CHAPTER 11

# センサーの監視

この章では、拒否された攻撃者リストを監視およびクリアする方法、アクティブなホスト ブロックとネットワーク ブロックを監視および設定する方法、レート制限を設定および管理する方法、IP ログを設定およびダウンロード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。

# 拒否された攻撃者

この項では、拒否された攻撃者を設定する方法について説明します。取り上げる事項は次のとおりです。



## 概要

Denied Attackers パネルに、拒否された攻撃者のすべての IP アドレスとヒット カウントが表示されます。すべての IP アドレスのヒット カウントをリセットしたり、拒否された攻撃者のリストをクリアしたりすることができます。

## サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

拒否された攻撃者のリストを監視およびクリアするには、管理者である必要があります。

## フィールド定義

Denied Attackers パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Attacker IP**：センサーが拒否している攻撃者の IP アドレス。
- **Victim IP**：センサーが拒否している被害先の IP アドレス。
- **Port**：センサーが拒否しているホストのポート。
- **Protocol**：攻撃者が使用しているプロトコル。
- **Percentage**：インライン モードでセンサーによって拒否されるトラフィックの率。
- **Hit Count**：拒否された攻撃者のヒット カウントを表示します。
- **Virtual Sensor**：仮想センサーの名前。現在、IPS 5.1 では 1 つの仮想センサー「vs0」だけをサポートしています。

ボタンの機能：

- **Reset All Hit Counts**：拒否された攻撃者のヒット カウントをクリアします。
- **Clear List**：拒否された攻撃者のリストをクリアします。
- **Refresh**：パネルの内容をリフレッシュします。

## 拒否された攻撃者リストの監視

拒否された攻撃者のリストとそれらのヒット カウントを表示するには、次の手順を実行します。

**ステップ 1**　管理者特権を持つアカウントを使用して IDM にログインします。

**ステップ 2**　**Monitoring > Denied Attackers** をクリックします。

Denied Attackers パネルが表示されます。

**ステップ 3**　**Refresh** をクリックして、リストをリフレッシュします。

**ステップ 4**　**Reset All Hit Counts** をクリックして、ヒット カウントを最初からやり直します。

**ステップ 5**　**Clear List** をクリックして、拒否された攻撃者のリスト全体をクリアします。

# アクティブなホスト ブロックの設定および管理

この項では、アクティブなホスト ブロックを管理する方法について説明します。取り上げる事項は次のとおりです。



## 概要

Active Host Blocks パネルで、ホストのブロッキングを設定および管理できます。

アクティブなホスト ブロックは、特定のホストからのトラフィックを（そのブロックを削除するまで）永続的にブロックするか、指定された期間ブロックします。宛先 IP アドレスと、宛先のプロトコルおよびポートを指定することにより、接続をベースにしたブロックを実行することもできます。

アクティブなホスト ブロックは、送信元 IP アドレスによって定義されます。既存のブロックと同じ送信元 IP アドレスを持つブロックを追加すると、新しいブロックによって古いブロックが上書きされます。

ブロックの期間を指定する場合は、値を 1 ～ 70560 分（49 日）の範囲にする必要があります。時間を指定しない場合、ホスト ブロックはセンサーがリブートされるかブロックが削除されるまで有効になります。

## サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

アクティブなホスト ブロックを設定するには、管理者またはオペレータである必要があります。

## フィールド定義

この項では、アクティブなホスト ブロックのフィールドの定義を示します。取り上げる事項は次のとおりです。



### Active Host Blocks パネル

Active Host Blocks パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Source IP**：ブロックの送信元 IP アドレス。
- **Destination IP**：ブロックの宛先 IP アドレス。
- **Destination Port**：ブロックの宛先ポート。

- **Protocol**：プロトコルのタイプ（TCP、UDP、または ANY）。
  デフォルトは ANY です。
- **Minutes Remaining**：ブロックの残り時間（分単位）。
- **Timeout (minutes)**：ブロックのオリジナルのタイムアウト値（分単位）。
  有効な値は 1 ～ 70560 分（49 日）です。
- **VLAN**：シグニチャを発生させたデータを伝送した VLAN を示します。

