



ネットワーク トラフィックの監視と 攻撃シグニチャの抽出

この章では、パケットダンプ キャプチャ機能を使用してネットワークの動作を阻害しないネットワーク タップを行い、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方法について説明します。

この章は、次の項で構成されています。

- [パケットダンプ キャプチャについて](#)
- [自動パケットダンプ キャプチャのイネーブル化](#)
- [自動パケットダンプ キャプチャのディセーブル化](#)
- [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 キャプチャからのシグニチャの抽出と使用](#)

パケットダンプ キャプチャについて

ネットワークを阻害しないタップを通じてネットワークから直接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 Cisco Traffic Anomaly Detector Module (Detector モジュール) を設定できます。記録されたトラフィックのデータベースをクエリーすると、過去のイベントの分析や攻撃シグニチャの生成ができます。または、通常のトラフィック状況で Detector モジュールが以前に記録したトラフィック パターンと、現在のネットワーク トラフィック パターンを比較することが可能です。

特定の基準を満たすトラフィックだけを Detector モジュールが記録するようにフィルタを設定することも、トラフィック データをすべて記録して Detector モジュールが表示するトラフィック情報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 (GNU zip) プログラムによって圧縮およびエンコードされる PCAP 形式でトラフィックを保存します。これには、記録されたデータを記述する Extensible Markup Language (XML) 形式のファイルが付属します。

記録されたトラフィックから、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) が出現しているかどうかを判別できます。Detector モジュールは、記録されたトラフィックを分析し、シグニチャを抽出することができます。これを使用して、シグニチャに一致するパケット ペイロードを含むすべてのトラフィックをブロックするように、フレックスコンテンツ フィルタを設定できます。

Detector モジュールは、次のようにトラフィックを記録できます。

- 自動: トラフィック データをパケットダンプ キャプチャ ファイルに継続的に記録します。
新しいパケットダンプ キャプチャ ファイルによって、以前に記録されたキャプチャ ファイルは置き換えられます。以前に記録されたパケットダンプ キャプチャ ファイルを保存するには、それらのファイルをネットワーク サーバにエクスポートする必要があります。
- 手動: 記録セッション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。

新しいパケットダンプ キャプチャ ファイルによって、以前に記録されたキャプチャ ファイルは置き換えられます。以前に記録されたキャプチャ ファイルを保存するには、新しい記録セッションをアクティブにする前に、それらのファイルをネットワーク サーバにエクスポートする必要があります。

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 モジュールは、同時に最大 4 つのゾーンの手動記録セッションを実行できます。

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 ファイルのためにディスク スペースを解放するには、古いファイルを削除する必要があります。

自動パケットダンプ キャプチャのイネーブル化

Detector モジュールによるネットワーク トラフィックの自動記録をアクティブにして、ネットワークの問題のトラブルシューティングや、攻撃トラフィックの分析を行うことができます。パケットダンプ キャプチャ フィルタを使用すると、指定した基準に一致するトラフィックのみを記録するよう Detector モジュールを設定できます。また、すべてのトラフィックを記録して、表示するとき、記録済みトラフィックにパケットダンプ キャプチャ フィルタを適用することもできます。

Detector モジュールは、トラフィックをキャプチャ バッファに記録します。キャプチャ バッファのサイズが 20 MB に達するか、10 分経過すると、Detector モジュールはバッファされた情報を圧縮形式でローカル ファイルに保存し、バッファをクリアして、トラフィックの記録を続けます。

Detector モジュールは、パケットダンプ キャプチャ ファイルに、IP の要約を示します。これは、(トラフィック量に応じて) 最も頻繁に検出された送信元 IP アドレスの要約です。

Detector モジュールは、自動パケットダンプ キャプチャ ファイルに命名規則を適用します。これらのファイルには、Detector モジュールがトラフィックを記録した日時とトラフィックの処理方法に関する情報が記載されています。表 11-1 に、自動パケットダンプ キャプチャ ファイル名のセクションの説明を示します。

