CHAPTER 17

# センサーのモニタリング

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在のところ、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。現時点では、他に IPS バージョン 7.1 をサポートしている Cisco IPS センサーはありません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以上および ASA 8.4(2) 以上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。

IDM を使用すると、パフォーマンス、統計情報、接続などセンサーのすべての側面をモニタできます。拒否された攻撃者およびイベントのリストを表示することもできます。IP ロギングの設定、ホスト ブロックとネットワーク ブロックのセットアップ、およびレート制限の設定と管理を行うことができます。OS 識別名と異常検出をモニタできます。ここでは、センサーをモニタする方法について説明します。次の事項について説明します。

# イベントのモニタリング

ここでは、センサー上のイベント データをフィルタリングおよび表示する方法について説明します。次の事項について説明します。



## [Events] ペイン

[Events] ペインを使用すると、イベント データをフィルタリングおよび表示できます。タイプ、時間、またはその両方に基づいて、イベントをフィルタリングできます。デフォルトでは、過去 1 時間のすべての alert イベントのおよび error イベントが表示されます。これらのイベントにアクセスするには、[View] をクリックします。

[View] をクリックすると、イベントの時間範囲をまだ設定していない場合は、IDM によってイベントの時間範囲が定義されます。範囲の終了時刻を指定していない場合は、[View] をクリックした時刻が終了時刻として定義されます。

センサーから大量のイベントを取得する際にシステム エラーを発生させないよう、IDM では 1 度に表示するイベントの数を制限できます（1 ページあたりの最大行数は 500 行）。他のイベントを表示するには、[Back] および [Next] をクリックします。

## [Events] ペインのフィールド定義

[Events] ペインには、次のフィールドがあります。

- [Show Alert Events]：表示するアラートのレベルを設定できます。
  - Informational
  - Low
  - Medium
  - High

  デフォルトでは、すべてのレベルがイネーブルです。
- [Threat Rating (0-100)]：脅威レーティング値の範囲（最小レベルおよび最大レベル）を変更できます。
- [Show Error Events]：表示するエラーのタイプを設定できます。
  - Warning
  - Error
  - Fatal

  デフォルトでは、すべてのレベルがイネーブルです。
- [Show Attack Response Controller events] : ARC（以前の名称は Network Access Controller）イベントが表示されます。デフォルトではディセーブルです。

（注）　NAC は、ARC と呼ばれていますが、Cisco IPS では、IDM および CLI 全体での名前の変更を完了していません。

- [Show status events] : イベントのステータスが表示されます。デフォルトではディセーブルです。
- [Select the number of the rows per page] : ページあたりの表示行数を指定できます。有効な範囲は 100 ～ 500 です。デフォルトは 100 です。
- [Show all events currently stored on the sensor] : センサー上に格納されているすべてのイベントを取得します。
- [Show past events] : 時間数または分数を指定してさかのぼり、過去のイベントを表示できます。
- [Show events from the following time range] : 指定した時間範囲からイベントを取得します。

# [Event Viewer] ペインのフィールド定義

[Event Viewer] ペインには、次のフィールドがあります。

- [#] : 結果のクエリーに含まれているイベントの順位番号を識別します。
- [Type] : イベント タイプ（Error、NAC、Status、または Alert）を識別します。
- [Sensor UTC Time] : イベントの発生時刻を識別します。
- [Sensor Local Time] : センサーの現地時間。
- [Event ID] : センサーがイベントに割り当てた数値 ID。
- [Events] : イベントの概要。
- [Sig ID] : alert イベントの原因となり、イベントを起動したシグニチャを識別します。
- [Performed Actions] : センサーが実行したアクション。

# イベントの表示の設定

イベントの表示方法を設定するには、次の手順を実行します。

**ステップ 1**　IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Events] を選択します。

**ステップ 3**　[Show Alert Events] で、表示するアラートのレベルに対応するチェックボックスをオンにします。

**ステップ 4**　[Threat Rating] フィールドに、脅威レーティングの最小および最大の範囲を入力します。

**ステップ 5**　[Show Error Events] で、表示するエラーのタイプに対応するチェックボックスをオンにします。

**ステップ 6**　ARC（以前の名称は Network Access Controller）イベントを表示するには、[Show Attack Response Controller events] チェックボックスをオンにします。

**ステップ 7**　ステータス イベントを表示するには、[Show status events] チェックボックスをオンにします。

**ステップ 8**　[Select the number of the rows per page] フィールドに、ページあたりの表示行数を入力します。デフォルトは 100 です。値は 100、200、300、400、または 500 です。

**ステップ 9**　表示するイベントの時刻を設定するには、次のいずれかのオプション ボタンをクリックします。

- [Show all events currently stored on the sensor]

- [Show past events]：過去のイベントを表示するためにさかのぼる時間と分を入力します。
- [Show events from the following time range]：開始時刻および終了時刻を入力します。

**ヒント**　変更を破棄するには、[Reset] をクリックします。

**ステップ 10**　設定したイベントを表示するには、[View] をクリックします。

**ステップ 11**　カラム内のソート順を上または下に移動する場合は、右側をクリックすると上矢印および下矢印が表示されます。

**ステップ 12**　100 行単位でページを切り替えるには、[Next] または [Back] をクリックします。

**ステップ 13**　イベントの詳細を表示するには、イベントを選択し、[Details] をクリックします。イベントの詳細が別のダイアログボックスに表示されます。イベント ID が、このダイアログボックスのタイトルになっています。

## イベント ストアのクリア

イベント ストアをクリアするには、**clear events** コマンドを使用します。

イベント ストアからイベントをクリアするには、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**　イベント ストアをクリアします。

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

**ステップ 3**　イベントをクリアする場合は、**yes** と入力します。

# 拒否攻撃者の設定およびモニタリング

ここでは、拒否攻撃者リストのモニタ方法について、次のトピックに分けて説明します。

- 「[Denied Attackers] ペイン」（P.17-4）
- 「[Denied Attackers] ペインのフィールド定義」（P.17-5）
- 「拒否された攻撃者リストのモニタリングと拒否された攻撃者の追加」（P.17-5）

## [Denied Attackers] ペイン

**（注）**　拒否された攻撃者リストのモニタおよびクリアを行うには、管理者でなければなりません。

[Denied Attackers] ペインには、拒否された攻撃者のすべての IP アドレスおよびヒット カウントが表示されます。すべての IP アドレスに対するヒット カウントのリセットや、拒否された攻撃者のリストのクリアを行うことができます。拒否された攻撃者をモニタ対象に設定することもできます。

（注）　リセットおよびクリアは、表内のすべての項目に適用されます。

# [Denied Attackers] ペインのフィールド定義

[Denied Attackers] ペインには、次のフィールドがあります。

- [Virtual Sensor]：攻撃者を拒否している仮想センサー。
- [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攻撃対象の 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。
- [Requested Percentage]：インライン モードのときにセンサーで拒否すると設定したトラフィックのパーセンテージ。
- [Actual Percentage]：センサーで実際に拒否するインライン モードのトラフィックのパーセンテージ。

  （注）　センサーでは、要求されたパーセンテージと完全に一致する割合で拒否しようとしますが、割り切れないパーセンテージの場合があるため、センサーは要求されたしきい値を下回ることがあります。

- [Hit Count]：拒否された攻撃者のヒット カウントが表示されます。

# 拒否された攻撃者リストのモニタリングと拒否された攻撃者の追加

拒否された攻撃者のリストとヒット カウントの表示、拒否された攻撃者の追加と削除、拒否された攻撃者のリストのクリア、およびヒット カウントのリセットを行うには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Time-Based Actions] > [Denied Attackers] を選択します。

