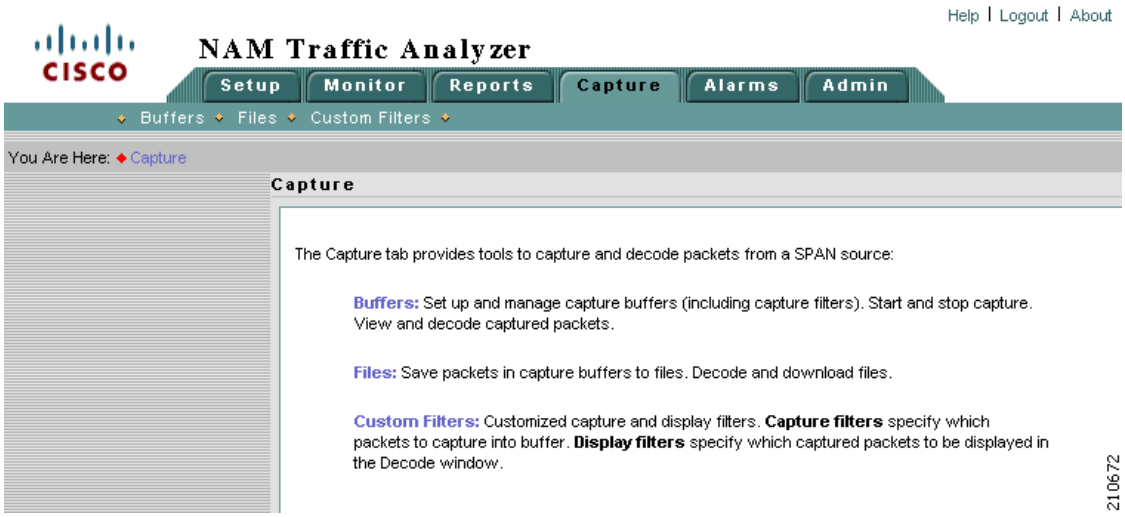
CHAPTER 6

パケット データのキャプチャとデコード

Capture タブでは、パケット データのキャプチャ、フィルタリング、およびデコード用の複数のバッファの設定、ファイル制御システム内のデータ管理、およびパケットの内容表示を行うことができます。

Capture タブ（図 6-1）には、パケット データのキャプチャおよびデコードに使用できるオプションが示されます。

図 6-1　Capture タブ



Capture タブでは、3 つのオプションを選択できます。

- バッファ（P.6-2）

  パケット データのキャプチャおよびデコード用の基本操作にアクセスするには、Buffers オプションを使用します。
- ファイル（P.6-15）

  ファイルを保存、デコード、またはダウンロードするには、Files オプションを使用します。
- カスタム キャプチャ フィルタ（P.6-21）

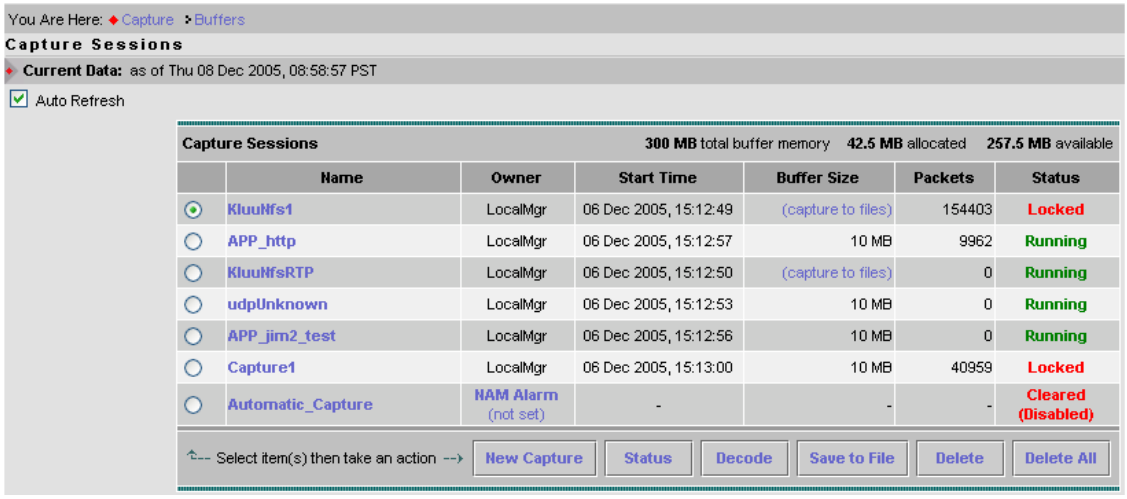
  カスタマイズしたキャプチャ フィルタおよび表示フィルタを作成するには、Custom Filters オプションを使用します。

バッファ

Capture Buffers （図 6-2）ウィンドウには、キャプチャ バッファのリストが表示されます。複数のキャプチャ バッファおよび 1 つの自動キャプチャ バッファを設定できます。

（注）　Auto Refresh チェックボックスをオンにすると、Capture Buffers ウィンドウが 60 秒ごとに自動的にリフレッシュされます。

図 6-2　Capture Buffers



Capture Buffers のフィールド（表 6-1）で、Capture Buffers のフィールドについて説明します。

表 6-1　Capture Buffers のフィールド

操作	説明
Name	キャプチャ バッファの名前
Owner	バッファの所有者
Start Time	キャプチャの開始時刻
Buffer Size	バッファのサイズ （注）　(Capture to files) は、キャプチャが 1 つ以上のファイルに格納されていることを示しています。
Packets	パケット数

表 6-1　Capture Buffers のフィールド（続き）

操作	説明
Status	現在のキャプチャの状態： • Running：パケット キャプチャが進行中です。 • Paused：パケット キャプチャが一時停止しています。キャプチャされたパケットはバッファに残っていますが、新しいパケットはキャプチャされていません。 • Cleared：キャプチャは（ユーザによって）中止され、バッファはクリアされます。 • Locked：バッファがいっぱいになったため、キャプチャがロック（中止）されました。

Capture Buffers での操作（表 6-2）で、Capture Buffers ウィンドウで行うことができる操作について説明します。

表 6-2　Capture Buffers での操作

操作	説明
New Capture	クリックすると、新しいキャプチャ バッファを作成できます。「キャプチャ設定の構成」を参照してください。
Status	クリックすると、選択したキャプチャの状態と設定値が表示されます。
Settings	クリックすると、キャプチャ設定の修正、キャプチャの一時停止、クリア、および再開を行うことができます。「キャプチャ設定の構成」を参照してください。
Decode	クリックすると、デコードされたパケットを表示できます。「パケット デコード情報の表示」を参照してください。
Save to File	クリックすると、バッファをファイルに保存できます。「ファイル」を参照してください。
Delete	クリックすると、バッファを削除できます。
Delete All	クリックすると、すべてのバッファを削除できます。

キャプチャ設定の構成

Capture Settings ウィンドウでは、新しいキャプチャ設定を構成したり、キャプチャ プロセスを制御したりすることができます。キャプチャ フィルタを設定して、キャプチャするパケットを絞り込むこともできます。

