CHAPTER 20

イベント モニタリングの設定

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。他の Cisco IPS センサーは、いずれも現在 IPS 7.1 を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、IME イベント モニタリングとおよびその設定方法について説明します。内容は次のとおりです。

イベント モニタリングについて

[Event Monitoring] ペインにはイベントのビューがあります。ビューには、リアルタイム イベントまたは履歴イベント（データベースに格納されたイベント）が表示されます。IME には事前定義されたビューがあります。ユーザ独自のビューを作成することもできます。事前定義されたビューについて、削除や変更の保存を行うことはできません。[Event Monitoring] ペインの左側にビュー ツリーが表示され、右側でビューの設定や表示を行います。

[Event Monitoring] ペインの右側は 3 つの部分で構成されます。

- [View Settings]：5 つのタブがあります。これらのタブを使用して、表示するイベントや表示方法を指定します。イベントは、フィルタ、グループ、色、フィールド、およびビューの種類別に表示できます。

フィルタを使用して、ビューを詳細にリストアップできます。グループを使用して、ビュー内でデータを並べ替えることができます。色を使って、特定のデータを目立たせることができます。たとえば、特定の攻撃者 IP アドレスからのイベントを検索する場合、重大度が「高」であるイベントを強調表示して、それらのイベントに特定の色を適用できます。表示するフィールドを選択し、その順序（昇順/降順）を指定できます。

- [Events table] : ビューにイベントを表示します。ツールバーを使用するか、またはメニューを右クリックして行を選択し、さまざまなアクションを実行することで、イベントを操作できます。
- [Event Details] : [Events table] で 1 つの行を選択すると、ペインの [Event Details] セクションにそのイベントの詳細が表示されます。

[Group By]、[Color Rules]、[Fields]、および [General] タブ

[Group By] タブでは、イベントの属性に基づいてイベントをグループ化できます。グループ レベルは、最大 4 つまでネストできます。たとえば、まず重大度に基づいてグループ化し、次に攻撃者 IP アドレスに基づいてグループ化することなどができます。選択基準は、フィルタを作成する場合と同様です。

[Color Rules] タブでは、特定の基準に基づいてイベントを選択し、選択したイベントにさまざまな背景色や前景色を適用できます。選択基準は、フィルタを作成する場合と同様です。色は上から下に向かって適用する必要があります。最初の一致で、色規則が適用されます。

[Fields] タブでは、イベント データを参照したいフィールドの追加や削除を行うことができます。また、それらのフィールドをリスト内で上下に移動させて、表示する順序を設定できます。選択基準は、フィルタを作成する場合と同様です。

[General] タブでは、ビューを選択して説明を加えることができます。事前定義されたビューと作成したビューを利用できます。これらのビューは、[Event Monitoring] ペインの左側の [Event Views] ツリーに表示されます。

フィルタについて

（注） [Filter] タブと [Add Filter] ダイアログボックスのフィールドで IPv6 アドレスおよび IPv4 アドレスがサポートされるようになりました。

IME では特定のビューのフィルタリング プロパティを設定できるため、参照したいイベントだけを表示することが可能です。イベントにフィルタを適用しないと、すべてのイベントが表示されます。フィルタを適用すると、フィルタに指定した基準に一致するイベントだけが表示されます。

参照したい情報だけをビューに表示するように、さまざまな基準を使用してフィルタを作成できます。イベントは、1 つのレベルまたは列を使ってグループ化できます。また、次の基準を使ってグループ化することも可能です。

- 重大度
- 日付
- 時刻
- デバイス
- シグニチャ名

- シグニチャ ID
- 攻撃者の IP アドレス
- 攻撃対象者の IP アドレス
- 実行されたアクション
- 攻撃対象者のポート
- 脅威レーティング
- リスク レーティング
- レピュテーション

ワンポイントアドバイス　たとえば、重大度が「高」のすべてのイベントに関心がある場合、フィルタの [Severity] セクションで [High] チェックボックスをオンにしてフィルタを作成します。このフィルタを適用すると、重大度が「高」のイベントだけが表示されます。

事前定義されたフィルタを使用するか、または新しいフィルタを追加することができます。事前定義されたフィルタの編集や削除を行うことはできません。各フィールドには、カンマ区切りの値を入力します。フィールドでは、1 つのエントリ、範囲、および NOT 演算子がサポートされます。たとえば、[attacker IP address] では、次の形式がサポートされます。

- 10.1.1.1,10.1.1.5
- 10.1.1.1-10.1.1.15
- !10.1.1.1

（注）　感嘆符（!）は「除外する」ことを意味します。

フィルタを使用して、次のようなクエリを実行できます。

- Attacker IP address（攻撃者 IP アドレス）が 10.1.1.1 または 10.1.1.5 で、Signature ID（シグニチャ ID）が ID 5042 のイベントを表示する
- Risk rating（リスク レーティング）が 75-100 で、Attacker IP address（攻撃者 IP アドレス）が 192.2.3.3 のイベントを表示する