**ステップ 3**　リストをリフレッシュするには、[Refresh] をクリックします。

**ステップ 4**　拒否された攻撃者のリスト全体をクリアするには、[Clear List] をクリックします。

**ステップ 5**　拒否されたすべて攻撃者に対してヒット カウントをリセットするには、[Reset All Hit Counts] をクリックします。

**ステップ 6**　拒否された攻撃者をモニタ対象のリストに追加するには、[Add] をクリックします。

**ステップ 7**　[Attacker IP] フィールドに、攻撃者の IP アドレスを入力します。

（注）　IPv4 と IPv6 の IP アドレスを入力できます。

**ステップ 8**　[Specify Victim Address or Port] チェックボックスをオンにし、IP アドレスとポート番号を入力します。

**ステップ 9**　[Specify Virtual Sensor] チェックボックスをオンにし、ドロップダウン リストから仮想センサーを選択します。

**ヒント**　変更を廃棄して [Denied Attackers] ペインに戻るには、[Cancel] をクリックします。

**ステップ 10**　[OK] をクリックして変更を保存します。拒否された攻撃者が [Denied Attacker] リストに表示されます。

**ステップ 11**　拒否された攻撃者をリストから削除するには、そのエントリを選択し、次に [Delete] をクリックします。

# ホスト ブロックの設定

ここでは、ホスト ブロックの設定方法について説明します。次の事項について説明します。

- 「[Host Blocks] ペイン」（P.17-6）
- 「[Host Block] ペインのフィールド定義」（P.17-7）
- 「[Add Active Host Block] ダイアログボックスのフィールド定義」（P.17-7）
- 「ホスト ブロックの設定および管理」（P.17-8）

# [Host Blocks] ペイン

**（注）**　接続ブロックとネットワーク ブロックは、適応型セキュリティ アプライアンスではサポートされません。適応型セキュリティ アプライアンスでは、追加の接続情報があるホスト ブロックだけがサポートされます。

**（注）**　アクティブ 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。

ホストのブロッキングを設定および管理するには、[Host Blocks] ペインを使用します。ホスト ブロックでは、特定のホストからのトラフィックを永続的に拒否するか（ブロックを削除するまで）、指定期間拒否します。宛先 IP アドレスおよび宛先のプロトコルとポートを指定することにより、接続に基づいてブロックできます。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。

ブロックの時間を指定する場合は、1 ～ 70560 分（49 日間）の範囲の値にする必要があります。時間を指定しなかった場合、ホスト ブロックは、センサーが再起動されるか、ブロックが削除されるまで有効なままになります。

（注）　接続ブロックとネットワーク ブロックは、適応型セキュリティ アプライアンスではサポートされません。適応型セキュリティ アプライアンスでは、追加の接続情報があるホスト ブロックだけがサポートされます。

# [Host Block] ペインのフィールド定義

[Host Blocks] ペインには、次のフィールドがあります。

- [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]：プロトコルの種類（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)]：ブロックの元のタイムアウト値（分単位）。有効な値は、1 ～ 70560 分（49 日間）です。
- [VLAN]：シグニチャを起動したデータを伝送していた VLAN を示します。

  （注）　ブロック要求に VLAN ID は含まれていますが、セキュリティ アプライアンスには渡されません。管理コンテキストにログインしている場合、センサーでは FWSM 2.1 以上ではブロックを実行できません。

- [Connection Block Enabled]：ホストの接続をブロックするかどうか。

  （注）　接続ブロックとネットワーク ブロックは、適応型セキュリティ アプライアンスではサポートされません。適応型セキュリティ アプライアンスでは、追加の接続情報があるホスト ブロックだけがサポートされます。

# [Add Active Host Block] ダイアログボックスのフィールド定義

[Add Active Host Block] ダイアログボックスには、次のフィールドがあります。

- [Source IP]：ブロックの送信元 IP アドレス。
- [Enable connection blocking]：ホスト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]（任意）：ブロックの宛先ポート。
  - [Protocol]（任意）：プロトコルの種類（TCP、UDP、または ANY）。デフォルトは ANY です。

（注）　接続ブロックとネットワーク ブロックは、適応型セキュリティ アプライアンスではサポートされません。適応型セキュリティ アプライアンスでは、追加の接続情報があるホスト ブロックだけがサポートされます。

- [VLAN]（任意）：シグニチャを起動したデータを伝送していた VLAN を示します。

（注）　ブロック要求に VLAN ID は含まれていますが、セキュリティ アプライアンスには渡されません。管理コンテキストにログインしている場合、センサーでは FWSM 2.1 以降ではブロックを実行できません。

- [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]：ブロックの継続時間（分数）。有効な値は、1 ～ 70560 分（49 日間）です。
- [No Timeout]：ブロックのタイムアウトなしを選択できます。

# ホスト ブロックの設定および管理

ホスト ブロックを追加、削除、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Time-Based Actions] > [Host Blocks] を選択し、[Add] をクリックしてホスト ブロックを追加します。

**ステップ 3**　[Source IP] フィールドに、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 4**　接続ベースのブロックにするには、[Enable Connection Blocking] チェックボックスをオンにします。

（注）　接続ブロックは、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をブロックします。

（注）　接続ブロックとネットワーク ブロックは、適応型セキュリティ アプライアンスではサポートされません。適応型セキュリティ アプライアンスでは、追加の接続情報があるホスト ブロックだけがサポートされます。

**a.**　[Destination IP] フィールドに、宛先 IP アドレスを入力します。

**b.**　（任意）[Destination Port] フィールドに、宛先ポートを入力します。

**c.**　（任意）[Protocol] ドロップダウン リストから、プロトコルを選択します。

**ステップ 5**　（任意）[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 6**　タイムアウトを設定します。

- 時間の長さを指定したブロックを設定するには、[Enable Timeout] オプション ボタンをクリックし、[Timeout] フィールドに時間を分単位で入力します。
- ブロックに特定の期間を設定しない場合は、[No Timeout] オプション ボタンをクリックします。

**ヒント** 変更を廃棄して、[Add 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 7** [Apply] をクリックします。新しいホスト ブロックが [Host Blocks] ペインのリストに表示されます。

**ステップ 8** ホスト ブロック リストの内容をリフレッシュするには、[Refresh] をクリックします。

**ステップ 9** ブロックを削除するには、リストでホスト ブロックを選択して、[Delete] をクリックします。[Delete Host Block] ダイアログボックスが開き、このブロックを削除してよいかどうかを確認するメッセージが表示されます。

**ヒント** 変更を廃棄して、[Delete 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 10** ブロックを削除するには [Yes] をクリックします。ホスト ブロックは [Host Blocks] ペインのリストに表示されなくなりました。

# ネットワーク ブロックの設定

ここでは、ネットワーク ブロックの設定方法について説明します。次の事項について説明します。



## [Network Blocks] ペイン

**（注）** 接続ブロックとネットワーク ブロックは、適応型セキュリティ アプライアンスではサポートされません。適応型セキュリティ アプライアンスでは、追加の接続情報があるホスト ブロックだけがサポートされます。

**（注）** 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。

ネットワークのブロッキングを設定および管理するには、[Network Blocks] ペインを使用します。ネットワーク ブロックでは、特定のネットワークからのトラフィックを永続的に拒否するか（ブロックを削除するまで）、指定期間拒否します。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 サブネット マスクも受け入れられます。