表 11-1 自動パケットダンプ キャプチャ ファイル名のセクション

セクション	説明
Function/Zone Name	パケットダンプ キャプチャ時に Detector モジュールが実行していたゾーン機能とゾーン名。ゾーン機能には次のものがあります。 <ul style="list-style-type: none"> • detect: ゾーン異常の検出中に Detector モジュールがトラフィックを記録しました。 • learn: ゾーン ラーニング プロセス中または保護およびラーニング プロセス中に、Detector モジュールがトラフィックを記録しました。
Capture start time	Detector モジュールがトラフィックの記録を開始した時刻。
Capture end time	(オプション) Detector モジュールがトラフィックの記録を終了した時刻。Detector モジュールが現在トラフィックをファイルに記録している場合、終了時刻は表示されません。
Dispatch	Detector モジュールがトラフィックの処理に使用した方式。Detector モジュールは、受信したすべてのトラフィックをドロップするので、 dropped 方式のみをサポートしています。

Detector モジュールは、ラーニング プロセスから 1 つのパケットダンプ キャプチャ ファイルを保存します。ゾーン保護がイネーブルになっている場合は、次の 2 種類のパケットダンプ キャプチャ ファイルを保存します。

- 過去 10 分間のトラフィック
- 現在のトラフィック

ゾーン保護をアクティブにするか、Detector モジュールによるネットワーク トラフィックの自動記録をアクティブにすると、Detector モジュールは保護プロセス中に記録した以前のパケットダンプ キャプチャ ファイルをすべて消去し、新しいパケットダンプ キャプチャ ファイルを作成します。以前のパケットダンプ キャプチャ ファイルを保存するには、それらのファイルを File Transfer Protocol (FTP; ファイル転送プロトコル) 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イネーブルにするには、次の手順を実行します。

■ 自動パケットダンプ キャプチャのイネーブル化

-
- 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 メニューで **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 フォームの Packet-Dump Parameters 領域で、**On** をクリックします。
 - ステップ 5** **OK** をクリックして、自動パケットダンプの設定を保存します。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。
-

自動パケットダンプ キャプチャのディセーブル化

自動パケットダンプ機能をディセーブルにして、Detector モジュールによるゾーン トラフィックの記録を停止することができます。

自動パケットダンプ機能をディセーブルにするには、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 メニューで **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 フォームの Packet-Dump Parameters 領域で、**Off** をクリックします。
 - ステップ 5** **OK** をクリックして自動パケットダンプをディセーブルにします。Detector モジュールは、ゾーン トラフィックの記録を停止します。
-

手動パケットダンプ キャプチャのアクティブ化

Detector モジュールをアクティブにしてトラフィックの記録を開始し、特定の期間のトラフィックを記録したり、トラフィックの記録に Detector モジュールが使用する基準を変更したりできます。

指定された数のパケットを記録した場合、またはラーニング プロセスまたはゾーン保護が終了した場合、Detector モジュールはトラフィックの記録を停止し、手動パケットダンプ キャプチャをファイルに保存します。

Detector モジュールは、転送されたトラフィック、ドロップされたトラフィック、および応答されたトラフィックのパケットダンプ キャプチャ ファイルに、IP の要約を示します。これは、(トラフィック量に応じて) 最も頻繁に検出された送信元 IP アドレスの要約です。

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 モジュールは、同時に 10 個までのゾーンの手動パケットダンプ キャプチャを記録できます。

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。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)。

この項は、次の内容で構成されています。

- [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、ゾーン トラフィックの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 メニューで **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 11-2](#) に、Start Packet-Dump フォームに表示されるパラメータの説明を示します。