新しいキャプチャを設定するには、次の手順を実行します。

ステップ 1　**Capture** > **Buffers** を選択します。

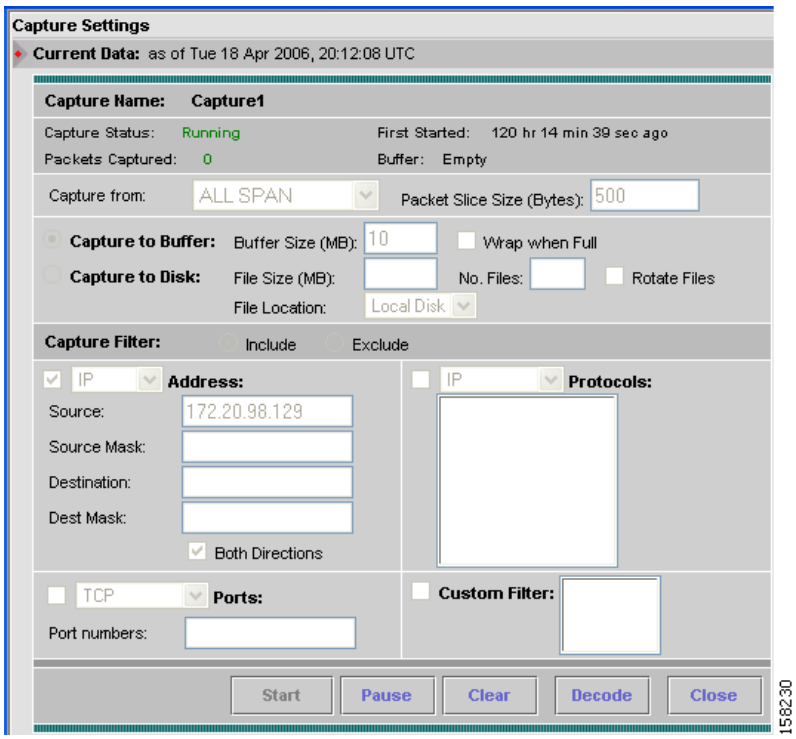
ステップ 2　新しいキャプチャをセットアップするには、**New Capture** を選択します。また、既存のバッファを選択して **Settings** をクリックすると、キャプチャ設定を変更、一時停止、クリア、または再開できます。

NAM Traffic Analyzer は Capture Settings ウィンドウ（図 6-3）を表示します。Capture Settings ウィンドウには、キャプチャ名を入力するためのフィールド、および表 6-3 で説明している 4 つのステータス インジケータがあります。

表 6-3　Capture Settings のステータス インジケータ

ステータス インジケータ	説明
Capture Status	現在のキャプチャの状態： • Running：パケット キャプチャが進行中です。 • Paused：パケット キャプチャが一時停止しています。キャプチャされたパケットはバッファに残っていますが、新しいパケットはキャプチャされていません。 • Cleared：キャプチャは（ユーザによって）中止され、バッファはクリアされます。 • Locked：バッファがいっぱいになったため、キャプチャがロックされました。
Packets Captured	キャプチャされ、キャプチャ バッファに保存されたパケットの数。 （注）　キャプチャ バッファがいっぱいで、キャプチャが wrap-when-full モードの場合、新しいパケットが到着すると古いパケットがバッファから破棄されるため、キャプチャされたパケットの数は変動することがあります。
First Started	現在のキャプチャが開始された時刻を示します。必要に応じて何度でもキャプチャを一時停止および再開できます。キャプチャを中止して新しいキャプチャを開始する場合、このフィールドに新しいキャプチャの開始時刻が表示されます。
Buffer	現在のバッファの状態：Empty、Space Available、Full（Wrap）、または Full（Locked）。

図 6-3　Capture Settings



ステップ 3　必要に応じて、Capture Settings フィールド（表 6-4）に情報を入力します。

表 6-4　Capture Settings のフィールド

フィールド	説明	使用法
Capture Name	キャプチャの名前。	キャプチャ名を入力します。
Capture from	パケットのキャプチャ元であるデータ ソース。	リストからエントリを選択します。
Packet Slice Size	キャプチャされたパケットのサイズを制限するために使用する、バイト単位のスライス サイズ。	12 ～ 8192 の数値を入力します。 バッファが小さい場合、できるだけ多くのパケットをキャプチャするには、小さなスライス サイズを使用します。 指定したスライス サイズよりもパケット サイズが大きい場合、パケットはキャプチャ バッファに保存される前に「スライス」されます。たとえば、パケットが 1000 バイトでスライス サイズが 200 バイトの場合、パケットの最初の 200 バイトだけがキャプチャ バッファに保存されます。
Capture to Buffer	オンにすると、キャプチャはバッファに格納されます。	**Buffer Size** および **Wrap when Full** の値を入力します。
Buffer Size	キャプチャ バッファのサイズ（MB 単位）。	1 からプラットフォームの最大値までの数値を入力します。システム メモリが少ない場合は、割り当てられる実際のバッファ サイズが、ここで指定した数値よりも小さくなることがあります。キャプチャを開始すると、このフィールドには、割り当てられた実際のバッファ サイズが表示されます。 **（注）** WS-SVC-NAM-1 デバイスは 125 MB まで、WS-SVC-NAM-2 デバイスは 300 MB まで設定できます。NM-NAM デバイスは 70 MB まで設定できます。
Wrap when Full	オンにすると、バッファ内のデータがバッファ サイズを超えた場合にデータをラップします。	Check Wrap when Full をオンにすると、連続キャプチャがイネーブルになります。 **（注）** バッファがいっぱいの場合は、新しい入力パケット用の空きを作成するために、古いパケット データが削除されます。
Capture to File(s)	オンにすると、キャプチャをファイルに格納します。	**File Size** および **No. Files** の値を入力します。 **（注）** 作業ファイル用に約 400MB の空きディスク容量が予約されます。使用可能なディスク容量が 400MB を下回る場合は、ディスクへのキャプチャ セッションを新たに開始することはできません。
File Size (MB)	各キャプチャ ファイルの最大サイズ。	ファイル サイズは 1 ～ 1000 MB です。
File Location	プルダウン メニューからオプションを選択します。	デフォルトのローカル ディスクを使用するか、または以前に設定したリモート ストレージの場所を選択します。**Admin > System** をクリックし、コンテンツ メニューから Capture Data Storage を選択して、（NFS および iSCSI）リモート ストレージの場所を追加できます。
No. Files	連続キャプチャに使用するファイル数。	ファイル数は、1 ～ 50 です。

表 6-4　Capture Settings のフィールド（続き）

フィールド	説明	使用法
Rotate Files	オンにすると、連続キャプチャでファイルをローテーションします。	リモート ストレージでのみ使用可能です。 リモート ストレージの設定については、P.2-17 の「キャプチャ データ ストレージ」を参照してください。
Capture Filter: Include		Include（包含）フィルタは、フィルタ条件と一致するパケットだけをキャプチャします。
Capture Filter: Exclude		Exclude（排除）フィルタは、フィルタ条件を*除外*するパケットをキャプチャします。

ステップ 4　バッファにキャプチャする場合は、**Capture to Buffer** をオンにし、**Buffer Size** に MB 単位でサイズを入力します。最近のデータを連続してキャプチャする場合は、**Wrap when Full** をオンにします。

このタイプのキャプチャは、最大で Buffer Size に設定されたサイズまでパケット データを格納します。**Wrap when Full** がオフの場合は、データ量がバッファ サイズに達すると、キャプチャは終了します。

ステップ 5　ファイルにキャプチャする場合は、**Capture to File(s)** をオンにして、**File Size** および **No. Files** に値を入力します。

複数のファイルにキャプチャする場合は、ファイル名に拡張子が追加されます。たとえば、キャプチャ名が **CaptureA** の最初のファイルは **CaptureA_1**、2 番目のファイルは **CaptureA_2** といった具合にラベルが付けられます。

ステップ 6　ファイルにキャプチャする場合は、**Rotate Files** をオンにして、最近のパケット データを連続してキャプチャします。

Rotate Files オプションは、リモート ストレージでのみ使用できます。リモート ストレージの設定については、P.2-17 の「キャプチャ データ ストレージ」を参照してください。

（注）　**Rotate Files** オプションを選択している場合に、ファイル数が最大数に達すると、最も古いファイルが上書きされます。たとえば、**No. Files** を 10 に指定し、NAM がキャプチャ データをファイル **CaptureA_10** に書き込んだ場合、次の書き込み時にはファイル **CaptureA_1** が上書きされます。最近のキャプチャを判別するには、各ファイルのタイムスタンプをチェックします。

ステップ 7　Capture Filter ペインで、Include または Exclude をオンにします。

Include（包含）フィルタは、フィルタ条件と一致するパケットだけをキャプチャします。Exclude（排除）フィルタは、フィルタ条件を*除外*するパケットをキャプチャします。

