



# パケットダンプ機能の管理

パケットダンプ キャプチャ機能を使用すると、ネットワークの動作を阻害しないネットワーク タップを使用して、ゾーンのトラフィックのパターンを記録および観察することができます。

この章は、次の項で構成されています。

- [パケットダンプ キャプチャの概要](#)
- [自動パケットダンプ キャプチャのイネーブル化とディセーブル化](#)
- [手動パケットダンプ キャプチャのアクティブ化](#)
- [パケットダンプ キャプチャの表示](#)
- [パケットダンプ キャプチャ ファイルの管理](#)
- [パケットダンプのシグニチャの抽出と使用](#)

## パケットダンプ キャプチャの概要

ゾーンのトラフィックを記録し、記録したトラフィックからデータベースを作成するように **Detector** を設定することができます。記録したトラフィックのデータベースにクエリーを実行することにより、過去のイベントの分析やトラフィックのシグニチャの抽出を実行したり、現在のネットワークのトラフィック パターンと **Detector** が以前に通常の状態に記録したトラフィック パターンを比較することができます。

フィルタを設定すると、特定の条件に適合するトラフィックのみを **Detector** で記録することができます。また、すべてのトラフィック データを記録して、**Detector** で表示するデータをフィルタリングすることもできます。**Detector** は、トラフィックを **gzip** 圧縮された **Packet Capture (PCAP)** 形式で保存し、記録されたデータを記述した **Extensible Markup Language (XML)** 形式のファイルがこれに付属します。

パケットダンプ機能の重要な用途は、パケットダンプ キャプチャに含まれている攻撃パケットのペイロードに、共通のパターン (シグニチャ) が現れているかどうかを特定することです。**Detector** では、パケットダンプ キャプチャを分析し、発見した任意のシグニチャを抽出することができます。シグニチャ情報を使用してフレックスコンテンツ フィルタを作成すると、シグニチャに一致するパケット ペイロードを含んでいるトラフィックをすべてブロックできます。

**Detector** は、次の 2 つの方法でトラフィックを記録します。

- 自動パケットダンプ キャプチャ : **Detector** は、トラフィック データを継続的にパケットダンプ キャプチャ ファイルに記録します。
- 手動パケットダンプ キャプチャ : **Detector** は、この機能をアクティブにしたときにトラフィックをパケットダンプ キャプチャ ファイルに記録します。

新しい自動パケットダンプ キャプチャ ファイルによって、以前のファイルは置き換えられます。記録したトラフィックを保存するには、**Detector** でもう一度トラフィックを記録する前に、パケットダンプ キャプチャ ファイルを FTP サーバにエクスポートします。ゾーンに対して同時にアクティブにできる手動パケットダンプ キャプチャは、1 つのみです。ただし、手動パケットダンプ キャプチャと自動パケットダンプ キャプチャを同時にアクティブにすることはできません。**Detector** でトラフィックを手動で同時に記録できるゾーンの数は、最大で 10 です。

デフォルトでは、Detector は、すべてのゾーンの手動パケットダンプ キャプチャ ファイル用に 5 MB のディスク スペースを割り当てています。すべてのゾーンの手動および自動パケットダンプ キャプチャ ファイルは、50 MB まで保存できます。将来のパケットダンプ キャプチャ ファイルのためにディスク スペースを解放するには、古いパケットダンプ キャプチャ ファイルを削除します。

## 自動パケットダンプ キャプチャのイネーブル化とディセーブル化

自動パケットダンプ機能は、オンまたはオフに設定します。自動パケットダンプをオンにすると、Detector は継続的にゾーンのトラフィックを記録します。

自動パケットダンプ機能を設定するには、次の手順を実行します。

- 
- ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。
  - ステップ 2** ゾーンのメイン メニューの **Configuration > General** を選択します。General 画面が表示され、ゾーンの現在の設定が示されます。
  - ステップ 3** **Config** をクリックします。Config 画面が表示されます。
  - ステップ 4** Zone Form の Packet-Dump parameters 領域で、次のいずれかのオプションをクリックします。
    - **On** : 自動パケットダンプ キャプチャ機能をイネーブルにします。
    - **Off** : 自動パケットダンプ キャプチャ機能をディセーブルにします。
  - ステップ 5** パケットダンプに使用するディスク スペースの最大容量を入力します。ディスク スペースの単位は、メガバイト (MB) で指定します。
  - ステップ 6** 次のいずれかのオプションをクリックします。
    - **OK** : 自動パケットダンプの設定をゾーンの設定の一部として保存します。自動パケットダンプ キャプチャ機能をイネーブルにした場合、Detector はすべてのゾーン トラフィックの記録を開始します。
    - **Clear** : フォームの情報をデフォルト値に戻し、追加した情報をすべて消去します。
    - **Cancel** : 情報を保存せずに Config 画面を終了します。
-

## 手動パケットダンプ キャプチャのアクティブ化

この項の手順では、Detector で手動パケットダンプ キャプチャの開始と終了のタイミングを制御する方法について説明します。手動パケットダンプ キャプチャは、ゾーンごとに 1 つのみアクティブにできます。自動パケットダンプ キャプチャとともにアクティブにすることもできます。

デフォルトでは、Detector は、すべてのゾーンの手動パケットダンプ キャプチャファイル用に 5 MB のディスク スペースを割り当てています。すべてのゾーンの手動および自動パケットダンプ キャプチャ ファイルは、50 MB まで保存できません。将来のパケットダンプ キャプチャ ファイルのためにディスク スペースを解放するには、不要になったパケットダンプ キャプチャ ファイルをすべて削除します（「[パケットダンプ キャプチャ ファイルの削除](#)」の項を参照）。

この項では、次の手順について説明します。

- [手動パケットダンプ キャプチャの開始](#)
- [手動パケットダンプ キャプチャの停止](#)