表 11-2 Start Packet-Dump フォームのパラメータ

パラメータ	説明
Capture name	パケットダンプ キャプチャ ファイルの名前。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せんが、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適用するフィルタ。Detector モジュールは、フィルタの式に適合するトラフィックだけをキャプチャします。この式の構文は、フレックスコンテンツ フィルタの式の構文と同じです (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の式の構文について」の項を参照)。
Dispatch value	Detector モジュールがキャプチャするゾーン トラフィック。Detector モジュールの Dispatch の値は Dropped です。
Sample rate	サンプリング レート (パケット / 秒単位)。1 ～ 10000 の値を入力します。 Detector モジュールは、同時に実行されるすべての手動キャプチャ用に、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。 パケットダンプ キャプチャのサンプリング レートを大きくすると、Detector モジュールのリソースの消費量が多くなります。大きいレート値は注意して使用することをお勧めします。
Number of packets	記録するパケットの数。Detector モジュールは、指定され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 OK をクリックして、手動パケットダンプ キャプチャを開始します。

手動パケットダンプ キャプチャの停止

Detector モジュールは、キャプチャをアクティブにするときにユーザによって指定され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、指定されたパケットの数を 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 メニューで **Diagnostics > Packet-Dump > Stop Packet-Dump** を選択します。Detector モジュールは、手動パケットダンプ キャプチャを停止します。

パケットダンプ キャプチャの表示

この項では、パケットダンプ キャプチャ ファイルのリストを表示する方法、1つのパケットダンプ キャプチャ ファイルの内容を表示する方法、および2つのパケットダンプ キャプチャの結果を比較する方法について説明します。

この項は、次の内容で構成されています。

- [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 ファイル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 メニューで **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 11-3 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 11-3 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 ファイルの名前。
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。
Packet Dump Filter	Detector モジュールがトラフィックを記録するときに使用するユーザ定義フィルタ。フィルタは TCPDump 形式です。この式の構文は、フレックスコンテンツ フィルタの式の構文と同じです (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の式の構文について」の項を参照)。
Dispatch	Detector モジュールが記録したトラフィックのタイプ。Dispatch の値は Dropped または All です。どちらの値も Detector モジュールがすべてのトラフィックを記録したことを示します。

表 11-4 に、Packet-Dump List 画面の機能ボタンの説明を示します。

表 11-4 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。 <ul style="list-style-type: none"> • 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 キャプチャ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 キャプチャ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 ファイルの詳細情報を 1 つまたは 2 つ表示します (「 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)。
Rename	パケットダンプ キャプチャ ファイルの名前を変更します (「 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 ファイルをコピーします (「 パケットダンプ キャプチャ ファイルのコピー 」の項を参照)。
Export/Import	パケットダンプ キャプチャ ファイルをエクスポートまたはインポートします (「 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 ファイルを削除します (「 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 メニューで **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、**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 11-5 に、Detector モジュールが Packet-Dump Capture Analysis 画面の Capture Parameters 領域と View Parameters 領域に表示する情報を示します。

表 11-5 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	パラメータ	説明
Capture Parameters	Name	キャプチャ ファイルの名前。
	Start time	キャプチャを開始した時刻。
	End time	キャプチャを終了した時刻。
	Packets	キャプチャ ファイルに含まれているパケットの数。
	Packet Dump filter	Detector モジュールがトラフィックを記録するときに使用するユーザ定義フィルタ。フィルタは TCPDump 形式です。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。
	Dispatch	Detector モジュールが記録したトラフィックのタイプ。Dispatch の値は Dropped または All です。どちらの値も Detector モジュールがすべてのトラフィックを記録したことを示します。
View Parameters	Query	<p>キャプチャ情報を表示するために Detector モジュールが使用するデータ プロファイル。</p> <ul style="list-style-type: none"> • Top 20: SrcIP / DstIP / SrcPort / DstPort / Protocol • Distribution: SrcIP / DstIP / SrcPort / DstPort / SrcReservedPorts / DstReservedPorts / Protocol / TTL / Length • Packets list <p>各クエリー タイプに対して Detector モジュールが表示する情報の詳細については、表 11-6 を参照してください。</p>
	Display filter	Detector モジュールがパケットダンプ キャプチャ ファイルの表示時に使用するフィルタ。Detector モジュールは、パケットダンプ キャプチャ ファイルの中でフィルタの基準に一致した部分のみを表示します。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。