ステップ 8　次のいずれかのチェックボックスをオンにして、該当するフィルタ タイプをイネーブルにします。

- **Address** では、IP、IPIP4、IPv6、GRE.IP、または MAC アドレスのタイプに基づいてトラフィックがフィルタリングされます（P.6-8 の「アドレス フィルタを使用したキャプチャ」を参照してください）。
- **Protocols** では、特定のプロトコルに基づいてトラフィックがフィルタリングされます（P.6-9 の「プロトコル フィルタを使用したキャプチャ」を参照してください）。

- **Ports** では、ポート フィルタが使用されます（P.6-10 の「ポート フィルタを使用したキャプチャ」を参照してください）。
- **Custom Filter** では、カスタマイズしたフィルタが使用されます（P.6-10 の「カスタム フィルタを使用したキャプチャ」を参照してください）。

  カスタム キャプチャ フィルタの作成と編集の詳細については、P.6-21 の「カスタム キャプチャ フィルタ」を参照してください。

ステップ 9　Capture Settings での操作（表 6-5）に示されている操作のいずれかを選択します。

表 6-5　Capture Settings での操作

操作	説明
Start	クリックすると、キャプチャ操作が開始されます。
Pause	クリックすると、キャプチャ操作が一時停止されます。キャプチャ データはキャプチャ バッファに残りますが、新しいデータは格納されません。Start をクリックすると、キャプチャが再開します。
Clear	クリックすると、キャプチャが中止され、キャプチャ バッファがクリアされます。キャプチャ設定を変更する前に、キャプチャ バッファをクリアする必要があります。
Decode	クリックすると、キャプチャ バッファが表示されます。
Close	クリックすると、キャプチャ ウィンドウが閉じられます。

たとえば、111.122 クラス B ネットワークの HTTP および HTTPS パケットだけをキャプチャするには、次の手順を実行します。

ステップ 1　**Inclusive** チェックボックスをオンにします。

ステップ 2　**Address** チェックボックスをオンにします。

ステップ 3　IP ボタンをクリックします。

ステップ 4　**Both Directions** チェックボックスをオンにします。

ステップ 5　Source に `111.122.0.0` と入力します。

ステップ 6　Source Mask に `255.255.0.0` と入力します。

ステップ 7　**Protocol** チェックボックスをオンにします。

ステップ 8　**Shift** キーを押したまま、リストで HTTP と HTTPS をクリックして選択します。

アドレス フィルタを使用したキャプチャ

Address チェックボックスをオンにした場合は、必要に応じて Capture Settings Address Filter ダイアログボックス（表 6-6）に情報を入力します。

（注）　IPIP4 または GRE.IP などのトンネル アドレスでフィルタリングする場合、フィルタは内部または外部 IP ヘッダーのアドレスを照合します。

表 6-6　Capture Settings Address Filter ダイアログボックス

フィールド	説明	使用法
Address	どのアドレスをフィルタリングするかを指定します。	• パケットの送信元 / 宛先 MAC アドレスを使用するには、MAC を選択します。 • パケットの送信元 / 宛先 IP アドレスを使用するには、IP を選択します。 • IP プロトコル 4 経由でトンネルされるものを含む IP アドレスの場合は、IPIP4 を選択します。 • GRE 経由でトンネルされるものを含む IP アドレスの場合は、GRE.IP を選択します。 • IP バージョン 6 を使用するアドレスの場合は、IPv6 を選択します。
Both directions	フィルタが双方向のトラフィックに適用されるかどうかを指定します。	送信元がホスト A で宛先がホスト B の場合、双方向をイネーブルにすると、A から B および B から A のパケットがフィルタリングされます。 送信元がホスト A で宛先が指定されていない場合、双方向をイネーブルにすると、ホスト A へのパケットとホスト A からのパケットの両方がフィルタリングされます。
Source	パケットの送信元アドレス。	• IP、IPIP4、および GRE.IP アドレスの場合は、有効な IPv4 アドレスをドット付きの 4 つの数字列形式 *n.n.n.n*（*n* は 0 ～ 255）で入力します。 • IPv6 アドレスの場合は、有効な IPv6 アドレスを許可された任意の IPv6 アドレス形式で入力します。次の例を参考にしてください。 — 1080::8:800:200C:417A — ::FFF:129.144.52.38 （注）　有効なテキスト表現については、RFC 2373 を参照してください。 • MAC アドレスの場合は、*hh hh hh hh hh hh*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。

表 6-6　Capture Settings Address Filter ダイアログボックス（続き）

フィールド	説明	使用法
Source Mask	送信元アドレスに適用されるマスク。 • Source Mask のビットが 1 に設定されている場合、アドレス内の対応ビットは関連があります。 • Source Mask のビットが 0 に設定されている場合、アドレス内の対応ビットは無視されます。	• IP、IPIP4、および GRE.IP アドレスの場合は、有効な IPv4 アドレスをドット付きの 4 つの数字列形式 *n.n.n.n*（*n* は 0 ～ 255）で入力します。デフォルト（ブランクの場合）は 255.255.255.255 です。 • IPv6 アドレスの場合は、有効な IPv6 アドレスを許可された任意の IPv6 アドレス形式で入力します。IPv6 アドレスのデフォルト マスク（ブランクの場合）は、ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff です。 **（注）** 有効なテキスト表現については、RFC 2373 を参照してください。 MAC アドレスの場合は、*hh hh hh hh hh hh*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。 デフォルトは ff ff ff ff ff ff です。
Destination	パケットの宛先アドレス。	• IP、IPIP4、および GRE.IP アドレスの場合は、有効な IPv4 アドレスをドット付きの 4 つの数字列形式 *n.n.n.n*（*n* は 0 ～ 255）で入力します。デフォルト（ブランクの場合）は 255.255.255.255 です。 • IPv6 アドレスの場合は、有効な IPv6 アドレスを許可された任意の IPv6 アドレス形式で入力します。次の例を参考にしてください。 — 1080::8:800:200C:417A — ::FFF:129.144.52.38 **（注）** 有効なテキスト表現については、RFC 2373 を参照してください。 MAC アドレスの場合は、*hh hh hh hh hh hh*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。 デフォルトは ff ff ff ff ff ff です。
Dest.Mask	宛先アドレスに適用されるマスク。 • Dest.Mask のビットが 1 に設定されている場合、アドレス内の対応ビットは関連があります。 • Dest.Mask のビットが 0 に設定されている場合、アドレス内の対応ビットは無視されます。	• IP、IPIP4、および GRE.IP アドレスの場合は、有効な IPv4 アドレスをドット付きの 4 つの数字列形式 *n.n.n.n*（*n* は 0 ～ 255）で入力します。デフォルト（ブランクの場合）は 255.255.255.255 です。 • IPv6 アドレスの場合は、有効な IPv6 アドレスを許可された任意の IPv6 アドレス形式で入力します。IPv6 アドレスのデフォルト マスク（ブランクの場合）は、ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff です。 **（注）** 有効なテキスト表現については、RFC 2373 を参照してください。 MAC アドレスの場合は、*hh hh hh hh hh hh*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。 デフォルトは ff ff ff ff ff ff です。

プロトコル フィルタを使用したキャプチャ

Protocol チェックボックスをオンにした場合は、キャプチャする 1 つ以上のプロトコルをドロップダウン リストから選択します。

複数のプロトコルを選択するには、Shift キーを押した状態でクリックします。

ポート フィルタを使用したキャプチャ

Capture Settings ウィンドウで、Ports チェックボックスをオンにして、1 つのポートを入力するか、または複数のポートをカンマで区切って入力します。

カスタム フィルタを使用したキャプチャ

ステップ 1　**Custom** チェックボックスをオンにします。

（注） Custom Filter チェックボックスをオンにすると Address Filter チェックボックスおよび Protocol Filter チェックボックスがディセーブルになり、Address Filter チェックボックスまたは Protocol Filter チェックボックスをオンにすると Custom Filter チェックボックスがディセーブルになります。

ステップ 2　リストから、1 つまたは複数のカスタム キャプチャ フィルタを選択します。複数のフィルタを選択するには、Shift キーを押した状態でクリックします。複数のカスタム フィルタを選択した場合、フィルタの条件は論理和がとられます（いずれかに一致）。