**注意**　ブロック要求に VLAN ID が含まれていても、その ID はファイアウォールに渡されません。管理コンテキストにログインしている場合、センサーは FWSM 2.1 以降ではブロックを実行できません。

- **Connection Block Enabled**：ホストへの接続をブロックするかどうか。

ボタンの機能：

- **Add**：Add Active Host Block ダイアログボックスを開きます。
  このダイアログボックスから、ホストの手動ブロックを追加できます。
- **Delete**：アクティブなホスト ブロックのリストから該当の手動ブロックを削除します。
- **Refresh**：テーブルの内容をリフレッシュします。

## Add Active Host Block ダイアログボックス

Add Active Host Block ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Source IP**：ブロックの送信元 IP アドレス。
- **Enable connection blocking**：ホストへの接続をブロックするかどうか。
- **Connection Blocking**：接続ブロッキングのパラメータを設定できます。
  - **Destination IP**：ブロックの宛先 IP アドレス。
  - **Destination Port**：（オプション）ブロックの宛先ポート。
  - **Protocol**：（オプション）プロトコルのタイプ（TCP、UDP、または ANY）。
    デフォルトは ANY です。
- **VLAN**：（オプション）シグニチャを発生させたデータを伝送した VLAN を示します。

**注意**　ブロック要求に VLAN ID が含まれていても、その ID はファイアウォールに渡されません。管理コンテキストにログインしている場合、センサーは FWSM 2.1 以降ではブロックを実行できません。

このフィールドはオプションです。

- **Enable Timeout**：ブロックのタイムアウト値（分単位）を設定できます。
- **Timeout**：ブロックを続ける時間（分単位）。
  有効な値は 1 ～ 70560 分（49 日）です。
- **No Timeout**：ブロックにタイムアウトを指定しません。

ボタンの機能：

- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

## アクティブなホスト ブロックの設定および管理

アクティブなホスト ブロックを設定および管理するには、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 IDM にログインします。

**ステップ 2**　**Monitoring > Active Host Blocks** をクリックします。

Active Host Blocks パネルが表示されます。

**ステップ 3**　**Add** をクリックして、アクティブなホスト ブロックを追加します。

Add Active Host Block ダイアログボックスが表示されます。

**ステップ 4**　ブロックするホストの送信元 IP アドレスを入力します。

**ステップ 5**　ブロックを接続ベースにする場合は、**Enable Connection Blocking** チェックボックスを選択します。

**（注）**　接続ブロックでは、特定の送信元 IP アドレスから特定の宛先 IP アドレスおよび宛先ポートへのトラフィックがブロックされます。

a. **Destination IP** フィールドに宛先 IP アドレスを入力します。
b. （オプション）**Destination Port** フィールドに宛先ポートを入力します。
c. **Protocol** リストからプロトコルを選択します。

**ステップ 6**　（オプション）**VLAN** フィールドに、接続ブロックの VLAN を入力します。

**ステップ 7**　ブロックに一定の時間を設定する場合は、**Enable Timeout** チェックボックスを選択します。

**ステップ 8**　**Timeout** フィールドに、時間（分単位）を入力します。

**ヒント**　変更を元に戻して Add Active Host Block ダイアログボックスを閉じるには、**Cancel** をクリックします。

**ステップ 9**　ブロックに一定の時間を設定しない場合は、**No Timeout** チェックボックスを選択します。

**ステップ 10**　**Apply** をクリックします。

その IP アドレスにブロックが設定されている場合は、エラー メッセージが発生します。

Active Host Blocks パネルのリストに新しいアクティブなホスト ブロックが表示されます。

**ステップ 11** **Refresh** をクリックして、アクティブなホスト ブロックのリストの内容をリフレッシュします。

**ステップ 12** ブロックを削除するには、リストでアクティブなホスト ブロックを選択して、**Delete** をクリックします。

Delete Active Host Block ダイアログボックスで、該当のブロックを本当に削除するかどうかをたずねられます。

**ヒント** 変更を元に戻して Delete Active Host Block ダイアログボックスを閉じるには、**Cancel** をクリックします。

**ステップ 13** **Yes** をクリックしてブロックを削除します。

# ネットワーク ブロックの設定および管理

この項では、ネットワーク ブロックを管理する方法について説明します。取り上げる事項は次のとおりです。



## 概要

Network Blocks パネルで、ネットワークのブロッキングを設定および管理できます。

ネットワーク ブロックは、特定のネットワークからのトラフィックを（そのブロックを削除するまで）恒常的にブロックするか、指定された期間ブロックします。

ネットワーク ブロックは、送信元 IP アドレスとネットマスクによって定義されます。ネットマスクは、ブロックされるサブネットを定義します。ホストのサブネット マスクも受け入れられます。