### 手動パケットダンプ キャプチャの開始

手動パケットダンプ キャプチャを開始するには、事前にゾーンをアクティブ（ゾーンのトラフィックをラーニングしているか、異常を検出している）にする必要があります。

手動パケットダンプ キャプチャを開始するには、次の手順を実行します。

- 
- ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。
  - ステップ 2** ゾーンのメイン メニューの **Diagnostics > Packet-Dump > Start Packet-Dump** を選択します。Start Packet-Dump 画面が表示されます。
  - ステップ 3** パケットダンプ キャプチャのパラメータを設定します。表 11-1 に、Start Packet-Dump Form に表示されるパラメータの説明を示します。

表 11-1 Start Packet-Dump Form のパラメータ

パラメータ	説明
Capture name	パケットダンプに割り当てられる名前。1 ～ 63 文字の英数字文字列を入力します。文字列にアンダースコア ( _ ) を含めることはできますが、スペースを含めることはできません。
Packet-Dump filter	(オプション) 記録するトラフィックを指定するために定義するフィルタ。Detector は、フィルタの式に適合するトラフィックのみをキャプチャします。この式の規則は、フレックスコンテンツ フィルタの式の規則と同じです (第 5 章「ゾーンのフィルタの設定」のフレックスコンテンツ フィルタの式の構文についてを参照)。
Dispatch value	Detector がキャプチャするゾーンのトラフィック。トラフィックのタイプをドロップダウン リストから選択します。 <ul style="list-style-type: none"> <li>• <b>all</b> : すべてのトラフィックをキャプチャします。</li> <li>• <b>dropped</b> : Detector がドロップしたトラフィックのみをキャプチャします。</li> <li>• <b>forwarded</b> : Detector がゾーンに転送する正当なトラフィックのみをキャプチャします。</li> <li>• <b>replied</b> : 検証の試行で Detector のスプーフィング防止機能およびゾンビ防止機能が送信元に返送したトラフィックのみをキャプチャします。</li> </ul>

表 11-1 Start Packet-Dump Form のパラメータ (続き)

パラメータ	説明
Sample rate	<p>サンプリング レート (pps 単位)。1 ~ 10000 の値を入力します。</p> <p>Detector は、同時に実行される手動キャプチャの累積で最大 10000 パケット / 秒のパケットダンプ キャプチャ レートをサポートします。</p> <p>パケットダンプ キャプチャのサンプリング レートを大きな値に設定すると、リソースの消費量が多くなります。パフォーマンスが低下する可能性があるため、大きいサンプリング レート値を使用する場合は注意してください。</p>
Number of packets	<p>記録するパケットの数。指定した数のパケットを記録すると、Detector は手動パケットダンプ キャプチャを停止し、情報をキャプチャのバッファからファイルに保存します。1 ~ 5000 の整数を入力します。</p>

**ステップ 4** 次のいずれかのオプションをクリックします。

- **OK** : パケットダンプ キャプチャのパラメータを保存します。Detector は、キャプチャおよびローカル データベースへの情報の記録を開始します。
- **Clear** : フォームの情報をデフォルト値に戻し、追加した情報をすべて消去します。
- **Cancel** : 情報を保存せずに Start Packet-Dump 画面を終了します。

## 手動パケットダンプ キャプチャの停止

キャプチャをアクティブにした場合、Detector は指定した数のパケットを記録すると手動パケットダンプ キャプチャを停止します。ただし、手動パケットダンプ キャプチャは、Detector が指定した数のパケットを記録する前でも停止できません。

手動パケットダンプ キャプチャを停止するには、次の手順を実行します。

- 
- ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。
- ステップ 2** ゾーンのメイン メニューの **Diagnostics > Packet-Dump > Stop Packet-Dump** を選択します。手動パケットダンプ キャプチャが停止します。
-



## パケットダンプ キャプチャの表示

この項の手順では、パケットダンプ キャプチャの詳細の表示、2つのパケットダンプ キャプチャの比較など、さまざまなパケットダンプ キャプチャ表示オプションにアクセスする方法について説明します。

この項では、次の手順について説明します。

- [パケットダンプ キャプチャのリストの表示](#)
- [パケットダンプ キャプチャの詳細の表示](#)
- [Packet-Dump Capture details 画面の表示の変更](#)
- [2つのパケットダンプ キャプチャの比較](#)

## パケットダンプ キャプチャのリストの表示

パケットダンプ キャプチャのリストを表示するには、次の手順を実行します。

- 
- ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。
- ステップ 2** ゾーンのメイン メニューの **Diagnostics > Packet-Dump > Packet dump list** を選択します。Packet-Dump list 画面が表示されます。
- 

表 11-2 に、パケットダンプのリストに含まれているフィールドの説明を示します。

表 11-2 パケットダンプのリスト

フィールド	説明
Name	パケットダンプ キャプチャに割り当てられている名前。
Start Time	パケットダンプ キャプチャを開始した日時。
Stop Time	パケットダンプ キャプチャを終了した日時。
Type	パケットダンプ キャプチャのタイプ（自動または手動）。
Size	パケットダンプ キャプチャによって生成されるファイルのサイズ。

## ■ パケットダンプ キャプチャの表示

表 11-2 パケットダンプのリスト (続き)

フィールド	説明
Packet Dump Filter	キャプチャ ファイルに記録した情報に Detector が適用したユーザ定義フィルタ。
Dispatch	Detector が記録したトラフィックのタイプ。次の 4 つのタイプがあります。 <ul style="list-style-type: none"> <li>• <b>All</b> : すべてのトラフィック。</li> <li>• <b>Dropped</b> : Detector がドロップしたトラフィックのみ。</li> <li>• <b>Forwarded</b> : Detector がゾーンに転送する正当なトラフィックのみ。</li> <li>• <b>Replied</b> : 検証の試行で Detector のスプーフィング防止機能およびゾンビ防止機能が送信元に返送したトラフィックのみ。</li> </ul>