（注） リストが空の場合は、P.6-21 の「カスタム キャプチャ フィルタの作成」でカスタム キャプチャ フィルタの作成方法を参照してください。

ステップ 3　選択したカスタム キャプチャ フィルタを表示または編集するには、**Custom Filters > Capture Filters** の順に選択します。

（このステップはオプションです。）

自動キャプチャ（アラームによってトリガーされるキャプチャ）の使用

アラームによって自動的に開始または中止（一時停止）されるキャプチャを設定できます。**Capture > Buffer** の順に選択して Automatic Capture 設定を構成してから、**Setup > Alarms** の順に選択し、キャプチャをトリガーするアラームを設定します。

開始と停止という 2 つのタイプのキャプチャ トリガーがあります。一度に設定できるキャプチャ トリガーは 1 つだけです。アラームの設定の詳細については、P.3-56 の「アラームしきい値の設定」を参照してください。

開始キャプチャ トリガーの場合、最初にキャプチャ バッファを一時停止状態にする必要があります。バッファがクリアされているか実行中の場合、開始キャプチャ トリガーは動作しません。

停止キャプチャ トリガーの場合、最初にキャプチャ バッファが実行中になっている必要があります。バッファが一時停止またはクリアされている場合、停止トリガーは動作しません。最適な結果を得るためには、バッファ モードを Wrap when full に設定することをお勧めします。

パケット デコード情報の表示

バッファにパケットをいくつかキャプチャした後、Packet Decoder を使用してパケットの内容を表示できます。

Packet Decoder ウィンドウは、次の 4 つの部分で構成されます。

- Packet Decoder の操作
- Packet browser ペイン
- プロトコル デコード（P.6-14 の「詳細なプロトコル デコード情報の表示」を参照）
- パケットの 16 進数ダンプ

パケット デコード情報を表示するには、次の手順を実行します。

ステップ 1　**Capture > Buffers** または **Capture > Files** を選択します。

ステップ 2　キャプチャ バッファまたはファイルを選択し、**Decode** をクリックします。

Packet Decoder ウィンドウは、図 6-4 のように表示されます。

図 6-4　Packet Decoder ウィンドウ

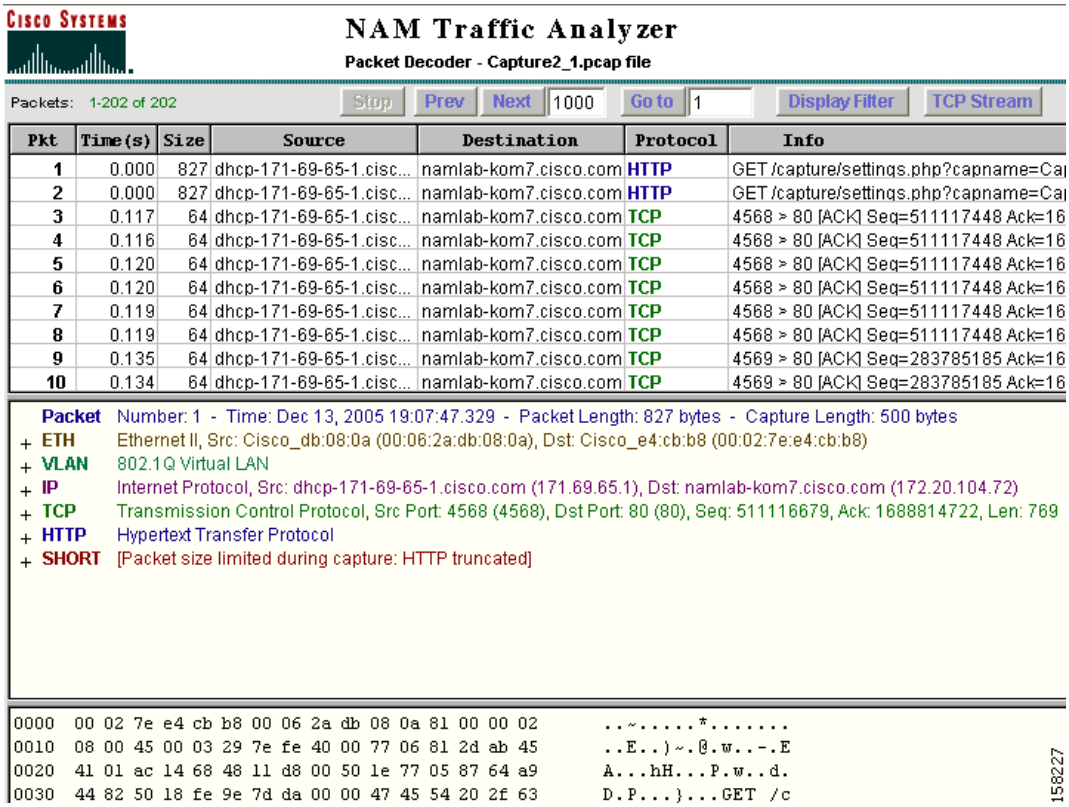


表 6-7 に、Packet Decoder の操作を示します。

表 6-7　Packet Decoder の操作

ボタン	説明
Stop	パケットのロードを中止します。
Prev	NAM からの直前のパケット ブロックをロードおよびデコードします。
Next	NAM からの次のパケット ブロックをロードおよびデコードします。
Go To	指定したパケット番号から始まるパケット ブロックをロードおよびデコードします。
Display Filter	Display Filter ダイアログを起動します。「Packet Decoder に表示されるパケットのフィルタリング」を参照してください。
TCP Stream	選択した TCP パケットの TCP ストリームに従います。

表 6-8 に、Packet Browser ペインに表示される情報を示します。

表 6-8　Packet Browser

フィールド	説明
Pkt	キャプチャ シーケンスの番号順に表示されたパケット番号。デコード（表示）フィルタがアクティブな場合、パケット番号は連続しないことがあります。
Time	表示された最初のパケット（バッファ内の最初のパケットではありません）に関して、パケットがキャプチャされた時間。 （注）　絶対時間を調べるには、Detail ウィンドウを参照します。
Size	パケットのサイズ（バイト単位）。
Source	パケットの送信元。ホスト名、IP、IPX、または MAC アドレスとして表示されることがあります。 （注）　IP アドレスのホスト名解決をオンまたはオフにするには、Setup タブをクリックして、Preferences でこの設定を変更します。
Destination	パケットの宛先。ホスト名、IP、IPX、または MAC アドレスとして表示されることがあります。
Protocol	パケットのトップ レベルのプロトコル。
Info	パケットの内容に関する短いテキスト情報。

Packet Decoder でのパケットの表示

パケット ブラウザを使用して、キャプチャしたパケットのリストを表示したり、次のことを実行したりできます。

- プロトコル、IP アドレス、MAC アドレス、カスタム表示フィルタによるフィルタリング
- **Next**、**Previous**、および **Go To** ボタンを使用したキャプチャ バッファからのパケットのロード