これらのフィルタ定義は、[Manage Filter Rules] ダイアログボックスに表示されます。[Risk Rating]、[Threat Rating]、[Destination Port] の各フィールドでは、次の形式がサポートされます。

- =
- !=
- >
- >=
- <
- <=
- 範囲内
- 範囲外

[Filter] タブおよび [Add Filter] ダイアログボックスのフィールド定義

[Filter] タブおよび [Add Filter] ダイアログボックスには、次のフィールドが表示されます。

- [Filter Name]：このフィルタの名前を入力するか、デフォルトのフィルタ名から選択できます。
- [Attacker IP]：このフィルタに含める攻撃者の IP アドレス。有効な値は、*ip_address* および *ip_address_range* です（例：10.0.0.1、!10.0.0.1、!10.1.1.1）。

  （注）　感嘆符（!）は「除外する」ことを意味します。

- [Victim IP]：このフィルタに含める攻撃対象の IP アドレス。有効な値は、*ip_address* および *ip_address_range* です（例：10.0.0.1、!10.0.0.1、!10.1.1.1）。
- [Signature Name/ID]：このフィルタに含めるシグニチャの名前/ID。有効な値は、*signature_name*、*signature_id*、*signature_id/subsig_id*、または *signature_id_range* です。次に例を示します。
  - no_checkpoint
  - no_checkpoint, 3320
  - no_checkpoint, 3320/1
  - 3300-400
- [Victim Port]：このフィルタに含める攻撃対象ポート。有効な値は、*number または number_range* です（例：>=80、70-100、<90、!100）。
- [Severity]：このフィルタに含める重大度。
- [Risk Rating]：このフィルタに含めるリスク レーティング。有効な値は、*number または number_range* です（例：>=80、70-100、<90、!100）。
- [Reputation]：このフィルタに含めるレピュテーション スコア。有効値の範囲は、-10.0 ～ 10.0 です。
- [Threat Rating]：このフィルタに含める脅威レーティング。有効な値は、*number または number_range* です（例：>=80、70-100、<90、!100）。
- [Action(s) Taken]：フィルタがアラート内で検索するアクションを選択できます。アクションは文字列であり、選択することもできれば、自由形式で入力することも可能です。
- [Sensor Name(s)]：このフィルタに含めるセンサーを指定できます。
- [Virtual Sensor]：このフィルタに含める仮想センサーを指定できます。
- [Status]：このフィルタにステータス（[All]、[New]、[Assigned]、[Closed]、[Detected]、[Acknowledged]）を割り当てることができます。

  [Status] フィールドは、特定のイベントの分析結果を後で使用するために保存しておく場合などに役立ちます。注釈を追加し、ステータスを [Acknowledged] に変更することにより、ステータスでフィルタ処理を実行し、承認されたケースをすべて表示して、追加の分析を行うことができます。
- [Victim Locality]：フィルタ処理を行う参加/アドレス アラート内のアラート属性。この属性は、イベント アクション規則変数に定義されます。
- [Color Parameters]：イベントの色規則を設定できます（次のオプションは [Color Rules] タブでフィルタを追加する場合にのみ表示されます）。
  - [Foreground]：イベントの前景色が表示され、使用する色を選択できます。

- [Background]：イベントの背景色が表示され、使用する色を選択できます。
- [Font Type]：イベントのフォント タイプとして、太字、イタリック、またはその両方を選択できます。
- [Preview Text]：イベントがビューにどのように表示されるかを確認できます。

イベント ビューの操作

イベント ビューを操作するには、次の手順を実行します。

ステップ 1　[Event Monitoring] > [Event Monitoring] > [Event Views] を選択します。

[Event Monitoring] ペインの左側に、事前定義されたビューが 5 つ表示されます（[Basic View]、[Blocked Attacks View]、[Dropped Attacks View]、[Grouped Severity View]、and [Real-Time Colored View]）。イベントは、[View] ペインの下部に表示されます。

ステップ 2　ビューを作成するには、[New] をクリックします。

ステップ 3　[New View] ダイアログボックスの [Name] フィールドにビューの名前を入力し、[OK] をクリックします。マイ ビューの下にあるペインの左側に、新しいビューが表示されます。1 つのイベントに対して、フィルタを作成して適用できます。

詳細情報

- 1 つのイベントを調べる手順については、「1 つのイベントを調べる」（P.20-5）を参照してください。
- フィルタを作成して適用する手順については、「イベント ビューのフィルタの設定」（P.20-7）を参照してください。

1 つのイベントを調べる

1 つのイベントを調べるには、次の手順を実行します。

ステップ 1　[Event Monitoring] > [Event Monitoring] > [Event Views] > [Basic View] を選択します。