Packet-Dump Capture Analysis 画面には、次のボタンがあります。

- Change View : 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 : 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 ファイルのコピー](#)」の項を参照)。
- Extract Signatures : 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 (「[パケットダンプ キャプチャからの攻撃シグニチャの抽出](#)」の項を参照)。

表 11-6 に、選択したクエリーのタイプに応じて Detector モジュールが表示するキャプチャ情報の説明を示します (「[Packet-Dump Capture details 画面の表示の変更](#)」の項を参照)。

表 11-6 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/ <i>Criteria</i> <i>Criteria</i> は、次のいずれかです。 <ul style="list-style-type: none"> • SrcIP • DstIP • SrcPort • DstPort • Protocol 	#	パケットダンプキャプチャの実行中に、記録する各インシデントに対して Detector モジュールが割り当てたシーケンス番号。
	Key	IP アドレス、ポート番号、またはプロトコル番号。選択するクエリータイプによって異なります。
	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。
	%	パケットダンプキャプチャの中で基準に合致するパケットの割合。
Distribution/ <i>Criteria</i> <i>Criteria</i> は、次のいずれかです。 <ul style="list-style-type: none"> • SrcIP • DstIP • SrcPort • DstPort • SrcReservedPorts • DstReservedPorts • Protocol • TTL • Length 	x-axis	選択した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	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、記録した各インシデントに対して Detector モジュールが割り当てたシーケンス番号。
	Time	パケットダンプをキャプチャした時刻。
	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	パケットのプロトコル番号。
	Info	パケットに関する追加情報。



(注)

カラムの情報に基づいて 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** 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 メニューで **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** **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 4** 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 11-7 に、Change Packet-Dump View Parameters フォームに表示されるパラメータの説明を示します。

表 11-7 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。Query ドロップダウン リストから、次のいずれかのプロファイルを選択します。</p> <ul style="list-style-type: none"> • TOP 20: SrcIP / DstIP / SrcPort / DstPort / Protocol: 選択した基準に基づいてパケットをグループ化し、値が最も大きい 20 個のグループを表示します。たとえば、表示基準に Src IP を選択した場合、Detector モジュールは送信元 IP アドレスに基づいてパケットをグループ化し、出現回数が最も大きい 20 個の送信元 IP アドレスに関する情報を表示します。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 : 定義した基準に関して、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。 <p>プロファイルにより、表示形式 (テーブルまたはグラフ) が決まります。</p>
Display filter	<p>(オプション) 表示するパケットを指定するユーザ定義のフィルタ。Detector モジュールは、パケットダンプ キャプチャ ファイルの中でフィルタの基準に一致した部分のみを表示します。この式の規則は、フレックスコンテンツ フィルタの TCPDump 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の式の構文について」の項を参照)。</p>
Display Pattern	<p>(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。Detector モジュールは、パケットダンプ キャプチャ ファイルの中でパターンの基準に一致した部分のみを表示します。このパターンの規則は、フレックスコンテンツ パターンの規則と同じです (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 フィルタのパターンの構文について」の項を参照)。使用する表示パターンを入力します。</p>
Start Offset	<p>(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。Start Offset パラメータは、Display Pattern フィールドにパターンを入力した場合にのみ適用されます。使用する開始オフセットを入力します。</p>

表 11-7 Change Packet-Dump View Parameters (続き)

パラメータ	説明
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。End Offset パラメータは、Display Pattern フィールドにパターンを入力した場合にのみ適用されます。使用する終了オフセットを入力します。

ステップ 5 **OK** をクリックしてパケットダンプ表示を変更します。Detector モジュールは、選択され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。

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 メニューで **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ときに使用します (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 キャプチャから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

この項は、次の内容で構成されています。

- [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 ファイルのコピー](#)
- [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