（注）　これらの機能を使用するには、キャプチャを一時停止または停止する必要があります。

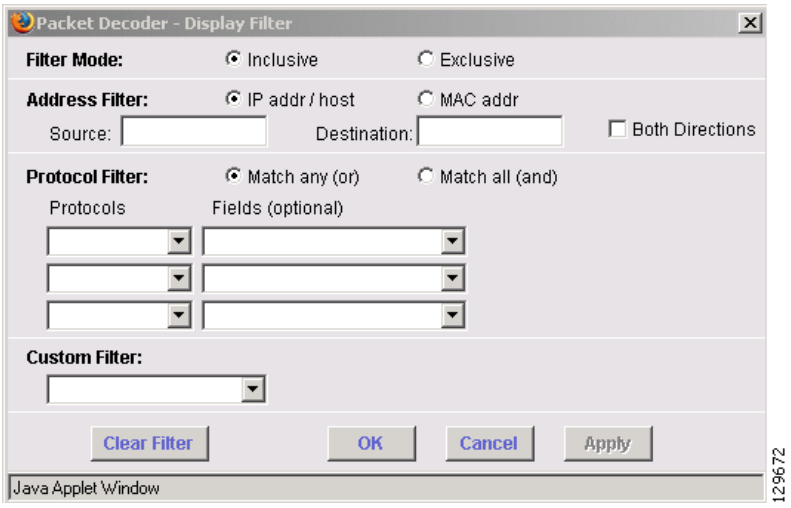
Packet Decoder に表示されるパケットのフィルタリング

Packet Decoder に表示されたパケットをフィルタするには、次の手順を実行します。

ステップ 1　Packet Decoder ウィンドウで、Display Filter ボタンをクリックします。

Packet Decoder - Display Filter ウィンドウ（図 6-5）が表示されます。

図 6-5　Packet Decoder - Display Filter ウィンドウ



ステップ 2　次の操作を行います。

- **Filter Mode** について次のいずれかを選択します。
  - **Inclusive** を選択すると、条件に一致するパケットが表示されます。
  - **Exclusive** を選択すると、条件に一致しないパケットが表示されます。
- **Address Filter** について次のように選択します。
  - IP アドレスの場合は **IP address** フィルタ。
  - MAC アドレスの場合は **MAC Address** フィルタ。
  - **Source** では、送信元アドレスを指定できます。指定する必要のない場合はブランクのままにすることができます。
  - **Destination** では、宛先アドレスを指定できます。指定する必要のない場合はブランクのままにすることができます。
  - **Both Directions** をオンにすると、どちらの方向に移動するパケットも照合できます。
- **Protocol Filter** について次のように定義します。
  - いずれかのプロトコルまたはフィールドに一致するパケットを表示するには、**Match any** を選択します。

  または
  - すべてのプロトコルまたはフィールドに一致するパケットを表示するには、**Match all** を選択します。
  - **Protocols** リストからプロトコルを選択します。

（注）　プロトコル名の先頭の数文字を入力して、目的のプロトコルに直接移動できます。タイプミスをした場合にリセットするには、**Esc** キーまたは **Space** キーを押します。

　　－　必要に応じて、Fields リストからプロトコルのフィールドを選択し、フィールド値を指定します。

- **Custom Filter** について選択します。カスタム表示フィルタの設定方法については、「カスタム表示フィルタ」を参照してください。

ステップ 3　プロトコル名、IP アドレス、MAC アドレス、照合テキスト、またはカスタム デコード フィルタを指定します。

ステップ 4　**Filter** をクリックします。

ステップ 5　フィルタ条件を*除外*するパケットを表示するには、Filter ボタンの横の **exclusive** チェックボックスをオンにします。

詳細なプロトコル デコード情報の表示

詳細なプロトコル情報を表示するには、次の手順を実行します。

ステップ 1　詳細情報を必要とするパケット番号を強調表示します。

パケットに関する詳細情報が、Protocol Decode ペインおよびウィンドウ下部の 16 進数ダンプ ペインに表示されます。

（注）　Protocol Decode ペインで詳細を強調表示すると、対応するバイトが下の 16 進数ダンプ ペインで強調表示されます。

ステップ 2　情報を調べるには、下部ペインのスクロール バーを使用します。

ヒント
- プロトコルは、Packet Browser および Protocol Decode ペインの両方で色分けされます。
- プロトコル情報を縮小および展開するには、Protocol Decode ペインでプロトコル名をクリックします。
- ペインのサイズを調整するには、ペイン フレームをクリックし、上または下にドラッグします。

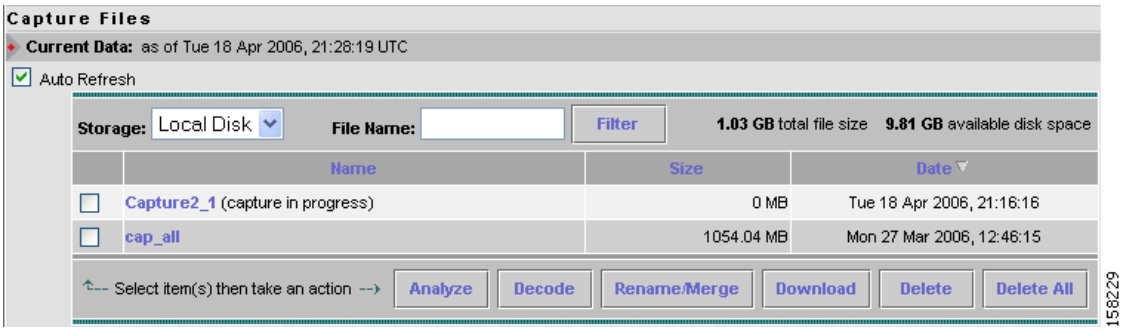
ファイル

保存済みのキャプチャ ファイルを分析、デコード、マージ、ダウンロード、または削除するには、Files オプションを使用します。キャプチャ バッファをファイルに保存する方法については、P.6-2 の「バッファ」および表 6-2 を参照してください。ファイルは、Sniffer **.enc** ファイル形式でダウンロードできます。

Capture > **Files** を選択すると、Capture Files ウィンドウ（図 6-6）が表示されます。

（注）　Auto Refresh チェックボックスをオンにすると、Capture Files ウィンドウが 60 秒ごとに自動的にリフレッシュされます。

図 6-6　Capture Files ウィンドウ



Capture Files ウィンドウには、次のオプションがあります。

- プルダウン リストからストレージの場所を選択すると、その場所にあるキャプチャ ファイルが表示されます。リモート ストレージのサブディレクトリは、NAM がそれらのリモート ディレクトリに対してフル アクセス権を持つ場合にだけ一覧されます。
- キャプチャを選択して **Analyze** をクリックすると、ファイルのパケットが表示されます。
- キャプチャを選択して **Decode** をクリックすると、ファイルのパケットが表示されます。
- **Rename/Merge** をクリックすると、ファイルのパケットがマージされます。ファイルのパケットは、古い順にマージされます。
- **Download** をクリックすると、ファイルが Sniffer **.enc** ファイル形式でコンピュータにダウンロードされます。
- **Delete** または **Delete All** をクリックすると、ファイルが削除されます。

キャプチャ ファイルの分析

Capture Files ウィンドウの Analyze ボタンをクリックすると、キャプチャ期間のトラフィック レート（バイト / 秒）、ネットワーク トラフィックに関連付けられたホスト、会話、およびアプリケーションのリストを含むさまざまな統計情報を取得できます。図 6-7 に、Capture Analysis ウィンドウの例を示します。

このウィンドウでは、特定のネットワーク トラフィック セットのより詳細な表示にドリル ダウンすることもできます。**Traffic over Time** グラフの上のペインでは、**From:** および **To:** フィールドにグラフに示されている時間が表示されます。また、Protocol フィールド、Host/subnet フィールド、および **Drill-Down** ボタンもあります。

Traffic over Time グラフの各スライスには、キャプチャ ファイルの Granularity に設定された一定時間のトラフィック量が表示されます。

From: および **To:** フィールドに時間を入力し、**Drill-Down** をクリックすると、特定の時間に関するより詳細な情報を表示できます。また、特定の **プロトコル**または**ホスト / サブネット** アドレスについてドリル ダウンすることもできます。