ステップ 2　イベントを収集する期間を設定します。

ステップ 3　1 つのイベントを調べるには、リストでイベントを選択し、ツールバーの [Event] をクリックします。[Event] ドロップダウン リストから、次の情報を表示できます（これらの情報は、ウィンドウの下部にタブ形式で表示される [Event Details] セクションにも表示されます）。

- [Summary]：そのイベントに関する情報の要約が表示されます。
- [Explanation]：そのイベントに関連付けられたシグニチャの説明および関連シグニチャ情報が表示されます。
- [Related Threats]：関連する脅威と MySDN 内の詳細情報へのリンクが表示されます。
- [Trigger Packet]：イベントをトリガーしたパケットに関する情報が表示されます。
- [Context Data]：パケット コンテキスト情報が表示されます。
- [Actions Taken]：展開されたイベント アクションのリストが表示されます。

- [Notes]：イベントに名称（New、Assigned、Acknowledged、Closed、または Deleted）を割り当てることにより、イベントに対してアクションを実行できます。[Notes] フィールドに注釈を入力し、[Save Note] をクリックして保存します。

ステップ 4　このイベントの詳細を印刷するには、[Show All Details] をクリックして、イベントの詳細をプリンタ対応のウィンドウに表示します。

ステップ 5　選択したイベントから属性を追加するには、[Filter] ドロップダウン メニューから [Add to Filter] > [Attacker IP/Victim IP/Signature ID] を選択します。ウィンドウの上部に [Filter] タブが表示されます。

ステップ 6　このイベントからフィルタを作成するには、[Filter] ドロップダウン メニューから [Create a Filter] を選択します。

ステップ 7　このイベントに関連付けられたシグニチャを編集するには、[Edit Signature] をクリックします。[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] へ移動し、シグニチャを編集できます。

ステップ 8　このイベントからイベント アクション規則フィルタを作成するには、[Create Rule] をクリックします。[Configuration] > *sensor_name* > [Policies] > [IPS Policies] > [Add Event Action Filter] へ移動し、イベント アクション規則フィルタを追加できます。

ステップ 9　攻撃者を阻止するには、[Stop Attacker] ドロップダウン メニューから次のオプションのいずれかを選択します。

- [Using Inline Deny]：このオプションを選択すると、[Configuration] > *sensor_name* > [Sensor Monitoring] > [Time-Based Actions] > [Denied Attackers] > [Add Denied Attacker] へ移動します。
- [Using Block on another device]：このオプションを選択すると、[Configuration] > *sensor_name* > [Sensor Monitoring] > [Time-Based Actions] > [Host Blocks] > [Add Host Block] へ移動します。

ステップ 10　このイベントに関係する IP アドレスに対して ping、traceroute、DNS、および whois を実行するには、これらのコマンドを [Tools] ドロップダウン メニューから選択します。

ping を使用すると、基本的なネットワーク接続を診断できます。ping により、センサーが応答するかどうかを簡単に確認できます。traceroute を使用すると、IP パケットが宛先に到達するまでのルートを表示できます。whois を使用すると、ドメイン名または IP アドレスの所有者を確認できます。DNS ルックアップを使用すると、電話帳を調べるように、ホスト名を IP アドレスに変換できます。

ステップ 11　イベントを保存、削除、またはコピーするには、[Other] ドロップダウン リストから実行するアクションを選択します。

ステップ 12　ビューに加えた変更を保存するには、[Apply] をクリックします。変更を破棄する場合は、[Reset] をクリックします。

詳細情報

- フィルタを追加する手順については、「イベント ビューのフィルタの設定」（P.20-7）を参照してください。
- イベント アクション規則フィルタを追加する手順については、「イベント アクション フィルタの設定」（P.11-16）を参照してください。
- 拒否攻撃者を追加する手順については、「拒否攻撃者の設定とモニタリング」（P.19-4）を参照してください。
- ホスト ブロックを追加する手順については、「ホスト ブロックの追加、削除、管理」（P.19-8）を参照してください。
- ツールの詳細については、「デバイスでのツールの使用」（P.2-6）を参照してください。

イベント ビューのフィルタの設定

（注）　[Filter] タブと [Add Filter] ダイアログボックスのフィールドで IPv6 アドレスおよび IPv4 アドレスがサポートされるようになりました。