ブロックの期間を指定する場合は、値を 1 ～ 70560 分（49 日）の範囲にする必要があります。時間を指定しない場合、ブロックはセンサーがリブートされるかブロックが削除されるまで有効になります。

## サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

ネットワーク ブロックを設定するには、管理者またはオペレータである必要があります。

## フィールド定義

この項では、ネットワーク ブロックのフィールドの定義を示します。取り上げる事項は次のとおりです。



### Network Blocks パネル

Network Blocks パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：ブロックの IP アドレス。
- **Mask**：ブロックのネットワーク マスク
- **Minutes Remaining**：ブロックの残り時間（分単位）。
- **Timeout (minutes)**：ブロックのオリジナルのタイムアウト値（分単位）。
  有効な値は 1 ～ 70560 分（49 日）です。

ボタンの機能：

- **Add**：Add Network Block ダイアログボックスを表示します。
  このダイアログボックスから、ネットワークのブロックを追加できます。
- **Delete**：ブロックのリストから該当のネットワーク ブロックを削除します。
- **Refresh**：テーブルの内容をリフレッシュします。

### Add Network Block ダイアログボックス

Add Network Block ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Source IP：**ブロックの IP アドレス。
- **Netmask**：ブロックのネットワーク マスク。
- **Enable Timeout**：ブロックのタイムアウト値（分単位）を示します。
- **Timeout**：ブロックの期間（分単位）を示します。
  有効な値は 1 ～ 70560 分（49 日）です。
- **No Timeout**：ブロックにタイムアウトを指定しません。

ボタンの機能：

- **Apply**：該当のブロックをすぐにセンサーに送信します。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

## ネットワーク ブロックの設定および管理

ネットワーク ブロックを設定および管理するには、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 IDM にログインします。

**ステップ 2**　**Monitoring > Network Blocks** をクリックします。

Network Blocks パネルが表示されます。

**ステップ 3**　**Add** をクリックして、ネットワーク ブロックを追加します。

Add Network Block ダイアログボックスが表示されます。

**ステップ 4**　ブロックするネットワークの送信元 IP アドレスを入力します。

**ステップ 5**　**Netmask** リストからネットマスクを選択します。

**ステップ 6**　ブロックに一定の時間を設定する場合は、**Enable Timeout** チェックボックスを選択します。

**ステップ 7**　**Timeout** フィールドに、時間（分単位）を入力します。

**ヒント**　変更を元に戻して Add Network Block ダイアログボックスを閉じるには、**Cancel** をクリックします。

**ステップ 8**　**Apply** をクリックします。

ブロックがすでに追加されている場合は、エラー メッセージが発生します。

Network Blocks パネルのリストに新しいネットワーク ブロックが表示されます。

**ステップ 9**　**Refresh** をクリックして、ネットワーク ブロックのリストの内容をリフレッシュします。

**ステップ 10**　ブロックを削除するには、リストでネットワーク ブロックを選択して **Delete** をクリックします。

Delete Network Block ダイアログボックスで、該当のブロックを本当に削除するかどうかをたずねられます。

**ステップ 11**　**Yes** をクリックしてブロックを削除します。

# レート制限の設定および管理

この項では、レート制限とその設定方法について説明します。取り上げる事項は次のとおりです。



## 概要

レート制限を使用すると、センサーがネットワーク デバイス上の指定したトラフィック クラスのレートを制限します。レート制限の応答は、Host Flood エンジンと Net Flood エンジン、および TCP ハーフオープン SYN シグニチャに対してサポートされます。ARC は、Cisco IOS バージョン 12.3 以降を実行するネットワーク デバイスでレート制限を設定することができます。ルータでのレート制限の設定については、P.8-27 の「ルータのブロッキングまたはレート制限のデバイス インターフェイスの設定」を参照してください。マスター ブロッキング センサーは、レート制限要求をブロッキング転送センサーに転送することもできます。詳細については、P.8-37 の「マスター ブロッキング センサーの設定」を参照してください。