図 6-7　Capture Statistical Analysis ウィンドウ

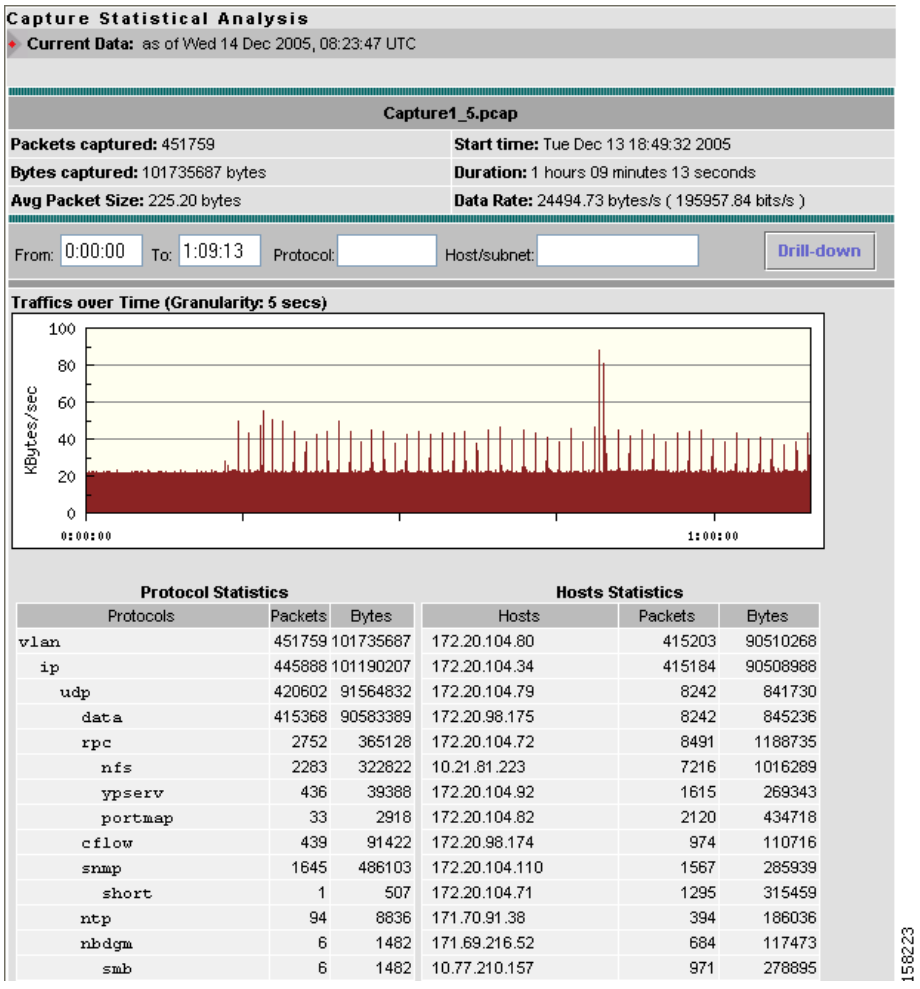


表 6-9 に、Capture Analysis ウィンドウのさまざまな領域を示します。

表 6-9　Capture Analysis ウィンドウのフィールド

フィールド	説明
Capture Overview	キャプチャされたパケット数、キャプチャされたバイト数、平均パケット サイズ、キャプチャの開始時間、キャプチャ期間、データ転送レート（バイト / 秒とビット / 秒の両方）を含む、表示されたキャプチャの要約を示します。
Traffic over Time	ネットワーク トラフィックのグラフィック イメージ（KB/ 秒）を表示します。
Protocol Statistics	プロトコルごとに、転送されパケット数とバイト数を表示します。
Hosts Statistics	ホスト アドレスごとに、転送されパケット数とバイト数を表示します。

キャプチャ ファイルのデコード

キャプチャ ファイルのデコードについては、P.6-11 の「パケット デコード情報の表示」で説明しています。

キャプチャ ファイルの名前の変更とマージ

Rename/Merge ボタンを使用して、単一のキャプチャ ファイルの名前を変更したり、複数のキャプチャ ファイルを 1 つのファイルにマージしたりできます。

キャプチャ ファイルの名前の変更

キャプチャ ファイルの名前を変更するには、次の手順を実行します。

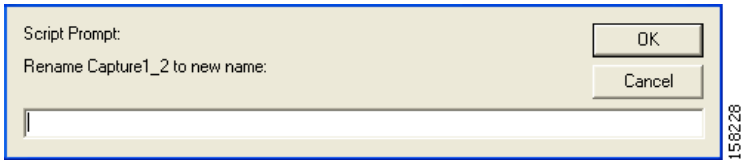
ステップ 1　**Capture** > **Files** を選択します。

ステップ 2　キャプチャのリストからキャプチャ ファイルを選択します。

ステップ 3　**Rename/Merge** をクリックします。

ダイアログボックスが表示され、選択したキャプチャ ファイルの新しい名前を入力するように要求されます。

図 6-8　Rename Capture File ダイアログボックス



ステップ 4　キャプチャ ファイルの新しい名前を入力し、**OK** をクリックします。

キャプチャ ファイルのマージ

複数のキャプチャ ファイルを 1 つのキャプチャ ファイルにマージするには、次の手順を実行します。

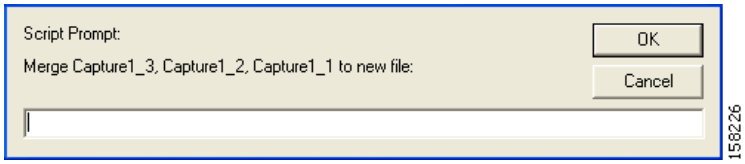
ステップ 1　**Capture** > **Files** を選択します。

ステップ 2　キャプチャのリストから、2 つ以上のキャプチャ ファイルを選択します。

ステップ 3　**Rename/Merge** をクリックします。

ダイアログボックスが表示され、マージしたキャプチャ ファイルの新しい名前を入力するように要求されます。

図 6-9　Merging Capture Files ダイアログボックス



ステップ 4　マージしたキャプチャ ファイルの名前を入力し、**OK** をクリックします。

キャプチャ ファイルは、最も古いものから最新のものへ、タイムスタンプの順番でマージされます。

キャプチャ ファイルのダウンロード

次に、キャプチャ ファイルをコンピュータにダウンロードする手順を示します。1 度に 1 つのキャプチャ ファイルしかダウンロードできません。

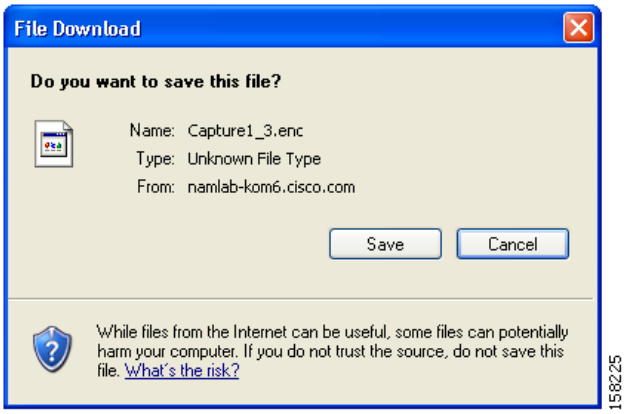
ステップ 1　**Capture** > **Files** を選択します。

ステップ 2　キャプチャのリストからキャプチャ ファイルを選択します。

ステップ 3　**Download** をクリックします。

File Download ダイアログボックスが表示され、「**Do you want to save this file?**」というファイルの保存を確認するメッセージが表示されます。

図 6-10　Download Capture File ダイアログボックス



ステップ 4　**Save** をクリックします。

Save As ダイアログボックスが開きます。ここで、ファイルの名前を変更し、選択した場所にそのファイルを保存できます。

キャプチャ ファイルの削除

キャプチャ ファイルを削除するには、次の手順を実行します。

ステップ 1　**Capture** > **Files** を選択します。

ステップ 2　キャプチャのリストからキャプチャ ファイルを選択します。

ステップ 3　**Delete** をクリックします。

ダイアログボックスが表示され、「**Delete the following file(s)?**」というファイルの削除を確認するメッセージとファイル名が表示されます。

ステップ 4　ファイルを削除するには **OK** をクリックします。または、ファイルをそのまま残すには **Cancel** をクリックします。

すべてのキャプチャ ファイルの削除

1 度にすべてのキャプチャ ファイルを削除するには、次の手順を実行します。

ステップ 1　**Capture** > **Files** を選択します。

ステップ 2　キャプチャのリストからキャプチャ ファイルを選択します。

ステップ 3　**Delete All** をクリックします。

ダイアログボックスが表示され、「**Delete all capture file(s)?**」という全キャプチャ ファイルの削除を確認するメッセージが表示されます。