フィルタを設定するには、次の手順を実行します。

ステップ 1　[Event Monitoring] を選択し、[New] をクリックします。

ヒント　リストで複数の項目を選択するには、**Ctrl** キーを押しながらクリックします。

ステップ 2　[New View] ダイアログボックスで、新しいビューの名前を入力します。ビュー ツリーのマイ ビューの下に、新しいビューが表示されます。

ステップ 3　[View Settings] > [Filter] をクリックします。

ステップ 4　[Filter Name] ドロップダウン メニューから、このフィルタのフィルタ名を選択するか、[Note] アイコンをクリックしてから [Add] をクリックし、新しいファイルを追加します。

a. [Filter Name] フィールドに、このフィルタの名前を入力します。

b. [Attacker IP] フィールドに攻撃者の IP アドレスを入力するか、[Note] アイコンをクリックして一意の IP アドレスまたは IP アドレスの範囲を追加し、[OK] をクリックします。

c. [Victim IP] フィールドに攻撃対象の IP アドレスを入力するか、[Note] アイコンをクリックして一意の IP アドレスまたは IP アドレスの範囲を追加し、[OK] をクリックします。

d. [Signature Name/ID] フィールドにシグニチャ名またはシグニチャ ID を入力するか、[Note] アイコンをクリックし、シグニチャ タイプを選択して、[OK] をクリックします。

e. [Victim Port] フィールドに攻撃対象ポートを入力するか、[Note] アイコンをクリックして必要な条件を満たす攻撃対象ポートを入力し、[OK] をクリックします。

f. このフィルタの重大度を選択します。

g. [Risk Rating] フィールドに、このフィルタのリスク レーティングを入力するか、[Note] アイコンをクリックして必要な条件を満たすリスク レーティングを入力し、[OK] をクリックします。

h. [Reputation] フィールドに、このフィルタのレピュテーション スコアを入力するか、[Note] アイコンをクリックして必要な条件を満たすレピュテーションを入力し、[OK] をクリックします。

i. [Threat Rating] フィールドに、このフィルタの脅威レーティングを入力するか、[Note] アイコンをクリックして必要な条件を満たす脅威レーティングを入力し、[OK] をクリックします。

j. [Actions Taken] フィールドに、このフィルタをトリガーするアクションを入力するか、[Note] アイコンをクリックして、このフィルタをトリガーするアクションのチェックボックスをオンにし、[OK] をクリックします。

k. [Sensor Name(s)] フィールドに、このフィルタの影響を受けるセンサーの名前を入力するか、[Note] アイコンをクリックして、このフィルタを適用するセンサーのチェックボックスをオンにし、[OK] をクリックします。

l. [Virtual Sensor] フィールドに、このフィルタを適用する仮想センサーを入力します。

m. [Status] ドロップダウン メニューから、フィルタ処理を行うステータスを選択します。

n. [Victim Locality] フィールドに、フィルタ処理の対象とする作成済みのイベント アクション規則変数の名前を入力します。

ステップ 5　グループを設定するには、[Group By] タブをクリックします。

a. [Group events based on the following criteria] チェックボックスをオンにし、ドロップダウン メニューからカテゴリを選択することにより、イベントをグループ化するための階層を構築します。

b. [Grouping Preferences] で、[Single Level]、[Show Group Columns]、[Show Count Columns] の各チェックボックスをオンにできます。[Show Group Columns] チェックボックスをオンにした場合は、カウント カラムのみを表示できます。

ステップ 6　色規則を追加するには、[Color Rules] タブをクリックしてから [Add] をクリックします。

a. [Filter Name] フィールドに、この色規則フィルタの名前を入力します。

b. [Enable] チェックボックスをオンにします。

（注） [Enable] チェックボックスをオンにしなければ、色規則フィルタは有効になりません。

c. [Packet Parameters] では、この色規則フィルタを適用する IP アドレス、シグニチャ名、攻撃対象ポートを入力します。

d. [Rating and Action Parameters] では、この色規則フィルタを適用する重大度、リスク レーティング、脅威レーティング、およびアクションを入力します。

e. [Other Parameters] では、この色規則フィルタを適用するセンサー名、仮想センサー名、ステータス、攻撃対象の所在地を入力します。

f. [Color Parameters] では、この色規則フィルタの前景色、背景色、およびフォント タイプを選択し、[OK] をクリックします。

ヒント これらのフィールドに入力する値の正しい形式を確認するために、[Note] アイコンをクリックしてください。

ステップ 7　フィールドとその順序を編集するには、[Fields] タブをクリックし、[Add >>]、[<< Remove]、[Move Up]、および [Move Down] をクリックして、表示するフィールドを選択し、希望する順序どおりにフィールドを並べ替えます。

ステップ 8　[General] タブをクリックし、[View Description] フィールドをクリックして、ビューの説明を入力します。

ステップ 9　[Save As] をクリックして新しいビューを作成し、[Name] フィールドにビューの名前を入力します。設定が新しいビューにコピーされます。

ステップ 10　[Save] をクリックして、ビューに加えた変更を保存します。フィルタが [Filter Name] ドロップダウン メニューに表示されます。

ステップ 11　ビューに加えた変更を保存するには、[Apply] をクリックします。変更を破棄する場合は、[Reset] をクリックします。