CHAPTER 11

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

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 モジュールを設定できます。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って、過去のイベントの分析やトラフィック シグニチャの抽出ができます。また、現在のネットワーク トラフィックのパターンと Detector モジュールが以前に通常のトラフィック状態で記録したトラフィックのパターンとを比較することも可能です。

Detector モジュールが特定の基準を満たすトラフィックだけを記録するように、フィルタを設定できます。また、すべてのトラフィック データを記録し、Detector モジュールが表示するトラフィックをフィルタリングすることもできます。Detector モジュールは、gzip 圧縮された Packet Capture（PCAP）形式でトラフィックを保存します。これには、記録されたデータについて記述する Extensible Markup Language（XML）形式のファイルが付属します。

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 モジュールでは、パケットダンプ キャプチャを分析し、検出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 モジュールは、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 モジュールは、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。以前のパケットダンプ キャプチャ ファイルは新しいファイルに置き換えられます。以前のパケットダンプ キャプチャ ファイルを保存しておくには、それらのファイルを FTP サーバにエクスポートする必要があります。
- 手動パケットダンプ キャプチャ : Detector モジュールは、ユーザが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 モジュールで再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す。Detector モジュールでは、同時に最大 4 つのゾーンのトラフィックを手動で記録できます。

デフォルトでは、Detector モジュールは、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 20 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、80 MB まで保存できます。追加のパケットダンプ キャプチャ ファイルを保存するためにディスク スペースを解放するには、古い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**に設定すると、Detector モジュールは継続的にゾーンのトラフィックを記録します。新しいパケットダンプ 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。以前のパケットダンプ キャプチャ ファイルを保存しておくには、それらのファイルを FTP サーバにエクスポートする必要があります(「パケットダンプ キャプチャ ファイルのエクスポート」の項を参照)。

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　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 モジュールはすべてのゾーン 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 キャプチャの管理

この項の手順では、Detector モジュール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 モジュールは、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 20 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、80 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、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 > 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 モジュールは、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 モジュール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。 • **all**：すべてのトラフィックをキャプチャします。 • **dropped**：Detector モジュールがドロップしたトラフィックのみをキャプチャします。 • **forwarded**：Detector モジュール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。 • **replied**：検証の試行で Detector モジュール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。

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

パラメータ	説明
Sample rate	サンプリング レート（pps 単位）。1 ～ 10000 の値を入力します。 Detector モジュールは、同時に実行される手動キャプチャすべてについて、累積最大 10,000 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。 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。
Number of packets	記録するパケットの数。Detector モジュールは、ユーザが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、キャプチャ バッファ内の情報をファイルに保存します。1 ～ 5000 の整数を入力します。

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　モジュールは、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

Detector モジュールは、ユーザがキャプチャをアクティブにした際に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、指定の数のパケットを Detector モジュールが記録する前に、ユーザは手動パケットダンプ キャプチャを停止できます。

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 > 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 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。

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 モジュールが適用したユーザ定義フィルタ。
Dispatch	Detector モジュールが記録したトラフィックのタイプ。 • **All**：すべてのトラフィック。 • **Dropped**：Detector モジュールがドロップしたトラフィックのみ。 • **Forwarded**：Detector モジュールがゾーンに転送する正当なトラフィックのみ。 • **Replied**：検証の試行で Detector モジュール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。

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。 • **Start**：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。 • **Stop**：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。
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（「パケットダンプ キャプチャの詳細の表示」および「2 つのパケットダンプ キャプチャの比較」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（「手動パケットダンプ キャプチャ ファイルの名前変更」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（「パケットダンプ キャプチャの全体コピーの保存」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（「パケットダンプ キャプチャ ファイルのエクスポート」および「パケットダンプ キャプチャ ファイルのインポート」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（「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 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。

表 11-4 に、Detector モジュールが Packet-Dump capture analysis 画面のキャプチャと表示の各パラメータ領域に表示する情報を示します。