ブロックの時間を指定する場合は、1 ～ 70560 分（49 日間）の範囲の値にする必要があります。時間を指定しなかった場合、ブロックは、センサーが再起動されるか、ブロックが削除されるまで有効なままになります。

（注）　接続ブロックとネットワーク ブロックは、適応型セキュリティ アプライアンスではサポートされません。適応型セキュリティ アプライアンスでは、追加の接続情報があるホスト ブロックだけがサポートされます。

# [Network Blocks] ペインのフィールド定義

[Network Blocks] ペインには、次のフィールドがあります。

- [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)] : ブロックの元のタイムアウト値（分単位）。有効な値は、1 ～ 70560 分（49 日間）です。

# [Add Network Block] ダイアログボックスのフィールド定義

[Add Network Block] ダイアログボックスには、次のフィールドがあります。

- [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 日間）です。
- [No Timeout] : ブロックのタイムアウトなしを選択できます。

# ネットワーク ブロックの設定および管理

ネットワーク ブロックを追加、削除、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 IDM にログインします。

**ステップ 2**　**[Monitoring] >** [Sensor Monitoring] > [Time-Based Actions] > [Network Blocks] を選択し、[Add] をクリックしてネットワーク ブロックを追加します。

**ステップ 3**　[Source IP] フィールドに、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 4**　[Netmask] ドロップダウン リストからネットマスクを選択します。

**ステップ 5**　タイムアウトを設定します。

- 時間の長さを指定したブロックを設定するには、[Enable Timeout] オプション ボタンをクリックし、[Timeout] フィールドに時間を分単位で入力します。
- ブロックに特定の期間を設定しない場合は、[No Timeout] オプション ボタンをクリックします。

ヒント　変更を取り消して、[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 6**　[Apply] をクリックします。ブロックがすでに追加されていると、エラー メッセージが表示されます。新しいネットワーク ブロックが [Network Blocks] ペインのリストに表示されます。

**ステップ 7**　ネットワーク ブロック リストの内容をリフレッシュするには、[Refresh] をクリックします。

**ステップ 8**　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が開き、このブロックを削除してよいかどうかを確認するメッセージが表示されます。

**ステップ 9**　ブロックを削除するには [Yes] をクリックします。ネットワーク ブロックは [Network Blocks] ペインのリストに表示されなくなりました。

# レート制限の設定

ここでは、レート制限の設定方法および管理方法について説明します。次の事項について説明します。



## [Rate Limits] ペイン

（注）　レート制限を追加するには、管理者でなければなりません。

レート制限の設定および管理には、[Rate Limits] ペインを使用します。レート制限では、1 つのネットワーク デバイス インターフェイス上で許可される、指定されたタイプのトラフィックの量を、最大帯域幅キャパシティに対するパーセンテージで制限します。このパーセンテージを超えるトラフィックは、ネットワーク デバイスによってドロップされます。レート制限では、指定したターゲット ホストへのトラフィックまたは設定したインターフェイス/方向と交差するすべてのトラフィックを制限できます。レート制限は、永続的に使用するか、期間を指定して使用できます。レート制限は、プロトコル、オプションの宛先アドレス、およびオプションのデータ値によって識別されます。

レート制限はパーセントで指定するため、さまざまな帯域幅キャパシティを持つインターフェイス上のさまざまな実際の制限に変換できます。レート制限のパーセント値は、1 以上 100 以下の整数でなければなりません。

## [Rate Limits] ペインのフィールド定義

[Rate Limits] ペインには、次のフィールドがあります。

- [Protocol]：レート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で許可される最大帯域幅のパーセント。このレートを超える適合トラフィックはドロップされます。
- [Source IP]：レート制限されるトラフィックの送信元ホストの IP アドレス。
- [Source Port]：レート制限されるトラフィックの送信元ホストのポート。

- [Destination IP]：レート制限されるトラフィックの宛先ホストの IP アドレス。
- [Destination Port]：レート制限されるトラフィックの宛先ホストのポート。
- [Data]：特定のプロトコルのトラフィックをより正確に修飾するために必要な追加情報。たとえば、echo-request を使用すると、ICMP プロトコル トラフィックのレート制限は ping に絞られます。
- [Minutes Remaining]：このレート制限が有効な残り時間（分単位）。
- [Timeout (minutes)]：このレート制限の合計時間（分単位）。

# [Add Rate Limit] ダイアログボックスのフィールド定義

[Add Rate Limit] ダイアログボックスには、次のフィールドがあります。

- [Protocol]：レート制限するトラフィックのプロトコル（ICMP、TCP、または UDP）。
- [Rate (1-100)]：レート制限されたトラフィックで許容される最大帯域幅のパーセンテージ。
- [Source IP]（任意）：レート制限されるトラフィックの送信元ホストの IP アドレス。
- [Source Port]（任意）：レート制限されるトラフィックの送信元ホストのポート。
- [Destination IP]（任意）：レート制限されるトラフィックの宛先ホストの IP アドレス。
- [Destination Port]（任意）：レート制限されるトラフィックの宛先ホストのポート。
- [Use Additional Data]：さらに、echo-reply、echo-request、halfOpenSyn などの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]：タイムアウトを分単位で指定できます（1 ～ 70560）。

# レート制限の設定および管理

レート制限を追加、削除、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Time-Based Actions] > [Rate Limits] を選択し、[Add] をクリックしてレート制限を追加します。

**ステップ 3**　[Protocol] ドロップダウン リストから、レート制限するトラフィックのプロトコル（ICMP、TCP、または UDP）を選択します。

**ステップ 4**　[Rate] フィールドに、レート制限（1 ～ 100 %）を入力します。

**ステップ 5**　（任意）[Source IP] フィールドに、送信元 IP アドレスを入力します。

**ステップ 6**　（任意）[Source Port] フィールドに、送信元ポートを入力します。

**ステップ 7**　（任意）[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 8**　（任意）[Destination Port] フィールドに、宛先ポートを入力します。

**ステップ 9**　（任意）レート制限で追加データを使用することを設定するには、[Use Additional Data] チェックボックスをオンにします。

**ステップ 10**　[Select Data] ドロップダウン 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 11**　タイムアウトを設定します。

- レート制限に特定の期間を設定しない場合は、[No Timeout] オプション ボタンをクリックします。
- 分単位のタイムアウトを設定するには、[Enable Timeout] オプション ボタンをクリックし、[Timeout] フィールドに分単位の期間（1 ～ 70560）を入力します。

**ヒント**　変更を廃棄して、[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 12**　[Apply] をクリックします。新しいレート制限が [Rate Limits] ペインのリストに表示されます。

**ステップ 13**　レート制限リストの内容をリフレッシュするには、[Refresh] をクリックします。

**ステップ 14**　レート制限を削除するには、リストで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が開き、このレート制限を削除してよいかどうかを確認するメッセージが表示されます。

**ヒント**　[Delete Rate Limit] ダイアログボックスを閉じるには、[No] をクリックします。

**ステップ 15**　レート制限を削除するには [Yes] をクリックします。レート制限は、レート制限リストに表示されなくなりました。

# IP ロギングの設定

ここでは、IP ロギングの設定方法について説明します。次の事項について説明します。



## IP ロギングについて

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

最も単純な IP ロギングは IP アドレス 1 個で構成されます。IP アドレスで指定したホストに関連するすべての IP トラフィックをキャプチャするように、センサーを設定できます。センサーでは、この IP アドレスを持つ最初の IP パケットを検出した時点で収集を開始し、設定したパラメータに応じて収集を続行します。その IP アドレスで IP トラフィックをログに記録する時間（分単位）、パケットの数、バイト数などを指定できます。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。