表 11-3 に、Packet-Dump list 画面の機能ボタンの説明を示します。

表 11-3 Packet-Dump list 画面の機能ボタン

ボタン	説明
Stop/Start	手動パケットダンプの動作を制御します。現在の動作ステータスに応じて、手動パケットダンプ機能を Stop または Start に切り替えます。  次のいずれかをクリックします。 <ul style="list-style-type: none"> <li>• <b>Start</b> : 手動パケットダンプ キャプチャを開始します。このボタンは、手動パケットダンプが動作していないときのみ表示されます。</li> <li>• <b>Stop</b> : 現在の手動パケットダンプ キャプチャを終了します。このボタンは、手動パケットダンプ機能が動作しているときのみ表示されます。</li> </ul>
View	パケットダンプ キャプチャの詳細情報を 2 つまで表示します (「 <a href="#">パケットダンプ キャプチャの詳細の表示</a> 」および「 <a href="#">2 つのパケットダンプ キャプチャの比較</a> 」の項を参照)。

表 11-3 Packet-Dump list 画面の機能ボタン (続き)

ボタン	説明
Rename	パケットダンプ キャプチャに新しいファイル名を適用します (「 <a href="#">手動パケットダンプ キャプチャ ファイルの名前変更</a> 」の項を参照)。
Copy	パケットダンプ キャプチャをコピーします (「 <a href="#">パケットダンプ キャプチャの全体コピーの保存</a> 」の項を参照)。
Export/Import	パケットダンプ キャプチャをアップロードまたはダウンロードします (「 <a href="#">パケットダンプ キャプチャ ファイルのエクスポート</a> 」および「 <a href="#">パケットダンプ キャプチャ ファイルのインポート</a> 」の項を参照)。
Delete	パケットダンプ キャプチャをリストおよびデータベースから削除します (「 <a href="#">パケットダンプ キャプチャ ファイルの削除</a> 」の項を参照)。

## パケットダンプ キャプチャの詳細の表示

パケットダンプ キャプチャの詳細を表示するには、次の手順を実行します。

- ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。
- ステップ 2** ゾーンのメイン メニューの **Diagnostics > Packet-Dump > Packet-Dump List** を選択します。Packet-Dump list 画面が表示されます。
- ステップ 3** 表示するパケットダンプ キャプチャの隣にあるチェックボックスをオンにします。
- ステップ 4** **View** をクリックします。Packet-Dump capture analysis 画面が表示されます。表示される情報に画面フィルタを適用する方法の詳細については、「[Packet-Dump Capture details 画面の表示の変更](#)」の項を参照してください。

## ■ パケットダンプ キャプチャの表示



(注) カラムの情報を基準として Top 20 テーブルと Packets List テーブルの情報をソートするには、テーブルのカラム ヘッダーをクリックします。

表 11-4 に、Packet-Dump capture analysis 画面の Capture Parameters 領域と View Parameters 領域に Detector が表示する情報の説明を示します。

表 11-4 パケットダンプのキャプチャと表示のパラメータ

画面領域またはボタン	パラメータ	説明
Captureparameters	Name	キャプチャ ファイルの名前。
	Start time	キャプチャの開始時刻。
	End time	キャプチャの終了時刻。
	Packets	Detector がキャプチャの期間に記録したパケット数。
	Packet Dump filter	キャプチャ ファイルに記録した情報に Detector が適用したユーザ定義フィルタ。
	Dispatch	Detector が記録したトラフィックのタイプ。次の 4 つのタイプがあります。 <ul style="list-style-type: none"> <li>• <b>All</b> : すべてのトラフィック。</li> <li>• <b>Dropped</b> : Detector がドロップしたトラフィックのみ。</li> <li>• <b>Forwarded</b> : Detector がゾーンに転送する正当なトラフィックのみ。</li> <li>• <b>Replied</b> : 検証の試行で Detector のスプーフィング防止機能およびゾンビ防止機能が送信元に返送したトラフィックのみ。</li> </ul>

表 11-4 パケットダンプのキャプチャと表示のパラメータ（続き）

画面領域またはボタン	パラメータ	説明
ViewParameters	Query	<p>Detector がキャプチャ情報の表示に使用したデータ プロファイル。</p> <ul style="list-style-type: none"> <li>• Top 20: SrcIP / DstIP / SrcPort / DstPort / Protocol</li> <li>• Distribution: SrcIP / DstIP / SrcPort / DstPort / SrcReservedPorts / DstReservedPorts / Protocol / TTL / Length</li> <li>• Packets list</li> </ul> <p>各タイプのクエリーに対して Detector がテーブル形式とグラフ形式で表示する情報の詳細については、表 11-5 を参照してください。</p>
	Display filter	表示するパケットダンプ キャプチャ情報を指定したユーザ定義フィルタ。
	Change View ボタン	表示パラメータを変更します（「 <a href="#">Packet-Dump Capture details 画面の表示の変更</a> 」の項を参照）。
Save ボタン		パケットダンプ キャプチャのコピーを別のファイル名で保存します（「 <a href="#">パケットダンプ キャプチャの全体コピーの保存</a> 」の項を参照）。
ExtractSignatures ボタン		トラフィックのシグニチャをパケットダンプ キャプチャから抽出します（「 <a href="#">パケットダンプのシグニチャの抽出と使用</a> 」の項を参照）。

表 11-5 に、選択したクエリーのタイプによって Detector が表示するテーブルとグラフの情報を示します（「[Packet-Dump Capture details 画面の表示の変更](#)」の項を参照）。