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
Capture parameters	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	キャプチャの期間中に Detector モジュールが記録したパケットの数。
	Packet Dump filter	キャプチャ ファイルに記録した情報に Detector モジュールが適用したユーザ定義フィルタ。
	Dispatch	Detector モジュールが記録したトラフィックのタイプ。 • **All**：すべてのトラフィック。 • **Dropped**：Detector モジュールがドロップしたトラフィックのみ。 • **Forwarded**：Detector モジュールがゾーンに転送する正当なトラフィックのみ。 • **Replied**：検証の試行で Detector モジュール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。

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
View Parameters	Query	キャプチャ情報を表示するために Detector モジュールが使用したデータ プロファイル。 • Top 20: SrcIP / DstIP / SrcPort / DstPort / Protocol • Distribution: SrcIP / DstIP / SrcPort / DstPort / SrcReservedPorts / DstReservedPorts / Protocol / TTL / Length • Packets list 各クエリー タイプに対して Detector モジュールがテーブル形式または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。
	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（「Packet-Dump Capture details 画面の表示の変更」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（「パケットダンプ キャプチャの全体コピーの保存」の項を参照）。
Extract Signatures ボタン		パケットダンプ キャプチャからトラフィックのシグニチャを抽出します（「パケットダンプのシグニチャの抽出と使用」の項を参照）。

表 11-5 に、ユーザが選択するクエリー タイプに応じて Detector モジュールが表示するテーブル形式またはグラフ形式の情報を示します（「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 モジュール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 モジュール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。

（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。

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 に、Change Packet-Dump View Parameters フォームのパラメータの説明を示します。

表 11-6　Change Packet-Dump View Parameters

パラメータ	説明
Query	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。 • **TOP 20: SrcIP / DstIP / SrcPort / DstPort / Protocol**：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。 • **Distribution: SrcIP / DstIP / SrcPort / DstPort / SrcReservedPorts / DstReservedPorts / Protocol / TTL / Length**：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。 • **Packet View**：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。

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

パラメータ	説明
Display filter	（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「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）。使用する表示フィルタを入力します。
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 モジュールは、ユーザが選択した表示パラメータに基づいて、Packet-Dump Capture details 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　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　「基準キャプチャ」として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　「参照キャプチャ」として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 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。この機能は、シグニチャを抽出する場合に使用します（Detector モジュール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。

Detector モジュールが Packet-Dump capture analysis 画面に表示す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

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。ユーザが自動パケットダンプのコピーを保存すると、Detector モジュールはそのコピーを手動パケットダンプ ファイルとして保存します。

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。

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 FTP サーバまたは SFTP 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 ファイルを 1 つエクスポートすることも、特定のゾーンのパケットダンプ キャプチャ ファイルをすべてエクスポートすることもできます。Detector モジュールは、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ます。これには、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 list** を選択します。Packet-Dump list 画面が表示されます。

ステップ 3　FTP 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 FTP Server Parameters ウィンドウが表示されます。

ステップ 4　Export FTP Server Parameters フォームで、使用する FTP 方式を選択します。

- **FTP**：File Transfer Protocol（ファイル転送プロトコル）
- **SFTP**：Secure File Transfer Protocol（セキュア ファイル転送プロトコル）

ステップ 5　Export FTP Server Parameters フォームで、使用する FTP サーバを選択します。

- **Use default FTP definitions**：CLI を使用して Detector モジュールの設定に定義した FTP サーバに、パケットダンプ キャプチャをエクスポートします。
- **Use temporary FTP server**：Detector モジュールの設定に定義していない FTP サーバに、パケットダンプ キャプチャをエクスポートします。FTP サーバに関する次の情報を入力します。
  - **Address**：FTP サーバの IP アドレス。
  - **Path**：Guard がパケットダンプ キャプチャ ファイルを保存する FTP サーバ上ディレクトリのフル パス。
  - **Username**：（オプション）FTP サーバのログイン名。ユーザ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 モジュールはパスワードを入力するように求めます。