アクティブなレート制限のリストは、ARC の統計情報で確認できます。詳細については、P.10-14 の「統計情報の表示」を参照してください。

レート制限を追加するには、プロトコル、宛先 IP アドレス、およびレート制限イベントの生成が可能なシグニチャのいずれかに一致するデータ値の組み合せを指定します。手順については、P.11-13 の「レート制限の設定および管理」を参照してください。また、アクションを Request Rate Limit に設定し、さらにこれらのシグニチャの率を設定する必要があります。表 11-1 に、サポートされているシグニチャとパラメータを示します。

**表 11-1　レート制限のシグニチャ**

| シグニチャ ID | シグニチャ名 | プロトコル | 許可される宛先 IP アドレス | データ |
|---|---|---|---|---|
| 2152 | ICMP Flood Host | ICMP | ○ | echo-request |
| 2153 | ICMP Smurf Attack | ICMP | ○ | echo-reply |
| 4002 | UDP Flood Host | UDP | ○ | なし |
| 6901 | Net Flood ICMP Reply | ICMP | × | echo-reply |
| 6902 | Net Flood ICMP Request | ICMP | × | echo-request |
| 6903 | Net Flood ICMP Any | ICMP | × | なし |
| 6910 | Net Flood UDP | UDP | × | なし |
| 6920 | Net Flood TCP | TCP | × | なし |
| 3050 | TCP HalfOpenSyn | TCP | × | halfOpenSyn |

## サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

レート制限を設定するには、管理者またはオペレータである必要があります。

# フィールド定義

この項では、レート制限のフィールドの定義を示します。取り上げる事項は次のとおりです。



## Rate Limits パネル

Rate Limits パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Protocol**：レートを制限するトラフィックのプロトコル。
- **Rate**：レート制限されたトラフィックに許可された、帯域幅の最大容量に対する率。
  この率を超えて一致したトラフィックはドロップされます。
- **Source IP**：（オプション）レート制限されたトラフィックの送信元ホストの IP アドレス。
- **Source Port**：（オプション）レート制限されたトラフィックの送信元ホストのポート。
- **Destination IP**：レート制限されたトラフィックの宛先ホストの IP アドレス。
- **Destination Port**：（オプション）レート制限されたトラフィックの宛先ホストのポート。
- **Data**：（オプション）特定のプロトコルのトラフィックをさらに正確に限定するために必要な追加の識別情報。
  たとえば、echo-request の場合、ICMP プロトコルのトラフィックはレート制限の ping に絞られます。
- **Minutes Remaining**：該当のレート制限が有効である残り時間（分単位）。
- **Timeout (minutes)**：該当のレート制限の合計時間（分単位）。

ボタンの機能：

- **Add**：Add Rate Limit ダイアログボックスを表示します。
  このダイアログボックスから、レート制限のオプションを設定できます。
- **Delete**：テーブルから該当エントリを削除します。
- **Refresh**：テーブルの内容をリフレッシュします。

## Add Rate Limit ダイアログボックス

Add Rate Limit ダイアログボックスには次のフィールドとボタンがあります。

フィールドの説明：

- **Protocol**：レート制限されたトラフィックのプロトコル（ICMP、TCP、または UDP）。
- **Rate**：レート制限されたトラフィックに許可された、帯域幅の最大容量に対する率。
- **Source IP**：（オプション）レート制限されたトラフィックの送信元ホストの IP アドレス。
- **Source Port**：（オプション）レート制限されたトラフィックの送信元ホストのポート。
- **Destination IP**：（オプション）レート制限されたトラフィックの宛先ホストの IP アドレス。
- **Destination Port**：（オプション）レート制限されたトラフィックの宛先ホストのポート。
- **Use Additional Data**：（オプション）echo-reply、echo-request、halfOpenSyn などの追加データを指定するかどうかを選択できます。
- **Timeout**：タイムアウトをイネーブルにするかどうかを選択できます。
  - **No Timeout**：タイムアウトをイネーブルにしません。
  - **Enable Timeout**：タイムアウト（分単位）を指定できます（1 ～ 70560）。