表 11-5 キャプチャパラメータのテーブルとグラフの詳細

クエリーのタイプ	パラメータ	説明
Top 20: SrcIP / DstIP / SrcPort / DstPort / Protocol	#	パケットダンプ キャプチャの実行中に、記録する各イベントに対して Detector が割り当てるシーケンス番号。
	Key	IP アドレス、ポート番号、またはプロトコル番号 (選択する Top 20 クエリータイプに応じて異なる)。
	Packets	パケットダンプ キャプチャに含まれているパケットの数。
	%	キャプチャに含まれている、Top 20 キーに関連するパケットの割合。
Distribution: SrcIP / DstIP / SrcPort / DstPort / SrcReservedPorts / DstReservedPorts / Protocol / TTL / Length	x-axis	選択する分布アトリビュートの単位。IP アドレス、ポート番号、プロトコル番号など。
	y-axis	分布アトリビュートに関連しているパケットの数。
Packets List	#	パケットダンプ キャプチャの実行中に、記録する各イベントに対して Detector が割り当てるシーケンス番号。
	Time	パケットダンプ イベントが発生した時刻。
	SrcIp	パケットの送信元 IP アドレス。
	SrcPort	パケットの送信元ポート。
	DstIp	パケットの宛先 IP アドレス。
	DstPort	パケットの宛先ポート。
	Protocol	パケットが使用しているプロトコル (番号)。
	Info	パケットに関する追加情報。

## Packet-Dump Capture details 画面の表示の変更

Packet-Dump Capture details 画面の表示を変更するには、次の手順を実行します。

- ステップ 1** Packet-Dump Capture details 画面で、**Change View** をクリックします。Change Packet-Dump View Parameters ウィンドウが表示されます。
- ステップ 2** パケットダンプ キャプチャの表示パラメータを設定します。

表 11-6 は、Change Packet-Dump View Parameters フォームのパラメータについて説明します。

**表 11-6 Change Packet-Dump View Parameters**

パラメータ	説明
Query	<p>表示するデータ プロファイル。プロファイルによって表示形式も決まります（テーブルまたはグラフ）。使用するプロファイルを Query ドロップダウンリストから選択します。</p> <ul style="list-style-type: none"> <li>• <b>TOP 20: SrcIP / DstIP / SrcPort / DstPort / Protocol</b> : 送信元 IP アドレス (SrcIP) や宛先ポート (DstPort) などの選択した Query アトリビュートに関連しているイベントを、多いものから順に 20 個表示します。この情報はテーブル形式で表示されます。</li> <li>• <b>Distribution: SrcIP / DstIP / SrcPort / DstPort / SrcReservedPorts / DstReservedPorts / Protocol / TTL / Length</b> : 選択した Query アトリビュートに関して、パケットがどのように分布しているかを示すグラフを表示します。</li> <li>• <b>Packet View</b> : 送信元 IP アドレスと宛先 IP アドレス、送信元ポートと宛先ポートなど、パケットの詳細を表示します。この情報はテーブル形式で表示されます。</li> </ul>
Display filter	<p>(オプション) 表示するパケットダンプ情報を指定するユーザ定義のフィルタ。表示フィルタの式の規則は、フレックスコンテンツ フィルタの式の規則と同じです(第 5 章「<a href="#">ゾーンのフィルタの設定</a>」の「<a href="#">フレックスコンテンツ フィルタの式の構文について</a>」を参照)。使用する表示フィルタを入力します。</p>

表 11-6 Change Packet-Dump View Parameters (続き)

パラメータ	説明
Display pattern	(オプション) パケットの内容と照合するための正規表現データ パターン (第 5 章「ゾーンのフィルタの設定」の「フレックスコンテンツ フィルタのパターンの構文について」の項を参照)。使用するデータ パターンを入力します。
Start offset	(オプション) パケット ペイロードの先頭から、パターン マッチングを開始する位置までのオフセット(バイト単位)。デフォルトは 0 (ペイロードの先頭) です。使用する開始オフセットを入力します。
End offset	(オプション) パケット ペイロードの先頭から、パターン マッチングを終了する位置までのオフセット(バイト単位)。デフォルトは、パケット長 (ペイロードの末尾) です。使用する終了オフセットを入力します。

**ステップ 3** 次のいずれかのオプションをクリックします。

- **OK** : 表示パラメータを保存します。Detector は、選択した表示パラメータに基づいてパケットダンプ キャプチャの詳細画面をアップデートします。
- **Clear** : フォームの情報をデフォルト値に戻し、追加した情報をすべて消去します。
- **Cancel** : 情報を保存せずに View Parameter ウィンドウを閉じます。

## 2 つのパケットダンプ キャプチャの比較

2 つのパケットダンプ キャプチャの詳細を比較するには、次の手順を実行します。

**ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。



- ステップ 2** ゴーンのメインメニューの **Diagnostics > Packet Dump list** を選択します。Packet-Dump list 画面が表示されます。
- ステップ 3** パケットダンプ キャプチャの隣にあるチェックボックスをオンにして、**基準** キャプチャとして表示します。
- ステップ 4** パケットダンプ キャプチャの隣にあるチェックボックスをオンにして、**参照** キャプチャとして表示します。
- ステップ 5** **View** をクリックします。Packet-Dump capture analysis 画面が表示され、基準と参照のパケットダンプ キャプチャの詳細が示されます。
- ステップ 6** (オプション) **Swap Base and Reference** をクリックして、2つのパケットキャプチャを切り替えます。基準キャプチャを参照キャプチャにして、参照キャプチャを基準キャプチャにします。シグニチャを抽出する場合は、この機能を使用します (Detector は基準キャプチャからシグニチャを抽出します)。シグニチャの抽出については、「[パケットダンプのシグニチャの抽出と使用](#)」の項を参照してください。
- 

Packet-Dump capture analysis 画面に表示される情報の詳細については、「[パケットダンプ キャプチャの詳細の表示](#)」の項を参照してください。