ログ ファイルは、次の 3 つのいずれかの状態になります。

- Added：IP ロギングを追加した時点
- 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 つの状態すべてを合わせたファイルの数は、20 個に制限されています。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）** ログは、センサーによって解放されるまでセンサー上に残ります。センサー上の IP ログ ファイルは管理できません。

IP ログ ファイルを WireShark や TCPDUMP などのスニフィング ツールで表示するために、FTP または SCP サーバにコピーすることができます。ファイルは、ファイル拡張子 pcap を付けて、PCAP バイナリ形式で格納されます。

# [IP Logging] ペイン

**（注）** IP ロギングを設定するには、管理者でなければなりません。

[IP Logging] ペインには、システムに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。
- 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。
  - 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 アラートが IP ロギング テーブルに表示されます。

# [IP Logging] ペインのフィールド定義

[IP Logging] ペインには、次のフィールドがあります。

- [Log ID]：IP ログの ID。
- [Virtual Sensor]：IP ログが関連付けられている仮想センサー。
- [IP Address]：ログをキャプチャするホストの IP アドレス。
- [Status]：IP ログの状態。有効な値は、added、started、completed です。
- [Start Time]：最初にキャプチャされたパケットのタイムスタンプ。
- [Current End Time]：キャプチャされた最新パケットのタイムスタンプ。キャプチャが完了していない場合は、タイムスタンプはありません。

- [Alert ID]：IP ログをトリガーしたイベント アラートがあれば、このアラートの ID。
- [Packets Captured]：キャプチャされたパケットの現在のカウント。
- [Bytes Captured]：キャプチャされたバイトの現在のカウント。

# [Add IP Logging]/[Edit IP Logging] ダイアログボックスのフィールド定義

[Add IP Logging]/[Edit IP Logging] ダイアログボックスには、次のフィールドがあります。

- [Virtual Sensor]：IP ログのキャプチャ元の仮想センサーを選択できます。
- [IP Address]：ログをキャプチャするホストの IP アドレス。

（注）　IPv4 と IPv6 の IP アドレスを入力できます。

- [Maximum Values]：IP ロギング用の値を設定できます。
  - [Duration]：パケットの最大キャプチャ期間。範囲は 1 ～ 60 分です。デフォルトは 10 分です。

（注）　[Edit IP Logging] ダイアログボックスの場合、[Duration] フィールドは、編集を IP ロギングに適用することによって 1 回拡張される時間です。

  - [Packets]（任意）：キャプチャするパケットの最大数。範囲は 0 ～ 4294967295 パケットです。
  - [Bytes]（任意）：キャプチャするバイトの最大数。範囲は 0 ～ 4294967295 バイトです。

# IP ロギングの設定

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

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Time-Based Actions] > [IP Logging] を選択し、[Add] をクリックしてホスト ブロックを追加します。

**ステップ 3**　[Virtual Sensor] ドロップダウン リストから、IP ロギングをオンにする仮想センサーを選択します。

**ステップ 4**　[IP Address] フィールドに、IP ログをキャプチャするホストの IP アドレスを入力します。

存在しており、Added 状態または Started 状態のキャプチャを追加すると、エラー メッセージが表示されます。

（注）　IPv4 と IPv6 の IP アドレスを入力できます。

**ステップ 5**　[Duration] フィールドに、IP ログをキャプチャする期間を分単位で入力します。範囲は 1 ～ 60 分です。デフォルトは 10 分です。

**ステップ 6**　（任意）[Packets] フィールドに、キャプチャするパケットの数を入力します。範囲は 0 ～ 4294967295 パケットです。

**ステップ 7**　（任意）[Bytes] フィールドに、キャプチャするバイト数を入力します。範囲は 0 ～ 4294967295 パケットです。

**ヒント**　変更を廃棄して、[Add IP Log] 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] をクリックして、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。ログ ID の付いた IP ログが [IP Logging] ペインのリストに表示されます。

**ステップ 9**　リストにある既存のログ エントリを編集するには、エントリを選択して [Edit] をクリックします。

**ステップ 10**　[Duration] フィールドで、パケットをキャプチャする期間（分単位）を編集します。

**ステップ 11**　[Apply] をクリックして、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。編集した IP ログが [IP Logging] ペインのリストに表示されます。

**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。

**ステップ 13**　[OK] をクリックして、このログの 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。

**ステップ 15**　ログをローカル マシンに保存します。WireShark を使用してログを表示できます。

# 異常検出 KB のモニタリング

ここでは、異常検出 KB での作業方法について説明します。次の事項について説明します。



## [Anomaly Detection] ペイン

**（注）**　異常検出 KB をモニタするには、管理者でなければなりません。

[Anomaly Detection] ペインには、すべての仮想センサーの KB が表示されます。[Anomaly Detection] ペインでは、次の操作を実行できます。

- 特定の KB に関するしきい値の表示
- KB の比較
- KB のロード
- KB を現在の KB にする
- KB の名前変更

- KB のダウンロード
- KB のアップロード
- 1 つまたはすべての KB の削除

（注）　[Anomaly Detection] のボタンは、リストで 1 行だけ選択したときにアクティブになります。ただし、[Compare KBs] は例外で、2 行選択できます。このいずれでもない数の行を選択した場合は、いずれのボタンもアクティブになりません。

# KB について

KB にはツリー構造があり、次の情報を含みます。

- KB の名前
- ゾーン名
- プロトコル
- サービス

KB には、各サービスのスキャナのしきい値およびヒストグラムが保持されています。学習受け入れモードを自動に設定し、アクションを循環に設定した場合は、24 時間ごとに新しい KB が作成されて次の 24 時間に使用されます。学習受け入れモードを自動に設定し、アクションを保存だけに設定した場合、新しい KB は作成されますが、現在の KB が使用されます。学習受け入れモードを自動に設定していない場合、KB は作成されません。

（注）　学習受け入れモードでは、センサーの現地時間が使用されます。

スキャナのしきい値は、単一の送信元 IP アドレスでスキャンできるゾーン IP アドレスの最大数を定義します。ヒストグラムのしきい値は、指定された数を超えるゾーン IP アドレスをスキャンできる送信元 IP アドレスの最大数を定義します。

異常検出では、攻撃が行われていないときに学習したヒストグラムからの逸脱を検出した場合（つまり、定義されている数を超えるゾーン宛先 IP アドレスを同時にスキャンする送信元 IP アドレスの数が超過した場合）、ワーム攻撃であると識別します。たとえば、スキャニングしきい値が 300 で、ポート 445 のヒストグラムの場合、異常検出では、350 個のゾーン宛先 IP アドレスをスキャンするスキャナを検出すると、マス スキャナが検出されたことを示すアクションを生成します。ただし、このスキャナでは、ワーム攻撃が進行中かどうかはまだ確認されていません。

表 17-1 は、この例を示します。

**表 17-1　ヒストグラムの例**

| | | | |
|---|---|---|---|
| 送信元 IP アドレスの数 | 10 | 5 | 2 |
| 宛先 IP アドレスの数 | 5 | 20 | 100 |