ボタンの機能：

- **Apply**：変更を適用してダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

## レート制限の設定および管理

レート制限を設定および管理するには、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 IDM にログインします。

**ステップ 2**　**Monitoring > Rate Limits** をクリックします。

Rate Limits パネルが表示されます。

**ステップ 3**　**Add** をクリックして、レート制限を追加します。

Add Rate Limit ダイアログボックスが表示されます。

**ステップ 4**　レートを制限するトラフィックのプロトコル（ICMP、TCP、または UDP）を **Protocol** リストから選択します。

**ステップ 5**　**Rate** フィールドにレート制限（1 ～ 100）を入力します。

**ステップ 6**　（オプション）**Destination IP** フィールドに宛先 IP アドレスを入力します。

**ステップ 7**　レート制限で追加データを使用するように設定する場合は、**Use Additional Data** チェックボックスを選択します。

**ステップ 8**　**Select Data** リストから、追加データ（echo-reply、echo-request、または halfOpenSyn）を選択します。

**ステップ 9**　タイムアウト（分単位）を設定する場合は、**Enable Timeout** チェックボックスを選択します。

**ステップ 10**　**Timeout** フィールドに、時間を分単位で入力します（1 ～ 70560）。

**ヒント**　変更を元に戻して Add Rate Limit ダイアログボックスを閉じるには、**Cancel** をクリックします。

**ステップ 11**　レート制限に一定の時間を設定しない場合は、**No Timeout** チェックボックスを選択します。

**ステップ 12**　**Apply** をクリックします。

Rate Limits パネルのリストに新しいレート制限が表示されます。

**ステップ 13**　**Refresh** をクリックして、Rate Limits リストの内容をリフレッシュします。

**ステップ 14** レート制限を削除するには、リストからレート制限を選択して、**Delete** をクリックします。

Delete Rate Limit ダイアログボックスで、該当のレート制限を本当に削除するかどうかをたずねられます。

**ヒント** **No** をクリックすると、Delete Rate Limit ダイアログボックスが閉じます。

**ステップ 15** **Yes** をクリックしてレート制限を削除します。

該当のレート制限はレート制限のリストに表示されなくなります。

# IP ロギングの設定

最も単純な IP ロギングは 1 つの IP アドレスから構成されます。IP アドレスで指定したホストに関連するすべての IP トラフィックを取り込むように、センサーを設定できます。センサーは、この IP アドレスを持つ最初の IP パケットを認識するとすぐに収集を開始し、設定されているパラメータに基づいて収集を継続します。その IP アドレスで IP トラフィックをログに記録する期間を分単位で指定することもできれば、ログに記録するパケット数、またはログに記録するバイト数を指定することもできます。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。

ログ ファイルは次の 3 つの状態のいずれかになります。

- Added：IP ロギングが追加された場合
- Started：センサーが最初のパケットを認識した時点で、ログ ファイルが開き Started 状態になります。
- Completed：IP ロギング制限に達した場合

3 つの状態すべてのファイル数は 20 までに制限されています。IP ログは循環バッファに保存されます。循環バッファでは、新しい IP ログが古い IP ログを上書きするため、いっぱいになることはありません。

**（注）** ログは、センサーがそれらを再要求するまでセンサー上に残ります。センサー上の IP ログ ファイルを管理することはできません。

IP ログ ファイルを Ethereal や TCP Dump などのスニフィング ツールで表示できるように、それらを FTP サーバまたは SCP サーバにコピーできます。ファイルは、PCAP バイナリ形式で保存され、pcap ファイル拡張子が付きます。

**注意** IP ロギングを有効にすると、システム パフォーマンスは低下します。

この項で取り上げる事項は次のとおりです。



## 概要

IP Logging パネルには、このシステムでダウンロードできるすべての IP ログが表示されます。

IP ログは、2 通りの方法で生成されます。

- Add IP Logging ダイアログボックスで IP ログを追加する場合
- シグニチャのイベント アクションとして次のいずれかを選択する場合
  - **Log Attacker Packets**
  - **Log Pair Packets**
  - **Log Victim Packets**