## パケットダンプ キャプチャ ファイルの管理

この項では、次の手順について説明します。

- 手動パケットダンプ キャプチャ ファイルの名前変更
- パケットダンプ キャプチャの全体コピーの保存
- パケットダンプ キャプチャ ファイルのフィルタ適用済みコピーの保存
- パケットダンプ キャプチャ ファイルのエクスポート
- パケットダンプ キャプチャ ファイルのインポート
- パケットダンプ キャプチャ ファイルの削除

### 手動パケットダンプ キャプチャ ファイルの名前変更

名前を変更できるのは、手動パケットダンプ キャプチャのみです。

手動パケットダンプ キャプチャの名前を変更するには、次の手順を実行します。

- 
- ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。
  - ステップ 2** ゾーンのメイン メニューの **Diagnostics > Packet Dump list** を選択します。Packet-Dump list 画面が表示されます。
  - ステップ 3** 名前を変更するパケットダンプ キャプチャの隣にあるチェックボックスをオンにし、**Rename** をクリックします。Rename ウィンドウが表示されます。
  - ステップ 4** パケットダンプ キャプチャに適用する名前を New name フィールドに入力します。パケットダンプ キャプチャの名前は英数字にします。アンダースコア ( \_ ) とハイフン ( - ) を含めることができますが、スペースを含めることはできません。
  - ステップ 5** 次のいずれかのオプションを選択します。
    - **OK** : パケットダンプ キャプチャを新しい名前でローカル データベースに保存します。
    - **Clear** : Rename Form に追加した情報をすべて消去します。

- **Cancel** : 情報を保存せずに Rename ウィンドウを閉じます。
- 

## パケットダンプ キャプチャの全体コピーの保存

保存機能を使用すると、パケットダンプ キャプチャの全体コピーをローカルデータベースに作成できます。自動パケットダンプのコピーを保存する場合、Detector は手動パケットダンプ ファイルとしてコピーを保存します。

保存機能を使用しても、元のパケットダンプ キャプチャはデータベースから削除されません。このため、新しいキャプチャのために追加のディスク スペースが必要な場合は、元のパケットダンプ キャプチャを手動で削除する必要があります（「[パケットダンプ キャプチャ ファイルの削除](#)」の項を参照）。

パケットダンプ キャプチャの全体コピーを保存するには、次の手順を実行します。

---

- ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。
- ステップ 2** ゾーンのメイン メニューの **Diagnostics > Packet Dump list** を選択します。Packet-Dump list 画面が表示されます。
- ステップ 3** コピーするパケットダンプ キャプチャの隣にあるチェックボックスをオンにします。
- ステップ 4** **View** をクリックします。Packet-Dump capture analysis 画面が表示されます。
- ステップ 5** **Save** をクリックします。Save ウィンドウが表示されます。
- ステップ 6** 新しいファイル名を New name フィールドに入力します。

## ■ パケットダンプ キャプチャ ファイルの管理

**ステップ 7** 次のいずれかのオプションを選択します。

- **OK**: パケットダンプ キャプチャの全体コピーをローカル データベースに保存します。
- **Clear**: Save Form に追加した情報をすべて消去します。
- **Cancel**: 情報を保存せずに Save ウィンドウを閉じます。

## パケットダンプ キャプチャ ファイルのフィルタ適用済みコピーの保存

コピー機能を使用すると、パケットダンプ キャプチャ ファイルのコピーを作成してフィルタを適用し、元のパケットダンプ キャプチャを一部のみ選択してコピーすることができます。

コピー機能を使用しても、元のパケットダンプ キャプチャはデータベースから削除されません。このため、新しいキャプチャのために追加のディスク スペースが必要な場合は、元のパケットダンプ キャプチャを手動で削除する必要があります（「[パケットダンプ キャプチャ ファイルの削除](#)」の項を参照）。

パケットダンプ キャプチャのフィルタ適用済みコピーを保存するには、次の手順を実行します。

**ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

**ステップ 2** ゾーンのメイン メニューの **Diagnostics > Packet Dump list** を選択します。Packet-Dump list 画面が表示されます。

**ステップ 3** コピーするパケットダンプ キャプチャの隣にあるチェックボックスをオンにし、**Copy** をクリックします。Copy (save as) ウィンドウが表示されます。

**ステップ 4** パケットダンプ キャプチャのコピーの名前を New name フィールドに入力します。パケットダンプ キャプチャの名前は英数字にします。アンダースコア ( \_ ) とハイフン ( - ) を含めることができますが、スペースを含めることはできません。

**ステップ 5** (オプション) キャプチャ全体をコピーしない場合は、パケットダンプ キャプチャのコピーに適用するフィルタを定義します。このフィルタの式の規則は、フレックスコンテンツ フィルタの式の規則と同じです (第 5 章「ゾーンのフィルタの設定」の「フレックスコンテンツ フィルタの式の構文について」を参照)。

**ステップ 6** 次のいずれかのオプションを選択します。

- **OK**: パケットダンプ キャプチャのフィルタ適用済みコピーをローカル データベースに保存します。
- **Clear**: Copy (save as) Form に追加した情報をすべて消去します。
- **Cancel**: 情報を保存せずに Copy (save as) ウィンドウを閉じます。

## パケットダンプ キャプチャ ファイルのエクスポート

パケットダンプ キャプチャ ファイルを手動でネットワーク サーバにエクスポートできます。パケットダンプ キャプチャ ファイルのエクスポートは、1 つのファイルでも、特定ゾーンのすべてのファイルでも可能です。Detector は、パケットダンプ キャプチャ ファイルを gzip 圧縮された PCAP 形式でエクスポートし、記録されたデータについて記述する XML 形式のファイルがこれに付属します。XML スキーマについては、このバージョンに付属の Capture.xsd ファイルを参照してください。