異常検出では、ポート 445 で 50 個を超えるゾーン宛先 IP アドレスを同時にスキャンする送信元 IP アドレスを 6 つ識別すると、異常検出でポート 445 へのワーム攻撃を識別したことを示す、送信元 IP アドレス未指定のアクションを作成します。動的なフィルタしきい値の 50 は、新しい内部スキャンしきい値に指定されるため、新しいスキャンしきい値（50）を超えてスキャンする送信元 IP アドレスごとの追加の動的フィルタを異常検出で作成するために、異常検出では、スキャナのしきい値定義を小さくします。

KB が学習した内容は、異常検出ポリシーごとまたはゾーンごとにオーバーライドできます。ネットワーク トラフィックが判明している場合は、false positive を制限するためにオーバーライドを使用する必要が生じることもあります。

# [Anomaly Detection] ペインのフィールド定義

[Anomaly Detection] ペインには、次のフィールドおよびボタンがあります。

- [Virtual Sensor]：KB を格納している仮想センサー。
- [Knowledge Base Name]：KB の名前。

（注）　デフォルトでは、日付が KB の名前になります。デフォルトの名前は、日付と時刻（year-month-day-hour_minutes_seconds）です。初期 KB は、最初の KB で、デフォルトのしきい値を持つ KB です。

- [Current]：Yes は、現在ロードされている KB を示します。
- [Size]：KB のサイズ（KB）。通常の範囲は、1 KB 未満から 500 ～ 700 KB までです。
- [Created]：KB の作成日。

**ボタンの機能**

- [Show Thresholds]：選択した KB の [Thresholds] ウィンドウが開きます。このウィンドウでは、スキャナのしきい値および選択した KB のヒストグラムを表示できます。
- [Compare KBs]：[Compare Knowledge Bases] ダイアログボックスが開きます。このダイアログボックスでは、選択した KB と比較する KB を選択できます。このダイアログボックスから [Differences between knowledge bases *KB name* and *KB name*] ウィンドウが開きます。
- [Load]：選択した KB をロードします。選択した KB が現在の KB になります。
- [Save Current]：[Save Knowledge Base] ダイアログボックスが開きます。このダイアログボックスでは、選択した KB のコピーを保存できます。
- [Rename]：[Rename Knowledge Base] ダイアログボックスが開きます。このダイアログボックスでは、選択した KB を名前変更できます。
- [Download]：[Download Knowledge Base From Sensor] ダイアログボックスが開きます。このダイアログボックスでは、リモート センサーから KB をダウンロードできます。
- [Upload]：[Upload Knowledge Base to Sensor] ダイアログボックスが開きます。このダイアログボックスでは、リモート センサーに KB をアップロードできます。
- [Delete]：選択した KB を削除します。
- [Delete All]：すべての KB を削除します。
- [Refresh]：[Anomaly Detection] ペインがリフレッシュされます。

# しきい値の表示

ここでは、KB しきい値情報の表示方法について説明します。次の事項について説明します。

- 「[Threshold for KB_Name] ウィンドウ」（P.17-19）
- 「[Thresholds for KB_Name] ウィンドウのフィールド定義」（P.17-19）

- 「KB しきい値のモニタリング」（P.17-19）

## [Threshold for KB_Name] ウィンドウ

[Thresholds for *KB_Name*] ウィンドウには、選択した KB の次のしきい値情報が表示されます。

- ゾーン名
- プロトコル
- 学習されたスキャナのしきい値
- ユーザ設定のスキャナのしきい値
- 学習されたヒストグラム
- ユーザ設定のヒストグラム

しきい値情報は、ゾーン、プロトコル、およびポートでフィルタリングできます。ゾーンとプロトコルの組み合わせごとに、2 つのしきい値が表示されます。これは、スキャナのしきい値およびヒストグラムのしきい値で、学習された（デフォルト）モードまたはユーザ設定可能なモードのいずれかに対するしきい値です。

## [Thresholds for *KB_Name*] ウィンドウのフィールド定義

[Thresholds for *KB_Name*] ウィンドウには、次のフィールドがあります。

- [Filters]：ゾーンまたはプロトコルでしきい値情報をフィルタリングできます。
  - [Zones]：すべてのゾーン、外部のみ、不正のみ、または内部のみでフィルタリングします。
  - [Protocols]：すべてのプロトコル、TCP のみ、UDP のみ、またはその他のみでフィルタリングします。

（注）　特定のプロトコルを選択した場合は、すべてのポートまたは単一のポート（TCP および UDP）でフィルタリングするか、すべてのプロトコルまたは単一のプロトコル（その他）でフィルタリングすることもできます。

- [Zone]：ゾーン名（external、internal、または illegal）がリストされます。
- [Protocol]：プロトコル（[TCP]、[UDP]、または [Other]）がリストされます。
- [Scanner Threshold (Learned)]：スキャナのしきい値の学習された値がリストされます。
- [Scanner Threshold (User)]：スキャナのしきい値のユーザ設定がリストされます。
- [Histogram (Learned)]：学習されたヒストグラムの値がリストされます。
- [Histogram (User)]：ヒストグラムのユーザ設定値がリストされます。

## KB しきい値のモニタリング

KB しきい値をモニタするには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] を選択します。

**ステップ 3**　最新の KB 情報で [Anomaly Detection] ペインをリフレッシュするには、[Refresh] をクリックします。

**ステップ 4**　KB のしきい値を表示するには、リストで KB を選択し、[Show Thresholds] をクリックします。[Thresholds for *KB_Name*] ウィンドウが表示されます。デフォルト表示では、すべてのゾーンおよびすべてのプロトコルが表示されます。

**ステップ 5**　単一のゾーンだけを表示するように、表示をフィルタリングするには、[Zones] ドロップダウン リストからゾーンを選択します。

**ステップ 6**　単一のプロトコルだけを表示するように、表示をフィルタリングするには、[Protocols] ドロップダウン リストからプロトコルを選択します。デフォルト表示では、TCP プロトコルまたは UDP プロトコルについてはすべてのポートが表示され、その他のプロトコルについてはすべてのプロトコルが表示されます。

**ステップ 7**　TCP または UPD の場合に単一のポートを表示するように表示をフィルタリングするには、[Single Port] オプション ボタンをクリックし、[Port] フィールドにポート番号を入力します。

**ステップ 8**　その他のプロトコルの場合に単一のプロトコルを表示するように表示をフィルタリングするには、[Single Protocol] オプション ボタンをクリックし、[Protocol] フィールドにプロトコル番号を入力します。

**ステップ 9**　最新のしきい値情報でウィンドウをリフレッシュするには、[Refresh] をクリックします。

# KB の比較

ここでは、KB の比較方法について説明します。次の事項について説明します。

- 「[Compare Knowledge Base] ダイアログボックス」（P.17-20）
- 「[Differences between knowledge bases KB_Name and KB_Name ] ウィンドウ」（P.17-20）
- 「[Difference Thresholds between knowledge bases KB_Name and KB_Name] ウィンドウ」（P.17-21）
- 「KB の比較」（P.17-21）

## [Compare Knowledge Base] ダイアログボックス

2 個の KB を比較して、相違点を表示できます。しきい値の差異が指定したパーセンテージを超えているサービスを表示することもできます。[Details of Difference] 列には、特定のポートまたはプロトコルが含まれている KB またはしきい値パーセンテージの差異の程度が表示されます。

### フィールド定義

[Compare Knowledge Bases] ダイアログボックスには、次のフィールドがあります。

- すべての KB を含むドロップダウン リスト。

## [Differences between knowledge bases *KB_Name* and *KB_Name* ] ウィンドウ

[Differences between knowledge base *KB_Name* and *KB_Name*] ウィンドウには、次のタイプの情報が表示されます。