手動パケットダンプ キャプチャ ファイルの名前は変更できますが、自動パケットダンプ キャプチャ ファイルの名前は変更できません。自動パケットダンプ キャプチャ ファイルの名前を変更するには、ファイルをコピーする必要があります（「[パケットダンプ キャプチャ ファイルのコピー](#)」の項を参照）。

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 メニューで **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** 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** New name フィールドにパケットダンプ キャプチャ ファイルの新しい名前を入力します。名前は 1 ~ 63 文字の英数字文字列にします。アンダースコアとダッシュ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。
 - ステップ 5** **OK** をクリックして、パケットダンプ キャプチャを新しい名前で保存します。
-

パケットダンプ キャプチャ ファイルのコピー

パケットダンプ キャプチャ ファイル（またはファイルの一部）を新しい名前でもコピーできます。Detector モジュールは、既存の自動パケットダンプ キャプチャ ファイルを新しいファイルで上書きします。コピー オプションを使用することにより、後で使用できるように自動パケットダンプ キャプチャ ファイルを保存できます。自動パケットダンプ キャプチャ ファイルまたは手動パケットダンプ キャプチャ ファイルをコピーすると、Detector モジュールはそれらを手動ファイルとして保存し、元のパケットダンプ キャプチャ ファイルを削除しません。ディスク スペースを解放する必要がある場合は、元のパケットダンプ キャプチャ ファイルを手動で削除します（「[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 キャプチャをコピーするには、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 メニューで **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** 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。Packet-Dump Capture Analysis 画面が表示されます。
- ステップ 4** New name フィールドにパケットダンプ キャプチャ ファイルの新しい名前を入力します。名前は 1 ~ 63 文字の英数字文字列にします。アンダースコアとダッシュ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。
- ステップ 5** (オプション) パケットダンプ キャプチャ ファイルのコピーに Detector モジュールが使用するフィルタを定義します。Detector モジュールは、パケットダンプ キャプチャ ファイルの中でフィルタの基準に一致した部分のみをコピーします。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の式の構文について」の項を参照)。
- ステップ 6** **OK** をクリックして、パケットダンプ キャプチャを新しい名前で保存します。

パケットダンプ キャプチャ ファイルの詳細を表示して (「[パケットダンプ キャプチャの詳細の表示](#)」の項を参照)、**Save** をクリックすることによって、ファイルをコピーすることもできます。Detector モジュールが、表示されているファイルの一部を保存します。パケットダンプ キャプチャ ファイルの表示に Detector モジュールが使用するフィルタをユーザが設定すると、Detector モジュールは同じフィルタを使用して、パケットダンプ キャプチャ ファイルの中でフィルタの基準に一致した部分を保存します。

パケットダンプ キャプチャ ファイルのエクスポート

ファイル転送プロトコル (FTP)、Secure File Transfer Protocol (SFTP; セキュア ファイル転送プロトコル)、または Secure Copy Protocol (SCP) を使用してファイルを転送するネットワーク サーバに、手動でパケットダンプ キャプチャ ファイルを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 モジュールは、gzip (GNU zip) プログラムによって圧縮およびエンコードされる PCAP 形式でパケットダンプ キャプチャ ファイルをエクスポートします。これには、記録されたデータを記述する 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。

<http://www.cisco.com/public/sw-center/> にある Software Center から、このバージョンに付属の .xsd ファイルをダウンロードできます。

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 メニューで **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** エクスポートするパケットダンプ キャプチャ ファイル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。Export File Server Parameters ウィンドウが表示されます。

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。

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 サーバを選択します。

- **Use automatic export file server definitions** : CLI コマンド **export packet-dump** を使用して、Detector モジュール 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。転送方式は、次のいずれかです。
 - FTP : FTP を指定します。
 - SFTP : SFTP を指定します。
 - SCP : SCP を指定します。