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 キャプチャを FTP サーバに保存します。
- **Clear**：Select FTP Server Parameters フォームに追加した情報をすべて消去します。
- **Cancel**：パケットダンプ キャプチャを保存せずに Export FTP Server parameters ウィンドウを閉じます。

パケットダンプ キャプチャ ファイルのインポート

パケットダンプ キャプチャ ファイルを FTP サーバまたは SFTP サーバから Detector モジュールにインポートできます。このインポートにより、ユーザは過去のイベントを分析したり、現在のネットワーク トラフィックのパターンと Detector モジュールが以前に通常のトラフィック状態で記録したトラフィックのパターンとを比較したりできます。Detector モジュールは、パケットダンプ キャプチャ ファイルを XML 形式と PCAP 形式の両方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 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 FTP Server Parameters ウィンドウが表示されます。

ステップ 4　Select FTP Server Parameters フォームで、File name フィールドにパケットダンプ キャプチャのファイル名を入力します。

ステップ 5　Select FTP Server Parameters フォームで、使用する FTP 方式を選択します。

- **FTP**：File Transfer Protocol（ファイル転送プロトコル）
- **SFTP**：Secure File Transfer Protocol（セキュア ファイル転送プロトコル）

ステップ 6　Import FTP Server Parameters フォームで、使用する FTP サーバを選択して定義します。

- **Use default FTP definitions**：CLI を使用して Detector モジュールの設定に定義した FTP サーバから、パケットダンプ キャプチャをインポートします。
- **Use temporary FTP server**：Detector モジュールの設定に定義していない FTP サーバから、パケットダンプ キャプチャをインポートします。FTP サーバに関する次の情報を入力します。
  - Address：FTP サーバの IP アドレス。
  - Path：FTP サーバ上のパケットダンプ キャプチャのフル パス名。
  - Username：（オプション）FTP サーバのログイン名。ユーザ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 モジュールはパスワードを入力するように求めます。

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 キャプチャを FTP サーバに保存します。
- **Clear**：Select FTP Server Parameters フォームに追加した情報をすべて消去します。
- **Cancel**：パケットダンプ キャプチャを保存せずに Import FTP Server Parameters 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 つだけです。Detector モジュールには、10 を超えるパケットダンプ キャプチャ ファイルを保存できません。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 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 モジュール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、同一タイプの将来の攻撃を迅速に検出するためにそのシグニチャを使用できます。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 モジュール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 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 ウィンドウが開きます。

表 11-7 に、Detector モジュールが Packet-Dump signature extraction ウィンドウに表示するシグニチャ情報を示します。

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 モジュールでシグニチャの抽出元となるパケット ダンプ キャプチャの名前。
Pattern	Detector モジュールがパケットダンプ 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 モジュール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 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 ウィンドウが開きます。表 11-8 に、Detector モジュールが Packet-Dump signature extraction ウィンドウに表示するシグニチャ情報を示します。

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 モジュールでシグニチャの抽出元となるパケット ダンプ キャプチャの名前。
Pattern	Detector モジュールがパケットダンプ 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 モジュール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 モジュールでは、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

- 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 画面が表示されます。

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 11-9 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	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。 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。 http://www.iana.org/assignments/protocol-numbers
Dst Port	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 ～ 65535 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。 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。 http://www.iana.org/assignments/port-numbers
Expression	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「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）。使用する式を入力します。

表 11-9　フレックスコンテンツ フィルタのパラメータ（続き）

パラメータ	説明
Pattern	Detector モジュールは、ユーザが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	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。 アクションを Action ドロップダウン リストから選択します。 • **count**：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。 • **drop**：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。
State	フレックスコンテンツ フィルタの動作状態。 動作状態を State ドロップダウン リストから選択します。 • **enable**：Detector モジュール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。 • **disable**：Detector　モジュールは、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**：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。