- Zone
- Protocol
- Details of Difference

表示する相違のパーセンテージを指定できます。デフォルトは 10% です。

### フィールド定義

[Differences between knowledge bases *KB_Name* and *KB_Name*] ウィンドウには、次のフィールドがあります。

- [Specify Percentage of Difference] : デフォルトの 10 % から変更して、異なるパーセンテージの相違を表示できます。
- [Zone] : KB の相違点のゾーン（external、internal、または illegal）が表示されます。
- [Protocol] : KB の相違点のプロトコル（[TCP]、[UDP]、または [Other]）が表示されます。
- [Details of Difference] : 2 番めの KB にある相違点の詳細が表示されます。

## [Difference Thresholds between knowledge bases *KB_Name* and *KB_Name*] ウィンドウ

[Difference Thresholds between knowledge base *KB_Name* and *KB_Name*] ウィンドウには、次のタイプの情報が表示されます。

- ナレッジ ベース名
- ゾーン名
- プロトコル
- スキャナのしきい値（学習およびユーザ設定）
- ヒストグラム（学習およびユーザ設定）

### フィールド定義

[Difference Thresholds between knowledge base *KB_Name* and *KB_Name*] ウィンドウには、次のタイプの情報が表示されます。

- [Knowledge Base] : KB 名が表示されます。
- [Zone] : ゾーンの名前（external、internal、または illegal）が表示されます。
- [Protocol] : プロトコル（[TCP]、[UDP]、または [Other]）が表示されます。
- [Scanner Threshold (Learned)] : スキャナのしきい値の学習された値がリストされます。
- [Scanner Threshold (User)] : スキャナのしきい値のユーザ設定がリストされます。
- [Histogram (Learned)] : 学習されたヒストグラムの値がリストされます。
- [Histogram (User)] : ヒストグラムのユーザ設定値がリストされます。

## KB の比較

2 個の KB を比較するには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] を選択します。

**ステップ 3**　最新の KB 情報で [Anomaly Detection] ペインをリフレッシュするには、[Refresh] をクリックします。

**ステップ 4**　比較する KB 1 つをリストから選択し、[Compare KBs] をクリックします。

**ステップ 5**　ドロップダウン リストから比較対象の KB を選択します。

（注）　または Ctrl キーを押しながら KB を 2 個選択して、リスト内の複数の KB を選択できます。

**ステップ 6**　[OK] をクリックします。[Differences between knowledge bases *KB_Name* and *KB_Name*] ウィンドウが表示されます。

（注）　2 個の KB 間に相違点がない場合、リストは空です。

**ステップ 7**　相違のパーセンテージをデフォルトの 10 % から変更する場合は、[Specify Percentage of Difference] フィールドに新しい値を入力します。

**ステップ 8**　相違点の詳細を表示するには、行を選択してから [Details] をクリックします。詳細を表示した [Difference Thresholds between knowledge bases *KB_Name* and *KB_Name*] ウィンドウが表示されます。

# 現在の KB の保存

ここでは、現在の KB を保存、ロード、または削除する方法について説明します。次の事項について説明します。



## [Save Knowledge Base] ダイアログボックス

KB はさまざまな名前で保存できます。KB を保存しようとしたときに異常検出がアクティブでないと、エラーが生成されます。KB の名前がすでに存在する場合は、新しい名前を選択したのか、デフォルトを使用したのかにかかわらず、古い KB が上書きされます。また、KB ファイルのサイズには制限があるため、新しい KB が生成されて制限に達する場合は、一番古い KB が削除されます（ただし、現在の KB でも初期 KB でもないことが前提）。

（注）　初期 KB は上書きできません。

### フィールド定義

[Save Knowledge Base] ダイアログボックスには、次のフィールドがあります。

- [Virtual Sensor]：保存された KB の仮想センサーを選択できます。
- [Save As]：デフォルトの名前を受け入れるか、保存された KB の新しい名前を入力できます。

## KB のロード

（注）　KB をロードすると、その KB が現在の KB として設定されます。

KB をロードするには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] を選択します。

**ステップ 3**　ロードする KB をリストで選択して、[Load] をクリックします。[Load Knowledge Base] ダイアログボックスが開き、このナレッジ ベースをロードしてよいかどうかを確認するメッセージが表示されます。

**ステップ 4**　[Yes] をクリックします。これで、この KB の [Current] 列に Yes が表示されました。

## KB の保存

新しい KB および仮想センサーを指定して KB を保存するには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] を選択します。

**ステップ 3**　新しい KB として保存する KB をリストで選択して、[Save Current] をクリックします。

**ステップ 4**　[Virtual Sensor] ドロップダウン リストから、この KB を適用する仮想センサーを選択します。

**ステップ 5**　[Save As] フィールドでデフォルトの名前を受け入れるか、KB の新しい名前を入力します。

**ヒント**　変更を廃棄して、[Save Knowledge Base] 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 6**　[Apply] をクリックします。新しい名前の KB が [Anomaly Detection] ペインのリストに表示されます。

## KB の削除

（注）　現在の KB としてロードされている KB および初期 KB は削除できません。

KB を削除するには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] を選択します。

**ステップ 3**　削除する KB をリストで選択して、[Delete] をクリックします。[Delete Knowledge Base] ダイアログボックスが開き、このナレッジ ベースを削除してよいかどうかを確認するメッセージが表示されます。

**ステップ 4**　[Yes] をクリックします。KB は [Anomaly Detection] ペインのリストに表示されなくなりました。

## KB の名前変更

**（注）**　初期 KB は名前変更できません。

KB を名前変更するには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] を選択します。

**ステップ 3**　名前変更する KB をリストで選択して、[Rename] をクリックします。

**ステップ 4**　[New Name] フィールドに KB の新しい名前を入力します。

**ステップ 5**　[Apply] をクリックします。新しい名前の KB が [Anomaly Detection] ペインのリストに表示されます。

## KB のダウンロード

FTP プロトコルまたは SCP プロトコルを使用して、リモートの場所に KB をダウンロードできます。リモート URL、ユーザ名、およびパスワードが必要です。

### フィールド定義

[Download Knowledge Base From Sensor] ダイアログボックスには、次のフィールドがあります。

- [File Transfer Protocol]：ファイル転送プロトコルとして SCP または FTP を選択できます。
- [IP address]：KB のダウンロード元リモート センサーの IP アドレス。
- [Directory]：リモート センサー上の KB のパス。
- [File Name]：KB のファイル名。
- [Username]：リモート センサー上のユーザ アカウントのユーザ名。
- [Password]：リモート センサー上のユーザ アカウントのパスワード。

## KB のダウンロード

センサーから KB をダウンロードするには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] を選択します。

**ステップ 3**　センサーから KB をダウンロードするには、[Download] をクリックします。

**ステップ 4**　[File Transfer Protocol] ドロップダウン リストから、使用するプロトコル（SCP または FTP）を選択します。

**ステップ 5**　[IP address] フィールドに、KB をダウンロードするセンサーの IP アドレスを入力します。

**ステップ 6**　[Directory] フィールドに、KB のあるセンサー上の場所のパスを入力します。

**ステップ 7**　[File Name] フィールドに、KB のファイル名を入力します。

**ステップ 8**　[Username] フィールドに、センサーに定義されているユーザ アカウントに対応するユーザ名を入力します。

**ステップ 9**　[Password] フィールドに、センサーに定義されているユーザ アカウントのパスワードを入力します。

**ヒント**　変更を廃棄して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 10**　[Apply] をクリックします。新しい KB が [Anomaly Detection] ペインのリストに表示されます。

