CHAPTER 11

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

Cisco Guard（Guard）では、ネットワークの動作を阻害しないタップを使用してネットワークから直接トラフィックを記録し、記録されたトラフィックからデータベースを作成するように設定できます。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 Guard 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 Guard 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 Guard 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。

Guard 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。Guard 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。

Guard 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。
- 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す。Guard は、同時に 10 個まで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、Guard 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。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

ネットワークの問題をトラブルシューティングしたり、攻撃トラフィックを分析したりするために、Guard 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ことができます。また、すべてのトラフィックを記録し、記録されたトラフィックを表示するときにパケットダンプ キャプチャ フィルタを適用できます。

Guard 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 50 MB に達するか、10 分経過すると、Guard 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。

Guard は、次のパケット処理方法に応じて、キャプチャ期間中に最大 3 種類のキャプチャ ファイルを作成できます。

- Forwarded：Guard がゾーンに転送した正当なトラフィックの送信元 IP アドレス。
- Dropped：Guard がドロップした悪意のあるトラフィックの送信元 IP アドレス。
- Replied：検証の試行で、Guard 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宛先 IP アドレス。

転送されたパケットダンプ キャプチャ ファイルのみが存在するという状況は、キャプチャ期間中にゾーンが攻撃を受けなかったことを表します。Guard が、ドロップされたキャプチャ ファイルおよび応答されたキャプチャ ファイルも作成した場合は、ゾーンに対する攻撃があることを表します。3 種類のパケットダンプ キャプチャ ファイルごとに、Guard は 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 IP アドレスの要約です。

応答されたパケットダンプ キャプチャ ファイルに Guard が示す IP の要約情報を使用して、スプーフィングを利用した攻撃の送信元を特定できます。また、Guard は、この情報をキャプチャ ファイルから取り出して、Replied IP Summarization という見出しでゾーン攻撃レポートに表示します（第 10 章「Guard およびゾーンの動作の監視」の「応答された IP の要約情報について」の項を参照）。

注意　応答された IP の要約結果を正確なものにするため、そのゾーンに対する攻撃中、パケットダンプ キャプチャ機能をイネーブルのままにしておく必要があります。攻撃中にパケットダンプ キャプチャ機能をディセーブルにすると、応答された IP の要約情報を表示できなかったり、情報が正確でなくなったりすることがあります。Guard は、パケットダンプ自動キャプチャ機能をイネーブルにした場合にのみ、応答された IP の要約情報を攻撃レポートに表示できます（パケットダンプ機能を手動でアクティブにした場合、応答された IP の要約情報は表示されません）。

（注）　IP の要約プロセスは多くのリソースを消費します。リソースが少なくなると、Guard はプロセスを一時停止し、ゾーン ログに表示されるログ メッセージを発行します。キャプチャの xml ファイルには、障害が原因でキャプチャ ファイルに IP の要約情報がないというステータス アトリビュートが含まれます。

Guard 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、Guard 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 Guard 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。 • **protect**：ゾーン保護中に Guard 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、Guard がトラフィックを記録しました。
Capture start time	Guard 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）Guard がトラフィックの記録を終了した時刻。Guard 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	Guard がトラフィックの処理に使用した方式。この方式は、次のいずれかです。 • **forwarded**：Guard はトラフィックを正当なものと識別し、ゾーンに転送しました。 • **dropped**：Guard はトラフィックを悪意あるものと識別し、ドロップしました。 • **replied**：Guard は、正当なトラフィックの一部であるか攻撃の一部であるかを確認するために、スプーフィング防止機能またはゾンビ防止機能による処理の一環として、開始側のクライアントに応答を送信しました。

ラーニング プロセスまたは保護およびラーニング機能をイネーブルにすると、Guard は作成したすべてのパケットダンプ キャプチャ ファイルを保存します。ゾーン保護をイネーブルにすると、Guard は過去のパケットダンプ キャプチャ ファイルを 1 セットだけ保存します。ゾーン保護がイネーブルになっているときに、すべてのパケットダンプ キャプチャ ファイルを保存するには、作成したパケットダンプ キャプチャ ファイルを自動的にネットワーク サーバにエクスポートするように Guard を設定します。