ステップ 4　すべてのファイルを削除するには **OK** をクリックします。または、ファイルをそのまま残すには **Cancel** をクリックします。

カスタム キャプチャ フィルタ

カスタム キャプチャ フィルタを使用すると、データのキャプチャ時に不必要な情報をすべて無視する特別なフィルタを作成および保存できます。

データのキャプチャ時にカスタム フィルタを使用する方法については、P.6-10 の「カスタム フィルタを使用したキャプチャ」を参照してください。

カスタム キャプチャ フィルタの設定および管理のヘルプについては、次のトピックを参照してください。

カスタム キャプチャ フィルタの作成

カスタム キャプチャ フィルタを作成するには、次の手順を実行します。

ステップ 1　**Capture** > **Custom Filters** を選択します。

Custom Capture Filters ダイアログボックスが表示されます。

ステップ 2　**Create** をクリックします。

Custom Capture Filter ダイアログボックス（表 6-10）が表示されます。

ステップ 3　必要に応じて、各フィールドに情報を入力します。

表 6-10　Custom Capture Filter ダイアログボックス

フィールド	説明および使用法
Filter Name	新しいフィルタの名前を入力します。
Description	フィルタの短い説明。 1 ～ 35 文字の説明を入力します。
Protocol	パケットと照合するプロトコル。 ドロップダウン リストからカプセル化を選択して、プロトコルを選択します。
Data	パケットと照合するデータ パターン。Offset フィールドを使用して、データをチェックする開始位置を指定します。 *hh hh hh ...*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。 たとえば、10 進数の *15* を指定する場合は、16 進数の *0f* を使用します。10 進数 *255* の場合は、16 進数 *ff* を使用します。10 進数 *16* の場合は、16 進数 *10* を使用します。その他の例については、P.6-23 の「カスタム キャプチャ フィルタ式作成のヒント」を参照してください。 使用しない場合は、ブランクにします。 パケットが短すぎて照合するデータが足りない場合、パケットは照合に失敗します。

表 6-10　Custom Capture Filter ダイアログボックス（続き）

フィールド	説明および使用法
Data Mask	データ照合に適用されるマスク。 *hh hh hh ...*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。 すべてのデータ ビットが関連する場合は、ブランクにします。 Data Mask のビットが 1 に設定されている場合、パケット内の対応ビットは照合アルゴリズムに関連があります。 Data Mask のビットが 0 に設定されている場合、パケット内の対応ビットは無視されます。 Data Mask を指定しない場合、または Data フィールドよりも短い場合は、Data フィールドの長さになるまで Data Mask に「1」ビットが埋め込まれます。たとえば、Data フィールドに 4 バイト値を入力し、Data Mask フィールドをブランクにした場合は、Data Mask に *ff ff ff ff* を指定したのと同じになります。
Data Not Mask	反転データ照合に適用されるマスク。 *hh hh hh ...*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。 反転データ照合を行わない場合は、ブランクにします。 0 に設定された（または指定されていない）Data Not Mask 内のビットの場合、パケット内の関連ビットは、Data フィールド内の対応ビットと一致している必要があります。 1 に設定された Data Not Mask のビットの場合、パケット内の少なくとも 1 つの関連ビットは Data フィールド内の対応ビットと異なっている必要があります。 Data Not Mask を指定しない場合、または Data フィールドよりも短い場合は、Data フィールドの長さになるまで Data Not Mask に「0」ビットが埋め込まれます。
Offset	パケット データ照合を開始するオフセット（Base からのバイト数）を 10 進数で入力します。 このオフセットは、Data、Data Mask、および Data Not Mask の各フィールドに適用されます。
Base	オフセットを計算するためのベースとして、absolute またはプロトコルを選択します。 absolute を選択した場合、オフセットはパケットの絶対開始位置（イーサネット フレームの先頭）から計算されます。WS-SVC-NAM-1 および NAM-2 デバイスのオフセットを計算するときは、802.1q ヘッダーを考慮する必要があります。 プロトコルを選択した場合、オフセットはパケットのプロトコル部分の先頭から計算されます。パケットにプロトコルが含まれていない場合、パケットはこの照合に失敗します。
Status	パケットと照合するステータス。 0 ～ 65535 の数値を入力します。不要な場合はブランクにします。 イーサネット パケット キャプチャの場合、ステータス ビットは次のとおりです。 ビット 0 : 1518 オクテットよりも長いパケット ビット 1 : 64 オクテットよりも短いパケット ビット 2 : CRC またはアラインメント エラー たとえば、イーサネット フラグメントは 6 のステータス値（ビット 1 と 2 のセット）。

表 6-10　Custom Capture Filter ダイアログボックス（続き）

フィールド	説明および使用法
Status Mask	ステータス照合に適用されるマスク。0 ～ 65535 の数値を入力します。すべてのステータス ビットが関連する場合は、ブランクにします。 Status Mask のビットが 1 に設定されている場合、パケット ステータス内の対応ビットは照合アルゴリズムに関連があります。 Status Mask ビットが 0 に設定されている場合、パケット ステータス内の対応ビットは無視されます。 Status Mask を指定しない場合、または Status フィールドよりも短い場合は、Status フィールドの長さになるまで Status Mask に「1」ビットが埋め込まれます。
Status Not Mask	反転ステータス照合に適用されるマスクとして、0 ～ 65535 の数値を入力します。 反転ステータス照合を行わない場合は、ブランクにします。 0 に設定された（または指定されていない）Status Not Mask 内のビットの場合、パケットの関連ステータス ビットは、Status フィールド内の対応ビットと一致している必要があります。 1 に設定された Status Not Mask のビットの場合、ステータス パケットの少なくとも 1 つの関連ビットは Status フィールド内の対応ビットと異なっている必要があります。 Status Not Mask を指定しない場合、「0」ビットが埋め込まれます。

ステップ 4　ファイルを作成するには、**Apply** をクリックします。または、変更を取り消すには、**Reset** をクリックします。

カスタム キャプチャ フィルタ式作成のヒント

TOS 値は、IP ヘッダーのバイト 1（2 番目のバイト）に保存されます。16 の TOS 値（0x10）を持つ IP パケットを照合するには、次のように入力します。

Data：10
Offset：1
Base：IP

Data Mask に何も指定されていない場合、有効な値は *ff* です。

IP パケットの送信元アドレスは、IP ヘッダーのバイト 12 ～ 15 に保存されます。15.16.17.18 の送信元アドレスを持つ IP パケットを照合するには、次のように入力します。

Data：0f 10 11 12
Offset：12
Base：IP

15.*.*.18 の送信元アドレスを持つ IP パケット（* は 0 ～ 255 の任意の数値）を照合するには、次のように入力します。

Data：0f 00 00 12
Data Mask：ff 00 00 ff
Offset：12
Base：IP

送信元アドレスが 15.16.17.18、宛先アドレスが 15.16.17.19 と異なる IP アドレスで照合するには、次のように入力します。

Data：f0 10 12 12 0f 10 11 13
Data Mask：ff ff ff ff ff ff ff ff
Data Not Mask：00 00 00 00 00 00 00 00
Offset：12
Base：IP