## KB のアップロード

FTP プロトコルまたは SCP プロトコルを使用して、リモートの場所から KB をアップロードできます。リモート URL、ユーザ名、およびパスワードが必要です。

### フィールド定義

[Upload Knowledge Base to Sensor] ダイアログボックスには、次のフィールドがあります。

- [File Transfer Protocol]：ファイル転送プロトコルとして SCP または FTP を選択できます。
- [IP address]：KB のアップロード先リモート センサーの IP アドレス。
- [Directory]：センサー上の KB のパス。
- [File Name]：KB のファイル名。
- [Virtual Sensor]：この KB を関連付ける仮想センサー。
- [Save As]：新しいファイル名で KB を保存できます。
- [Username]：センサー上のユーザ アカウントのユーザ名。
- [Password]：センサー上のユーザ アカウントのパスワード。

## KB のアップロード

KB をセンサーにアップロードするには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] を選択します。

**ステップ 3**　KB をセンサーにアップロードするには、[Upload] をクリックします。

**ステップ 4**　[File Transfer Protocol] ドロップダウン リストから、使用するプロトコル（SCP または FTP）を選択します。

**ステップ 5**　[IP address] フィールドに、KB のダウンロード先センサーの IP アドレスを入力します。

**ステップ 6**　[Directory] フィールドに、KB のあるセンサー上の場所のパスを入力します。

**ステップ 7**　[File Name] フィールドに、KB のファイル名を入力します。

**ステップ 8**　[Virtual Sensor] ドロップダウン リストから、この KB を適用する仮想センサーを選択します。

**ステップ 9**　[Save As] フィールドに、新しい KB の名前を入力します。

**ステップ 10**　[Username] フィールドに、センサーに定義されているユーザ アカウントに対応するユーザ名を入力します。

**ステップ 11**　[Password] フィールドに、センサーに定義されているユーザ アカウントのパスワードを入力します。

**ヒント**　変更を廃棄して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 12**　[Apply] をクリックします。新しい KB が [Anomaly Detection] ペインのリストに表示されます。

# OS ID の設定

ここでは、センサーの学習した OS マッピングおよびインポートした OS マッピングの表示方法について説明します。次の事項について説明します。

- 「学習したオペレーティング システムの設定」（P.17-26）
- 「インポートしたオペレーティング システムの設定」（P.17-27）

## 学習したオペレーティング システムの設定

**（注）**　[Learned OS] ペインのリストをクリアするか、エントリを削除するには、管理者またはオペレータである必要があります。

[Learned OS] ペインには、ネットワーク上のトラフィックを監視してセンサーが学習した、学習した OS マッピングが表示されます。センサーは、TCP セッション ネゴシエーションを検査して、各ホストで実行されている OS を判別します。

リストをクリアするかエントリを 1 つ削除するには、行を選択してから [Delete] をクリックします。[Refresh] をクリックして、リストを更新します。[Export] をクリックして、表に現在表示されている学習した OS をカンマ区切りの Excel ファイル（CSV を使用）または HTML ファイルにエクスポートします。Ctrl-C を使用してクリップボードに内容をコピーしておき、Ctrl-V を使用してメモ帳や Word に貼り付けることもできます。

**（注）**　パッシブ OS フィンガープリントがまだイネーブルで、ホストがまだネットワーク上で通信している場合、学習した OS マップは即座に再設定されます。

### フィールド定義

[Learned OS] ペインには、次のフィールドがあります。

- [Virtual Sensor]：OS 値が関連付けられている仮想センサー。
- [Host IP Address]：OS 値のマッピング先の IP アドレス。
- [OS Type]：この IP アドレスと関連付けられている OS タイプ。

### 学習した OS リストの値の削除およびクリア

学習した OS 値を削除するか、リスト全体をクリアするには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Dynamic Data] > [OS Identifications] > [Learned OS] を選択します。

**ステップ 3**　リスト内のエントリを削除するには、そのエントリを選択し、[Delete] をクリックします。学習した OS の値が [Learned OS] タブのリストに表示されなくなります。

**ステップ 4**　学習した OS 値の最新のリストを取得するには、[Refresh] をクリックします。学習した OS のリストがリフレッシュされます。

**ステップ 5**　学習した OS の値をすべてクリアするには、[Clear List] をクリックします。これで、学習した OS のリストは空になりました。

**ステップ 6**　学習した OS のリストを CSV 形式および HTML 形式に保存するには、[Export] をクリックします。Ctrl-C を使用して、[Learned OS] ペインの内容をコピーしてから、Ctrl-V を使用して内容をメモ帳や Word に貼り付けることもできます。

## インポートしたオペレーティング システムの設定

**（注）**　[Imported OS] ペインのリストをクリアするか、エントリを削除するには、管理者またはオペレータである必要があります。

CSA MC を外部インターフェイス製品としてセットアップした場合、[Imported OS] ペインには、センサーが CSA MC からインポートした OS マップが表示されます。外部製品インターフェイスを追加するには、[Configuration] > [External Product Interfaces] を選択します。リストをクリアするかエントリを 1 つ削除するには、行を選択してから [Delete] をクリックします。

### フィールド定義

[Imported OS] ペインには、次のフィールドがあります。

- [Host IP Address] : OS 値のマッピング先の IP アドレス。
- [OS Type] : この IP アドレスと関連付けられている OS タイプ。

### インポートした OS リストの値の削除およびクリア

インポートした OS 値を削除するか、リスト全体をクリアするには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Dynamic Data] > [OS Identifications] > [Imported OS] を選択します。

**ステップ 3**　リスト内のエントリを削除するには、そのエントリを選択し、[Delete] をクリックします。インポートした OS の値が [Imported OS] タブのリストに表示されなくなります。

**ステップ 4**　インポートした OS の値をすべてクリアするには、[Clear List] をクリックします。これで、インポートした OS のリストは空になりました。

**ステップ 5**　最新のインポートした OS 値でペインを更新するには、[Refresh] をクリックします。

# フロー状態のクリア

ここでは、センサー データベースのクリア方法について説明します。次の事項について説明します。



## [Clear Flow States] ペイン

**注意**　アラート データベースをクリアすると、進行中のすべてのサマリー アラートが削除されます。その結果、最終サマリー アラートは抑制されます。アラート データベースは、トラブルシューティングを目的とする場合に限りクリアすることを推奨します。

[Clear Flow States] ペインでは、ノード、アラート、またはインスペクタのデータベースなど、データベースの一部またはすべての内容をクリアできます。仮想センサー名を指定しなかった場合は、すべての仮想センサー データベースがクリアされます。

データベース内のノードをクリアすると、センサーは再起動時と同様に初期状態で起動します。オープンされているすべての TCP ストリーム情報は削除され、新しいパケットの受信時に新しい TCP ストリーム ノードが作成されます。

インスペクタ データベースをクリアした場合、TCP 情報および状態情報は保持されますが、今後のアラートにつながる可能性のあるすべてのインスペクション レコードは削除されます。新しいインスペクション レコードは、新しいパケットを取得すると作成されます。

アラート データベースをクリアする場合は、アラート データベース全体がクリアされます。

## [Clear Flow States] ペインのフィールド定義

[Clear Flow States] ペインには、次のフィールドがあります。

- [Clear Nodes]：パケット ノード、TCP セッション情報、インスペクタ リストなど、パケット データベース要素全体がクリアされます。
- [Clear Inspectors]：ノードに含まれているインスペクタ リストがクリアされます。TCP セッション情報およびノードはクリアされません。インスペクタ リストは、センサーの実行中に収集されたパケットの動作と監視結果を表します。
- [Clear Alerts]（非推奨）：アラート ノード、Meta インスペクタ情報、サマリー状態、イベント カウント構造を含む、アラート データベースをクリアします。