パケットダンプ キャプチャをエクスポートするには、次の手順を実行します。

**ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

**ステップ 2** ゾーンのメイン メニューの **Diagnostics > Packet-Dump > Packet-Dump List** を選択します。Packet-Dump list 画面が表示されます。

## ■ パケットダンプ キャプチャ ファイルの管理

**ステップ 3** ネットワーク サーバにコピーするパケットダンプ キャプチャの隣にあるチェックボックスをオンにし、**Export** をクリックします。すべてのパケットダンプ キャプチャを選択するには、テーブルのヘッダーにあるチェックボックスをオンにします。Export File Server Parameters ウィンドウが表示されます。

**ステップ 4** Select File Server Parameters フォームで、次のいずれかのオプションから使用するネットワーク サーバを選択して定義します。

- **Use automatic export file server definitions : CLI export packet-dump** コマンドを使用して Detector コンフィギュレーション内に定義したネットワーク サーバにパケットダンプ キャプチャ ファイルをエクスポートします。
- **Use the following server definition** : 定義したネットワーク サーバにパケットダンプ キャプチャ ファイルをエクスポートします。ネットワーク サーバに関する次の情報を入力します。

— **Transfer method** : 使用する転送プロトコルを選択します。

転送方式は、次のいずれかです。

**FTP** : FTP サーバにパケットダンプ キャプチャ ファイルをエクスポートします。

**SFTP** : Secure FTP (SFTP) サーバにパケットダンプ キャプチャ ファイルをエクスポートします。

**SCP** : Secure Copy (SCP) サーバにパケットダンプ キャプチャ ファイルをエクスポートします。

SFTP および SCP は、SSH に依存してセキュアな転送を提供します。そのため、SFTP サーバまたは SCP サーバに攻撃レポートをエクスポートする前に、Detector がセキュアな通信に使用するキーを設定していない場合、Detector はパスワードを入力するように求めます。SFTP および SCP 用のキーは、Detector CLI を使用しないと設定できません。

— **Address** : ネットワーク サーバの IP アドレス。

— **Path** : 完全パス名。パスを指定しない場合、サーバはユーザのホームディレクトリに 1 つ以上のファイルを保存します。

— **Username** : ネットワーク サーバのログイン名。FTP サーバを定義する場合、username 引数はオプションです。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。

— **Password** : (オプション) リモート FTP サーバのパスワード。ユーザ名を入力してパスワードを入力しなかった場合、Detector はパスワードを入力するように求めます。

**ステップ 5** **OK** をクリックして、パケットダンプ キャプチャ ファイルをネットワーク サーバにエクスポートします。

---

## パケットダンプ キャプチャ ファイルのインポート

パケットダンプ キャプチャ ファイルをネットワーク サーバから Detector にインポートできます。この機能により、過去のイベントを分析したり、現在のネットワークのトラフィック パターンと Detector が以前に通常の状態では記録したトラフィック パターンを比較することができます。Detector は、パケットダンプ キャプチャ ファイルを XML 形式と PCAP 形式でインポートします。

パケットダンプ キャプチャをインポートするには、次の手順を実行します。

---

**ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

**ステップ 2** ゾーンのメイン メニューの **Diagnostics > Packet-Dump > Packet-Dump List** を選択します。Packet-Dump list 画面が表示されます。

**ステップ 3** **Import** をクリックします。Import File Server Parameters ウィンドウが表示されます。

**ステップ 4** パケットダンプ キャプチャ ファイルの名前を File name フィールドに入力します。

**ステップ 5** Select File Server Parameters フォームで、次のいずれかのオプションから使用するネットワーク サーバを選択して定義します。

- **Use automatic export file server definitions : CLI export packet-dump** コマンドを使用して Detector コンフィギュレーション内に定義したネットワーク サーバからパケットダンプ キャプチャ ファイルをインポートします。

## ■ パケットダンプ キャプチャ ファイルの管理

- **Use the following server definition** : 定義したネットワーク サーバからパケットダンプ キャプチャ ファイルをインポートします。ネットワーク サーバに関する次の情報を入力します。
  - **Transfer method** : 使用する転送プロトコルを選択します。  
転送方式は、次のいずれかです。
    - FTP** : FTP サーバからパケットダンプ キャプチャ ファイルをインポートします。
    - SFTP** : Secure FTP (SFTP) サーバからパケットダンプ キャプチャ ファイルをインポートします。
    - SCP** : Secure Copy (SCP) サーバからパケットダンプ キャプチャ ファイルをインポートします。SFTP および SCP は、SSH に依存してセキュアな転送を提供します。そのため、SFTP サーバまたは SCP サーバからパケットダンプ キャプチャ ファイルをインポートする前に、Detector がセキュアな通信に使用するキーを設定していない場合、Detector はパスワードを入力するように求めます。SFTP および SCP 用のキーは、Detector CLI を使用しないと設定できません。
  - **Address** : ネットワーク サーバの IP アドレス。
  - **Path** : 完全パス名。パスを指定しない場合、サーバはユーザのホームディレクトリからファイルをコピーします。
  - **Username** : ネットワーク サーバのログイン名。FTP サーバを定義する場合、username 引数はオプションです。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
  - **Password** : (オプション) リモート FTP サーバのパスワード。ユーザ名を入力してパスワードを入力しなかった場合、Detector はパスワードを入力するように求めます。

**ステップ 6** **OK** をクリックして、パケットダンプ キャプチャ ファイルをネットワーク サーバからインポートします。

---



## パケットダンプ キャプチャ ファイルの削除

ゾーンごとに保存できる手動パケットダンプ キャプチャ ファイルは 1 つのみであり、Detector にはパケットダンプ キャプチャ ファイルを 10 個まで保存できません。新しいキャプチャのためにディスク スペースを確保するには、以前のパケットダンプ キャプチャを削除する必要があります。