ゾーン保護をアクティブにするか、Guard 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、Guard 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。

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。

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　パケットダンプ キャプチャ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　**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。Guard 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、Guard 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。Guard 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

Guard によるゾーン トラフィックの記録、キャプチャ ファイルの作成を、手動でアクティブにできます。これによって、特定の期間のトラフィックをキャプチャすることができます。Guard が記録するトラフィックの種類を、次のように指定することもできます。

- Forwarded：Guard がゾーンに転送した正当なトラフィック。
- Dropped：Guard がドロップした悪意のあるトラフィック。
- Replied：検証の試行で、Guard 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。
- All：転送、ドロップ、および応答されたトラフィック。

Guard 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。Guard は、すべてのトラフィック タイプを含んでいるキャプチャ ファイルについては IP の要約を示しません。

（注）　IP の要約プロセスは多くのリソースを消費します。リソースが少なくなると、Guard はプロセスを一時停止し、ゾーン ログに表示されるログ メッセージを発行します。キャプチャの xml ファイルには、障害が原因でキャプチャ ファイルに IP の要約情報がないというステータス アトリビュートが含まれます。

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、Guard 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。

デフォルトでは、Guard 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、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）。

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。Guard 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。

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、ゾーンを保護している）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適用するフィルタ。Guard は、フィルタ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 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	Guard がキャプチャするゾーン トラフィック。ドロップダウン リストから、次のいずれかのトラフィック タイプを選択します。 • all：すべてのトラフィックをキャプチャします。 • dropped：Guard 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：Guard がゾーンに転送した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、Guard 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。
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。 Guard は、蓄積されるパケットダンプ キャプチャの最大レート 10000 pps を、すべての同時実行手動キャプチャでサポートします。 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、Guard 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。Guard 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

Guard 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、指定した数のパケットを Guard が記録する前に、手動パケットダンプ キャプチャを停止することができます。

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 メニューで、**Diagnostics > Packet-Dump > Stop Packet-Dump** を選択します。Guard が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 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	Guard 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 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	Guard が記録したトラフィックのタイプ。トラフィック タイプは、次のいずれかです。 • All：すべてのトラフィック。 • Dropped：Guard がドロップしたトラフィック。 • Forwarded：Guard がゾーンに転送した正当なトラフィック。 • Replied：検証の試行で、Guard 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。

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。 • 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 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）。
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、Packet-Dump Capture Analysis 画面の Capture Parameters 領域と View Parameters 領域に Guard が表示する情報の説明を示します。

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	Guard 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	Guard が記録したトラフィックのタイプ。次のものがあります。 • All：すべてのトラフィック。 • Dropped：Guard がドロップしたトラフィック。 • Forwarded：Guard がゾーンに転送した正当なトラフィック。 • Replied：検証の試行で、Guard 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。
View Parameters	Query	キャプチャ情報を表示するために Guard が使用するデータ 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 それぞれのクエリー タイプに対して Guard が表示する情報の詳細については、表 11-7 を参照してください。
	Display filter	Guard 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。Guard 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。

View Parameters 領域にある IP の要約テーブルには、パケットダンプ キャプチャに記録され、最も頻繁に検出された IP アドレスに関する情報が表示されます。表 11-6 に、IP の要約テーブルに表示されるフィールドの説明を示します。

（注） 2 つのパケットダンプ キャプチャを表示して 2 つのキャプチャを比較する場合（「2 つのパケットダンプ キャプチャの比較」の項を参照）、IP の要約テーブルは表示されません。