**注意**　アラート データベースをクリアすると、進行中のすべてのサマリー アラートが削除されます。その結果、最終サマリー アラートは抑制されます。アラート データベースは、トラブルシューティングを目的とする場合に限りクリアすることを推奨します。

- [Clear All]：すべての仮想センサー データベースがクリアされます。
- [Specify a Single Virtual Sensor (otherwise all virtual sensors will be cleared)]：特定の仮想センサーのデータベースをクリアできます。

## フロー状態のクリア

フロー状態をクリアするには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Properties] > [Clear Flow States] を選択します。

**ステップ 3**　クリアする値のオプション ボタンをクリックします。

- Clear Nodes
- Clear Inspectors
- Clear Alerts（非推奨）
- Clear All

**注意**　アラート データベースをクリアすると、進行中のすべてのサマリー アラートが削除されます。その結果、最終サマリー アラートは抑制されます。アラート データベースは、トラブルシューティングを目的とする場合に限りクリアすることを推奨します。

**ステップ 4**　1 つの仮想センサーのフロー状態をクリアするには、[Specify a Single Virtual Sensor (otherwise all virtual sensors will be cleared)] チェックボックスをオンにします。すべての仮想センサーのフロー状態をクリアする場合は、ステップ 6 に進みます。

**ステップ 5**　ドロップダウン リストから、フロー状態をクリアする仮想センサーを選択します。

**ステップ 6**　[Clear Flow State Now] をクリックします。

# ネットワーク セキュリティの健全性のリセット

**（注）**　ネットワーク セキュリティの健全性をリセットするには、管理者でなければなりません。

[Reset Network Security Health] ペインでは、ネットワーク セキュリティの健全性のステータスおよび計算をリセットできます。[Home] ページの [Network Security Health] ガジェットがクリアされます。仮想センサー名を指定しなかった場合は、すべての仮想センサー ネットワーク セキュリティ ヘルス情報がクリアされます。

### フィールド定義

[Reset Network Security Health] ペインには、次のフィールドがあります。

- [Specify a Single Virtual Sensor (otherwise network security for all virtual sensors will be reset)]：特定の仮想センサーのネットワーク セキュリティ データをクリアできます。

### ネットワーク セキュリティ ヘルス データのリセット

ネットワーク セキュリティ ヘルス データをリセットするには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Properties] > [Reset Network Security Health] を選択します。

**ステップ 3**　1 つの仮想センサーのネットワーク セキュリティの健全性をリセットするには、[Specify a Single Virtual Sensor (otherwise network security for all virtual sensors will be reset)] チェックボックスをオンにします。すべての仮想センサーのデータをリセットする場合は、ステップ 5 に進みます。

**ステップ 4**　ドロップダウン リストから、ネットワーク セキュリティ ヘルス データをクリアする仮想センサーを選択します。

**ステップ 5**　[Reset Network Security Health Now] をクリックします。[Home] ページの [Network Security Health] ガジェット内のデータがクリアされます。

**（注）**　[Network Security] ガジェットに表示される脅威のしきい値を変更するには、[Configuration] > [Event Action Rules] > [rules0] > [Risk Category] を選択します。

### 詳細情報

- ネットワーク セキュリティ データなど [Sensor Health] ガジェットの詳細については、「[Sensor Health] ガジェット」（P.2-4）を参照してください。
- センサー ヘルスを設定する手順については、「センサー ヘルスの設定」（P.16-9）を参照してください。
- リスク カテゴリを設定する手順については、「リスク カテゴリの設定」（P.9-35）を参照してください。

# 診断レポートの生成

**（注）**　診断を実行するには、管理者でなければなりません。

**（注）**　診断レポートの生成には、数分かかることがあります。

トラブルシューティング用に、センサーの診断情報を取得できます。診断レポートには、TAC がセンサーのトラブルシューティングに使用することを目的として、ログ、ステータス、設定などの内部システムの情報が含まれています。レポートは、[Diagnostics Report] ペインで表示したり、[Save] をクリックしてハード ディスク ドライブに保存したりできます。

### ボタンの定義

[Diagnostics Report] ペインには、次のボタンがあります。

- [Save]：[Save As] ダイアログボックスが開いて、診断レポートのコピーをハード ディスク ドライブに保存できます。
- [Generate Report]：診断プロセスが開始されます。

この処理は、完了まで数分かかることがあります。プロセスが完了すると、レポートが生成され、更新されたレポートで表示がリフレッシュされます。

### 診断レポートの生成

**注意**　診断プロセスの開始後は、IDM 内のその他いずれのオプションもクリックせず、[Diagnostics] ペインからも移動しないでください。このプロセスは、センサーの他のいずれの作業を実行するよりも前に完了する必要があります。

診断を実行するには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Support Information] > [Diagnostics Report] を選択し、[Generate Report] をクリックします。

**（注）**　この診断プロセスは、完了までに数分かかることがあります。プロセスの実行が完了すると、更新された結果で表示がリフレッシュされます。

**ステップ 3**　このレポートをファイルとして保存するには、[Save] をクリックします。[Save As] ダイアログボックスが開いて、レポートをハード ディスク ドライブに保存できます。

# 統計情報の表示

[Statistics] ペインには、次のカテゴリの統計情報が表示されます。

- 分析エンジン

  [Analysis Engine] セクションには、グローバル相関統計情報が含まれています。
- 異常検出
- イベント ストア
- 外部製品インターフェイス
- ホスト
- インターフェイス設定
- ロガー
- Network Access（現行名称は Attack Response Controller）
- 通知
- OS 識別名
- トランザクション サーバ
- 仮想センサー
- Web サーバ

### ボタンの定義

[Statistics] ペインには、次のボタンがあります。

- [Refresh]：Web サーバ、トランザクション ソース、トランザクション サーバ、Network Access Controller、ロガー、ホスト、イベント ストア、分析エンジン、インターフェイス設定、認証など、センサー アプリケーションに関する最新情報が表示されます。

（注）　Cisco IPS 5.1 以降 Attack Response Controller と呼ばれる Network Access Controller は、統計情報出力では、まだ Network Access Controller としてリストされます。

### 統計情報の表示

センサーの統計情報を表示するには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Support Information] > [Statistics] を選択します。

**ステップ 3**　変更時に統計情報が更新されるようにするには、[Refresh] をクリックします。

# システム情報の表示

[System Information] ペインには、次のような情報が表示されます。

- TAC 連絡情報
- プラットフォーム情報
- ブートしたパーティション
- ソフトウェア バージョン
- アプリケーション（MainApp、Analysis Engine、および CollaborationApp）のステータス
- インストールされたアップグレード
- PEP 情報
- メモリ使用量
- ディスク使用量

### ボタンの定義

[System Information] ペインには、次のボタンがあります。

- [Refresh]：ソフトウェア バージョンや PEP 情報など、センサーに関する最新情報が表示されます。

### システム情報の表示

システム情報を表示するには、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 IDM にログインします。

**ステップ 2**　[Monitoring] > [Sensor Monitoring] > [Support Information] > [System Information] を選択します。[System Information] ペインには、システムに関する情報が表示されます。

**ステップ 3**　[Refresh] をクリックします。ペインがリフレッシュされて、新しい情報が表示されます。