CHAPTER 12

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手順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」（P.12-1）
- 「自動 IP ロギングの設定」（P.12-2）
- 「特定の IP アドレスに関する手動での IP ロギングの設定」（P.12-3）
- 「IP ログの内容の表示」（P.12-4）
- 「アクティブな IP ログの停止」（P.12-5）
- 「表示する IP ログ ファイルのコピー」（P.12-7）

IP ロギングについて

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

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。記録する IP トラフィックの期間、記録するパケット数、および記録する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、センサーが IP パケットを記録するようにすることもできます。センサーで、IP トラフィックを記録する期間、記録するパケット数とバイト数を指定できます。センサーから IP ログをコピーし、Wireshark または TCPDUMP など、libpcap 形式でパケット ファイルを読み取り可能なツールで分析できます。

（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。循環バッファは、新しい IP ログによって古いログが上書きされるので、いっぱいになることがありません。

（注） 各アラートは、そのアラートにより作成された IP ログを参照します。複数のアラートが同じ IP アドレスに対して IP ログを作成する場合、すべてのアラートに対して 1 つの IP ログだけが作成されます。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、IP ログをトリガーした最初のアラートのイベント ID だけが示されます。

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*, and **ip-log-bytes** *number* 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**：記録するパケット数を示します。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示します。有効な値は 0 ～ 65535 分です。デフォルトは 30 分です。
- **ip-log-bytes**：記録する最大バイト数を示します。有効な値は 0 ～ 2147483647 です。デフォルトは 0 です。

（注） 自動 IP ログでは、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が継続されます。

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。

自動 IP ロギングは、シグニチャごとに、またはイベント アクションのオーバーライドとして設定します。次のアクションによって、自動 IP ロギングがトリガーされます。

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

自動 IP ロギング パラメータを設定するには、次の手順に従います。

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。

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

ステップ 3　センサーで記録するパケット数を指定します。

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

ステップ 4　センサーでパケットを記録する期間を指定します。

```
sensor(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。

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

ステップ 6　設定を確認できます。

```
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 サブ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　Enter を押して変更を適用するか、**no** と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.12-7）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.8-15）および「イベント アクション オーバーライドの設定」（P.7-16）を参照してください。

特定の IP アドレスに関する手動での IP ロギングの設定

特定の IP アドレスに対して、仮想センサーで IP パケットを手動で記録するには、**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終了する仮想センサー。
- *ip_address*：指定した送信元/宛先 IP アドレスを含むパケットを記録します。
- *minutes*：ロギングをアクティブにする期間。指定できる範囲は 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。有効な範囲は 0 ～ 4294967295 です。デフォルトは 1000 パケットです。
- *numBytes*：記録するバイトの最大数。有効な範囲は 0 ～ 4294967295 です。値 0 は、バイト数を制限し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、3 つのパラメータ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。

指定した IP アドレスに対して、仮想センサーでパケットを手動で記録するには、次の手順に従います。

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 アドレスに関する 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#
```

この例は、IP アドレス 10.16.0.0 との間で送受信されるすべての IP パケットを 5 分間ログに記録するセンサーを示します。

（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** コマンドで IP ログのステータスをモニタします。

```
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、そのアラートにより作成された IP ログを参照します。複数のアラートが同じ IP アドレスに対して IP ログを作成する場合、すべてのアラートに対して 1 つの IP ログだけが作成されます。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、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、「アクティブな IP ログの停止」（P.12-5）を参照してください。
- IP パケットをシグニチャに関連したイベントとして記録するには、「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.12-7）を参照してください。

IP ログの内容の表示

使用可能な IP ログの内容について説明を表示するには、**iplog-status** [**log-id** *log_id*] [**brief**] [**reverse**] [| {**begin** *regular_expression* | **exclude** *regular_expression* | **include** *regular_expression* }] コマンドを使用します。

ログが作成されるときに、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た場合、ステータスは `started` に変化します。パケット数の制限などに達したため、ログが完了した場合、ステータスは `completed` に変わります。

次のオプションが適用されます。

- *log_id*：（任意）ステータスを確認するファイルのログ ID。
- **brief**：（任意）各ログに対して IP ログ ステータス情報の概要を表示します。
- **reverse**：（任意）発生の逆順（最新のログが先頭）でリストを表示します。
- |：（任意）そのあとに出力処理の指定が続くことを示します。
- *regular_expression*：IP ログ ステータス出力で検索するすべての正規表現。

- **begin**：**more** コマンドの出力を検索し、指定したストリングの最初のものから出力を表示します。
- **exclude**：特定の正規表現を含む行が除外されるように、IP ログ ステータス出力をフィルタリングします。
- **include**：特定の正規表現を含む行が含まれるように、IP ログ ステータス出力をフィルタリングします。

IP のログの内容を表示するには、次の手順に従います。

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。

```
sensor# iplog-status
Log ID:                 2425
IP Address 1:           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 1:           10.2.3.1
IP Address 2:           10.2.3.4
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。

```
sensor# iplog-status brief
Log ID   VS    IP Address1   Status      Event ID   Start Date
2425     vs0   10.1.1.2      started     N/A        2003/07/30
2342     vs0   10.2.3.1      completed   209348     2003/07/30
sensor#
```

アクティブな IP ログの停止

`started` 状態にあるログのロギングを停止し、`added` 状態にあるログを削除するには、**no iplog** [**log-id** *log_id* | **name** *name*] コマンドを使用します。**no iplog** コマンドによって、IP ログが消去または削除されることはありません。このコマンドは、その IP ログで追加のパケットのキャプチャを停止することをセンサーに指示するだけです。

（注）　added 状態の IP ログで **no iplog** コマンドを使用すると、IP ログが停止されます。added 状態は、IP ログがまだ空である（パケットがない）ことを示します。パケットがない場合に IP ログを停止すると、空の IP ログが停止されます。空のログは、停止したときに削除されます。

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 を調べるには、**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。

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 を調べます。

```
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、そのアラートにより作成された IP ログを参照します。複数のアラートが同じ IP アドレスに対して IP ログを作成する場合、すべてのアラートに対して 1 つの IP ログだけが作成されます。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、IP ログをトリガーした最初のアラートのイベント ID だけが示されます。

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　仮想センサーで、すべての IP ロギング セッションを停止します。

```
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#
```

ログが停止した場合、そのステータスは completed と表示されます。

表示する IP ログ ファイルのコピー

FTP サーバまたは SCP サーバに IP ログ ファイルをコピーし、Wireshark または 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。**iplog-status** コマンドを使用して、ログ ID を取得できます。
- *destination_url*：コピー先ファイルの場所。URL またはキーワードです。

コピー元およびコピー先の URL の形式は、ファイルによって変わります。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 です。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 です。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るプロンプトが表示されます。

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　**iplog-status** コマンドで IP ログ ステータスをモニタし、コピーするログ ファイルのログ ID のステータスが completed になるまで待ちます。

```
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 ログを目的の FTP 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　Wireshark や TCPDUMP などのスニフィング 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/ を参照してください。