SFTP および SCP は、Secure Shell (SSH: セキュア シェル) 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、セキュアな通信のために Detector モジュールで使用するキーを設定していない場合、パスワードを入力するように Detector モジュールから求められます。SFTP および SCP 用のキーを設定するには、Detector モジュールの CLI を使用する必要があります。
 - **Address** : ネットワーク サーバの IP アドレス。
 - **Path** : Detector モジュールがパケットダンプ キャプチャ ファイルを保存する完全パス名を入力します。パスを指定しない場合、ネットワーク サーバはユーザのホーム ディレクトリにパケットダンプ キャプチャ 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、パスワードを入力するように Detector モジュールから求められます。

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

ネットワーク サーバから Detector モジュールにパケットダンプ キャプチャ ファイルをインポートして、過去のイベントを分析したり、以前に通常のトラフィック状況で Detector モジュールが記録したトラフィック パターンと現在のネットワーク トラフィック パターン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。ゾーンのマイン メニューが表示されます。

ステップ 2 ゾーンのマイン メニューで **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 FTP Server Parameters ウィンドウが表示されます。

ステップ 4 File Name フィールドに、インポートするファイルの完全パスおよびファイル名を入力します (ファイル拡張子を除く)。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。



(注) ファイル拡張子を指定しないでください。ファイル拡張子を指定すると、インポート プロセスは失敗します。

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 サーバを選択します。

- **Use automatic export file server definitions** : CLI コマンド **export packet-dump** を使用して、Detector モジュール 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。
- **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。転送方式は、次のいずれかです。
 - FTP : FTP を指定します。
 - SFTP : SFTP を指定します。
 - SCP : SCP を指定します。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、セキュアな通信のために Detector モジュールで使用するキーを設定していない場合、パスワードを入力するように Detector モジュールから求められます。SFTP および SCP 用のキーを設定するには、Detector モジュールの CLI を使用する必要があります。
 - **Address** : ネットワーク サーバの IP アドレス。
 - **Path** : Detector モジュールがパケットダンプ キャプチャ ファイルをインポートする完全パス名を入力します。パスを指定しない場合、ネットワーク サーバはユーザのホーム ディレクトリからパケットダンプ キャプチャ 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、パスワードを入力するように Detector モジュールから求められます。

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

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、古いパケットダンプ キャプチャ ファイルを削除します。

最大 10 個のパケットダンプ キャプチャ ファイルを Detector モジュールに保存できます。新しいファイル用にスペースを割り当てるには、以前の手動パケットダンプ キャプチャ ファイル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 メニューで **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。Detector モジュールが、パケットダンプ キャプチャ ファイルを削除します。

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。

パケットダンプ キャプチャからのシグニチャの抽出と使用

攻撃シグニチャは、攻撃パケットのペイロードに出現する共通のパターンを示します。Detector モジュールをアクティブにして、異常トラフィックのシグニチャを生成してから、この情報を使用して同じタイプの将来の攻撃を迅速に識別することができます。この機能を使用すると、(たとえばウイルス対策ソフトウェア会社やメーリングリストから) 攻撃シグニチャが発行される前であっても、新しい Distributed Denial of Service (DDoS; 分散型サービス拒絶) 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。

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に使用して、悪意のある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 フィルタのパターンの構文について」の項を参照してください。

トラフィックが通常状態のときに Detector モジュールが記録した追加パケットダンプ キャプチャ ファイルを、参照ファイルとして指定できます。参照用のパケットダンプ キャプチャ ファイルを指定した場合、Detector モジュールは異常なトラフィックからシグニチャを生成し、通常のトラフィック状態のときに記録されたトラフィックにシグニチャが出現する時間の割合を示します。トラフィックが通常状態のときの記録に攻撃シグニチャが高い確率で出現しても、このシグニチャは正確な攻撃パターンを示していない可能性があります。

この項は、次の内容で構成されています。

- [パケットダンプ キャプチャからの攻撃シグニチャの抽出](#)
- [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 キャプチャ表示用の表示パターンとしての攻撃シグニチャの使用](#)