  このシグニチャに基づく攻撃をセンサーが検出したときに、IP ログが作成されます。IP ログをトリガーしたイベント アラートは、IP ロギング テーブルに表示されます。

## サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

IP ロギングを設定するには、管理者である必要があります。

## フィールド定義

この項では、IP ロギングのフィールドの定義を示します。取り上げる事項は次のとおりです。

- IP Logging パネル（P.11-16）
- Add and Edit IP Logging ダイアログボックス（P.11-17）

### IP Logging パネル

IP Logging パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Log ID**：IP ログの ID。
- **IP Address**：ログを取り込むホストの IP アドレス。
- **Status**：IP ログのステータス。
  有効な値は、added、started、または completed です。
- **Event Alert**：ある場合は IP ログをトリガーしたイベント アラート。
- **Start Time**：最初に取り込んだパケットのタイムスタンプ。
- **Current End Time**：最後に取り込んだパケットのタイムスタンプ。
  取り込みが完了していない場合は、タイムスタンプは表示されません。
- **Packets Captured**：現在の取り込んだパケット数。
- **Bytes Captured**：現在の取り込んだバイト数。

ボタンの機能：

- **Add**：Add IP Logging ダイアログボックスを表示します。
  このダイアログボックスで、IP ログを追加できます。
- **Edit**：Edit IP Logging ダイアログボックスを表示します。
  このダイアログボックスで、この IP ログに関連付けられた値を変更できます。
- **Download**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Stop**：開始した IP ログの取り込みを停止します。
- **Refresh**：テーブルの内容をリフレッシュします。

### Add and Edit IP Logging ダイアログボックス

Add and Edit IP Logging ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：ログを取り込むホストの IP アドレス。
- **Maximum Values**：IP ロギングの値を設定します。
  - **Duration**：パケットを取り込む最長期間。

  （注） Edit IP Logging ダイアログボックスの場合、**Duration** フィールドは、IP ロギングに編集を適用した後に延長された時間です。

    値は 1 ～ 60 分です。デフォルトは 10 分です。
  - **Packets**：（オプション）取り込むパケットの最大数。
    範囲は、1 ～ 4294967295 個のパケットです。
  - **Bytes**：（オプション）取り込む最大バイト数。
    範囲は、0 ～ 4294967295 バイトです。

ボタンの機能：

- **Apply**：変更を適用してダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

## IP ロギングの設定

特定のホストの IP トラフィックをログに記録するには、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 IDM にログインします。

**ステップ 2**　**Monitoring > IP Logging** をクリックします。

IP Logging パネルが表示されます。

**ステップ 3**　**Add** をクリックして、IP ロギングを追加します。

Add IP Logging ダイアログボックスが表示されます。

**ステップ 4**　IP ログの取り込み元となるホストの IP アドレスを入力します。

Added または Started 状態で取り込みが追加されると、エラー メッセージが表示されます。

**ステップ 5**　**Duration** フィールドに IP ログを取り込む分数を入力します。

**ステップ 6**　（オプション）**Packets** フィールドに取り込むパケット数を入力します。

**ステップ 7**　（オプション）**Bytes** フィールドに取り込むバイト数を入力します。

**ステップ 8**　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

IP Logging パネルのリストに IP ログとログ ID が表示されます。

**ステップ 9**　リストに既存のエントリを編集するには、それを選択して **Edit** をクリックします。

Edit IP Logging ダイアログボックスが表示されます。

**ステップ 10**　パケットを取り込む期間を編集します。

**ステップ 11**　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

IP Logging パネルのリストに編集した IP ログが表示されます。

**ステップ 12**　IP ロギングを停止するには、停止するログのログ ID を選択し、**Stop** をクリックします。

Stop IP Logging ダイアログボックスが表示されます。

**ステップ 13**　**OK** をクリックして、そのログの IP ロギングを停止します。

**ステップ 14**　IP ログをダウンロードするには、ログ ID を選択し、**Download** をクリックします。

Save As ダイアログボックスが表示されます。

**ステップ 15**　ログをローカル マシンに保存します。保存したログは、Ethereal で表示できます。