CHAPTER 21

レポートの設定と生成

（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 レポートについて説明し、その設定と生成についても取り上げます。内容は次のとおりです。

IME レポートについて

IME では、さまざまなフィルタを使用してカスタマイズ可能な各種レポートを作成できます。レポートは、棒グラフまたは円グラフを示すウィンドウで構成されます。ウィンドウにはグラフの作成に使用された表形式のデータも表示されます。

IME レポートには、次の 6 種類があります。

- 上位攻撃者（Top Attacker）レポート：一定の時間における上位攻撃者の IP アドレスを示します。上位何番目までの攻撃者の IP アドレスを表示するかを指定できます。上位攻撃者（Top Attacker）レポートには、事前定義されたレポートが 4 つあります。
  - 上位攻撃者（基本）（Basic Top Attacker）
  - 上位 10 攻撃者（直前の 1 時間）（Top 10 Attackers Last 1 Hour）
  - 上位 10 攻撃者（直前の 8 時間、重大度高）（Top 10 Attackers Last 8 Hours with High Severity）
  - 上位 20 主要攻撃者（直前の 24 時間）（Top 20 Critical Attackers Last 24 Hours）
- 上位攻撃対象（Top Victim）レポート：一定の時間における上位攻撃対象者の IP アドレスを示します。上位何番目までの攻撃対象者の IP アドレスを表示するかを指定できます。上位攻撃対象（Top Victim）レポートには、事前定義されたレポートが 4 つあります。
  - 上位攻撃対象者（基本）（Basic Top Victim）
  - 上位 10 攻撃対象者（直前の 1 時間）（Top 10 Victims Last 1 Hour）

  - 上位 10 攻撃対象者（直前の 8 時間、重大度高）（Top 10 Victims Last 8 Hours with High Severity）
  - 上位 20 攻撃対象者（アクションが拒否された攻撃者情報あり）（Top 20 Victims with Action Denied Attacker）
- 上位シグニチャ（Top Signature）レポート：一定の時間において開始された上位シグニチャを示します。上位何番目までのシグニチャを表示するかを指定できます。上位シグニチャ（Top Signature）レポートには、事前定義されたレポートが 4 つあります。
  - 上位シグニチャ（基本）（Basic Top Signature）
  - 上位 10 シグニチャ（直前の 1 時間）（Top 10 Signatures Last 1 Hour）
  - 上位 10 シグニチャ（直前の 8 時間、重大度高）（Top 10 Signatures Last 8 Hours with High Severity）
  - 上位 20 シグニチャ（直前の 24 時間）（Top 20 Critical Signatures Last 24 Hours）
- 攻撃（Attacks Over Time）レポート：一定の時間における攻撃を示します。事前定義されたレポートが 5 つあります。
  - 攻撃（基本）（Basic Over Time Attack）
  - ブロックされた攻撃（直前の 24 時間）（Attacks Blocked in Last 24 Hours）
  - ドロップされた攻撃（直前の 24 時間）（Attacks Dropped in Last 24 Hours）
  - 攻撃（直前の 1 時間）（Attacks Over Time Last 1 Hour）
  - 重大な攻撃（直前の 24 時間）（Critical Attacks Over Last 24 Hours）
- フィルタ処理されたイベントとすべてのイベント（Filtered Events vs All Events）レポート：一定期間における、全イベントに対する一連のイベントを表示します。事前定義されたレポートが 1 つあります。
  - ネガティブ レピュテーション イベント（Negative Reputation Events）
- グローバル相関レポート：センサーの実行が開始された後のグローバル相関レポートを表示します。グローバル相関レポートには、事前定義されたレポートが 2 つあります。
  - レピュテーション フィルタ（Reputation Filter）
  - グローバル相関

ユーザ定義のレポートとデモ レポート（事前定義されたレポートのサンプル）もあります。

[Reports] ウィンドウは、2 つの部分に分かれています。左側ペインの [Report] ツリーには、レポートリストがツリー形式で表示されます。右側ペインの [Report Settings] ペインには、レポートが表示されます。[Report] ツリーには、事前定義された一連のレポート（上位攻撃者（基本）（Basic Top Attacker）など）や、[My Reports] ノード下にユーザ定義レポートを保存する場所が含まれます。リストからレポートを選択し、[Generate Report] をクリックすると、[Report Settings] ペインの下半分に、対応するレポートがグラフや表とともに表示されます。[Reports Setting] ペインには [General] と [Filter] という 2 つのタブがあり、これらのタブを使用してレポートをカスタマイズできます。

IME では、レポートを PDF または RTF ファイルとして保存したり、印刷したりすることもできます。

（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。

レポートの設定と生成

（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。

レポートに含める項目数と時間間隔を設定して、レポートをカスタマイズできます。IP アドレスの解決には、DNS を使用することもできます。フィルタを使用して、レポートに含める情報の種類をさらに絞り込むこともできます。

レポートの設定および生成を行うには、次の手順を実行します。

ステップ 1　[Report] ツリーで [New] をクリックして表示される [New Report] ダイアログボックスに、新しいレポートの名前を入力し、ドロップダウン リストからレポートの種類を選択して、[OK] をクリックします。[Report] ツリーの [My Reports] に、新しいレポートが表示されます。

ステップ 2　レポートを選択し、[General] タブでレポートを設定します。

- **a.** [Report Description] フィールドに、このレポートの説明を入力します。
- **b.** [Top] フィールドに、このレポートに上位何番目までのイベントを表示するかを入力します。
- **c.** DNS アドレス解決を使用する場合は、[Resolve Addresses Using DNS] チェックボックスをオンにします。
- **d.** 期間を入力するか、カスタム時間を入力して、このレポートの時間間隔を設定します。

ステップ 3　[Filter] タブの [Filter Name] ドロップダウン メニューからフィルタ名を選択するか、またはフィルタを追加して、[Note] アイコンをクリックします。

ステップ 4　[Manage Filter Rules] ダイアログボックスで、レポートのフィルタ フィールドを設定します。

ステップ 5　[Generate Report] をクリックします。統計情報（グラフ形式と表形式）とともに、レポートが [Report Settings] ペインの下半分に表示されます。

ステップ 6　表示をカスタマイズするには、[Display Type] ドロップダウン メニューで [Bar] または [Pie Chart] を選択します。

ステップ 7　[Print] をクリックしてレポートを印刷するか、または [Save] をクリックしてレポートを PDF 形式か RFT 形式でハードディスク ドライブに保存します。

ステップ 8　1 つの IP アドレスに関するイベントを表示するには、[Events for] ドロップダウン リストから IP アドレスを選択します。

詳細情報

- フィルタを作成する手順については、「フィルタの設定」（P.3-17）を参照してください。
- 1 つの IP アドレスに関するイベントを設定する手順については、「個々の上位攻撃者および上位攻撃対象の IP アドレスに対する 1 つのイベントを調べる」（P.3-14）を参照してください。
- 1 つのシグニチャに関するイベントを設定する手順については、「上位シグニチャに対する 1 つのイベントを調べる」（P.3-16）を参照してください。