パケットダンプ キャプチャからの攻撃シグニチャの抽出

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 メニューで **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ます。
- ステップ 4** (オプション) 参照ファイル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。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。
- 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。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 7 **Extract Signatures** をクリックします。Detector モジュールがシグニチャを基準パケットダンプ キャプチャから抽出します。Packet-Dump Signature Extraction ウィンドウが表示されます。

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の説明を示します。

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。
% Reference	シグニチャが参照キャプチャ ファイルに出現する時間の割合。

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](#)」の項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 モジュールは、パケットダンプ キャプチャから抽出するシグニチャを使用して、フレックスコンテンツ フィルタを作成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** 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。詳細については、「[パケットダンプ キャプチャからの攻撃シグニチャの抽出](#)」の項を参照してください。
- 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、**Insert Content Filter** をクリックします。Flex-Content Filters > Add Filter - Step 2 画面が表示されます。
- ステップ 3** 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 フォームに表示されるフィルタ 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>http://www.iana.org/assignments/protocol-numbers</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 ～ 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。</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>http://www.iana.org/assignments/port-numbers</p>
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 (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。
Pattern	パケットの内容と照合するための正規表現データ パターンを指定します (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。
Match Case	フィルタが照合するパターン式が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。Action ドロップダウン リストから、次のいずれかのアクションを選択します。</p> <ul style="list-style-type: none"> 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。

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	フレックスコンテンツ フィルタの動作状態を指定します。State ドロップダウン リストから、次のいずれかの動作状態を選択します。 <ul style="list-style-type: none"> enable : Detector モジュールはフィルタをトラフィック フローに適用し、フィルタと一致するフローに対して、設定されているアクションを実行します。 disable : Detector モジュールは、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 4 OK をクリックして、新しいフレックスコンテンツ フィルタを保存します。

パケットダンプ キャプチャ表示用の表示パターンとしての攻撃シグニチャの使用

Detector モジュールは、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、パケットダンプ キャプチャの表示をフィルタリングできます。

攻撃シグニチャをパケットダンプ キャプチャ表示用の表示パターンとして使用するには、次の手順を実行します。

ステップ 1 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。詳細については、「[パケットダンプ キャプチャからの攻撃シグニチャの抽出](#)」を参照してください。

ステップ 2 Packet-Dump Signature Extraction ウィンドウで、表示パターンとして使用するシグニチャを選択し、**Use as View Filter** をクリックします。Packet-Dump Capture Analysis 画面が表示されます。

表 11-10 に、Detector モジュールが Packet-Dump Capture Analysis 画面の Capture Parameters 領域と View Parameters 領域に表示する情報を示します。

表 11-10 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	パラメータ	説明
Capture Parameters	Name	キャプチャ ファイルの名前。
	Start time	キャプチャを開始した時刻。
	End time	キャプチャを終了した時刻。
	Packets	キャプチャ ファイルに含まれているパケットの数。
	Packet Dump filter	Detector モジュールがトラフィックを記録するときに使用するユーザ定義フィルタ。フィルタは TCPDump 形式です。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。
	Dispatch	Detector モジュールが記録したトラフィックのタイプ。Dispatch の値は DROPPED または ALL です。どちらの値も Detector モジュールがすべてのトラフィックを記録したことを示します。

表 11-10 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	パラメータ	説明
View Parameters	Query	<p>キャプチャ情報を表示するために Detector モジュールが使用するデータ プロファイル。</p> <ul style="list-style-type: none"> • Top 20: SrcIP / DstIP / SrcPort / DstPort / Protocol • Distribution: SrcIP / DstIP / SrcPort / DstPort / SrcReservedPorts / DstReservedPorts / Protocol / TTL / Length • Packets list <p>各クエリー タイプに対して Detector モジュールが表示する情報の詳細については、表 11-6 を参照してください。</p>
	Display filter	<p>Detector モジュールがパケットダンプ キャプチャ ファイルの表示時に使用するフィルタ。Detector モジュールは、パケットダンプ キャプチャ ファイルの中でフィルタの基準に一致した部分のみを表示します。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。</p>

■ パケットダンプ キャプチャからのシグニチャの抽出と使用