パケットダンプ キャプチャを削除するには、次の手順を実行します。

- 
- ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。
  - ステップ 2** ゾーンのメイン メニューの **Diagnostics > Packet-Dump > Packet-Dump List** を選択します。Packet-Dump list 画面が表示されます。
  - ステップ 3** 削除するパケットダンプ キャプチャの隣にあるチェックボックスをオンにし、**Delete** をクリックします。すべてのパケットダンプ キャプチャを選択するには、テーブルのヘッダーにあるチェックボックスをオンにします。ローカル データベースからパケットダンプ キャプチャが削除されます。
-

## パケットダンプのシグニチャの抽出と使用

シグニチャは、パケットダンプ キャプチャに含まれている攻撃パケットのペイロードに、共通して現れるパターンです。Detector をアクティブにして異常なトラフィックのシグニチャを抽出し、その後の同じタイプの攻撃を迅速に発見するためにそのシグニチャを使用することができます。この機能を使用すると、ウィルス対策ソフトウェア会社からシグニチャやメーリング リストが発行される前に、新しい攻撃とインターネット ワームを検出することができます。

シグニチャの抽出プロセスの実行中、Detector はフレックスコンテンツ フィルタのパターン式の構文を使用して攻撃シグニチャを生成します。このシグニチャをフレックスコンテンツ フィルタのパターンとして使用し、異常なトラフィックをフィルタリングして排除できます。詳細については、第 5 章「ゾーンのフィルタの設定」の「フレックスコンテンツ フィルタの式の構文について」の項を参照してください。

この項では、次の手順について説明します。

- [パケットダンプ キャプチャのシグニチャの抽出](#)
- [参照キャプチャを使用したパケットダンプ キャプチャのシグニチャの抽出](#)
- [フレックスコンテンツ フィルタへの攻撃シグニチャの追加](#)

### パケットダンプ キャプチャのシグニチャの抽出

パケットダンプ キャプチャから攻撃シグニチャを抽出するには、次の手順を実行します。

- 
- ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。
  - ステップ 2** ゾーンのメイン メニューの **Diagnostics > Packet-Dump > Packet-Dump List** を選択します。Packet-Dump list 画面が表示されます。
  - ステップ 3** シグニチャの抽出元となるパケットダンプ キャプチャの隣にあるチェックボックスをオンにし、**View** をクリックします。Packet-Dump capture analysis 画面が表示されます。

**ステップ 4 Extract Signatures** をクリックします。パケットダンプからシグニチャが抽出され、Packet-Dump signature extraction ウィンドウが表示されます。

表 11-7 に、Packet-Dump signature extraction ウィンドウに表示されるシグニチャの情報を示します。

**表 11-7 パケットダンプからのシグニチャ抽出のパラメータ**

パラメータ	説明
Capture name	Detector がシグニチャを抽出したパケットダンプ キャプチャの名前。
Pattern	Detector がパケットダンプ キャプチャから抽出したシグニチャ パターンのリスト (省略形式)。パターンの上にマウス ポインタを置くと、パターン全体が表示されます。
Start offset	パケット ペイロードの先頭から、パターン マッチングを開始する位置までのオフセット (バイト単位)。デフォルトは 0 (ペイロードの先頭) です。
End offset	パケット ペイロードの先頭から、パターン マッチングを終了する位置までのオフセット (バイト単位)。デフォルトは、パケット長 (ペイロードの末尾) です。

Detector が表示するシグニチャの 1 つをフレックスコンテンツ フィルタに追加するには、「[フレックスコンテンツ フィルタへの攻撃シグニチャの追加](#)」の手順を参照してください。

## 参照キャプチャを使用したパケットダンプ キャプチャのシグニチャの抽出

パケットダンプ キャプチャ ファイルからシグニチャを抽出して、別のパケットダンプ キャプチャ ファイルを参照ファイルとして指定することができます。この参照ファイルは、トラフィックが通常状態のときに記録されたトラフィック キャプチャ ファイルである必要があります。Guard は、トラフィックが通常状態のときに記録されたトラフィックの中に、シグニチャが存在している時間の割合を特定します。正常のトラフィック状態で記録されたトラフィックに攻撃シグニチャが高い確率で出現しても、攻撃のパターンを意味するとは限りません。

参照ファイルを使用してパケットダンプ キャプチャから攻撃のシグニチャを抽出するには、次の手順を実行します。

- ステップ 1** ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。
- ステップ 2** ゾーンのメイン メニューの **Diagnostics > Packet-Dump > Packet-Dump List** を選択します。Packet-Dump list 画面が表示されます。
- ステップ 3** 基準キャプチャとして使用するパケットダンプ キャプチャの隣にあるチェックボックスをオンにします。
- ステップ 4** 参照キャプチャとして使用するパケットダンプ キャプチャの隣にあるチェックボックスをオンにし、**View** をクリックします。Packet-Dump capture analysis 画面が表示されます。
- ステップ 5** (オプション) **Swap Base and Reference** をクリックして、2つのパケットキャプチャを切り替えます。基準キャプチャを参照キャプチャにして、参照キャプチャを基準キャプチャにします。基準キャプチャからシグニチャが抽出されます。
- ステップ 6** **Extract Signatures** をクリックします。基準のパケットダンプからシグニチャが抽出され、Packet-Dump signature extraction ウィンドウが表示されます。表 11-7 に、Packet-Dump signature extraction ウィンドウに表示されるシグニチャの情報を示します。

表 11-8 パケットダンプからのシグニチャ抽出のパラメータ

パラメータ	説明
Capture name	Detector がシグニチャを抽出したパケットダンプ キャプチャの名前。
Pattern	Detector がパケットダンプ キャプチャから抽出したパターンのリスト (省略形式)。パターンの上にマウス ポインタを置くと、パターン全体が表示されます。
Start offset	パケット ペイロードの先頭から、パターン マッチングを開始する位置までのオフセット (バイト単位)。デフォルトは 0 (ペイロードの先頭) です。
End offset	パケット ペイロードの先頭から、パターン マッチングを終了する位置までのオフセット (バイト単位)。デフォルトは、パケット長 (ペイロードの末尾) です。