カスタム キャプチャ フィルタの編集

カスタム キャプチャ フィルタを編集するには、次の手順を実行します。

ステップ 1　**Capture** > **Custom Filters** を選択します。

Custom Capture Filters ダイアログボックスが表示されます。

ステップ 2　編集するフィルタを選択して、**Edit** をクリックします。

Custom Capture Filter ダイアログボックス（表 6-10 を参照）が表示されます。

ステップ 3　必要に応じて、各フィールドに情報を入力します。

ステップ 4　次のいずれかを実行します。

- 変更を適用するには、**Apply** をクリックします。
- 変更を取り消すには、**Reset** をクリックします。

カスタム キャプチャ フィルタの削除

カスタム キャプチャ フィルタを削除するには、次の手順を実行します。

ステップ 1　**Capture** > **Custom Filters** を選択します。

Custom Capture Filters ダイアログボックスが表示されます。

ステップ 2　削除するフィルタを選択して、**Delete** をクリックします。

ステップ 3　確認のダイアログボックスで、次のいずれかを選択します。

- フィルタを削除するには、**OK** をクリックします。
- 取り消すには、**Cancel** をクリックします。

カスタム表示フィルタ

カスタム表示フィルタを使用して、カスタマイズしたフィルタを作成および保存すると、Decode ウィンドウで使用して表示するパケットを制限できます。

カスタム表示フィルタの設定および管理のヘルプについては、次のトピックを参照してください。

- カスタム表示フィルタの作成（P.6-25）
- カスタム表示フィルタの編集（P.6-28）
- カスタム表示フィルタの削除（P.6-28）

カスタム表示フィルタの作成

カスタム表示フィルタを作成するには、次の手順を実行します。

ステップ 1　**Capture** > **Custom Filters** を選択します。

ステップ 2　コンテンツで **Display Filters** をクリックします。

Custom Display Filters ダイアログボックスが表示されます。

ステップ 3　**Create** をクリックします。

Custom Decode Filter ダイアログボックス（表 6-11）が表示されます。

ステップ 4　必要に応じて、各フィールドに情報を入力します。

表 6-11　Custom Decode Filter ダイアログボックス

フィールド	説明	使用法
Filter Name	キャプチャ フィルタの名前。	作成するフィルタの名前を入力します。
Description	キャプチャ フィルタの説明。	フィルタの説明を入力します。
Protocol	パケットと照合するプロトコル。	リストからプロトコルを選択します（プロトコルに関係なくすべてのパケットを照合する場合は **All** を選択します）。
Address（MAC または IP）	MAC アドレスまたは IP アドレスのどちらでフィルタリングするかを指定します。	パケットの送信元または宛先 MAC アドレスを使用してフィルタリングするには、MAC を選択します。 パケットの送信元または宛先アドレスを使用してフィルタリングするには、IP を選択します。
Both Directions	フィルタが双方向のトラフィックに適用されるかどうかを指定します。	送信元がホスト A で宛先がホスト B の場合、双方向をイネーブルにすると、A から B および B から A のパケットがフィルタリングされます。 送信元がホスト A で宛先が指定されていない場合、双方向をイネーブルにすると、ホスト A へのパケットとホスト A からのパケットの両方がフィルタリングされます。

表 6-11　Custom Decode Filter ダイアログボックス（続き）

フィールド	説明	使用法
Source	パケットの送信元アドレス。	IP アドレスの場合は、*n.n.n.n*（*n* は 0 ～ 255）または *n.n.n.n/s*（*s* はサブネット マスク 0 ～ 32）を入力します。 MAC アドレスの場合は、*hh hh hh ...*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。
Destination	パケットの宛先アドレス。	IP アドレスの場合は、*n.n.n.n*（*n* は 0 ～ 255）または *n.n.n.n/s*（*s* はサブネット マスク 0 ～ 32）を入力します。 MAC アドレスの場合は、*hh hh hh hh hh hh*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。
Offset	パケット データ照合を開始する Base からのオフセット（バイト数）。	10 進数を入力します。
Base	オフセットが計算されるベース。 absolute を選択した場合、オフセットはパケットの絶対開始位置（たとえば、イーサネット フレームの先頭）から計算されます。 プロトコルを選択した場合、オフセットはパケットのプロトコル部分の先頭から計算されます。パケットにプロトコルが含まれていない場合、パケットはこの照合に失敗します。	**absolute** またはプロトコルを選択します。
Data Pattern	パケットと照合するデータ。	*hh hh hh ...*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。 使用しない場合は、ブランクにします。
Filter Expression	複雑なフィルタ条件を設定する高度な機能。 最も単純なフィルタにより、プロトコルまたはフィールドの存在をチェックできます。たとえば、単純なフィルタ式 **ipx** を使用して、IPX プロトコルを含むすべてのパケットを表示できます。	P.6-27 の「カスタム デコード フィルタ式作成のヒント」を参照してください。

ステップ 5　次のいずれかを実行します。

- フィルタを作成するには、**Apply** をクリックします。
- 変更を取り消すには、**Reset** をクリックします。

カスタム デコード フィルタ式作成のヒント

表 6-12 に示されている論理演算子および比較演算子を使用して、カスタム デコード フィルタ式を構築できます。

表 6-12　論理演算子と比較演算子

演算子	意味
and	論理積
or	論理和
xor	排他的論理和
not	論理否定
==	等しい
!=	等しくない
>	不等号（大なり）

カッコ内で部分式をグループ化することもできます。フィルタ式では次のフィールドを使用できます。

フィールド	フィルタ基準	フォーマット
eth.addr eth.src eth.dst	MAC アドレス	*hh hh hh hh hh hh*（h は 0 ～ 9 または a ～ f の 16 進数）。
ip.addr ip.src ip.dst	IP アドレス	*n.n.n.n* または *n.n.n.n/s*（n は 0 ～ 255 の数値、s は 0 ～ 32 のハイフンを含まないホスト名）。
tcp.port tcp.srcport tcp.dstport	TCP ポート番号	0 ～ 65535 の 10 進数。
udp.port udp.srcport udp.dstport	UDP ポート番号	0 ～ 65535 の 10 進数。
protocol	プロトコル	Custom Decode Filter ダイアログボックスの Protocol リストをクリックして、フィルタリングできるプロトコルのリストを確認します。
protocol [*offset*:*length*]	プロトコルのデータ パターン	*hh:hh:hh:hh...*（hh は 0 ～ 9 または a ～ f の 16 進数）。 *offset* および *length* は 10 進数。 *offset* は 0 から開始し、パケットの *protocol* 部分の先頭と関連しています。
frame.pkt_len	パケット長	パケット長を表す 10 進数。切り捨てられたキャプチャ パケット長ではありません。

カスタム デコード フィルタ式の例

- 111.122.133.144 からの SNMP パケットを照合するには、次のように入力します。

```
snmp and (ip.src == 111.122.133.144)
```

- 111.122 クラス B ネットワークからの IP パケットを照合するには、次のように入力します。

```
ip.addr == 111.122.0.0/16
```

- ポート 80 への TCP パケットおよびポート 80 からの TCP パケットを照合するには、次のように入力します。

  ```
  tcp.port == 80
  ```

- TOS 値は、IP ヘッダーのバイト 1（2 番目のバイト）に保存されます。16 の TOS 値（0x10）を持つ IP パケットを照合するには、次のように入力します。

  ```
  ip[1:1] == 10
  ```

- TCP 確認応答番号は、TCP ヘッダーのバイト 8 ～ 11 に保存されます。確認応答番号 12345678（0xBC614E）を持つ TCP パケットを照合するには、次のように入力します。

  ```
  tcp[8:4] == 00:BC:61:4E
  ```

（注）　Custom Decode Filter ダイアログボックスでは、フィルタ式を他のフィールドと組み合せて使用できます。この場合、フィルタ式は他の条件との論理積がとられます。
無効または矛盾するフィルタ式では、パケットは照合されません。

カスタム表示フィルタの編集

カスタム表示フィルタを編集するには、次の手順を実行します。

ステップ 1　**Capture** > **Custom Filters** を選択します。

ステップ 2　コンテンツで **Display Filters** をクリックします。

Custom Display Filters ダイアログボックスが表示されます。

ステップ 3　編集するフィルタを選択して、**Edit** をクリックします。

ステップ 4　必要に応じて、各フィールドの情報を変更します。

ステップ 5　次のいずれかを実行します。

- 変更を適用するには、**Apply** をクリックします。
- 変更を取り消すには、**Reset** をクリックします。

カスタム表示フィルタの削除

カスタム表示フィルタを削除するには、次の手順を実行します。

ステップ 1　**Capture** > **Custom Filters** を選択します。

ステップ 2　コンテンツで **Display Filters** をクリックします。

Custom Display Filters ダイアログボックスが表示されます。

ステップ 3　削除するフィルタを選択して、**Delete** をクリックします。

ステップ 4　確認のダイアログボックスで、次のいずれかを選択します。

- フィルタを削除するには、**OK** をクリックします。
- 取り消すには、**Cancel** をクリックします。