表 11-6　IP の要約テーブルに含まれているフィールドの説明

フィールド	説明
Subnet	記録されたパケット タイプにおいて最も頻繁に検出された IP アドレス。転送されたパケット タイプとドロップされたパケット タイプの場合、表示される IP アドレスはパケットの送信元 IP アドレスです。応答されたパケット タイプの場合、IP アドレスはパケットの宛先 IP アドレスです。
Subnet Mask	記録されたパケット タイプ（転送、ドロップ、または応答）のサブネット マスク。
Weight(%)	Guard が記録したサンプルの総数における、そのサブネット IP アドレスからのサンプルの割合。
Unique Addresses	そのサブネットに属する一意のアドレスの数。

表 11-7 に、選択したクエリーのタイプに応じて Guard 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 11-7　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/*Criteria* *Criteria* は、次のいずれかです。 • 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 Guard 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。選択したクエリーの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/*Criteria* *Criteria* は、次のいずれかです。 • 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。

表 11-7　キャプチャ パラメータのテーブルとグラフの詳細（続き）

クエリーのタイプ	パラメータ	説明
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 Guard が割り当てるシーケンス番号。
	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 analysis 画面には、次の機能ボタンがあります。

- 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）。

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 11-8 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 11-8　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。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。 • 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、Guard 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。 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。
Display filter	（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。Guard 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 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）。
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。Guard 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 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。 攻撃シグニチャを表示パターンとして使用することもできます。詳細については、「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」の項を参照してください。
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。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。
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、パケットダンプの表示を変更します。Guard 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（Guard は、シグニチャを基準キャプチャから抽出します）。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。

Guard 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

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）を新しい名前でコピーできます。Guard 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、Guard 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 Guard が使用するフィルタを定義します。Guard 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 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。Guard 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 Guard が使用するフィルタをユーザが設定すると、Guard 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

FTP、Secure File Transfer Protocol（SFTP）、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。Guard 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、Guard の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）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 Guard 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 Guard から求められます。SFTP および SCP 用のキーを設定するには、Guard 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**：Guard 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、Guard 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

ネットワーク サーバから Guard 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 Guard 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。Guard は、パケットダンプ キャプチャ ファイルを XML と PCAP の両方の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、Guard の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、Guard 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、Guard 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、Guard 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**：Guard 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、Guard 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

デフォルトでは、Guard 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。

最大 10 個のパケットダンプ キャプチャ ファイルを Guard 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　削除する各パケットダンプ 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。Guard 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。Guard 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、（たとえばウィルス対策ソフトウェア会社やメーリング リストから）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。

Guard 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。第 5 章「ゾーン 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 Guard 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。参照パケットダンプ キャプチャ ファイルを指定した場合、Guard は異常なトラフィックからシグニチャを生成し、通常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

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。Guard は、シグニチャを基準キャプチャから抽出します。

ステップ 7　**Extract Signatures** をクリックします。Guard 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 11-9 に、Guard 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 11-9　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	Guard による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	Guard 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。

Guard 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

Guard 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」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 11-10 に、Flex-Content Filter フォーム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 11-10　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

表 11-10　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
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（第 5 章「ゾーン 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 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	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。 • 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。 • enable：Guard 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：Guard 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

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

表 11-11　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	Guard 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	Guard が記録したトラフィックのタイプ。次のものがあります。 • All：すべてのトラフィック。 • Dropped：Guard がドロップしたトラフィック。 • Forwarded：Guard がゾーンに転送した正当なトラフィック。 • Replied：検証の試行で、Guard 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。
View Parameters	Query	キャプチャ情報を表示するために Guard が使用するデータ 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 それぞれのクエリー タイプに対して Guard が表示する情報の詳細については、表 11-7 を参照してください。
	Display filter	Guard 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。Guard 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。

表 11-12 に、選択したクエリーのタイプに応じて Guard 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 11-12　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/*Criteria* *Criteria* は、次のいずれかです。 • 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 Guard 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。選択したクエリーの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/*Criteria* *Criteria* は、次のいずれかです。 • 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	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 Guard が割り当てるシーケンス番号。
	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。