していなくても、1000 番目のパケットを取り込んだ後でロギングを停止します。

特定の IP アドレスの IP パケットのロギングを停止する場合は、P.8-7 の「アクティブな IP ログの停止」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場合は、P.8-3 の「自動 IP ロギングの設定」を参照してください。IP ログ ファイルのコピーと表示については、P.8-9 の「IP ログ ファイルのコピーと表示」を参照してください。

特定の IP アドレスの仮想センサーでパケットを手動でログに記録するには、次の 3 つの手順を実行します。

ステップ 1　管理者特権またはオペレータ特権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 アドレスの IP ロギングを開始します。

```
sensor# iplog vs0 10.16.0.0 duration 5
Logging started for virtual sensor vs0, IP address 10.16.0.0, Log ID 1
Warning: IP Logging will affect system performance.
sensor#
```

この例では、センサーが IP アドレス 10.16.0.0 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 をメモしておいてください。

ステップ 3　**iplog-status** コマンドで、IP ログのステータスを監視します。

```
sensor# iplog-status
Log ID:              1
IP Address 1:        10.16.0.0
Virtual Sensor:      vs0
Status:              added
Event ID:            0
Bytes Captured:      0
Packets Captured:    0
sensor#
```

（注）　各アラートは、そのアラートのために作成された IP ログを参照します。複数のアラートにより同一の IP アドレスに対して IP ログが作成される場合は、すべてのアラートについて IP ログが 1 つだけ作成されます。各アラートは、同一の IP ログを参照します。しかし、IP ログ ステータスの出力は、IP ログをトリガーした最初のアラートのイベント ID だけを表示します。

アクティブな IP ログの停止

started 状態のログのロギングを停止したり、added 状態のログを削除したりするには、**no iplog** [**log-id** *log-id* | **name** *name*] コマンドを使用します。

（注） added の状態の IP ログに対して **no iplog** コマンドを使用すると、IP ログが停止します。added の状態は、その IP ログが空のままである（パケットがない）ことを意味します。パケットが存在しない状態での停止は、空の IP ログの停止ということです。空のログは、停止すると削除されます。

（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、センサーに対してその IP ログでの追加パケットの取り込みを停止するようにシグナルを送信するだけです。

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停止する仮想センサー。

（注） IPS 5.0 バージョン 0 では仮想センサーは 1 つだけです。

1 つまたはすべての IP ロギング セッションを停止するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権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 セッションを停止するには、次の手順を実行します。

a. **iplog-status** コマンドを使用して、停止するセッションのログ ID を検索します。

```
sensor# iplog-status
Log ID:              1
IP Address 1:        10.16.0.0
Virtual Sensor:      vs0
Status:              added
Event ID:            0
Bytes Captured:      0
Packets Captured:    0
sensor#
```

（注） 各アラートは、そのアラートのために作成された IP ログを参照します。複数のアラートにより同一の IP アドレスに対して IP ログが作成される場合は、すべてのアラートについて IP ログが 1 つだけ作成されます。各アラートは、同一の IP ログを参照します。しかし、IP ログ ステータスの出力は、IP ログをトリガーした最初のアラートのイベント ID だけを表示します。

b. IP ログ セッションを停止します。

```
sensor# no iplog log-id 137857512
```

ステップ 3　仮想センサー上のすべての IP ロギング セッションを停止するには、次のコマンドを実行します。

```
sensor# no iplog name vs0
```

ステップ 4　IP ロギングが停止したことを確認します。

```
sensor# iplog-status
Log ID:              1
IP Address 1:        10.16.0.0
Virtual Sensor:      vs0
Status:              completed
Event ID:            0
Bytes Captured:      0
Packets Captured:    0
sensor#
```

ログが停止すると、ステータスに completed と表示されます。

IP ログ ファイルのコピーと表示

IP ログ ファイルを FTP サーバまたは SCP サーバにコピーして、Ethereal や tcpdump などのスニフィング ツールで表示できるようにするには、**copy iplog** *log-id destination-url* コマンドを使用します。

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。ログ ID は、**iplog-status** コマンドを使用して取得できます。
- *destination-url*：コピー先のファイルの場所。URL またはキーワードです。

コピー元およびコピー先の 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場合は、パスワードの入力を求められます。

IP ログ ファイルを FTP サーバまたは 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 と表示されるまで、**iplog-status** コマンドを使用して IP ログのステータスを監視します。

```
sensor# iplog-status
Log ID:              2425
IP Address:          10.1.1.2
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:          10.2.3.1
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　IP ログを FTP サーバまたは SCP サーバにコピーします。

```
sensor# copy iplog 2342 ftp://root@10.16.0.0/user/iplog1
Password: ******** Connected to 10.16.0.0 (10.16.0.0). 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　Ethereal 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。

Ethereal の詳細については、http://www.ethereal.com を参照してください。tcpdump の詳細については、http://www.tcpdump.org/ を参照してください。