Detector が表示するシグニチャの 1 つをフレックスコンテンツ フィルタに追加するには、「[フレックスコンテンツ フィルタへの攻撃シグニチャの追加](#)」の手順を参照してください。

## フレックスコンテンツ フィルタへの攻撃シグニチャの追加

Detector では、パケットダンプ キャプチャから抽出したシグニチャを使用して、フレックスコンテンツ フィルタを構築することができます。このフレックスコンテンツ フィルタを使用して、攻撃シグニチャに一致するゾーン トラフィックをブロックすることができます。

攻撃シグニチャをフレックスコンテンツ フィルタに追加するには、次の手順を実行します。

**ステップ 1** 次のいずれかの手順を実行して、パケットダンプ キャプチャからシグニチャを抽出します。

- [パケットダンプ キャプチャのシグニチャの抽出](#)

## ■ パケットダンプのシグニチャの抽出と使用

- [参照キャプチャを使用したパケットダンプ キャプチャのシグニチャの抽出](#)

- ステップ 2** Packet-Dump signature extraction ウィンドウで、フレックスコンテンツ フィルタで使用するシグニチャを選択します。
- ステップ 3** Add をクリックします。Flex-Content Filters > Add filters - step 2 画面が表示されま
- ステップ 4** フレックスコンテンツ フィルタのパラメータを設定します。表 11-1 に、Flex-Content Filter Form に表示されるフィルタのパラメータの説明を示します。

表 11-9 フレックスコンテンツ フィルタのパラメータ

パラメータ	説明
Description	フレックスコンテンツ フィルタを説明するテキスト。
Protocol	<p>特定のプロトコルを使用しているトラフィックを処理します。0 ~ 255 のプロトコル番号を入力します。すべてのプロトコルタイプを指定するには、アスタリスク (*) を入力します。</p> <p>有効なプロトコル番号のリストについては、次の Internet Assigned Numbers Authority (IANA) の Web サイトを参照してください。</p> <p><a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a></p>
Dst Port	<p>特定の宛先ポートに向かうトラフィックを処理します。0 ~ 65,535 の宛先ポート番号を入力します。すべての宛先ポートを指定するには、アスタリスク (*) を入力します。</p> <p>有効なポート番号のリストについては、次の Internet Assigned Numbers Authority (IANA) の Web サイトを参照してください。</p> <p><a href="http://www.iana.org/assignments/port-numbers">http://www.iana.org/assignments/port-numbers</a></p>
Expression	<p>指定した式に基づいてトラフィックをフィルタリングします。フィルタの式の規則は、フレックスコンテンツ フィルタの式の規則と同じです (第 5 章「ゾーンのフィルタの設定」の「<a href="#">フレックスコンテンツ フィルタの式の構文について</a>」の項を参照)。使用する式を入力します。</p>

表 11-9 フレックスコンテンツ フィルタのパラメータ (続き)

パラメータ	説明
Pattern	Detector は、選択したパケットダンプのシグニチャを Pattern フィールドにコピーします。この結果、パケットの内容と照合するための正規表現データ パターンが指定されます。
Match Case	データ パターン式で大文字と小文字を区別するかどうかを指定します。大文字と小文字を区別するデータ パターン式として定義するには、チェックボックスをオンにします。
Start Offset	パケットの内容の先頭から、パターン マッチングを開始する位置までのオフセットを指定します (バイト単位)。デフォルトは 0 (ペイロードの先頭) です。開始オフセットは、pattern フィールドに適用されます。0 ~ 2047 の整数を入力します。
End Offset	パケットの内容の先頭から、パターン マッチングを終了する位置までのオフセットを指定します (バイト単位)。デフォルトは、パケット長 (ペイロードの末尾) です。終了オフセットは、pattern フィールドに適用されます。0 ~ 2047 の整数を入力します。
Action	<p>トラフィックに対してフレックスコンテンツ フィルタが実行するアクションを指定します。</p> <p>アクションを Action ドロップダウン リストから選択します。</p> <p>Detector は、Detector がフィルタに一致するトラフィック フロー パケットをカウントすることを示す <b>count</b> アクションをサポートします。</p>
Guard Action	<p>GUARD ゾーン テンプレートを使用してゾーンを作成した場合、Cisco Guard が使用する Flex-Content フィルタ アクションを設定できます。アクションを Action ドロップダウン リストから選択します。</p> <ul style="list-style-type: none"> <li><b>count</b>: フィルタに一致するトラフィック フロー パケットをカウントします。</li> <li><b>drop</b>: フィルタに一致するトラフィック フロー パケットをドロップします。</li> </ul>

表 11-9 フレックスコンテンツ フィルタのパラメータ (続き)

パラメータ	説明
State	<p>フレックスコンテンツ フィルタの動作状態。</p> <p>動作状態を State ドロップダウン リストから選択します。</p> <ul style="list-style-type: none"> <li>• <b>enable</b> : Detector はフレックスコンテンツ フィルタをトラフィック フローに適用し、一致が検出されると設定されたアクションを実行します。</li> <li>• <b>disable</b> : Detector はトラフィック フローにフレックスコンテンツ フィルタを適用しません。</li> </ul>

**ステップ 5** 次のいずれかのオプションを選択します。

- **OK** : 新しいフレックスコンテンツ フィルタを保存します。Flex-Content filters 画面が表示されます。
- **Clear** : フォームの情報をデフォルト値に戻し、追加した情報をすべて消去します。
- **Cancel** : 情報を保存せずに Flex-Content filters 画面を終了します。